

1. Lecture 1.

Group theory is all about the symmetries of *objects*. For our purposes, every *object* is a set equipped with certain *properties*. A function $f : X \rightarrow X$ is called a *symmetry* (or an *automorphism*) of X if it satisfies the following properties:

- (1) f is a bijection.
- (2) f preserves the *properties* of X .
- (3) The inverse function f^{-1} preserves the *properties* of X .

Let $\text{Symm}(X)$ denote the collection of all symmetries of X . Then:

- (1) Clearly, the identity function 1_X belongs to $\text{Symm}(X)$.
- (2) By definition, if $f \in \text{Symm}(X)$, then $f^{-1} \in \text{Symm}(X)$.
- (3) If $f, g \in \text{Symm}(X)$, then $f \circ g \in \text{Symm}(X)$.

Hence, $(\text{Symm}(X), \circ, 1_X, \bullet^{-1})$ is a group. This serves as a [meta-example](#) for constructing groups.

More generally, it is extremely useful to think of any group as the symmetry group of an object, or at least to examine to what extent a given group G can be realized as the group of symmetries of an object X .

Window to future. A *category* consists of a collection of *objects* and *arrows* between the objects. Here are some examples.

- (1) **Set.** Objects are sets and arrows are functions.
- (2) **Group.** Objects are groups and arrows are group homomorphisms.
- (3) **F -vec.** Objects are F -vector spaces, and arrows are F -linear maps.
- (4) **Ring.** Objects are rings and arrows are ring homomorphisms.
- (5) **Top.** Objects are topological spaces and arrows are continuous maps.
- (6) **Met.** Objects are metric spaces and arrows are contractions:

$$f : X \rightarrow Y \quad \text{such that} \quad d_Y(f(x_1), f(x_2)) \leq d_X(x_1, x_2).$$

Symmetric group. Let us investigate the category of sets. Considering a set X does not have any *extra property*, its group of symmetries is

$$S_X := \{\sigma : X \rightarrow X \mid \sigma \text{ is a bijection}\}.$$

The group $(S_X, \circ)$ is called the *symmetric group* of X . The symmetric group of $\{1, \dots, n\}$ is denoted by S_n . Note that the cardinality of S_n is $n!$. Recall that the cardinality of a group G is called its *order*.

Question. How much does the group S_X depend on the set X ?

To answer this question, we start by specifying when we consider two objects to be the same: we say $X \simeq Y$ if there exist arrows $f : X \rightarrow Y$ and $g : Y \rightarrow X$ such that $f \circ g = 1_Y$ and $g \circ f = 1_X$.

For two sets X and Y , this simply means that there exists a bijection $f : X \rightarrow Y$. Let us recall what this means for two groups G and H . Recall that a function $f : G \rightarrow H$ is called a group homomorphism if $f(xy) = f(x)f(y)$ for all $x, y \in G$. Recall that if $f : G \rightarrow H$ is a group homomorphism, $f(1_G) = 1_H$ and $f(x^{-1}) = f(x)^{-1}$. Hence, every group homomorphism preserves all the properties of a group. A group homomorphism $f : G \rightarrow H$ is called an *isomorphism* if it is bijective. Note that if f is a bijective group homomorphism, then f^{-1} is also a group homomorphism. Therefore, our definition of a group isomorphism is consistent with the categorical notion of isomorphism given above.

Let us go back to the question above. Assuming that X and Y are *isomorphic sets*, we are wondering whether S_X and S_Y are *isomorphic groups*. By assumption, there exists a bijection $f : X \rightarrow Y$. We would like to assign to each element $\sigma \in S_X$ an element of S_Y . Consider the following diagram:

$$\begin{array}{ccc} X & \xrightarrow{\sigma} & X \\ \downarrow f & & \downarrow f \\ Y & \xrightarrow{?} & Y \end{array}$$

Following the arrows, we find out that the dashed arrow is given by the function $f \circ \sigma \circ f^{-1}$. This leads the following lemma.

LEMMA 1. *Suppose $f : X \rightarrow Y$ is a bijection. Then*

$$c_f : S_X \rightarrow S_Y, \quad c_f(\sigma) := f \circ \sigma \circ f^{-1}$$

is a group isomorphism.

PROOF. *Well-definedness.* Since f , σ , and f^{-1} are bijections, the function $f \circ \sigma \circ f^{-1}$ is in S_Y .

Group homomorphism. For all $\sigma_1, \sigma_2 \in S_X$, we have

$$\begin{aligned} c_f(\sigma_1) \circ c_f(\sigma_2) &= (f \circ \sigma_1 \circ f^{-1}) \circ (f \circ \sigma_2 \circ f^{-1}) \\ &= f \circ (\sigma_1 \circ \sigma_2) \circ f^{-1} = c_f(\sigma_1 \circ \sigma_2). \end{aligned}$$

Bijection. Note that $c_f \circ c_{f^{-1}} = 1_{S_Y}$ and $c_{f^{-1}} \circ c_f = 1_{S_X}$. This completes the proof. $\square$

Note that the above lemma holds in any category: if $f : X \rightarrow Y$ is an isomorphism in a category $\mathcal{C}$, then

$$c_f : \text{Symm}(X) \rightarrow \text{Symm}(Y), \quad c_f(\sigma) := f \circ \sigma \circ f^{-1}$$

is a group isomorphism. Go over the proof and see why all the steps work.

A non-trivial interesting result that you will prove later in this course is that for finite sets of cardinality at least 7 every isomorphism between S_X and S_Y is of the above form, and this is not the case if $|X| = 6$.

THEOREM 2. (1) Suppose X is a finite set and $|X| > 6$. If $\theta : S_X \rightarrow S_Y$ is group isomorphism, then there exists a bijection $f : X \rightarrow Y$ such that $\theta = c_f$.

(2) There exists an isomorphism $\theta : S_6 \rightarrow S_6$ which is not of the form c_f .

Automorphism group of a graph. Let us recall that an undirected graph X consists of a vertex set V and an edge set E , where every element of E is a non-empty subset of V of size at most 2. We often visualize a graph by representing its vertices as points and connecting two vertices v and w whenever $\{v, w\}$ is an edge. If $\{v\}$ is an edge, we draw a *loop* at the vertex v . For a graph X and two

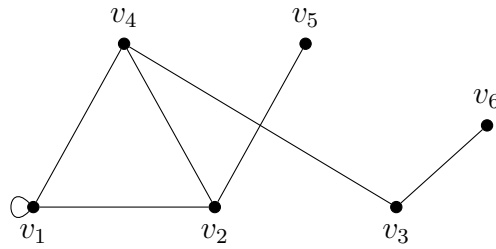


FIGURE 1. An undirected graph.

vertices v and w , we sometimes write $v \sim w$ if $\{v, w\}$ is an edge.

A symmetry of X is a bijection $f : V \rightarrow V$ such that for every $v, w \in V$

$$\{v, w\} \in E \Leftrightarrow \{f(v), f(w)\} \in E;$$

this means v and w are connected precisely when $f(v)$ and $f(w)$ are. A symmetry of a graph X is called an *automorphism* of X . The set of all automorphisms of X is denoted by $\text{Aut}(X)$. Via our meta-example we know that $\text{Aut}(X)$ is a group. Note that if f is an automorphism of X , so is f^{-1} . Hence, this definition is

consistent with the categorical version given above. In a graph X , the degree of a vertex v is the number of edges that contain v . A loop is counted twice! For instance the list of degree of vertices of the graph given in Fig.1 is

$$\deg v_1 = 4, \deg v_2 = 3, \deg v_3 = 2, \deg v_4 = 3, \deg v_5 = 1, \deg v_6 = 1.$$

Note for $f \in \text{Aut}(X)$, $\deg f(v) = \deg v$.

Let us find out what the automorphism group of the graph given in Fig.1 is. By the above remark, we know that for every $f \in \text{Aut}(X)$,

$$\begin{aligned} f(v_1) &= v_1, \\ f(v_2), f(v_4) &\in \{v_2, v_4\}, \\ f(v_3) &= v_3, \\ f(v_5), f(v_6) &\in \{v_5, v_6\}. \end{aligned}$$

This means we may put a *pin* on v_1 and v_3 . These vertices are invariant under symmetries of X . If a vertex v is fixed, then its neighbors, i.e. vertices that are connected to v , are getting permuted by a symmetry. Hence,

$$f(v_4), f(v_6) \in \{v_4, v_6\} \quad \text{as they are neighbors of } v_3.$$

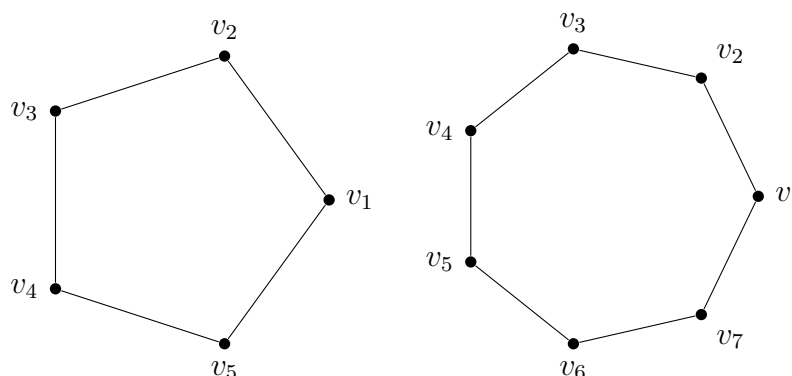
Thus $f(v_4) \in \{v_2, v_4\} \cap \{v_4, v_6\} = \{v_4\}$. Hence, v_4 is another fixed point of the group of automorphisms of X . This implies that

$$f(v_2) = v_2 \quad \text{and} \quad f(v_6) = v_6.$$

Therefore, $f(v_5) = v_5$. This means $\text{Aut}(X) = \{1_V\}$ is trivial.

In the above argument, you see the importance of finding *invariant properties*. The importance of conservation laws in physics has similar flavor: they are invariants under the symmetries of the universe.

Dihedral group. Let X_n be a cycle with n vertices.



Thinking of this graph as a regular n -gon, can you describe its symmetries? Certainly, rotations and reflections are symmetries of the graph. Are there any others? More generally, how can we systematically describe and encode all symmetries of a mathematical object? How can we turn our geometric intuition into precise mathematical arguments? Often the language of algebra is the most convenient for presenting our arguments. How can we capture the n -cycle using an algebraic object? As the name suggests, a cyclic group of order n might be useful. We label the vertices of the n -cycle by elements of $\mathbb{Z}/n\mathbb{Z}$. Note that i is connected to j if and only if $i - j = \pm 1$.

Interlude. Cayley graph. Suppose G is a group and $S \subseteq G$. We say that S is a generating set of G if the smallest subgroup of G containing S is G . Equivalently, S is a generating set of G if every element of G can be written as a product of elements of S and their inverses. We say that S is *symmetric* if $s^{-1} \in S$ for every $s \in S$. Given a symmetric generating set S of a group G , we may construct a (connected) graph $\text{Cay}(G; S)$, called the *Cayley graph* of G with respect to S . The vertex set of $\text{Cay}(G; S)$ is G , and two elements g_1 and g_2 are connected if and only if $g_2 = sg_1$ for some $s \in S$. Note that $g_2 = sg_1$ implies $g_1 = s^{-1}g_2$ and $s^{-1} \in S$, the relation is symmetric.

Note that $S = \{\pm 1\}$ is a symmetric generating set of $\mathbb{Z}/n\mathbb{Z}$, and the associated Cayley graph is an n -cycle.

With this labeling, a *rotation* is given by the function

$$\sigma : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}, \quad \sigma(i) := i + 1,$$

and a *reflection* is given by

$$\tau : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}, \quad \tau(i) := -i.$$

Considering $\text{Aut}(X_n)$ is a group, we have

$$\langle \sigma, \tau \rangle \subseteq \text{Aut}(X_n).$$

In particular, $\sigma^i \tau^j \in \text{Aut}(X_n)$ for all integers i and j . Note that

$$\sigma^i(x) = x + i \quad \text{and} \quad \tau^j(x) = (-1)^j x.$$

Hence, the order $\text{ord}(\sigma)$ is n and the order $\text{ord}(\tau)$ is 2.

(Recall. Order of an element $g \in G$ is the smallest positive integer n such that $g^n = 1$. Here are two of the main properties of order:

$$g^n = g^m \quad \text{if and only if} \quad m \equiv n \pmod{\text{ord}(g)},$$

$$\text{ord}(g^n) = \frac{\text{ord}(g)}{\gcd(n, \text{ord}(g))}.)$$

Therefore,

$$\{\text{id}, \sigma, \dots, \sigma^{n-1}\} \cup \{\tau, \sigma\tau, \dots, \sigma^{n-1}\tau\} \subseteq \langle \sigma, \tau \rangle \subseteq \text{Aut}(X_n).$$

For $\phi \in \text{Aut}(X_n)$, suppose $\phi(0) = j$. Then $\phi(0) = \sigma^j(0)$. Therefore, $\sigma^{-j} \circ \phi$ is an automorphism of X_n which sends 0 to 0. Since the only neighbors of 0 are 1 and -1 . We deduce that $\sigma^{-j} \circ \phi(1)$ is either 1 or -1 . Note that $\tau(0) = 0$ and $\tau(-1) = 1$. Thus, either

$$(1) \quad \sigma^{-j} \circ \phi(0) = 0 \quad \text{and} \quad \sigma^{-j} \circ \phi(1) = 1,$$

or

$$(2) \quad \tau \circ \sigma^{-j} \circ \phi(0) = 0 \quad \text{and} \quad \tau \circ \sigma^{-j} \circ \phi(1) = 1.$$

The next *rigidity* result completes our understanding of $\text{Aut}(X_n)$.

LEMMA 3. *If $\theta \in \text{Aut}(X_n)$, $\theta(0) = 0$, and $\theta(1) = 1$, then $\theta = \text{id}$.*

PROOF. It is easy to show $\theta(k) = k$ using strong induction on k . □

By Lemma 3, (1), and (2), we obtain that either

$$\sigma^{-j} \circ \phi = \text{id}$$

or

$$\tau \circ \sigma^{-j} \circ \phi = \text{id}.$$

The former implies $\phi = \sigma^j$, and the latter implies $\phi = \sigma^j \circ \tau$. Hence

$$\text{Aut}(X_n) = \langle \sigma, \tau \rangle = \{\text{id}, \sigma, \dots, \sigma^{n-1}\} \cup \{\tau, \sigma\tau, \dots, \sigma^{n-1}\tau\}.$$

To get a complete understanding of the group $\text{Aut}(X_n)$, we must compute $(\sigma^j \circ \tau) \circ \sigma^i$ and $(\sigma^j \circ \tau) \circ (\sigma^i \circ \tau)$. Note that

$$\tau(\sigma(\tau^{-1}(x))) = \tau(\sigma(-x)) = \tau(-x + 1) = x - 1 = \sigma^{-1}(x).$$

Hence, $\tau\sigma\tau^{-1} = \sigma^{-1}$.

Interlude. Inner automorphism. For every $g, x \in G$, we say gxg^{-1} is the conjugate of x by g .

LEMMA 4. For every group G and $g \in G$, the map

$$c_g : G \rightarrow G, \quad c_g(x) := gxg^{-1}$$

is a group automorphism.

PROOF. The argument is quite similar to the proof of Lemma 1: *Group homomorphism*.

$$c_g(x_1)c_g(x_2) = (gx_1g^{-1})(gx_2g^{-1}) = g(x_1x_2)g^{-1} = c_g(x_1x_2).$$

Bijection. One can easily check that

$$c_g \circ c_{g^{-1}} = c_{g^{-1}} \circ c_g = 1_G,$$

so c_g is a bijection. This completes the proof. $\square$

An automorphism of G is called an *inner automorphism* if it is of the form c_g for some g . The set of all inner automorphisms is denoted by $\text{Inn}(G)$.

Note that if G is an abelian group, then every inner automorphism is trivial. For instance, $\text{Inn}(\mathbb{Z}^2) = \{1\}$, but $\text{Aut}(\mathbb{Z}^2) \simeq \text{GL}_2(\mathbb{Z})$.

In your second week HW assignment, you will show that $\text{Inn}(G)$ is a normal subgroup of $\text{Aut}(G)$ and investigate some of its properties.

Going back to computations in the group $\text{Aut}(X_n)$, observe that $c_\tau(\sigma) = \sigma^{-1}$. Hence, for every integer k ,

$$c_\tau(\sigma^k) = c_\tau(\sigma)^k = \sigma^{-k}.$$

Therefore,

$$\tau\sigma^k\tau = \sigma^{-k}$$

for all $k \in \mathbb{Z}$. Thus

$$\begin{aligned}(\sigma^i \tau)(\sigma^j \tau) &= \sigma^i(\tau \sigma^j \tau) = \sigma^i \sigma^{-j} = \sigma^{i-j} \\ (\sigma^i \tau) \sigma^j &= \tau(\tau \sigma^i \tau) \sigma^j = \tau \sigma^{-i} \sigma^j = \tau \sigma^{-i+j}.\end{aligned}$$

Now, we know the full multiplication table of the finite group $\text{Aut}(X_n)$. This finite group is called a *dihedral group* and is denoted by D_{2n} .

Window to future. Group presentation Note that the above computations were carried out using only the following relations:

$$\sigma^n = \tau^2 = 1 \quad \text{and} \quad \tau \sigma \tau^{-1} = \sigma^{-1}.$$

Later in the course, we will discuss *group presentations* where a group is defined by a generating set together with relations that they are required to satisfy. Then we will show that

$$\langle a, b \mid a^n = 1, b^2 = 1, bab^{-1} = a^{-1} \rangle.$$

is a presentation of the dihedral group D_{2n} .