Permutation groups

Defn Given a set S, we define the group of permutations of S, denoted by $\mathrm{Sym}(S)$ or $\Sigma(S)$ as follows:

$$(\mathrm{Sym}(S), *) = \left(\{\text{bijections from } S \to S\}, \text{composition of functions}\right) \quad \text{i.e.}$$

If $f, g \in \mathrm{Sym}(S)$, then $f * g : S \to S$ by $s \mapsto f(g(s))$.

- Associative : ~~...~~ $f(g(h(s))) = (f \circ g)(h(s)) = ((f*g)*h)(s)$
  $\quad\quad = F((g\circ h)(s)) = (f * (g*h))(s)$. (Just function composition)
- ~~...~~ id_S is the identity
- Given $f \in \mathrm{Sym}(S)$, $f^{-1} : S \to S$ exists (it's a bijection).

Defn If $n \in \mathbb{Z}_{>0}$ we write Sym_n or S_n for $\mathrm{Sym}(\{1,2,\dots,n\})$.
Moreover, if S is any set of size n we have $S_n \simeq \mathrm{Sym}(S)$.

Exercise Verify ~~...~~. So, show that a bijection $\phi : \{1,2,\dots,n\} \to S$ induces an isomorphism of groups $S_n \xrightarrow{\sim} \mathrm{Sym}(S)$.

S_n is called the symmetric group on n elements.

- $|S_n| = n! = n \cdot (n-1) \cdot (n-2) \cdots 1$

n choices for $f(1)$ — n-1 choices for $f(2)$ — 1 choice for $f(n)$

$f : \{1,\dots,n\} \to \{1,\dots,n\}$ is a bijection.

- S_n "permutes" n elements:

For example S_3 can be thought of as the ~~...~~ different ways to reorder

$(1,2,3) \mapsto (1,2,3)$ $\quad (id_{\{1,2,3\}})$

$\mapsto (2,1,3)$

$\mapsto (2,3,1)$

$\mapsto (3,1,2)$

$\mapsto (3,2,1)$

$\mapsto (1,3,2)$

Defn Let $(G, *)$ be a group and S a set. A group action of $(G,*)$ on S is a map $\mu: G\times S \to S$ satisfying

1) $\forall x, y \in G$, $s \in S$ we have $\mu(x*y, s) = \mu(x, \mu(y,s))$
2) $\mu(e, s) = s$.

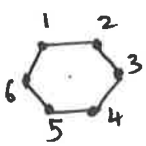
- One usually writes $x(s)$ for $\mu(x,s)$ and thus the axioms become, $(x*y)(s) = x(y(s))$ and $e(s) = s$.

Ex. $\mathrm{Sym}(S)$ acts on S by $\mu: \mathrm{Sym}(S)\times S \to S$, $(f, s) \mapsto f(s)$

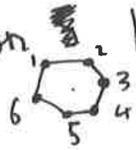
- [Trivial action] G any group and S any set, we have an action $\mu: G\times S \to S$ by $(g,s) \mapsto s$ $(g(s) = s \ \forall g \in G, s \in S)$

- [Conjugation] G acts on itself as a set by conjugation:
  $\mu: G \times G \to G$, $(g, s) \mapsto g*s*g^{-1}$

- [left regular representation] G acts on itself by multiplication on the left,
  $\mu: G\times G \to G$, $(g,s) \mapsto g*s$.

- ~~Rotations~~ Symmetries of  from Lecture 1:

  Let $S = \{1, 2, \ldots, 6\}$ and $G = \mathbb{Z}/6\mathbb{Z} = \{[0], [1], \ldots, [5]\}$.

  Then G acts on  by $[i] \mapsto$ rotate about the center by $i\left(\frac{2\pi}{6}\right)$ radians

More formally we have a map, $\mu: G\times S \to S$ by

- $[0](s) = s \ \forall s \in S$
- $[1]$ maps $1 \mapsto 6$, $2 \mapsto 1$, $3 \mapsto 2$, $4 \mapsto 3$, $5 \mapsto 4$, $6 \mapsto 5$
- $[2]$ maps $1 \mapsto 5$, $6 \mapsto 4$, ...

Exercise: Check this is an action.

Given an action of G on S, we have a map $\phi_g : S \to S$, $s \longmapsto g(s)$.

This is a bijection:

- If $g(s_1) = g(s_2)$, then $g^{-1} * (g(s_1)) = g^{-1} * (g(s_2))$
  $\Rightarrow e(s_1) = e(s_2)$
  $\Rightarrow s_1 = s_2$. Thus ϕ_g is injective.
- If $s \in S$, then $g^{-1}(s) \in S$ and $g(g^{-1}(s)) = (g * g^{-1})(s) = e(s) = s$.
  Thus ϕ_g is surjective.

More succinctly, $\phi_{g^{-1}} = (\phi_g)^{-1}$ i.e.
$(\phi_g \circ \phi_{g^{-1}})(s) = (g * g^{-1})(s) = e(s) = s$.
$\Rightarrow \phi_g \circ \phi_{g^{-1}} = id_S$

Prop We have a homomorphism, $\phi : G \longrightarrow Sym(S)$, $g \longmapsto \phi_g$.

~~Pf First let's check ϕ_g is a homomorphism. Well,~~
~~Well $\phi(gh) = \phi_{gh} : S \to S$, $s \mapsto (gh)(s) = (g*h)(s) = g(h(s))$~~

Pf Well, $\phi(gh) = \phi_{gh}$ maps $s \longmapsto (gh)(s) = g(h(s))$. Thus it's the same as the map $\phi_g \circ \phi_h : S \to S$, $s \mapsto \phi_g(\phi_h(s)) = \phi_g(h(s)) = g(h(s))$.

Thus $\phi(gh) = \phi_g \circ \phi_h = \phi(g) \circ \phi(h)$ ∎

Conversely, any homomorphism $\phi : G \longrightarrow Sym(S)$ gives an action $G \times S \longrightarrow S$, $(g, s) \longmapsto \phi(g)(s)$.

Thus {group actions of G on S} is the same as $\{\phi : G \to Sym(S) \text{ a homomorphism}\}$

Defn An action G on S is called <u>faithful</u> if, the induced map $\phi : G \to Sym(S)$, $g \mapsto \phi_g$ is <u>injective</u>

- G can be thought of as a subgroup of $Sym(S)$ as $G \cong \phi(G) \leq Sym(S)$.

$\boxed{\text{Big}}$ [Cayley's theorem] Let G be a group, then G is isomorphic to a subgroup of $Sym(G)$. If $|G|=n$, then G is isomorphic to a subgroup of S_n.

PF The left regular representation induces a map, $\phi: G \longrightarrow Sym(G)$ and by our previous remark, it suffices to show that ~~ϕ is faithful~~ action is faithful.

Assume $\phi(g) = \phi(h)$

$\Rightarrow \phi_g = \phi_h$

$\Rightarrow g*s = h*s \quad \forall\, s \in \underline{G}$

Since G is a group, cancellation $\Rightarrow g=h$. Thus ϕ is injective ∎

Conclusion To study/understand finite groups, it's enough to understand finite symmetric groups.

Exercises: ① Which of the following are group actions?

a) for $n \in \mathbb{Z}$, $n: \mathbb{R} \to \mathbb{R}$, $n(x) = x+n$

b) $\mathbb{Z}/6\mathbb{Z}$, $X = \mathbb{Z}/7\mathbb{Z}$, $n(x) = x^n$

② Is the following faithful/transitive?

a) $GL_2(\mathbb{R})$ on $\mathbb{R}^2$ by, $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix}$

b) $\mathbb{Z}$ acting on $\mathbb{Z}/9\mathbb{Z}$ by $n(m) = [m+n]$.