Lecture 10: Groups

Rajat Mittal

IIT Kanpur

We have already seen an abstract structure called *field*. Intuitively, a set where two operations can be *performed* (and distributivity holds) is a field. It might be simpler to look at sets with just one operation, such structures (set+operation) will be called a group. A more formal definition will be given below.

We will look at groups, examples of groups and various properties of groups. It is illuminating to see that all groups have lot of common properties, and they follow from the basic structure of groups. These notes will end by looking at some applications of group theory.

1 Groups

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

We already have an idea from the discussion on definition of a field. An operation can be *performed* over S if

1. Addition is allowed: for all $a, b \in S$, $a + b \in S$ and $a + b = b + a$.
2. Subtraction is allowed: There exist inverse for every element a called $-a$ and identity $0 \in S$, such that,

$$a + 0 = 0 + a = a \text{ and } a + (-a) = (-a) + a = 0.$$

Note 1. We assumed that the operation satisfies associativity.

If a set, with an operation, satisfies these properties then it will be called an *commutative group* or an *abelian group*. If we remove the restriction of operation being commutative, then the resulting abstract structure is called a *group*.

Definition 1. *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 2. 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 $x * y$.

We denote a group by its set and the operation, e.g., $(\mathbb{Z}, +)$ is the group of integers under addition. Specifically, it is a commutative group. Let us define a commutative group formally.

Definition 2. *A group is called* commutative *or* abelian *if, $\forall a, b \in G : a * b = b * a$.*

Exercise 1. Show that integers form an abelian group under addition (In other words, Integers have a group structure with respect to addition). Do they form a group under multiplication?

Exercise 2. Show that the identity is unique.

$$e_2 = e_1 = e_2 * e_1$$

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.

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. Let's look at a few different ones.

- The set of all permutations of $\{1, 2, \cdots, n\}$ under composition. What is the inverse element? This group is called the *symmetric group*, and is denoted by S_n.
- 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 $n \times n$ 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 under matrix multiplication. What is the identity element?

Note 3. The operation is as important as the set to define a group.

Exercise 4. Define field in terms of commutative groups.

Exercise 5. Show that inverse is unique.

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?

Can we represent a group in a succinct way? One natural way to represent a group is the *multiplication table* of the group. It is a matrix with both rows and columns indexed by group elements. The $(i, j)^{th}$ entry denotes the sum of i^{th} and j^{th} group element. For example, let's look at the multiplication table of $\mathbb{Z}_5^*$ under multiplication.

	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 6. 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 $\mathbb{Z}_5^*$?

We can prove a cancellation law. Given $a, b, x \in G$, we know $ax = bx \Rightarrow a = b$, similarly $xa = xb \Rightarrow a = b$. These are called respectively the right and the left cancellation law. This shows that every row (and column) is just a permutation of all elements of the group (why?).

Multiplication table gives us all the information about the group, but it 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 Order of a group element

In this section, we will look at various properties of groups. Before we do that, let me warn you about a possible mistake which many beginners do.

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 of the theorems given below, notice that we will only use the already known properties like closure, associativity, inverse and existence of identity. Later, these derived properties can be used to prove other results.

This distinction can be made more clear by an analogy. 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 and identity). 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 let's play football. We will use G to denote a group.

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 give x again, so let's compose x with itself. Since G is a group, all elements in the sequence $(x^2 := x * x, x^3 := x^2 * x, \cdots)$ will be elements of the group G (closure). 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 7. 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.

Let us prove another property of group elements: for all $x \in G$, x 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 the order of x is n, i.e., $x^n = e$. Multiply this equality by x^{-n} and we get $x^{-n} = e$. Hence, the order of x^{-1} is less than n.

Exercise 8. We did not define x^{-n}. What do you think it should be?

□

If the group G is finite, we have shown that the order of any element is less than the cardinality of the group ($|G|$ is also called the order of G).

Actually, order of an element can be restricted to just the divisors of the order of the group. Let us look at the theorem and the proof carefully.

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 $x^n = e$ and n is a multiple of d ($d \mid n$).*

Proof. We will prove the theorem in two steps. Let d be the order of an element x.

– 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.

The conclusion follows from these two steps.

For the first part, cancellation law implies that the set $S_x = \{xg : g \in G\}$ is equal to G (as a set). In other words, all elements of S_x are distinct 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 expression,

$$e = x^n.$$

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

For the second part, suppose $m = kd + r$ by division algorithm. Here, k is the quotient and $r < d$ is the remainder. Looking at the exponent,

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

This implies that there exist $r < n$, s.t. $x^r = e$. From the definition of order, $r = 0$. Hence, d divides m.

Actually the proof given above is not correct.

Exercise 9. Where is the mistake in the proof? Hint: It is in the first part.

□

Exercise 10. Show that Thm. 1 implies Fermat's theorem.

Look at group $\mathbb{Z}_p^*$.

If you look at the proof of fact that $x^n = e$, we used commutativity. So, we have only proved Thm. 1 for a *commutative*(*abelian*) group. It turns out that it is true for non-commutative groups too. Using a very different technique, we will prove the full generalization later. Second part of the proof is correct for any group. That means, $x^m = e$ iff d divides m, where d is the order of x.

3 Cyclic groups

Let n be the order of an element x in a group G. Denote the set of elements generated by x as $\langle x \rangle$,

$$\langle x \rangle = \{x, x^2, \cdots, x^{n-1}, x^n = e\}.$$

Notice that if we multiply two elements of $\langle x \rangle$, we get an element of $\langle x \rangle$. Also, identity e is present in $\langle x \rangle$.

Exercise 11. Show that every element in $\langle x \rangle$ has an inverse in $\langle x \rangle$.

This shows that $\langle x \rangle$ is a group!

What happens when n 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 3. *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,*

$$\langle x \rangle = \{\cdots, x^{-2}, x^{-1}, e, x, x^2, \cdots\}$$

Please note a few things here:

– For an infinite group, we need to consider inverses explicitly. For a finite group, inverses occur in the positive powers.

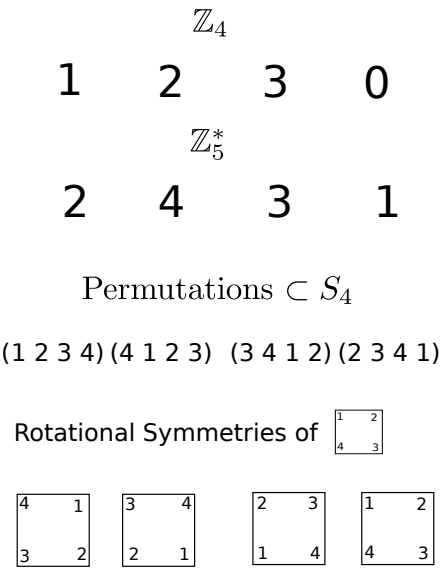

Fig. 1. Different cyclic groups

– We can similarly define the group *generated* by the set S, $\langle S \rangle$. It is the group containing all possible elements obtained from S through composition (assuming inverses).

Exercise 12. Show that a cyclic group is Abelian.

The structure of a cyclic group seems very simple. You take an element and keep composing it. What different kind of cyclic groups can be there? Look at various examples of cyclic groups of order 4 in figure 3.

Though, if you look closely, all these sets have the same structure. Look at the two groups $C_4 := \{e, x, x^2, x^3\}$ and $\mathbb{Z}_5^*$. The two multiplication tables are,

$\mathbb{Z}_5^*$:

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

C_4:

	e	x	x^2	x^3
e	e	x	x^2	x^3
x	x	x^2	x^3	e
x^2	x^2	x^3	e	x
x^3	x^3	e	x	x^2

A closer look reveals that the multiplication tables are exactly the same, if we make the following transformations,

$$e \to 1, x \to 2, x^2 \to 4, x^3 \to 3.$$

When can we say that two groups are similar? Let us formalize the notion of similarity now.

3.1 Isomorphism and homomorphism of a group

Clearly, two sets are equal if and only if there is a bijection between them. The problem is, bijection need not respect composition between elements.

That means, the composition properties of two groups might be completely different even if they have a bijection between them. A bijection between two sets just means that they have the same size.

Exercise 13. 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 coprime to 8.

Look at the orders of different elements in these groups.

Hence, for group similarity, we need to take care of composition too. A mapping ϕ *goes well* with the composition if,

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

So, we need a mapping which satisfies two properties: a bijection and goes well with the composition.

A bijection ϕ between two groups G_1 and G_2, $\phi : G_1 \to G_2$, is called an *isomorphism* if and only if,

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

We define two groups to be similar if there exist an *isomorphism* between the two, and the two groups are called *isomorphic*.

If a mapping goes well with composition but is not a bijection, it is called a *homomorphism*. 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 14. Give a homomorphism which is not an isomorphism from a group G to itself.

Every element goes to identity.

3.2 Cyclic groups and $\mathbb{Z}_n$

Armed with the notion of similarity, we can show that every cyclic group of order 4 is similar to $\mathbb{Z}_4$. More generally, we get the following theorem.

Theorem 2. *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).

Since the order is finite, group G is,

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

Let's 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 ϕ,

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

Where second equality from the fact that $x^n = 1$ and last from the definition of group $\mathbb{Z}_n$. This shows that ϕ is an isomorphism.

□

Exercise 15. Show that there is an isomorphism between a cyclic group of infinite size and $\mathbb{Z}$.

Using the previous theorem and exercise, 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. The fundamental theorem of finite abelian group asserts that every finite group can be *decomposed* in terms of cyclic groups. It is outside the scope of this course, but we encourage the reader to look at it independently.

4 Subgroups

We noticed that $\langle x \rangle$, for any $x \in G$, itself was a group under the operation of G. The subsets of group which satisfy properties of a group under the same operation are called subgroups.

Exercise 16. What are the subgroups of $\mathbb{Z}$ under addition?

Formally,

Definition 4. *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 4. The subgroup has the same operation as the original group itself

Exercise 17. Why did we not consider associativity, existence of identity?

They follow from the parent group. In case of groups, we need identity to define inverses.

Every group G has two trivial subgroups, e and the group G itself. This are called the trivial subgroups of the group G.

Let's 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).
- 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.

Proof.
- Identity: $e \in C(G)$ follows from $eg = ge = g$ for all $g \in G$.
- Closure: suppose $h, k \in C(G)$, then for any $g \in G$,

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

Hence, $C(G)$ is closed.
- Inverse: note that $gh = hg$ is equivalent to $h^{-1}gh = g$ and $g = hgh^{-1}$.

□

Exercise 18. What are the subgroups of a cyclic group?

Remember that a cyclic group is isomorphic to $\mathbb{Z}_n$.

4.1 Cosets

A subgroup H is a subset of a group G, such that, H itself satisfies the properties of a group. This implies in particular, if we multiply any two elements of H, we remain in H. Our next step in understanding the structure of the group G is, how does a subgroup interacts with elements outside the subgroup?

Suppose h is an element of H. Due to closure property, for any element h_1 of H, $h_1 h$ will lie in H. Let g_1 be an element outside H. What about $g_1 h$? Can it lie inside H?

Exercise 19. Show that $g_1 h$ is not in H.

What can we say about elements of type g_1h, where h belongs to H?

We will define a new relation R. Elements (g_1, g_2) are in relation R if and only if $g_1h = g_2$ for an element $h \in H$. We can show that this relation is an equivalence relation.

Exercise 20. Try to prove that it is an equivalence relation before looking at the hint below.

- Reflexivity: follows from the fact that $e \in H$.
- Symmetric: follows from the fact that if $h \in H$ then $h^{-1} \in H$.
- Transitivity: follows because $h_1 \in H$ and $h_2 \in H$ implies $h_1h_2 \in H$.

This implies that we have equivalence classes with respect to relation R, which will partition the group G.

Exercise 21. What are those equivalence classes?

The equivalence class of an element $g \in G$ is,

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

These sets gH are called *cosets* of the subgroup H in group G. Formally,

Definition 5. *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*,*

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

gH is called the left coset because g is multiplied on the left. We can similarly define the right cosets Hg. Without loss of generality, we will talk about left cosets below, same properties hold true for right cosets.

Exercise 22. How are left and right coset related for commutative groups?

Exercise 23. Is the set $gH = \{gh|\ h \in H\}$, for a $g \in G$, a subgroup?

It depends on whether $g \in H$ or not.

These cosets might not be subgroups, but they are closely related to the subgroup H. They help us understand the structure of G with respect to H.

Given two cosets, g_1H and g_2H, they are either completely distinct or completely same (because g_1H, g_2H are same as the equivalence class of g_1 and g_2). They are same if there exist $h \in H$ such that $g_1h = g_2$, otherwise, they are completely distinct.

Not just that, these equivalence classes turn out to have same number of elements. 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 $k = |H|$.

Let us summarize our results using a matrix. The columns will be indexed by elements of the group G and rows will be indexed by elements of the subgroup H. Column g represents the coset gH.

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

We have shown the following properties.

1. Two columns are exactly the same or completely distinct as sets.
2. Every column have the same size as a set and is equal to $|H|$ (no repeated elements).

3. Every element of group G is present in at least one column. First property implies that it is present in exactly one column.

Combining these three properties, distinct columns of the above matrix partition group G into sets of size $|H|$.

Exercise 24. What are the number of distinct cosets?

$\frac{|G|}{|H|}$. In other words, $|G|$ is always divisible by $|H|$.

This conclusion is beautifully summarized in Lagrange's theorem.

Theorem 3. *Lagrange: Given a group G and a subgroup H of this group, the order of H divides the order of G.*

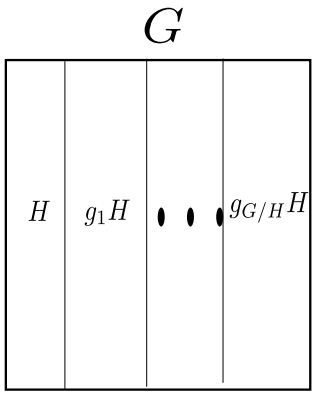

Fig. 2. Coset decomposition

This is a very strong result on the structure of a group G. 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, 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.

At least we can construct one subgroup easily, the subgroup generated by a single element.

Exercise 25. 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.

$\langle x \rangle$ is a subgroup.

Above exercise shows that $x^n = e$ for any element x of a group G.

Exercise 26. What is the implication of above fact on group S_n? Can you prove it directly?

Exercise 27. What does Lagrange's theorem say about groups with prime order?

Show that it is cyclic and then use the classification of cyclic groups.

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? Interested readers can refer to Sec. 7, we will not cover it in the course.

5 Dihedral group

We have done most of the exercises for the group $\mathbb{Z}$ or the group $\mathbb{Z}_n$. Both of these groups are commutative. We will introduce the first non-commutative subgroup in this section. This group emerges from geometry and not from number theory, contrary to other groups you have seen till now.

Definition 6. *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 Fig. 5 for all the symmetries of a pentagon.

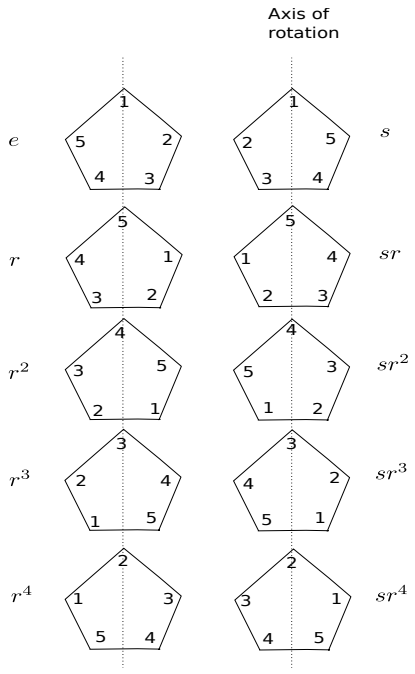

Fig. 3. Symmetries of a pentagon

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

Exercise 28. What is the inverse of rotation r. Convince yourself that the set of rotations form a cyclic group.

On the other hand, reflection is the inverse of itself. So, 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 in $\{0, 1, \cdots, n-1\}$. While using this notation, rs means, we apply s first and then r.

This group is not commutative, as shown by the following exercise.

Exercise 29. Convince yourself that $rs \neq sr$.

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

Notice how permutation affects the vertices.

This relation tells us, how to interchange r and s in any expression involving both these quantities. This way we can convert any element of the group generated by r and s to be of the form $s^i r^j$.

The above discussion shows the important properties (defining properties) of the 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 properties mentioned above, will be isomorphic to D_{2n}.

In the beginning of the course we asked a question. How many different necklaces of 6 beads can be formed using 3 colors? In the question, the numbers 3 and 6 are arbitrarily chosen. To answer this question in a meaningful way, we need to construct a strategy or a theorem which will answer the above question for any such numbers. But to understand the question better, let's ask a simpler question.

Exercise 31. How many different necklaces of 4 beads can be formed using 2 colors?

If we look at the question carefully, the first guess would be $2^4 = 16$, the number of ways we can choose colors of the four beads. Though, all these colorings need not be different.

What do we mean by *different* necklaces? It might happen that two different colorings (σ_1 and σ_2) might be the same in the sense that σ_1 can be obtained from σ_2 using rotation (or some symmetry in general). Look at Fig. 5 for one such example.

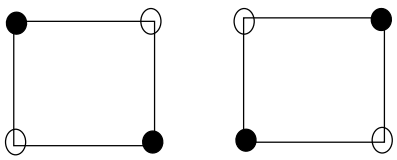

Fig. 4. Two colorings giving the same necklace

Using brute force, we can come up with all possible different necklaces for 2 white and 2 black beads (Fig. 5).

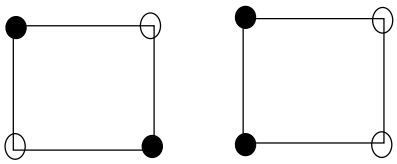

Fig. 5. Possible different necklaces with 2 white and 2 black beads

Exercise 32. What is the total number of distinct necklaces of 4 beads with 2 colors?

1 necklace if we choose exactly 4, 3, 1 or 0 black beads. So, there are $4 + 2 = 6$ different necklaces.

You can convince yourself that the question is much harder if we take bigger numbers. What should we do? When are two necklaces equivalent?

Two necklaces are equivalent if we can obtain one by applying a symmetry to other necklace (like rotation or reflection). We know that the symmetries form the dihedral group, D_{2n}. Our strategy would be to develop a general framework for groups to answer these question about distinct necklaces.

6 Group action

The first thing to notice in the necklace problem is that there are two different objects of interest. One is the set of all necklaces (set of all colorings of the necklaces) and other is the set of symmetries. A symmetry can be applied to a coloring to obtain another coloring. This can be seen as an application of a group (symmetries) on a set (coloring).

Abstractly, given a group G and a set A, every element g of G *acts* on set A. It means, for every element g there is a function from A to A, called its action on G. For the sake of brevity, we will denote the function corresponding to the element $g \in G$ with g itself. Hence, the value of $x \in A$ after action of g will be called $g(x)$.

Exercise 33. What is the group and what is the set for the necklace problem?

It is NOT the set of distinct necklaces.

Let's look at the formal definition.

Definition 7. *Given a group G and a set A, a group action from G to A assigns a function $g : A \to A$ for every element g of group G. A valid group action satisfies the following properties.*

- *Identity takes any element $x \in A$ to x itself, i.e., $e(x) = x$ for every $x \in A$.*
- *For any two group elements $g_1, g_2 \in G$, their functions are consistent with the group composition,*

$$g_1(g_2(x)) = (g_1 g_2)(x).$$

Using this definition, it can be shown that $g(x) \neq g(y)$ for two distinct element x, y of A.

Exercise 34. Prove this.

Look at the action of g^{-1}.

Hence, action of g is a permutation on the elements of A. This gives us another representation of group elements. For any group action on A of size m, we have a permutation representation for any element $g \in G$ in terms of a permutation on m elements. In the following sections, we will keep this representation in mind.

Exercise 35. Show that the left multiplication $g : G \to G$ defined by $g(h) = gh$ is a group action of G on G itself.

Note 5. Actually a slightly stronger theorem holds. It is called *Cayley's theorem*, and is given below. We will not show the proof of this theorem.

Theorem 4. *Cayley's theorem: Every group of order n is isomorphic to some subgroup of S_n.*

6.1 Orbits

After defining group action, we will look back at the original question. What necklaces are similar in terms of the group action? Clearly, if a necklace can be obtained from another by the action of a symmetry, they are similar. We will define two elements to be related if one can be obtained by other using a group element.

Suppose we are given action of group G on a set A. Let's define a relation between the elements of A. If $\exists\ g :\ g(x) = y$ then we will say that x, y are related ($x \sim y$). We can easily prove that this relation is an equivalence relation.

- Reflexive: Why?
- Symmetric: Suppose $x \sim y$ because $g(x) = y$. Then consider $x = ex = (g^{-1}g)(x) = g^{-1}y$, implying $y \sim x$.
- Transitive: Show it as an exercise.

Hence, this equivalence relation will partition the set A into distinct equivalence classes. The equivalence class corresponding to $x \in A$ is the orbit $(G(x))$ of element x. In other words,

$$G(x) = \{g(x) : \ g \in G\}.$$

Now we will look at two counting questions,

1. What is the size of these orbits?
2. How many distinct orbits are there?

Why are we interested in these questions? Let us look at this concept from the example of necklaces. If a necklace x can be obtained from another necklace y by the action of a symmetry then they are related (in the necklace case indistinguishable).

Exercise 36. Convince yourself that the number of distinct necklaces is the same as the number of distinct orbits (equivalence classes) under the dihedral group D_{2n}.

We will answer both the counting questions under the general group-theoretic framework. As a special case, this will solve the necklace problem.

6.2 Stabilizers

Remember, the orbit of $x \in A$ under the action of G can be defined as,

$$G(x) = \{g(x) : \ g \in G\}.$$

If every $g \in G$ took x to a different element, the size of the orbit would be $|G|$. Most of the time many group elements take x to the same element y of A.

Let's define this set as G(x,y),

$$G(x, y) = \{g \in G : \ g(x) = y\}.$$

Exercise 37. Does the set $G(x, y)$ form a subgroup of G? Under what conditions will it form a subgroup?

What about closure?

The answer to the previous exercise is, $G(x, y)$ is a group when $x = y$. The set $G_x := G(x, x)$ is called the stabilizer of x,

$$G_x = \{g \in G : \ g(x) = x\}.$$

Exercise 38. Prove that G_x is a subgroup of G.

Once we have a subgroup G_x, the natural question to ask is, what are the cosets? This is where we get lucky.

Suppose, y is an element of the orbit $G(x)$. So, there exist an $h \in G$, s.t., $h(x) = y$. Then, $G(x, y)$ is precisely the coset hG_x.

Lemma 1. *Given a $y \in A$, s.t., $h(x) = y$. The coset hG_x is same as the set $G(x, y)$.*

Proof. $\Rightarrow$: an element in hG_x is of the form $hg,\ g \in G_x$. Then $hg(x) = h(x) = y$. So $hG_x \subseteq G(x, y)$.

$\Leftarrow$: Suppose $g \in G(x, y)$, i.e., $g(x) = y$. Then, you can show that,

Exercise 39. $h^{-1}g \in G_x$

Again, you can show that $h^{-1}g \in G_x$ implies $g \in hG_x$.

Exercise 40. Show the above implication. Be careful, it is not just the same as multiplying by h on both sides.

From the previous exercise, $G(x, y) \subseteq hG_x$. □

Hence, for every element y in the orbit $G(x)$, there is a coset. It is an easy exercise to convince yourself that every coset will correspond to a single element in the orbit $G(x)$. So the number of elements in the orbit is equal to the number of cosets. But we know that the number of cosets can be calculated from Lagrange's theorem. Hence,

$$|G| = |G_x||G(x)|.$$

Note 6. G_x is a subset of G, but $G(x) \subseteq A$. The equation works because we show a one to one relation between $G(x)$ (orbit) and the cosets of G_x in G.

6.3 Burnside's lemma

We now know the size of the orbit in terms of the stabilizer. Given an element x with stabilizer G_x, the number of elements in its orbit is $\frac{|G|}{|G_x|}$. Can this formula help us in counting the number of distinct orbits?

We will give every element in A a weight of $\frac{1}{|G(x)|}$ (so that weight of every orbit becomes 1). The number of distinct orbits is now the sum of weights of all elements of A.

$$\text{Number of distinct orbits } = \sum_{x \in A} \frac{1}{|G(x)|} = \frac{1}{|G|} \sum_{x \in A} |G_x|.$$

The total summation in RHS is equal to the number of pairs $(g \in G, x \in A)$, s.t., $g(x) = x$.

Suppose, we make a matrix with rows indexed by elements of G and columns indexed by elements of A. The entry (g, x) is one if $g(x) = x$ and 0 otherwise.

	x_1	x_2	$\cdots$	$x_{\lvert A\rvert}$
g_1	0	1	$\cdots$	1
g_2	0	0	$\cdots$	1
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$g_{\lvert G\rvert}$	1	0	$\cdots$	0

Observe, number of 1's in the matrix is equal to $\sum_{x \in A} |G(x)|$. Each term in the summation, $|G_x|$, is the number of 1's in the column corresponding to x. By double counting (learnt in combinatorics), we can count the number of 1's in the matrix by taking the sum row-wise too.

The rows correspond to a group element $g \in G$, and a row counts the number of x's which remain unchanged under the action of g. Suppose, $S(g)$ is set of elements of A fixed by g.

$$S(g) = \{x : \ g(x) = x, \ x \in A\}.$$

Calculating the number of 1's in the matrix row-wise, we get the orbit-counting (Burnside's) lemma.

Lemma 2 (Burnside's lemma (Orbit-counting)). *Given a group action of G over A. The number of distinct orbits can be written as,*

$$\textit{Number of distinct orbits } = \frac{1}{|G|} \sum_{g \in G} |S(g)|.$$

Note 7. The summation is now over G instead of A.

One natural question you might ask is, how did this benefit us? Previously we were summing over all possible $x \in A$, and now we are summing up over all $g \in G$. The reason is, in general, the size of group G will be much smaller than the size of set A. If there were c colors and n beads; size of A is c^n, but size of G is just $2n$.

Let us get back to over original question. How many necklaces can be formed with c colors having n beads?

What is A and what is G. Again, G is the dihedral group D_{2n}. The set A should represent all possible colorings (necklaces, when the placement of beads is fixed).

Suppose, the set of beads is represented by B and set of colors is represented by C. A coloring is essentially a function $N : B \to C$. There are $|C|^{|B|}$ number of necklaces and there set is represented by C^B.

Note 8. The size of group is much smaller than the size of the set.

To apply Burnside's lemma, we need to find, how many colorings in C^B are fixed by an element g of the dihedral group D_{2n}? If we represent g as a permutation on the elements of B, a coloring c is fixed by g if any pair of vertices in the same cycle of g get the same color (according to c).

Exercise 41. Convince yourself that the statement above is true.

In other words, if there are n_g number of cycles in the permutation representation of g, $|S(g)| = |C|^{n_g}$ number of colorings get fixed by g. Applying Burnside's lemma,

$$\text{Number of distinct necklaces } = \frac{1}{|D_{2n}|} \sum_{g \in D_{2n}} |C|^{n_g}.$$

This is called *Polya's enumeration theorem.* There is a stronger version of Polya's theorem too, but, we will not be able to cover it in this course.

Let's look at an example where Orbit-counting lemma will help us in answering the question about necklaces. First, try to solve this exercise yourself. Later, you can look at the solution given below.

Exercise 42. How many necklaces of 6 beads can be formed using 3 colors?

Arrange the beads on the vertices of a regular 6-gon. The group G is D_{12} and set A is the set of all possible colorings. The total number of colorings is 3^6.

For every element of G, we will calculate the number of elements of A fixed by it.

- Identity e: Fixes all (3^6) elements.
- Rotation by t beads means $gcd(6, t)$ cycles (Why? What is the size of the cycle?). So $n_r, n_{r^5} = 1; n_{r^2}, n_{r^4} = 2; n_{r^3} = 3$.
- If the rotation is along the axis passing through two vertices, then 3 cycles.
- If the rotation is along the axis passing through mid point of two edges, there are 4 cycles.

So, by Orbit-counting lemma,

$$\text{Number of distinct orbits } = \frac{1}{12}(3^6 + (2 \times 3^1) + (2 \times 3^2) + 3^3 + (3 \times 3^3) + (3 \times 3^4)) = \frac{1104}{12} = 92.$$

For other examples of application of Burnside's lemma, please look at section 21.4 of Norman Biggs book([2]). There is a nice example in Peter Cameron's notes on Group Theory too (section 1.3, [3]).

7 Extra reading: Normal subgroup

Suppose, we are given two elements g, n from a group G. The *conjugate* of n by g is the group element gng^{-1}.

Exercise 43. When is the conjugate of n equal to itself?

Clearly, the conjugate of n by g is n itself iff n and g commute.
We can similarly define the conjugate of a set $N \subseteq G$ by g,

$$gNg^{-1} := \{gng^{-1} : \ n \in N\}.$$

Definition 8. *Normal subgroup: A subgroup N of G is* normal *if for every element g in G, the conjugate of N is N itself.*

$$gNg^{-1} = N \quad \forall g \in G.$$

We noticed that $gng^{-1} = n$ iff g, n commute with each other.

Exercise 44. When is $gNg^{-1} = N$?

In this case, the left and right cosets are the same for any element g with respect to subgroup N. Hence, a subgroup is normal if its left and right cosets coincide.

Exercise 45. Show that the following are equivalent. So, you need to show that each of them applies any other.

1. N is a normal subgroup.
2. The set $S = \{g : gN = Ng\}$ is G itself.
3. For all elements $g \in G$, $gNg^{-1} \subseteq N$.

Hint: Instead of showing all $2 \times \binom{3}{2}$ implications, you can show 1) $\Rightarrow$ 2) $\Rightarrow$ 3) $\Rightarrow$ 1.
Last equivalence, $gNg^{-1} \subseteq N \Rightarrow N \subseteq g^{-1}Ng$. Since this is true for all $g's$, just consider it for g and g^{-1} together.

7.1 Quotient group

We have introduced the concept of normal subgroups without really emphasizing why it is defined. Let's move to our original question. What can be said about the set of cosets, do they form a group?

Suppose G is a group and H is a subgroup. Denote by S, the set of cosets of G with respect to H. For S to be a group it needs a law of composition. The most natural composition rule which comes to mind is,

$$(gH)(kH) = (gk)H.$$

Here, gH and kH represent two different cosets. The problem with this definition is, it might not be *well-defined*. It might happen that $g' \in gH$ and $k' \in kH$ when multiplied give a totally different coset $(g'k')H$ as compared to $(gk)H$.

Exercise 46. Show that this operation is well-defined for commutative (abelian) groups.

What about general groups? Normal subgroups come to the rescue.

Theorem 5. *Suppose G is a group and H is its subgroup, the operation,*

$$(gH)(kH) = (gk)H,$$

is well defined if and only if H is a normal subgroup.

Note 9. Every subgroup of a commutative group is normal.

Proof. $\Rightarrow$): We need to show: if the operation is well defined, then $ghg^{-1} \in H$ for every $g \in G, h \in H$. Consider the multiplication of H with $g^{-1}H$. Since $e, h \in H$, we know $eH = hH$. Since the multiplication is well defined,

$$(eg^{-1})H = (eH)(g^{-1}H) = (hH)(g^{-1}H) = (hg^{-1})H \quad \Rightarrow \quad g^{-1}H = (hg^{-1})H.$$

Again, using the fact that $e \in H$, $hg^{-1} \in g^{-1}H$. This implies $hg^{-1} = g^{-1}h' \quad \Rightarrow ghg^{-1} = h'$ for some $h' \in H$.

$\Leftarrow$): Suppose N is a normal subgroup. Given $g' = gn$ and $k' = kn'$, where $g, g', k, k' \in G$ and $n, n' \in N$, we need to show that $(gk)N = (g'k')N$.

$$(g'k')N = (gnkn')N.$$

Exercise 47. Show that there exist $m \in N$, s.t., $nk = km$. Hence complete the proof.

□

With this composition rule we can easily prove that the set of cosets form a group (exercise).

Definition 9. *Given a group G and a normal subgroup N, the group of cosets formed is known as the* quotient group *and is denoted by $\frac{G}{N}$.*

Using Lagrange's theorem,

Theorem 6. *Given a group G and a normal subgroup N,*

$$|G| = |N|\left|\frac{G}{N}\right|$$

7.2 Relationship between quotient group and homomorphisms

Let us revisit the concept of homomorphisms between groups. The homomorphism between two groups G and H is a mapping $\phi : G \to H$ that preserves composition.

$$\phi(gg') = \phi(g)\phi(g')$$

For every homomorphism ϕ we can define two important sets.

- Image: The set of all elements h of H, s.t., there exists $g \in G$ for which $\phi(g) = h$.

$$Img(\phi) = \{h \in H : \quad \exists g \in G \quad \phi(g) = h\}$$

  Generally, you can restrict your attention to $Img(\phi)$ instead of the entire H.
- Kernel: The set of all elements of G which are mapped to identity in H.

$$Ker(\phi) = \{g \in G : \quad \phi(G) = e_H\}$$

Note 10. We have used the subscript to differentiate between the identity of G and H.

Note 11. $Img(\phi)$ is a subset of H and $Ker(\phi)$ is a subset of G.

Exercise 48. Prove that $Img(\phi)$ and $Ker(\phi)$ form a group under composition with respect to H and G respectively.

Exercise 49. Show that $Ker(\phi)$ is a normal subgroup.

There is a beautiful relation between the quotient groups and homomorphisms. We know that $Ker(\phi)$ is the set of elements of G which map to identity. What do the cosets of $Ker(\phi)$ represent. Let's take two elements g, h of a coset $gKer(\phi)$. By definition of cosets, $h = gk$ where $\phi(k) = e_H$. By the composition rule of homomorphism, $\phi(g) = \phi(h)$.

Exercise 50. Prove that $\phi(g) = \phi(h)$ if and only if g and h belong to the same coset with respect to $Ker(\phi)$.

The set of elements of G which map to the same element in H are called the fibers of ϕ. The previous exercise tell us that fibers are essentially the cosets with respect to $Ker(\phi)$ (the quotient group).

The fibers are mapped to some element in $Img(\phi)$ by ϕ. Hence, there is a one to one relationship between the quotient group $\frac{G}{Ker(\phi)}$ and $Img(\phi)$. Actually the relation is much stronger.

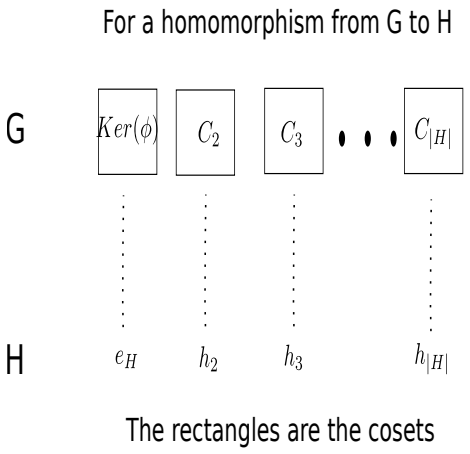

Fig. 6. Relationship between the quotient group and the image of homomorphism

It is an easy exercise to show that the mapping between quotient group $\frac{G}{Ker(\phi)}$ and $Img(\phi)$ is an isomorphism.

Exercise 51. Prove that the above mapping is an isomorphism.

Again applying the Lagrange's theorem,

$$|G| = |Ker(\phi)||Img(\phi)|.$$

Fig. 11 depict that every element of quotient group is mapped to one element of image of ϕ. We also know that this mapping is *well-behaved* with respect to composition.

$$\phi((gKer(\phi))(hKer(\phi))) = \phi(gKer(\phi))\phi(hKer(\phi))$$

There is an abuse of notation here, which highlights the main point too. The notation $\phi(gKer(\phi))$ represents the value of ϕ on any element of $gKer(\phi)$. We know that they all give the same value. The study

of homomorphism is basically the study of quotient group. The study of quotient group can be done by choosing a representative for every coset and doing the computation over it (instead of the cosets).

We have shown that $Ker(\phi)$ is normal. It can also be shown that any normal subgroup N is a kernel of some homomorphism ϕ (exercise).

References

1. K. H. Rosen. Discrete Mathematics and Its Applications. *McGraw-Hill*, 1999.
2. N. L. Biggs. Discrete Mathematics. *Oxford University Press*, 2003.
3. P. J. Cameron. Notes on finite group theory. *http://www.maths.qmul.ac.uk/ pjc/notes/gt.pdf*, 2013.