Orbit-Stabilizer Theorem

Let $\mu : G \times S \longrightarrow S$ be an action of a group $(G, *)$ on a set S.
$(g, x) \longrightarrow g(x) \Leftarrow$ 1/ $e(x) = x$
2/ $(f * g)(x) = f(g(x))$ $\forall x \in S, f, g \in G$

Definition The orbit of $x \in S$ under the action μ is the subset

$$Orb(x) := \{g(x) \mid g \in G\} \subset S$$

Proposition $\{Orb(x)\}_{x \in S}$ is a partition of S.

Proof

- $e(x) = x \Rightarrow x \in Orb(x) \Rightarrow \bigcup_{x \in S} Orb(x) = S$
- Let $x, y \in S$ and $Orb(x) \cap Orb(y) \neq \emptyset$

$\Rightarrow \exists\ h_1, h_2 \in G$ such that $h_1(x) = h_2(y)$

$\Rightarrow x = h_1^{-1}(h_2(y)) = (h_1^{-1} * h_2)(y)$ and

$y = h_2^{-1}(h_1(x)) = (h_2^{-1} * h_1)(y)$

Let $g \in G$, then

$g(x) = g((h_1^{-1} * h_2)(y)) = (g * h_1^{-1} * h_2)(y) \in Orb(y) \Rightarrow Orb(x) \subset Orb(y)$

$g(y) = g((h_2^{-1} * h_1)(x)) = (g * h_2^{-1} * h_1)(x) \in Orb(x) \Rightarrow Orb(y) \subset Orb(x)$

$\Rightarrow Orb(x) = Orb(y)$

$\square$

Definition An action is <u>transitive</u> iff $Orb(x) = S$ for any $x \in S$.

Remark An action is transitive $\Leftrightarrow$ Given $x, y \in S$, $\exists g \in G$ such that $g(x) = y$

Example Left Regular Representation is <u>always</u> transitive
$(y * x^{-1})(x) = y \quad \forall x, y \in G$

Conjugation is <u>not always</u> transitive. For example $G = GL_n(\mathbb{R})$.

$$Orb(I_n) = \{ A I_n A^{-1} \mid A \in GL_n(\mathbb{R}) \} = \{I_n\} \neq GL_n(\mathbb{R})$$ Not all matrices are similar

action by conjugation

Conjugacy class of $h \in G$ = $Orb(h) = \{ g * h * g^{-1} \mid g \in G \}$

Exercise to check

<u>Definition</u> Let $x \in S$. The stabilizer subgroup of x is the subgroup $Stab(s) := \{ g \in G \mid g(x) = x \} < G$

<u>Orbit-Stabilizer Theorem</u> Let G act on S and $x \in G$

The map $\phi : G/_{Stab(x)} \longrightarrow Orb(x)$ is a bijection.

$$h\,Stab(x) \longrightarrow h(x)$$

In particular $(G : Stab(x)) < \infty \Rightarrow (G : Stab(x)) = |Orb(x)|$

<u>Proof</u>

We must first show it is <u>well defined</u>.

Let $g, h \in G$ such that $g\,Stab(x) = h\,Stab(x)$

$\Rightarrow g^{-1} * h \in Stab(x) \Rightarrow (g^{-1} * h)(x) = x \Rightarrow h(x) = g(x)$

<u>Injective</u> : Let $g\,Stab(x), h\,Stab(x) \in G/_{Stab(x)}$ such that

$\phi(g\,Stab(x)) = \phi(h\,Stab(y)) \Rightarrow g(x) = h(x) \Rightarrow (g^{-1} * h)(x) = x$

$\Rightarrow g^{-1} * h \in Stab(x) \Rightarrow g\,Stab(x) = h\,Stab(x)$

<u>Surjective</u> : $\phi(g\,Stab(x)) = g(x) \quad \forall g \in G$.

$\square$

<u>Corollary</u> : If G acts on a set S and $|G| < \infty$, then

$\forall x \in S$, $|G| = |Stab(x)| \cdot |Orb(x)|$

<u>Proof</u> $\phi : G/_{Stab(x)} \longrightarrow Orb(x)$ a bijection

$$g\,Stab(x) \longmapsto g(x)$$

$$\Rightarrow \quad \left| G/\mathrm{Stab}(x) \right| = \left| \mathrm{Orb}(x) \right| \quad \Rightarrow \frac{|G|}{|\mathrm{Stab}(x)|} = \left| \mathrm{Orb}(x) \right|$$

$$\Rightarrow \quad |G| = |\mathrm{Stab}(x)| \cdot |\mathrm{Orb}(x)|$$

$\square$

We can clever group actions to prove interesting things about groups.

Sylows Theorem

must be prime

Let G be a finite group and $p^n \mid |G|$ where p is a prime and $n \in \mathbb{N}$. Then $\exists H \subset G$, a subgroup, such that $|H| = p^n$.

Proof

Let $|G| = p^n m$, where $m = p^r u$ with $HCF(u, p) = 1$

Strategy: Come up with a set S with an action of G such that $\exists x \in S$ with $|\mathrm{Stab}(x)| = p^n$

S = Collection of all (unordered) subsets of G of size p^n.

after fixing an orderin

Let $x = \{w_1, w_2, \ldots, w_{p^n}\}$. We define an action of G on S by

$$\mu: G \times S \longrightarrow S$$
$$(g, x) \longmapsto \underbrace{\{g * w_1, g * w_2, \ldots, g * w_{p^n}\}}_{= g(x)}$$

- <u>Claim</u> $\forall x \in S$, $|\mathrm{Stab}(x)| \leq p^n$

Define the function $f : \mathrm{Stab}(x) \longrightarrow x$
$g \longrightarrow g * \omega_1$

Let $g, h \in \mathrm{Stab}(x)$ such that $f(g) = f(h)$
(c.c.)

$\Rightarrow$ $g * \omega_1 = h * \omega_1$ $\Rightarrow$ $g = h$

$\Rightarrow$ f injective $\Rightarrow$ $|\mathrm{Stab}(x)| \leq |x| = p^n$

- <u>Claim</u> $\exists x \in S$ such that $|\mathrm{Stab}(x)| \geq p^n$

Observe that

$|S|$ = Number of ways of choosing p^n elements from a set of size $p^n m = p^n . p^r . u$

$$\Rightarrow |S| = \binom{p^n m}{p^n} = \frac{p^n m!}{p^n! \, (p^n m - p^n)!} = \frac{p^n m (p^n m - 1) \dots (p^n m - (p^n - 1))}{p^n (p^n - 1) \dots (p^n - (p^n - 1))}$$

$$= p^r u \frac{(p^n m - 1)}{(p^n - 1)} \cdot \frac{(p^n m - 2)}{(p^n - 2)} \cdot \dots \frac{(p^n m - (p^n - 1))}{(p^n - (p^n - 1))}$$

If $j \in \mathbb{N}$ and $j < p^n$ $\Rightarrow$ j divisible by p at most $n-1$ times

Hence

Number of times p divides $p^n m - j$ = Number of times p divides j = Number of times p divides $p^n - j$

$\Rightarrow \quad \dfrac{(p^n m - j)}{(p^n - j)}$ has no factors of p in its prime decomposition $\forall\ 0 < j < p^n$.

$\Rightarrow \quad |S|$ is divisible by p exactly r times.

Recall that $\{Orb(x)\}_{x \in S}$ partition S. Let $x_1, \ldots, x_k$ be representatives of each orbit. Then

$$|Orb(x_1)| + |Orb(x_2)| + \ldots + |Orb(x_k)| = |S|$$

We deduce that there must be some $x_i \in S$ such that $|Orb(x_i)|$ is not divisible by p more than r times.

For this x let $|Orb(x_i)| = p^s v$, $s \leq r$ and $HCF(v, p) = 1$
$(r - s \geq 0)$

$$\Rightarrow \quad |Stab(x_i)| = \frac{|G|}{|Orb(x_i)|} = \frac{p^n \cdot p^r u}{p^s v} = p^n \cdot p^{r-s} \frac{u}{v} \in \mathbb{N}$$

u, v coprime to p and $p^n \cdot p^{r-s} \frac{u}{v} \in \mathbb{N} \Rightarrow \frac{u}{v} \in \mathbb{N}$

$$\Rightarrow \quad |Stab(x_i)| \geq p^n$$

But $|Stab(x)| \leq p^n \quad \forall x \in S$

$$\Rightarrow \quad |Stab(x_i)| = p^n$$

$\square$