

①

Properties of "Left multiplication by g " functions.

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



$$\begin{aligned} L_g: G &\longrightarrow G \\ : x &\longmapsto gx \quad (\forall x \in G) \end{aligned}$$

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

Property ①

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

① — $L_g = L_e$ in the identity function $\mathbb{1}_G: G \rightarrow G$.

Proof: Given any $x \in G$, $L_e(x) = e \cdot x = x$.
 \uparrow \uparrow
 $\text{def of } L_e$ $e = \text{identity of } G$.

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

$\Rightarrow L_e = \mathbb{1}_G$ the identity function: $G \rightarrow G$.

□

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

$$\boxed{\textcircled{2} - L_g \circ L_h = L_{gh}}$$

Proof

Take any $x \in G$.

(2)

$$\begin{aligned}
 \text{Then } (L_g \circ L_h)(x) &= L_g(L_h(x)) \quad \dots \text{ def} \circ \text{ composition} \\
 &= L_g(h \cdot x) \quad \dots \text{ def } L_h \\
 &= g \cdot (h \cdot x) \quad \dots \text{ def } L_g \\
 &= (gh) \cdot x \quad \dots \text{ associativity in } G \\
 &= L_{gh}(x) \quad \dots \text{ def } L_{gh}.
 \end{aligned}$$



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

True for all $x \in G$

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



Property ③

L_g is a bijection : $G \rightarrow G$.

Proof

This is a consequence of properties ① & ②

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

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

\uparrow Prop ② \uparrow Prop ①

$$L_{g^{-1}} \circ L_g = L_{g^{-1}g} = L_e = \mathbb{1}_G \quad \text{a bijection.}$$

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



(3)

Property (4)

The collection of bijections

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

is a subgroup of $\text{Perm}(G)$.

Proof → It is closed under composition by property ②

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

→ 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).

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

$$\Phi: G \longrightarrow \{L_g \mid g \in G\} \subseteq \text{Perm}(G)$$

: $g \longmapsto L_g$ is an isomorphism of groups.

Proof of ⑤ $\rightarrow \Phi$ injective.

(4)

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.

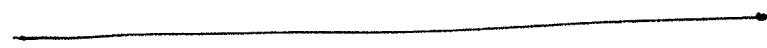
$$\Rightarrow L_{g_1}(e) = L_{g_2}(e)$$

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

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

We have shown $(\Phi(g_1) = \Phi(g_2)) \rightarrow (g_1 = g_2)$.

Thus Φ is injective.



$\rightarrow \Phi$ is surjective.

This is true by defn 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

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

$\rightarrow \Phi$ respects the multiplications.

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

$$\Phi(g_1 g_2) \stackrel{\text{defn of } \Phi}{=} L_{g_1 g_2} = L_{g_1} \circ L_{g_2} \quad \text{--- property ②}$$

$$= \bar{\phi}(g_1) \circ \bar{\phi}(g_2) \quad \text{--- def} = \bar{\phi}$$

That is --.

$$\begin{array}{ccc} \bar{\phi}(g_1 g_2) & = & \bar{\phi}(g_1) \circ \bar{\phi}(g_2) \\ \uparrow & & \uparrow \\ \text{multiplication} & & \text{composition in the} \\ \text{in } G & & \text{subgroup } \{L_g \mid g \in G\} \text{ of } \text{Perm}(G) \end{array}$$

$\bar{\phi}$ respects group operations.

$\Rightarrow \bar{\phi}$ is an isomorphism of groups.



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

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

\rightarrow 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 .

\rightarrow 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 .