Contents

Chapter 1

Groups

1.1 Group Actions

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

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

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 the set $\{1, \ldots, n\}$ from the right in a rather natural way:*

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

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

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

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:

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

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

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

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

$$\forall x, y \in X: \quad x \equiv y \mod G \iff \exists g \in G: \; xg = y, \tag{1.1}$$

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

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

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

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

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

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

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

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

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

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

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

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

it's true that

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

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

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

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

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

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

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

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

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

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

we get that $|Z(G)|$ is also divisble by p. □

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

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

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, $x_1 = x_2 = \cdots = x_{p-1} = x_p$. 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 transveral for the action of $\mathbb{Z}_p$ on Ω, meaning that:

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

Then, we have that

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

Since

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

are both divisible by p, so is

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

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

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

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

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 $H \leqslant G$ 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^α 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^β divides $|G| - i = p^\alpha m - i$, then p^β also divides $p^\alpha - i$ since, if there is a $q \in \mathbb{Z}$ such that $p^\alpha m - i = qp^\beta$, then $i = \left(p^{\alpha-\beta} m - q\right) p^\beta$ with $p^{\alpha-\beta} m - q \in \mathbb{Z}$, so p^β divides both p^α and i. Thus, p^β divides the difference $p^\alpha - i$;

ii. If p^β divides $p^\alpha - i$, then $p^\alpha - i = qp^\beta$ for some $q \in \mathbb{Z}$. So, we get that $i = \left(p^{\alpha-\beta} - q\right) p^\beta$ and, because $p^{\alpha-\beta} - q$ belongs to $\mathbb{Z}$, p^β divides i. Thus, p^β divides the difference $p^\alpha m - i$.

Now, let G act on $\Omega(p, G)$ from the right by translations:
$$\Omega(p, G) \times G \to \Omega(p, G), \quad (X, g) \mapsto Xg,$$
where $Xg = \{xg : x \in X\}$. Now, because we have that
$$|\Omega(p, G)| = \sum_{X \in T} |\mathrm{orb}(X, G)|,$$
and p does not divide $|\Omega(p, G)|$, we know that p does not divide $|\mathrm{orb}(X_0, G)|$ for some $X_0 \in \Omega(p, G)$. Take $H = \mathrm{stab}(X_0, G)$. It follows that p^α divides $|H|$ since, by Lagranges's Theorem, it divides
$$|G| = (G : \mathrm{stab}(X_0, G))\, |\mathrm{stab}(X_0, G)| = |\mathrm{orb}(X_0, G)||H|,$$
and p does not divide $|\mathrm{orb}(X_0, G)|$. Thus, $p^\alpha \leqslant |H|$. Now, take any $a \in X_0$ and define
$$H \to X_0, \quad g \mapsto ag.$$
Notice that ag belongs to X_0 for every $g \in H = \mathrm{stab}(X_0, G)$, so the function above is well defined. It's clearly injective, so $|H| \leqslant |X_0| = p^\alpha$. Therefore, $|H| = p^\alpha$. This completes the proof. □

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 $H \leqslant G$ of order $|H| = p^\alpha$ is called a p-Sylow subgroup of G. Let*

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

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

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, for any given $H \in \mathit{Syl}(p,G)$, we have that*

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

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

Proof. Consider the action of G on $\mathrm{Syl}(p,G)$ from the right by conjugation,

$$\mathrm{Syl}(p,G) \times G \to \mathrm{Syl}(p,G) \quad (H,g) \mapsto H^g = g^{-1}Hg.$$

□

Theorem 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, $n_p \,|\, m$ and $n_p \equiv 1 \pmod{p}$.*