Lecture 17

Group actions

17.1 Goals

1. Understand the definition of a group action.

2. See examples of group actions.

3. Understand that the automorphisms of an object always acts on the object.

4. Understand that the above is a "universal example," meaning any other group action can be recast as a homomorphism to the automorphism group.

5. Become comfortable with the notion of order of a group, and order of an element of a group.

17.2 Group actions

I have, sneakily, already used the idea of actions when speaking about matrices. Concretely, I saw that "two-by-two matrices act on $\mathbb{R}^2$." At the time, you probably inferred this means that a 2-by-2 matrix knows how to take in a given two-dimensional vectors and output two-dimensional vector.

This concept generalizes in the following way. Let X be any set. Then there may be a way in which some group G acts on X.

Example 17.2.1. Let G be the set of symmetries of a shape X. (For example, X might be a non-square mattress, and G might be its four-element group of symmetries). Then certainly, given a symmetry $g \in G$, g operates on the shape X, so every point $x \in X$ gets sent to some point $gx \in X$.

It would not be a mistake to say that in most interactions between geometry and group theory, we study groups for the sake of their potential actions on geometric objects. So let's finally define what a group action is.

Definition 17.2.2 (Group action)**.** Let G be a group and X a set. A *left group action*, or group action for short, is a function $G \times X \to X$—where we will denote the image of (g, x) by the notation gx—satisfying the following:

1. For every $x \in X$, we have $ex = x$.

2. For every $g, h, \in G$ and $x \in X$, we have $g(hx) = (gh)x$.

Remark 17.2.3. Consider a function $G \times X \to X$. If you fix an element $g \in G$, we obtain a function $X \to X$ given by $x \mapsto gx$. So you can think of a group action as a collection of transformations from X to itself, where each $g \in G$ defines a transformation.

Remark 17.2.4. The first condition (1) says that the identity element acts by "doing nothing" on all elements of X. Let's carefully interpret conditin (2). Given an element x, we get a new element $hx \in X$. We could then compute where g sends this element. On the other hand, we could have first multiplied gh to get an element of G. Then we could ask where gh sends x. The condition demands that x ends up—regardless of which journey it takes—at the same point.

Remark 17.2.5. There is also the notion of a *right group action*, which is given by a function $X \times G \to X$ satisfying $xe = x$ and $(xg)h = x(gh)$. As you will prove in Exercise 17.5.5, any left group action gives rise to a right group action by declaring $xg := g^{-1}x$; and vice versa.

Example 17.2.6. Let G be any group and X any set. Consider the function $G \times X \to X$ which sends the pair (g, x) to x. In other words, this $gx = x$ for all g, x. You can check this is a group action. It is called the *trivial* group action on X.

Example 17.2.7. Let $G = GL_2(\mathbb{R})$ be the group of 2-by-2 invertible matrices. Let $X = \mathbb{R}^2$. Then we have an action $GL_2(\mathbb{R}) \times \mathbb{R}^2 \to \mathbb{R}^2$ by sending a pair $(A, \vec{x})$ to $A\vec{x}$. In other words, matrix multiplication (by invertible matrices) is a group action on $\mathbb{R}^2$.

Example 17.2.8. Here is a fun one. Consider an equilateral triangle T, and let G be the group of symmetries of T (preserving all distances). As we've discussed before, any such symmetry must send vertices to vertices. So let V be the set of vertices of T. V consists of 3 elements. I claim that G has an action on V.

Indeed, if g is a symmetry of T and v is a vertex of v, let $gv = g(v)$ denote the vertex that v is sent to under g. Then the identity symmetry e of course doesn't move vertices, so $ev = e(v) = v$. Moreover, gh is the symmetry called "do h, and then do g" so we have that $(gh)v = g(h(v)) = g \cdot (hv)$. This proves that the function

$$G \times V \to V, \qquad (g, v) \mapsto g(v)$$

is a group action.

In fact, there are more variations on this theme. Let E be the set of edges of T. Then G also acts on E, as any symmetry of T will send edges to edges.

Example 17.2.9. More generally, if P is any polygon and G is the group of symmetries of P (preserving all distances), G acts on the set of vertices of P. If E is the set of edges of P, then G acts on E.

Even more generally, if P is now a polyhedron, and G its group of symmetries (preserving distances), then G will act on the set of faces of P.

17.3 Symmetric groups

There are some groups that tautologically act on some sets.

Definition 17.3.1. Let X be a set. We let $\mathrm{Aut}(X)$ denote the set of bijections from X to itself. We call $\mathrm{Aut}(X)$ the group of *automorphisms of* X, and sometimes *set automorphisms of* X. $\mathrm{Aut}(X)$ is also sometimes called the *symmetric group on* X.

When X is the set $\{1, 2, \ldots, n\}$, it is common to write S_n instead of $\mathrm{Aut}(X)$. S_n is called *the symmetric group on n letters.*

We will justify the word "group" after these examples:

Example 17.3.2. Let $X = \{1, 2\}$. Then there are exactly two elements of $\mathrm{Aut}(X) = S_2$. A function called id_X, which is defined by

$$\mathrm{id}_X(1) = 1, \qquad \mathrm{id}_X(2) = 2.$$

(So for all $x \in X$, we declare $\mathrm{id}_X(x) = x$.) This is called the *identity function* from X to itself.

The other element of S_2 is the "swap," which I'll call σ for no good reason. This function is defined by

$$\sigma(1) = 2, \qquad \sigma(2) = 1.$$

The function σ is an injection (because the two elements of X are sent to distinct elements) and a surjection (because σ hits all elements of X) and hence a bijection. You can check that σ is its own inverse.

Example 17.3.3. Let $X = \{1, 2, 3\}$. There are exactly six elements of $\mathrm{Aut}(X) = S_3$. The easiest to understand is id_X, the identity function—it is defined by $\mathrm{id}_X(x) = x$ (for all $x \in X$). The other 5 are specified by permuting elements of X.

Let's understand why there are 6 bijections from X to itself. To specify a bijection $\tau : X \to X$, one must specify $\tau(1)$. There are, of course, three options for $\tau(1)$. (The options are 1, 2, 3) Now let's specify $\tau(2)$. If we demand τ to be an injection, one now has only two remaining choices for $\tau(2)$. Finally, $\tau(3)$ is the last remaining element of X not hit by $\tau(1), \tau(2)$. Thus we see

$$3 \times 2 \times 1 = 6$$

different bijections from X to itself.

The above examples generalize:

Proposition 17.3.4. S_n is a set with $n! = n \times (n-1) \times \ldots \times 2 \times 1$ elements.

Now let's justify the fact that we are calling $\mathrm{Aut}(X)$ a group.

Proposition 17.3.5. For any set X, $\mathrm{Aut}(X)$ is a group under composition.

Proof. To be clear, given two elements $f, g \in \mathrm{Aut}(X)$, the group operation is given by $fg = f \circ g$.

First, let's make sure this is indeed a function that takes two automorphisms of X and outputs an automorphism of X (as opposed to just another function). Well, if f and g are bijections, then so is their composition $f \circ g$.

Now let us prove that this binary operation satisfies the three group properties.

First, the identity element is the identity function: id_X. Concretely, this is the function $\mathrm{id}_X(x) = x$. Then for any $f \in \mathrm{Aut}(X)$, we have that $(f \circ \mathrm{id}_X)(x) = f(\mathrm{id}_X(x)) = f(x)$. Thus, $f \circ \mathrm{id} = f$. Likewise, $(\mathrm{id}_X \circ f)(x) = \mathrm{id}_X(f(x)) = f(x)$, so $\mathrm{id}_x \circ f = f$. We have shown that id_X is an identity element for the binary operation of composition.

Next, inverses. Given $f \in \mathrm{Aut}(X)$, we know there exists an inverse function f^{-1} because f is a bijection. Then $(f \circ f^{-1})(x) = f(f^{-1}(x)) = x$ by definition of inverse; this shows $f \circ f^{-1} = \mathrm{id}_X$. Similarly, $(f^{-1} \circ f)(x) = f^{-1}(f(x)) = x$, so $f^{-1} \circ f = \mathrm{id}_X$. This shows f^{-1} is indeed the inverse of f under the binary operation of composition.

Finally, function composition is always associative: $f \circ (g \circ h) = (f \circ g) \circ h$.

We have finished showing that $\mathrm{Aut}(X)$ is a group. □

I began this section by saying that some groups tautologically have an action on some sets. We now see why I said that:

Example 17.3.6. Let X be a set. Then $\mathrm{Aut}(X)$ acts on X, by declaring

$$\mathrm{Aut}(X) \times X \to X, \qquad (f, x) \mapsto f(x).$$

Put another way, we declare $fx = f(x)$. The axioms of a group action are checked straightforwardly:

$$\mathrm{id}_X\, x = \mathrm{id}_X(x) = x$$

(by definition of the function id_X), and finally

$$(f \circ g)x = (f \circ g)(x) = f(g(x)) = f \cdot (gx).$$

Moreover, $\mathrm{Aut}(X)$ is the "universal" example of a group acting on X. That I am able to articulate this is another use of group homomorphisms.[1]

[1]Early on in one's math career, it's hard to appreciate the utility of certain frameworks. Group homomorphisms, just like ring homomorphisms, are useful because they can probe properties of one group using another group. But even more importantly, group homomorphisms give us a language for organizing natural phenomena we see in the mathematical world.

The next proposition says that an action of G on X is the same thing as a group homomorphism $G \to \mathrm{Aut}(X)$.

Proposition 17.3.7. Fix a group action $G \times X \to X$. By sending every $g \in G$ to the function $f_g : x \mapsto gx$, we have a group homomorphism

$$G \to \mathrm{Aut}(X), \qquad g \mapsto f_g.$$

Moreover, this function (from the set of all group actions, to the set of all group homomorphisms) is a bijection. In other words, there is a one-to-one correspondence between group actions of G on X, and group homomorphisms from G to $\mathrm{Aut}(X)$.

Proof. Let's first show that f_g is indeed an element of $\mathrm{Aut}(X)$. For this, let us note that

$$(f_{g^{-1}} \circ f_g)(x) f_{g^{-1}}(f_g(x)) = g^{-1} \cdot gx = (g^{-1}g)x = ex = x.$$

(The first equality is by the definition of $f_\bullet$, the next is by the definition of group action, the next is by the definition of g^{-1}, and the last is by definition of group action.) The above equalities prove that $f_{g^{-1}} \circ f_g = \mathrm{id}_X$. One can likewise show that $f_g \circ f_{g^{-1}} = \mathrm{id}_X$, so f_g is a bijection (with inverse $f_{g^{-1}}$. This shows f_g is indeed in $\mathrm{Aut}(X)$. In particular, we have verified indeed that the assignment $g \mapsto f_g$ is a function from G to $\mathrm{Aut}(X)$.

Now let us show that this is a group homomorphism. For this, we must show that $f_{gh} = f_g \circ f_h$. This follows by definition of group action:

$$f_{gh}(x) = (gh)(x) = g \cdot hx = f_g(hx) = f_g(f_h(x)) = (f_g \circ f_h)(x).$$

Because the above equality holds for all x, $f_{gh} = f_g \circ f_h$.

To prove the last statement, we will provide an inverse to the construction. Let $\phi : G \to \mathrm{Aut}(X)$ be a homomorphism. Then we define a function $G \times X \to X$ by $(g, x) \mapsto \phi(g)(x)$. In other words, $gx = \phi(g)(x)$. We leave it to the reader to verify that this assignment is an inverse assignment. □

17.4 Order

Every lecture in the "groups" unit, my hope is to give examples, and also to illustrate some general terminology and facts we can use to study all groups. Today we'll talk about the notion of order.

Definition 17.4.1 (Order)**.** Let G be a finite group. The *order* of G is the number of elements in G. When G contains exactly n elements, we say that G is a *group of order* n.

When G is not finite, we often say that G is a group of infinite order. We may sometime say "countable order" or "uncountable order" for groups of countable or uncountable cardinality, respectively.

Example 17.4.2. $\mathbb{Z}/n\mathbb{Z}$ is a group of order n.

If X is a finite set of k elements, $\mathrm{Aut}(X)$ is a group of order $k!$.

The word order is also used not just to describe groups, but also elements of a group, in the following way:

Definition 17.4.3 (Order of an element)**.** Let G be a group and $g \in G$. The smallest positive integer $n \geq 1$ for which $g^n = e$ is called the *order* of g. We say that g is an *element of order* n.

If there is no such integer (so that g^n never equals e regardless of $n \geq 1$) we say that g is an element of infinite order.

Example 17.4.4. The identity element of a group is the only element of order 1.

Example 17.4.5. In $\mathbb{Z}$, every element (except 0) has infinite order.

Example 17.4.6. In $\mathbb{Z}/n\mathbb{Z}$, the element 1 has order n.

Example 17.4.7. In $\mathbb{Z}/6\mathbb{Z}$, 1 has order 6, 2 and 4 have order 3, and 3 has order 2. (You should check this.)

More generally, if $k \in \mathbb{Z}/6\mathbb{Z}$ and we represent k as a number between 0 and $n-1$, then the order of k is $lcm(k,n)/k$, where $lcm(k,n)$ is the least common multiple of k and n.

Remark 17.4.8. We saw in Exercise 16.4.6 that udnerstanding orders of elements can be useful. For example, if G is isomorphic to H, then G has elements of order 5 if and only if H does. (And 5 is not special here.)

17.5 Exercises

Exercise 17.5.1. Find the orders of the following groups:

(a) $GL_2(\mathbb{Z}/2\mathbb{Z})$

(b) $GL_2(\mathbb{Z}/2\mathbb{Z}) \times GL_2(\mathbb{Z}/2\mathbb{Z})$

(c) $\mathbb{Z}/2\mathbb{Z} \times GL_2(\mathbb{Z}/2\mathbb{Z})$

(d) $S_n \times \mathbb{Z}/(n+1)\mathbb{Z}$.

Exercise 17.5.2. Find the order of the element 3 (which is our lazy notation for [3]) in each of the following groups:

1. $\mathbb{Z}/2\mathbb{Z}$
2. $\mathbb{Z}/3\mathbb{Z}$
3. $\mathbb{Z}/4\mathbb{Z}$
4. $\mathbb{Z}/6\mathbb{Z}$
5. $\mathbb{Z}/7\mathbb{Z}$
6. $\mathbb{Z}/2021\mathbb{Z}$

Exercise 17.5.3. Find the order of the element $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ (which is our lazy notation for $\begin{pmatrix} [1] & [1] \\ [0] & [1] \end{pmatrix}$) in each of the following groups:

1. $GL_2(\mathbb{Z}/2\mathbb{Z})$
2. $GL_2(\mathbb{Z}/3\mathbb{Z})$
3. $GL_2(\mathbb{Z}/6\mathbb{Z})$
4. $GL_2(\mathbb{Z}/2021\mathbb{Z})$

Exercise 17.5.4. For each of the following examples of G, X and function $G \times X \to X$, say whether the function is a group action. If an example is not a group action, say which property (or properties) of a group action is (are) violated.

1. $G = X$, and $(g, x) \mapsto gx$ is group multiplication.
2. $G = X$, and $(g, x) \mapsto g^{-1}x$ is group multiplication of x with g^{-1}.

3. $G = \mathbb{Z}$, $X = \{0, 1\}$, and $(n, x) \mapsto x$ if n is even, while $(n, x) \mapsto$ the unique non-x element of X when n is odd.

4. $G = GL_2(\mathbb{R})$, $X = \mathbb{R}$. For any $A \in GL_2(\mathbb{R})$ and $x \in \mathbb{R}$, declare (A, x) to be sent to the x_1-coordinate of the vector $A \begin{pmatrix} x \\ 0 \end{pmatrix}$.

5. $G = X$, and $(g, x) \mapsto gxg^{-1}$.

6. For any function $g : Y \to Y$ and subset $A \subset Y$, define $g(A) = \{g(a) \,|\, a \in A\}$. Now let $X = \mathcal{P}(Y)$ be the power set of Y (that is, X is the set of all subsets of Y). For $G = \mathrm{Aut}(Y)$, consider the function $G \times X \to X$ given by $(g, A) \mapsto g(A)$.

Exercise 17.5.5. Suppose one has a left group action $G \times X \to X$. Define a function $X \times G \to X$ by $(x, g) \mapsto g^{-1}x$ (where $g^{-1}x$ uses the given left group action). Prove that this function is a right group action (Remark 17.2.5).

Conversely, given a right group action $X \times G \to X$, shows that the assignment $(g, x) \mapsto xg^{-1}$ defines a left group action.