Properties of "Left multiplication by g" functions.

Setup: G a group, $g \in G$

$$\rightsquigarrow$$

$$L_g : G \longrightarrow G$$
$$: x \longmapsto gx \quad (\forall x \in G)$$

is a function from G to G called "Left multiplication by g".

Property ① If $g = e$ the identity element of G, then

① — $\boxed{L_g = L_e}$ is the identity function $1\!\!1_G : G \to G$.

Proof: Given any $x \in G$, $\underset{\text{def}^{\underline{n}} \text{ of } L_e}{L_e(x) \overset{\uparrow}{=}} e.x \underset{e = \text{identity of } G.}{\overset{\uparrow}{=}} x$.

Thus $L_e(x) = x$ for all $x \in G$.

$\Rightarrow L_e = 1\!\!1_G$ the identity function $: G \to G$.

[G]

Property ② If $g, h \in G$ then the composition of their left multiplication functions is another left multiplication function. In particular,

② — $\boxed{L_g \circ L_h = L_{gh}}$

<u>Proof</u> Take any $x \in G$.

Then $(L_g \circ L_h)(x) = L_g(L_h(x))$ ---- defⁿ of composition

$= L_g(h.x)$ ---- defⁿ of L_h

$= g.(h.x)$ ---- defⁿ of L_g

$= (gh).x$ ---- associativity in G

$= L_{gh}(x)$ ---- defⁿ of L_{gh}.

(& $gh \in G$ because G is a group).

True for all $x \in G$

$\Rightarrow \boxed{L_g \circ L_h = L_{gh}}$ ☒

<u>Property ③</u> L_g is a bijection : $G \to G$.

<u>Proof</u> This is a consequence of properties ① & ②

G a group $\Rightarrow g^{-1} \in G$ & we can compose the functions L_g and $L_{g^{-1}}$

$$L_g \circ L_{g^{-1}} \underset{\text{Prop ②}}{=} L_{gg^{-1}} = L_e \underset{\text{Prop ①}}{=} 1\!\!1_G \quad \text{a bijection.}$$

$$L_{g^{-1}} \circ L_g \overset{\text{Prop ②}}{=} L_{g^{-1}g} = L_e \overset{\text{Prop ①}}{=} 1\!\!1_G \quad \text{a bijection.}$$

1st row tells us that L_g is surjective
2nd row tells us that L_g is injective $\Big\} \Rightarrow L_g$ a bijection ☒

Property (4) The collection of bijections

$$\{L_g \mid g \in G\} \subseteq \mathrm{Perm}(G)$$

is a subgroup of Perm (G).

Proof → It is closed under composition by property (2)

$$L_g \circ L_h = L_{gh} \quad \text{is in this set.}$$

→ It contains the identity $L_e = \mathbb{1}_G$.

→ It contains inverses. In the proof of property (3) we established that

$$L_{g^{-1}} \circ L_g = \mathbb{1}_G = L_g \circ L_{g^{-1}}$$

This means that $L_{g^{-1}}$ is the inverse of L_g.

→ It is associative since composition of functions is associative (proven in class). $\square$

Property (5) [Cayley's Theorem] The function

$$\begin{aligned} \Phi : G &\longrightarrow \{L_g \mid g \in G\} \subseteq \mathrm{Perm}(G) \\ : g &\longmapsto L_g \end{aligned}$$

is an isomorphism of groups.

Proof of 5. → Φ injective.

Suppose $\Phi(g_1) = \Phi(g_2)$. Then $L_{g_1} = L_{g_2}$. These are two functions which are equal. If we apply them to the same input e (= identity element of G), we will get same output.

$$\Rightarrow L_{g_1}(e) = L_{g_2}(e)$$

$$\Rightarrow g_1 e = g_2 e \quad \text{--- def}^{\underline{n}} \text{ of } L_g$$

$$\Rightarrow g_1 = g_2 \quad \text{---- } e = \text{identity in } G.$$

We have shown $\left(\Phi(g_1) = \Phi(g_2)\right) \longrightarrow (g_1 = g_2)$.

Thus Φ is injective.

→ Φ is surjective.

This is true by def$^{\underline{n}}$ of the target group $\{L_g \mid g \in G\}$ and the function Φ.

Given $L_g \in \{L_g \mid g \in G\}$, by definition of Φ we have

$$\Phi(g) = L_g \quad , \text{ so } \Phi \text{ is surjective.}$$

→ Φ respects the multiplications.

Given any $g_1, g_2 \in G$, we have

$$\Phi(g_1 g_2) \underset{\text{def}^{\underline{n}} \text{ of } \Phi}{=} L_{g_1 g_2} = L_{g_1} \circ L_{g_2} \quad \text{--- property 2}$$

$$= \Phi(g_1) \circ \Phi(g_2) \quad \text{--- def}^{=} \text{ of } \Phi$$

That is ...

$$\underbrace{\Phi(g_1 g_2)}_{\substack{\uparrow \\ \text{multiplication} \\ \text{in } G}} = \underbrace{\Phi(g_1) \circ \Phi(g_2)}_{\substack{\uparrow \\ \text{composition in the} \\ \text{subgroup } \{L_g \mid g \in G\} \text{ of } \mathrm{Perm}(G)}}$$

Φ respects group operations.

$\Rightarrow$ Φ is an isomorphism of groups. $\boxtimes$

"Every group is isomorphic to a subgroup of permutations of some set." $\leftarrow$ Cayley's Theorem (restated)

Remark   The fact that $L_g : G \to G$ is a bijection, and in particular is injective is very useful.

$\to$ We used it in looking at symm () to pass from 24 symmetries which preserve right-handedness to 24 new symmetries which take right-hands into left-hands. The fact that we obtained 24 distinct new symmetries followed from injectivity of L_g.

$\to$ It is used in the proof of Lagrange's Theorem, to conclude that each $L_g(H)$ has the same number of elements as H.