

# Contents

<b>1</b>	<b>Groups</b>	<b>1</b>
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, for any  $x \in X$ , following common terminology, we define:

- i. The  $G$ -orbit of  $x$  in  $X$  to be the set:

$$\text{orb}(x, G) = \{y \in X : y = gx \text{ for some } g \in G\};$$

- ii. The  $G$ -stabilizer of  $x$  in  $G$  to be the set

$$\text{stab}(x, G) = \{g \in G : xg = x\}.$$

**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, the center of  $G$  is not trivial.*

*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  $x \in G$ . By Lagrange's Theorem, the number

$$(G : \text{stab}(x, G)) = |\text{orb}(x, G)|,$$

is a divisor of  $|G|$  that is greater than 1 for every  $x \in G \setminus Z(G)$  (thus, divisible by  $p$ ). Since

$$\begin{aligned} |G| &= \sum_{x \in T} |\text{orb}(x, G)| \\ &= \sum_{x \in T \cap Z(G)} |\text{orb}(x, G)| + \sum_{x \in T \setminus Z(G)} |\text{orb}(x, G)| \\ &= |Z(G)| + \sum_{x \in T \setminus Z(G)} (G : \text{stab}(x, G)) \end{aligned}$$

we get that  $|Z(G)|$  is also divisible by  $p$ .  $\square$

**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  $\Omega$  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  $\Omega$ , 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  $\Omega$ , 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.  $\square$

**Proposition 4.** *Let  $G$  be a finite group and  $p$  a prime divisor of  $|G|$ , say  $|G| = p^\alpha m$  with  $\alpha > 0$  and  $(p, m) = 1$ . Then, there exists  $H \leq G$  such that  $|H| = p^\alpha$ .*

*Proof.* Let

$$\Omega(p, G) = \{X \subset G : |X| = p^\alpha\},$$

be the set of all the sets of order  $p^\alpha$  in  $G$ . Our objective is to show that there is a subgroup of  $G$  among the elements of  $\Omega(p, G)$ . First, notice that  $p$  does not divide

$$|\Omega(p, G)| = \binom{|G|}{p^\alpha} = \frac{|G| \cdots (|G| - i) \cdots (|G| - p^\alpha + 1)}{p^\alpha \cdots (p^\alpha - i) \cdots 1}.$$

In fact, for any  $i \in \{1, \dots, p^\alpha - 1\}$ , we get that:

- i. If  $p^\beta$  divides  $|G| - i = p^\alpha m - i$ , then  $p^\beta$  also divides  $p^\alpha - i$  since, if there is a  $q \in \mathbb{Z}$  such that  $p^\alpha m - i = qp^\beta$ , then  $i = (p^{\alpha-\beta}m - q)p^\beta$  with  $p^{\alpha-\beta}m - q \in \mathbb{Z}$ , so  $p^\beta$  divides both  $p^\alpha$  and  $i$ . Thus,  $p^\beta$  divides the difference  $p^\alpha - i$ ;
- ii. If  $p^\beta$  divides  $p^\alpha - i$ , then  $p^\alpha - i = qp^\beta$  for some  $q \in \mathbb{Z}$ . So, we get that  $i = (p^{\alpha-\beta} - q)p^\beta$  and, because  $p^{\alpha-\beta} - q$  belongs to  $\mathbb{Z}$ ,  $p^\beta$  divides  $i$ . Thus,  $p^\beta$  divides the difference  $p^\alpha m - i$ .

Now, let  $G$  act on  $\Omega(p, G)$  from the right by translations:

$$\Omega(p, G) \times G \rightarrow \Omega(p, G), \quad (X, g) \mapsto Xg,$$

where  $Xg = \{xg : x \in X\}$ . Now, because we have that

$$|\Omega(p, G)| = \sum_{X \in T} |\text{orb}(X, G)|,$$

and  $p$  does not divide  $|\Omega(p, G)|$ , we know that  $p$  does not divide  $|\text{orb}(X_0, G)|$  for some  $X_0 \in \Omega(p, G)$ . Take  $H = \text{stab}(X_0, G)$ . It follows that  $p^\alpha$  divides  $|H|$  since, by Lagrange's Theorem, it divides

$$|G| = (G : \text{stab}(X_0, G)) |\text{stab}(X_0, G)| = |\text{orb}(X_0, G)| |H|,$$

and  $p$  does not divide  $|\text{orb}(X_0, G)|$ . Thus,  $p^\alpha \leq |H|$ . Now, take any  $a \in X_0$  and define

$$H \rightarrow X_0, \quad g \mapsto ag.$$

Notice that  $ag$  belongs to  $X_0$  for every  $g \in H = \text{stab}(X_0, G)$ , so the function above is well defined. It's clearly injective, so  $|H| \leq |X_0| = p^\alpha$ . Therefore,  $|H| = p^\alpha$ . This completes the proof.  $\square$

**Definition 3.** Let  $G$  be a finite group and  $p$  a prime divisor of  $|G|$ , say  $|G| = p^\alpha m$  with  $\alpha > 0$  and  $(p, m) = 1$ . Then, a subgroup  $H \leq G$  of order  $|H| = p^\alpha$  is called a  $p$ -Sylow subgroup of  $G$ . Let

$$\text{Syl}(p, G) = \{H \leq G : |H| = p^\alpha\},$$

be the set of all  $p$ -Sylow subgroups of  $G$  and  $n_p = |\text{Syl}(p, G)|$  be the number of  $p$ -Sylow subgroups of  $G$ .

**Lemma 1.** Let  $G$  be a finite group and  $p$  a prime divisor of  $|G|$ . Then, for any  $H \in \text{Syl}(p, G)$  and any  $p$ -subgroup  $P$  of  $G$ , we have  $P \cap N_G(H) = P \cap H$ .

*Proof.* We argue by contradiction. Suppose that  $P \cap H < P \cap N_G(H)$  and then take any  $x \in P \cap (N_G(H) \setminus H)$ . Now,  $H\langle x \rangle \leq G$  because  $H\langle x \rangle = \langle x \rangle H$  since  $x \in N_G(H)$ . Also,  $|x|$  is a power of  $p$  because  $p \in P$  and, finally,  $p \notin H$  implies that  $(\langle x \rangle : H \cap \langle x \rangle) > 1$ . Thus, we conclude that

$$|H\langle x \rangle| = \frac{|H||x|}{|H \cap \langle x \rangle|} > |H|,$$

which is a contradiction since no  $p$ -subgroup of  $G$  has order greater than that of a  $p$ -Sylow subgroup of  $G$ . Therefore, we must have  $P \cap N_G(H) = P \cap H$ .  $\square$

**Theorem 2.** Let  $G$  be a finite group and  $p$  a prime divisor of  $|G|$ , say  $|G| = p^\alpha m$  with  $\alpha > 0$  and  $(p, m) = 1$ . Then, we have that:

- i.  $n_p \equiv 1 \pmod{p}$ ;
- ii. for any given  $H \in \text{Syl}(p, G)$ , we have that

$$\text{Syl}(p, G) = \{H^g : g \in G\},$$

that is, any two  $p$ -Sylow subgroups of  $G$  are conjugate to one another;

- iii.  $n_p$  divides  $m$ .

*Proof.* Let  $H \in \text{Syl}(p, G)$  be any  $p$ -Sylow subgroup of  $G$ . Let  $H$  act on  $\text{Syl}(p, G)$  from the right by conjugation:

$$\text{Syl}(p, G) \times H \rightarrow \text{Syl}(p, G), \quad (K, g) \mapsto K^g = g^{-1}Kg.$$

Notice that, for any  $K \in \text{Syl}(p, G)$ , it's true that

$$\text{stab}(K, H) = \{x \in H : K^x = K\} = N_G(K) \cap H = K \cap H.$$



Then, we get that

$$\begin{aligned} n_p &= \sum_{K \in T} |\text{orb}(K, H)| = \sum_{K \in T} (H : \text{stab}(K, H)) \\ &= \sum_{K \in T} (H : H \cap N_G(K)) = \sum_{K \in T} (H : K \cap H), \end{aligned}$$

and because  $(H : K \cap H)$  is a power of  $p$  that is equal to 1 exactly once, namely, for  $K = H$ , we conclude that  $n_p \equiv 1 \pmod{p}$ .

Now we would like to show that any  $p$ -subgroup of  $G$  lies in some  $p$ -Sylow subgroup of  $G$ . Let  $P$  be any  $p$ -subgroup of  $G$  and let it act on  $\text{Syl}(p, G)$  from the right by conjugation

$$\text{Syl}(p, G) \times P \rightarrow \text{Syl}(p, G), \quad (K, x) \mapsto K^x.$$

Since  $p$  does not divide

$$n_p = \sum_{K \in T} |\text{orb}(K, P)| = \sum_{K \in T} (P : \text{stab}(K, P)) = \sum_{K \in T} (P : K \cap P),$$

there must exist some  $K \in \text{Syl}(p, G)$  such that  $(P : K \cap P) = 1$  but, then  $P = K \cap P$  and so  $P \subset K$ . In particular, if  $H, K$  are any  $p$ -Sylow subgroups of  $G$ , then there exists  $x \in G$  such that  $H^x = K$ .

Finally, because we now know that

$$\text{Syl}(p, G) = \{H^x : x \in G\},$$

we get that

$$n_p = |\text{orb}(H, G)| = (G : N_G(H)) = \frac{(G : H)}{(N_G(H) : H)} = \frac{m}{(N_G(H) : H)},$$

□

