Lecture 01: Symmetries of objects.

Wednesday, September 26, 2018 8:57 PM

Groups are symmetries of objects. What do we mean by a symmetry of an object \( X \)? Roughly, it means a function \( f: X \to X \) that preserves “properties” of \( X \); and \( f^{-1}: X \to X \) exists and preserves “properties” of \( X \).

To understand this better, we look at a few examples:

At the level of set theory. When \( X \) is just a non-empty set, then any bijection \( f: X \to X \) is a symmetry of \( X \).

This group is denoted by \( S_X \), and is called the symmetric group of \( X \); \( S_X := \{ f: X \to X \mid f \text{ is a bijection} \} \).

For a positive integer \( n \), we write \( S_n \) instead of \( S_{\{1, \ldots, n\}} \).

You have seen that \( |S_n| = n! \).

Symmetries of a graph \( G = (V, E) \).

A symmetry of a graph \( G \) is a function \( f: V \to V \) st.

1. \( f \) is a bijection
2. \( \forall v, w \in E \iff f(v)w, f(w)v \in E \)

(at the level of set theory) \( v \) is connected to \( w \) iff \( f(v) \) is connected to \( f(w) \).
The automorphism group of an n-cycle. In this example, we would like to describe elements of $\text{Aut}(\mathbb{Z}/n\mathbb{Z})$.

Typically in order to understand the group of symmetries of an object with "lots" of symmetries we use the following steps:

1. Find a rich set of symmetries;

2. Prove a type of "rigidity";

Can you give me a few symmetries of $\mathbb{Z}/n\mathbb{Z}$?

"Rotations": Let $\tau \in S_n$, $1 \mapsto 2 \mapsto 3 \mapsto \cdots \mapsto n$

Then $\tau, \tau^2, \ldots, \tau^{n-1}$ are distinct.

"Reflections": Let $\sigma \in S_n$,

$1 \mapsto 1, 2 \mapsto n, 3 \mapsto n-1, \ldots$

So far we have found $\id, \tau, \ldots, \tau^{n-1}, \sigma, \tau \sigma, \ldots, \tau^{n-1} \sigma$.

$\text{Aut}(\mathbb{Z}/n\mathbb{Z})$. 
Next you can see the following "rigidity":

An automorphism that fixes 1 and 2 is identity; prove by induction on $i$ that $\gamma(i)=i$.

Now we show $\text{Aut}(\pi_1) = \langle \text{id, } \tau, \ldots, \tau^{n-1}, \sigma, \tau \cdot \sigma, \ldots, \tau^{n-1} \cdot \sigma \rangle$.

Suppose $\gamma \in \text{Aut}(\pi_1)$. So $\exists i$ s.t. $\tau^{-i} \cdot \gamma(i) = 1$.

Since $\tau^{-i} \cdot \gamma$ is an automorphism, $\tau^{-i} \cdot \gamma(2)$ is connected to 1. Hence either $\tau^{-i} \cdot \gamma(2) = 2$ or $\tau^{-i} \cdot \gamma(2) = n$.

**Case 1.** $\tau^{-i} \cdot \gamma(2) = 2$. Then, by rigidity, $\tau^{-i} \cdot \gamma = \text{id}$.

And so $\gamma = \tau^i$.

**Case 2.** $\tau^{-i} \cdot \gamma(2) = n$. Then $\sigma \cdot \tau^{-i} \cdot \gamma$ fixes 1 and 2.

Hence, by rigidity, $\gamma = \tau^i \cdot \sigma^{-1} = \tau^i \cdot \sigma$.

What happened to other reflections?

Geometrically we can construct $n$ other reflections.

![Diagram of reflections](image-url)
So $\sigma_i(1) = \tau^i \cdot \sigma(1)$ and $\sigma_i(2) = \tau^i \cdot \sigma(2)$; hence by rigidity $\sigma_i = \tau^i \cdot \sigma$.

$\text{Aut}(\mathbb{Z}^2)$ is called the dihedral group $D_{2n}$. So we just showed that $D_{2n}$ has $n$ rotations (including identity) and $n$ reflections.

What is the order of $\tau$? $\text{ord}(\tau) = n$.

What is the order of $\sigma$ (and $\tau^i \cdot \sigma$)? Since these are reflections, $\text{ord}(\tau^i \cdot \sigma) = 2$. In particular, $\tau \cdot \sigma \cdot \tau \cdot \sigma = \text{id}$. And so $\sigma \cdot \tau \cdot \sigma^{-1} = \tau^{-1}$.

What is the order of $\tau^i$? Recall that $\text{ord}(\tau^i) = \frac{\text{ord}(\tau)}{\gcd(i,n)}$, and so $\text{ord}(\tau^i) = \frac{n}{\gcd(i,n)}$.

Symmetries of a metric space $(X,d)$.

$f: X \to X$ is a symmetry if it is a bijection and $d(x_1,x_2) = d(f(x_1),f(x_2))$ (it preserves distance).
Such a map is called an isometry.

Group of isometries of the Euclidean plane. To understand this group we follow a method similar to the case of dihedral group.

Lots of elements. Rotations, reflections, and translations.

Rigidity. If an isometry fixes three points \(A, B, C\) that are not co-linear, then it is identity.

(A point \(D\) in a plane is uniquely determined by \(1AD1, 1BD1,\) and \(1CD1\).) [GPS works based on a similar observation.]

Suppose \(Y \in \text{Isom}(E)\). So \(\exists\) a translation \(T\) s.t.

\[ T^{-1} \cdot Y(0,0) = (0,0). \]

Then \(\exists\) a rotation \(R\) centered at \((0,0)\) s.t.

\[ R^{-1} \cdot T^{-1} \cdot Y(1,0) = (1,0). \]

Hence either \(R^{-1} \cdot T^{-1} \cdot Y(0,1) = (0,1)\)

or \(R^{-1} \cdot T^{-1} \cdot Y(0,1) = (0,-1).\)

Therefore again by rigidity we deduce
Lecture 01: Group action

Wednesday, September 26, 2018  11:36 PM

\[ \text{Isom}(E) = \xi T \circ R \mid T \text{ is a translation } \] 
\[ R \text{ is a rotation about } (0,0) \] 
\[ U \xi T \circ R \circ L \mid T \text{ is a translation } \] 
\[ R \text{ is a rotation about } (0,0) \] 
\[ L(x, y) = (x, -y) \text{ the reflection about the } x \text{-axis} \]

Identifying \( E \) with \( \mathbb{R}^2 \) and using linear algebra, we get

\[ \text{Isom}(E) = \xi f : \mathbb{R}^2 \rightarrow \mathbb{R}^2 \mid f(v) = K v + b \] 
\[ K \text{ orthogonal } 2 \times 2 \text{ matrix} \]
\[ \text{be } \mathbb{R}^2 \]

Next we start with an abstract group \( G \) and an object \( X \) and try to view \( G \) as possible symmetries of \( X \).

**Def.** Let \( G \) be a group, and \( X \) be a non-empty set.

A (left) action of \( G \) on \( X \) is \( m : G \times X \rightarrow X \), \( m(g, x) = g \cdot x \)

which has the following properties:

1. \( \forall x \in X, e \cdot x = x \) where \( e \) is the neutral element of \( G \).
2. \( \forall x \in X, \forall g_1, g_2 \in G, g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x \).

We say \( G \) acts on \( X \), and write \( G \curvearrowright X \).
Suppose $X$ is an object; think about a set, a graph, Euclidean plane, a vector space, a group, a ring, etc. Then

$$\text{Symm}(X) \to X.$$ 

Let’s try to guess what the action is. Recall that

$$\text{Symm}(X) := \{ f : X \to X \mid \begin{array}{l} (1) \text{ } f \text{ is a bijection} \\ (2) \text{ } f \text{ and } f^{-1} \text{ preserve structure of } X \end{array} \}. $$

We need to define $m : \text{Symm}(X) \times X \to X$.

$(f, x) \mapsto ?$

The group action should tell us what the group element $f$ does to the point $x$. As soon as we phrase the question in this way, we automatically answer $f(x)$. So let

$m : \text{Symm}(X) \times X \to X$, $m(f, x) := f(x)$.

Why is it a group action?

$m(id, x) = id.(x) = x$ ✓

$f_1 \cdot (f_2 \cdot x) = f_1(f_2(x)) = (f_1 \circ f_2)(x) = (f_1 \circ f_2)\cdot x$ ✓.
The above example immediately gives us a lot of interesting examples:

\[ S_n \triangleleft \mathbb{S}_{1,2,\ldots,n} \quad (\sigma, i) \mapsto \sigma(i) \]

(Vector space \( \mathbb{R}^n \)) \[ \text{GL}_n(\mathbb{R}) \triangleleft \mathbb{R}^n, \quad (A, v) \mapsto Av \]

\( \text{nn invertible, real matrices} \)

(A group \( G \)) A “symmetry” of a group is called an automorphism.

\[ \text{Aut}(G) = \{ \phi : G \to G \mid (1) \phi \text{ is a bijection} \quad \phi \text{ is a bijection} \] \[ (2) \phi, \phi^{-1} \text{ preserve structure of } G \}

To understand (2), let’s recall what a group homomorphism is.

Def. Suppose \( H_1 \) and \( H_2 \) are two groups; then \( f : H_1 \to H_2 \) is called a group homomorphism if

(a) \( f(e_{H_1}) = e_{H_2} \)

(b) \( f(hh') = f(h)f(h') \quad \forall h, h' \in H \)

(c) \( f(h^{-1}) = f(h)^{-1} \quad \forall h \in H \)

Let \( \text{Hom}(H_1, H_2) := \{ f : H_1 \to H_2 \mid f \text{ is a group hom.} \} \)
Exercise (b) implies (a) and (c).

Exercise If \(\phi \in \text{Hom}(H_1, H_2)\) is bijective, then \(\phi^{-1} \in \text{Hom}(H_2, H_1)\).

So \(\text{Aut}(G) = \{ \phi : G \to G \mid \phi \text{ is a bijection and} \}
\forall g, g' \in G, \phi(gg') = \phi(g)\phi(g')\)
and \(\text{Aut}(G) \subseteq G, (\phi, g) \mapsto \phi(g)\).

Next we would like to parametrize all the possible

group actions of a group \(G\) on a set \(X\) (the same
can be done for any object). This means to find out

what functions \(m : G \times X \to X\) give us a group action.

One can think of such a function as a family of functions
from \(X\) to \(X\) that is indexed over \(G\):

\[
m : G \times X \to X \quad \mapsto \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xi \quad \xis a bijection.
Next we show

**Theorem.** Let $G$ be a group and $X$ be a non-empty set.

Let $\text{act}(G, X) := \{ m : G \times X \to X \mid \text{a left group action} \}$.

Then $\Phi : \text{act}(G, X) \to \text{Hom}(G, S_X)$,

$$((\Phi(m))(g))(x) := m(g, x)$$

and $\Psi : \text{Hom}(G, S_X) \to \text{act}(G, X)$,

$$\Psi(f)(g, x) := (f(g))(x)$$

are well-defined and inverse of each other.

---

**Proof.**

1. \[ ((\Phi(m))(g_1 g_2))(x) = (g_1 g_2) \cdot x \]
   \[ = g_1 \cdot (g_2 \cdot x) \]
   \[ = (\Phi(m))(g_1)(g_2 \cdot x) \]
   \[ = (\Phi(m))(g_1) \circ (\Phi(m))(g_2))(x) \]

And so $((\Phi(m))(g_1 g_2) = (\Phi(m))(g_1) \circ (\Phi(m))(g_2)$.

2. \[ (\Phi(m))(e)(x) = e \cdot x = x \]

And so $(\Phi(m))(e) = \text{id}_X$.

3. Step 1 and 2 imply $\Phi(m)(g^{-1}) \circ \Phi(m)(g) = \text{id}_X$. 
and so \((\Phi(m))(g) \in S_x\) for any \(g \in G\). Therefore, by Step 1, \(\Phi(m) \in \text{Hom}(G, S_x)\).

Step 4. \(g \cdot x := (\Phi(g))(x)\) for \(g \in \text{Hom}(G, S_x)\).

Then \(\Phi(e) = \text{id}_X\); and so \(e \cdot x = (\Phi(e))(x) = x\).

\((g_1g_2) \cdot x = \Phi(g_1g_2)(x) = \Phi(g_1) \cdot \Phi(g_2)(x) = \Phi(g_1) (\Phi(g_2)(x)) = g_1 \cdot (g_2 \cdot x)\).

Hence \(\Phi\) is well-defined.

Step 5. \([\Phi \circ \Phi](m)\) \((g, x)\)

\[= \Phi(\Phi(m))(g, x) = \Phi(\Phi(m))(g) \cdot (x) = m(g, x)\]

Thus \(\Phi \circ \Phi = \text{id}\).

Step 6. \(\Phi((\Phi \circ \Phi))(g))(x) = \Phi(\Phi(\Phi(g)))(x) = \Phi(\Phi(g, x)) = \Phi(\Phi(g))(x)\); and so \(\Phi \circ \Phi = \text{id}\).
Ex. (The left translation action) $G \rightarrow G$ by the left translation; that means $g \cdot x := gx$.

By the previous theorem this action corresponds to a group homomorphism $f: G \rightarrow S_G$, $(f(g))(x) := gx$. Cayley’s theorem that $f$ is injective and so any group can be embedded into a symmetric group.

**Theorem (Cayley)** A group $G$ can be embedded into the symmetric group $S_G$.

**Proof.** By the above argument $f: G \rightarrow S_G$, $(f(g))(x) := gx$ is a group homomorphism. So it is enough to show $f$ is injective; that means $\ker f = \{e \}$.

Suppose $f(g) = \text{id}$. Then $(f(g))(e) = e$; and so $g = ge = e$.

**Proof.** (Since this is an important result, we give a self-contained argument which is the same as above.)
For all $g \in G$, let $l_g : G \to G$, $l_g(g') := gg'$.

**Step 1.**

$$(l_g \circ l_{g'}) (g) = l_g (l_{g'} (g)) = g_1 (g_2 g) = (g_1 g_2) g = l_{g_1 g_2} (g)$$

And so $l_g \circ l_{g'} = l_{g_1 g_2}$. 

**Step 2.**

$l_e (g) = eg = g$; and so $l_e = \text{id}$. 

**Step 3.** By Steps 1 and 2, $l_{g^{-1}}$ is the inverse of $l_g$; and so $l_g \in S_G$.

**Step 4.** By Steps 1 and 3, $g \mapsto l_g$ is a group hom $f : G \to S_G$.

**Step 5.**

$g \in \ker f \implies f(g) = \text{id}_G \implies (f(g))(e) = e$

$$\implies g = ge = e.$$  

Ex. (The left translation on cosets) Suppose $G$ is a group and $H$ is a subgroup. Then $G \to G/ H$ by left translations; that means $g \cdot (g' H) := gg' H$. 