Generalised Cayley's Theorem.

Statement: Every group G is isomorphic to a subgroup of the group of all permutations on G, $A(G)$.

Proof: G is a G-set, where the group action of G on G is defined by the group operation.

Let $g \in G$, and let us define $T_g : G \to G$ by

$T_g(a) = ga, \ \forall a \in G$.

Let $a, b \in G$. Then $T_g(a) = T_g(b) \Leftrightarrow ga = gb$

$\Leftrightarrow a = b$ [by left cancellation law]

$\therefore T_g$ is well defined ($\Leftarrow$) & one-one ($\Rightarrow$).

Also, $b = g(g^{-1}b) = T_g(g^{-1}b)$, $g^{-1}b \in G$ (domain).

$\therefore$ For $b \in G$ (co-domain), $\exists\, g^{-1}b \in G$ (domain) s.t.

$$T_g(g^{-1}b) = b.$$

$\Rightarrow T_g$ is onto.

$\therefore T_g$ is a bijection & hence $T_g \in A(G)$.

Let $g_1, g_2 \in G$. Then $T_{g_1g_2}(a) = (g_1g_2)a = g_1(g_2a)$

$= T_{g_1}(g_2a) = T_{g_1}(T_{g_2}(a))$

$= (T_{g_1} \circ T_{g_2})(a), \ \forall a \in G$

$$\Rightarrow T_{g_1g_2} = T_{g_1} \circ T_{g_2}.$$

Let us define $\phi : G \to A(G)$ by

$$\phi(g) = T_g, \ \forall g \in G.$$

Let $g, h \in G$ s.t. $g = h$

$\Rightarrow ga = ha, \ \forall a \in G$.

$\Rightarrow T_g(a) = T_h(a) \Rightarrow T_g = T_h$

$\Rightarrow \phi(g) = \phi(h) \Rightarrow \phi$ is well-defined

Now for $g_1, g_2 \in G$,

$\phi(g_1g_2) = T_{g_1g_2} = T_{g_1} \circ T_{g_2} = \phi(g_1) \circ \phi(g_2), \ \forall g_1, g_2 \in G$

$\Rightarrow \phi$ is a homomorphism

$\therefore$ This group action induces a homomorphism $\phi : G \to A(G)$.

Now $\ker \phi = \{g \in G : \phi(g) = T_g = \text{identity permutation on } G\}$

$= \{g \in G : T_g(a) = a, \forall a \in G\}$

$= \{g \in G : ga = a, \forall a \in G\}$

$= \{g \in G : g = aa^{-1} = e\} = \{e\}$.

$\therefore$ ϕ is a monomorphism.

Finally, ϕ is onto, because each element of $A(G)$ is of the form T_g for some $g \in G$; and since $T_g = \phi(g)$, the pre-image of T_g is g in G.

$\therefore$ ϕ is an isomorphism.

Since $\phi(G) \leq A(G)$, hence $G \simeq \phi(G)$.

$\therefore$ $G \simeq$ a subgroup of $A(G)$. (proved).

<u>Theorem</u>: Let G be a group and $H \leq G$. Let $S = \{aH \mid a \in G\}$. Then prove that there exists a homomorphism $\psi : G \to A(S)$ (the group of all permutations on S) such that $\ker \psi \subseteq H$.

<u>Proof</u>: Here S is a G-set, where the group action $(\therefore G \times S \to S)$ of G on S is defined by $g \cdot aH = (ga)H$, $\forall g \in G$.

Verify: $e \cdot aH = (ea)H = aH$; $(g_1 g_2) \cdot aH = (g_1 g_2 a)H = g_1 \cdot (g_2 a)H = g_1 \cdot [g_2 \cdot aH]$.

<u>To prove</u>: this group action induces a homomorphism $\psi : G \to A(S)$.

Let $g \in G$ and let us define $T_g : S \to S$ by $T_g(aH) = (ga)H$, $\forall aH \in S$.

Let $aH, bH \in S$. Then $T_g(aH) = T_g(bH) \Leftrightarrow (ga)H = (gb)H$

$\Leftrightarrow (ga)^{-1}(gb) \in H \Leftrightarrow (a^{-1}g^{-1})(gb) \in H$

$\Leftrightarrow a^{-1}(g^{-1}g)b \in H \Leftrightarrow a^{-1}b \in H$

$\Leftrightarrow aH = bH$; $a, b \in G$.

$\therefore$ T_g is one-one.

Now for $(ga)H \in S$ (codomain), $\exists\, aH \in S$ (domain) s.t. $T_g(aH) = (ga)H \Rightarrow T_g$ is onto

$\boxed{\text{Alternatively, } \underline{T_g \text{ onto}}: \text{ For } xH \in S,\ x \in G,\ xH = (g(g^{-1}x))H = T_g((g^{-1}x)H)}$

$\therefore$ T_g is a bijection & hence $T_g \in A(S)$.

Let $g_1, g_2 \in G$. Then $T_{g_1 g_2}(aH) = (g_1 g_2 a)H$, $\forall aH \in S$:

$$= (g_1(g_2 a))H = T_{g_1}((g_2 a)H)$$
$$= T_{g_1}(T_{g_2}(aH)), \ \forall aH \in S, a \in G.$$
$$= (T_{g_1} \circ T_{g_2})(aH).$$

$\therefore T_{g_1 g_2} = T_{g_1} \circ T_{g_2}$.

Let us define $\psi : G \to A(S)$ by $\psi(g) = T_g$, $\forall g \in G$.

Let $g_1, g_2 \in G$ s.t. $g_1 = g_2$. Then for $a \in G \Rightarrow g_1 a = g_2 a$.

$$\Rightarrow (g_1 a)^{-1}(g_2 a) = e \in H \quad [\because H \leq G]$$
$$\Rightarrow (g_1 a)H = (g_2 a)H$$
$$\Rightarrow T_{g_1}(aH) = T_{g_2}(aH), \ \forall aH \in S.$$
$$\Rightarrow T_{g_1} = T_{g_2} \Rightarrow \psi(g_1) = \psi(g_2), \ \forall g_1, g_2 \in G.$$

$\therefore \psi$ is a well-defined function.

Now $\psi(g_1 g_2) = T_{g_1 g_2} = T_{g_1} \circ T_{g_2} = \psi(g_1) \circ \psi(g_2)$, $\forall g_1, g_2 \in G$.

$\therefore \psi : G \to A(S)$ is a homomorphism

Now $\operatorname{Ker}\psi = \{g \in G : \psi(g) = T_g \equiv \text{the identity map on } S\}$.

$$= \{g \in G : T_g(aH) = aH, \ \forall aH \in S\}$$
$$= \{g \in G : (ga)H = aH, \ \forall aH \in S\}$$

In particular, when $a = e$, $(ga)H = aH \Rightarrow (ge)H = eH$

$$\Rightarrow gH = H \Rightarrow g \in H.$$

$\therefore$ If $g \in \operatorname{Ker}\psi$, then $\Rightarrow g \in H$.

$\therefore$ $\underline{\operatorname{Ker}\psi \subseteq H}$. (proved)