Group theory

Jacob Zhang, Shend Zhjeqi

The idea of the three lecture series on group theory that we are going to cover is to gain an intuitive understanding of group theory.

1 Examples

Definition 1. Let M be a set. A binary operation on M is an assignment of an element of M to each ordered pair of elements of M.

Examples of binary operations include addition on the set of natural numbers or integers, and subtraction on the set of integers. Subtraction is not a binary operation on the set of natural numbers because, for example, the ordered pair (3; 5) does not correspond to a natural number. 1. Consider the operations: (a) addition of numbers; (b) subtraction of numbers, and (c) multiplication of numbers. For which of the following subsets of the set of integers are they binary operations? (1) The set of all even integers; (2) the set of all odd integers; (3) the set of all negative integers, and (4) the set of all positive integers

Any transformation of a figure to itself, preserving the distances between all of its points, is called a symmetry of that figure. In example 1, the rotations of the equilateral triangle are its symmetries.

Example 1: Find all symmetries of an equilateral triangle (Complete the multiplication table.)

Example 3: Construct the multiplication table for a square.

2 Groups of transformations

Definition: Let M be a set. A bijective map from the set M to itself, $g : M \to M$, is called a transformation of the set M.

Definition 4. Let G be a non-empty set of transformations of a set M having the following properties: (1) if transformations g_1 and g_2 are in G, then their composition $g_3 = g_1 g_2$ is in G; (2) if transformation g is in G, then the inverse transformation g is in G. Such a set of transformations G will be called a group of transformations.

Exercise: Prove that every group of transformations contains an identity transformation e, such that $e(A) = A$ for every element A of the set M.

Exercise: Prove that $eg = ge = g$ for every transformation g.

Exercise: Prove that for any three transformations g_1, g_2, and g_3, the following equality holds: $g_1(g_2 g_3) = (g_1 g_2)g_3$.

Example: Symmetries of a regular n-gon.

3 Groups

Definition 5: A group is a set G of elements of arbitrary nature, together with a binary operation $a \cdot b$ defined on G, such that the following conditions hold:

(1) the operation is associative, that is, $(ab)c = a(bc)$ for every a, b, and c in G;

(2) there exists an element e in G, such that $ea = ae = a$ for every element a in G; this element e is called the identity element of the group G;

(3) for each element a in G, there exists an element a^{-1} in G such that $aa^{-1} = a^{-1}a = e$; this element is called the inverse of a.

Exercise: Do the following sets form groups under multiplication?
(a) All real numbers, and
(b) all non-zero real numbers?

Exercise Do the positive real numbers form a group under multiplication?

Exercise Do the natural numbers $(0, 1, 2, ...)$ form a group: (a) under addition, (b) under multiplication?

Exercise Prove that in any group, there is a unique identity element.

Exercise Prove that for any element a in a group, there is a unique inverse of a.

Exercise Prove that (a) $e^{-1} = e$; (b) for any element a in a group, $(a^{-1})^{-1} = a$.

Definition 6 Two elements a and b of a group are said to commute if $ab = ba$. If all elements of a group commute with each other, then the group is called commutative or abelian.

Exercise Let a and b be any elements of a group G. Prove that the equations $ax = b$ and $ya = b$ each have a unique solution in G.

Exercise Let $a \cdot a = e$ for every element a in a group G. Prove that the group G is commutative.

Exercise: $a^m \cdot a^n = a^{m+n}$, $(a^m)^n = a^{mn}$, $(a^{-1})^m = (a^m)^{-1}$

Section 4: CYCLIC GROUPS

Definition 7 Let a be an element of a group G. The smallest positive integer n such that an = e is called the order of the element a. If such an n does not exist, then we say that a is an element of infinite order.

Definition 8 If an element a has order n and all the elements of a group G are equal to one of $e, a, a^2, \cdots, a^{n-1}$, then the group G is called a cyclic group of order n, generated by a, and the element a is called a generator of the group.

Section 5: ISOMORPHISMS

Definition 10 Suppose we are given two groups G_1 and G_2, and suppose there exists a bijective map φ from the elements of the group G_1 to the elements of the group G_2 (see section 2), such that multiplication in G_1 corresponds to multiplication in G_2, i.e., if $\varphi(a) = a_0, \varphi(b) = b_0, \varphi(c) = c_0$ and $ab = c$ in the group G_1, then in the group G_2, $a_0b_0 = c_0$. Then φ is called an isomorphism from the group G_1 to the group G_2, and groups between which we can define an isomorphism are called isomorphic. The condition that the bijective map φ is an isomorphism can be written the following way: $\varphi(ab) = \varphi(a) \cdot \varphi(b)$ for any elements a and b of

the group G_1; here the multiplication ab is performed in G_1 and the multiplication $\varphi(a) \cdot \varphi(b)$ is performed in G_2.

Exercise Prove that any infinite cyclic group is isomorphic to the group of integers under addition.

Exercise Let $\varphi : G \to F$ be an isomorphism. Prove that $\varphi(e_G) = e_F$, where e_G and e_F are the identity elements of G and F, respectively.

Zen: Under isomorphism, the way objects interact between each other is completely preserved.

Exercise Show that inverses are sent to inverses, and the order of an element is preserved.

Exercise(HW) Find, up to isomorphism, all groups that have: (a) 2 elements, (b) 3 elements. Give an example of two groups that have the same number of elements and are non-isomorphic.

Now, let a be an arbitrary element of the group G. Consider the map $\varphi(a)$ from the set of elements of the group G to itself, defined by $\varphi_a(x) = ax$ for any element x in G. Prove that $\varphi(a)$ is a transformation of the set of elements of the group G (i.e., it is a bijective map from the set of elements of G to itself). We show that $\{\varphi_a | \, a \in G\}$ form a group. Moreover, G is isomorphic to this group.

Section 6: SUBGROUPS

Definition: Let G be a group under $*$. Then a subgroup H is so that $H \subseteq G$ and it is a group under $*$.

Exercise Prove that the intersection of any number of subgroups of a group G is also a subgroup of the group G.

HOMEWORK

Exercise(HW) Find the orders of all elements in the groups of symmetries of an equilateral triangle, square and rhombus. Show that the rotations of a regular n-gon form a cyclic group. Suppose the element a has order n. Prove that $a^m = e$ if and only if $m = nd$, where d is an arbitrary integer. Suppose that a has prime order p and let m be an arbitrary integer. Prove that either $a^m = e$ or a^m has order p. Let $d = \gcd(m, n)$, and suppose that a has order n. Prove that a^m has order $n = d$. Let a be an element of infinite order. Prove that the elements $\cdots, a^{-2}, a^{-1}, a^0 = e, a, a^2, \cdots$ are all distinct.

Exercise:(HW) Determine whether the following groups are commutative
(a) the group of rotations of a triangle;
(b) the group of rotations of a square;
(c) the group of symmetries of a square;
(d) the group of symmetries of a rhombus, and
(e) the group of symmetries of a rectangle.

Exercise (HW) Show that the collection of the isomorphisms from G to G is a group in itself with the operation of composition.

Exercise(HW) Prove that the group of all real numbers under addition is isomorphic to the group of all positive real numbers under multiplication.

Exercise: (HW) Recall, in class we mentioned what are all the symmetries of an equilateral triangle but never showed that those are the only ones. So, your task is to show that what was claimed in lecture is true, and moreover, classify all the symmetries of the regular n-gon (bijective maps of the regular n-gon that preserve distance between any two points).