CAYLEY'S THEOREM

SEBASTIAN CASALAINA

1. The statement of Cayley's Theorem

For a set S, we will denote by $(\mathrm{Bij}(S), \circ)$ the group of bijections $f : S \to S$ under composition.

Theorem 1.1 (Cayley's Theorem)**.** *Let $(G, \cdot)$ be a group. There is an injective group homomorphism*

$$\Phi : (G, \cdot) \longrightarrow (\mathrm{Bij}(G), \circ)$$

defined by the rule that for all $g, h \in G$, we have $\Phi(g)(h) = gh$.

We will prove Cayley's Theorem below. Before we do that, we mention here that Cayley's Theorem is often stated for finite groups in the following form:

Corollary 1.2. *Let G be a finite group of order n. Then G is isomorphic to a subgroup of S_n, the symmetric group on n letters.*

Proof. Cayley's Theorem gives an injective homomorphism of groups $\Phi : G \hookrightarrow \mathrm{Bij}(G)$. Then since there is a bijection of sets $G \to \{1, \ldots, n\}$, we have an isomorphism of groups $\Psi : \mathrm{Bij}(G) \to \mathrm{Bij}(\{1, \ldots, n\}) =: S_n$. □

2. The group of bijections of a set

Given a set S, we recall that $(\mathrm{Bij}(S), \circ)$, the set of bijections $f : S \to S$ under composition, form a group. Namely, we have a map

$$\circ : \mathrm{Bij}(S) \times \mathrm{Bij}(S) \to \mathrm{Bij}(S)$$

$$(f, g) \mapsto f \circ g.$$

The identity element of $\mathrm{Bij}(S)$ is Id_S, since

$$\mathrm{Id}_S \circ f = f$$

for all $f \in \mathrm{Bij}(S)$. If $f \in \mathrm{Bij}(S)$, then the inverse element of f under the group law is given by the inverse map f^{-1}, since

$$f^{-1} \circ f = \mathrm{Id}_S\,.$$

Composition of maps is associative. Thus $(\mathrm{Bij}(S), \circ)$ is a group.

Date: September 26, 2016.

3. Proof of Cayley's Theorem

Given a group G, there is a map of sets

$$\Phi : G \to \mathrm{Map}(G, G)$$
$$\Phi(g)(h) = gh, \qquad \text{for all} \quad g, h \in G.$$

Part of the assertion of Cayley's Theorem is that $\mathrm{Im}(\Phi) \subseteq \mathrm{Bij}(G, G) \subseteq \mathrm{Map}(G, G)$. In other words, given $g \in G$, the claim is that the map $\Phi(g) : G \to G$ is a bijection. To show that $\Phi(g)$ is a bijection, we need to show that it is injective and surjective.

First let us show that if $g \in G$, then $\Phi(g)$ is injective. This means, that given $h_1, h_2 \in G$, then if $\Phi(g)(h_1) = \Phi(g)(h_2)$, we need to show that $h_1 = h_2$. Well,

$$gh_1 =: \Phi(g)(h_1) = \Phi(g)(h_2) := gh_2.$$

Then composing with g^{-1} on the left, we have that

$$h_1 = g^{-1}gh_1 = g^{-1}gh_2 = h_2.$$

Thus $\Phi(g)$ is injective.

Let us now show that $\Phi(g)$ is surjective. This means that given $h \in G$, we need to exhibit $h' \in G$ such that $\Phi(g)(h') = h$. Well, given $h \in G$, if we set $h' = g^{-1}h$, then

$$h = gh' = \Phi(g)(h').$$

Thus $\Phi(g)$ is surjective. We have now succeeded in showing that if $g \in G$, then $\Phi(g) \in \mathrm{Bij}(G, G)$.

The next claim of Cayley's Theorem is that

$$\Phi : G \to \mathrm{Bij}(G, G)$$

is a group homomorphism. In other words, given $g_1, g_2 \in G$, the claim is that

$$\Phi(g_1g_2) = \Phi(g_1) \circ \Phi(g_2).$$

It is enough to check this holds when the maps are applied to each $h \in G$. In other words, for $h \in G$, we have

$$\Phi(g_1g_2)(h) := (g_1g_2)h = g_1(g_2h) = (\Phi(g_1) \circ \Phi(g_2))(h).$$

Thus $\Phi(g_1g_2) = \Phi(g_1) \circ \Phi(g_2)$.

The last claim of Cayley's Theorem is that Φ is injective. In other words, given $g_1, g_2 \in G$, if $\Phi(g_1) = \Phi(g_2)$, then the claim is that $g_1 = g_2$. To prove this, apply $\Phi(g_1)$ and $\Phi(g_2)$ to the identity element of G:

$$g_1 = \Phi(g_1)(e) = \Phi(g_2)(e) = g_2.$$

This shows that Φ is injective, and completes the proof of Cayley's Theorem.

4. The example of the dihedral group

Recall the dihedral group:

E:Dih (4.1)
$$D_n = \{\mathrm{Id}, R, \ldots, R^{n-1}, D, DR, \ldots, DR^{n-1}\},$$

where we compose under the rules that $R^n = \mathrm{Id}$, $D^2 = \mathrm{Id}$, and $DR = R^{n-1}D$. Then Cayley's Theorem tells us there is an injective group homomorphism

$$\Phi : D_n \longrightarrow \mathrm{Bij}(D_n) \cong S_{2n}.$$

We can tell that Φ is not surjective (for $n > 1$) by counting elements (the order of D_n is $2n$, whereas the order of S_{2n} is $(2n)!$).

Exercise 4.1. If we label the elements of D_n from $1, \ldots, 2n$, in the order given above in (4.1), what is the permuation associated to R; i.e., under the induced isomorphism $\Psi : \mathrm{Bij}(D_n) \to S_{2n}$, what is the element $\Psi \circ \Phi(R)$?

Exercise 4.2. Can you find an injective homomorphism $\phi : D_n \longrightarrow S_n$? Are any of the homomorphisms you find surjective?

University of Colorado, Department of Mathematics, Campus Box 395, Boulder, CO 80309-0395

E-mail address: casa@math.colorado.edu