Lecture 2: Groups

Rajat Mittal ⋆

IIT Kanpur

These notes are about the first abstract mathematical structure we are going to study, *groups*. You are already familiar with *set*, which is just a collection of objects. Most of the sets we encounter in mathematics are useful because of the operations we can perform on them. We can do addition, multiplication, AND, OR, take power etc..

Sets, by definition, need not have such operations. For example, $S = \{Apple, Oranges, CS203, Monitor\}$ is a set. But, if we look at more interesting sets like integers, matrices, permutations etc., we generally have operations which can be done on them. For example, you can add matrices, multiply permutations, add and multiply integers and so on.

Our next task is to define an abstract object (say a special set) with operation to compose elements inside the object. But first lets ask a basic question. What are the nice properties of addition of two natural numbers? What about integers?

To begin with, it is great that we can add two numbers, that is, the addition of any two numbers is a number. Another property not present in natural numbers is that we can always solve $a + x = b$ (a, b are given, x is unknown). Notice that we have to assume the existence of *Zero*.

Exercise 1. Can you think about other properties? Do they follow from the properties mentioned above?

1 Groups

A group G is a set with binary operation $*$, s.t.,

1. Closure: For any two elements $a, b \in G$; their composition under the binary operation $a * b \in G$.
2. Associativity: For all $a, b, c \in G$, we have $a * (b * c) = (a * b) * c$. This property basically means that any bracketing of $a_1 * a_2 * \cdots * a_k$ is same (exercise).
3. Identity: There is an element *identity* (e) in G, s.t., $a * e = e * a = a$ for all $a \in G$.
4. Inverse: For all $a \in G$, there exist $a^{-1} \in G$, s.t., $a * a^{-1} = a^{-1} * a = e$.

Note 1. Some texts define binary operation as something which has *closure* property. In that case, the first property is redundant. For the sake of brevity, it is sometimes easier to write xy instead of $x * y$.

Sometime we denote a group by its set and the operation, e.g., $(\mathbb{Z}, +)$ is the group of integers under addition.

Exercise 2. Show that integers form a group under addition (In other words, Integers have a group structure with respect to addition). Do they form a group under multiplication?

You can think of groups as being inspired by integers. In other words, we wanted to abstract out some of the fundamental properties of integers. We will later see that all groups share some properties with integers, but more interestingly, there are a lot of other groups which do not look like integers. That means there are some properties of integers which are not captured by the definition of groups. So what properties of integers do you think is not captured by groups?

To start with, we haven't specified *commutativity* as one of the basic properties. The properties are chosen so that we have many examples of groups and simultaneously we can prove a lot of theorems (properties) of this group structure. Later we will see that some important groups do not have commutativity property.

Definition 1. *A group is called* commutative *or* abelian *if,* $\forall a, b \in G; a * b = b * a$.

⋆ Thanks to the book from Dummit and Foote

1.1 Examples of groups

Exercise 3. Can you think of any other group except integers under addition? Is it commutative?

The whole exercise of abstraction will be a waste if integers (addition) is the only set which follow group property. Indeed, there are many examples of groups around you, or at least in the mathematics books around you.

- Integers, Rationals, Reals, Complex numbers under addition. Clearly for all these 0 is the identity element. The inverse of an element is the negative of that element.
- Rationals, Reals, Complex numbers (without zero) under multiplication. Identity for these groups is the element 1. Why did we exclude integers?
- Positive rationals, positive reals under multiplication.
- The group $\mathbb{Z}_n$, set of all remainders modulo n under addition modulo n. Will it be a group under multiplication? How can you make it a group under multiplication?

Till now all the examples taken are from numbers. They are all subsets of complex numbers. Lets look at a few diverse ones.

- The symmetries of a regular polygon under composition. In other words, the operations which keep the polygon fixed. The symmetries are either obtained through rotation or reflection or combination of both. This group is called *Dihedral group*.
- The set of all permutations of $\{1, 2, \cdots, n\}$ under composition. What is the inverse element?
- The set of all $n \times n$ matrices under addition. The identity in this case is the all 0 matrix,

$$\begin{pmatrix} 0 \cdots 0 \\ \vdots \ddots \vdots \\ 0 \cdots 0 \end{pmatrix}$$

- The set of all $n \times n$ invertible matrices of real numbers. What is the identity element?

We have seen so many examples of groups. Are they all *similar* (we will define the word *similar* later). Can we represent a group in a succinct way. One of the trivial representation is the *multiplication table* of the group. It is a matrix with rows and columns both indexed by group elements. The $(i, j)^{th}$ entry denotes the sum of i^{th} and j^{th} group element. For example, lets look at the multiplication table of $\mathbb{Z}_5^+$ under multiplication. Here $\mathbb{Z}_5^+$ denotes all the remainders modulo 5 Co-prime to 5 (gcd with 5 is 1).

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Exercise 4. Notice that every element occurs exactly once in every row and every column. Do you think this property is true for any group or just $\mathbb{Z}_5$?

Multiplication table gives us all the information about the group but is a pretty long description. Specifically it is quadratic in the size of the group. It turns out that groups have lot of properties which can help us in giving a more succinct representation. We already showed one property, that the identity is unique. What other theorems can be shown for groups?

2 Properties of groups

To start with, we need to define few quantities. Suppose we are given an element $x \neq e$ of group G. What other elements can be constructed with x. The composition with identity will not give anything new, so lets compose it with itself. Since G is a group, $x^2 := x * x, x^3 := x^2 * x$ (notice the new notation) and so on will be elements of group G. In this way we can create new elements in G except if these elements start repeating.

Suppose G is finite, then sooner or later there will exist i and j, s.t., $x^i = x^j$.

Exercise 5. Show that the first element which will repeat is e.

The least positive j for which $x^j = e$ is called the *order* of x and is denoted by $|x|$. Clearly the only element with order 1 is e and everything else will have a bigger order.

We will now go on to prove more properties of groups, but before that there is a warning. Groups are inspired by numbers and the notations are very similar. It is not surprising that sometimes you can get carried away and use properties of integers which are not really true for groups (e.g., commutativity).

For all the proofs for the theorems given below, notice that we will use the already known properties like closure, associativity, inverse, existence of identity. Then using those theorems we can prove other results. Now check your proofs for the exercises given in this section above.

This distinction can be made more clear by an analogy which we will use later too. Working with groups is like playing *football*. In general, for any activity you use your hands, feet or any other tool. But in case of football there is a restriction that you only use your feet. Using your feet you develop other skills which can be used to score a goal.

Our goal would be to prove theorems. Our feet will be the defining properties of groups (closure, associativity, inverse, identity). And the intermediate theorems would be like dribbling or kicking. You should not foul (use properties of integers) to prove a theorem (score a goal). So lets play football. We will use G to denote a group.

- The inverse of an element is unique.
  Proof: Suppose a has two inverses b and c. Then $c = (ba)c = b(ac) = b$. What properties of groups did we use in this proof.
- Cancellation laws: Given $a, b, x \in G$, we know $ax = bx \Rightarrow a = b$, and also $xa = xb \Rightarrow a = b$. These are called respectively the right and the left cancellation law.

  Exercise 6. Prove the assertion. What does it say about the rows (or columns) of multiplication table?

- $x \in G$ and x^{-1} have the same order.
  Proof: We will show that order of x^{-1} is at most the order of x, by symmetry this will prove the assertion. Suppose $x^n = e$. Multiply this equality by x^{-n} and we get $x^{-n} = e$ and hence the order of x^{-1} is less than n.

  Exercise 7. We did not define x^{-n}. What do you think it should be?

For a finite group we have shown that its order is less than the cardinality (also called the order) of the group. Actually order of an element can be restricted to just the divisors of the order of the group. Look carefully at the following theorem and proof.

Theorem 1. *Suppose G is a finite group with n elements (n is the order of the group). If d is the order of an element $x \in G$ then n is a multiple of d ($d \mid n$).*

Proof. We will prove the theorem in two steps. First, we will show that $x^n = e \ \ \forall x \in G$. Second, if there is any m, s.t., $x^m = e$ then d divides m. From these two steps the conclusion can be easily inferred.

From the cancellation laws, it is clear that $S_x = \{xg : g \in G\} = G$ as a set. All elements of S_x are distinct, in G and hence they are just a permutation of elements of G. Taking the product over all elements of S_x,

$$\Pi_{s \in S_x} s = \Pi_{g \in G} xg = x^n \Pi_{g \in G} g = x^n \Pi_{s \in S_x} s.$$

Using the first and the last step,

$$e = x^n.$$

So for every element $x \in G$, we know $x^n = e$.

For the second part, suppose $m = kd + r$ by division. Here k is the quotient and $r < d$ is the remainder. Then looking at x^m,

$$e = x^m = x^{kd+r} = x^r.$$

So there exist $r < n$, s.t. $x^r = e$. By the definition of order, $r = 0$. Hence d divides m.

Actually the proof given above is not correct.

Exercise 8. Where is the mistake in the proof? Hint: It is in the first part.

□

If you look at the proof of fact that $x^n = e$, then it was proved using commutativity. So we have only proved that for a *commutative* or *abelian* group the thm. **??** is true. It turns out that it is true for non-commutative groups too. We will prove the full generalization later with a different technique.

3 Isomorphism and homomorphism of a group

As discusses above we want to find out what kind of groups are there. Are they all *similar*. Let us formalize the notion of similarity now. Clearly if two sets are equal if and only if there is a bijection between them. But the bijection need not respect the composition. That means the composition properties of two groups might be completely different even if they have a bijection between them.

Exercise 9. Would you say that groups $(\mathbb{Z}_4, +)$ and $(\mathbb{Z}_8^+, \times)$ similar (both have four elements). The second group is the set of all remainders modulo 8 which are Co-prime to 8.

Hint: Look at the orders of different elements in these groups.

Hence for group similarity, we need to take care of composition too. Two groups are considered same if they are *isomorphic* to each other. In other words there exist an *isomorphism* between the two. To define, a group G_1 is isomorphic to group G_2, if there exist a bijection $\phi : G_1 \to G_2$, s.t.,

$$\forall g, h \in G_1 : \quad \phi(g)\phi(h) = \phi(gh).$$

The second property takes care of the composition. A related notion is called *homomorphism* where we drop the bijection criteria. So G_1 is homomorphic to G_2 if there exist a *map* $\phi : G_1 \to G_2$, s.t.,

$$\forall g, h \in G_1 : \quad \phi(g)\phi(h) = \phi(gh).$$

Exercise 10. Give a homomorphism which is not an isomorphism from a group G to itself.

4 Assignment

Exercise 11. For any $a_1, a_2, \cdots, a_k \in G$, show that expression $a_1 * a_2 * \cdots * a_k$ is independent of bracketing.

Hint: Show it using induction that all expression are same as $a_1 * (a_2 * (\cdots * a_k) \cdots)$.

Exercise 12. Prove that the identity is unique for a group.

Exercise 13. Which Groups are commutative from the list of groups given in the section **??**?

Exercise 14. Prove that $G = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$ is a group under addition.

Exercise 15. Which of them are groups under addition?

– The set of all rational numbers with absolute value < 1.
– The set of all rational number with absolute value ≥ 1.
– The set of all rational numbers with denominator either 1 or 2 in the reduced form.

Exercise 16. Find the order of following,

– 3 in $\mathbb{Z}_5, +$.
– 5 in $\mathbb{Z}_7, \times$.
– Transpositions in permutations. What about product of disjoint transpositions?

Exercise 17. Give an example of a finite group where order of an element is different from order of the group.

Exercise 18. If all elements have order 2 for a group G, prove that it is abelian.

Exercise 19. Show that if G_1 is isomorphic to G_2 then G_2 is isomorphic to G_1.

Exercise 20. Show an isomorphism from real numbers with addition to positive real numbers with multiplication.