Chapter 5

Groups II

1 Group actions

Definition 5.1. Let G be a group and X a set. A left **action** of of G on X is a function $G \times X \to X$ (with the image of (g, x) being denoted $g \cdot x$) satisfying

1) $\forall x \in X, \quad e_G \cdot x = x$
2) $\forall x \in X \; \forall g, h \in G, \quad (gh) \cdot x = g \cdot (h \cdot x)$

We also say that G acts on X and denote this by $G \curvearrowright X$.

Example 5.2. 1. $S_n \curvearrowright \{1, 2, \ldots, n\}$, for example $(132) \cdot 3 = 2$

2. D_n acts on the vertices of a regular n-gon
3. $GL(n, K)$ acts on K^n (having fixed a basis for K^n)
4. $GL(n, K)$ acts on $\{W \mid W \leqslant K^n\}$ (having fixed a basis for K^n)
5. $\mathbb{Z}/2\mathbb{Z} \curvearrowright \mathbb{C}$, $[0] \cdot z = z$, $[1] \cdot z = \overline{z}$

Example 5.3. Here are two important examples in which a group acts on itself.

1. $G \curvearrowright G$ by left multiplication: $g \cdot x = gx$
2. $G \curvearrowright G$ by conjugation: $g \cdot x = gxg^{-1}$

Remark. Let S_X denote the group of all bijections from X to X (with operation given by function composition). An action $G \curvearrowright X$ corresponds to a homomorphism $G \to S_X$ in the following sense.

Exercise 144. (a) Suppose that a group G acts on a set X.

   (i) Let $g \in G$. Show that the map $\varphi_g : X \to X$, $\varphi_g(x) = g \cdot x$ is a bijection.
   (ii) Show that the map $\Phi : G \to S_X$ given by $\Phi(g) = \varphi_g$ is a homomorphism.

(b) Suppose that G is a group, X a set and that $\Psi : G \to S_X$ is a homomorphism. Show that there is an action of G on X defined by $g \cdot x = \Psi(g)(x)$.

Definition 5.4. Suppose that $G \curvearrowright X$ and let $x \in X$.

1) The **orbit** of x is the set $O(x) = \{g \cdot x \mid g \in G\} \subseteq X$ (sometimes denoted $G \cdot x$)
2) The **stabiliser** of x is $\mathrm{Stab}(x) = \{g \in G \mid g \cdot x = x\}$
3) $x \in X$ is a **fixed point** if $\mathrm{Stab}(x) = G$
4) The action is **transitive** if $\forall x, y \in X \; \exists g \in G, \; g \cdot x = y$
   (i.e., there is only one orbit)

Exercise 145. Show that $\mathrm{Stab}(x)$ is a subgroup of G.

Example 5.5.

1. $S_3 \curvearrowright \{1,2,3\}$, $\mathrm{Stab}(2) = \{e,(13)\}$, $O(2) = \{1,2,3\}$, the action is transitive
2. $G = \langle(123)\rangle \leqslant S_5$, $X = \{1,2,3,4,5\}$, $\mathrm{Stab}(2) = \{e\}$, $O(2) = \{1,2,3\}$, $\mathrm{Stab}(5) = G$, $O(5) = \{5\}$
3. $X = \{1,2,3,4\}$ (identified with the vertices of a square), $G = D_4$, $\mathrm{Stab}(1) = \{e, rs\}$, $O(1) = \{1,2,3,4\}$ (using our standing notational conventions for the dihedral groups as in section 3.6.)
4. $G \curvearrowright G$ by left multiplication, $\mathrm{Stab}(g) = \{e\}$, $O(g) = G$
5. $G \curvearrowright G$ by conjugation, $\mathrm{Stab}(g)$ is called the **centraliser** of g

$$C_G(g) = \{h \in G \mid hg = gh\}$$

$O(g) = \{hgh^{-1} \mid h \in G\}$ is called the **conjugacy class** of g.

Lemma 5.6

Let G be a group acting on a set X. The orbits partition X.

Proof. We need to show that every element of X is contained in exactly one orbit. Clearly $x = e \cdot x \in O(x)$. We need to show that if $O(x) \cap O(y) \neq \emptyset$, then $O(x) = O(y)$. Let $z \in O(x) \cap O(y)$. Then there are $g, h \in G$ such that $z = g \cdot x$ and $z = h \cdot y$. Then $x = g^{-1} \cdot z$, $y = h^{-1} \cdot z$, and

$$\begin{aligned} w \in O(x) &\implies w = k \cdot x \quad \text{for some } k \in G \\ &\implies w = k \cdot (g^{-1} \cdot z) = (kg^{-1}) \cdot z = (kg^{-1}) \cdot (h \cdot y) = (kg^{-1}h) \cdot y \\ &\implies w \in O(y) \end{aligned}$$

So $O(x) \subseteq O(y)$. Similarly $O(y) \subseteq O(x)$. $\square$

Exercise 146. Any subgroup G of S_4 acts on the set $\{1,2,3,4\}$ in a natural way. For each choice of G given below, describe the orbits of the action and the stabilizer of each point.

(a) $G = \langle(123)\rangle$

(b) $G = \langle(1234)\rangle$

(c) $G = \langle(12),(34)\rangle$

(d) $G = S_4$

(e) $G = \langle(1234),(14)\rangle$ (which is isomorphic to D_4)

Exercise 147. Let $X = \mathbb{R}^3$ and let $v \neq 0$ be a fixed element of X. Show that

$$\alpha \cdot x = x + \alpha v \quad (x \in X, \alpha \in \mathbb{R})$$

defines an action of the additive group of the real numbers on X. Give a geometrical description of the orbits.

Exercise 148. Find the conjugacy classes in the quaternion group described in Exercise 111.

Exercise 149. Find the conjugates of the follwing:

(a) (123) in S_3

(b) (123) in S_4

(c) (1234) in S_4

(d) (1234) in S_n where $n \geqslant 4$

(e) $(12\ldots m)$ in S_n where $n \geqslant m$

Exercise 150. Let $\tau \in S_n$. Suppose that $\sigma = (12\ldots k)$. Show that $\tau\sigma\tau^{-1} = (\tau(1)\tau(2)\ldots\tau(k))$. What is the result if σ is replaced by a general element of S_n? Use this to describe the conjugacy classes of S_n.

Exercise 151. Suppose that g and h are conjugate elements of a group G. Show that $C_G(g)$ and $C_G(h)$ are conjugate subgroups of G.

Exercise 152. Determine the centralizer in $GL(3,\mathbb{R})$ of the following matrices:

(a) $\begin{bmatrix}1&0&0\\0&2&0\\0&0&3\end{bmatrix}$ (b) $\begin{bmatrix}1&0&0\\0&1&0\\0&0&2\end{bmatrix}$ (c) $\begin{bmatrix}1&1&0\\0&1&0\\0&0&2\end{bmatrix}$ (d) $\begin{bmatrix}1&1&0\\0&1&0\\0&0&1\end{bmatrix}$ (e) $\begin{bmatrix}1&1&0\\0&1&1\\0&0&1\end{bmatrix}$

2 The orbit-stabiliser relation and applications

Theorem 5.7: The orbit-stabiliser relation

Let G be a group and $G \curvearrowright X$ an action on a set X. Denote by $G/\operatorname{Stab}(x)$ the set of left cosets of $\operatorname{Stab}(x)$. Then, for all $x \in X$ the map $G/\operatorname{Stab}(x) \to O(x)$ given by $g\operatorname{Stab}(x) \mapsto g \cdot x$ is a bijection. If G is finite, then

$$|G| = |O(x)|\,|\operatorname{Stab}(x)|$$

Proof. Denote the map by Φ. We first show that the map is well-defined.

$$g\operatorname{Stab}(x) = h\operatorname{Stab}(x) \implies g^{-1}h \in \operatorname{Stab}(x) \implies (g^{-1}h)\cdot x = x \implies h \cdot x = g \cdot x$$

Now that the map is injective.

$$\begin{aligned}\Phi(g\operatorname{Stab}(x)) = \Phi(h\operatorname{Stab}(x)) &\implies g\cdot x = h \cdot x \implies g^{-1}\cdot(g\cdot x) = g^{-1}\cdot(h\cdot x) \implies (g^{-1}g)\cdot x = (g^{-1}h)\cdot x\\ &\implies x = (g^{-1}h)\cdot x \implies g^{-1}h \in \operatorname{Stab}(x)\\ &\implies g\operatorname{Stab}(x) = h\operatorname{Stab}(x)\end{aligned}$$

And surjective:

$$y \in O(x) \implies y = g\cdot x \quad \text{(for some } g \in G) \implies y = \Phi(g\operatorname{Stab}(x))$$

If G is finite, then we have:

$$\begin{aligned}|G| &= [G : \operatorname{Stab}(x)]\,|\operatorname{Stab}(x)| && \text{(by Lagrange's theorem)}\\ &= |O(x)|\,|\operatorname{Stab}(x)| && \text{(since } \Phi \text{ is a bijection)}\end{aligned}$$

□

We'll now look at some consequences of the orbit-stabiliser relation. The first are contained in the following exercises.

Exercise 153. Let G be the subgroup of S_{15} given by

$$G = \langle (1,12)(3,10)(5,13)(11,15), (2,7)(4,14)(6,10)(9,13), (4,8)(6,10)(7,12)(9,11)\rangle$$

Find the orbits in $X = \{1,\dots,15\}$ under the action of G. Deduce that the order of G is a multiple of 60.

Exercise 154. If a group G of order 5 acts on a set X with 11 elements, must there be an element of the set X which is left fixed by every element of the group G? What if G has order 15 and X has 8 elements?

The next result is a result of applying the orbit-stabiliser relation to the conjugacy action of a group on itself. First a definition.

Definition 5.8. Let G be a group. The **centre** of G, denoted $Z(G)$, is the set of elements that commute with all elements of G. That is, $Z(G) = \{g \in G \mid \forall h \in G,\ gh = hg\}$.

Remark. The centre of G consists of all fixed points of the action of G on itself by conjugation.

Example 5.9. 1. $Z(\mathbb{Z}) = \mathbb{Z}$ 2. $Z(D_4) = \{e, r^2\}$ 3. $Z(S_3) = \{e\}$

Exercise 155. Show that $Z(G)$ is a normal subgroup of G.

Exercise 156. Suppose that G is a group with centre Z and is such that G/Z is a cyclic group. Show that there exists an element $h \in G$ such that every element of G can be written in the form $g = h^i z$ with $i \in \mathbb{Z}$ and $z \in Z$. Deduce that G is commutative.

Theorem 5.10

Let G be a group of size p^n where $p \in \mathbb{N}$ is prime and $n \in \mathbb{N}$. Then $|Z(G)| \geqslant p$.

Proof. Consider G acting on itself by conjugation. The orbits partition G and $Z(G)$ is the union of all orbits having size 1. Therefore, G is a disjoint union

$$G = Z(G) \cup C_1 \cup C_2 \dots C_k \tag{$*$}$$

where the C_i are the orbits having size at least 2. By the orbit-stabiliser relation we have that for all i, $|C_i| \mid |G|$. Therefore $p \mid |C_i|$ for all i, and hence $p \mid |Z(G)|$ by ($*$). □

Theorem 5.11

Let G be a group of size p^n where $p \in \mathbb{N}$ is prime and $n \in \mathbb{N}$. Suppose that G acts on a finite set X. If p does not divide $|X|$, then the action has a fixed point.

Proof. Denote the orbits of the action as O_1, O_2,. . . , O_k. By the orbit-stabiliser relation $|O_i| \mid |G| = p^n$. Therefore $\forall i$, $|O_i| = 1$ or $p \mid |O_i|$. Suppose, for a contradiction, that there are no orbits of size 1. Then we would have $p \mid |X|$ since $|X| = |O_1| + \cdots + |O_k|$. □

Example 5.12. Let $p \in \mathbb{N}$ be a prime. Recall that $\mathbb{F}_p$ denotes the filed with p elements. Let $G \leqslant GL(3, \mathbb{F}_p)$ be given by

$$G = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \mid a, b, c \in \mathbb{F}_p \right\}$$

Note the $|G| = p^3$. Let X be the set of all 1-dimensional subspaces of $\mathbb{F}_p^3$. Then G acts on X (since $GL(3, \mathbb{F}_p)$ does). Explicitly, after fixing a basis $\mathcal{B}$ for $\mathbb{F}_p^3$ we identify $\mathbb{F}_p^3$ with $M_{3\times 1}(\mathbb{F}_p)$ and define $g \cdot \mathrm{span}(u) = \mathrm{span}(gu)$. The number of 1-dimensional subspaces is given by

$$|X| = \frac{p^3 - 1}{p - 1} = p^2 + p + 1$$

Since p does not divide $p^2 + p + 1$ we conclude (from the above theorem) that there is a 1-dimensional subspace that is fixed by G.

Theorem 5.13

Let $p \in \mathbb{N}$ be prime and G a group. If $|G| = p^2$, then either $G \cong \mathbb{Z}/p^2\mathbb{Z}$ or $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Remark. As a consequence, if $|G| = p^2$ then G is abelian.

Proof. Suppose that G is not cyclic. We need to show that $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. By Theorem 5.10, $|Z(G)| > 1$. Let $g \in Z(G) \setminus \{e\}$. Since G is not cyclic and $g \neq e$, we have $|g| = p$. Let $H = \langle g \rangle$. Then $H \lhd G$ since $g \in Z(G)$. By Lagrange's Theorem, $|G/H| = |G|/|H| = p$. Hence G/H is cyclic. Let $x \in G$ be such that xH generates G/H. Then

$$G/H = \{eH, xH, x^2H, \dots, x^{p-1}H\}$$

It follows that $\langle x, g \rangle = G$.

Define a map $\varphi : \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \to G$ by $\varphi([a]_p, [b]_p) = x^a g^b$. Since both x and g have order p, this map is well-defined. It is a homomorphism since

$$\begin{aligned} \varphi(([a_1]_p, [b_1]_p) + ([a_2]_p, [b_2]_p)) &= \varphi(([a_1 + a_2]_p, [b_1 + b_2]_p)) \\ &= x^{a+1+a_2} g^{b_1+b_2} = x^{a_1} x^{a_2} g^{b_1} g^{b_2} \\ &= x^{a_1} g^{b_1} x^{a_2} g^{b_2} && \text{(since } xg = gx\text{)} \\ &= \varphi([a_1]_p, [b_1]_p)\varphi([a_2]_p, [b_2]_p) \end{aligned}$$

Since $x, g \in \mathrm{im}(\varphi)$ and $\langle x, g \rangle = G$, the homomorphism is surjective, It is therefore also injective since $|G| = |\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}| = p^2$. □

Exercise 157. Describe the finite groups having exactly one or exactly two or exactly three conjugacy classes.

3 Cauchy's Theorem

We know from Lagrange's theorem that if $g \in G$, then $|g|$ divides $|G|$. The converse is in general false, that is, $m \mid |G|$ does not imply that there exists an element in G of order m. But it does hold for prime divisors.

Theorem 5.14: Cauchy's theorem

Let G be a finite group and $p \in \mathbb{N}$ a prime. If p divides |G| , then there exists $g \in G$ with $|g| = p$.

Proof. Let $X = \{(x_1, \dots, x_p) \in G^p \mid x_1x_2 \dots x_p = e\}$. Note that $|X| = |G|^{p-1}$ and therefore $p \mid |G|$. The group $\mathbb{Z}/p\mathbb{Z}$ acts on X by cyclic permutation, that is:

$$[1]_p \cdot (x_1, \dots, x_p) = (x_p, x_1, \dots, x_{p-1}) \qquad [2]_p \cdot (x_1, \dots, x_p) = (x_{p-1}, x_p, x_1, \dots, x_{p-2}) \quad \text{etc}$$

Note that a fixed point of this action is of the form $(x, x, \dots, x)$ with $x^p = 1$. One such fixed point is $(e, \dots, e)$. Our goal is to show that there exists at least one other orbit of size 1. By the orbit stabiliser relation, all orbits have size that divides $|\mathbb{Z}/p\mathbb{Z}| = p$. If there were only one orbit of size 1, we would have $|X| = 1 + kp$ for some $k \in \mathbb{N}$ which contradicts the fact that $p \mid |X|$. $\square$

Exercise 158. Show that if p is a prime number, then any group of order $2p$ must have a subgroup of order p and that this subgroup must be normal.

Exercise 159. Let $p \in \mathbb{N}$ be prime. Show that, up to isomorphism, there are exactly two groups of order $2p$.

4 Burnside orbit counting lemma

Definition 5.15. Given an action $G \curvearrowright X$ and an element $g \in G$, the **fixed point set** of g is

$$X^g = \{x \in X \mid g \cdot x = x\}$$

Lemma 5.16: Burnside counting lemma

Let G be a finite group acting on a finite set X. Let N be the number of orbits of the action. Then

$$N = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

Proof. Consider the set $S = \{(g, x) \in G \times X \mid g \cdot x = x\}$. We will count the elements on S in two ways. Firstly,

$$|S| = \sum_{g \in G} |\{x \in X \mid g \cdot x = x\}| = \sum_{g \in G} |X^g| \tag{1}$$

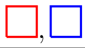
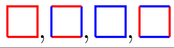
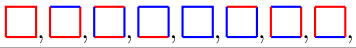
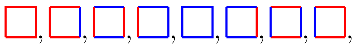
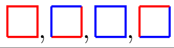
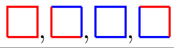
For the second count denote the orbits of the action by $O_1, \dots, O_N$. We have

$$\begin{aligned}
|S| &= \sum_{x \in X} |\{g \in G \mid g \cdot x = x\}| = \sum_{x \in X} |\operatorname{Stab}(x)| \\
&= \sum_{i=1}^{N} \sum_{x \in O_i} |\operatorname{Stab}(x)| && \text{(since the orbits partition } X\text{)} \\
&= \sum_{i=1}^{N} \sum_{x \in O_i} \frac{|G|}{|O_i|} && \text{(by the orbit-stabiliser relation)} \\
&= |G| \sum_{i=1}^{N} \sum_{x \in O_i} \frac{1}{|O_i|} = |G| \sum_{i=1}^{N} 1 = N|G| && (2)
\end{aligned}$$

Equating (1) and (2) gives the desired result. $\square$

Example 5.17. How many ways are there to colour the sides of a square using two colours? There are a total of 2^4 different colourings, but some are equivalent in the sense that one can be obtained from the other by applying a reflection or a rotation.

More precisely, if we let X denote the set of all colourings, then $|X| = 16$ and D_4 acts on X. The number of "different" (i.e., non-equivalent) colourings is given by the number of orbits. To find the number of orbits, we can apply the Burnside Lemma. For that we need to consider the set X^g.

$g \in D_4$	X^g	$\lvert X^g \rvert$
e	all colourings	16
r, r^3		2
r^2		4
s		8
$r^2 s$		8
rs		4
$r^3 s$		4

The number of colourings (up to symmetry) is given by the number of orbits, which by Burnside's lemma is:

$$\frac{1}{|D_4|}\sum_{g\in D_4}|X^g| = \frac{1}{8}(16+2+2+4+8+8+4+4)$$
$$= \frac{48}{8} = 6$$

Up to symmetry, there are six different colourings of the square.

Exercise 160. There are 70 (which is $\binom{8}{4}$) ways to colour the edges of an octagon so that four edges are green and four edges are red. Let X be the set of such coloured octagons (so $|X| = 70$). The group D_8 acts on X and two colourings are considered to be equivalent if they are in the same orbit. Use Burnside's orbit counting lemma to find the number of equivalence classes (i.e., orbits).

5 Sylow Theorems

The Sylow theorems are an important tool for understanding finite groups. We know from Cauchy's theorem that if the order of a group G is divisible by a prime p, then G contains a subgroup of order p. The first Sylow theorem generalises this to subgroups of size that is a power of p.

Theorem 5.18: First Sylow theorem

Let G be a finite group, $p \in \mathbb{N}$ a prime and $s \in \mathbb{N}$. If p^s divides $|G|$, then G has a subgroup of size p^s.

Proof. We proceed by induction on $|G|$. If $|G| < p$, then there is nothing to prove, so we assume that $|G| > p$. The inductive hypothesis is that for all groups H with $|H| < |G|$ we have that if $p^t \mid |H|$ (for some $t \in \mathbb{N}$), then there exists a subgroup of H having size p^t. We split into two cases.

Case 1: Suppose first that G contains a proper subgroup $H \subsetneqq G$ such that $p \nmid [G : H]$. Since $p^s \mid |G| = [G : H]|H|$ it follows that $p^s \mid |H|$. By the induction hypothesis H (hence G) contains a subgroup $K \leqslant H$ with $|K| = p^s$.

Case 2: Suppose that every proper subgroup of G has index divisible by p. We first show that $|Z(G)|$ is divisible by p. Considering the action of G on itself by conjugation we have

$$|G| = |Z(G)| + |C_1| + |C_2| + \cdots + |C_k| \qquad (*)$$

where the C_i are the conjugacy classes of size at least 2. For each i, fix some $g_i \in C_i$. From the orbit-stabiliser relation and Lagrange's theorem we have that

$$|C_i| = |G|/|C_G(g_i)| = [G : C_G(g_i)]$$

Since this index is at least 2, $C_G(g_i)$ is a proper subgroup of G and therefore $[G : C_G(g_i)]$ is divisible by p. Therefore, from $(*)$, $|Z(G)|$ is divisible by p.

By Cauchy's theorem there is an element $z \in Z(G)$ with $|z| = p$. Let $N = \langle z\rangle \leqslant Z(G)$. Then $|N| = p$ and N is a normal subgroup of G. Let $H = G/N$. Then $|H| = |G|/p$ and therefore $|H| < |G|$ and $p^{s-1} \mid |H|$. By the inductive hypothesis there is a subgroup $K \leqslant H$ with $|K| = p^{s-1}$. Denote by π the natural projection homomorphism $\pi : G \to H = G/N$, $\pi(g) = gN$. Let $L = \pi^{-1}(K) = \{g \in G \mid \pi(g) \in K\}$. Then L is a subgroup of G and has order p^s.

Exercise 161. Use the first isomorphism theorem to prove that L has size p^{s-1}.

$\square$

Definition 5.19. A group of order p^s for some prime p and some $s \in \mathbb{N}$ is called a ***p*-group**. A **Sylow *p*-subgroup** of a finite group G is a subgroup $H \leqslant G$ such that

1) H is a p-group
2) $[G : H]$ is not divisible by p

Remark. 1. The condition that $[G : H]$ be not divisible by p is equivalent to the condition that if $|H| = p^s$ then s is the largest element in $\mathbb{N}$ for which $p^s \mid |G|$.

2. The first Sylow theorem shows that p-Sylow subgroups exist for all primes p that divide $|G|$.

Theorem 5.20: Second Sylow theorem

Let G be a finite group. Any two Sylow p-subgroups of G are conjugate.

Theorem 5.21: Third Sylow theorem

Let $p \in \mathbb{N}$ be prime and Let G be a finite group such that $p \mid |G|$. Denote by n_p be the number of Sylow p-subgroups of G. Then

1) $n_p \mid |G|$
2) $n_p \equiv 1 \pmod p$

Theorem 5.22: Fourth Sylow theorem

Let G be a finite group and $H \leqslant G$ a subgroup. If H is a p-group, then H is contained in a Sylow p-subgroup.