Discrete Structures

- Discrete Objects – can count. why?
  - ↳ computers process bits of info.
    - ↳ discrete entities.
  - ↳ needed to understand mathematical algorithms, computation
- photons are discrete packets of energy ($1h\nu, 2h\nu, 3h\nu$).
- Discrete structures give you mathematical tools to

- Assignments – 30% wt. of $\frac{1}{2}$ sem grade.
  Quizz – 32% wt of $\frac{1}{2}$ sem grade
  Mid sem – 38% wt of $\frac{1}{2}$ sem grade

Discrete Structures Chapter 1 : The Foundations : Logic and Proof

Propositional Logic

- how to pose correct questions in maths? - propositional logic

* Propositions are mathematical statements that are either true or false. There is no ambiguity.
  e.g.) what did you have for lunch? wrong. not proposition.
  - $2+2=4$. correct proposition. } can assign truth
  - $2+2=5$ correct proposition. } values to these.
  - there is no greatest integer - correct proposition, true.

e.g.)
- a proposition p: T/F, cannot be both.

Starting from a proposition, we can build new propositions
- p: apply few operators to build new propositions

→ **Proposition Operators:**

1) Negation: unary operator
- if p is a proposition, then negation of p ($\neg p$, not p) is the complement / opposite of p.

p	$\neg p$
T	F
F	T

$\neg p$: "It is not the case that p."

2) Conjunction (and): binary operator
- Let p and q be two propositions, then the conjuction of p and q is the proposition $p \wedge q$.

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

$p \wedge q$ is True when both p and q are true, and false otherwise.

3) Disjunction (OR): Binary operation.

Let p and q be two propositions; then the disjunction of p and q is the proposition $p \vee q$.

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

$p \vee q$ is false when both p and q are false, and ~~false~~ true otherwise.

4) XOR (exclusive OR):

Let p and q be two propositions; then the XOR of p and q is $p \oplus q$.

$p \oplus q$ is true only when exactly one of p or q is true.

p	q	$p \oplus q$
T	F	T
T	T	F
F	T	T
F	F	F

5) Implication:

Let p and q be two propositions; then the implication of p and q is the proposition $p \to q$.

"$p \to q$" means premise if p, then q!!

$p \to q$ is false when p is true and q is false, and true otherwise.

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

conclusion

vacuously true.

if premise only is false. then who cares

both are true only when q is true } used in proofs.

3) Disjunction (OR): binary operation.

Let p and q be two propositions; then the disjunction of p and q is the proposition $p \vee q$.

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

$p \vee q$ is false when both p and q are false, and ~~false~~ true otherwise.

4) XOR (exclusive OR):

Let p and q be two propositions; then the XOR of p and q is $p \oplus q$.

p	q	$p \oplus q$
T	F	T
T	T	F
F	T	T
F	F	F

$p \oplus q$ is true only when exactly one of p or q is true.

5) Implication:

Let p and q be two propositions; then the implication of p and q is the proposition $p \to q$.

"$p \to q$" means premise if p, then q!!

p	q	$p \to q$
T	T	T
T	F	F
F	T	T / ~~F~~
F	F	

$p \to q$ is false when p is true and q is false, and true otherwise.

conclusion

vacuously true.

if premise only is false then who cares

both are true only when q is true } used in proofs.

e.g.) $p \to q \equiv \neg p \vee q$ → ~~wrong~~? true

↳ this means that both have the exact same truth tables.

6) Biconditional Statement (iff) : $p \leftrightarrow q$

This ($p \leftrightarrow q$) is true when both p and q have the same truth values and false otherwise.

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

"if p then q, but q only if p."

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

• if two compound propositions A, B are equivalent $A \equiv B$, then $A \leftrightarrow B$ is always true.

→ e.g.) $x^2 + 4 \geq 0$ iff $|x| \geq 2$.

i) propositionality depends on variable

ii) biconditionality:

if this is true, then that is also true

if this is true, then that is also true.

* need to prove both ways for iff.

→ if $A \equiv B$:

A	B	$A \leftrightarrow B$
T	T	T
F	F	T
T	T	T
F	F	T

where $A \leftrightarrow B$ is a tautology (all values are True).

* if a compound proposition is ALWAYS false it is called a contradiction / fallacy.

e.g.) $p \vee \neg p$ is a tautology

$p \wedge \neg p$ is a logical contradiction

- 1) $p \to q$
  2) $q \to p$ → converse
  3) $\neg q \to \neg p$ → contrapositive.
  4) $\neg p \to \neg q$ → inverse.

Used when trying to prove stuff.

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

$\Rightarrow$ • $p \to q$ is logically eqv to $\neg q \to \neg p$.

• $q \to p$ is logically eqv to $\neg p \to \neg q$

* an implication and its contrapositive are logically eq
* the converse and inverse are logically equivalent.

e.g.) If I'm hungry I am sad. $(p \to q)$.
if I'm not sad, I'm not hungry $(\neg q \to \neg p)$

Sometimes, when an implication is tough to prove, we prove its contrapositive.

Important Logical Identities

1) $p \wedge T \equiv p$; $p \vee T \equiv T$

2) $p \vee F \equiv p$; $p \wedge F \equiv F$

3) $\neg(\neg p) \equiv p$

4) $p \vee p \equiv p$; $p \wedge p \equiv p$

5) $p \vee q \equiv q \vee p$ commutative laws; $p \wedge q \equiv q \wedge p$

6) $(p \vee q) \vee r \equiv p \vee (q \vee r)$ associative; $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$

7) $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ (right because it obeys commutative law)

$\equiv (p \vee q) \wedge (q \vee r)$ does not obey ↺

** ⇒ ↳ truth value of this proposition changes upon commutation.

$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ distributive laws.

Absorption laws:

1) $p \vee (p \wedge q) \equiv p$. (q is absorbed)

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

$= p \wedge (p \vee q) = p$?

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

logically equivalent

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

3)

de Morgan's laws

1) $\neg(p \wedge q) \equiv \neg p \vee \neg q$.

2) $\neg(p \vee q) \equiv \neg p \wedge \neg q$.

↳ not the case that both p and q are true

↳ either p or q is false

↳ not p or not q is true.

* $\neg(p_1 \wedge p_2 \wedge p_3 \ldots \wedge p_k) \equiv \neg p_1 \vee \neg p_2 \vee \neg p_3 \ldots \vee \neg p_k$

Q) e.g.) Show that $\neg(p \vee (\neg p \wedge q)) \equiv \neg p \wedge \neg q$.

LHS: $\neg p \wedge \neg(\neg p \wedge q)$

$\neg p \wedge (p \vee \neg q)$ ⤵ distribute.

~~$(\neg p \wedge p) \vee \neg q$~~

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

$F \vee (\neg p \wedge \neg q) \equiv \neg p \wedge \neg q$ //.

Predicates and Quantifiers

e.g.) $P(n) = n^2 + n + 41$ is prime for all non-negative integers

n, P(n).

$P(0) = 41$ prime

$P(1) = 43$ prime

$P(20) = 461$ prime.

$P(40) = 40^2 + 40 + 41$

$= 40(40+1) + 41$

$= 41 \cdot 40 + 41$

$= 41 \times 41$

not prime.

$$P(n) = n^2 + n + 41$$
$$= n^2 + 2 \cdot n \cdot \frac{1}{2} + \left(\frac{1}{4}\right) + 40.75.$$
$$= \left(n + \frac{1}{2}\right)^2 + 40.75.$$

- P(n) is a proposition which has a

⊛ $\forall n \in \mathbb{N}_0, P(n)$

universal quantifier ↑ ↓ predicate.

- predicates are propositions that have a truth value only when values are assigned to the variables.

ly (OR) Truth value depends on 1 or more variables.

- quantifiers tell you the extent to which we claim the proposition.

- Universal Quantifier: $\forall x \in D, P(x)$.
  - $\forall$: quantifier. "For all x in D, $P(x)$" is true
  - should work for every x.
- Existential Quantifier: $\exists x \in D, P(x)$
  - $\exists$: there exists at least one
  - Predicate is true for at least one x.

- Statement:
  - $\forall x (\$) P(x)$.
  - ~~$\exists x, P(x)$~~
  - $\exists x, P(x)$.

(Stmt) when true? $\forall x \in D$

There exists an x for which $P(x)$ is

(Stmt) when false? there exists an x for which $P(x)$ is false.

for all x $P(x)$ is false.

$\Rightarrow$ $\forall$ in negation of $\exists$ } that's crazy.
$\exists$ in negation of $\forall$ }

(#) It is not the case that everyone likes to dance.

(#) There exists someone who does not like to dance.

$\Rightarrow$ ~~the negation of~~ : $\neg(\forall x, P(x)) \equiv \exists x, \neg P(x)$.
$\neg(\exists x, P(x)) \equiv \forall x, \neg P(x)$.

e.g.) $D = \{x_1, x_2, \dots, x_n\}$

$(\forall x, P(x)) \equiv P(x_1) \wedge P(x_2) \wedge P(x_3) \dots \wedge P(x_n)$.

$\neg(\forall x, P(x)) \equiv \neg(P(x_1) \wedge P(x_2) \wedge \dots \wedge P(x_n))$

$\equiv \neg P(x_1) \vee \neg P(x_2) \dots \vee \neg P(x_n)$

$\equiv \exists x, \neg P(x)$

(*) For every even integer $n > 2$, there exists primes p and q such that $n = (p+q)$ → Goldbach's conjecture.

evens, primes

② $\exists p, q \in$ primes such that $n = p+q$.

① $\forall n \in$ evens, ③

-{23.

$(\forall n \in \text{evens} - \{2,3\}) \rightarrow (\exists p, q \in \text{primes}, n = p+q)$

if p ~~then~~ q.

⊙ $\exists p, q \in$ primes, $\forall n \in$ evens, $n = p+q$. ✗ wrong not goldbachs

*? ↳ There exists primes p, q, such that for every even no. 72, $n = p+q$.

eg. 3, 5, 12 $3+5 \neq 12$.

HW

∘ $\forall p, q \in$ primes, $\exists n \in$ evens, $n = p+q$.

True: for all primes (p, q) sum = even no. so there exists some even $n = p+q$. -{2,3}

*' $\exists p, q \in$ primes s.t. $\forall n \in$ evens, $n = p+q$.

↓ at least 1 pair of

There exists primes p, q such that for all $n \in$ even, $n = p+q$

↓

that 1 pair must hold for all n.

↓

false -

Read quantifiers as loops in book

Q) $P(x,y,z) = x+y=z$ over $x,y,z \in \mathbb{R}$.

i) $\forall x \forall y \exists z \; P(x,y,z)$. True always.

ii) $\exists z \; \forall x \forall y \; P(x,y,z)$. False always.
(There exists a z, for all the x and y s.t. $x+y=z$ not possible, false.)

Q) The sum of two positive integers is always +ve.

$\forall x, \forall y \in \mathbb{Z}^+ \; \exists \; z \in \mathbb{Z}^+$ such that $z = x+y$.

$\forall x,y \in \mathbb{Z}^+, ((x>0) \wedge (y>0)) \longrightarrow (x+y) > 0.)$

Q) $\exists x \forall y, P(x,y) \longrightarrow \forall y \exists x \, P(x,y)$ is a valid assertion. Show that this is wrong?

- Proof:
Let D be the domain for (x,y)
and P be some predicate over D.

Show: If $\exists x \forall y, P_0(x,y) \quad x,y \in D$ — (1)
then $\exists y \forall x \in D, P_0(x,y)$. — (2)

suppose (1) holds; then by def. of '$\exists$',
for some $d_0 \in D$, $\forall y \in D$, $P_0(d_0, y)$ is true $\forall y \in D$.

(2)

computational model C solves problem P in time T if

$\forall x \in P$, $C(x)$ outputs "YES" in "T steps"

$\forall x \notin P$, $C(x)$ outputs NO in "T steps"

→ Satisfyability Problem (SAT):

- T=1, F=0.

  $P \vee \neg Q$., whenever the compound prop. evaluates to 1, it means there are certain assignments to P, q existing to compound it to 1.

  We then say the compound prop. is satisfiable.

  ↗ n var/literals.

- $P(x_1, x_2, \ldots, x_n) = (x_1 \vee x_2 \vee \neg x_3) \wedge (x_4 \vee x_5 \vee \neg x_6) \wedge \ldots \ldots \wedge (x_{n-2} \vee x_{n-1} \vee \neg x_n)$

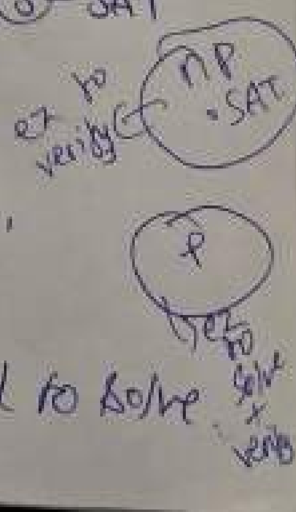
  ↳ each bracket (clause) contains 3 vars in disjunctions and all clauses are in conjunction

  ↳ if we assign bits to each var we get a bit string. e.g. P(1, …… 1)

  3 var in 1 clause.

- Problem: There exists no algorithm that solves 3-SAT in t = polynomial (n). (steps)

  (K-SAT) for K=1,2 this is efficient, K≥3 not efficient yet.



- These problems are easy to ~~solve~~ verify but ~~not~~ hard to solve.

- every NP problem can be reduced to a SAT problem.
  ∴ if SAT is solved ezzz.
- $P \subseteq NP$.

Proof Techniques

- Start with a few axioms
  e.g. there is a least integer in $\mathbb{N}$
- Then use logical references
  $(P \to Q) \wedge (Q \to R) \longrightarrow (P \to R)$.
- Zermelo-Frankel Set Theory with Choice (ZFC).
  ↳ to do everything from ground(0).
  ↳ too primitive.
- Important Words;

i) Theorem;
The most important propositions
(The main claim).

ii) Lemma;
Preliminary Proposition used for proving later propositions
↳ Proving smaller, stand-alone, propositions to help prove the theorem.

iii) Corollary;
Proposition that follows in just a few logical steps from a theorem/lemma.

* How to formally state logical deductions:

antecedent

i) $\frac{P,\ P \to Q}{Q}$; if $\Rightarrow [P \wedge (P \to Q)] \to Q$.

Q ↓ conclusion.

Modus Ponens (to affirm).

ii) $\frac{P \to Q,\ Q \to R}{P \to R}$ shows transitivity.

$[(P \to Q) \wedge (Q \to R)] \to [P \to R]$

iii) $\frac{\neg P \to \neg Q}{Q \to P}$ contrapositive.

prove $\bot$ ⇒ you've proved the bottom.

① Direct Proof:

- Steps to prove $P \to Q$.
  1) write "Assume P"
  2) show that Q follows logically $(P \to Q)$.

e.g.) P: if n is even, then n^2 is even. If n is odd, then n^2 is odd.

proof: Suppose n is even

then $n = 2k$ for $k \in \mathbb{N}_0$

then $n^2 = 4k^2 = 2(2k^2)$ which is even.

$P \to Q \therefore Q$ ✓

ii) suppose n is odd

then $n = 2k+1$, for $k \in \mathbb{N}_0$.

then $n^2 = (2k+1)^2 = 4k^2+4k+1$

$= 2(2k^2+2k)+1 \quad (2b+1)$

which is odd. ∎//

e.g.) P: if $0 \le x \le 2$, then $-x^3+4x+1 > 0$.

suppose $0 \le x \le 2$, then $x, 2-x, x+2$ are all non-negative.

$-x^3+4x = x(4-x^2)$

$= x(2+x)(2-x)$.

≥ 0.

$\therefore -x^3+4x+1 > 0$. ∎//

② Proof By contraposition

- when direct proofs reach a dead end, indirectly prove by using its contrapositive. $p \to q$ $\neg q \to \neg p$.

e.g.) "if r is irrational, then $\sqrt{r}$ is irrational."

can't start w/ P ∴ do $\neg q \to \neg p$

let $\sqrt{r}$ be rational $\Rightarrow \sqrt{r} = \frac{p}{q}$; $p, q \in \mathbb{Z}, q \neq 0$.

$\sqrt{r} \cdot \sqrt{r} = \frac{p}{q} \cdot \frac{p}{q}$

$(\sqrt{r})^2 = \frac{p^2}{q^2} \Rightarrow r = \frac{p^2}{q^2}$; $q \neq 0 \Rightarrow q^2 \neq 0$.

∴ r is also rational. ∎//.

" multiplication obey's closure property on $\mathbb{Q}$

e.g.) ~~Proof by~~

"if n^2 is even, then n is even."

i) direct: $n^2 = 2k$

$n = \sqrt{2k}$. → how do we go from here?

↓

prove contrapositive.

③ Proof of Equivalence.

- used to prove biconditionals: $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$ ✓ ✓

need to show that both hold.

Why IB closing the chain allowed?

e ..., p_n are equivalent.

$p_1 \leftrightarrow p_2 \leftrightarrow p_3 \leftrightarrow \dots \leftrightarrow p_n$

↳ here we establish a chain of equivalences.

$(p_1 \rightarrow p_2) \wedge (p_2 \rightarrow p_3) \wedge \dots \wedge (p_{n-1} \rightarrow p_n) \wedge (p_n \rightarrow p_1)$

↳ close the chain.

- if $n = 3$:

$(p_1 \rightarrow p_3) \wedge (p_3 \rightarrow p_2) \wedge (p_2 \rightarrow p_1)$.

↳ using transitivity.

$p_2 \rightarrow p_1$ is also shown,

biconditionals are all shown.

e.g.) "The s.d. of a sequence of values $x_1, x_2, \ldots, x_n$ is 0, iff, all the values are equal to their mean".

$$\sigma(x_1, \ldots, x_n) = \sqrt{\frac{\sum (x_i)^2}{n} - \left(\frac{\sum x_i}{n}\right)^2} = \sqrt{\frac{1}{n} \sum_{i=1}^{n} (x_i - M)^2}$$

↳ quantifies how much from the mean ~~does~~ the data fluctuates?

$$M = \frac{1}{n} \sum_{i=1}^{n} x_i.$$

Proof:

i) Suppose all $x_i = M$.
Then $\sigma(x_1, x_2, \ldots x_n) = 0$ clearly.

ii) Suppose $\sigma(x_1, x_2, \ldots, x_n) = 0$.
Then $\frac{1}{n}[(x_1 - M)^2 + (x_2 - M)^2 + (x_3 - M)^2 + \ldots + (x_n - M)^2] = 0$
only when each are individually 0.
$\Rightarrow x_1 = x_2 = \ldots = x_n = 0$.
(modus ponens). □ //

(4) Proof by contradiction

- Suppose we want to prove P is true:
assume P is false or $\neg P$ is true
through logical inferences arrive at a contradiction ($\neg P \Rightarrow F$)
conclude.
contrapositive
$T \rightarrow P$ //.

e.g.) P: "Let $x, y \in \mathbb{N}_0$, then $\frac{x+y}{2} \geq \sqrt{xy}$."

& using proof by contradiction;

suppose $\frac{x+y}{2} < \sqrt{xy}$.

$x + y < 2\sqrt{xy}$

$x^2 + 2xy + y^2 < 4xy$

$x^2 - 2xy + y^2 < 0$

$(x-y)^2 < 0$ not possible.
which is a contradiction.
as squares of integers are always non-neg
□ //

eg.) "$\sqrt{2}$ is irrational"

we use contradiction;

Let $\sqrt{2}$ be rational $\Rightarrow \sqrt{2} = \frac{p}{q}$, $p, q \in \mathbb{N}$, s.t. p, q are coprimes.

$2q^2 = p^2 \Rightarrow p^2$ is even

$\Rightarrow p$ is even ∵ sqr of odd = odd.

$p = 2m$

$2q^2 = 2^2m^2$

q^2 is even.

$\Rightarrow q$ is even $\Rightarrow q = 2n$.

if p and q are both even, they must have a common factor of 2, meaning they are not co-prime, which is a contradiction.

$\Rightarrow \sqrt{2}$ is irrational. □//.

⑤ Proof by Induction

- useful for when we try to ascertain the correctness of propositions over all natural numbers.

- Peano's Induction axiom;

Suppose A is a set of positive integers and

i) $1 \in A$

ii) if $k \in A$, then $k+1 \in A$.

Then $A \equiv \mathbb{N}$.

- Define A by saying:

$n \in A$ iff $P(n)$ is true.

The proposition we want to prove

$A = \mathbb{N}$, which means

$P(n)$ is true $\forall n \in \mathbb{N}$.

i) Show $1 \in A$ (P(1) is true).

ii) Show $a \in A \Rightarrow a+1 \in A$

then $A = \mathbb{N}$

1) Prove the base case (P(1) is true)

2) Whenever the statement is true for some $n \geq 1 \in \mathbb{N}$, then it is also true for $n+1$. Show $P(n) \rightarrow P(n+1)$ (Inductive hypothesis)

$$\frac{P(1),\ \forall k \in \mathbb{N}\ (P(k) \rightarrow P(k+1))}{\forall n \in \mathbb{N}\ P(n).}$$

$= 2n+3 < 2^{n+1}$

Harmonic Numbers:

$H_j ; j = \{1, 2, 3, \dots\}$.

$H_j = 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{j}$

Q) Prove that $H_{2^n} \geq 1 + \frac{n}{2}$ $\forall n \in \mathbb{N}_0$.

→ least no. always.

i) $H_{2^n} \geq 1 + \frac{n}{2}$ is $P(n)$.

base case : $n = 0$

$P(1) = H_2 \geq 1 + \frac{1}{2}$.

$1 + \frac{1}{2} \geq 1 + \frac{1}{2}$ ✓

$P(0)$ is true as $H_{2^0} = H_1 = 1 \geq 1$.

ii) Let $H_{2^k} \geq 1 + \frac{k}{2}$ be true

iii) $H_{2^{k+1}} = H_{2^k \cdot 2} = 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{2^k} + \frac{1}{2^k+1} + \frac{1}{2^k+2} + \dots + \frac{1}{2^k+2^k-1} + \frac{1}{2^{k+1}}$

$H_{2^{k+1}} \geq \left(1 + \frac{k}{2}\right) + \underbrace{\frac{1}{2^k+1} + \frac{1}{2^k+2} + \dots + \frac{1}{2^{k+1}}}_{2^k \text{ terms in this sum.}}$

$= H_{2^{k+1}} \geq \left(1 + \frac{k}{2}\right) + 2^k \cdot \frac{1}{2^k+2^k}$ → Substitute each 1, 2, 3 w last term.

$H_{2^{k+1}} \geq 1 + \frac{k+1}{2}$.

$P(k+1)$ is true.

, $a_n = 2n+1$.

⑥ Strong Induction

•

assume ($\rightarrow$ ~~k~~) all proved true.

then $k \rightarrow k+1$, proof

1) base case : P(1) is true

2) inductive hypothesis : if P(k) is true $\forall\ 1 \leq k \leq n$

then prove ~~P(k+1)~~ P(n+1) is also true.

$\therefore$ P(n) is true $\forall\ n \in \mathbb{N}$.

• Why?

• Proposition: Let P(n) be a proposition over $\mathbb{N}$

Let $a \in \mathbb{N}$ and suppose:

i) P(a) is true,

ii) $\forall\ n \geq a$, if P(k) is true $\forall\ a \leq k \leq n$ then

P(n+1) is also true.

$\therefore$ P(n) is T $\forall\ n \geq a$.

Proof:

1. We suppose $P(a)$ is true (basic step).
2. Define $q(n) = \bigwedge_{k=a}^{n} P(k) = P(a) \wedge P(a+1) \wedge \dots \wedge P(n)$

- If $q(n)$ is T, then $P(n)$ is T.
- So it is sufficient to prove that $q(n)$ is true $\forall n \geq a$. → by weak induction.

(Then we conclude $P(n)$ is true $\forall n \geq a$.)

- We prove this by weak induction.

→ Basic case: $q(a)$ is true. $\because P(a)$ is T.

Inductive step: Assume for some $n \geq a$, $q(n)$ is true

Then $P(k)$ is true $\forall a \leq k \leq n$.

Then by (ii) $P(n+1)$ is true.

(Then $q(n+1)$ is true.)

So $P(k)$ is true $\forall a \leq k \leq n+1$.

$\therefore q(n)$ is true $\forall n \geq a$.

6) Proposition: Given $n \in \mathbb{N}_0$, define a_n recursively as follows

$a_0 = 1$, $a_1 = 3$, $a_n = 2a_{n-1} - a_{n-2}$ for $n \geq 2$.

Prove that $\forall n \geq 0$, $a_n = 2n+1$.

* weak induction; base case ✓
; assume true for n =
; proving true for $(n+1)$ → ✗ $(n+1)$ depends on n and $n-1$ ∴ weak fails

* there are two base cases a_0, a_1 ∵ the formula is defined from a_2 onwards.

Proof:

i) Consider $n=0$ and $n=1$
clearly $a_0 = 2(0)+1 = 1$
$a_1 = 2(1)+1 = 3$.

ii) Suppose for $n \geq 1$, we have $a_k = 2k+1$, $\forall\ 0 \leq k \leq n$. } inductive hypothesis

iii) $a_{n+1} = 2a_n - a_{n-1}$

$a_n = 2n+1$ from hypothesis
$a_{n-1} = 2(n-1)+1 = 2n-1$
$\therefore a_{n+1} = 2(2n+1) - (2n-1)$
$= 4n+2-2n+1$
$= 2n+3$ ← $2n+2+1$
$a_{n+1} = 2(n+1)+1$

Chapter 2: Functions, Set Theory, Matrices, Sequences

* $(S=T) \longleftrightarrow (\forall x, (x \in S \Leftrightarrow x \in T))$

* $S \subseteq T$: if elements of S are contained in T.

  $\forall x, x \in S \rightarrow x \in T.$

$(S=T) \longleftrightarrow (S \subseteq T \wedge T \subseteq S)$

$(S=T) \longleftrightarrow (\forall x, (x \in S \rightarrow x \in T) \wedge (x \in T \Rightarrow x \in S))$

* Strict Subsets:

  $S \subset T$ if

  i) $S \subseteq T$ $\wedge$ ii) $\exists x, x \in T \wedge x \notin S.$

  ie: $\forall x (x \in S \rightarrow x \in T) \wedge \exists x (x \in T \wedge x \notin S)$

* $\phi = \{\}$

  For any set S, $\phi \subseteq S$. | $\phi \subset S$ iff $S \neq \phi$.

  Proof:

  $\forall x, \underline{x \in \phi} \rightarrow x \in S$ by dfn. of subsets.

  ↳ False ∴ implication is vacuously true.

- $P(S) = \{x \mid x \subseteq S\}$ power set of S.
- $P(\{0,1\}) = \{\emptyset, \{0\}, \{1\}, \{0,1\}\}$

$P(\emptyset) = \{\emptyset\}$

$P(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$

- $S, |S| = n$

$S = \{s_1, s_2, \cdots, s_n\}$

↓

include 2 choices or exclude $\therefore 2^n$.

x is a set a member of itself?

e.g. $R = \{R, \{2,3\}, 4\}$.

→ Consider the set of all sets, S, that are not members of themselves.

(e.g. R = set of all cups

R' = set of all things not cups

R' must itself be a member of R'.

↳ R is not a member of itself as set of all cups is NOT a cup.

(cont. on nxt pg)

Cartesian Products

- ordered.
- n-tuple.
- let S, T be sets

$S \times T = \{(s,t) \mid s \in S \wedge t \in T\}$.

$S_1 \times S_2 \times S_3 \cdots \times S_n = \{(s_1, s_2, \cdots, s_n) \mid s_i \in S_1 \wedge s_2 \in S_2 \wedge s_3 \in S_3 \cdots\}$

- $S^n = S \times S \times S \cdots \times S$ n times
- $S = \{0,1\}$.

$S^n = S \times S \times S \cdots \times S$ is the set of all bit strings of length n.

- $\overline{A \cap B} = \bar{A} \cup \bar{B}$

$A \overline{\cap} B$ is $\{x \mid \neg(x \in A \wedge x \in B)\}$.

$\{x \mid (x \notin A \vee x \notin B\}$

$\bar{A} \cup \bar{B}$.

• $S = \{x \mid x \notin x\}$ (Set of all sets x, s.t. x does not belong to itself).

* Does $S \in S$?
  ↳ contradiction, logical paradox
  ↳ if $S \in S$, then def. is false
  ↳ if $S \notin S$, then S must be included.

  $S \in S \iff S \notin S$. } def. of sets has some loops.

  Bertrand-Russel paradox? / Cantor's diagonilization

∴ ZFL Set theory is better

Functions

• two sets, assign elements of one set to the other with certain restrictions.

• $f: S \to T$
  for every element s in S, ∃ a unique/singular $t \in T$.

• $R = \{y \mid y = f(x)\}$, $R \subseteq$ co-domain → set of all elements in codomain that have a pre-image in the domain.

• $y = f(x)$ → y is image of x
  x is pre-image of y.

• Injective Functions (One-one): if for Every element $t \in Range(f)$ there exists at most 1 $s \in S$ s.t. $f(s) = t$,

↳ $f(x) = f(y) \Rightarrow x = y$ if f is injective.
↳ test for injectivity?

• Surjective (onto) Function: f is onto $\iff$ co-domain(f) = range(f)

$\forall y \in T, \exists x \in S, \text{ s.t. } y = f(x)$

• $f: \mathbb{N} \to \mathbb{N}$, $f(x) = 2x$.

↳ not onto, does not output odds.

• $f: \mathbb{Z}^+ \to \mathbb{Z}^+$ $f(x) = x^2$

↳ not onto, only outputs perfect squares

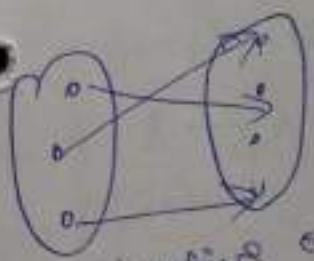
• $f: \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$.

↳ not onto, -ve no.'s are skipped.

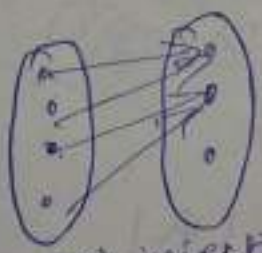
• $f: \mathbb{R}^+ \to \mathbb{R}^+$ $f(x) = x^2$ ✓ onto.

• Bijective functions:
injective ∧ surjective.

•



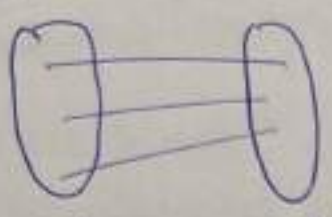
injective only
(one-one)



not injective.
not surj.

• if $f: S \to T$ is bijective, $f^{-1}: T \to S$ exists

- $f: S \to T$



→ graph.
→ lines are called edges of the graph.
→ $|S|$ no. of edges for every functions
$|E| = |S|$ (every element in S is mapped)

$|S|$ $|T|$

i) Suppose f is surjective, $|S| \geq |T|$

ii) Suppose f is injective, $|T| \geq |S|$.

- ~~if we want to compare the~~
  $|S| = |T| \Rightarrow$ bijective function.
  ∴ if we check, bijection, surjection, injection, we can compare cardinality of even infinite sets.

- Bter Schroeder - Bernstein Theorem &
  * for any pair of sets S&T if $|S| \leq T$ ($\exists$ an injection S→T) and $S \geq T$ ($\exists$ a surjection S→T) then $|S| = |T|$
  ($\exists$ a bijection S→T).

* ~~po~~ |power set of $|\mathbb{N}| = |\mathbb{R}|$
  $|P(P(\mathbb{N}))| > |\mathbb{R}|$.

- holds for ∞ sets also

Theorem:
If A → B one-one
B → A one-one
then A → B bij

- Given two sets S and T,

  $(|S| = |T|\ ?) \iff (S \text{ bij. } T\ ?)$.

- Infinites are different in nature:
  ↳ many properties of finites sets do not extend to ∞ sets.

  i) for any finite set S and $8 \notin S$

  $$|S \cup \{S\}| = |S| + 1.$$

  If S is infinite, is it still true? ↓

- Proposition: Let A be a set and $b \notin A$. Then A is infinite iff ∃ a bijection from A to $A \cup \{b\}$

  i) A is finite $\longrightarrow \neg(A \text{ bij } A \cup \{b\})$

  (taking contrapositive)

  A bij $A \cup \{b\} \longrightarrow$ A is infinite. Q.E.D.

  ii) Suppose A is infinite (countably).
  Then, we can generate an infinite sequence $a_0, a_1, \ldots, a_n$ of different elements in A. (because it is an ∞ set).

  Let $f: A \to A \cup \{b\}$
  $f(a_0) = b$
  $f(a_{n+1}) = a_n \ ; \ n \in \{0, 1, 2, \ldots\}$
  for the rest; $f(a) = a \ ; \ a \in A - \{a_0, a_1, \ldots a_n\}$

  every element in A is assigned to an element in $A \cup \{b\}$

  ↳ for the rest of the uncountably ∞ elements.

  ↳ similar to Hilbert's hotel: full rooms, 1 new guy comes in.

• **Countable Sets:** A set is countable if it is finite or if it has the same cardinality as $\mathbb{N}$

S is countable $\iff |S| \leq \mathbb{N}$.

• If we can index every element of the set with $\mathbb{N}$ it is countable

• for countable sets, elements can be listed in order
ie. $S_0, S_1, S_2, \ldots$
↳ if we generate this list $f(i) = S_i$ } if S is ∞
$\Rightarrow \mathbb{N}$ bij S } ↵
$|\mathbb{N}| = |S|$ }

S is finite ($|S| < |\mathbb{N}|$).

* S is countable → S is finite ($|S| < |\mathbb{N}|$).
→ S is infinite ($|S| = |\mathbb{N}|$) (bij with $\mathbb{N}$)

• infinite sets for which $\nexists$ $\mathbb{N}$ bij S are called countably ∞ sets

• Set of all computable problems is countably ∞.
Set of ALL problems is uncountably ∞.

Properties of Countable Sets

1) Unions:

$A \cup \{b\}$

↳ countably ∞ $\Rightarrow$ $a_0 \to b$
$a_1 \to a_0$
$a_2 \to a_1$
...

$\mathbb{R}$ is uncountable

~~Proof~~;

$A \cup B = C$; A, B is countably ∞

$|A| = |\mathbb{N}|$ We need to establish $\mathbb{N}$ bij $A \cup B$.

$|B| = |\mathbb{N}|$.

→ If A and B are countable, so is $A \cup B$;

i) $a_0, a_1, \ldots, b_0, b_1 \ldots$

↳ need to create an ordering of $A \cup B$ for creating a mapping.

~~$a_0 + a_1 + \ldots$~~

↳ invalid; a does not end
b does not begin

ii) $a_0 b_0 a_1 b_1 a_2 b_2 a_3 b_3 \ldots$

$\mathbb{N}$ bij $A \cup B$

↳ if $A \cap B \neq \emptyset$

~~$f: \mathbb{N} \to A \cup B$~~

~~$f(2i-1) = a_i$~~

↳ valid indexing.

Proof;

- list the elements of $A \cup B$ as $a_0, b_0, a_1, b_1, a_2, b_2 \ldots$

If there are duplicate elements, delete all but the first occurence.

→ what about $A_1 \cup A_2 \ldots \cup A \ldots$? ← Union of a countable number of sets, each of which is countable, is also countable

- Can we establish a bij from $\mathbb{N} \to \mathbb{N}_0$?

Yes!

$1 \to 0$
$2 \to 1$
$3 \to 2$
$\ldots$
$a_{n+1} \to a_n$ //

} a sequence has been established.

2) Cross Product of two countable sets;

- $C = A \times B$; A, B are countably ∞.

* Let $A = \{a_0, a_1, a_2, \ldots\}$
$B = \{b_0, b_1, b_2, \ldots\}$
$C = \{(a_i, b_j)\}$; need to establish $\mathbb{N}$ bij C.

- ① (a_0, b_0), ② (a_0, b_1) ④ (a_0, b_2) ..... ∞ list, does not terminate.
③ (a_1, b_0), ⑤ (a_{+1}, b_1) (a_1, b_2) ....
⑥ (a_2, b_0) $(a_2 b_1)$ $(a_2 b_2)$ ....

↳ if we count row-wise, we will never be able to index to the second row

* ↳ we go diagonally

$f(1) = (a_0, b_0)$ } sum 0

$f(2) = (a_0, b_1)$, $f(3) = (a_1, b_0)$ } } sum 1

$f(4) = \ldots$

$f(1)$ = sum of subscripts = 0

$f(2) \Rightarrow$ sum of subscripts = 1.

$f(3) \Rightarrow$

$\therefore \exists$ a bij $\mathbb{N}$ to $A \times B = C$

~~let = $A \times B$~~

$\Rightarrow$ C is countable.

3) Any subset S of $\mathbb{N}$ is countable;

Proof;

- if S is finite it is trivial.
- well-ordering principle: every subset of $\mathbb{N}$ has a least n in it.

→ Let $T \subset \mathbb{N}$

by well ordering principle, T has a least element t_0.

Then $T - \{t_0\}$ is empty (finite → countable) OR.

it has more elements.

$T / \{t_0\}$ is a subset of $\mathbb{N}$, remove its least element t_1.

$T \{t_0\} - \{t_1\}$ → same as above, repeat.

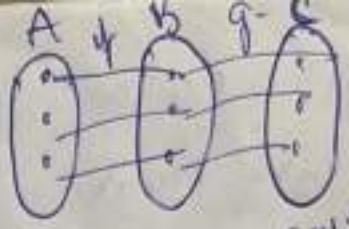
∴ either T is finite or elements of T can be sequenced in ascending order $\{t_0, t_1, \ldots\}$.

↪ T is countably ∞; ~~f bij $\mathbb{N}$;~~

$\mathbb{N}$ bij T.

- A bij B. (let)

(A $\overset{f}{\text{bij}}$ B) $\wedge$ (B $\overset{g}{\text{bij}}$ C) $\quad |A| = |C|$



$\Rightarrow \exists$ A bij C $\quad g \circ f$.

this is a transitive relationship $\quad A \to C$ - $g(f(x))$

4(*) Any subset of a countable set is countable.

~~$\mathbb{N}$ bij P $\mathbb{N}$ bij~~ S.

{Let S be a countable set} + {transitivity}

{we know this is true for $S = \mathbb{N}$.}

~~S to $\mathbb{N}$ $\mathbb{N}$ to P~~

~~S $\Rightarrow$ P.~~

Proof:

S to $\mathbb{N}$. (bij $\because$ S is countable) say $f: S \to \mathbb{N}$

let $T \subseteq S$.

$Z = \{f(t) \mid t \in T\}$, images corresponding to the elements of T

$g: T \to Z$ is a bij $\quad Z \subseteq \mathbb{N}$.

$h: Z \to \mathbb{N}$ is a bij

$(T \text{ bij } Z) \wedge (Z \text{ bij } \mathbb{N})$ $\quad \therefore T \subseteq \mathbb{N}$. (from previous)

$h \circ g(x)$ is a bij from $T \to \mathbb{N}$ //

$\therefore T \subseteq S$ is countable.

5) $\mathbb{Z}$ is countable.

$\mathbb{Z} = \{\ldots -2, -1, 0, 1, 2, \ldots\}$.

define; $f: \mathbb{N} \to \mathbb{Z}$ as follows

$f(1) = 0$

$f(2k) = k$, $f(2k+1) = -k$.

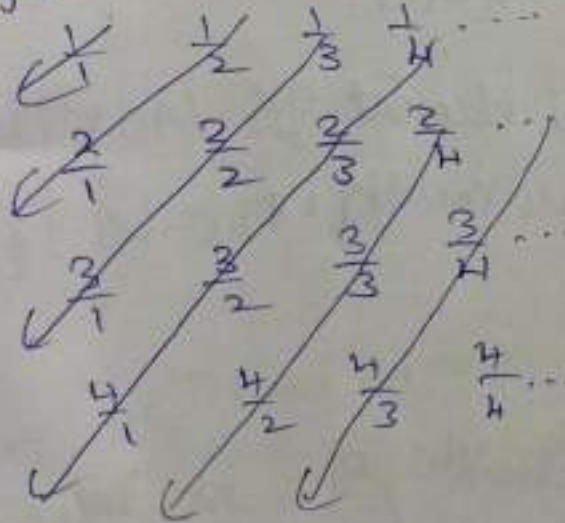
$f(0) = 0$
$f(1) = 0$.
$f(2) = 1$
$f(-2) = -1$
$f(-1) = 1$.

if bij exists → inverse exists

6) The set $\mathbb{Q}^+$ is countable.

- $q = (a,b) = a/b$, $a, b \in \mathbb{N}$ ∴ $\mathbb{N} \times \mathbb{N} = \mathbb{Q}^+$ sort of by this def.

Proof:



This way of indexing implies

$\exists$ $\mathbb{N}$ bij B.

$f: \mathbb{N} \to B$

$B = \mathbb{Q}^+ \cup (\frac{2}{2}, \frac{3}{3}, \frac{4}{4} \ldots)$

∵ B is countable

$\mathbb{Q} \subseteq B$, $\mathbb{Q}$ is also countable

~~Alternatively;~~

Uncountable Sets

- Any set S is uncountable if it is not countable.
  → cannot establish $S \overset{bij}{\sim} \mathbb{N}$ | $\mathbb{N} \overset{bij}{\sim} S$.
  → uncountable sets are always ∞.

Theorem:

The set S, ~~which is an~~ of all infinite sequence of binary digits, is uncountable.

$$S = \{ s_1, s_2, s_3, \dots \}$$

$$s_i = d_1^{(i)} d_2^{(i)} d_3^{(i)} \dots, d_j^{(i)} = \{0,1\}.$$

$\forall$ 2 indices: (i) denotes the element.
Subscript denotes the dig it.

Proof:

Proof by contradiction;
Suppose $f: \mathbb{N} \to S$ is a bijection

$f(1) = s_1 = d_1^{(1)} d_2^{(1)} d_3^{(1)} d_4^{(1)} \dots$
$f(2) = s_2 = d_1^{(2)} d_2^{(2)} d_3^{(2)} d_4^{(2)} \dots$
$\dots$
$f(3) = s_3 = d_1^{(3)} d_2^{(3)} d_3^{(3)} d_4^{(3)} \dots$

- construct an ∞ sequence of bits which has no index in the mapping.
- pick diagonally, invert and construct.

$s^+ = \neg d_1^{(1)} \neg d_2^{(2)} \neg d_3^{(3)} \dots$
↳ this is not in set S → contradiction proved □.

• diagonalization is used to prove many sets are uncountable.

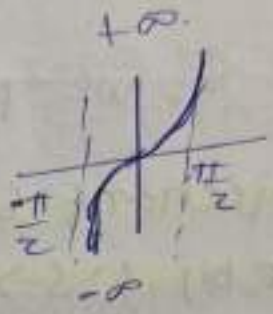
e.g.) Prove $\mathbb{R}$ is uncountable;

• if $\mathbb{R}$ is countable, any subset of $\mathbb{R}$ should be countable.

* $|\mathbb{R}| = |[0,1]|$

↳ 

$y = \tan x$



↳ $y = \tan\left(\pi\left(x - \frac{1}{2}\right)\right)$ is a $[0,1]$ bij $\mathbb{R}$.

$f: [0,1] \to \mathbb{R}$.

(*) $|\mathbb{N}| < |\mathbb{R}|$ iff $\exists$ an injection ✓✓

$f: \mathbb{N} \to \mathbb{R}$ $f(x) = x$ is an injection

(*) there are two groups of infinities.

$\mathbb{N}$ like ∞s, $\mathbb{R}$ like ∞s

• are there larger infinities?

* Cantor's Theorem

- For any set S, $|S| < |P(S)|$

Proof:

→ show injection $S \to P(S)$, no surjection

i) For finite sets this is obvious; $\forall S, |S| < |P(S)| = 2^{|S|}$

ii) For infinite S, we prove

a) $\exists$ injection $f: S \to P(S)$

b) $\nexists$ ~~no~~ bij $f: S \to P(S)$.

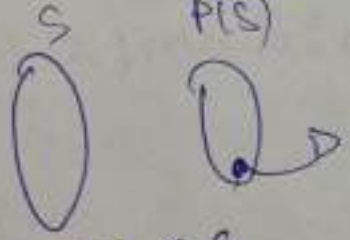
a) Map every element of S to a singleton subset.

define $f: S \to P(S)$ s.t

$f(x) = \{x\} \quad \forall x \in S$.

This is an injection.

b)



all $x \in P(x) \subseteq S$

to show $\nexists$ a surjection, come up with an element t for which there is no pre-image in S.

For any function $f: S \to P(S)$ we will provide a set $T \subseteq S$ ($T \in P(S)$) s.t T has no pre-image in S.

- $f: S \to P(S)$

  $\forall x \in S, \; f(x) \subseteq S$. ($\because f(x) \in P(S)$)

- $\forall x \in S$; $\boxed{x \in f(x) \vee x \notin f(x)}$

  ↳ let S = set of all students

  $\forall x \in S$, $f(x)$ is set of all students that x believes will score A in D.S.

$\forall x \in S$, either $x \in f(x)$ $\vee$ $x \notin f(x)$

- define $T = \{x \in S \mid x \notin f(x)\} \subseteq S$, $T \in P(S)$.
  (this cannot have a pre-image in S)

Suppose $\exists\ x$ s.t. $f(x) = T$ (there is some pre-image for T in S).

(i) Suppose $x \notin f(x)$, $x \in T$.
but $\therefore T = f(x)$, $x \in f(x)$ contradiction.

(ii) Suppose $x \in f(x)$, $x \in T \rightarrow x \notin f(x)$
contradiction.

$\rightarrow$ T has no pre-image in S

$\therefore |S| < |P(S)|$ □//.

T = set of all students who don't think they can A.

let $\exists$ some student who believes exactly these students get an A. $f(x) = T$,

what about that student?

- $|\mathbb{N}| < |\mathbb{R}|$
- $|\mathbb{N}| < |P(\mathbb{N})| < |P(P(\mathbb{N}))| \ldots$
- $|\mathbb{R}| = |P(\mathbb{N})|$ $\mathbb{R}$ bij $P(\mathbb{N})$

Continuum Hypothesis

There is no infinite set X s.t.

$$|\mathbb{N}| < |X| < |\mathbb{R}|.$$

Chapter 3: Permutations and Combinations

- fundamental principle of counting; (Product Rule)

n_1 ways to do task T_1
$n_2 \longrightarrow T_2$
....
$n_i \longrightarrow T_i$

$T_1, T_2, T_3 \ldots T_i$ } are all mutually independent events.
$(T_1 \wedge T_2 \wedge T_3 \ldots)$

$T_1 T_2 \ldots T_i$ can be accomplished in succession in $n_1 n_2 \ldots n_i$ ways.

- cartesian product of $T_1 \times T_2 \ldots \times T_i$

- Sum Rule;

$n_1 \rightarrow T_1$
$n_2 \rightarrow T_2$
...
only one of T_i happens at once

mutually disjoint tasks
no. of ways to accom
these $(T_1 \vee T_2 \ldots \vee T_i)$

- mutually disjoint ~~element~~ events; ↳ both events cannot happen at the same time. (same as exclusive).
- mutually dependent / independent.

- Let $|S| = n$, there are 2^n possible subsets of S.

↳ no. of n length binary string (bij) P(S).

$S = \{x_1, x_2, \ldots, x_n\}$ → take each element, does it belong to a subset or not?

$\{x_3, x_5\}$
$0\,0\,1\,0\,1\,0\,0\,0 \ldots 0$.

each subset corresponds to a binary string of length n. ⇝ ∴ total no. of n-len. binary strings = no of subsets.

- $|\{0,1\}^n| = |\{0,1\}|^n = 2^n$.

Permutation

- arranging the elements of a set in some order. → ordering matters (extending def. of sets)
- $\{a,b,c\}$ → if we write the set in different orders to obtain new permutation.

- each element of the set S has an index
  define a permutation $\sigma : S_i \to S_j$ $\sigma(i) = j$
  ↳ initially element at index i, after permuting indexed to j.
  ↳ σ is a bij from S_i to S_j (indices of S)

- $S = (a_1, \ldots, a_n)$ $n!$ ways.

- Set of all permutations $S(\sigma) = \{ \ldots \}$.
  $S(\sigma)$ has $n!$ elements.

→ K-Permutation

- set of n elements, take K of them and permute (arrange in some order) K of them.
- pick sequence of K elements and order them.
  $S = \{a_1, a_2, \ldots, a_n\}$. $K \leq n$.
  i) pick K_1 permute K_s. → chose K elements.
  ↳ $n(n-1)(n-2)\ldots(n-(k-1))$
  ↳ then permute K elements $k!$

$$\frac{(n-0)(n-1)(n-2)\cdots(n-(k-1))\times k!\times(n-k)(n-k-1)\cdots 1}{(n-k)(n-k-1)\cdots 1}$$

1st place can be filled in n ways

$$\frac{n!\cdot k!}{(n-k)!}$$?

$\overline{1^{st}}$ $\overline{2^{nd}}$ $\overline{3^{rd}}$ $\overline{4^{th}}$ $\overline{5^{th}}$ $\cdots$ $\overline{r.}$

H.W.

$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$

using set theory.

Combination

- Set of length n, picking subsets of length k.
  no ordering here.
- picking/selecting subsets of cardinality k from a set of cardinality n.

K-Permutation With Repetitions

- $S = \{a_1, \ldots, a_n\}$.
  K-permutations : n^k ways (∵ repetition is allowed)

K-Combination with Repetitions

- no ~~Std~~ repetition in subsets? So how do we define it?
- K-comb. of n elements has 2 features (with repetition)
  (a) order does not matter
  (b) Repetition ~~(not)~~ allowed

• we need to define a new set (multi-set)

where $\{1,2,3\} \neq \{1,2\}$.

• Multi-Sets;

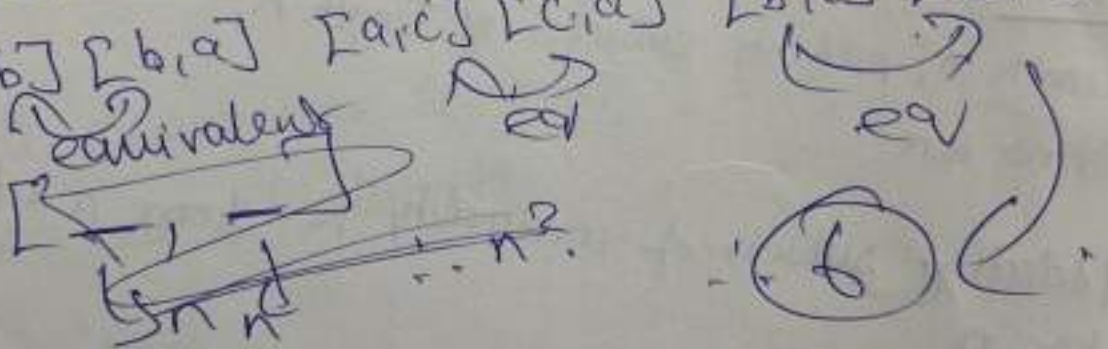
$A = [1,1,5,10,3,8,8]$ * ordering does not matter so if we permute we get the same multi-set.

$|A|$ = no. of elements it has, with repetition.

(*) How many multisets of cardinality 2 can be made from $\{a,b,c\}$.

$[a,a]$ $[b,b]$ $[c,c]$

$[a,b]$ $[b,a]$ $[a,c]$ $[c,a]$ $[b,c]$ $[c,b]$



• can construct multisets of cardinality 4 from a set of size 3.

(*) Claim: The no. of k-combination with repitition from a set S of n elements is the number of multi-sets of cardinality k that can be made from the elements of S.

(*) How many multisets of cardinality 5 can be made from $\{a,b,c,d\}$?

- $X = \{a, b, c, d\}$.

Multiset Sep.

$[a,a,a,a,a]$ aaaaa|||

$[a,b,b,c,d]$ a|bb|c|d $\Rightarrow$ we can do this as ordering does not matter here.

fix to position of a's. n_1 n_2 n_3 n_4
$* \mid ** \mid * \mid *$

OR $n_1 + n_2 + n_3 + n_4 = K$.

↓
Star-Bar encoding

no. of multisets of cardinality 5 = no. of ways we can put these bars b/w the stars,

$k + \cancel{4-1} = 3$:

- # K-combinations with repetitions $\equiv$ # K-cardinality multisets.

~~$\binom{k}{3}$~~ *

- $S = \{a, b, c, d\}$, count # 5 cardinality multisets of S.

$[a,a,a,a,a]$ aaaaa|||

$[a,a,b,c,d]$ aa|b|c|d

5 *'s, 3 |'s ∴ no. of 5-cardinality multisets is the same as the number of ways we can ~~partition~~ place 3 bars b/w 5 stars.

↳ $= \binom{8}{3}$ _ | _ | _ _ | _ _

put bars in any 3, fill rest with *'s

(*) $S = \{s_1, s_2, \ldots s_n\}$ K-cardinality multisets.

i) K stars ii) n−1 bars.

$**\,|\,*\,|\,\ldots\ldots\,|\,\ldots*$

$s_1 \quad s_2 \quad \ldots \quad s_3$

$\binom{K+n-1}{n-1}$ = total no. of K-cardinality multisets
= total no. of K-combinations with repetitions.

- $x_1 + x_2 + x_3 + x_4 = 20$ $\quad S = \{x_1, x_2, x_3, x_4\}$. How many 20-cardinality multisets of S?

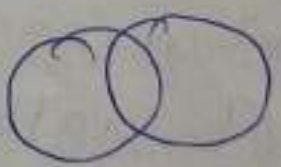
$***\,|\,**\,|\,*\,|\,*$

$x_1 \quad x_2 \quad x_3 \quad x_4$.

$23C_3$.

Inclusion & Exclusion Principle

- for disjoint sets, cardinality of $A \cup B = n(A) + n(B)$
- in reality many sets have many intersection
∴ we use inclusion-exclusion.

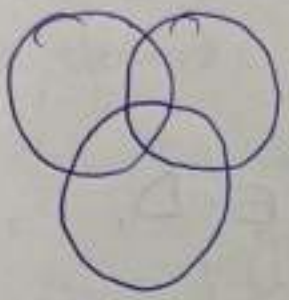


- $|A \cup B| = |A| + |B| - |A \cap B|$

↳ elements common to A and B are counted twice

- $|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3|$
  elements which are in any two sets are counted twice.
  elements in all 3 are counted thrice.

- $\therefore |A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_2 \cap A_3| - |A_3 \cap A_3|$
  elements in all 3: added thrice — subtracted thrice
  $\therefore + |A_1 \cap A_2 \cap A_3|$.



- Generally;

$$|A_1 \cup A_2 \cup A_3 \ldots \cup A_n| = (|A_1| + |A_2| + \ldots + |A_n|) - [(|A_1 \cap A_2| + |A_2 \cap A_3| + \ldots + |A_n \cap A_1|] + |A_1 \cap A_2 \cap A_3| + |A_2 \cap A_3 \cap A_4| + \ldots$$

$|A_1 \cap A_2 \cap A_3| + |A_2 \cap A_3 \cap A_4| + \ldots$: $n C_3$ terms.

$|A_1 \cap A_2| + |A_2 \cap A_3| + \ldots + |A_n \cap A_1|$: $n C_2$ terms.

$$|A_1 \cup A_2 \ldots \cup A_n| = \left| \bigcup_{i=1}^{n} A_i \right| = \sum_{\phi \neq K \subseteq \{1,2,\ldots,n\}} (-1)^{|K|+1} \left| \bigcap_{j \in K} A_j \right|$$

$\bigcap_{j \in K} A_j$: j-wise intersection.

i) generate subsets of size 1
ii) generate subsets of size 2.
...

Proof:
Δ is an element in K of these sets
any such elements is counted only once.
→ added K times in $\sum_{i=1}^{n} |A_i|$
→ $\sum_{1 \le i < j \le K} |A_i \cap A_j|$ subtracted $K C_2$ times

$\rightarrow \sum_{1 \le r < m < n \le k} |A_r \cap A_m \cap A_n|$ added $\binom{k}{3}$ times

$\therefore \#_8 = \binom{k}{1} - \binom{k}{2} + \binom{k}{3} - \binom{k}{4} + \binom{k}{5} \ldots$

$\because (1-x)^n = \binom{n}{0} - \binom{n}{1}x + \binom{n}{2}x^2 - \binom{n}{3}x^3 \ldots$

$1 - (1-x)^n = \binom{n}{1}x - \binom{n}{2}x^2 + \binom{n}{3}x^3 \ldots$

put $x = 1$

$\Rightarrow \binom{k}{1} - \binom{k}{2} + \binom{k}{3} \ldots = 1$ // Q.E.D.,

$= \#_5$.

Derangements

- can have any seed and permute it.

  ↓

  ∵ all elements are distinct we can index them

  so a permutation is also basically a

  bij $\pi : [n] \to [n]$. $[n] = \{1, 2, \ldots, n\}$

  let $\pi_0 = \{1, 3, 5, \ldots\} \rightarrow \exists\ i : \pi(i) = i$

  ↳ index of 1 not changed.

  can we count only those permutations for which the position of any index i is no longer i.

- let $X = \{\pi\}$ $\quad |S| \subseteq |X|$.

  $S = \{\sigma \mid \sigma(i) \neq i\}$

- such permutations are called derangements.

- S is the set of all derangements $\sigma : [n] \to n$.

(*) Count no. of derangements $\Pi : [n] \to [n]$.

Set of all permutations has cardinality $n!$.

$$|X| = n!$$

- Suppose A_i is set of all permutations that fixes a single element i.

Index of i is i even of after all permutations.

$$(n) = n! - \left| \bigcup_{i=1}^{n} A_i \right|$$

$|A_1|$ = no. of ~~elements in~~ permutations in which element 1 in $[n]$ is fixed.

$|A_2|$ = no. of permutations in which element 2 in $[n]$ is fixed ... etc.

Subtracting these from all permutations

The permutations left after subtracting;

$\neg$(either 1 is fixed $\vee$ either 2 is fixed .....)

$= ($1 is not fixed $\wedge$ 2 is not fixed ....$)$.

- by inclusion-exclusion.

$$\left| \bigcup_{i=1}^{n} A_i \right| = \sum_{\emptyset \neq K \subseteq \{1,2,\dots n\}} (-1)^{|K|+1} \left| \bigcap_{j \in K} A_j \right|$$

↳ how many permutations we get when we fix j indices.

$$= \sum_{K=1}^{n} (-1)^{K+1} \binom{n}{k} (n-k)!$$

$\binom{n}{k}$: no. of ways of choosing subsets of size k

$(n-k)!$ → permuting the rest of the sets

$$= \sum_{k=1}^{n} (-1)^{k+1} \frac{n!}{k!}$$

$$\therefore d(n) = n! - \sum_{k=1}^{n} (-1)^{k+1} \frac{n!}{k!}$$

$$d(n) = \sum_{k=0}^{n} (-1)^{k} \frac{n!}{k!}$$

Probability of derangements $\sum_{k=0}^{n} \frac{(-1)^k}{k!} = P(d(n))$

as $n \to \infty$

$P(d(n)) \to \frac{1}{e}$.

- $X = \{\pi : [n] \to [n]\}$. $S \subseteq X$

  $|X| = n!$ (total permutations).

  $S = \{\pi : [n] \to [n] \mid \pi(i) \neq i, \forall i \in [n]\}$.

  $|S| < n!$

Pigeon Hole Principle

- K+1 pigeons, K holes, then there will be one hole at least which has 2 pigeons.
- in a room with 366 people, at least 2 will have same bday
- $f: X \to Y \quad |X| > |Y|$
  f has to be a many-one function.
- if we place $\geq n$ pigeons into K holes, then at least one contains $\lceil \frac{n}{K} \rceil$ or more pigeons.

Q) During 30 days a student solves at least one problem every day from a list of 45 problems, Show that there is a period of several consecutive days in which they solve exactly 14 problems

Proof:

Let a_i be the number of problems solved during the first i days.

$0 < a_1 < a_2 < a_3 < \dots < a_{30} \leq 45$. mutually distinct.

add 14 everywhere.

$14 < a_1+14 < a_2+14 < a_3+14 < \dots < a_{30}+14 \leq 59$

60 numbers upper bounded by 59 ~~(all distinct)~~

by pigeonhole, two no.s have to be equal.

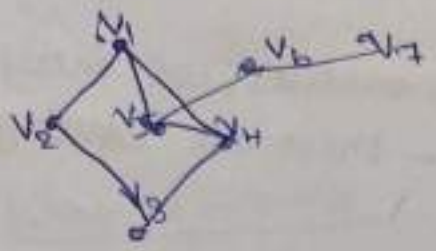
$\Rightarrow$ a_i list = a_i+14 list. only.

$a_j = a_i + 14$ for some $i, j \Rightarrow a_j - a_i = 14$.

from day $i+1, i+2, \dots, j$ student solved 14 problems //

Chapter 4: Graph Theory insanely important.

- Sequences of vertices and ~~groups~~ edges.



'.' nodes / vertices

'—' edge → connects two vertices.

- can define an edges as ~~ordered~~ pairs

(V_1, V_2) ; (V_1, V_4), ...

- $G = (V, E) \equiv G(V, E)$

A graph G is a set of vertices and edges

$V = \{V_1, V_2, \ldots, V_7\}$, $E \subseteq V \times V$.

$E = \{(V_1, V_2)\ (V_1, V_4)\ (V_1, V_5)$
$\ldots\ldots\}$.

- a graph $G(V, E)$ consists of V, a non-empty set of vertices and $E \subseteq V \times V$ set of edges associated with V.

- $(V_i, V_j) \wedge (V_j, V_i)$ represent the same edge if the graph G is undirected.

↳ (like symmetric relation type).

- Graphs can also be directed using arrowed-edges.

∴ Edges are now ordered pairs.

$(V_i, V_j) \neq (V_j, V_i)$

- mostly deal with undirected graphs.

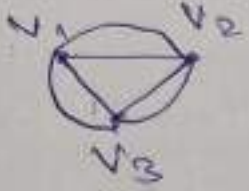
- $E = \emptyset$ possible

eg.

• What about (v_i, v_i) → self loop.

} Markov-Chaining.

•

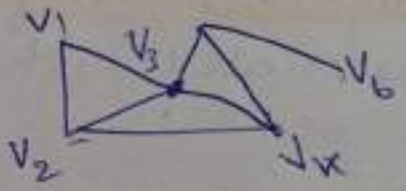


• b/w the same pair of vertices, we may have multiple edges. – these are multigraphs.

• Simple Graphs

A graph in which each edge connects two different vertices and where no two edges connect the same pair of vertices (no multigraphs) and where there are no self loops.

•



A vertex v_i is adjacent to a vertex v_j ((v_i, v_j) are neighbours) if they are the end points of an edge, e.

$\leftrightarrow$

e is incident with the vertices (v_i, v_j).

• Degree of a Vertex i

$\deg: V \to \mathbb{N}_0$.

$\deg(V)$ = the no. of edges incident of V
= the no. of vertices adjacent to V.

e.g. $\deg(v_1) = 2$ any isolated vertex has degree 0.
$\deg(v_3) = 4$.

e increases the degree of its end points by 1

Self loops (by convention) increase the degree of a vertex by 2.

Handshaking Lemma

- $G(V, E)$, then $\sum_{v \in V} \deg(v) = 2|E|$
- each edge contributes for 2 degrees ~~for~~
- Corollary: An undirected graph has an even no. of vertices of odd degree.

$\sum \deg(v) \rightarrow \sum \deg(a)$; a = even degree-d vertices

$\sum \deg(b)$; odd degree-d vertices

↓

no. of elements summed must be even for full to be even //.

Directed Graphs

- each edge has a definite directionality.
- if (u, v) is an edge of a directed graph G, u is said to be adjacent to v, while v is adjacent from u. u is the initial vertex while v is the terminal vertex.

edges → outgoing edge → out degree
edges → incoming edge → in degree

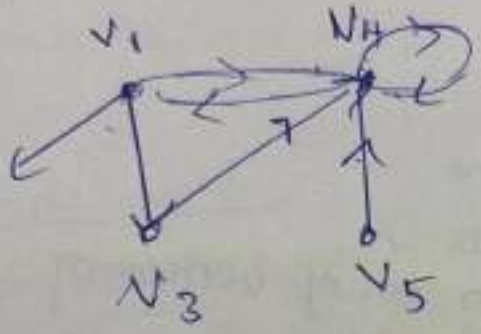
} two types of degrees

Degrees for Directed Graphs

- For a D.G. $G(V, E)$, the in-degree of a vertex v $\deg^-(v)$ is the no. of incoming edges to v.

  the out-degree $\deg^+(v)$ = # out-going edges from v.

e.g.



$\deg^-(v_H) = 4$; self loop is out-going and incoming.

$\deg^+(v_H) = 2$;

- $\sum \deg^+(v) = \sum \deg^-(v) = |E|$.

any directed edge contributes 1 to $\sum \deg^+$ from the vertex it begins at and 1 to $\sum \deg^-$ from the vertex it ends at.

Examples of Graphs (Simple)

1) Complete Graph; (K_n)

- each vertex is connected to every other vertex (n).

K_1 K_2 K_3 K_4 K_5

$\deg(v) = n-1 \quad \forall K_n$

$|E| = \binom{n}{2} = \frac{n(n-1)}{2}$

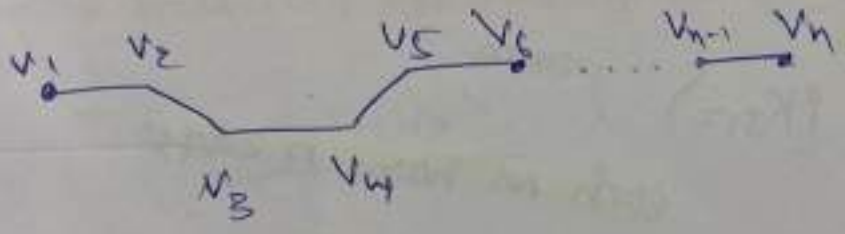
- all vertices have degree 'k', then the graph is called an n-regular graph

2) Line Graph (L_n)

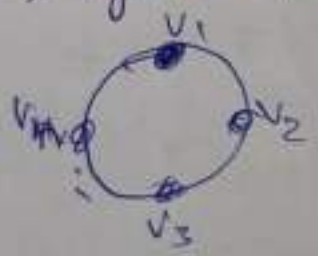
n vertices, n-1 edges in sequence

$G = (V, E) \quad V = \{v_1, v_2, \dots v_n\}$

$E = \{(v_1, v_2), (v_2, v_3) \dots (v_{n-1}, v_n)\}$



3) Cycle Graph (C_i)



$\deg(v) = 2$

$|E| = n$

Line graph with "closing the chain": $+ (v_n, v_1)$.

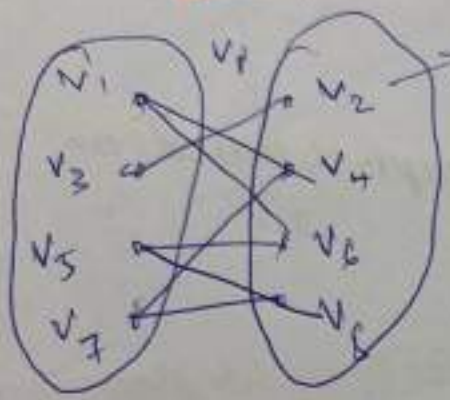
4) Bipartite Graphs ($B_{m,n}$)

- Set of vertices can be partitioned into two disjoint sets s.t. all edges in the graph go from vertices in one set to the other.

↓

no edges between two vertices in the same set.

$V = V_1 \cup V_2$ (V_1, V_2 are disjoint)



V_1 → V_2.

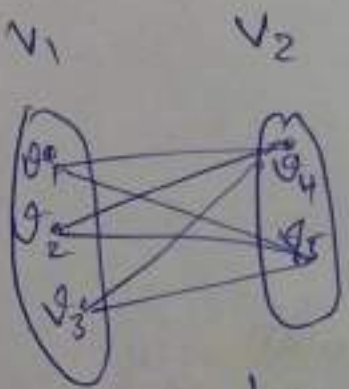
* functions are a kind of bipartite graphs.

$E \subseteq V \times V$

$E \subseteq V_1 \times V_2$.

5) Complete bipartite graphs $K_{m,n}$;

- every vertex in V_1 is connected to every vertex in V_2.



$K_{3,2}$

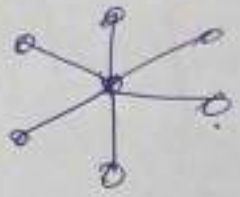
each m has n edges

$\therefore |E| = mn$

for $K_{m,n}$ $\deg(v) = n$.
$v \in V_1$

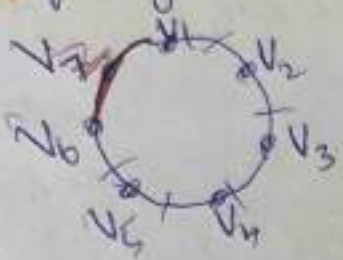
$\deg(v) = m$.
$v \in V_2$

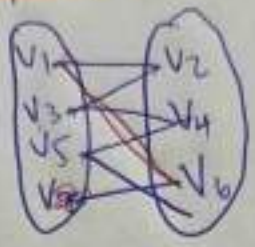
$E = V_1 \times V_2$.



$K_{1,6}$ (bipar complete bipartite)

- cycle graphs are bipartite





C_6 is bipartite.
C_7 is not bipartite.

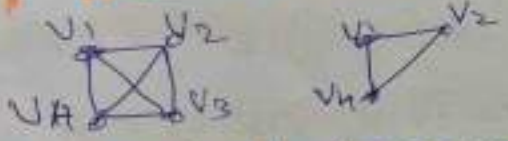
- two graphs which may look different may be the same.

Operations on Graphs

(1) Sub-Graphs $G_1(V, E)$

$H = G_1(W, F)$ s.t. $W \subseteq V$

$F \subseteq E$.



- if $H \neq G_1$, H is a proper sub-graph of G.

$G_1 = \{(V_1, V_2)\ (\text{etc.}) \ldots\}$

- always write all the edges of V as ordered pair to make it easier?

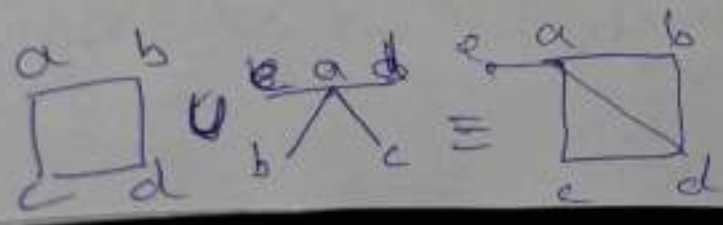
(2) Union of two simple Graphs

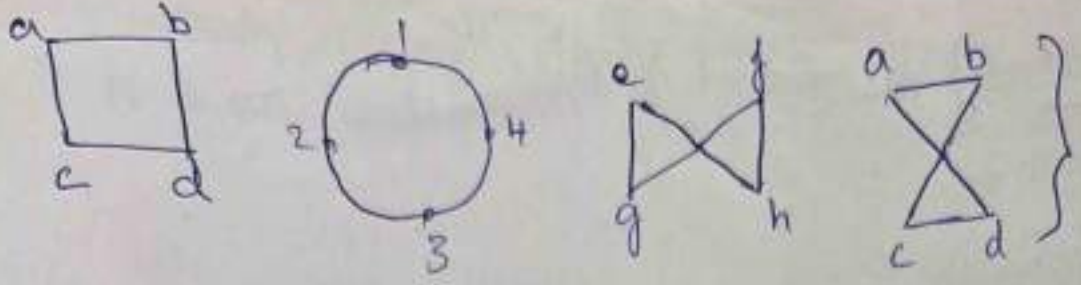
$G_1(V_1, E_1)$, $G_2(V_2, E_2)$

$K = G_1 \cup G_2$.

$K(V_1 \cup V_2, E_1 \cup E_2)$.

write $V_1 = \{\ldots\}$
$V_2 = \{\ldots\}$
$E_1 = \{\ldots\}$
$E_2 = \{\ldots\}$
take their Union.





isomorphic graphs

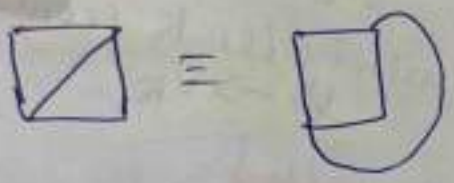
Graph Isomorphisms

- the above graphs are the same (= relabelling of vertices)

- a → 1
  b → 2
  c → 3
  d → 4

  one-to-one correspondence (bij) b/w vertices of the first graph and second graph.

  • many

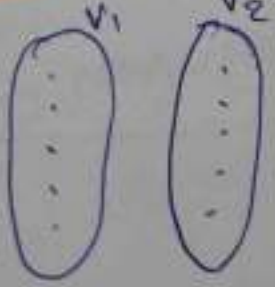


- if $G_1(V_1, E_1)$ and $G_2(V_2, E_2)$ are graphs, then we say G_1 is isomorphic to G_2 ($G_1 \cong G_2$) iff ∃ a bijection $f: V_1 \to V_2$ s.t. for any two vertices (u, v) in the first graph G_1, if u, v are adjacent in G_1 then $f(u), f(v)$ are also adjacent in G_2.

  ↳ same no. of edges, same degree

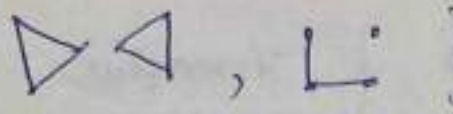
- graphs of n vertices, how many bijections are possible $f: V_1 \to V_2$?

  n! bij.



in the mapping $f: V_1 \to V_2$.
v and f(v) must have
i) same degree
ii) same no. of edges
iii) same no. of vertices

} if not non-isomorphic.

-  } disconnected graphs.

- Graph Connectivity:

- **Path:**
  - ↳ go from vertex to vertex along edges only.
  - ↳ a path has a certain length
  - ↳ paths are sequences of vertices → connected via edges. ~~that start and end~~

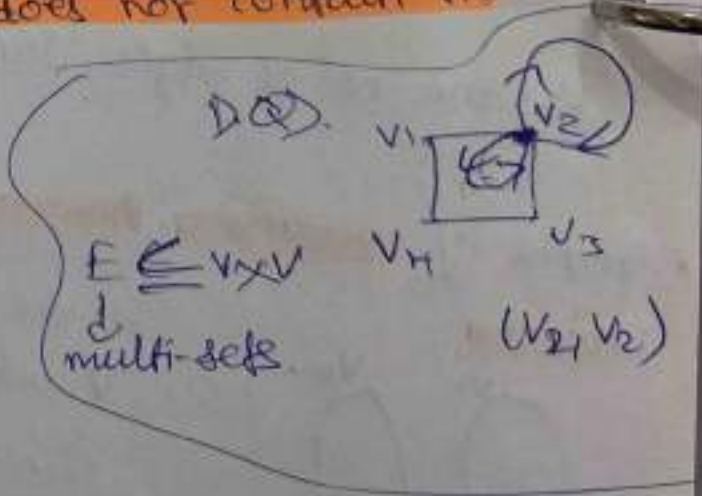
* Let $k \in \mathbb{N}_0$ and G, an undirected graph. Then a path is a sequence of vertices $v_0, v_1, v_2, \dots, v_k$ and edges $(v_0, v_1)(v_2, v_2)(v_2, v_3) \dots (v_{k-1}, v_k)$ s.t. $(v_i, v_{i+1}) \in E \ \forall \ 0 \le i \le k-1$
  - ↳ path of len k from $v_0 \to v_k$.

- Length of a path is the no. (word) of edges traversed.

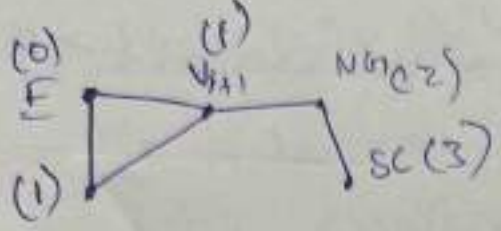
* A path of length >0 that begins and ends at the same vertex is called a circuit / cycle.

* A path is called simple if it does not contain the same edge twice.
  - ↳ travel distinct edges only.

- in an undirected graph
  $(b,c) = (c,b)$



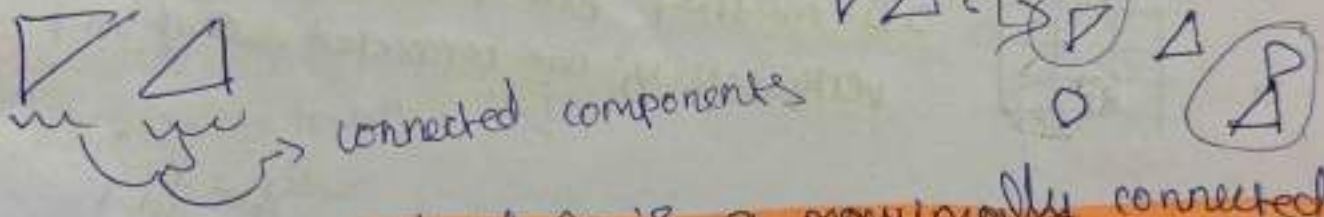
- We can define a "Collab. graph".
  - it is an undirected graph
  - Erdos number.



(1) if directly

Erdos number - length of the shortest path b/w Erdos and any researcher.

* An undirected graph is called connected if there is a path between every pair of distinct vertices of the graph.



connected components

A connected component of G_1 is a maximally connected subgraph of G_1.

① Sub. ② connected ③ Have connected any more V/E to sub while preserving connectivity.

↳ there is no other proper subgraph of G_1 which contains the connected components.

v_1 —— v_2 is a subgraph, not a connected component as we can add v_3 and connect it.

- any connected ~~subgraph of~~ G_1 is a connected component.

• Claim: There is a simple path between every pair of distinct vertices in a connected graph.

Proof:

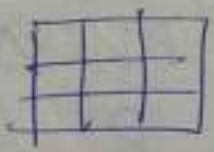
Let $x_0, x_1, \ldots, x_n$ be a path of the shortest length b/w u & v.

then it is a simple path.

Prove by contradiction;

Say it was not simple path → ∃ repeated edges.

• how would you input a graph to a computer?



2D-matrix, put 1 in a[i][j] if vertices v_i, v_j are connected, 0 if not.

• If $|V| = n$,

A_G is an $n \times n$ matrix (adjacency)

$$a_{ij} = \begin{cases} 1, \text{ if } (v_i, v_j) \in E \\ 0, \text{ otherwise} \\ x, \text{ if its a multigraph} \end{cases}$$

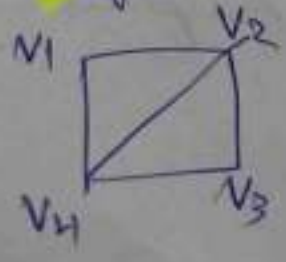
→ x represents the no. of edges b/w (v_i, v_j)

↗ then E becomes a multiset.

• for non directed graphs if $(v_i, v_j) \in E$, then $(v_j, v_i) \in E$.

∴ A_G will be a symmetric matrix.

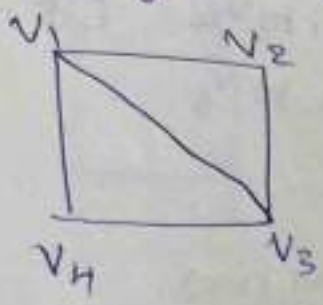
• diagonal elements = 1 if self loops exist.



$$\begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

- incident matrix, laplacian matrix, are ways of representing graphs

Counting K-length paths b/w Vertices



how many 3-length paths exist b/w V_1, V_4?

(V_1, V_2, V_3, V_4)

(V_1, V_4, V_1, V_4)

$\vdots$ many.

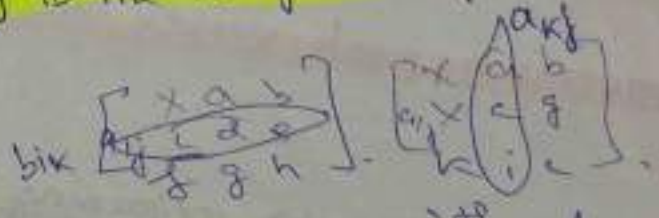
→ * adjacency matrix helps us in counting this.

Claim: if A_G is the adjacency matrix of G, then the # k-length paths b/w v_i and v_j is given by the $(i,j)^{th}$ entry of A_G^k.

Proof by induction:

1) $k=1$; path of length 1 is just an edge.
∴ it holds

2) assume $(i,r)^{th}$ entry of A_G^k is the no. of k-length paths b/w (v_i, v_r) (b_{ir})



3) $A_G^{k+1} = A_G^k \cdot A_G$

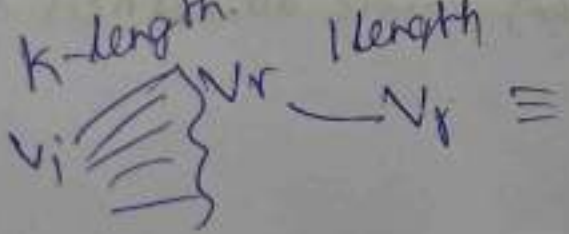
$(A_G^k)_{ij} = b_{ij}$

$(A_G^{k+1})_{ij} = C_{ij} = \sum_{r=1} b_{ir} \times a_{rj}$

need to look at all k length paths possible (all diff V_r).

b_{ir}: k length

a_{rj}: and 1 length. (entry from A_G).



$\equiv$ (k+1) length (v_i, v_j) path.

$$c_{ij} = \sum_{r=1} b_{ir} \times a_{rj} = b_{i1} \times a_{1j} + b_{i2} \times a_{2j} + \dots$$

path of len k from v_i to v_1 and path of len 1 from v_1 to v_j $\Rightarrow$ path of len $k+1$ from v_i to v_j

OR v_i to v_2 OR ...
v_2 to v_j

Sum over r_i need to consider all intermediate vertices.

- Spectral graph theory, eigen values/vectors.

Euler and Hamilton Circuits

- Can we travel along the edges of a graph ~~and return~~ starting at v_0 and return to it by

(Q1) traversing each edge exactly once (eulerian ckt)

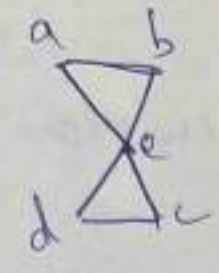
(Q2) traversing each vertex exactly once

Q1) Euler Ckt: Simple ckt containing every edge of G.

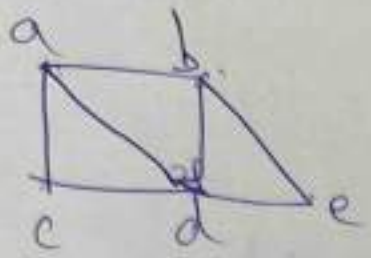
Euler Path: Simple path (not a ckt) containing every edge of G.

Q2) Hamilton Ckt: Simple ckt that passes through every vertex exactly once.

Hamilton path: Simple path (not a ckt) covers all vertices of the graph exactly



(a, b, e, c, d, e, a)
euler ckt ✓



(a, c, d, e, b, d, (a, b) euler path.
(a, b, d, c, a, d, e, b) euler path.

* A connected ~~pe~~graph has an Eulerian circuit iff every ~~ver~~vertex of the graph has even degree.

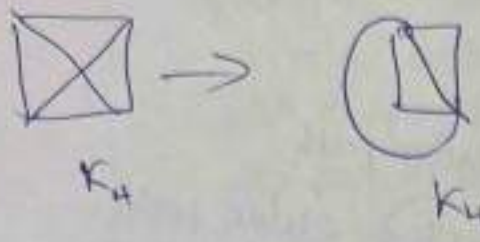
(5 for any intermediate ~~edg~~ vertex, if an edge enters it, an edge must

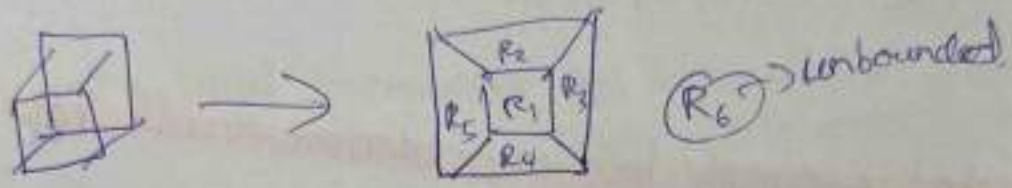
* A connected graph has an eulerian path (not a ckt) iff every vertex has even degree except the starting and ending vertices.

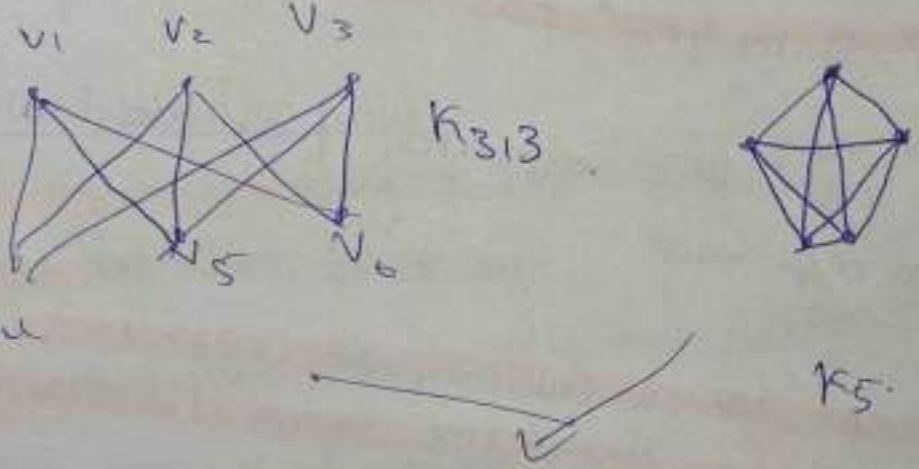
• Konigsberg's bride problem (not a Eulerian ckt)

Planar Graphs

- no two edges should cross, while drawing the graph on the plane

- 

- 

- 

If we remove a single vertex,
they become planar.

- If for any (connected ~~graph~~) planar simple graph Gr of $|V|$ vertices and $|E|$ ~~vertices~~ edges, $r = |E| - |V| + 2$ (r = no. of regions).
- degree of regions - ~~how many edges do you~~ len of path to encircle the region with a circuit.
- $\sum_{i,\, R_j \in R} \deg(R_i) = 2|E|$

- Let G be a connected simple planar graph

(i) with $|V| \geq 3$ then $|E| \leq 3|V| - 6$.

OR

(ii) with $|V| \geq 3$ and no cycles of length 3 then $|E| \leq 2|V| - 4$.

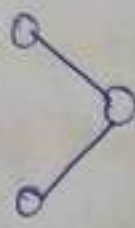
Trees

Chapter 10: Trees

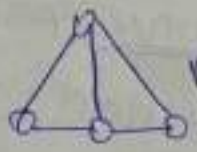
→ what?, examples, theorems, Applications.

"You don't pluck a flower with an axe."

- Special kind of graphs:
- Tree = A connected, acyclic graph.
  - ↳ simple circuit = cycle
    acyclic no simple
- Sort of captures the min. no. of edges required to draw a graph?
- Examples of trees:

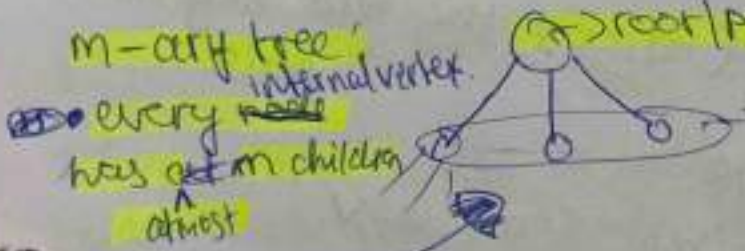


tree ✓,



not a tree. if we added an extra edge only, it does not become a tree.

e.g. of trees we already know! Recursion tree, family tree,



(every binary tree is also a trinary tree)

- Rooted tree; ~~every no~~
  - ↳ every node at least
- Search trees, segment trees, red-black trees, Splay trees, Hoffman trees, Phylogenetic Trees?.
- for ~~connected~~ directed graphs, check the underlying undirected graph

- Theorem 1: A graph is a tree iff any two nodes are connected by exactly one and only one path. (simple path)
  (I) (II) the

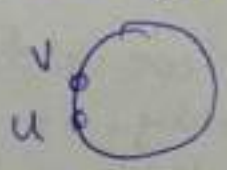
Proof:

i) if part; → unique path: ∃ only 1 path b/w/two the nodes

if any two nodes are connected by a unique path, then the graph is a tree. Prove.

∀ any two nodes are connected ✓ 1st cond met. (uniquely)

Let a cycle exist. Prove by contradiction.



⇒ ∄ a unique path

contradiction.

ii) only if part;

Or is a tree:

⇒ 2 nodes are connected (∃ a path b/w any two nodes)

↳ let it not be unique

⇒ 2 paths exist b/w some u, v.

⇒ a cycle exists

∴ not a tree

∴ the two nodes are connected only by one path.

∎

- Theorem 2: ~~Every node has a unique parent~~
Every tree on n nodes has exactly (n-1) edges.

Proof: Induction on n. (~~Strong~~).

n=1, |E|=0 ✓

Suppose every tree on k nodes has (k-1) edges

Consider a tree on (k+1) nodes

(leaves are nodes which do not have children)

take any rooted tree.

If the tree is finite, there must exist a leaf.

(If no leaf, every node has children → ∞ tree)

↓

Delete a leaf node from tree T, to get T'

T' is also a tree (∃ a unique path b/w any two nodes)

T' is a tree with k nodes → has (k-1) edges

∴ add back 1 edge + 1 node that we deleted.

∴ k+1 nodes → k edges. // □.

Alternatively:

Start with n nodes (isolated) as a forest of n trees, where each tree is a node.

add an edge without creating a cycle

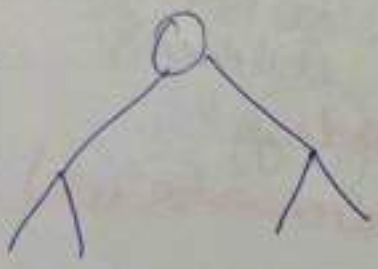
↳ edge must connect 2 trees only. Then these 2 trees become 1 tree.

how many edges do we need to add so that the forest becomes one tree → (n-1 edges).

Tree Traversals

- arrays take linear time to search
  same array if stored as a binary search tree, takes only log n time

- Traversal ~~algorithms~~: pre-order, in-order, post-order.
  n! ways of printing a tree
  (n nodes ---- print 1 → (n-1) left etc.)



i) Root first → pre-order
   recurse leftwards
   recurs rightwards

ii) recurse left
   visit root
   recurse right
   ↓ in-order

iii) recurse Left
   recurse right
   visit root
   ↓ post-order

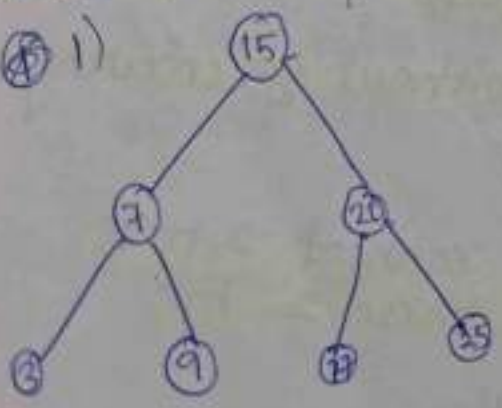
ways to visit all nodes.

(nomenclature based on position of root wrt recursion)

binary search tree:
for every node, every value in its right subtree is greater.

- Examples.

(A) i)



balanced - full binary tree
(BST sort).

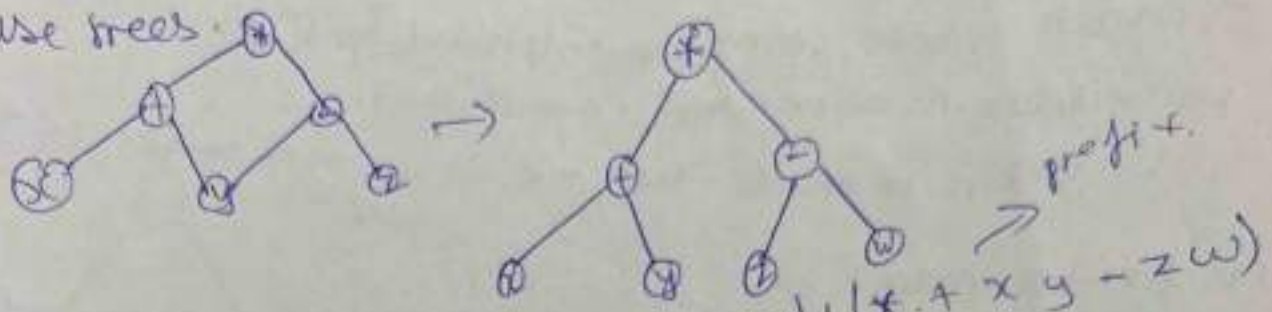
i) Pre order traversal
15, 7, 3, 9, 20, 17, 25

ii) In-order traversal:
3, 7, 9, 15, 17, 20, 25.
(sorted the array)

iii) Post-order Traversal:
3, 9, 7, ~~20~~ 17, 25, 20, 15.

• Instead of a BST, we use arithmetic expression

(x+y) * (z-w) → we needn't use parenthesis if we use trees.



pre-order traversal: (* + x y - z w)

post order traversal: x y + z w - * postfix

order traversal: x + y * z - w → need ( )
infix.

• Only 3 famous traversals
Others (n!-3) are too cryptic. (no order at all)

• comparison, addition, multiplication.
↓ one pass
↓ multiple passes
} decimal rep. is the most efficient we know.

(decimal system is just a representation).
IN is not 1, 2, 3...
17, 3 is a representation of IN only, but not the concept of IN.

• in ML & and AI, multiplication is the most frequent operation.

* pre and post order traversals only can be generalised for ternary trees.
⇒ ∄ multiple in-order traversals.

Huffman Tree / Code

E.g.) abaaacabbaacadb

Q) encode above string into alphabet of {0,1}.

Naive Solution: a=00, b=01, c=10, d=11.

↳ 30 bits to encode. Can we do it in a smaller no. of bits.

- Pre-fix free codes:

  i) one codeword should not be the prefix of another code word.

  if a=0, b=00. confusion arises.

- a=0

  0 1 0 0 0 0 0 11 0 00

  a b a a a c

  8 a's 8
  4 b's 8
  2 c's 6
  1 d 3

  } 25 bits.

  wt

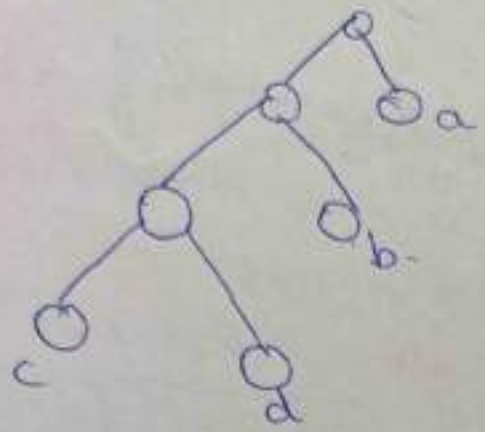
- w(a) = 8
  w(b) = 4
  w(c) = 2
  w(d) = 1

  $\frac{w(x)}{\text{len. of str}} = \text{freq.}(x)$

- Leaves only can be ~~trees~~ codes. Internal vertices cannot be vertices.

i) Each leaf is a char. ∴ (4 leaves)

ii) needs to minimize (8 * len(root to a)) + 4 * (len(root to b)) ... -



a = 1
b = 01
c = 000
d = 001

25 bits at best.

$x_1, x_2, \ldots, x_n$ (list of alphabets)

frequencies $f_1, f_2, \ldots, f_n$.

$f_i = \frac{\text{occ}(x_i)}{L}$

Find i, j s.t. f_i, f_j are last two least frequencies.

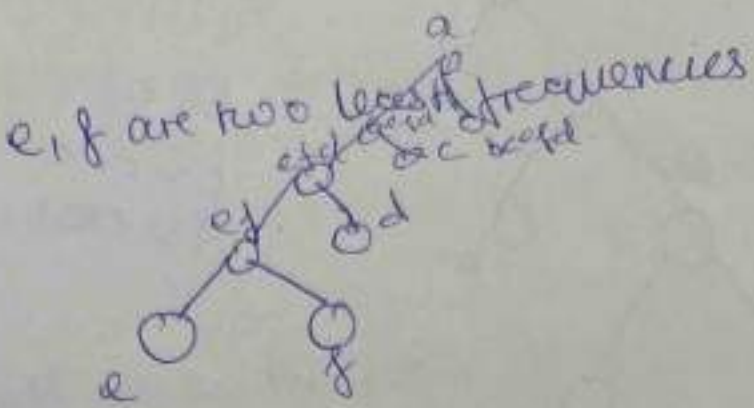
build a tree with x_i, x_j as the bottommost leaves

$f_{ij} = f_i + f_j$

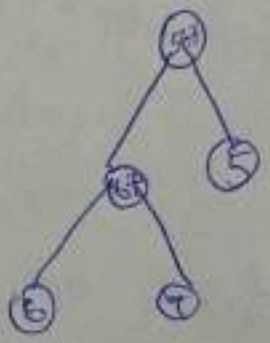
recursive soln.

- 32 a's
  17 b's
  9 c's
  7 d's
  2 e's
  1 f.
  ---
  68 = L

6 alphabets = n.



- x_1: $w(x_1) = 19$
  x_2: $w(x_2) = 17$
  x_3: $w(x_3) = 16$
  $x_4 = w(x_4) = 13$
  $x_5 = w(x_5) = 12$
  $x_6 = w(x_6) = 7$
  $x_7 = w(x_7) = 5$
  ---
  8 9 = L.



Basics of Modular Arithmetic

- $4 \equiv -1 \pmod 5$

- Find all n if $11 \equiv 5 \pmod n$.

  if $a \equiv b \bmod n$ then $n \mid a-b$

  $\Rightarrow n \mid 11-5 \Rightarrow n \mid 6$.

  $n = 1, 2, 3, 6$ $n > 1$ strictly for modular arithmetic

  $\therefore \boxed{n = 2, 3, 6}$

- divide a by n, leaves quotient q, rem r.

  $a = q \cdot n + r$.

  $a - r = q \cdot n \Rightarrow n$ divides $a - r$

  $a = qn + r \Rightarrow \boxed{a \equiv r \pmod n}$ //

  ↳ eg.) divide 13 by 5; $\underset{a}{13} = \underset{n}{5} + \underset{q}{2} + \underset{r}{3}$

  divide by $n \Rightarrow \bmod n \Rightarrow \bmod 5$

  $13 \equiv 3 \pmod 5$.

  using this basically.

  $\bmod n$ world $\Rightarrow \{0, 1, 2, \ldots, n-1\}$ as possible nos.

- $2 \equiv -3 \pmod 5$
  $-8 \equiv 7 \pmod 5$
  $-3 \equiv -8 \pmod 5$
  } all true check using $a \equiv b \pmod n \Rightarrow n \mid a-b$ interpretation.

- can add, subtract, and multiply (exponentiate) congruences, same way as normal arithmetic.

  ↳ e.g.) Solve $x^2 + 3 \equiv 0 \pmod 7$.

  $x^2 \equiv -3 \pmod 7 \Rightarrow 7 \mid x^2 + 3$

  $x^2 \equiv 4 \pmod 7 \Rightarrow 7 \mid x^2 - 4$

  take $\sqrt{}$ only. $\boxed{x \equiv 2 \pmod 7}$?

  $\rightarrow x \equiv -2 \pmod 7 \Rightarrow \boxed{x \equiv 5 \pmod 7}$ //.

  add 7 to 3. but 0 to LHS.

  $\rightarrow nk \equiv 0 \pmod n$

• Dividing over congruences may be problematic.

↳ eg. $10 \equiv 4 \pmod 6$. $\quad 5 \equiv 2 \pmod 3$.

$\downarrow$

$5 \equiv 2 \pmod 6$. ✗WRONG.

↳ dividing both sides including n too holds the congruence. if a, b, n have common factors

Q) Solve $x^2 \equiv 2 \pmod 4$ ⇒ Quadratic residues?

↳ What no. in $(\bmod 4)\ \{0,1,2,3\}$ when squared is congruent to 2 in mod 4.

the only possible x's even allowed is $\{0, 1, 2, 3\} \in x$

x^2 for this in $(\bmod 4)$ is $\{0, 1, 0, 1\} \in x^2$

∴ never going to be congruent to $2 \pmod 4$

∴ no soln.

* A perfect sqr can never be congruent to 2 mod 4

$ax \equiv ay \pmod n \rightarrow x \equiv y \pmod n$ iff $\gcd(a, n) = 1$

Q) $3x \equiv 1 \pmod 5$

• fractions are not defined.
multiply both sides by inverse of 3.

$3^{-1} \cdot 3x \equiv 3^{-1} \cdot 1 \pmod 5$

$x \equiv 3^{-1} \pmod 5$

↳ the no. we are looking for is the "inverse of 3 (mod 5)"

↳ $3x \equiv 1 \pmod 5$

↳ inverse of $a \pmod n$ exists iff $\gcd(a, n) = 1$

used this here.

OR

$3x \equiv 1 \pmod 5$

$3x \equiv 6 \pmod 5$ ∵ a, b ~~have a common factor and n does not, division works here?~~

→ $x \equiv 2 \pmod 5$ //

Chinese Remainder Theorem

- used to solve a bunch of congruences with one variable but different moduli which are ~~to~~ prime (relatively).

$$\left.\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\cdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}\right\} \; m_i\text{s are all relatively prime to each other}$$

$\exists$ a unique x satisfying these congruences.

$$x = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1} + \cdots + a_n M_n M_n^{-1}) \pmod{M}.$$

a_is are given already.
find M and M_i

- eg.)

$$\left.\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 2 \pmod 7 \end{aligned}\right\} \Rightarrow x \equiv (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \pmod{M}.$$

$x \equiv$

$\rightarrow \cdots (3,5,7)$ relatively prime.

How to find M and M_i and M_i^{-1}?

① $M = m_1 \times m_2 \times m_3 \times \cdots \times m_n$ { product of all moduli (n) }

$\Rightarrow M = 3 \times 5 \times 7 = 105$

② $M_1 = \frac{M}{m_1}$, $M_2 = \frac{M}{m_2}$, $M_3 = \frac{M}{m_3}$ ..... $M_i = \frac{M}{m_i}$

$\Rightarrow M_1 = 35$, $M_2 = 21$, $M_3 = 15$

③ $M_i \times M_i^{-1} = 1 \pmod{m_i}$

$M_1 \times M_1^{-1} \equiv 1 \pmod{m_1}$
$35 \times M_1^{-1} \equiv 1 \pmod 3$
$M_1^{-1} = 2$ *

* { can do extended euclidean algorithm }

$M_2 \times M_2^{-1} = 1 \pmod{m_2}$
$21 \times M_2^{-1} \equiv 1 \pmod 5$
$M_2^{-1} = 1$

$M_3 \times M_3^{-1} \equiv 1 \pmod{m_3}$
$15 \times M_3^{-1} = 1 \bmod 7$
$M_3^{-1} = 7$.

How to find Inverse Modulo?

eg) $27^{-1} \pmod{392}$ ans $\in \{0, 1, 2, \ldots, 391\}$.

$27^{-1} \pmod{392} \Rightarrow 27 \cdot x \equiv 1 \mod(392)$; x is 27^{-1}

$392 = (27) \times 14 + (14)$

$27 = (14) \times 1 + (13)$

$14 = (13) \times 1 + 1$

$14 - 13 \cdot 1 = 1$

① — $14 + 13(-1) = 1$

② — $27 + 14(-1) = 13$.

③ — $392 + 27(-14) = 14$.

write above 3 eqn like this after hitting $r = 1$.

Sub for 13 in ① from ②:

$14 + [27 + 14(-1)](-1) = 1$ simplify.

$14 - 27 + 14 = 1$.

$2(14) + 27(-1) = 1$ replace 14 with ③.

$2[392 + 27(-14)] + 27(-1) = 1$ simplify.

$2(392) + 27(-28) + 27(-1) = 1$

$2(392) + 27(-28) = 1$ $\pmod{392}$ throughout.

replace -28 into the right $\pmod{392}$ form

$2(392) + 27(363) = 1 \pmod{392}$

$2(392) \equiv 0 \pmod{392} \Rightarrow 27 \cdot 363 = 1 \pmod{392}$

$\Rightarrow 27^{-1} \mod(392) = 363$.

* inverse only exists i.e. $a^{-1} \pmod{n}$ exists only when $\gcd(a, n) = 1$.

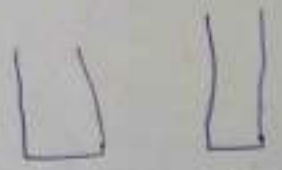
Modular Arithmetic

- $a \equiv b \pmod{n}$

  when we divide a with n, we get the remainder b

  $a \equiv b \pmod{n} \iff n \mid a-b$

- Puzzle:



3L jar 5L jar

Measure exactly 1L

Soln: $3x+5y=1,\ x,y \in \mathbb{Z}$

- 

3L 6L

$3x+6y=1$ has no soln!!!

LHS is a multiple of 3

- $ax+by = \gcd(a,b)$

  soln exists.

Understanding GCD

- consider a,b s.t $a \geq b$

  $GCD(a,b) = ?$

  $a = p \cdot q$; p,q are 500 dig primes

  $b = p \cdot r$; "

Thm: Assume $a \geq b$

Then $GCD(a,b) = GCD(b, a \bmod b)$

Proof:

$c|a$ and $c|b$ (c is a common divisor).

Then $c|a \bmod b = a - mb = ck_1 - mck_2 = c(\cdot)$

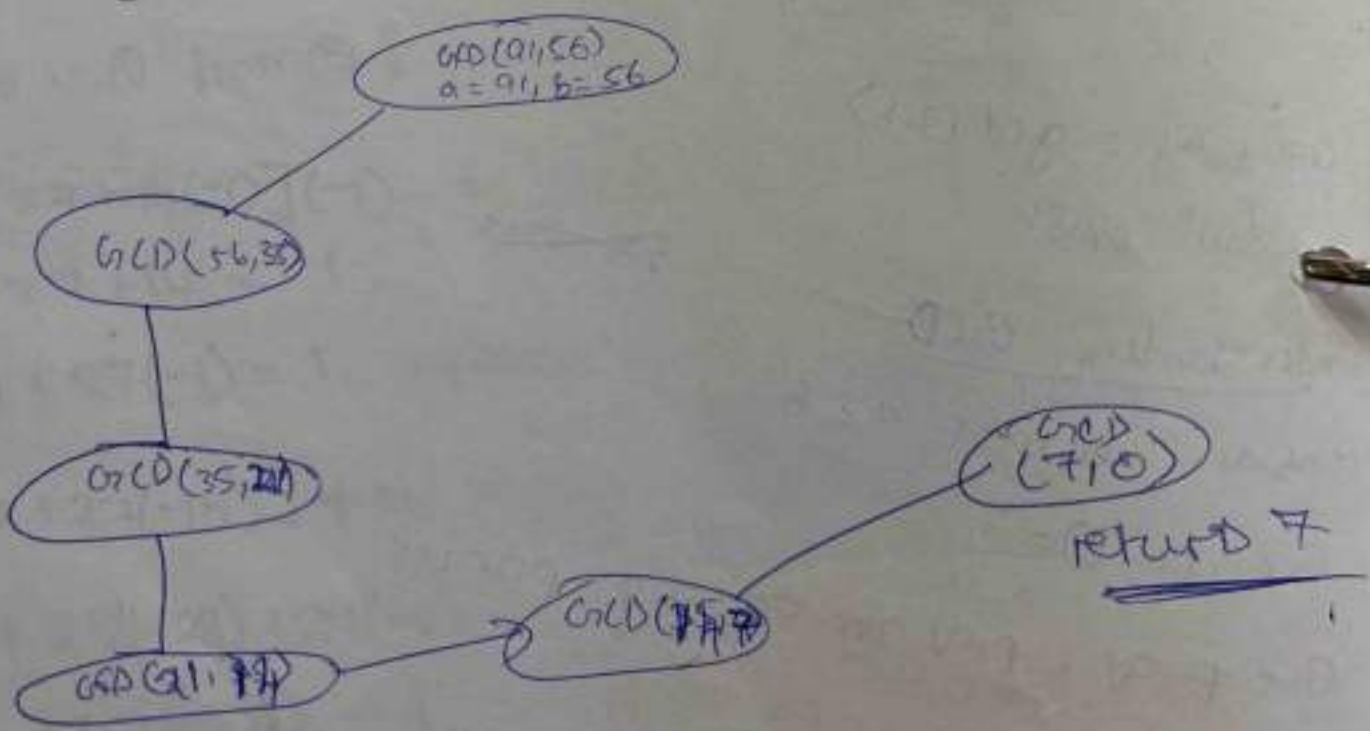
GCD Algorithm: Euclid's Algorithm.

$a \geq b$,

```
GCD(a, b)
    if (b == 0)
        return a;

    else
        return (GCD(b, a%b));
```

e.g.) GCD(91, 56)



Thm: The euclid's GCD Algorithm takes $\leq 2\log_2(\min(a,b))+1$ steps

Proof:

$GCD(a,b) \rightarrow gcd(b, a \cdot 1 \cdot b)$

note: $a \cdot 1 \cdot b \leq \frac{a}{2}$

$\rightarrow b \geq \frac{a}{2}$, $a \cdot 1 \cdot b = a - b \leq \frac{a}{2}$

$\rightarrow b \leq \frac{a}{2}$, $a \cdot 1 \cdot b < b \leq \frac{a}{2}$.

$GCD(a \cdot 1 \cdot b,\ b \cdot 1 \cdot (a \cdot 1 \cdot b))$

$\log_2 a$ steps (2 at a time)

$\leq 2\log_2 a$

$O(\log(\min(a,b)))$ time.

e.g.) $a = 91,\ b = 56,\ gcd = 7$

$91x + 56y = 7$

$91 = 56 + 35$

$56 = 1 \cdot 35 + 21$

$35 = 1 \cdot 21 + 14$

$21 = 1 \cdot 14 + 7$ gcd

$14 = 2 \cdot 7 + 0$

$7 = 1 \cdot 21 - 1 \cdot 14$

$\Rightarrow 21 = 1 \cdot 35 - 1 \cdot 14$

$35 = 91 \cdot 1 - 56 \cdot 1$

$21 = 1 \cdot 56 - 1 \cdot 35$

$21 = 1 \cdot 56 - (1 \cdot 91 - 56 \cdot 1)$

$21 = 2 \cdot 56 - 1 \cdot 91$

$56^{-1} \bmod 91$

$91 = 56 \cdot 1 + 35$

$56 = 35 \cdot 1 + 19$

$35 = 19 \cdot 1 + 16$

$19 = 16 \cdot 1 + 3$

$16 = 3 \cdot 5 + 1$

$16 + 3(-5) = 1$ restart

$19 + 16(-1) = 3$

$35 + 19(-1) = 16$

$56 + 35(-1) = 19$

$91 + 56(-1) = 35$

$16 + (19 + 16(-1))(-5) = 1$

$1(56) + 19(-5) = 1$

$(35 + 19(-1))6 + 19(-5) = 1$

$35(6) + 19(-11) = 1$

$35(6) + (56 + 35(-1))(-11) = 1$

$35(6) + 56(-11) + 35(11) = 1$

$56(-11) + 35(17) = 1$

$56(-11) + (91 + 56(-1))(17) = 1$

$56(-28) + 91(17) = 1$

$56 \cdot 63 = 1 \bmod 91$

Chinese Remainder Theorem

- Solve; $x \equiv a_1 \pmod{n_1}$ Assume n_i's are relatively prime.
  $x \equiv a_2 \pmod{n_2}$
  $\vdots$
  $x \equiv a_k \pmod{n_k}$
  - - - - - - -

e.g.) number $x \leq 100$

$x \cdot 1 \cdot 2 = 0$ ⇝ even no. ≤ 100
$x \cdot 1 \cdot 3 = 1$ ⇝ even $3k_1+1 \Rightarrow k_1 =$ odd.
$x \cdot 1 \cdot 5 = 2 \Rightarrow$ even $5k_2+2 \Rightarrow k_2 =$ odd.
$x \cdot 1 \cdot 7 = 3 \Rightarrow$ even $7k_3+3 \Rightarrow k_3 =$ odd.

(52)

$x = 3k_1+1 = 5k_2+2 = 7k_3+3$

$3k_1+1 = 5k_2+2$

Solution: Natural method;
$x < 210$

if $x \cdot 2 = 0$
$x \cdot 3 = 0$ $\Rightarrow x \cdot 210 = 0$ $\therefore x = 210z; z \in \mathbb{Z}$
$x \cdot 5 = 0$
$x \cdot 7 = 0$

$\therefore x \equiv 0 \pmod{210}$
x is any no. that gives rem 0

if $x \cdot 2 = 1$
$x \cdot 3 = 0$
$x \cdot 5 = 0$ ⇢ $x \cdot 105 = 0$
$x \cdot 7 = 0$

$\therefore x \equiv 0 \pmod{105}$

$x \equiv 105 \pmod{210}$

if $x \cdot 2 = 0$
$x \cdot 3 = 1$ ⇒ $x \equiv 70 \pmod{210}$
$x \cdot 5 = 0$
$x \cdot 7 = 0$

if $x \equiv 0$
$x \equiv 3 = 1$
$x \equiv 5 = 1$
$x \equiv 7 = 0$.

$x \equiv 126 \pmod{210}$

if $x \equiv 2 = 0$
$x \equiv 3 = 0$
$x \equiv 5 = 0$
$x \equiv 7 = 1$

$x \equiv 120 \mod 210$

$[0,1,2,3] = 0[1,0,0,0] + 1[0100] + 2[0010] + 3[0001]$

$= [70 + 2(126) + 3(120)] \mod 210$.

$= 70$
252
360
682

$(682) \mod 210$
$= 52 \pmod{210}$ //.

If $x \equiv 2 = 1$
$x \equiv 3 = 2$
$x \equiv 5 = 4$
$x \equiv 7 = 3$.

$[1,2,4,3] = 1[1000] + 2[0400] + 4[0010] + 3[0001]$

420

$= (105 + 2(70) + 4(126) + 3(120)) \mod 210$

$105 + 140 = 35 \mod 210$.

504
420
84

84
$119 \mod 210$.
150
$269 \Rightarrow 59$.

360
210
150

$x \equiv 59 \pmod{210}$

$N = \prod_{i=1}^{k} n_i$

x_i be s.t. $\frac{N}{n_i} x_i \bmod n_i = 1$

$$\left\{ a_1 \left[\frac{N}{n_1} \cdot x_1\right] + a_2 \left[\frac{n}{n_2} \cdot x_2\right] + \cdots + a_k \left[\frac{N}{n_k} \cdot x_k\right] \right\} \bmod N.$$

$$x \equiv \sum_{i=1}^{k} a_i \left[\frac{N}{n_i} x_i\right] \pmod N$$

$\frac{N}{N_1} \cdot x_i \pmod{n_i} = 1$ solve for x_i

if $g = GCD(a,b)$, $ax + bY = g$ (prev. Thm)

$GCD\left(\frac{N}{n_i}, n_i\right) = 1$

$\therefore \frac{N}{n_i} \cdot X + n_i Y = 1$ $\exists$ some x, y. for this to hold,

$\exists x, y \in Z$ s.t. $\left(\frac{N}{n_i} x + n_i Y = 1\right) \Rightarrow \frac{N}{n_i}$ $x_i = x$.

$ax + by = 1 \Rightarrow ax = 1 \pmod b$

$x = a^{-1} \pmod b$ $\frac{1}{a}$

$\therefore x_i \equiv \left(\frac{N}{n_i}\right)^{-1} \bmod (n_i)$ ~~n_i should not be n~~

$$x \equiv \sum_{i=1}^{k} a_i \cdot \left[\frac{\prod_{\delta=1}^{k} n_\delta}{n_i} \left(\frac{\prod_{j=1}^{k} n_i}{n_i} \right)^{-1} \pmod{n_i} \right] \pmod{\prod_{j=1}^{k} n_j}$$

$x \cdot 1 \cdot 2 = 0$

$x \cdot 1 \cdot 3 = 1$

$x \cdot 1 \cdot 5 = 2$

$x \cdot 1 \cdot 7 = 3$

$$x \equiv 0[\,] + 1 \cdot \left[\frac{2 \cdot 3 \cdot 5 \cdot 7}{3} \cdot \left(\left(\frac{2 \cdot 10}{3}\right)^{-1} \bmod\right.\right.$$

$30^{-1} \bmod 7$

$2^{-1} \bmod 7$

$\equiv 4.$

Q) $x \equiv 13 \pmod{17}$.

$x \equiv 7 \pmod{19}$

$$x \equiv 13\left[\frac{17 \cdot 19}{17}\left(\left(\frac{17 \cdot 19}{17}\right)^{-1} \bmod 17\right)\right] + 7\left[\frac{17 \cdot 19}{19}\left(\left(\frac{17 \cdot 19}{19}\right)^{-1} \bmod 19\right)\right]$$

$\bmod (17 \cdot 19)$.

$$x \equiv 13[19(2^{-1} \bmod 17)] + 7[17(17^{-1} \bmod (19)] \bmod (17 \cdot 19)$$

$$x \equiv 13 \cdot 19 \cdot 9 + 7 \cdot 17 \cdot 9.$$

$17 \cdot y = 1 \bmod 19$

$17x = 19y + 1$

$$x \equiv 64 \pmod{323}.$$

- $\phi(n)$ euler totient function.

  It counts the no. of +ve integers less than and co-prime to n.

  if $n = a_1^{k_1} a_2^{k_2} a_3^{k_3}$ a_i primes.

$$\phi(n) = n \prod_{i=1} \left(1 - \frac{1}{a_i}\right)$$

$\phi(p)$

$a \equiv 1 \bmod p.$

Birthday Paradox

How many people are required to have a clash of birthdays with probability ≥ 0.5?

Ans: 23

Q) N objects. Picking q random objects with replacement (one at a time).

What is the probability of picking the same object again?

i) if $n=1$, $q=1$, prob $=0$. if $n=1$, $q>1$, prob $=1$

ii) if $n=10$, $q=1$, prob $=0$; if $n=10$, $q=2$, prob $=\frac{1}{10}$.

Thm: $\frac{q(q-1)}{2N} \leq P[\text{collision}] \leq \frac{q(q-1)}{2N}$.

proof:

$P[\text{no collision}] = 1 - P[\text{collision}]$.

$P[\text{NO collision}]$ is no repeated picking

$P[\text{no collision}] = P[\text{no coll. } q-1 \text{ trials}] \times P[\text{no. coll } q^{th} \text{ trial}]$

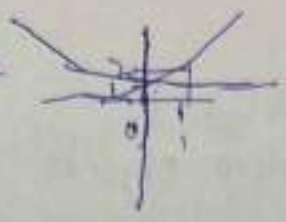
$P[\text{no collision}] = P[\text{no. coll } q-1 \text{ trials}] \times \left(1 - \frac{q-1}{N}\right)$

$P[\text{NO. collision}] = P[\text{no. coll. } q-2 \text{ trials}] \left(1 - \frac{q-2}{N}\right)\left(1 - \frac{q-1}{N}\right)$

$\therefore P[\text{NO. collision}] = \prod_{i=0}^{q-1} \left(1 - \frac{i}{N}\right)$

$P(\text{collision}) = 1 - \prod_{i=0}^{q-1} \left(1 - \frac{i}{N}\right)$.

• fact: $0 \le x \le 1$

$1 - \frac{x}{2} \le e^{-x} \le 1 - x$ 

$$P[\text{no coll.}] = \prod_{i=0}^{q-1} \left(1 - \frac{i}{N}\right).$$

$0 \le \frac{i}{N} < 1$ always.

replace $\frac{i}{N}$ with $e^{-\frac{i}{N}}$.

$$\le \prod_{i=1}^{q-1} e^{-\frac{i}{N}} = e^{-\frac{1}{N}\sum_{i=1}^{q-1} i} = e^{-\frac{q(q-1)}{2N}}$$

$$\le 1 - \frac{q(q-1)}{2N}$$

$P(A \cup B) \le P(A) + P(B)$

Q) Long GH bit prods.
How many prods need to a collision, with prob $\frac{1}{2}$.

$N = 2^{64}$ $q = ?$

$$0.5 \sim \frac{q(q-1)}{2^{87}} \le P[\text{collision}] \le \frac{q(q-1)}{2N}$$

$$2^{86} = q(q-1)$$

$$q \ge 2^{32}.$$

(d) a/c attempts for a marked fish

Recurrence Relations:

→ Taxonomy:

order	linearity	Homogeneous	Constant coeff.
First	linear	Homogeneous	const. coeff
Second	non-linear	non-homogeneous	non-const. coeff.
⋮	⋮		

properties of recurrence relations

Example: $a_1, a_2, a_3, \cdots, a_{n-1}, a_n$

$a_n = f_1(n) \cdot a_1(n) + f_2(n) \cdot a_2(n) + \cdots + f_{n-1}(n) \cdot a_{n-1}(n) + f_0(n)$.

- displaying n numbers recursively:
- displaying the n^{th} no. recursively using the previous $n-1$ terms.

(1) Order → the no. of previous terms the n^{th} term depends on.
e.g. fib(n) = fib(n-1) + fib(n-2) is a second order recurrence relation.

$a_n = a_{n-i} + x$ is i^{th} order.

$a_n = a_{n-1} + a_{n-2} + a_{n-3} + \cdots + a_{n-i}$ is also i^{th} order.

→ how far in the history we need to go to define a_n.

② Linearity: $a_n = a_{n-1} + a_{n-2}$ if variables are powers 1
(prev. terms to n, which n depends on ≡ var.)

$a_n = g(n, a_{n-1}, \dots, a_{n-i})$ order i

linear if a_{n-j}^{k} $k=1$ $\forall j \le i$

③ Homogeneity: $a_n = a_{n-1} + a_{n-2} + f(n)$
terms that don't depend on previous terms but on n.

if $f(n)=0$ → homo
$f(n) \neq 0$ → non-homo

e.g. $a_n = a_{n-1} + 5n$ non-homo.

④ Constant coeff: coeff don't depend on n.

Ex:

- 1st order: $a_n = 5a_{n-1}$
linear, homo, const. coeff. } $a_n = A5^{n-1}$
$a_1 = A$.

1st order → 1 boundary cond.
2nd order → 2 boundary cond

G.P.

- linear, homo, non-const coeff, first-order;

$a_n = n a_{n-1}$, $a_1 = A$

$f(n) = ?$ $f(1) = A$
$f(2) = a_2 = 2 \cdot A$ ∴ $f(n) = n! A$.
$f(3) = a_3 = 3 \cdot 2 \cdot A$.
$f(4) = a_4 = 4 \cdot 3 \cdot 2 \cdot A$.

$a_n = n^2 a_{n-1}$ $a_1 = A$

$f(1) = A$ $f(n) = (n!)^2 A$.
$f(2) = (2)^2 A$
$f(3) = 3^2 (2)^2 A$

- first order, non-linear, homo, const coeff

$a_n = (a_{n-1})^2$

- 1st O, non-lin, homo, non-const

$a_n = f(n)(a_{n-1})^2$

- 1st O, non-lin, non-homo, non-const.

$a_n = f(n)(a_{n-1})^2 + g(n)$; $g(n) \neq 0$

- 1st O, lin, homo, const coeff

$a_n = a_{n-1} + 2a_{n-2}$

2nd O, nonlin, non-homo, ...

- Our focus on:
second order + linear + (4) cases.

- $a_n = a_{n-1} + f(n)$: non homo. first order
$a_1 = A$. ~~$f(1) = 0$~~

~~$a_2 =$~~

If we solve these telescopically,

$a_n - a_{n-1} = f(n)$.
$a_{n-1} - a_{n-2} = f(n-1)$
$a_{n-2} - a_{n-3} = f(n-2)$
$a_{n-3} - a_{n-4} = f(n-3)$
...
$a_2 - a_1 = f(2)$

$\sum_{i=2} f(i) = a_n - a_1$

$\downarrow$

$a_1 + \sum_{i=2} f(i) = a_n$

- eg $a_n = 2a_{n-1} + n$ → first order, lin., non-homo

$a_1 = A$.

Solve by expansion:

$a_n = 2[2a_{n-2} + n-1] + n$ ⟶

$= 2[2[2a_{n-3} + n-2] + n-1] + n$

$= 2[2[2a_{n-3}$ ~~$+ n-2] + n-1] + n$~~

$2[4a_{n-3} + 2n-4 + n-1] + n$

$8a_{n-3} + 4n - 8 + 2n + 2 + n$

$8a_{n-3} + 7n - 10$

$2^3(n-3) + 2^2(n-2) + 2^1(n-1) + 2^0(n-0)$

$\forall i \; a_n = 2^i a_{n-i} + \sum_{j=0}^{i-1} 2^j (n-j)$

if $i = n-1$

$a_n = 2^{n-1} a_1 + \sum_{j=0}^{n-2} 2$

$a_n = a_n^{(h)} + a_n^{(p)}$ (P)

$a_n - 2a_{n-1} = n$.

$a_n^{(h)}$: $a_n - 2a_{n-1} = 0$ $a_n = r^n$.

$r^n - 2r^{n-1} = 0$

$r = 2 \therefore a_n^{(h)} = \alpha 2^n$ ←①

a_{np}: $a_n - 2a_{n-1} = n$.

form is n : guess is

$a_n = A_1 n + A_0$.

$(A_1 n + A_0) - 2(A_1(n-1) + A_0) = n$

$A_1 n + A_0 - 2A_1 n + 2A_1 - 2A_0 = n$

$2A_1 - A_1 n - A_0 = n$

$A_1(2-n) - A_0 = n$ ←②.

$(-A_1 n) + (2A_1 - A_0 - n) = 0$

make this true always.

$A_1 = 0, \; A_0 = -1$.

$\therefore a_n^{(p)} = 0n - 1$

$a_n^{(p)} = -1$

$\therefore a_n = \alpha 2^n - 1$

$a_n =$

• Solve: $a_n = a_{n-1} + a_{n-2}$

$a_0 = 0$

$a_1 = 1$

How to Solve 2nd order, Linear, Homogeneous Recurrences?

→ Solution:

Suppose $a_n = r^n$ → for lin., & homogeneous always (for any order)

$r^n = r^{n-1} + r^{n-2}$

$r^n = r^{n-2}(r+1)$; $r \neq 0$

$r^2 = r+1$

$r^2 - r - 1 = 0$

$r = \frac{1 \pm \sqrt{1+4}}{2} = \frac{1 \pm \sqrt{5}}{2}$,

#2 soln (r_1, r_2) ∵ second order

$r_1 = \frac{1+\sqrt{5}}{2}$, $r_2 = \frac{1-\sqrt{5}}{2}$

$\therefore a_n = A\left(\frac{1+\sqrt{5}}{2}\right)^n + B\left(\frac{1-\sqrt{5}}{2}\right)^n$

$a_0 = A + B = 0$

$a_1 = A\left(\frac{1+\sqrt{5}}{2}\right) + B\left(\frac{1-\sqrt{5}}{2}\right) = 1$

$A\left[\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}\right] = 1$ $\quad A\sqrt{5} = 1$

$A = \frac{1}{\sqrt{5}}$, $B = -\frac{1}{\sqrt{5}}$

$\therefore a_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$ // closed form soln

↳ fibonacci sequence.

8) suppose $a_n = a_{n-1} + a_{n-2}$

$a_0 = 5$

$a_1 = 0.$

$a_n = A\left(\frac{1+\sqrt{5}}{2}\right)^n + B\left(\frac{1-\sqrt{5}}{2}\right)^n$ } everything till this step is same as 6H.

$a_0 = A + B = 5 \qquad B = 5 - A.$

$a_1 = A\left(\frac{1+\sqrt{5}}{2}\right) + B\left(\frac{1-\sqrt{5}}{2}\right) = 0$

$A\left(\frac{1+\sqrt{5}}{2}\right) + 5\left(\frac{1-\sqrt{5}}{2}\right) - A\left(\frac{1-\sqrt{5}}{2}\right) = 0.$

$A\left(\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}\right) = \frac{5(\sqrt{5}-1)}{2}$

$A(\sqrt{5}) = \frac{\sqrt{5}(\sqrt{5}-1)}{2}$

$\therefore B = \frac{10}{2} - \frac{\sqrt{5}(\sqrt{5}-1)}{2} = \frac{10-5+\sqrt{5}}{2} = \frac{5+\sqrt{5}}{2}.$

$\therefore a_n = \frac{\sqrt{5}(\sqrt{5}-1)}{2}\left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{5+\sqrt{5}}{2}\right)\left(\frac{1-\sqrt{5}}{2}\right)^n.$ closed form soln.

- In the obtained Q.E.
  i) Distinct roots → like above
  ii) equal roots?
  iii) complex roots?

Q) $a_n = 2a_{n-1} - a_{n-2}$.

$a_0 = 0, a_1 = 1$

$a_n = r^n$.

$r^n = 2r^{n-1} - r^{n-2}$

$r^2 \cdot r^{n-2} = r^{n-2}(2r-1)$; $r \neq 0$.

$r^2 - 2r + 1 = 0$.

$(r-1)^2 = 0 \quad r = 1$.

general form for distinct real roots

$a_n = Ar_1^n + Br_2^n$,

General form for non-distinct roots; $a_n = (A+Bn)r^n$

(after finding r then

$a_n = A \cdot 2^n + B \cdot n$

$a_n = 2A - B$

$a_0 = 2A - B = 0$

$a_1 = 2A - B = 1$

$a_n = (A+Bn)(1)^n = A + Bn$.

$a_0 = A = 0 \quad \therefore a_n = Bn$.

$a_1 = B \cdot 1 = 1$

$0, 1, 2, 3, 4, \ldots$

about complex roots;

Q) $a_n = T_1 a_{n-1} + T_2 a_{n-2}$

$r^n = T_1 r^{n-1} + T_2 r^{n-2}$

$r^2 - T_1 r - T_2 = 0$.

$\lambda_1^2 + H T_2 < 0$. $(1, -1)$.

General form for complex roots:

$a_n = Ar_1^n + Br_2^n$

$A, B \in \mathbb{C}$

$\Rightarrow$

$0, 1, 1, 0, -1, -1, 0, 1, \ldots$

$a_0 = 0$

$a_1 = 1$.

$a_n = a_{n-1} - a_{n-2}$.

$r^n = r^{n-1} - r^{n-2}$

$r^2 \cdot r^{n-2} = r^{n-2}(r-1)$

$r^2 - r + 1 = 0$

$r = \frac{1 \pm \sqrt{-3}}{2} = \frac{1 \pm i\sqrt{3}}{2}$.

$z = |z| e^{i\theta}$.

$z^n = |z|^n e^{in\theta} = |z|^n (\cos n\theta + i \sin n\theta)$

$a_n = A r_1^n + B r_2^n$.

$r_1 = |r_1| \cdot e^{i\theta_1}$

$r_2 = |r_2| e^{i\theta_2} = |r_2| e^{-i\theta}$

$\therefore a_n = A[|r_1|^n (\cos n\theta + i \sin n\theta)] + B[|r_1|^n (\cos n\theta - i \sin n\theta)]$.

$a_n = |r_1|^n (A+B) \cos n\theta + |r_1|^n (A-B) i \sin n\theta$. $= K_1 \cos n\theta + K_2 \sin n\theta$.

Should be real $\therefore$ complex $= 0$.

~~$\Rightarrow 2A = 0$~~

A, B complex conj. makes this real.

$\therefore$ Solve for complex conj. A, B.

$a_n = A \cos n\theta + B \sin n\theta$

$r_1 = \frac{1+\sqrt{3}}{2}$, $r_2 = \frac{1-\sqrt{3}}{2}$,

$\theta = \frac{\pi}{3}$.

Solve for a, b using boundary conditions.

$a_0 = 0$

$a_1 = 1$.

$a_n = A \cos \frac{n\pi}{3} + B \sin \frac{n\pi}{3}$.

$\Rightarrow A = 0$.

$B = \frac{2}{\sqrt{3}}$.

$\therefore a_n = \frac{2}{\sqrt{3}} \sin \frac{n\pi}{3}$ //.

• Non-Homogeneous Recurrences;

Q1) $a_n = 2a_{n-1} + 7^n \mid a_0 = 1$

$a_n = a_n^{(h)} + a_n^{(p)}$.

$a_n^{(h)} = a_n - 2a_{n-1} = 0$.

$a_n = r^n \Rightarrow r^n - 2r^{n-1} = 0$

$r - 2 = 0 \Rightarrow r = 2$. $\therefore a_n^{(h)} = \alpha 2^n$ — (1).

Why do we write α here? you always get constant when we solve 1st order homo. don't solve for const yet, turn it non-homo and then use boundary and find α.

$a_n^{(p)} \Rightarrow a_n - 2a_{n-1} = 7^n$ r : form is $a_n^{(p)} = Ar^n$

$a_n^{(p)} = A7^n$.

$A7^n - 2 \cdot A7^{n-1} = 7^n$

$5A = 7$

$A = \frac{7}{5}$ $\therefore a_n^{(p)} = \frac{7}{5} \cdot 7^n = \frac{7^{n+1}}{5}$

$\therefore a_n = \alpha 2^n + \frac{7}{5}^{n+1}$ $\quad a_0 = 1$

$a_0 = \alpha + \frac{7}{5} = \frac{5}{5}$ $\quad \alpha = -\frac{2}{5}$

$\therefore a_n = -\frac{2}{5} 2^n + \frac{7^{n+1}}{5}$ ☐//.

if we get $\alpha 2^n$ — (1)

$2a_{n-1} + (2^n) \rightarrow A2^n$

↳ need to consider $A2^n \cdot n$ now!

↓

how does all this work?

basics of recurrences?

- $a_n = ca_{n-1} + f(n)$

* guess $a_n^{(p)}$ based on $f(n)$.

$a_n^{(p)}$	$f(n)$
r^n	r^n if r^n is not a homogeneous soln
nr^n	if r^n is a homogeneous sol^n.

Q2) $a_n = 3a_{n-1} + 7(3)^n$, $a_0 = 1$

$a_n^{(h)}$: $a_n - 3a_{n-1} = 0$ $a_n = r^n$

$r^n - 3r^{n-1} = 0$ $\therefore a_n = \alpha 3^n$ ①.

$r - 3 = 0$

$r = 3$

$a_n^{(p)}$:- $7(3^n)$ $A3^n \cdot n$ $\because 3^n$ is a homogeneous sol^n too.

$a_n^{(h)}$

$A \cdot n \cdot 3^n - 3 \cdot A \cdot 3^{n-1}(n-1) = 7(3)^n$

$3An - 3An + 3A = 7(3)$

$A = 7$

$\therefore a_n = \alpha 3^n + 7n \cdot 3^n$

$a_0 = \alpha + 0 = 1$ $\therefore \boxed{a_n = 3^n + 7n3^n}$ //

Q3) $a_n = a_{n-1} + a_{n-2} + 3^n$, $a_0 = 0$ $a_1 = 1$

$a_n^{(h)}$: $a_n - a_{n-1} - a_{n-2} = 0$ $a_n = r^n$

$r^n - r^{n-1} - r^{n-2} = 0$

$r^2 - r - 1 = 0$.

$r_1 = \frac{1+\sqrt{5}}{2}$, $r_2 = \frac{1-\sqrt{5}}{2}$

$\therefore a_n^{(h)} = A\left(\frac{1+\sqrt{5}}{2}\right)^n + B\left(\frac{1-\sqrt{5}}{2}\right)^n$ — (1).

if 3^n was r_1 or r_2 guess is $A3^n n$

if 3^n was r_1 and r_2 $A \cdot 3^n \cdot n^2$ is guess

$a_n^{(p)}$: $3^n \Rightarrow Ar^n \Rightarrow A3^n$ $a_n^{(p)}$

$A3^n = A$.

$A3^2 - A3^1 - A3^0 = 3^2$

$9A - 3A - A = 9$

$5A = 9$

$A = \frac{9}{5} \Rightarrow a_n^{(p)} = \frac{9}{5} \cdot 3^n = \frac{3^{n+1}}{5} \cdot \frac{9}{5}(3^n)$.

$\therefore a_n = \alpha\left(\frac{1+\sqrt{5}}{2}\right)^n + \beta\left(\frac{1-\sqrt{5}}{2}\right)^n + \frac{3^{n+1}}{5}$.

$a_0 = \alpha + \beta + \frac{3}{5} = 0$. $\beta = -\frac{3}{5} - \alpha$.

$a_1 = \alpha\left(\frac{1+\sqrt{5}}{2}\right) + \beta\left(\frac{1-\sqrt{5}}{2}\right) + \frac{9}{5} = 1$.

$\alpha\left(\frac{1+\sqrt{5}}{2}\right) - \left(\frac{3}{5} + \alpha\right)\left(\frac{1-\sqrt{5}}{2}\right) + \frac{9}{5} = \frac{5}{5}$.

$\alpha\left(\frac{1+\sqrt{5}}{2}\right) - \left(\frac{3}{5}\left(\frac{1-\sqrt{5}}{2}\right) + \alpha\left(\frac{1-\sqrt{5}}{2}\right)\right) = -\frac{4}{5}$.

$\alpha\left(\frac{1+\sqrt{5}}{2}\right) - \alpha\left(\frac{1-\sqrt{5}}{2}\right) - \frac{3}{5}\left(\frac{1-\sqrt{5}}{2}\right) = -\frac{4}{5}$

$\alpha\left(\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}\right) = \frac{3}{5}\left(\frac{1-\sqrt{5}}{2}\right) - \frac{4}{5}$

$\alpha\sqrt{5} =$

ans:

$a_n = \left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1-\sqrt{5}}{2}\right)^n + \frac{9}{5}(3^n)$

$A+B=-\frac{9}{5}$.

$A\left(\frac{1+\sqrt{5}}{2}\right)+B\left(\frac{1-\sqrt{5}}{2}\right)=-\frac{22}{5}$.

$B\left(\frac{1+\sqrt{5}}{2}\right)-B\left(\frac{1-\sqrt{5}}{2}\right)=-\frac{9}{5}\left(\frac{1+\sqrt{5}}{2}\right)+\frac{22}{5}$

$B\sqrt{5}=-\frac{9-9\sqrt{5}}{10}+\frac{44}{10}$

$B\sqrt{5}=\frac{35-9\sqrt{5}}{10}$

$B=\frac{(35-9\sqrt{5})\sqrt{5}}{10\sqrt{5}\sqrt{5}}=\frac{35\sqrt{5}-9\cdot 5}{10\cdot 5}$

~~$B=7\sqrt{5}-9$~~ $B=\frac{-9+7\sqrt{5}}{10}$

$A=-\frac{18}{10}-\frac{7\sqrt{5}-9}{10}=\frac{-7\sqrt{5}-9}{10}$

$\therefore a_n=\left(\frac{-9-7\sqrt{5}}{10}\right)\left(\frac{1+\sqrt{5}}{2}\right)^n+\left(\frac{-9+7\sqrt{5}}{10}\right)\left(\frac{1-\sqrt{5}}{2}\right)^n+\frac{9}{5}(5^n)$

Q8) $a_n = 2a_{n-1} - a_{n-2} + 2(1)^n,\ a_0 = 0,\ a_1 = 1$

$a_n^{(h)}$: $r^2 - 2r + 1 = 0$.

$(r-1)^2 \therefore r_1 = 1,\ r_2 = 1.$

$a_n^{(h)} = (A + Bn) r^n = (A + Bn) 1^n$ — ①.

$a_n^{(p)}$: $2(1)^n$, $\Rightarrow \alpha\, 2(1)^n$ but $r = 1$ is a repeated root of the homogeneous part

$\therefore a_n^{(p)} = \alpha\, 2(1)^n n^2$ is guess;

$\rightarrow \alpha 2(1)^n n^2 - 2 \cdot \alpha \cdot 2(1)^{n-1}(n-1)^2 + \alpha \cdot 2(1)^{n-2}(n-2)^2 = 2(1)^n.$

$\alpha n^2 - 2\alpha(n-1)^2 + \alpha(n-2)^2 = 1.$

$\alpha[n^2 - 2(n-1)^2 + (n-2)^2] = 1.$

$\alpha[n^2 + n^2 - 4n + 4 - 2(n^2 - 2n + 1)] = 1$

$\alpha[2n^2 - 4n + 4 - 2n^2 + 4n - 2] = 1$

$\alpha \cdot 2 = 1 \quad \alpha = \frac{1}{2}$,

(b) $a_n = 4a_{n-1} - 3a_{n-2} + 7\left(\frac{3}{2}\right)^n \quad a_0 = 0 \quad a_1 = 1$

$a_n^{(h)}$: $a_n - 4a_{n-1} + 3a_{n-2} = 0.$

$r^2 - 4r + 3 = 0$

$(r-3)(r-1) = 0 \quad r_1 = 3, r_2 = 1.$

$\therefore a_n^{(h)} = A3^n + B(1)^n$ — (1)

$a_n^{(p)}$: $7\left(\frac{3}{2}\right)^n \Rightarrow a_n^{(p)} = d \cdot 7\left(\frac{3}{2}\right)^n$ guess.

$d \cdot 7 \cdot 3^n - 4 \cdot d \cdot 7 \cdot 3^{n-1} + 3 \cdot d \cdot 7 \cdot 3^{n-2} = 7 \cdot 3^n$

$9dn - 12d(n-1) + 3d(n-2) = 9$

$9dn - 12dn + 12d + 3dn - 6d = 9$

$6d = 9$

$d = \frac{9}{6} = \frac{3}{2}$ ✗ $d = \frac{21}{2}$ actually

just guess $C3^n$ no 7? 7?

$a_n = A3^n + B + \frac{21}{2}3^n \cdot n$ //.

$a_n = -\frac{81}{4}(3)^n + \frac{81}{4} + \frac{21}{2}n \cdot 3^n$ //

$+\frac{4}{8}\left(\frac{81}{4}2\right) + \frac{42}{2}, 9 = \frac{378 - 244}{2}$

$\begin{array}{r} 378 \\ 244 \\ \hline 134 \end{array}$

correct!!! $\frac{134}{2} = 67$.

Non-Homogeneous Recurrence Relations

Solve $a_n = a_n^{(h)} + a_n^{(p)}$ → particular part → guess the form and solve

1) homogeneous part → Solve normally

$f(n)$	$a_n^{(p)}$
c	A
n	$A_1 n + A_0$
n^2	$A_2 n^2 + A_1 n + a_0$
r^n	Ar^n

(Q) $a_{n+1} - 2a_n + 2^n \; ; n \geq 0, a_0 = 1$

$a_n = a_n^{(h)} + a_n^{(p)}$

i) $a_n^{(h)}$ & $a_{n+1} - 2a_n = 0$ homogeneous part; solve like always this is r^n.

$a_{n+1} = 2a_n$; let $a_n^{(h)} = r^n$

$r^{n+1} = 2r^n \Rightarrow r = 2 \Rightarrow a_n^{(h)} = A2^n$ (general form for linears?)

ii) $a_n^{(p)}$: $a_{n+1} - 2a_n = 2^n$ particular part; from is $2^n \Rightarrow r^n$ ∴ guess is A.

$a_n = Ar^n \Rightarrow a_n^{(p)} \Rightarrow A(2^n)$

~~$A \cdot 2^{n+1} = 2 \cdot A \cdot 2^n = 2^n$~~

* because we have 2^n common make $a_n^{(p)} = A \cdot 2^n \cdot n$ to solve particular part.

$A \cdot 2^{n+1}(n+1) - 2 \cdot A \cdot 2^n \cdot n = 2^n \Rightarrow a_n^{(p)} = \frac{1}{2} \cdot 2^n \cdot n$

$2A(n+1) - 2An = 1$ $\qquad a_n^{(p)} = 2^{n-1} \cdot n$

$2An + 2A - 2An = 1$

$A = \frac{1}{2}$.

$a_n = a_n^{(h)} + a_n^{(p)}$

$a_n = \alpha 2^n + n 2^{n-1}$ ∵ $a_0 = 1$ found α;

$a_0 = 2 \cdot 1 \cdot 0 = 1 \Rightarrow \alpha = 1$

∴ $a_n = 2^n + n \cdot 2^{n-1}$ //

(1) $a_{n+2} + 3a_{n+1} + 2a_n = 3^n$; $n \geq 0$, $a_0 = 0$, $a_1 = 1$

$a_n = a_n^{(h)} + a_n^{(p)}$

i) $a_n^{(h)}$: $a_{n+2} + 3a_{n+1} + 2a_n = 0$ $\quad a_n = r^n$

$r^{n+2} + 3r^{n+1} + 2r^n = 0$

$r^2 + 3r + 2 = 0$.

$(r+2)(r+1) = 0 \Rightarrow$ ~~$r = -2, r = -1$~~ two distinct roots

general form is: $a_n = A r_1^n + B r_2^n$

$a_n = A(-2)^n + B(-1)^n$ we know a_0, a_1

$\therefore a_0 = A + B = 0$

$a_1 = -2A - B = 1$

$-A = 1 \quad A = -1, \; B = 1$

$\therefore a_n = -(-2)^n + (-1)^n$.

$a_n = (-1)(-1)^n(2)^n + (-1)^n$.

$a_n^{(h)} = (-1)^n(1 - 2^n)$ // — (1)

don't find A, B here.

ii) $a_n^{(p)}$: $a_{n+2} + 3a_{n+1} + 2a_n = 3^n$ of the form s^n ∴ guess is $a_n = A3^n$.

if no need to multiply by n ∴ other rs are $-2, -1$;

only if $r^{(h)}$ and $r^{(p)}$ sols match, multiply $r^{(p)}$ by n

(i sol'n common)

$\Rightarrow A3^{n+2} + 3 \cdot A \cdot 3^{n+1} + 2 \cdot A 3^n = 3^n$

$9A + 9A + 2A = 1 \Rightarrow a_n^{(p)} = \frac{1}{20} 3^n$ ✓✓

$20A = 1$

$A = \frac{1}{20}$ ✗

$\Rightarrow$ ~~$a_n = (-1)^n(1-2^n) + \frac{1}{20}3^n$~~ //.

* * *

$a_n = A(-2)^n + B(-1)^n + \frac{1}{20}3^n$ solve A, B now?!?

$\Rightarrow a_n = \frac{-11}{5}(-2)^n + \frac{3}{11}(-1)^n + \frac{1}{20}(3^n)$ $n \geq 0$

1) $a_0 \equiv 4 \bmod 5$

$a_0 \equiv 10 \bmod 11$

$a_0 \equiv 2 \bmod 7.$

$a_1 = 4, a_2 = 10, a_3 = 2$

$M = 5 \times 11 \times 7 = 385$

$M_1 = 77, M_2 = 35, M_3 = 55$

$a_0 \equiv (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod M.$

$a_0 \equiv (4 \cdot 77 \cdot 3 + 10 \cdot 35 \cdot 6 + 2 \cdot 55 \cdot 6) \pmod{385}$

$a_0 \equiv (924 + 2100 + 660) \pmod{385}$

$a_0 \equiv 3684 \pmod{385}$

$a_0 \equiv 219 \pmod{385}$

$M_1^{-1} \equiv 77^{-1} \bmod 5$

$77 \cdot M_1^{-1} \equiv 1 \bmod 5$

$M_1^{-1} = 3$

231

$M_2^{-1} \cdot 35 \equiv 1 \bmod 11$

$M_2^{-1} = 35^{-1} \bmod 11.$

$11 = 35 \times 0 + 11$

$35 = 11 \times 3 + 2$

$11 = 2 \times 5 + 1$

$\Rightarrow$ $11 + 2(-5) = 1$

$35 + 11(-3) = 2$

$11 + 35(-0) = 11$

$11 + (35 + 11(-3))(-5) = 1$

$11 + 35(-5) + 11(15) = 1$

$11(16) + 35(-5) = 1.$

$11(16) + 35(6) \equiv 1 \bmod 11$

$35 \cdot 6 \equiv 1 \bmod 11$

$6 \equiv 35^{-1} \bmod 11$

-5 in mod 11 is 6.

$M_2^{-1} = 6$

$M_3^{-1} \cdot 55 \equiv 1 \bmod 7.$

$55^{-1} \bmod 7.$

$7 = 55 \times 0 + 7$

$55 = 7 \times 7 + 6$

$7 = 6 + 1 \quad + 1$

$\Rightarrow$ $7 + 6(-1) = 1$

$55 + 7(-7) = 6$

$7 + 55(-0) = 7.$

$7 + (55 + 7(-7))(-1) = 1$

$7 + 55(-1) + 7(7) = 1$

$7(8) + 55(-1) = 1$ in mod 7 world.

$7(7) + 55 \cdot 6 = 1 \bmod 7$

$6 \equiv 55^{-1} \bmod 7$

$8 \equiv 1, \quad -1 \equiv 6.$

$M_3^{-1} = 6$

2) $a_1 \equiv 8 \bmod 11$

$a_1 \equiv 5 \bmod 7$.

$a_1 \equiv (8 \cdot 7 \cdot 8 + 5 \cdot 11 \cdot 2) \bmod 77$

$a_1 = (448 + 110) \bmod 77$

$a_1 \equiv 558 \bmod 77$

$a_1 \equiv 19 \bmod 17$

$a_1 = 8, a_2 = 5$

$M = 11 \times 7 = 77$

$M_1 = 7, M_2 = 11$

$M_1^{-1} \equiv 7^{-1} \bmod 11$

$7 \cdot M_1^{-1} \equiv 1 \bmod 11$

$M_1^{-1} = 8$

$M_2^{-1} = 11^{-1} \bmod 7$

$11 \cdot M_2^{-1} \equiv 1 \bmod 7$.

$M_2^{-1} = 2$

$a_1 \equiv a_0 + 3 \cdot 1^2 \pmod 5$.

$a_1 \equiv 4 + 3 \bmod 5$

$a_1 \equiv 7 \bmod 5$

$a_1 \equiv 2 \bmod 5$.

$a_0 \equiv a_1 + 3 \cdot 2^2 \pmod 5$

$a_2 \equiv 6a_0 - a_1 \pmod{11}$

$a_2 \equiv 4a_1 - 3a_0 - 2 \pmod 7$

$a_2 \equiv 20 - 6 - 2 \pmod 7$

$a_2 \equiv 12 \bmod 7$

$a_2 \equiv 5 \pmod 7$ — (3).

$\Rightarrow$

$a_2 \equiv 2 + 12 \bmod 5$.

$a_2 \equiv 4 \bmod 5$. — (1).

$a_2 \equiv 6(10) - 8 \pmod{11}$

$a_2 \equiv 52 \bmod 11$

$a_2 \equiv 8 \pmod{11}$ — (2).

$a_1' = 4, a_2 = 8, a_3 = 5$

$m_1 = 5, m_2 = 11, m_3 = 7$

$M = 385$,

$M_1 = 77, M_2 = 35, M_3 = 55$

$M_1^{-1} = 3, M_2^{-1} = 6, M_3^{-1} = 6$

$M_1^{-1} \equiv 77^{-1} \bmod 5$ (from (1)).

$M_2^{-1} = 35^{-1} \bmod 11$

$M_3^{-1} = 55^{-1} \bmod 7$

$\Rightarrow a_2 \equiv 5$.

$a_2 \equiv (4 \cdot 77 \cdot 3 + 8 \cdot 35 \cdot 6 + 5 \cdot 55 \cdot 6) \bmod 385$

$a_2 \equiv (924 + 1680 + 1650) \pmod{385}$.

$a_2 \equiv 4254 \pmod{385}$

$a_2 \equiv 19 \pmod{385}$.

3) $a_{100} \pmod 5$?

in mod 5 's world;

the reccurence relation can be stated as;

$a_n = a_{n-1} + 3n^2$, $a_0 = 4$.

$0 \le a_i \le 4$, $i \in \mathbb{N}$ only.

$a_n - a_{n-1} = 3n^2$

$a_{n-1} - a_{n-2} = 3(n-1)^2$

$a_{n-2} - a_{n-3} = 3(n-2)^2$

...

$a_2 - a_1 = 3(2)^2$

$+ \quad a_1 - a_0 = 3(1)^2$

$a_n - a_0 = 3[n^2 + (n-1)^2 + (n-2)^2 + \dots + 2^2 + 1^2]$.

$a_n - a_0 = 3 \cdot \frac{n(n+1)(2n+1)}{6}$ ↳ sum of first n squares

$a_n \equiv \frac{n(n+1)(2n+1)}{2} + a_0 \pmod 5$

$a_n \equiv \frac{n(n+1)(2n+1)}{2} + 4 \pmod 5$

$a_{100} = \frac{50 \cdot 101 \cdot 201}{1} + 4 \pmod 5$

$a_{100} \equiv 1015054 \pmod 5$

$a_{100} \equiv 4 \pmod 5$

4) $a_{150} \pmod{35}$.

find a_{150} in mod 5 world. -(i)

a_{150} in mod 7 world. -(ii)

use CRT to find it in mod 35 world. -(iii).

(i) from Q3 $\because$ in mod 5's world $a_n \equiv \frac{n(n+1)(2n+1)}{2} + 4 \pmod 5$

$a_{150} = \frac{150 \cdot 151 \cdot 301}{2} + 4 \mod 5$

$a_{150} = 3408829 \pmod 5 \Rightarrow \boxed{a_{150} \equiv 4 \mod 5}$

(ii) To find a_{150} in mod 7's world, we first need to solve the reccurence relation in mod 7's world.

$a_n = 4a_{n-1} - 3a_{n-2} - 2$; $a_0 = 2, a_1 = 5 \pmod 7$.

$\because$ not homogeneous $\rightarrow$ cannot apply $a_n = r^n$ ✗.

Group Theory

*

Def. of A Group

- A non-empty set (usually called G), and a binary operator (·) (binary operator means it takes two arguments and gives an output) is a group if the following four properties hold;

1) Closure: $\forall a,b \in G,\ a \cdot b \in G$ as well.
2) Associativity: $\forall a,b,c \in G,\ (a \cdot b) \cdot c = a \cdot (b \cdot c)$ → property of the operation.
3) Existence of Identity: $\exists\ e \in G$ s.t. $\forall a \in G,\ a \cdot e = a = e \cdot a$
4) Existence of Inverse: $\forall a \in G,\ \exists\ b \in G$ s.t. $a \cdot b = e = b \cdot a$

□//.

- Why do we need such objects?
  2> vast applications (CS, E&E)

Examples

1) $(\mathbb{Z}, +)$ is a group.

Proof; Show above 4 properties hold.

i) Closed: $\forall a,b \in \mathbb{Z}$ $a+b \in \mathbb{Z}$ too ∴ yes
ii) Associative: $\forall a,b,c \in \mathbb{Z}$, $(a+b)+c = (a+b)+c$ ∴ yes
iii) Identity: $\forall a \in \mathbb{Z}$, $\exists$ an element 0 s.t. $a+0 = 0+a$ ∴ yes
iv) Inverse $\forall a \in \mathbb{Z}$, $\exists$ an element $-a \in \mathbb{Z}$ s.t. $a+(-a) = 0 = (-a)+a$ ∴ yes

∴ this is $(\mathbb{Z}, +)$ is a group.

↳ Special group as it is also commutative;
$\forall a,b \in \mathbb{Z}$, $(a+b = b+a)$

∴ such special groups are called Abelian Groups / commutative Groups.

• $(\mathbb{Z}, *)$ is not a group as its inverse does not exist in $\mathbb{Z}$ (multiplication).

* inverse * ~~identity~~ element = identity.

Q) Let G be the set of all 2×2 matrices over $\mathbb{R}$. s.t. $ad-bc\neq0$ ↓ inverse exists

$(G, *)$? (matrix multiplication).

is it a group? Yes. ∴ is a group.

$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ over $\mathbb{R}$ $\quad ad-bc$

i) inverse:

$\begin{bmatrix} a & b \\ c & d \end{bmatrix} * \begin{bmatrix} w & x \\ y & z \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} w & x \\ y & z \end{bmatrix} * \begin{bmatrix} a & b \\ c & d \end{bmatrix}$

does $\begin{bmatrix} w & x \\ y & z \end{bmatrix}$ exist within G?

$\Rightarrow wz - xy \neq 0$

$A^{-1} = \frac{\text{adj } A}{|A|}$.

$\begin{bmatrix} w & x \\ y & z \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

$\begin{bmatrix} w & x \\ y & z \end{bmatrix} = \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$ works?

$\therefore w = \frac{d}{ad-bc}$,

$\frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \frac{1}{ad-bc} \begin{bmatrix} ad-bc & db-bd \\ -ac+ac & -bc+ad \end{bmatrix}$

$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ □//.

∴ G is indeed a group □//.

Q) $G = \{-1, 1\}$, Operation: Multiplication (like in $\mathbb{R}$)

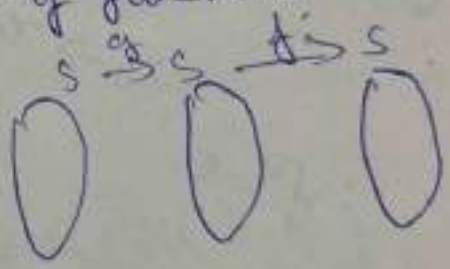
1) closed ✓
2) associative ✓ — Real $\times$ is associative so if G is closed it is also associative on G.
3) identity ✓
4) inverse ✓
5) commutative ✓ } Abelian Group.

2) Finite Group → has finite no. of elements.

$o(G) = 2$ order of group.

Consider set S.
Let G be the set of all one to one functions from S to S,
$f: S \to S$. (Usually G is $A(S)$ here). A for Automorphism.
↳ If S is finite f's are bijections in that case.
⇒ if $n(S) = n$, $o(A(S)) = n!$
∴ if S is finite, $o(A(S)) = |S|!$

• Define an operation called; "composition of functions"
$f \circ g$.



Th^m: $(A(S), \circ)$ is a group. Why?
i) Any one-one f and g composed is also a one-one
ii) Associative $f \circ (g \circ h) = (f \circ g) \circ h$.
iii) Identity: $f(x) = x$
iv) Inverse: f^{-1} iff $|S|$ finite,
* $(A(S), \circ)$ is called a Symmetric group, over S.

• Th^m: S_3 is a non-abelian group. S_n : size of $A(S)$ / n = size of S.

Proof:

$|S_3| = 3! = 6$ ($S_3 \equiv A(S)$ when $|S|=3$)

$S = \{x_1, x_2, x_3\}$.

f: $x_1 \to x_2$, $x_2 \to x_1$, $x_3 \to x_3$ | g: $x_1 \to x_2$, $x_2 \to x_3$, $x_3 \to x_1$

(* for S_n $n \geq 3$, do 3 like this, map rest to themselves)

fog: $x_1 \to x_1$, $x_2 \to x_3$, $x_3 \to x_2$ → non-abelian ∴ not commutative

$g^2 = g \circ g$: $x_1 \to x_3$, $x_2 \to x_1$, $x_3 \to x_2$

gof: $x_1 \to x_3$, $x_2 \to x_2$, $x_3 \to x_1$.

$g^3 = g \circ g \circ g$: $x_1 \to x_1$, $x_2 \to x_2$, $x_3 \to x_3$ $= fg$.

$\therefore g^3 = e$.

$g^2 = g^{-1}$

$f^2 = f \circ f$: $x_1 \to x_1$, $x_2 \to x_2$, $x_3 \to x_3$

$\therefore f^2 = e$.

$S_3 = \{e, f, g, g^2, fog, gof\}$ → 6 elements (unique found)

↳ any other function b/w $S \to S$ is basically one of these

↳ eg $f^{-1} \circ g^2 = ?$

* any group is isomorphic to a symmetric group → cauchy, ↳ galois's field etc.

↳ universal groups, ...

↳ hardware for diff. functions.

Th^m: In any group

① e is unique

② inverse of a is unique

③ $(a^{-1})^{-1} = a$

④ $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$

// left right cancellations
$a \cdot x = a \cdot y \Rightarrow x = y$

Proof:

i) Suppose the contrary; e and f are identity elements.
we show that $e = f$ ∴ unique:

$\forall a \in G$, $a \cdot e = a = e \cdot a$

~~$a \cdot f = a = f \cdot a$~~

∴ true $\forall a \in G$, should be true for $a = f$ too:

~~$a \cdot f = f$~~ $f \cdot e = f = e \cdot f$ — ①

also: $\forall a \in G$, $a \cdot f = a = f \cdot a$

∴ $e \in G$, $a = e$ holds: $e \cdot f = e = f \cdot e$ — ②

} $\Rightarrow e = f$ □// $a \in D$.

2) ~~Suppose~~ If $ax = ay$ then $x = y$. Show this. This means a^{-1} is unique because $a_1^{-1} \cdot a = e = a_2^{-1} \cdot a$ — from this → contradiction □//.

$a_1^{-1} \cdot a = a_2^{-1} \cdot a \Rightarrow a_1^{-1} = a_2^{-1}$

∴ sufficient to show cancellation law holds: Let b be an inverse of a.

$x = e \cdot x = (b \cdot a) \cdot x = b \cdot (a x)$ — associative law

$= b \cdot (a y)$ hypothesis

$= (b \cdot a) \cdot y$ associative

$= e y$

$= y$

∴ ~~$x = y$ if~~ if $ax = ay$ then $x = y$ □//

3) $(a^{-1})^{-1} = a$.

$a^{-1} \cdot (a^{-1})^{-1} = e = a^{-1} \cdot a$

$a^{-1} \cdot (a^{-1})^{-1} = a^{-1} \cdot a$ left cancellation $\Rightarrow$ $(a^{-1})^{-1} = a$ //Q.E.D.

4) $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$

$(ab)^{-1} ab = e$

$ab\,(b^{-1}a^{-1}) = e$ //Q.E.D.

Sub-Groups

- given a group G, if a subset H of G forms a group with the same operation, then H is a subgroup of G?

Let $(G, \cdot)$ be a group.

if $H \subseteq G$ is a group with $\cdot$ $(H, \cdot)$ is a group in itself.

then H is a sub-group of G

e.g.

$(\mathbb{Z}, +)$ is a group.

Let $H = (\{n : n \equiv 0 \bmod 3\}, +)$. ~~H is a group?~~

closure ✓, associative ✓.

H is a group, + subgroup

Th^M: $H \subseteq G$ is a subgroup of G iff

(a) $\forall a, b \in H$, $ab \in H$ (if G is finite, closure alone is sufficient)

(b) $\forall a \in H$, $a^{-1} \in H$ (if G is infinite, need closure and inverse)

Proof;

$e \in H$. why? if $a \in H$ then $a^{-1} \in H$ (b)

$a \cdot a^{-1} \in H$ by closure (a)

$\therefore e \in H$.

assuming (a) (b) prove e, associativity, $\Rightarrow H$ is a group

$\because H \subseteq G$, H is a subgroup.

If G is finite (a) $\rightarrow$ H is a subgroup of G;

$\Rightarrow$ H is finite

Let $a \in H$.

$a^2 \in H, a^3 \in H, \ldots \forall i \in \mathbb{N}\ a^i \in H$ but H is finite

$\exists i, j$ s.t. $a^i = a^j$ $i \neq j$

Let $i > j$

$a^{i-j} = e$

$a(a^{i-j-1}) = e$

$\therefore a^{-1} = a^{i-j-1} \in H$ □//.

* Associativity is a property of the operator. ∴ set does not matter.

if G is finite, every closed subset of G is a group;

- $\forall a, b \in G$
- Let $a \equiv b \pmod H$ if $a \cdot b^{-1} \in H$ → defining $a \equiv b \pmod H$ as $a \cdot b^{-1} \in H$ (H is a subgroup of G)

e.g. $G = \mathbb{Z}$ ∴ $(\mathbb{Z}, +)$ is a group G.

$H = (\{x \mid 3 \mid x\}, +)$ is a subgroup H of G.

$a, b \in G$, $a \equiv b \pmod H$ if $a - b$ is a multiple of 3.

Th^m $a \equiv b \bmod H$) relation is an equivalence relation.

i) Reflexive: $\forall a \in G$, $a \equiv a \pmod H$.

$a \cdot a^{-1} \in H$. ; $e \in H \to$ true $\square$ $\therefore$ reflexive $\square //$

ii) Symmetric: $\forall a, b \in G$, if $a \equiv b \bmod H$ then $b \equiv a \bmod H$:

$a \cdot b^{-1} \in H \iff b a^{-1} \in H$.

$ab^{-1} \in H \iff (ab^{-1})^{-1} \in H$ by dfy. of subgroup

$\Rightarrow b \cdot a^{-1} \in H$ $\square //$

iii) Transitive: $\forall a, b, c \in G$, if $a \equiv b \bmod H$, $b \equiv c \bmod H$ then $a \equiv c \bmod H$

$ab^{-1} \in H$, $bc^{-1} \in H$ given

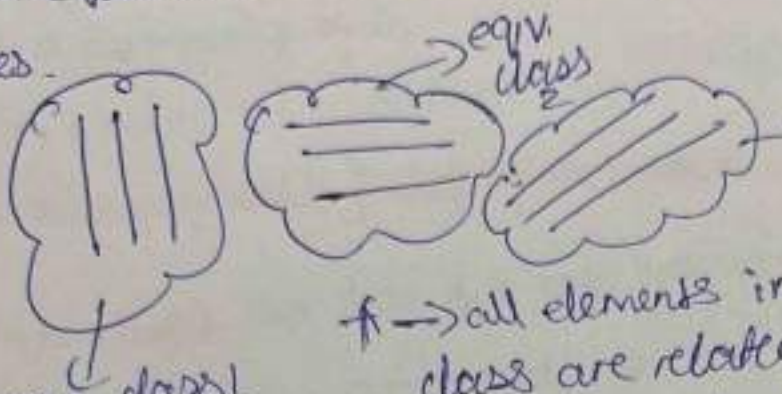
by closure $ab^{-1} \cdot bc^{-1} = ac^{-1} \in H$ $\square //$

- congruence modulo subgroups
- congruence, ~~etc~~ equivalence relations partition the set into equivalence classes.
- eqv. classes

DS Tut 7/11/24 - Group Theory

Equivalence Classes

- if R is an equivalence relation, R partitions the set into eqv. classes.



↑ → all elements in an equivalence class are related to each other

* → no two elements in different equivalence classes are related to each other.

i.e) eqv. class of 'a' = $\{x \mid xRa\}$?

Bezoz's Theorem
if gcd(a,b) = 1, ∃ x, y s.t $ax + by = 1$

- magmas, quasi-groups etc.
- abelian groups

e.g.) define a set G_n as the set of all naturals less than n and coprime to n; and an operation $\times \pmod n$. is it a group?

i) closure: $\forall a, b \in G_n$, $a \cdot b \in G_n$

a does not share a factor with n
b does not share a factor with n
∴ a×b cannot share a factor with n ↓ trivial.

$a \times b \pmod n \equiv ab - kn$ cannot share a factor with n

∴ $a \cdot b \pmod n \in G_n$ ∴ closure ✓ //.

What are the eqv. classes?

↳ Defn: [Right coset]

- The right coset of 'a' wrt H = $\{ha \mid h \in H\}$ → takes every element of H and operates with a. $a \in G$

$a \in G$, H is a subgroup of G

e.g. if $a = b \bmod H \Rightarrow ab^{-1} \in H$.

• left coset $\{ah \mid h \in H\}$.

$[a] = \{x \mid a = x \bmod H\}$ def. of eqv. class

- Th^m: $[a] = \{ha \mid h \in H\}$ eqv. class of a under this eqv. relation is the right coset of a.

Proof: Let $x \in [a] \Rightarrow a \equiv x \bmod H \Rightarrow ax^{-1} \in H$

$\Rightarrow$ i) if $ax^{-1} \in H$, $\because H$ is a subgroup of G

$(ax^{-1})^{-1} \in H \Rightarrow xa^{-1} \in H \Rightarrow \exists h \in H$ s.t. $xa^{-1} = h$.

$x = ha$.

$\therefore \forall x \in [a], x \in \{ha \mid h \in H\}$

$\Rightarrow [a] \subseteq \{ha \mid h \in H\}$.

ii) Let $x \in \{ha \mid h \in H\} \Rightarrow \exists h \in H$ s.t. $x = ha$

$ax^{-1} = a(ha)^{-1} = a \cdot a^{-1}h^{-1} = h^{-1}$

$\because h \in H$, $h^{-1} \in H \therefore ax^{-1} \in H, \therefore \Rightarrow a \equiv x \bmod H$

$\Rightarrow x \in [a]$

$\therefore \forall x \in \{ha \mid h \in H\}, x \in [a]$

$\Rightarrow \{ha \mid h \in H\} \subseteq [a]$

$\Rightarrow \{ha \mid h \in H\} = [a]$ □// Q.E.D.

- How many elements in the eqv. classes?

- $Ha; Hb$
  if $a \neq b$, right cosets are disjoint.

one-to-one map b/w Ha and Hb.
order of all cosets is same.

Thm: All cosets > are (formed by H) of the same size, namely $o(H)$.

↳ size of all equivalence classes formed by $\equiv \bmod H$ is size $o(H)$.

- **Thm:** if G is a finite group, then for any sub-group H, $o(H)$ divides $o(G)$.

Proof:
H is a subgroup of G.
Let $H = \{h_1, h_2, h_3, \ldots, h_r\}$
i) $o(H) = o(aH)$ case.
ii) $\exists (a \notin H) \wedge a(G)$
consider: $h_1\ h_2\ h_3 \ldots h_r$
$ah_1\ ah_2\ ah_3 \ldots ah_r$

• Cor: if $o(G)$ is prime, then G and $\{e\}$ are the only subgroups.

• Converse of Lagrange is not true.

Th^m: $\forall a \in G, \; a^{o(a)} = e$

$\{e, a, a^2, a^3, \ldots, a^{o(a)-1}\}$

e.g. $N = 15$, $\phi(15) = 8$

$Z_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$

$a \in Z_{15}^*$

$a^8 \bmod 15 \equiv 1$.

$a = 2$: $\{2, 4, 8, 1\}$

$o(2) = 4 \mid o(Z_{15}^*) = 8$.

Th^m: Euler's Theorem. (Totient)

$\forall a \in [0, N-1]$, $\gcd(a, N) = 1$,

$$a^{\phi(N)} \equiv 1 \bmod N$$

$\phi(N)$ is number of 'coprime to N' numbers $< N$.

e.g. $N = 7$; $a = 2$.

$2^{\phi(7)} = 2^6 \bmod 7 = 1$

• Th^m: Fermat's Little Th^m:

If p is prime

$a^p \equiv a \bmod (p)$.

e.g.) $S_3 = \{e, f, g, fg, gf, g^2\}$

$H = \{e, g, g^2\}$

Right coset of H wrt f: $Hf = \{ef, gf, g^2f\}$

Left coset of H wrt f: $fH = \{fe, fg, fg^2\}$.

↳ Left coset may / may not be equal to right cosets. only for "normal subgroups".

* Z_n^* is a group of order $\phi(N)$,

cyclic subgroup $\{e, a, a^2 \ldots\}$

$o(a)$

$o(a) \mid \phi(N)$

$a^{o(a)} = 1$

$a^{\phi(N)} = 1$

connectivity

alternating rings

- Two sub-groups H and K.

Define $HK = \{x \in G \mid x = hk, h \in H, k \in K\}$

i) all elements in the group which can be written as HK where $h \in H, k \in K$.

* is HK a subgroup of G?

ans. below:

Th^m:

HK is a sub-group iff $HK = KH$.

Proof:

i) Assume $HK = KH$. We show HK is a subgroup of G.

let $h_1k_1 \in HK$, $h_1 \in H, k_1 \in K$, $h_2k_2 \in HK$.

a) need to show that HK is closed.

does $(h_1k_1)(h_2k_2)$ belong to HK?

$= h_1(k_1h_2)k_2$.

$k_1h_2 = h'k'$ ∵ $HK = KH$

$= h_1(h'k')k_2 = (h_1h')(k'k_2) \in HK$.

$h''k'' \in HK$ ☐/L

∴ it is closed

b) what about inverse?

let $hk \in HK$, what about $(hk)^{-1}$.

$(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$. ∴ inverse also exists in HK.

∴ HK is a subgroup ☐/L ①.

ii) Assume HK is a subgroup of G, show $HK = KH$.

↳ closure + inverse are there

a) ~~Let $h_1k_1 \in HK$, $h_2k_2 \in HK$.~~

we know ∵ closure, $(h_1k_1)(h_2k_2) \in HK$.

Let $hk \in HK$.

∵ HK is a subgroup $(hk)^{-1} \in HK$

$\Rightarrow k^{-1}h^{-1} \in HK$

$k^{-1}h^{-1}$ is an element of KH.

$\Rightarrow HK \subseteq KH$. //

b) Let $kh \in KH$ $k \in K$, $h \in H$.

∴ $h^{-1}k^{-1} \in HK$

$(h^{-1}k^{-1})^{-1} \in HK$.

$= kh \in HK$

kh is an element of KH

$\Rightarrow KH \subseteq HK$.

∴ $HK = KH$. □ //, Q.E.D.

if HK is subgroup iff $HK = KH$.

Cor: if G is Abelian, then product of subgroups is a subgroup.

(commutativity, trivial).

Normal ~~Group~~ Subgroups

- A subgroup N is normal if $\forall g \in G$, $\forall n \in N$, $gng^{-1} \in N$.

  for all g in G, for all n in the subgroup N of G, $g * n * g^{-1}$ is present in the sub-group N of G.

  ↳ left cosets are equal to right cosets for Normal subgroups.

- eg.) $G = (Z, +)$, $N = (\{n / 3 | n\}, +$ ~~mods~~$)$

  $g+n-g$. $\forall g, \forall n$.

  $g+n-g = n \in N$ ∴ N is a normal subgroup □//

⇒ Th^m: N is a normal subgroup of G iff $\forall g \in G$, $\forall n \in N$ $g \cdot N \cdot g^{-1} \subseteq N$; $gNg^{-1} = \{gng^{-1} | n \in N\}$

Proof:

i) forward is trivial by definition:

if N is a normal subgroup of G

then by def $\forall g \in G$, $\forall n \in N$, $gng^{-1} \in N$

$\Rightarrow gNg^{-1} \subseteq N$ - (a).

ii) $g^{-1} N (g^{-1})^{-1} \subseteq N$ also

$g^{-1} N g \subseteq N$.

$N = eNe = g^{-1}(g N g^{-1})g \subseteq g^{-1} N g \subseteq N$.

$N \subseteq g^{-1} N g$

• Th^m: N is a normal subgroup of G iff set of all left cosets of N are the same as set of all right cosets of N.

Proof: if N is normal

$\forall g \in N$ of G, $gNg^{-1} = N$ — (1)

Left coset of N = $gN = \{gn \mid n \in N\}$.

Right coset of N = $Ng = \{ng \mid n \in N\}$.

(1) $\Rightarrow (gNg^{-1}) \cdot g = Ng \Rightarrow gN = Ng$.

Proof: if left coset = right coset

$\forall g \in G$, left coset $gN = Ng'$

$e \in N$.

$g \in gN$; $g \in Ng' = Ng$.

$\therefore gN = Ng' = Ng \Rightarrow gN = Ng$ ∎ // Q.E.D.

$\because$ right coset ≡ eqv. class

$\exists$ only 1 right coset containing g.

$g \equiv g' \bmod N$

Product of Subsets of Group G

$AB = \{ab \mid a \in A \wedge b \in B\}$

• Product of $(Na)(Nb) = ?$

Th^m: Product of ~~right~~ two right cosets of a normal subgroup N is also a right coset.

Proof:

Na, N is normal.

$Na = \{na \mid n \in N\}$.

$Nb = \{nb \mid n \in N\}$.

$(Na)(Nb) = \{$ ~~$na \cdot nb \mid n \in N\}$~~. $x \in Na, y \in Nb\}$.

$xy = (n_1 a)(n_2 b)$ | $Na = aN$

$= (an_3)(n_2 b)$ | $Nb = bN$.

$= a(n_3 n_2)b = an_4 b$.

$an_2 \in aN = Na$.

$an_2 = n_3 a$.

$xy = (n_1 a)(n_2 b) = n_1(an_2)b = n_1 n_3 ab$.

$xy = n_4 ab$ } right coset wrt ab.

$\therefore (Na)(Nb) = Nab$.

$= \{nab \mid n \in N, a, b, \in G\}$.

5

- $\mathbb{Z}$ = set, + = operation.
  $\mathbb{Z}_n$ = 0 to n-1 set

a subgroup is a subset of

- coset implies shifting a group.
  all multiples of 5.

  $5K+1 \rightarrow$ coset shifted by 1
  $5K+2 \rightarrow$ coset shifted by 2
  } all of these cosets are mutually disjoint

  all of these cosets partition $\mathbb{Z}$, completely.

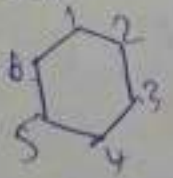
- ghg^{-1}: what does this really mean?
  ↳ connected to similar matrices.
  "matrix A is similar to B if $\exists$ P s.t. $A = PBP^{-1}$"

- $(\mathbb{Z}_{12} = \{0,1,\dots,11\}, + \bmod 12)$
  Let $A = \{0,3,6,9\} \subseteq \mathbb{Z}_{12}$, + mod 12
  is a subgroup.
  $\{1,4,7,10\}$ is A+1 coset shift
- Size of all cosets of a subgroup = size of subgroup

- Size of subgroup has to divide size of main group. (Lagrange's theorem). here $|A| = 4 \Rightarrow 12/4 = 3$ ∴ we get 3 cosets for A.

- Conjugation in Group Theory: (ghg^{-1}).

D_6: dihedral 6 reflections 6 rotations (elementary operations that result in a new transformation).

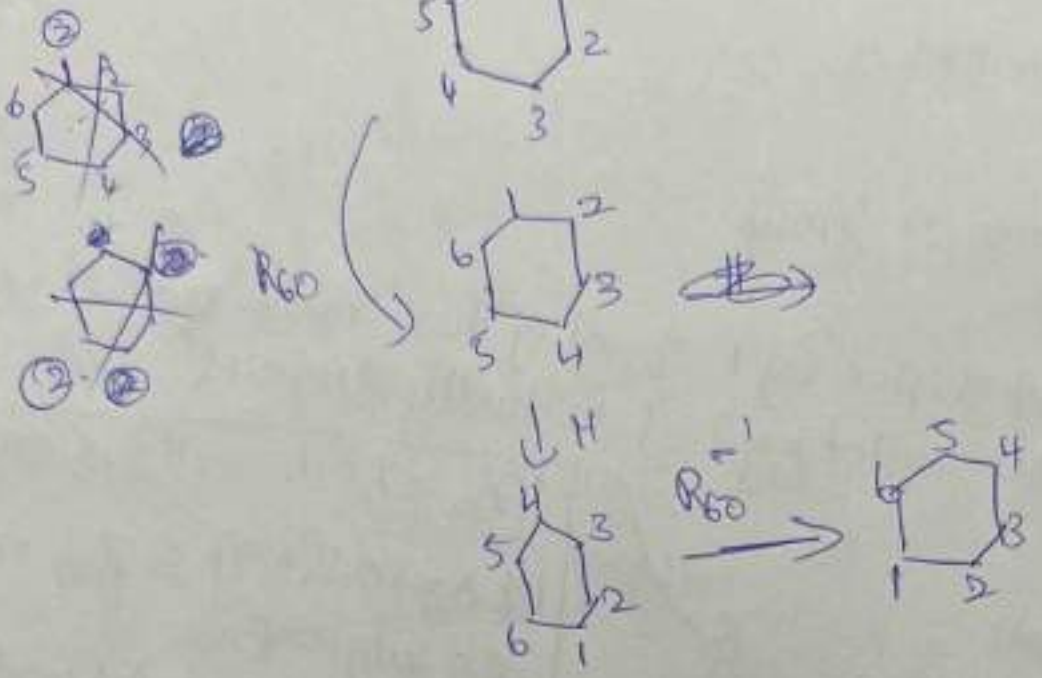


↳ any other comb. of any operations is just one of these.

$\{R_0, R_{60}, R_{120}, R_{180}, R_{240}, R_{300}\}$

• consider R_{60}, & H. (H = horz axis reflection / flip).

$R_{60} H R_{60}^{-1}$



• ghg^{-1} is same as performing H but from a diff. perspective.

• Normal Subgroup; No matter from which perspective we perform the action, it is the same action/result from all perspectives?

$H = \{a, b, c\}$

gag^{-1} gbg^{-1} gcg^{-1}

$\|$ $\|$ $\|$

b c a.

normal subgroup:

$\forall g \in G, \{gag^{-1}, gbg^{-1}, gcg^{-1}\}$ produce H exactly together,

- Cosets partition an entire set.
  ↳ shifting.

- Z.
  take set as all multiples of 9.
  how many cosets → 9. → how many shifts from original

9K	9K+1	9K+2
9K+3	9K+4	9K+5
9K+6	9K+7	9K+8

→ (9K+3)+9K stays 9K+3.
⇒ 9K+8 + 9K+1 forms 9K.
⇒ e = 9K
⇒ inverse works too.
⇒ these cosets forms a group

the collection set of called quotient groups.

⇒ every element in 9K+1 operated with 9K+3 must land in 9K+4 for quotient.
↳ closure def.

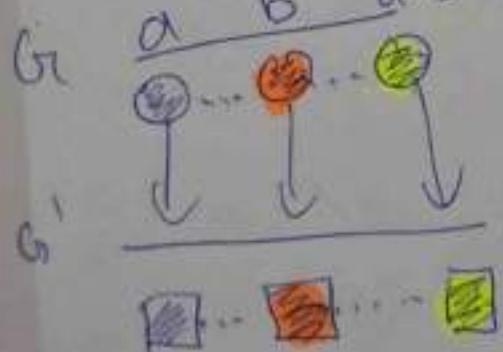
Z = og set.
9K = subgroup.
▦ = cosets of subgroup.

Homomorphism

- trying to relate two groups
  ↳ create homomorphism to an easier group to work with.

$f: G \to G'$; $f(ab) = f(a)f(b)$

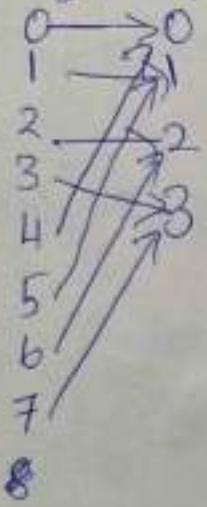
$f(a) \cdot f(b) = f(ab)$



blue sqr × org sqr = green square.

mod 3, mod 5
{0,1,2} {0,1,2,3,4}

- Z_8, Z_4. # in any homomorphism e→e maps,



- G_1, G_2 don't have to be same size.
- NOT one-one,

↓

~~one-one~~ ~~invertible~~ homomorphisms are called isomorphisms.

if the isomorphism is onto

- m, n co-prime : $\phi(m)\phi(n) = \phi(m,n)$.

$n = 2^a 3^b 5^c$

$\phi(n) = n(1-\frac{1}{2})(1-\frac{1}{3})(1-\frac{1}{5})$

Quotient Group G/N

({Na | a ∈ G}, product) → Q.Gr. G/N
set of all right co-set.

- Proof that this is a group :

i) closure → Yes

ii) Associativity → (Na)[(Nb)(Nc)] = [(Na)(Nb)](Nc)

Na[Nbc] = [Nab][Nc]

N(abc) = N(abc) ∴ Yes //.

iii) Identity → Ne

∴ (Na)(Ne) = Nae = Na = Nea = (Ne)(Na)

∴ Yes //.

iv) inverse :

(Na)(Na⁻¹) = Naa⁻¹ = Ne.

∴ Yes ∴ Group // Q.E.D

e.g.) G = (Z, +)

N = (multiples of 3, +).

G/N = ({N+0, N+1, N+2}, product) → resembles Z mod 3

(N+a)(N+b) = N+(a+b)

Homomorphisms

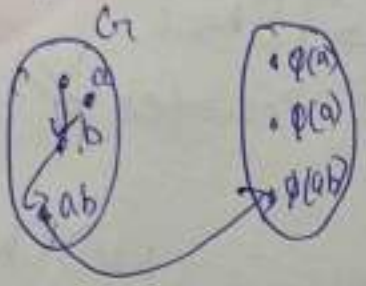
- $\phi: G \to G'$ is a homomorphism from group G to G' if;

  $\forall a, b \in G$, $\phi(ab) = \phi(a)\,\phi(b)$

  ϕ is a function from group G to group G'.

  ab is in group G.

  $\phi(a)\,\phi(b)$ is in group G'



i) apply ab in G, get ab.
ii) apply ϕ to ab,

OR

i) apply ϕ to a, ϕ to b, get $\phi(a)$, $\phi(b)$ in G'
ii) operate $\phi(a)\,\phi(b)$.

$\Rightarrow$ these two are equivalent if ϕ is a homomorph.

- Example:

  $G = (\mathbb{R}, +)$
  $G' = (\mathbb{R}^+, *)$.

  $\phi: G \to G'$
  $\phi(a) = 2^a$

Let $a, b \in G$. $2^{a+b} = \phi(ab)$

$\phi(a) = 2^a$
$\phi(b) = 2^b$

$\phi(a) \cdot \phi(b) = 2^a \cdot 2^b = 2^{a+b} = \phi(ab)$

$\therefore \phi$ is a homomorphism.

Thm: Given a group G and a Normal subgroup N of G, then $\phi : G \to G/N$, $\phi(a) = Na$ is a homomorphism.

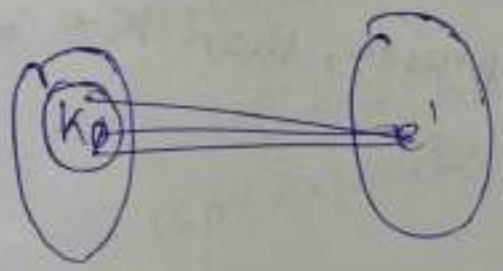
Proof:

- G/N is a quotient group with all the right cosets as the set and product as operation.
  ↳ (The product we define a long ago).

$$\ast \Rightarrow \phi(ab) = Na \cdot b \xrightarrow{???} = Na \cdot Nb = \phi(a)\phi(b) \quad // \text{Q.E.D.}$$

Kernel of a Homomorphism ϕ

- $\phi : G \to G'$, the kernel of ϕ; $K_\phi = \{x \in G \mid \phi(x) = e'\}$
  ↳ identity element in G'.



The set of xs $\in G$ ~~which~~ whose image under ϕ is e' in G'.

Thm: For any homomorphism $\phi : G \to G'$
$\phi(e) = e'$ and $\phi(x^{-1}) = [\phi(x)]^{-1}$
and therefore K_ϕ can never be empty as $e \in K_\phi$ always.

~~PTO~~ ~~Hard~~

Proof:

i) $\forall a, b \in G$, $\phi(ab) = \phi(a)\phi(b)$.

let $b = a^{-1}$ $\quad \phi(a \cdot a^{-1}) = \phi(a)\phi(a^{-1})$

$\phi(e) = \phi(a)\phi(a^{-1}) = e'$

$\Rightarrow \phi(a^{-1}) = (\phi(a))^{-1}$ //-

i) but how to prove $\phi(e) = e'$?

$\phi(ee) = \phi(e)\phi(e)$

$\phi(e) = \phi(e)\phi(e)$.

$\phi(e)(\phi(e))^{-1} = \phi(e)\phi(e)(\phi(e))^{-1}$

$e' = \phi(e)e'$

$e' = \phi(e)$ $\square$ // Q.E.D.

Thm: If $\phi : G \to G'$ is a homomorphism, then $K\phi$ is a normal subgroup of G.

→ prove subgroup, then normal.

Proof:

i) $K\phi = \{x \in G \mid \phi(x) = e'\}$. how is this a subgroup? ↩

show closure + inverse

closure

let $x, y \in K\phi$.

$\phi(x) = e' \quad \phi(y) = e'$

↳ $\phi(xy) = e'$

$\therefore xy \in K\phi$.

inverse

let $x \in K\phi$.

$\phi(x^{-1}) = (\phi(x))^{-1} = e'^{-1} = e'$

$\phi(x) = e'$

$\therefore x^{-1} \in K\phi$.

- how to show K_ϕ is normal?

$\forall g \in G$, $\forall k \in K_\phi$

$gkg^{-1} \in K_\phi$ if K_ϕ is a normal subgroup of G.

$\phi(gkg^{-1}) = \phi(g)\,\phi(k)\,\phi(g^{-1})$ ($\because k \in K_\phi$, $\phi(k) = e'$).

$= \phi(g)\, e'\, \phi(g^{-1})$

$= \phi(g)\,\phi(g^{-1}) = \phi(g)\,\phi(g)^{-1} = e'$.

$\therefore gkg^{-1} \in K_\phi$. // Q.E.D.

~~Thm: if $\phi: G \to G'$ is a homomorphism~~

Isomorphism

- special kind of homomorphism.
  - ↳ if homomorphism is one-one then it is an isomorphism.
- if it is one-one and onto then we say G is isomorphic to G'. $G \cong G'$
- ~~if we have~~. ↳ This means they are essentially the same group and have the same structure.

Thm: if $\phi: G \to G'$ is a homomorphism from G to G' then $G/K_\phi \cong G'$.

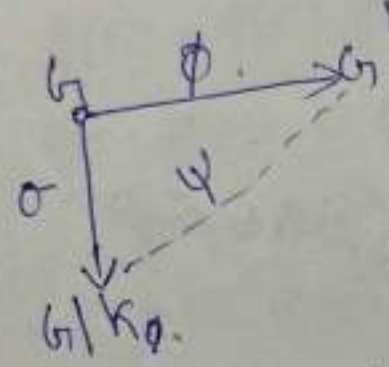
Proof

K_ϕ is a normal subgroup.

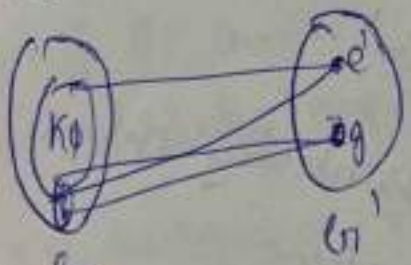
$\exists\ \sigma: G \to G/K_\phi$ is always a homomorphism

$\phi: G \to G'$.

if there is a homomorphism b/w $G \to G'$ and $G \to G/K_\phi$, then there is an isomorphism from G/K_ϕ to G' that is onto



- $\phi: G \to G'$, $e \in K_\phi$ always.



choose $g \in G'$.

if $\phi(x) = g$ (x is a pre-image of g).

then we can find all pre-images of G.

$\phi(y) = g \Rightarrow y \in K_\phi x$.

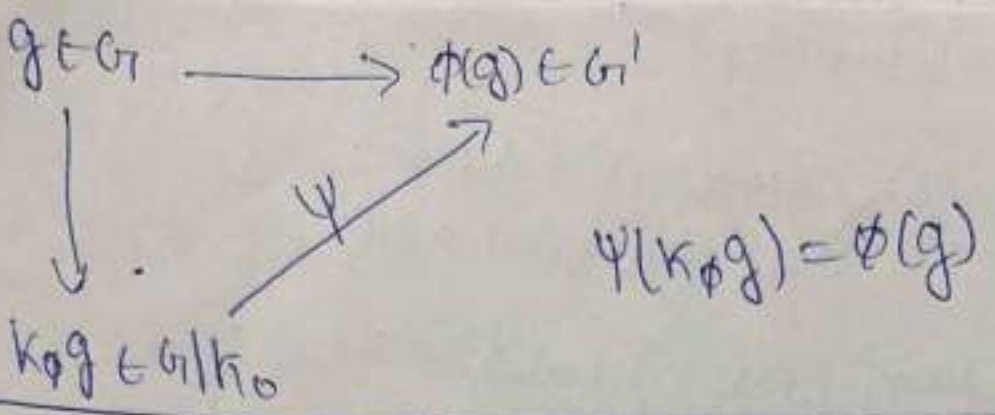
→ set of all preimages of g.

(right coset of K_ϕ)

if it is onto, no. of $|G'|$ = no. of right cosets of K_ϕ.

no. of right cosets of K_ϕ = cardinality of G

i.e. order of G/K_ϕ



$$\psi(K_\phi g) = \phi(g)$$

Ring Theory

Definitions

- A ~~set~~ non-empty set R, with two associated binary operations $+, \cdot$ $(R, +, \cdot)$ is a ~~ring~~ ~~of~~ non-associative ring if.
  - (a) $(R, +)$ is an abelian group ($+$ is some operation rardo)
  - (b) ~~(R+)~~ Distributive law $a \cdot (b+c) = a \cdot b + a \cdot c$ and $(b+c) \cdot a = b \cdot a + c \cdot a$
  - (c) closure $\forall a, b \in R \quad ab \in R$ only (other 4 don't hold)

(say if only closure and distribution law hold for R over '$\cdot$' is called a non-associative group)

* if we add (d) associativity $\forall abc \in R \; a(bc) = (ab) \cdot c$ $(R, +, \cdot)$ is then called an associative ~~group~~ ring.

x if we add (e) identity $\exists I \in R$ s.t. $\forall a \in R \; aI = a = I \cdot a$. $(R, +, \cdot)$ is then called a (Associative) ring with unit identity.

* if we add (f) inverse: $\forall a \in R \; \exists b$ s.t. $ab = I = ba$. (over $(R, \cdot)$) $(R, +, \cdot)$ is then called.

Y if (g) commutativity holds over $(R, \cdot)$ then it is called

(a)-(b) (g) → commutative ring.

division ring → (a) (b) { (R,+) is abelian, (R\{0},·) is a grp.

field → (a) (b)
(R,+) abelian, (R\{0},·) is abelian

Examples of Rings

- (R,+,*) is a ~~ring → commutative ring~~ field

- ({0,1,2,3,4,5}, +, * (mod 6)).

(R,+) is abelian
(R,*) is closed.
distribution holds
commutative holds
I = 1,
inverse does not exist for 2,3.
∵ 2^{-1} mod 6 (gcd(2,6) ≠ 1)

} this is a commutative ring with unit

- ($\mathbb{E}$, +, *) → evens

($\mathbb{E}$,+) is abelian
(E,*) is closed
(E,*) is associative
(E,*) is commutative
(E,*) inverse does not exist
(E,*) identity does not exist
(E,+,*) distributive holds.

• $(\mathbb{Z}, +, *)$ commutative

Th^{m}: $a \in R$ and $a \neq 0$ is called a zero divisor if $\exists\, b \neq 0$ s.t $a \cdot b = 0$.

e.g. in $(\{0,1,2,3,4,5,6\}, +, * \bmod 6)$ $\quad \because 2 \cdot 3 = 6 \bmod 6 = 0$ //.

2, 3 are zero divisors

* commutative rings with unit element are of 2 types

1) have zero divisors

2) don't have zero divisors → "Integral Domain"

~~Analogous~~ **Th^{m} :** ∀

* In any ring $(R, +, \cdot)$

$\forall\, a \in R,\ 0 \cdot a = a \cdot 0 = 0$.

$\forall\, a, b \in R,\ a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$

Proof:

i) $0 \cdot a = (0+0) \cdot a$

$0 \cdot a = 0 \cdot a + 0 \cdot a$

$0 = 0 \cdot a$

$a \cdot 0 = a \cdot (0+0)$

$a \cdot 0 = a \cdot 0 + a \cdot 0$

$0 = a \cdot 0$

ii) $a \cdot (-b) = a \cdot (0-b) = a \cdot 0 - a \cdot b = -a \cdot b$.

$(-a) \cdot b = (0-a) \cdot b = 0 \cdot b - a \cdot b = -a \cdot b$.

OR RA style -

Th^m Every finite integral domain is a field.

$\{0,1,2,3,4,5,6\}, +, *$ (mod 7)

mod n commutative ring. if n is prime it has no zero divisors.

↳ ∴ it is a finite integral domain ∴ it is a field

$\Rightarrow (S, +, *$ mod (prime)) is always a field.

Proof:

integral domain → comm. ring, ~~(identity) unit element~~, no zero divisors.

field → comm. ring, $(R\setminus\{0\}, *)$ is abelian.

∴ D is I, and a^{-1} may not exist in integral domain

‖ have to exist for fields.

∴ need to prove ∃ a^{-1} exists

1) Multiplicative Identity exists

2→ finite domain $\{x_1, x_2, \cdots, x_n\} = D$.

$a \neq 0$, $a \in D$

consider $\{a\cdot x_1, a\cdot x_2, a\cdot x_3, \cdots, a\cdot x_n\}$

all are distinct (∵ if not $ax_1 = ax_2 \Rightarrow a(x_1 - x_2) = 0$.

but no zero divisors

∴ a is not a zero div

but then $x_1 = x_2$)

$\exists x_i$ s.t. $a \cdot x_i = a$.

$\forall y \in D$, $y \cdot x_i = ?$ Let $y = a \cdot x_j$

$y \cdot x_i = a \cdot x_j \cdot x_i$

$y \cdot x_i = x_j \cdot a \cdot x_i$ ∵ comm. ring.

$y \cdot x_i = x_j \cdot a = a \cdot x_j = y$.

∴ $y \cdot x_i = y \quad \forall y \in D \Rightarrow x_i$ is identity.

∴ in any finite integral domain, a multiplicative identity exists

∎

2) Multiplicative inverse exists.

$a \cdot x_k = x_i = 1$

$x_k = a^{-1}$ //,

* prove other side using $x_i \cdot a$, $x_2 \cdot a$, ...

to show $x_i \cdot a = a$

and $a^{-1} \cdot a = x_i$

// QED

- any mod p under +x form finite fields (p is prime).
- $\{0,1,2,3,4,5,6\}, +, \times\}$ mod 7 → char of this field is 7.

let $a \in$ $a+a+a+a+a+a+a = 0$ always.

- Characteristic field:

→ A field is said to be char = 0 if $ma = 0 \Rightarrow m = 0$.

else

char = $p \neq 0$ s.t. $\underbrace{a+a+\cdots+a}_{p \text{ times}} = p \cdot a = 0$.

- char. of reals is 0.

Groups	Rings
• cosets ⟷ (R+I)	• cosets
• normal subgroups	ideals
• homomorphisms	homomorphism.
• Kernel is a normal subgroup	Kernel is an Ideal
• Quotient Groups	• Quotient Rings
• if $\phi: G \to G'$ is a homo., $G/K_\phi \cong G'$	$\sigma: R \to R/I_\phi$ is a homo., $R/I_\phi \cong R'$ (R/I_ϕ is isomorphic to R')

Ring Homomorphisms

- $\phi: R \to R'$ is a homomorphism if
  - i) $\forall a, b \in R$, $\phi(a+b) = \phi(a) + \phi(b)$
  - ii) $\forall a, b \in R$, $\phi(ab) = \phi(a)\phi(b)$

($\phi(a+b)$: operations in R; $\phi(a)+\phi(b)$: operations in R')

Thm: $\phi(0) = 0$.
$\phi(-a) = -\phi(a)$, $\forall a \in R$.

$\because R$ is an abelian group w.r.t $(R, +)$.

Kernel of ~~ϕ~~ (homo), I_ϕ

$I_\phi = \{x \in R \mid \phi(x) = 0\}$ mapped to ↳ identity in R'.

Thm: if $\phi: R \to R'$ is a homomorphism, then:

a) $(I_\phi, +)$ is a group.

b) $\forall r \in R, \forall a \in I_\phi, ar \in I_\phi \; ra \in I_\phi$.

Proof:

a) R is an abelian group wrt +,
$(I_\phi, +)$ is a normal subgroup.
trivial.

b) $\phi(ar) = \phi(a) \cdot \phi(r)$
$\phi(ar) = 0 \cdot \phi(r) = 0$ → last class.

Ideals

- A subset U of R is an ideal if:

a) $(U, +)$ is a group

b) $\forall r \in R, \forall u \in U, u \cdot r \in U$ and $r \cdot u \in U$

Quotient Ring R/U ; U is an ideal.

- Let R/U ~~be the set of~~ all

$R/U = \{\{u + a \mid u \in U\} \mid a \in R\}$

↳ * right cosets are generated through addition.

$R/U = \{u + a \mid a \in R\}$.

$U + a = \{u + a \mid u \in U\}$.

G/N is the set of all right co-sets of N.

R/U is the set of all right cosets of U

- $(R/U, +, \cdot)$

$(U+a) + (U+b) = U + (a+b)$

$(U+a) * (U+b) = U + (a*b)$

↳ $(U+a)$ $(U+b)$ $(U+c)$

$[(U+a)+(U+b)] \cdot (U+c)$

$= [U+(a+b)] \cdot (U+c)$

$= U + (a+b) \cdot c$

$U + ac + bc.$

Ideals

- Trivial ideals
  - ↳ identity
  - ↳ const. to 0.

$U = \{0\}$.

$U = R$.

- $G : G \to (G/N, *)$ | $\sigma : R \to R/N$

$\sigma(a) = Na$ | $\sigma(a) = U + a$

Rings → Fields → special kinds of rings.

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$

When will a ring behave a field?

Thm: If every ideal U of the (commutative) ring R is trivial then R is a field.

Proof:

$Ra = \{ra \mid r \in R\}$.

↳ is an ideal → both trivial ideal.

$\therefore Ra = R$, $a^{-1} \in R \therefore \exists r$ s.t. $ra = a^{-1}$

$\Rightarrow$ inverse exists → identity exists

$\therefore$ field //.