

MA1100T Quick Notes

§1 Logic

1.1 Statement vs. Proposition vs. Predicate

- A **statement** is a sentence.
- A **proposition** is a statement that is either true or false, but not both.
- A **predicate** is an assignment of truth values to elements of some domain.

1.2 Implications

“On Wednesdays, we wear pink.” – *Mean Girls*

Denoted as $p \rightarrow q$, if it is Wednesday today, then I should probably wear pink. If it is not Wednesday, it doesn't mean I cannot wear pink, so we have

| p | q | $p \rightarrow q$ |
|-----|-----|-------------------|
| 0 | 1 | 1 |

Moreover, $p \rightarrow q \equiv \neg p \vee q$.

1.3 Logical Equivalence

- Two propositional formulas are **logically equivalence** if \forall assignment of truth values of propositions, they have the same truth value.
- Two propositional formulas are **not logically equivalence** if \exists assignment of truth values of propositions, they have different truth values.

1.4 If and only if

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

| p | q | $p \leftrightarrow q$ |
|-----|-----|-----------------------|
| 1 | 1 | 1 |
| 1 | 0 | 0 |
| 0 | 1 | 0 |
| 0 | 0 | 1 |

1.4.1 Necessity and Sufficiency

- If $p \rightarrow q$ then p is **sufficient** for q .
- If $p \leftarrow q$ then p is **necessary** for q .

Example (SJTU Mathematics Contest 2023)

If α : “The equation of a hyperbola is $x^2 - y^2 = a^2$, $a > 0$ ” and β : “The asymptotes of this hyperbola form an angle of $\pi/2$ ”.

| α | β | α implies β ? | β implies α ? |
|----------|---------|--|--|
| 1 | 1 | True | False since $(x-1)^2 - y^2 = a^2$ also works |
| 1 | 0 | False since β is true | False since the angle equals $\pi/2$ |
| 0 | 1 | True, consider $(x-1)^2 - y^2 = a^2$ | False since $(x-1)^2 - y^2 = a^2$ also works |
| 0 | 0 | True, consider $x^2 - 4y^2 = a^2$ and $\theta = 52.13^\circ$ | True, if $\theta \neq \pi/2$, the equation doesn't have to be $x^2 - y^2 = a^2$ |

As we can see, “ α implies β ” is tally to “ $\alpha \rightarrow \beta$ ” but “ β implies α ” does not tally to “ $\beta \rightarrow \alpha$ ” so for β , α is **sufficient** but not **necessary**.

1.5 Tautology & Contradiction

- If $F_1 \equiv F_2$, then $F_1 \leftrightarrow F_2$ is a **tautology**.
- If $F_1 \not\equiv F_2$, then $F_1 \leftrightarrow F_2$ is a **contradiction**.

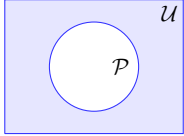
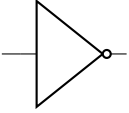
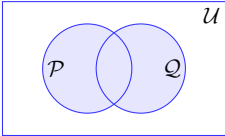
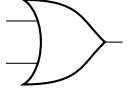
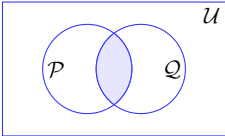
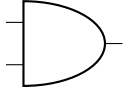
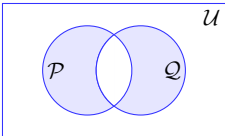
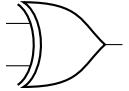
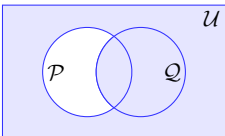
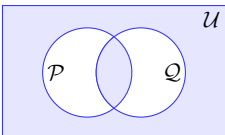
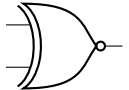
1.6 Useful Denial

F_2 is a **useful denial** of F_1 iff $F_1 \equiv \neg F_2$.

1.7 Boolean Algebra in Words

- $p \rightarrow q$: shown in §1.2
- $p \wedge \neg p$ is a contradiction: Nothing can be both true and false at the same time.
- $p \vee \neg p$ is a tautology: Something must either be true or false right? Hence “to be or not to be” is true.
- $\neg(P \vee Q) \equiv (\neg P) \wedge (\neg Q)$: Let say if I ask you: “Tea or coffee?”. If you want tea but not coffee, then P is true and Q is false, negating lets you drink coffee but not tea, you only drank coffee in the end.
- $\neg(\forall x)(P(x)) \equiv (\exists x)(\neg P(x))$: I don't drink coffee every day, I drank tea on Wednesday.
- $\neg(\exists x)(P(x)) \equiv (\forall x)(\neg P(x))$: Haha you can't find me drinking coffee for all days – I drank tea every day.

1.8 Boolean, Set Theory, Bitwise Operations, Logic Gates

| Boolean | Set Theory | Bitwise | Logic Gates |
|-----------------------|--|---|---|
| $\neg p$ |  <p>p^c</p> <p>Complement</p> | $\text{NOT } x = (2^{\lfloor \log_2 x \rfloor + 1} - 1) - x$ $\text{NOT } 10110101 = 01001010$ |  |
| $p \vee q$ |  <p>$p \cup q$</p> <p>Union</p> | $101101 \text{ OR } 011001 = 111101$ $\begin{array}{r} 101101 \\ \text{OR } 011001 \\ \hline 111101 \end{array}$ |  |
| $p \wedge q$ |  <p>$p \cap q$</p> <p>Intersection</p> | $101101 \text{ AND } 011001 = 001001$ $\begin{array}{r} 101101 \\ \text{AND } 011001 \\ \hline 001001 \end{array}$ |  |
| $p \oplus q$ |  <p>$p \Delta q$</p> <p>Symmetric Difference</p> | $101101 \text{ XOR } 011001 = 110100$ $\begin{array}{r} 101101 \\ \text{XOR } 011001 \\ \hline 110100 \end{array}$ |  |
| $p \rightarrow q$ |  <p>$p \rightarrow q$</p> <p>Implies</p> | $101101 \text{ THEN } 011001 = 011011$ $\begin{array}{r} 101101 \\ \text{THEN } 011001 \\ \hline 011011 \end{array}$ | |
| $p \leftrightarrow q$ |  <p>$p \leftrightarrow q$</p> <p>Equivalent</p> | $101101 \text{ XNOR } 011001 = 001011$ $\begin{array}{r} 101101 \\ \text{XNOR } 011001 \\ \hline 001011 \end{array}$ |  |

1.9 More on Quantifiers

- The **universal quantification** $\forall xP(x)$ states that “**for all** x such that $P(x)$ is true”.
- The **existential quantification** $\exists xP(x)$ states that “**there exists** x such that $P(x)$ is true”.

1.9.1 Equivalent Formulae on Finite Sets

Let the domain of $P(x)$ be a set with finite cardinality, assign the elements $x_1, x_2, x_3, \dots, x_k$,

- $\forall xP(x) \equiv \bigwedge_{i=1}^k P(x_i)$
- $\exists xP(x) \equiv \bigvee_{i=1}^k P(x_i)$

By the inductive process, we can also deduce De Morgan’s law.

$$\neg \left(\bigwedge_{i=1}^k P(x_i) \right) \equiv \bigvee_{i=1}^k (\neg P(x_i))$$

1.9.2 Quantifiers Overloading

Consider the following sentence

“Everyone who takes a break can have a snack.”

Let \mathcal{P} be the set of people, and \mathcal{S} be the set of all snacks. We say that $H(p, s)$ equals “person p had snack s ”. Consider the following formulae:

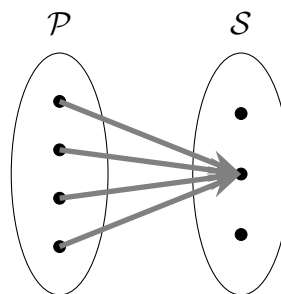
(a)

$$(\exists s)(\forall p)H(p, s)$$

In words, we have

“There exists a snack s (probably KitKat) such that every person p , p ate s .”

It is an **all-to-one** situation here.



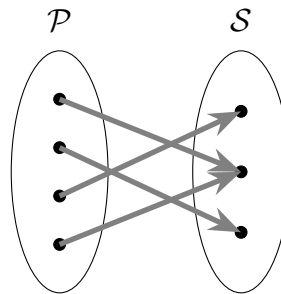
(b)

$$(\forall p)(\exists s)H(p, s)$$

In words, we have

“For all people p , there exists a snack s such that p ate s .”

It is a **one-to-one** situation here.



Moreover, we can stack quantifiers.

- x is irrational: $(\forall p \in \mathbb{Z})(\forall q \in \mathbb{Z})(x \neq p/q) \equiv (\nexists (p, q) \in \mathbb{Z}^2)(x = p/q)$.
- x is rational: $(\exists p \in \mathbb{Z})(\exists q \in \mathbb{Z})(x = p/q) \equiv \neg(\forall (p, q) \in \mathbb{Z}^2)(x \neq p/q)$.

§2 Proofs

No notes GG.

2.1 Tutorial 1

Problem 2.1

In this problem we consider binary logical operators in propositional logic.

1. How many are there?
2. Prove that there are exactly two binary logical operators \star in propositional logic such that $p \star (p \vee q)$ is a tautology.

1. $2^{2 \times 2} = 16$ of them
- 2.

| p | q | $p \vee q$ | $p \star (p \vee q)$ |
|-----|-----|------------|----------------------|
| 1 | 1 | 1 | 1 |
| 1 | 0 | 1 | 1 |
| 0 | 1 | 1 | 1 |
| 0 | 0 | 0 | 1 |

Since we know

| p | q | $p \star q$ |
|-----|-----|-------------|
| 1 | 1 | 1 |
| 0 | 1 | 1 |
| 0 | 0 | 1 |

But we don't know the case when p is true and q is false – there are two possibilities, hence there exists two such binary logical operators.

Problem 2.2

Define predicates $P(x)$ and $Q(x)$ with the same domain such that the formulas $\exists x(P(x) \rightarrow Q(x))$ and $(\exists x P(x)) \rightarrow (\exists x Q(x))$ have different truth values. Be sure to include brief justifications for the truth values of the two formulas (i.e., write down which one is true, which one is false, and why they are each true or false.)

Since $\exists x(P(x) \rightarrow Q(x))$ is a *useful denial* of $(\exists x P(x)) \rightarrow (\exists x Q(x))$, we have

$$\begin{aligned}\neg \exists x(P(x) \rightarrow Q(x)) &\equiv \forall x(P(x) \wedge \neg Q(x)) \\ (\exists x P(x)) \rightarrow (\exists x Q(x)) &\equiv (\neg \exists x P(x)) \vee (\exists x Q(x))\end{aligned}$$

If $\forall x(P(x) \wedge \neg Q(x))$ is true, then $\forall x, P(x)$ and $\neg Q(x)$ are true, but this implies $\neg \exists x P(x)$ and $\exists x Q(x)$ are false, hence $(\neg \exists x P(x)) \vee (\exists x Q(x))$ is false, no solution.

If $\forall x(P(x) \wedge \neg Q(x))$ is false, then $\neg \exists x P(x)$ and $\exists x Q(x)$ are false.

Set $P(x)$ be “ x is odd” and $Q(x)$ be “ x is prime”. Let $9 \in \mathcal{U}$ so $\exists x P(x)$. Next choose $4 \in \mathcal{U}$ so $\neg \exists x P(x)$ is true and $\forall x(P(x) \wedge \neg Q(x))$ is false.

Therefore an answer is $\boxed{P(x): \text{“}x \text{ is odd”}, Q(x): \text{“}x \text{ is prime”}, \mathcal{U} = \{4, 9\}}$.

The statement $\exists x(P(x) \rightarrow Q(x))$ is true whereas $(\exists x P(x)) \rightarrow (\exists x Q(x))$ is false.

Problem 2.3

Same question as the previous, except with the formulas $\forall x(P(x) \vee Q(x))$ and $(\forall x P(x)) \vee (\forall x Q(x))$.

Negating gives

$$\begin{aligned}\neg(\forall x)(P(x) \vee Q(x)) &\equiv \exists x(\neg P(x) \wedge \neg Q(x)) \\ (\forall x P(x)) \vee (\forall x Q(x)) &\equiv (\neg \exists x \neg P(x)) \vee (\neg \exists x \neg Q(x))\end{aligned}$$

Assume $\forall x P(x)$ and $\forall x Q(x)$ are false, then $\exists x(\neg P(x) \wedge \neg Q(x))$ is false. This implies that $\forall x(P(x) \vee Q(x))$ is true.

Set $P(x)$ be “ x is odd” and $Q(x)$ be “ x is prime”. Let $9 \in \mathcal{U}$ so $\forall x Q(x)$ is

false. Next, choose $4 \in \mathcal{U}$ so $\forall x P(x)$ is false and $\forall x(P(x) \vee Q(x))$ is true.

Therefore an answer is $\boxed{P(x): \text{“}x \text{ is odd”}, Q(x): \text{“}x \text{ is prime”}, \mathcal{U} = \{2, 9\}}$.

The statement $\forall x(P(x) \vee Q(x))$ is true whereas $(\forall x P(x)) \vee (\forall x Q(x))$ is false.

Problem 2.4

Prove that if m and n are integers such that mn is even, then either m is even or n is even. In your proof, point out where you are using the following facts (1): every integer is either even or odd; (2) no integer is both even and odd.

We will prove by contradiction. For the sake of contradiction, assume m, n are odd integers by (1). We can express $m = 2k + 1$ and $n = 2\ell + 1$ for some integer k, ℓ . Thus

$$mn = (2k + 1)(2\ell + 1) = 2(2k\ell + k + \ell) + 1$$

which is odd by (2) since it is not divisible by 2.

Problem 2.5

Prove that for every two distinct rational numbers, there is an irrational number in between them. (Recall we proved in lecture that $\sqrt{2}$ is irrational. If you want to claim any other number is irrational, you have to prove your claim first.)

Assume that the two rational numbers are a/b and c/d respectively (a, b, c, d are integers throughout this problem), and that $a/b < c/d$. Choose the number $\frac{a}{b} + \frac{\sqrt{2}}{C}$ for sufficiently large C .

Claim — For some rational number r/s where r, s are coprime integers, and an integer C , the number $\frac{r}{s} + \frac{\sqrt{2}}{C}$ is irrational.

For the sake of contradiction, assume that $\frac{r}{s} + \frac{\sqrt{2}}{C} = \frac{m}{n}$ for some coprime integers m, n . A quick simplification yields

$$2(ns)^2 = C^2(ms - nr)^2$$

This implies that $C(ms - nr)$ is even. In any case, we have $\nu_2(2(ns)^2)$ is odd but $\nu_2(C^2(ms - nr)^2)$ is even, hence a contradiction.

Remark. One may choose $C = \left\lceil \frac{\sqrt{2}}{\frac{c}{d} - \frac{a}{b}} \right\rceil$

Problem 2.6

Prove or disprove: The sum of two irrational numbers is irrational.

Choose $1 \pm \sqrt{2}$, thus $(1 + \sqrt{2}) + (1 - \sqrt{2}) = 2$ is rational.

§3 Induction

3.1 Some Examples

Problem (McCarthy)

Let x be an integer, and

$$f(x) = \begin{cases} x - 10 & x > 100; \\ f(f(x + 11)) & x \leq 100 \end{cases}$$

Then $f(x) = 91$ for all $x \leq 101$.

If $90 \leq x \leq 99$, then $f(x) = f(f(x + 11)) = f(x + 1)$.

If $x = 100$, then $f(100) = f(f(111)) = f(101) = 91$.

This concludes that for all integers $90 \leq x \leq 100$ we have $f(x) = 91$.

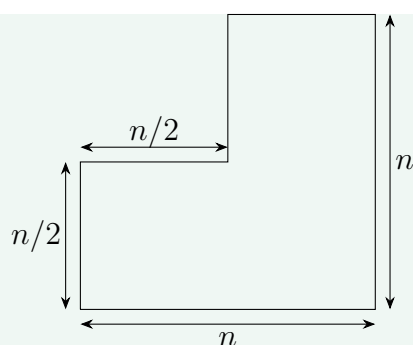
And by the inductive process, let's say $90 - 11k \leq x \leq 100 - 11k$ for some nonnegative integer k . We've proved that case $k = 0$. For other k , $f(f(x)) = f(x + 11)$ which can be proved by induction.

Problem (Golomb, 1965)

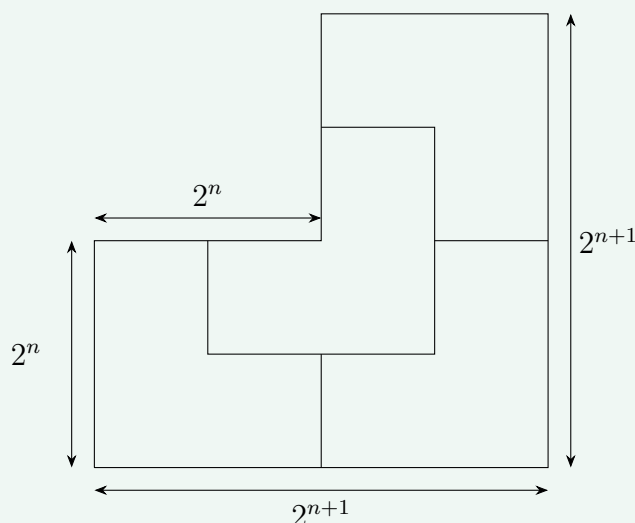
Prove that any $2^n \times 2^n$ board with one square removed can be tiled with L-shaped triominoes.

Indeed, we have to use induction twice, as follows:

Claim — Define an ℓ -block of size n to be a shape on the board as follows:



then an ℓ -block of size 2^{n+1} can be tiled by ℓ -blocks of size 2^n . A construction can easily show this



Base Case: $n = 1$ is just an L-shaped triomino.

Inductive Step: is shown in the construction above.

Now we have to deal with the entire square.

Claim — Any $2^n \times 2^n$ board with one square removed can be tiled with L-shaped triominoes.

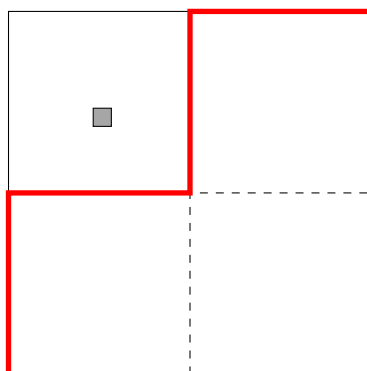
We'll proceed by induction.

Assume that for some positive integer n , any $2^n \times 2^n$ board with one square removed can be tiled with L-shaped triominoes.

Base Case: $n = 1$ can be tiled with only one L-shaped triomino.

Inductive Step: Let the square removed be X . Divide the $2^{n+1} \times 2^{n+1}$ board into four equal smaller $2^n \times 2^n$ boards. By the pigeonhole principle, exactly one of the $2^n \times 2^n$ boards must contain X . Let this $2^n \times 2^n$ board be B . The three other $2^n \times 2^n$ boards form an ℓ -block of size 2^{n+1} , which can be tiled.

On the other hand, B can be tiled according to our inductive hypothesis.



3.1.1 A False Induction Proof

“Assume that for any $n \geq 1$ horses, they have the same color.” Taking the first n horses and last n horses, we can conclude that $n + 1$ horses have the same color.

The “problem of the problem” lies in the fact that 2 horses, they can have different colors. Hence $P(1) \rightarrow P(2)$ does not hold true.

3.1.2 Well-Ordering Principle

Theorem (Well-Ordering Principle)

An **ordered set** is said to be **well-ordered** if each and every nonempty subset has a smallest or least element.

This is the foundation of proof by infinite descent.

3.2 Beyond Induction: Infinite Descent

Problem (IMO 1988)

Let a and b be positive integers such that $ab + 1$ divides $a^2 + b^2$. Show that

$$\frac{a^2 + b^2}{ab + 1}$$

is the square of an integer.

FTSOC, let $\frac{a^2 + b^2}{ab + 1} = k$ for some nonsquare integer k . Rearranging gives

$$a^2 - kab + (b^2 - k) = 0$$

Assume that (a, b) is a solution and WLOG assume $a \geq b$. FTSOC let $a + b$ be minimal. Then (a', b) is also a solution by the quadratic equation in a . By the

Vieta's formulas, we have

$$\begin{cases} a + a' = kb \\ aa' = b^2 - k \end{cases}$$

By the first equation, we know that a' is an integer. And by the second equation

$$a' = \frac{b^2 - k}{a} \neq 0$$

since $b^2 - k$ cannot equal to 0.

On the other hand, by $a'^2 + b^2 = k(a'b + 1)$ implies that $a' > 0$.

Bounding gives

$$a' = \frac{b^2 - k}{a} \leq \frac{a^2 - k}{a} = a - \frac{k}{a} < a$$

Therefore $a > a'$ which leads to a contradiction by minimality.

3.3 Tutorial 2

Problem 3.1

For each of the following sentences, explain (in one sentence) whether it is true or false. The scope of x and y is taken to be \mathbb{R} .

1. $\forall x \exists y (x^2 = y)$
2. $\forall y \exists x (x^2 = y)$
3. $\exists x \forall y (x^2 = y)$
4. $\exists y \forall x (x^2 = y)$
5. $\forall x \forall y (x^2 = y)$
6. $\exists x \exists y (x^2 = y)$

1. **True**, the value of y is uniquely determined by the value of x^2 .
2. **False**, choose a negative y .
3. **False**, $x^2 = y$ but $x^2 \neq y + 1$ for every real y .
4. **False**, if $y = 0$ choose positive x , conversely if $y^2 > 0$ choose $x = 0$.
5. **False**, $1^2 \neq 0$.
6. **True**, choose $x = y = 0$.

Problem 3.2

Prove that for every nonzero integer a and b , there is a positive integer c such that a and b both divide c . (Remember, we don't know yet that the lcm exists.) Then prove that there is a smallest positive integer c such that a and b both divide c .

(i) Choose $c = |ab| = |a||b|$.

Claim — For all nonzero integer n and a positive integer m , n divides m if and only if $|n|$ divides m .

If n is positive, then there's nothing to consider.

If $n < 0$ divides m , then m/n is an integer. $|n|/m = -n/m$ which is an integer so $|n|$ divides m .

If $|n|/m = -n/m$ is an integer, then n/m is an integer as well.

So by (i) we know that there exists such c . Moreover, we know that $c/|a|$ and $c/|b|$ are natural numbers. Assume otherwise, c does not have a smallest value, then $c/|a|$ does not have a smallest value, contradicting to the Well-Ordering principle.

Problem 3.3

Use induction to prove that for every n in \mathbb{N} , 3 divides $n^3 - n$. (If you want to use facts about division modulo 3 you have to prove them first. The proof I have in mind doesn't use such facts.)

Base Case: $n = 0$, then $n^3 - n = 0 = 3 \times 0$ so 3 divides $n^3 - n$.

Inductive Step: Assume that $n^3 - n$ is divisible by 3 for some n in \mathbb{N} . Let $n^3 - n = 3k$ for some integer k . We hope to prove that $(n+1)^3 - (n+1)$ is divisible by 3.

$$\begin{aligned} (n+1)^3 - (n+1) &= n^3 + 3n^2 + 2n \\ &= (n^3 + 3n^2 + 2n + 2(3k)) - 2(3k) \\ &= (3n^3 + 3n^2) - 2(3k) \\ &= 3(n^3 + n^2 - 2k) \end{aligned}$$

Problem 3.4

Define a sequence $\{a_n\}_n$ of real numbers by $a_0 = 0$ and $a_{n+1} = (a_n)^2 + \frac{1}{4}$ for $n \in \mathbb{N}$. Prove that for all n in \mathbb{N}^+ , we have $0 < a_n < 1$.

It is easy to show that $a_{n+1} > 0$ by $(a_n)^2 + \frac{1}{4} \geq \frac{1}{4} > 0$ for all $n \in \mathbb{N}$.

Claim — $a_n < \frac{1}{2}$ for all $n \in \mathbb{N}$.

We will prove by induction.

Base Case: $a_0 = 0 < \frac{1}{2}$.

Inductive Step: Assume that for some $n \in \mathbb{N}$, we have $a_n < \frac{1}{2}$, we wish to prove that $a_{n+1} < \frac{1}{2}$.

By

$$a_{n+1} = (a_n)^2 + \frac{1}{4} < \left(\frac{1}{2}\right)^2 + \frac{1}{4} = \frac{1}{2}$$

Hence each term $a_n, n \in \mathbb{N}^+$ satisfy $0 < a_n < \frac{1}{2} < 1$.

Problem 3.5

What rule(s) of addition for real numbers (among associativity and commutativity) guarantees that $(a + b) + (c + d) = a + (b + (c + d))$? Use induction to prove that for every $n \in \mathbb{N}^+$ and every sequence of real numbers $\{a_i\}_{i=0}^n$ and $\{b_i\}_{i=0}^n$, we have $\sum_{i=0}^n (a_i + b_i) = \sum_{i=0}^n a_i + \sum_{i=0}^n b_i$. In your proof, specify which rules of addition you use and where.

Left associativity:

$$(a + b) + (c + d) = a + b + (c + d)$$

Right associativity:

$$a + b + (c + d) = a + (b + (c + d))$$

We will proceed by induction.

Base Case: $(a_1) + (b_1) = (a_1 + b_1)$ which is obviously true.

Inductive Step: We assume that $\sum_{i=0}^n (a_i + b_i) = \sum_{i=0}^n a_i + \sum_{i=0}^n b_i$, we want

$$\sum_{i=0}^n (a_i + b_i) + (a_{n+1} + b_{n+1}) = \left(\sum_{i=0}^n a_i + a_{n+1} \right) + \left(\sum_{i=0}^n b_i + b_{n+1} \right)$$

Let $p \stackrel{L}{=} q$ if q can be shown equal to p by using left associativity. Similarly define $p \stackrel{R}{=} q$ for right associativity and $p \stackrel{C}{=} q$ for commutativity.

From the right, we have

$$\begin{aligned} \left(\sum_{i=0}^n a_i + a_{n+1} \right) + \left(\sum_{i=0}^n b_i + b_{n+1} \right) &\stackrel{L}{=} \sum_{i=0}^n a_i + a_{n+1} + \left(\sum_{i=0}^n b_i + b_{n+1} \right) \\ &\stackrel{R}{=} \sum_{i=0}^n a_i + \left(a_{n+1} + \left(\sum_{i=0}^n b_i + b_{n+1} \right) \right) \end{aligned}$$

While from the left, using our inductive hypothesis, we have

$$\begin{aligned} \sum_{i=0}^n (a_i + b_i) + (a_{n+1} + b_{n+1}) &= \sum_{i=0}^n a_i + \sum_{i=0}^n b_i + (a_{n+1} + b_{n+1}) \\ &\stackrel{R}{=} \sum_{i=0}^n a_i + \left(\sum_{i=0}^n b_i + (a_{n+1} + b_{n+1}) \right) \\ &\stackrel{C}{=} \sum_{i=0}^n a_i + \left((a_{n+1} + b_{n+1}) + \sum_{i=0}^n b_i \right) \\ &\stackrel{L}{=} \sum_{i=0}^n a_i + \left(a_{n+1} + b_{n+1} + \sum_{i=0}^n b_i \right) \\ &\stackrel{R}{=} \sum_{i=0}^n a_i + \left(a_{n+1} + \left(b_{n+1} + \sum_{i=0}^n b_i \right) \right) \\ &\stackrel{C}{=} \sum_{i=0}^n a_i + \left(a_{n+1} + \left(\sum_{i=0}^n b_i + b_{n+1} \right) \right) \end{aligned}$$

So we have shown that both sides equal

$$\sum_{i=0}^n a_i + \left(a_{n+1} + \left(\sum_{i=0}^n b_i + b_{n+1} \right) \right)$$

and therefore we are done.

Problem 3.6

Suppose S is a nonempty subset of \mathbb{Z} which is bounded above by some integer m , i.e., $s < m$ for all $s \in S$. Use well-ordering to prove that S has a largest element.

Step 1: If $m > 0$ then for every element in S , we subtract it by m so that we end up with another set of integers T . If $m \leq 0$ then just let $T = S$. Thus T is a set of nonpositive integers.

Step 2: Similarly, for every element in T , multiply by -1 so that we end up with another set of integers U . Each element in U is nonnegative, hence it is a subset of \mathbb{N} .

By the well-ordering principle, U has a smallest element. So T has a largest element and S has a largest element since S, T, U are one to one mappings.

Remark. One can consider the sets of all values $m - s$.

Problem 3.7

Define the predicate $P(n, m)$ to say that there is a finite sequence of positive integers $\{a_i\}_{i=0}^j$ such that

$$\frac{n}{m} = \frac{1}{a_0 + \frac{1}{a_1 + \frac{1}{\ddots + \frac{1}{a_j}}}}.$$

The domain of $P(n, m)$ is the set $\{(n, m) : n, m \in \mathbb{N}^+, n < m\}$. For example, $P(7, 9)$ is true, as witnessed by the sequence $a_0 = 1, a_1 = 3, a_2 = 2$. $P(1, 4)$ is true, as witnessed by $a_0 = 4$. (Make sure you understand these computational examples before proceeding.) The goal of this question is to prove that $P(n, m)$ holds for all m and n (in its domain, of course).

1. Suppose $n < m$ are positive integers such that n does not divide m . Prove that there is a largest positive integer a such that $\frac{n}{m} < \frac{1}{a}$.
2. In the context of the previous part, prove that $0 < m - an < n$.
3. Suppose $n < m$ are positive integers such that for all positive integers $n' < n$, $P(n', n)$ holds. Prove that $P(n, m)$ holds.
4. Convince yourself that we have a proof that $P(n, m)$ holds for all m and n .

1. Rearranging gives $a < m/n$, which by [Problem 3.6](#) there is a largest element.

Remark. By $n/m = 1/a$ we can show that a exists and $a > 0$.

2. For the left part of the inequality, rearranging inequality gives

$$\begin{aligned} a &< m/n \\ an &< m \\ 0 &< m - an \end{aligned}$$

For the right part of the inequality, since m/n is not an integer, there exists a positive integer k such that $k < m/n < k + 1$.

If $a < k$ then $a + 1 \leq k < m/n$ which is a contradiction since a is largest positive integer less than m/n . Therefore $k = a$.

Hence

$$\begin{aligned} m/n &< a + 1 \\ m &< an + n \\ m - an &< n \end{aligned}$$

3. By rewriting n/m ,

$$\begin{aligned} \frac{n}{m} &= \frac{1}{\frac{m}{n}} \\ &= \frac{1}{a + \frac{m - an}{n}} \end{aligned}$$

Since $m - an < n$, $P(m - an, n)$ holds. So in this case, let $a_0 = a$, which clearly shows that $P(n, m)$ holds.

4. **Base Case:** A quick check shows that $P(1, 2), P(1, 3), P(2, 3)$ holds.

$$\frac{1}{2} = \frac{1}{1 + \frac{1}{1}} \quad \frac{1}{3} = \frac{1}{2 + \frac{1}{1}} \quad \frac{2}{3} = \frac{1}{1 + \frac{1}{2}}$$

Inductive Step: Now assume that $m = 4$ for example. Then by our induction hypothesis for every integer $2 \leq n < 4$, the statement $P(n, m)$ holds. Assume that for all integers $1 \leq k < n$, $P(k, n)$ holds. Consider $P(k', n + 1)$ where k' is an integer $1 \leq k' < n + 1$. If $n = 1$, choose $a_0 = m$.

Therefore, we have proved that for all integers $1 \leq n < m$, the statement $P(n, m)$ holds.

§4 Sets

4.1 Fundamental Notations

- **Subset** $A \subseteq B$, **Proper Subset** $A \subset B$ or $A \subsetneq B$
- **Union of Sets:** $\bigcup_{i=0}^n A_i = A_1 \cup A_2 \cup A_3 \cup \cdots \cup A_n$
- **Intersection of Sets:** $\bigcap_{i=0}^n A_i = A_1 \cap A_2 \cap A_3 \cap \cdots \cap A_n$
- **Set Difference:** $A - B$, if $a \in A$ and $a \in B$ then $a \notin A - B$
- **Symmetric Difference:** $A \Delta B = (A \cup B) - (A \cap B)$

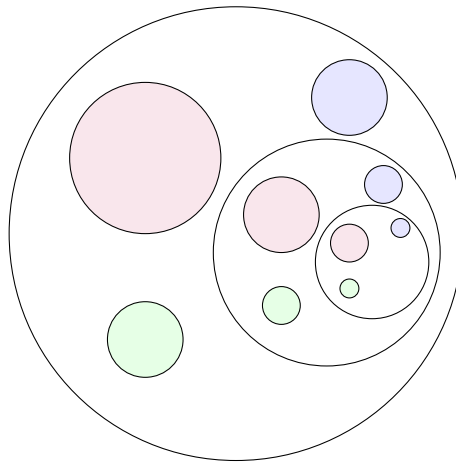
- **Power Set:** $\mathcal{P}(A) = \{X : X \subseteq A\}$
- **Cartesian Product:** $A \times B = \{(a, b) : a \in A \wedge b \in B\}$

Informally, we write $\prod_{i=1}^n X_i = X_1 \times X_2 \times X_3 \times \cdots \times X_n$.

4.2 Russell's Paradox, Zermelo-Fraenkel Set Theory and Axiom of Choice (ZFC)

4.2.1 Russell's Paradox

Consider the set \mathcal{S} that contains ALL sets x that do not contain itself. In other words, $x \notin x$. An illustration below demonstrates how a set can contain itself.



Now, if $\mathcal{S} \in \mathcal{S}$, then \mathcal{S} does not contain itself, by \mathcal{S} is already in \mathcal{S} ! Contradiction.

However, if $\mathcal{S} \notin \mathcal{S}$, then by negation \mathcal{S} must contain itself. But we cannot find \mathcal{S} in \mathcal{S} ! Contradiction again.

An analogy by **Veritasium** on self-referencing paradox is as follows:

Assume that there's a law in a village that states that the barber has to shave every man who doesn't shave himself. But since the barber is also a man who doesn't shave himself, someone must shave the barber, which is the barber himself! Contradiction.



4.2.2 Zermelo-Fraenkel Set Theory

There are 10 axioms in ZFC. As we proceed, one can progressively lay down the foundations of set theory.

1. **Axiom of extensionality**: $A = B$ if $\forall x((x \in A) \leftrightarrow (x \in B))$
2. **Axiom of empty set**: There is a unique empty set \emptyset (by Extensionality).
3. **Axiom of pairing**: For every two sets A, B , there exists set $C = \{A, B\}$ such that $A \in C$ and $B \in C$.
4. **Axiom of union**: Let A be a set of sets, there exists a set $\bigcup A$ such that the elements in $\bigcup A$ are the elements in the sets in A .

Now we can have a set of more than 2 elements.

5. **Axiom schema of specification (Aussonderungsaxiom)**: For every formula $\varphi(x)$ and set A , there exists a set S with its elements are the elements x in A such that $\varphi(x)$ holds.
 - This allows us to construct the unary intersection set $\bigcap A$.

Let A be a set of sets, there exists a set $\bigcap A$ such that the elements in $\bigcap A$ are the elements that is in every set in A .

- **Berry's Paradox**:

6. **Axiom of power set**: For every set A , there exists a set $\mathcal{P}(A)$ whose elements are the subsets of A .
7. **Axiom of infinity**: There exists a set X , such that $\emptyset \in X$ and whenever $x \in X$ we have $x \cup \{x\} \in X$, the **successor** of x .

Therefore, we can construct the set

$$\begin{aligned} X_0 &= \emptyset \\ X_1 &= \{\emptyset\} \\ X_2 &= \{\emptyset, \{\emptyset\}\} \\ X_3 &= \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \\ X_4 &= \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\} \end{aligned}$$

This axiom allows us to construct a set with infinitely many elements.

We can construct the set of natural numbers.

$$\mathbb{N} = \{x \in X : (\forall Y)(\emptyset \in Y \wedge \forall y \in Y(y \cup \{y\} \in Y) \rightarrow y \in X)\}$$

This proves the induction on \mathbb{N} .

If $\phi(n)$ is a formula such that $\phi(\emptyset)$ is true, and that if $\phi(n)$ is true implies $\phi(n \cup \{n\})$ is true, then $\phi(n)$ holds for all $n \in \mathbb{N}$.

8. **Axiom schema of replacement**: For every formula $\varphi(x, y)$ and set A , if for every $x \in A$ there's a **unique** y such that $\varphi(x, y)$, then there's a set with exactly those y such that there exists some $x \in A$ with $\varphi(x, y)$.

Thus we can build the set

$$\{y : (\exists x \in A)\varphi(x, y)\} = \{f(x) : x \in A\}$$

Thus **every function has a range**.

9. **Axiom of foundation**: For every nonempty set (of sets) A , we have an element x such that for every $a \in A$, we have $a \notin x$.

This, with the axiom of pairing, assures that **no set is an element of itself** $x \notin x$.

4.3 Well-Orderedness

A relation $<$ on a set A is **well-order** if:

- It is **transitive**, $a < b, b < c$ implies $a < c$.
- It satisfies **trichotomy**, either $a < b$, $a = b$ or $a > b$.
- Every subset X of A has a $<$ -least element,

$$(\forall X \subseteq A)(X = \emptyset \vee (\exists x \in X)(\forall y \in X)(y \not< x))$$

A relation R on a set A is **well-founded** if

$$(\forall X \subseteq A)(X = \emptyset \vee (\exists x \in X)(\forall y \in X)((y, x) \notin R))$$

Noetherian Induction: Suppose $\phi(x)$ is a formula such that for all $y \in A$, $\phi(x)$ holds for all $x \in A$ satisfying $(x, y) \in R$ then $\phi(y)$ holds. Then $\phi(x)$ holds for all $x \in A$.

For instance, take R to be the $<$ “smaller than” relation. Then for all x such that $x < y$ and $\phi(x)$ holds, then $\phi(y)$ holds. Also, there exists an x (least element) such that for all y , $y \not< x$ holds.

Proof of induction on well-orders: Let x be some element such that $\phi(x)$ is false, then the set $\{x \in X : \neg\phi(x)\}$ is nonempty. Choose the $<$ -least element y in this set, contrary to our assumption that for all $x < y$, $\phi(x)$ holds then $\phi(y)$ holds.

Proof of induction on well-founded: Assume that x is an element such that $\phi(x)$ is false, then the set $\{x \in X : \neg\phi(x)\}$ is nonempty. Choose the element y such that for every $x \in X$, $(x, y) \notin R$, which is a contradiction.

4.3.1 Axiom of Choice

For every set X of sets, with $\emptyset \notin X$, there exists a **choice function** $F : X \rightarrow \bigcup X$

such that for every $S \in X$ we have $F(S) \in S$.

This fails in ZF due to the fact that we cannot guarantee a “formula” in replacement.

4.4 Tutorial 3

Problem 4.1

Let m and n be positive integers. Given a chocolate bar with dimensions m units by n units, your task is to break it down into mn many 1 unit by 1 unit squares. The only operation you can perform is to take a single piece and break it vertically or horizontally. (You can't break multiple pieces in one operation!) Use strong induction to prove that one needs at least $mn - 1$ operations for this task. (Optional: Is $mn - 1$ operations enough?)

Claim — We actually need exactly $mn - 1$ operations.

Assume that after the k 'th operation ($k \in \mathbb{N}^+$), we have $P(k)$ pieces. For convention, we also assume $P(0) = 1$. Since after each operation, one of the pieces breaks into two pieces, hence we have

$$P(k+1) = P(k) + 1$$

This is due to the fact that no matter how we break the chocolate the pieces remain rectangle and that rectangles are convex.

Claim — $P(k) = k + 1$ for all $k \in \mathbb{N}$.

Base Case: $k = 0$ we have $P(0) = 1$ as defined.

Inductive Step: Assume that $P(k) = k + 1$ holds true for some $k \in \mathbb{N}$, then we have

$$P(k+1) = P(k) + 1 = k + 2$$

as desired.

Problem 4.2

Prove that for all sets A , B and C , we have $(A - B) - C = (A - C) - (B - C)$. (As mentioned in lecture, do not prove this by translating the set identity into a propositional tautology.)

Proof. (\subseteq) Let a be an element of the set $(A - B) - C$. By set difference we can deduce that $a \in A$ but $a \notin B$ and $a \notin C$.

While on the other hand, $A - C$ is the set of all elements k which $k \in A$ but $k \notin C$. $B - C$ is the set of all elements ℓ which $\ell \in B$ but $\ell \notin C$.

Taking the difference $(A - C) - (B - C)$ gives the set of all elements k such that

$k \in A$ but $k \notin B$ and $k \notin C$. So $a \in (A - C) - (B - C)$.

(\supseteq) Let $a \in (A - C) - (B - C)$ so this means that $a \in A - C$ but $a \notin B - C$. Since $a \in A - C$ we have $a \in A$ but $a \notin C$. On the other hand, by $a \notin B - C$ we have $a \notin B$.

On the other hand, from $a \in A$ and $a \notin B$ we have $a \in A - B$, and by $a \notin C$ we have $a \in (A - B) - C$ as desired. \square

Problem 4.3

Prove that for all sets x and y , the set $\{\{x\}, \{x, y\}\}$ is an element of $\mathcal{P}(\mathcal{P}(\{x, y\}))$.

By the definition of power set, we have

$$\mathcal{P}(\mathcal{P}(\{x, y\})) = \mathcal{P}(\{\emptyset, \{x\}, \{y\}, \{x, y\}\})$$

If the set $\{\{x\}, \{x, y\}\}$ is an element of a power set $\mathcal{P}(\{\emptyset, \{x\}, \{y\}, \{x, y\}\})$, then this set must be a subset of $\{\emptyset, \{x\}, \{y\}, \{x, y\}\}$.

This is true since $\{x\} \in \{\emptyset, \{x\}, \{y\}, \{x, y\}\}$ and $\{x, y\} \in \{\emptyset, \{x\}, \{y\}, \{x, y\}\}$.

Problem 4.4

Prove or disprove: For all sets A, B, C and D , if $A \times B \subseteq C \times D$ then $A \subseteq C$ and $B \subseteq D$.

I claim that this is false.

Consider $A = \emptyset, B = \{x\}, C = \{y\}, D = \{z\}$.

Then $A \times B = \emptyset$, whereas $C \times D = \{(y, z)\}$.

So $A \times B \subseteq C \times D$ is true but B is not a subset of D since $x \in B$ but $x \notin D$.

Problem 4.5

Prove or disprove: For all sets $\{A_i\}_{i \in I}$ and $\{B_i\}_{i \in I}$, we have $(\bigcap_{i \in I} A_i) \cup (\bigcap_{i \in I} B_i) = \bigcap_{i \in I} (A_i \cup B_i)$.

I claim that this is false.

Consider $I = \{1, 2\}$ and

$$\begin{array}{ll} A_1 = \{a\} & A_2 = \{b\} \\ B_1 = \{b\} & B_2 = \{a\} \end{array}$$

Then we have

$$\bigcap_{i \in I} A_i = A_1 \cap A_2 = \emptyset$$

$$\bigcap_{i \in I} B_i = B_1 \cap B_2 = \emptyset$$

So we have $(\bigcap_{i \in I} A_i) \cup (\bigcap_{i \in I} B_i) = \emptyset$.

But on the other hand,

$$\bigcap_{i \in I} (A_i \cup B_i) = (A_1 \cup B_1) \cap (A_2 \cup B_2) = \{a, b\}$$

which is a counterexample of this statement.

Problem 4.6

Suppose $\{A_i\}_{i \in \mathbb{N}}$ are sets. Prove that

$$\bigcup_{i=0}^{\infty} \bigcap_{j=i}^{\infty} A_j \subseteq \bigcap_{i=0}^{\infty} \bigcup_{j=i}^{\infty} A_j.$$

Let $\mathcal{A} = \bigcup_{i=0}^{\infty} \bigcap_{j=i}^{\infty} A_j$ and $\mathcal{B} = \bigcap_{i=0}^{\infty} \bigcup_{j=i}^{\infty} A_j$. If each of $\bigcap_{j=i}^{\infty} A_j = \emptyset$ for all $i = 0, 1, 2, \dots$, then $\mathcal{A} = \emptyset$ and we are done.

Assume that for some element a , there exist an index k such that

$$a \in \bigcap_{j=k}^{\infty} A_j$$

This means for every index $N \geq k$, we must have $a \in A_N$.

Now that we want to show $a \in \bigcup_{j=i}^{\infty} A_j$ for all $i = 0, 1, 2, \dots$.

If $i \leq k$, we have

$$a \in \left(\bigcup_{j=i}^{k-1} A_j \right) \cup A_k \cup \left(\bigcup_{j=k+1}^{\infty} A_j \right)$$

If $i > k$, then we have

$$a \in \bigcup_{j=i}^{\infty} A_j$$

since $i > k$. Hence we have proven that for all $i = 0, 1, 2, \dots$, $a \in \bigcup_{j=i}^{\infty} A_j$ and therefore $a \in \mathcal{B}$ as desired.

Remark.

- An *index* is a natural number.

- We define $\bigcup_{i=j}^k A_j = \emptyset$ if $k < j$.

§5 Functions

A function $f : A \rightarrow B$ with its graph G is an ordered triplet (A, B, G) defined by

$$(\forall a \in A)(\exists! b \in B)((a, b) \in G)$$

We say that A is the **domain**, B is the **codomain** of f , and $f[A]$ the **range** of f .

Two functions can be different if they differ just by A , even if their expression are the same.

5.1 Well Defineness

If a function maps an element in the domain of f to zero element or more than one element, then the function f is not **well-defined**.

Some examples of not well-defined functions

- $f : \mathbb{R} \rightarrow \mathbb{R}$ and $f(x) = 1/x$ since $f(0)$ is not defined.
- $f : \mathbb{R}^+ \rightarrow \mathbb{R}$ defined by $f(x)^2 = x$.
- $f : \mathbb{R} \rightarrow \mathbb{N}$ defined by $f(x) = x + 1$.
- $f : A \rightarrow \emptyset$ and A is nonempty.

5.2 Functions Terminology

Consider some function $f : A \rightarrow B$.

- **Surjectivity**

$$(\forall b \in B)(\exists a \in A)(f(a) = b)$$

- **Injectivity**

$$(\forall a, b \in A)(f(x) = f(y) \rightarrow x = y)$$

- **Bijectivity**

$$(\forall b \in B)(\exists a \in A)(f(a) = b) \wedge (\forall a, b \in A)(f(x) = f(y) \rightarrow x = y)$$

- **Inverse Functions**

– f has a **left inverse** $g \circ f = \text{id}_A$ iff f is injective.

(\Rightarrow) Let $g(f(a)) = a$ and $g(f(b)) = b$ and $a \neq b$, obviously $f(a) \neq f(b)$.

(\Leftarrow) Let $f : A \rightarrow B$ be injective, define a function $g : B \rightarrow A$ carefully as follows:

- * For each $b \in B$, if $f(a) = b$ then we define $g(b) = a$.
- * For other $b \in B - \text{range}(f)$, set some $a_0 \in A$, define $g(b) = a_0$.

It suffices to show g is well-defined.

For every $b \in B$, it is mapped to some $a \in A$ by our assumption of g . For each b , $g(b)$ is mapped to only one unique value, either a_0 or some a due to $f(a) = b$ (unique since f is injective).

Considering all a 's, if $f(a) = b$ then $g(b) = a$, which satisfies $g \circ f = \text{id}_B$.

– f has a **right inverse** $f \circ g = \text{id}_B$ iff f is surjective.

(\Rightarrow) For all $b \in B$, we have $f(g(b)) = b$, hence f is surjective.

A Proof by AC: (\Leftarrow) If $f : A \rightarrow B$ is surjective, then consider the following set

$$X = \{f^{-1}[\{b\}] \subseteq A : b \in B\}$$

Thus $\emptyset \notin X$, since f is surjective. By the axiom of choice, there exists some function H such that for every $\mathcal{X} \in X$, we have $H(\mathcal{X}) \in \mathcal{X}$.

- Let $X \subseteq A$ and g be a function such that for every $x \in X$ we have $f(x) = g(x)$, then g is a **restriction** of f . This is denoted as $g = f \upharpoonright X$.

5.3 Some Other Properties

- Let $f : X \rightarrow Y$ and $A, B \subseteq X$, then

$$f[A \cup B] = f[A] \cup f[B]$$

$$f[A \cap B] = f[A] \cap f[B]$$

5.4 Introduction to Category Theory

Category theory is the study of **mathematical structures** and their relations. – Wikipedia

Some mathematical structures include:

| Structures | Description | Examples |
|--------------------|--|---|
| Sets | A collection of different things | $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \{\pi, e, i\}$ |
| Groups | A non-empty set closed under a binary operation | $(\mathbb{R}, +), S_n, A_n, \text{GL}_n(\mathbb{Z})$ |
| Rings | A non-empty set closed under two binary operations | $\mathbb{Z}/6\mathbb{Z}, M_2(\mathbb{R})$ |
| Fields | A non-empty set closed under two binary operations and their inverse operations | $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ |
| Vector Spaces | A non-empty set with a binary operator and a binary function | $\mathbb{R}^2, \mathbb{C}^2$ |
| Modules | Similar to vector spaces but the scalars form a ring | $M_n(\mathbb{R})$ |
| Metric Spaces | An ordered pair of a set and a metric | Euclidean Distance Hamming Distance Chebyshev Distance |
| Topological Spaces | A set A of sets such that for every collection of sets, their union and intersection is in A | $\{\{\}, \{1, 2, 3, 4\}\}$ $\{\{1, 2\}, \{1, 2, 3\}\}$ |
| Partial Orders | An arrangement of a set such that for certain pairs of elements one precedes the other | \mathbb{R} |
| Manifolds | A space that is "modeled on" the Euclidean space | Circles, Spheres |
| Graphs | A set of objects such that some pairs of objects are "related" | $K_7, K_{2,5}, C_4$ |

While at the same time, we have different kinds of **morphisms**. A morphism is a mapping that preserves structures.

| Morphisms | Description |
|----------------|---|
| Monomorphism | Injectivity $f \circ g_1 = f \circ g_2$ implies $g_1 = g_2$ then f is monomorphic |
| Epimorphism | Surjectivity $g_1 \circ f = g_2 \circ f$ implies $g_1 = g_2$ then f is epimorphic |
| Isomorphism | Bijectivity Both left and right inverses exist |
| Endomorphism | A function from itself to itself |
| Automorphism | An isomorphic endomorphism |
| Homomorphism | A map preserving algebraic structures |
| Homeomorphism | A bijective continuous mapping between two topological spaces |
| Diffeomorphism | Isomorphism of differentiable manifolds |

5.5 Tutorial 4

Problem 5.1

Prove that for every set A and B such that $A \subseteq B$, we have $\bigcup A \subseteq \bigcup B$.

Let $X \in A$ then $X \in B$. Therefore $X \subseteq \bigcup A$ and $X \subseteq \bigcup B$. For every element in X , say a , since $a \in X$ we have $a \in \bigcup A$ and $x \in \bigcup B$, as desired.

Problem 5.2

Prove that for every set A , we have $A \subseteq \mathcal{P}(\bigcup A)$. When does the reverse inclusion $A \supseteq \mathcal{P}(\bigcup A)$ hold?

For some element $X \in A$, we have $X \subseteq \bigcup A$. So we have $X \in \mathcal{P}(\bigcup A)$ as desired.

Since each of the elements of A is in $\mathcal{P}(\bigcup A)$, if reverse inclusion appears, we want to solve

$$A = \mathcal{P}(\bigcup A)$$

Claim — A is non-empty.

Proof. Assume otherwise, $\mathcal{P}(\bigcup A) = \{\emptyset\}$, contradiction. ■

Claim — Let $X \in A$ and $Y \subseteq X$, then $Y \in A$.

Proof. For each element $y \in Y$, we have $y \in X$ and $y \in \bigcup A$, therefore $Y \subseteq \bigcup A$ so we have $Y \in \mathcal{P}(\bigcup A) = A$. ■

By the claim above, A has at least one element. If this element is the empty set, then $A = \mathcal{P}(\bigcup A)$ holds. Otherwise, by **Claim 2** A have at least two elements since the empty set $\emptyset \in A$.

Claim — If $X \in A$ and $Y \in A$, then $(X \cup Y) \in A$.

Proof. Let $x \in X$ and $y \in Y$, we have $x \in \bigcup A$ and $y \in \bigcup A$. Consider the set $X \cup Y$, each of its elements are in $\bigcup A$, therefore $(X \cup Y) \in \mathcal{P}(\bigcup A) = A$. ■

Problem 5.3

Define a relation \prec on the Cartesian product $\mathbb{N} \times \mathbb{N}$ as follows: $(a, b) \prec (c, d)$ if and only if either $a < c$, or $(a = c \text{ and } b < d)$. (Here $<$ refers to the standard ordering on \mathbb{N} .) Our aim is to prove that \prec is a well-order on $\mathbb{N} \times \mathbb{N}$, which would imply (by what we discussed in lecture) a corresponding induction principle.

1. Prove that \prec is transitive.
2. Prove that \prec satisfies trichotomy.
3. Prove that every nonempty subset of $\mathbb{N} \times \mathbb{N}$ has a least element with respect to the ordering \prec .

1. Assume that $(a, b) \prec (c, d)$ and $(c, d) \prec (e, f)$, we consider all four cases:

- a) If $a < c$,

If $c < e$ then $a < e$ so $(a, b) \prec (e, f)$.

If $c = e$ and $d < f$ then $a < c = e$ so $(a, b) \prec (e, f)$.

- b) If $a = c$ and $b < d$,

If $c < e$ then $a = c < e$ so $(a, b) \prec (e, f)$.

If $c = e$ and $d < f$ then $a = c = e$ and $b < d < f$ so $(a, b) \prec (e, f)$.

2. Assume that for some $(a, b), (c, d)$, both $(a, b) \prec (c, d)$ and $(a, b) \succ (c, d)$ do not hold, then:

By $(a, b) \prec (c, d)$ does not hold, we have $a < c$ and $(a = c \text{ and } b < d)$ do not hold.

By $(a, b) \succ (c, d)$ does not hold, we have $a > c$ and $(a = c \text{ and } b > d)$ do not hold.

Since $a < c$ and $a > c$ do not hold, we must have $a = c$. And since $(a = c \text{ and } b < d)$ and $(a = c \text{ and } b > d)$ do not hold, we only have $b = d$, therefore $(a, b) = (c, d)$.

3. For every nonempty subset A of $\mathbb{N} \times \mathbb{N}$, iterate through all (a, b) . First choose all elements with a minimum, let this value be a' , and then iterate through all (a', b) , choose the element with b minimum, say b' . This is the consequence of the well-ordering principle. We claim that (a', b') is the least element.

For every other (c, d) , if $a' < c$ then we are done. If $a' = c$ then if $b' < d$ and we are done. Otherwise if $b' = d$ then $(a', b') = (c, d)$.

Problem 5.4

Come up with a set X and a function $f : X \rightarrow X$ such that $f \circ f = f$ but f is not id_X .

Consider the set $X = \{0, 1\}$ and $f(x) = 0$ the constant function, then $f \circ f = 0$, $f = 0$.

Problem 5.5

Prove that if $f : A \rightarrow B$ and $g : C \rightarrow D$ are one-to-one functions such that $g \circ f$ is defined, then $g \circ f$ is one-to-one.

If $\text{ran}(g \circ f)$ is empty, we are done.

Assume otherwise, let $a \in A$, $c \in C$, $d \in D$ such that $f(a) = c$ and $g(c) = d$.

Since g is one-to-one, for any two distinct $g(c_1) = d_1$, $g(c_2) = d_2$, we must have $c_1 \neq c_2$. If $c_1 \neq c_2$ implies $f(a_1) \neq f(a_2)$. Then since $f(a_1) \neq f(a_2)$ and f is one-to-one, we have $a_1 \neq a_2$.

To wrap up, $g(f(a_1)) \neq g(f(a_2))$ implies $a_1 \neq a_2$, so $g \circ f$ is one-to-one.

Problem 5.6

Suppose $f : A \rightarrow B$ and $g : C \rightarrow D$ are functions such that $g \circ f$ is defined. Prove that for every $X \subseteq D$, we have

$$f^{-1}[B \cap g^{-1}[X]] = (g \circ f)^{-1}[X].$$

(\subseteq) Let $a \in f^{-1}[B \cap g^{-1}[X]]$, then $f(a) \in B \cap g^{-1}[X]$, which means $f(a) \in g^{-1}[X]$. Since $f(a) \in g^{-1}[X]$, we have $g(f(a)) \in X$.

Since $g(f(a)) \in X$ we have $a \in (g \circ f)^{-1}[X]$.

(\supseteq) Let $a \in (g \circ f)^{-1}[X]$, then $g(f(a)) \in X$. Therefore $f(a) \in B$ since $f : A \rightarrow B$, and $f(a) \in g^{-1}[X]$ since $g(f(a)) \in X$.

Yet, we have $f(a) \in B \cap g^{-1}[X]$. We can conclude that $a \in f^{-1}[B \cap g^{-1}[X]]$.

More Practices For Midterm!

Problem

Come up with a set D and three predicates $P(x)$, $Q(x)$, and $R(x)$, all with domain D , such that

$$\forall x(P(x) \rightarrow Q(x)) \vee \forall x(P(x) \rightarrow R(x))$$

and

$$\forall x(P(x) \rightarrow (Q(x) \vee R(x)))$$

have opposite truth values. Briefly justify your answer.

Consider $D = \{9, 15\}$ with the predicates

- $P(x)$ be “ x is in D ”
- $Q(x)$ be “ x is a multiple of 5”
- $R(x)$ be “ x is a perfect square”

Then the statement $\forall x(P(x) \rightarrow Q(x))$ is false since $x = 9$ is not a multiple of 5. The statement $\forall x(P(x) \rightarrow R(x))$ is false too since $x = 15$ is not a perfect square, hence

$$\forall x(P(x) \rightarrow Q(x)) \vee \forall x(P(x) \rightarrow R(x))$$

is false.

However the statement $\forall x(P(x) \rightarrow (Q(x) \vee R(x)))$ is true since $x = 15$ satisfies $Q(x)$ and $x = 9$ satisfies $R(x)$.

Problem

We aim to prove that every rational number between 0 and 1 can be written as the sum of distinct positive reciprocals. (This is stated precisely in d).)

- (a) Suppose $n < m$ are positive integers such that n does not divide m . Use well-ordering to prove that there is a **smallest** positive integer a such that

$$a \leq m - 1 \quad \text{and} \quad \frac{1}{a} < \frac{n}{m}.$$

Be sure to point out where you use the assumption that n does not divide m .

- (b) In the context of a), prove further that

$$an - m < n.$$

Be sure to point out where you use the assumption that n does not divide m .

- (c) In the context of a), prove further that

$$\frac{n}{m} < \frac{2}{a}.$$

(Suggestion: Use b).)

- (d) Using a)–c) or otherwise, prove that for every rational number r such that $0 < r < 1$, there are **distinct** positive integers $\{a_i\}_{i=0}^j$ such that

$$r = \sum_{i=0}^j \frac{1}{a_i}.$$

- (a) From the second inequality, we have $m/n < a$. Since n does not divide m , $n \neq 1$ since 1 divides every positive integer, hence n is at least 2 by the well-ordering principle on $\mathbb{N}^+ - \{1\}$.

Now we claim that such a exists. First, we show the existence of a .

Since n is at least 2, m is at least 3. Choose $a = m - 1 \geq 2$, we want to show that $m/n < m - 1$.

First, since $n \geq 2$ and $m \geq 3$, we have

$$\frac{1}{m} + \frac{1}{n} \leq \frac{1}{2} + \frac{1}{3} < 1$$

Multiplying both sides by mn ,

$$\begin{aligned} m + n &< mn \\ m &< n(m - 1) \end{aligned}$$

$$\frac{m}{n} < m - 1$$

Since the set of all possible values of a is nonempty, and is a subset of \mathbb{N} , there must be a smallest value due to well-ordering.

- (b) For the sake of contradiction let there be a smaller value than a , then it must be at least $a - 1$, contradicting that a is the smallest value, therefore $a - 1 \leq m/n$. But since n does not divide m , m/n is not an integer, so $a - 1 < m/n$.
- (c) We have proved in (a) that $m/2 < m - 1$ for all $m \geq 3$. If $a \geq 3$, we have

$$\frac{a}{2} < a - 1 < \frac{m}{n}$$

Thus $n/m < 2/a$.

However, if $a = 2$ (we have shown in (a) that $a = 2$ is the minimum possible value of a), we have

$$\frac{a}{2} = a - 1 < \frac{m}{n}$$

- (d) Consider the fraction n/m , which is less than 1 since $n < m$ and greater than 0. We will prove by induction.

Let $P(n, m)$ be the predicate that $r = n/m$ is representable as a sum of reciprocals of distinct positive integers.

Base Case: $n = 1$, we have

$$r = \frac{1}{m}$$

Inductive Step: Assume that for all $1 \leq k < n$, we have $P(k, m)$ is true, regardless the choice of m ($m > k$). Now we want to prove that $P(n, m)$ is true, for all positive integer $m > n$.

First choose $a_0 = a$, so

$$\frac{n}{m} - \frac{1}{a} = \frac{an - m}{am}$$

Since we have proved that $an - m < n$, it suffices to show that $a_1 > a_0 = a$.

By $an - m < n$, $a/2 < n/m$, and that $\frac{an - m}{ma} - \frac{1}{a_1} \geq 0$, we can deduce that

$$\begin{aligned} a &\geq 2 \\ a^2 &\geq 2a \\ \frac{a^2}{2} &\geq a \end{aligned}$$

Therefore,

$$a_1 \geq \frac{am}{an - m} > \frac{am}{n} > \frac{a^2}{2} \geq a$$

This means that in the representation of $\frac{an - m}{am}$, each term in the sequence $\{a_i\}$ is greater than a , and by our induction hypothesis, we have proved that $\frac{n}{m}$ is representable. \square

Problem

Prove or disprove each of the following statements:

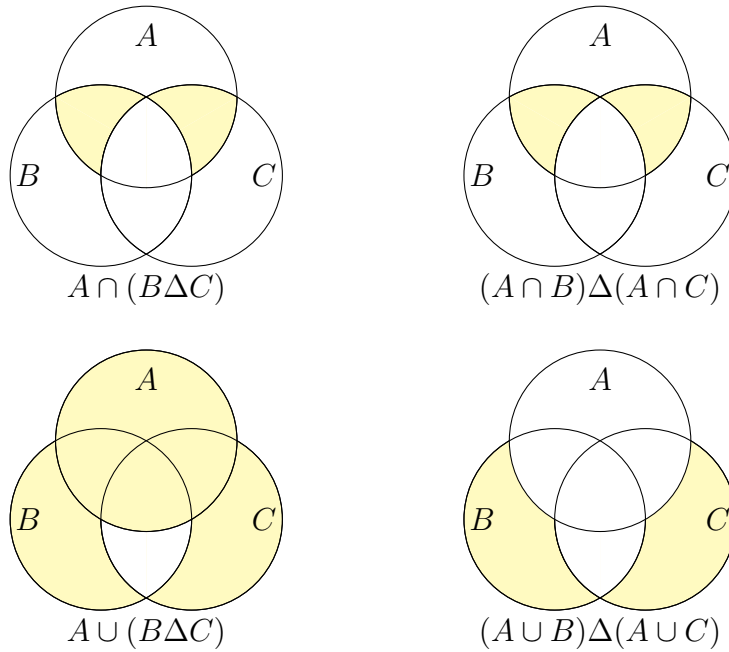
- (a) For all sets A , B , and C ,

$$A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C).$$

- (b) For all sets A , B , and C ,

$$A \cup (B \Delta C) = (A \cup B) \Delta (A \cup C).$$

We may first draw the Venn diagram (not a formal proof) to illustrate.



- (a) I claim that this is true.

(\subseteq) Let $a \in A \cap (B \Delta C)$, then $a \in A$ and $a \in B \Delta C$, which implies that either $a \in B$ or $a \in C$ but $a \notin B \cap C$. By symmetry, assume that $a \in B$.

Thus $a \in A \cap B$ but $a \notin A \cap C$, therefore $a \in (A \cap B) \Delta (A \cap C)$.

(\supseteq) Let $a \in (A \cap B) \Delta (A \cap C)$, then either $a \in A \cap B$ or $a \in A \cap C$ but not both. By symmetry, assume $a \in A \cap B$ and $a \notin A \cap C$, then $a \in A$ and $a \in B$ but $a \notin C$.

So $a \in B\Delta C$ since $a \in B$ but $a \notin C$, and that since $a \in A$, we have $a \in A \cap (B\Delta C)$.

(b) I claim that this is false.

Consider an element $a \in A$ but $a \notin B$ and $a \notin C$, then surely $A \in A \cup (B\Delta C)$.

But since $a \in A \cup B$ and $a \in A \cup C$, we have $a \notin (A \cup B)\Delta(A \cup C)$.

Problem

For every set F , we define its closure

$$\text{cl}(F) = \bigcup_{X \in F} \mathcal{P}(X).$$

Prove that for every set F ,

$$\text{cl}(\text{cl}(F)) = \text{cl}(F).$$

Experimenting by $F = \{\{a, b\}, \{a, c\}, \{d\}\}$, then

$$\text{cl}(F) = \{\emptyset, \{a\}, \{b\}, \{a, b\}, \{c\}, \{a, c\}, \{d\}\}$$

$$\text{cl}(\text{cl}(F)) = \{\emptyset, \{a\}, \{b\}, \{a, b\}, \{c\}, \{a, c\}, \{d\}\}$$

the set of all subsets of the sets in F .

(\subseteq) Let $A \in \text{cl}(\text{cl}(F))$, then

$$A \in \bigcup_{Y \in \text{cl}(F)} \mathcal{P}(Y)$$

which means that there exists some set $Y \in \text{cl}(F)$ such that $A \in \mathcal{P}(Y)$. Yet $A \subseteq Y$.

On the other hand, since $Y \in \text{cl}(F)$, there exists some $X \in F$ such that $Y \in \mathcal{P}(X)$. Since $Y \in \mathcal{P}(X)$, we know that $Y \subseteq X$. All together with $A \subseteq Y$, we have $A \subseteq X$ so $A \in \mathcal{P}(X)$.

Lastly we have

$$A \in \bigcup_{X \in F} \mathcal{P}(X)$$

as desired.

(\supseteq) Let $A \in \text{cl}(F)$, then $A \in \bigcup_{X \in F} \mathcal{P}(X)$, which means that there exists some

$X \in F$ such that $A \in \mathcal{P}(X)$, or that $A \subseteq X$. Since $X \in \mathcal{P}(X)$, $X \in \text{cl}(F)$ and by definition,

$$\text{cl}(\text{cl}(F)) = \bigcup_{Y \in \text{cl}(F)} \mathcal{P}(Y)$$

Choose $Y = X$, then since $X \in \text{cl}(X)$ and $X \in \mathcal{P}(X)$, we have $X \in \text{cl}(\text{cl}(F))$.

Problem

Prove for every two distinct irrational numbers, there is an irrational number (strictly) in between.

Claim — The sum of an irrational number and a rational number is irrational.

Proof. Assume towards a contradiction, let $r \neq 0$ be an irrational number and q be a rational number, and $r + q = s$ and s is a rational number.

Let $q = a/b$ and $s = c/d$ ($bd \neq 0$) so we have

$$r = \frac{c}{d} - \frac{a}{b} = \frac{bc - ad}{bd}$$

contradiction since r is irrational. ■

Now consider two irrational numbers r and s such that $r < s$, consider $d = s - r$. Since we can always express d in the decimal form

$$d = \overline{a_1 a_2 \dots a_k . a_{k+1} a_{k+2} \dots}$$

From left to right, iterate through all numbers until we have the first number $a_i \neq 0$ at some decimal place K .

Case 1: If $a_i \neq 1$ then consider the number d' , for which the K decimal place equals $a_i - 1$ and all the other digits being 0. Then $0 < d' < d$, and d' is a rational number since we can express d' in the form of $(a_i - 1)/10^n$ for some integer n .

Now consider the irrational number $r + d'$, which has been proven irrationality in our claim.

We have

$$r < r + d' < r + d = s$$

Case 2: If $a_i = 1$, then consider the number d'' , for which the decimal place right of a_i (this decimal place is originally a_{i+1} in d) equals 1. Similarly, we have $0 < d'' < d$ and we can express d'' as 10^{-n} for some integer n .

Therefore we consider the number $r + d''$, gives

$$r < r + d'' < r + d = s$$

as desired.

Even even even more problems

Problem

Prove or disprove: For all predicates $P(x), Q(x), R(x)$ with domain D ,

$$\forall x((P(x) \vee Q(x)) \rightarrow R(x))$$

and

$$\forall x(P(x) \rightarrow (Q(x) \vee R(x)))$$

have different truth values.

Problem

Let X be any set such that $\emptyset \in X$ and such that for any $x \in X$, one has $\{x\} \in X$.

The sequence A_1, A_2, \dots of elements of X is defined recursively as follows:

$$A_1 := \emptyset, \quad \text{and} \quad \text{for each } n \in \mathbb{N}, \text{ we let } A_{n+1} := \{A_n\}.$$

Show that for any $i, j \in \mathbb{N}$ with $i \neq j$, one has $A_i \neq A_j$.

Problem

Prove that

- (a) For all sets A, B and C ,

$$A \Delta B \Delta C = (A \cap B \cap C) \cup (A - (B \cup C)) \cup (B - (C \cup A)) \cup (C - (A \cup B))$$

- (b) For a function f^{-1} and sets A, B ,

$$f^{-1}[A \Delta B] = f^{-1}[A] \Delta f^{-1}[B]$$

Problem

Prove or disprove

- (a) For any sets A and B , there exists a unique set X with the following property:

$$\text{For any set } T, \text{ one has } T \subseteq X \text{ if and only if } T \cup B \subseteq A.$$

- (b) For any sets A and B , there exists a unique set X with the following property:

$$\text{For any set } T, \text{ one has } T \supseteq X \text{ if and only if } T \cup B \supseteq A.$$

Problem

Define $\prod_{i=1}^n A_i = A_1 \times A_2 \times \cdots \times A_n$ for $n \geq 2$, prove that

$$\left(\prod_{i \in I} A_i \right) - \prod_{i \in I} B_i = \bigcup_{\substack{j \in I \\ A_j \not\subseteq B_j}} \left[(A_j - B_j) \times \prod_{\substack{i \in I \\ i \neq j}} A_i \right]$$

Problem

The *Fibonacci numbers* f_n , $n \in \mathbb{Z}^+$, are defined recursively by the formulas $f_1 = 1$, $f_2 = 1$, and $f_n = f_{n-1} + f_{n-2}$ for all $n \geq 3$.

- Find the first ten Fibonacci numbers f_1, \dots, f_{10} .
- Compute $f_1 + f_2$, $f_1 + f_2 + f_3$, $f_1 + f_2 + f_3 + f_4$, $f_1 + f_2 + f_3 + f_4 + f_5$.
- Conjecture a formula for the sum $f_1 + \cdots + f_n$ of the first n Fibonacci numbers, where $n \geq 1$, and then prove the formula is correct using induction.
- Use induction to prove that for all integers $k \geq 1$, $5 \mid f_{5k}$.

Problem

Prove for every two irrational numbers, there is a rational number strictly in between.

Problem

Prove that for all $x \in \mathbb{R}$, at least one of $\sqrt{3} + x$ and $\sqrt{3} - x$ is irrational.

Assume otherwise, let $\sqrt{3} - x$ and $\sqrt{3} + x$ are rational numbers, then $(\sqrt{3} - x) + (\sqrt{3} + x)$ is a rational number, which is obviously false.

The Actual Midterm Problems**Problem**

Come up with predicates $P(x)$ and $Q(x)$ with the same domain such that the formulas

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

and

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

have opposite truth values. Briefly justify your answer.

Problem

Recall the Fibonacci numbers:

Problem**Problem****Problem**

§6 Number Theory

6.1 Some Terminologies

- **Divisibility**: If a divides b then $a|b$.
Division Theorem: Let a, b be positive integers, then there exists unique (q, r) such that $a = qb + r$, where
 - q , the **quotient**, a nonnegative integer and
 - r , the **remainder**, an integer satisfying $0 \leq r < b$.
- Prime generating number:

$$p_1 p_2 p_3 \cdots p_n + 1$$

- The **greatest common divisor** of a, b , denoted by $\gcd(a, b)$ is the largest positive divisor that divides both a, b .
- The **lowest common multiple** of a, b , denoted by $\text{lcm}(a, b)$ is the least positive integer that can be divided by a, b .
- **Ideals** in \mathbb{Z} : Let I be a nonempty subset of \mathbb{Z} , then I is an ideal if:
 - For every $a, b \in I$, $a - b \in I$.
 - For every $a \in I$, if $n \in \mathbb{Z}$ then $an \in I$.
- **Bézout's Identity**: For nonzero integers a, b , there is some positive integer k , such that $k|a$ and $k|b$ then there exists some integers m, n such that $ma + nb = k$.
- **Fundamental Theorem of Arithmetic**: For each positive integer a , there exists a **finite support** $e_a : \mathcal{P} \rightarrow \mathbb{N}$ such that

$$a = \prod \{p^{e_a(p)} : e_a(p) \neq 0\}$$

with \mathcal{P} the set of primes.

Moreover, $a \mapsto e_a$ is a bijection. That is, **every positive integer has a unique prime factorization**.

6.2 Properties of Ideals in \mathbb{Z}

- Any ideal is either $\{0\}$ or an unbounded set (It is both unbounded above and below).
- Every two consecutive elements in I is “equally spaced”.
- For elements $a_1, a_2, a_3, \dots, a_n \in I$, their linear combination (in \mathbb{Z}) is also in I .
- There exists a unique positive integer $k \in I$ so that $I = \{nk : n \in \mathbb{Z}\}$.
- For every $a, b \in I$, $\gcd(a, b) \in I$.

6.3 Modular Arithmetic

- Define $R_b(a) \in \{0, 1, 2, \dots, b-1\}$ to be the remainder when a is divided by b .
- Define $[b] = \{0, 1, 2, \dots, b-1\}$, the set of remainders when divided by b .
- The addition in $[b]$ is defined as

$$R_b(a) +_b R_b(a') = R_b(a + a')$$

This is defined since

- $R_b(a) + R_b(a')$ always has a value.
- There is only one unique value $R_b(a + a')$.

We may define multiplication \cdot_b similarly.

- **Congruence Classes:** The set $C_b(a)$ is the set of all integers x satisfying $R_b(x) = R_b(a)$.
- **Universal Property of C_b :** Let X be a set and $f : \mathbb{Z} \rightarrow X$ is a function such that if $b|(a - a')$ then $f(a) = f(a')$, then there is a **unique** function $g : Q_b \rightarrow X$ such that

$$f = g \circ C_b$$

Sketch of Proof: We shall prove that there's at least one function, that is, consider the function

$$g(C) = f(a)$$

for all $a \in C$. It can be shown that g is well-defined.

Now assume that there exists another function h that satisfies all the said properties. Then for all C_b , we have

$$g(C_b(a)) = f(a) = h(C_b(a))$$

so indeed $g = h$.

6.4 Tutorial 5

Problem 6.1

Suppose $f : \mathbb{N} \rightarrow \mathbb{N}$ is a function. Prove that if $A \subseteq \mathbb{N}$ is bounded, then $f[A]$ is bounded as well.

We will prove by induction.

Base Case: If A is bounded by 0, then $f[A] = \{f(0)\}$ is bounded.

Inductive Step: Assume that all sets A bounded by $k \in \mathbb{N}$ for all $k \leq n$ with $n \in \mathbb{N}$, $f[A]$ is bounded. Consider some set bounded by $n + 1$, that is, the largest element in A equals $n + 1$. By considering $f \upharpoonright A - \{n + 1\}$, this function is bounded. Assume that $f[A - \{n + 1\}]$ is bounded by M , then $f[A]$ is bounded by $\max\{M, f(n + 1)\}$.

Problem 6.2

Prove that for every function $f : X \rightarrow Y$ and every family $(A_i)_{i \in I}$ of subsets of X , we have $f[\bigcap_{i \in I} A_i] \subseteq \bigcap_{i \in I} f[A_i]$. When does equality hold?

Let $a \in f[\bigcap_{i \in I} A_i]$, then there exists some $x \in \bigcap_{i \in I} A_i$ such that $f(x) = a$. So we have $x \in A_i$ for all $i \in I$. This means that $a \in f[A_i]$ for all $i \in I$. Hence $a \in \bigcap_{i \in I} f[A_i]$.

For every $a \in \bigcap_{i \in I} f[A_i]$, $a \in f[A_i]$ for all A_i . Thus for each A_i , there exists some $x_i \in A_i$ such that $f(x_i) = a$ (can have multiple x in A_i). If $a \in f[\bigcap_{i \in I} A_i]$, then some x has to be in all of A_i . Equality holds when the said criteria is satisfied.

Problem 6.3

Prove that a function $f : A \rightarrow B$ is onto if and only if whenever functions $g, h : B \rightarrow C$ are such that $g \circ f = h \circ f$, then $g = h$.

(\Rightarrow) Let f be a surjective function, then for every $b \in B$, there exists some $a \in A$ such that $f(a) = b$. Thus for every $b \in B$, we have $g(b) = h(b)$, so $g = h$.

(\Leftarrow) Let $g \circ f = h \circ f$ and $g = h$. Since g, h are functions, every $g(b)$ with $b \in B$ must be defined. Therefore, for each $b \in B$, there exists some $a \in A$ such that $f(a) = b$ is defined, therefore f is surjective.

Problem 6.4

Say an integer is 1 mod 4 if it equals $4k + 1$ for some integer k .

1. Prove that if integers a and b are 1 mod 4, then ab is 1 mod 4.
2. Prove by strong induction on x that if all primes which divide $x \in \mathbb{N}^+$ are 1 mod 4, then x is itself 1 mod 4.
3. Prove that the set of primes which are **not** 1 mod 4 is unbounded.

1. Let $a = 4k + 1$ and $b = 4\ell + 1$ for some integers k, ℓ , then

$$ab = (4k + 1)(4\ell + 1) = 4(4k\ell + k + \ell) + 1$$

2. **Base Case:** The first prime in the form of $4k + 1$ is 5.

Inductive Step: Assume that all integers n satisfying $1 \leq n \leq x$, if n is in the form of 1 mod 4, then all primes which divides n are also in the form of 1 mod 4. We want to show that $x + 4$ satisfies the statement.

If $x + 4$ is prime, then we are done.

Hence assume otherwise, $x + 4$ is not prime. Let p be a prime dividing $x + 4$, set $x + 4 = pm$ for some integer m , we have $1 < p, m < x + 4$. By our induction hypothesis, both p and m are in the form of 1 mod 4 since the largest value of p and m is x and not $x + 1, x + 2$ or $x + 3$. Therefore by 1. $x + 4 = pm$ is in the form of 1 mod 4.

3. The primes that are not in the form of 1 mod 4 are
 - in the form of 2 mod 4, the only prime is 2.
 - in the form of 3 mod 4, the first few primes are 3, 7, 11, ...

Therefore, it will be worth discussing the boundedness of the primes in the form of 3 mod 4.

By 2., the contrapositive statement states that if x is in the form of 3 mod 4 (which is not in the form of 1 mod 4), then not all of the primes dividing x is in the form of 1 mod 4.

Assume towards a contradiction, consider the sequence $p_1, p_2, p_3, \dots, p_N$, all prime numbers greater than 3 in the form of 3 mod 4 in increasing order. Thus p_N is the greatest prime satisfying the statement. The first few terms

are 7, 11, 19, Consider the number

$$M = 4p_1p_2p_3 \dots p_N + 3$$

This number has at least one prime divisor d in the form of $3 \bmod 4$, but not p_i for all $i = 1, 2, 3, \dots, N$ since they leave a remainder 3 when dividing M .

Now we know that d is not in the sequence $\{p_i\}$, by our assumption we obtain $d > p_N$, contradiction.

§7 Relations

- An equivalence relation \sim should satisfy 3 criteria:
 1. **Reflexive**: $a \sim a$.
 2. **Symmetric**: $a \sim b$ implies $b \sim a$.
 3. **Transitive**: $a \sim b$ and $b \sim c$ implies $a \sim c$.
- Let \sim be a relation on A . The **quotient** is defined as A/\sim ,

$$A/\sim = \{\{a' \in A : a' \sim a\} \in \mathcal{P}(A) : a \in A\}$$

For example, let the equivalence relation be \sim such that if $R_b(a) = R_b(a')$ then $a \sim a'$ for some positive integer b . Then the quotient set on the nonnegative integer is

$$\{\{0, b, 2b, \dots\}, \{1, b+1, 2b+1, \dots\}, \dots, \{b-1, 2b-1, 3b-1, \dots\}\}$$

Another example, let the relation be the usual equality on the set \mathbb{Z} , then

$$\mathbb{Z}/\sim = \{\dots, \{-2\}, \{-1\}, \{0\}, \{1\}, \{2\}, \dots\}$$

- The **equivalence class** of $a \in A$ is denoted by $[a]_\sim$, that is,

$$[a]_\sim = \{a' \in A : a' \sim a\}$$

- The **quotient map** π of some element $a \in A$ is defined by

$$\pi(a) = [a]_\sim$$

It can be shown that

$$(a \sim a') \rightarrow ([a]_\sim = [a']_\sim) \rightarrow (\exists b \in A)(a, a' \in [b]_\sim) \rightarrow ([a]_\sim \cap [a']_\sim \neq \emptyset)$$

- **Universal Property of Equivalence Relations**: Let X be a set and $f : A \rightarrow X$ is a function such that if $a \sim a'$ then $f(a) = f(a')$, then there is a **unique** function $g : A/\sim \rightarrow X$ such that

$$f = g \circ \pi$$

- Let $\mathbf{Maps}(A, B)$ denote the set of all functions from A to B . Thus by the Universal Property of Equivalence Relations, the function

$$\mathbf{Maps}(A/\sim, X) \rightarrow \{f \in \mathbf{Maps}(A, X) : (\forall a, b \in A)(a \sim b \rightarrow f(a) = f(b))\}$$

is a bijection.

- A **partition** of a set X is a set $P \subseteq \mathcal{P}(X) - \{\emptyset\}$ given by
 - $\bigcup P = X$
 - $C, D \in P \rightarrow C \cap D = \emptyset$ or $C = D$

Thus the quotient set A/\sim is a partition of A .

Moreover the function

$$\mathcal{G} : \{\text{equivalence relations on } A\} \rightarrow \{\text{partitions of } A\}$$

is bijective.

Sketch of Proof: First note that $P = A/\sim$, so \mathcal{G} is well-defined and surjective. Since we can construct a function \mathcal{H} such that it maps a partition to an equivalence relation in A , so \mathcal{G} is bijective.

- Constructing \mathbb{Z}, \mathbb{Q}

Consider the equivalence relation \sim given by $(m, n) \sim (p, q)$ if

$$m + q = n + p$$

for all $m, n, p, q \in \mathbb{N}$. Thus $\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/\sim$. We may define the addition on \mathbb{Z} by

$$[(m, n)]_{\sim} +_{\mathbb{Z}} [(p, q)]_{\sim} = [(m + p, n + q)]_{\sim}$$

Similarly, we may construct \mathbb{Q} from \mathbb{Z} . Consider a relation \approx given by $(m, n) \approx (p, q)$ if

$$m \cdot_{\mathbb{Z}} q = n \cdot_{\mathbb{Z}} p$$

for all $(m, n), (p, q) \in \mathbb{Z} \times (\mathbb{Z} - \{0_{\mathbb{Z}}\})$.

7.1 Tutorial 6

Problem 7.1

Prove that if I is an ideal, then there is a unique positive integer $k \in I$ such that $I = \{nk : n \in \mathbb{Z}\}$.

Whenever a positive integer satisfies the property of k in the problem, then this number is *aquaesulian*.

For the sake of contradiction, assume that there are more than one aquaesulian numbers, let the two smallest possible values be k and k' with $k < k'$. This

means that other aquaesulian numbers must be greater than k .

Obviously k, k' are in I . But we can see that

$$0 < k < k'$$

By choosing k' , we will not be able to represent k in terms of nk' , therefore a contradiction.

Problem 7.2

Prove that if I is an ideal and $a, b \in I$, then $na + mb \in I$ for every $n, m \in \mathbb{Z}$. Conclude that if $a, b \in I$ are nonzero, then $\gcd(a, b) \in I$ as well.

Since $a \in I$, then for every $n \in \mathbb{Z}$, $na \in I$. Similarly, $-mb \in I$. So $na - (-mb) \in I$.

Since $|a|, |b| \in I$, so without loss of generality assume $a, b > 0$. By Bézout's Identity, there exists integers m, n so that $na + mb = \gcd(a, b)$, hence $\gcd(a, b) \in I$.

Problem 7.3

Prove that if a, b , and k are positive integers, then $\gcd(ka, kb) = k \cdot \gcd(a, b)$. (Suggestion: use Bézout's identity.)

Claim — For every prime p , positive integers a, b , we have $e_{\gcd(a, b)}(p) = \min\{e_a(p), e_b(p)\}$.

Proof. Without loss of generality, assume $e_a(p) \leq e_b(p)$. If it happens that for some p , $e_{\gcd(a, b)}(p) > e_a(p)$, then $\gcd(a, b)$ does not divide a . Therefore we proved our claim by maximality of $e_{\gcd(a, b)}(p)$. ■

Assume for some prime $e_a(p) \leq e_b(p)$, then

$$e_{\gcd(ka, kb)}(p) = e_{ka}(p) = e_k(p) + e_a(p) = e_k(p) + e_{\gcd(a, b)}(p) = e_{k \cdot \gcd(a, b)}(p)$$

Remark. We can prove that if $a|b$ and $b|a$ then $a = b$.

Remark. A rather clever way is to let $a = \gcd(a, b) \cdot c$ and $b = \gcd(a, b) \cdot d$.

Problem 7.4

Suppose a, b, c are nonzero integers such that $c \mid ab$.

1. Define $I = \{n \in \mathbb{Z} : c \mid an\}$. Prove that I is an ideal.
2. Use part 1 to prove that $c \mid a \cdot \gcd(b, c)$.

1. First we show that I has at least two elements, b and c are both in I .

Now assume that n and n' are in I , then $n - n'$ is in I since $c|a(n - n')$.

Moreover, if $c|an$, then for every integer m , $c|anm$ so nm is in I .

2. By Bézout's identity, if b, c are in I then $\gcd(b, c)$ is in I , so choose $n = \gcd(b, c)$, we have $c|a \cdot \gcd(b, c)$.

Problem 7.5

A positive integer a is said to be *square-free* if there is no integer $k \geq 2$ such that $k^2 \mid a$. Prove that a is square-free if and only if $e_a(p) \leq 1$ for all primes p .

Assume otherwise, there exists some prime p' such that $e_a(p') \geq 2$.

We have

$$a = (p')^{e_a(p')} \times \prod \{p^{e_a(p)} : e_a(p) \neq 0 \wedge p \neq p' \wedge p \in P\}$$

Let the latter product be m , which is a positive integer. Note that

$$a = (p')^{e_a(p')}m = (p')^2 \times (p')^{e_a(p')-2}m$$

Hence a is now divisible by $(p')^2$.

Problem 7.6

Suppose a, b , and k are positive integers. Prove that $(\gcd(a, b))^k = \gcd(a^k, b^k)$.

Let p be a prime and without loss of generality assume $e_a(p) \leq e_b(p)$, so $e_{a^k}(p) \leq e_{b^k}(p)$. Then

$$\begin{aligned} e_{(\gcd(a, b))^k}(p) &= k e_{\gcd(a, b)}(p) = k e_a(p) \\ e_{\gcd(a^k, b^k)}(p) &= e_{a^k}(p) = k e_a(p) \end{aligned}$$

Problem 7.7

Given $b \in \mathbb{N}^+$, prove that the function $\cdot_b : [b] \times [b] \rightarrow [b]$ defined by $R_b(a) \cdot_b R_b(a') = R_b(a \cdot a')$ is well-defined.

- (i) We first prove that for every c, d in $[b]$, $c \cdot_b d$ has a value. This is true since R_b is onto.
- (ii) Now we prove that for every c, d in $[b]$, $c \cdot_b d$ has at most one value.

Assume that there exists a_1, a'_1, a_2, a'_2 such that $R_b(a_1) = R_b(a_2) = c$ and $R_b(a'_1) = R_b(a'_2) = d$. By the Division theorem, assume that

$$a_1 = bq_1 + c$$

$$a'_1 = bq'_1 + d$$

$$a_2 = bq_2 + c$$

$$a'_2 = bq'_2 + d$$

Thus $R_b(a_1 \cdot a'_1) = cd = R_b(a_2 \cdot a'_2)$. Followed by $b|(a_1 \cdot a'_1 - a_2 \cdot a'_2)$ we have $R_b(a_1 \cdot a'_1) = R_b(a_2 \cdot a'_2)$ as desired.

Problem 7.8

Given $b \in \mathbb{N}^+$:

1. Prove that the "function" $\oplus : [b] \times \mathbb{Z} \rightarrow [b]$ defined by $R_b(a) \oplus a' = a + a'$ is **not well-defined**.
2. Prove that the "function" $\boxplus : [b] \times \mathbb{Z} \rightarrow \mathbb{Z}$ defined by $R_b(a) \boxplus a' = a + a'$ is **not well-defined**.

1. We want to show that $a + a'$ does not always have a value in $[b]$. By letting $a' = b$ we have $a + a' \geq b$ which is certainly not in $[b]$.
2. We want to show that $a + a'$ can have more than one values. Note that

$$a + a' = R_b(a) \boxplus a' = R_b(a + b) \boxplus a' = a + b + a'$$

But we know that b cannot equal to 0, hence a contradiction.

§8 Cardinality

8.1 Finite Sets

- We say that two sets A and B is **equinumerous** $A \approx B$ if there exists a bijection between A and B .

Therefore, a set is **finite** if it is equinumerous to some $[n]$ where $n \in \mathbb{N}$. If a set is not finite, then it is **infinite**.

- **Cantor Theorem** states that for every set X , $X \not\approx \mathcal{P}(X)$.

Sketch of Proof: Consider a function $f : X \rightarrow \mathcal{P}(X)$. Consider $A \in \mathcal{P}(X)$ such that

$$A = \{x \in X : x \notin f(x)\} \in \mathcal{P}(X)$$

We claim that there doesn't exist an element $x \in X$ that maps to A .

If $x \in A$ then $f(x) = A$ contradicting the definition of A since $x \notin f(x)$.

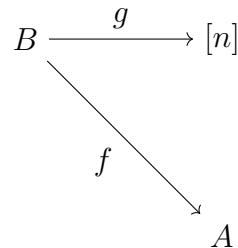
If $x \notin A$ then there is some $y \in X$ such that $f(y) = A$, then $y \in A$, contradiction.

- Pigeonhole Principle on $[n]$: Every injective function $f : [n] \rightarrow [n]$ is surjective.

It can be proved that for every finite set A , there is a unique n such that $A \approx [n]$.

- Let $A \approx [n]$ for some $n \in \mathbb{N}$, we say that A has **cardinality** n , denoted by $|A| = n$.
- If $A \subsetneq B$ and B is finite, then there is no injection from B to A .

Sketch of Proof:



Consider a bijective function $g : B \rightarrow [n]$. If f happens to be injective, then the function

$$g \circ f \circ g^{-1} : [n] \rightarrow [n]$$

is injective as well (since g^{-1} and f are injective). By the Pigeonhole principle $g \circ f \circ g^{-1}$ is surjective, hence it is bijective.

Choose some $b \in B - A$ such that $g(b) \in [n]$. Thus there exists some $m \in [n]$ such that

$$g(f(g^{-1}(m))) = g(b)$$

Since g is injective so $f(g^{-1}(m)) = b$. But we know that fact that $b \notin A$ hence $b \notin \text{range}(f)$, thus a contradiction.

- Some properties of finite sets include:
 - The subset of a finite set is finite.
 - If A, B is finite with $A \subsetneq B$, then $|A| < |B|$.
 - If A and B are finite, then $|A| \leq |B|$ if and only if there is an injection from A to B .

8.2 Infinite Sets

- We say that a set $A \subseteq \mathbb{R}$ is bounded in \mathbb{R} if there exists $u, \ell \in \mathbb{R}$ such that for all $a \in A$, $\ell \leq a \leq u$. Otherwise, it is **unbounded** in \mathbb{R} .
- **Archimedean Property**: For every positive integers x, y there exists a positive integer n such that $nx > y$.

Boundedness via Archimedean Property: Assume that A is unbounded in \mathbb{N} , then $A \subseteq \mathbb{Q}$ but we don't know if A is bounded in \mathbb{Q} , similar to \mathbb{R} .

Bounded sets need not to be infinite.

- A set A is **countable** if it is equinumerous to \mathbb{N} or finite. Otherwise A is **uncountable**. If A is equinumerous to \mathbb{N} , we say that A is **countably infinite**.

A set A is countable if and only if A has an injection to \mathbb{N} .

Sketch of Proof:

(\Rightarrow) implies A is finite or $A \approx \mathbb{N}$. If A is finite then we are done, else A has a bijection to \mathbb{N} .

(\Leftarrow) Consider an injection $f : A \rightarrow \mathbb{N}$. Consider $g : \mathbb{N} \rightarrow \text{range}(f)$. If $\text{range}(f)$ is finite then we are done. Otherwise, we “count” the elements as follows:

Let

$$g(n) = \min(\text{range}(f) - \{g(m) : m < n, m \in \mathbb{N}\})$$

Then g is a bijection from \mathbb{N} to $\text{range}(f)$, hence $A \approx \mathbb{N}$.

- Some properties that follow:
 - Any subset of a countable set is countable.
 - If $X \subseteq \mathbb{N}$ then $X \approx \mathbb{N}$.
 - If there’s an injection from A to B then there’s a surjection from B to A .
 - A nonempty set A is countable if and only if there’s a surjection from \mathbb{N} to A .
 - The union of two countable sets is countable.
- The Cartesian product of two countable sets is countable.

Sketch of Proof: Consider $f : A \rightarrow X$ and $g : B \rightarrow Y$ be bijections, hence $A \times B \approx X \times Y$ so $(a, b) \rightarrow (f(a), g(b))$ is a bijection.

Hence, the Cartesian product of a finite number of countable sets is countable.

- $\text{Maps}([n], X) \approx X^n$ for $n \in \mathbb{N}$.

Sketch of Proof: We proof by induction. It suffices to prove that

$$\text{Maps}([n+1], X) \approx \text{Maps}([n], X) \times X$$

Consider the bijection from the function $f \in \text{Maps}([n+1], X)$ to $(f \upharpoonright [n], f(n))$.

The mapping is injective. Assume $f \neq g$ but they map to the same image $(f \upharpoonright [n], f(n))$. By definition we must have a and $a \in [n+1]$ such that $f(a) \neq g(a)$. If $a \in [n]$ then $f \upharpoonright [n] \neq g \upharpoonright [n]$. If $a = n$ then $f(n) \neq g(n)$. Either case leads to a contradiction.

The mapping is surjective since for every function f , we have $[n] \cup \{n\} = [n+1]$, hence $(f \upharpoonright [n], f(n))$ is defined and there is such function $f \in \text{Maps}([n+1], X)$.

- A corollary will be if $A \approx B$ then $\text{Maps}(A, X) \approx \text{Maps}(B, X)$.

Sketch of Proof: Fix bijection $f : A \rightarrow B$, then the mapping $g : B \rightarrow X$ to $g \circ f : A \rightarrow X$ is a bijection.

This mapping is injective. For any two distinct functions $g, h \in \text{Maps}(B, X)$, there exists some $b \in B$ such that $g(b) \neq h(b)$. If $g(f(a)) = h(f(a))$ for all $a \in A$, then suppose $f(a) = b$ since f is bijective, then $g(b) = h(b)$, a contradiction.

This mapping is surjective. We may prove that the inverse mapping is injective. Let there be two distinct functions $g_1 \circ f_1 : A \rightarrow X$ and $g_2 \circ f_2 : A \rightarrow X$. Since f is constant, so $g_1 \neq g_2$, hence the inverse mapping is injective.

- Consider $\mathbb{N}^{<\mathbb{N}}$ be the set of all finite sequences of natural numbers. $\mathbb{N}^{<\mathbb{N}}$ is countably infinite. This can be proved by using the Fundamental Theorem of Arithmetic.

Consider $X^{<\mathbb{N}}$, the set of all finite sequences with values in X . If $X \approx \mathbb{N}$ then $X^{<\mathbb{N}} \approx \mathbb{N}$.

- Now if there's an injection $f : A \rightarrow B$, we denote $A \preceq B$. If $A \not\preceq B$ then we write $A \prec B$.
- **Cantor-Schröder-Bernstein Theorem:** For all sets $A \preceq B$ and $B \preceq A$, then $A \approx B$.

Sketch of Proof: Assume injective functions $f : A \rightarrow B$ and $g : B \rightarrow A$. We want to prove that f is surjective.

Assume that f is not surjective, it suffices to show that we can modify f to obtain h such that $h : A \rightarrow B$ is surjective.

Define $C_0 = g[B - \text{range}(f)]$ and $C_{n+1} = g[f[C_n]]$ recursively. Using this “cut and paste” strategy we can define a function $h : A \rightarrow B$ given by

$$h(a) = \begin{cases} g^{-1}(a) & \text{if } a \in C_n \text{ for some } n, \\ f(a) & \text{otherwise.} \end{cases}$$

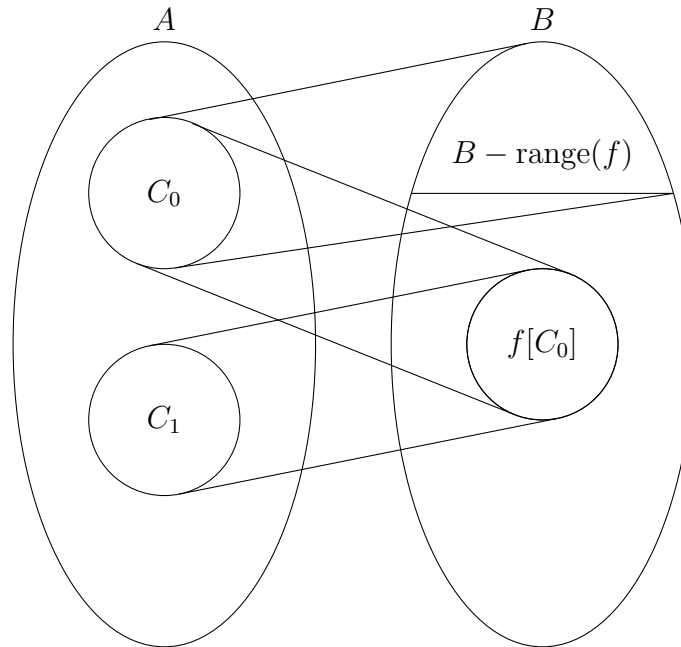
It remains to show that h is well-defined, injective and surjective. Throughout the proof, let $C = \bigcup \{C_0, C_1, C_2, \dots\}$.

First, we notice that each of $C_n \subseteq \text{range}(g)$ along with $A - C$ are pairwise disjoint since g is injective. Similarly, each of $f[C_n]$ along with $f[A - C]$ are pairwise disjoint. Thus h is well-defined since every of $a \in A$, $h(a)$ is defined and has a unique value.

Now we show that h is injective. Assume that $a, a' \in A$ are distinct elements. If $h(a) = g^{-1}(a)$ and $h(a') = g^{-1}(a')$ then we are done by definition of C_n . If $h(a) = f(a)$ and $h(a') = f(a')$ we are done too since f is injective.

Yet, let $h(a) = f(a)$ and $h(a') = g^{-1}(a')$. But we have shown that $f[C_n]$ and $f[A - C]$ are disjoint.

Now we show that h is surjective. If $b \in \text{range}(f) - C$ then choose some a such that $h(a) = f(a) = b$. If $b \in f[C]$ then there is some $a \in A$ such that $g(b) = a$. Thus, choose $h(g(b))$.



- A set is **Dedekind infinite** if it is equinumerous to a proper subset of itself. In fact, every infinite set A is Dedekind infinite.

Sketch of Proof: Consider an injection $f : \mathbb{N} \rightarrow A$. This function is defined due to Choice. Define function $g : A \rightarrow A - \{f(0)\}$ as

$$g(a) = \begin{cases} a & \text{if } a \notin \text{range}(f), \\ f(n+1) & \text{if } a = f(n). \end{cases}$$

The goal here is to “shift” everything in $\text{range}(f)$ by 1. In fact g is obviously bijective. Hence we’ve shown that $A \approx A - \{f(0)\}$.

- A set \mathcal{C} is a **chain** if for every $X, Y \in \mathcal{C}$ we have $X \subseteq Y$ or $Y \subseteq X$.

For example,

$$\{\{1\}, \{1, 3\}, \{1, 3, 4, 5\}, \{1, 3, 4, 5, 7\}\}$$

is a chain. Note that \emptyset and $\{\emptyset\}$ are chains.

- **Zorn’s Lemma:** Suppose \mathcal{S} is a set such that every $\mathcal{C} \subseteq \mathcal{S}$, we have $\bigcup \mathcal{C} \in \mathcal{S}$. Then there’s some $M \in \mathcal{S}$ which is **maximal**, that is, for every $X \in \mathcal{S}$, $M \not\subset X$.

We will prove Zorn’s Lemma in Tutorial 9.

- Let I be an ideal of R , for any ideal I' being a proper subset of I , I' is a

proper ideal of I .

- There is a proper ideal M of some ring R which is maximal, that is, there is no proper ideal I such that $M \subset I$.

Sketch of Proof: Let \mathcal{S} be the set of all proper ideals of R , we shall show that \mathcal{S} satisfies the assumptions of Zorn's Lemma.

Suppose $\mathcal{C} \subseteq \mathcal{S}$ is a chain, it suffices to show that $\bigcup \mathcal{C}$ is a proper ideal. To show this, consider the element 1_R .

If $1_R \in \bigcup \mathcal{C}$ then 1_R is in some element I in \mathcal{C} . But this makes $I = R$ since for every $r \in R$ we have $r \cdot 1_R \in I$.

Now we show that $\bigcup \mathcal{C}$ is an ideal. Let $a \in I$ and $b \in J$ with $I, J \in \mathcal{C}$. Without loss of generality assume $I \subseteq J$, so $a, b \in J$. Since J is an ideal, $a + b \in J$, thus $a + b \in \bigcup \mathcal{C}$.

For some $r \in R$ and $a \in \bigcup \mathcal{C}$ with $a \in I$. Since I is an ideal so $r \cdot a \in I$, hence $r \cdot a \in \bigcup \mathcal{C}$.

Applying Zorn's Lemma gives the desired result.

- For sets A, B , either $A \preceq B$ or $B \preceq A$.

Sketch of Proof: Assume that $A \not\preceq B$, let \mathcal{S} be the set of graphs of injections from A to B such that $\text{dom}(f) \subseteq A$ and $\text{range}(f) \subseteq B$.

Similarly, let $\mathcal{C} \subseteq \mathcal{S}$ be a chain, we show that $\bigcup \mathcal{C} \in \mathcal{S}$.

First we show that $\bigcup \mathcal{C}$ is "well defined", as in if (a, b) and (a, b') are in $\bigcup \mathcal{C}$ then $b = b'$. Since $(a, b) \in f$ and $(a, b') \in f'$ for some $f, f' \in \mathcal{C}$ and they are injections, assume $f \subseteq f'$, so $(a, b), (a, b') \in f'$ and hence $b = b'$.

Now we show that $\bigcup \mathcal{C}$ is injective. Assume $a \neq a'$ with $(a, b), (a', b') \in \bigcup \mathcal{C}$, similarly we have $(a, b), (a', b') \in f$ for some $f \in \mathcal{C}$. Thus $b \neq b'$.

By Zorn's Lemma, there is a maximal graph G in \mathcal{S} . Since $A \not\preceq B$, $\text{dom}(G) \subset A$. If $\text{range}(G) \subset B$, then we can extend G so that it maps some $a \in A - \text{dom}(G)$ to $b \in B - \text{range}(G)$. Now we consider $G^{-1} : B \rightarrow \text{dom}(G)$ which completes the proof.

- **Continuum Hypothesis**

Every set is either finite, countably infinite, or has the cardinality of the real numbers.

It turns out that the answer to this is independent of ZFC.

8.3 Tutorial 7

Problem 8.1

For each of the following properties, either give an example of a relation (on a set of your choice) with said property, or prove that for every set A , no relation on A can have said property.

1. Reflexive but neither symmetric nor transitive.
2. Symmetric and transitive, but not reflexive.
3. Symmetric but neither reflexive nor transitive.

1. The relation $a \sim b$ given by $a - b < 2$ on the set $\{5, 6, 7\}$.
2. Impossible, since $a \sim b$ and $b \sim a$ implies $a \sim a$ by transitivity.

True, define A to be the singleton so that it is vacuously true.

3. The relation $a \sim b$ given by $a + b = 1$ on $\{0, 1\}$.

Problem 8.2

Fix a set X . Let S_X denote the set of all bijections from X to X . Define a relation \sim on S_X as follows: $f \sim g$ if there is some $h \in S_X$ such that $g = h^{-1} \circ f \circ h$. Prove that \sim is an equivalence relation. (This equivalence relation is usually called conjugacy. Typical sets X of interest include $[n]$ and \mathbb{N} .)

1. **Reflexivity:** Choose $h = f$ so $f = f^{-1} \circ f \circ f$ implies $f \sim f$.
2. **Symmetry:** Assume that $f \sim g$, then there exists some h such that $g = h^{-1} \circ f \circ h$. Choose h^{-1} , then $f = h \circ g \circ h^{-1}$ as desired.
3. **Transitivity:** Assume that $f \sim g$ and $g \sim k$, we have

$$\begin{aligned} g &= h_1^{-1} \circ f \circ h_1 \\ k &= h_2^{-1} \circ g \circ h_2 \end{aligned}$$

Choose $h_1 \circ h_2$, so that $(h_1 \circ h_2)^{-1} = h_2^{-1} \circ h_1^{-1}$, thus

$$k = h_2^{-1} \circ h_1^{-1} \circ f \circ h_1 \circ h_2$$

This shows that $f \sim k$.

Problem 8.3 (Universal Property of Cartesian Products)

For each Cartesian product $A_1 \times A_2$, define the projection $\pi_1 : A_1 \times A_2 \rightarrow A_1$ by $\pi_1(a_1, a_2) = a_1$. Similarly, define $\pi_2 : A_1 \times A_2 \rightarrow A_2$ by $\pi_2(a_1, a_2) = a_2$. (It is worth thinking about why these functions are well-defined.) Prove that for any set B and any functions $p_1 : B \rightarrow A_1$ and $p_2 : B \rightarrow A_2$, there is a unique function $f : B \rightarrow A_1 \times A_2$ such that $p_1 = \pi_1 \circ f$ and $p_2 = \pi_2 \circ f$.

I claim that the function $f(b) = (p_1(b), p_2(b))$ is a unique function satisfying the problem for any $b \in B$. It is trivial to check that the function satisfies the conditions.

We assume that there exists some function $f' \neq f$ such that f' satisfies the properties above. Then there exists some b' such that

$$f'(b') \neq (p_1(b'), p_2(b'))$$

So at least one of $\pi_1(f'(b')) \neq p_1(b')$ or $\pi_2(f'(b')) \neq p_2(b')$ must hold. Without loss of generality, assume that $\pi_1(f'(b')) \neq p_1(b')$, but this contradicts the condition that $p_1 = \pi_1 \circ f$.

Problem 8.4

Fix a function $\sigma : A \rightarrow B$ which is onto. Define a relation \sim on A by $a \sim a'$ if $\sigma(a) = \sigma(a')$. As mentioned in lecture, \sim is an equivalence relation. Prove that for every set X and every function $f : A \rightarrow X$ such that if $a \sim b$, then $f(a) = f(b)$, there is a unique function $h : B \rightarrow X$ such that $f = h \circ \sigma$.

I claim that there's only one such function h , defined by $h(b) = f(a)$ for all $b = \sigma(a')$ satisfying $a' \in [a]_{\sim}$.

Suppose we have another function $k : B \rightarrow X$ such that $f = k \circ \sigma$, then we have

$$h(\sigma(a)) = f(a) = k(\sigma(a))$$

so $h = k$.

Problem 8.5

Suppose A is a set.

1. Prove that for every relation R on A , there is an equivalence relation S on A such that $R \subseteq S$.
2. For every relation R on A , consider the relation

$$E = \bigcap \{S \subseteq A \times A : R \subseteq S \text{ and } S \text{ is an equivalence relation on } A\}.$$

(Notice this intersection is well-defined because of part 1.) Prove that E is an equivalence relation.

Remark. A relation R is a set that whenever aRb then $(a, b) \in R$.

For convenience, let X be a set that whenever $(a, b) \in R$ then $\{a, b\} \in X$.

1. For every $(a, b) \in R$ such that aRb , we define aSa and bSa by symmetry, aSa for every $a \in \bigcup X$ for reflexivity (but not necessary bRa) Therefore $R \subseteq S$.
2. a) **Reflexivity:** For every R and for every S , whenever $a \in \bigcup X$ then aSa since S is reflexive.

So let $a \in X_i$ for all i , then aS_ja for all j , hence E is reflexive.

- b) **Symmetry**: Let $a, b \in X_i$ for all i , then aS_jb and bS_ja for all j . Hence E is symmetric.
- c) **Transitivity**: For every $a, b, c \in X_i$ for all i , we have

$$aS_jb \quad bS_jc$$

for all j , thus E is transitive.

Problem 8.6

Suppose \sim is an equivalence relation on a set A . Prove that there is some set X and some function $f : A \rightarrow X$ such that for all $a, a' \in A$, we have $a \sim a'$ if and only if $f(a) = f(a')$. (Hint: It is enough to quote a relevant result from lecture.)

First we assume that A is non-empty, hence X is non-empty. Clearly there exists a function f such that $f : A \rightarrow X$ and $f(a) = f(a')$ when $a \sim a'$.

By the Universal Property of Equivalence Relations, there exists a unique function $g : A/\sim \rightarrow X$ such that $f = g \circ \pi$.

(\Rightarrow) is proved by definition. (\Leftarrow) assume that $f(a) \neq f(a')$ so $g(\pi(a)) \neq g(\pi(a'))$. This means that $\pi(a) \neq \pi(a')$ which means a is not equivalent to a' .

Problem 8.7

Define a relation on $(\mathbb{R} \times \mathbb{R}) - \{(0, 0)\}$ by $(a, b) \sim (c, d)$ if there is some nonzero $\lambda \in \mathbb{R}$ such that $\lambda a = c$ and $\lambda b = d$.

1. Prove that \sim is an equivalence relation.
2. Describe the equivalence class of $(-1, 2)$. In general, what do the sets in the partition corresponding to \sim look like, when interpreted as a subset of the plane \mathbb{R}^2 ? (That is, interpret each (a, b) as the point with x -coordinate a and y -coordinate b .)

1. We now prove that \sim is an equivalence relation.

- a) **Reflexivity**: Choose $\lambda = 1$, so $(a, b) \sim (a, b)$.
- b) **Symmetry**: Choose $1/\lambda$. This is valid since $\lambda \neq 0$. Thus

$$\begin{aligned} \lambda a &= c, & \lambda b &= d \\ c/\lambda &= a, & d/\lambda &= b \end{aligned}$$

- c) **Transitivity**: Let $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$ given by

$$\lambda_1 a = c, \quad \lambda_1 b = d$$

$$\lambda_2 c = e, \quad \lambda_2 d = f$$

Then choose $\lambda_1 \lambda_2$, we have

$$\lambda_1 \lambda_2 a = e, \quad \lambda_1 \lambda_2 b = f$$

2. Assume that $(-1, 2) \sim (x, y)$, we have

$$-\lambda = x, \quad 2\lambda = y$$

Eliminating λ as a variable gives

$$y = -2x$$

It is a line with gradient -2 and discontinuous at $(0, 0)$.

Problem 8.8

Define an equivalence relation \sim on $\mathbb{N} \times \mathbb{N}$ by $(m, n) \sim (p, q)$ if $m + q = p + n$. (This is the equivalence relation used to define \mathbb{Z} from \mathbb{N} in set theory, but the context of this question is different. In particular, we freely assume basic properties of \mathbb{Z} , subtraction, absolute value, etc.)

1. We attempt to define a function $f : (\mathbb{N} \times \mathbb{N}) / \sim \rightarrow \mathbb{N}$ by $f([(m, n)]_\sim) = m + n$. Prove that f is not well-defined.
2. We attempt to define a function $g : (\mathbb{N} \times \mathbb{N}) / \sim \rightarrow \mathbb{N}$ by $g([(m, n)]_\sim) = |m - n|$. Prove that g is well-defined.

1. The problem here is that, for example. $[(m, n)]_\sim$ is equivalent to $[(m + 1, n + 1)]_\sim$ but they are sent to different values.

$$m + n + 2 = f([(m + 1, n + 1)]_\sim) = f([(m, n)]_\sim) = m + n$$

2. First we prove that each $[(m, n)]_\sim$, it is mapped to one value $|m - n|$. Assume that two pairs $(m, n) \sim (p, q)$ but $|m - n| \neq |p - q|$. But by definition we have $m + q = p + n$ or $m - n = p - q$, so certainly $|m - n| = |p - q|$.

Now we want to prove that each of $f([(m, n)]_\sim)$ is mapped to some value in the codomain of f , which is trivial since $|m - n|$ is nonnegative.

8.4 Tutorial 8

Problem 8.9

Given a set A , construct a bijection between the power set $\mathcal{P}(A)$ and the set of functions from A to $\{0, 1\}$. (Suggestion: If you're stuck, try doing this for a small finite set A .)

We hope to construct a bijective function $f : \mathcal{P}(A) \rightarrow \text{Maps}(A, \{0, 1\})$.

For every set $X \in \mathcal{P}(A)$, consider each element $a \in A$. Assume $f(X) = g$ be a function as follows: if $a \in X$ then $g(a) = 1$ or else $g(a) = 0$.

I claim that f is a bijective function. Assume that there exist two distinct sets X, Y such that $f(X) = f(Y)$. Since they are not equal, there exists some $x \in X$ but $x \notin Y$. Thus $g_X(x) = 1$ but $g_Y(x) = 0$, contradiction.

Remark. The function g is the **characteristic function** of g .

Problem 8.10

The previous question, together with Cantor's theorem, implies that for every set A , there is no surjection from A to $\text{Maps}(A, \{0, 1\})$. Come up with a "direct" proof of this latter fact.

Assume that for every $a \in A$ gets mapped to some function $f_a : A \rightarrow \{0, 1\}$ in $\text{Maps}(A, \{0, 1\})$. Consider the function

$$f_a(x) = \begin{cases} 0 & \text{if } f_x(a) = 1 \\ 1 & \text{if } f_x(a) = 0 \end{cases}$$

For all $x \in A$. But this fails when $x = a$.

Problem 8.11

Construct a bijection between the intervals $[0, 1]$ and $(0, 1)$. (Suggestion: Try a piecewise definition. Intuitively, $(0, 1)$ has "infinitely much space" for you to "squeeze" in the points 0 and 1. You may find inspiration in Hilbert's Hotel.)

Define a function $f : [0, 1] \rightarrow (0, 1)$,

$$f(x) = \begin{cases} 0.5^{k+1} & \text{if } x = 0.5^k \text{ for some natural number } k, \\ 1 - 0.3^{k+1} & \text{if } x = 1 - 0.3^k \text{ for some natural number } k, \\ x & \text{otherwise.} \end{cases}$$

One can easily check that f is bijective by using number theory.

Problem 8.12

Suppose A is a finite set such that every element of A is finite. Prove that $\bigcup A$ is finite.

Consider $X \approx [m]$ and $Y \approx [n]$ for some $m, n \in \mathbb{N}$, then $X \cup Y \approx [k]$ where $k \leq m + n$.

Now assume that A has r finite sets, each has cardinality $a_1, a_2, a_3, \dots, a_r$. Thus assume the cardinality of $\bigcup A$ be S , then we have

$$S \leq a_1 + a_2 + a_3 + \dots + a_r$$

Problem 8.13

Let A be an infinite set. Prove that for every finite $X \subseteq A$, there is some finite $Y \subseteq A$ such that $X \subsetneq Y$.

Assume otherwise, we claim that for every subset Y of A not equal to X , X is not a subset of Y implies A is finite.

If A is finite, choose $X = A$, then our claim holds.

If A is infinite, for every set X and Y , there exists some $a_{(X,Y)} \in A$ such that $a_{(X,Y)} \in X$ but $a_{(X,Y)} \in Y$. If Y contains all elements of X , then since X is finite and A is infinite, we can choose some $a \in A$ so that $a \in Y$ but $a \notin X$, this makes X a proper subset of Y .

Problem 8.14

Prove that if A is finite and $f : A \rightarrow A$ is onto, then f is one-to-one.

Let $A \approx [n]$ for some $n \in \mathbb{N}$, assume that for all sets $B \approx [k]$ and surjective functions $f : B \rightarrow B$ for all natural numbers $k < n$, f is injective. We hope to prove that whenever $f : A \rightarrow A$ is surjective then f is injective.

Base Case: $n = 0$, trivial.

Inductive Step: Consider a subset $X \subset A$ and $X \approx [n-1]$ (We assume $n \geq 1$). Then since $f \upharpoonright X$ is surjective, then $f \upharpoonright X$ is bijective, hence $f[X] \approx X$.

Consider the only element $a \notin X$ but $a \in A$. Since $f[A] - f[X] \neq \emptyset$, we have $f(a) \in f[A] - f[X]$. Lastly, since $f[A] - f[X] \cap f[X] = \emptyset$, f is injective on A .

Problem 8.15

In this problem, we take \mathbb{Q} to be a quotient of $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$, as defined in lecture.

1. Prove that \mathbb{Q} is countable.
2. Prove that the set of single-variable polynomials with rational coefficients is countable.
3. A real number is *algebraic* if it is a root of some single-variable polynomial with rational coefficients. Prove using Choice (or any of its consequences that we proved) that the set of algebraic numbers is countable. (You may use facts about polynomials such as the fundamental theorem of algebra without proving them, but you should state them clearly and explain how you're using them.)
4. (Optional) Prove part 3 without using Choice.

1. We show that there is a surjection from \mathbb{N} to \mathbb{Q} , and hence \mathbb{Q} is countable.

For every $(a, b) \in \mathbb{Q}$, there is a natural number cd mapped to (a, b) defined by

$$c = \begin{cases} 2^a & \text{if } a \text{ is nonnegative} \\ 3^{-a} & \text{if } a \text{ is negative} \end{cases}$$

and

$$d = \begin{cases} 5^b & \text{if } b \text{ is positive} \\ 7^{-b} & \text{if } b \text{ is negative} \end{cases}$$

In fact, this mapping is injective, hence \mathbb{Q} is countable.

2. We have proven that $\mathbb{N}^{<\mathbb{N}}$ is countable, thus we want to show that $\mathbb{Q}^{<\mathbb{N}}$ is countable. Moreover, we have shown in 1. that there exists a bijection from \mathbb{Q} to \mathbb{N} since $\mathbb{Q} \approx \mathbb{N}$.

For every set of such polynomials of degree n , say $S_n = \{P(x) \in \mathbb{Q}[x] : \deg(P) = n\}$, consider the set of polynomials of degree n with coefficients of natural numbers, say $T_n = \{P(x) \in \mathbb{N}[x] : \deg(P) = n\}$, then $S_n \approx T_n$. This is because there exists a bijection from S_n to T_n as $\mathbb{Q} \approx \mathbb{N}$. For each $Q(x) \in S_n$, the coefficients of $Q(x)$ have a bijective mapping to some natural number, hence $Q(x)$ is mapped to some unique $R(x) \in T_n$.

In fact, this problem is equivalent to proving $\mathbb{Q}^{<\mathbb{N}} \approx \mathbb{N}$.

3. Let the set of algebraic numbers be \mathbb{A} . For every polynomial of rational coefficient of degree n , we know that this polynomial has at most n algebraic roots.

Assume that each polynomial has countably infinite many roots, thus this set has $\mathbb{Q}^{<\mathbb{N}} \times \mathbb{N}$ roots. But we know

$$\mathbb{Q}^{<\mathbb{N}} \times \mathbb{N} \approx \mathbb{N} \times \mathbb{N} \approx \mathbb{N}$$

and that \mathbb{A} is a proper subset of $\mathbb{Q}^{<\mathbb{N}} \times \mathbb{N}$, hence the set of algebraic numbers is countably infinite.

§9 Properties Of Real Numbers

9.1 Tutorial 9

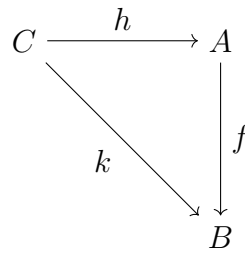
Problem 9.1

Suppose $A \preceq B$. Prove that for each set C , we have $\text{Maps}(C, A) \preceq \text{Maps}(C, B)$.

Consider an injection $f : A \rightarrow B$, we hope to construct an injection $g : \text{Maps}(C, A) \rightarrow \text{Maps}(C, B)$.

For some function $h : C \rightarrow A$, let $h(c_i) = a_i$, where $c_i \in C$ and $a_i \in A$. This function will be mapped to some function $k : C \rightarrow B$ with $k(c_i) = b_i$ for all $c_i \in C$ and $b_i \in B$ and $f(a_i) = b_i$, that is,

$$f(h(c)) = k(c)$$



it suffices to prove that g is well-defined and is injective.

g is well-defined as for every h , we can find some k since $k \in \text{Maps}(C, B)$. Since f is injective, if there exists some function k' such that $g(h) = k'$ then there exists some i' such that $k(c_{i'}) = b_{i'}$ but $k(c_{i'}) \neq b_{i'}$, contradicting the well-definedness of f .

To show that g is injective, assume $h \neq h'$, functions from C to A . Thus there exists some $c \in C$ such that $h(c) \neq h'(c)$. By injectivity of f , we have $f(h(c)) \neq f(h'(c))$, or $k(c) \neq k'(c)$, thus $k \neq k'$.

Problem 9.2

The following statements can be proven without Choice, but they may have "easier" proofs with Choice. Prove each of them (using Choice or any of its consequences, if you want).

1. The set of injections from \mathbb{N} to \mathbb{N} is uncountable.
2. If A is Dedekind infinite and $A \preceq B$, then B is Dedekind infinite.
3. If A is infinite, then $\mathbb{N} \preceq \mathcal{P}(\mathcal{P}(A))$.

1. By the previous tutorial we have proved that $\text{Maps}(\mathbb{N}, \{0, 1\})$ is uncountable. There exists a surjection from $\{f : f = \text{Injections from } \mathbb{N} \text{ to } \mathbb{N}\}$ to $\text{Maps}(\mathbb{N}, \{0, 1\})$, say g . Let $f \in \{f : f = \text{Injections from } \mathbb{N} \text{ to } \mathbb{N}\}$ and $h \in \text{Maps}(\mathbb{N}, \{0, 1\})$, then g maps f to h by

$$h(n) = R_2(f(n))$$

then there exists an injection from $\text{Maps}(\mathbb{N}, \{0, 1\})$ to $\{f : f = \text{Injections from } \mathbb{N} \text{ to } \mathbb{N}\}$ by Choice. Thus the set of injections from \mathbb{N} to itself is uncountable.

2. Let $f : A \rightarrow B$ be an injection, then there exists some $\mathfrak{A} \subset A$ with $\mathfrak{A} \approx A$. Consider some $a' \in A$ but $a' \notin \mathfrak{A}$. We hope to construct some bijection $g : \mathfrak{A} \rightarrow \mathfrak{B}$ for some $\mathfrak{B} \subset B$. Consider $g(a) = f(a)$ for all $a \in \mathfrak{A}$, thus the function $g : \mathfrak{A} \rightarrow \text{range}(f) - \{f(a')\}$ is bijective. Thus $\text{range}(g)$ is a proper subset of B and is infinite.
3. Since A is infinite, we have $\mathbb{N} \preceq A$. Let there be such injective function $F : \mathbb{N} \rightarrow A$. Consider an injective function $g : \mathbb{N} \rightarrow \mathcal{P}(\mathcal{P}(A))$ being

$$f(n) = a \quad \text{then} \quad g(n) = \{\{a\}\}$$

Remark. Another solution without Choice is to consider

$$n \mapsto \{X \subseteq A : |X| = n\}$$

Problem 9.3

Assume that for every set Y and every partition P of Y , there is a choice function $G : P \rightarrow Y$. Prove that for every set X with $\emptyset \notin X$, there is a choice function $F : X \rightarrow \bigcup X$. (Hint: X may not be a partition but there is a trick to "transform" it into one.)

Assume that there exists some $x \in \bigcup X$ such that there exists distinct $A, A' \in X$ with $x \in A$ and $x \in A'$. Since both cannot be singletons simultaneously, at least one of them has at least two elements, say A . Now, consider a set X' defined by

$$X' = (X - \{A\}) \cup \{A - \{x\}\}$$

Iterate this process until we obtain a partition of X . It is a partition since for every $x \in \bigcup X$, exactly one of $A' \in X$ satisfies $x \in A'$. Thus there exists such choice function F by assumption.

Problem 9.4

Suppose X is a set with $\emptyset \notin X$. Consider the set \mathcal{S} consisting of all $G \subseteq X \times \bigcup X$ such that G is a graph of a function F with $\text{dom}(F) \subseteq X$ and $F(A) \in A$ for every $A \in \text{dom}(F)$.

1. Prove that if $\mathcal{C} \subseteq \mathcal{S}$ is a chain, then $\bigcup \mathcal{C} \in \mathcal{S}$.
2. Use Zorn's lemma to prove that there is a choice function for X .

1. Let \mathcal{C} be a chain, that is, for every $A, B \in \mathcal{C}$ we have $A \subseteq B$ or $B \subseteq A$. We shall show that $\bigcup \mathcal{C}$ is in \mathcal{S} . Assume that $(\mathfrak{A}, a) \in A$, $(\mathfrak{B}, b) \in B$ and $A, B \in \mathcal{C}$. By definition, there exists functions F_A, F_B with $F_A(\mathfrak{A}) \in \mathfrak{A}$ and $F_B(\mathfrak{B}) \in \mathfrak{B}$. Without loss of generality, let $A \subseteq B$. Since $a, b \in B$, we have $F_B(\mathfrak{A}) \in \mathfrak{A}$ too. Thus $(\mathfrak{A}, a), (\mathfrak{B}, b)$ satisfies the said property, hence they are in \mathcal{S} .
2. By Zorn's lemma, there is some maximal set $M \in \mathcal{S}$.

Claim — $\text{dom}(F_M) = X$.

Proof. Assume otherwise, there exists some $S \in X - \text{dom}(F_M)$. We can define some M' such that $(F_{M'}(S), S) \in M'$, contradicting the maximality of M . ■

So for every $S \in X$, there is a function F_M such that $F_M(S) \in S$.

Problem 9.5

Fix a set C . A function $F : \mathcal{P}(C) \rightarrow \mathcal{P}(C)$ is said to be **monotone** if $X \subseteq Y \subseteq C$ implies $F(X) \subseteq F(Y)$. (For example, if c is a fixed element of C , then the function $X \mapsto X - \{c\}$ is monotone. Note that in the definition of monotone, we do not require that $F(X) \subseteq F(Y)$ implies $X \subseteq Y$. We do not require that $X \subseteq F(X)$ either.) If F is monotone, define

$$S = \bigcap \{X \subseteq C : F(X) \subseteq X\}.$$

1. Prove that the above intersection is well-defined. (This should be a one-line proof.)
2. Prove that $F(S) = S$.
3. Suppose $A \subseteq B \subseteq C$ and that $f : C \rightarrow A$ is a bijection. Prove that the function $F : \mathcal{P}(C) \rightarrow \mathcal{P}(C)$ defined by $F(X) = (C - B) \cup f[X]$ is monotone.
4. By the previous parts, we know there is some set $S \subseteq C$ such that $S = (C - B) \cup f[S]$. Use S to construct a bijection $g : C \rightarrow B$. (Hint: Given $x \in C$, consider cases depending on whether $x \in S$.)

Consider such S be

$$S = \bigcup \{\{1, 2, 3\}, \{2, 3, 4\}, \{2, 3, 5\}\}$$

with $F(\{1, 2, 3\}) = \{2, 3\}$, $F(\{2, 3, 4\}) = \{2, 4\}$, $F(\{2, 3, 5\}) = \{2, 3, 5\}$.

1. It is well-defined as each $X, F(X) \in \mathcal{P}(C)$.
2. For all $X \in \{X \subseteq C : F(X) \subseteq X\}$, we have $S \subseteq X$ by the definition of S . Thus we have $F(S) \subseteq F(X)$. Since $F(X) \subseteq X$, we have $F(S) \subseteq X$ for all such X . We may deduce that $F(S) \subseteq \bigcap \{X : F(X) \subseteq X\} = S$.

Assume otherwise, let $a \in F(S)$ with $a \in Y$ but $a \notin \bigcap \{X : F(X) \subseteq X\}$ for some $Y \in \{X : F(X) \subseteq X\}$, then for some $X' \in \{X : F(X) \subseteq X\}$, we must have $F(S) \not\subseteq X'$, leading to a contradiction.

3. Assume that $X, Y \subseteq C$, and $X \subseteq Y$, by bijectivity we have $f[X] \subseteq f[Y]$. Moreover, since $C - B$ and $f[Y]$ are disjoint, we have $F(X) \subseteq F(Y)$.
4. Fix S , we construct a bijection g as follows:

$$g[c] \subseteq \begin{cases} f[S] & \text{if } c \subseteq (C - B) \cup f[S] \\ B - f[S] & \text{if } c \subseteq B - f[S] \end{cases}$$

That is, $(C - B) \cup f[S]$ gets sent to $f[S]$, this is bijective since f is bijective. On the other hand, $B - f[S]$ gets sent to $B - f[S]$, which is obviously bijective.

Remark. This is indeed an alternate proof of the Cantor-Schröder-Bernstein.

§10 p -adic Numbers

10.1 Motivation

Consider the diophantine equation

$$x^2 - 3y^2 = 8$$

We can prove that this equation has no solution by taking modulo 3, that is, $x^2 \equiv 2 \pmod{3}$. But does this always work? That is, given any polynomial P with integer coefficients, there is a prime $p \in \mathbb{P}$ such that $P \equiv 0 \pmod{p}$ has no solution.

- **Hensel's Lemma:** Let f be a polynomial with integer coefficients and r, k with $f(r) \equiv 0 \pmod{p^k}$, and $f'(r) \not\equiv 0 \pmod{p^k}$, then for positive integers $m \leq k$, there exists an integer s such that $f(s) \equiv 0 \pmod{p^{k+m}}$ and that s is unique modulo p^{k+m} .

For example, take $f(n) = n^3 - 2$ and $p = 5$, we have

$$\begin{aligned} 3^3 - 2 &\equiv 0 \pmod{5} \\ 3^3 - 2 &\equiv 0 \pmod{5^2} \\ 53^3 - 2 &\equiv 0 \pmod{5^3} \\ 303^3 - 2 &\equiv 0 \pmod{5^4} \\ &\vdots \end{aligned}$$

10.2 p -adic Integers

p -adic integers are sequences $\alpha = (x_0, x_1, x_2, \dots)$ defined recursively by

$$x_k \equiv x_{k-1} \pmod{p^k}$$

up to equivalence modulo p^{k+1} . We let \mathbb{Z}_p be the set of p -adic numbers. It can be shown that $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ as witnessed by the constant sequence $x \mapsto (x, x, x, \dots)$.

Some properties of p -adic numbers include:

- **Addition & Multiplication:** Component-wise, can be shown by congruency.
- **Addition Identity:** The constant 0 sequence.
- **Multiplication Identity:** The constant 1 sequence.
- If $\alpha, \beta \in \mathbb{Z}_p$ are nonzero, then $\alpha\beta$ is nonzero.
- **Relation to the p -base expansion:** Consider $p = 3$ and $x = 86$. Taking x modulo p^k gives

| | | | | | | |
|---|----------------------------|------------------------------|------------------------------|------------------------------|------------------------------|---------|
| | 86 | 86 | 86 | 86 | 86 | \dots |
| | $\downarrow \text{mod } 3$ | $\downarrow \text{mod } 3^2$ | $\downarrow \text{mod } 3^3$ | $\downarrow \text{mod } 3^4$ | $\downarrow \text{mod } 3^5$ | |
| | 2 | 5 | 5 | 86 | 86 | \dots |
| | | | | | | |
| 2 | 1 | 0 | 0 | 1 | 0 | \dots |

So $(2, 5, 5, 86, 86, 86, \dots)$ is a 3-adic number. Notice that $86 = \dots 00010012_3$, and that

$$\begin{aligned}
 0 + 2 \times 3^0 &= 2 \\
 2 + 1 \times 3^1 &= 5 \\
 5 + 0 \times 3^2 &= 5 \\
 5 + 0 \times 3^3 &= 5 \\
 5 + 1 \times 3^4 &= 86 \\
 &\vdots
 \end{aligned}$$

Hence the p -adic numbers conveys the p -base expansion.

10.3 p -adic Valuation

- The p -adic valuation $v(\alpha)$ of a p -adic integer α is defined by

$$v(\alpha) = \begin{cases} \min \{i : \alpha(i) \neq 0\} & \alpha \neq 0 \\ \infty & \text{otherwise} \end{cases}$$

That is, the least index with its entry being nonzero.

Similarly, for integers n , we define the p -adic valuation $\nu_p(n)$,

$$\nu_p(n) = \max \{k : p^k | n\}$$

- The **absolute value** $|\alpha|_p$ is defined by $|\alpha|_p = p^{-\nu_p(\alpha)}$. Thus we have

$$|\alpha|_p \in \{1, p^{-1}, p^{-2}, \dots, 0\}$$

Some properties of the absolute value include:

- $|\alpha|_p + |\beta|_p \geq |\alpha + \beta|_p$. In fact, $\max \{|\alpha|_p, |\beta|_p\} \geq |\alpha + \beta|_p$. Equality holds when $|\alpha|_p \neq |\beta|_p$. If $|\alpha|_p = |\beta|_p$, it is inconclusive as

$$(1, 1, 1, 1, \dots) + (-1, -1, -1, -1, \dots) = (0, 0, 0, 0, \dots)$$

$$(1, 1, 1, 1, \dots) + (1, 1, 1, 1, \dots) = (2, 2, 2, 2, \dots)$$

considering sequences in \mathbb{Z}_7 .

One can prove that

$$|\alpha|_p + |\beta|_p \geq \max \{|\alpha|_p, |\beta|_p\} \geq |\alpha + \beta|_p$$

- $|\alpha|_p |\beta|_p = |\alpha\beta|_p$.
- The absolute value of the constant sequence $\alpha = (p^n, p^n, p^n, \dots)$ converges to 0 as $n \rightarrow \infty$ since $|\alpha|_p = p^{-n}$.
- The set $\{\alpha \in \mathbb{Z}_p : |\alpha|_p < 1\}$ forms a maximal ideal.
- Let x be a constant sequence (x, x, x, \dots) , then we have

$$|x| \cdot \prod_{p \leq \infty} |x|_p = 1$$

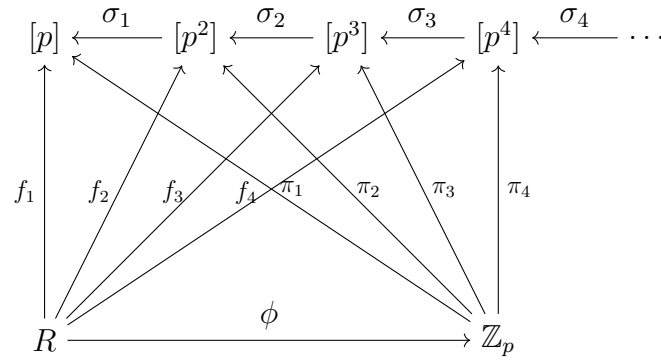
- **Hasse Principle:** A polynomial $P \in \mathbb{Z}[x]$ has roots modulo each p^k if and only if it has a root in \mathbb{Z}_p .

What does it mean to have roots in \mathbb{Z}_p ? Consider the equation $x^2 - x = 0$. A 3-adic solution to equation is $(0, 0, 0, \dots)$.

Roughly speaking, a theorem or property holds over \mathbb{Q} if and only if it holds over \mathbb{R} and \mathbb{Q}_p for all p (Conrad, n.d.).

10.4 The Universal Property of p -adic Integers

Let p be a prime. Assume that σ_k are mappings such that $\sigma_k \circ f_{k+1} = f_k$ for all k , then there exists a unique ring homomorphism $\phi : R \rightarrow \mathbb{Z}_p$ such that $\pi_k \circ \phi = f_k$.



10.5 Definition and Properties of \mathbb{Q}_p

- A p -adic integer α has a **multiplicative inverse** if and only if $\alpha(0) \neq 0$ or $|\alpha|_p = 1$.
- For example, let $p = 5$, the multiplicative inverse of $\alpha = (1, 2, 3, 4, \dots)$ is $(1, 13, 42, 469, \dots)$.
- We define \mathbb{Q}_p to be the set of all sequences $\alpha = \left(\frac{a_1}{p^k}, \frac{a_2}{p^k}, \frac{a_3}{p^k}, \frac{a_4}{p^k}, \dots \right)$ for $k \in \mathbb{N}$ and $(a_1, a_2, a_3, \dots) \in \mathbb{Z}_p$.
- For any $\alpha \in \mathbb{Q}_p$, we have

$$|\alpha|_p \in \{\dots, p^2, p, 1, p^{-1}, p^{-2}, \dots\}$$

Thus \mathbb{Z}_p is bounded by \mathbb{Q}_p in terms of $|\cdot|_p$.

- Still, we can construct $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ by follows: Consider $m, n \in \mathbb{Z}$ with $\gcd(m, n) = 1$. Let $n = p^{\nu_p(n)}\ell$, then

$$\frac{m}{n} = \frac{m}{\ell} \frac{1}{p^{\nu_p(n)}} \in \mathbb{Q}_p$$

since $m/\ell \in \mathbb{Z}_p$ (multiplicative inverse) and $p \nmid \ell$.

10.6 Absolute Values

Define an **absolute value** $|\cdot|$ to be a function mapping from an integral domain to the reals satisfying

- $|x| \geq 0$
- $|x| = 0$ if and only if $x = 0$
- $|x + y| \leq |x| + |y|$
- $|xy| = |x||y|$

For example, the square root of the ordinary absolute value is an *absolute value*.

Moreover, if this absolute value satisfies $|a + b| \leq \max\{|a|, |b|\}$, then this absolute value is an **ultrametric**.

Ostrowski's Theorem: Every nontrivial absolute value in \mathbb{Q} is a positive power of the usual absolute value (in \mathbb{R}) or $|\cdot|_p$, the p -adic absolute value.

Hasse-Minkowski Theorem: Let F be a **quadratic form** (homogenous polynomial of degree 2). F has a nonzero root in \mathbb{Q} if and only if it has a nonzero root in every \mathbb{Q}_p with $p \leq \infty$. ($\mathbb{Q}_\infty = \mathbb{R}$)

10.7 Some Applications of p -adic Numbers

- $x^2 = 2$ has no solution in \mathbb{Q} : This is equivalent to say that $x^2 = 2$ has no solution in \mathbb{Q}_2 . By

$$\begin{aligned} |x^2|_2 &= |x|_2^2 \\ |2|_2 &= \frac{1}{2} \end{aligned}$$

By $|x|_2 \in \{\dots, 4, 2, 1, 1/2, 1/4, \dots, 0\}$ we can see that there is no solution.

- The partial sums of harmonic sequence $H_n = \sum_{i=1}^n \frac{1}{i}$ is not an integer. This can be shown by $|H_n|_2 > 1$.

10.8 Tutorial 10

Problem 10.1

Prove that \mathbb{Q} is dense in \mathbb{R} in two ways:

1. By thinking of \mathbb{R} as the set of all Dedekind cuts (and \mathbb{Q} as the set of all cuts of the form $\{q : q < r\}$ where r is rational);
2. Using only the axioms of \mathbb{R} (i.e., that \mathbb{R} is a Dedekind complete ordered field).

Recall that \mathbb{Q} is dense in \mathbb{R} if for every $r < s$ in \mathbb{R} there exists $q \in \mathbb{Q}$ with $r < q < s$.

1. Assume that $r < s$ be two real numbers. We may define

$$R := \{q_r \in \mathbb{Q} : q_r < r\}$$

$$S := \{q_s \in \mathbb{Q} : q_s < s\}$$

If there is no rational number between r and s , then if $q \in R$ we have $q \in S$ and hence by definition since $R = S$ we have $r = s$.

2. We want to find a pair (m, n) with $nr < m < ns$. Consider $n(s - r) > 0$. There exists some n such that $n(s - r) > 1$ or $n > 1/(s - r)$. For such n , since the interval (nr, ns) has length more than 1, there exists an integer in between.

Problem 10.2

Prove that for each real number r , there is some integer n such that $n \leq r < n + 1$. (Henceforth, we will refer to n by $\lfloor r \rfloor$.)

Assume otherwise, for every integer n we have either $n < r$ or $r \leq n$. If r is an integer then choose $n = r$ so $n = r < n + 1$. Hence assume that r is not an integer.

If $1 < r$ then $2 < r$ or else $1 < r < 2$. Continue the same argument, then for all $n = 1, 2, 3, \dots$ we have $n < r$ which is absurd.

If $r < 1$ then $r < 0$ or else $0 < r < 1$. Similarly for all $n = 1, 0, -1, -2, \dots$ we have $r < n$ hence a contradiction.

Problem 10.3

Suppose A is a nonempty bounded subset of \mathbb{R} . Prove that $s = \sup(A)$ if and only if for every $n \in \mathbb{N}^+$, $s + \frac{1}{n}$ is an upper bound of A and $s - \frac{1}{n}$ is not an upper bound of A .

(\Rightarrow) Assume that $s = \sup(A)$, then for all $x \in A$ we have $x \leq s$. Thus $x \leq s \leq s + 1/n$, so $s + 1/n$ is an upper bound of A .

If $s \in A$, then obviously $s - 1/n$ is not an upper bound. If $s \notin A$, let n be the minimum positive integer such that $s - 1/n$ is an upper bound of A , then since $s - 1/n < s$ contradicting the minimality of s .

(\Leftarrow) Assume that for all $n \in \mathbb{N}^+$, $s + 1/n$ is an upper bound of A and $s - 1/n$ is not an upper bound. That is, for all n , for all $r \in A$ we have $r < s + 1/n$. If $r > s$, let $r = s + \varepsilon$, we have $0 < \varepsilon < 1/n \leq 1$. But this means that $n < 1/\varepsilon$ or that n is bounded, so this is not true for all n , hence $r \leq s$. If $r \leq s$ then $r \leq s < s + 1/n$ so s is an upper bound of A .

Assume that there exists some $s' < s$ such that for all $r \in A$ we have $r < s'$. Since for all n there exists some $r_n \in A$ such that $s - 1/n < r_n$, so we have $s - 1/n < r_n < s'$ and hence $n < 1/(s - s')$. This is not true for all n , hence s is the smallest upper bound.

Problem 10.4

Define a relation \sim on $\text{Maps}(\mathbb{Z}, \mathbb{Z})$ as follows: $f \sim g$ if $f - g$ is bounded, i.e., there is some $b \in \mathbb{N}$ such that for all $n \in \mathbb{Z}$, $|f(n) - g(n)| \leq b$.

1. Prove that \sim is an equivalence relation.
2. We attempt to define a binary operator $+$ on $\text{Maps}(\mathbb{Z}, \mathbb{Z})/\sim$ as follows: $[f]_\sim + [g]_\sim = [f + g]_\sim$, where $+$ on the right denotes pointwise addition of functions. Prove that $+$ (on $\text{Maps}(\mathbb{Z}, \mathbb{Z})/\sim$) is well-defined.
3. Let R be the set of all $f \in \text{Maps}(\mathbb{Z}, \mathbb{Z})$ such that the set $\{f(a + b) - f(a) - f(b) : a, b \in \mathbb{Z}\}$ is a bounded subset of \mathbb{Z} . We attempt to define a binary operator \times on R/\sim as follows: $[f]_\sim \times [g]_\sim = [f \circ g]_\sim$, where (as usual) \circ denotes function composition. Prove that \times is well-defined.
4. (Optional, hard) Prove that \times (on R/\sim) is commutative.

1. **Reflexivity:** For all f , we have $|f(n) - f(n)| = 0 \leq b$ for all $b \in \mathbb{N}$.

Symmetry: Let $f \sim g$, then $|f(n) - g(n)| \leq b$ and $|f(n) - g(n)| = |g(n) - f(n)|$ so $|g(n) - f(n)| \leq b$, so $g \sim f$.

Transitivity: Let $f \sim g$ and $g \sim h$ so there exists b_f, b_g such that $|f(n) - g(n)| \leq b_f$ and $|g(n) - h(n)| \leq b_g$. By definition, we have

$$\begin{aligned} -b_f &\leq f(n) - g(n) \leq b_f \\ -b_g &\leq g(n) - h(n) \leq b_g \end{aligned}$$

Summing up gives

$$-(b_f + b_g) \leq f(n) - h(n) \leq b_f + b_g$$

or $|f(n) - h(n)| \leq b_f + b_g$.

2. First we prove that $[f]_\sim + [g]_\sim$ has only one unique value.

Note that $[f + g]_\sim$ has at least one element — $f + g$ itself. Assume that $[f]_\sim + [g]_\sim = [h]_\sim$. Fix f, g and $h = f + g$, then for some $f_1 \in [f]_\sim$ and $g_1 \in [g]_\sim$, assume that $|f_1 - f| \leq F$ and $|g_1 - g| \leq G$, thus we have

$$|(f_1 + g_1) - (f + g)| \leq F + G$$

so $f_1 + g_1$ is in $[f + g]_\sim$.

Obviously $f + g$ is in $\text{Maps}(\mathbb{Z}, \mathbb{Z})$.

3. Similarly, we want to prove that $[f]_\sim \times [g]_\sim$ has only one unique value.

Note that $[f \circ g]_\sim$ has at least one element — $f \circ g$ itself. Fix f, g . Now assume that $f_1 \in [f]_\sim$ and $g_1 \in [g]_\sim$.

By the definition of \sim ,

$$|f_1(g(n)) - f(g(n))| \leq F_1$$

so $f_1 \circ g \in [f \circ g]_{\sim}$.

On the other hand, by the definition of R ,

$$|f(g(n)) - f(g(n) - g_1(n)) - f(g_1(n))| \leq F$$

Since $g(n) - g_1(n)$ is bounded, thus $f(g(n) - g_1(n))$ is bounded, hence $f(g(n)) - f(g_1(n))$ is bounded.

Remark. We should show that $f \circ g$ is in R . This can be shown by the 4 bounded expressions

$$g(a+b) - g(a) - g(b)$$

$$f(g(a+b) - g(a) - g(b))$$

$$f(g(a) + g(b)) - f(g(a)) - f(g(b))$$

$$f(g(a+b)) - f(g(a+b) - g(a) - g(b)) - f(g(a) + g(b))$$

Which gives

$$f(g(a+b)) - f(g(a)) - f(g(b))$$

Remark. This is the construction of the [Eudoxus reals](#).

§11 Mathematics and Technology

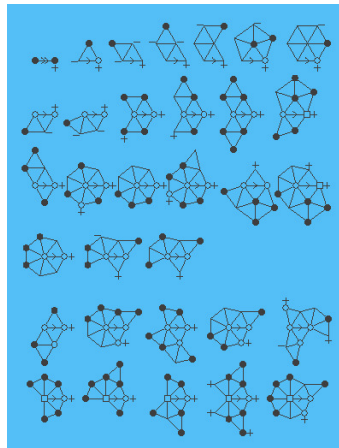
11.1 The History of Technology in Maths

- Early 1800's: [Weierstrass function](#)

$$f(x) = \sum_{n=0}^{\infty} a^n \cos(b^n \pi x)$$

disproved that continuous functions are differentiable.

- Late 1800's: [Four-color Theorem](#): For any loopless planar graph G we have $\chi(G) \leq 4$.
 - False proofs by Kempe (1879), Tait (1880), these proofs stood unchallenged for 11 years.
 - 1970s: Appel, Haken computer-aided proof (> 1000 cases)



A visualization from Thomas (1995)

– The existence of **proof by exhaustion**.

11.2 Values of Mathematics

Some questions to reconsider about:

- Among possible theorems to prove, why prove these?
- Among possible proofs of statement, why favour certain proofs?

11.3 Math in Technology

- Universal Turing Machine (1930s) → Transistors → Digital Computer

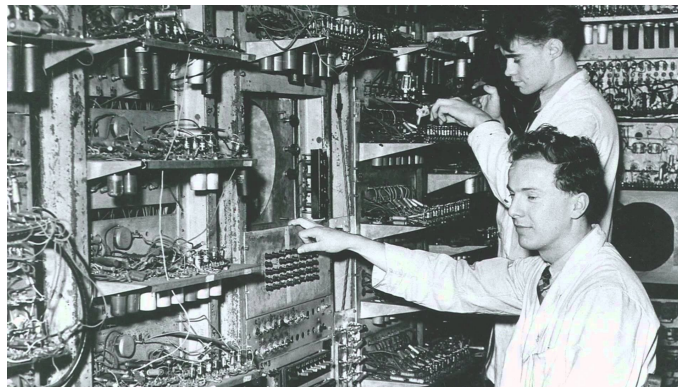
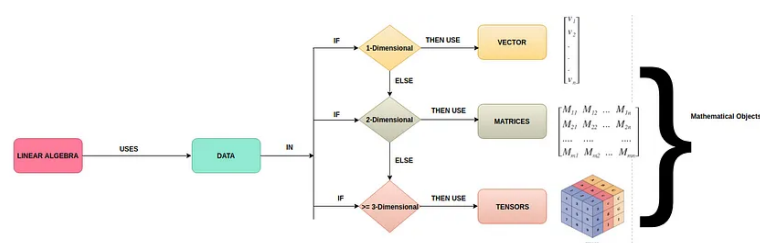


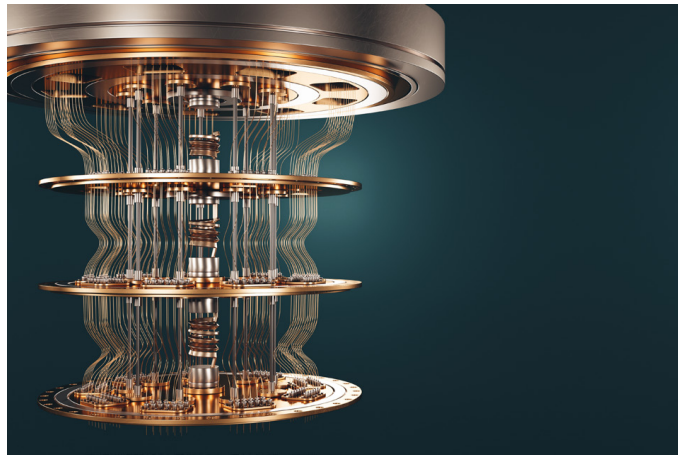
Photo of Alan Turing and the Turing Machine in 1936 (Pivotal)

- Linear algebra → computers → optimisation, graphics → AI



A visualization of AI by Shafi (2020)

- Quantum mechanics → superconductors → quantum computers



- Non-Euclidean geometry → general relativity → GPS

11.4 Technology in Math

- **Education:** Blended learning, proofs expanded on demand (i.e. Github Copilot)

```
// write a binary search algorithm
const binarySearch = (arr, target) => {
  let left = 0;
  let right = arr.length - 1;
  let middle = Math.floor((left + right) / 2);
  while (arr[middle] !== target && left <= right) {
    if (target < arr[middle]) {
      right = middle - 1;
    } else {
      left = middle + 1;
    }
    middle = Math.floor((left + right) / 2);
  }
  return arr[middle] === target ? middle : -1;
}
```

Github Copilot

- **Communication:** Stack Exchange, Stack Overflow, arXiv, blogs



Stack Exchange

- **Experimental Math:** Computation is used to explore math properties and patterns.

- **Boolean Pythagorean Triples Problem**: For any partition of $\{1, 2, \dots, 7825\}$ into 2 sets, one of them contains a Pythagorean triple. (7825 is the smallest possible number)
- **Kepler's Conjecture**
- Searching for counterexamples (i.e. for RH, Collatz, ...)
- **Tools**: [Lean Search](#), AlphaProof, AlphaGeometry, [OEIS](#), ...