Last lecture: $\boxed{L3}$

Defined groups
1) Closed
2) Associativity
3) Identity
4) Inverse

Examples: $\mathbb{Z}_n$

① $x * y = x + y + xy, \quad \{x \in \mathbb{R}, x \neq -1\}$

$$(x * y) * z = (x + y + xy) * z = x + y + xy + z + xz + yz + xyz$$
$$= x * (y + z + yz)$$
$$= x * (y * z)$$

$$x + e + xe = x$$
$$e(1+x) = 0$$
$$e = 0 \qquad (x \neq -1)$$

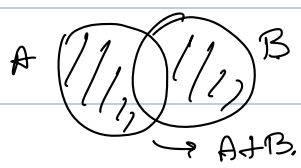
$$x + x^{-1} + xx^{-1} = 0$$
$$x + x^{-1}(1+x) = 0$$
$$\Rightarrow x^{-1} = -\frac{x}{1+x}$$

② D is a set, then the power set of D is the set P_D of all the subsets of D.

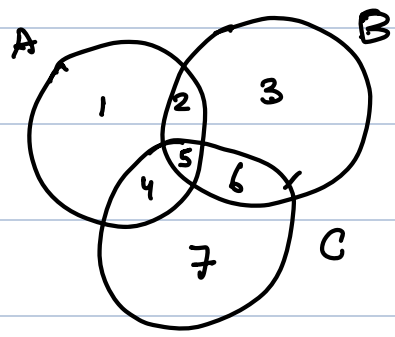
$$P_D = \{A : A \subseteq D\}$$

Operation + defined as

$$A + B = (A - B) \cup (B - A).$$



$(A+B)+C$



$A+B$

$\downarrow$

$1+4+3+6$

$(A+B)+C \quad 1+3+5+7$

$A+(B+C) \longrightarrow$

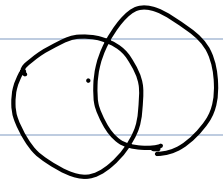
$B+C := 3+2+4+7$

$A+(B+C) := 1+3+5+7$

Associativity ✓

Identity

$A + E = A$



$(A - E) \cup (E - A)$

$E = \emptyset$

Inverse

$A + A^{-1} = \emptyset$

$(A - A^{-1}) \cup (A^{-1} - A) = \emptyset \rightarrow$ identity

$A^{-1} = A$

$D = \{a, b, c\}$

$P_D = \{\{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}, \emptyset\}$

Ex.3 A Coin Game

2 coins on a table, at positions A & B.

8 possible moves:

M_1: Flip over the coin at A.

M_2: " " " " " B.

M_3: " " both coins

M_4: Switch the "

M_5: Flip at A then switch

M_6: " " B then "

M_7: " both coins then switch

I: Do not change anything.

$A = \{I, M_1, \ldots, M_7\}$

operation: Perform any 2 moves in succession.

$M_4 * M_1 = M_2 * M_4 = M_6$

Associativity: $(M_i * M_j) * M_k$ performing M_i, M_j in succession, then move M_k;

$\langle G, * \rangle$

$M_i * (M_j * M_k)$ performing M_i, then M_j & M_k in succession.

Identity: I

Inverse: Look at the group table below

Order of a group

$|G|$ = no. of elements in G.

G is finite if $|G| < \infty$.

$|\mathbb{Z}_n| = n$

$|\mathbb{Z}_n^*| = ?$

$\varphi(n)$

	I	M_1	M_2	M_3	M_4	M_5	M_6	M_7
I	I	M_1	M_2	M_3	M_4	M_5	M_6	M_7
M_1	M_1	I	M_3	M_2	M_5	M_4	M_7	M_6
M_2	M_2	M_3	I	M_1	M_6	M_7	M_4	M_5
M_3	M_3	M_2	M_1	I	M_7	M_6	M_5	M_4
M_4	M_4	M_6	M_5	M_7	I	M_2	M_1	M_3
M_5	M_5	M_7	M_4	M_6	M_1	M_3	I	M_2
M_6	M_6	M_4	M_7	M_5	M_2	I	M_3	M_1
M_7	M_7	M_5	M_6	M_4	M_3	M_1	M_2	I

Remarks on notation:

Suppress the notation $*$.

$ab = a * b$

$a^2 = a * a$

$a^n = \underbrace{a * a * \cdots * a}_{n \text{ time}}$

$a^{-n} = (a^{-1})^n$

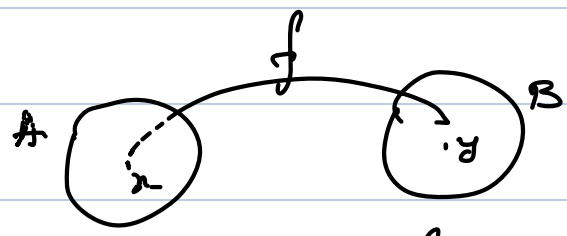
in $\mathbb{Z}$, $a^n = \underbrace{a + a + \cdots + a}_{n \text{ time}} = na$

Further examples:

$f : A \to B$

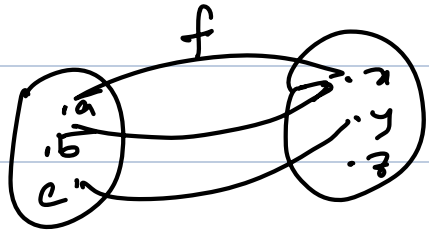
every $x \in A$

unique $f(x) \in B$
$= y$



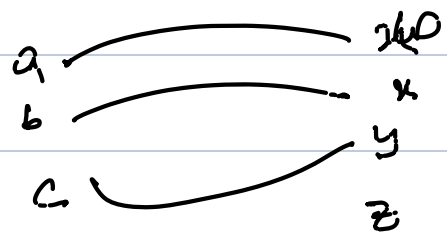
domain of $f = A$

$f(A)$ = range of f



ran $= \{x, y\}$.

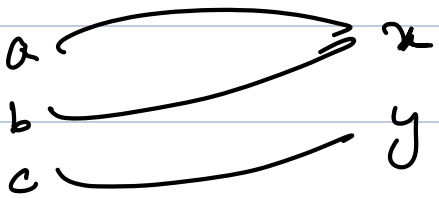
Injective : each element of B is image of no more than 1 element of A



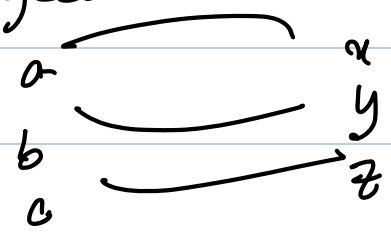
$f(a) = f(b)$

$\Rightarrow a = b$

Surjective : each element of B is image of at least 1 element of A



Bijective : both injective & surjective



Composition of funcⁿ.

$f : A \to B$ & $g : B \to C$

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

$f(x) = 2x \quad ; g(x) = x+1$

$f(g(x)) = 2x+2$

$g(f(x)) = 2x+1$

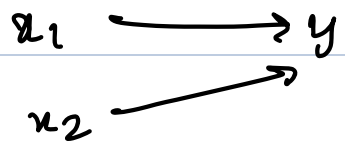
f, g injective, then $g \circ f$ injective

f, g surjective, " $g \circ f$ surjective

f, g bijective, " $g \circ f$ bijective

$f: A \to B$ not injective

no inverse



$f(x_1) = y$

$f^{-1}(y) = x_1$

$f(x_2) = y$

$f^{-1}(y) = x_2$

$f: A \to B$ not surjective

$\exists\, y \in B$ not in A

$f^{-1}(y)$ does not exist.

f^{-1} cannot be a fun^n from B to A.

if bijective $\to f^{-1}$ exists

$S_X = \{ f: X \to X : f \text{ is a bijection} \}$

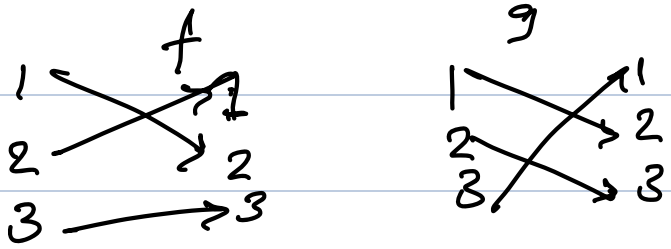
closed under composition

Associative

Identity $\quad id_X(x) = x$

Inverse $\quad f \circ f^{-1}(y) = f(x) = y = id_X(y)$

Not commutative



$g(f(1)) = g(2) = 3$

$f(g(1)) = f(2) = 1$

$g \circ f \neq f \circ g$.

$S_X \to$ non-abelian $\boxed{L4}$

$|X| = \infty$, S_X fairly hard to understand

$|X| = n$

Does not matter what X is, only matters that X has 'n' elements.

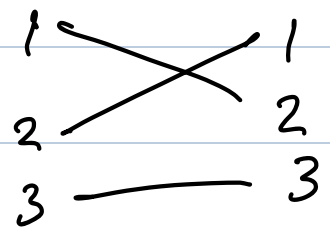
$X = \{1, 2, \ldots, n\}$

S_X symmetric group of n elements

An element of S_n is a bijection from $\{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$

rearranges the nos. 1 to n.

σ of $\{1, 2, 3\}$



permutation of the integers 1 through 1 to n.

Defn: S_n: set of all permutations of the set $\{1, 2, \ldots, n\}$.

How many

n choices for $\sigma(1)$

$n-1$ " " $\sigma(2)$

$\vdots$

$n(n-1) \cdots 1 = n!$

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & & \sigma(n) \end{pmatrix}$$

$\sigma(1) = 2 \quad \sigma(2) = 1 \quad \sigma(3) = 3$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ \sigma(\tau(1)) & \sigma(\tau(2)) & \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$\sigma\tau \neq \tau\sigma$

S_3 is non abelian

Prop^n: For $n \geq 3$, S_n is a non abelian group.

Pf: Let $\sigma, \tau \in S_3$ as defined

$n > 3$

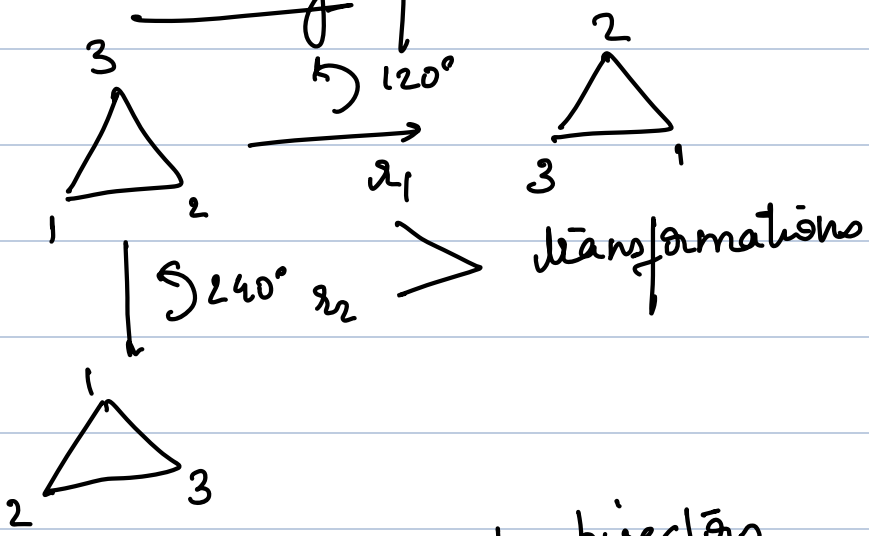
$\tilde{\sigma}, \tilde{\tau} \in S_n$

$$\tilde{\sigma}(i) = \begin{cases} \sigma(i) & 1 \leq i \leq 3 \\ i & i > 3 \end{cases}$$

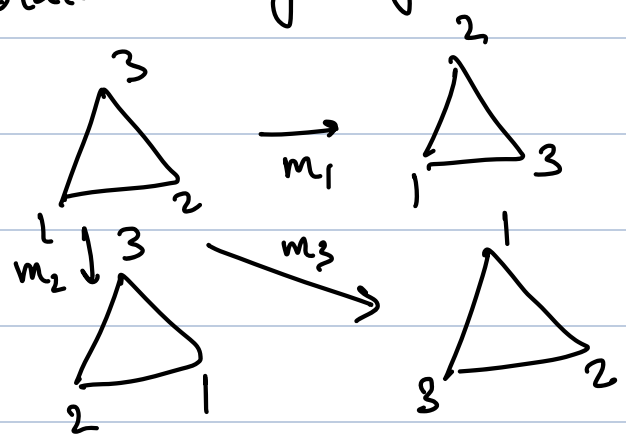
$\tilde{\tau}$

$\tilde{\sigma} \circ \tilde{\tau} \neq \tilde{\tau} \circ \tilde{\sigma}$. S_n is non abelian

Dihedral group



Rotation along angle bisectors



identity transformation i : unmoved.

$\{i, r_1, r_2, m_1, m_2, m_3\}$ set of symmetries of the Δ.

Exactly the transformations of the Δ that reorder the vertices in a way that exploits the symmetry of the equilateral Δ.

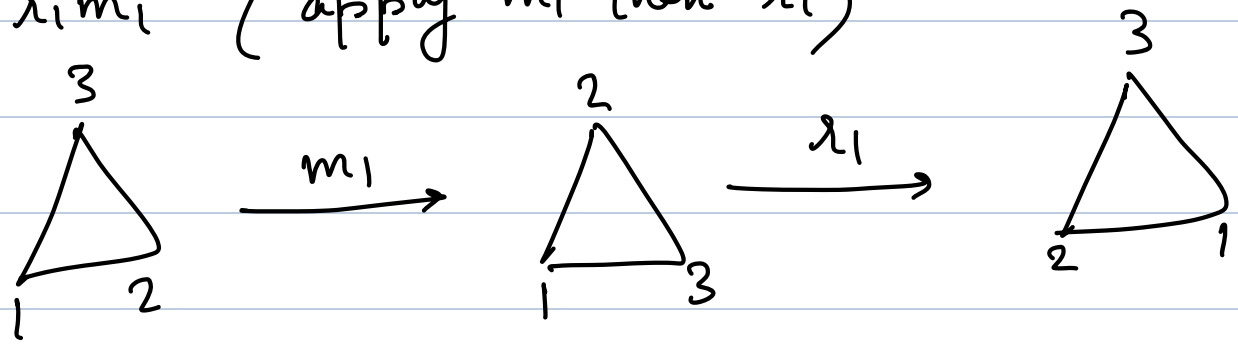
D_3

D_n : nth dihedral group (set of symmetries of a regular n-gon)

operation : composition of transformations

Order of $D_n = 2n$ (n rotations, n reflections)

$r_1 m_1$ (apply m_1 then r_1)



<u>Properties</u>

Thm: Let G be a group. Then

(i) The identity element $e \in G$ is unique.

(ii) Every $a \in G$ has a unique inverse in G.

(iii) For every $a \in G$, $(a^{-1})^{-1} = a$

(iv) For all $a, b \in G$, $(a \cdot b)^{-1} = b^{-1}a^{-1}$

Pf: (i) $a = a \cdot e = e \cdot a = a \cdot f = f \cdot a$, Then $e = f$ (to show)

$e \cdot a = a \quad \forall\, a \in G$

$e \cdot f = f$ — (i)

Since $b \cdot f = b \quad \forall\, b \in G$

$e \cdot f = e$ — (ii)

$\Rightarrow f = e$.

To prove other parts, we first prove "cancellation"

<u>Cancellation Laws</u> Let G be a group, & let $a, b, c \in G$. Then:

(i) If $ab = ac$, Then $b = c$

(ii) $ba = ca$ then $b = c$

Pf (i) $ab = ac$

$a^{-1}(ab) = a^{-1}(ac)$ By associativity,

$\Rightarrow (a^{-1}a)b = (a^{-1}a)c$

$\Rightarrow b = c$

(ii) $ba = ca$

$ba a^{-1} = ca a^{-1}$

$b = c$

Pf. of (ii) of thm. 1

suppose $a \in G$ &

$ax = xa = e$

& $ay = ya = e$

$\Rightarrow ax = ay \Rightarrow x = y$ by above

(iii) $(a^{-1})^{-1} = a$ To prove

$a^{-1}(a^{-1})^{-1} = e$

$a a^{-1}(a^{-1})^{-1} = a.e$

$(a^{-1})^{-1} = a$

(iv) For all $a, b \in G$

$(ab)^{-1} = b^{-1}a^{-1}$ T.P.

$ab(ab)^{-1} = e$

$a^{-1}ab(ab)^{-1} = a^{-1}.e = a^{-1}$

$b^{-1}a^{-1}ab(ab)^{-1} = b^{-1}a^{-1}$

Q.1 $(ab)^2 = a^2b^2$ for all $a, b \in G$,
show that G must be Abelian.

Q.2 If G is an abelian group, Then for all $a, b \in G$ & all integer

$$(a \cdot b)^n = a^n \cdot b^n$$

$$abab = aa^2b^2$$

$$ba = ab$$

Q.3 $(a \cdot b)^i = a^i b^i$ for 3 consecutive integer i $\forall a, b \in G$

show that G is abelian

$$(ab)^i = a^i b^i$$

$$(ab)^{i+1} = a^{i+1} b^{i+1}$$

$$(ab)^{i+2} = a^{i+2} b^{i+2}$$

$$(ab)^i ab = a^i a b^i b$$

$$a^i b^i a = a^i a b^i$$

$$(ab)^{i+1} ab = a^{i+1} a b^{i+1} b$$

$$b^{i+1} ab = ab^{i+1}$$

$$b^i ba = abb^i \quad ab^i b$$

$$= b^i ab$$

Q.4 If G is of even order, prove it has an element $a \neq e$ satisfying $a^2 = e$.

—— x —— . $\boxed{L5}$

The order of an element & cyclic group.

Def^n: Given a group G & an element $a \in G$, we define

$$\langle a \rangle = \{ a^n : n \in \mathbb{Z} \}$$
$$= \{ \ldots, a^{-2}, a^{-1}, e, a, a^2, a^3 \ldots \}$$

Prop^n: Let G be a group, & let $a \in G$.

(a) $a^n a^m = a^{n+m} \quad \forall\, n, m \in \mathbb{Z}$

(b) $(a^n)^{-1} = a^{-n} \quad \forall\, n \in \mathbb{Z}$

(c) $(a^n)^m = a^{nm} \quad \forall\, m, n \in \mathbb{Z}$

Powers of elements

Let $G = \mathbb{Z}_{12}$.

Powers of 2.

Powers of 3

elements have finite order.

Defn: Let G be a group. An element $a \in G$ has finite order if $\exists\, n \in \mathbb{Z}^+$ s.t $a^n = e$. The smallest such integer is called the "order" of a.

$o(a)$ $(|a|)$

no such integer Then a has infinite order.

Ex. 1. The identity element in any group has order 1.

2. In $\mathbb{Z}_{12}$, $o(2) = 6$
$o(3) = 4$

3. D_3 $o(m_1) = 2 = o(m_2) = o(m_3)$
$o(r_1) = o(r_2) = 3$

4. In $\mathbb{Z}$, 5 has infinite order, so do all other el

Which elements have finite order?

Prop^n: Let G be a finite group. Then every element $a \in G$ has finite order.

Pf: Consider the set

$$\{a^n : n \geq 0\} = \{e, a, a^2, \dots\}.$$

cannot be infinite!

$$a^i = a^j \quad j \neq i$$

assume $j > i$.

Then, $a^{j-i} = a^j a^{-i} = a^i a^{-i} = e$

$\Rightarrow$ a has finite order $(o(a) \leq j-i)$

Since $a \in G$ was arbitrary, the result follows.

Converse of above prop^n?

If G is a group in which every element has finite order, is G finite?

No!

$GL_n(\mathbb{R}) \longrightarrow$ infinite group

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

finite order

Thm. 2: (Properties of order) G group. $a \in G$

① $o(a) = o(a^{-1})$

② If $o(a) = n$ & $m \in \mathbb{Z}$, then $a^m = e$ iff $n \mid m$.

③ If $a \in G$ & $o(a) = n$ then
$a^i = a^j$ iff $i \equiv j \ (n)$.

④ If $a \in G$ has infinite order. Then all powers of a are all distinct
$(a^i = a^j$ iff $i = j)$

Pf. ① Case 1: Suppose a has finite order. $o(a) = n$. Then,

$$(a^{-1})^n = a^{-n} = (a^n)^{-1} = e.$$

So, $o(a^{-1}) \leq n = o(a)$.

Let $m = o(a^{-1})$, then

$$a^m = ((a^{-1})^{-1})^m = (a^{-1})^{-m}$$
$$= ((a^{-1})^m)^{-1} = e$$

$n \leq m$. Thus, $n = m$ & $o(a) = o(a^{-1})$.

Case 2: Suppose a has infinite order.
Then, for all $n \in \mathbb{Z}^+$, we have

$$a^n \neq e.$$

$$(a^{-1})^n = a^{-n} = (a^n)^{-1} \neq e.$$

$\forall n \in \mathbb{Z}^+$

$\Rightarrow a^{-1}$ must have infinite order as well.

Pf. of (2) If $n|m$, it is easy.
$m = nd$ for some $d \in \mathbb{Z}$. Then

$$a^m = a^{nd} = (a^n)^d = e^d = e.$$

If $m \geq n$
$m = qn + r$. Then

$$e = a^m = a^{qn+r} = (a^n)^q a^r$$
$$= a^r$$

But $r < n$, & n is the smallest positive power of a which yields the identity. Therefore

$$r = 0$$

& $n|m$.

(3) $a^{j-i} = e$ iff $n = o(a) \mid j-i$
$i \equiv j \mod n$.

Thm. Let G be a group, $a \in G$ an element of finite order, say $o(a) = n$, & let $m \in \mathbb{Z}$. Then

$$o(a^m) = \frac{n}{\gcd(m,n)}$$

Pf: Let $d = \gcd(m,n)$. Then

$$(a^m)^{n/d} = (a^n)^{m/d} = e$$

$$\Rightarrow \quad o(a^m) \leq n/d$$

Suppose that $k \in \mathbb{Z}^+$ &

$$a^{mk} = (a^m)^k = e$$

$$\Rightarrow \quad n \mid mk$$

$$\Rightarrow \quad n/d \mid mk/d$$

But $\gcd(m/d, n/d) = 1$

$$\Rightarrow \quad n/d \mid k.$$

$$\Rightarrow \quad n/d \leq k$$

so $o(a^m) = n/d$.

Cyclic groups

Def^n: For $a \in G$, $\langle a \rangle$ cyclic subgroup generated by a

Def^n: A group G is called cyclic if $G = \langle a \rangle$ for some $a \in G$.
The element a is called a 'generator' for G.

Ex. $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$

$\mathbb{Z}_n = \langle 1 \rangle$
$\hookrightarrow$ more generators — discussion later.

$\langle \mathbb{Q}, + \rangle$ not cyclic

$\frac{np}{q} = 1/r$ choose r (prime) $\nmid q$

$\Rightarrow npr = q$
$\Rightarrow r \mid q$
$\rightarrow \Leftarrow$

D_3 is not cyclic

Thm. (i) If $G = \langle a \rangle$ is cyclic, then $|G| = o(a)$

(ii) The generators of a finite cyclic group $G = \langle a \rangle$ of order n are precisely the elements a^r for which $\gcd(r, n) = 1$.

Pf: If a has infinite order
$\Rightarrow G$ is infinite

if $o(a) = n$ $\quad a^i = a^j$ iff $i \equiv j \mod n$,

elements of G: $e, a, a^2, \ldots, a^{n-1}$,

(ii) $$o(a^r) = \frac{n}{\gcd(r,n)}$$

Now, $G = \langle a^r \rangle$ iff $o(a^r) = n$
iff $\gcd(r,n) = 1$

$\boxed{L-6}$

The previous result allows us to characterize the generators of $\mathbb{Z}_n$.

Recall $\mathbb{Z}_n = \langle 1 \rangle$

other generators $= 1^m$ where $\gcd(m,n) = 1$
$= m$

$\Rightarrow$ An element $m \in \mathbb{Z}_n$ is a generator of $\mathbb{Z}_n$ iff $\gcd(m,n) = 1$.

Thm.
Let G be a finite cyclic group. Then for any $b \in G$, we have

(i) $b^{|G|} = e$

(ii) $o(b) \mid |G|$

Pf. of (i) Let $G = \langle a \rangle \Rightarrow |G| = o(a)$

$b = a^k$ for some $k \in \mathbb{Z}$

$$b^{|G|} = b^{o(a)} = a^{k\,o(a)} = e$$

(ii) By a previous result.

Remark: The last result is true for any finite group. Will see this later!

Thm. Every cyclic group is abelian.

The converse is not true!

There are abelian groups that are not cyclic.

Ex. $(\mathbb{Q}, +)$.

Klein 4-group $V_4 = \{e, a, b, c\}$

$$a^2 = b^2 = c^2 = e \quad \&$$

$$ab = c, \; bc = a, \; ca = b.$$

Check: Abelian & non-cyclic

Subgroups

Let $(G, *)$ be a group. A subgroup of G is a nonempty subset $H \subseteq G$ with the property that $(H, *)$ is a group.

Notation: $H \leq G$.

$H < G$ but $H \neq G$,

H is a proper subgroup of G.

To check subgroup, Things to verify

(i) H is closed under the operation on G.

(ii) The identity element $e \in G$ is in H.

(iii) For every $a \in H$, its inverse $a^{-1} \in H$.

Examples: Trivial subgroups

(i) $\{e\}, G$

(ii) $n\mathbb{Z} \leq \mathbb{Z}$

(iii) $\mathbb{Q} \leq \mathbb{R}$

(iv) Set of rotations

$H = \{i, r_1, r_2, \ldots, r_{n-1}\}$ in D_n

closed ✓

identity $i \in H$, for any $1 \leq j \leq n-1$,

$r_j^{-1} = r_{n-j}$

(v) $SL_n(\mathbb{R}) \leq GL_n(\mathbb{R})$

<u>Cyclic subgroups</u>

$\langle a \rangle$ called 'cyclic subgroup' generated by a.

$\downarrow$

smallest possible subgroup of G which contains a.

i.e if $H \leq G$ & $a \in H$, then $\langle a \rangle \subseteq H$

Subgroup criteria

Can collapse the usual subgroup axioms into a single condition.

Thm A Let G be a group. A non empty subset $H \subseteq G$ is a subgroup iff whenever $a, b \in H$, $ab^{-1} \in H$.

Pf. Suppose that $H \leq G$, let $a, b \in H$
then $ab^{-1} \in H$

Conversely, suppose that $ab^{-1} \in H$ $\forall$ $a, b \in H$
Then for any $a \in H$, take $a = b$

$e = aa^{-1} \in H$. $(\Rightarrow e \in H)$

$a^{-1} = e.a^{-1} \in H$ (H is closed under inverses)

if $a, b \in H$ $\Rightarrow$ $b^{-1} \in H$

$\Rightarrow$ $b^{-1}a^{-1} \in H$

$ab = ((ab)^{-1})^{-1} = (b^{-1}a^{-1})^{-1} \in H$

More interesting but works only for finite subset of a group G.

Thm. B Let G be a group & H a non empty finite subset of G. Then $H \leq G$ iff H is closed under the operation on G.

Pf: $\Leftarrow$ Need to verify $e \in H$
$a^{-1} \in H$ for every $a \in H$

$\{e\} \leq G$,
assume that H is non trivial,
i.e $a \neq e \in H$

Since H is closed

$$a, a^2, a^3 \ldots \in H$$

Since H is finite

$$a^i = a^j \quad \text{for some}$$
$$1 \leq i < j \leq |H|$$

$$a^{j-i} = e$$
$$\Rightarrow e \in H.$$

Now observe that $j-i-1 \geq 0$, so

$$a^{j-i-1} \in H$$

Now, $a a^{j-i-1} = e \in H$

$\Rightarrow a^{-1} = a^{j-i-1} \in H.$

$\Rightarrow H \leq G.$

$\boxed{1-7}$

Subgroups of cyclic groups

Thm. 1 A subgroup of a cyclic group is cyclic.

Pf: let $G = \langle a \rangle$

$H \leq G$

Assume $H \neq \{e\} \Rightarrow$

H contains an element $b \neq e$ which is of the form a^m for some $m \in \mathbb{Z}$ since $G = \langle a \rangle$.

Let m be the smallest positive integer for which $a^m \in H$

Claim: $H = \langle a^m \rangle$

Pf. Suppose $a^n \in H$

$n = qm + r$

$a^n = (a^m)^q a^r$

$\Rightarrow a^r \in H \qquad (a^r = a^n a^{-mq})$

But $r < m$ (assumed m smallest)

$\Rightarrow \quad r = 0$

$$a^n = (a^m)^q$$

$$a^n \in \langle a^m \rangle$$

$$\Rightarrow \quad H \subseteq \langle a^m \rangle$$

$$\& \quad \langle a^m \rangle \subseteq H$$

$$\Rightarrow \quad H = \langle a^m \rangle.$$

Thm. 2 Let $G = \langle a \rangle$ be a cyclic group of order n. If m is a positive divisor of n. Then G has exactly 1 subgroup of order m.

Pf: First, we show that G has a subgroup of order m whenever $m \mid n$.

Suppose $m \mid n$

Consider $b = a^{n/m}$

$$o(b) = o(a^{n/m}) = \frac{n}{\gcd(n, n/m)} = \frac{n}{n/m}$$

$$= m$$

$\langle b \rangle \subseteq G$ of order m

Uniqueness: Suppose $a^j \in G$ s.t

$$o(a^j) = m$$

$$m = o(a^j) = \frac{n}{\gcd(j,n)} = \frac{n}{\gcd(n, n/m)}$$

$$\Rightarrow \gcd(j,n) = \gcd(n, n/m) = n/m$$

$$\Rightarrow \frac{n}{m} \mid j$$

$$\Rightarrow j = kn/m$$

$$a^j = (a^{n/m})^k = b^k$$

$$\Rightarrow a^j \in \langle b \rangle$$

& since both have same no. of elements

$$\langle a^j \rangle = \langle b \rangle.$$

Ex. All subgroups of $\mathbb{Z}_{12}$.

divisors: $\underbrace{1, 2, 3, 4, 6 \text{ \& } 12}_{\text{1 subgroup of each order}}$

order	1 :	$\{0\}$	$\langle 12 \rangle$	$\langle 3 \rangle$
"	2 :	$\{0, 6\}$	$\langle 6 \rangle$	$\langle 2 \rangle$
"	3 :		$\langle 4 \rangle$	$\langle 1 \rangle$

Lagrange's theorem

Recall, For $G = \langle a \rangle$ finite,
$o(b) \mid o(G)$ for any $b \in G$.

$\Rightarrow$ if $H < G = \langle a \rangle$, then
$H = \langle a^m \rangle$ for some $m \in \mathbb{Z}$,

and $o(H) = o(a^m)$

$$o(a^m) = \frac{o(a)}{\gcd(m, o(a))}$$

$$\Rightarrow o(a^m) \mid o(a)$$

$$\Rightarrow o(H) \mid o(G).$$

But this holds more generally,

Thm. (Lagrange). Let G be a finite group & $H < G$. Then $|H|$ divides $|G|$.

We will prove this later!

Number of elements of each order in a finite cyclic group.

Let $G = \langle a \rangle$ & $|G| = n$

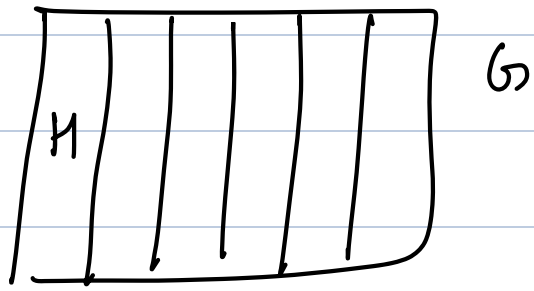
Exactly 1 subgroup of order $d \mid n$.
Let it be $\langle b \rangle$
$$o(b) = d.$$
Any other element of order d will also generate the same subgroup $\langle b \rangle$.
But b^k will generate b if & only if $\gcd(k, d) = 1$

$\Rightarrow$ If d is a positive divisor of n, the no. of elements of order d in a cyclic group of order n is $\phi(d)$.

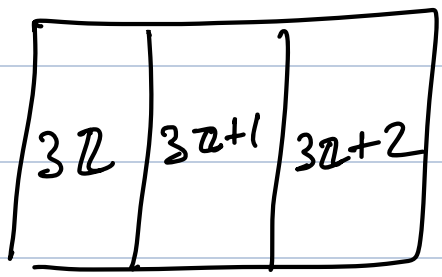
Ex. # of elements of order 6 in $\mathbb{Z}_8$ $= \phi(6)$
$\mathbb{Z}_{640}$
$\mathbb{Z}_{10}$

Lagrange's thm.

Partition G into subsets using H



For eg. $G = \mathbb{Z}$



Equivalence relation is a method of <u>partitioning</u> a group.

Thm. Let $\sim$ be an equivalence relation on a set S. The equivalence classes of $\sim$ partition S, in the sense that

① Given $a, b \in S$, either $[a] \cap [b] = \emptyset$ or $[a] = [b]$.

② S is the union of all the equivalence classes of $\sim$. Every element of S belongs

to some equivalence class (& only 1 by ①)

Pf: ① If $[a] \cap [b] \neq \emptyset$

$\exists\ c \in [a] \cap [b]$

$\Rightarrow\ a \sim c$ & $b \sim c$

$\Rightarrow\ a \sim b \Rightarrow a \in [b]$

$\Rightarrow [a] \subset [b]$

$[b] \subset [a]$

$\Rightarrow [a] = [b$

② Every $a \in S$ belongs to one of the equivalence classes. $a \in [a]$.

Now, partition G into subsets, each determined by a fixed subgroup H.

Let G be a group & $H \subset G$. Define a relation $\sim_H$ on G by:

$a \sim_H b$ if & only if $ab^{-1} \in H$.

Check: It is an equivalence relation!

What are the equivalence classes of $\sim_H$?

$$[a]_H = \{ b \in G : b \sim_H a \}$$
$$= \{ b \in G : ba^{-1} \in H \}$$

$$ba^{-1} = h \Rightarrow b = ha.$$

Define $Ha = \{ ha : h \in H \}$

$\Rightarrow$ $[a]_H \subseteq Ha$

Given $b = ha \in Ha$.

$\Rightarrow ba^{-1} = h \in H$

$\Rightarrow b \in [a]_H$

$\Rightarrow Ha \subseteq [a]_H$

$\Rightarrow Ha = [a]_H$.

Def^n: Sets of the form Ha for $a \in G$ are called (right) cosets of H in G.

Thm. G group, H subgroup

Ha equivalence classes

If $a, b \in G$, then $Ha \cap Hb = \emptyset$

or $Ha = Hb$

$\Leftrightarrow ab^{-1} \in H$

G is union of all the right cosets of H, so the cosets partition G.

$\boxed{L-8}$

<u>Pf. of Lagrange's thm.</u>

Let $Ha_1, \ldots, Ha_k$ denote the distinct cosets of H in G.

Cosets of H partition G

$$|G| = \#(Ha_1) + \cdots + \#(Ha_k).$$

For each i, define $f_i : H \to Ha_i$ by
$f_i(h) = ha_i$

bijection

$\Rightarrow \# H = \#(Ha_i) \ \forall i$

if $h_1, h_2 \in H$
$h_1 a_i = h_2 a_i$,
$\Rightarrow h_1 = h_2$

$\Rightarrow \quad \# G = k \cdot \# H.$

$\Rightarrow \# H \mid \# G.$

Def^n: The no. of distinct (right) cosets of H in G is called index of H in G,

$[G : H]$.

Set of all right cosets of H in G denoted by G/H, so

$$\# G/H = [G : H]$$

Lagrange's thm. in terms of index

If G is a finite group, $H \leq G$ then

$$|G| = [G : H]\,|H|.$$

Examples:

Cosets of H in G

① Let $G = S_3$ & $H = \{(1), (13)\}$. Then the left coset of H in G are

$(1)H = H$

$(12)H = \{(12), (132)\} = (132)H$

$(13)H = \{(13), (1)\} = H$

$(23)H = \{(23), (123)\} = (123)H$

(2) $H = \langle a^5 \rangle$ & $G = \langle a \rangle$ & $o(a) = 15$

Left cosets of H in G

$\langle a^5 \rangle = \{1, a^5, a^{10}\}$

$a\langle a^5 \rangle = \{a, a^6, a^{11}\}$

$a^2\langle a^5 \rangle = \{a^2, a^7, a^{12}\}$

$a^3\langle a^5 \rangle = \{a^3, a^8, a^{13}\}$

$a^4\langle a^5 \rangle = \{a^4, a^9, a^{14}\}$.

$$o(a^5) = \frac{15}{3} = 5$$

# of left cosets of H in $G = 5$

Properties of cosets

Let $H \leq G$, & let $a, b \in G$. Then,

(1) $a \in aH$

(2) $aH = H$ iff $a \in H$

(3) $aH = bH$ iff $a \in bH$

(4) $aH = bH$ or $aH \cap bH = \emptyset$

(5) $aH = bH$ iff $a^{-1}b \in H$.

(6) $|aH| = |bH|$,

(7) $aH = Ha$ iff $H = aHa^{-1}$,

(8) $aH \leq G$ iff $a \in H$.

Consequences of Lagrange's thm.

1. $|a| \mid |G|$
2. Groups of prime order are cyclic.
3. $a^{|G|} = e$
4. Orbit - Stabilizer thm. (Statement later)

Permutation groups

S_n : Set of all permutations of the set $A = \{1, 2, \ldots, n\}$

$$\alpha = \begin{pmatrix} 1 & 2 & & n \\ \alpha(1) & \alpha(2) & & \alpha(n) \end{pmatrix}$$

Cycle notation: $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{pmatrix}$

$(1\ 2)(3\ 4\ 6)(5)$

can drop the cycles which fix.

$= (12)(346)$

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix} \qquad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}$$

$\alpha = (12)(3)(45)$

$\beta = (153)(24)$

$\alpha\beta = (12)(3)(45)(153)(24)$

$= (14)(253)$

Properties of permutations

<u>Products of disjoint cycles</u>

Thm. Every permutation of a finite set can be written as a cycle or as a product of disjoint cycles.

Pf. sketch $\alpha \in S_n$

Write α in disjoint cycle form

$a_2 = \alpha(a_1)$, $a_3 = \alpha(a_2) = \alpha^2(a_1)$

.. until $a_1 = \alpha^m(a_1)$ (since $a_1, \alpha(a_1), \alpha^2(a_1) \ldots$ is finite)

$\alpha = (a_1\ a_2 \quad a_m) \ldots$

Choose $b_1 \in A = \{1, 2, \ldots, n\}$ not

$b_1 \neq a_t$ for $1 \leq t \leq m$.

$b_2 = \alpha(b_1)$, $b_3 = \alpha^2(b_1) \ldots$

$b_1 = \alpha^k(b_1)$

$\alpha^i(a_1) = \alpha^j(b_1)$

$\alpha = (a_1\ a_2\ \ a_m)(b_1\ b_2 \ldots b_k) \ldots (c_1\ c_2 \ldots c_l)$

Thm. Disjoint cycles commute.

If the pair of cycles $\alpha = (a_1, a_2 \ldots a_m)$
$\beta = (b_1\ b_2\ \ b_m)$ have no entries in common

$\alpha\beta = \beta\alpha$

$S = \{a_1\ a_2 \ldots, a_m,\ b_1 \ldots, b_n,\ c_1 \ldots c_l\}$

α & β are permutations of S

fixed by both α & β

$\alpha\beta(x) = \beta\alpha(x) \quad \forall\, x \in S$

Pf $x = a_i$

$\alpha\beta(a_i) = \alpha(a_i) = a_{i+1}$

$\beta\alpha(a_i) = \beta(a_{i+1}) = a_{i+1}$

same for b_i

Thm. (Order) The order of a permutation of a finite set written in disjoint cycle = l.c.m. of the lengths of the cycles.

Pf. <u>sketch</u> Let $k = \text{lcm}(m, n)$

α length m

$\alpha^k = e$; $\beta^k = e$ β " n

$(\alpha\beta)^k = \alpha^k \beta^k = e$ (α & β commute disjoint)

Let $o(\alpha\beta) = t$

$t \mid k$

$(\alpha\beta)^t = \alpha^t \beta^t = e$

$\alpha^t = \beta^{-t}$ no common symbol

$\Rightarrow \alpha^t = \beta^{-t} = e$

$\Rightarrow m \mid t$ & $n \mid t$ $\Rightarrow$ $k = \text{lcm}(m,n) \mid t$

$\Rightarrow t = k$. $\boxed{L-9}$

Possible orders of elements of S_6

" disjoint cycle structure of element of S_6

n-cycle $\underline{n}$

$(\underline{6})$

$(\underline{5})(\underline{1})$

$(\underline{4})(\underline{2})$

$(\underline{3})(\underline{3})$

$(\underline{4})(\underline{1})(\underline{1})$

$\vdots$

Special kind of permutations : cycle of length 2 - transpositions

$(a\ b)$ $\quad a \neq b$

Thm. Every permutation in S_n $(n>1)$, is a product of transpositions.

Pf sketch $\quad e = (12)(12)$

every permutation can be written as

$(a_1 \ldots a_k)(b_1 \ldots b_t) \ldots (c_1 \ldots c_s)$

$(a_1 a_k)(a_1 a_{k-1}) \ldots (a_1 a_2) \ldots$

$(1632)(457) = (12)(13)(16)(47)(45)$

# of 2-cycles varies with each permutation.

$(12345) = (54)(53)(52)(51)$

$(12345) = (54)(52)(21)(25)(23)(13)$

Thm. (Always even / always odd)

If α can be expressed as a product of an even (odd) no. of 2-cycles, then every decomposition of α into 2-cycles must have an even / odd no. of 2-cycles

$$\alpha = \beta_1 \cdots \beta_r = \gamma_1 \cdots \gamma_s.$$

r & s are both even / both odd.

Pf. sketch. $\beta_1 \cdots \beta_r = \gamma_1 \cdots \gamma_s$ implies

$$e = \gamma_1 \cdots \gamma_s \beta_r^{-1} \cdots \beta_1^{-1}$$

$$= \gamma_1 \cdots \gamma_s \beta_r \cdots \beta_1$$

(2-cycle is its own inverse)

$s+r$ is even

$\Rightarrow$ both r & s are even

Even permutations form a group

A_n Alternating group of degree n.

Thm. Set of even permutations in S_n form a subgroup of S_n.

Thm. For $n>1$, A_n has order $n!/2$

Pf. For each odd permutation α,

$(12)\alpha$ is even and

$(12)\alpha \neq (12)\beta$ when $\alpha \neq \beta$.

$\Rightarrow$ At least as many even as odd

For each even α

$(12)\alpha$ is odd

$\Rightarrow$ At least as many odd as even

$\Rightarrow$ # even = # odd

Ex. What is the maximum order of any element in A_{10}?

$|A_{10}| = \frac{10!}{2}$

2 permutations with the same cycle structure have the same order.

$(1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9)$

$(1\ 2\ 3\ 4\ 5\ 6\ 7)$

$(1\ 2\ 3\ 4\ 5)$

$(1\ 2\ 3)$

e

$(1\ 2\ 3\ 4\ 5\ 6\ 7)(8\ 9\ 10)$

$\not\phi$

$(1\ 2\ 3\ 4)(5\ 6)$

$(1\ 2\ 3\ 4\ 5)(6\ 7\ 8)$

$(1\ 2\ 3)(4\ 5\ 6)(7\ 8\ 9)$

$(1\ 2)(3\ 4)(5\ 6)(7\ 8)$

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

(ii) S_5

$\rightarrow$ fit cycles of high LCM

$(12)(3\ 4\ 5) \rightarrow$ LCM $= 6$

maximal order $= 6$

(iii) S_{10}

$(1\ 2\ 3)(4\ 5)(6\ 7\ 8\ 9\ 10)$

$\downarrow_3 \quad \downarrow_2 \quad \downarrow_5$

maximal order $= 30$

(i) A_{10} not even

maximal order $\rightarrow 21$

A_6

$(1\ 2\ 3\ 4\ 5)$

$(1\ 2\ 3)$

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

$(1\ 2\ 3)(4\ 5\ 6)$

$(1\ 2\ 3\ 4)(5\ 6)$

L-10

Normal subgroups & Quotient groups.

Let $G = S_3$ & $H = \{e, \phi\}$

$[G : H] = 3 \Rightarrow$ 3 right cosets of H in G
3 left " " " "

Right cosets

$H = \{e, \phi\}$ $\qquad$ $H = \{e, \phi\}$

$H\psi = \{\psi, \phi\psi\}$ $\qquad$ $\psi H = \{\psi, \psi\phi = \phi\psi^2\}$

$H\psi^2 = \{\psi^2, \phi\psi^2\}$ $\qquad$ $\psi^2 H = \{\psi^2, \psi^2\phi = \phi\psi\}$

Right coset $\neq$ left coset $\quad (H\psi \neq \psi H)$

Let $N = \{e, \psi, \psi^2\}$
index $= 2$

R.C $\qquad$ L.C

$N = \{e, \psi, \psi^2\}$ $\qquad$ $\phi N = \{\phi, \phi\psi, \phi\psi^2\}$

$N\phi = \{\phi, \psi\phi, \psi^2\phi\}$ $\qquad$ $= \{\phi, \psi^2\phi, \psi\phi\}$

For some subgroups $R.C = L.C$

Galois $\longrightarrow$ special

Def^n: $N \leq G$, N is a normal subgp of G if $\forall\, g \in G$ & $n \in N$, $gng^{-1} \in N$.

N is a normal subgrp

iff $gNg^{-1} \subset N \quad \forall g \in G$

<u>lemma</u>: $N \trianglelefteq G$ iff $gNg^{-1} = N \quad \forall g \in G$

$$n = ene^{-1}$$

<u>lemma</u>: The subgrp $N \leq G$ is a normal subg iff every left coset = right coset

Pf. Let $N \trianglelefteq G$

$\Rightarrow$ $gNg^{-1} = N$

$(gNg^{-1})g = Ng$

$gN = Ng$

Conversely $gN = Ng$ –

$gNg^{-1} = N \Rightarrow N \trianglelefteq G.$

<u>Examples</u>: (i) Every subgroup of an Abelian group is normal.

(ii) $Z(G) = \{ g \in G : gx = xg \ \forall x \in G \}$ center of a

subgroup check! group.
normal subgroup

$h \in Z(G)$

$ghg^{-1} = gg^{-1}h = h \in Z(G)$

(iii) $A_n \trianglelefteq S_n$.

$\sigma \in A_n$. $\sigma = (a_1 \dots a_k)(b_1 \dots)$

$\tau\sigma\tau^{-1}(\tau(a_1) \dots)(\quad)$

$\tau\sigma\tau^{-1} \longrightarrow$ conjugate same cycle

↳ even $\in A_n$ structure of σ

for any $\tau \in S_n$

(iv) $SL_2(\mathbb{R}) \trianglelefteq GL_2(\mathbb{R})$

$A \in SL_2(\mathbb{R})$

$\det(XAX^{-1}) = \det X . \det A . \det X^{-1}$

$= 1$

$\Rightarrow XAX^{-1} \in SL_2(\mathbb{R})$.

Factor / Quotient groups.

Set of left (or right) cosets of H in G is a group — called the Factor group of G by H denoted as G/H

$G/H = \{ aH \mid a \in G \}$

operation : $(aH)(bH) = abH$

$\downarrow$

is well defined, i.e

is a function

$a_1 = a_2$

$f(a_1) = f(a_2)$

$G/H \times G/H \longrightarrow G/H$

$(a_1, a_2) = (b_1, b_2)$

$f((a_1, a_2)) = f((b_1, b_2))$

$\Rightarrow (a_1H, a_2H) = (b_1H, b_2H)$

$\Rightarrow a_1H = b_1H$ &

$a_2H = b_2H$

$f((a_1H, a_2H)) = a_1a_2H$

$f((b_1H, b_2H)) = b_1b_2H$

To prove: $a_1a_2H = b_1b_2H$

Now $a_1H = b_1H$

$\Rightarrow b_1 = a_1h$ for some $h \in H$

& $a_2H = b_2H$.

$\Rightarrow b_2 = a_2h'$ for some $h' \in H$

$$\Rightarrow \quad b_1 b_2 H = a_1 h a_2 h' H$$
$$= a_1 h a_2 H$$
$$= a_1 h H a_2 \qquad (H \trianglelefteq G)$$
$$= a_1 H a_2$$
$$= a_1 a_2 H$$

Identity : $eH \in G/H$

Inverse : $(aH)^{-1} = a^{-1}H \in G/H$

Associativity ✓

Ex. Let $G = \mathbb{Z}_{18}$ & let

$$H = \langle 6 \rangle = \{0, 6, 12\}$$

$$G/H = \{0+H, 1+H, 2+H, 3+H, 4+H, 5+H\}$$

$$(5+H) + (4+H) = 5+4+H$$
$$= 9+H$$
$$= 3+6+H$$
$$= 3+H$$

Order of G/H : $[G:H]$

Why are quotient groups important?

When $|G| < \infty$, $H \neq \{e\}$,

$|G/H| < |G|$.

easier to understand.

Applications: (L-11)

A_4 has no subgroup of order 6.

Same as saying:

There is no subgroup of index 2 in A_4.

Pf: Suppose $H \leq A_4$ s.t

$[A_4 : H] = 2$

$\Rightarrow |H| = 6$

(1)

Now we show: For each $g \in A_4$, $g^2 \in H$.

then, each 3-cycle $(a\,b\,c)$ in A_4

is a square → order 3.

since $(a\,b\,c) = ((a\,b\,c)^2)^2$

$\Rightarrow H$ contains all 3-cycles in A_4.

8 3-cycles while $|H| = 6$

such a H dne.

So, let us show (1)

If $g \in H$ then $g^2 \in H$

If $g \notin H$, then gH is a left coset of H different from H.

Since $[G:H] = 2$

$\Rightarrow$ only left cosets of H are H & gH.

Which one is g^2H?

If $g^2H = gH$

$\Rightarrow g^2 \in gH$

$\Rightarrow g^2 = gh$ for some $h \in H$

$\Rightarrow g = h$

$\Rightarrow g \in H$

$\rightarrow\leftarrow$

$\Rightarrow g^2H = H$

$\Rightarrow g^2 \in H$.

Index 2-subgroups are normal

$[G:H] = 2$

S_n not simple for $n > 2$.

Show for any $g \in G$

$$gH = Hg$$

If $g \in H$ then

let $g \notin H$ $\quad gH \neq H$

Since $H \cup gH = G$

left coset partition G

lly right coset partition G $\quad Hg \neq H$

$$\Rightarrow gH = Hg.$$

Thm. (G/Z thm.)

Let G be a group & let $Z(G)$ be the center of G.

If $G/Z(G)$ is cyclic, then G is abelian.

$$\langle g\, Z(G) \rangle = G/Z(G)$$

$$aZ(G) = (gZ(G))^i = g^i Z(G)$$

Illy $\quad bZ(G) = g^j Z(G)$

$$a = g^i x \ \& \ b = g^j y \qquad x, y \in Z(G)$$

$$ab = g^i x g^j y$$

$$= g^{i+j} xy = g^j g^i yx$$

$$= g^j y g^i x = ba$$

Contrapositive is used more, i.e

if G is non-Abelian, then $G/Z(G)$ is not cyclic.

(i) G abelian $\Rightarrow$ G/H abelian

G cyclic $\qquad$ G/H cyclic

Define centralizer

$$C(g) = \{x \in G : xg = gx\}.$$

$C(g) \leq G$

if $\langle g \rangle \trianglelefteq G$, then $C(g) \trianglelefteq G$.

Def^n: Center

$$Z(G) = \{ x \in G : xg = gx \ \forall g \in G \}$$

$Z(S_3)$

$Z(GL_2(\mathbb{R}))$

$Z(G) \trianglelefteq G$

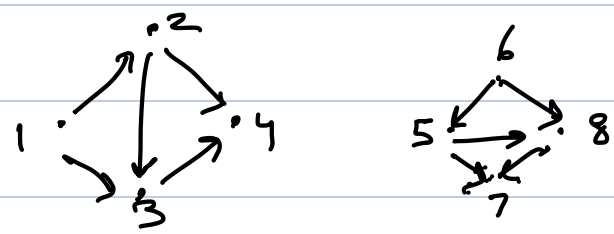
Isomorphism

"isomorphic" same structure

In geometry: congruence, similarity

plane motion transformation

Ex. Flow network:



1-1 correspondence $A \longrightarrow B$

is called isomorphism

$1 \to 6$
$2 \to 5$
$3 \to 8$
$4 \to 7$

Def.^{n}: Let G_1 and G_2 be groups. A bijective function $f: G_1 \to G_2$ with the property that for any 2 elements $a, b \in G_1$,

$$f(ab) = f(a)f(b)$$

is called an isomorphism from G_1 to G_2.

operation of G_1 operation of G_2

If there exist an isomorphism from G_1 to G_2, we say that G_1 is isomorphic to G_2.

Symbolically this is denoted as

$$G_1 \cong G_2 .$$

How to see if groups are isomorphic?

Find an isomorphism & show it is an isomorphism.

Steps:

(a) Come up with a candidate (mapping) for isomorphism ϕ

(b) 1-1. Prove ϕ is one-one, i.e

$$\phi(a) = \phi(b) \Rightarrow a = b.$$

(c) Onto. for any $\bar{g} \in G_2$, $\exists\, g \in G_1$ s.t

$$\phi(g) = \bar{g}$$

(d) Operation preserving. $\phi(ab) = \phi(a)\phi(b) \quad \forall\, a, b \in G_1$

combining + mapping = mapping & combining

Ex. 1 $f: \mathbb{R} \longrightarrow \mathbb{R}^+$

$f(x) = e^x$

injective ✓

surjective ✓ $y \in \mathbb{R}^+$

o.p ✓ $x = \ln y$)

Ex. 2. $G \to \mathbb{Z}$ $G \cong \mathbb{Z}$

$\langle a \rangle$ infinite

$a^k \to k$.

Ex. 3 $G \longrightarrow \mathbb{Z}_n$

$\langle a \rangle$ finite cyclic

$G \cong \mathbb{Z}_n$

$a^k \to k \bmod n$

Usually easier to show that groups are not isomorphic if G_1 has a property which G_2 does not have (& vice versa), they are not isomorphic!

(i) G_1 Abelian, G_2 not

(ii) G_1 has an element of order 2, G_2 has no element of order 2

(iii) G_1 is generated by 2 elements, G_2 not, etc..

list not exhaustive!

Arthur Cayley discovered:

(Cayley's thm.) Every group is isomorphic to a group of permutations.

Ex. 4 $\quad \mathbb{Z}_{10}^* \simeq \mathbb{Z}_4$

$\mathbb{Z}_{10}^* = \{1, 3, 7, 9\} = \langle 3 \rangle$

cyclic group of order 4

$3^4 \bmod 10 = 1$

$3^2 \bmod 10 = 9$

$3^3 \bmod 10 = 7$

$\mathbb{Z}_{10}^* \not\simeq \mathbb{Z}_{12}^* \qquad \mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$

$\phi : \mathbb{Z}_{10}^* \longrightarrow \mathbb{Z}_{12}^*$

$1^2 = 1$

$5^2 = 1$

$7^2 = 1$

$11^2 = 1$

$\phi(ab) = \phi(a)\phi(b)$

$\phi(9) = \phi^2(3) \in \mathbb{Z}_{12}^*$

$= 1$

but $\phi(1) = 1 \quad \Rightarrow \quad \phi$ is not one-one

not isomorphic

Ex. 5 $\quad \phi : \mathbb{Q} \longrightarrow \mathbb{Q}^* \quad (\mathbb{Q} \setminus \{0\})$

$\phi(a) = -1$

$\phi(a) = \phi\left(\frac{a}{2} + \frac{a}{2}\right) = \phi^2\left(\frac{a}{2}\right)$

but no $r \in \mathbb{Q}$ s.t $r^2 = -1$.

Pf. of <u>Cayley's</u> thm.

Wish to show that $G \cong$ a group of permutations

Q. "What group of permutations"

Q. "Permutation of what set?

Permutations of G

Find a group $\bar{G}$ of permutations that we believe is isomorphic to G.

& in doing so, use G.

For any $g \in G$, define

$$T_g : G \to G$$

$$T_g(x) = gx \quad \forall x \in G$$

Show: T_g is a permutation of G:

(i) T_g is injective. $T_g(x_1) = T_g(x_2)$

$$gx_1 = gx_2$$

$$x_1 = x_2$$

(ii) T_g is surjective

if $y \in G$, take $x = g^{-1}y$.

$$T_g(g^{-1}y) = g \cdot g^{-1}y = y$$

$\Rightarrow$ T_g is a permutation of G.

Let $\bar{G} = \{ T_g : g \in G \}$ set of all permutation T_g as g ranges over all elements of G.

Infact $\bar{G} \leq S_G$ (group of all permutations of G)

show it is a subgroup under composition

$$T_g T_h(x) = T_g(hx) = ghx$$
$$= T_{gh}(x)$$
$$T_g T_h = T_{gh}$$

T_e identity

$T_{g^{-1}}$ inverse of T_g.

Finally, we define the isomorphism from

$$\phi : G \to \bar{G}$$
$$\phi(g) = T_g$$

One-one: $T_g = T_h$

$$\Rightarrow T_g(e) = T_h(e)$$
$$ge = he$$
$$\Rightarrow g = h$$

onto: clear (every element of $\bar{G}$ is T_g, & $T_g = \phi(g)$)

Lastly $\phi(g_1 g_2) = T_{g_1 g_2}$

$$= T_{g_1} \cdot T_{g_2}$$
$$= \phi(g_1) \circ \phi(g_2)$$

$$G \cong \bar{G}$$

Properties of isomorphism:

(i) $G \cong G$

(ii) $G_1 \cong G_2$ & $G_2 \cong G_3 \Rightarrow G_1 \cong G_3$

(iii) $G_1 \cong G_2$ & $G_2 \cong G_1$

$\mathbb{R} \simeq \mathbb{C}(+)$

$\mathbb{C}^* \simeq \mathbb{C}$ $(|z|=1)$

Properties of isomorphism acting on element

$\phi : G \to \bar{G}$, isomorphism

(i) $\phi(e) = \bar{e}$

(ii) $\phi(a^n) = \phi(a)^n$

(iii) $ab = ba$ iff $\phi(a)\phi(b) = \phi(b)\phi(a)$

(iv) $G = \langle a \rangle$ iff $\bar{G} = \langle \phi(a) \rangle$

(v) $o(a) = o(\phi(a))$ $\forall a \in G$

(vi) $x^k = b$ same no. of sol.^{n} in G as $x^k = \phi(b)$ in $\bar{G}$

(vii) $|G| < \infty$

G & $\bar{G}$ have same no. of elements of every order.

$\boxed{L-12}$

Automorphisms :

Def^n: (Automorphism) An isomorphism from a group G to itself is called an automorphism.

Ex. Let G be any group, $a \in G$

$\varphi_a : G \to G \quad \varphi_a(x) = axa^{-1}$,

φ_a is an automorphism

$\varphi_a(xy) = axya^{-1} = axa^{-1}aya^{-1} = \varphi(x)\varphi(y)$

φ_a is called inner automorphism induced by a.

$\mathrm{Aut}(G)$ = set of all automorphisms of G

$\mathrm{Inn}(G)$ = set of all inner automorphisms of G.

Thm. $\mathrm{Aut}(G)$, $\mathrm{Inn}(G)$ are groups under composition

$\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$

Remark: $|\mathrm{Inn}(G)|$ may not be equal to $|G|$!

Ex. $\mathrm{Aut}(\mathbb{Z}_{10})$?

$\alpha \in \mathrm{Aut}(\mathbb{Z}_{10})$

Possible group elements α ?

if $\alpha(1)$ is known, $\alpha(k)$ is known for any k.

$\alpha(k) = \alpha(1 + 1 + \cdots + 1) = k\alpha(1)$.

Only need to determine possible choices of $\alpha(1)$.

$o(\alpha(1)) = o(1) = 10$

$\alpha(1) = 1$,

$\alpha(1) = 3$; $\alpha(1) = 7$; $\alpha(1) = 9$.

α_1 $\quad \alpha_3$ $\quad \alpha_7$ $\quad \alpha_9$

all are automorphisms

$\alpha_3^2(1) = \alpha_3(\alpha_3(1)) = \alpha_3(3) = 9 = \alpha_9(1)$

$\alpha_3^3(1) = \alpha_3(9) = 27 = 7 \bmod 10 = \alpha_7(1)$

$\alpha_3^4(1) = \alpha_3(7) = 1 = \alpha_1(1)$

$\Rightarrow o(\alpha_3) = 4$.

$\Rightarrow \quad \mathrm{Aut}(\mathbb{Z}_{10}) = \langle \alpha_3 \rangle$ cyclic of order 4

$\cong \mathbb{Z}_4 \cong \mathbb{Z}_{10}^*$

Infact,

Thm. $\mathrm{Aut}(\mathbb{Z}_n) \cong U_n \quad (\mathbb{Z}_n^*)$

$T: \mathrm{Aut}(\mathbb{Z}_n) \to \mathbb{Z}_n^*$

$T(\alpha) = \alpha(1)$

One-one: $\quad T(\alpha) = T(\beta)$

$\Rightarrow \alpha(1) = \beta(1)$

$\Rightarrow \quad \alpha(k) = \beta(k)$ for any $k \in \mathbb{Z}_n$

$\Rightarrow \alpha = \beta$

Onto: $\quad k \in \mathbb{Z}_n^*$

Consider $\alpha_k : \mathbb{Z}_n \to \mathbb{Z}_n$

$\alpha_k(m) = mk \bmod n$

α_k is an automorphism

$$\alpha_k(u+v) = (u+v)k \bmod n$$
$$= \alpha_k(u) + \alpha_k(v)$$

$$T(\alpha_k) = \alpha_k(1) = k$$

$\Rightarrow$ onto

Operation preserving : $T(\alpha\beta) = (\alpha\beta)(1) = \alpha(\beta(1))$

$$= \alpha(\underbrace{1+\cdots\cdots+1}_{\beta(1) \text{ times}})$$

$$= \alpha(1) + \cdots + \alpha(1) = \alpha(1)\beta(1)$$

$$T(\alpha)T(\beta)$$

Homomorphisms : generalization of isomorphism

Def^n: $\phi : G \to \overline{G}$ (homomorphism)

$$\phi(ab) = \phi(a)\phi(b)$$

Def^n (kernel of a homomorphism)

$$\operatorname{Ker}\phi = \{ g \in G : \phi(g) = e \}$$

$\operatorname{Ker}\phi$ if ϕ is an isomorphism

$\operatorname{Ker}\phi = \{e\}$ also when ϕ is 1-1.

Ex. $GL_2(\mathbb{R}) \to \mathbb{R}^*$

$\phi : A \mapsto \det A$

$\operatorname{Ker}\phi = SL_2(\mathbb{R})$

Ex. $\phi : \mathbb{Z} \to \mathbb{Z}_n$ $\quad \phi(m) = m \bmod n$

$\operatorname{Ker} \phi = \langle n \rangle$

Properties of homomorphisms

Thm. Let $\phi : G \to \bar{G}$

(i) $\phi(e) = \bar{e}$

(ii) $\phi(g^n) = \phi(g)^n \quad \forall n \in \mathbb{Z}$

(iii) if $o(g) < \infty$ then $o(\phi(g)) \mid o(g)$.

(iv) $\operatorname{Ker} \phi \leq G$

(v) $\phi(a) = \phi(b)$ iff $a \operatorname{Ker} \phi = b \operatorname{Ker} \phi$

(vi) $\phi(g) = g'$

$$\phi^{-1}(g') = \{ x \in G : \phi(x) = g' \}$$
$$= g \operatorname{Ker} \phi$$

$\phi(a) = \phi(b) \Rightarrow e = \phi(ab^{-1})$

$ab^{-1} \in \operatorname{Ker} \phi$

$a \in b \operatorname{Ker} \phi$

Corollary: ϕ group homomorphism from $G \to \bar{G}$

$\operatorname{Ker} \phi \trianglelefteq G$.

$gng^{-1} \in \operatorname{Ker} \phi$ for $n \in \operatorname{Ker} \phi$

$\phi(gng^{-1}) = \phi(g)\phi(n)\phi(g^{-1}) \quad \phi(n) = e$

$= \phi(gg^{-1}) = \phi(e) = e$

Determining all homomorphisms from a cyclic group to a cyclic group.

Problems:

1. $\mathbb{Q} \not\cong \mathbb{Z}$
2. If G has exactly 1 subgroup H of order k, then $H \trianglelefteq G$.
3. Let $H = \{id, (12)(34), (13)(24), (14)(23)\}$
   Prove that $H \trianglelefteq S_4$
4. $H = \langle (1234) \rangle \ntrianglelefteq S_4$

Sol^n: For any $g \in G$, $gHg^{-1} = H$.

$gHg^{-1} \leq G$

$h \to ghg^{-1}$ $\quad (H \xleftrightarrow{\text{bijects}} gHg^{-1})$

$|gHg^{-1}| = |H| = k$.

ghg^{-1} has same cycle structure as h

No other products of disjoint 2-cycles other than those in H.

$\{id, (1234), (13)(24), (1432)\}$

$(12)(1234)(12)^{-1} = (1342)$ → not in H

(3) Describe all homomorphisms from $\mathbb{Z} \to \mathbb{Z}_4$
which of them are onto?
" .. . $\mathbb{Z}_6 \to \mathbb{Z}_8$

$\phi : \mathbb{Z} \to \mathbb{Z}_4$

$\phi(1)$ $\quad (\phi(n) = n \cdot \phi(1))$

For any $a \in \mathbb{Z}_4$

$\phi(n) = an \bmod 4$

4 homomorphism:

$\phi(1) = 0$ $\quad$ Ker $= \mathbb{Z}$, image $= \{0\}$

$\phi(1) = 1$ $\quad$ Ker $= 4\mathbb{Z}$ $\quad$ " $= \mathbb{Z}_4$

$\phi(1) = 2$ $\quad$ Ker = set $\quad$ " $\langle 2 \rangle$

$2n$ is a multiple of 4

$\Rightarrow$ even

$\phi(1) = 3$ $\quad$ Ker $= 4\mathbb{Z}$ $\quad$ image $= \mathbb{Z}_4$

Homomorphisms from $\mathbb{Z}_n \to \mathbb{Z}_m$

$\phi_a : \mathbb{Z}_n \to \mathbb{Z}_m$

$x \mapsto a \cdot x \bmod m$

$1 \to a$

order of a | $o(i) = n$

& " " " | m

$o(a) \mid \gcd(m,n)$

# of elements of a fixed order d in any fix cyclic gp $\leftarrow \mathbb{Z}_n$

$= \phi(d)$

$$\sum_{d \mid \gcd(m,n)} \phi(d) = \gcd(m,n)$$

Claim: $\displaystyle\sum_{d \mid n} \phi(d) = n$

$S = \{1, 2, \ldots, n\}$

$A_d = \{ k \leq n \text{ s.t } \gcd(k,n) = d \}$

$n = \sum |A_d| = \sum \varphi(n/d) = \sum \varphi(d)$

$A_{k/d} = \gcd(k/d, n/d) = 1$

$\varphi : \mathbb{Z} \to \mathbb{Z}_n$

$\varphi(i)$ can go to any where $\varphi(n/d)$

$\varphi(i) = a$

$\varphi(x+y) = a(x+y)$

$= ax + ay$

$= \varphi(x) + \varphi(y)$

Isomorphism theorems

Already know, we can get a normal subgroup ($\ker \phi$) from a homomorphism. Converse is also true! i.e.

every normal subgroup of a group G gives rise to homomorphism of groups.

let $H \trianglelefteq G$. Define a 'natural' homomorphism

$$\phi : G \to G/H$$

$$\phi(g) = gH$$

$$\phi(g_1 g_2) = g_1 g_2 H = g_1 H g_2 H$$
$$= \phi(g_1)\phi(g_2)$$

$$\ker \phi = \{ g \in G : \phi(g) = H$$
$$gH = H \iff g \in H \}$$
$$= H$$

Relationship bet^n homomorphisms, quotient groups, normal

(1st isomorphism thm.) If $\psi : G \to H$ is a group homomorphism with $K = \ker \psi$, then $K \trianglelefteq G$.

$$G/K \simeq \psi(G)$$

$$\phi : G/K \longrightarrow \psi(G)$$

$$\phi(gK) = \psi(g)$$

$$\phi(gKhK) = \phi(ghK)$$
$$= \psi(gh) = \psi(g)\psi(h)$$

Problems :

Which of the following maps are homomorphisms? Find the kernel.

(a) $\phi : \mathbb{R}^* \longrightarrow GL_2(\mathbb{R})$ defined by
$$\phi(a) = \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}$$

(b) $\phi : GL_2(\mathbb{R}) \to \mathbb{R}$ defined by
$$\phi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = a+d$$

(c) $\phi : GL_2(\mathbb{R}) \longrightarrow \mathbb{R}^*$ defined by
$$\phi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = ad - bc$$

(d) $\phi : \mathbb{Z} \to \mathbb{Z}$
$$\phi(n) = 7n$$

(e) Describe all the homomorphisms from
$$\mathbb{Z}_{24} \to \mathbb{Z}_{18}$$

(f) Describe all the homomorphisms from
$$\mathbb{Z} \longrightarrow \mathbb{Z}_{12}.$$

(g) $\phi : G \to H$ homomorphism & G is abelian, prove that $\phi(G)$ is also abelian.

(h) $\phi : G \to H$ homomorphism & G is cyclic, prove that $\phi(G)$ is also cyclic.

(i) Prove or disprove: $\mathbb{Q}/\mathbb{Z} \cong \mathbb{Q}$.

$b\left(\frac{a}{b} + \mathbb{Z}\right) = \mathbb{Z}$

$\Rightarrow o\left(\frac{a}{b} + \mathbb{Z}\right) \leq b$

$\Rightarrow$ every element has finite order.

POST MID - SEM

Group Action : map

G group, X a set

$f : G \times X \longrightarrow X$

$f(g, x) = g.x$ satisfying

(i) $f(g, f(h, x)) = f(gh, x) \quad \forall\, g, h \in G,\ x \in X$

(ii) $f(e, x) = x \quad \forall\, x \in X$

Faithful group action: Different elements of G act on X in different ways

$\forall\ g_1 \neq g_2 \in G,\ \exists\, x \in X$ s.t $g_1.x \neq g_2.x$

Information encoded in a group action has 2 basic parts.

(A) Where points go — Orbit

(B) How points stay put. $\longrightarrow$ stabilizer

Def^n (Orbit) Let G be a group acting on X. Let $x \in X$

$$\mathrm{Orb}_x = O_x = \{ g \cdot x \mid g \in G \} \subset X$$

Def^n (Stabilizer) $G_x = \mathrm{Stab}_x = \{ g \in G \text{ s.t. } g \cdot x = x \} \subset G$

Def^n (Fixed point) $x \in X$ is a fixed pt. of an action if $g \cdot x = x \quad \forall \; g \in G$

Remark: If $x \in X$ is a fixed point then

$$\mathrm{Orb}_x = \{x\}$$
$$G_x = G$$

Ex. 1. Let $G = GL_2(\mathbb{R})$, $X = \mathbb{R}^2$

$$GL_2(\mathbb{R}) \times \mathbb{R}^2 \longrightarrow \mathbb{R}^2$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} au+bv \\ cu+dv \end{pmatrix}$$

Consider $\begin{pmatrix} 0 \\ 0 \end{pmatrix} \in \mathbb{R}^2$

$$\mathrm{Orb}_{\begin{pmatrix} 0 \\ 0 \end{pmatrix}} = \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right\}$$

$$\mathrm{Stab}_{\begin{pmatrix} 0 \\ 0 \end{pmatrix}} = GL_2(\mathbb{R})$$

Ex. 2 When a group G acts on itself by left multiplication

$$G \times G \longrightarrow G$$

$$f(g, h) = g \cdot h = gh$$

$e \in G$

$$\mathrm{Orb}_e = G$$

$$\mathrm{Stab}_e = \{e\}$$

Ex. 3 When a group G acts on itself by conjugation

$$G \times G \longrightarrow G$$

$$f(g, h) = ghg^{-1}$$

$t \in G$

$$\mathrm{Orb}_t = \{ gtg^{-1}, g \in G \}$$

↳ special name: called the <u>conjugacy class of t.</u>

$$G_t = \mathrm{Stab}_t = \{ g \in G : gtg^{-1} = t \}$$

$$= \{ g \in G : gt = tg \}$$

centralizer of t. $= C(t)$

Thm (a) Diff orbits of a group action are disjoint & form a partition of X.

(b) For each $x \in X$, $G_x \leq G$ and

$$G_{gx} = g G_x g^{-1} \quad \forall g \in G$$

(c) For each $x \in X$, there is a bijection

$$f : G/G_x \longrightarrow Orb_x$$

$$f(gG_x) = g \cdot x$$

Consequently, $\boxed{|G/G_x| = |Orb_x|}$

Orbit stabilizer thm / formula

Pf: (a) If 2 orbits overlap, they must coincide

Suppose $z \in Orb_x \cap Orb_y$

$$\Rightarrow \quad z = g_1 \cdot x = g_2 \cdot y$$

To show: $Orb_x = Orb_y$

Let $u \in Orb_x$

$$\Rightarrow \quad u = g \cdot x = g g_1^{-1} \cdot z$$

$$= g g_1^{-1} g_2 \cdot y \in Orb_y$$

Remark $Orb_x \neq \emptyset$

$x \in Orb_x$

every element belongs to its own orbit

Orbits partition X & $Orb_x = [x]$

(b) One-one

$$f(gG_x) = f(hG_x)$$
$$g\cdot x = h\cdot x$$
$$h^{-1}g\cdot x = x$$
$$\Rightarrow h^{-1}g \in G_x \Rightarrow g \in hG_x$$
$$gG_x = hG_x$$

(c) Onto $y \in Orb_x$

$$y = g\cdot x$$
$$gG_x = y$$

$|Orb_x| = \#$ of cosets of G_x in G.

Remark: The orbits of a group action are a partition of the set include 2 special cases.

(i) Conjugacy classes are a partition of a group. (Conjugacy action)

(ii) Left cosets of a subgroup partition the group. (right coset multiplication)

Corollary: For $|G| < \infty$, acting on a set.

(i) The size of every orbit divides the size of G.

(ii) Points in a common orbit have conjugate stabilizer

i.e.

if $x, y \in Orb_z$

then $\exists\ g \in G$ s.t

$$G_x = g G_y g^{-1}.$$

Consequently, (ii) implies that the size of the stabilizer is same for all points in an orbit.

— x —

20/3/24

Corollary: Let G act on X, $|X| < \infty$, let the different orbits of X under this action be represented by $x_1, x_2 \ldots, x_t$. Then

$$X = \bigcup_{i=1}^{t} Orb_{x_i}$$

$$|X| = \sum_{i=1}^{t} |Orb_{x_i}| = \sum_{i=1}^{t} [G : G_{x_i}]$$

Special case: G acting on G itself by conjugation; we get the class equation.

$$G \times G \to G$$

$$(g, h) \mapsto ghg^{-1}$$

$G_t = \text{Stab}_t = \text{Centralizer of } t = C(t)$

$= \{ g \in G : gt = tg \}$

$$|G| = \sum_{i=1}^{t} [G : C(g_i)] \quad \text{——} \quad (1)$$

Remark: $[G : C(g_i)] = 1$ iff $g_i \in Z(G)$

Pf: $[G : C(g_i)] = 1 \iff G = C(g_i)$

$\iff g_i t = t g_i \ \forall \ t \in G$

$\iff g_i \in Z(G)$

Break (1) into 2 part

$$|G| = \sum_{\substack{i=1 \\ g_i \in Z(G)}}^{t} [G : C(g_i)] + \sum_{\substack{i=1 \\ g_i \notin Z(G)}}^{t} [G : C(g_i)]$$

$$\boxed{|G| = |Z(G)| + \sum_{\substack{i=1 \\ g_i \notin Z(G)}}^{t} [G : C(g_i)]}$$

Class equation

Example (1) If G is abelian, then

$|G| = |Z(G)|$

Ex. (2):

Class equation for S_3

Orbit of S_3 (or conjugacy classes of S_3)

Recall: elements with same cycle structure are conjugate

This implies $\Rightarrow$ 3 conjugacy classes

3 cycles, transposition, identity

$$|S_3| = |Z(S_3)| + \frac{|S_3|}{|C_{S_3}((12))|} + \frac{|S_3|}{|C_{S_3}((123))|}$$

$$= 1 + 3 + 2$$

$\Rightarrow |C_{S_3}((12))| = 6/3 = 2$

Illy $|C_{S_3}((123))| = 3$

$C_{S_3}((12)) = \langle (12) \rangle$

Ex. 3: If $|G| = p^n$, with p prime, then $Z(G)$ is non trivial.

Let $|Z(G)| = m$

Now $|C(g_i)| \mid |G| \Rightarrow |C(g_i)| = p^{k_i}$

- If G is abelian, then $Z(G) = G$, done.
- If G is non-abelian, then $m < p^n$ &

$$p^n = m + \sum_i \frac{p^n}{p^{k_i}}$$

- $p \mid$ LHS, $p \mid \dfrac{p^n}{p^{L_i}}$, so $p \mid m$

$\Rightarrow Z(G)$ non trivial.

Ex. 4: Let $|G| = p^2$, where p is prime. Then G is abelian.

Pf: Since $Z(G) \neq \{e\} \Rightarrow |Z(G)| = p$ or p^2.

if $Z(G) = p^2$ done.

Suppose $Z(G) = p$

$\Rightarrow Z(G)$ is cyclic & $|G/Z(G)| = p$

$G/Z(G) = \langle aZ(G) \rangle$ is also cyclic

$gZ(G) = a^m Z(G)$ for some $m \in \mathbb{Z}$.

$\Rightarrow g = a^m x$ for $x \in Z(G)$

Ly $h = a^n y$ $\quad y \in Z(G)$

$gh = a^m x a^n y = a^n y a^m x = hg$

$\Rightarrow G$ is abelian $\Rightarrow |Z(G)| = p^2$.

Class equ.^{n} for D_4

Center of $D_4 = \{(1), (13)(24)\}$

Conjugacy classes $\{(13)(24)\}$, $\{(1432), (1234)\}$, $\{(12)(34), (14)(23)\}$.

Thus Class eqn $8 = 2+2+2+2$.

Burnside Lemma.

Intuitively, Burnside's lemma count the no. of arrangements of an object if its symmetries are considered 'same'.

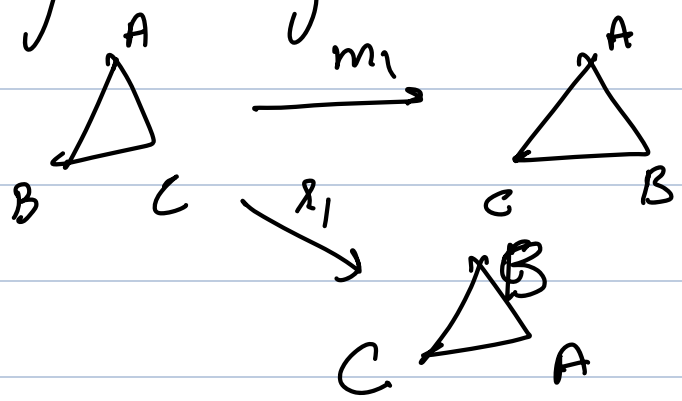
It provides a formula to count the no. of objects, where 2 objects that are symmetric by rotation or reflection are not categorized as distinct.

For eg. to find the no. of colorings of a fixed 6-sided cube using n colors,

\# of colorings $= n^6$ since each side has the option of each color

but many would be same if we were allowed to rotate the cube.

For assymetric objects $\rightarrow$ use binomial thm., etc.



all 3 represent different coloring

In order to count the no. of distinct colorings of an object, can apply Burnside's & Polya's enumeration:

$g \in G$ $\quad$ Fix_g

Def^n (Fixed set of g) $= \{x \in X : g.x = x\} \subseteq X$

Ex. $G = \{(1), (12), (34), (12)(34)\}$

$X = \{1, 2, 3, 4\}$ $\quad$ $G \times X \to X$, $\sigma . x = \sigma(x)$

$\mathrm{Fix}_{(1)} = \{1, 2, 3, 4\}$

$\mathrm{Fix}_{(12)} = \{3, 4\}$

$\mathrm{Fix}_{(34)} = \{1, 2\}$

$\mathrm{Fix}_{(12)(34)} = \emptyset$

<u>Burnside's Lemma</u>:

Let $|G| < \infty$, $|X| < \infty$, & let r be the no. of orbits of G on X, then

$$r = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}_g|$$

Pf: Count the no. of pairs (g, x), $g \in G$ & $x \in X$ s.t $g.x = x$ in 2 different ways.

Let $n = \{(g, x) \in G \times X \text{ s.t } g.x = x\}$

For a fixed element $g \in G$, # of x s.t $g.x = x$ is Fix_g

$$\Rightarrow n = \sum_{g \in G} |\mathrm{Fix}_g|$$

For a fixed $x \in X$, # of g s.t $g.x = x$ is $|G_x|$

$$\Rightarrow \quad n = \sum_{x \in X} |G_x|$$

$$\Rightarrow \quad \sum_{g \in G} |\mathrm{Fix}\, g| = \sum_{x \in X} |G_x|$$

Consider RHS & break this further

Let $x \in X$ consider Orb_x

For each $y \in \mathrm{Orb}_x$ $|G_y|$ is same

$$\Rightarrow \quad \sum_{y \in \mathrm{Orb}_x} |G_y| = |\mathrm{Orb}_x| \cdot |G_x| \quad \text{—} *$$

By Orbit-Stabilizer $|G_x| = |G| / |\mathrm{Orb}_x|$

$s, t \in \mathrm{Orb}_x$

$|\mathrm{Orb}_s| = |\mathrm{Orb}_t|$

$\Rightarrow |G_s| = |G_t|$

$(*) \Rightarrow$

$$\sum_{y \in \mathrm{Orb}_x} |G_y| = |\mathrm{Orb}_x| \cdot |G_x| = |G|$$

$$\sum_{x \in X} |G_x| = \sum_{\text{orbits}} \sum_{y \in \mathrm{Orb}_x} |G_y|$$

$$\sum_{g \in G} \mathrm{Fix}\, g = \#\text{ of orbits} \cdot |G|$$

$$\Rightarrow \quad \#\text{ of orbits} = \frac{1}{|G|} \cdot \sum_{g \in G} \mathrm{Fix}\, g$$

Recall, Lagrange's thm.

Also recall, converse of Lagrange's thm. does not hold true in general.

i.e let $|G| < \infty$, $|G| = n$. If $d | n$, then d is the order of a subgroup of G

(Ex. A_4 has no subgroup of order 6)

Ludwig Sylow (1832 - 1918)

Def.^{n}: G group, p prime

(i) A group of order p^α for some $\alpha \geq 1$ is called a p-group.

subgroups of G which are p-groups are called p-subgroups.

(ii) If $|G| = p^\alpha m$; $p \nmid m$, $\alpha \geq 1$, then a subgroup of order p^α is called a Sylow p-subgroup of G.

(iii) The set of all Sylow p-subgroups of G will be denoted by $Syl_p(G)$ &

$$\# \, Syl_p(G) = n_p(G).$$

(iv) Conjugate subgroups:

Let $H, K \leq G$, H & K are conjugate in G if there is an element $g \in G$ s.t

$$H = gKg^{-1}.$$

Thm. (Sylow's thm.)

Let $|G| = p^\alpha m$, p prime, $p \nmid m$.

(i) $Syl_p(G) \neq \emptyset$, i.e Sylow p-subgroups of G exist.

(ii) If $P \in Syl_p(G)$ & Q is a p-subgroup of G, then there exists $g \in G$ s.t

$$Q \leq gPg^{-1} \quad \text{i.e.}$$

Q is contained in some conjugate of P.

In particular, any 2 Sylow p-subgroups are conjugate in G.

(iii) $n_p(G) \equiv 1 \mod p \iff p \mid n_p(G) - 1$ —(a)

$$n_p(G) = [G : N_G(P)] \qquad \text{——— (b)}$$

where P is any Sylow p-subgroup of G

& $N_G(P) = \{ g \in G \text{ s.t } gPg^{-1} = P \}$

Note: If $H \trianglelefteq G$ then $N(H) = G$ & vice versa.

$$n_p(G) \mid m \qquad \text{——— (c)}$$

Corollary: Let P be a Sylow p-subgroup of G.

TFAE:

(i) P is the unique Sylow p-subgroup of G, i.e, $n_p(G) = 1$

(ii) $P \trianglelefteq G$

(iii) $X \subseteq G$ s.t $o(x)$ is a power of p $\forall x \in X$, then $\langle X \rangle$ is a p-group.

Pf. of corollary:

(i) $\Leftrightarrow$ (ii)

$$n_p = 1 \Leftrightarrow [G : N_G(P)] = 1$$
$$\Leftrightarrow G = N_G(P)$$
$$\Leftrightarrow P \trianglelefteq G$$

(i) $\Rightarrow$ (iii) let $X \subseteq G$ s.t $o(x)$ is a power of p $\forall x \in X$

let $x \in X$

Consider $Q = \langle x \rangle$ $\rightarrow$ cyclic subgroup generated by x

$\Rightarrow$ Q is a p-subgroup of G (since $o(x)$ is a power of p)

By Sylow's thm ;

$Q \leq gPg^{-1}$ for some $g \in G$

Since $n_p = 1$ (only 1 Sylow p-subgrp)

$\Rightarrow$ $gPg^{-1} = P$

$\Rightarrow$ $Q \leq P$

$\Rightarrow$ $x \in P$

but x was arbitrary

$\Rightarrow$ $X \subseteq P$

$\Rightarrow$ $\langle X \rangle \leq P$ $\Rightarrow$ $|\langle X \rangle| \mid |P|$

$\Rightarrow$ $\langle X \rangle$ is a p-group.

(iii) $\Rightarrow$ (i) homework

Ex. $|S_3| = 2 \cdot 3$

Sylow 2-subgroup & Sylow 3-subgroup

$n_2 \equiv 1 \mod 2$	$n_3 \mid 2$
$n_2 \mid 3$	$n_3 \equiv 1 \mod 3$
$n_2 = 1$ or 3	$n_3 = 1$ or $\cancel{2}$
	$n_3 = 1$

$\Rightarrow$ Unique Sylow 3-subgp.

$\Rightarrow$ Unique Sylow 3-subgp $\triangleleft S_3$

$\{e, (123), (132)\} = A_3 \triangleleft S_3$

Application of Sylow's thm.

Def^n: A group G is simple if it has no nontrivial normal subgroup

Note $\{e\}, G \to$ trivial normal subgroup

(i) Sylow's thm is used mostly to show a certain group is simple

Thm. 1 The smallest non-abelian simple group is A_5 and it is unique upto isomorphism.

The pf. involves 3 steps

Step 1: There is no simple non-abelian group of order less than 60. ($|A_5| = 60$)

Step 2: A_5 is a simple non-abelian group of order 60

Step 3: Upto isomorphism, the only simple non-abelian group of order 60 is A_5.

Pf. of Step 1:

1	~~2~~	~~3~~	~~4~~	~~5~~	~~6~~	~~7~~	~~8~~	~~9~~	~~10~~
~~11~~	~~12~~	~~13~~	~~14~~	~~15~~	~~16~~	~~17~~	~~18~~	~~19~~	~~20~~
~~21~~	~~22~~	~~23~~	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	~~29~~	~~30~~
~~31~~	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	~~37~~	~~38~~	~~39~~	~~40~~
~~41~~	~~42~~	~~43~~	~~44~~	~~45~~	~~46~~	~~47~~	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	~~53~~	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	~~59~~	60

We shall eliminate all possibilities of simple non-abelian groups with order less than 60.

(i) Groups of prime order $\rightarrow$ cyclic $\rightarrow$ abelian

2 3 5 7 11 13 17 19 23

29 31 37 41 43 47 53 59

(ii) $|G| = 45 = 5 \cdot 3^2$

Sylow 5-subgroup, Sylow 3-subgroup

$n_5 \mid 9$ & $5 \mid n_5 - 1$

$n_5 = 1, \cancel{3}, \cancel{9}$

$\Rightarrow n_5 = 1 \Rightarrow$ Unique Sylow 5-subgroup $\triangleleft G$

$\Rightarrow G$ is not simple.

$|G| = 45$

(iii) $|G| = 40 = 5 \cdot 2^3$

Sylow 5-subgroup, Sylow 2-subgrp.

$n_5 \mid 8$ & $5 \mid n_5 - 1$

$n_5 = 1, \cancel{2}, \cancel{4}, \cancel{8}$

Unique Sylow 5-subgp. $\triangleleft G$

$\Rightarrow G$ is not simple.

$|G| = 40.$

(iv) $|G| = 2^p q$ s.t p prime & $q = 2^p - 1$ is prime

Claim: G is not simple.

$n_q \equiv 1 \mod q$; $n_q \mid 2^p$

$\Rightarrow n_q = 2^k$; $k \leq p$

& $q \mid n_q - 1$

$\Leftrightarrow 2^p - 1 \mid 2^k - 1 \Rightarrow k = p$ or $k = 0$

If $n_q = 1$ (done)

If $n_q = 2^k = 2^p$

assume $H_1, H_2, \ldots, H_{2^p}$ Sylow q-subgroups (has order q)

Since all of them are prime order, intersection of any 2 of them is trivial.

Thus, the total no. of non-identity elements of order q is

$$(q-1)\,2^p = |G| - 2^p$$

$\Rightarrow$ The Sylow 2-subgroup must be contained entirely within the 2^p elements.

$\Downarrow$

The Sylow 2-subgroup is unique

$\Rightarrow$ " " " is normal

$\Rightarrow$ G is not simple.

$2^p(2^p-1)$

p prime $\quad p=2$

$|G| = 4\cdot 3 = 12 \qquad p=2$

$|G| = 8\cdot 7 = 56 \qquad p=3$

$p=4$

(v) $|G| = p^k m \quad , \quad m < p \quad , \quad k \neq 0, \; m \neq 1$

Claim: $n_p = 1$ consequently G is not simple

$n_p \equiv 1 \bmod p, \quad n_p \mid m$

$n_p = 1 + lp \mid m$

but $m < p$

$\Rightarrow l = 0$

$\Rightarrow n_p = 1$

Unique Sylow p-subgroup $\trianglelefteq G$

$|G| = 3\cdot 2 = 6 \qquad p=3$

$3^2\cdot 2 = 18$

$3^3\cdot 2 = 54$

$5\cdot 2 = 10 \qquad p=5$

$5^2\cdot 2 = 50$

$5\cdot 3 = 15 \qquad 5\cdot 4 = 20$

$7 \cdot 2 = 14$ $\quad p = 7$

$7 \cdot 3 = 21$

$7 \cdot 4 = 28$

$7 \cdot 5 = 35$

$7 \cdot 6 = 42$

$11 \cdot 2 = 22$ $\quad p = 11$

$11 \cdot 3 = 33$

$11 \cdot 4 = 44$

$11 \cdot 5 = 55$

$13 \cdot 2 = 26$ $\quad p = 13$

$13 \cdot 3 = 39$

$13 \cdot 4 = 52$

$17 \cdot 2 = 34$ $\quad p = 17$

$17 \cdot 3 = 51$

$19 \cdot 2 = 38$ $\quad p = 19$

$19 \cdot 3 = 57$

$23 \cdot 2 = 46$ $\quad p = 23$

$29 \cdot 2 = 58$ $\quad p = 29$

(vi) $|G| = p^{*}$, $Z(G) \neq \{e\}$

$|G| = p^2$

Claim: G is abelian

$|Z(G)| = p$ or $|Z(G)| = p^2$

if $|Z(G)| = p$ then $G/Z(G)$ is cyclic

$\Rightarrow$ G is abelian

$\Rightarrow |Z(G)| = p^2$

(vii) $|G| = p^3$ $\quad Z(G) \neq \{e\}$

$|Z(G)| = p, p^2, p^3 \hookrightarrow$ abelian

if $|Z(G)| = p^2$

$\Rightarrow$ $G/Z(G)$ cyclic $\Rightarrow$ G is abelian

$\Rightarrow$ $Z(G) \neq p^2$.

$\Rightarrow |Z(G)| = p$ $\quad$ ($Z(G)$ is non-trivial normal subgp)

$\Rightarrow$ G is not simple

$|G| = 4, 8, 9, 27, 25, 49$

(viii) $|G| = 30 = 2 \cdot 3 \cdot 5$

$n_2 \mid 15 \qquad n_3 \mid 10 \qquad n_5 \mid 6$

$n_2 \equiv 1 \ (2) \qquad n_3 \equiv 1 \ (3) \qquad n_5 \equiv 1 \ (5)$

$n_3 = 1, \cancel{2}, \cancel{5}, 10 \qquad n_5 = 1, \cancel{2}, \cancel{3}, 6$

if $n_3 = 10$ & $n_5 = 6$

10 subgps of order 3
6 " " " 5 $\Big\}$ cyclic of prime order

$$(10.3 - 10) + (6.5 - 6)$$
$$= 44$$
$$|G| \geq 44$$
$$\rightarrow\leftarrow$$

either $n_3 = 1$ or $n_5 = 1$ or both

$\Rightarrow$ G is not simple.

(ix) $|G| = 24, 36, 48$

Use the following lemma:

lemma: If G is simple & non-abelian, its order divides $\frac{n_p!}{2}$ where

$$n_p = [G : N_G(P)]$$

$|G| = 24 = 2^3 . 3$

$n_3 \equiv 1 \ (3)$

$n_3 \mid 8$

$n_3 = 1, \cancel{2}, 4, \cancel{8}$

if $n_3 = 4$

$\frac{4!}{2} = 12$

$n_2 \equiv 1 \ (2)$

$n_2 \mid 3$

$n_2 = 1$ or 3

if $n_2 = 3$

$\frac{3!}{2} = 3$

$24 \nmid 12$

$\Rightarrow$ G is not simple

$24 \nmid 3$

$\Rightarrow$ G is not simple

$|G| = 36 = 2^2 \cdot 3^2$

$n_2 \equiv 1 \ (2)$

$n_2 \mid 9$

$n_2 = 1, 3, 9$

$\frac{3!}{2} = 3$

$|G| \nmid 3$

$\Rightarrow$ G is not simple

$n_3 \equiv 1 \ (3)$

$n_3 \mid 4$

$n_3 = 1, \cancel{2}, 4$

if $n_3 = 4$

if $\frac{4!}{2} = 12 \Rightarrow |G| \nmid 12$

G is not simple

$|G| = 48 = 2^4 \cdot 3$

$n_2 \equiv 1 \ (2)$

$n_2 \mid 3$

$n_2 = 1, 3$

$\frac{3!}{2} = 3$

$|G| \nmid 3$

$n_3 \equiv 1 \ (3)$

$n_3 \mid 16$

$n_3 = 1, \cancel{2}, 4, \cancel{8}, 16$

Cauchy's thm. (Abelian groups)

Let G be a finite group s.t for a prime p, $p \mid |G|$, then there exists an element of order p in G.

Pf: Induction on $|G|$.

We will assume that the thm. holds true for any group of order less than the order of G.

Since $|G| > 1 \Rightarrow \exists\, x \neq e \in G$

If $|G| = p \Rightarrow o(x) = p$

Hence, assume that $|G| > p$

Case 1: Suppose $p \mid o(x) \Rightarrow o(x) = mp$ for some $m > 0$

Consider x^m

$$o(x^m) = \frac{o(x)}{\gcd(m, o(x))}$$

$$= \frac{mp}{\gcd(m, mp)} = p$$

$\Rightarrow$ there is an element $x^m \in G$ s.t

$$o(x^m) = p$$

Case 2: Suppose $p \nmid o(x)$

Let $N = \langle x \rangle$. $N \trianglelefteq G$

Consider the factor group G/N.

Since $p \mid |G|/|N|$ & $|G/N| < |G|$.

Applying induction on $|G|$, we get

an element $\bar{y} \in G/N$ s.t $o(\bar{y}) = p$

$\bar{y} = yN$ for some $y \in G$

Also, $o(\bar{y}) \mid o(y)$ (since $\bar{y}^{o(y)} = N$)

$\Rightarrow p \mid o(y)$

Let $o(y) = kp$

Consider $y^k \in G$

$$o(y^k) = \frac{kp}{\gcd(k, kp)} = p$$

$\Rightarrow$ there exists an element $y^k \in G$ s.t $\phi(y^k) = p$.

10/4/24

Proposition 1: Let G be a group & $N \leq G$. Then $N \trianglelefteq G$ iff N is a union of conjugacy classes of G

Pf. later

Conjugacy classes of the symmetric groups

① $\rho(b_1\, b_2 \ldots b_k)\rho^{-1} = (\rho(b_1)\ \rho(b_2) \quad \rho(b_k))$.

② $\Rightarrow$ 2 cycles are conjugate in S_n iff they have the same cycle type.

$(1\ 2\ 3\ 4)(3\ 5\ 4)$ is it conjugate to $(1\ 2\ 3\ 4)\ (5\ 1\ 3)$?

Conjugacy classes in A_5.

2 elements ρ & ρ' from A_5 might be conjugate in S_5 without being conjugate in A_5.

Indeed if $\phi \rho \phi^{-1} = \rho'$ with $\phi \in S_5$, there is no reason that one can choose ϕ to be an even permutation.

If one cannot choose ϕ to be an even permutation, the S_5-conjugacy class of ρ split into two A_5-conjugacy classes.

Element of A_5

(i) 5-cycles

$(1\ 2\ 3\ 4\ 5)$ $\quad 4! = 24$

(ii) 3-cycles $(1\ 2\ 3)$

${}^5C_3$ & each can be ordered in 2 ways

${}^5C_3 \times 2 = 20$

(iii) Product of 2 disjoint cycles $(1\ 2)(3\ 4)$

missing no. can be chosen in 5 different ways

remaining 4 nos. can be split into 2 pairs in 3 different ways

15

(iv) Identity

Thm. A_5 is simple.

Pf. Let $N \trianglelefteq A_5$

$|N| \mid 60 \Rightarrow 2, 3, 4, 5, 6, 10, 12, 15, 20, 30$

N is the union of conjugacy classes, its order must equal the sum of the cardinalities of those conjugacy classes.

Orders of the 5 conjugacy classes of A_5 are:

$1, 12, 12, 15, 20$

Combinations:

$1 \qquad 1+12+12$

$1+12 \qquad 1+12+15$

$1+15$

$1+20$

↳ no match between this list & the list of possible orders above.

$\Rightarrow$ No normal subgroup of A_5.

List of conjugacy classes in A_5.

(i) Product of 2 disjoint cycles:

Assume ρ is conjugate to $(12)(34)$ in S_5.

i.e. $\rho = \phi (12)(34) \phi^{-1}$

If $\phi \in A_5$ ✓

If not replace ϕ by $\phi \circ (12) \longrightarrow$ even

$$\phi(12)(12)(34)(12)\circ\phi^{-1} = \phi(12)(34)\phi^{-1}$$
$$= \rho$$

$\Rightarrow$ ρ belong to the conjugacy class of $(12)(34)$.

(ii) 3-cycle:

* Assume that $\rho = \phi(123)\phi^{-1}$

If ϕ is not even, replace by

$\phi(45) \longrightarrow$ even

Then $\phi(45)(123)(45)\phi^{-1} = \phi(123)\phi^{-1} = \rho$

$\Rightarrow$ ρ & (123) conjugate in A_5.

(iii) 5-cycle:

Not all 5 cycles are conjugate in A_5

$$(12)(12345)(12) = (21345)$$

$$g^{-1}\sigma g = (g(1)\ g(2)\ g(3)\ g(4)\ g(5))$$

$g(1)=2$ $g(2)=1$ $g(3)=3$ $g(4)=4$ $g(5)=5$

$g(1)=1$ $g(2)=3$ $g(3)=4$ $g(4)=5$ $g(5)=2$

$$(21345) = (13452)$$

odd, 2 A_5-conjugacy classes of 5-cycle

Cardinalities of the 2 conjugacy classes equal

C is one, $(12)C(12)^{-1}$ is the other one

* . $a, b, c, d, e \in \{1, 2, 3, 4, 5\}$ are distinct Then

$$(a\,d\,e)(a\,b\,c)(a\,d\,e)^{-1} = (e\,b\,c)$$

are conjugate in A_5

can replace a single element by any element not in that 3-cycle.

** $$((a\,b)(c\,e))^{-1}(a\,b)(c\,d)(a\,b)(c\,e)$$
$$= (a\,b)(c\,d)$$

replace a single element by an element fixed by this permutation.

$$C = \{\rho\sigma\rho^{-1} \mid \rho \text{ even}\}$$
$$C' = \{\rho\sigma\rho^{-1} \mid \rho \text{ odd}\}$$

$\sigma = (1\,2\,3\,4\,5)$

any 2 elements from one of the sets are conjugate in A_5 & there is no "cross conjugation" betn them in A_5.

If $\rho\sigma\rho^{-1} = \alpha(\phi\sigma\phi^{-1})\alpha^{-1}$

ρ even, ϕ odd & α even

then $\phi^{-1}\alpha^{-1}\rho$ is odd & commutes with σ

$\longrightarrow\leftarrow$

σ is an n-cycle in S_n

$\rho\sigma = \sigma\rho \Rightarrow \rho$ is a power of σ

$\rho(i) = i$ then $\rho\sigma^{-i}$ fixes 1.

<u>Thm.</u> A_n is simple $n \geq 5$

Pf. Induction on $n = 5$.

Assume that $N \subseteq A_n$ is a non-trivial proper & normal subgroup.

$I_n = \{1, 2, \ldots, n\}$

For any $a \in I_n$

G_a permutations fixing a,

$G_a \simeq A_{n-1}$

all conjugates

since if ϕ fixes a then

$(cd)(ab)\phi(ab)(cd)$ fixes b

$N \trianglelefteq A_n$

$N \cap G_a \trianglelefteq G_a$

$N \cap G_a = G_a \Rightarrow N = A_n$

12/4/24

Direct Products

Def.^{n}: (i) Let $(G_1, *_1), \ldots, (G_n, *_n)$ be groups. The Direct product

$G_1 \times G_2 \times \cdots \times G_n$ with operation $*$ where $*$ is given by

For $h_i, g_i \in G_i$ $\forall$ $1 \leq i \leq n$,

$$(g_1, g_2, \ldots, g_n) * (h_1, h_2, \ldots, h_n) = (g_1 *_1 h_1, g_2 *_2 h_2, \ldots, g_n *_n h_n)$$

(ii) (Direct product of an infinite countable no. of groups)

$G_1 \times G_2 \times \cdots$ is the set of sequences $(g_1, g_2, \ldots)$ $g_i \in G_i$ s.t

$$(g_1, g_2, \ldots) * (h_1, h_2, \ldots) = (g_1 *_1 h_1, g_2 *_2 h_2, \ldots)$$

Prop.^{n} 1: If $G_1, \ldots, G_n$ are groups, their direct product is a group with

order $= |G_1| |G_2| \cdots |G_n|$

Prop^n 2:- Order of an element

$(g_1, g_2 \ldots, g_n) \in G_1 \times \cdots \times G_n$

is

$o((g_1, g_2 \ldots, g_n)) = \text{lcm}(o(g_1), \ldots, o(g_n))$

Prop^n 3: $G_i \cong \{(1, 1, \ldots 1, g_i, 1, \ldots 1) ; g_i \in G_i\}$

Remark: The direct product introduced here is actually an external direct product

$G_1 \times G_2 \cdots \times G_n$ also represented as $G_1 \oplus G_2 \oplus \cdots \oplus G_n$

Ex. (i) $\mathbb{Z}_8^* \oplus \mathbb{Z}_{10}^*$

$= \{(1,1), (1,3), (1,7), (1,9), (3,1),$
$(3,3), (3,7), (3,9),$
$(5,1), (5,3), (5,7), (5,9),$
$(7,1), (7,3), (7,7), (7,9)\}$

$(3,7) * (7,9) = (5,3)$

(ii) $\mathbb{Z}_2 \oplus \mathbb{Z}_3 = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\}$

$= \langle (1,1) \rangle$

$2(1,1) = (0,2)$

$3(1,1) = (1,0)$

$\mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_6$

$\mathbb{Z}_m \oplus \mathbb{Z}_n \overset{?}{\cong} \mathbb{Z}_{mn}$

Not always!

True iff $\gcd(m,n) = 1$

$\mathbb{Z}_5 \oplus \mathbb{Z}_{12} \cong \mathbb{Z}_{60}$

(iii) Let G be a group s.t $|G| = 4$.

Then either

$G = \{e, a, b, ab\}$ where

$o(a) = o(b) = o(ab) = 2$

or $G = \{e, a, a, a^2\}$

$G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$

$e \to (0,0)$

$a \to (1,0)$; $b \to (0,1)$

$ab \to (1,1)$

$\hookrightarrow \quad G \cong \mathbb{Z}_4$

(iv) Find no. of elements of order 10 in $\mathbb{Z}_{100} \oplus \mathbb{Z}_{25}$

Sol^n: $o((a,b)) = 10$

$\operatorname{lcm}(o(a), o(b)) = 10$

$\Rightarrow \quad o(a) = 10, \quad o(b) = 1$ or 5 — (i)

or $\quad o(a) = 2, \quad o(b) = 5$ — (ii)

Case 1: $o(a) = 10$ & $o(b) = 1$ or 5

Recall, for each positive divisor k of n, $G = \langle x \rangle$ (where $|G| = n$), G has a unique subgroup $\langle x^{n/k} \rangle$ of order k

$\mathbb{Z}_{100}$ has a unique cyclic subgroup of order 10.

Any cyclic subgroup of order 10 has $\phi(10) = 4$ generators.

$\Rightarrow$ 4 choices for a

5 choices for b ($o(b) = 1$ or $\rightarrow$ 1 choice

$o(b)=5)$

$\Rightarrow$ 20 choices for (a,b) $\quad$ 4 choices

$\Rightarrow$ 20 possibilities for (a,b) s.t $o(a,b)=10$

Case 2: $\quad o(a)=2$, $\quad o(b)=5$

1 choice for a $\quad$ 4 choices for b

Total 4 choices for (a,b) s.t $o(a,b)=10$

$\Rightarrow$ $2+2=20+4$ elements in $\mathbb{Z}_{100} \oplus \mathbb{Z}_{25}$ s.t $o(a,b)=10$.

Def^n: (i) A group G is finitely generated if there is a finite subset A of G s.t $G=\langle A\rangle$.

(ii) For each $r \in \mathbb{Z}$ with $r \geq 0$.

Let $\mathbb{Z}^r = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$ be the direct product of r copies of $\mathbb{Z}$

$\hookrightarrow$ called the "free abelian group of rank r".

Note that any finite group is finitely generated.

Thm. 1 (Fundamental Theorem of finitely generated Abelian groups)

Let G be a finitely generated Abelian group. Then

(i) $G \cong \mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_s}$ for some integers $r, n_1, \ldots, n_s$ satisfying the following properties:

(a) $r \geq 0$ & $n_j \geq 2$ $\forall j$, and

(b) $n_{i+1} \mid n_i$ for $1 \leq i \leq r-1$.

(ii) The expression in (i) is unique:

If $G \cong \mathbb{Z}^t \times \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_u}$ where t & $m_1, \ldots, m_u$ satisfy (i) & (ii).

Then, $t = r$ & $u = s$ & $m_i = n_i$ $\forall i$

Remark: (1) The integer 't' is called the 'free rank of G'.

(2) The integers $n_1, n_2, \ldots, n_s$ are called as 'invariant factors of G'.

(3) A f.g. abelian group is a finite group iff $r = 0$.

15/4/24

Thm 1: $|G|, |H| < \infty$ cyclic

Then $G \oplus H$ is cyclic iff $(|G|, |H|) = 1$

Pf. Let $|G| = m$, $|H| = n$

$|G \oplus H| = mn$

Let $G \oplus H$ be cyclic

Claim: $d = \gcd(m, n) = 1$

Pf. Let $G \oplus H = \langle (g, h) \rangle$

$(g,h)^{mn/d} = (g^{mn/d}, h^{mn/d})$

$= (e, e)$

$\Rightarrow mn = o((g,h)) \mid mn/d \Rightarrow d = 1$

$\rightarrow \leftarrow$

Let $d = 1$

Claim: $G \oplus H$ is cyclic

Let $G = \langle g \rangle$, $H = \langle h \rangle$

$d = \gcd(m, n) = 1$

$o((g,h)) = \operatorname{lcm}(o(g), o(h)) = mn$

$\Rightarrow$ $G \oplus H$ is cyclic.

Corollary 1: $G_1 \oplus \cdots \oplus G_n$, G_i is cyclic $\forall i$ is cyclic iff

$$\gcd(|G_i|, |G_j|) = 1 \quad \forall\, i \neq j$$

$\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_8 \not\cong \mathbb{Z}_{48}$

not cyclic

$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$

$\checkmark \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_5$

$\checkmark \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{30}$

$\times \cong \mathbb{Z}_{60}$

We will formulate the F.T.F.A.G in another way & use this formulation for our purpose.

F.T.F.A.G.

Thm. (elementary divisor decomposition of G)

Let G be an abelian group of order $n > 1$ & let

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}.$$

Then,

(i) $G \cong A_1 \oplus A_2 \oplus \cdots \oplus A_k$, where

$$|A_i| = p_i^{\alpha_i}.$$

(ii) For each $A \in \{A_1, A_2, \ldots, A_k\}$ with $|A| = p^{\alpha}$,

$$A \cong \mathbb{Z}_{p^{\beta_1}} \oplus \mathbb{Z}_{p^{\beta_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{\beta_t}}$$

with $\beta_1 \geq \beta_2 \geq \cdots \geq \beta_t \geq 1$ &

$$\beta_1 + \beta_2 + \cdots + \beta_t = \alpha$$

(iii) The decomposition in (i) & (ii) is unique, i.e. if

$G \cong B_1 \oplus B_2 \oplus \cdots \oplus B_m$, with

$|B_i| = p_i^{\alpha_i}$ $\forall i$, then

$B_i \cong A_i$ & B_i & A_i have same invariant factors.

Remark: The integer p^{β_j} $\rightarrow$ elementary divisor

of G.

Let us look at an algorithm for constructing all abelian groups of any order.

Ex. $|G| = p^k$

We will look at the case $k = 1, 2, 3, 4$.

(i) $|G| = p$

$$G \cong A_1$$

$$A_1 \cong \mathbb{Z}_{p^{\beta_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{\beta_t}}$$

$$\beta_1 + \cdots + \beta_t = \alpha$$

here $\alpha = 1 \Rightarrow t = 1$

$$\Rightarrow \beta_1 = 1$$

$$A_1 \cong \mathbb{Z}_p$$

$$G \cong \mathbb{Z}_p$$

$\longrightarrow \leftarrow$

(ii) $|G| = p^2$

$$G \cong A_1$$

$$\beta_1 + \beta_2 = 2$$

$\beta_1 = 2$ or $\beta_1 = 1 = \beta_2$

$G \cong \mathbb{Z}_{p^2}$ or $G \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$

(iii) $|G| = p^3$ $\qquad G \cong A_1$

$$\beta_1 + \beta_2 + \beta_3 = 3$$

$$\beta_1 = \beta_2 = \beta_3 = 1$$

$$G \cong \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$$

$$\beta_1 = 2 \;\&\; \beta_2 = 1$$

$$G \cong \mathbb{Z}_{p^2} \oplus \mathbb{Z}_p$$

$$\beta_1 = 3$$

$$G \cong \mathbb{Z}_{p^3}$$

(iv) $|G| = p^4$ $\qquad G \cong A_1$

$$\beta_1 + \beta_2 + \beta_3 + \beta_4 = 4$$

$$\beta_i = 1 \quad \forall\, 1 \le i \le 4$$

$$G \cong \boxed{\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p}$$

$$\beta_1 = \beta_2 = 2$$

$$G \cong \boxed{\mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2}}$$

$$\beta_1 = 2, \quad \beta_2 = \beta_3 = 1$$

$$G \cong \boxed{\mathbb{Z}_{p^2} \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p}$$

$$\beta_1 = 3, \quad \beta_2 = 1$$

$$G \cong \boxed{\mathbb{Z}_{p^3} \oplus \mathbb{Z}_p}$$

$\beta_1 = 4$

$G \cong \boxed{\mathbb{Z}_{p^4}}$

Q. Find all abelian groups of order 360

$360 = 2^3 \cdot 3^2 \cdot 5$

$G \cong A_1 \oplus A_2 \oplus A_3$

$|A_1| = 2^3$ & $|A_2| = 3^2$ & $|A_3| = 5$

$A_1 \cong \mathbb{Z}_8$

or $\cong \mathbb{Z}_4 \oplus \mathbb{Z}_2$

or $\cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

$A_2 \cong \mathbb{Z}_9$

or $\cong \mathbb{Z}_3 \oplus \mathbb{Z}_3$

$A_3 \cong \mathbb{Z}_5$

We obtain the non-isomorphic abelian group of order 360 by taking 1 abelian group from each of the 3 lists.

(i) $\mathbb{Z}_8 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5$

(ii) $\mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$

(iii) $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5$

(iv) $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$

(v) $\mathbb{Z}_9 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5$

(vi) $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 + \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$

Remark: If we have a specific abelian group of order 360, we cannot identify which of the above groups it is isomorphic to without some additional work, which usually involve checking the no. of elements in each group with a particular order.

But, we do know that it is definitely 1 of the groups on the list.

$|G| = 2^3 \cdot 3^2 \cdot 5 = 360$

Invariant factors

$n_1 = 360$ $\qquad \mathbb{Z}_{360}$

$n_1 = 2^3 \cdot 3 \cdot 5$; $n_2 = 3$ $\qquad \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$

$n_1 = 2^2 \cdot 3^2 \cdot 5$; $n_2 = 2$ $\qquad \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$

$n_1 = 2^2 \cdot 3 \cdot 5$; $n_2 = 2 \cdot 3$ $\qquad \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$

$n_1 = 2 \cdot 3 \cdot 5$; $n_2 = 2 \cdot 3$, $n_3 = 2$

$\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \mathbb{Z}_{n_3}$

$\mathbb{Z}_{360}$

$\mathbb{Z}_{120} \oplus \mathbb{Z}_3$

$\mathbb{Z}_{180} \oplus \mathbb{Z}_2$

$\mathbb{Z}_{60} \oplus \mathbb{Z}_6$

$\mathbb{Z}_{30} \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_2$

$\mathbb{Z}_8 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}$

Obtaining elementary divisor from invariant factor

Ex. $(60, 6)$

$60 = 2^2 \cdot 3 \cdot 5$ & $6 = 2 \cdot 3$

$\mathbb{Z}_{60} \simeq \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$

$\mathbb{Z}_6 \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_3$

$\mathbb{Z}_{60} \oplus \mathbb{Z}_6 \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_5$

elementary divisor

$(2, 3, 3, 4, 5)$

Obtaining invariant factor from elementary divisor

Ex. $(8, 3, 3, 5)$

$G \cong \mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$.

$|G| = 360 = 2^3 \cdot 3^2 \cdot 5$

The prime powers are 2^3, then $3, 3$, then 5

largest factors are $2^3 \cdot 3 \cdot 5 = 120$

remaining factor 3

Invariant factor $(120, 3)$

so $G \cong \mathbb{Z}_{120} \oplus \mathbb{Z}_3$

Ex: $(4, 3, 3)$

invariant factor $(12, 3)$

Remark: Using the uniqueness statement of the F.T.F.A.G (both formulations), we can determine whether any 2 direct product of finite cyclic groups are isomorphic.

Ex. Check if $\mathbb{Z}_6 \oplus \mathbb{Z}_{15} \cong \mathbb{Z}_{10} \oplus \mathbb{Z}_9$

Step 1: Determine if orders are same

Step 2: " " they have same elementary divisors.

$\mathbb{Z}_6 \oplus \mathbb{Z}_{15}$

$\rightarrow \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$

$(2, 3, 3, 5)$

$\mathbb{Z}_{10} \oplus \mathbb{Z}_9$

$\hookrightarrow \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_9$

$(2, 5, 9)$

$\Rightarrow \mathbb{Z}_6 \oplus \mathbb{Z}_{15} \not\cong \mathbb{Z}_{10} \oplus \mathbb{Z}_9$

$a \in \mathbb{Z}_{10} \oplus \mathbb{Z}_9$

$o(a) = 9$

$\mathbb{Z}_6 \oplus \mathbb{Z}_{15} \rightarrow$ no element of order 9