CmpE 220

Lecture Notes

Fall 2023

H. Bicken Yilmaz

Defn: A proposition (statement) is a declarative sentence that is either TRUE or FALSE

Ex: S_1: 5 is an integer ✓ prop.

S_2: Do not run fast ✗ not prop

S_3: $(x+y)^2 = x^2 + y^2$ ✗

S_4: For all $x, y \in \mathbb{R}$ $(x+y)^2 = x^2 + y^2$ ✓

S_5: This statement is false ✗

Gödel incompleteness theorem

⊛ Using logical connectives we form new props out of prev. given props.

Statement Connective	Symbol
and	$\wedge$
or	$\vee$
implies	$\Rightarrow$
if and only if	$\Leftrightarrow$
not	$\neg$ or $\sim$

Given that P, Q are statements, then $P \wedge Q$, $P \vee Q$, $P \Rightarrow Q$, $P \Leftrightarrow Q$, $\neg P$ are also statements.

Ex: $(P \wedge q) \vee r$

↳ main connective

Defn: The main connective in a sentence is the last connective to be applied.

Ex: $\neg (p \vee q)$: $\neg$ is the main connective.

Condition Statement $P \Rightarrow q$: P implies q

hypothesis ↩ ↪ conclusion

if P then q

q provided that P

P is a sufficient condition that q

P	q	$P \Rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

* Note that any implication with a true conclusion is true
* Note that any " " " false hypotesis " "

Examples

1) $p: x=-1$ $\quad q: x-1=-2$ TRUE

Contrapositive

$p \Rightarrow q \equiv \neg q \Rightarrow \neg p$ ↳ equivalent

Converse of $p \Rightarrow q$ is $q \Rightarrow p$

Contrapositive

$\neg q: x-1 \neq -2$ $\quad \neg p: x \neq -1$

$\neg q \Rightarrow \neg p$ TRUE

ex2:

$p: x=-1$ $\quad q: x^2=1$ $\quad p \Rightarrow q$ TRUE

$q \Rightarrow p$ FALSE

Biconditional Statement:

$p \iff q$: p iff q

- $p \iff q$ is defined to be true if both $p \Rightarrow q$ and $q \Rightarrow p$ are TRUE.

$p \Rightarrow q$ — p is a sufficient condition for q

q is a necessary " " p

$p \iff q$ — p is a sufficient and necessary condition for q

Defn: Let $p, q, r, s \ldots$ be props. Any new prop formed by them using the signs $\neg, \vee, \wedge, \Rightarrow, \iff$ are said to be complex props.

Let A, B complex props; A and B are said to be logically equivalent $(A \equiv B)$ if A and B have the same truth values for all possible truth values of $p, q, r \ldots$

⊛ Main Logical Equivalences (You can directly use in proofs)

- $\neg\neg p \equiv p$ Rule of double negation
- $p \Rightarrow q \equiv \neg p \vee q$ OR form of implication
- $p \Rightarrow q \equiv \neg q \Rightarrow \neg p$ contrapositive of an impl.
- $\neg(p \vee q) \equiv \neg p \wedge \neg q$
- $\neg(p \wedge q) \equiv \neg p \vee \neg q$

} de Morgan's Law

Theorem: Associativity of conjunction ($\wedge$) and disjunction ($\vee$)

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

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

ex: Let p, q, r be props. Then the followings are tautologies (always TRUE)

a) $\left[(p \Rightarrow q) \wedge (q \Rightarrow r)\right] \Rightarrow (p \Rightarrow r)$

Rules of Inference

⊛ A premise is a statement that is assumed in the context of a proof.

⊛ A proof is a step by step demonstration that a statement can be derived from a collection of premises. Each step of a proof is either a premise or can be shown to be a consequence of prev. steps using certain rules of inference.

⊛ Modus Ponens Rule (MP)

$$[p \wedge (p \Rightarrow q)] \Rightarrow q$$

Ex: Let's assume the following statements are true,

s_1: "If it is raining then there are clouds in the sky" TRUE

s_2: "It is raining" TRUE

Conclusion: "There are clouds in the sky." By using MP rule

⊛ Adjoining Premises Rule

Any statement that can be proved from the premises can be adjoined to the premises in a proof.

Ex:

1) $p \vee q \Rightarrow (\neg p \Rightarrow q)$
2) $p \vee q$
3) $\neg p$
4) $q \Rightarrow r$

→ Prove r

Proof: 1) $p \vee q$ (premise)

2) $(p \vee q) \Rightarrow (\neg p \Rightarrow q)$ (premise)

3) $\neg p \Rightarrow q$ (by MP (1 and 2))

4) $\neg p$ (premise)

5) q (Adj. step 3 , mp (3,4))

6) $q \Rightarrow r$

7) r (Adj 5,6 , mp (5,6))

Direct Proof of an Implication

To prove an implication $p \Rightarrow q$ from a set of premises R, it is sufficient to assert a hypothesis P as an aditional premise and show that the conclusion q is provable from the augmented set of premises.

⊛ Due to the tautology $[R \Rightarrow (p \Rightarrow q)] \Leftrightarrow [(R \wedge p) \Rightarrow q]$

Adjunction Rule

If both p and q are provable from the set of promises R, then $p \wedge q$ is provable from the set of premises R

⊛ Due to the tautology: $[(R \Rightarrow p) \wedge (R \Rightarrow q)] \Leftrightarrow [R \Rightarrow (p \wedge q)]$

Substitution Rule

If we have the premise $p \Leftrightarrow q$ then we can substitute p for q and q for p.

Contradiction Rule

To prove q from a set of premises R, it is sufficient to use $\neg q$ as an additional premise to deduce a contradiction.

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

Discussion → How to prove $p \Rightarrow q$

1) Assume p and show q (direct proof)

2) Prove $\neg q \Rightarrow \neg p$ (proof by contrapositive)

→ Assume $\neg q$ → reach $\neg p$

3) Assume $\neg(p \Rightarrow q)$ ie $\neg(\neg p \vee q)$ and reach contradiction
ie $p \wedge \neg q$

Predicate Calculus

Not all mathematical statements are propositions.

$-1 < 5$ this is a prop and it is TRUE

$x^2 - 4 = 0$ not a proposition because it depends on the value of x

Predicate Calculus involves logical connectives used in propositional calculus and also variables, predicates, and quantifiers.

Defn: Variable is a symbol representing an unspecified object that can be chosen from a univ. set U.

Defn: A predicate is a sentence $P(x_1, x_2, \ldots x_n)$ involving variables $x_1, x_2 \ldots x_n$ with the property that

" when specific values from the universal set are assigned to $x_1, \ldots x_n$, the resulting statement is either TRUE or FALSE".

ex: $U = \mathbb{R}$ $\quad x^2 < y^2 - 1$ $\rightarrow$ false for $x = y = 0$

True for $x = 0 \quad y = 4$

$\mathbb{N} = \{0, 1, 2 \dots\}$ natural nums

$\mathbb{N}^+ = \{1, 2 \dots\}$ positive natural nums

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

$\mathbb{Q} = \{\text{rational nums}\} = \left\{\frac{p}{q} \mid p, q \in \mathbb{Z},\ q \neq 0\right\}$

$\mathbb{R} = \{\text{real nums}\} = \{\text{Equivalence classes of Cauchy Sequences}\}$?

$\mathbb{C} = \{x + yi \mid x, y \in \mathbb{R}\}$

$A = \{x \in \mathbb{Q} \mid x < \sqrt{2}\}$ → $\sqrt{2}$ is an upper bound. Not in the set A

$B = \{x \in \mathbb{R} \mid x < \sqrt{2}\}$ → $\sqrt{2}$ " " " " In the set B

What is the LEAST u.b. that is rational?

↳ There is no such element.

⊛ Solution Set

If $P(x)$ is a predicate then the set of elements from a given universe U that make $P(x)$ true is called the solution set for $P(x)$ in U and it is written as $\{x : P(x)\}$

Quantifiers

The expression like "for any x", "for every x", "for all x",

"There exist some x", "there exist x", "there exists at least one x"

are symbolized by quantifiers.

① Universal Quantifier $(\forall x)$

② Existential Quantifier $(\exists x)$

③ Descriptive Quantifier $(\exists! x)$ "There exists a unique"

? is it TRUE $(\forall x \in \mathbb{R} \quad \forall y \in \mathbb{R})$ that $x^2+y^2=(x+y)^2$

No

? is it TRUE $(\exists x \in \mathbb{R} \quad \exists y \in \mathbb{R})$ that $x^2+y^2=(x+y)^2$

Yes

? is it TRUE $(\forall x \in \mathbb{R} \quad \exists y \in \mathbb{R})$ $\exists$ such that $x^2+y^2=(x+y)^2$

Yes

A symbol cannot apper in a mathematical statement unless it is first introduced by a quantifier

Compare

1) $\forall x \in \mathbb{R}^+ \; \exists y \in \mathbb{R}^+ \ni \; y < x$ true

2) $\exists y \in \mathbb{R}^+ \; \forall x \in \mathbb{R}^+ \ni \; y < x$ false

Proof of 1: let $x_0 \in \mathbb{R}^+$ take $y = \frac{x_0}{5}$ then $y \in \mathbb{R}^+$ ✓, $y < x_0$ ✓

4.10.23

Ex: Every real number is either positive, negative, or zero.

$\forall x \in \mathbb{R} \quad x > 0 \vee x < 0 \vee x = 0$ (restricted form)

$\equiv$

$\forall x \quad x \in \mathbb{R} \Rightarrow x > 0 \vee x < 0 \vee x = 0$ (standart form)

STD	RESTRICTED
$\forall x \quad x \in \mathbb{R} \Rightarrow P(x)$	$\forall x \in \mathbb{R} \quad P(x)$
$\exists x \quad x \in \mathbb{N}$ and $P(x)$	$\exists x \in \mathbb{N} \quad P(x)$
$\forall x \; \forall y \quad x, y \in \mathbb{R} \Rightarrow S(x,y)$	$\forall x \in \mathbb{R} \; \forall y \in \mathbb{R} \quad S(x,y)$

Ex: $x \in U_p$ Universal set of people

$y \in U_f$ " " " fruits

$L(x,y)$ person x likes to eat y

1) $\forall x \in U_p \quad \forall y \in U_f \quad L(x,y)$

Every person likes every fruit

2) $\forall x \in U_p \quad \exists y \in U_f \quad L(x,y)$

Every person likes at least one fruit

3) $\exists x \in U_p \quad \forall y \in U_f \quad f(x,y)$

There is at least a person that likes every fruit.

Negation of Statements with Quantifiers

Q: All people have red hair. $\longrightarrow \forall x \in U_p \quad p(x)$

$\neg$ Q: There is at least one person who doesn't have red hair. $\longrightarrow \exists x \in U_p \quad \neg p(x)$

p(x): person x has red hair

Ex: Write the statements with quantifiers and variables and then negate them.

1) The square of every non-zero real number is positive.

+ $\forall x \in \mathbb{R} \setminus \{0\} \quad x^2 > 0$	+ $\forall x \ (x \in \mathbb{R} \setminus \{0\} \Rightarrow x^2 > 0)$
- $\exists x \in \mathbb{R} \setminus \{0\} \quad x^2 \leq 0$	- $\exists x \ (x \in \mathbb{R} \setminus \{0\}$ and $x^2 \leq 0)$

Rule $\quad \neg [\forall x \in \mathbb{R} \ p(x)] \equiv \exists x \in \mathbb{R} \ \neg p(x)$

Rule $\quad \neg [\forall x \exists y \ R(x,y)] \equiv \exists x \forall y \ \neg R(x,y)$

Ex: find the negation of

$\forall \varepsilon \in \mathbb{R}^+ \quad \exists N \in \mathbb{N} \quad x_N > 0$ and $|x_N - L| < \varepsilon$

Neg: $\exists \varepsilon \in \mathbb{R}^+ \quad \forall N \in \mathbb{N} \quad x \leq 0$ or $|x_N - L| \geq \varepsilon$

Proof Techniques

1) Direct proof of an implication

2) Proof by cases

3) Proof by contrapositive

4) Proof by contradiction

5) Biconditional Proof

6) Proof by Mathematical Induction

Defn: An integer $z \in \mathbb{Z}$ is called even if there exists an $x \in \mathbb{Z}$ $\ni$ $z = 2x$

Defn: Suppose that $a, b \in \mathbb{Z}$, we say a divides b or a is a divisor of b or b is a multiple of a if there exists an integer c such that $ac = b$. we define it as $a \mid b$

$$\forall a, b \in \mathbb{Z} \quad a \mid b \Leftrightarrow \exists c \in \mathbb{Z} \quad ac = b$$

Defn: A natural number n is called prime iff it has exactly two divisors. in $\mathbb{N}$ (1 and n)

Defn: Let $a, b \in \mathbb{Z}$, not both equal to zero. The greatest common divisor of a and b (denoted by $gcd(a,b)$) is the unique integer with the following props.

i) $d \mid a \wedge d \mid b$

ii) if $d_1 \in \mathbb{Z}$ and $(d_1 \mid a$ and $d_1 \mid b)$ then $d_1 \mid d$

iii) $d > 0$

① Direct Proof of an Implication

To prove an implication by direct proof tech, we assume the hypothesis is true and we use the hypothesis along with other known true statements and relevent definitions to deduce the conclusion.

Outline of the proof of "$p \Rightarrow q$"

Proof: Assume (suppose) p

$\equiv$ } → known true statements and inference rules and relevant defn.s

Therefore q

Examples:

Theorem: If x is odd, then x^2 is odd

Proof: Suppose x is odd

$\Rightarrow \exists n \in \mathbb{Z} \quad x = 2n+1$

$\Rightarrow x^2 = 4n^2 + 4n + 1$

$\Rightarrow x^2 = 2\underbrace{(2n^2+2n)}_{\in \mathbb{Z}} + 1$

So $\exists h \in \mathbb{Z} \ni x^2 = 2h+1$

Therefore x^2 is odd.

Theorem: If x, y, u, v are real numbers with $x<y \wedge u<v$

then $x+u < y+v$

Proof: Assume $x, y, u, v \in \mathbb{R}$ ∋ $x<y \wedge u<v$

① ②

① $\Rightarrow x+u < y+u$

② $\Rightarrow u+y < v+y$

So $x+u < y+u < y+v$

Therefore $x+u < y+v$

Prove that if $x \in \mathbb{R}$ and $x^2-4x+6=x$ then $\underbrace{x=2 \text{ or } x=3}$

Proof: Suppose $x \in \mathbb{R}$ and $x^2-4x+6=x$

then $x^2-5x+6=0$

then $(x-2)(x-3)=0$

then $x=2$ or $x=3$

Prove that $\forall x, y \in \mathbb{R}^+$ if $x \le y$ then $\sqrt{x} \le \sqrt{y}$

Proof: suppose $x \le y$

so $0 \le y-x$

so $0 \le (\sqrt{y})^2 - (\sqrt{x})^2$

so $0 \le \underbrace{(\sqrt{y}+\sqrt{x})}_{>0}(\sqrt{y}-\sqrt{x})$

so $0 \le (\sqrt{y}-\sqrt{x})$

so $\sqrt{x} \le \sqrt{y}$

(2) Proof by Cases

To prove an implication in which the hypothesis is an "OR statement" it is necessary and sufficient to consider two cases.

i) prove that the conclusion follows from the first statement.

ii) " " " " " " second " .

Some technique if there are more than two cases.

Ex $\forall x, y \in \mathbb{R} \quad |x+y| \leq |x| + |y|$

Proof:

case i) $x \geq 0 \quad y \geq 0$ then $|x| = x \quad |y| = y$ So $|x+y| = x+y \leq x+y = |x|+|y|$

case ii) $x \geq 0 \quad y < 0$ then $|x| = x \quad |y| = -y$

$x+y$? two cases for this

case ii.1) $x+y \geq 0$ then $|x+y| = x+y \leq x-y = |x|+|y|$

case ii.2) $x+y \leq 0$ they $|x+y| = -x-y \leq x-y = |x|+|y|$

case iii) $x < 0 \quad y \geq 0$ similar to case two.

case iv) $x < 0 \quad y < 0$ then $|x| = -x \; |y| = -y \quad |x+y| = -x-y \leq -x-y = |x|+|y|$

Ex If $n \in \mathbb{N}$ then $1 + (-1)^n (2n-1)$ is a multiple of 4

exercise

③ Proof by contrapositive

Recall that $p \Rightarrow q \equiv \neg q \Rightarrow \neg p$

To prove $p \Rightarrow q$ statements, we may prove "$\neg q \Rightarrow \neg p$"

> Theorem: if p then q
>
> proof: (contrapositive proof)
>
> Suppose $\neg q$
>
> ≡≡≡
>
> Therefore $\neg p$

Ex Let x be an integer. If $\underbrace{x^2-6x+5}_{\circledast}$ is even then x is odd.

Proof: (Proof by contrapositive)

Assume x is even.

So $\exists k \in \mathbb{Z} \ni x = 2k$

So $x^2-6x+5 = 4k^2-12k+5 = 2(\overbrace{2k^2-6k+2}^{\in \mathbb{Z}})+1$

So $\exists h \in \mathbb{Z} \ni \circledast = 2h+1$

So $\circledast$ is not even

④ Proof by contradiction

> Thm: p
>
> Proof: Assume for contradiction $\neg p$
>
> ≡≡≡
>
> we get c
>
> ≡≡≡
>
> we get $\neg c$
>
> Thus $\neg p \Rightarrow c \wedge \neg c$, so p is true.

Thm: The number whose square is $2 = 2^*$

2^* is not rational.

Proof: Assume for contradiction 2^* is rational

So $2^* = \frac{a}{b}$ $a, b \in \mathbb{Z}$ $b \neq 0$ $\gcd(a,b) = 1$

So $(2^*)^2 = \frac{a^2}{b^2}$ i.e. $2 = \frac{a^2}{b^2}$

So $2b^2 = a^2$ (Δ)

So a^2 is even

So a is even

So $\exists k \in \mathbb{Z}$ $2k = a$

So $(2k)^2 = a^2 = 2b^2$ (by Δ)

So $4k^2 = 2b^2$

So $2k^2 = b^2$

So b^2 is even

So b is even

So $\gcd(a,b) \geq 2$

$\therefore \times$

Hence 2^* is NOT rational

Defn: A real number x is called rational if there exists integers a, b such that $b \neq 0$ and $x = \frac{a}{b}$. A real number y is called irrational if y is not rational.

Thm: There exists infinitely many prime numbers.

Proof: Assume for contradiction there are finite number of primes.

So let $\mathbb{R}$ be the set of prime numbers.

i.e. $\mathbb{R} = \{p_1, p_2 \cdots \underline{\underline{p_n}}\}$
largest

Now consider $p = p_1 p_2 \cdots p_n + 1$

So p is positive and $p > 1$ and $p > p_n$

also p is not a prime number since p_n is the largest.

So p is the product of some prime numbers.

So $\exists p_k \in \mathbb{R} \ni p_k \mid p$

So $\exists c \in \mathbb{Z} \quad p_k \cdot c = p$

Then $1 = p - (p-1)$

$= p_k \cdot c - (p_1 p_2 \cdots p_n)$

$= p_k \left(c - \prod_{\substack{i=1 \\ i \neq k}}^{n} p_i\right)$

(and we know that $p_k > 1$)

→ Thus $p_k \mid 1$

Alternative:

Proof: Assume for contradiction there are finite number of primes.

So let $\mathbb{R}$ be the set of prime numbers.

i.e. $\mathbb{R} = \{p_1, p_2 \dots \underline{\underline{p_n}}\}$ (largest)

Now consider $p = p_1 p_2 \cdots p_n + 1$

So p is positive and $p > 1$ and $p > p_n$

also p is not a prime number since p_n is the largest.

$p \mid p_i$ — p is not divided by any prime so it must be a prime itself.

1

Ex: Suppose $\forall a \in \mathbb{Z}$ if $\underbrace{a^2 - 2a + 7}_{(**)}$ is even $\overbrace{\text{(*)}}$ then a is odd.

Proof: Assume for a contradiction (*) and a is even

for some $a \in \mathbb{Z}$

Thus $\exists k \in \mathbb{Z} \ni a^2 - 2a + 7 = 2k$

$\exists c \in \mathbb{Z} \ni a = 2c$

So $a^2 - 2a + 7 = 4c^2 - 4c + 7 = 2\underbrace{(2c^2 - 2c + 3)}_{\in \mathbb{Z}} + 1$

Thus $a^2 - 2a + 7$ is odd.

Remark: Proofs by contradiction of statements of the form

$p \Rightarrow q$ can usually be replaced by proofs by contrapositive.

2nd Proof: (by contrapos.)

Suppose a is even want $(**)$ is odd

So $\exists c \in \mathbb{Z}$ $a = 2c$

So $4c^2 - 4c + 7 = (**)$

So $2(\underbrace{2c^2 - 2c + 3}_{\in \mathbb{Z}}) + 1 = (**)$

So $(**)$ is odd

---

(5) Biconditional Proof

$$[p \Leftrightarrow q] \equiv [p \Rightarrow q \wedge q \Rightarrow p]$$

Proposition $P \Leftrightarrow Q$

Proof: (1) first we will prove $P \Rightarrow Q$

Suppose P

$\equiv$

Hence Q

(2) Then we will prove $Q \Rightarrow P$

Suppose Q

$\equiv$

Hence P

Proposition: Let n be an integer. Then n is odd iff n^2 is odd.

Proof: $(P \Rightarrow Q)$

Suppose n is odd. want: n^2 is odd

So $\exists k \in \mathbb{Z} \ni n = 2k+1$

So $n^2 = 4k^2 + 4k + 1 = 2\underbrace{(2k^2+2k)}_{\in \mathbb{Z}} + 1$

So n^2 is odd.

$(Q \Rightarrow P)$

Let's prove by contrapositive

Suppose n is even: want: n^2 is even

So

$=$
$=$
$=$

(*) Proof of existential statements

To prove "$\exists x\ p(x)$" we have to find an object a_0 and show a_0 has property $P()$. i.e. $p(a_0)$ is true.

(*) Disproving of Universal statements

To disprove "$\forall x\ p(x)$" we have to prove the negation i.e. "$\exists x\ \neg p(x)$". So we have to find an object a_0 and show that $P(a_0)$ is false.

(*) Disproving of existential statements.

To disprove "$\exists x\ p(x)$" we have to prove the negation. i.e. "$\forall x\ \neg p(x)$". By a proof technique.

Ex: $\forall x \in \mathbb{R}$ if $x < y$ then $x^2 < y$ Disprove by counterexample: $x = -2$ $y = 1$

Buna benzer sinav sorusu var.

⑥ Principle of Mathematical Induction

Well ordering principle of Natural Numbers:

Every nonempty subset of $\mathbb{N}$ has a smallest element in $\mathbb{N}$

Question: Is it true that $1 + 3 + 5 + \cdots + (2n-1) \stackrel{?}{=} n^2$

$n = 1$	1	$n^2 = 1$
$n = 2$	4	$n^2 = 4$
$n = 3$	9	$n^3 = 9$
	⋮	

Mathematical Induction (MI)

Let $P_1, P_2, \ldots P_n$ be propositions

Assume

H1) P_1 is true (Basis step)

H2) $\forall n$ $n = 1, 2 \ldots$ the implication $P_n \Rightarrow P_{n+1}$ (Induction step)

Then $\forall n$ $n = 1, 2 \ldots$ proposition P_n is true

Read Proof

Ex: Prove that $\forall n \in \mathbb{N}$ $1^2+2^2+\dots+n^2 = \frac{n(n+1)(2n+1)}{6}$

Proof: by MI

Basis step: P_1 is true since $1^2 = \frac{1\cdot 2\cdot 3}{6}$

Induction Step: Assume P_n is true want: P_{n+1} is true

So $1^2+2^2\dots n^2 = \frac{n(n+1)(2n+1)}{6}$

So $1^2+2^2\dots n^2+(n+1)^2 = \frac{n(n+1)(2n+1)}{6} + (n+1)^2$

So $= (n+1)\left[\frac{n(2n+1)}{6} + n+1\right]$

$= (n+1)\cdot\left[\frac{2n^2+n+6n+6}{6}\right]$

$= (n+1)\cdot\left[\frac{2n^2+7n+6}{6}\right]$

$= \frac{(n+1)\cdot(n+2)(2n+3)}{6}$

So P_{n+1} is true

Hence $\forall n$ P_n by MI

Ex: Let $x>0$ Prove that $\forall n = 1,2\dots$ $(1+x)^n \geq 1+nx$

Proof by MI

Basis step: $n=1$ $(1+x)^1 \geq 1+x$ ✓

Induction step: Assume P_n is true for some n want: P_{n+1} is true

So $(1+x)^n \geq 1+nx$

mult by $1+x$ ↷

So $(1+x)^{n+1} \geq (1+nx)(1+x)$

So $(1+x)^{n+1} \geq \underbrace{(1+nx+x)}_{1+(n+1)x} + \underbrace{nx^2}_{>0} \geq 1+(n+1)x$

So P_{n+1} is true

Hence P_n is true $\forall n = 1,2,3\ldots$ by MI

Principle of Mathematical Induction (General form) please read

Principle of Strong Mathematical Induction

↳ Let $P_{k_0}, P_{k_0+1}, \ldots P_n$ be a list of statements

If i) P_{k_0} is true

ii) If $P_{k_0}, \ldots P_n$ are all true then P_{n+1} is true

i.e. $(P_{k_0} \wedge P_{k_0+1} \ldots \wedge P_n) \Rightarrow P_{n+1}$

Then P_n is true for all $n \geq k_0$

Ex: Each integer greater then 1 is either prime or is a product of primes.

P_n : $\forall n \in \mathbb{N}$ $n \geq 2$ n " " " " " " "

Proof by strong mathematical induction:

Basis step: P_2 is true since 2 is a prime.

Induction step: Assume $P_2, P_3, \ldots P_n$ are TRUE Want: P_{n+1} is true.

Now consider $(n+1)$ is either prime or not prime

case 1: if $n+1$ is prime then P_{n+1} is true

case 2: if $n+1$ is not prime

So $\exists a,b \in \mathbb{N}$ $n+1 = a \cdot b$ where $a,b < n+1$ $a,b > 1$

by induction hypothesis of the induction step

we have P_a and P_b are true.

Then each of a and b is either prime or multiples of primes

So $a = q_1 \cdot \dots \cdot q_s$ where q_i's are primes

$b = r_1 \cdot \dots \cdot r_k$ where r_i's are primes

Hence $n+1 = a \cdot b = q_1 \cdot \dots \cdot q_s \cdot r_1 \cdot \dots \cdot r_k \rightarrow$ multiples of primes.

$\therefore P_{n+1}$ is true

Hence $\forall_n P_n \quad n \geq 2$

Pigeon Hole Principle

If k is a positive integer and $k+1$ or more objects are placed into k boxes, then there is at least one box containing two or more objects.

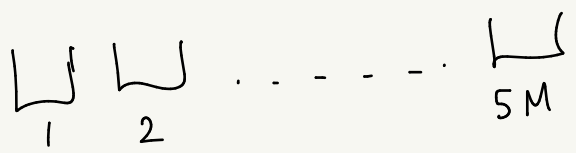
(Proof by contrapositive or contradiction for interested)

Ex: Prove that there are at least two people having same number of hairs on their head (excluding the people with no hair)

Proof: avg number of hairs on head = 100.000

max is $\approx$ 1.000.000

world population: 7.7b 2020



Generalized PHP

If N objects are placed into k boxes then there exists one box containing at least $\lceil \frac{N}{K} \rceil$ objects.

Ex: What is the minimum number of students required in a discrete math class to be sure that at least 6 of them will recieve the same grade if there are 5 possible grades.

26

Recall: $\mathbb{N} = \{0,1,2 \dots\}$ $\quad \mathbb{Z} = \{\dots -1,0,1 \dots\}$

$\mathbb{N}^+ = \{1,2 \dots\}$ $\quad Q = \{\frac{p}{q} \mid p,q \in \mathbb{Z}\ q \neq 0\}$

Set: Collection of objects having a certain property.

Defn: An obj. x belonging to set A is said to be a member or an element of A. Denote this as $\underbrace{x \in A}_{\text{element}}$ $\underbrace{x \notin A}_{\text{not an element.}}$

Two sets are equal iff they have the same elements.

What does it mean to have $A \neq B$

↳ $\exists x\ (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)$

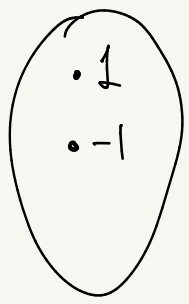
(*) Representation of Sets

1) Listing of elements $\{-1, 4, \Delta\}$

2) Giving a property shared by the elements of the set

$A = \{x \mid x \text{ is a real number and } x^2 = 1\}$

3) By Venn Diagrams



Notation: Let $a, b \in \mathbb{R}$ $a < b$

$$[a,b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$$

$$(a,b) = \{x \in \mathbb{R} \mid a < x < b\}$$

⊛ The unique set with no elements is called <u>empty set</u> or the <u>null set</u> and denoted by $\emptyset$ or $\{\}$

Ex: $A = \{x \in \mathbb{R} \mid x > x\} = \emptyset$

Important Defn: Given two sets A and B. If every element of A is also an element of B, then we say <u>A is a subset of B</u> and denote it by $A \subseteq B$.

If A is a subset of B and $A \neq B$, then we write $A \subset B$. In this case, we say A is <u>a proper subset of B</u>.

$$A \subseteq B \iff \underbrace{\forall x \in U \quad x \in A \Rightarrow x \in B}_{\forall x \in A \quad x \in B}$$

$$A \not\subseteq B \iff \underbrace{\exists x \in U \quad x \in A \wedge x \notin B}_{\exists x \in A \quad x \notin B}$$

Given any set B $\quad \emptyset \subseteq B \quad$ TRUE

Proof: Assume for a contradiction $\emptyset \not\subseteq B$

So $\exists x \in U \quad \underbrace{x \in \emptyset}_{\text{False}} \wedge x \notin B$

$\lightning$

Alt:

$\forall x \in U \quad \underbrace{x \in \emptyset}_{\text{False}} \Rightarrow x \in B$

TRUE

Prop:

- $A \subseteq A$
- $(A \subseteq B \wedge B \subseteq C) \Rightarrow (A \subseteq C)$
- For any set A $\quad \emptyset \subseteq A$

For proving $A = B$ we need to prove $A \subseteq B \wedge B \subseteq A$

Set Operations

Defn: Let A be a set in a universal set U, the complement of A denoted by A^c is $A^c = \{x \in U \mid x \notin A\}$

Defn: Let $E = \{x \in U \mid p(x)\}$

$F = \{x \in U \mid q(x)\}$

So $E \cap F = \{x \in U \mid p(x) \wedge q(x)\}$

$$E \cup F = \{x \in U \mid p(x) \vee q(x)\}$$

Defn: Two sets A and B are said to be disjoint if $A \cap B = \emptyset$

Defn: Given two sets A and B, the difference set $A \setminus B =$

$$\{x \mid x \in A \wedge x \notin B\}$$

Symmetric Difference: $A \triangle B = (A \setminus B) \cup (B \setminus A)$

Defn: (Power set) Let S be a set. The power set of S is denoted by $P(S)$ or 2^S is the set of all subsets of S.

$$P(S) = \{x \mid x \subseteq S\}$$

i.e. $x \in P(S) \Rightarrow x \subseteq S$

Lemma: A and B two sets

i) $A \cap B = \emptyset \iff A \subseteq B^c$

ii) $(A \cap B)^c = A^c \cup B^c$
$(A \cup B)^c = A^c \cap B^c$
} De Morgan's Laws for sets

Proofs:

(i) ($\Rightarrow$) Assume $A \cap B = \emptyset$ want: $A \subseteq B^c$

Let $x \in A$ be arbitrary.

So $x \notin B$ since $A \cap B = \emptyset$

So $x \in B^c$

$\therefore A \subseteq B^c$

($\Leftarrow$) Assume for a contradiction

$A \subseteq B^c \wedge \quad A \cap B \neq \emptyset$

So $\exists x_0 \in (A \cap B)$

So $(x_0 \in A) \wedge (x_0 \in B)$

So $(x_0 \in A) \wedge (x_0 \notin B^c)$

$\hookrightarrow x_0$ must be in B^c since $A \subseteq B^c$

$\lightning$

ii) Prove $(A \cap B)^c = A^c \cup B^c$

We have to prove $\underbrace{(A \cap B)^c \subseteq (A^c \cup B^c)}_{1}$ and $\underbrace{(A \cap B)^c \supseteq (A^c \cup B^c)}_{2}$

① Let $x \in (A \cap B)^c$

So $x \notin (A \cap B)$

Hence $x \notin A$ OR $x \notin B$ (by definition of intersection)

So $x \in A^c$ OR $x \in B^c$

So $x \in (A^c \cup B^c)$

$\therefore (A \cap B)^c \subseteq (A^c \cup B^c)$

② Let $x \in (A^c \cup B^c)$

So $(x \in A^c)$ OR $(x \in B^c)$

So $(x \notin A)$ OR $(x \notin B)$

Then $x \notin (A \cap B)$ (by defn. of int.)

So $x \in (A \cap B)^c$

$\therefore (A \cap B)^c \supseteq (A^c \cup B^c)$

① Let $x \in A \triangle B$ be arbitrary

So $x \in (A \setminus B) \cup (B \setminus A)$

So $x \in (A \setminus B)$ or $x \in (B \setminus A)$

So $(\underbrace{x \in A}_{1} \wedge \underbrace{x \notin B}_{2}) \vee (\underbrace{x \in B}_{3} \wedge \underbrace{x \notin A}_{4})$

Want $x \in (A \cup B) \setminus (A \cap B)$

$x \in (A \cup B) \quad x \notin (A \cap B)$

$(x \in A \vee x \in B) \wedge (x \notin A \vee x \notin B)$

$(1 \wedge 2) \vee (3 \wedge 4)$

$(1 \vee 3) \wedge (2 \vee 4)$

1

Exercise: Prove: $A \triangle B = (A \cup B) \setminus (A \cap B)$

i.e. $(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$

show $A \triangle B \subseteq (A \cup B) \setminus (A \cap B)$

$A \triangle B \supseteq (A \cup B) \setminus (A \cap B)$

Product Sets (Cartesian Product)

Given two sets A and B, the product set (or cartesian product) of A and B is, $A \times B = \{(a,b) \mid a \in A \quad b \in B\}$

(a,b) → ordered pair
- → 2nd comp.
- → 1st component

$A \times A = \{(x,y) \mid x \in A \quad y \in A\} = A^2$

In general $A \times B \neq B \times A$

Ex: $\mathbb{R}^2$ → cartesian plane or euclidean plane

$\mathbb{R} \times \{0\}$ → x-axis

$\{0\} \times \mathbb{R}$ → y-axis

Ex: Let $A = [1,3] \quad B = [2,5)$

$A \times B = \{(x,y) \mid x \in [1,3] \quad y \in [2,5)\}$

$= \{(x,y) \mid 1 \leq x \leq 3 \quad 2 \leq y < 5\}$

$B \times A = \{(x,y) \mid 2 \leq x < 5 \quad 1 \leq y \leq 3\}$

$(x,y) \neq \{x,y\}$

different objects

$\Rightarrow \{x,y\} = \{y,x\}$

But $(x,y) \neq (y,x)$

not necessarily.

$\{x,x\} = \{x\}$

$(x,x) \neq (x)$

Exercise: Let A and B two nonempty sets

Prove that $A \times B = B \times A$ iff $A = B$

Ex: Let A and B any two sets

Prove by contrapos. $A \times B = \emptyset \Rightarrow A = \emptyset$ OR $B \neq \emptyset$

Proof. Assume $A \neq \emptyset \wedge B \neq \emptyset$ want: $A \times B \neq \emptyset$

So $\exists a_0 \in A \quad \exists b_0 \in B$ → better to write with words this is wrong.

So $(a_0, b_0) \in A \times B$

So $A \times B \neq \emptyset$

Ex: Prove for any A, B, C non-empty sets

$$A \times (B \cap C) = (A \times B) \cap (A \times C)$$

Proof: let $(x,y) \in A \times (B \cap C) \Leftrightarrow x \in A \wedge y \in B \cap C$

$\Leftrightarrow x \in A \wedge y \in B \wedge y \in C$

(1) (2) (3)

$\Leftrightarrow (x,y) \in A \times B$ by (1) and (2)

$(x,y) \in A \times C$ by (1) and (3)

$\Leftrightarrow (x,y) \in (A \times B) \cap (A \times C)$

$\therefore A \times (B \cap C) = (A \times B) \cap (A \times C)$

⊛ Properties

a) $A \cap (B \cap C) = (A \cap B) \cap C$ ... Associativity of $\cap$

b) $A \cup (B \cup C) = (A \cup B) \cup C$ ..... " " $\cup$

c) $A \cap B = B \cap A$ ..... Commutativity of $\cap$

d) $A \cup B = B \cup A$ ..... " " $\cup$

e) $A \cap \emptyset = \emptyset$

f) $A \cap A = A$ ..... Idempotency of $\cap$

$A \cup A = A$ ..... " " $\cup$

g) If $A \subseteq B$ and $A \subseteq C$ then $A \subseteq B \cap C$

Proof: Assume $A \subseteq B \wedge A \subseteq C$ want: $A \subseteq B \cap C$

case $A = \emptyset$

trivial

case $A \neq \emptyset$

Let $a \in A$ be arbitrary

So $a \in B$ since $A \subseteq B$

So $a \in C$ since $A \subseteq B$

So $a \in B \cap C$

$\therefore A \subseteq (B \cap C)$

Prop: i) $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$

ii) $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$

Family of Sets

Ex: For any $n \in \mathbb{N}$

$$A \cup (B_1 \cap B_2 \cdots \cap B_n) = (A \cup B_1) \cap (A \cup B_2) \cap \cdots \cap (A \cup B_n)$$

Proof: By MI

Basis step: $A \cup B_1 = A \cup B_1$

Ind step: Assume P_n holds

$$A \cup (B_1 \cap \cdots B_n) = (A \cup B_1) \cap \cdots \cap (A \cup B_n)$$

want: P_{n+1} holds

We know that $A \cup (B_1 \cap \cdots B_n \cap B_{n+1}) = \left[A \cup (B_1 \cap \cdots B_n)\right] \cap (A \cup B_{n+1})$

By induction step assumption we know that this ↑ equals

$$(A \cup B_1) \cap (A \cup B_2) \cap \cdots \cap (A \cup B_n) \cap (A \cup B_{n+1})$$

So P_{n+1} holds.

Let $I = \{1,2,3,4\}$ let A_1, A_2, A_3, A_4 be sets we can represent them as $\{A_i \mid i \in I\} = \{A_1, A_2, A_3, A_4\}$

$$\bigcup_{i \in I} A_i = \{x \in U \mid \exists\, i_0 \in I \ni x \in A_{i_0}\}$$

$$x \in \bigcup_{i \in I} A_i \iff \exists\, i_0 \in I \text{ s.t. } x \in A_{i_0}$$

$$\bigcap_{i \in I} A_i = \{x \in U \mid \forall i \in I \quad x \in A_i\}$$

$$x \in \bigcup_{i \in I} A_i \iff \forall i \in I \quad x \in A_i$$

Ex: $I = \{2, 3, 4, \dots\}$ $\quad A_n = \left[\frac{1}{n}, 1\right]$

$\bigcup_{n \in I} A_n = ?$ $\quad (0,1]$

① $\bigcup_{n \in I} A_n \subseteq (0,1]$ Proof: Let $x \in \bigcup A_n$

So $\exists n_0 \in I \ni x \in A_{n_0}$

So $x \in \left[\frac{1}{n_0}, 1\right]$

So $x \in (0,1]$

② $(0,1] \subseteq \bigcup_{n \in I} A_n$ Proof: Let $x \in (0,1]$

so $x > 0$

So $\exists \frac{p}{q} \in \mathbb{Q}$ $0 < \frac{p}{q} < x$ by denseness $\mathbb{Q}$

choose N_0 as q

So $\exists N_0 \in I \ni 0 < \frac{1}{N_0} < x \leq 1$

So $x \in A_{N_0}$

So $x \in \bigcup_{n \in I} A_n$

$\therefore (0,1] \subseteq \bigcup_{n \in I} A_n$

Claim: Denseness of rational numbers: $\forall a, b \in \mathbb{R}$

$a \neq b \quad \exists q \in \mathbb{Q} \quad a < q < b$

Ex: Let $A_i = \{(x,y) \mid x, y \in \mathbb{R} \quad x^2 + y^2 \leq i\}$ $\quad i \in \mathbb{N}$

Prove that $\bigcup_{i \in \mathbb{N}} A_i = \mathbb{R}^2$

Prove that $\bigcap_{i \in \mathbb{N}} A_i = \{(0,0)\}$

Relations ⭐⭐⭐

Let A and B two sets. A relation R from A into B is any subset of the product set $A \times B$ and denoted by $R \subseteq A \times B$. We write $(x,y) \in R$ or xRy for related pairs.

$A = B =$ all humans

$R_1 = \{(x,y) \in A \times B \mid x \text{ is brother of } y\}$

$R_2 = \{(x,y) \in A \times B \mid x \text{ and } y \text{ are of the same nationality}\}$

Defn: If $A = B$ $R \subseteq A \times A$ is said to be a relation on A

Defn: Let R be a relation on A i.e. $R \subseteq A \times A$

⭐ a) R is said to be reflexive if $\forall x \in A \quad xRx$

b) R is said to be irreflexive if $\forall x \in A \quad x \not R x$ i.e $\forall x \in A \quad (x,x) \notin R$

⭐ c) R " " " " symmetric if $\forall x,y \in A \quad xRy \Rightarrow yRx$

d) R " " " " asymmetric if $\forall x,y \in A \quad xRy \Rightarrow y \not R x$

⭐ e) R " " " " anti-symmetric if $\forall x,y \in A \quad xRy \wedge yRx \Rightarrow x = y$

⭐ f) R " " " " transitive if $\forall x,y,z \in A \quad xRy \wedge yRz \Rightarrow xRz$

Ex: $A = \{a, b, c\}$

$R_1 = \{(a,a), (a,b), (b,a), (b,c)\}$

	reflexive	irreflexive	sym	asym	anti-sym	transitive
R_1	X	X	X	X	X	X

a) R is reflexive $\iff \forall x \in A \quad xRx$

R is not-reflexive $\iff \exists x \in A \quad x \not R x$

b) R is irreflexive $\iff \forall x \in A \quad x \not R x$

R is not irreflexive $\iff \exists x \in A \quad xRx$

c) R is symmetric $\iff \forall x, y \in A \quad xRy \Rightarrow yRx$

R is not symmetric $\iff \exists x, y \in A \quad xRy \wedge y \not R x$

d) R is asymmetric $\iff \forall x, y \in A \quad xRy \Rightarrow y \not R x$

R is not asymmetric $\iff \exists x, y \in A \quad xRy \Rightarrow yRx$

e) R is anti-symmetric $\iff \forall x, y \in A \quad xRy \wedge yRx \Rightarrow y = x$

R is not anti-sym. $\iff \exists x, y \in A \quad xRy \wedge yRx \wedge y \neq x$

f) R is transitive $\iff \forall x, y, z \in A \quad xRy \wedge yRz \Rightarrow xRz$

R is not transitive $\iff \exists x, y, z \in A \quad xRy \wedge yRz \wedge x \not R z$

Ex: $A = \{a, b, c, d\}$ $R = \{(a,a), (b,a), (b,b), (c,c), (d,d), (d,c)\}$

	reflexive	irreflexive	sym	asym	anti-sym	transitive
R	✓	X	X		✓	

Ex: Let $A = \mathbb{R}$ $\quad R = \{(x,y) \mid x \geq y\}$

	reflexive	irreflexive	sym	asym	anti-sym	transitive
R	✓				✓	✓

$(x,x) \in R$
for all $x \in R$

→ Assume $(xy) \in R \wedge (yx) \in R$

so $x \geq y \wedge y \geq x$

so $x = y$

→ Assume $(xy) \in R \wedge (yz) \in R$ want: $(xz) \in R$

so $x \geq y \wedge y \geq z$

so $x \geq z$

so $(xz) \in R$

Ex: $A = \mathbb{Z}$ $\quad R = \{(n,m) \mid 7 \mid n-m\}$

Reflexivity: Let $n \in \mathbb{Z}$ be arbitrary

$n-n = 0 = 7 \cdot 0$

So $7 \mid n-n$

So $(n,n) \in R$

Symmetric: Assume xRy want: yRx

So $7 \mid x-y$

So $\exists k \in \mathbb{Z}$ s.t. $7k = x-y$

So $-k \cdot 7 = y - x$

($-k \in \mathbb{Z}$)

So $7 \mid y - x$

Antisymmetric

$(1,8) \in R \wedge (8,1) \in R$ but $1 \neq 8$

Transitive

Assume $xRy \wedge yRz$ want: xRz

So $7 \mid (x-y) \wedge 7 \mid y-z$

So $\exists k_1 \in \mathbb{Z} \ni 7k_1 = x-y$

$\exists k_2 \in \mathbb{Z} \ni 7k_2 = y-z$

$7k_1 + 7k_2 = x - z$

So $7(k_1 + k_2) = x - z$

($k_1 + k_2 \in \mathbb{Z}$)

So $7 \mid x - z$

Defn: Let A be a set. The identity relation on A, denoted by Id_A is $I_{dA} = \{(x,x) \mid x \in A\}$

Defn: Let R be a relation from A to B then the inverse of R written as R^{-1} is the relation on B to A and

$R^{-1} = \{(x,y) \in B \times A \mid (y,x) \in R\}$

Prop: A rel. R on A is symm. iff $R = R^{-1}$

Want: $R = R^{-1}$

Proof: ($\Rightarrow$) Assume R on A is symm.

Let $(x,y) \in R$ be arbitrary.

So $(y,x) \in R$

So $(x,y) \in R^{-1}$ since defn of R^{-1}.

$\therefore R \subseteq R^{-1}$

Let $(x,y) \in R^{-1}$ be arbitrary.

So $(y,x) \in R$

So $(x,y) \in R$ since R is symm.

$\therefore R \supseteq R^{-1}$

Hence $R = R^{-1}$

($\Leftarrow$) Assume $R = R^{-1}$

Want: R is symmetric.

$\forall (a,b) \in R \quad (b,a) \in R$

$\forall (a,b) \in A \times A \quad (a,b) \in R \Rightarrow (b,a) \in R$

Suppose $(a,b) \in R$

So $(b,a) \in R^{-1}$

So $(b,a) \in R$ since $R = R^{-1}$

$\therefore R$ is symmetric.

Defn: Let R be a relation from A into B and let S be a relation from B into C. The composition of S and R is the relation $S \circ R$ from A to C given by

$$S \circ R = \{(x,z) \in A \times C \mid \exists y \in B \quad x R y \wedge y S z\}$$

Ex: $A=\{a,b\}$ $B=\{c,d\}$ $C=\{e,f,g\}$

$R_1=\{(a,c),(b,d)\}$ $R_2=\{(a,c),(b,c)\}$ $S_1=\{(d,e),(d,f),(d,g)\}$ $S_2=S_1$

$S_1 \circ R_1 = \{(b,e),(b,f),(b,g)\}$

$S_2 \circ R_2 = \emptyset$

Characterization

Let R be a relation on A

R is Reflexive $\iff Id_A \subseteq R$

R is sym $\iff R = R^{-1}$

R is antisym $\iff R \cap R^{-1} \subseteq Id_A$

R is transitive $\iff R \circ R \subseteq R$

(*) Equivalence Relation

Let A be a set and R be a rel. on A If R is refl, sym and trans then R is said to be an equivalence relation on A

Ex: $A=\{$all lines in $\mathbb{R}^2\}$

same → $\forall L_1, L_2 \in A \quad L_1 R L_2$ iff $L_1 \parallel L_2$

→ $R=\{(L_1,L_2) \in A \times A \mid L_1 \parallel L_2\}$

Refl ✓

Symm ✓

Trans ✓

Ex: R is a rel. on $\mathbb{Z}$ $\quad nRm \iff 7 \mid n-m$

symm: Assume nRm so $\exists k \in \mathbb{Z} \ni 7k = n-m$

so $m-n = 7(-k)$ $\in \mathbb{Z}$

so $7 \mid m-n$

so mRn ✓

refl: Let x in $\mathbb{Z}$ be arbitrary

So $x-x=0$

So $7 \mid x-x$

So xRx ✓

Trans ✓

Equivalence Classes

Let R be an equivalence relation on A.

Let $x \in A$, equivalence class of x, denoted by $\bar{x}$, is defined as

$$\bar{x} = \{y \in A \mid xRy\}$$

Remark: Let R be an equivalence rel on A and $A \neq \emptyset$.

Let $x \in A$ $\quad \bar{x}$ = non empty since $x \in \bar{x}$ (at least)

Ex: Let R be a rel. on $\mathbb{Z}$ $\quad nRn \iff 3 \mid n-m$ $\quad R$: refl ✓ sym ✓ trans ✓

$\bar{0} = \{n \in \mathbb{Z} \mid 0Rn\} = \{\ldots -3, 0, 3 \ldots\}$

$\bar{1} = \{n \in \mathbb{Z} \mid 1Rn\}$

$\bar{2} = \{n \in \mathbb{Z} \mid 3Rn\} = \{\ldots -3, 0, 3 \ldots\}$

same

We only have 3 eq. classes. $\bar{0}, \bar{1}, \bar{2}$

$\{\bar{0}, \bar{1}, \bar{2}\} = \mathbb{Z}/R$

Quotient Set wrt R

Defn: Let A be a set and R be an equ. rel. on A

for any $x \in A$ let $\bar{x}$ be the equiv classes

For the set $A/R = \{\bar{x} \mid x \in A\}$

A/R is called quotient of A by R.

Prop: Let R be an equiv. rel on A.

Let $x, y \in A$ $\quad xRy \iff \bar{x} = \bar{y}$

$\bar{x} = \{y \in A \mid xRy\}$

Proof: ($\Rightarrow$) Assume $\underbrace{xRy}_{\star}$ want: $\bar{x} = \bar{y}$

Take an element $z \in \bar{x}$:

So xRz

So $\underbrace{zRx}_{\Delta}$ since R is symm.

So zRy by $(\star)$ and (Δ) and trans. of R

So yRz since R is symm

So $z \in \bar{y}$ by defn of equiv. class

$\therefore \bar{x} \subseteq \bar{y}$

Take an element $z \in \bar{y}$

So $yRz_{(\square)}$

So xRz by $(\square)$ $(\star)$ and trans.

So $z \in \bar{x}$

So $\bar{y} \subseteq \bar{x}$

($\Leftarrow$) Assume $\bar{x} = \bar{y}$ want: xRy

Take $z \in \bar{x}$ so $\underbrace{xRz}_{\star}$

↳ also $\in \bar{y}$ So yRz so $\underbrace{zRy}_{\square}$ due to sym.

So xRy because of transitivity. $(\star, \square)$

Alternative: $y \in \bar{y}$ so $y \in \bar{x}$ since $\bar{x} = \bar{y}$ So xRy

Prop: Let R be an equiv. rel on set A. Then for any $x, y \in A$

if $x \not R y$ then $\bar{x} \cap \bar{y} = \emptyset$

Proof: Assume for a contradiction $\underbrace{x \not R y}_{\square} \wedge \bar{x} \cap \bar{y} \neq \emptyset$

So $\exists a \in A \quad a \in (\bar{x} \cap \bar{y})$

so $\underbrace{xRa}_{(\star)}$ and yRa

so $aRy_{(\Delta)}$

so $\underbrace{xRy}$ by trans. by ($\star$ and Δ)

contradicts with ($\square$).

Corollary: Let R be an equiv. relation on a set A.

Then for any $x, y \in A$ either $\bar{x} \cap \bar{y} = \emptyset$ or $\bar{x} = \bar{y}$

Defn: A family of subsets $(A_\alpha)_{\alpha \in I}$ of a set A is said to be a partition of A. If we have

i) $\bigcup_{\alpha \in I} A_\alpha = A$

ii) $\forall \alpha, \beta \quad \alpha \neq \beta \Rightarrow A_\alpha \cap A_\beta = \emptyset$

iii) $\forall \alpha \in I \quad A_\alpha \neq \emptyset$

Ex: Let $A = \mathbb{N}$ A_1 = even natural numbers

A_2 = odd natural numbers

$\{A_1, A_2\} \rightarrow$ forms a partition for $\mathbb{N}$.

Ex: Let $A = \mathbb{N}$ $\quad A_0 = \{0\}$

$A_1 = \{1\}$

$\vdots$

If R is an equiv reln on A

$A/R = \{\bar{x} \mid x \in A\}$ forms a partition for A

Prop: If $(A_\alpha)_{\alpha \in I}$ is a partition of A then there exists an equivalence relation R on A such that the quotient set

$A/R = \{A_\alpha \mid \alpha \in I\}$

Proof: Assume $(A_\alpha)_{\alpha \in I}$ is a partition of A Want: $\exists R$ eq. reln s.t. $A/R = \{A_\alpha\}$

Lets define R on A xRy iff $\exists \alpha \in I$ $x, y \in A_\alpha$

Need to show: 1) R is eq. rel.

2) $A/R = \{A_\alpha\}_{\alpha \in I}$

(1) refl: Let $x \in A$ be arbitrary so $\exists \alpha \in I$ $x \in A_\alpha$ since $\{A_\alpha\}$ is a partition so xRx since x and x are elements of A_α

symm: Assume xRy so $\exists \alpha \in I$ $x, y \in A_\alpha$ by defn of R.

so yRx by defn. of R.

trans: Assume xRy and yRz so $\exists \alpha \in I$ $x, y \in A_\alpha$

$\exists \beta \in I$ $y, z \in A_\beta$

So $y \in A_\alpha \cap A_\beta$

So $A_\alpha = A_\beta$ (or $\alpha = \beta$) since $A_\alpha \cap A_\beta = \emptyset$ when $\alpha \neq \beta$

So $x, y, z \in A_\alpha$

So xRz

Hence R is an equ. reln.

(2) We need to prove $A/R \subseteq \{A_\alpha\} \wedge \{A_\alpha\} \subseteq A/R$

2.a) Let $\bar{x} \in A/R$ be arbitrary then $x \in A$

then $\exists \alpha \in I \quad x \in A_\alpha$ (since $\cup A_\alpha = A$)

claim: $\bar{x} = A_\alpha$

- let $y \in \bar{x}$ (be arbitrary) then yRx

  so $y \in A_\alpha$ (since $x \in A_\alpha$)

  $\therefore \bar{x} \subseteq A_\alpha$

- let $y \in A_\alpha$ be arbitrary then xRy since both x and y are elements of A_α and by def. of R

  so $y \in \bar{x}$

  $\therefore A_\alpha \subseteq \bar{x}$

Hence $\bar{x} = A_\alpha$

Hence the claim is true, therefore $A/R \subseteq \{A_\alpha\}$

2.b) Let $A_{\alpha_0} \in \{A_\alpha\}_{\alpha \in I}$ be arb. for some $\alpha_0 \in I$

Want: $A_{\alpha_0} \in A/R$

then let $x \in A_{\alpha_0}$ then like the above proof

$A_{\alpha_0} = \bar{x}$

So $A_{\alpha_0} = \bar{x} \in A/R$

$\therefore \{A_\alpha\}_{\alpha \in I} \subseteq A/R$

Q.E.D.

Order Relation

Defn: R be a rel on a set A, if R is reflexive, antisymmetric and trans. then R is said to be an order reln.

Recall: R is antisymm $\iff \forall x,y \in A \quad xRy \wedge yRx \Rightarrow x=y$

Ex: Let $A=\mathbb{R}$ $\quad xRy \iff x \leq y$ $\quad R$ is an order relation

Ex: Let $\mathcal{P}$ be a collection of sets

$A,B \in \mathcal{P} \qquad ARB \iff A \subseteq B$

refl: Let $A \in \mathcal{P}$ be arbitrary, then $A \subseteq A$ so ARA ✓

anti-symm: Let $A,B \in \mathcal{P}$ be arbitrary, assume $ARB \wedge BRA$

want: $A=B$

So $A \subseteq B \wedge B \subseteq A$

so $A=B$

transitivity: Let $A,B,C \in \mathcal{P}$ be arbt. Assume $ARB \wedge BRC$

want: ARC

So $A \subseteq B \wedge B \subseteq C$

So $\forall \alpha \in A \quad \alpha \in B \quad \forall \beta \in B \quad \beta \in C$

So $\forall \alpha \in A \quad \alpha \in C$

So $A \subseteq C$

So ARC

Defn: Let A be a set and "$\leq$" be an ordered rel on A.
Then $(A, \leq)$ is said to be an ordered set.

Defn: Let $(A, \leq)$ be an ordered set. Let $a, b \in A$ a, b are
comparable if $a \leq b$ or $b \leq a$

Defn: Let $(A, \leq)$ be an ordered set. "$\leq$" is said to be
a total order reln. if $\forall a, b \in A$ $a \leq b$ or $b \leq a$

i.e. "$\leq$" is a total order reln. iff any two elm. of A are comparable.

$(\mathbb{Z}, \leq)$ → total order $\quad$ $(2^A, \subseteq)$ ⟶ not a total order.

⊛ Upper bound of a set

Let A be a set and "$\leq$" some order reln. on A
Let $B \subseteq A$ a subset of A $(B \neq \emptyset)$

Defn: We say B is bounded above if $\exists a \in A$
s.t. $\forall x \in B$ $x \leq a$. In this case a is an upper bound for B.

Let $A = \mathbb{R}$ $B = \mathbb{N}$ → B is not bounded above
i.e. $\forall a \in \mathbb{R}$ $\exists n \in \mathbb{N}$ $n \leq a \leq n+1$

Defn: Let $(A, \leq)$ be an ordered set $B \neq \emptyset$ $B \subseteq A$ a subset of A.

We say that $a \in A$ is the (lowest upper bound of B if we have:

i) $\forall x \in B \quad x \leq a$

ii) If $a' \in A$ satisfies $x \leq a'$ for any $x \in B$ then $a \leq a'$.

Ex: $A = \mathbb{R}$ $B = \left\{ \frac{n-1}{n} \mid n = 1, 2, 3 \dots \right\}$

$\sup(B)$

$\text{lub}(B) = 1$

i) Show $\forall n \quad \frac{n-1}{n} \leq 1 \rightarrow$ trivial

ii) Assume for a contradiction $\left(\exists a' \in \mathbb{R} \quad \forall b \in B \quad b \leq a'\right) \wedge \left(a' < 1\right)$

Claim: $\exists n_0 \in \mathbb{N}^+ \ni a' < \frac{N_0 - 1}{N_0} \leq 1$

Take $N_0 = \left\lceil \frac{1}{1-a'} \right\rceil + 1$

So $\frac{1}{N_0} < 1 - a'$

So $a' < \frac{N_0 - 1}{N_0}$

So a' is not an upperbound

$a' < 1 - \frac{1}{N_0}$ $\quad a' - 1 < -\frac{1}{N_0}$ $\quad 1 - a' > \frac{1}{N_0}$ $\quad N_0 > \left\lceil \frac{1}{1-a} \right\rceil + 1$

⊛ Lower Bound of a set

Let $(A, \leq)$ be an ordered set. Let $B \neq \emptyset$ subset A

We say $a \in A$ is a lower bound for B if $\forall x \in B \quad a \leq x$

If there exists a lower bound for the set B we call B is bdd below.

Ex: $A = \{a, b, c, d\}$

$\leq = \{(a,a), (b,b), (c,c), (d,d), (a,c), (a,d), (b,c), (b,d)\}$

Let $B = \{c, d\}$ Is B bdd. below? Yes a is a lower bd. for B

b " " " " " "

Completeness Axiom of $\mathbb{R}$

Every non-empty subset of $\mathbb{R}$ that is bdd. above (below)

has a supremum (infimum)

Prop: Let $(A, \leq)$ be an ordered set and let $B \subseteq A$

if a and b are glb for B then $b = a$

Proof: Assume a, b glb for B

So $b \leq a \wedge a \leq b$ since ....

So $a = b$ since $\leq$ is anti-symmetric.

Mapping (Functions)

Let A and B be two sets and R be a relation from A into B.

Defn: A relation R from A into B is said to be a mapping

if $\forall x \in A$ there exists exactly one $y \in B$ satisfying

xRy.

(i.e. $\forall x_1, x_2 \in A$ If $x_1 = x_2$ then $f(x_1) = f(x_2)$)

$xRy \doteq R(x) = y$

Defn: The domain of a relation $R^{A\to B}$ $dom(R)$ or $D(R)$ is the set of all $x \in A$ such that $\exists y \in B$ satisfying xRy.

$$D(R) = \{x \mid \exists y \in B \; xRy\}$$

Defn: The image or range of a relation R from A to B, $Img(R)$ is the set of all $y \in B$ such that $\exists x \in A$ satisfying xRy.

Defn: mapping ✓

Notation: If R is a mapping from A into B then for $(x,y) \in R$ or xRy we write $y = R(x)$

$$R: A \to B, \quad x \mapsto R(x)$$

⊛ Composition of two Mappings

Let A, B, C be 3 sets, $f: A \to B$ $g: B \to C$ be two mappings. We define a new mapping denoted gof

$$(gof)(x) = g(f(x)) \qquad gof: A \to C, \quad x \longrightarrow g(f(x))$$

⊛ One-to-one (injective) mappings

A mapping $f: A \to B$ is said to be one-to-one (injective) if

$\forall x_1, x_2 \in A \quad x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$

$f(x_1) = f(x_2) \Rightarrow x_1 = x_2$

Warning: $\forall x_1, x_2 \in A \quad x_1 = x_2 \Longrightarrow f(x_1) = f(x_2)$

This is NOT 1-1 ness

Prop: Let A, B, C be 3 sets with $f: A \to B$ $g: B \to C$ be both 1-1 mappings. Then $g \circ f$ is also 1-1.

Proof: $g \circ f : A \to C$

Want: $g \circ f(x_1) \neq g \circ f(x_2)$

Or (Assume $x_1, x_2 \in A \wedge x_1 \neq x_2$

Want: $x_1 = x_2$

Assume $g \circ f(x_1) = g \circ f(x_2)$

So $g(f(x_1)) = g(f(x_2))$

So $f(x_1) = f(x_2)$ since g is 1-1

So $x_1 = x_2$ since f is 1-1

⊛ Onto (Surjection) Mapping

A mapping $f: A \to B$ is said to be onto (surjective) if for any $y \in B$ there exists at least one $x \in A$ st $f(x) = y$

Ex: $f: \mathbb{R} \to \mathbb{R}$

$x \longrightarrow \sin(x)$

Prove or disprove f is onto:

Ans: I choose to disprove

Consider $y = 2$

$\forall x \in \mathbb{R} \quad f(x) \neq 2$

Prop: Let A, B, C be 3 sets $f: A \to B$ $g: B \to C$ be onto mappings. Then $g \circ f: A \to C$ is onto.

Proof: Let $y \in C$ be arbitrary. Want: $\exists x \in A$ $g \circ f(x) = y$

So $\exists w \in B$ $g(w) = y$ since g is onto.

So $\exists x \in A$ $f(x) = w$ since f is onto.

So $g \circ f(x) = y$.

(*) Bijective Mapping (Bijection)

Def: Let A and B be two sets $f: A \to B$ a mapping is said to be a bijective mapping (iff) f is both 1-1 and onto.

Notation: Let X and Y be two sets and $f: X \to Y$ be a mapping. For any subset A of X we write $f(A) = \{y \in Y \mid \exists x \in A \ f(x) = y\}$ (the image of the set A)

Defn: For any subset B of Y we define preimage of the set B $\overleftarrow{f}(B) = \{x \in X \mid \exists y \in B \ f(x) = y\} = \{x \in X \mid f(x) \in B\}$

Recall: For $A \subseteq X$

$$y \in f(A) \iff \exists x \in A \text{ s.t. } y = f(x)$$
$$\iff y = f(x) \text{ for some } x \in A$$

Prop: Let $f: X \to Y$ be a mapping and $A_1 \subseteq X$ $A_2 \subseteq X$ then

1) $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$
2) $A_1 \subseteq A_2 \Rightarrow f(A_1) \subseteq f(A_2)$
3) $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$

Proof:

(1) we will prove $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$

Let $y \in f(A_1 \cup A_2)$ be arbitrary want: $y \in f(A_1) \cup f(A_2)$

So $\exists a \in A_1 \cup A_2$ s.t. $f(a) = y$

So $a \in A_1$ or $a \in A_2$

So $f(a) \in f(A_1)$ or $f(a) \in f(A_2)$

So $f(a) \in f(A_1) \cup f(A_2)$

So $y \in f(A_1) \cup f(A_2)$

Let $y \in f(A_1) \cup f(A_2)$ want: $y \in f(A_1 \cup A_2)$

So $y \in f(A_1)$ or $y \in f(A_2)$

So $\exists x_1 \in A_1$ s.t $f(x_1) = y$

OR $\exists x_2 \in A_2$ s.t. $f(x_2) = y$

So $\exists x \in (A_1 \cup A_2)$ s.t $f(x) = y$ since $x_1 \in A_1 \Rightarrow x_1 \in A_1 \cup A_2$, $x_2 \in A_2 \Rightarrow x_2 \in A_1 \cup A_2$

So $y = f(x) \in f(A_1 \cup A_2)$

(2) We will prove $A_1 \subseteq A_2 \Rightarrow f(A_1) \subseteq f(A_2)$

Assume $A_1 \subseteq A_2$ Want: $f(A_1) \subseteq f(A_2)$

Let $y \in f(A_1)$ be arbitrary then $\exists x \in A_1$ s.t. $f(x) = y$

So $x \in A_2$ since $A_1 \subseteq A_2$

So $y = f(x) \in f(A_2)$

So $f(A_1) \subseteq f(A_2)$

Q E. D.

(3) Let $y \in f(A_1 \cap A_2)$ Want: $y \in f(A_1) \cap f(A_2)$

:

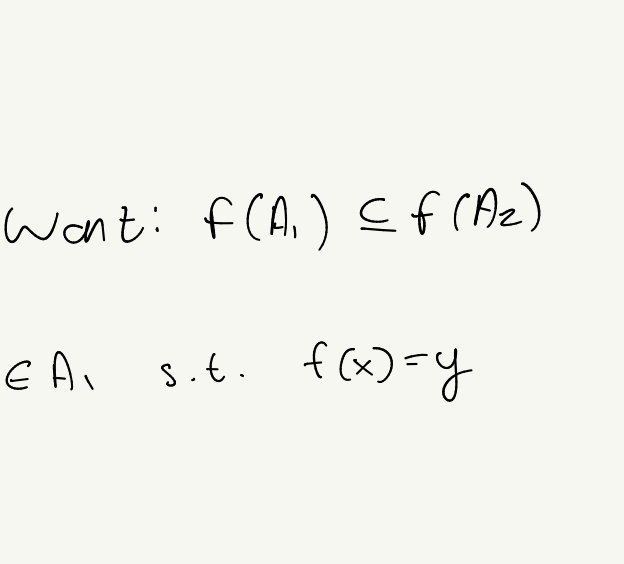
exercise

(*) Prove or **disprove** $f(A_1) \cap f(A_2) \subseteq f(A_1 \cap A_2)$

$A_1 = \{1,2\}$ $f(1) = \Delta$

$f(3) = \Delta$

$A_2 = \{2,3\}$ $f(2) = \square$



$f(A_1) = \{\Delta, \square\}$ $f(A_2) = \{\Delta, \square\}$

$f(A_1 \cap A_2) = \{\square\}$

$\{\Delta, \square\} \not\subseteq \{\square\}$

Prop: Let $f: X \to Y$ be a mapping.

Then f is injective iff $\forall A_1, A_2 \subseteq X \quad f(A_1 \cap A_2) = f(A_1) \cap f(A_2)$

Proof: ($\Rightarrow$) Assume f is 1-1 Want: $f(A_1 \cap A_2) = f(A_1) \cap f(A_2)$

From previous prop. $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$ ✓

Let $y \in f(A_1) \cap f(A_2)$ then $y \in f(A_1) \wedge y \in f(A_2)$

So $\exists x_1 \in A_1$ s.t. $y = f(x_1)$ and $\exists x_2 \in A_2$ s.t. $y = f(x_2)$

So $y = f(x_1) = f(x_2)$

So $x_1 = x_2$ since f is 1-1

Hence $x = x_1 = x_2 \in A_1 \cap A_2$ So $y = f(x) \in f(A_1 \cap A_2)$

$\therefore f(A_1) \cap f(A_2) \subseteq f(A_1 \cap A_2)$ ✓

($\Leftarrow$) Assume $f(A_1 \cap A_2) = f(A_1) \cap f(A_2)$ (△) Want: f is 1-1

Let $x_1, x_2 \in X$ and $x_1 \neq x_2$ we'll show $f(x_1) \neq f(x_2)$

Choose $A_1 = \{x_1\}$ $A_2 = \{x_2\}$

$f(A_1 \cap A_2) = f(\emptyset) = \emptyset$

$f(A_1) \cap f(A_2) = \emptyset$ by △

So $f(x_1) \neq f(x_2)$

So f is 1-1

Prop: Let X, Y be two sets and $f: X \to Y$ a mapping

then for $B_1 \subseteq Y$ and $B_2 \subseteq Y$ we have

1) $f^{\leftarrow}(B_1 \cup B_2) = f^{\leftarrow}(B_1) \cup f^{\leftarrow}(B_2)$

2) $B_1 \subseteq B_2 \Rightarrow f^{\leftarrow}(B_1) \subseteq f^{\leftarrow}(B_2)$

3) $f^{\leftarrow}(B_1 \cap B_2) = f^{\leftarrow}(B_1) \cap f^{\leftarrow}(B_2)$

Proof (2): Assume $B_1 \subseteq B_2$ Want: $f^{\leftarrow}(B_1) \subseteq f^{\leftarrow}(B_2)$

Let $x \in f^{\leftarrow}(B_1)$ be arbitrary

So $f(x) \in B_1$

So $f(x) \in B_2$ since $B_1 \subseteq B_2$

So $x \in f^{\leftarrow}(B_2)$

Proof (3):

$(\subseteq)$ $f^{\leftarrow}(B_1 \cap B_2) \subseteq f^{\leftarrow}(B_1)$ since $B_1 \cap B_2 \subseteq B_1$ and (2)

$f^{\leftarrow}(B_1 \cap B_2) \subseteq f^{\leftarrow}(B_2)$ since " $\subseteq B_2$ " "

Hence $\underset{*_1}{f^{\leftarrow}(B_1 \cap B_2)} \subseteq \underset{*_2}{f^{\leftarrow}(B_1) \cap f^{\leftarrow}(B_2)}$

$(\supseteq)$ Let $x \in f^{\leftarrow}(B_1) \cap f^{\leftarrow}(B_2)$

So $x \in f^{\leftarrow}(B_1) \wedge x \in f^{\leftarrow}(B_2)$

So $f(x) \in B_1 \wedge f(x) \in B_2$

So $f(x) \in (B_1 \cap B_2)$

So $x \in f^{\leftarrow}(B_1 \cap B_2)$

$\therefore *_2 \subseteq *_1$

Prop: let $f: X \to Y$ be a mapping, Then f is surjective (onto) iff $\forall B \subseteq Y$ $f(f^{\leftarrow}(B)) = B$

$(\Rightarrow)$ Proof by contradiction:

f is surj $\wedge$ $\exists B \subseteq Y$ $f(f^{\leftarrow}(B)) \neq B$

case 1: $\exists a \in f(f^{\leftarrow}(B)) \wedge a \notin B$ Not possible

case 2: $\exists a \in B \wedge a \notin f(f^{\leftarrow}(B))$ Δ_3

for this a there must be some x st $f(x) = a$

since f is surjective.

but $x \in f^{\leftarrow}(B)$ which means $a \in f(f^{\leftarrow}(B))$ contradicts with Δ_3

Alternative Proof for ($\Rightarrow$)

Assume f is surj want: Δ_1

Let $B \subseteq Y$ be arbitrary

Let $y \in f(f^{\leftarrow}(B))$, then $\exists x\, f^{\leftarrow}(B)$ $f(x) = y$

We know that $f(x) \in B$ since $x \in f^{\leftarrow}(B)$

So $y = f(x) \in B$ $\therefore f(f^{\leftarrow}(B)) \subseteq B$

Let $y \in B$

Since f is surj. $\exists x \in X$ $f(x) = y \in B$

So $x \in f^{\leftarrow}(B)$ so $y = f(x) \in f(f^{\leftarrow}(B))$

$\therefore B \subseteq f(f^{\leftarrow}(B))$

($\Leftarrow$) Proof by contradiction

Assume $(\Delta_1) \wedge f$ is not surjective $\star_7$

Δ_1 must also hold for $B = Y$

$f(f^{\leftarrow}(Y)) = Y$

Due to $\star_7$ $\exists y_0 \in Y$ $\forall x \in X$ $f(x) \neq y_0$

So $y_0 \notin f(f^{\leftarrow}(Y))$ but $f(f^{\leftarrow}(Y)) = Y$ $\lightning$

Invertible Mapping

Let X, Y be two sets, $f: X \to Y$ a mapping

Defn: We say that a mapping $f: X \to Y$ is invertible if

$\exists g$ a mapping $g: Y \to X$ s.t.

i) $\forall x \in X \quad g \circ f(x) = x$

ii) $\forall y \in Y \quad f \circ g(y) = y$

Then such a mapping g is called the inverse of f, and we write $g = f^{-1}$

Defn: Let $f: A \to B$ $g: A \to B$ two mappings

Then $f = g$ iff $\forall x \in A \quad f(x) = g(x)$

silebilirsiniz bunu gerek bile yok dedi sidi

Lemma: Let A, B, C, D be sets $f: A \to B$ $g: B \to C$ $h: C \to D$

Then $(h \circ g) \circ f = h \circ (g \circ f)$

Thm: If $f: X \to Y$ is invertible, then its inverse is unique.

Proof. Assume g and h are both inverse of f.

$g: Y \to X$

$h: Y \to X$

$\wedge \quad g \circ f(x) = x = h \circ f(x) \quad \forall x \in X$

$f \circ g(y) = y = f \circ h(y) \quad \forall y \in Y$

$\forall y \in Y \quad f \circ g(y) = f \circ h(y)$ so $f \circ g = f \circ h$

Then $g \circ (f \circ g) = g \circ (f \circ h)$ ↘ associativity

Then $(g \circ f) \circ g = (g \circ f) \circ h$

So $\forall y \in Y \quad g(y) = h(y)$ since $(g \circ f)(x) = x$

Finite Sets and Combinatorics.

Defn: Two sets A and B are said to be equinumerous if there exists a bijection $f: A \to B$. We write $A \approx B$

Defn: A set A is said to be finite if it contains finitely many elements. i.e. A is finite if $A = \emptyset$ or if there exists a natural number $n \neq 0$ s.t. $A \approx \mathbb{N}_n$ where $\mathbb{N}_n = \{1, 2, 3 \dots n\}$

If $A \approx \mathbb{N}_n$ we write $\text{card}(A) = n$

Theorem: Suppose A, B, C are sets, then

i) $A \approx A$

ii) $A \approx B \Rightarrow B \approx A$

iii) $A \approx B \wedge B \approx C \Rightarrow A \approx C$

Proof: exercise

Thm: Suppose A, B, A', B' are sets $A \cap B = \emptyset = A' \cap B'$

if $\underbrace{A \approx A' \wedge B \approx B'}_{\Delta}$ then $\underbrace{A \cup B \approx A' \cup B'}_{\star}$

Proof: Assume Δ Want: $\star$

exercise.

Corollary: If A and B are disjoint finite sets then $card(A \cup B) = card(A) + card(B)$

Proof: exercise

Prop: Let A be non-empty finite set

If $x \in A$ then $A \setminus \{x\}$ is finite and $card(A \setminus \{x\}) = card(A) - 1$

Proof: consider sets with 1 element so $card(A) = 1$

$A \setminus \{x\} = \emptyset$ ✓

consider sets with more elements $card(A) > 1$

Let $x \in A$ be arbitrary and $f(x) = i \in \mathbb{N}_n$

Define $g: A \setminus \{x\} \to \mathbb{N}_{n-1}$

$$g(a) = \begin{cases} f(a) & \text{if } f(a) < i \\ f(a)-1 & \text{if } f(a) > i \end{cases}$$

Thus g is $\underbrace{1\text{-}1 \text{ and onto func.}}_{\text{exercise}}$ between $A \setminus \{x\}$ and $\mathbb{N}_{n-1}$

Theorem: If A is finite set and $B \subseteq A$ then B is finite.

exercise

Prop: If A, B are finite sets $\wedge$ $A \cap B \neq \emptyset$ then $\text{card}(A \cup B) = \text{card}(A) + \text{card}(B) - \text{card}(A \cap B)$

Proof: We know that $A \cup B = A \cup (B \setminus A)$ and $A \cap (B \setminus A) = \emptyset$

$B \setminus A \subseteq \underbrace{B}_{\text{finite}}$ So $B \setminus A$ is finite

So $A \cup B$ is finite

$\text{Card}(A \cup B) = \text{card}(A) + \underbrace{\text{card}(B \setminus A)}_{\textcircled{A}}$

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

$(A \cap B) \cap (B \setminus A) = \emptyset$

$\text{card}(A \cap B) = \text{card}(B \setminus A)$

$+ \text{card}(B)$

$= \text{card}(A) + \text{card}(B) - \text{card}(A \cap B)$

$\underbrace{A \cup B}_{\text{finite finite}}$

finite if $A \cap B \neq 0$

and $\text{card}(A \cup B) = \text{card}(A) + \text{card}(B)$

Prop: If A and B are finite sets then $A \times B$ is also finite and $\text{card}(A \times B) = \text{card}(A) \cdot \text{card}(B)$

Proof: i) If $B = \emptyset$ $\text{card}(B) = 0$ $A \times B = \emptyset$ ✓

ii) If $B \neq \emptyset \neq A$

Assume $\text{card}(B) = m$ $\text{card}(A) = n$

So $A = \{a_1, a_2, \ldots, a_n\}$

So $A \times B = \{a_1\} \times B \cup \{a_2\} \times B \cup \cdots \{a_n\} \times B$

$= \bigcup_{a \in A} \{a\} \times B$ ⊛

Note that $\{a_i\} \times B \cap \{a_j\} \times B = \emptyset$ if $i \neq j$

First we need to prove $\{a_i\} \times B$ is finite for all $a_i \in A$

$\exists f$ bij between B and $\mathbb{N}_m$

Now define $g: \{a\} \times B \to B$

$(a, b) \to b$

claim: g is bij

$\therefore \{a\} \times B \simeq B$

and we know $B \simeq \mathbb{N}_m$ so $\{a\} \times B \simeq \mathbb{N}_m$

$\therefore$ $card(\{a\} \times B) = m \quad \forall a \in A$

from $\circledast$ $card(A \times B) = \sum_{k=1}^{n} card(\{a_k\} \times B)$

$= \sum_{k=1}^{n} card(B) = n \cdot m = card(A) \cdot card(B)$

Prop: If $card(X) = n$ then $card(P(X)) = 2^n$

Proof: By MI

Induction Basis:

If $n = 0$ $X = \emptyset$ $P(X) = \{\emptyset\}$ $card(P(X)) = 2^0 = 1$ ✓

Induction Step:

Assume P_{n_0} is true Want P_{n_0+1} is true

So if $card(X) = n$ then $card(P(X)) = 2^n$

Lets consider arbitrary X with n_0+1 elements

$X = \{a_1, a_2 \cdots a_{n_0}, a_{n_0+1}\}$

Now consider $X' = \{a_1, \cdots a_{n_0}\}$ with n_0 elements

by induction hypothesis we know $card(P(X')) = 2^{n_0}$

$P(X') = \{A_1, A_2 \cdots A_{2^{n_0}}\}$

What are the subsets of X?

only these
- any subsets of X' is also subset of X
- the sets $A_1 \cup \{a_{n_0+1}\}$, $A_2 \cup (a_{n_0+1}) \cdots$, $A_{2^{n_0}} \cup (a_{n_0+1})$
- are also subsets of X

Hence $\{a_1, \ldots - a_{n_0+1}\}$ has $2^{n_0} + 2^{n_0}$ subsets ✓

$\therefore P_{n+1}$ is true

Hence we conclude P_n is true $\forall n \geq 0$ by MI

Theorem: Let X, Y be finite sets and $f: X \to Y$ a mapping then

i) If f is 1-1 then $\text{card}(X) \leq \text{card}(Y)$

ii) If f is onto then $\text{card}(X) \geq \text{card}(Y)$

iii) If f is bij then $\text{card}(X) = \text{card}(Y)$

Proof: execise

Question: How many 1-1 mappings are there from X into Y ?

$X = \{a_1, \ldots a_k\}$ @MI execise

$Y = \{b_1 \ldots \ldots b_n\}$

on

Theorem: from the set $X = \{a_1 \cdots a_k\}$ into set $Y = \{b_1 - - - b_n\}$

$k \leq n$ there exists $\frac{n!}{(n-k)!}$ 1-1 mappings.

Question: Let X, Y be finite sets if $\text{card}(X) = \text{card}(Y)$ then how many bijections are there from X into Y

Ans: $n!$ exercise.

Let $X = \{a_1, a_2, a_3 \dots a_n\}$ be a finite set with $\text{card}(X) = n$

For $1 \leq p \leq n$ define $A_p = \{A \subseteq X \mid \text{card}(A) = p\}$

$A_1 = \{\{a_1\}, \{a_2\} \dots \{a_n\}\}$

$A_2 = \{\{a_1, a_2\}, \{a_1, a_3\} \dots \{a_1, a_n\},$

$\{a_2, a_3\} \dots \{a_2, a_n\},$

$\vdots$

$\{a_{n-1}, a_n\}\}$

<u>Theorem:</u> Let X be finite $\text{card}(X) = n$ $\quad 1 \leq p \leq n$

$$\text{card}(A_p) = \frac{n!}{p!(n-p)!}$$

Proof:

Hint: There is a connection with 1-1 mappings from $\{a_1, a_2 \dots a_p\}$ into $\{a_1, a_2 \dots a_n\}$

Infinite Sets and Cardinals

Defn: A set B which is not finite is said to be infinite.

i.e. $\forall n \in \mathbb{N}$ $\nexists$ f bij $f : \mathbb{N}_n \to B$

How can we compare card. of these infinite sets?

$\mathbb{N} = \{0, 1, 2, \dots\}$

$\mathbb{N}^+ = \{1, 2, 3 \dots\}$

$\mathbb{N}^+ \subset \mathbb{N}$ But $\exists f$ bij $f : \mathbb{N} \to \mathbb{N}^+$, $n \to n+1$

1-1) Assume $f(n_0)=f(n_1)$ so $n_0+1=n_1+1$

so $n_0=n_1$

onto) Let $n \in \mathbb{N}^+$ consider $n-1 \in \mathbb{N}$? ✓

then $f(n-1)=n$

Defn: Let X, Y be two sets

a) If there is a bij $f: X \to Y$ then we write $card(X) = card(Y)$

b) If " exists No bij but there exists a 1-1 mapping $f: X \to Y$

then we write $card(X) < card(Y)$

c) If there exists No bij but there exists an onto mapping $f: X \to Y$

then we write $card(X) > card(Y)$

Theorem: (Cantor - Bernstein): Let X, Y be two sets. if there exists a 1-1 mapping $f: X \to Y$ and a 1-1 mapping $g: X \to Y$ then there exists a bijection $h: X \to Y$

i.e., The theorem states that $card(X) \leq card(Y)$ and $card(Y) \leq card(X)$ then $card(X) = card(Y)$.

Theorem: (Cantor) For any set $A \neq \emptyset$ $\text{card}(A) < \text{card}(P(A))$

Proof: We will show that there exists a 1-1 mapping $f: A \to P(A)$

But there exists NO bij $\varphi: A \to P(A)$

1-1 mapping: Let $f: A \to PA$
$x \mapsto \{x\}$ then f is 1-1

since $x \neq y \Rightarrow f(x) = \{x\} \neq \{y\} = f(y)$

No bij

case 1: A is finite:

$\text{card}(A) = n$ $\text{card}(P(A)) = 2^n$ so $2^n \neq n$ hence $\nexists$ bij.

case 2: A is infinite:

Assume for a contradiction $\exists\, \varphi$ bij $\varphi: A \to \mathcal{P}(A)$

$\forall x \in A$ $\varphi(x) \in P(A)$ so $\varphi(x) \subseteq A$

Trick

Let $B = \{x \in A \mid x \notin \varphi(x)\}$

since φ is onto $\exists\, x_0 \in A$ s.t. $\varphi(x_0) = B$

case $x_0 \in B$

so $x_0 \notin \varphi(x_0)$

$x_0 \notin B$

case $x_0 \notin B$

so $x_0 \in \varphi(x_0)$

$x_0 \in B$

Remark: $\text{card}(\mathbb{N}) < \text{card}(P(\mathbb{N})) < \text{card}(P(P(\mathbb{N})))$

⊛ Continium Hypothesis

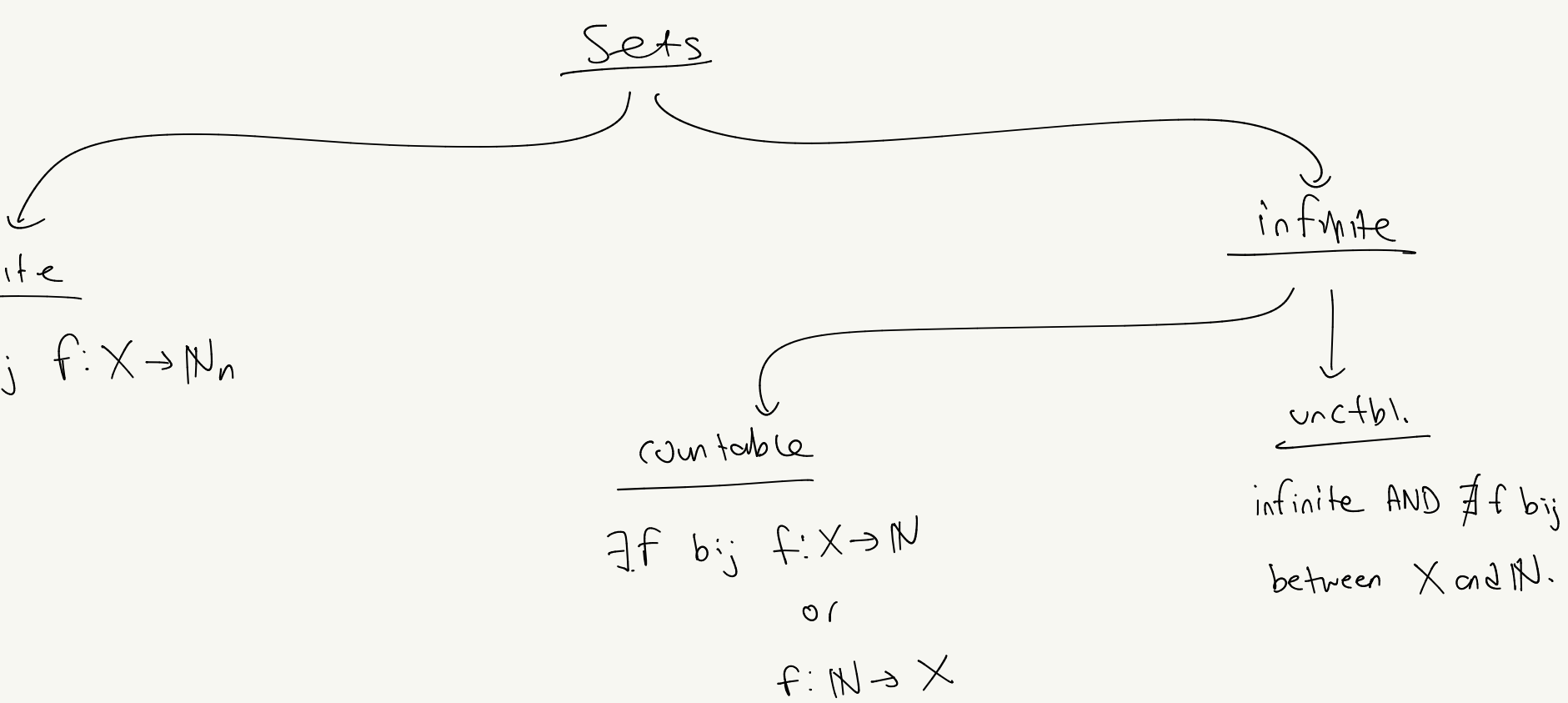
There is no set X. s.t. $\text{card}(\mathbb{N}) < \text{card}(X) < \text{card}(2^{\mathbb{N}})$

Countable and Unctb. Sets

Defn: An infinite set X is said to be countable infinite (denumerable) if there exists a bij from $\mathbb{N}$ into X.

- A set is countable if it is finite or denumerable.

Defn: An infinite set which is Not ctbl. is said to be uncountable.



$\mathbb{N} \times \mathbb{N}$ ctbl?

$\mathbb{Q}$ ctbl?

any subset of $\mathbb{N}$ ctbl?

$\mathbb{R}$ ctbl?

Show that $card(\mathbb{E}) = card(\mathbb{N})$

↳ even natural nums

Proof: consider $f: \mathbb{N} \to \mathbb{E}$

$n \mapsto 2n$

claim: f is a bij

1-1: Let $x, y \in \mathbb{N}$ be arbitrary $x \neq y$ Want. $f(x) \neq f(y)$

$f(x) = 2x \neq 2y = f(y)$ ✓

onto: Let $e \in \mathbb{E}$ arbitrary so e is even Want. find $k \in \mathbb{N}$ $f(k) = e$

so $e = 2k$ for some $k \in \mathbb{N}$.

so $f(k) = e$

Let $H = \{1, 2, 4, 8, 16 \ldots\}$ so H is denumerable

consider $f: \mathbb{N} \to H$

$n \mapsto 2^n$

Prop: $\mathbb{N} \times \mathbb{N}$ is denumerable.

Proof: We will find 1-1 mapping from $\mathbb{N}$ into $\mathbb{N} \times \mathbb{N}$.

and from $\mathbb{N} \times \mathbb{N}$ into $\mathbb{N}$.

(Cantor-Bernstein Theorem)

Let $f: \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ 1-1: let $f(n_1) = f(n_2)$ want: $n_1 = n_2$

$n \mapsto (n, 0)$ so $(n_1, 0) = (n_2, 0)$

so $n_1 = n_2$

Let $g: \mathbb{N}\times\mathbb{N} \to \mathbb{N}$

$(n,m) \to 2^n 3^m$

1-1 : suppose $g(n,m) = g(r,s)$ want: $n=r \wedge m=s$

so $2^n 3^m = 2^r 3^s$

Assume for a contr. $r<n$ then $n-r \geq 1$

so $\underbrace{2^{n-r}}_{\text{even}}\, 3^m = \underbrace{3^s}_{\text{odd}}$ ↯ $r \not< n$

Assume for a contr. $r>n$ then $r-n \geq 1$

so $\underbrace{3^m}_{\text{odd}} = \underbrace{2^{r-n}\, 3^s}_{\text{even}}$ ↯ $r \not> n$

$\therefore r=n.$

Hence $2^n 3^m = 2^r 3^s$

↓

simplifies to

$3^m = 3^s$

If $m>s$ $3^{m-s}=1$ not poss.

If $m<s$ $3^{s-m}=1$ " "

$\therefore m=s$

Hence $(n,m)=(r,s)$

$\therefore g$ is 1-1

Hence $\mathbb{N}\times\mathbb{N} \simeq \mathbb{N}$ $\exists$ bij by Cantor-Bernstein

---

Prop: An infinite set X is denum. iff we can write X as $= \{a_0, a_1, \dots\}$

$= \{a_n \mid n \in \mathbb{N}\}$

Prop: Any infinite subset of $\mathbb{N}$ is denum.

Proof: Let $A \subseteq \mathbb{N}$ be infinite

Let's use cantor-bernstein. Then

Consider: $f: A \to \mathbb{N}$

$x \mapsto x$

f is 1-1

Consider $f': \mathbb{N} \to A$

$k \mapsto n_k$ where $n_0 = \min(A)$

$n_1 = \min(A \setminus \{n_0\})$

$n_2 = \min(A \setminus \{n_0, n_1\})$

$\vdots$

f' is 1-1

$$n_k = \min\left(A \setminus \bigcup_{i=0}^{k-1} \{v_i\}\right)$$

A is denumerable by Cantor-Bernstein

Remark: An infinite subset of a ctbl. set is also ctbl.

Prop: If A and B are two denum. sets then $A \cup B$ is also denum.

Proof: Assume A and B are two denum sets. Want: $A \cup B$ is denum.

So $A = \{a_0, a_1, \dots\}$

$B = \{b_0, b_1, \dots\}$

case-1) $A \cap B = \emptyset$

Define $\varphi : \mathbb{N} \to A \cup B$

$$n \mapsto \begin{cases} a_{n/2} & \text{if } n \text{ is even} \\ b_{\frac{n-1}{2}} & \text{if } n \text{ is odd} \end{cases}$$

$0 \to a_0$

$1 \to b_0$

$2 \to a_1$

$3 \to b_1$

$\vdots$

case-2) $A \cap B \neq \emptyset$

exercise

Remark: If $A_1, A_2, A_3 \dots A_n$ are denum. sets then $A_1 \cup A_2 \cup \dots A_n$ is denum.

Thm: Let $A_0, A_1, A_2 \dots A_n \dots$ $(n \in \mathbb{N})$ be countably many denum. sets.

If $A_i \cap A_j = \emptyset$ for $i \neq j$ then $A = \bigcup_{n \in \mathbb{N}} A_n$ is denum.

Proof:

Let $A_0, A_1, \ldots, A_n, \ldots$ be denum sets $\wedge$ $A_i \cap A_j = \emptyset$ for $i \neq j$

Want: A is denum.

$A_0 = \{a_0^0, a_1^0, a_2^0 \ldots\}$

$A_1 = \{a_0^1, a_1^1, a_2^1 \ldots\}$

$\vdots$

$A_n = \{a_0^n, a_1^n, a_2^n \ldots\}$

So $A = \bigcup_{n \in \mathbb{N}} A_n = \{a_n^m \mid n \in \mathbb{N} \; m \in \mathbb{N}\}$

Define $\varphi : \mathbb{N} \times \mathbb{N} \to A$

$(n, m) \mapsto a_m^n \in A$

claim: φ is bij

if we prove this we are done.

1-1 : Assume $\varphi(n,m) = \varphi(n',m')$

So $a_m^n = a_{m'}^{n'}$

So $a_m^n \in A_n$ $a_{m'}^{n'} \in A_{n'}$ we have $A_n \cap A_{n'} = \emptyset$ when $n \neq n'$

So $n = n'$

Then $a_m^n = a_{m'}^n$ In the same set A_n, these elements can be equal if $m = m'$

$\therefore f$ is 1-1

Onto: f is onto since all the elements of A are in the form a_m^n so (n, n) maps to arbitrary a_n^n

Remark: The theorem is also true if A_i's are not pairwise disjoint

OR if some of the A_i's are finite.

Thm: $\mathbb{Q}$ is denumerable (ctbl. infinite)

Proof: $\mathbb{Q} = \mathbb{Q}^+ \cup \mathbb{Q}^- \cup \{0\}$ and $\mathbb{Q}^+ \approx \mathbb{Q}^-$

$\checkmark$ 1-1 $\varphi: \mathbb{Q}^+ \to \mathbb{N}^+ \times \mathbb{N}^+$
$q \mapsto \varphi(q) = (a,b)$ where $q = \frac{a}{b}$, $b \neq 0$, $\gcd(a,b) = 1$

$\checkmark$ 1-1 $\psi: \mathbb{N}^+ \times \mathbb{N}^+ \to \mathbb{Q}^+$
$(a,b) \to \psi(a,b) = 2^a 3^b$

So we can only focus on $\mathbb{Q}^+$

$$\mathbb{Q}^+ = \left\{ \frac{p}{q} \mid p, q \in \mathbb{N} \quad q \neq 0 \right\}$$

Let $A_1 = \left\{ \frac{p}{1} \mid p \in \mathbb{N} \right\}$

$A_2 = \left\{ \frac{p}{2} \mid p \in \mathbb{N} \right\}$

$\vdots$

$\mathbb{Q}^+ = \bigcup_{n=1}^{\infty} A_n$ ctbl union of denum. sets are denum.

Is $\mathbb{R}$ ctbl.? NO.

Thm: The interval $A = (0,1)$ is unctbl.

Proof: Assume for a contradiction A is ctbl. infinite (denum)

So I can list the elements of A.

$x_0 = 0.a_0^0 a_1^0 a_2^0 \dots$
$x_1 = 0.a_0^1 a_1^1 a_2^1 \dots$
$\vdots$
$x_n = 0.a_0^n a_1^n a_2^n \dots \dots \dots a_n^n \dots$
$\vdots$

$b = 0.b_0 b_1 b_2 \dots b_n$

$$b_i = \begin{cases} 5 & \text{if } a_i^i \neq 5 \\ 6 & \text{otherwise} \end{cases}$$

$b \in (0,1)$
but
b is not here

$b \notin \{x_0, x_1, \dots\}$

Hence $(0,1)$ unctbl.

Prop: any $a, b \in \mathbb{R}$ with $a < b$ the interval (a, b) is unctbl.

Proof: $\varphi : (0,1) \to (a,b)$

$$t \mapsto (1-t)a + tb$$

claim: φ is a bijection (proof exercise)

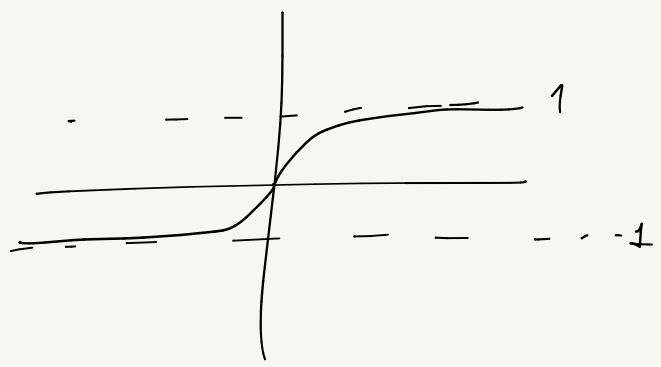
$$\text{card}(a,b) = \text{card}(0,1)$$

$\therefore (a,b)$ is unctbl.

Fact: The set $\mathbb{R}$ has the same card with the interval $(-1,1)$

$$\varphi : \mathbb{R} \to (-1,1)$$

$$x \mapsto \frac{x}{1+|x|}$$



Claim: φ is a bij

1-1: Assume $x, y \in \mathbb{R}$ $x \neq y$ be orbitrary. want: $\varphi(x) \neq \varphi(y)$

case 1: $x, y > 0$ $\quad \varphi(x) = \frac{x}{1+x}$ $\quad \varphi(y) = \frac{y}{1+y}$

Assume for a contradiction $\frac{x}{1+x} = \frac{y}{1+y}$

$$x + \cancel{xy} = y + \cancel{xy} \quad x = y$$

$\therefore \times$

So $\varphi(x) \neq \varphi(y)$

case2: $x, y < 0$, same case

case3: $x > 0$ $y < 0$ WLOG

$$\varphi(x) = \frac{x}{1+x} \qquad \varphi(y) = \frac{y}{1-y}$$

$\varphi(x) > 0$

$\varphi(y) < 0$

so $\varphi(x) \neq \varphi(y)$

claim: φ is onto

Let $y_0 \in (-1,1)$ be arbitrary

Now consider $x_0 = \frac{y_0}{1-|y_0|}$ claim: this x_0 is mapped to y_0

$\varphi(x_0) = y_0$ ✓

Fact: Let $S_{0,1}$ be the set of all ↓ infinite sequences consisting of zeros and 1s.

down

$S_{0,1}$ is unctbl.

Proof: We will prove it with direct proof by finding a bij btw $S_{0,1}$ and $\mathcal{P}(\mathbb{N})$

$$\varphi : S_{0,1} \to \mathcal{P}(\mathbb{N})$$

$$(a_i) \mapsto \mathcal{P}(a_i) = \bigcup_{a_i=1} \{i\}$$

when $a_i = 0$ or 1

claim: φ is bij

exercise

Proof: Assume for a contradiction $S_{0,1}$ is denum (ctbl. inf.)

$A = \{I_i\}$ where $I_i = (i, i+1]$ $\quad i \in \mathbb{N}$

$= \{I_0, I_1, I_2 \ldots\}$

Introduction to Algebra

Defn: Let X be any non-empty set. A binary operation on X means a mapping from $X \times X$ into X.

Notation: $f(x,y) \triangleq x * y$ or $x \triangle y$ or $x \triangleq y$

Binary operations on $\mathbb{N}$.

Ex: $n * m = n + m$ $\quad (n,m) \in \mathbb{N}\times\mathbb{N} \longmapsto n+m \in \mathbb{N}$

$n * m = n \cdot m$ $\quad (n,m) \in \mathbb{N}\times\mathbb{N} \mapsto n \cdot m \in \mathbb{N}$

Ex: Let Y be any set and $X = 2^Y$

$(A,B) \in X \times X \longmapsto A \cup B \in X$ is an operation on X

Defn: Let X be any set and $*$ be any operation on X. We say that

i) $*$ is commutative if $\forall x,y \in X \quad x * y = y * x$

ii) $*$ is associative if $\forall x,y,z \in X \quad x * (y * z) = (x * y) * z$

Ex: Let $X = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d \in \mathbb{R} \right\}$ (set of 2×2 matrices)

Then $+$ is commutative & associative.

$\cdot$ is not commutative & associative

Notation: A set X with "an operation $*$ defined on X" will be denoted by $(X, *)$

Defn: Let $(X, *)$ be a set with op., we say that $(X, *)$ has a neutral element (unit elem.) if there exists $e \in X$ s.t. $\forall x \in X \quad x * e = x = e * x$.

Ex: 1) $(\mathbb{N}, +)$ $e = 0$

2) $(\mathbb{N}, \cdot)$ $e = 1$

3) let $X = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d \in \mathbb{R} \right\}$

$(X, +)$ $e = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

$(X, \cdot)$ $e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Prop: Any set $(X, *)$ with an op. has at most one neutral elt.

Proof: Assume for a contradiction $(X, *)$ has more than one neutral elt.

WLOG lets consider two distinct neutral elts.

$e_1 \neq e_2$

So $e_1 * e_2 = e_1 = e_2 * e_1$ since e_2 is a neutral elt.

$e_2 * e_1 = e_2 = e_1 * e_2$ " e_1 " " " " .

So $e_2 * e_1 = e_2 \neq e_1 = e_2 * e_1$ ⚡

Hence $(X, *)$ has at most one neutral elt.

Defn: Let $(X, *)$ be a set with op. Assume that $(X, *)$ has a neutral elt. $e \in X$. We say that an elt. $a \in X$ is invertible if there exists some $b \in X$ satisfying $b * a = e = a * b$

In this case b is said to be the inverse of a and denoted by a^{-1} or $-a$.

Summary:

e neutral elt. $\triangleq$ (is defined) $\exists e \in X \quad \forall a \in X \quad a * e = a = e * a$

$a \in X$ is invertible if $\exists a' \in X$ s.t. $a * a' = e = a' * a$

Ex: 1) $(\mathbb{N}, +) \to e = 0$ only e is invertible (for $x \in \mathbb{N}^+ \quad -x \notin \mathbb{N}$)

2) $(\mathbb{Z}, +) \to e = 0$ $\forall x \in \mathbb{Z} \quad -x \in \mathbb{Z}$ so $-x$ is the inverse

3) $(\mathbb{Z}, \cdot) \to e = 1$ only 1 and -1 is invertible.

4) $X = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \right\}$

$(X, \cdot) \to e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ M is invertible iff $\det M \neq 0$ $\det M = (ad - bc)$

ex: $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ is not invertible

ex: $\underbrace{\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}}_{N}$ for some fixed $\theta \in \mathbb{R}$

$\det N = 1$ so N is invertible.

$$N^{-1} = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$$

$$N \cdot N^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = N^{-1} \cdot N$$

Prop: Let $(X, *)$ be a set with an assoc. op. Let e be the unit elt. If some $x \in X$ is invertible then the inverse of x is unique.

Proof: Assume for a contradiction .... $x \in X$ is invertible but it is not unique. So there are at least two different inverses of x. Let's call them $y \in X$ and $z \in X$ and $y \neq z$.

$$\begin{aligned} \text{So } y = y * e &= y * (x * z) \quad \text{by assoc.} \\ &= (y * x) * z \\ &= e * z \\ &= z \end{aligned}$$

$\lightning$

Hence the inverse of x is uniquely determined under these assumptions.

Ex: Let $\perp$ be an operation defined on $\mathbb{Q} \setminus \{-1\} = \mathbb{Q}^*$

$\forall a, b \in \mathbb{Q}^* \quad a \perp b = a + ab + b$

comm: Let $a, b \in \mathbb{Q}^*$ $\underbrace{a \perp b = a + ab + b = b + ba + a = b \perp a}$ since $+$ and $\cdot$ commutative on $\mathbb{Q}$

$\therefore \perp$ is comm on $\mathbb{Q}^*$

assoc: exercise.

unit elt: Is there a unit elt. for $\mathbb{Q}^*$?

We need to find e that is satisfying $a \perp e = a = e \perp a$

$$a \perp e = a + ae + e = a$$

$$\text{so } ae + e = 0$$

$$\text{so } e(a+1) = 0$$

$$e = 0 \quad \text{since } a \neq -1$$

Is every elt. of $\mathbb{Q}^*$ invertible?

Let $a \in \mathbb{Q}^* = \mathbb{Q} \setminus \{-1\}$ find $a' \in \mathbb{Q}^*$ s.t. $a \perp a' = 0 = a' \perp a$

We need to find a' s.t. $a + aa' + a' = 0$

$$a'(a+1) = -a$$

$$a' = \frac{-a}{a+1} \quad \text{since } a \neq -1$$

$$\text{so } a' = \mathbb{Q}^*$$

$\therefore a' = \frac{-a}{a+1}$ is the inverse of a under $(\mathbb{Q}^*, \perp)$

Prop: Let $(X, \star)$ be a set with an assoc. op. $\star$

If $x, y \in X$ are two invertible elts in X then $x \star y$

is also invertible and $(x \star y)^{-1} = y^{-1} \star x^{-1}$

Proof: Let e be the neutral elt. $(X, \star)$

We need to show $\underbrace{(x \star y) \star (y^{-1} \star x^{-1})}_{\triangle} = e = (y^{-1} \star x^{-1}) \star (x \star y)$

$$\triangle = ((x \star y) \star y^{-1}) \star x = (x \star \underbrace{(y \star y^{-1})}_{e}) \star x^{-1}$$

$= x * x^{-1} = e$

similarly $(y^{-1} * x^{-1}) * (x * y) = e$

⊛ Axiom of Choice

Let $\{X_i \mid i \in I\}$ be a family of non-empty sets indexed by the index set I, then there exists a function

$$F: I \to \bigcup_{i \in I} X_i \quad \text{s.t. for each } i \in I \quad F(i) \in X_i$$

F is called the choice func.

$F(I) = \{x \mid F(i) = x \in X_i \ \ i \in I\}$

Claim: If $\{X_i \mid i \in I\}$ is a collection of pairwise disjoint sets i.e. $\forall i,j \in I \quad i \neq j \Rightarrow X_i \cap X_j = \emptyset$

then $i \neq j \Rightarrow F(i) \neq F(j)$ so a choice func. F is one-to-one.

Claim: The axiom of choice says there is a set formed by choosing one element out of each set X_i in our collection of sets.

⊛ Equivalence Relation and Operations

Let $(X, *)$ be a set with op. and R be an equivalence relation on X.

Defn: We say that R is compatible with $*$ if we have

$$\forall x,y,z \in X \qquad xRy \Rightarrow x*zRy*z \quad \text{and} \quad z*xRz*x$$

Ex/ Let $X = \mathbb{R}$ $\quad * : +$ $\quad xRy \iff x-y \in \mathbb{Z}$

So R is an equiv reln. on $\mathbb{R}$.

Is R compatible with R?

Assume $x,y,z \in R \wedge xRy$

want: $(x+z)R(y+z) \wedge (z+x)R(z+y)$

So $x-y \in \mathbb{Z}$

So $(x+z)-(y+z) \in \mathbb{Z}$

So $(x+z)R(y+z)$

enough since $+$ is commutative.

$\therefore$ R is comp. with $+$

Ex: Let $X = \mathbb{R}$ $*$: mult. $\mathbb{R}$ same ↑

Is $\mathbb{R}$ comp. with $*$.

No! Take $x=1$ $y=0$ $z=\frac{1}{2}$

$x \mathbb{R} y$ but $x \cdot z \not\mathbb{R}\, y \cdot z$

$\frac{1}{2} \not\mathbb{R}\, 0$

Ex: Let $X = \mathbb{R}$ $*$: + $\forall x,y \in \mathbb{R}$ $x \mathbb{R} y \Leftrightarrow \cos(x) = \cos(y)$

$\mathbb{R}$ is an equ. reln. ✓

Is $\mathbb{R}$ comp with $*$? No. Consider $x = \frac{\pi}{3}$ $y = -\frac{\pi}{3}$ $z = \frac{\pi}{3}$

$x \mathbb{R} y$ but $x + z \not\mathbb{R}\, y + z$

Ex: $X = \mathbb{Z}$ $*$: + $\forall x,y \in X$ $x \mathbb{R} y \Leftrightarrow 5 \mid x-y$

$\mathbb{R}$ is eqv. reln. ✓

Is $\mathbb{R}$ comp. with $*$? yes. exercise.

Ex: $X = \mathbb{Z}$ $*$: · $\forall x,y \in X$ $x \mathbb{R} y \Leftrightarrow 5 \mid x-y$

$\mathbb{R}$ eq. rel. ? ✓

Is $\mathbb{R}$ comp with $*$? Yes bc.

Let $x,y \in X$ $x \mathbb{R} y \Rightarrow 5 \mid x-y$

$\Rightarrow 5 \mid z(x-y) = zx - zy$

$\Rightarrow zx \mathbb{R} zy$

enough since · is commutative.

⊛ Homomorphism

Let $(X, *)$ and $(Y, \circ)$ be two sets with op.

Defn: A mapping $f: X^{(*)} \to Y^{(\circ)}$ is said to be a homomorphism

if for all $x_1, x_2 \in X$ $f(x_1 * x_2) = f(x_1) \circ f(x_2)$

Ex: Consider $(\mathbb{R}, +)$ and $(\mathbb{R}, \cdot)$ $f(x) = 2^x$

Claim: f is a homomorphism between $(\mathbb{R}, +)$ and $(\mathbb{R}, \cdot)$

Let $x_1, x_2 \in X$ be arbitrary.

Observe that $f(x_1 + x_2) = 2^{x_1 + x_2}$

Also $f(x_1) \cdot f(x_2) = 2^{x_1} \cdot 2^{x_2} = 2^{x_1 + x_2}$ same

Ex: $f: (\mathbb{R}, \cdot) \to (\mathbb{R}, \cdot)$

$x \longmapsto 2^x$

Take $x_1 = 3$ $x_2 = 3$ $f(x_1 \cdot x_2) = f(9) = 2^9$

$f(x_1) \cdot f(x_2) = 2^3 \cdot 2^3 = 2^6$

So not a homomorphism.

Ex: Let $f: (\mathbb{R}^+, \cdot) \longrightarrow (\mathbb{R}, +)$

$x \longmapsto \ln x$

Claim: f is a homomorphism

btw ...

Direct Proof

Assume $x_1, x_2 \in \mathbb{R}^+$ be arbitrary

so $f(x_1)$ and $f(x_2) \in \mathbb{R}$

Observe that $f(x_1 \cdot x_2) = \ln(x_1 \cdot x_2) = \ln x_1 + \ln x_2$

$= f(x_1) + f(x_2)$ ✓

Prop: Let $(X, *)$ and $(Y, \circ)$ be two sets with ops.

AND $f: X \to Y$ be an onto homomorphism.

1) if $(X, *)$ is commutative then so is $(Y, \circ)$.

2) if $(X, *)$ is assoc. " " " " .

3) if e_* is the neutral elt. of $(X, *)$ $e' = f(e_*)$

is the neutral elt. of $(Y, \circ)$

4) if $(X, *)$ has a neutral elt. $x \in X$ is invertible

then $f(x)$ is also invertible and $(f(x))^{-1} = f(x^{-1})$

Proof:

1) Assume $(X, *)$ is commutative

want: $(Y, \circ)$ is comm

$\downarrow$

$y_1 \circ y_2 = y_2 \circ y_1$

Let $y_1, y_2 \in Y$ be arbitrary.

Since f is an onto homomorphism

$\exists x_1, x_2 \in X \quad f(x_1) = y_1$

$f(x_2) = y_2$

$f(x_1 * x_2) = f(x_1) \circ f(x_2) = y_1 \circ y_2$

$f(x_2 * x_1) = f(x_2) \circ f(x_1) = y_2 \circ y_1$

Also note that $x_1 * x_2 = x_2 * x_1$ since $*$ is comm. So $y_1 \circ y_2 = y_2 \circ y_1$

2) Assume $(X, *)$ is assoc.

Let $y_1, y_2, y_3 \in Y$

So $\exists x_1, x_2, x_3 \in X \quad f(x_1) = y_1, f(x_2) = y_2, f(x_3) = y_3$ since f is onto.

$$(y_1 \circ y_2) \circ y_3 = (f(x_1) \circ f(x_2)) \circ f(x_3)$$

$$= (f(x_1 * x_2)) \circ f(x_3)$$

since f is homomorphism

$$= f((x_1 * x_2) * x_3)$$

$$= f(x_1 * (x_2 * x_3)) \rightarrow \text{since } * \text{ is assoc.}$$

$$= f(x_1) \circ f(x_2 * x_3) \rightarrow \text{since } f \text{ is homomorphism}$$

$$= f(x_1) \circ (f(x_2) \circ f(x_3)) \rightarrow \text{" " "}$$

$$= y_1 \circ (y_2 \circ y_3)$$

$\therefore (Y, \circ)$ is assoc.

3) Assume e_* is neutral elt. of $(X, *)$

Let $y \in Y$ be arbitrary.

Want: $e' = f(e_*)$ is neutral elt of $(Y, \circ)$

So $\exists\, x_1 \in X$ $\underbrace{f(x_1) = y}$ since f onto.

So $e_* * x_1 = x_1 = x_1 * e_*$ since

e_* is neutral elt.

So $\underbrace{f(e_* * x_1)} = f(x_1) = y$

$\hookrightarrow = f(e_*) \circ f(x_1)$ since f is homomorphism.

Similarly $f(e_*) \circ \underbrace{f(x_1)}_{y} = y = \underbrace{f(x_1)}_{y} \circ f(e_*)$

So $f(e_*)$ is the identity element of $(Y, \circ)$

4) Assume $(X, *)$ has a neutral elt. AND $x \in X$ is invertible. (Δ)

Let e_* be the neutral elt. of $(X, *)$

Want: $f(x)$ is invertible and $(f(x))^{-1} = f(x^{-1})$

$\Delta \Rightarrow \exists\, x' \in X \quad x * x' = e = x' * x$ x' is the inv. of x

Let $y = f(x)$ and consider $y' = f(x')$

We'll show $y \circ y' = e' = f(e) = y' \circ y$

$y \circ y' = f(x) \circ f(x') = f(x * x') = f(e)$

$y' \circ y = f(x') \circ f(x) = f(x' * x) = f(e)$

So $y^{-1} = (f(x))^{-1}$ $\therefore$ y is invertible in $(Y, \circ)$

(*) Isomorphism

Let $(X, *)$ and $(Y, \circ)$ be two sets with ops.

Defn: A mapping $f: X \to Y$ is said to be an isomorphism if f is bijection AND homomorphism.

Ex: $X = \mathbb{R}$ $+$ $\quad$ $Y = \mathbb{R}^+$ $\cdot$ $\quad$ $f: X \to Y$, $x \mapsto e^x$ $\quad$ Is f an Isomorphism? Yes.

1) $f(x+y) = e^{x+y} = e^x \cdot e^y = f(x) \cdot f(y)$

2) f is bij

1-1: Let $x_1, x_2 \in X$ be arbitrary $\quad$ Want: $f(x_1) \neq f(x_2)$

Assume $x_1 \neq x_2$

$f(x_1) = e^{x_1} \quad f(x_2) = e^{x_2}$

$\neq$ since $x_1 \neq x_2$

$\therefore f$ is 1-1

ontoness: let $y \in \mathbb{R}^+$ so consider $\ln(y) \in \mathbb{R}$

$f(\ln(y)) = y$ ✓

$\therefore$ f is onto.

Ex: Let $X = \mathbb{R}^+$ $\cdot$ $f(x) = \ln(x)$

$Y = \mathbb{R}$ $+$

f is bij + f is homomorphism = f is isomorphism.

Homomorphism

Let $x_1, x_2 \in \mathbb{R}^+$ be arbitrary.

$f(x_1 \cdot x_2) = \ln(x_1 \cdot x_2) = \ln x_1 + \ln x_2 = f(x_1) + f(x_2)$

$\therefore$ f is hom.

1-1

Assume $f(x_1) = f(x_2)$ want: $x_1 = x_2$

So $\ln(x_1) = \ln(x_2)$

so $x_1 = x_2$

$\therefore$ f is 1-1

onto

exercise

Ex: Let $X = \mathbb{R}$ $Y = \mathbb{R}$ $*: \cdot$ $0: \cdot$ $f(x) = |x|$

$f(x_1 x_2) = |x_1 x_2| = |x_1||x_2| = f(x_1) f(x_2)$

$\therefore$ f is homomorphism

But f is not onto so f is not bij. (also not 1-1)

So f is not isomorphism.

Prop: Let $(X, +)$, $(Y, \circ)$ be two sets with ops.

and $f: X \to Y$ be an isomorphism.

Then $f^{-1}: Y \to X$ is also an isomorphism.

Proof: Exercise.

Groups and Rings

Defn: Let X be a non-empty set with an op. $\oplus$,

$(X, \oplus)$, is said to be a group if

1) $\oplus$ is closed (i.e. $\forall x_1, x_2 \in X \quad x_1 \oplus x_2 \in X$)

2) $\oplus$ op. is assoc.

3) there exists identity elt. $e \in X$ s.t. $\forall x \in X \quad e \oplus x = x = x \oplus e$

4) every elt. of X ($x \in X$) has inverse elt.

Defn: Let X be a non-empty set with two operations

$\oplus$ and $\odot$. $(X, \oplus, \odot)$ is said to be a ring if

the followings hold.

a) $(X, \oplus)$ is a comm. group

b) $\odot$ is an assoc. op.

c) $\odot$ is distributive over the op. $\oplus$

i.e. $\forall x,y,z \in X \quad x \odot (y \oplus z) = (x \odot y) \oplus (x \odot z)$

and $(y \oplus z) \odot x = (y \odot x) \oplus (z \odot x)$

Defn: The ring $(X, +, \cdot)$ is said to be comm. ring if the op "$\cdot$" is comm.

Defn: If the ring $(X, \oplus, \odot)$ has a neutral el. for $\odot$ then $(X, \oplus, \odot)$ is called a ring with unit (or unitary ring)

Defn: Let $(X, *)$ (Y, o) be two groups. Let e_*, e_o be the unit elements of $(X, *)$ (Y, o) respectively. Let $f: X \to Y$ be a homomorphism.

The kernel of f, denoted by $\ker(f)$ is defined by following:

$$\ker f = \{x \in X \mid f(x) = e_o\}$$

Note that $\ker f$ is non-empty since $e_* \in \ker f$

Defn: Let $(G, *)$ be a group and let H be a non-empty subset of G. If $(H, *)$ is also a group then we say $(H, *)$ is a subgroup of $(G, *$

Thm: Let $(X, *)$ (Y, o) be two groups. If $f: X \to Y$ a homomorphism, then $(\ker(f), *)$ is a subgroup of X.

Proof: $\ker(f)$ is a subset of X. Let's show it is a group.

$*$ op is assoc. since $(X, *)$ is a group.

id. elt: Let e_* be the unit elt of $(X, *)$

$f(e_*) = e_o$ since f is a homomorphism. So $e_* \in \ker(f)$

So id. elt. is an elt. of $\ker(f)$

inv. elt. Let $x \in \ker(f)$ want: $x^{-1} \in \ker(f)$

So $f(x) = e_o$

So consider $f(x^{-1}) = f(x)^{-1} = (e_o)^{-1} = e_o$

proved before

So $x^{-1} \in \ker(f)$

$(\ker(f), *)$ is closed:

let $x_1, x_2 \in \ker(f)$ arb. want: $x_1 * x_2 \in \ker(f)$

$f(x_1 * x_2) = \underbrace{f(x_1)}_{e_o} \circ \underbrace{f(x_2)}_{e_o} = e_o$

$\therefore x_1 * x_2 \in \ker(f)$

Ex: Let $\mu = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} = m \;\middle|\; \det(m) = 1 \right\}$ $(\mu, \cdot)$ is a group?

exercise

Ex: Let $X = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a, b, c, d \in \mathbb{R} \right\}$

Let $+, \cdot$ be the usual adition and mult. of matrices.

$(X, +, \cdot)$ is it a ring?

$$\left.\begin{aligned} \mu \cdot (N+P) &= \mu N + \mu P \\ (N+P) \cdot \mu &= N\mu + P\mu \end{aligned}\right\} \; ?$$