3.2 The Orbit-Stabilizer Theorem

Definition 3.2.1. *Let* G *be a group and let* S *be a set. We say that* G acts on S *if every element* g *of* G *induces a permutation* π_g *of the set* S*, subject to the following conditions*

1. *The identity element of* G *acts as the identity permutation on* S *- it leaves every element of* S *fixed.*
2. *If* g *and* h *are two elements of* G*, then the permutation* π_{gh} *of* S *is* $\pi_g \circ \pi_h$.

The second condition above is about compatibility of the action on S with the group operation of G. When we think of G acting on the set S, it means that group elements move the elements of S around. Informally we can think of hitting elements of S with group elements to move them around in S. A particular group element can be applied to all the elements of S and it rearranges them. How exactly this happens depends on the context, but the examples of Section 3.1 are fairly typical. The second condition above says that applying the element h to the set S and then applying g should be the same as applying gh in one step.

Notation: If G is a group acting on a set S, let $g \in G$ and $x \in S$. The notation $g \cdot x$ is often used to refer to element of S that results from applying (the permutation determined by) g to the element x. Then condition 2. above says

$$g \cdot (h \cdot x) = gh \cdot x,$$

for all $g, h \in G$ and all $x \in S$.

A good exercise at this point is to think about the examples of Section 3.1 in the context of this formal definition.

Suppose that the group G acts on the set S, and let $x \in S$.

Definition 3.2.2. *The* orbit *of* x *under the action of* G*, denoted* $O_G(x)$ *or* $G \cdot x$*, is defined as the subset of* S *consisting of all elements that can be reached from* x *by applying elements of* G.

$$G \cdot x = \{g \cdot x : g \in G\}.$$

Note that if G is finite, then the number of elements in the orbit of x is at most equal to the order of G, but it might be less.

We note the following properties of orbits.

1. For every $x \in S$ we have $x \in G \cdot x$ since $x = \mathrm{id} \cdot x$.
2. If $y \in G \cdot x$ for some $x \in S$, then $G \cdot y = G \cdot x$.
   To see this note that $y = h \cdot x$ (for some $h \in G$) means that $g \cdot y = g \cdot (h \cdot x) = gh \cdot x$ for all $g \in G$. Thus every element of $G \cdot y$ belongs to $G \cdot x$. On the other hand $y = h \cdot x$ implies that $x = h^{-1} \cdot y$, so $x \in G \cdot y$ and hence $G \cdot x \subseteq G \cdot y$.
3. It follows from 2. above that if some element z of S belongs to the orbits of both x and y, then $G \cdot z$ is equal to both $G \cdot x$ and $G \cdot y$, so these are equal to each other. So if the orbits determined by two different elements intersect, then they coincide fully. The alternative is that they don't intersect at all.
4. So the action of G *partitions* the set S into a collection of disjoint subsets, which are orbits. Note that G acts separately upon each orbit, in the sense that elements of G do not move elements of S from one orbit to another, they only move elements around within their own orit.
5. An action with only one orbit is called *transitive*. If G acts transitively on the set S, it means that given any elements x, y of S there is an element g of G for which $g \cdot x = y$.

Definition 3.2.3. *The* stabilizer *in* G *of the element* x *of* S*, denoted* $\mathrm{Stab}_G(x)$*, is the subset of* G *consisting of those elements that leave* x *fixed.*

$$\mathrm{Stab}_G(x) = \{g \in G : g \cdot x = x\}.$$

Lemma 3.2.4. *Let* G *be a group acting on a set* S *and let* $x \in S$*. Then* $\mathrm{Stab}_G(x)$ *is a subgroup of* G.

Proof. The the identity element of G belongs to $\mathrm{Stab}_G(x)$ is immediate from our definition of group action.

Suppose now that $g, h \in \mathrm{Stab}_G(x)$. Then

$$gh \cdot x = g \cdot (h \cdot x) = g \cdot x = x,$$

so $gh \in \mathrm{Stab}_G(x)$ and $\mathrm{Stab}_G(x)$ is closed under the group operation of G.

Finally, if $g \in \mathrm{Stab}_G(x)$ then $g \cdot x = x$ and so $g^{-1} \cdot (g \cdot x) = g^{-1} \cdot x$. Also $g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = id \cdot x = x$. Hence $g^{-1} \cdot x = x$ which means $g^{-1} \in \mathrm{Stab}_G(x)$. □

The most fundamental theorem about group actions is the *Orbit-Stabilizer Theorem*, which states that the size of the orbit of an element is equal to the index of its stabilizer in the group. This applies to any situation in which the relevant orbit is finite, although for simplicity we state it only for finite groups.

Theorem 3.2.5. *(Orbit-Stabilizer Theorem) Let G be a finite group acting on a set S, and let $x \in S$. Then the number of elements in the orbit $G \cdot x$ is equal to $[G : \mathrm{Stab}_G(x)]$.*

Note: Recall that $[G : \mathrm{Stab}_G(x)]$ is the *index* of $\mathrm{Stab}_G(x)$ in G, which is the number of distinct left cosets of $\mathrm{Stab}_G(x)$ in G.

Proof. Let g and h be elements of G and consider when the elements $g \cdot x$ and $h \cdot x$ of $G \cdot x$ are equal.

$$g \cdot x = h \cdot x \iff g^{-1}g \cdot x = g^{-1}h \cdot x \iff x = g^{-1}h \cdot x.$$

Thus $g \cdot x = \cdot x$ if and only if $g^{-1}h = t$ for some $t \in \mathrm{Stab}_G(x)$. This occurs if and only if $h = gt$ which means that h belongs to the left coset of $\mathrm{Stab}_G(x)$ determined by g, which means that g and h determine the same left coset of $\mathrm{Stab}_G(x)$. Thus the number of distinct elements of the orbit of x is equal to the number of distinct left cosets of $\mathrm{Stab}_G(x)$ in G, as required. □

Note that Theorem 2.2.9 may be regarded as an instance of the Orbit-Stabilizer Theorem, where the action in question is the conjugation action of the group G on itself, defined by

$$g \cdot x = gxg^{-1}, \text{for } g \in G \text{ and } x \in G.$$

In this case the orbit of the element x is the set of all gxg^{-1} as g runs through the group, i.e. the conjugacy class of x. The stabilizer of x is the set of elements g of G for which $gxg^{-1} = x$, i.e. for which $gx = xg$. This is the set of group elements that commute with x, or the centralizer of x in G. Thus the Orbit-Stabilizer Theorem says that the number of distinct conjugates of x in G is the index in G of $C_G(x)$, which is Theorem 2.2.9.

We finish this chapter with another classical theorem, which again highlights the importance of the symmetric group amongst all finite groups. Cayley's Theorem shows that any finite group, via its action on itself by left multiplication, may be considered to be a group of permutations of n objects and thus may be considered to be a subgroup of the symmetric group S_n. The group S_n has order $n!$ which is much greater than n obviously, but Cayley's Theorem says that amongst the subgroups of S_n are copies of every group of order n.

To state the theorem and to clarify the meaning of "copies", we need a definition.

Definition 3.2.6. *Two groups are said to be* isomorphic to each other *if after some relabelling of their elements they become exactly the same.*

For example, the group $\{1, i, -1, -i\}$ of complex fourth roots of unity and the group $\{id, R_{90}, R_{180}, R_{270}\}$ are isomorphic to each other. Each of them is is a cyclic group of order 4, and after relabelling their elements a, b, c, d (in the order in which they are written above), their group tables become identical, as the superscripts show below.

If two groups are isomorphic it means that they are structurally identical, and differ only in how their elements are labelled. We can now state Cayley's Theorem.

Theorem 3.2.7 (Cayley, 1854)**.** *Let G be a group of order n. Then G is isomorphic to some subgroup of the symmetric group S_n.*

Cayley's Theorem says that, in principle, if you want to understand all finite groups you really only need to understand the symmetric groups. This does not translate so easily into practice though, because the symmetric group S_n is so much bigger than any group of order n. Nevertheless Cayley's Theorem is a strong reason to be interested in the study of the symmetric groups.

To indicate how Cayley's Theorem can be proved, we go back to the example of the group $\{1, i, -1, i\}$ under multiplication of complex numbers. This group (like all groups) acts on itself by *left multiplication*. Multiplying all four group elements (on the left) by $1, i, -1$ or $-i$ produces a permutation of the set $\{1, i, -1, -i\}$ as follows.

$$1: \begin{array}{ccc} 1 & \to & 1 \\ i & \to & i \\ -1 & \to & -1 \\ -i & \to & -i \end{array} \qquad i: \begin{array}{ccc} 1 & \to & i \\ i & \to & -1 \\ -1 & \to & -i \\ -i & \to & 1 \end{array} \qquad -1: \begin{array}{ccc} 1 & \to & -1 \\ i & \to & -i \\ -1 & \to & 1 \\ -i & \to & i \end{array} \qquad -i: \begin{array}{ccc} 1 & \to & -i \\ i & \to & 1 \\ -1 & \to & i \\ -i & \to & -1 \end{array}$$

So each element of the group corresponds to a permutation of the four objects $1, i, -1, -i$. In considering these permutations themselves, we don't care any more that $1, i, -1, -i$ are the four elements of the group that we started with, we just consider each permutation as a permutation of the four objects. To emphasize this point, we can relabel the four elements as a, b, c, d, and represent each of our group elements as a permutation of a, b, c, d (written now in cycle notation).

$$1 \leftrightarrow \mathrm{id},\ i \leftrightarrow (a\ b\ c\ d),\ -1 \leftrightarrow (a\ c)(b\ d),\ -i \leftrightarrow (a\ d\ c\ b).$$

These four permutations form a subgroup of S_4 that is isomorphic to the group $\{1, i, -1, -i\}$.

This correspondence between the elements of G and the permutations that they determine of the n group elements works in exactly the same way for all finite groups and is the basis of the proof of Cayley's Theorem. The permutations determined by the different elements of G are essentially the orderings of the group that are written into the rows of the group table. Two different elements of the group cannot determine the same permutation, since this would mean that the group table would have two identical rows.

A more general proof of Cayley's Theorem is given below, but the idea is exactly the same as for this example.

Proof. (of Cayley's Theorem). Let G be a group of order n, with elements $g_1(= \mathrm{id}), g_2, g_3, \ldots, g_n$. Let $g \in G$ (so g is one of the g_i). Define a function ϕ_g from G to G by

$$\phi_g(g_i) = gg_i.$$

Note that each gg_i is an element of G, and that gg_i and gg_j are different whenever g_i and g_j are different. Thus ϕ_g is a permutation of the n elements of G. If you write out the group table for G, then ϕ_g is the permutation of the elements of G that is written into the row corresponding to g. Thus each element of G can be associated to a particular permutation of the n elements of G, which may be regarded as an element of S_n. We have a correspondence

$$g \leftrightarrow \phi_g$$

between g and the set $\{\phi_g : g \in G\}$ of permutations.

Finally, for elements g and h of G, notice that for each g_i

$$\phi_g(\phi_h(g_i)) = \phi_g(hg_i) = g(hg_i) = ghg_i = \phi_{gh}(g_i).$$

Thus the composition of $\phi_g \circ \phi_h$ of the permutations corresponding to g and h is the permutation corresponding to the product gh in G. This means that the above correspondence between group elements and permutations is not only a correspondence of elements of G with elements of S_n, it is also a correspondence of the group operation of G with composition of permutations in S_n. Thus it establishes that G is isomorphic to a subgroup of S_n. □