PART II Permutations, Cosets, Direct Products

Section 8 Groups of Permutations

Today we examine how permutations have a group structure and how every group can be viewed in terms of permutations.

Intuitive idea:

A permutation of objects is a rearrangement of them on a line

$$\begin{array}{cccccc} a & b & c & d & e & f \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ e & b & f & a & c & d \end{array}$$

Definition

A *permutation* of a set A is a 1-1 and onto function $\sigma : A \to A$.

Examples $A = \{1, 2, 3\}$

Permutation of A: $\sigma = \begin{array}{ccc} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 \end{array}$ $\quad \sigma(1) = 2 \quad \sigma(2) = 3 \quad \sigma(3) = 1$

Permutation of A: $\tau = \begin{array}{ccc} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 1 & 3 \end{array}$ $\quad \tau(1) = 2 \quad \tau(2) = 1 \quad \tau(3) = 3$

Consider $\sigma \circ \tau$

$\sigma \circ \tau(1) = \sigma(\tau(1)) = \sigma(2) = 3$
$\sigma \circ \tau(2) = \sigma(\tau(2)) = \sigma(1) = 2$
$\sigma \circ \tau(3) = \sigma(\tau(3)) = \sigma(3) = 1$

$\sigma \circ \tau = \begin{array}{ccc} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 2 & 1 \end{array}$

Consider $\tau \circ \sigma$

$\tau \circ \sigma(1) = \tau(\sigma(1)) = \tau(2) = 1$
$\tau \circ \sigma(2) = \tau(\sigma(2)) = \tau(3) = 3$
$\tau \circ \sigma(3) = \tau(\sigma(3)) = \tau(1) = 2$

$\tau \circ \sigma = \begin{array}{ccc} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 3 & 2 \end{array}$

Note $\sigma \circ \tau$ and $\tau \circ \sigma$ are permutations of A but $\sigma \circ \tau \neq \tau \circ \sigma$.

Notation $\sigma \circ \tau = \sigma\tau$

Notation $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ $\quad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ $\quad \sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

> **Theorem** Suppose A is a set. The set of permutations of A is a group under operation $\circ$ (function composition)
>
> $\mathcal{G}_1$ Function composition is associative.
>
> $\mathcal{G}_2$ Identity element is $i : A \to A$, $i(x) = x$.
>
> $\mathcal{G}_3$ Inverse of σ is inverse function σ^{-1}.
> $\sigma\sigma^{-1}(x) = x$, so $\sigma\sigma^{-1} = i$.

Definition If $A = \{1, 2, 3, \dots n\}$, the group of permutations on A is called the symmetric group on n letters and is denoted S_n. Thus $|S_n| = n!$

Ex $S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}$

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

$\cong$

+	0	1
0	0	1
1	1	0

Thus $S_2 \cong \mathbb{Z}_2$

Ex $S_3 = \left\{ \underset{\rho_0}{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}}, \underset{\rho_1}{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}}, \underset{\rho_2}{\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}}, \underset{\mu_1}{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}}, \underset{\mu_2}{\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}}, \underset{\mu_3}{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}} \right\}$

S_3

	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_2	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ	ρ_2	ρ_0

Notice that S_3 is non-abelian. It turns out to be the smallest nonabelian group.

Cayleys Theorem

Every group is isomorphic to a group of permutations.

The proof uses an idea you've probably observed before:

The rows of a mult. table are all permutations of the top row. The idea is to associate each row with its permutation.

	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Cayley's Theorem

Every group G is isomorphic to a group of permutations.

Proof (Outline)

Given $x \in G$, define function $\lambda_x : G \to G$ as $\lambda_x(g) = xg$

Note λ_x is 1-1 $\quad \lambda_x(a) = \lambda_x(b) \Rightarrow \cancel{xa} = xb \Rightarrow a = b$

Note λ_x is onto $\quad$ If $a \in G$ then $\lambda_x(x^{-1}a) = xx^{-1}a = a$.

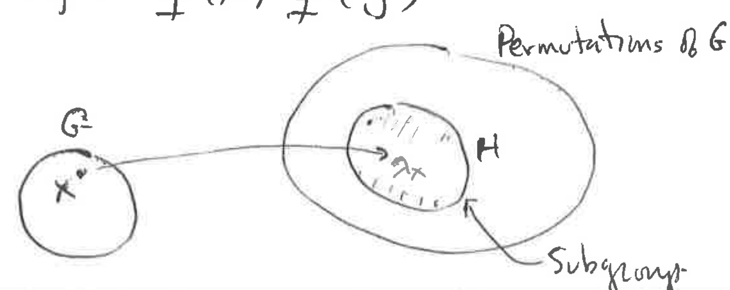
Thus λ_x is a permutation of G

Note $\lambda_x \lambda_y = \lambda_{xy}$

Define $\Phi : G \longrightarrow \begin{pmatrix}\text{Permutations} \\ \text{of } G\end{pmatrix}$ as $\Phi(x) = \lambda_x$

Then $\Phi(xy) = \lambda_{xy} = \lambda_x \lambda_y = \Phi(x)\Phi(y)$

Also check Φ is 1-1.



An illustration of Cayley's Theorem

Consider the group $\mathbb{Z}_3$:

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

Cayley's Theorem says this is isomorphic to a group of permutations. <u>What</u> group of permutations?

To answer that, note:

$$\lambda_0 = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 2 \end{pmatrix}$$

$$\lambda_1 = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix}$$

$$\lambda_2 = \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix}$$

These 3 permutations obey the following multiplication table, which is structurally identical to that of $\mathbb{Z}_3$.

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