Group Action

Liming Pang

1 Definition of Groups Actions

Definition 1. \( G \) is a group, and \( X \) is a set. A \textbf{group action} (also called \textbf{group operation}) of \( G \) on \( X \) is a map

\[
G \times X \longrightarrow X
\]

\[
(g,x) \mapsto g.x
\]

satisfying:

1. \( 1.x = x \) for any \( x \in X \)
2. \( g_1.(g_2.x) = (g_1g_2).x \) for any \( g_1, g_2 \in G \), any \( x \in X \).

We see from the definition that when a group action of \( G \) on \( X \) is given, each \( g \in G \) induces a function \( \tau_g : X \longrightarrow X \) sending \( x \) to \( g.x \)

Proposition 2. If \( G \) acts on \( X \), then any \( g \in G \) induces a bijection:

\[
\tau_g : X \longrightarrow X
\]

\[
x \mapsto g.x
\]

Proof. We need to verify \( \tau_g \) is bijective, which can be done by verifying \( \tau_g^{-1} \) is the inverse function of \( \tau_g \).

\[
\tau_g \circ \tau_g^{-1}(x) = g.(g^{-1}.x) = (gg^{-1}).x = 1.x = x
\]

\[
\tau_g^{-1} \circ \tau_g(x) = g^{-1}.(\tau.x) = (g^{-1}g).x = 1.x = x
\]

Example 3. \( S_n \) acts on \( X = \{1,2,...,n\} \) in a natural way: \( \sigma \in S_n \) acts on \( k \in X \) by \( \sigma.k = \sigma(k) \)
Example 4. $G$ is a group, then $G$ can act on itself by left multiplication: $g.x = gx$

Example 5. $GL_n(\mathbb{R})$ acts on $\mathbb{R}^n$ by matrix multiplication:

$$GL_n(\mathbb{R}) \times \mathbb{R}^n \to \mathbb{R}^n$$

$$(A, \vec{u}) \mapsto A\vec{u}$$

Example 6. A group $G$ acts on itself by conjugation: $g.x = g x g^{-1}$

Definition 7. $G$ is a group acting on a set $X$, and $x \in X$. The orbit of $x$ is defined to be

$$O(x) = \{ y \in X | g.x = y \text{ for some } g \in G \}$$

Lemma 8. $G$ acts on $X$. The relation on $X$ defined by $x \sim y$ if $y = g.x$ for some $g \in G$ is an equivalence relation, and each orbit is an equivalence class.

Proof. (i). For any $x \in X$, $1.x = x$, so $x \sim x$

(ii). If $x \sim y$, then $y = g.x$ for some $g \in G$, $x = 1.x = (g^{-1}g).x = g^{-1}.g.x = g^{-1}.y$, so $y \sim x$

(iii). If $x \sim y$ and $y \sim z$, then there exist $g_1, g_2 \in G$ such that $y = g_1.x$ and $z = g_2.y$, so $z = g_2.(g_1.x) = (g_1g_2).x$, $x \sim z$

We can thus conclude it is an equivalence relation. And it follows directly by definition that each equivalence class is an orbit.

Corollary 9. The orbits form a partition of $X$.

Example 10. In the example of $GL_n(\mathbb{R})$ acting on $\mathbb{R}^n$ by matrix multiplication, there are two orbits: $\mathbb{R}^n \setminus \{\vec{0}\}$ and $\{\vec{0}\}$.

$\{\vec{0}\}$ is an orbit since for any $A \in GL_n(\mathbb{R})$, $A.\vec{0} = \vec{0}$

$\mathbb{R}^n \setminus \{\vec{0}\}$ is the only other orbit since for any $\vec{v} \neq \vec{0}$, we can extend $\vec{v}$ to a basis ($\vec{v}_1 = \vec{v}, \vec{v}_2, ..., \vec{v}_n$). Then let the matrix $B \in GL_n(\mathbb{R})$ be the one whose $i$-th column is $\vec{v}_i$ for $1 \leq i \leq n$, we see that $\vec{v} = B.\vec{e}_1$, so $O(\vec{e}_1) = \mathbb{R}^n \setminus \{\vec{0}\}$ is an orbit.

Definition 11. A group $G$ acts on a set $X$. If there is only one orbit for this action, we say the action is transitive.

Example 12. $G$ acting on itself by left multiplication is a transitive action: for any $x \in G$, let $g = x \in G$, then $x = g.1$, $x \in O(1)$, so there is only one orbit.
Lemma 13. An action of $G$ on $X$ is transitive if and only if for any $x \in X, y \in X$, there exists $g \in G$ such that $y = g.x$

Proof. if $G$ acts transitively on $X$, then there is only one orbit, we get $O(x) = O(y)$, in particular $y \in O(y) = O(x)$, so there exists $g \in G$ such that $y = g.x$

Conversely, for any $x \in X, y \in X$, if $x = g.y$ for some $g \in G$, then $O(x) = O(y)$, so there is only one orbit.

Definition 14. $G$ acts on $X$. Define the stabiliser of $x \in X$ to be

$$G_x = \{ g \in G | g.x = x \}$$

Proposition 15. $G$ acts on $X$, and $x \in X$, then $G_x$ is a subgroup of $G$.

Proof. (1). If $g, g' \in G_x$, $(gg').x = g.(g'.x) = g.x = x$, so $gg' \in G_x$

(2). $1.x = x$, so $1 \in G_x$

(3). If $g \in G_x$, then $g.x = x \implies g^{-1}.(g.x) = g^{-1}.x \implies (g^{-1}g).x = g^{-1}.x \implies 1.x = g^{-1}.x \implies g^{-1} \in G_x$ □

Example 16. $G$ acts on $G$ by left multiplication, then for any $x \in G, G_x = \{ g \in G | gx = x \} = \{1\}$

Example 17. $G$ acts on $G$ by conjugation. Each orbit $O(x) = \{ gxg^{-1} \in G | g \in G \}$ is called a conjugacy class of $G$.

$G_x = \{ g \in G | gxg^{-1} = x \}$ is called the normaliser of $x$.

Proposition 18. $G$ is a group acting on $X$. $x \in X, g_1, g_2 \in G$. Then $g_1.x = g_2.x$ if and only if $g_1G_x = g_2G_x$

Proof. $g_1.x = g_2.x \iff g_2^{-1}(g_1.x) = g_2^{-1}(g_2.x) \iff (g_2^{-1}g_1).x = x \iff g_2^{-1}g_1 \in G_x \iff g_1G_x = g_2G_x$ □

Exercise 19. $G$ is a group acting on $X$. $x, x' \in X$ and $g \in G$ such that $x' = g.x$. Prove

$$G_{x'} = gG_xg^{-1} = \{ ghg^{-1} | h \in G_x \}$$

Proposition 20. $X$ is a set, $P(X)$ is the group bijections $X \longrightarrow X$ with composition of functions. $G$ is a group. Then there is a one-to-one correspondence between the groups actions of $G$ on $X$ and homomorphisms $G \longrightarrow P(X)$. 
Proof. If there is a $G$-action on $X$, then we can define a homomorphism

$$G \rightarrow P(X)$$

where $\Phi(g) : X \rightarrow X$ is defined by $\Phi(g)(x) = g.x$ (It is left as an exercise to check $\phi$ is a homomorphism.)

Conversely, given a homomorphism $\Phi : G \rightarrow P(X)$, we can define a $G$-action on $X$ by $g.x = \Phi(g)(x)$ (It is also left as an exercise to check this is a group action)

\[\square\]

2 Applications

Theorem 21. (The Counting Formula) $G$ is a finite group acting on a set $X$. For each $x \in X$, let $G_x$ be the stabiliser of $x$ and $O(x)$ be the orbit of $x$. Then:

$$|G| = |G_x||O(x)|$$

i.e. $|O(x)| = [G : G_x]$

Proof. Define $f : G/G_x \rightarrow O(x)$ by $f(gG_x) = g.x$

By Proposition 18, $f(g_1G_x) = f(g_2G_x)$ if and only if $g_1G_x = g_2G_x$, it follows $f$ is well-defined and also injective.

The surjectivity of $f$ follows directly from the definition of orbit.

\[\square\]

Example 22. $D_n$ acts on the set $V$ of $n$ vertices of a regular $n$-gon. This is a transitive action, so for any vertex $v \in V$, its orbit $O(v) = V$. So

$$G_v = \frac{|D_n|}{|V|} = \frac{2n}{n} = 2$$

And explicitly, the two elements in $G_v$ are identity and reflection along the line passing through $v$ and the centre of the $n$-gon.

Proposition 23. If $H, K$ are finite subgroup of $G$, then

$$|HK| = \frac{|H| \times |K|}{|H \cap K|}$$
Proof. The product group $H \times K$ acts on $G$ by $(h,k) \cdot g = h g k^{-1}$. (It is left as an exercise to verify that this is a group action.)

Consider then stabiliser of the identity:

$$G_1 = \{(h,k) \in H \times K | (h,k) \cdot 1 = 1\} = \{(h,k) \in H \times K | h = k\} = \{(x,x) | x \in H \cap K\}$$

So $|G_1| = |H \cap K|$. The Counting Formula then can be applied to conclude

$$|H \times K| = |O(1)| = \frac{|H \times K|}{|G_1|} = \frac{|H| \times |K|}{|H \cap K|}$$

Recall that a group $G$ can act on itself by conjugation. Each orbit of this action is a conjugacy class $C_x$, so all the conjugacy classes form a partition of $G$.

For $x \in G$, it is easy to see $|O(x)| = 1$ if and only if $gxg^{-1} = x$ for any $g \in G$, which is same as $x \in Z(G)$. So the partition described above implies:

**Proposition 24.** (Class Equation) $|G|$ is a finite group, then:

$$|G| = |Z(G)| + \sum_{x \in S} |C_x| = |Z(G)| + \sum_{x \in S} \frac{|G|}{|N(x)|}$$

where $S$ is a set of representatives of conjugacy classes with size at least 2, $C_x$ is the conjugacy class of $x$, and $N(x)$ is the normaliser of $x$.

**Proposition 25.** If $p$ is a prime number, then every group of order $p^2$ is abelian.

**Proof.** Let $G$ be a group of order $p^2$. By the Class Equation:

$$p^2 = |G| = |Z(G)| + \sum_{x \in S} |C_x|$$

Since for any $x \in S$, $1 < |C_x| < |G| = p^2$ and $|C_x|$ is divisible by $p$, we see $|C_x| = p$, so the above class equation implies $|Z(G)|$ is divisible by $p$, i.e., $|Z(G)| = p$ or $|Z(G)| = p^2$.

Now we are going to show the case $|Z(G)| = p$ is impossible, then we conclude $|Z(G)| = G$, which is same as $G$ abelian.

Suppose $|Z(G)| = p$, we take $g \in G \setminus Z(G)$. Note $Z(G) \subseteq N(g)$ and $g \in N(g)$, so $|N(g)| \geq |Z(G)| + 1 = p + 1$. But $|N(g)|$ divides $|G| = p^2$ since $|N(g)|$ is a subgroup of $G$, we get $|N(g)| = G$, which means $g \in Z(G)$, contradiction. 

\[ \square \]
**Theorem 26. (Cauchy’s Theorem)** If $G$ is a group, and $p$ is a prime number that divides $|G|$, then $G$ has an element of order $p$.

**Proof.** Let $C_p = < a >$, the cyclic group of order $p$. $C_p$ acts on

$$Y = \{(g_1, g_2, ..., g_p) \in G \times ... \times G | g_1 g_2 ... g_p = 1 \}$$

by the rule

$$a.(g_1, g_2, ..., g_{p-1}, g_p) = (g_2, g_3, ..., g_p, g_1)$$

(Note that if $g_1 g_2 ... g_p = 1$, then the product of a cyclic permutation of them is still 1)

$$|Y| = |G|^{p-1},$$

since the last coordinate is determined by the first $n - 1$ coordinates.

And observe that $(g_1, ..., g_p)$ is a fixed point if and only if $g_1 = g_2 = ... = g_p = g$ for some $g \in G$ such that $g^p = 1$.

Since the size of each orbit divides $|C_p| = p$, and $|Y| = |G|^{p-1}$ is divisible by $p$, there must be some other fixed points besides $(1, ..., 1)$, and those fixed points $(x, ..., x)$ where $x \neq 1$ give elements $x \in G$ of order $p$. 

\[\square\]