

## 12 Group Actions

**Definition 12.1.** An *action* of a group  $G$  on a set  $X$  is defined to be a homomorphism:

$$\alpha : G \rightarrow S_X$$

written  $\alpha(g)(x) = g \cdot x = "gx"$ . Here  $S_X$  is the group of permutations of  $X$ .

This definition can be rephrased as follows. The action gives a mapping

$$G \times X \rightarrow X$$

sending each  $(g, x) \in G \times X$  to  $g \cdot x \in X$  so that

1.  $e \cdot x = x$  for all  $x \in X$  and
2.  $g \cdot (h \cdot x) = (gh) \cdot x$  for all  $g, h \in G$  and  $x \in X$ .

A very important example of an action is the *conjugation action* of a group  $G$  on itself (i.e., on  $X = G$ ). This is given by:

$$g \cdot x := gxg^{-1}.$$

**Definition 12.2.** The *orbit*  $O(x)$  of an element  $x \in X$  is defined to be the set

$$O(x) = Gx = \{gx \mid g \in G\}.$$

The notation  $O(x)$  is used since the action is not always multiplication.

Note that, since  $e \in G$ , the orbit of  $x$  contains  $ex = x$  itself:

$$x \in O(x)$$

We proved in class that the orbits  $O(x)$  of an action of  $G$  on  $X$  form a *partition* of  $X$ , i.e.:

$$X = \coprod O(x_i)$$

In other words

1. The orbits are either disjoint or equal.
2.  $X$  is a union of orbits. ( $X = \cup O(x)$ ).

(Note that, in order to get a disjoint union, we needed to choose a representative  $x_i$  from each orbit.)

**Example 12.3.** The orbit of  $x \in G$  under the conjugation action is the set of conjugates of  $x$ :

$$O(x) = x^G = \{y \in G \mid y = gxg^{-1} \text{ for some } g \in G\}$$

**Example 12.4.** The orbit of  $x = (12)(345)$  in  $S_5$  is

$$O((12)(345)) = \{(ab)(cde)\}.$$

**Definition 12.5.** The *stabilizer* of  $x \in X$  is the set

$$G_x = \{g \in G \mid gx = x\}$$

**Theorem 12.6.** *The stabilizer is always a subgroup of  $G$ .*

*Proof.* Obvious. □

**Example 12.7.** When the action is conjugation, the stabilizer of  $x \in X = G$  is called the *centralizer* of  $x$  in  $G$ .

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

Note:  $C_G(x)$  always contains  $e$  and  $x$ . It also contains all powers of  $x$  so:

$$\langle x \rangle \leq C_G(x) \leq G$$

The centralizer is related to the *center* of  $G$ :

1.  $Z(G) = \cap_{x \in G} C_G(x)$
2.  $x \in Z(G)$  iff  $C_G(x) = G$ .

**Example 12.8.** Suppose that  $X = G/H$  is the set of cosets of  $H$ . (This means that the elements of  $X$  are subsets  $gH \subseteq G$ .) The action of  $G$  on  $X = G/H$  is given by left multiplication:

$$g \cdot xH = gxH$$

Then the stabilizer of  $H = eH$  (considered as one element of  $X = G/H$ ) is

$$G_H = \{g \in G \mid gH = H\} = H.$$

(The stabilizer of the element  $H$  is the subgroup  $H$ .)

## 12.1 Orbit size formula

The main theorem about stabilizers is the following.

**Theorem 12.9 (Orbit size formula).** *The size of the orbit of  $x \in X$  is equal to the index of the stabilizer:*

$$|O(x)| = |G : G_x| = \frac{|G|}{|G_x|}$$

Another version of the same formula is:

$$|G_x| = \frac{|G|}{|O(x)|}.$$

**Example 12.10.** Take that conjugation action of  $G$  on  $G$ . Then  $|O(x)|$  is the number of conjugates of  $x$  and  $G_x = C_G(x)$ . So the formula is

$$\#conj \text{ of } x = |G : C_G(x)| = \frac{|G|}{|C_G(x)|}$$

For example, if  $x \in Z(G)$  then  $|O(x)| = 1$  and  $C_G(x) = G$ .

**Example 12.11.**  $G = S_n$ ,  $X = \{1, 2, \dots, n\}$ . The action of  $S_n$  on  $X$  is *transitive* which means there is only one orbit:  $O(n) = X$ . The stabilizer of  $n$  is  $S_{n-1}$  which has  $(n-1)!$  elements and

$$|G_n| = |S_{n-1}| = (n-1)! = \frac{|S_n|}{|X|} = \frac{n!}{n}$$

*Proof of orbit size formula.* By definition

$$|G : G_x| = |G/G_x|$$

To show that this number is the same as  $|O(x)|$  it suffices to construct a bijection

$$\phi : O(x) \rightarrow G/G_x.$$

Define the mapping  $\phi$  by

$$\phi(y) = \{g \in G \mid y = gx\}$$

If  $y \in O(x)$  then there is at least one element  $g \in G$  so that  $y = gx$ . So  $\phi(y)$  is not the empty set. Choose one of these elements, say  $g_0$ .

$$y = g_0x.$$

Claim:  $\phi(y) = g_0G_x$ .

Pf: ( $\supseteq$ ) Take any element  $g_0h \in g_0G_x$ . Then  $h \in G_x$  means that  $hx = x$  so

$$g_0hx = g_0x = y \quad \Rightarrow \quad g_0h \in \phi(y)$$

( $\subseteq$ ) Suppose that  $g \in \phi(y)$ . Then  $y = gx = g_0x$  so

$$g_0^{-1}gx = x.$$

In other words,  $g_0^{-1}g \in G_x$  or  $g \in g_0G_x$ .

This shows that  $\phi(y)$  is a well-defined element of  $G/G_x$ . Now we have to show it is 1-1 and onto.

$\phi$  is 1-1 If  $y_1 \neq y_2$  then obviously,

$$\phi(y_1) = \{g \in G \mid gx = y_1\}$$

$$\phi(y_2) = \{g \in G \mid gx = y_2\}$$

are disjoint sets so they are not equal.

$\phi$  is onto Take any coset  $gG_x \in G/G_x$ . Then  $gG_x = \phi(gx)$ . □

## 12.2 Class formula

List the orbits of  $X$  without repetition:  $X = \coprod O(x_i)$ . Then

$$|X| = \sum |O(x_i)| = \sum |G : G_{x_i}|.$$

When we take this formula for the conjugation action of  $G$  on  $G$  we get the class formula. The first form of the formula:

$$|G| = \sum |G : C_G(x_i)|$$

But some of the terms are equal to 1. This happens when  $C_G(x_i) = G$ , i.e., when  $x_i$  is central. Each central element of  $G$  is in its own conjugacy class and contributes 1 to the above sum so we get the following.

**Theorem 12.12 (Class formula).** *If  $G$  is a finite group then*

$$|G| = |Z(G)| + \sum_{x_i \notin Z(G)} |G : C_G(x_i)|.$$

The important point is that each of the summands  $|G : C_G(x_i)|$  are now greater than 1.

**Definition 12.13.** A  $p$ -group is a finite group  $P$  of order  $p^k$  where  $p$  is prime and  $k \geq 0$ . (The trivial group is a  $p$ -group for every prime  $p$ .)

**Corollary 12.14.** *Every nontrivial  $p$ -group  $P$  has a nontrivial center  $Z(P)$ .*

*Proof.* Each summand in the class formula

$$|P : C_P(x_i)| = \frac{|P|}{|C_P(x_i)|}$$

is a number  $> 1$  that divides  $|P| = p^k$ . Thus it is a nontrivial power of  $p$ . This means that all the terms in the class formula are divisible by  $p$  except possibly  $|Z(P)|$ . This final number must also be divisible by  $p$ .  $\square$

## 12.3 Cauchy's Theorem

One of the applications of the class formula is the proof of Cauchy's Theorem.

**Theorem 12.15 (Cauchy's Theorem).** *If a prime  $p$  divides the order of a group  $G$  then  $G$  contains an element of order  $p$ .*

*Proof.* By induction on  $|G|/p$ .

If  $|G|/p = 1$  then  $G$  is cyclic of order  $p$  and every nontrivial element of  $G$  has order  $p$ .

Suppose that  $|G|/p > 1$  and the theorem holds for all groups of order less than that of  $G$ . There are two cases. Either  $G$  is abelian or it is nonabelian.

Case 1  $G$  is abelian.

Choose  $x \neq e$  in  $G$ . Then  $\langle x \rangle \trianglelefteq G$  and

$$|G| = |\langle x \rangle| \cdot |G/\langle x \rangle|$$

Therefore, either  $p$  divides  $|\langle x \rangle| = o(x)$  or  $p$  divides  $|G/\langle x \rangle|$ .

- (a) If  $p$  divides  $o(x)$  then  $o(x) = pn$  which implies that  $x^n$  has order  $p$ . So  $g = x^n$  is the element we are looking for.
- (b) If  $p$  divides  $|G/\langle x \rangle|$  then the quotient group  $G/\langle x \rangle$  has an element of order  $p$  by induction (since it is smaller than  $G$ ). Suppose that this element is  $g\langle x \rangle$ . Then

$$(g\langle x \rangle)^n = \langle x \rangle \text{ iff } p|n$$

If we let  $n = o(g)$  then  $(g\langle x \rangle)^n = g^n\langle x \rangle = e\langle x \rangle = \langle x \rangle$  so  $p|n$  and  $n = pk$ . This implies that  $g^k$  has order  $p$ .

Case 2  $G$  is nonabelian.

In this case we use the class formula:

$$|G| = |Z(G)| + \sum_{x_i \notin Z(G)} |G : C_G(x_i)|.$$

There are two cases. Either  $|Z(G)|$  is divisible by  $p$  or it isn't.

- (a) If  $p$  divides  $|Z(G)|$  then  $Z(G)$  contains an element of order  $p$  by induction. ( $Z(G) < G$  since  $G$  is nonabelian.)
- (b) If  $p$  does not divide  $|Z(G)|$  then, by the class formula, there must be some  $x_i$  so that  $p$  does not divide the index  $|G : C_G(x_i)|$ . But then  $p$  has to divide the order of the centralizer since

$$|G| = |C_G(x_i)| \cdot |G : C_G(x_i)|$$

By induction,  $C_G(x_i)$  contains an element of order  $p$ .

□

## 12.4 Groups of small order

This is where we classify groups of order  $\leq 7$  up to isomorphism.

**Lemma 12.16.** *The index of the center of  $G$  cannot be a prime number.*

*Proof.* By contradiction. Suppose that  $|G : Z(G)| = p$ . Then the quotient group  $G/Z(G)$  is a cyclic group generated by one element, say  $gZ(G)$ . This means that

$$G = \coprod g^i Z(G)$$

Take any two elements of  $G$ . They must be  $g^i x, g^j y$  where  $x, y \in Z(G)$ . But then:

$$g^i x g^j y = g^i g^j x y = g^j y g^i x$$

since  $x, y$  are central. In other words, any two elements of  $G$  commute. So  $G$  is abelian and  $Z(G) = G$  has index 1. The index could not have been prime.  $\square$

**Theorem 12.17.** *Every group of order  $p^2$  is abelian.*

*Proof.* Suppose that  $P$  has  $p^2$  elements. Then how many elements does  $Z(P)$  have?

By Lagrange,  $|Z(P)|$  divides  $p^2$  so it is either 1,  $p$  or  $p^2$ . By Corollary 12.14,  $|Z(P)| \neq 1$ . By the lemma  $|Z(P)| \neq p$ . So  $|Z(P)| = p^2$  and  $P = Z(P)$  which means that  $P$  is abelian.  $\square$

**Theorem 12.18.** *Every group of order 4 is either cyclic or isomorphic to  $\mathbb{Z}_2 \times \mathbb{Z}_2$ .*

*Proof.* Suppose that  $G$  has order 4. Then either  $G$  has an element of order 4 or it doesn't.

1. If  $G$  has an element of order 4 then it is cyclic. ( $G \cong \mathbb{Z}_4$ ).
2. If  $G$  has no element of order 4 then its three nontrivial elements must all have order 2. Say

$$G = \{e, a, b, c\}$$

Then  $ab = c$ . Why? Because it can't be anything else.

- (a)  $ab = a$  implies  $b = e$  by cancellation.
- (b)  $ab = b$  implies  $a = e$  by cancellation.
- (c)  $ab = e$  implies  $a = b^{-1} = b$  since  $b^2 = e$ .

Therefore, the entire multiplication table is determined. (The product of any two nontrivial elements is the third except that  $x^2 = e$  for all  $x$ .) The conclusion is that there is only one group of this kind. It must be  $\mathbb{Z}_2 \times \mathbb{Z}_2$ .  $\square$

**Theorem 12.19.** *Every group of order 6 is either cyclic or isomorphic to  $S_3$ .*

*Proof.* Suppose that  $G$  has order 6. By Cauchy,  $G$  contains elements  $a, b \in G$  of order  $o(a) = 2$ ,  $o(b) = 3$ . The subgroup  $H = \langle b \rangle$  is a normal subgroup of  $G$  since it has index 2. Consequently,

$$aHa^{-1} = H$$

This means that  $aba^{-1}$  is one of the two nontrivial elements of  $H = \{e, b, b^2\}$ . In either case a complete list of all of the elements of  $G$  is given by:

$$G = \{e, b, b^2, a, ab, ab^2\}$$

1. If  $aba^{-1} = b$  then  $G$  is abelian since any two elements commute. The multiplication table is given by

$$\begin{array}{ccc} \cdot & b^j & ab^j \\ b^i & b^{i+j} & ab^{i+j} \\ ab^i & ab^{i+j} & b^{i+j} \end{array}$$

2. If  $aba^{-1} = b^2$  then  $G$  is nonabelian and the multiplication table is given by

$$\begin{array}{ccc} \cdot & b^j & ab^j \\ b^i & b^{i+j} & ab^{j-i} \\ ab^i & ab^{i+j} & b^{j-i} \end{array}$$

This proves that there is only one commutative group of order 6 (up to isomorphism). Thus it must be  $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$ . This also shows that there is only one nonabelian group of order 6 (up to isomorphism). It must be  $S_3 \cong D_6$ .  $\square$

**Definition 12.20.** The *dihedral group*  $D_{2n}$  is the group having  $2n$  elements:

$$D_{2n} = \{e, b, b^2, \dots, b^{n-1}, a, ab, ab^2, \dots, ab^{n-1}\}$$

where  $a^2 = e = b^n$  and  $aba^{-1} = b^{-1}$ . These rules determine the complete multiplication table of  $D_{2n}$ :

$$\begin{array}{ccc} \cdot & b^j & ab^j \\ b^i & b^{i+j} & ab^{j-i} \\ ab^i & ab^{i+j} & b^{j-i} \end{array}$$