KHARAGPUR COLLEGE
DEPARTMENT OF MATHEMATICS

STUDY MATERIALS

SUBJECT: MATHEMATICS HONOURS

CLASS: B. Sc. Hons. 3RD Year

SEMESTER: 5 TH

PAPER: C12T

NAME OF THE PAPER: GROUP THEORY –II

UNIT – I

Dr. Sangita Chakraborty

Associate Professor

Department of Mathematics

Kharagpur College

Email: sangita@kharagpurcollege.ac.in

19/08/2020. RECAP LECTURE NOTE - 1 Jishan ...
... GROUP THEORY-2

Homomorphism → A map $\phi : (G, o) \to (G', *)$ s.t.
$\phi(a o b) = \phi(a) * \phi(b)$, $\forall a, b \in G$.

① It preserves the algebraic structure of the system.

② A one-to-one homomorph. is called monomorphism
An onto " " " epi "
A one-to-one & onto homomorph. " " iso " .

③ A homomorph. $\phi(a) = e_{G'}$, $\forall a \in G$, is called Trivial homo.
⇒ there always exists a homomorph. from a group to a group

④ Let $\phi : (G, o) \to (G', *)$ be a homomorphism.
Then
(i) $\phi(e_G) = e_{G'}$ (ii) $\phi(a^{-1}) = \{\phi(a)\}^{-1}$, $\forall a \in G$.
(iii) $\phi(a^n) = \{\phi(a)\}^n$, $n \in \mathbb{Z}$; $a \in G$
(iv) $o(\phi(a)) \mid o(a)$, if $o(a)$ is finite; $a \in G$.

⑤ Homomorphic image of ϕ = $\mathrm{Im}\,\phi = \phi(G) = \{\phi(a) : a \in G\}$
$\phi(G) \leq G'$.

⑥ If ϕ is an isomorphism, then
(i) G ableian ⇔ G' also abelian / $\phi(G)$ abelian.
⇍ if ϕ is epimorph.
(ii) G cyclic ⇔ G' " cyclic / $\phi(G)$ cyclic.
⇍ if ϕ is epimorph.
if $G = \langle a \rangle$ ⇒ G' or $\phi(G) = \langle \phi(a) \rangle$.

⑦ $\mathrm{Ker}\,\phi = \{a \in G : \phi(a) = e_{G'}\} \subseteq G$.
(i) $\mathrm{Ker}\,\phi \trianglelefteq G$. [i.e, $\mathrm{Ker}\,\phi$ is a normal subgroup of G]
(ii) ϕ is monomorph. ⇔ $\mathrm{Ker}\,\phi = \{e_G\}$.
(iii) if ϕ is epimorph, then ϕ is isomorph. ⇔ $\mathrm{Ker}\,\phi = \{e_G\}$

⑧ If ϕ is an isomorphism, then
(i) $o(a) = o(\phi(a))$, $\forall a \in G$. [isomorph preserves the order]
(ii) G & G' have the same cardinality.

⑨ ϕ isomorph. $\Rightarrow \phi^{-1}$ also isomorph.

⑩ $G \simeq G' \Rightarrow G' \simeq G$.

⑪ ϕ & ψ isomorph. $\Rightarrow \psi \circ \phi$ also isomorph...

⑫ Two finite cyclic ~~sub~~groups of the same order are isomorphic.

⑬ Two infinite cyclic groups are isomorphic.

⑭ A finite cyclic group of order $n \simeq (Z_n, \oplus_n)$.

⑮ Isomorphism Theorem:–
$\phi: G \to G'$ be an onto homomorphism and $H = \ker\phi$. Then $G/H \simeq G'$.

NOTE. An isomorphism preserves
(i) the commutative property of groups,
(ii) the cyclic " " ",
(iii) the order of the elements of groups.

Automorphism →

- An isomorphism from a group G onto itself is called an automorphism.
- The set of all automorphisms of G is denoted by $Aut(G)$.
- Theorem → $Aut(G)$ forms a group under the mapping composition.

PROOF → Let $\alpha, \beta, \gamma \in Aut(G)$. Then the maps $\alpha : G \to G$, $\beta : G \to G$, $\gamma : G \to G$ are all bijections.

$\alpha o \beta : G \to G$ is then a bijection.

$\Rightarrow \alpha o \beta$ is an automorphism, so $\alpha o \beta \in Aut(G)$.

$\therefore$ $Aut(G)$ is closed w.r.t. the composition of maps.

We have, $\alpha o(\beta o \gamma) = (\alpha o \beta) o \gamma$, as composition is associative.

$\therefore$ Associative property holds in $Aut(G)$.

The identity map $I_G : G \to G$ defined by

$I_G(a \circledast b) = a \circledast b$, $\forall a, b \in G$.

$= I_G(a) \circledast I_G(b)$. $\Rightarrow I_G$ is a homomorphism.

Also we have I_G is a bijection, and hence I_G is an automorphism $\in Aut(G)$.

For any $\alpha \in Aut(G)$, $\{I_G o \alpha\}(a) = I_G\{\alpha(a)\} = \alpha(a)$, $\forall a \in G$.

Also, $\{\alpha o I_G\}(a) = \alpha\{I_G(a)\} = \alpha(a)$, $\forall a \in G$.

$\Rightarrow I_G o \alpha = \alpha o I_G$, $\forall \alpha \in Aut(G)$.

$\therefore$ I_G is the identity element in $Aut(G)$.

For any $\alpha \in Aut(G)$, $\alpha : G \to G$ being a bijection, $\alpha^{-1} : G \to G$ exists and also a bijection.

Let $a, b, x, y \in G$ s.t. $\alpha(a) = x$, $\alpha(b) = y$; $\alpha^{-1}(x) = a$, $\alpha^{-1}(y) = b$.

NOTE: $\circledast$ is the b.c. of the group G

$$\boxed{\begin{aligned} &\alpha\circ\alpha^{-1}(x) = \alpha\{\alpha^{-1}(x)\} = \alpha(a) = x. \Rightarrow \alpha\circ\alpha^{-1} = I_G \\ &\alpha^{-1}\circ\alpha(a) = \alpha^{-1}(x) = a. \Rightarrow \alpha^{-1}\circ\alpha = I_G \end{aligned}}$$

Now $\alpha^{-1}(x \bullet y) = \alpha^{-1}\{\alpha(a)\bullet\alpha(b)\} = \alpha^{-1}\circ\{\alpha(a \circledast b)\}$, [$\because \alpha$ is a homo...]

$= (\alpha^{-1}\circ\alpha)(a\circledast b) = I_G(a\circledast b) \quad = a \bullet b = \alpha^{-1}(x)\bullet\alpha^{-1}(y)$.

$\Rightarrow$ α^{-1} is a homomorphism, also it being a bijection, α^{-1} is an automorphism, hence $\alpha^{-1} \in Aut(G)$.

$\therefore$ Inverse of any $\alpha \in Aut(G)$ exists in $Aut(G)$.

$\therefore$ $Aut(G)$ forms a group under the composition of mapping.

REMARK: (1) $Aut(G)$ is a non-abelian group, since $\alpha\circ\beta \neq \beta\circ\alpha$, in general.

(2) $Perm(G) \equiv$ the set of permutations on G.
$Aut(G) \leq Perm(G) \longrightarrow$ show it.
Let $\alpha, \beta \in Aut(G)$, then $\alpha\circ\beta^{-1} : G \to G$ exists and is a bijection.

Let $x, y \in G$. Then

$(\alpha\circ\beta^{-1})(x\circledast y) = \alpha\circ\{\beta^{-1}(x\circledast y)\} = \alpha\circ\{\beta^{-1}(x)\circledast\beta^{-1}(y)\}$, [$\because \beta^{-1}$ is a homomorphism]

$= \{(\alpha\circ\beta^{-1})(x)\}\circledast(\alpha\circ\beta^{-1})(y)$, [$\because \alpha$ is a homomorphism]

$\Rightarrow$ $\alpha\circ\beta^{-1}$ is a homomorphism, also it being a bijection, it is an automorphism.

$\therefore$ $\alpha\circ\beta^{-1} \in Aut(G)$ for $\alpha, \beta \in Aut(G)$.

Also, $Aut(G)$ is a non-empty subset of $Perm(G)$, as $I_G \in Aut(G)$, I_G is also called trivial automorphism.

$\therefore$ $Aut(G) \leq Perm(G)$.

Note: In general, there are many bijections which do not preserve the structure of the group.

Inner Automorphism →

An automorphism $I_g : G \to G$ defined by $I_g(x) = gxg^{-1}$, $x \in G$, is said to be an inner automorphism of G determined by g.

REMARK: It is also called the conjugation by g map.

☐ Prove that the conjugation by g map is an automorphism.

Proof: For $x, y \in G$, $I_g(xy) = g(xy)g^{-1} = gxg^{-1}gyg^{-1}$

$$= (gxg^{-1})(gyg^{-1})$$
$$= I_g(x) \circ I_g(y), \ \forall x, y \in G.$$

$\Rightarrow I_g$ is a homomorphism. $\longrightarrow$ (i)

Let $I_g(x) = I_g(y) \Rightarrow gxg^{-1} = gyg^{-1} \Rightarrow g^{-1}(gxg^{-1}) = g^{-1}(gyg^{-1})$

$$\Rightarrow xg^{-1} = yg^{-1} \Rightarrow x = y.$$

$\Rightarrow I_g$ is injective. $\longrightarrow$ (ii)

Let $I_g(x) = p \in G$. Then $gxg^{-1} = p$

$$\Rightarrow xg^{-1} = g^{-1}p \Rightarrow x = g^{-1}pg \in G.$$

$\therefore$ An arbitrary element $p \in G$ (codomain) has a pre-image $x (= g^{-1}pg)$ in G (domain).

$\Rightarrow I_g$ is surjective $\longrightarrow$ (iii)

From (i), (ii) & (iii), it follows that I_g is an automorphism

☐ Show that $I_g = I_G$ if $g \in Z(G)$.

If $g \in Z(G)$, then $gx = xg \ \forall x \in G$.

Now $I_g(x) = gxg^{-1} = xgg^{-1} = xe = x, \ \forall x \in G$.

$\Rightarrow$ $\underline{I_g = I_G}$, the identity automorphism.

- $Inn(G) \rightarrow$ denotes the set of all inner automorphisms of G.
- $Inn(G) \leq Aut(G) \leq Perm(G)$.
- $Inn(G) \trianglelefteq Aut(G)$.

To show: (i) $Inn(G) \leq Aut(G)$ (ii) $Inn(G) \trianglelefteq Aut(G)$.

(i) $I_e(x) = exe^{-1} = x$, $\forall x \in G$; $e \equiv$ identity of G.

$\Rightarrow I_e = I_G \in Inn(G)$.

$\Rightarrow Inn(G)$ is a non-empty subset of $Aut(G)$.

Let $I_{g_1}, I_{g_2} \in Inn(G)$. Then for $g_1, g_2 \in G$, we have

$$(I_{g_1} \circ I_{g_2})(x) = I_{g_1}(I_{g_2}(x)) = I_{g_1}(g_2 x g_2^{-1}) = g_1(g_2 x g_2^{-1})g_1^{-1}$$
$$= (g_1 g_2) x (g_1 g_2)^{-1} = I_{g_1 g_2}(x), \text{ where } g_1 g_2 \in G, \forall x \in G.$$

$\Rightarrow I_{g_1} \circ I_{g_2} \in Inn(G)$.

Now $(I_g \circ I_{g^{-1}})(x) = I_g(g^{-1} x g) = g(g^{-1} x g) g^{-1} = (gg^{-1}) x (gg^{-1})$.
$= exe^{-1} = I_e(x)$, $\forall x \in G$.

Also, $(I_{g^{-1}} \circ I_g)(x) = I_{g^{-1}}(g x g^{-1}) = g^{-1}(g x g^{-1}) g = exe^{-1} = I_e(x)$.

Hence $I_g \circ I_{g^{-1}} = I_{g^{-1}} \circ I_g = I_e$

$\Rightarrow I_{g^{-1}}$ is the inverse of I_g, and $I_{g^{-1}}(x) = g^{-1} x (g^{-1})^{-1} \in Inn(G)$ [since $g^{-1} \in G$].

Hence,

$I_{g_1} \circ I_{g_2} \in Inn(G)$ and $I_{g^{-1}} \in Inn(G)$.

$\Rightarrow$ $\underline{Inn(G) \leq Aut(G)}$. (proved)

(ii) Let $\alpha \in Aut(G)$, and $I_g \in Inn(G)$.

$$(\alpha \circ I_g \circ \alpha^{-1})(x) = \alpha \circ [I_g\{\alpha^{-1}(x)\}] = \alpha \circ [g \alpha^{-1}(x) g^{-1}]$$
$$= \alpha(g)\{\alpha \circ \alpha^{-1}(x)\}\alpha(g^{-1}) \quad [\because \alpha \text{ is a homomor.}]$$
$$= \alpha(g) I_G(x) \alpha(g^{-1}) = \alpha(g)\, x\, [\alpha(g)]^{-1}$$
$$= I_{\alpha(g)}(x), \ \forall x \in G.$$

$\therefore \alpha \circ I_g \circ \alpha^{-1} \in Inn(G)$, for all $\alpha \in Aut(G)$.

$\therefore$ $\underline{Inn(G) \trianglelefteq Aut(G)}$. (proved)

Another Approach to
Show that $Inn(G) \leq Aut(G)$.

<u>Proof</u>: $I_e(x) = e x e^{-1} = x, \ \forall x \in G$.

$\Rightarrow I_e = I_G \in Inn(G)$. $\Rightarrow Inn(G)$ is non-empty.

Let $I_{g_1}, I_{g_2} \in Inn(G)$, where $g_1, g_2 \in G$.

$$(I_{g_1} \circ I_{g_2})(x) = I_{g_1} \circ I_{g_2}(x) = I_{g_1}(g_2 x g_2^{-1})$$
$$= g_1 (g_2 x g_2^{-1}) g_1^{-1} = (g_1 g_2) x (g_1 g_2)^{-1}$$
$$= I_{g_1 g_2}(x), \ \forall x \in G, \ [\because g_1 g_2 \in G]$$

$$\Rightarrow I_{g_1} \circ I_{g_2} = I_{g_1 g_2} \in Inn(G).$$

Let $I_g \in Inn(G)$ for any $g \in G$.
I_g being a bijective map defined as
$I_g : G \to G$ by $I_g(x) = g x g^{-1}, \ x \in G$,
there exists a inverse map $I_g^{-1} : G \to G$.
Now let us assume $y \in G$ (codomain) s.t.

$$y = I_g(x) = g x g^{-1} \text{ for } x \in G \text{ (domain)}.$$
$$\Rightarrow x = g^{-1} y g \Rightarrow I_g^{-1}(y) = g^{-1} y g, \ y \in G \text{ (codomain)}$$

i.e., we can write $\exists$ a inverse map I_g^{-1} of I_g s.t. $I_g^{-1}(x) = g^{-1} x g, \ x \in G$ (codomain).
$$= I_{g^{-1}}(x), \ x \in G.$$

$$\therefore \ I_g^{-1} = I_{g^{-1}} \in Inn(G).$$

$$\therefore \ Inn(G) \leq Aut(G).$$

Theorem: G is an abelian group if and only if $I_g = I_G$, $\forall g \in G$.

Prove: Let G be abelian and $g \in G$.

Then $I_g(x) = gxg^{-1} = xgg^{-1} = xe = x$, $\forall x \in G$.

$\Rightarrow I_g = I_G$, $\forall g \in G$.

Conversely, let $I_g = I_G$, $\forall g \in G$

Then $I_g(x) = I_G(x)$, $\forall x \in G$

$\Rightarrow gxg^{-1} = x$, $\forall x \in G$, $\forall g \in G$.

$\Rightarrow (gxg^{-1})g = xg \Rightarrow gx = xg$, $\forall x, g \in G$.

$\Rightarrow$ G is abelian.

Cor: If G be a non-abelian group, then G has a non-trivial inner automorphism.

Because, as G is non-abelian, $\exists$ distinct $a, b \in G$ s.t. $ab \neq ba$

$\Rightarrow a \neq bab^{-1} = I_b(a)$

$\therefore I_b(a) \neq a \Rightarrow I_b \neq I_G$.

$\Rightarrow$ Inner automorphism I_b is not equal to the trivial automorphism I_G.

Theorem: $Inn(G) \simeq G/Z(G)$ (*) Donot use this proof. An alternative is in pg. 12.

Proof: Let us consider the map $\phi : G \to Inn(G)$ by $\phi(x) = I_x$ $\forall x \in G$.

We claim: ϕ is surjective. Because,

if $I_x(g) = y \in G$, then $xgx^{-1} = y \Rightarrow g = x^{-1}yx \in G$

i.e., y has a pre-image $g = x^{-1}yx$ in G.

To show: ϕ is a homomorphism.

Let $x, y \in G$. Then $\phi(xy) = I_{xy} = I_x \circ I_y = \phi(x)\phi(y)$.

[$\because I_{xy}$ is a homomorphism]

$\therefore \phi$ is an onto homomorphism.

[$I_{xy}(g) = (xy)g(xy)^{-1} = x(ygy^{-1})x^{-1} = I_x(ygy^{-1})$]

Determine $\operatorname{Ker}\phi$:

$x \in \operatorname{Ker}\phi \Leftrightarrow \phi(x) = I_e = I_G$ $\left[\because I_e(g) = ege^{-1} = g, \forall g \in G \Rightarrow I_e = I_G.\right]$

Remark:

Alternative proof of this theorem is noted in page No. 12.

$\Leftrightarrow I_x = I_e$

$\Leftrightarrow I_x(g) = I_e(g), \forall g \in G.$

$\Leftrightarrow xgx^{-1} = ege^{-1} = g$

$\Leftrightarrow xg = gx, \forall g \in G.$

$\Leftrightarrow x \in Z(G).$

$\therefore \operatorname{Ker}\phi = Z(G).$

$\therefore$ By the isomorphism theorem, we have

$$I_{nn}(G) \simeq G/Z(G).$$

Theorem: Let G be a group and the map $\alpha : G \to G$ is defined by $\alpha(x) = x^{-1}$, $x \in G$. Then α is an automorphism if and only if G is abelian.

Proof: Let α be an automorphism and $x, y \in G$.

Then $\alpha(xy) = \alpha(x)\alpha(y) \Rightarrow (xy)^{-1} = x^{-1}y^{-1}$, $[\because \alpha$ is a homo..$]$

$\Rightarrow [(xy)^{-1}]^{-1} = (x^{-1}y^{-1})^{-1}$

$\Rightarrow xy = yx, \forall x, y \in G.$

$\Rightarrow$ G is abelian.

Conversely, let G be abelian.

Then for $x, y \in G$, $\alpha(xy) = (xy)^{-1} = y^{-1}x^{-1}$

$= x^{-1}y^{-1}$ $[\because G$ is abelian$]$

$= \alpha(x)\alpha(y).$

$\therefore \alpha$ is a homomorphism.

Let $\alpha(x) = \alpha(y) \Rightarrow x^{-1} = y^{-1} \Rightarrow (x^{-1})^{-1} = (y^{-1})^{-1} \Rightarrow x = y.$

$\therefore \alpha$ is injective.

Let $y \in G$ be arbitrary s.t. $\alpha(x) = y \Rightarrow x^{-1} = y$

$\Rightarrow (x^{-1})^{-1} = y^{-1} \Rightarrow x = y^{-1} \in G.$

$\therefore y$ has a pre-image $(x=)y^{-1}$ in G.

$\therefore \alpha$ is surjective, and therefore α is an automor...

EXAMPLES OF AUTOMORPHISM : EX-15 (S.K. Mapa).

(i) Let $G=(\mathbb{C},+)$ and $\phi: G \to G$ is defined by $\phi(z)=\bar{z}$, $z \in \mathbb{C}$. Show that ϕ is an automorphism.

Let $z_1, z_2 \in \mathbb{C}$. Then $\phi(z_1 z_2) = \overline{z_1 z_2} = \bar{z}_1 \bar{z}_2 = \phi(z_1)\phi(z_2)$

$\Rightarrow \phi$ is a homomorphism.

Let $\phi(z_1)=\phi(z_2) \Rightarrow \bar{z}_1 = \bar{z}_2 \Rightarrow \bar{\bar{z}}_1 = \bar{\bar{z}}_2 \Rightarrow z_1 = z_2$

$\Rightarrow \phi$ is one-one.

Let $p \in \mathbb{C}$ be arbitrary s.t. $\phi(z)=p$,

$\Rightarrow \bar{z}=p \Rightarrow \bar{\bar{z}}=\bar{p}$

$\Rightarrow z=\bar{p} \in \mathbb{C}$.

$\therefore p$ has a pre-image $(z=)\ \bar{p}$ in $\mathbb{C}$.

$\Rightarrow \phi$ is onto.

$\therefore \phi$ is a homomorphism and a bijection, hence ϕ is an automorphism.

(ii) Let $G=\{1, i, -1, -i\}$ and $\phi: G \to G$ is defined by $\phi(x)=x^3$, $x \in G$. Examine if ϕ is an automor...

Let $x, y \in G$. Then $\phi(xy)=(xy)^3 = x^3 y^3 = \phi(x)\phi(y)$

$\Rightarrow \phi$ is a homomorphism.

Let $\phi(x)=\phi(y) \Rightarrow x^3=y^3 \Rightarrow x=y$ in G. [check!]

$\Rightarrow \phi$ is one-one.

ϕ is onto since each element of G has a pre-image in G.

$\therefore \phi$ is an automorphism.

(iii) Let $G=(\mathbb{Z}_6,+)$ and $\phi: G \to G$ is defined by $\phi(x)=2\bar{x}$, $\bar{x} \in \mathbb{Z}_6$. Examine if ϕ is an auto..

Let $\bar{x}, \bar{y} \in \mathbb{Z}_6$. Then $\phi(xy) = 2\overline{xy} = 2\bar{x}\bar{y} \neq \phi(x)\phi(y)$

$\Rightarrow \phi$ is not a homomorphism

$\therefore \phi$ is not an automorphism.

Check! ϕ is onto but not one-one. $\phi(\mathbb{Z}_6)=\{\bar{0},\bar{2},\bar{4}\}$

$\uparrow$ image set.

(iv) Let $G = (\mathbb{Z}_5, +)$ and $\phi : G \to G$ is defined by
$\phi(\bar{x}) = 2\bar{x}$, $\bar{x} \in \mathbb{Z}_5$.
Let $\bar{x}, \bar{y} \in \mathbb{Z}_5$. Then $\phi(\bar{x}\bar{y}) = 2\bar{x}\bar{y} = 2\bar{x}\,\bar{y} \neq \phi(\bar{x})\phi(\bar{y})$
$\Rightarrow \phi$ is not a homomorphism.
Image set $\phi(\mathbb{Z}_5) = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\} = \mathbb{Z}_5$.
ϕ is one-one and $\mathbb{Z}_5$ is a finite set, so
ϕ is onto also.
In any case, ϕ is <u>not</u> an automorphism

<u>16</u>. Let G be a commutative group of order n.
If $\gcd(m,n) = 1$, prove that the mapping
$\phi : G \to G$ defined by $\phi(x) = x^m$, $x \in G$ is
an automorphism.

Let $a, b \in G$, and $\phi(a) = \phi(b)$

$$\Rightarrow a^m = b^m \Rightarrow a^m b^{-m} = e$$
$$\Rightarrow (ab^{-1})^m = e \quad [\because G \text{ is commutative}]$$
$$\Rightarrow O(ab^{-1}) \mid m$$

Since $O(G) = n$ and $ab^{-1} \in G$, then
$O(ab^{-1}) \mid n$.
Since $\gcd(m,n) = 1$ and $O(ab^{-1}) \mid m$, $O(ab^{-1}) \mid n$,
then $O(ab^{-1}) = 1 \Rightarrow ab^{-1} = e \Rightarrow a = b$.

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

$\therefore \phi$ is injective.

Since G is a finite group of order n
and ϕ is injective $\Rightarrow \phi$ is surjective too.

$\therefore \phi$ is a <u>bijection</u>.

Now, $\phi(ab) = (ab)^m = a^m b^m \quad [\because G \text{ is commutative}]$
$= \phi(a)\phi(b) \Rightarrow \phi$ is a <u>homomorphism</u>

$\therefore \phi$ is an <u>automorphism</u>. (proved)

17. Let G be a group such that $Aut(G)=\{I_G\}$. Prove that G is a commutative group and $a^2=e$ for all $a\in G$.

Let $a,b\in G$. Then $ab = I_G(ab)$
$= I_G(a)\circ I_G(b)$ [$\because I_G$ is an homomorph.]
$= I_G(b)\circ I_G(a)$ [$\because Aut(G)=\{I_G\}$ is commutative]

Then $\Rightarrow$ $ab=ba$
$\Rightarrow$ G is commutative.

Now, $a^2 = a.a = I_G(a.a)$
$= I_G(a)\circ I_G(a)$ [$\because I_G$ is an automorph.]
$= I_G(a)\circ I_G^{-1}(a)$ [$\because I_G = I_G^{-1}$]
$= I_G(a)\circ I_G(a^{-1})$
$= I_G(a.a^{-1}) = I_G(e) = e$

$\therefore$ $a^2 = e \;\; \forall a\in G.$ (proved)

Remark: Here G is commutative and all non-identity element have order 2.

Examples:

① Let G be a cyclic group of order 12. Examine if the map $\phi: G\to G$ defined by $\phi(x)=x^3, x\in G$, is an automorphism.

Let $G=\langle a\rangle$. Then $O(a)=12$, as $O(G)=12$.

Now $O(\phi(a)) = O(a^3) = \dfrac{O(a)}{\gcd(3,12)} = \dfrac{12}{3} = 4.$

$\Rightarrow$ $O(a)\neq O(\phi(a))$, showing that ϕ does not preserve the order of elements.

So ϕ is not an isomorphism.

$\therefore$ ϕ is NOT an automorph.

(2) Let $G = S_3$. Examine if the map $\phi : G \to G$ defined by $\phi(x) = x^{-1}$, $x \in G$, is an automorph..

As S_3 is a non-abelian group, the map $\phi(x) = x^{-1}$ fails to be homomorphism.

$\therefore$ $\phi : S_3 \to S_3$ defined by $\phi(x) = x^{-1}$ can not be an automorphism.

(3) Let $G = \langle a \rangle$ and $O(G) = n$. Prove that $Aut(G)$ is a group of order $\phi(n)$, where $\phi(n)$ is the number of positive integers less than n and prime to n. [That is to prove: If $G = \langle a \rangle$ and $O(G) = n$, then $O(Aut(G)) = \phi(n)$]

Let $T : G \to G$ be an automorphism, $\in Aut(G)$.

Since a is a generator of G,

so $\phi(a)$ " " " " $\phi(G) = G$ here.

Now the generators of G are a^m, where $m < n$ and $\gcd(m, n) = 1$.

Let us take m s.t. $m < n$ and $\gcd(m,n) = 1$ and consider the map $T : G \to G$ defined by $T(x) = x^m$, $x \in G$.

T is a homomorphism, because for $x, y \in G$, $T(xy) = (xy)^m = x^m y^m$ [$\because G$ is abelian]

$= T(x)T(y)$.

$\ker T = \{x \in G : T(x) = e_G\}$

Now $x \in G \Rightarrow O(x) | n$; $T(x) = e_G \Rightarrow x^m = e_G$

$\Rightarrow O(x) | m$.

Since $\gcd(m,n) = 1$, $O(x)|m$, $O(x)|n$, $\Rightarrow O(x) = 1$.

$\Rightarrow x = e_G \Rightarrow \ker \phi = \{e_G\} \Rightarrow T$ is one-to-one.

Since G is finite, T is onto also.

$\therefore$ T becomes an automorphism.

$\therefore$ The number of automorph.. of $G = \underline{\phi(n)}$. (proved)

Ex: Let G be a finite group and ϕ be an automorphism of G such that for all $a \in G$, $\phi(a) = a$ iff $a = e$. Show that for all $g \in G$, there exists $a \in G$ s.t. $g = a^{-1}\phi(a)$.
Also deduce that G is commutative if $\phi^2 = i_G$.

Solution: Let $G = \{a_1, a_2, \cdots, a_n\}$ and
let $S = \{a_1^{-1}\phi(a_1), \cdots, a_n^{-1}\phi(a_n)\}$.
Then $S \subseteq G$, since $\phi: G \to G$ is an automorph.

Claim: the elements of S are distinct.

For, $a_i^{-1}\phi(a_i) = a_j^{-1}\phi(a_j)$

$\Leftrightarrow \phi(a_i)[\phi(a_j)]^{-1} = a_i a_j^{-1} \Leftrightarrow \phi(a_i a_j^{-1}) = a_i a_j^{-1}$ [$\because \phi$ is an automorph]

$\Leftrightarrow a_i a_j^{-1} = e$ [by the given condition]

$\Leftrightarrow a_i = a_j$, which is a contradiction.

$\therefore |S| = n$ and $S = G$.

Let $g \in G$. Then $g \in S$. $\Rightarrow$ $\underline{g = a^{-1}\phi(a)}$ for some $a \in G$. (proved)

2nd part: We have, for $g \in G$, $g = a^{-1}\phi(a)$ for some $a \in G$.

Then $g = i_G(g) = \phi^2[a^{-1}\phi(a)]$ by the given condition

$= \phi[\phi(a^{-1}\phi(a))] = \phi[\phi(a^{-1})\phi^2(a)]$

$= \phi[(\phi(a))^{-1} I_G(a)] = \phi[(\phi(a))^{-1} a]$

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

$\Rightarrow \phi(g) = \phi(\phi(g^{-1})) = \phi^2(g^{-1}) = I_G(g^{-1}) = g^{-1}, \forall g \in G.$

Let $a, b \in G$, then $(ab)^{-1} = \phi(ab) = \phi(a)\phi(b)$

$= a^{-1}b^{-1}$

$= (ba)^{-1}$

$\Rightarrow ab = ba$

$\Rightarrow G$ is commutative.

Lecture-11.4. (12) 8/9/2020.

Applications of factor groups to homomorphism group

Theorem :- $G/Z(G) \cong Inn(G)$.

Proof :- Let us consider the mapping

$T : G/Z(G) \longrightarrow Inn(G)$ by $T(gZ) = I_g$, $gZ \in G/Z(G)$

<u>T is well defined</u> and <u>one-to-one</u>. Because, for $gZ, hZ \in G/Z(G)$ and $gZ = hZ$, we have

$$\boxed{\begin{array}{l}\Rightarrow \text{well defined} \\ \Leftarrow \text{one-one.}\end{array}}$$

$$\begin{aligned}
&\Leftrightarrow g^{-1}h \in Z \; ; \; g, h \in G. \\
&\Leftrightarrow g^{-1}hx = xg^{-1}h ; x \in G \\
&\Leftrightarrow g(g^{-1}hx) = g(xg^{-1}h) \\
&\Leftrightarrow hx = (gxg^{-1})h \\
&\Leftrightarrow hxh^{-1} = gxg^{-1}. \\
&\Leftrightarrow I_h = I_g, \text{ or, } I_g = I_h. \\
&\Leftrightarrow T(gZ) = T(hZ).
\end{aligned}$$

<u>T is onto</u> : Because, let $I_g \in Inn(G)$.
Then $g \in G. \Rightarrow gZ \in G/Z(G)$,
such that $T(gZ) = I_g$.

<u>T is homomorphism</u>: Because,

$T(gZ * hZ) = T(ghZ)$, $[\because Z(G) = Z \trianglelefteq G]$.
$= I_{gh}$

Now $I_{gh}(x) = (gh)x(gh)^{-1} = ghxh^{-1}g^{-1}$

$= I_g(hxh^{-1}) = I_g \circ I_h(x) = (I_g \circ I_h)(x)$.

$\Rightarrow I_{gh} = I_g \circ I_h$.

$\therefore T(gZ * hZ) = T(ghZ) = I_{gh} = I_g \circ I_h$
$= T(gZ) \circ T(hZ)$.

$\therefore$ T is an isomorphism.

Hence $G/Z(G) \simeq Inn(G)$. (proved)

<u>Remark</u>: One application of the above theorem is noted down in the Example ⑤ page no. 11.

(4). If G be an infinite-cyclic group, prove that $O(\mathrm{Aut}(G)) = 2$.

Since G is an infinite cyclic group, $G \simeq (\mathbb{Z},+)$.

To determine all automorph.. of $(\mathbb{Z},+)$.

Let T be an automorph.. of $(\mathbb{Z},+)$.

Since $\mathbb{Z} = \langle 1 \rangle$, image group $\mathbb{Z} = \langle T(1) \rangle$.

As the only generators of $(\mathbb{Z},+)$ are 1 & -1,

$\therefore$ $T(1) = 1$, or -1.

If $T(1) = 1$, then $T(n) = T(\underbrace{1+1+\cdots+1}_{n \text{ term}}) = nT(1)$

$= n$, $n \in \mathbb{Z}$.

$\Rightarrow$ T is an identity automorph..

If $T(1) = -1$, then $T(n) = nT(1) = -n$, $n \in \mathbb{Z}$.

$\therefore$ $\underline{O(\mathrm{Aut}(G)) = 2}$. (proved)

(5). Find the number of $\mathrm{Inn}(S_3)$.

Since S_3 is an non-abelian group, its centre $Z(S_3)$ is a proper subgroup of S_3, and $S_3/Z(S_3)$ is a non-cyclic group.

Since $O(S_3) = 6$, $O(Z(S_3)) \mid 6$, but $O(Z(S_3)) \neq 6$.

If $O(Z(S_3)) = 2$, $O(S_3/Z(S_3)) = \dfrac{O(S_3)}{O(Z(S_3))} = \dfrac{6}{2} = 3$, a prime.

$\Rightarrow S_3/Z(S_3)$ is cyclic, a contradiction.

If $O(Z(S_3)) = 3$, $O(S_3/Z(S_3)) = \frac{6}{3} = 2$, a prime.

$\Rightarrow$ $S_3/Z(S_3)$ is cyclic, a contradiction

$\therefore$ $O(Z(S_3)) = 1$. Then $O(S_3/Z(S_3)) = O(S_3) = 6$.

~~$\Rightarrow O(S_3/Z(S_3)) \simeq S_3$~~.

Since $\mathrm{Inn}(S_3) \simeq O(S_3/Z(S_3))$, then $O(\mathrm{Inn}(S_3)) = \underline{6}$.

Ex. Determine the elements of Aut(Z_{10}).

Z_{10} forms a group w.r.t. addition mod 10, $\oplus_{10}$.
$(Z_{10}, \oplus_{10}) = \langle \bar{1} \rangle$. Other generators are:
$\bar{3}, \bar{7}, \& \bar{9}$ [integer < 10 & prime to 10].

Any automorphism of the group $(Z_{10}, \oplus_{10})$ will completely depend on where $\bar{1}$ is sent by the automorphism:

$$\left.\begin{aligned} \phi_{\bar{1}} &: \bar{1} \to \bar{1} \\ &: \bar{2} \to \bar{2} \\ &\;\;\vdots \\ &: \bar{9} \to \bar{9} \end{aligned}\right\} \text{identity automorph.}$$

$$\left.\begin{aligned} \phi_{\bar{3}} &: \bar{1} \to \bar{3} \\ &: \bar{2} \to \bar{6} \\ &: \bar{3} \to \bar{9} \\ &: \bar{4} \to \bar{2} \\ &: \bar{5} \to \bar{5} \\ &: \bar{6} \to \bar{8} \\ &: \bar{7} \to \bar{1} \\ &: \bar{8} \to \bar{4} \\ &: \bar{9} \to \bar{7} \\ &: \bar{0} \to \bar{0} \end{aligned}\right\}$$

[because, generator has to go to generator]

Similarly,
$\phi_{\bar{7}} : \bar{1} \to \bar{7}$, $\phi_{\bar{9}} : \bar{1} \to \bar{9}$

$\therefore$ The only possible automorphisms in the group $(Z_{n}, \oplus_{10})$ are $\phi_{\bar{1}}, \phi_{\bar{3}}, \phi_{\bar{7}}; \phi_{\bar{9}}$

$\therefore$ Aut$(Z_n) = \{\phi_{\bar{1}}, \phi_{\bar{3}}, \phi_{\bar{7}}, \phi_{\bar{9}}\}$.

Infact, the formula for finding the automorphism for the group $(Z_n, \oplus_{10})$ is as follows:

$$\left.\begin{aligned} \phi_{\bar{1}}(\bar{K}) &= \bar{K}, \quad \bar{K} \in Z_n \\ \phi_{\bar{3}}(\bar{K}) &= \bar{3}K \\ \phi_{\bar{7}}(\bar{K}) &= \bar{7}.K \\ \phi_{\bar{9}}(\bar{K}) &= \bar{9}.K \end{aligned}\right\}$$

Because, as for example,

$\phi_{\bar{3}}(\bar{1}) = \bar{3}$, $\phi_{\bar{3}}(\bar{2}) = \phi_{\bar{3}}(\bar{1}) + \phi_{\bar{3}}(\bar{1})$
$= \bar{3} + \bar{3}$
$= 2 . \bar{3}$

$\phi_{\bar{3}}(\bar{3}) = \bar{3} + \bar{3} + \bar{3}$
$= 3 . \bar{3}$

$\phi_{\bar{3}}(\bar{K}) = \underbrace{\bar{3} + \cdots + \bar{3}}_{K \text{ times}}$
$= K \cdot \bar{3}$

Automorphism Group [Aut(G)] of infinite cyclic group

<u>Prob</u>: If G is an infinite cyclic group find $Aut(G)$.

<u>Solution</u>: Let $G = \langle a \rangle = \{a^i \mid i \in Z\}$ be an infinite cyclic group.

Let $T \in Aut(G)$.

$\therefore$ $T : G \to G$ is 1-1, onto, homomorphism

Let $a \in G \Rightarrow T(a) \in G = \langle a \rangle$

$\Rightarrow T(a) = a^m$ for some $m \in Z$.

Since T is onto, so for $a \in G$, $\exists$ $x \in G$

s.t. $T(x) = a$

where $x \in G \Rightarrow x = a^n$, for some $n \in Z$

Now $a = T(x) = T(a^n)$

$= \{T(a)\}^n$, since T is homomorph

$= (a^m)^n = a^{mn}$

$\Rightarrow a^{mn-1} = e \Rightarrow mn - 1 = 0$

$\Rightarrow mn = 1$

$\Rightarrow m = +1$ or -1

$\therefore$ $T(a) = a$ or $T(a) = a^{-1}$

$Aut(G) = \{I_G, T(a) = a^{-1}\}$

$O(Aut(G)) = 2$

$\Rightarrow$ <u>$Aut(G)$ is cyclic & $\simeq Z_2$.</u>

<u>Eg</u>: $G = (Z, +)$ is an infinite cyclic group.

<u>$Aut(Z) \simeq Z_2$</u> .

Lecture # 6 on 1?/04/2020.

Prob: Show that $Aut(\mathbb{Z}_n) \simeq U_n$, for each $n \in \mathbb{Z}^+$.

Solution: Let us define a map $T: Aut(\mathbb{Z}_n) \to (U_n, \odot_n)$ by $T(\phi) = \phi(\bar{1})$, $\forall\, \phi \in Aut(\mathbb{Z}_n)$.

Now for a +ve integer m,

$$m\phi(\bar{1}) = \underbrace{\phi(\bar{1}) + \cdots + \phi(\bar{1})}_{(m \text{ times})} = \phi(\bar{1} + \bar{1} + \cdots + \bar{1}), \text{ since } \phi \text{ is homomorph.}$$
$$= \phi(m\cdot\bar{1}) = \phi(\bar{m}).$$

Now $\phi(\bar{m}) = \bar{0}$ if and only if $n | m$.

$\Rightarrow$ $O(\phi(\bar{1})) = n$, where $\phi(\bar{1})$ is a generator of the group $(\mathbb{Z}_n, \oplus_n)$, as an automorphism of $\mathbb{Z}_n$ must sent generator of $\mathbb{Z}_n$ to generators of $\mathbb{Z}_n$.

Note: Isomorphisms preserve the order of elements so an element of order n must be sent to an element of order n;
i.e., the generator of $\mathbb{Z}_n$ must be sent to another generator of $\mathbb{Z}_n$.

Now $O(\phi(\bar{1})) = n \Rightarrow \phi(\bar{1}) \in U_n$ [or $U(n)$], since $\phi(\bar{1})$ is a generator of $(\mathbb{Z}_n, \oplus_5) \Leftrightarrow \phi(\bar{1}) \in U_n$.

$\therefore$ $T(\phi) = \phi(\bar{1})$, where $\phi(\bar{1}) \in U_n$.

$\Rightarrow$ T is well-defined.

To prove: T is homomorphism,

Let us take $\phi, f \in Aut(\mathbb{Z}_n)$.

Then $T(\phi \circ f) = (\phi \circ f)(\bar{1}) = \phi(f(\bar{1}))$
$= \phi(\bar{K})$, where let $f(\bar{1}) = \bar{K} \in \mathbb{Z}_n$

$$\Rightarrow T(\phi \circ f) = \phi(\underbrace{\bar{1} + \bar{1} + \cdots + \bar{1}}_{(K \text{ factors})}) = \phi(\bar{1}) + \cdots + \phi(\bar{1})$$
$$= K\cdot\phi(\bar{1}) = K\cdot\bar{1}\,\phi(\bar{1}) \quad [\because \bar{1} \in U_n \text{ is the identity element}]$$
$$= \bar{K}\,\phi(\bar{1}) = f(\bar{1}) \odot_n \phi(\bar{1}), \quad [f(\bar{1}) \in U_n \text{ also}]$$
$$= \phi(\bar{1}) \odot_n f(\bar{1}) \quad [\because (U_n, \odot_n) \text{ is a commutative group}]$$
$$= T(\phi) \odot_n T(f), \ \forall\, \phi, f \in Aut(\mathbb{Z}_n).$$

$\Rightarrow$ T is a homomorphism.

To prove: T is one-one.

$$\text{Ker}\, T = \{\phi \in \text{Aut}(Z_n) : T(\phi) = \bar{1}\}$$
$$= \{\phi \in \text{Aut}(Z_n) : \phi(\bar{1}) = \bar{1}\}$$
$$= \{\phi = I_G, \text{ the identity automorph}, G = Z_n\}.$$

$\Rightarrow T$ is a monomorphism

To prove: T is onto. Let $\bar{t} \in U_n$. Then $\gcd(t,n)=1$.

First, to show $\exists$ a map $\phi : Z_n \to Z_n$ defined by $\phi(\bar{m}) = \overline{mt}$, $\forall\, \bar{m} \in Z_n$, such that $\phi \in \text{Aut}(Z_n)$.

Let $\bar{r}, \bar{s} \in Z_n$ s.t. $\bar{r} = \bar{s}$

$$\Leftrightarrow r - s = nq, \text{ for some } q \in Z.$$
$$\Leftrightarrow rt - st = nqt$$
$$\Leftrightarrow \overline{rt} = \overline{st}$$
$$\Leftrightarrow \phi(\bar{r}) = \phi(\bar{s})$$

This proves, ϕ is one-one $\Leftrightarrow$ ϕ is well-defined

To show: ϕ is onto.

Let $\bar{r} \in Z_n$. Since $\gcd(t,n) = 1$, $\exists\, p, q \in Z$ s.t. $1 = tp + nq$

$$\Rightarrow r = tpr + nqr$$
$$\Rightarrow \bar{r} = \overline{prt} + \overline{nqr}$$
$$= \overline{(pr)t} + \bar{0}$$
$$\Rightarrow \bar{r} = \overline{(pr)t}$$

$\therefore \overline{(pr)t} = \bar{r} \in Z_n$ (domain)

$\therefore$ for any $\bar{r} \in Z_n$ (codomain), $\exists\, \overline{(pr)t} \in Z_n$ (domain)

$\Rightarrow \phi$ is onto.

To show now: ϕ is homomorphism

Let $\bar{p}, \bar{q} \in Z_n$, $\phi(\bar{p} \oplus_n \bar{q}) = \overline{(p+q)t} = \overline{pt} \oplus_n \overline{qt}$
$$= \phi(\bar{p}) \oplus_n \phi(\bar{q})$$

$\Rightarrow \phi$ is a homomorphism.

$\therefore \phi$ is an automorphism and so $\phi \in \text{Aut}(Z_n)$.

To show: T is onto. $T(\phi) = \phi(\bar{1}) = \overline{1 \cdot t} = \bar{t} \in U_n$.

$\therefore T : \text{Aut}(Z_n) \to (U_n, \odot_n)$ is an isomorphism. (proved) [illegible] Lecture [illegible]   [illegible]-2020

Characteristic Subgroup:

1. Let G be a group and H be its subgroup $[H \leq G]$. If $\phi \in Aut(G)$ and $\phi(H) = \{\phi(h) : h \in H\}$, then show that $\phi(H) \leq G$.

$\phi(H)$ is a non-empty subset of G, since $e \in H$, $\phi(e) = e\ (\in G) \in \phi(H)$.

Let $a, b \in \phi(H)$. So that $a = \phi(h_1)$, $b = \phi(h_2)$; for some $h_1, h_2 \in H$.

Now $ab^{-1} = \phi(h_1)[\phi(h_2)]^{-1} = \phi(h_1)\phi(h_2^{-1})$, [$\because \phi$ is a homomorphism]

$= \phi(h_1 h_2^{-1})$, since ϕ is a homomorph.

$\in \phi(H)$, since $H \leq G$, $h_1, h_2 \in H \Rightarrow h_1 h_2^{-1} \in H$.

$\therefore$ $\phi(H) \leq G$.

2. Let G be a group and N be a normal subgroup of G $[N \triangleright G]$. Show that $\phi(N) \triangleright G$, ϕ being an automorphism of G.

By 1, we have $\phi(N) \leq G$.

To prove: $\phi(N)$ is normal in G.

Let us take $g \in G$ and $a \in \phi(N)$ s.t. $a = \phi(n)$, $n \in N$, and $g = \phi(g_1)$ for $g_1 \in G$. [$\because \phi : G \to G$]

$\therefore$ $gag^{-1} = \phi(g_1)\phi(n)[\phi(g_1)]^{-1} = \phi(g_1)\phi(n)\phi(g_1^{-1})$

$= \phi(g_1 n g_1^{-1}) \in \phi(N)$, since $N \triangleright G$, $g_1 n g_1^{-1} \in N$.

$\Rightarrow$ $\phi(N) \triangleright G$

Definition $\longrightarrow$ A subgroup C of G is said to be a characteristic subgroup of G, if $\phi(C) \subset C$, $\forall\, \phi \in Aut(G)$.

Note: char. subgroup is mapped into itself by every automorphism of the group, as $\phi(C) \subset C$.

[illegible]: A characteristic subgroup of G must be a normal subgroup of G.

<u>BUT</u>, the converse is NOT true.

For some $g \in G$, let us define an inner automorphism $\phi_g : G \to G$ by $\phi_g(x) = gxg^{-1}$, $x \in G$.

By the definition of the char. subgroup C of G, we have $\phi(C) \subset C$, $\forall \phi \in \mathrm{Aut}(G)$.

$\therefore \quad \phi_g(C) \subset C, \ \forall g \in G$, as $\phi_g \in \mathrm{Aut}(G)$.

$\Rightarrow gag^{-1} \in C, \ \forall g \in G, \ \forall a \in C$.

$\Rightarrow \underline{C \triangleright G}$.

<u>Note</u>: Every char. subgroup of G is normal, because every conjugation map is an inner automorphism.

<u>Converse Part</u>:

<u>Example</u>: For Klein's 4-group, $G = \{e, a, b, ab\}$ with $a^2 = e$, $b^2 = e$ and $ab = ba$. $O(a) = O(b) = O(ab) = 2$

Let us take a subgroup $C = \{e, a\}$ of G, and
$\phi = \begin{pmatrix} e & a & b & ab \\ e & b & a & ab \end{pmatrix}$ where ϕ is an automorphism of G.

$C = \{e, a\}$ is normal in G, because $\forall g \in G$, $gCg^{-1} \subset C$. (<u>Verify it</u>). Since G is abelian, every subgroup of G is normal.

But $\phi(C) = \{\phi(e), \phi(a)\} = \{e, b\} \not\subset C$

$\Rightarrow \phi(C)$ is <u>not a char. subgroup</u> of G, <u>though</u> $\underline{C \triangleright G}$.

<u>Remark</u>: Determine $\mathrm{Aut}(G)$, G being Klein's 4-group.

$\mathrm{Aut}(G) = \left\{ \begin{pmatrix} e & a & b & ab \\ e & a & b & ab \end{pmatrix}, \begin{pmatrix} e & a & b & ab \\ e & a & ab & b \end{pmatrix}, \begin{pmatrix} e & a & b & ab \\ e & b & a & ab \end{pmatrix}, \begin{pmatrix} e & a & b & ab \\ e & b & ab & a \end{pmatrix}, \begin{pmatrix} e & a & b & ab \\ e & ab & a & b \end{pmatrix}, \begin{pmatrix} e & a & b & ab \\ e & ab & b & a \end{pmatrix} \right\}$. $\underline{|\mathrm{Aut}(G)| = 6}$.

Since $O(a) = O(b) = O(ab) = 2$, $O(e) = 1$, $O(\phi(a)) = O(\phi(b)) = O(\phi(ab)) = 2$.

[illegible] 3! [illegible]

Examples:

(1) $Z(G)$, the centre of a group G is a char. subgroup of G.

To prove: $\phi(Z) \subset Z$, where $Z = Z(G)$, $\phi \in Aut(G)$.

Let $x \in Z(G)$. $\Rightarrow xg = gx$, $\forall g \in G$.

Since ϕ is one-one $\Rightarrow \phi(xg) = \phi(gx)$

" ϕ is homomorph $\Rightarrow \phi(x)\phi(g) = \phi(g)\phi(x)$

For $x \in Z$, $\exists z \in \phi(Z)$ s.t. $\phi(x) = z$. $\Bigg\} \Rightarrow z\phi(g) = \phi(g)z$, $\forall g \in G$.

Since ϕ is onto $\Rightarrow zg' = g'z$, $\forall g' \in G$. $[\underset{\in G}{g' = \phi(g)}]$

$\Rightarrow z \in Z(G)$.

$\therefore$ $z \in \phi(Z) \Rightarrow z \in Z$

$\therefore$ $\underline{\phi(Z) \subset Z}$.

(2) Every subgroup of a cyclic group is characteristic.

Let $G = \langle a \rangle = \{a^n : n \in \mathbb{Z}\}$ and $C \leq G$

s.t. $C = \langle a^m \rangle$.

Let $z \in \phi(C) = \{\phi(x) : x \in C\}$, so that $x = (a^m)^q, q \in \mathbb{Z}$

Then $z = \phi(x) = \phi\{(a^m)^q\} = \phi(a^{mq}) = [\phi(a)]^{mq}$

$= [\{\phi(a)\}^q]^m = (a^p)^m$, since $G = \langle \phi(a) \rangle$, then $\{\phi(a)\}^q = a^p$ for some $p \in \mathbb{Z}$.

$= (a^m)^p \in C$.

$\therefore$ $z \in \phi(C) \Rightarrow z \in C$.

$\therefore$ $\underline{\phi(C) \subset C} \Rightarrow C$ is a char. subgroup of G.

Commutator Subgroup :

<u>Commutator</u> : An element of the group G which is of the form $ghg^{-1}h^{-1}$, for some $g, h \in G$, is called a commutator, $[g,h]$.

The identity element e is always a commutator and it is the only commutator if and only if G is abelian.

For, $e = [e,e] = eee^{-1}e^{-1} \Rightarrow e$ is a commutator.

Now if $ghg^{-1}h^{-1} = e$, then $\Leftrightarrow gh(hg)^{-1} = e$

$\Leftrightarrow gh = e(hg) = hg$, for $g, h \in G$

$\Leftrightarrow$ <u>G is abelian</u>.

Definition: The subgroup of a group G that is generated by all the commutators of the group, is called the <u>commutator subgroup</u>, denoted by $[G,G]$, defined by

$$G' = [G,G] = \langle ghg^{-1}h^{-1} : g, h \in G \rangle.$$

<u>REMARK</u>: This subgroup is important because it is the smallest normal subgroup of G s.t. the quotient group G/G' is abelian.

⊛ In some sense it provides a measure of how far the group is from being abelian; the larger the normal subgroup is, the "less abelian" the group is.

⊛ If G is abelian, then $ghg^{-1}h^{-1} = e$ for $\forall g, h \in G$.

$\Rightarrow G' = [G,G] = \{e\}$.

$\therefore$ Quotient group $G/G' (= G)$, which is abelian.

We define the commutator subgroup $[G,G]$ as:
$[G,G] = \{x_1 x_2 \cdots x_n \mid n \geq 1\}$, where each x_i is a commutator in G; i.e., $x_i = [a_i, b_i]$, $\forall i = 1, 2, \cdots, n$.
<u>i.e.</u>, $[G,G]$ is the collection of all finite products of commutators in G.
Also, $[G,G]$ is the subgroup generated by all the commutators in G. So for each $c \in [G,G]$, we have $c = x_1 x_2 \cdots x_n$.

To Prove $[G,G]$ is a normal subgroup of G.
First to show that $[G,G]$ is a subgroup of G.
$e = e e e^{-1} e^{-1} \in [G,G]$
$\Rightarrow [G,G]$ is a non-empty subset of G.
Let us take $c, d \in [G,G]$ such that
$c = x_1 x_2 \cdots x_n$; $d = y_1 y_2 \cdots y_m$; where each x_i and each y_i is a commutator in G.
Now $cd = x_1 x_2 \cdots x_n y_1 y_2 \cdots y_m \in [G,G]$.
$c^{-1} = (x_1 x_2 \cdots x_n)^{-1} = x_n^{-1} x_{n-1}^{-1} \cdots x_2^{-1} x_1^{-1}$
If $x_i = [a_i, b_i] = a_i b_i a_i^{-1} b_i^{-1}$, then
$x_i^{-1} = (a_i b_i a_i^{-1} b_i^{-1})^{-1} = b_i a_i b_i^{-1} a_i^{-1} = [b_i, a_i]$, which is also a commutator ~~and hence~~ $\cancel{x_i^{-1} \in [G,G]\ \forall i}$.
is also finite products of commutators in G.
$\therefore$ c^{-1} is also finite products of commutators in G.
$\therefore$ $c \in [G,G] \Rightarrow c^{-1} \in [G,G]$.
$\therefore$ $[G,G]$ is a subgroup of G.
Next to show that $[G,G]$ is normal in G.
Let $g \in G$. $gcg^{-1} = g x_1 x_2 \cdots x_n g^{-1}$
$$= g x_1 (g^{-1} g) x_2 (g^{-1} g) \cdots (g^{-1} g) x_n g^{-1}$$
$$= (g x_1 g^{-1})(g x_2 g^{-1}) \cdots (g x_n g^{-1})$$
If $x_i = a_i b_i a_i^{-1} b_i^{-1}$, then $g x_i g^{-1} = g a_i b_i a_i^{-1} b_i^{-1} g^{-1}$
$$= g a_i (g^{-1} g) b_i (g^{-1} g) a_i^{-1} (g^{-1} g) b_i^{-1} g^{-1}$$
$$= (g a_i g^{-1})(g b_i g^{-1})(g a_i^{-1} g^{-1})(g b_i^{-1} g^{-1})$$
$$= (g a_i g^{-1})(g b_i g^{-1})(g a_i g^{-1})^{-1}(g b_i g^{-1})^{-1}$$

$\therefore\ g x_i g^{-1} = [g a_i g^{-1}, g b_i g^{-1}],\ \forall i = 1, 2, \ldots, n.$

So $g c g^{-1} = [g a_1 g^{-1}, g b_1 g^{-1}][g a_2 g^{-1}, g b_2 g^{-1}] \cdots [g a_n g^{-1}, g b_n g^{-1}]$.
$\in [G, G]$.

$\therefore\ \underline{[G,G] \trianglelefteq G}$. (proved)

To prove that a commutator subgroup is a characteristic subgroup of a group G.

Let C be a characteristic subgroup of G and $[G,G]$ " " commutator " " G.

To show that $\phi([G,G]) \subset [G,G],\ \forall \phi \in \mathrm{Aut}(G)$.

Let $[G,G] = \langle x y x^{-1} y^{-1} \mid x, y \in G \rangle$. Then for some $c \in [G,G]$, we have, $c = \prod_{1 \le i \le n} x_i = \prod_{1 \le i \le n} [a_i, b_i]$

$$= \prod_{1 \le i \le n} a_i b_i a_i^{-1} b_i^{-1}$$

If $\phi \in \mathrm{Aut}(G)$, then $\phi(c) = \phi\left(\prod_{1 \le i \le n} a_i b_i a_i^{-1} b_i^{-1}\right)$

$$= \prod_{1 \le i \le n} \phi(a_i b_i a_i^{-1} b_i^{-1})$$

$$= \prod_{1 \le i \le n} \phi(a_i) \phi(b_i) \phi(a_i^{-1}) \phi(b_i^{-1})$$

$$= \prod_{1 \le i \le n} \phi(a_i) \phi(b_i) (\phi(a_i))^{-1} (\phi(b_i))^{-1}$$

$$= \prod_{1 \le i \le n} [\phi(a_i), \phi(b_i)]$$

$\therefore\ \phi(c) \in [G,G],\ \forall c \in [G,G],\ \forall \phi \in \mathrm{Aut}(G)$.

Thus $\phi([G,G]) \subset [G,G]$.

$\Rightarrow$ $[G,G]$ is a characteristic subgroup of G. (proved)