# 23. Group actions and automorphisms

Recall the definition of an action:

**Definition 23.1.** *Let $G$ be a group and let $S$ be a set.*

*An* ***action*** *of $G$ on $S$ is a function*

$$G \times S \longrightarrow S \qquad \textit{denoted by} \qquad (g, s) \longrightarrow g \cdot s,$$

*such that*

$$e \cdot s = s \qquad \textit{and} \qquad (gh) \cdot s = g \cdot (h \cdot s)$$

In fact, an action of $G$ on a set $S$ is equivalent to a group homomorphism (invariably called a **representation**)

$$\rho \colon G \longrightarrow A(S).$$

Given an action $G \times S \longrightarrow S$, define a group homomorphism

$$\rho \colon G \longrightarrow A(S) \qquad \text{by the rule} \qquad \rho(g) = \sigma \colon S \longrightarrow S,$$

where $\sigma(s) = g \cdot s$. Vice-versa, given a representation (that is, a group homomorphism)

$$\rho \colon G \longrightarrow A(S),$$

define an action

$$G \cdot S \longrightarrow S \qquad \text{by the rule} \qquad g \cdot s = \rho(g)(s).$$

It is left as an exercise for the reader to check all of the details.

The only sensible way to understand any group is let it act on something.

**Definition-Lemma 23.2.** *Suppose the group $G$ acts on the set $S$. Define an equivalence relation $\sim$ on $S$ by the rule*

$$s \sim t \qquad \textit{if and only if} \qquad g \cdot s = t \qquad \textit{for some } g \in G.$$

*The equivalence classes of this action are called* ***orbits****.*

*The action is said to be* **transitive** *if there is only one orbit (necessarily the whole of $S$).*

*Proof.* Given $s \in S$ note that $e \cdot s = s$, so that $s \sim s$ and $\sim$ is reflexive.

If $s$ and $t \in S$ and $s \sim t$ then we may find $g \in G$ such that $t = g \cdot s$. But then $s = g^{-1} \cdot t$ so that $t \sim s$ and $\sim$ is symmetric.

If $r$, $s$ and $t \in S$ and $r \sim s$, $s \sim t$ then we may find $g$ and $h \in G$ such that $s = g \cdot r$ and $t = h \cdot s$. In this case

$$t = h \cdot s = h \cdot (g \cdot r) = (hg) \cdot r,$$

so that $t \sim r$ and $\sim$ is transitive. $\square$

**Definition-Lemma 23.3.** *Suppose the group $G$ acts on the set $S$. Given $s \in S$ the subset*

$$H = \{\, g \in G \,|\, g \cdot s = s \,\},$$

*is called the* ***stabiliser*** *of $s \in S$.*

*$H$ is a subgroup of $G$.*

*Proof.* $H$ is non-empty as it contains the identity. Suppose that $g$ and $h \in H$. Then

$$(gh) \cdot s = g \cdot (h \cdot s) = g \cdot s = s.$$

Thus $gh \in H$, $H$ is closed under multiplication and so $H$ is a subgroup of $G$. □

**Example 23.4.** *Let $G$ be a group and let $H$ be a subgroup. Let $S$ be the set of all left cosets of $H$ in $G$. Define an action of $G$ on $S$,*

$$G \times S \longrightarrow S$$

*as follows. Given $gH \in S$ and $g' \in G$, set*

$$g' \cdot (gH) = (g'g)H.$$

*It is easy to check that this action is well-defined. Clearly there is only one orbit and the stabiliser of the trivial left coset $H$ is $H$ itself.*

**Lemma 23.5.** *Let $G$ be a group acting transitively on a set $S$ and let $H$ be the stabiliser of a point $s \in S$. Let $L$ be the set of left cosets of $H$ in $G$. Then there is an isomorphism of actions (where isomorphism is defined in the obvious way) of $G$ acting on $S$ and $G$ acting on $L$, as in* (23.4). *In particular*

$$|S| = \frac{|G|}{|H|}.$$

*Proof.* Define a map

$$f \colon L \longrightarrow S$$

by sending the left coset $gH$ to the element $g \cdot s$. We first have to check that $f$ is well-defined. Suppose that $gH = g'H$. Then $g' = gh$, for some $h \in H$. But then

$$\begin{aligned} g' \cdot s &= (gh) \cdot s \\ &= g \cdot (h \cdot s) \\ &= g \cdot s. \end{aligned}$$

Thus $f$ is indeed well-defined. $f$ is clearly surjective as the action of $G$ is transitive. Suppose that $f(gH) = f(gH)$. Then $gS = g's$. In this case $h = g^{-1}g'$ stabilises $s$, so that $g^{-1}g' \in H$. But then $g$ and $g'$ are in the same left coset and $gH = g'H$. Thus $f$ is injective as well as surjective, and the result follows. $\square$

Given a group $G$ and an element $g \in G$ recall the centraliser of $g$ in $G$ is

$$C_g = \{\, h \in G \mid hg = gh \,\}.$$

The centre of $G$ is then

$$Z(G) = \{\, h \in H \mid gh = hg \,\},$$

the set of elements which commute with everything; the centre is the intersection of the centralisers.

**Lemma 23.6** (The class equation)**.** *Let $G$ be a group.*

*The cardinality of the conjugacy class containing $g \in G$ is the index of the centraliser, $[G : C_g]$. Further*

$$|G| = |Z(G)| + \sum_{[G:C_g]>1} [G : C_g],$$

*where the second sum run over those conjugacy classes with more than one element.*

*Proof.* Let $G$ act on itself by conjugation. Then the orbits are the conjugacy classes. If $g \in$ then the stabiliser of $g$ is nothing more than the centraliser. Thus the cardinality of the conjugacy class containing $g$ is $[G : C_g]$ by (23.3).

If $g \in G$ is in the centre of $G$ then the conjugacy class containing $G$ has only one element, and vice-versa. As $G$ is a disjoint union of its conjugacy classes, we get the second equation. $\square$

**Lemma 23.7.** *If $G$ is a $p$-group then the centre of $G$ is a non-trivial subgroup of $G$. In particular $G$ is simple if and only if the order of $G$ is $p$.*

*Proof.* Consider the class equation

$$|G| = |Z(G)| + \sum_{[G:C_g]>1} [G : C_g].$$

The first and last terms are divisible by $p$ and so the order of the centre of $G$ is divisible by $p$. In particular the centre is a non-trivial subgroup.

If $G$ is not abelian then the centre is a proper normal subgroup and $G$ is not simple. If $G$ is abelian then $G$ is simple if and only if its order is $p$. $\square$

**Theorem 23.8.** *Let $G$ be a finite group whose order is divisible by a prime $p$.*

*Then $G$ contains at least one Sylow $p$-subgroup.*

*Proof.* Suppose that $n = p^k m$, where $m$ is coprime to $p$.

Let $S$ be the set of subsets of $G$ of cardinality $p^k$. Then the cardinality of $S$ is given by a binomial

$$\binom{n}{p^k} = \frac{p^k m(p^k m-1)(p^k m-2)\dots(p^k m-p^k+1)}{p^k(p^k-1)\dots 1}$$

Note that for every term in the numerator that is divisible by a power of $p$, we can match this term in the denominator which is also divisible by the same power of $p$. In particular the cardinality of $S$ is coprime to $p$.

Now let $G$ act on $S$ by left translation,

$$G \times S \longrightarrow S \qquad \text{where} \qquad (g, P) \longrightarrow gP.$$

Then $S$ is breaks up into orbits. As the cardinality is coprime to $p$, it follows that there is an orbit whose cardinality is coprime to $p$. Suppose that $X$ belongs to this orbit. Pick $g \in X$ and let $P = g^{-1}X$. Then $P$ contains the identity. Let $H$ be the stabiliser of $P$. Then $H \subset P$, since $h \cdot e \in P$. On the other hand, $[G : H]$ is coprime to $p$, so that the order of $H$ is divisible by $p^k$. It follows that $H = P$. But then $P$ is a Sylow $p$-subgroup. □

**Question 23.9.** *What is the automorphism group of $S_n$?*

**Definition-Lemma 23.10.** *Let $G$ be a group.*

*If $a \in G$ then conjugation by $G$ is an automorphism $\sigma_a$ of $G$, called an* ***inner automorphism*** *of $G$. The group $G'$ of all inner automorphisms is isomorphic to $G/Z$, where $Z$ is the centre. $G'$ is a normal subgroup of* $\operatorname{Aut}(G)$ *the group of all automorphisms and the quotient is called the* ***outer automorphism*** *group of $G$.*

*Proof.* There is a natural map

$$\rho \colon G \longrightarrow \operatorname{Aut}(G),$$

whose image is $G'$. The kernel is isomorphic to the centre and so

$$G' \simeq G/Z,$$

by the first Isomorphism theorem. It follows that $G' \subset \operatorname{Aut}(G)$ is a subgroup. Suppose that $\phi \colon G \longrightarrow G$ is any automorphism of $G$. I claim that

$$\phi\sigma_a\phi^{-1} = \sigma_{\phi(a)}.$$

Since both sides are functions from $G$ to $G$ it suffices to check they do the same thing to any element $g \in G$.

$$\begin{aligned}\phi\sigma_a\phi^{-1}(g) &= \phi(a\phi^{-1}(g)a^{-1}) \\ &= \phi(a)g\phi(a)^{-1} \\ &= \sigma_{\phi(a)}(g).\end{aligned}$$

Thus $G'$ is normal in $\mathrm{Aut}(G)$. □

**Lemma 23.11.** *The centre of $S_n$ is trivial unless $n = 2$.*

*Proof.* Easy check. □

**Theorem 23.12.** *The outer automorphism group of $S_n$ is trivial unless $n = 6$ when it is isomorphic to $\mathbb{Z}_2$.*

**Lemma 23.13.** *If $\phi\colon S_n \longrightarrow S_n$ is an automorphism of $S_n$ which sends a transposition to a transposition then $\phi$ is an inner automorphism.*

*Proof.* Since any automorphism permutes the conjugacy classes, $\phi$ sends transpositions to transpositions. Suppose that $\phi(1,2) = (i,j)$. Let $a = (1,i)(2,j)$. Then $\sigma_a(i,j) = (1,2)$ and so $\sigma_a\phi$ fixes $(1,2)$. It is obviously enough to show that $\sigma_a\phi$ is an inner automorphism. Replacing $\phi$ by $\sigma_a\phi$ we may assume $\phi$ fixes $(1,2)$.

Now consider $\tau = \phi(2,3)$. By assumption $\tau$ is a transposition. Since $(1,2)$ and $(2,3)$ both move 2, $\tau$ must either move 1 or 2. Suppose it moves 1. Let $a = (1,2)$. Then $\sigma_a\phi$ still fixes $(1,2)$ and $\sigma_a\tau$ moves 2. Replacing $\phi$ by $\sigma_a\phi$ we may assume $\tau = (2,i)$, for some $i$. Let $a = (3,i)$. Then $\sigma_a\phi$ fixes $(1,2)$ and $(2,3)$. Replacing $\phi$ by $\sigma_a\phi$ we may assume $\phi$ fixes $(1,2)$ and $(2,3)$.

Continuing in this way, we reduce to the case when $\phi$ fixes $(1,2)$, $(2,3)$, $\dots$, and $(n-1,n)$. As these transpositions generate $S_n$, $\phi$ is then the identity, which is an inner automorphism. □

**Lemma 23.14.** *Let $\sigma \in S_n$ be a permutation. If*

*(1) $\sigma$ has order 2,*
*(2) $\sigma$ is not a tranposition, and*
*(3) the conjugacy class generated by $\sigma$ has cardinality*

$$\binom{n}{2},$$

*then $n = 6$ and $\sigma$ is a product of three disjoint tranpositions.*

*Proof.* As $\sigma$ has order two it must be a product of $k$ disjoint tranpositions. The number of these is

$$\frac{1}{k!}\binom{n}{2}\binom{n-2}{2}\dots\binom{n-2k+2}{2}.$$

For this to be equal to the number of transpositions we must have

$$\frac{1}{k!}\binom{n}{2}\binom{n-2}{2}\cdots\binom{n-2k+2}{2}=\binom{n}{2},$$

that is

$$n! = 2^k(n-2k)!k!\binom{n}{2}.$$

It is not hard to check that the only solution is $k = 3$ and $n = 6$. $\square$

Note that if there is an outer automorphism of $S_6$, it must switch transpositions with products of three disjoint transpositions. So the outer automorphism group is no bigger than $\mathbb{Z}_2$.

The final thing is to actually write down an outer automorphism. This is harder than it might first appear. Consider the complete graph $K^5$ on 5 vertices. There are six ways to colour the edges two colours, red and blue say, so that we get two 5-cycles. Call these colourings magic.

$S_5$ acts on the vertices of $K^5$ and this induces an action on the six magic colourings. The induced representation is a group homomorphism

$$i\colon S_5 \longrightarrow S_6,$$

which it is easy to see is injective. One can check that the tranposition $(1,2)$ is sent to a product of three disjoint tranpositions. But then $S_6$ acts on the left cosets of $i(S_5)$ in $S_6$, so that we get a representation

$$\phi\colon S_6 \longrightarrow S_6,$$

which is an outer automorphism.