9. Group Actions

Groups are often best understood as symmetries of some mathematical object:

S_n permutes the set $\{1, 2, \dots, n\}$

D_{2n} is the symmetry group of a regular n-gon

$GL_n \mathbb{R}$ is the group of isomorphisms of the linear space $\mathbb{R}^n$

Def: A *left action* of a group G on a set S is a map

$$\rho : G \times S \to S$$

such that (i) $\rho(e, s) = s$ $\quad \forall s \in S$

(ii) $\rho(g, \rho(h, s)) = \rho(gh, s)$ $\quad \forall s \in S, g, h \in G$

Note: Each g gives rise to a map $\rho(g, -) : S \to S$, and (i) and (ii) imply that this has an inverse $\rho(g^{-1}, -) : S \to S$

See Section 12 for proof

Let $\mathrm{Sym}(S)$ denote the group of bijections $S \to S$.

Indeed, to give a left action $\rho : G \times S \to S$ is equivalent to give a group homomorphism

$$\rho : G \longrightarrow \mathrm{Sym}(S) \qquad g \longmapsto \rho(g, -)$$

Ex: $G = GL_n \mathbb{R}$, $S = \mathbb{R}^n$

$\rho(A, v) := Av$

Ex: G a group, S any set

$\rho(g, s) := s$ defines the trivial action;

it corresponds to the trivial map $\rho : G \to \mathrm{Sym}(S)$;

Notation: We often simplify notation: $\rho(g, s) \equiv g.s \equiv gs$

Note: Every left action ρ gives rise to a right action $\bar{\rho}(s, g) := \rho(g^{-1}, s)$

Ex: Our convention has been that S_n acts on the right:

$$\rho(k, \sigma) = k\sigma$$

Def: Let G act (on the left of) S. Define:

(i) the orbit of $s \in S$ is the set

$$Orb(s) = \{ gs \in S \mid g \in G \} \subseteq S$$

(ii) the stabilizer of $s \in S$ is the set

$$Stab(s) \overset{!}{=} \{ g \in G \mid gs = s \} \subseteq G$$

If there is only one orbit, the action is transitive

Ex: $GL_n \mathbb{R}$ acts on $\mathbb{R}^n$

there are two orbits: $Orb(\underline{0}) = \{\underline{0}\}$; $Orb(\underline{e}_1) = \mathbb{R}^n \setminus \{\underline{0}\}$

the corresponding stabilizers are: $Stab(\underline{0}) = GL_n \mathbb{R}$; $Stab(\underline{e}_1) = \left\{ A \in GL_n \mathbb{R} \,\middle|\, A = \begin{pmatrix} 1 & * \\ 0 & \\ \vdots & \\ 0 & \end{pmatrix} \right\}$

Ex: G acts (on the left) on itself by conjugation: $p(g,x) := gxg$

$Orb(x) = Conj(x)$ conjugacy class of x

$Stab(x) = \{ g \in G \mid gxg^{-1} = x \}$

$= \{ g \in G \mid gx = xg \}$

$= C(x)$ centralizer of x in G

Ex: $H \subseteq G$ a subgroup

G acts on G/H by $p(g, xH) := gxH$

$Orb(H) = G/H$

$Stab(H) = H$

$Orb(xH) = \{ gxH \mid g \in G \} = G/H$

$Stab(xH) = \{ g \in G \mid gxH = xH \}$

$= \{ g \in G \mid x^{-1} g x \in H \}$

$= \{ g \in G \mid g \in xHx^{-1} \}$

$= xHx^{-1}$

The action is transitive!

Let G act (on the left) of S.

Prop$_1$: The orbits of G partition S.

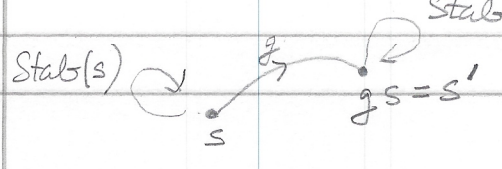
proof: As $e \in G$ and $es = s$ for all $s \in S$, $s \in Orb_G(s)$
$\Rightarrow S = \bigcup_{s \in S} Orb_G(s)$ and $Orb_G(s) \neq \emptyset$
Assume $t \in Orb_G(s) \cap Orb_G(s')$.
Then $t = gs$ and $t = g's'$ for some $g, g' \in G$.
Hence, $gs = g's'$ and $s = g^{-1}g's'$.
So $s \in Orb_G(s')$, and $Orb_G(s) \subseteq Orb_G(s')$
Similarly, $Orb_G(s) \supseteq Orb_G(s')$.

Prop$_2$: The stabilizers, $Stab_G(s)$, are subgroups of G.

proof:
- $e \in Stab_G(s)$ as $es = s$
- if $g, h \in Stab_G(s)$ then $(gh)s = g(hs) = gs = s$ and hence $gh \in Stab_G(s)$
- if $g \in Stab_G(s)$ then $g^{-1}s = g^{-1}(gs) = (g^{-1}g)s = es = s$ and hence $g^{-1} \in Stab_G(s)$

Prop$_3$: If s and s' are in the same orbit then $Stab_G(s)$ and $Stab_G(s')$ are conjugate in G.

proof: As s, s' are in the same orbit, $\exists g \in G : gs = s'$.
Then for $x \in Stab_G(s)$,
$$(gxg^{-1})s' = gxg^{-1}(gs) = gx(es) = g(xs) = gs = s'$$
Hence, $g\, Stab_G(s)\, g^{-1} \subseteq Stab_G(s')$
and similarly, $g^{-1}\, Stab_G(s')\, g \subseteq Stab_G(s)$.



10. Orbit-Stabilizer Theorem

Let G be a finite group acting on S.

Th: For all $s \in S$, $|G| = |\text{Stab}(s)| \times |\text{Orb}(s)|$

proof: By Lagrange's Theorem, $|G/\text{Stab}(s)| = |G|/|\text{Stab}(s)|$.

Define $\phi : G/\text{Stab}(s) \longrightarrow \text{Orb}(s)$

$g\,\text{Stab}(s) \longmapsto gs$

"$\Rightarrow$" "$\Leftarrow$"

ϕ is well-defined and injective as:

$$g\,\text{Stab}(s) = h\,\text{Stab}(s)$$
$$\Leftrightarrow\ g^{-1}h\,\text{Stab}(s)$$
$$\Leftrightarrow\ g^{-1}hs = s$$
$$\Leftrightarrow\ hs = gs$$

ϕ is also surjective and hence, ϕ is a bijection.

Note: The Lagrange's Theorem can be seen to be a special case of Orbit-Stabilizer Theorem:
Let G act on G/H via $p(g, kH) = gkH$.
Then, as seen before, $\text{Orb}(H) = G/H$ and $\text{Stab}(H) = H$.
So $|G| = |\text{Orb}(H)|\,|\text{Stab}(H)| = |G/H|\,|H|$.

Def: A set with an action of G is called a **G-set**.
If S and T are two G-sets, a **map of G-sets** is a map $f: S \to T$ such that $f(gs) = gf(s)$ $\forall s \in S, g \in G$

Note: Every transitive G-set S is isomorphic to the G-set G/H with $p(g, kH) = gkH$ for some subgroup H.
Indeed, pick $s \in S$ and put $H = \text{Stab}(s)$ then
$G/H \longrightarrow S$; $gH \longmapsto gs$ is a bijection of G-sets.

Def: Let G act on S. The set of fixed points is the set

$$\begin{aligned} Fix(S) &= \{ s \in S \mid Stab(s) = G \} \\ &= \{ s \in S \mid Orb(s) = \{s\} \} \end{aligned}$$

Th: Let G be a group of order $|G| = p^n$ for p a prime, $n \geq 1$. Let G act on a finite set S. Then

$$|S| = |Fix(S)| \pmod p$$

proof: The orbits partition S. So

$$|S| = |Fix(S)| + \sum_s |Orb(s)|$$

where the sum is taken over orbit representatives with $|Orb(s)| > 1$.

This is because $|Orb(s)| = 1$ iff $s \in Fix(s)$.

By the Orbit-Stabilizer Theorem,

$$|Orb(s)| = |G| / |Stab(s)|$$

By Lagrange, $|Stab(s)| \mid p^n$.

Thus, if $|Orb(s)| > 1$ then $p \mid |Orb(s)|$

Hence

$$|S| = |Fix(S)| \pmod p$$

Applications: groups acting on groups

Prop: Let G be a group of order $|G| = p^n$, p prime, $n > 1$. Then the centre $Z(G)$ is non-trivial.

proof: G acts on G by conjugation: $\rho(g, x) = gxg^{-1}$

Then $Z(G) = Fix(G)$.

Hence, by the Theorem,

$$|Z(G)| \equiv |G| \equiv 0 \pmod p$$

As $e \in Z(G)$, $Z(G)$ has at least p elements.

Cor: If $|G| = p^2$ then $G \simeq C_{p^2}$ or $G \simeq C_p \times C_p$.

proof. If G has an element of order p^2 then $G \simeq C_{p^2}$.
Assume now that it does not.
By the Proposition above, $\exists\, x \neq e \in Z(G)$.
Let $y \in G \setminus \langle x \rangle$.
Then $\langle x \rangle \cap \langle y \rangle = \{e\}$ and $\langle x \rangle \langle y \rangle = \{x^r y^s \mid r,s = 0,\dots,p-1\} = G$
Also x commutes with y.
So: $(x^r y^s)(x^{r'} y^{s'}) = x^{r+r'} y^{s+s'}$ and $G = C_p \times C_p$.

Recall, that the order $o(g)$ of an element g in a finite group G divides $|G|$.
The following is a partial inverse to this.

Cauchy's Theorem. Let G be a finite group and p be prime.
Then there exist an element $g \in G$ with $o(g) = p$.

proof: Let $S = \{(g_1,\dots,g_p) \in G^p \mid g_1 \cdots g_p = e\} \simeq G^{p-1}$
C_p acts on S by cyclic permutation:

$$g_1 \cdots g_p = e \Rightarrow g_p g_1 g_2 \cdots g_{p-1} = g_p (g_1 g_2 \cdots g_{p-1} g_p) g_p^{-1} = g_p e g_p^{-1} = e$$

$$(g_1,\dots,g_p) \in Fix(S) \iff g_1 = g_2 = \cdots = g_p \text{ and } g_1 \cdots g_p = e$$
$$\iff g_i = x \text{ for } i = 1,\dots,p \text{ and } o(x) = p \text{ or } o(x) = 1$$

There is only one element with $o(x) = 1$, and $(e,e,\dots,e) \in Fix(S)$.
By the above Theorem,

$$|S| \equiv |Fix(S)| \mod p$$

But $|S| = |G|^{p-1} \equiv 0 \mod p$ as $p \mid |G|$
So $|Fix(S)| \geq p$ and G contains at least $p-1$ elements of order p.