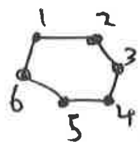
Orbit - Stabiliser

Defn. Let $(G,*)$ be a group acting on a set S. The orbit of s, denoted $\mathrm{orb}(s)$, is the set $\{g(s) : g \in G\}$.

[One can obtain this as the equivalence class of $[s]$ where the relation is $s \sim r \iff \exists\, g \in G$ such that $g(s) = r$]

Ex. • The orbit of 1 in



under ~~that~~ the action of $\mathbb{Z}/6\mathbb{Z}$ is $\{1,2,3,4,5,6\}$

Defn Let G be a group acting on a set S. G acts transitively on S if there is only one orbit.

$\iff \mathrm{orb}(s) = S \;\; \forall\, s \in S$

$\iff \forall\, s,t \in S, \; \exists\, g \in G$ such that $g(s) = t$.

Ex • The action of $\mathbb{Z}/n\mathbb{Z}$ on the regular n-gon given by rotation is transitive

• $\mathrm{Sym}(S)$ acting naturally on S is transitive.
(Given $s_1, s_2 \in S$, $\exists$ a bijection $f : S \longrightarrow S$ mapping $s_1 \longmapsto s_2$)

• Conjugation of G is transitive $\iff$ G is trivial
($\mathrm{orb}(e) = \{geg^{-1} : g \in G\} = \{e\}$)

• The left regular rep. of G on G is transitive.

Defn Given $s \in S$, the stabiliser of s is
$$\mathrm{stab}(s) := \{g \in G : g(s) = s\}.$$

Prop $\mathrm{stab}(s) \leq G$ is a subgroup.

Pf
- $e(s) = e \Rightarrow e \in \mathrm{stab}(s)$
- $g \in \mathrm{stab}(s) \Rightarrow g(s) = s$
  $\Rightarrow g^{-1}(g(s)) = g^{-1}(s)$
  $\Rightarrow (g^{-1} * g)(s) = g^{-1}(s)$
  $\Rightarrow e(s) = g^{-1}(s)$
  $\Rightarrow s = g^{-1}(s) \Rightarrow g^{-1} \in \mathrm{Stab}(s)$.
- $g, h \in \mathrm{stab}(s) \Rightarrow (g * h)(s) = g(h(s)) = g(s) = s$
  $\Rightarrow g * h \in \mathrm{stab}(s)$

Since $\mathrm{stab}(s)$ is a subgroup, $G/\mathrm{stab}(s) = \{x \cdot \mathrm{stab}(s) : x \in G\}$ is the set of left cosets.

~~Since~~ Note,
$$\begin{aligned} x \sim_L y &\Leftrightarrow x^{-1} * y \in \mathrm{stab}(s) \\ &\Leftrightarrow (x^{-1} * y)(s) = s \\ &\Leftrightarrow (x(x^{-1} * y))(s) = x(s) \\ &\Leftrightarrow y(s) = x(s). \end{aligned}$$

Thus, there is a map of sets,
$$\begin{aligned} \phi : G/\mathrm{stab}(s) &\longrightarrow \mathrm{orb}(s) \\ x\,\mathrm{stab}(s) &\longmapsto x(s) \end{aligned}$$

Prop ϕ is a bijection

Pf The equivalence above proves injectivity. Surjectivity follows from the definition of $\mathrm{orb}(s) = \{x(s) : x \in G\}$ ∎

Big [Orbit-Stabilizer theorem] Let G be a group acting on a set S. Let $s \in S$ be an element of finite orbit ($|\mathrm{orb}(s)| < \infty$). Then $\mathrm{stab}(s) \leq G$ has finite ~~order~~ index and

$$[G : \mathrm{stab}(s)] = |\mathrm{orb}(s)|.$$

Pf By definition, $[G : \mathrm{stab}(s)]$ ~~$= G/\mathrm{stab}(s)$~~
$= |G/\mathrm{stab}(s)| = |\mathrm{orb}(s)|$ ∎

Cor Let G be a finite group acting on a set S and $s \in S$.
Then $|G| = |\mathrm{stab}(s)| \cdot |\mathrm{orb}(s)|$.

Pf If G is a finite group and H a subgroup. The proof of Lagrange's theorem shows that $|G| = |H| \cdot [G : H]$.
Take $H = \mathrm{stab}(s)$ ∎

This is immensely helpful in showing the existence of subgroups.

Thm Let G be a non-trivial group of order p^n, for p a prime.
Then the center, $Z(G)$, of G is non-trivial.

Pf Let G act on itself by conjugation. By Hwk 2, 6c,d,
~~orb~~ $\mathrm{orb}(g) = |G/Z(g)| > 1 \iff g \notin Z(G)$.

By orbit stabiliser, $|\mathrm{orb}(g)| \mid p^n \implies p \mid |\mathrm{orb}\, g| \;\forall g \notin Z(G)$
Since the orbits form a partition of G we obtain,
$|G| = p^n = |Z(G)| + p \cdot k$.

If $Z(G) = \{e\}$ is trivial $\implies p^n = |\{e\}| + pk = 1 + pk$.
This contradicts divisibility. Thus $Z(G)$ is non-trivial ∎

Conjugacy class of $g = \{hgh^{-1} : h \in G\} = \mathrm{orb}(g)$ under conjugation action.

Now we can prove a partial converse to Lagrange's theorem

Thm [Sylow's first] Let G be a finite group such that $p^n \mid |G|$, where p is a prime & $n \geq 1$. Then there exists a subgroup of order p^n.

Pf Let $|G| = p^n m$ with $m = p^r u$ and $\gcd(p,u)=1$.
Let $S = \{$subsets of G of size $p^n\}$. Note that $|S| = \binom{p^n m}{p^n}$

G acts on S as follows: If $A = \{A_1, \dots, A_{p^n}\} \in S$
$$\Rightarrow g(A) := \{g \cdot A_1, \dots, g \cdot A_{p^n}\}.$$

① $|\mathrm{stab}(A)| \leq p^n$: Define $f : \mathrm{stab}(A) \longrightarrow A$, $g \mapsto g \cdot A_1$. ← first entry of a ordered set.
This is an injective map ($f(g)=f(h) \Rightarrow gA_1 = hA_1 \Rightarrow g = h$ (cancellation)).
Thus $|\mathrm{stab}(A)| \leq |A| = p^n$.

② $|S| = p^r v$ with $\gcd(p,v)=1$:
$$|S| = \binom{p^n m}{p^n} = \frac{(p^n m)!}{p^n!\,(p^n m - p^n)!} = \prod_{j=0}^{p^n-1} \frac{p^n m - j}{p^n - j} = m \prod_{j=1}^{p^n-1} \frac{p^n m - j}{p^n - j}$$

[Exercise: Show that $\prod_{j=1}^{p^n-1} \frac{p^n m - j}{p^n - j}$ has no factors of p (Hint: For $1 \leq j \leq p^n - 1$, j is divisible p at most $n-1$ times. Thus $p^n - j$ has the same number of factors of p as j]

Thus $|S| = m \cdot k$ with $\gcd(k,p)=1 \Rightarrow |S| = p^r u k$ and $\gcd(uk, p) = 1$.
Since S is a disjoint union of orbits, $\exists\, A \in S$ s.t. $|\mathrm{orb}(A)| = p^s t$ with $s \leq r$ and $\gcd(p,t)=1$. By orbit stabiliser, $|\mathrm{stab}(A)| = \dfrac{p^{n+r} u}{p^s t} = p^{n+r-s} \cdot \dfrac{u}{t}$.
Since $|\mathrm{stab}(A)| \in \mathbb{Z} \Rightarrow \frac{u}{t} \in \mathbb{Z}$ as u, t coprime to p.
Thus $|\mathrm{stab}(A)| \geq p^{n+r-s} \geq p^n$. Thus $|\mathrm{stab}(A)| = p^n$ and ← refer to ①
$\mathrm{stab}(A)$ is the desired subgroup ∎