Group Theory:

Motivation:

Set of all bijections of $X \to X$

eg: $f: \{1,2,3\} \longrightarrow \{1,2,3\}$

f is Bijective.

1) Group

A group is a set G with a binary operation

$$G \times G \longrightarrow G$$

$$(g_1, g_2) \longmapsto g_1 \cdot g_2$$

Satisfying these properties

1) $\forall a,b \in G$, $ab \in G$ (closure)
2) $\exists e_0 \in G$ s.t $ge_0 = g = e_0 g$ $\forall g \in G$ Identity
3) $\exists e_1 \in G$ s.t $g \cdot g^{-1} = e_1$ $\forall g \in G - \{e_0\}$ Inverse
4) $\forall a,b,c \in G$ $a(bc) = (ab)c$ Associative

$\therefore$ we say $(G, \cdot)$ is a group.

Examples of Groups:

* $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$

* $(Q-\{0\}, \cdot)$, $(R-\{0\}, \cdot)$, $(C-\{0\}, \cdot)$

Q: S_n which is the permutation group $\forall n \geq 1$. $X \to X$

→ a) $a, b \in S_n \Rightarrow ab \in S_n$

b) $a, I_x \in S_n \Rightarrow aI_x = a = I_x a$

c) $\forall a \in S_n \ \exists b \in S_n \Rightarrow ab = I_x = ba$

d) $\forall a, b, c \in S_n \Rightarrow a(bc) = (ab)c$

Q: $Q_n = e^{i\frac{2\pi}{n}} = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)$

But by de-moivre theorem $Q_n^n = 1$ (Primitive roots of unity)

$Q_n^m \neq 1$ if $0 < m < n$

Let $G = \{1, Q_n \cdots Q_n^{n-1}\}$; $(G, \cdot)$

This is a group

a) $\forall a, b \in G \Rightarrow ab \in G$

b) $\forall a, 1 \in G$ s.t $a \cdot 1 = a = 1 \cdot a$

c) $\forall a, b, c \in G$; $a(bc) = (ab)c$

d) $\forall a \in G \ (a = Q_n^i) \ \exists b \in G \ (b = Q_n^{n-i})$

s.t $a \cdot b = 1 = b \cdot a$

∴ G is a group.

* $GL_n(\mathbb{R})$, $SL_n(\mathbb{R})$, $(M_{m\times n}(\mathbb{R}), +)$

General linear group $(GL_n(\mathbb{R}), \cdot)$

special linear group $(SL_n(\mathbb{R}), \cdot)$

Definition: A group $(G, \cdot)$ is called abelian if $a \cdot b = b \cdot a \quad \forall a, b \in G$

examples: $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q}-\{0\}, \cdot)$, $(\mathbb{R}-\{0\}, \cdot)$

But S_n is not abelian for $n \geq 3$.

Why: Fix $\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 3 & 2 & 1 & \cdots & n \end{pmatrix} = \alpha$

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

$\beta \cdot \alpha \neq \alpha\beta$ (check)

$\therefore S_n$ is not abelian.

Definition

A group G is called finite if $|G| < \infty$.

Examples: S_n is finite $\forall n \geq 1$

Ans: This is because S_n has $n!$ elements.

$(n \to 1, (n-1) \to 2 \cdots 1 \to n)$

$(\therefore n!$ elements)

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are not finite

Definition: if $|G| < \infty$ then $|G|$ is called the order of the group. ($|G| = \#$ elements)

Properties:

* Cancellation: Let G be a group
$\forall a, b, c \in G$

if $ab = ac \Rightarrow b = c$

. $ab = ac \Rightarrow a^{-1}(ab) = a^{-1}(ac)$

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

$= e_0 b = e_0 c$

$= b = c$

} check properties

* G has a unique identity element

Suppose G has two identities e_0', e_0''

Then $e_0' e_0' = e_0'$ and $e_0' e_0'' = e_0''$

$\Rightarrow e_0' e_0' = e_0' e_0''$ { Cancellation }

$\Rightarrow e_0' = e_0''$

* G has a unique inverse

Let $g \in G$. Suppose g has 2 inverses g_1 & g_2.

Then $g_1 g = e = g_2 g$

$\Rightarrow g_1 = g_2$ QED

Q: $\forall g \in G \ (g^{-1})^{-1} = g$

$= g^{-1} \cdot g = e = g \cdot g^{-1}$

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

Q: $\forall g, h \in G \Rightarrow (gh)^{-1} = h^{-1}g^{-1}$

$= (h^{-1}g^{-1})(gh) = e = (gh)(h^{-1}g^{-1})$

$= (h^{-1}g^{-1})(gh) = e$

$= (h^{-1}g^{-1}) = (gh)^{-1}$

QED

Multiplication Table:

$\therefore G = \{1, -1, i, -i\}$ Quaternions

$|G| < \infty$

	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

$S_3 = \{(123), (21), (31), (32), (231), (312)\}$

	(123)	(21)	(31)	(32)	(231)	(312)
(123)	(123)	(21)	(31)	(32)	(231)	(312)
(21)	(21)	(123)	(312)	(231)	(132)	(132)
(31)	(31)	(231)	(123)	(312)	(213)	(213)
(32)	(32)	(312)	(231)	(123)	(321)	(321)
(231)	(231)	(321)	(132)	(213)	(123)	(312)
(312)	(312)	(321)	(132)	(213)	(312)	(123)

QED

Q: Show that $\forall a \in G \quad \exists n$ s.t $a^n = e_0$ $|G| < \infty$

Ans: Let $G = \{ e, a, a^2 \ldots \ldots \}$

$\therefore \exists n, m \in \mathbb{Z}^+$ s.t $a^m = a^n$ $\boxed{n \neq m}$

Assume $m > n$

Then $a^m a^{-n} = a^n \cdot a^{-n} = e_0$

$a^{m-n} = e$

now let $n = m - n > 0$

$\therefore a^n = e$

QED

This is not true if $|G| = \infty$

Ex: Let $G = \mathbb{Z}$, $1 \in G$ ie $(G, +)$

Now $1 + 1 \ldots$ (n terms) $\neq 0$

$\therefore$ Not true

Q: $|G| < \infty$. Show that $\exists n$ s.t $a^n = e_0$ $\forall a \in G$

Ans: We know $\forall a \in G \quad \exists n_a$ s.t $a^{n_a} = e_0$

Let $n = \prod_{a \in G} n_a$; $G = \{ a_1, a_2 \ldots$

Then $a^n = e_0 \quad \forall a \in G$

now $a_1^n = a_1^{(n_{a_1} \ldots n_{a_{|G|}})}$

$$= \underbrace{a_1 \cdot a_1 \cdots a_1}_{n a_1} \cdot \underbrace{a_1 \cdot a_1 \cdots a_1}_{n a_1} \cdots \underbrace{a_1 \cdot a_1 \cdots a_1}_{n a_1}$$

$$= e \cdot e \cdot e \cdots e$$

$$= e$$

$$= (e)^{n a_2 \cdots n a_{|G|}} = \underline{\underline{e}}$$

∴ This works for all $a \in G$

QED.

Q: Let $a^n = e$ and $n \mid m$, then $a^m = e$.

Ans: now since $n \mid m \Rightarrow m = nk$

But $a^n = e$

$\Rightarrow (a^n)^k = e^k$

$\Rightarrow a^{nk} = e$

$\Rightarrow \underline{\underline{a^m = e}}$ QED.

Q: $|G| \leq 5$ is abelian

Ans: if G is not abelian then $\exists\ a, b \in G$ s.t $ab \neq ba$.

↓

Using Contrapositive

Case 1: $|G| = 1$

Then $G = \{e\}$ is abelian

Case 2: $|G|=2$ $G=\{e,a\}$ $a\neq e$

Then G is abelian, $ae=a=ea$

Case 3: $|G|=3$ $G=\{e,a,b\}$ $e\neq a\neq b$

Now I claim $ab=e$ $\begin{cases} ab=a \Rightarrow b=e \\ ab=b \Rightarrow a=e \\ \times \end{cases}$

$\therefore ab=e=ba$

$ea=a=ae$ $\therefore$ Abelian

$eb=b=be$

Case 4: $|G|=4$ $G=\{e,a,b,ab\}$ $e\neq a\neq b\neq ab$

Now $ea=a=ae$

$eb=b=be$

$e(ab)=ab=(ab)e$

Now to find ba

I claim $ba=ab$ as $\begin{cases} ba=e \Rightarrow a=b^{-1} \times \\ ba=a \Rightarrow b=e \\ ba=b \Rightarrow a=e \\ \times \end{cases}$

$\therefore ba=ab$

$\Rightarrow G$ is also abelian again.

Case 5: $|G|=5$ $G=\{e,a,b,ab,ba\}$ $e\neq a\neq b\neq ab\neq ba$

Now $ea=a=ae$

$be = b = eb$

$(ab)e = ab = e(ab)$

$(ba)e = ba = e(ba)$

Claim: $aba = b$ and $bab = a$

$aba = b \Rightarrow$

- $a(ba) = e \Rightarrow ba = a^{-1}$
- $(ab)a = e \Rightarrow ab = a^{-1}$
- $\times$ {unique inverse}
- $(ab)a = a \Rightarrow ab = e$
- $a(ba) = a \Rightarrow ba = e$
- $aba = ab \Rightarrow a = e$
- $\times$

Similarly $bab = a$

Next claim: $a^2 = b^2$

$\Rightarrow$ Since $aba = b \Rightarrow baba = b^2$

$bab = a \Rightarrow baba = a^2$

$\Rightarrow a^2 = b^2$

Next $a^2 = e \Rightarrow$

- $a^2 = a \Rightarrow a = e$
- $a^2 = b \Rightarrow b^2 = b \Rightarrow b = e$
- $a^2 = ab \Rightarrow a = b$
- $a^2 = ba \Rightarrow a = b$
- $\times$

$\therefore a^2 = e = b^2$

Now since $bab = a$

$babb = ab$

$\Rightarrow bab^2 = ab$ $\quad \therefore$ G is abelian

$\Rightarrow ba = ab$

QED

Q: Let $G = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid a \in R \right\}$

G is abelian

Ans: Let $M_1 = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ $\quad M_2 = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$

now $M_1 \cdot M_2 = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix}$

$M_2 \cdot M_1 = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix}$

$\therefore M_2 \cdot M_1 = M_1 \cdot M_2$ QED

CHAPTER I OVER :)

Subgroups:

Let G be a group. A subgroup H of G is a subset of G which has:

i) $\forall a, b \in H \Rightarrow a \cdot b \in H$

ii) $e \in H$

iii) $\forall a \in H \Rightarrow a^{-1} \in H$

Examples: a) $\mathbb{Z}$ is a subgroup of $\mathbb{Q}$ $(+)$

b) $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ $(+)$

c) $\mathbb{Q} - \{0\} \subseteq \mathbb{R} - \{0\} \subseteq \mathbb{C} - \{0\}$ $(\cdot)$

d) $H = \{ mn \mid n \in \mathbb{Z} \}$ for a fixed $m \in \mathbb{N}$

Odd integers do not form a subgroup as $0 \notin$ odd integers.

e) $a\mathbb{Z} = \{ an \mid n \in \mathbb{Z} \}$ $\forall a \in \mathbb{N}$

Theorem: Every subgroup of $\mathbb{Z}$ is of the form $a\mathbb{Z}$ for some $a \in \mathbb{Z}^+$.

Proof: Let H be a subgroup of $\mathbb{Z}$.

If $H = \{0\} = 0 \cdot \mathbb{Z} = \{ 0 \cdot n \mid n \in \mathbb{Z} \} = \{0\}$

Suppose $H \neq \{0\}$. So H contains an integer $n \neq 0$.

In fact, H contains a positive integer $n > 0$.

Let $n \neq 0$ be an element of H.

i) $n > 0 \rightarrow$ done

ii) $n < 0 \Rightarrow -n > 0$. Since $n \in H$, $-n \in H$. $(H \subseteq G)$

Now let 'a' be the smallest positive integer contained in H.

Claim: $\boxed{H = a\mathbb{Z}}$

Let $b \in H$, $b > 0$.

As 'a' is the smallest $\therefore b \geq a$.

now $a|b \Rightarrow \boxed{b = ap + q}$ $\therefore \boxed{p \in \mathbb{Z}}$ $\boxed{0 \leq q \leq a}$

$\Rightarrow \underline{b - ap = q}$ $\begin{cases} a \in H \\ -ap \in H \\ b \in H \end{cases}$ $\{\in a + \underbrace{\ldots}_{p} \in a\}$

$\therefore \Rightarrow b - ap \in H$

$\therefore q \in H$. But $q < a$.

$\Rightarrow$ q can't be positive and 'a' is the smallest positive integer in H.

$\therefore b = ap \Rightarrow b \in a\mathbb{Z}$

$\therefore$ every positive integer in H is a multiple of a.

Next: If $b \in H$, $b < 0$, then $(-b) > 0$

$\therefore -b \in H$, $ap \in H$, for some $p \in \mathbb{Z}$

$\therefore b = (-ap)$ $\therefore b$ is a multiple of a.

$\therefore H \subseteq aZ$.

Now next $aZ \subseteq H$ as $a \in H$ and H is a subgroup.

$\therefore H = aZ$.

QED.

Remark: Trivial subgroups

$\{e\}, G \subseteq G$

Next:

Let G be a group, $a \in G$

Definition: subgroup generated by 'a' $= \{a^n \mid n \in Z\}$

$\{\ldots a^{-3}, \ldots a^3\} = \langle a \rangle$

If a subgroup H of G contains a then $a^n \in H$

$\forall n \in Z$. So $H \supseteq \langle a \rangle$.

$\therefore \langle a \rangle$ is the smallest subgroup of G containing 'a'.

Def: G is called cyclic if $\exists a \in G$ s.t $\langle a \rangle = G$

$\therefore G = \{\ldots, a^{-3}, \ldots, e, \ldots a^3\}$

Examples: $(\mathbb{Z}, +)$ is cyclic

as $\langle 1 \rangle = \mathbb{Z}$

$\{-1, 1\}$ is a generator of $\mathbb{Z}$

Definition: The order of a, $a \in G$ is the order of $\langle a \rangle$ if $\langle a \rangle$ is finite. Order of a is $o(a)$.

Example: * G be any group; $o(e) = 1$

$(\langle e \rangle = \{e\})$

* $G = \mathbb{Z}$, $o(a) = \infty$ if $a \neq 0$
* $S_3 = \{(12), (13), (23), (123), (132), (321)\}$

Q. $|G| = n$

G is cyclic $\Leftrightarrow$ G contains one element of order n

And $\Rightarrow$ Since G is cyclic then $G = \langle a \rangle$ $\exists\, a \in G$

But $|G| = n$ $\therefore$ $\langle a \rangle = o(a) = n$

$\Leftarrow$ Let $a \in G$ s.t $o(a) = n$

Now since $\Rightarrow \exists\, A \subseteq G$ s.t it is generated by a and $o(a) = n$

$\therefore$ As $|G| = n \Rightarrow A = G = \langle a \rangle$

QED.

Note: A cyclic group is abelian.

Q: Suppose that G has only the trivial subgroups. Then G is cyclic.

Ans: If $G = \{e\}$ then G is cyclic.

If $G \neq \{e\}$, $a \in G$. Let $H = \langle a \rangle \neq \{e\}$

But then by definition $\langle a \rangle = G$

$\therefore$ G is cyclic.

QED

★ **Definition:**

The center of G, denoted $Z(G)$

$$Z(G) := \{ g \in G \mid ag = ga \ \forall a \in G \}$$

Proposition: $Z(G)$ is a subgroup of G

Proof: Let $g_1, g_2 \in Z(G)$

i) Closure: $g_1 \in Z(G)$, $g_2 \in Z(G)$ then $g_1 \cdot g_2 \in Z(G)$

as $Z(G) = \{ g_1 g_2 \in G \mid a(g_1 g_2) = (g_1 g_2)a \ \forall a \in G \}$

$$= \{ (g_1 g_2)a = g_1(g_2 a) = g_1(a g_2) = (g_1 a) g_2 = a(g_1 g_2) \}$$

ii) Identity

$e \in Z(G) : ea = ae \quad \forall a \in G$

iii) Inverse

$g \in Z(G)$

Now $g^{-1}a = (a^{-1}g)^{-1} = (ga^{-1})^{-1} = ag^{-1}$

($a^{-1}g$: proved before; ga^{-1}: $g \in Z(G)$)

$\therefore Z(G)$ is a subgroup $\blacksquare$.

Prop: If G is abelian, then $Z(G) = G$

★ **Definition:** Let $a \in G$

The centralizer of a, denoted $C(a)$ is

$$C_G(a) := \{ \forall g \in G \mid ag = ga \}$$

Q: $C_G(a)$ is a subgroup of G

Ans: Let $g_1, g_2 \in C_G(a)$

i) Closure

$(g_1 g_2)a = (g_1)(g_2 a) = g_1(ag_2) = (g_1 a)g_2$

$= a(g_1 g_2)$

ii) $e \in C_G(a)$ (Identity)

as $ea = ae$

iii) $g \in C_G(a)$ (Inverse)

$\Rightarrow ag = ga$

$\Rightarrow g^{-1}agg^{-1} = g^{-1}gag^{-1}$

$\Rightarrow g^{-1}a = ag^{-1}$

$\therefore C_G(a) \subseteq G.$ QED

Q: $Z(G) \subseteq C_G(a) \quad \forall a \in G$

Ans: Let $g \in Z(G)$

$\Rightarrow \forall a \in G,\ ga = ag$

But this then

$\Rightarrow \forall a \in G : g \in C_G(a)$

$\therefore Z(G) \subseteq C_G(a)$ QED

Q: If G is abelian then, $C_G(a) = G \quad \forall a \in G$

Ans: Since G is abelian, let $a \in G$

$$C_G(a) = \{ \forall g \in G : ag = ga \}$$

But since G is abelian and a was arbitary

$\Rightarrow C_G(a) = G.$

CHAPTER 2 ENDS

Group Homomorphisms

Let G, G' be two groups.

Definition: Let $\phi : G \to G'$
s.t $\phi(ab) = \phi(a) \cdot \phi(b)$ $\forall a, b \in G$

Examples: ★ Let $\phi : \mathbb{Z} \to \mathbb{Z}$

$$\phi(a) = na$$

This is a group homomorphism as

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

★ $\phi : \mathbb{Z} \to \{-1, 1\}$ or
$\phi : \mathbb{Z} \to \mathbb{Z}_2$ { $\mathbb{Z}_2$ is a group }

$$\phi(a) = \begin{cases} 0 & \text{if } a \text{ is even} \\ 1 & \text{if } a \text{ is odd} \end{cases}$$

★ $\phi : GL_n(\mathbb{R}) \to \mathbb{R} - \{0\}$

$$\phi(A) = \det(A)$$

True $\phi(AB) = \phi(A) \cdot \phi(B)$ $\forall A, B \in GL_n(\mathbb{R})$

$$= \det(A)\det(B)$$
$$= \det(AB) = \phi(AB)$$

★ G is an arbitary group. let $a \in G$

$$\phi : \mathbb{Z} \to G \quad (\mathbb{Z}, +)$$

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

$$\phi(m+n) = \phi(m) \cdot \phi(n), \ \forall\ m, n \in \mathbb{Z}$$

$$a^{m+n} = a^m \cdot a^n = \underline{\underline{a^{m+n}}}$$

★ G is abelian

$$\phi : G \to G$$

$$\phi(a) = a^2$$

$$\phi(ab) = \phi(a)\phi(b) \quad \forall\ a, b \in G$$

$$(ab)^2 = a^2 b^2 = aabb = a(ab)b$$

$$= (ab)(ab)$$

$$= \underline{\underline{(ab)^2}}$$

★ Same ϕ but G is not abelian

let $G = S_3$

$$\phi : S_3 \to S_3$$

$$\phi(f_i) = f_i^2 \quad \forall\ i \in \{1, 2, 3, 4, 5, 6\}$$

ϕ is not a group homomorphism.

$f_2 : (2\,1) \quad f_3 : (3\,1)$

$f_2 f_3 = (3\,1\,2) = f_6$

Now $\phi(f_2) = f_2^2 = f_1 = (1)(2)(3)$

$\phi(\sigma_3) = \sigma_3^2 = \sigma_1 = (1\,2\,3)$

But $\phi(\sigma_2\sigma_3) = \phi(\sigma_6) = \sigma_6^2 \neq (1\,2\,3)$

But $\phi(\sigma_2)\phi(\sigma_3) = \sigma_1^2 = (1\,2\,3)$

$\therefore$ Not a group homomorphism.

Properties:

Proposition: Let $\phi: G \to G'$ be a group homomorphism. Then

1) $\phi(e_G) = e_{G'}$
2) If $a \in G$ then $\phi(a^{-1}) = (\phi(a))^{-1}$

Proof: 1) $e_G \cdot e_G = e_G$

$\phi(e_G \cdot e_G) = \phi(e_G)$

$\Rightarrow \phi(e_G)\cdot\phi(e_G) = \phi(e_G) \in G'$

$\Rightarrow (\phi(e_G))^{-1}(\phi(e_G)\cdot\phi(e_G)) = e_{G'}$

$\Rightarrow \therefore \phi(e_G) = e_{G'}$

ii) Let $a \in G$ then $aa^{-1} = e_G$

$\phi(aa^{-1}) = \phi(e_G) = e_{G'}$ (i)

$\Rightarrow \phi(a)\cdot\phi(a^{-1}) = e_{G'}$

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

QED

Subgroups associated to a group homomorphism.

Let $\phi: G \to G'$

i) **Kernel of ϕ.** $\ker(\phi) = \{ a \in G \mid \phi(a) = e_{G'} \}$

ii) **Image of ϕ.** $\text{im}(\phi) = \{ \phi(a) \mid \forall\, a \in G \}$

Proposition: i) $\ker(\phi) \subseteq G$; subgroup

ii) $\text{im}(\phi) \subseteq G$; subgroup.

Proof: i) $\ker(\phi)$ is closed under the binary operation of G.

$a, b \in \ker(\phi) \Rightarrow \phi(a) = \phi(b) = e_{G'}$

$\Rightarrow \phi(ab) = \phi(a) \cdot \phi(b) = e_{G'}$

$\Rightarrow ab \in \ker(\phi)$

Neutral: $e_{G'} = \phi(e_G) \Rightarrow e_G \in \ker(\phi)$

Inverse: $a \in \ker(\phi) \Rightarrow \phi(a) = e_{G'}$

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

$= (e_{G'})^{-1} = e_{G'}$

$\Rightarrow a^{-1} \in \ker(\phi)$

ii) $\text{Im}\,\phi$ is closed under binary operation of G'.

$\phi(a), \phi(b) \in \text{Im}\,\phi$

$\Rightarrow \phi(a) \cdot \phi(b) = \phi(ab) \in \text{Im}\,\phi$

Neutral: $\phi(e_G) = e_{G'} \Rightarrow e_{G'} \in \text{Im}\,\phi$

Inverse: let $\phi(a) \in \operatorname{Im}\phi$

Then $(\phi(a^{-1})) = (\phi(a))^{-1}$

$\in \operatorname{Im}\phi$.

QED

Example: ★ $\phi: \mathbb{Z} \to \mathbb{Z}$ $n \in \mathbb{Z}$

$\phi(a) = na$

$\ker(\phi) = \{0\}$

$\operatorname{Im}\phi = \{na \mid a \in \mathbb{Z}\} = n\mathbb{Z}$

★ $\phi: GL_n(\mathbb{R}) \to \mathbb{R} - \{0\}$

$\phi(A) = \det(A)$

$\ker(\phi) = \{A \in GL_n(\mathbb{R}) \mid \det(A) = 1\}$

$= SL_n(\mathbb{R})$

$\operatorname{Im}\phi = \{\det A \mid A \in GL_n(\mathbb{R})\} \subseteq \mathbb{R} - \{0\}$

$= \mathbb{R} - \{0\}$

Why? for a non-zero real number $a \in \mathbb{R} - \{0\}$

$\exists A \in GL_n(\mathbb{R})$ s.t $\det(A) = a$

Let $A = \begin{bmatrix} a & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{bmatrix} = \det(A) = a$

* G be a group. Fix $a \in G$

$$\phi : \mathbb{Z} \longrightarrow G$$

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

$$\ker \phi = \{ n \in \mathbb{Z} \mid a^n = e_G \} \subseteq \mathbb{Z}$$

$$\operatorname{Im} \phi = \{ \phi(n) \mid n \in \mathbb{Z} \} = \{ a^n \mid n \in \mathbb{Z} \} = \langle a \rangle$$

Now $\ker \phi \subseteq \mathbb{Z}$

$$\Rightarrow \ker \phi = b\mathbb{Z} \quad \exists\, b \in \mathbb{Z}^+$$

Note: But $b = \operatorname{ord}(a)$

$\therefore \ker \phi = \{0\}$ if $b = 0$

$\ker \phi = b\mathbb{Z}$, $b > 0$ $(\operatorname{ord}(a) = b)$

Next:

Let $\phi : G \to G'$ be a group homomorphism

i) Injective : $a \neq b \Rightarrow \phi(a) \neq \phi(b)$

ii) Surjective : $\operatorname{Im} \phi = G'$

Proposition: ϕ is injective $\iff \ker(\phi) = \{e_G\}$

$\Rightarrow$ ϕ is injective.

Let $a \in \ker \phi$. Then $\phi(a) = e_{G'} = \phi(e_G)$

$\Rightarrow a = e_G$

So $\therefore \ker(\phi) = \{e_G\}$

$\Leftarrow \ker(\phi) = \{e_G\}$

Suppose $\phi(a) = \phi(b) \Rightarrow \phi(a)\phi(b)^{-1} = e_{G'}$

$\Rightarrow \phi(a) \cdot (\phi(b^{-1})) = e_{G'}$

$\Rightarrow \phi(ab^{-1}) = e_{G'}$

$ab^{-1} \in \ker \phi$

$\Rightarrow ab^{-1} = e_G$

$\Rightarrow a = b$

$\therefore \phi$ is injective

QED

Definition: An isomorphism is

$\phi: G \to G'$

i) Homomorphism

ii) Bijective

Prop: $\phi: G \to G'$ is a group isomorphism then $\phi^{-1}: G^{-1} \to G$ is also a group isomorphism.

Example: $G_1 = \{1, i, -1, -i\}$

$G_2 = \{e, a, a^2, a^3\}$

Then $\phi: G_1 \to G_2$ is isomorphic.

Let $\phi(a) = \begin{cases} 1 \to e \\ -1 \to a^2 \\ i \to a \\ -i \to a^3 \end{cases}$

$\Rightarrow G_1 \cong G_2$

Proposition: If $G_1 \cong G_2$ then

i) G_1 is abelian $\Leftrightarrow$ G_2 is abelian

ii) G_1 is cyclic $\Leftrightarrow$ G_2 is cyclic

Normal subgroup

Definition: Let G be a group. A normal subgroup H of G is a subgroup s.t given $g \in G$ then

$\Rightarrow ghg^{-1} \in H$

Example: ★ If G is abelian, then every subgroup is normal.

Ans: $ghg^{-1} = gg^{-1}h = h \in H$

★ Let $\phi: G \to G'$ be a group homomorphism. Then $\ker(\phi)$ is a normal subgroup of G.

Ans: Let $g \in G$ & $h \in \ker(\phi)$

$\Rightarrow ghg^{-1} \in \ker(\phi)$

But $\phi(ghg^{-1}) = \phi(g)\phi(h)\phi(g^{-1})$

$= \phi(g) \cdot e_{G'} \phi(g^{-1})$

$= \phi(g)\phi(g^{-1})$

$\Rightarrow \phi(e_G) = e_{G'} \in \ker\phi$

QED

★ Center of a group is normal.

$$Z(G) = \{ g \in G \mid ag = ga \ \forall a \in G \}$$

Now let $g \in G$, $h \in Z(G)$

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

$\{ h \in Z(G) \}$
$\{ g^{-1}h = hg^{-1} \}$

$\therefore$ QED

Equivalence Relations on a set S

i) $a \sim b \Rightarrow$ 'a' is related to 'b'.

$\Rightarrow$ a) $a \sim a \ \forall a \in S$

b) $a \sim b \Rightarrow b \sim a \ \forall a, b \in S$

c) $a \sim b, b \sim c \Rightarrow a \sim c \ \forall a, b, c \in S$.

Example: * $(\mathbb{Z}, =)$: $a \sim a$ if $a = a$.

* Let G be a group. $H \subseteq G$ be a subgroup.

Let $a, b \in G$. $a \sim b$ if $a^{-1}b \in H$

i) $a \sim a$: $a^{-1}a = e \in H$

ii) $a \sim b$: $a^{-1}b \in H \Rightarrow (a^{-1}b)^{-1} \in H$

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

$\Rightarrow b \sim a$

iii) $a \sim b, b \sim c$

$a^{-1}b \in H \quad b^{-1}c \in H$

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

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

$\Rightarrow a \sim c$

Equivalence Classes

Def: Let S be a set, $\sim$ be an equivalence relation on S.

Equivalence class:

$$[a] = \{b \in S \mid a \sim b\}$$

Example: * $H \subseteq G$ a subgroup. $a \sim b \Rightarrow a^{-1}b \in H$

$$[a] = \{b \in G \mid a^{-1}b \in H\}$$

$$= \{b \in G \mid a^{-1}b = h \in H\}$$

$$= \{b \in G \mid b = ah \in H\}$$

$= \{ah \in G \mid h \in H\}$

$=: aH$

QED

Proposition: Let S be a set. $\sim$ equivalence relation.

Then the equivalence classes of elements of S 'partition S'. S is a disjoint union of equivalence classes.

Proof: If $a \in S$, then $a \in [a]$ $\{a \sim a\}$

now $S = \bigcup_{a \in S} [a]$

Claim: If $[a]$ and $[b]$ are not disjoint then $[a] = [b]$

Proof: Let $c \in [a] \cap [b]$

$\Rightarrow a \sim c \wedge b \sim c$

$\Rightarrow a \sim b$ {Transitive}

$\Rightarrow a \in [b]$

$\Rightarrow b \in [a]$

$\Rightarrow [a] = [b]$

∴ It follows that S is a disjoint union of equivalence classes.

If $[a] \cap [b] \neq \emptyset$ then $[a] = [b]$.

Now take distinct equivalence classes; they are mutually disjoint.

Their union is S.

QED

Example: * $S = \mathbb{Z}$, $a \sim b$ if $a = b$

$[a] = \{a\}$

$\therefore \mathbb{Z} = \bigcup_{a \in S} [a]$

Problem: Describe all group homomorphisms from $\mathbb{Z} \to \mathbb{Z}$.

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

Ans: Suppose $\phi : \mathbb{Z} \to \mathbb{Z}$ is a group homomorphism.

Suppose $\phi(1) = a \in \mathbb{Z}$, $\phi(n)$?

$\therefore \phi(1+1) = \phi(1) + \phi(1)$

$\phi(2) = 2a$

$\Rightarrow \phi(n) = na$ if $n > 0$

$$\phi(-1) = -\phi(1)$$
$$= -a$$
$$\Rightarrow \phi(-n) = -na \text{ if } n < 0$$

$\therefore \forall n \in \mathbb{Z} \Rightarrow \phi(n) = na$

$\Rightarrow \phi$ is determined by $\phi(1)$.

Next: what are the possible choices for $\phi(1)$?

$\forall a \in \mathbb{Z}$, define a group homomorphism

$$\phi : \mathbb{Z} \to \mathbb{Z} \quad \phi(1) = a$$

Then ϕ is a homomorphism.

$\therefore$ The group homomorphism are determined by the image of 1 ie $\text{Im}(\phi(1))$

Problem: Which of these $\phi : \mathbb{Z} \to \mathbb{Z}$ are isomorphism?

And $\phi_a : \mathbb{Z} \to \mathbb{Z}$ $\phi_a(1) = a$

ϕ_a is injective but not surjective as

$\phi_a(1) = a$

for $a \geq 2$ ie $\phi_2(1) = 2 \Rightarrow \phi_2(n) = 2n \neq 1$
$n \neq \frac{1}{2} \in \mathbb{N}$

ϕ_a is not onto for $a \leq -2$.

Then ϕ_1 is the identity map on $\mathbb{Z}$

$\phi_{-1}(n) = -n$

$\phi_1(n) = n$

$\phi_0(n) = 0 \rightarrow$ not onto and not one-one.

Summary: * Every group homomorphism $\mathbb{Z} \to \mathbb{Z}$ is one of the homomorphism $\{\phi_a : a \in \mathbb{Z}\}$

* ϕ_a is an isomorphism $\Leftrightarrow a = 1 \mid -1$
* ϕ_a is injective $\Leftrightarrow a \neq 0$
* ϕ_a is surjective $\Leftrightarrow a = 1 \mid -1$

Problem: Let G be a group, and let $a \in G$.

Suppose that $\text{ord}(a) = n$ $[\text{ord}(a) = \min\{k : a^k = e : a^k\}]$

if $a^n = e$ $\exists n \in \mathbb{N}$

then $n \mid n$.

Solution: Consider the homomorphism

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

$\phi(m) = a^m$

ϕ : group homomorphism

$\ker \phi = n\mathbb{Z}$ $\quad n = \min(a^n = e)$

or $\ker \phi = 0$ [In our problem $\ker \phi \neq 0$ because $n \in \ker \phi$]

$\therefore$ $\ker \phi$ is generated by $\text{ord}(a)$.

Since $a^n = e$, $n \in \ker \phi$

But $\ker \phi = n\mathbb{Z}$

$\Rightarrow n \in n\mathbb{Z}$

$\Rightarrow n = n \cdot m \quad \exists\, m \in \mathbb{Z}$

$\Rightarrow m = \left(\frac{n}{n}\right)$

Q E D

Why? Take a, write powers of a

$P = \{a^1, a^2, a^3 \ldots$

Two possibilities: ★ we never encounter e

$|G| = \infty$ (after a)

★ $e \in \{\text{sequence}\}$, $\text{ord}(a)$ and $\text{ord}(a)$ is where e occurs. Then the sequence repeats.

Ex: $a^5 = e$

$[a, a^2, a^3, a^4, a^5 = e][a^6, a^7, a^8, a^9, e^2 = e] \ldots$

Problem: $\phi: G \to G'$ group homo

Let $a \in G$, $\text{ord}(a) = n$

$\Rightarrow$ what does it say for $\text{ord}(\phi(a))$.

Soln: $\text{ord}(a) = n \Rightarrow a^n = e_G$

$\Rightarrow \phi(a^n) = \phi(e_G) = e_{G'}$

$\Rightarrow (\phi(a))^n = e_{G'}$

$\Rightarrow \text{ord}(\phi(a)) \mid n.$ QED

In particular if $\phi: G \to G$ is a group homomorphism: $a \in G$, $\text{ord}(a) = 5$

$\therefore$ $\phi(a)$ has order either 1 or 5.

Lagrange Theorem & Cosets

Theorem: $H \subseteq G$

Then $a \sim b$ if $a^{-1}b \in H$

Equivalence classes

$[a] = \{ b \in G \mid a^{-1}b \in H \} = aH$

$aH \stackrel{\text{def}}{=} \{ ah \mid h \in H \}$

Def: If $H \subseteq G$ then **left cosets** of H are subsets aH, $a \in G$.

Right cosets Ha, $a \in G$.

Since **EC** partition the set, the **LC** partition G.

EC - equivalence classes

LC - left cosets

$$G = \bigcup_{i \in I} aH_i;\ a \in G \text{ and } \bigcap_{i \in I} aH_i = \emptyset$$

Proposition: $H \subseteq G$. $a \in G$

Then $|aH| = |H|$

Proof: Consider $\phi: H \to aH$

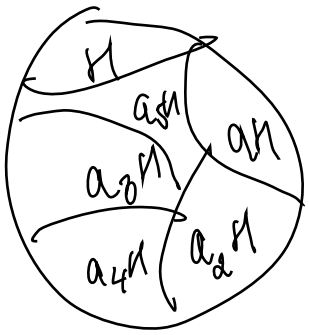
$\phi(h) = ah$

Then ϕ is bijective

And: Onto: $h = ah$

1-1: $ah_1 = ah_2 \Rightarrow h_1 = h_2$

$\therefore$ Same cardinality



$G = eH \cup a_1H \cup a_2H \cup a_3H \cdots \cup a_nH$

$n = \#LC$

$|G| = |eH| + |a_1H| + |a_2H| \cdots |a_nH|$

$|G| = n|H|$

$\Rightarrow \frac{|G|}{|H|} = n$

Def: The number of # LC in G is called the index of H in $G \Rightarrow [G:H]$.

Counting Formula

$|G| = [G:H]|H| \quad H \leq G$

Lagrange's Theorem: $|G| < \infty$, $H \leq G$. Then $|H| \mid |G|$.

Proof: Counting formula

Symmetric groups

* Cycle notation $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \Rightarrow (1\,2)$

Problem 1: p = prime number, $\text{ord}(G) = p$, then G is cyclic.

Soln: $1 \neq p$ (Prime number), G contains an element a which is different from e.

Consider $H = \langle a \rangle$

$H = \{e, a, a^2 \dots\}$

Lagrange: $|H| \mid |G| \Rightarrow |G| = p$ then $|H| = p$

and since $H = \langle a \rangle$

$\therefore$ QED

Problem 2: Let $\phi : G \to G'$ be a group homomorphism

Show $|G| = |\ker \phi| \cdot |\text{Im}\,\phi|$

Soln: Let $N = \ker \phi$, then we know N is a normal subgroup of G.

Let $H' = \text{Im}\,\phi$, then $H' \subseteq G'$.

$|G| = |H'| \cdot |N|$.

Recall: $a, b \in G$, $\phi(a) = \phi(b) \Rightarrow an = b \ \exists n \in N$

$$\left[\begin{array}{l} \phi(a) = \phi(b) \\ \Rightarrow \phi(a^{-1}b) = e_{G'} \\ a^{-1}b = \in N \\ b \in aN \end{array}\right]$$

$\Rightarrow aN = bN$ $\quad \begin{cases} aN = \{an \mid n \in N\} \\ bN = \{bn \mid n \in N\} \end{cases}$

Consider $L = \{aN, N, \ldots\}$ LC of N in G.

$\Rightarrow$ Denoted by G/N (G mod N).

Def: $\int : G/N \to H'$

$aN \to \phi(a)$

$\int$ is a bijection

$\star$ onto: Let $\phi(a) \in H'$ where $a \in G$

Then $\int(aN) = \phi(a) \in H'$

So every element of H' has an image

$\star$ 1-1 $\int(aN) = \int(bN)$

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

$\Rightarrow$ Bijection.

$\therefore |G/N| = |H'|$

$\Rightarrow [G : N] = |H'|$

$$\Rightarrow \frac{|G|}{|N|} = |H'|$$

$$\Rightarrow |G| = |H'| \cdot |N|$$

QED

Summary: $H \subseteq G$ N is normal

then G/N of left cosets of N in G under the operation $(aN)(bN) = (ab)N$

G/N is called the quotient group.

Natural group homomorphism

$$\phi : G \to G/N$$

$\therefore \phi$ is onto & $\ker(\phi) = N$

$\{$ Z is abelian $\Rightarrow$ Normal $\}$

e.g. $G = Z$ $N = 6Z$

$$\therefore G/N = Z/6Z = \{6Z, 1+6Z, 2+6Z, 3+6Z, 4+6Z, 5+6Z\}$$

$$\therefore = \{e, a_1, a_2, a_3, a_4, a_5\}$$

Now $a_1 \cdot a_1 = a_2$

$\vdots$

$(a_1)^6 = e$

$\therefore \langle a_1 \rangle = G/H = \{e, a_1^2, a_1^3, a_1^4, a_1^5\}$

$\therefore o(a_1) = 6$

Natural homomorphism

$\phi : \mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$

$\phi(n) = n + 6\mathbb{Z}$

$= 6p + r + 6\mathbb{Z} \quad \{0 \le r \le 5\}$

$= \boxed{r + 6\mathbb{Z}}$

ϕ is onto clearly

$\ker\phi = \{\phi(n) = e\} = 6\mathbb{Z} \quad \{r = 0\}$

(H)

Theorem: $\forall n, \mathbb{Z}/n\mathbb{Z}$ is a cyclic group of order n.

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

$(aH).(bH) = (ab)H$

$\left\{\begin{array}{l} G \\ H \subseteq G \\ H - \text{normal} \end{array}\right\}$

Is this well defined a group operation?

* Say $aH = a'H$, $bH = b'H$

$\Rightarrow aH.bH = a'H.b'H$

example: $G = S_3$, $H = \{e, c(12)\}$

Ans: Suppose we just define $aH.bH = abH$

★ $(23)H = (132)H$ — ①

$(23)H \cdot (23)H = (23)(23)H = eH = H$

But from ①

$(132)H \cdot (132)H = (132)(132) = (123)H$

But $H \neq (123)H$

∴ We need H needs to be normal. Here no problem because we have shown in the above proposition that the product of aH & bH is $= abH$.

is $a'H$ $b'H$ $a'b'H$

Isomorphism Theorems for groups

First Isomorphism theorem:

Let $\phi: G \to G'$ be a group homomorphism. Then we have a group isomorphism.

$$t: G/\ker\phi \xrightarrow{\sim} \text{im}\,\phi$$

Recall: $\ker\phi$ is a normal subgroup of G.

Proof: Consider the function

$$f: G/N \to H'$$

$\ker\phi = N$

$\text{im}\,\phi = H'$

$f(aN) = \phi(a)$

From previous we know that ϕ is bijective.

We need to show that ϕ is a homomorphism

$\therefore \phi((aN)(bN)) = \phi(aN)\phi(bN)$

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

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

But this is true as ϕ is a homomorphism.

$\therefore \phi$ is an isomorphism.

Hence $G/\ker\phi \cong \text{im}\,\phi$

Example: $\forall n \in \mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ is cyclic.

We will show that any cyclic group $\cong \mathbb{Z}/n\mathbb{Z}$ $\exists n \in \mathbb{Z}$.

Theorem: If G is cyclic then $\exists n \in \mathbb{Z}$ s.t $G \cong \mathbb{Z}/n\mathbb{Z}$. $n = \text{ord}(G)$

Proof: Let a be generator of G

$G = \{a^n \mid n \in \mathbb{Z}\} = \langle a \rangle$

Now let

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

$\phi(n) = a^n$

We have seen earlier that ϕ is a homomorphism.

$\phi(n) = a^n$; $\phi(n+m) = a^{n+m} = a^n \cdot a^m$
$= \phi(n)\phi(m)$

* $\phi : \mathbb{Z} \to G$ (Group homomorphism)
* ϕ is onto as G is generated by a.
* $\ker\phi \subseteq \mathbb{Z}$

Subgroups of $\mathbb{Z}$ are of the form $n\mathbb{Z}$, $\exists n \in \mathbb{Z}$.

$\therefore$ We have a group homomorphism
$\phi : \mathbb{Z} \to G$ s.t

(1) ϕ is onto
(2) $\ker\phi = n\mathbb{Z}$

Then by 1st Isomorphism theorem

$$\mathbb{Z}/\ker\phi \cong \operatorname{im}\phi \quad \{\operatorname{im}\phi = G \text{ as } G \text{ is onto}\}$$

$$\Rightarrow \boxed{\mathbb{Z}/n\mathbb{Z} \cong G}$$

ϕ FD

Example: $G = \{1, i, -i, -1\}$

G is cyclic of order 4.

Then we know $G \cong \mathbb{Z}/4\mathbb{Z}$ by 1st isomorphic theorem.

$\mathbb{Z} \to G$
$a \to i^a$

$\ker\phi = 4\mathbb{Z}$

$$\Rightarrow \boxed{\mathbb{Z}/\ker\phi \cong \operatorname{Im}\phi \cong G}$$

Examples: 1st Isomorphism theorem

★ $|G|=n$, G is cyclic then $G \simeq \mathbb{Z}/n\mathbb{Z}$

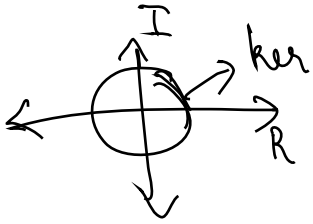
★ $\mathbb{C}^*$: nonzero complex numbers, with $(*)$

$\mathbb{R}^+$: positive real numbers "

Consider the

$$\phi : \mathbb{C}^* \longrightarrow \mathbb{R}^+$$
$$z \longrightarrow |z|$$
$$a+bi \longrightarrow a^2+b^2$$

Ans: $\ker\phi = \{ z \in \mathbb{C}^* : |z|=1 \} = S^1$



$\operatorname{Im}\phi$: If $r \in \mathbb{R}^+$

then $|r|=r$

$\therefore \phi$ is onto

$\therefore$ By (1st IT) $\Rightarrow \mathbb{C}^*/S^1 \simeq \mathbb{R}^+$

↳ left cosets of S^1 in $\mathbb{C}^*$

$$\mathbb{C}^*/S^1 = \{ zS^1 : z \in S^* \}$$

★ $GL_n(\mathbb{R})$

Let $\det : GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^*$

$$A \longrightarrow \det(A)$$

det is onto

$\ker(\det) = \{A \in GL_n(R) \mid \det(A) = 1\}$

$= SL_n(R)$

$\therefore$ (1ST) $\boxed{GL_n(R)/SL_n(R) \cong R^*}$

Remark: $\phi : G \to G'$ is a group homomorphism

Then $G/\ker\phi$ is isomorphic of G'.

$\therefore G/\ker\phi \subseteq G'$

In particular if $\ker\phi = \{e\}$

Then ϕ : 1–1

Then $G \subseteq G'$

Second Isomorphism Theorem (2 IT):

Let G be a group. Let H & N be 2 subgroups.

N is normal in G.

$\{ H \lhd G$ normal $\}$

Then: 1) $H \cap N \lhd H$

2) $HN \lhd G$, $N \lhd HN$

3) $H/H\cap N \cong HN/N$

Proof: 1) Let $h \in H$, $n \in N \cap H$

To show $hnh^{-1} \in H \cap N$

But $H \cap N \subseteq H$ since intersections of subgroups

* Now $hnh^{-1} \in N$

$h \in G$, $n \in N$; $N \triangleleft G$

* $hnh^{-1} \in H$

$h \in H$, $n \in H \cap N \subseteq H$

$\therefore hnh^{-1} \in H \cap N$

2) $HN = \{h \cdot n \mid h \in H, n \in N\} \subseteq G$

* $e \in H$, $e \in N \Rightarrow e \cdot e = e \in HN$

* Let $h_1 n_1, h_2 n_2 \in HN$. To prove $(h_1 n_1)(h_2 n_2) \in HN$

$N \triangleleft G \Rightarrow h_2^{-1} n_1 h_2 \in N$

Then let $n_3 = h_2^{-1} n_1 h_2$

$\Rightarrow n_1 h_2 = h_2 n_3$

Now $h_1 n_1 h_2 n_2 = h_1 h_2 n_3 n_2$

$= (h_1 h_2)(n_3 n_2)$

$= \in H \quad \in N$

$= \in HN$

* Let $hn \in HN$. $(hn)^{-1} = n^{-1} h^{-1} = \bar{n}^{-1} n \in HN$

By above

POV ~~★~~ If $N \lhd G$ then $g \in G$, $gN = Ng$

$\therefore HN \subseteq G$

Now $N = eN \subseteq HN$

$\therefore N \subseteq HN$

N is certainly $\lhd$ in HN, as $N \lhd G$.

$\{ N \subseteq HN \subseteq G \}$

$\therefore N \lhd HN$.

(3) To show $H/H \cap N \cong HN/N$

Consider $\phi : H \longrightarrow HN/N$

$\phi(h) = hN$

$HN/N = \{ aN \mid a \in HN \}$

$H \subseteq HN$

$\therefore hN \in HN/H$ if $h \in H$ }

Claim: ϕ is onto

$\ker \phi = H \cap N$

Proof: Let $aN \in HN/N$, $\therefore a \in HN$

Write $a = hn$, $h \in H$, $n \in N$

$\therefore aN = hnN = h(nN) = hN = \phi(h)$

$\therefore \phi$ is onto

Now $\ker \phi = \{ h \in H \mid \phi(h) = eN \}$

$= \{ h \in H \mid hN = N \}$

$$hN = N \iff h \in N$$

$$\therefore \quad = \{h \in H \mid h \in N\}$$

$$= \{h \in H \cap N\} = H \cap N$$

$\therefore$ By IST

$$\phi : H \to HN/N$$

$$H/\ker\phi \cong HN/N$$

$$\Rightarrow \boxed{H/H\cap N \cong HN/N}$$

$\square$ E.D

Third Isomorphism Theorem

Let G be a group. Let $H \lhd G$, $N \lhd G$ s.t $N \subseteq H \subseteq G$. Then

(1) $H/N \lhd G/N$.

(2) $G/H \cong \dfrac{G/N}{H/N}$

Proof:- i) $H \subseteq G$

We have a natural homomorphism $G \to G/N$

$$H \to G \to G/N$$

$$h \to h \to hN$$

$$\left\{ \begin{array}{l} G \to G/N \\ g \to gN \\ \text{gp homo} \end{array} \right\}$$

Consider the composition

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

$$h \to hN$$

$$\ker(\phi) = \{ h \in H \mid hN = N \}$$

$$= \{ h \in H \mid h \in N \} = H \cap N = N$$

$\therefore$ By LST $H/N \cong$ to a subgroup of G/N

We think of H/N as a subgroup of G/N

★ $H/N \subseteq G/N$

Let $gN \in G/N$; $hN \in H/N$, $g \in G, h \in H$

$$(gN)(hN)(gN)^{-1} = (gN)(hN)(g^{-1}N)$$

$$= gNhNg^{-1}N$$

$$= gNhg^{-1}NN$$

$$= gNhg^{-1}N$$

$$= ghNg^{-1}N$$

$$= ghg^{-1}NN$$

$$= ghg^{-1}N$$

[Note: $N \lhd G$ then $gN = Ng \; \forall g \in G$]

$\therefore$ Since $H \triangleleft G$, $ghg^{-1} \in H$, $g \in G$

$\therefore gHg^{-1}N \in H/N$

$\therefore \boxed{H/N \triangleleft G/N}$

2) T.S $G/H \cong (G/N)/(H/N)$

Consider: $\phi : G/N \longrightarrow G/H$

$\phi(gN) = gH$

ϕ is well defined to be a group homomorphism.

Why? Ans: If $gN = g'N$, $g, g' \in G$

$\Rightarrow g^{-1}g' \in N \Rightarrow g^{-1}g' \in H$

as $N \subseteq H$.

$\Rightarrow \boxed{gH = g'H}$

Well defined.

ϕ: is a group homomorphism

$\phi((gN)(g'N)) = \phi(gg'N)$

$= gg'H$

$= gH\,g'H$

$= \phi(gN)\,\phi(g'N)$

ϕ onto: And ϕ is onto.

Let $gH \in G/H$

$\phi(gN) = gH$ ∴ Onto

$\ker\phi = \{gN \in G/N \mid \phi(gN) = H\}$

$= \{gN \in G/N \mid gH = H\}$

$= \{gN \in G/N \mid g \in H\}$

$= H/N$ $\left\{ H/N = \{hN \mid h \in H\} \right\}$

∴ $\phi : G/N \to G/H$

∴ By 1st

$$\frac{(G/N)}{(H/N)} \cong G/H$$

Cauchy Theorem

Let G be a finite abelian group. Suppose that a prime number p divides the order of G. Then G has an element of order p.

Proof: Recall $\text{ord}(a) = \min\{a^t = e \mid t \in \mathbb{Z}\}$

2 cases:

I) G doesn't contain a subgroup H s.t

$$1 < |H| < |G|$$

Choose an element $a \in G$ s.t $a \neq e$.

Consider the subgroup $\langle a \rangle$ generated by a.

By hypothesis, $\langle a \rangle = G$ { as $H \leq G$ not trivial }

$\therefore$ G is cyclic.

Note: $|G| = \text{ord}(a)$

We know that $p \mid |G| = p \mid \text{ord}(a)$

Exercise: If G is cyclic, $|G| = n$ & $m \mid n$, then G contains an element of order m.

Proof: G is cyclic $= |\langle a \rangle| = n$

$m \mid n = n = mr \{ r \in \mathbb{Z} \}$

$G = \{e, a^1, a^2 \ldots a^{n-1}\}$

now $b \in G$ s.t $b = a^k$ $n > k \geq 1$

$$|G| = |a^n| = \frac{n}{m} = r$$

Hence $\square$ E.D { Proof concrete ends }

$\therefore$ By the exercise, G contains an element of order p.

Case 2: There is a subgroup H of G which is non trivial (i.e. $H \neq \{e\}$) and proper ($H \leq G$)

$1 < |H| < |G|$

Using induction on $|G|$.

Base case: $|G| = 2$

$G = \{e, a\}$

$\text{ord}(a) = 2 \{ a^2 = e \}$

Inductive hypothesis

$|H| < |G|$. a) Suppose that p divides $|H|$.

Then by induction $\{ G \Leftrightarrow H \text{ is abelian} \}$

H contains an element of order p. Then

so does G

i.e. $a \in H$, $\text{ord}(a) = p \Rightarrow a \in G$, $\text{ord}(a) = p$

b) Suppose that p does not divide $|H|$.

Counting Formulae: $|G| = [G:H]\,|H|$

Since G is abelian, every $H \triangleleft G$, $\therefore$

G/H is a group & $|G/H| = [G:H]$

$\therefore |G| = |H|\,|G/H| \Rightarrow p$ divides $|G/H|$

$\{$ since p divides $|G|$ & not $|H|$ by hypothesis $\}$

$|G/H| = \frac{|G|}{|H|} < |G| \quad \{\because |H| > 1\}$

$\therefore$ Induction hypothesis applies to G/H.

G is abelian $\Rightarrow$ G/H is abelian.

$\therefore$ So by the induction hypothesis, G/H contains an element of order p. Say $gH \in G/H$ has order p.

$\therefore (gH)^p = H$ and $gH \neq H$.

$\Rightarrow g^p H = H$ and $gH \neq H$

$\Rightarrow g^p \in H$ & $g \notin H$

Let $m = |H|$

Then Lagrange's theorem applied to H & g^p.

$\text{ord}(g^p)$ divides $|H| = m$.

$\Rightarrow (g^p)^m = e$

$\Rightarrow g^{pm} = e \Rightarrow (g^m)^p = e$

[If $a \in G$ $\text{ord}(g) = a$ then $g^{an} = e$ $\forall n$]

Then can we say $\text{ord}(g^m) = p$?

$\text{ord}(g^m) = \min \{(g^m)^d = e \mid d \in \mathbb{Z}\}$

Since $(g^m)^p = e$, we can say that $\text{ord}(g^m)$ divides p.

[Recall: If $\text{ord}(G) = a$, & $g^n = e$ then a divides n]

But since p is prime $\Rightarrow$ ord $(g^m) = 1$
ord $(g^m) = p$

$\hookrightarrow$ $g^m = e$ [not possible]

as : $g^m = e \Rightarrow (gH)^m = g^m H$
$= eH$
$= H$

Recall [ord $(gH) = p$] $\rightarrow$
Not possible as then
p divides m
$\Rightarrow p$ divides $|H|$

$\therefore$ ord $(g^m) = p$, g^m is the element we are looking for.

$\boxed{\theta = 0}$

Example: * Consider

$$G = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \right\}$$

$|G| = 4$, G is a subgroup of $GL_2(\mathbb{R})$.

Obviously G is abelian as $G = \{e, a_1, a_2, a_3\}$
$\Rightarrow a_1^2 = e = a_2^2 = a_3^2$

Now G has 1 element of order 1
G has 3 elements of order 2
G is called the "klein-4-group". Is it cyclic?

Ans: No it is not cyclic, it has no element of order 4.

The converse of lagrange's theorem fails here;
4 divides |G| but G has no element of order 4.

Similarly, this shows that p must be prime in Cauchy's theorem.

If G is cyclic of order 4 then
$G = \{1, a, a^2, a^3\}$
then G has an element of order 2, namely a^2.

Problem: Let G be a cyclic group, $H \subseteq G$. Then (G/H) is cyclic.

Proof: G is cyclic $\Rightarrow$ G abelian $\Rightarrow$ H is normal in G
$\therefore$ G/H is a group.

Since $G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$

$\therefore G/H = \{gH \mid g \in G\}$

We claim aH generates G/H write $g = a^n$ $\exists n$

$gH = a^n H = (aH)^n$

$\therefore G/H = \{(aH)^n \mid n \in \mathbb{Z}\}$

QED

Problem 2: G is abelian, $H \subseteq G$ is a subgroup. Show that G/H is abelian.

Proof: Let $aH, bH \in G/H$.

$(aH)\cdot(bH) = ab(H)$

$= ba(H)$ { G is abelian }

$= (bH)(aH)$

QED

Problem 3: Let $Z(G)$ be the centre of G. If $G/Z(G)$ is cyclic, show that G is abelian.

Soln: $Z(G) = \{a \in G \mid ga = ag \ \forall g \in G\}$

Let $a, b \in G$. We show that $ab = ba$

Since $G/Z(G)$ is cyclic, then let

$$G/Z(G) = \langle gZ(G) \rangle$$

We have $aZ(G), bZ(G) \in G/Z(G)$

$\therefore$ do $aZ(G) = (gZ(G))^i$

$bZ(G) = (gZ(G))^j$

for some integers i, j

$\Rightarrow aZ(G) = g^i Z(G)$

$bZ(G) = g^j Z(G)$

$\Rightarrow a = g^i x'$

where $x, x' \in Z(G)$

$\Rightarrow a = g^i x' \cdot x^{-1} = g^i x$ for some $x \in Z(G)$

$b = g^j y$ for $y \in Z(G)$

$$ab = (g^i x)(g^j y)$$
$$= (g^i g^j xy)$$
$$= g^{i+j} xy$$

$$ba = (g^j y)(g^i x) = g^j g^i yx = g^{j+i} yx = g^{i+j} xy$$

$\{xy = yx \in Z(G)$ in the centre as commutes$\}$

Problem: Let G be a cyclic group. $|G| < \infty$. Suppose $m \in \mathbb{Z}^+$ that divides $|G|$. Then show that g contains an element of order m.

Proof: Suppose $G = \langle a \rangle$

$|G| = n$

If $m \mid n$ then consider $a^{n/m}$.

$b^m = \left(a^{n/m}\right)^m = a^n = e$

Can we say $\text{ord}(b) = m$?

$\Rightarrow$ Not yet - solution

$\Rightarrow$ Why d.

$\text{ord}(b) = \min\{b^d = e \mid d \in \mathbb{Z}^+\}$

Suppose that $\exists\, d < m$, we have $b^d = e$

$b^d = e \Rightarrow \left(a^{n/m}\right)^d = e \Rightarrow a^{\frac{nd}{m}} = e$

$\therefore d < m$

$\frac{nd}{m} < n$

This contradicts the fact that n is the least order for a to be a

generator. $\{n$ is the smallest$\}$

$\therefore d \geq m$

QED $\Rightarrow \text{ord}(G) =$

Remark: Let $G \cong$ Klein 4-group $|G| = 4$

$G = S_3$ $|G| = 6$

Both are not cyclic

$\therefore$ It is crucial to assume G is cyclic.

Final Chapter Ahead

Symmetric groups:

Let $n \in \mathbb{Z}^+$, S_n – Symmetric group on n letters

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

★ $|S_3| = 6$, $S_3 = \{f_1, f_2, f_3, f_4, f_5, f_6\}$

$= \{e, (12), (23), (13), (123), (132)\}$

★ $S_1 = \{e\}$; There exists only one bijection $\{1\} \to \{1\}$

★ $S_2 = \{1, 2\} \to \{1, 2\}$

$\{$ e: identity $1 \to 1$, $2 \to 2$; (12): another $1 \to 2$, $2 \to 1$ $\}$

Q: Order of S_n?

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

$\therefore |S_n| = n!$

Cycle Notation

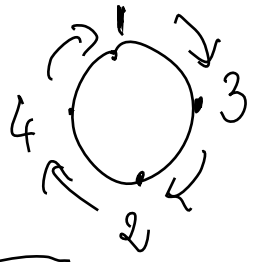
Example: Let $\sigma \in S_9$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 2 & 1 & 6 & 5 & 8 & 7 & 9 \end{pmatrix}$$

Rewriting rules

* Start with 1. See where it goes under σ.
* Put it next to 1
* repeat until we come to 1 again.

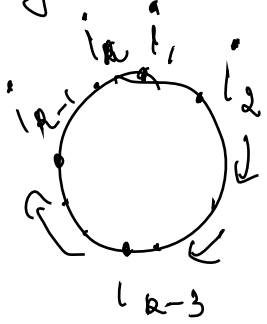
Eg: (1324)



* If identity, leave

$$\boxed{\sigma = (1324)(56)(78)}$$

Cycle decomposition of σ.



$$(i_1, i_2 \ldots i_k) = (i_2, i_3 \ldots i_k, i_1)$$

if $j \notin \{i_1 \ldots i_k\} \subseteq \{1 \ldots n\}$

Then $j \to j$

Example: Consider $(123) \subseteq S_6$

$1 \to 2$ $\quad 4 \to 4$

$2 \to 3$ $\quad 5 \to 5$

$3 \to 1$ $\quad 6 \to 6$

} fixed these $j \to j$

σ = disjoint cycles.

Proposition: Every $\sigma \in S_n$ has a decomposition as a product of disjoint cycles.

Ex: S_5 : $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$

$\therefore$ cycle notation = $(1\,2\,3\,4\,5)$

Property: If σ & τ are disjoint cycles then

$$\sigma\tau = \tau\sigma$$

Recall: S_n $n \geq 3$ not abelian

Ex: $(12)(123) = (1)(23) = (23)$ ~~#~~
$\sigma \quad \tau$

$(123)(12) = (13)(2) = (13)$
$\tau \quad \sigma$ Different.

Proof: However if σ & τ are disjoint cycles then

$\sigma\tau = \tau\sigma$.

Why: When we consider $\sigma\tau$, we look at indices in τ first. as they aren't present in σ it does not matter whether we consider it 1st or 2nd σ.

$(12)(34) = (34)(12)$

$\tau \qquad \tau \quad \sigma$

QED

Ex: $\sigma \in S_9$

$\sigma = (1324)(56)(78)$
$= (56)(1324)(78)$
$= (78)(56)(1324)$
$= (78)(1324)(56)$

} disjoint.

Let σ be a k-cycle in S_n

Let $\sigma = (i_1 i_2 \dots i_k)$

Property: The order of a k-cycle is k.

Pf: $\text{ord}(\sigma) = \min\{\sigma^d = e \mid d \in \mathbb{Z}^+\}$

$\sigma = (i_1 i_2 \dots i_k)$

$\begin{cases} i_1 \to i_2 \\ i_2 \to i_3 \\ \\ i_{k-1} \to i_k \end{cases}$

$\sigma^2 = \sigma \circ \sigma = i_1 \xrightarrow{\sigma} i_2 \xrightarrow{\sigma} i_3$

$(i_1 i_3 i_5 i_7 \dots i_{k-1}) \; i_3 \xrightarrow{\sigma} i_4 \xrightarrow{\sigma} i_5$

always / sometimes

$\therefore \sigma^2$ is not in k-cycle. { not in general true }

Why?: Ex: $\sigma = (1257) \in S_7$

$\sigma^2 = (1257)(1257) = (15)(27)$

σ - 4 cycle, σ^2 = 2 x 2 cycle

$\therefore$ $\sigma : i_1 \to i_2$ Since all are distinct from i_1 ie $i_2 \neq i_3 \neq \cdots$ $i_k \neq i_1$

$\sigma^2 : i_1 \to i_3$

$\sigma^{k-1} : i_1 \to i_k$ They are all k cycles

$k \mid 6 = e$

$\therefore$ So $\text{ord}(\sigma) = k$ ie $\sigma^k : i_1 \to i_1$

$\sigma^k(i_2) = i_2 \to i_2$

$\therefore$ $\sigma^k(i_k) = i_k$

$\sigma^k = e$

This proves the proposition

$\therefore$ So $\text{ord}((1235)) = 4$

Why? $(1235)^2 = (13)(25)$

$(1235)^3 = (1532)$

$(1235)^4 = (1235)$ $\to$ QED

What about the order of disjoint cycles?

Proposition: If $\sigma \in S_n$ has cycle decomposition

$$\sigma = \sigma_1 \sigma_2 \cdots \sigma_k$$

$\sigma_i = m_i$-a cycle.

Proof: Then $\text{ord}(\sigma) = \text{lcm}(m_i \mid i \in \{1 \ldots k\})$

But we know from before $\text{ord}(\sigma_i) = m_i$

Let $M = \text{lcm}\{m_1 \ldots m_k\}$

$$\sigma^M = (\sigma_1 \cdots \sigma_k)^M = \underbrace{(\sigma_1 \cdots \sigma_k)(\sigma_1 \cdots \sigma_k) \cdots (\sigma_1 \cdots \sigma_k)}_{M \text{ times}}$$

We know $\sigma_i \sigma_k = \sigma_k \sigma_i$ disjoint cycles

$$= \sigma_1^M \sigma_2^M \cdots \sigma_k^M$$

$\text{ord}(\sigma_1) = m_1$

and $m_1 \mid M$

$\therefore \sigma_1^M = e$

$\therefore = e \cdot e \cdots e$

$\sigma^M = e$

Now next to prove $\text{ord}(\sigma) = M$ is nothing smaller than M yields e.

Suppose $\sigma^N = e \ \exists N$

$$e = \sigma^N = \sigma_1^N \sigma_2^N \cdots \sigma_k^N$$

Suppose i is an index appearing in σ_1. Then it does not appear in $\sigma_2^N, \sigma_3^N \cdots \sigma_k^N$.
Hence $i \in \sigma_1^N$

$\therefore e$ fixes i

$\Rightarrow \sigma^N$ fixes i

$\Rightarrow \sigma_1^N \sigma_2^N \cdots \sigma_k^N$ fixes i

$\Rightarrow \sigma_1^N$ fixes i

Similarly σ_1^N fixes every index appearing in σ_1.

Hence $\sigma_1^N = e$

But $\text{ord}(\sigma_1) = m_1, \ \sigma_1^N = e \Rightarrow m_1 \mid N$

Ily $\text{ord}(\sigma_2) = m_2, \ \sigma_2^N = e \Rightarrow m_2 \mid N$

$\vdots$

$\text{ord}(\sigma_k) = m_k, \ \sigma_k^N = e \Rightarrow m_k \mid N$.

Since each $m_i \mid N \ \forall i \in \{1 \cdots k\}$ we have M divides N.

$M \leq N$. Since M is lcm

$\sigma^m = e$ and if $\sigma^N = e$ $\exists N$

then $m \leq N$.

$\Rightarrow \text{ord}(\sigma) = m$

QED

Example: $\sigma = (1324)(56)(78)$

$= \text{ord}(4)\ \text{ord}(2)\ \text{ord}(2)$

$= \text{LCM}(4,2,2) = 4$.

$\therefore \text{ord}(\sigma) = 4$

$\sigma = (2)(123) = (1)(23) = (23)$

$\therefore \sigma$ is a 2cycle; it is a product of a 2cycle & 3cycle.

But $\text{ord}(\sigma) = 2$ [2cycle]

But LCM of $(2,3) = 6$ [not applicable]

→ as $(12)(123)$ are not disjoint cycles.

Def A 2cycle is called a transposition.

$(i\ j) \Rightarrow i \to j$

$j \to i$

fixes everything else.

A transposition has order (2)

Prop: Every permutation can be written as a product of transpositions, not necessarily disjoint transpositions.

Example: $\sigma = (132) \in S_5$

★ Not possible as a product of disjoint transpositions

Reason: If $\sigma = \sigma_1 \sigma_2 \cdots \sigma_k$ where $X_{\sigma_i} \cap X_{\sigma_j} = \emptyset$

Then $\text{ord}(\sigma) = \text{LCM}(\text{ord}(\sigma_1) \cdots \text{ord}(\sigma_k))$

$= \text{LCM}(2 \cdots 2)$

$= \boxed{2}$

But $\sigma = 3$ cycle $\neq 2$

$\therefore (132) = (12)(13)$

$1 \to 3$ $\quad 1 \to 3 \to 3$

$3 \to 2$ $\quad 2 \to 2 \to 1$

$2 \to 1$ $\quad 3 \to 1 \to 2$

Proof: It suffices to show that a cycle σ can be written as a product of transpositions.

This is because given any permutation σ we can write $\sigma = \sigma_1 \cdots \sigma_k$ where $\sigma_1 \cdots \sigma_k$ are disjoint cycles

We can say σ is a k-cycle

Say $\sigma = (i_1 i_2 \dots i_k)$

$\sigma = (i_1 i_2)(i_2 i_3) \dots (i_{k-1} i_k)$

For the RHS. $i_1 \to i_2$ [always start from Rightmost]

$i_2 \to i_3$

$\vdots$

$i_{k-1} \to i_k$

$i_k \to i_1$ [go backwards]

$\therefore \sigma = (i_1 i_2)(i_2 i_3) \dots (i_{k-1} i_k)$

product of transpositions.

QED

Recall: i) $(12)(13)(14) = (23)(25)(12)(45)(15)$

3 transpositions 5 transpositions

ii) $(132) = \underbrace{(12)(13)}_{2} = \underbrace{(13)(32)}_{2}$

Theorem: Let $\rho \in S_n$ be a permutation.

Suppose that $\rho = \sigma_1 \cdots \sigma_k$ & $\rho = \tau_1 \cdots \tau_t$ where

$\sigma_1 \cdots \sigma_k$ } Transpositions
$\tau_1 \cdots \tau_t$ }

Then k and t are both even or both odd.

Let us introduce a polynomial

$$\begin{aligned} \int(x_1, x_2 \ldots x_n) &= (x_1 - x_2)(x_1 - x_3) \cdots (x_1 - x_n) \\ &= (x_2 - x_3) \cdots (x_2 - x_n) \\ &= \cdots \\ &= (x_{n-1} - x_n) \\ &= \prod_{1 \le i < j \le n} (x_i - x_j) \qquad \begin{matrix} 1 \le i \le n-1 \\ 2 \le j \le n \end{matrix} \end{aligned}$$

Example: $\int(x_1, x_2) = (x_1 - x_2)$

$\int(x_1 \ldots x_3) = \underbrace{(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)}$

$\int(x_1 \ldots x_4) = \int(x_1 \ldots x_3) \cdot (x_1 - x_4)(x_2 - x_4)(x_3 - x_4)$

Take an element $\sigma \in S_n$

Define $\sigma^* \int$ as follows

$$\sigma^* \int = \prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)})$$

Example: $n=2$

Then $\int(x_1, x_2) = x_1 - x_2$

$S_2 = \{e, (12)\}$ what is $\sigma^* \int$?

$$e^* \int = x_{e(1)} - x_{e(2)} = x_1 - x_2$$

$$(12)^* \int = x_{12(1)} - x_{12(2)} = x_2 - x_1$$ } same

$\sigma = (12)$

$\{$ image of i under i $\sigma(i)\}$

$$\sigma^* \int = x_{\sigma(1)} - x_{\sigma(2)} = x_2 - x_1 = -\int$$

* $n=3$

$$\int = (x_1 - x_2)(x_2 - x_3)(x_1 - x_3)$$

$S_3 = \{e, (12), (13), (23), (123), (132)\}$

$\sigma = (13)$ $\quad \sigma^* \int = (x_{\sigma(1)} - x_{\sigma(2)})(x_{\sigma(2)} - x_{\sigma(3)})(x_{\sigma(1)} - x_{\sigma(3)})$

$$= (x_3 - x_2)(x_2 - x_1)(x_3 - x_1)$$

$$= -\int$$

$\tau = (123)$

$$\tau^* \int = (x_{\tau(1)} - x_{\tau(2)})(x_{\tau(2)} - x_{\tau(3)})(x_{\tau(1)} - x_{\tau(3)})$$

$$= (x_2 - x_3)(x_3 - x_1)(x_2 - x_1)$$

$= \Delta$

$\therefore$ If $\sigma \in S_n$ then $\sigma^* \Delta$ is either Δ or $-\Delta$.

Why: $\Delta = \prod_{1 \le i < j \le n} (x_i - x_j)$

$\sigma^* \Delta = \prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)})$ $\left\{ \begin{array}{l} \sigma \text{ is a bijection} \\ \text{of } \{1 \dots n\} \end{array} \right.$

Q: If $\sigma, \tau \in S_n$, what is $(\sigma\tau)^* \Delta$?

How is this related to $\sigma^* \Delta$ and $\tau^* \Delta$?

Example: take $n=3$, $\sigma = (13)$, $\tau = (123)$

$\sigma\tau = (12)$

$$\begin{aligned} (\sigma\tau)^* \Delta &= (x_{\sigma\tau(1)} - x_{\sigma\tau(2)}) \\ &\quad (x_{\sigma\tau(2)} - x_{\sigma\tau(3)}) \\ &\quad (x_{\sigma\tau(1)} - x_{\sigma\tau(3)}) \\ &= (x_2 - x_1)(x_1 - x_3)(x_2 - x_3) \end{aligned}$$

$= -\Delta$

We have $(\sigma\tau)^* \Delta = \sigma^*(\tau^* \Delta)$

This holds in general. Why?

Why: $(\sigma\tau)^*\Delta = \prod_{1\le i<j\le n} (x_{\sigma\tau(i)} - x_{\sigma\tau(j)})$

$$= \prod_{1\le i<j\le n} (x_{\sigma(\tau(i))} - x_{\sigma(\tau(j))})$$

$$= \sigma^* \prod_{1\le i<j\le n} (x_{\tau(i)} - x_{\tau(j)})$$

$$= \sigma^*(\tau^*\Delta)$$

If we have a transposition then $\sigma^*\Delta = -\Delta$.

Proof: As a special case consider $\sigma = (12)$

$$\sigma^*\Delta = \prod_{1\le i<j\le n} (x_{\sigma(i)} - x_{\sigma(j)})$$

$$= (x_2 - x_1)(x_2 - x_3) \cdots (x_2 - x_n)$$
$$(x_1 - x_3) \cdots (x_1 - x_n)$$
$$\vdots \quad \ddots \quad \vdots$$

no change $\left\{ \right.$ as (12)

$\therefore$ Now notice only one change is $(x_2 - x_1)$

$$\therefore \boxed{\sigma^*\Delta = -\Delta}$$

Let $\sigma = (i\ j)$ with $i < j$

Let us check what is $\sigma^* f$.

Consider a term $x_u - x_v$, $u < v$.

To find $\sigma^* f$ we have to determine how many terms of the form $x_u - x_v$ change sign under σ.

Question: When does $x_u - x_v$ change to $x_a - x_b$ with $b < a$?

Proof: If $u \notin \{i, j\}$ & $v \notin \{i, j\}$, $x_u - x_v$ does not change under σ.

$$\sigma^*(x_u - x_v) = x_{\sigma(u)} - x_{\sigma(v)}$$

$u < v \Rightarrow \sigma(u) > \sigma(v)$ — This is what we want.

Remaining cases

Case 1: $u = i$, $v = j$ $\quad \sigma^*(x_u - x_v) = x_{\sigma(u)} - x_{\sigma(v)}$
$= (x_v - x_u)$
{Sign change}

Case 2: $u = i$, $v \neq j$

2.1) $u = i < v < j$; $\quad \sigma^*(x_u - x_v) = x_{\sigma(u)} - x_{\sigma(v)}$
$= x_j - x_v$
{No sign change}

2.2) $u = i < j < v$: $\quad \sigma^*(x_u - x_v) = x_{\sigma(u)} - x_{\sigma(v)}$
$= x_j - x_v$
{Sign change}

Case 3: $u=i$, $v=j$

3.1) $u<i<j=v$: $\sigma^*(x_u - x_v) = x_u - x_i$ { No sign change }

3.2) $i<u<j=v$: $\sigma^*(x_u - x_v) = x_u - x_i$ { sign change }

∴ The number of times sign changes

∴ → 1 ⇒ for $u=i$, $v=j$

→ → $u=i$ & v is directly between i & j

$$\underbrace{1,2\ldots i}_{u},\ \underbrace{i+1 \ldots\ldots j-1, j}_{v}$$

∴ $j-1-i$ choices

→ when $v=j$ & u is between i & j

$$1,2\ldots i,\ \underbrace{i+1\ldots j-1}_{u},\ j=v$$

∴ for $v=j$ there are $j-1-i$ choices for u.

∴ Finally the sign changes

$$1+(j-i+1)+(j-i+1) = \underbrace{1+2(j-i-1)}_{\text{odd number}}$$

∴ $\boxed{\sigma^* f = -f}$

QED

So now we have proved

① $(\sigma\tau)^* f = \sigma^*(\tau^* f)$ $\quad \sigma, \tau \in S_n$

② $\sigma^* f = -f$ if σ is a transposition

Now lets prove the original theorem

$$\rho = \sigma_1 \sigma_2 \cdots \sigma_k = \tau_1 \cdots \tau_k$$

we want to show k & t have the same parity.

Proof Let us look at $\rho^* f$.

$$\rho^* f = (\sigma_1 \cdots \sigma_k)^* f = (\sigma_1 \cdots \sigma_{k-1})^* (\sigma_k^* f) \quad \text{by ①}$$

$$= (\sigma_1^* \cdots \sigma_{k-1}^*)(-f) \quad [\text{by ②}]$$

$$= (-)^k f$$

$$\rho^* f = (\tau_1 \cdots \tau_t)^* f = (-1)^t f$$

But $\rho^* f = f$ or $\rho^* f = -f$

So $\cdots (-1)^k f = (-1)^t f$

$$\Rightarrow (-1)^k = (-1)^t = 1 \quad \left[\begin{array}{l} k=t \iff k+t \,\%\, 2 == 0 \\ k=t \iff k+t \,\%\, 2 == 1 \end{array}\right]$$

$$= -1$$

$\therefore k = t$

QED

Definition: Let $\sigma \in S_n$

We say σ is an even permutation if the number of transposition required to express σ as a product is even.

Example: Consider $(12)(32) \in S_n$

σ is even because

More generally: a k-cycle is even if k is odd

a k-cycle is odd if k is even

Why is this? $(i_1 \dots i_k) = \underbrace{(i_1 i_2) \cdots (i_{k-1} i_k)}_{k-1 \text{ transpositions}}$

$k \to \text{odd} \Rightarrow k-1 \Rightarrow \sigma$ is even

$k \to \text{even} \Rightarrow k-1 \Rightarrow \sigma$ is odd

Def: "Sign of a permutation"

$$\text{Sign}(\sigma) = \begin{cases} 1 & \sigma \text{ is even} \\ -1 & \sigma \text{ is odd} \end{cases}$$

Proposition: * Product of 2 even permutations is even (1)

* inverse of an even permutation is even (2)

Why: 1) σ_1, σ_2 are even $\Rightarrow$ $\sigma_1 = \tau_1 \cdots \tau_k$ k even

$\sigma_2 = \rho_1 \cdots \rho_t$ t even

$\sigma_1\sigma_2 = \tau_1\tau_2 \cdots \tau_k\rho_1 \cdots \rho_t$

$\therefore$ $k+t \Rightarrow$ even $\Rightarrow$ $\sigma_1\sigma_2$ is even

② σ is even, $\sigma = \sigma_1 \cdots \sigma_k$ k even

Then $\sigma^{-1} = \sigma_k^{-1} \cdots \sigma_1^{-1}$

{ Recall in any G $(ab)^{-1} = b^{-1}a^{-1}$

$\therefore$ σ^{-1} is even.

Let us define $A_n = \{ \sigma \in S_n \mid \sigma \text{ is even} \}$

By the proposition, A_n is a subgroup of S_n

* e is even. (0 transpositions)

A_n is called the alternating group.

Consider the group homomorphism: $\phi : S_n \to \{-1, 1\}$ $\phi(\sigma) = \operatorname{sgn}(\sigma)$

($\{-1, 1\}$ is a group under multiplication)

Check: $\phi(\sigma_1\sigma_2) = \operatorname{sgn}(\sigma_1\sigma_2)$

$= \operatorname{sgn}(\sigma_1)\operatorname{sgn}(\sigma_2)$

$= \phi(\sigma_1)\phi(\sigma_2)$

$\therefore$ ϕ is a group homomorphism

Assume $n \geq 2$

ϕ is onto : S_n contains even & odd permutations

$\ker \phi = A_n$ $\{e = \text{even}\}$

$\therefore$ By First Isomorphism Theorem

$$S_n / A_n \cong \{1, -1\}$$

$\therefore$ By counting formulas

$$|S_n / A_n| = 2$$

$$\therefore |S_n| = |A_n| 2$$

$$\Rightarrow |A_n| = \frac{|S_n|}{2} = \boxed{\frac{n!}{2}}$$

question : Do odd permutations also form a group??

Ans : No a e is not odd

Also (12) & (34) odd, but (12)(34) is even.

Group Actions Let G be a group. Let S be a set

We want to understand the meaning of "G acting on S"

We say "G acts on S" if there is a function

$$G \times S \longrightarrow S$$
$$(g, s) \longrightarrow gs \,/\, g \cdot s \,/\, g * s$$

Recall : $G \times S = \{(g, s) \mid g \in G, s \in S\}$

This function takes an element of G & an element of S and gives out $g * s$.

So this function acts like an action of G on S. This function has the following property:

① $e \cdot s = s \quad \forall s \in S$

② $(gg') \cdot s = g(g' \cdot s) \quad \forall g, g' \in G, s \in S$

Example: ① Consider an equilateral triangle

$S = \{A, B, C\}$

G = group of rotational symmetries of ΔABC

$\{e, r_1, r_2\}$ $\left\{ \begin{array}{l} r_1 : 120^\circ \text{ rotation} \\ r_2 : 240 \text{ rotation} \end{array} \right\}$

G acts on S Why?

Proof: $e \cdot A = A$, $e \cdot B = B$, $e \cdot C = C$ | $r_1 \cdot A = B$, $r_1 \cdot B = C$, $r_1 \cdot C = A$ | $r_2 \cdot A = C$, $r_2 B = A$, $r_2 C = B$

We get a $f: G \times S \to S$

Satisfying the properties

$(r_1 r_2) A$ $\left\{ \begin{array}{l} eA = A \\ r_1(r_2 A) = r_1 C = A \end{array} \right\}$

All satisfied

② $G = S_n$ acts on $\{1, 2, \ldots, n\}$

$\sigma \in S_n$, $i \in S$

$\sigma \cdot i = \sigma(i)$

Example: $G = S_4$ acts on $S = \{1, 2, 3, 4\}$

$\sigma = (1432) \in S_4$

$\sigma(1) = 4$

$\sigma \cdot 1 = 4$, $\sigma \cdot 2 = 1$, $\sigma \cdot 3 = 2$, $\sigma \cdot 4 = 3$

✓ $e \cdot i = i \quad \forall i \in S$ } S_n acts on Ω.

$[\sigma_1 \sigma_2) i = \sigma_1(\sigma_2(i))$ }

③ $G = GL_n(\mathbb{R})$ $S = \mathbb{R}^n \left\{ \begin{bmatrix} a_1 \\ a_n \end{bmatrix} \in \mathbb{R}^n, a_i \in \mathbb{R} \right\}$

$GL_n(\mathbb{R})$ acts on $\mathbb{R}^n$

Let $A \in GL_n(\mathbb{R})$, $v = \begin{bmatrix} a_1 \\ a_n \end{bmatrix} \in \mathbb{R}^n$

$A \cdot v = A \cdot \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}$ = product of matrices

$Av \in \mathbb{R}^n$

$\therefore I \cdot v = v$ }

$(AB)v = A(Bv)$ } $\Rightarrow GL_n(\mathbb{R})$ acts on $\mathbb{R}^n$

④ Let G be any group let $S = G$

Define the action as follows

$g \in G, s \in G$

define $g \cdot s = gs$

$\therefore G \times G \to G$

$(g, s) \to gs$

Is this a group action?

Ans $e \cdot s = es = s \in G$

$(g_1 g_2)s = g_1(g_2 s) \in G$ $\Big\}$ $\Rightarrow$ This is a group action.

$\Rightarrow$ Left multiplication on G

⑤ Another example $= G = S$

$g \in G, s \in G$

$g * s = gsg^{-1}$ = "conjugate of s by g"

Is this an action:

$e * s = ese^{-1} = se^{-1} = s$

$(g_1 g_2) * s = (g_1 g_2) s (g_1 g_2)^{-1} = (g_1 g_2) s (g_2^{-1} g_1^{-1})$

$= g_1 (g_2 s g_2^{-1}) g_1^{-1}$

$= g_1 (g_2 * s) g_1^{-1}$

$= g_1 * (g_2 * s)$

$\therefore$ This is an action

The action of G on itself is called the conjugation action.

Now: Let G be a group acting on S.

Let $s \in S$. The orbit of s (O_s) is

$$O_s = \{ gs \mid g \in G \}$$

Now $O_s \subseteq S$ [subset of S]

Example: ① $G = \{e, r_1, r_2\}$ $S = \{A, B, C\}$

Orbit of A.

$$O_A = \{A, B, C\} = S = O_B = O_C$$

② $G = S_n$, $S = \{1, \ldots n\}$

$$O_1 = \{1, 2, 3, \ldots n\} = S$$

$$\begin{cases} (12) \cdot 1 = 2 \\ (13)\, 1 = 3 \\ (1i)\, 1 = i \end{cases}$$

$$O_2 = O_3 \ldots O_n = S$$

③ $G = GL_n(\mathbb{R})$, $S = \mathbb{R}^n$

$$0 = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$$

$A \cdot 0 = 0 \quad \therefore O_0 = \{0\}$

Q: If $v \in \mathbb{R}^n, v \neq 0$ then $O_v = \mathbb{R}^n - \{0\}$

Fact: $\exists v, w \in \mathbb{R}^n, v \neq w \neq 0$ $\exists$ $A \in GL_n(\mathbb{R})$ s.t

$$A \cdot v = w$$

Proof: e.g. $O_v = \mathbb{R}^n - \{0\}$

Why: $O_v = \{ A \cdot v \mid A \in GL_n(\mathbb{R}) \}$

$= \{ w \mid w \in \mathbb{R}^n - \{0\} \}$

④ G acts on G by left multiplication

Let $s \in G$.

$O_s = \{ gs \mid g \in S \} \subseteq S = G$

Claim: $O_s = G$

Proof: Take $t \in G$. Can we find a group element $g \in G$ s.t $gs = t$

Yes: $g = ts^{-1}$

$(ts^{-1}) \cdot s = t(s^{-1}s) = t$

$\forall t \in G \in O_s$

$\therefore O_s = G$

⑤ G acts on itself by conjugation

$$g * s = gsg^{-1}$$

$$O_e = \{ g * e \mid g \in G \}$$

$$= \{ geg^{-1} \mid g \in G \} = \{ e \mid g \in G \}$$

$$= \{e\}$$

Suppose G is abelian, $s \in G$

$$O_s = \{ g * s \mid g \in G \}$$

$$= \{ gsg^{-1} \mid g \in G \}$$

$$= \{ sgg^{-1} \mid g \in S \}$$

$$= \{ s \}$$

Let G be a group acting on a set S.

Let $s \in S$, O_s always contains s.

$O_s \neq \emptyset$

$\therefore O_s = \{ gs \mid g \in G \}$ if $g = e$

Then $O_s = \{s\}$

Set-up: G is a group. S is a set. G acts on S. $G \times S \to S$

$(g, s) \to gs$

Define a relation $\sim$ on S as follows:

We say $s_1 \sim s_2$ if $\exists\, g \in G$ s.t. $gs_1 = s_2$

Question: Is $\sim$ an equivalence relation?

i) $s \sim s$? Yes, because $es = s$. (by definition of action)

ii) $s_1 \sim s_2 \Rightarrow s_2 \sim s_1$

$\therefore gs_1 = s_2 \Rightarrow g_1 = g^{-1}s_2$

$\Rightarrow s_1 = g^1 s_2$ where $g^{-1} = g^1$

$\therefore s_2 \sim s_1$

iii) $s_1 \sim s_2$, $s_2 \sim s_3 \Rightarrow s_1 \sim s_3$

$\Rightarrow g_1 s_1 = s_2 \Rightarrow (g_2 g_1) s_1 = s_3$

$g_2 s_2 = s_3 \Rightarrow (g'') s_1 = s_3 \quad (g'' = g_2 g_1)$

$\Rightarrow s_1 \sim s_3$

$\therefore$ It is an equivalence relation. (ER)

Recall that an ER partitions the set S into disjoint equivalence classes. (EC)

Let $s \in S$. What are the EC of s?

And $[s] = \{ t \in S \mid s \sim t \}$

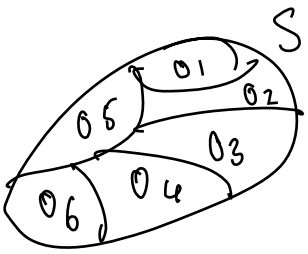
$= \{ t \in S \mid gs = t \ \exists g \in G \}$

$= \{ gs \mid \forall g \in G \}$

So. $\boxed{[s] = O_s}$ (Orbit of s)

Hence we conclude that G action on a set S, then S is partitioned by distinct orbits under G action on S.

In other words, S is a union of orbits & 2 distinct orbits are disjoint.



Consider a group G acting on a set S.

Let us fix $s \in S$. The stabilizer of s is the subset of G defined as:

$$G_s = \text{stab}(s) := \{ g \in G \mid gs = s \}$$

The set of group elements that fix s.

$O_s \subseteq S$

Lemma: G_s is a subgroup of G.

Proof: (i) $e \cdot s = s \Rightarrow e \in G_s$

(ii) $g_1, g_2 \in G_s \Rightarrow g_1 s = s \;\&\; g_2 s = s$

$\Rightarrow (g_1 g_2)s = g_1(g_2 s) = g_1 s = s$

$\Rightarrow (g_1 g_2) \in G_s$

(iii) $g \in G_s \Rightarrow gs = s \Rightarrow s = g^{-1}s$

$= g^{-1} \in G_s$

Note: Given an action of G on Ω & an element $s \in S$ we have

Orbit of $s = O_s = \{gs \mid \forall g \in G\}$

Stabilizer of $s = \text{stab}(s) = G_s = \{g \in G \mid gs = s\} \subseteq G$

Theorem: G acts on Ω. Then there exists a bijective function $\phi: G/G_s \to O_s$ Let $s \in S$.

G/G_s: The set of left cosets of G_s in G.

Remark: G/G_s is not a group because G_s is not necessarily a normal subgroup.

Proof: Define $\phi(gG_s) = gs \in O_s$

ϕ is well-defined: If $gG_s = hG_s$ we must ensure that $\phi(g) = \phi(h)$, we need to check $gs = hs$

Why?: If $gG_s = hG_s$

$\Rightarrow g = hg' \quad \exists g' \in G_s$

Why: If G is a group $H \subseteq G$.

If we have $g_1H = g_2H \Rightarrow g_1 \in g_1H = g_2H \Rightarrow g_1 \in g_2H$ $\quad g_1 = g_2h_1, \exists h \in H$

$\therefore$ now $gs = (hg^{-1})s = h(g^{-1}s) = hs$

$\hookrightarrow g^{-1} \in G_s = \{g^{-1}s = s\}$

$\therefore \phi(gG_s) = hs$ as required.

ϕ is 1-1 : $\phi(gG_s) = \phi(hG_s)$

$\Rightarrow gs = hs \Rightarrow (h^{-1}g)s = s$

$= h^{-1}g \in G_s$

$= \therefore (h^{-1}g)G_s = G_s$

$\Rightarrow \boxed{gG_s = hG_s}$

ϕ is onto : What is an element of orbit of s? It is of the form gs $\exists g \in G$.

$\therefore$ we have $\phi(gG_s) = gs$

$\therefore$ This theorem implies :

$$|G/G_s| = |O_s| \quad (\text{Assume } |G| < \infty)$$

$\therefore$ By counting formula

$$|G_s|\,[G : G_s] = |G|$$

But $[G : G_s] = |O_s|$

$\therefore |G_s||O_s| = |G|$

Applications: The number of elements in an orbit must divides $|G|$.

Recall: Orbits partition the set S.

Assume $|S| < \infty$

$\therefore S = O_{s_1} \amalg O_{s_2} \cdots \amalg O_{s_k}$

$\amalg$ - disjoint

$\therefore |S| = |O_{s_1}| + |O_{s_2}| \cdots + |O_{s_k}|$

for some $s_1, \ldots, s_k \in S$

Cayley's Theorem: Let G be a group, $|G| < \infty$ & $|G| = n$. Then G is isomorphic to a subgroup of S_n.

(Recall: S_n is the symmetric group on n letters).

Proof: We are going to consider the action of G on itself by left multiplication.

$\therefore$ $G \times G \to G$ $\quad$ $gs : gs \in G$

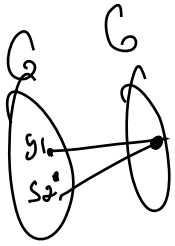
$(g, s) \to gs$

Fix $g \in G$. Consider

$$\phi_g : G \to G$$

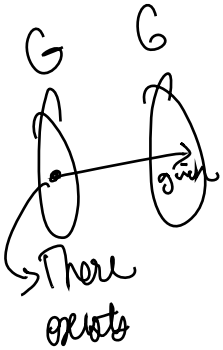
$$\phi_g(s) = gs$$

We claim that ϕ_g is a bijection.



ϕ_g is 1-1: $\phi_g(s_1) = \phi_g(s_2) \Rightarrow gs_1 = gs_2$

$\Rightarrow s_1 = s_2$



ϕ_g is onto: Let $a \in G$. Then $\phi_g(g^{-1}s) = s$

$\therefore \phi_g$ is bijective

Now we know $|G| = n$. What is S_n?

S_n = group of bijections of $\{1, 2 \ldots n\}$

= group of bijections of a set with n elements.

So S_n can be identified with the group of bijection of G.

Now we have a function

$$\psi : G \to S_n$$

$$\psi(g) = \phi_g$$

ϕ_g is bijection of G.

$\therefore \phi_g \in S_n$

Claim: ψ is a group homomorphism.

That is $\psi(g_1 g_2) = \psi(g_1) \circ \psi(g_2)$ $\forall g_1, g_2 \in G$

LHS & RHS are both functions from $G \to G$.

$S_n = \{\phi : G \to G \mid \phi \text{ is a bijection}\}$

$\therefore$ Both these functions are identical.

Let us take any arbitrary $s \in G$. Let us see what LHS & RHS to do.

LHS: $\psi(g_1 g_2) : G \to G$

$\psi(g_1 g_2)(s) = \phi_{g_1 g_2}(s) = (g_1 g_2)s$

RHS: $[\psi(g_1)\psi(g_2)](s) = \psi(g_1)(\psi(g_2)(s))$

$= \psi(g_1)(g_2 s)$

$= (g_1 g_2)s$

$\therefore$ LHS = RHS.

$\therefore$ ψ is a group homomorphism.

ψ is 1-1: Because it is a group homomorphism

It is to check $\ker \psi = \{e\}$?

Clearly $\{e \in \ker \varphi\}$

Suppose $g \in \ker \varphi$. This means

$\varphi(g) = \phi_g$ is the identity element of S_n.

So ϕ_g is the identity function $G \to G$

Hence $\phi_g(s) = s \quad \forall s \in S$

Then $gs = s \quad \forall s \in S$

$\Rightarrow (gs)s^{-1} = ss^{-1}$

$\Rightarrow g = e$

Now: $\varphi : G \to S_n$ is an injective group homomorphism.

So by first Isomorphism theorem

G is isomorphic to the image of φ.

$$G/\ker\varphi \cong \operatorname{im}\varphi$$

But $\ker\varphi = \{e\}$

$$\therefore \quad G \cong \operatorname{im}\varphi$$

But note $\operatorname{im}\varphi$ is a subgroup of S_n.

This proves Cayley's theorem.

Remark: Recall that a cyclic group is isomorphic to a quotient of the form $\mathbb{Z}/n\mathbb{Z}$ for some n.

Problem: Consider the action of G on itself by left multiplication. Find orbit decomposition of G; find the stabilizer of an element $s \in G$.

Soln: $G \times G \to G$, $(g, s) \to gs$ | Fix $s \in S$. What is O_s?

$O_s = \{gs \mid g \in G\} \subseteq G$

We have $O_s = G$: because if $t \in G$, then $(ts^{-1})s = t$

$\therefore$ Let $t \in O_s$.

$\therefore O_s = G \ \forall s \in G$

There is only one orbit for this action. This is an example of a transitive action.

$\therefore G = O_s \ \forall s \in G$

Now let $s \in G$. Find G_s: stab(s) $\left\{ \begin{matrix} gs = s \\ g = e \end{matrix} \right\}$

$G_s = \{g \in G \mid gs = s\} = \{e\}$

$\therefore$ Stabilizer of any element is just $\{e\}$.

Assume $|G| < \infty$. Recall the counting formula.

$|G| = |O_s| \, |\text{stab}(s)|$ [for a fixed element $s \in S$]

(large orbit $\Rightarrow$ small stabilizer
small orbit $\Rightarrow$ large stabilizer) QED

Problem 2: Do the same for the action of G on itself by conjugation, when G is abelian.

Soln: $G \times G \to G$

$(g, s) \longrightarrow gsg^{-1}$

Let $s \in G$. $O_s = \{ gsg^{-1} \mid g \in G \} = \{ gg^{-1}s \mid g \in G \} = \{ s \}$

$G_s = \{ g \mid gsg^{-1} = s \} = \{ g \in G \mid s = s \} = G$

$\therefore$ over here orbits are small; stabilizers are big.

Orbit decomposition: $G = \coprod_{s \in G} \{ s \}$

Problem 3: Again consider Problem 2. But G is not abelian. Show that

(1) G_s = centralizer of s:

(2) $s \in$ centre of $G \iff G_s = G$

Lem: Recall: Let G be a group; $g \in G$.

"centralizer of g"

$$C(g) := \{a \in G \mid ag = ga\}$$
$$= \{a \in G \mid aga^{-1} = g\}$$

"center of G"

$$Z(G) := \{a \in G \mid ag = ga \ \forall g \in G\}$$
$$= \{a \in G \mid aga^{-1} = g \ \forall g \in G\}$$

① $G_s = \{g \in G \mid gsg^{-1} = s\} = C(s)$

② $s \in Z(G) \iff sg = gs \ \forall g \in G$

$\iff gsg^{-1} = s \ \forall g \in G$

$\iff g \in G_s \ \forall g \in G$

$\iff G_s = G$

Problem 4: $G = GL_n(\mathbb{R})$, $S = \mathbb{R}^N$ $\quad G \times S \to S$

$A \cdot v = Av$ (matrix multiplication)

(i) Find orbit decomposition of $\mathbb{R}^N$

(ii) Find the stabilizer of $e_1 = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$

Soln (i): The orbit of the $\vec{0}$ is $\{0\}$.

$$A \cdot \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$$

- There is only one other orbit because given any non-zero vectors v_1 & v_2 $\exists\, A v_1 = v_2$ $\exists\, A \in GL_n(\mathbb{R})$

$\Rightarrow$ All non-zero vectors form an orbit

$$\mathbb{R}^n = \{0\} \cup \mathbb{R}^n - \{0\}$$

$\therefore$ There are exactly 2 orbits for this action.

(ii) $G_{e_1} = \text{stab}(e_1) = \{A \in GL_n(\mathbb{R}) \mid Ae_1 = e_1\}$

$$A = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{n1} \end{bmatrix}$$

$\therefore A \in G_{e_1} \Rightarrow Ae_1 = e_1 \Rightarrow \begin{bmatrix} a_{11} \\ \vdots \\ a_{n1} \end{bmatrix} = \begin{bmatrix} 1 \\ \vdots \\ 0 \end{bmatrix}$

$\text{Stab}(e_1) = G_{e_1} = \{A \in GL_n(\mathbb{R}) \mid \text{first column of } A \text{ is } e_1\}$

$$= \left\{ \begin{bmatrix} 1 & * \\ 0 & \boxed{*} \\ \vdots & \\ 0 & \end{bmatrix} \in GL_n(\mathbb{R}) \right\}$$

Problem 5: $G = GL_n(\mathbb{R})$, $S = \mathbb{R}^n$

Show that if $A \in GL_n(\mathbb{R})$ satisfies $A \cdot v = v$ $\forall v \in \mathbb{R}^n$,

then $A = I$.

Solution: We already saw $Ae_1 = e_1 \Rightarrow$ 1st column of A is e_1.

$\therefore$ $Ae_2 = e_2 \cdots Ae_n = e_n$

$\Rightarrow A = I_n$

This action is an example of a faithful action.

Definition: Let G act on S. Then "G acts faithfully on S" if $gs = s$ $\forall s \in S \Rightarrow g = e$.

Example: * Action of G on itself by left multiplication is faithful.

* Action of G on itself by conjugation is not faithful in general.

For example if G is abelian then

$G_S = G$ $\forall s \in S$.

Problem 6: Show that action of G on itself by conjugation is faithful $\iff Z(G) = \{e\}$

Problem 7: Let $G = S_3$. Compute the orbits for the action of S_3 on itself by conjugation.

Soln: $S_3 = \{e, (12), (13), (23), (123), (132)\}$

Defn: Orbits for the action of G on itself by conjugation are called conjugacy classes.

What is O_e?

$$O_e = \{geg^{-1} \mid g \in G\} = \{e\}$$

$$O_{12} = \{g(12)g^{-1} \mid g \in S_3\}$$

$e(12)e = (12)$

$(12)(12)(12) = (12)$

$(13)(12)(13) = (23)$

$(23)(12)(23) = (13)$

$(123)(12)(123)^{-1} = (123)(12)(132) = (23)$

$(132)(12)(132)^{-1} = (132)(12)(23) = (13)$

$\therefore$ Conjugacy class of (12)

$$O_{(12)} = \{(12), (23), (13)\}$$ All 2 cycles.

S_3 = disjoint union of conjugacy classes.

$= \{e\} \sqcup \{(12)(23), (13)\}$

Find $\mathcal{O}_{(123)}$

$(12)(123)(12) = (132) \Rightarrow (123) \sim (132)$

∴ We can conclude that $\{(123), (132)\}$ is a conjugacy class.

∴ $S_3 = \{e\} \sqcup \{(12), (23), (13)\} \sqcup \{(123), (132)\}$

QED

$|S_3| = |\{e\}| + |\{(12), (23), (13)\}| + |\{(123), (132)\}|$

Extra

In the case of a finite group acting on itself by conjugation

$|G| = |\mathcal{O}_{s_1}| + |\mathcal{O}_{s_2}| \cdots |\mathcal{O}_{s_k}|$

for some $s_1 \cdots s_k \in S$

is called the **class equation of G.**

∴ Class Eqn of S_3

$6 = 1 + 3 + 2 = 6$

$\mathcal{O}_{(12)} = \{(12), (23), (13)\}$

$|G_{(12)}| |\mathcal{O}_{(12)}| = 6 = |S_3|$ (By counting Formula)

$\Rightarrow |G_{(12)}| = 2$. What is $G_{(12)}$?

$$G_{(12)} = \{g \in S_3 \mid g(12)g^{-1} = (12)\}$$
$$= \{g \in S_3 \mid g(12) = (12)g\}$$

Clearly, $e \in G_{(12)}$ & $(12) \in G_{(12)}$

We know $|G_{(12)}| = 2$

$\therefore G_{(12)} = \{e, (12)\}$

$G_{(13)} = \{e, (13)\}$

$G_{(23)} = \{e, (23)\}$

$|G_{(123)}| = 6/2 = 3$

$e, (123) \in G_{(123)}$

Since $G_{(123)}$ is a subgroup of S_3, & $(123) \in G_{(123)}$

$\therefore (123)^{-1} \in G_{(123)}$. So $(132) \in G_{(123)}$

$\Rightarrow G_{(123)} = \{e, (123), (132)\}$

Sylow Theorems

Recall: G acts on S

$\cdot : G \times S \to S$

$(g, s) \to gs$

Counting formula: let $s \in S$

$\mathrm{Stab}(s) = G_s = \{ g \in G \mid gs = s \} \subseteq G$ [subgroup]

$O_s = \{ gs \mid \forall g \in G \} \subseteq S$ [subset]

$|G| = |G_s||O_s|$ ($G/G_s \xrightarrow{\sim} O_2$)

① G acts on itself by left multiplication

② G " " conjugation (class eqn)

$|G| = |C_1| + |C_2| \cdots |C_k|$

$C_1, C_2 \cdots C_k$ are distinct conjugacy classes of G;

"conjugacy class" = an Orbit for G acting on itself by conjugation.

Class eqn of S_3: $6 = 1 + 2 + 3$

Consider now the action of G on itself by left multiplication. We want to define an action of G on subsets of G.

Let $A \subseteq G$ be a subset, let $g \in G$

Define: $g \cdot A = \{ga \mid \forall a \in A\}$

Exercise: $P(G)$ (Powerset of G)

The above actions defines an action of G on $P(G)$.

★ 2. Let A be a subset. What is the stabilizer of A?

$$\text{stab}(A) = \{g \in G \mid gA = A\}$$

$gA = A$ means: $\{ga \mid a \in A\} = gA = A$

In other words, if $a \in A$ then $ga \in A$.

In particular it is not necessary that $ga = a$.

Now G acts on itself by left mults; $A \subseteq G$ subset.

Let $H = \text{stab}(A) = \{g \in G \mid gA = A\}$ $|G| < \infty$

Lemma: $|H|$ divides $|A|$.

Proof: Let $a \in A$. Then $ha \in A$ $\forall h \in H$.

So $\{ha \mid h \in H\} \subseteq A$

The H-orbit of a is completely inside A.

$$\{ha \mid h \in H\} = Ha \quad \text{"Right coset of } H\text{"}$$

Hence A is the union of H-orbits.

Why?: $a \in A \Rightarrow$ H-orbit of $a \subseteq A$

$$Ha \subseteq A$$

$$\therefore \boxed{A = \bigcup_{a \in A} Ha}$$

In fact we can write A as a disjoint union of cosets. $A = Ha_1 \sqcup Ha_2 \cdots \sqcup Ha_n$

$$\therefore |A| = |Ha_1| + |Ha_2| - \cdots |Ha_n|$$

$$= |H| + \cdots |H|$$

$$= n|H|$$

$$\therefore |A| = n|H|$$

QED

We are going to prove Sylow theorems.

Let G be a finite group. Let p be a prime number.

Say $|G| = n < \infty$. Write $n = p^e m$ where p, m are co-prime.
$e \geq 0, m \geq 1 \quad (p \nmid m)$

Example: $n=6, p=2$: $6 = 2^1 \cdot 3 \quad (e=1, m=3)$
$n=6, p=3$: $6 = 3^1 \cdot 2 \quad (e=1, m=2)$
$n=6, p=5$: $6 = 5^0 \cdot 6 \quad (e=0, m=6)$

★ **Def:** A Sylow p-subgroup of G is a subgroup of order p^e. Write $|G| = n = p^e \cdot m$

Example: A Sylow 2-subgroup of S_3 is a subgroup of order 2.

S_3 has 3 Sylow-2-subgroups. $(6 = 2^1 \cdot 3)$

S_3 has 1 Sylow 3-subgroups $(6 = 3^1 \cdot 2)$

S_3 has no Sylow-p-subgroups if $p \neq 2$ & $p \neq 3$

First Sylow Theorem: Let G be a finite group, let p be a prime number s.t $p \mid |G|$.

(Write $|G| = n = p^e m$, where $e > 0$, & p does not divide m.)

Then G has a sylow-p-subgroup.

Recall: Cauchy Theorem:- if G is an abelian group & $p \mid |G|$ then G has an element of order p.

∴ First Sylow-theorem is a vast generalization of Cauchy theorem.

Proof: Let S be the set of subsets of G of order p^e.

$n = p^e m$

$$\therefore S = \{ A \subseteq G \mid |A| = p^e \}$$

G acts on S by left multiplication.

$$g \cdot A = \{ ga \mid \forall a \in A \}$$

Exercise: If $|A| = p^e$, then $|gA| = p^e$, ie: $|A| = |gA|$.

Fact: $|S| = \binom{n}{p^e}$

$$= \left(\frac{n!}{(n-p^e)!(p^e)!} \right) = \frac{n(n-1)(n-2)\cdots(n-p^e+1)}{p^e(p^e-1)\cdots(1)}$$

② p does not divide $|S|$

$$|S| = \binom{n}{p^e} \cdot \binom{(n-1)}{p^e-1} \cdots \binom{n-(p^e-1)}{p^e-(p^e-1)}$$

The same factor of p divides $n-i$ & p^e-i for any

$$i = 0, 1 \ldots, p^e-1$$

Write $i = p^n \cdot k$. Then $n-i = p^n m - p^n k$

$$= p^n(p^{e-n} - k)$$

$(n < e)$

Hence $p^e - i = p^e - p^n k = p^n(p^{e-n}-1)$

$\hookrightarrow$ p^n is the largest power of p that divides both $n-i$ & p^e-i.

Key fact: p does not divide $|S|$.

G acts and by left multiplication.

We have the orbit decomposition of S:

$$|S| = |O_1| + |O_2| \cdots |O_k|$$

where $O_1, O_2 \ldots O_k$ ... are all distinct orbits for the action of G on S.

But now by the above fact, p does not divide $|S|$.

So $\exists$ an orbit O_i s.t p does not divide $|O_i|$.

Say O_i = orbit of A; $A \in S$. $\boxed{A \subseteq S}$

Now let $H = \text{stab}(A)$.

Claim: H is a sylow p-subgroub of G.

Proof: We know that H is a subgroup of G.

We need to show $|H| = p^e$.

By the lemma: $|H|$ divides $|A|$.

So $|H|$ is a power of p. (Because p is a prime)

We also have: $|G| = |\text{Stab}(A)|\,|\text{Orbit}(A)|$

$$\begin{matrix} |G| & = & |\text{Stab}(A)| & |\text{Orbit}(A)| \\ \| & & \| & \| \\ p^e m & = & p^i & r \end{matrix}$$

By choice of A, p does not divide r.

$p^e m = p^i r$, p does not divide r.

$\Rightarrow i = e$

So $|H| = p^e$.

QED

Cor: Let G be a finite group & let p be a prime that divides $|G|$. Then G has an element of order p. ($|G| = p^e m$)

Proof: By I(ST) (sylow theorem), G has a sylow p-subgroup say H.

$|H| = p^e$ Let $a \in H$. $a \neq e$

$\text{ord}(a) \mid |H|$ by lagrange's theorem.

$\Rightarrow \text{ord}(a) = p^{r}$ for some $1 \le r \le e$.

Now consider $b = a^{p^{r-1}}$ $\quad \langle b \rangle \subseteq G$

Then we claim $\text{ord}(b) = p$.

$$b^p = (a^{p^{r-1}})^p = a^{p^r} = e \quad \left(a^{\text{ord}(a)} = e\right)$$

$\therefore$ $\text{ord}(b)$ divides p. $\Rightarrow \text{ord}(b) = 1$ or $\text{ord}(b) = p$

If $\text{ord}(b) = 1 \Rightarrow b = e \Rightarrow a^{p^{r-1}} = e$

$\Rightarrow \text{ord}(a) \mid p^{r-1}$

$\Rightarrow p^r \mid p^{r-1}$

which is absurd.

$\therefore$ $\text{ord}(b) = p$, & b is the element we are looking for.

QED

Second Sylow theorem: Let G be a finite group. Let p be a prime that divides $|G|$. Then any 2 Sylow subgroups are "conjugate".

Recall: We say 2 subgroups H & K are conjugate if $H = gKg^{-1}$ $\exists g \in G$

Proof: Let H and K be two Sylow p-subgroups of G.

We will consider the action of K on G/H by conjugation.

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

Let $b \in K$, $aH \in G/H$ $\therefore b(aH) \overset{\text{def}}{=} (ba)H$

This is an action of K on G/H. ie $K \times G/H \longrightarrow G/H$

$(b, aH) \longrightarrow (ba)H$

Now G/H is the union of disjoint K-orbits.

$$|G/H| = |O_1| + |O_2| \cdots + |O_n|$$

where $O_1, \ldots O_n$ are the distinct K-orbits of G/H.

Now $|G| = n = p^e m$

$|H| = p^e$

$\therefore |G/H| = m$

$p \nmid m$

$p \mid |O_i|$ for some i.

Say O_i is the orbit of $aH \in G/H$.

Now counting formula applied to the K-action on G/H, and aH.

$$|K| = |\text{stab}(aH)|\,|\text{orbit}(aH)|$$
$$p^e = |\text{stab}(aH)|\,|O_{aH}|$$

But p does not divide $|O_{aH}|$. So $|\text{stab}(aH)| = p^e$,
$$|O_{aH}| = 1$$

$\therefore$ we have $\text{stab}(aH) \subseteq K \Rightarrow \text{stab}(aH) = K$

So we have $b(aH) = aH \;\forall\, b \in K$.
$$\Rightarrow (ba)H = aH \;\forall\, b \in K$$
$$\Rightarrow (ba) \in aH \;\forall\, b \in K$$
$$\Rightarrow b \in aHa^{-1} \;\forall\, b \in K$$
$$\Rightarrow K \subseteq aHa^{-1}$$

Note: $|K| = p^e$, $|H| = p^e \Rightarrow |aHa^{-1}| = p^e$

But $K \subseteq aHa^{-1} \Rightarrow \boxed{K = aHa^{-1}}$

QED

Example: $G = S_3$; G has 3 sylow-2-subgroups.

$6 = 2 \cdot 3$

$G = \{e, (12), (13), (23), (123), (132)\}$

subgroups

$H_1 = \{e, (12)\}$, $H_2 = \{e, (13)\}$, $H_3 = \{e, (23)\}$

By Second Sylow theorem $\Rightarrow H_1, H_2, H_3$ are all conjugate to each other.

Exercise: Find an element $a \in S_3$ s.t

$$aH_1a^{-1} = H_2$$

Cor: Suppose $|G| < \infty$ and a group G has only one Sylow p-subgroup H. Then H is normal in G.

Proof: To prove $H \triangleleft G$ we must show

$$g \in G, h \in H \Rightarrow ghg^{-1} \in H$$

Equivalently: Show that $gHg^{-1} = H \ \forall g \in G$

Proof: If H is a Sylow p-subgroup, then $|H| = p^e$.
Then if $g \in G$, $|gHg^{-1}| = p^e$; and then it is also gHg^{-1} is a subgroup of G.
So gHg^{-1} is a Sylow p-subgroup. By hypothesis

$$gHg^{-1} = H \quad \boxed{\text{QED}}$$

Example: $G = S_3$, $p = 3$; $6 = 3 \cdot 2$
We know $\exists$ only one Sylow 3-subgroup

$$H = \{e, (123), (132)\}$$

By cor, H is normal in G.

Third Sylow Theorem: Let $|G| < \infty$, & let $p \mid |G|$ (↳ prime).

$|G| = p^e m$, $p \nmid m$.

Now let 's' be the number of sylow p-subgroups of G. Then

(i) s divides m

(ii) $s = ap + 1$ for some $a \in \mathbb{N}$

Proof: Consider $\mathcal{S} = \{$ sylow p-subgroups of $G\}$

$= \{H \subseteq G \mid |H| = p^e\}$

We consider the action of G on $\mathcal{S}$ by conjugation.

ie $H \in S \Rightarrow \underbrace{g \cdot H = gHg^{-1}}_{\text{action preserves the subgroup}} \in S \ (g \in G)$.

Let $H \in S$.

Now $O_H = \{gHg^{-1} \mid g \in G\}$

$= S$ by second Sylow theorem

Now $\text{stab}(H) = \{g \in G \mid gHg^{-1} = H\}$

$=$ Normalizer of H

$= N(H)$ & $N \cdot \supseteq H$

By counting formula

$|G| = |O_H| \, |\text{stab}(H)|$

$p^e m = |S| \, |N(H)| = s \cdot |N(H)|$ $\quad \{|S| = s$ (Definition)$\}$

$\therefore p^e m = S \cdot |N(H)| = S \cdot |N|$

Now $H \leq N \leq G$. So $[G:N]$ divides $[G:H]$.

Why: $|G| = [G:H]|H|$

$= [G:N]|N|$

Since $H \leq N$ then by Lagrange's theorem

$|H| \mid |N|$. So we write

$|H| \cdot l = |N| \quad \exists\, l \in \mathbb{N}$ (naturals)

$\therefore |G| = [G:H]|H| = [G:N]|N|$

$= [G:N]|H| \cdot l$

$\Rightarrow [G:H] = [G:N]\, l$

$\Rightarrow [G:N] \mid [G:H]$ QED

Now by counting formula we have

$|G| = |N| \cdot S \Rightarrow S = \frac{|G|}{|N|} = [G:N]$

We know $[G:N] \mid [G:H]$

$\therefore S = \frac{|G|}{|N|} = [G:N]$

Now $[G:N] \mid [G:H] = \frac{|G|}{|H|} = \frac{p^e m}{p^e} = m$

$\therefore S \mid m$ QED Part (1)

Now part ②

We consider a different action.

Fix a sylow p-subgroup H.

We look on the action of H on S.

where $S = \{ H = H_1, H_2 \dots H_s \}$

H acts on S by conjugation.

What is the H-orbit of H?

$$\mathcal{O}_H = \{ gHg^{-1} \mid g \in H \} = \{ H \}$$

Let $i > 1$. Suppose that $\{H_i\}$ is an H-orbit of S.

Then $hH_ih^{-1} = H_i \quad \forall h \in H$

$\Rightarrow h \in$ Normalizer of H_i $\forall i$

$\Rightarrow H \subseteq N_i$

Recall: $N_i = N(H_i)$

$= \{ g \in G \mid gH_ig^{-1} = H_i \}$

We thus have

H & H_i are both subgroups of N_i.

Moreover H & H_i are in fact sylow p-subgroups of N_i.

(p^e) $H_i \subseteq N_i \subseteq G \quad (p^e m)$

$|N_i| = p^e m'$

By the second Sylow theorem (to N_i)

H and H_i are conjugate in N_i.

Then $\exists\, g \in N_i$ s.t. $gHg^{-1} = H$

$\Rightarrow g \in N_i \Rightarrow gH_ig^{-1} = H_i$ (since $gHg^{-1} = H$) $\Rightarrow H = H_i$

If $\{H_i\}$ is an H-orbit in S, then $H_i = H$.

So $\{H\}$ is the only singleton orbit in S.

Now look at orbit decomposition of S.

$$S = |S| = |O_1| + |O_2| \cdots |O_k|$$
$$= 1 + |O_2| \cdots |O_k|$$

$O_1 = \text{orb}(H) = \{H\}$

By the above argument, $|O_i| \geq 2 \quad \forall i = 2 \ldots k$

Applying counting formula: $O_i = \text{orb}(H_i)$

$$|H| = |\text{stab}(H_i)|\,|O_i|$$
$$p^e = \cdot \times |O_i|$$
$$\therefore |O_i| \mid p.$$

$\therefore$ for $i \geq 2$: $|O_i| \geq 2$ and $|O_i|$ divides p. $|O_i| = p \cdot a_i, a_i \geq 1$

$$S = |S| = |O_1| + |O_2| \cdots + |O_k|$$
$$= 1 + p \cdot a_1 + \cdots p \cdot a_k$$
$$= 1 + p(a_1 + \cdots a_k)$$
$$= 1 + p(a) \qquad \left[a = \sum_{i} a_i\right]$$

$$\therefore \boxed{S = 1 + ap}$$

QED

Example: $G = S_3$, $|G| = 6 = 2 \cdot 3 = 3 \cdot 2$

s_2 = The number of Sylow 2-subgroups

s_3 = The number of sylow 3-subgroups

By Third sylow theorem $\Rightarrow$

$6 = 2 \cdot 3$

$\left\{ \begin{array}{l} s_2 \text{ divides } 3 \\ s_2 = 1 + 2a \end{array} \right\}$ | we know $s_2 = 3$ // $s_3 = 1$

$6 = 5 \cdot 2$

$\left\{ \begin{array}{l} s_3 \text{ divides } 2 \\ s_3 = 1 + 3a \end{array} \right\}$ | $s_3 = 1$

If $G = S_3$, then $s_2 = 3$

If $G = \mathbb{Z}/6\mathbb{Z}$, $s_2 = 1$ ($\mathbb{Z}/6\mathbb{Z}$ has exactly one sylow-2 subgroup))

And $\mathbb{Z}/6\mathbb{Z} = \{0, 1, 2, 3, 4, 5\}$

$|G| = 2 \cdot 3$

$s_2 = 1 + 2a$ and $s_2 | 3$.

$s_2 \neq 3$ { eg: $\{3,4,5\} + \{3,4,5\} = \{0,2,4\} \notin \{3,4,5\}$ }

$\therefore s_2 = 1$. QED

Proposition: Any group of order 15 is cyclic.

Proof: We will show $G \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. (Isomorphic)

Describe: $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} = \{(a,b) \mid \begin{matrix} a \in \mathbb{Z}/3\mathbb{Z} \\ b \in \mathbb{Z}/5\mathbb{Z} \end{matrix}\}$

Component-wise addition. $(a,b)+(c,d) = (a+c, b+d)$

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

identity $= (0,0)$

$\therefore \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ is a group under this.

Let G be a group of $|G| = 15$. $15 = 3 \cdot 5$

So G has Sylow-3 subgroups & Sylow-5 subgroups.

$s_3 = \#$ Sylow-3 subgroups

$s_5 = \#$ " -5 "

By Third Sylow theorem: $\{ s_3 \mid 5$ and $s_3 = 1+3a \}$

$\Downarrow$

$s_3 = 1$

Similarly $\{ s_5 \mid 3$ and $s_5 = 1+5a \}$

$\Downarrow$

$s_5 = 1$

So in G $s_3 = 1$, $s_5 = 1$. $\quad H \to$, $K \to$

By second Sylow theorem: H and K are normal in G.

H is a Sylow 3-subgroup: $\Rightarrow |H| = 3$

$\Rightarrow H \cong \mathbb{Z}/3\mathbb{Z}$

(Previously proved)

Similarly $\Rightarrow K \cong \mathbb{Z}/5\mathbb{Z}$

We consider: $\phi: H \times K \longrightarrow G$

$(h,k) \longmapsto hk$

We first show $H \cap K = \{e\}$

Why: $H \cap K \subseteq K$

$H \cap K \subseteq H$

By Lagrange's theorem: $|H \cap K| \mid |H|$

$|H \cap K| \mid 3$

$\Rightarrow |H \cap K| = 1$ or $|H \cap K| = 3$

$\|$

$\{e\}$

If $|H \cap K| = 3$: also know $H \cap K \subseteq K$

$\therefore$ But $|H \cap K| \mid 5$

$\therefore 3 \nmid 5$

$\therefore H \cap K = \{e\}$

ϕ: is a homomorphism:

$\phi((h_1,k_1)\cdot(h_2,k_2)) = \phi((h_1,k_1)) \cdot \phi((h_2,k_2))$

$\phi((h_1h_2, k_1k_2)) = (h_1,k_1)\cdot(h_2k_2)$

$\Rightarrow h_1h_2k_1k_2 \overset{?}{=} h_1k_1h_2k_2$

We have: if $h \in H$, $k \in K$, then $hk = kh$

$(hkh^{-1})k^{-1} = h(khk^{-1})$ $(H \lhd G)$

$\in K$ $\quad \in H$ $\quad \in H$

$\downarrow$

$\in K$ $\therefore (hkh^{-1})k^{-1} \in K$ $\quad \therefore h(khk^{-1}) \in H$

as $K \lhd G$

But $K \cap H = \{e\} \Rightarrow hkh^{-1}k^{-1} = e$

$\Rightarrow \boxed{hk = kh}$

$\therefore$ finally $h_1h_2k_1k_2 \overset{?}{=} h_1k_1h_2k_2$

$\Rightarrow h_1k_1h_2k_2 = h_1k_1h_2k_2$

$\therefore \phi$ is a homomorphism.

Now ϕ is 1-1 : $\phi(h_1,k_1) = \phi(h_2,k_2)$

$\Rightarrow h_1k_1 = h_2k_2$

$\Rightarrow h_2^{-1}h_1 = k_2k^{-1} \Rightarrow h_2^{-1}h_1 = e \Rightarrow h_1 = h_2$

$\Rightarrow k_2k^{-1} = e \Rightarrow k_2 = k_1$

$h_2^{-1}h_1 \in H$, $k_2k^{-1} \in K$, $(H \cap K = \{e\})$

$\therefore \phi$ is 1-1

ϕ is onto : $\phi : H \times K \to G$

$(h,k) \longrightarrow hk$

Claim : $H \times K$ has 15 elements.

This implies ϕ is onto, because ϕ is 1-1 & $|G| = 15$

Why? We can show that $H \times K \subseteq G$. This is easy to check.

By lagrange $\Rightarrow |H \times K| \mid 15$: $|H \times K| > 5$

as $|K| = 5$ & $|H| = 3$

$\therefore \Rightarrow |H \times K| = 15$

Thus ϕ is an isomorphism.

$H \cong \mathbb{Z}/3\mathbb{Z}$, $K \cong \mathbb{Z}/5\mathbb{Z}$

$\therefore G \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ for any group $|G|=15$

In particular, $\mathbb{Z}/15\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong G$

QED $G \cong \mathbb{Z}/15\mathbb{Z}$ and hence G is cyclic.

Problem 1: Show that a group of order 100 has a normal subgroup of order 25.

Soln: $|G| = 100 = 5^2 \cdot 4$

$\exists$ A sylow 5-subgroup of G has order $5^2 = 25$.

Now s_{25} = # sylow 5-subgroups

Now by 3rd ST $s_{25} \mid 4$ & $s_{25} = 1+5a$

$\Downarrow$

$s_{25} = 1$

$\therefore$ By 2ST $\exists$ a normal subgroup of order 25.

Now sylow 2-subgroups of G have order 4.

$s_4 \mid 25$ $\Big\}$ $s_4 = 1$ or 5 or 25

$\downarrow$

$s_4 = 1+2a$

we don't know how many (G drawback of Sylow theorems).

QED

Problem 2: Let p and q be primes and $p<q$. Let $|G|=pq$. Show that G has a normal subgroup of order q.

Soln: Sylow q-subgroup of G have order q.

$s_q = \#$ sylow q-subgroups

Now by [3ST] $s_q \mid p$ & $s_q = 1+aq$

$\Downarrow$

$s_q = 1$ or $s_q = p$ ($p \neq 1+aq$ as $p<q$)

$\therefore s_q = 1$

$\therefore$ [by 2ST] $\exists$ a normal subgroup of Sylow-q.

[QED].

Problem 1: Let G be a group and p prime, $|G|=p^e$, $e \geq 1$. Show that the centre of G is non-trivial.

Recall: $Z(G) = \{g \in G \mid ga = ag \ \forall a \in G\}$

We want to show $Z(G) \neq \{e\}$, $|Z(G)| > 1$.

Soln: Consider the action of G on itself by conjugation.

Class equation:

$p^e = |G| = |C_1| + |C_2| \cdots |C_k|$ (conjugacy classes)

But one $C_1 = \{e\}$ (orbit of e)

$p^e = 1 + |C_2| \cdots |C_k|$

By counting formula

$p^e = |G| = |\text{stab}(a)| \, |\text{Og}|$

$\therefore |O_g| \mid p^e$.

$\therefore |O_g| = p^i$ for some $i = 0, 1, 2 \ldots, e$

$$p^e = 1 + \sum_{i=2}^{k} |C_i|$$

$$= 1 + p^{a_2} + p^{a_3} \ldots p^{a_k}$$

Suppose $a_2, a_3 \ldots a_k > 0$

Then $p^e = 1 + \underbrace{p^{a_2} + p^{a_3} \ldots p^{a_k}}_{\text{divisible by } p}$.

$\Rightarrow p$ divides 1; this is absurd (

$\therefore$ some $a_i = 0$. Say $a_2 = 0$

$|C_2| = 1 \Rightarrow C_2 = O_g$ has only one element

$$C_2 = O_g = \{ aga^{-1} \mid a \in G \} = \{ g \}$$

$$= aga^{-1} = g \quad \forall a \in G$$

$$\rightarrow ag = ga \quad \forall a \in G \Rightarrow g \in Z(G)$$

Remember $g \neq e$

$\therefore$ We have produced an element g in the center which is different from e.

So $|Z(G)| > 1$.

$\therefore$ p-groups have non-trivial center.

QED

Problem 2: Suppose G has order p, p^2 then G is abelian.

Soln: $|G|=p \Rightarrow G$ is a cyclic group $\Rightarrow G$ is abelian

So assume $|G|=p^2$.

To show G is abelian. Equivalently to show $Z(G)=G$.

Now we know

$(e) \subsetneq Z(G) \subseteq G$. Suppose $Z(G) \neq G$.

Choose $x \in G$, $x \notin Z(G)$.

Consider the centralizer of x:

$$C(x) := \{ g \in G \mid gxg^{-1}=x \} \subseteq G$$

Now $Z(G) \subseteq C(x)$

Why: $Z(G)=\{ g \in G \mid gag^{-1}=a \ \forall a \in G \}$

$$\therefore (e) \subsetneq Z(G) \subseteq C(x) \subseteq G$$
$$\quad\ \| \qquad\ \| \qquad\ \| \qquad\ \|$$
$$\quad\ 1 \qquad\ p \qquad\ p^2$$

$\therefore C(x)$ contains x $\Rightarrow Z(G) \subsetneq C(x)$
$Z(G)$ & x

$\therefore |C(x)| = p^2 = |G| = G \Rightarrow gx=xg \ \forall g \in G$

$\Rightarrow x \in Z(G)$

which is a contradiction because we chose $x \notin Z(G)$.

QED.

Problem 3: G is a finite group & $p^i \mid |G|$. Then G has a subgroup of order p^i.

Soln: WLOG, we can assume G is a p-group.
(ie $|G| = p^n$)

Why: $|G| = p^e m$, $p \nmid m$

Sylow 1 $\Rightarrow$ G has a subgroup of order p^e, say H.

> Take $i \leq e$ if we show H has a sub group of order i then G had a subgroup of order i.
>
> So we can restrict our attention to H.

$\therefore$ From now, assume $|G| = p^e$, $i \leq e$.

To show G has a subgroup of order p^i.

So $|Z(G)| \geq 1$. (p-group)

Choose an element $x \in Z(G)$. s.t $\text{ord}(x) = p$. (cor of Sylow 1)

$i \to$ new subgroup (not previous one)

Now let H be the subgroup generated by x.

$|H| = p$ & $\langle x \rangle = H$.

H is in fact normal in G: ($x \in Z(G)$)

$gx^n g^{-1} = x^n \in H$. ($\nearrow$)

$\therefore$ We can consider the quotient group G/H.

Let us consider $\phi: G \to G/H$; $|G/H| = \frac{|G|}{|H|} = \frac{p^e}{p} = p^{e-1}$

$g \to gH$

We use induction: $|G/H| = p^{e-1} < p^e$;

So assume by induction that G/H has a subgroup say K' s.t $|K'| = p^{i-1}$

$(p) \; G \xrightarrow{\phi} G/H$

$K \subseteq G/H$

$(p^{i-1}) \quad (p^{e-1})$

$\| \; \phi^{-1}(K')$

Kernel of $\phi = H$

$(K \subseteq G)$

Let $K = \phi^{-1}(K')$

So $K \subseteq G$. We claim that $|K| = p^i$.

Why?

We have

$$\begin{array}{ccc} G & \to & G/H \\ \cup & & \cup \\ K & \xrightarrow{\phi|_K} & K' \ni e \end{array} \Rightarrow \boxed{H \subset K}$$

★ 2

Kernel of $\phi|_K = H$

ϕ restricted to K.

And also $\phi|_K$ is onto.

By 1st Isomorphism theorem $\Rightarrow K/\ker(\phi|_K) \simeq K'$

$\Rightarrow K/H \simeq K'$

$\Rightarrow |K| = |K'||H|$

$= (p^{i-1}) \cdot p$

$\boxed{|K| = p^i}$

QED

Thus $K \subseteq G$ s.t $|K| = p^i$

End of Course ★