Lecture Notes: Abstract Algebra — Cayley's Theorem (Course By: Alvaro Lozano-Robledo)

Thobias K. Høivik

March 13, 2025

Theorem 1 (Cayley's Theorem)**.** *Every finite group is isomorphic to a subgroup of a permutation group.*

Example

$\mathbb{Z}/_3\mathbb{Z}$

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Notice how each row is a permutation of $\{0, 1, 2\}$, namely the permutations:

$$\begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 2 \end{pmatrix}$$
$$\begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix}$$
$$\begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix}$$

or alternatively,

$$(0)$$
$$(1, 2, 3)$$
$$(1, 3, 2)$$

written in single-line notation. Consider then the isomorphism

$$\phi : \mathbb{Z}/_3\mathbb{Z} \to \{(1), (123), (132)\} =< (123) >\subseteq S_3$$

$$0 \to (1)$$
$$1 \to (123)$$
$$2 \to (132)$$
$$\phi(n \text{ mod } 3) = (123)^n$$
$$\phi(n+m) = (123)^{n+m} = (123)^n(123)^m = \phi(n)\phi(m)$$
$$\mathbb{Z}/_3\mathbb{Z} \cong < (123) >$$

Lemma 1. *Let G be a finite group and $g \in G$. Let $\lambda_g : G \to G, \quad \lambda_g(a) = a \star g$. Then λ_g is a bijection.*

Proof. Since G is closed λ_g is well defined:

$$a \in G \land g \in G \Rightarrow a \star g \in G \land g \star a \in G$$

Suppose we have

$$\lambda_g(a) = \lambda_g(b), \quad a, b \in G$$

$$g \star a = g \star b$$
$$a = b$$
$$\because \forall g \in G : \exists g^{-1} \in G$$

hence λ_g is injective. Now to show surjectivity:

$$\lambda_g(a) = b$$
$$g \star a = b$$
$$a = g^{-1} \star b \in G$$

obviously, lol (tired). □

Proving the Theorem

Now to prove Cayley's Theorem 1.

Proof of Cayley's Theorem. Let G be a finite group, G $= \{g_1, g_2, \ldots, g_n\}$. For $g \in G$, let $\lambda_g : G \to G, \quad \lambda_g(a) = g \star a$, λ_g is a bijection as shown in 1, making $\lambda \in Sym(G)$ a permutation of G. $Sym(G) = Sym(\{g_1, g_2, \ldots, g_n\}) = Sym(\{1, 2, \ldots, n\}) = S_n$. Let $\overline{G} = \{\lambda_g : g \in G\} \subseteq S_n$.
Claim: $\overline{G} = \{\lambda_g : g \in G\}$ is a group. $< \overline{G}, \circ >$ is closed:

$$\lambda_g \circ \lambda_{g^\star}(a) = \lambda_g(\lambda_{g^\star}(a)) = gg'a$$
$$= \lambda gg^\star \in \overline{G} \quad \because gg^\star \in G$$

$< \overline{G}, \circ >$ is associative

$$(\lambda_x \circ \lambda_y) \circ \lambda_z$$
$$= \lambda_{xyz}$$
$$= \lambda_x \circ (\lambda_y \circ \lambda_z)$$

$< \overline{G}, \circ >$ has identity

$$\lambda_e(a) = e \star a = a$$

$< \overline{G}, \circ >$ has inverse

$$\lambda_g \circ \lambda_{g^{-1}} = \lambda_e$$

Moreover $G \cong \overline{G}$. Consider $\phi : G \to \overline{G}$

$$\phi(g) = \lambda_g$$

Injective:

$$\lambda_a(e) = \lambda_b(e) \Leftrightarrow ae = be \Leftrightarrow a = b$$

Surjective:

$$\lambda_a \in \overline{G}, \phi(a) = \lambda_a$$

by definition. Structure:

$$\phi(gh) = \lambda_{gh} = \lambda_g \circ \lambda_h = \phi(g)\phi(h)$$

thus we have an isomorphism.

$\square$