Proof of Cayley's Theorem, and an example: $G = \mathcal{S}_3$

1. We define ψ from G to the set of all functions $G \to G$ by, for a in G, $\psi(a)$ is left multiplication by a, i.e. $(\psi(a))(x) = ax \ \forall x \in G$.

   Ex: There are $6^6 = 46,656$ functions from $\mathcal{S}_3$ to itself; among them, the constant functions like $\begin{pmatrix} e & f & f^2 & g & fg & f^2g \\ f & f & f & f & f & f \end{pmatrix}$ and the 1–1 correspondences like $\begin{pmatrix} e & f & f^2 & g & fg & f^2g \\ f^2 & f & e & g & fg & f^2g \end{pmatrix}$. Each $\psi(g)$ above is one of these 46,656 functions.

$$\psi(e) = \begin{pmatrix} e & f & f^2 & g & fg & f^2g \\ e & f & f^2 & g & fg & f^2g \end{pmatrix} \quad \psi(f) = \begin{pmatrix} e & f & f^2 & g & fg & f^2g \\ f & f^2 & e & fg & f^2g & g \end{pmatrix}$$

$$\psi(f^2) = \begin{pmatrix} e & f & f^2 & g & fg & f^2g \\ f^2 & e & f & f^2g & g & fg \end{pmatrix} \quad \psi(g) = \begin{pmatrix} e & f & f^2 & g & fg & f^2g \\ g & f^2g & fg & e & f^2 & f \end{pmatrix}$$

$$\psi(fg) = \begin{pmatrix} e & f & f^2 & g & fg & f^2g \\ fg & g & f^2g & f & e & f^2 \end{pmatrix} \quad \psi(f^2g) = \begin{pmatrix} e & f & f^2 & g & fg & f^2g \\ f^2g & fg & g & f^2 & f & e \end{pmatrix}$$

   The second row of each $\varphi(g)$ is the row in the group table of $\mathcal{S}_3$ corresponding to g:

$\circ$	e	f	f^2	g	fg	f^2g
e	e	f	f^2	g	fg	f^2g
f	f	f^2	e	fg	f^2g	g
f^2	f^2	e	f	f^2g	g	fg
g	g	f^2g	fg	e	f^2	f
fg	fg	g	f^2g	f	e	f^2
f^2g	f^2g	fg	g	f^2	f	e

2. Next, we show ψ is actually into $S(G)$, the set of all 1–1 correspondences $G \to G$. There are $6! = 720$ 1–1 correspondences from $\mathcal{S}_3$ to itself.

   For finite G's, we saw this early on: Each row in the group table contains each element of G exactly once.

3. Then we show that ψ is 1–1, i.e., that different elements a of G give different functions $\psi(a)$.

   Two functions are equal iff they have the same output for each input from the domain. In our case, no two rows in the group table are the same, even in the first entry (under the identity): $\varphi(g_1) = \varphi(g_2)$ implies $(\varphi(g_1))(e) = (\varphi(g_2))(e)$, which is just $g_1 e = g_2 e$, or $g_1 = g_2$.

4. Finally, we show that ψ is a homomorphism. This just amounts to associativity in G.