Lecture 3: Subgroups

Rajat Mittal ⋆

IIT Kanpur

We are interested in studying the properties and structure of the group. By properties, we mean the theorems which can be proven about groups in general. Then any mathematical construct having the group structure (satisfy closure, associativity etc.) will satisfy those theorems.

Another important task is to understand the structure of group itself. It is deeply related to the properties of group. It ultimately helps us in figuring out which groups are similar (with respect to isomorphism) and can we list out all possible kind of groups (not isomorphic to each other).

One of the natural question is that if groups can exist inside a group.

Exercise 1. Can we have a subset of group which itself is a group under the group operation? Try to construct such a set in $\mathbb{Z}$.

1 Definition

As the intuition would suggest,

Definition 1. *A subset H of a group G is called a subgroup if it is not empty, closed under group operation and has inverses. The notation $H \leq G$ denotes that H is a subgroup of G.*

Note 1. The subgroup has the same operation as the original group itself

Exercise 2. Why did we not consider associativity, existence of inverse?

Every group G has two trivial subgroups, e and the group G itself. Lets look at few examples of non-trivial subgroups. Try to prove that each of them is a subgroup.

- $n\mathbb{Z}$, the set of all multiples of n is a subgroup of Integers.
- Under addition, integers ($\mathbb{Z}$) are a subgroup of Rationals ($\mathbb{Q}$) which are a subgroup of Reals ($\mathbb{R}$). Reals are a subgroup of Complex numbers, $\mathbb{C}$.
- $\mathbb{Z}^+$, the set of all positive integers is not a subgroup of $\mathbb{Z}$. Why?
- The set $S = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ is a subgroup of $\mathbb{R}$ under addition.
- Center of a group: The *center* of a group G is the set of elements which commute with every element of G.

  $$C(G) = \{h \in G : \ hg = gh \ \ \forall g \in G\}.$$

  We will show that center is the subgroup. Associativity follows from G and existence of identity is clear. Suppose $h, k \in C(G)$, then for any $g \in G$,

  $$g(hk) = hgk = (hk)g.$$

  Hence $C(G)$ is closed. For the inverse, note that $gh = hg$ is equivalent to $h^{-1}gh = g$ and $g = hgh^{-1}$. Hence existence of inverse follows (Why?).

⋆ Thanks to Dummit and Foote book and the book from Norman Biggs.

1.1 Cyclic groups

We noticed that $\{e\}$ is a subgroup of every group. Lets try to construct more subgroups. Suppose x is some element which is not the identity of the group G. If k is the order of x then $S_x = \{e, x, x^2, \cdots, x^{k-1}\}$ is a set with all distinct entries. It is clear from previous discussion of groups that S_x is a subgroup.

Exercise 3. Prove that S_x is a subgroup.

While proving the previous exercise, we need to use the fact that k is finite. What happens when k is infinite? Can we construct a group then? The answer is yes, if we include the inverses too. All these kind of groups, generated from a single element, are called *cyclic groups.*

Definition 2. *A group is called* cyclic *if it can be* generated *by a single element. In other words, there exist an element $x \in G$, s.t., all elements of G come from the set,*

$$< x >= \{\cdots, x^{-2}, x^{-1}, e, x, x^2, \cdots\}$$

There are many things to note here:

- For an infinite group, we need to consider inverses explicitly. For a finite group, inverses occur in the positive powers.
- The group *generated* by the set S is the group containing all possible elements obtained from S through composition (assuming associativity, inverses etc.).
- The notation for the group generated by S is $< S >$.

The structure of cyclic groups seem very simple. You take an element and keep composing. What different kind of cyclic groups can be there? Look at different examples of cyclic groups of order 4 in figure 1.1. The next theorem shows that all these are isomorphic.

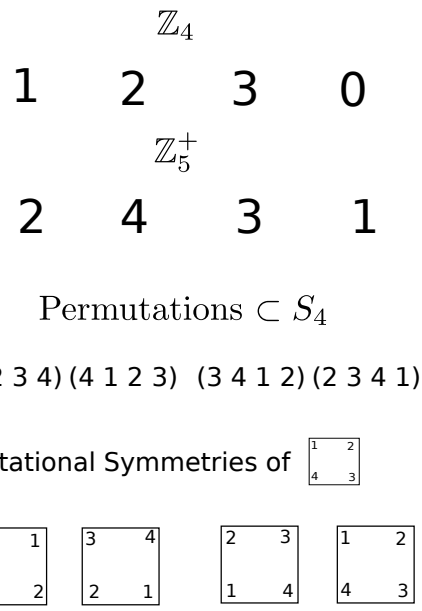

Fig. 1. Different cyclic groups

Theorem 1. *Every finite cyclic group G of order n is isomorphic to $\mathbb{Z}_n$.*

Proof. Suppose x is a generator for G. It exists by the definition of G. Then since the order is finite, group G is,

$$G = \{e, x, x^2, \cdots, x^{n-1}\}$$

Lets look at the obvious bijection ϕ from $\mathbb{Z}_n$ to G. The element k is mapped to x^k. It is a bijection because, the inverse maps x^k to k. For the above bijection,

$$\phi(j+k) = x^{j+k \mod n} = x^j * x^k = \phi(j) * \phi(k).$$

Where first inequality follows from the definition of $\mathbb{Z}_n$ and second from the fact that $x^n = 1$. This shows that ϕ is an isomorphism. Hence Proved. □

Using the previous theorem and exercise (assignment), we have given complete characterization of cyclic groups. This loosely means that we can get all the properties of any cyclic group of order n from $\mathbb{Z}_n$ and an infinite cyclic group with integers.

This is called a *classification* of cyclic groups. We would ideally like to give classification of groups and finding out more properties of groups. These two questions are not independent. We will explore both simultaneously and progress in one question helps in finding the answer for other.

Exercise 4. What are the subgroups of a cyclic group?

2 Cosets

The next step in understanding the structure of a group is to partition it using a subgroup. Suppose we are given a group G and its subgroup H. We will show that G can be partitioned into disjoint sets of equal size ($|H|$). This will imply that $|G|$ is always divisible by $|H|$. Lets define these parts first and then we can prove the fact given above.

Definition 3. *Cosets: The* left coset *(gH) of H with respect to an element g in G is the set of all elements which can be obtained by multiplying g with an element of H,*

$$gH = \{gh : \quad h \in H\}.$$

This is called the left coset because g is multiplied on the left. We can similarly define the right cosets Hg.

Exercise 5. How are left and right coset related for commutative groups?

Let us show some properties of these cosets. Remember not to use any illegal property while proving these. Without loss of generality we will assume that cosets are left. Same properties hold true for right ones too.

- Every element of G is in at least one coset. H is one of the cosets too.

  Proof. Exercise. □

- The cardinality of all cosets is equal and hence their cardinality is $|H|$.

  Proof. Consider a coset gH and a subgroup $H = \{h_1, h_2, \cdots, h_k\}$. The elements of the left coset gH are $\{gh_1, gh_2, \cdots, gh_k\}$. It is easy to show that any two elements in this set are distinct (why?). Hence all cosets have cardinality $k = |H|$. □

- For any two elements g_1, g_2 of G either g_1H, g_2H are completely distinct (disjoint) or completely same ($g_1H = g_2H$).

Proof. Suppose there is one element common in g_1H and g_2H (otherwise they are completely distinct). Say it is $g_1h_1 = g_2h_2$, then,

$$g_1 = g_2h_2h_1^{-1} \rightarrow \exists\ h \in H :\ g_1 = g_2h.$$

Now you can prove a simple exercise.

Exercise 6. If $\exists\ h \in H :\ g_1 = g_2h$ then show that $g_1H \subseteq g_2H$.

But if $g_1 = g_2h$ then $g_2 = g_1h^{-1}$. This will show from the previous exercise that $g_2H \subseteq g_1H$. Hence both the sets g_1H and g_2H are the same. □

Using the properties we have shown that the two columns of the following table are completely the same or completely distinct.

G/H	e	g_2	$\cdots$	g_n
e	e	g_2	$\cdots$	g_n
h_2	h_2	g_2h_2	$\cdots$	g_nh_2
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
h_k	h_k	g_2h_k	$\cdots$	g_nh_k

This conclusion is beautifully summarized in Lagrange's theorem.

2.1 Lagrange's theorem

Using the previous list of properties it is clear that if we look at the distinct cosets of H then they partition the group G into disjoint parts of equal size.

Exercise 7. What is the size of these parts?

Theorem 2. *Lagrange: Given a group G and a subgroup H of this group, the order of H divided the order of G.*

Proof. The proof is left as an exercise. You should try to do it without looking at the hint given in the next line.

Hint: From the previous discussion, the $\frac{|G|}{|H|}$ is just the number of distinct cosets of H. □

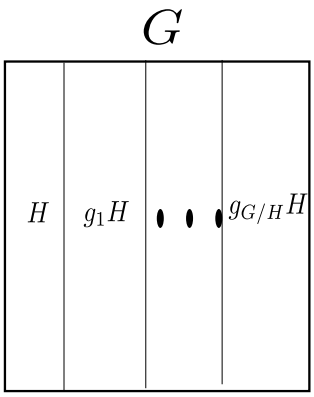

Fig. 2. Coset decomposition

Note 2. If the set of left and right cosets coincide the subgroup is called *normal*. In this case, the set of cosets actually forms a group, called the *quotient group* $\frac{G}{H}$ (What is the composition rule?).

This is a great discovery. The statement of Lagrange's theorem does not do justice to the implications. We started with an abstract structure with some basic properties like associativity, inverses etc. (group). The proof of Lagrange's theorem implies that if we can find a subgroup of the group then the whole group can be seen as a disjoint partition with all parts related to the subgroup. Notice that it is easy to construct a cyclic subgroup of a group.

Exercise 8. Prove that the order of an element always divides the order of a group. We had proved this for commutative groups in an earlier lecture.

Exercise 9. What does Lagrange's theorem say about groups with prime order?

Lets look at one application of Lagrange's theorem in the case of $\mathbb{Z}_m^\times$. We know that this group contains all the remainders mod m which are coprime (gcd is 1) to m. If m is a prime p then $\mathbb{Z}_p^\times$ contains $p-1$ elements. This proves the well known *Fermat's little theorem.*

Exercise 10. Fermat's little theorem: For a prime p and any number a,

$$a^{p-1} = 1 \mod p.$$

Prove this theorem.

3 Dihedral group

Till now most of the exercises we have done are for $\mathbb{Z}$ and $\mathbb{Z}_n$. These groups are commutative. This section will introduce you to a non-commutative subgroup.

Definition 4. *A Dihedral group D_{2n} is the group of symmetries of a regular n-gon.*

A regular n-gon can be rotated or reflected to get back the n-gon. The group D_{2n} is the group generated by reflection s and rotation r by the angle $\frac{2\pi}{n}$. Refer to figure 3 for all the symmetries of a pentagon.

For an $n-gon$ there are n rotations possible. The set of rotations form a cyclic group of order n.

Exercise 11. What is the inverse of rotation r. Convince yourself that set of rotations form a cyclic group.

On the other hand reflection is the inverse of itself. Hence it is an element of order 2. From the figure you can guess that there will be $2n$ symmetries of the form $s^i r^j$, where i ranges in $\{0,1\}$ and j is an element from $\{0,1,\cdots,n-1\}$. Using this notation, rs means we apply s first and then r.

Exercise 12. Convince yourself that $rs \neq sr$.

Notice that we have given a description of $2n$ elements of the dihedral group D_{2n}. How can we be sure that there are no more elements generated by r and s. What about $rsrs$?

Exercise 13. Show that $rs = sr^{-1}$.

This relation tell us how to interchange r and s in any expression involving both. This way we can convert any element of the group generated by r and s to be of the form $s^i r^j$ with i and j ranging appropriately.

The above discussion shows the important properties (defining properties) of dihedral group.

- An element of order 2, s.
- An element of order n, r.
- The commutation relation $rs = sr^{-1}$.
- $s \neq r^i$ for any i.

Any group which is generated by two elements with the above mentioned properties will be isomorphic to D_{2n}.

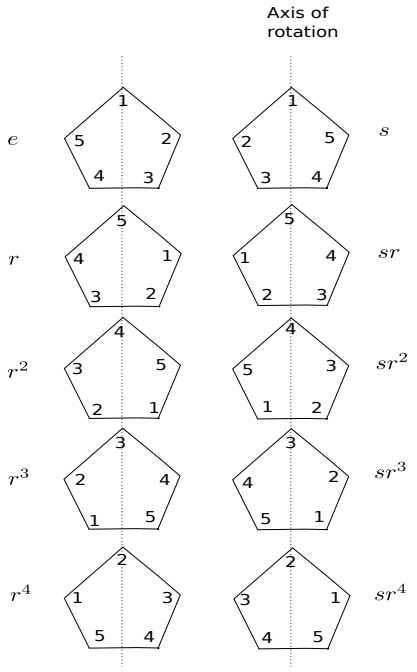

Fig. 3. Symmetries of a pentagon

4 Assignment

Exercise 14. List all possible subgroups of $\mathbb{Z}_6$ under addition.

Exercise 15. The *kernel* of a homomorphism $\phi : G \to L$ is the subset of G which maps to identity of L. Hence,

$$Ker(\phi) = \{g \in G : \ \phi(g) = e_L\}.$$

Similarly, the *image* of ϕ are the elements of L which have some element mapped to them through ϕ.

$$Img(G) = \{h \in L : \ \exists g \in G \text{ for which } \phi(g) = h.\}$$

show that $Img(G)$ and $Ker(G)$ are subgroups.

Exercise 16. Show that a subset H is a subgroup of G if it is non-empty and $\forall x, y \in H : \ xy^{-1} \in H$.

Note 3. Because H is a subset, the set of properties we need to check are much less.

Exercise 17. Show that $\mathbb{Z}_n$ is cyclic under addition. Give some examples of cyclic subgroups and some examples of non-cyclic subgroups in $\mathbb{Z}_n^+$ under multiplication.

Exercise 18. Show that all cyclic groups are commutative (abelian).

Exercise 19. Show that every cyclic group with infinite order (having infinite elements) is isomorphic to $\mathbb{Z}$ under addition.

Hint: Look for the obvious bijection between the group and $\mathbb{Z}$. Show that it is an isomorphism.

Exercise 20. Find the order of every element of group $\mathbb{Z}_p$ where p is a prime.

Exercise 21. Find the left cosets of $3\mathbb{Z}$ in group $\mathbb{Z}$.

Exercise 22. If order of a group G is prime p then show that it is isomorphic to $\mathbb{Z}_p$.

Exercise 23. Euler's theorem: For a number m, say $\phi(m)$ is the number of positive elements coprime to m and less than m. For any a which is co-prime to m,

$$a^{\phi(m)} = 1 \mod m.$$

Prove this theorem.

Exercise 24. Show that there always exist a cyclic subgroup of any finite group G.

Exercise 25. Show that the subgroup of a cyclic group is cyclic.