Inter-IIT Tech Meet Prep

Week 4: Group Theory

MathSoc IIT Delhi

Contents

1 Basic Definitions

Definition 1.1. *A **group** is a set G together with a binary operation $\cdot : G \times G \to G$ satisfying the following axioms:*

1. ***Associativity:*** *For all $a, b, c \in G$, we have $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.*
2. ***Identity element:*** *There exists an element $e \in G$ such that $e \cdot a = a \cdot e = a$ for all $a \in G$.*
3. ***Inverses:*** *For each $a \in G$, there exists an element $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.*

Note that we did not include closure as an axiom because the binary operation is defined as map from $G \times G$ to G, so it holds by definition.

Definition 1.2. *A **subgroup** H of a group G is a subset of G that is itself a group under the operation inherited from G.*

Definition 1.3. *The **order** of a group G, denoted $|G|$, is the number of elements in G. If G is infinite, we say it has infinite order. The **order of an element** $g \in G$ is the least positive integer n such that $g^n = e$, if such an n exists.*

2 Examples of Groups

- **The integers under addition:** $(\mathbb{Z}, +)$ is an infinite group. The identity is 0, and each integer has an inverse under addition.
- **The symmetric group:** S_n is the group of all permutations of n elements, with group operation given by composition. It has order $n!$.
- **Cyclic groups:** A group G is cyclic if there exists an element $g \in G$ such that every element of G can be written as g^n for some integer n.
- **Matrix groups:** The group $\mathrm{GL}_n(\mathbb{R})$ consists of all invertible $n \times n$ real matrices, with matrix multiplication as the operation.

3 Some More Definitions

Definition 3.1. *For an element $g \in G$ and a subgroup H of G, the **left cosets** of H in G are the sets obtained by multiplying each element of H by $g \in G$, where g is the* left factor*, i.e.*

$$gH = \{gh : h \in H\}, \quad \text{for } g \in G.$$

*The **right cosets** are defined similarly, with element g as a* right factor*, that is,*

$$Hg = \{hg : h \in H\}, \quad \text{for } g \in G.$$

For a subgroup H of G, two left (or right) cosets are either identical or disjoint. (Prove!)

Definition 3.2. Observe that every left or right coset of H has the same number of elements as H itself. Furthermore, the number of left cosets is equal to the number of right cosets. *We define this number to be the **index of** H **in** G and denote it by $[G : H]$.*

Definition 3.3. *Let $(G, *)$ and $(H, \circ)$ be groups. A function $\varphi : G \to H$ is called a **group homomorphism** if for all $g_1, g_2 \in G$, we have*

$$\varphi(g_1 * g_2) = \varphi(g_1) \circ \varphi(g_2).$$

Definition 3.4. *Let $(G, *)$ and $(H, \circ)$ be groups. A function $\varphi : G \to H$ is called a **group isomorphism** if:*

1. *φ is a group homomorphism, i.e.,*

$$\varphi(g_1 * g_2) = \varphi(g_1) \circ \varphi(g_2) \quad \text{for all } g_1, g_2 \in G,$$

2. *φ is bijective (both one-to-one and onto).*

*If such a map exists, we say that the groups G and H are **isomorphic**, and we write $G \simeq H$.*

4 Important Theorems

Theorem 4.1 (**Lagrange's Theorem**). *Let G be a finite group and H a subgroup of G. Then the order of H divides the order of G, i.e., $|G| = [G : H] \cdot |H|$, where $[G : H]$ denotes the index of H in G.*

Theorem 4.2 (**Cauchy's Theorem**). *Let G be a finite group and let p be a prime dividing $|G|$. Then G contains an element of order p.*

5 Combinatorics and Group Actions

A motivating problem

Ashutosh gifts a necklace to Gungun, his "quasi-girlfriend". As expected, she is delighted. This necklace is made of 8 beads which come in two colours, white & black. The next day, he crafts another necklace using the same resources—8 beads of 2 colours, and gifts it to Gungun. This time, however, she is unimpressed. She insists that it is the same necklace that he had gifted her the day before. Ashutosh protests, and says that he arranged the beads in a different way before stringing them together, but she proves her claim by rotating and flipping the necklace and demonstrating that it matches the previous one exactly. Ashutosh agrees (and, apologises, **of course!**) that the two necklaces are not truly distinct. He now begins exploring a new challenge: how many "genuinely different" necklaces he can make using 8 beads of two colours, so that each one brings a fresh smile to Gungun's face. This brings him to the problem: *How many distinct necklaces of 8 beads can be made using black and white beads?* At first glance, brute-force enumeration seems feasible for small numbers. For instance:

- 1 bead: 2 necklaces (black or white),
- 2 beads: 3 necklaces (BB, BW, WW),
- 3 beads: 4 necklaces (see Fig. 1),
- 4 beads: 6 necklaces (see Fig. 2).

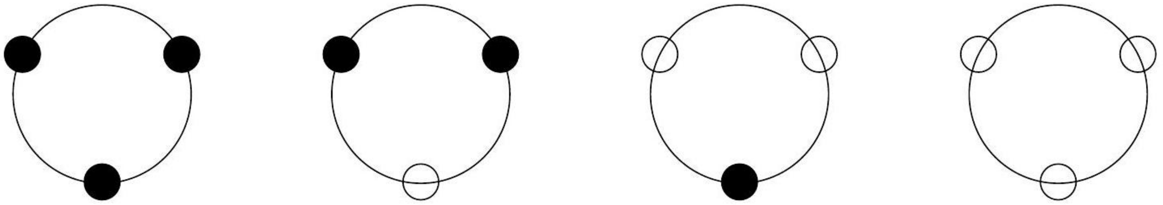

Figure 1: All 3-bead necklaces

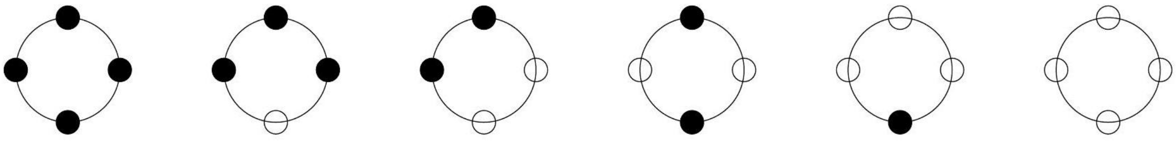

Figure 2: All 4-bead necklaces

Colourings and Symmetry

For 8 beads placed at the vertices of a regular octagon, there are $2^8 = 256$ colourings. However, many of these yield indistinguishable necklaces due to the octagon's symmetries (rotations and reflections).

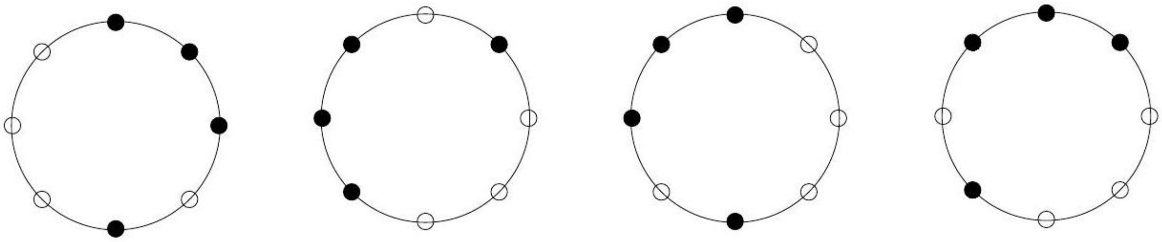

Figure 3: Different colourings representing the same necklace via rotation/reflection

Symmetries of the Octagon

The symmetries of the regular octagon form the dihedral group D_8, consisting of:

- 8 rotations (including the identity),
- 4 reflections through opposite vertices,
- 4 reflections through midpoints of opposite edges.

Two colourings are equivalent if one can be obtained from the other via a symmetry in D_8.

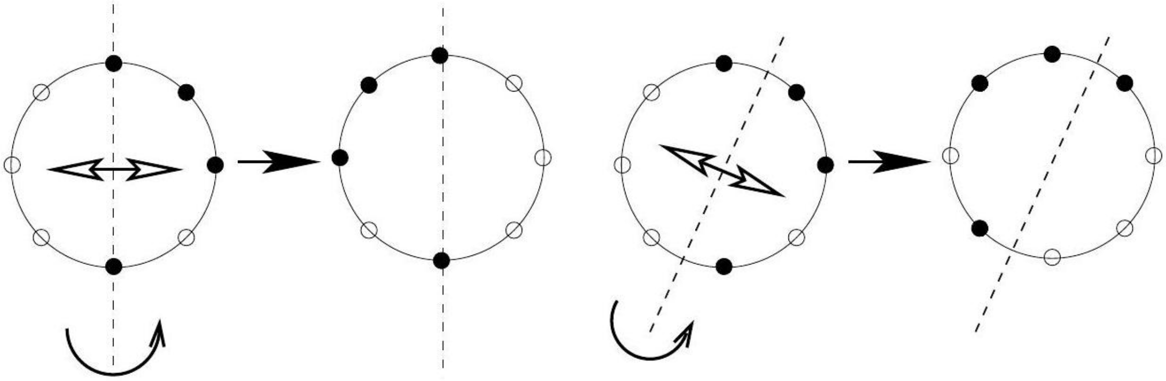

Figure 4: Flipping combined with rotation are equivalent to reflection

The Core Insight

The number of distinct necklaces is equal to the number of equivalence classes of colourings under the action of D_8. That is,

$$\text{Number of necklaces} = \text{Number of } D_8\text{-orbits on the set of 256 colourings.}$$

This sets the stage for applying the Orbit Counting Lemma (Burnside's Lemma).

Definition 5.1. *Let G be a group and X a set. We say that G acts on X, or that there is an action of G on X, or simply that X is a G-set, if there exists a function*

$$\cdot : G \times X \to X$$

satisfying the following axioms:

1. *$e \cdot x = x$ for every $x \in X$, where e denotes the identity element of the group G,*
2. *$g \cdot (h \cdot x) = (gh) \cdot x$ for every $x \in X$ and every $g, h \in G$.*

Definition 5.2. *Let a group G act on a set X. The **orbit** of an element $x \in X$, denoted $G \cdot x$, is the set:*

$$G \cdot x = \{g \cdot x \mid g \in G\}$$

This is the set of all elements to which x can be moved by the action of G.

Definition 5.3. *A **fixed point** $x \in X$ under an element $g \in G$ is an element such that $g \cdot x = x$. The set of all such elements is denoted X^g or X_g.*

Definition 5.4. *The **stabilizer** of $x \in X$, denoted G_x, is the set of all elements in G that fix x:*

$$G_x = \{g \in G \mid g \cdot x = x\}$$

Theorem 5.5 (**Burnside's Lemma**)**.** *Let G be a finite group acting on a set X. Then the number of orbits (i.e., distinct configurations under the group action) is:*

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

where X^g is the set of elements in X fixed by g.

Example: Coloring Vertices of a Square

Let X be the set of colorings of the four corners of a square using n colors. The group G includes 4 rotations: 0°, 90°, 180°, 270°.

- **Rotation 0° (Identity):** all n^4 colorings are fixed.
- **Rotation 90° or 270°:** all vertices must be the same color → n colorings.
- **Rotation 180°:** opposite vertices must match → n^2 colorings.

Total number of distinct colorings:

$$\frac{1}{4}(n^4 + n^2 + 2n)$$

6 Number Theory

Group theory provides elegant frameworks for understanding classical results in number theory. Many theorems, especially those concerning modular arithmetic and multiplicative structures, can be viewed as consequences of group-theoretic principles.

Multiplicative Groups Modulo n

Let $\mathbb{Z}_n^\times = \{a \in \mathbb{Z}_n : \gcd(a, n) = 1\}$. It forms a finite abelian group under multiplication modulo n.

Lemma 6.1. *$\mathbb{Z}_n^\times$ is a group under multiplication modulo n. Its order is $\phi(n)$, Euler's totient function.*

Fermat's Little Theorem (FLT)

Theorem 6.2 (Fermat's Little Theorem)**.** *Let p be a prime and $a \in \mathbb{Z}$ such that $p \nmid a$. Then:*

$$a^{p-1} \equiv 1 \pmod{p}$$

Group-Theoretic Proof. The set $\mathbb{Z}_p^\times$ is a group of order $p-1$. By Lagrange's Theorem, the order of any element divides $p-1$, so $a^{p-1} \equiv 1 \pmod{p}$.

Euler's Theorem

Theorem 6.3 (Euler's Theorem)**.** *If $\gcd(a, n) = 1$, then:*

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Group-Theoretic Interpretation. Follows from Lagrange's Theorem applied to the group $\mathbb{Z}_n^\times$ of order $\phi(n)$.

Wilson's Theorem

Theorem 6.4 (Wilson's Theorem)**.** *Let p be a prime. Then:*

$$(p-1)! \equiv -1 \pmod{p}$$

Group-Theoretic Perspective. In the group $\mathbb{Z}_p^\times$, every element has an inverse. Pairing each element with its inverse except for 1 and $p-1$ gives the product as -1.

7 Practice Problems

Problem 1

Assuming that a human can live up to 100 years maximum by optimizing the lifestyle, and that Ashutosh has a large supply of black and white beads, help him find the least number of beads such that by stringing this many beads to craft a necklace and gifting her a "fresh" such necklace each day, he can keep Gungun happy for the whole of her life. (Currently she is 20) How many distinct configurations of the necklace are possible in this case? [or you can help him find what Gungun's favourite colour is. If the necklace has this colour, she might be happier, and there will be more choices of colours.] Solve the same problem when the number of available colours for beads is 3. [hopefully some day she will not be having "quasi-" in her apposition anymore.]

Problem 2

Can an infinite group have only finitely many subgroups? Prove your claim.

Problem 3

Prove that in a finite group, number of elements having order 5 is divisible by 5. What if the group is infinite? Justify.

Problem 4

Let G be a finite group and p a prime dividing $|G|$. Prove that G contains an element of order p.

Problem 5

1. Show that there does not exist an isomorphism between $(\mathbb{Z}, +)$ and $(\mathbb{Q}, +)$.
2. Show that there does not exist an isomorphism between $(\mathbb{Q}, +)$ and $(\mathbb{Q}_{\neq 0}, \times)$.
3. Show that there does not exist an isomorphism between $(\mathbb{Z}, +)$ and $(\mathbb{Q}_{>0}, \times)$.
4. Show that there exists an isomorphism between the symmetric group S_3 and the dihedral group D_6.

Problem 6

Consider the group action of $\mathrm{GL}_2(\mathbb{R})$ on $\mathbb{R}^2$ defined by regular matrix-vector multiplication. Describe the stabilizer of an element $(x, y) \in \mathbb{R}^2$.

Problem 7

Consider the action of $\mathrm{GL}_2(\mathbb{R})$ on $\mathbb{C} \cup \{\infty\}$ given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}.$$

[Here, the fraction is defined to be infinity when the denominator is $0 + 0i$. And putting $z = \infty$ will yield the fraction to be $\frac{a}{c}$.]

What are the orbits? What is the stabilizer of a complex number z?

Problem 8

Consider a group G such that $g, h \in G$, $O(h) > O(g) = 2$ and $ghg^{-1} = h^2$. Then find $O(h)$.

Problem 9

For a natural number $n \in \mathbb{N}$, $((\mathbb{Z}/n\mathbb{Z})^*, \times)$ denotes the group of integers coprime to n under the operation of multiplication modulo n. If n is a prime power, then this group is known to be cyclic. Using this, prove that if $a^n \equiv a \pmod{n}$ for all $a \in \mathbb{Z}$, then for all primes satisfying $p \mid n$, we have $p - 1 \mid n - 1$.