Permutation Groups

Def. A **permutation** of a set A is a function $\phi: A \to A$ that's 1-1 and onto

We can think of a permutation as a rearrangement of the elements of A.

Ex. Let $A = \{1, 2, 3, 4, 5\}$. Examples of permutations:

$$\phi_1(\{1,2,3,4,5\}) = \{4,3,1,2,5\}$$

$$\phi_2(\{1,2,3,4,5\}) = \{5,2,3,1,4\}$$

ϕ_1	ϕ_2
$1 \to 4$	$1 \to 5$
$2 \to 3$	$2 \to 2$
$3 \to 1$	$3 \to 3$
$4 \to 2$	$4 \to 1$
$5 \to 5$	$5 \to 4$

We can form a new permutation by taking the composition of the above permutations: $\phi_2 \circ \phi_1(\{1, 2, 3, 4, 5\})$. This is permutation multiplication.

$\phi_2 \circ \phi_1$	i. e.	$\phi_2 \circ \phi_1$
$1 \to 4 \to 1$		$1 \to 1$
$2 \to 3 \to 3$		$2 \to 3$
$3 \to 1 \to 5$		$3 \to 5$
$4 \to 2 \to 2$		$4 \to 2$
$5 \to 5 \to 4$		$5 \to 4$

We can write ϕ_1 and ϕ_2 as:

$$\phi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 2 & 5 \end{pmatrix}$$

$$\phi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 1 & 4 \end{pmatrix}.$$

Then $\phi_2 \circ \phi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 1 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 2 & 5 \end{pmatrix}$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 2 & 4 \end{pmatrix}.$$

Theorem: Let A be a nonempty set, and let S_A be the set of permutations of A. Then S_A is a group under permutation multiplication.

Proof:

0) S_A is clearly closed under permutation multiplication.
1) Permutation multiplication is just a composition of functions and composition of functions is associative so this multiplication is as well.
2) The permutation $i(a) = a$ for all $a \in A$ acts as an identity.
3) For any permutation σ, σ^{-1} is just the permutation σ in the opposite direction that reverses what σ does.

For example, if $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 4 & 1 \end{pmatrix}$

then $\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{pmatrix}$ thus, $\sigma^{-1} \circ \sigma = i$ and $\sigma \circ \sigma^{-1} = i$.

Thus S_A is a group.

We will generally be concerned with S_A where A is a finite set, but that doesn't have to be the case.

Def. Let $A = \{1, 2, \ldots, n\}$. The group of all permutations of A is called the **symmetric group on n letters** and is denoted S_n.

Note that the number of permutations on n objects is $n!$

Thus, $|S_n| = n!$

Ex. Let's examine S_3.

$|S_3| = 3! = 6.$

Let $\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ $\mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ $\mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

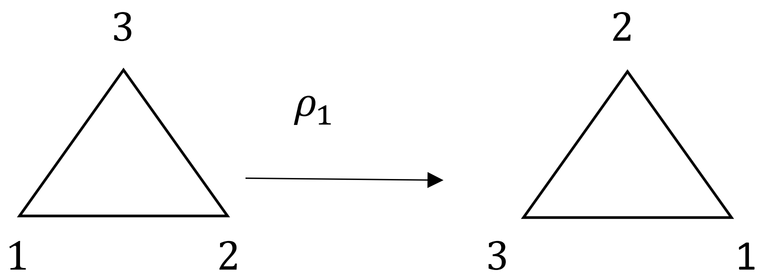
$\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ $\mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

It's easy (but cumbersome) to check the following multiplication table for S_3 (by taking compositions of these permutations):

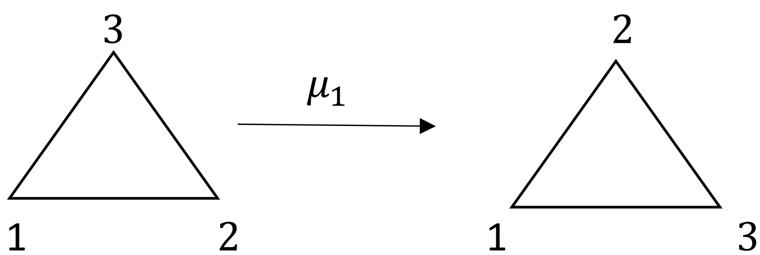
	$\boldsymbol{\rho_0}$	$\boldsymbol{\rho_1}$	$\boldsymbol{\rho_2}$	$\boldsymbol{\mu_1}$	$\boldsymbol{\mu_2}$	$\boldsymbol{\mu_3}$
$\boldsymbol{\rho_0}$	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
$\boldsymbol{\rho_1}$	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
$\boldsymbol{\rho_2}$	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
$\boldsymbol{\mu_1}$	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
$\boldsymbol{\mu_2}$	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
$\boldsymbol{\mu_3}$	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

Notice that S_3 is not abelian (e.g. $\rho_1\mu_1 = \mu_3$ but $\mu_1\rho_1 = \mu_2$). In fact, it's the smallest possible non-abelian group.

There is a natural correspondence between the elements of S_3 and the ways in which 2 copies of an equilateral triangle with vertices $1, 2, 3$ can be placed. S_3 is also called D_3, the 3rd dihedral group (symmetries of an equilateral triangle).



Rotation



Mirror image about an angle bisector.

D_4 is the 4th dihedral group which is the set of permutations of the vertices of a square corresponding to the symmetries of a square. This is called the octic group.

<u>Rotations</u>

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

$$\rho_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

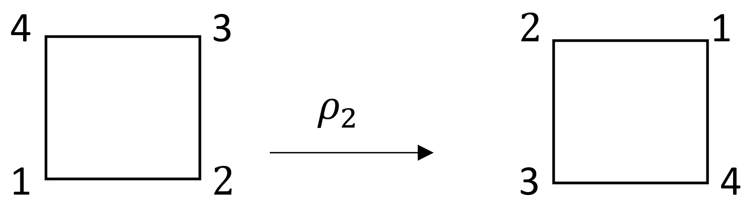
<u>Flips</u>

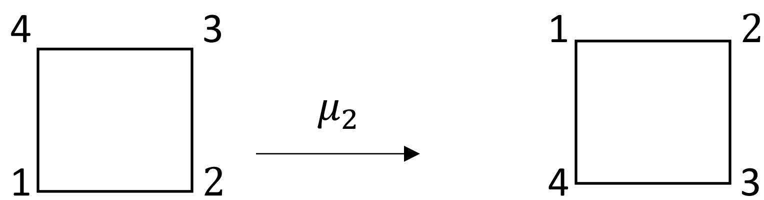
$$\mu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$\mu_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

$$\delta_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

$$\delta_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$





Multiplication table for D_4:

	$\boldsymbol{\rho_0}$	$\boldsymbol{\rho_1}$	$\boldsymbol{\rho_2}$	$\boldsymbol{\rho_3}$	$\boldsymbol{\mu_1}$	$\boldsymbol{\mu_2}$	$\boldsymbol{\delta_1}$	$\boldsymbol{\delta_2}$
$\boldsymbol{\rho_0}$	ρ_0	ρ_1	ρ_2	ρ_3	μ_1	μ_2	δ_1	δ_2
$\boldsymbol{\rho_1}$	ρ_1	ρ_2	ρ_3	ρ_0	δ_1	δ_2	μ_2	μ_1
$\boldsymbol{\rho_2}$	ρ_2	ρ_3	ρ_0	ρ_1	μ_2	μ_1	δ_2	δ_1
$\boldsymbol{\rho_3}$	ρ_3	ρ_0	ρ_1	ρ_2	δ_2	δ_1	μ_1	μ_2
$\boldsymbol{\mu_1}$	μ_1	δ_2	μ_2	δ_1	ρ_0	ρ_2	ρ_3	ρ_1
$\boldsymbol{\mu_2}$	μ_2	δ_1	μ_1	δ_2	ρ_2	ρ_0	ρ_1	ρ_3
$\boldsymbol{\delta_1}$	δ_1	μ_1	δ_2	μ_2	ρ_1	ρ_3	ρ_0	ρ_2
$\boldsymbol{\delta_2}$	δ_2	μ_2	δ_1	μ_1	ρ_3	ρ_1	ρ_2	ρ_0

D_4 is non-abelian.

Ex. Consider the following permutations in S_6:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 6 & 1 & 5 \end{pmatrix}$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 1 & 4 & 2 & 5 \end{pmatrix}.$$

Calculate $\sigma\tau^{-2}$ and σ^{66}.

First calculate τ^{-1}:

$$\tau^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 2 & 4 & 6 & 1 \end{pmatrix}.$$

$$\tau^{-2} = \tau^{-1}\,\tau^{-1}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 2 & 4 & 6 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 2 & 4 & 6 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 5 & 4 & 1 & 3 \end{pmatrix}.$$

$$\sigma\tau^{-2} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 6 & 1 & 5 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 5 & 4 & 1 & 3 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 1 & 6 & 4 & 2 \end{pmatrix}.$$

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 6 & 1 & 5 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 6 & 1 & 5 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 3 & 5 & 4 & 1 \end{pmatrix}.$$

$$\sigma^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 6 & 1 & 5 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 3 & 5 & 4 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 2 & 1 & 6 & 4 \end{pmatrix}.$$

$$\sigma^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 6 & 1 & 5 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 2 & 1 & 6 & 4 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}.$$

So $\sigma^4 = i$.

$\Longrightarrow \quad \sigma^{4k} = i$.

So $\sigma^{66} = \sigma^2 \cdot \sigma^{64} = \sigma^2 \cdot i = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 3 & 5 & 4 & 1 \end{pmatrix}$.

Def. The **orbit** of a under σ is the set $\{\sigma^n(a) | \, n \in \mathbb{Z}\}$.

Ex. Find the orbit of 5 under σ for the previous example.

$\sigma(5) = 1, \qquad \sigma^2(5) = \sigma(1) = 4, \qquad \sigma^3(5) = \sigma(4) = 6,$

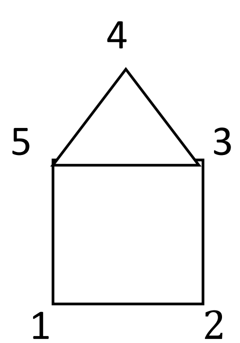
$\sigma^4(5) = \sigma(6) = 5.$

$$\text{Orbit}(5) = \{5,1,4,6\}.$$

Ex. Find the number of elements in the set $\{\sigma \in S_5 | \, \sigma(2) = 5\}$.

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ a & 5 & b & c & d \end{pmatrix}$ The number of elements is the same as the number of elements of S_4 so the number of elements is $4! = 24$.

Ex. Show that S_5 is non-abelian by finding 2 permutations that don't commute.



$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$$

$$\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix}$$

$$\rho\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$$

$$\mu\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 3 & 2 \end{pmatrix} \qquad \Rightarrow \rho\mu \neq \mu\rho.$$

Cayley's Theorem

Def. Let $f: A \to B$ be a function and let H be a subset of A. **The image of $\boldsymbol{H}$ under $\boldsymbol{f}$** is $\{f(h) | \, h \in H\}$ and is denoted by $f[H]$.

Lemma: Let G and G' be groups and let $\phi: G \to G'$ be a one to one function such that $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in G$. Then $\phi[G]$ is a subgroup of G' and ϕ is an isomorphism of G with $\phi[G]$.

Proof: We need to check the following two conditions for $\phi[G] \leq G'$.

1) We need to show $\phi[G]$ is closed under the multiplication in G'.
   Let $x', y' \in \phi[G]$.
   By definition there exist $x, y \in G$ such that $\phi(x) = x'$ and $\phi(y) = y'$. By hypothesis $\phi(xy) = \phi(x)\phi(y) = x'y'$.
   Thus $x'y' \in \phi[G]$, so $\phi[G]$ is closed under the multiplication in G'.

2) We need to show if $x' \in \phi[G]$, then so is its inverse.
   Assume $x' = \phi(x)$. Notice that:
   $e'\phi(e) = \phi(ee) = \phi(e)\phi(e) \implies \phi(e) = e'$.
   Thus we have:
   $e' = \phi(e) = \phi(xx^{-1}) = \phi(x)\phi(x^{-1}) = x'\phi(x^{-1})$ so $\phi(x^{-1})$ is the inverse of x' and $(x')^{-1} = \phi(x^{-1}) \in \phi[G]$.

Thus, $\phi(G)$ is a subgroup of G'.

By definition ϕ is an isomorphism of G with $\phi[G]$.

This lemma is used to prove:

Cayley's Theorem: Every group is isomorphic to a group of permutations.

Proof: Given a group G we will find a 1-1 map $\phi: G \to S_G$, where S_G is the group of permutations of G, such that $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in G$. Then by our lemma G will be isomorphic to $\phi[G] \leq S_G$.

To begin with, notice that for any fixed $x \in G$

$$\sigma_x: G \to G \text{ by}$$

$$g \to xg$$

Is a 1-1 map of G onto G, and hence σ_x is a permutation of G.

To see that σ_x is 1-1 notice that:

$$\sigma_x(g_1) = \sigma_x(g_2)$$

$$xg_1 = xg_2$$

$$\Longrightarrow \qquad g_1 = g_2 \quad \text{by the left cancellation law.}$$

To see that σ_x is onto, let $y \in G$ then $x^{-1}y \in G$ and

$$\sigma_x(x^{-1}y) = x(x^{-1}y)$$

$$= y.$$

Now we define $\phi: G \to S_G$ by:

$$\phi(x) = \sigma_x.$$

To finish the proof we just need to show that ϕ is 1-1 and $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in G$.

To see that ϕ is 1-1 notice that:

$$\phi(x) = \phi(y)$$

$$\sigma_x = \sigma_y, \quad \text{i.e.} \quad \sigma_x(g) = \sigma_y(g) \text{ for all } g \in G.$$

In particular, this relationship holds for $g = e$, the identity element.

$$\sigma_x(e) = \sigma_y(e)$$

$$xe = ye \quad \Longrightarrow \; x = y \quad \text{(cancellation law).}$$

So ϕ is 1-1.

To see that $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in G$:

$$\phi(xy) = \sigma_{xy} \qquad \Longrightarrow \qquad \sigma_{xy}(g) = (xy)g \quad \text{for all } g \in G$$

$$\phi(x)\phi(y) = \sigma_x \circ \sigma_y \qquad \Longrightarrow \; \sigma_x \circ \sigma_y(g) = \sigma_x(yg)$$

$$= x(yg) \quad \text{for all } g \in G.$$

Thus $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in G$.

Thus by our lemma, G is isomorphic to $\phi[G] \leq S_G$.

Ex. If $G = \mathbb{Z}_4$, find the isomorphism $\phi: G \to S_G$ described in the previous theorem.

Since $G = \mathbb{Z}_4$, the group operation is addition modulo 4, $xy = x + y$ (mod 4):

$$\sigma_x: \mathbb{Z}_4 \to \mathbb{Z}_4 \text{ by}$$

$$g \to (x + g) \text{ (mod 4)}.$$

For example, if $x = 2$:

$$\sigma_2(0) = 2 + 0 = 2$$

$$\sigma_2(1) = 2 + 1 = 3$$

$$\sigma_2(2) = 2 + 2 \text{ (mod 4)} = 0$$

$$\sigma_2(3) = 2 + 3 \text{ (mod 4)} = 1.$$

So σ_2 is the permutation:

$$\sigma_2 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \end{pmatrix}.$$

By our previous theorem:

$$\phi: \mathbb{Z}_4 \to S_{\mathbb{Z}_4} \text{ by } \phi(x) = \sigma_x$$

$$\phi(0) = \sigma_0 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 1 & 2 & 3 \end{pmatrix} \qquad \phi(2) = \sigma_2 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \end{pmatrix}$$

$$\phi(1) = \sigma_1 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \end{pmatrix} \qquad \phi(3) = \sigma_3 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 0 & 1 & 2 \end{pmatrix}.$$