Symmetric Groups

Def A permutation of a set $X$ is a bijection $X \rightarrow X$.

"rearrangement of elements of $X"$

Example $X = \{1, 2, \ldots, n\}$, some integer $n > 0$.

A permutation of $X$ is determined by

$1 \rightarrow a_1$

$2 \rightarrow a_2$

$\vdots$

$n \rightarrow a_n$

We write it as

$\begin{pmatrix}
1 & 2 & 3 & 4 & \ldots & n \\
(a_1 & a_2 & a_3 & a_4 & \ldots & a_n)
\end{pmatrix}$

The list $a_1, a_2, \ldots, a_n$ contains every element of $X$ exactly once.

Def The collection of all permutations of a set $X$ is the symmetric group on $X$, written $\text{Symm}(X)$.

Example If $X = \{1, 2, \ldots, n\}$ we write $S_n$ for $\text{Symm}(X)$.

Since elements of $\text{Symm}(X)$ are functions $X \rightarrow X$, we can compose them. This gives a map

$\text{Symm}(X) \times \text{Symm}(X) \rightarrow \text{Symm}(X)$

$(f, g) \rightarrow f \circ g$.
Example (infinite symmetric groups)

We have $S_n \hookrightarrow S_{n+1}$ by taking $f \in S_n$ and extending it to a function $\{1, 2, \ldots, n+1\} \to \{1, 2, \ldots, n+1\}$ that takes $f(n+1) = n+1$.

$S_{\infty} = \bigcup_{n=1}^{\infty} S_n$ is an infinite symmetric group.

We could also take

$X = \{1, 2, 3, \ldots\} = \mathbb{N}$, and take $\text{Symm}(X)$. We have

$S_{\infty} \leq \text{Symm}(\mathbb{N})$ naturally.

$S_{\infty}$ consists of those permutations of $\mathbb{N}$ such that $f(k) = k$ for all $k$ sufficiently large.

Def Let $a_1, \ldots, a_r$ be distinct elements of $X = \{1, 2, \ldots\}$. If $f \in S_n$ fixes each element of $X \setminus \{a_1, \ldots, a_r\}$ and $f(a_i) = a_{i+1}$ for $1 \leq i < r$, $f(a_r) = a_1$,

we say $f$ is an $r$-cycle and write $f = (a_1 a_2 \cdots a_r)$.

Example A 2-cycle $(a b)$ is called a transposition.
Def. Two permutations $\alpha, \beta \in S_n$ are \textit{disjoint} if
(1) $\alpha(k) \neq k$ implies $\beta(k) = k$,
and (2) $\beta(k) \neq k$ implies $\alpha(k) = k$.

Prop. Every permutation $\alpha \in S_n$ is a \textit{composite},
AKA a \textit{product}, of disjoint cycles.

Pf. By \textit{induction} on the number of \textit{natural} numbers
$k$ for which $\alpha(k) = k$; call this number $M$.

\underline{Case $m=0$} This is the \textit{identity} permutation. The statement
is clear.

\underline{Inductive step} Choose some $a_1$ "mixed by $a_i$" i.e.
such that $\alpha(a_1) \neq a_1$. Define $a_2 = \alpha(a_1)$, $a_3 = \alpha(a_2)$,
etc. Create a list $a_1, a_2, a_3, \ldots, a_l$ until the first time that
some element is repeated in the list. By construction,
the only repeat in the list is that $a_l = a_i$ for some
$1 < i < l$. If this $i \neq 1$, then

$$\alpha(a_{l-1}) = a_l = a_i = \alpha(a_{l-1})$$

which implies $a_{l-1} = a_{l-1}$ since $\alpha$ is \textit{injective}.
This is a \textit{contradiction}, so $a_l = a_1$.

We conclude that

$$\alpha \mid a_1, \ldots, a_{l-1} = (a_1 a_2 \ldots a_{l-1})$$.
Now $\sigma_1, \sigma_2, \ldots, n_3 \setminus \sigma_1, \ldots, \sigma_{N-3}$ is a permutation of $\sigma_1, \sigma_2, \ldots, n_3 \setminus \sigma_1, \ldots, \sigma_{N-3}$, so by our inductive hypothesis we have

\[ \sigma_1, \sigma_2, \ldots, n_3 \setminus \sigma_1, \ldots, \sigma_{N-3} = \beta_1 \cdots \beta_k \]

where the $\beta_i$ are disjoint cycles in the symmetric group on $\sigma_1, \sigma_2, \ldots, n_3 \setminus \sigma_1, \ldots, \sigma_{N-3}$. Each $\beta_i$ gives a cycle on $\sigma_1, \sigma_2, \ldots, n_3$ by acting as the identity on $\sigma_1, \ldots, \sigma_{N-3}$.

Finally, we have

\[ \sigma = \beta_1 \cdots \beta_k \circ (\sigma_1 \ldots \sigma_{N-3}), \]

as desired. \[\square\]

Definition 1: A group is a set $G$ equipped with a function

$\ast : G \times G \rightarrow G$ satisfying

(i) **associative law** $x \ast (y \ast z) = (x \ast y) \ast z \quad \forall x, y, z \in G$.

(ii) **identity** There is an element $e \in G$ satisfying $e \ast x = x = x \ast e \quad \forall x \in G$.

(iii) **inverses** For every $x \in G$ there is an element $x^{-1} \in G$ satisfying $x \ast x^{-1} = e = x^{-1} \ast x$. 
A group $G$ is abelian if $xy = yx$ for all $x, y \in G$.

We usually write $xy$ instead of $x \cdot y$.

**Example** $S_n$ is a group under composition of functions.

$S^1 \subset \mathbb{C}$ forms a group under multiplication.

Its subset of $n$th roots of unity $\mathbb{Z}_n$ is also a group.

Its subset $\mathbb{Z}_1$, which is the set of all roots of unity, is also a group.

**Lemma** Let $G$ be a group.

(i) If $xa = xb$ or $ax = bx$ then $a = b$.

(ii) The element $e \in G$ satisfying $ex = x = xe \forall x \in G$ is unique.

(iii) Each $x \in G$ has a unique inverse:

if $xx^{-1} = e = x^{-1}x$ and $xx' = e = x'x$ then $x^{-1} = x'$.

(iv) $(x^{-1})^{-1} = x$ for all $x \in G$. 
Def Let $G$ and $H$ be groups. A homomorphism from $G$ to $H$ is a function $f : G \to H$ satisfying $f(xy) = f(x)f(y)$ for all $x, y \in G$.

If $f$ is injective, surjective, bijective as a map of sets, it is called a monomorphism, epimorphism, isomorphism respectively.

Example $(\mathbb{Z}, +) \to (\mathbb{Q}, +)$ is a monomorphism. There does not exist a nonzero homomorphism $(\mathbb{Q}, +) \to (\mathbb{Z}, +)$.

Example For any field $F$, $F^* = F \setminus \{0\}$ is a group under multiplication.

Example $(\mathbb{C}^*, \cdot)$ is a group. $(\mathbb{C}, +) \to (\mathbb{C}^*, \cdot)$ is a homomorphism. Is it a monomorphism?
Def The \textbf{kernel} of a homomorphism \( f: G \to H \) is
\[ \ker(f) = \{ g \in G \mid f(g) = e \in H \} \].

The \textbf{image} of a subset \( A \subseteq G \) is
\[ f(A) = \{ f(a) \mid a \in A \} \].

\underline{Lemma} \( f: G \to H \) a homomorphism.
(1) \( f(e) = e \).
(2) \( f(g)^{-1} = f(g^{-1}) \).

\underline{Pf.} (1) \( f(e) = f(ee) = f(e)f(e) \). Cancel \( f(e) \).

(2) \( f(g)f(g^{-1}) = f(gg^{-1}) = f(e) = e \) by (1).
So \( f(g^{-1}) = f(g)^{-1} \). \( \square \).

\underline{Theoam} \( f: G \to H \) a homomorphism. Then
(1) \( f \) is a monomorphism iff \( \ker(f) = \{ e \} \).

(2) \( f \) is an isomorphism iff there is a homomorphism \( f^{-1}: H \to G \) such that
\[ f \circ f^{-1} = 1_H \text{ and } f^{-1} \circ f = 1_G. \]

\underline{Pf.} (1) If \( f \) is a monomorphism, then \( f^{-1}(h) \) is a singleton set for every \( h \in H \), so in particular \( f^{-1}(e) = \{ e \} \). On the other hand, if \( f^{-1}(e) = \{ e \} \), then \( f(g) = f(g_2) \Rightarrow f(g_1g_2^{-1}) = f(g_1)f(g_2)^{-1} = e \Rightarrow g_1g_2^{-1} = e. \)
(2) If such an \( f^{-1} \) exists then certainly \( f \) is a bijection, hence by definition an isomorphism. Conversely, if \( f \) is a bijection and a homomorphism then certainly an inverse function \( f^{-1} : H \to G \) exists as a map of sets. It is a homomorphism since, if \( h_1, h_2 \in H \), writing \( h_i = f(g_i) \) we get
\[
\begin{align*}
f^{-1}(h_1 h_2) &= f^{-1}(f(g_1) f(g_2)) = f^{-1}(f(g_1 g_2)) = g_1 g_2 \\
&= f^{-1}(h_1) f^{-1}(h_2).
\end{align*}
\]

**Def:** Let \( G \) be a group, \( H \subseteq G \) a nonempty subset such that \( H \) is a group under the restriction of the product on \( G \) to \( H \). Then \( H \) is a subgroup of \( G \).

**Exercise:** \( f : G \to H \) a homomorphism. Then \( \ker(f), \text{Im}(f) = f(G) \) are subgroups of \( G, H \) respectively.
Example (integers mod $n$)
Consider the set of subsets of $\mathbb{Z}$ of the form $k+n\mathbb{Z} = \{k+na \mid a \in \mathbb{Z}\}$, $k \in \mathbb{Z}$.

Addition of subsets:
$A+B = \{a+b \mid a \in A, b \in B\}.$

So
$(k+n\mathbb{Z}) + (l+n\mathbb{Z}) = \{k+na + l+nb \mid a, b \in \mathbb{Z}\}$
$= \{ (a+b) + n(a+b) \mid a, b \in \mathbb{Z}\} = (k+l) + n\mathbb{Z}.$

Check. This gives the set of such subsets of $\mathbb{Z}$ the structure of a group, written $(\mathbb{Z}/n\mathbb{Z}, +)$.

The function
$\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$
$a \mapsto a+n\mathbb{Z}$

is an epimorphism.

Categories
Def A category $\mathcal{C}$ consists of a class $\text{obj}(\mathcal{C})$ of objects together with
(i) a class of sets $\text{Hom}_{\mathcal{C}}(A, B)$, one for each pair of objects $(A, B) \in \text{obj}(\mathcal{C})$
[elements of $\text{Hom}_{\mathcal{C}}(A, B)$ are morphisms from $A$ to $B$]
(11) For each triple \((A, B, C)\) of objects of \(\mathcal{C}\), a function
\[
\text{Hom}_\mathcal{C}(B, C) \times \text{Hom}_\mathcal{C}(A, B) \rightarrow \text{Hom}_\mathcal{C}(A, C),
\]
called \underline{composition} and written \(g \circ f = gf\), satisfying

\(\text{a) associativity} \quad (h \circ g) \circ f = h \circ (g \circ f)\)

if \(f : A \rightarrow B\), \(g : B \rightarrow C\), \(h : C \rightarrow D\) are morphisms in \(\mathcal{C}\); and

\(\text{b) identity} \quad \text{for each } A \in \text{ob}(\mathcal{C}), \text{there is a}
\]
morphism \(1_A \in \text{Hom}_\mathcal{C}(A, A)\) such that for every (object \(B \in \text{ob}(\mathcal{C})\) and every)
morphism \(f : A \rightarrow B\) in \(\mathcal{C}\) we have \(f \circ 1_A = f\)

and for every morphism \(g : B \rightarrow A\) in \(\mathcal{C}\) we have \(1_A \circ g = g\).
Examples

1) Sets

   objects: sets
   morphisms: \( \text{Hom}_{\text{sets}} (A, B) = \{ \text{functions from } A \to B \} \)

   Composition is the usual composition of functions.

2) Groups

   objects: groups
   morphisms: \( \text{Hom}_{\text{groups}} (G, H) = \{ \text{group homomorphisms } G \to H \} \)

   Composition is composition.

3) \( \text{Vect}_F \) over a field \( F \)

   objects: \( F \)-vector spaces
   morphisms: \( \text{Hom}_{\text{Vect}_F} (V, W) = \{ \text{linear maps } V \to W \} \)

4) \( \text{Ho(Top)} \)

   objects: topological spaces
   morphisms: \( \text{Hom}_{\text{Top}} (X, Y) = \{ \text{homotopy classes of } f : X \to Y \} \)