

Contents

1	Groups	1
1.1	Group Actions	1
1.2	Applications	3

Chapter 1

Groups

1.1 Group Actions

Definition 1. A right action of a group G on a nonempty set X is a function

$$X \times G \rightarrow X, \quad (x, g) \mapsto xg,$$

such that:

- i. $x(gh) = (xg)h$ for all $g, h \in G$ and $x \in X$;
- ii. $x1 = x$ for all $x \in X$.

The set X is called a G -set. A left action is defined in a similar fashion.

Example 1. Let S_n be the symmetric group of degree n . Then, S_n acts on the set $\{1, \dots, n\}$ from the right in a rather natural way:

$$\{1, \dots, n\} \times S_n \rightarrow \{1, \dots, n\}, \quad (x, \alpha) \mapsto x^\alpha.$$

Example 2. Let G be a group. Then, G acts on itself from the right by conjugation:

$$G \times G \rightarrow G, \quad (x, g) \mapsto x^g = g^{-1}xg.$$

Definition 2. Let X be a G -set. Then, following common terminology, the set:

- i. $\text{orb}(x, G) = \{y \in X : y = gx \text{ for some } g \in G\}$ is called the G -orbit of x ;
- ii. $\text{stab}(x, G) = \{g \in G : xg = x\}$ is called the G -stabilizer of x ,

for any $x \in X$.

Proposition 1. *Let X be a G -set. Then, the binary relation given by*

$$(1.1) \quad \forall x, y \in X : \quad x \equiv y \pmod{G} \iff \exists g \in G : xg = y,$$

is an equivalence relation on X . Moreover, the equivalence class

$$\{y \in X : x \equiv y \pmod{G}\},$$

equals $\text{orb}(x, G)$, the G -orbit of x , for any point $x \in X$.

Proof. For any given x, y and z in X , we have that:

1. $x \equiv x \pmod{G}$ for every $x \in X$, since $x1 = x$;
2. If $x \equiv y \pmod{G}$, then $xg = y$ for some $g \in G$. But, then $yg^{-1} = x$ and so $y \equiv x \pmod{G}$;
3. If $x \equiv y \pmod{G}$ and $y \equiv z \pmod{G}$, then we have that $xg = y$ and $yh = z$ for certain $g, h \in G$. Therefore, $x(gh) = (xg)h = yh = z$ and so $x \equiv z \pmod{G}$.

Now, notice that if $y \in \{y \in X : x \equiv y \pmod{G}\}$, then $y = gx$ for some $g \in G$. Conversely, for any $g \in G$, $gx \equiv x \pmod{G}$ because $g^{-1} \in G$ and $g^{-1}(gx) = (g^{-1}g)x = 1x = x$. Therefore, we conclude that

$$\{y \in X : x \equiv y \pmod{G}\} = \{gx : g \in G\} = \text{orb}(x, G).$$

This completes the proof. □

Suppose that X is a finite G -set. Let $T \subset X$ be a set with the following properties:

1. $X = \bigcup \{\text{orb}(x, G) : x \in T\}$.
2. $\forall x, x' \in T : \quad x \neq x' \implies \text{orb}(x, G) \cap \text{orb}(x', G) = \emptyset$;

Then, it's clear that

$$(1.2) \quad |X| = \sum_{x \in T} |\text{orb}(x, G)| = \sum_{x \in T} (G : \text{stab}(x, G)).$$

Proposition 2. *Let X be a G -set. Then, for any $x \in X$, $\text{stab}(x, G)$ is a subgroup of G and the cardinality of $\text{orb}(x, G)$, the G -orbit of x , equals the index $(G : \text{stab}(x, G))$ of $\text{stab}(x, G)$ in G .*

Proof. Let $x \in X$ be given. The identity element of G obviously belongs to $\text{stab}(x, G)$ and, for any pair of elements $g, h \in \text{stab}(x, G)$, we have that

$$x(gh^{-1}) = (xg)h^{-1} = xh^{-1} = (xh)h^{-1} = x(hh^{-1}) = x1 = x,$$

and as such $gh^{-1} \in \text{stab}(x, G)$. Therefore, $\text{stab}(x, G)$ is a subgroup of G . Now, regarding the function

$$G/\text{stab}(x, G) \rightarrow \text{orb}(x, G), \quad \text{stab}(x, G)g \mapsto xg.$$

it's true that

$$\begin{aligned} xg = xh &\iff x(gh^{-1}) = x \iff gh^{-1} \in \text{stab}(x, G) \\ &\iff \text{stab}(x, G)g = \text{stab}(x, G)h, \end{aligned}$$

for every pair of elements $g, h \in G$, from what it follows that $\text{stab}(x, G)g \mapsto xg$ is an injective function, as well as

$$y \in \text{orb}(x, G) \iff \exists g \in G : y = xg \implies \text{stab}(x, G)g \mapsto y = xg,$$

which shows that $\text{stab}(x, G)g \mapsto xg$ is also onto. Henceforth, $|\text{orb}(x, G)| = (G : \text{stab}(x, G))$ as claimed. This completes the proof. \square

1.2 Applications

Proposition 3. *Let G be a finite p -group. Then, G has a nontrivial center.*

Proof. Let G act on itself from the right by conjugation. Then, we have that

$$\text{orb}(x, G) = \{x^g : g \in G\} = \{x\} \iff x \in Z(G),$$

for any $x \in G$. Therefore,

$$|G| = \sum_{x \in Z(G)} |\text{orb}(x, G)| + \sum_{x \notin Z(G)} |\text{orb}(x, G)| = |Z(G)| + \sum_{x \notin Z(G)} (G : \text{stab}(x, G))$$

\square

Theorem 1 (Cauchy). *Let G be a finite group and p be a prime divisor of $|G|$. Then, there is some $g \in G$ such that $|g| = p$.*

Proof. The graph of the function

$$f : G^{p-1} \rightarrow G, \quad (x_1, \dots, x_{p-1}) \mapsto \left(\prod_{i=1}^{p-1} x_i \right)^{-1},$$

is the set

$$\Omega = \left\{ (x_1, \dots, x_p) \in G^p : \prod_{i=1}^p x_i = 1 \right\},$$

which has $|G|^{p-1}$ elements in total, a number divisible by p . Consider the action of the additive group \mathbb{Z}_p on the set Ω from the right given by

$$(x_1, x_2, \dots, x_{p-1}, x_p) \cdot \bar{1} = (x_p, x_1, \dots, x_{p-2}, x_{p-1}).$$

The \mathbb{Z}_p -orbit of a point $x = (x_1, \dots, x_p) \in \Omega$ consists of the element x alone if, and only if, the coordinates $x_1, x_2, \dots, x_{p-1}, x_p$ of x are all equal to one another, that is, $x_1 = x_2 = \dots = x_{p-1} = x_p$. This is certainly the case for the element $(1, \dots, 1) \in \Omega$ whose coordinates are all equal to the identity element of G . Let $T \subset \Omega$ be a transversal for the action of \mathbb{Z}_p on Ω , meaning that:

1. $\Omega = \bigcup \{\text{orb}(x, \mathbb{Z}_p) : x \in T\}$;
2. $\forall x, x' \in T : x \neq x' \implies \text{orb}(x, \mathbb{Z}_p) \cap \text{orb}(x', \mathbb{Z}_p) = \emptyset$.

Then, we have that

$$|\Omega| = \sum_{x \in T} |\text{orb}(x, \mathbb{Z}_p)| = \sum_{|\text{orb}(x, \mathbb{Z}_p)|=1} 1 + \sum_{|\text{orb}(x, \mathbb{Z}_p)|>1} (\mathbb{Z}_p : \text{stab}(x, \mathbb{Z}_p)).$$

Since

$$|\Omega| \quad \text{and} \quad \sum_{|\text{orb}(x, \mathbb{Z}_p)|=1} (\mathbb{Z}_p : \text{stab}(x, \mathbb{Z}_p)),$$

are both divisible by p , so is

$$\sum_{|\text{orb}(x, \mathbb{Z}_p)|>1} 1.$$

This last sum would be equal to zero if there were no \mathbb{Z}_p -orbits of size 1 at all in Ω , but as we've already seen there's that of the element $x = (1, \dots, 1)$. Therefore, there must exist some $g \in G$, $g \neq 1$, with

$$\text{orb}((x, \dots, x), \mathbb{Z}_p) = \{(x, \dots, x)\},$$

from what we get that $x^p = 1$. This completes the proof. \square