Cayley's Theorem

Definition

Let G be a group and $g \in G$. Define $L_g : G \to G$ by:

$$L_g(x) = gx$$

Lemma

Let G be a group and $g \in G$:

L_g is a permutation of G

Proof

Assume $L_g(x) = L_g(y)$
$gx = gy$
$x = y$
$\therefore L_g$ is one-to-one.

Assume $y \in G$
$g^{-1} \in G$
Let $x \in G, g^{-1}x = y$
$L_g(x) = g(g^{-1}y) = (gg^{-1})y = ey = y$
$\therefore L_g$ is onto.

$\therefore L_g$ is a bijection, and thus a permutation of G.

Lemma

Let G be a group and $G' = \{L_g \mid g \in G\}$:

$$\forall\, L_{g_1}, L_{g_2} \in G', L_{g_1}L_{g_2} = L_{g_1g_2}$$

Proof

Assume $L_{g_1}, L_{g_2} \in G'$
Assume $x \in G$
$(L_{g_1}L_{g_2})(x) = L_{g_1}(L_{g_2}(x)) = L_{g_1}(g_2x) = g_1(g_2x) = (g_1g_2)x = L_{g_1g_2}(x)$

Lemma

Let G be a group and $G' = \{L_g \mid g \in G\}$:

G' is a group

Proof

Assume $L_{g_1}, L_{g_2} \in G'$
$g_1, g_2 \in G$

$L_{g_1}L_{g_2} = L_{g_1g_2}$
But by closure, $g_1g_2 \in G$
$L_{g_1g_2} \in G'$
$\therefore G'$ is closed under the operation.

Composition is associative
$\therefore G'$ is associative under the operation.

Let e be the identity element for G
Assume $g \in G$
$L_eL_g = L_{eg} = L_g$
$L_gL_e = L_{ge} = L_g$
$\therefore L_e$ is an identity for G'.

Assume $g \in G$
$g^{-1} \in G$
$L_{g^{-1}}L_g = L_{g^{-1}g} = L_e$
$L_gL_{g^{-1}} = L_{gg^{-1}} = L_e$
$\therefore G'$ is closed under inverses.

$\therefore G'$ is a group.

Theorem: Cayley

Every group is isomorphic to a group of permutations.

Proof

Let G a group and $G' = \{L_g \mid g \in G\}$ G' is a group (lemma)

Let $\phi : G \to G$ be defined by $\phi(g) = L_g$

Assume $\phi(g_1) = \phi(g_2)$
$L_{g_1} = L_{g_2}$
Assume $x \in G$
$L_{g_1}(x) = L_{g_2}(x)$
$g_1x = g_2x$
$g_1 = g_2$
$\therefore \phi$ is one-to-one.

Assume $L_g \in G'$
$g \in G$
$\phi(g) = L_g$
$\therefore \phi$ is onto and thus a bijection.

Assume $g_1, g_2 \in G$
$\phi(g_1g_2) = L_{g_1g_2} = L_{g_1}L_{g_2} = \phi(g_1)\phi(g_2)$ $\therefore \phi$ is a homomorphism and thus an isomorphism.

$\therefore G \simeq G'$