

Bhoris Dhanjal

Algebra IV

Lecture Notes
for SMAT402

Contents

1	Groups and subgroups	1
1.1	Binary operation	1
1.2	Group axioms	1
1.3	Examples of Groups	2
1.3.1	Group of integers modulo n	2
1.3.2	Klein-4 group (Vierergruppe)	2
1.3.3	Symmetric group	3
1.3.4	Alternating group	3
1.3.5	Dihedral group	3
1.4	Common properties of groups	3
1.4.1	Abelian group	3
2	Cyclic groups and cyclic subgroups	4
3	Lagrange's theorem and group homomorphisms	5

Chapter 1

Groups and subgroups

1.1 Binary operation

For a set V a function from $f : V \times V \rightarrow V$ is called a binary function if the following properties hold.

1. f is defined for all pairs of elements of V .
2. f is closed.

Example 1.1. $G = \{1, 2, 3\}$, then $+$ is not a binary operation as it is not closed under addition.

Example 1.2. $G = \{-1, 0, 1\}$, then $+$ is a binary operation.

Example 1.3. \mathbb{N} , then both $+$, \times are binary operations.

1.2 Group axioms

A group is an ordered pair $(G, *)$ where G is a non empty set and $*$ is a binary operation on G satisfying the following axioms:

1. **Closure:** $\forall a, b \in G$, $a * b$, is also in G
2. **Associativity:** $(a * b) * c = a * (b * c)$, $\forall a, b, c \in G$
3. **Identity:** $\exists e \in G$, called an identity of G , s.t. $\forall a \in G$ we have $a * e = e * a = a$
4. **Inverse:** $\forall a \in G \exists a^{-1} \in G$, called an inverse of a , s.t. $a * a^{-1} = a^{-1} * a = e$.

1.3 Examples of Groups

Example 1.4. $(\mathbb{N}, +)$ is not a group since it lacks additive identity.

Example 1.5. $(\mathbb{Z}, +)$ is a group while (\mathbb{Z}, \times) is not a group since it lacks multiplicative inverses.

Example 1.6. (\mathbb{Q}, \times) is not a group since 0 doesn't have an inverse. However $(\mathbb{Q} \setminus 0, \times)$ is a group.

Example 1.7. $n\mathbb{Z} = \{\dots, -2n, -n, 0, n, 2n, \dots\}$ with addition are subgroups of $(\mathbb{Z}, +)$.

Example 1.8. $S = \{1, -1, i, -i\}$, with multiplication is a cyclic group generated by i . Exercise make a Cayley table.

Example 1.9. $M_{n \times n}(\mathbb{R})$ for $n \times n$ matrices over \mathbb{R} forms a group under addition but not under matrix multiplication (because of lack of inverses).

Example 1.10. $GL_n(\mathbb{R})$ (i.e. General linear group - matrices with positive determinant) forms a group under multiplication.

Example 1.11. $SL_n(\mathbb{R})$ (i.e. Special linear group - matrices with $\det=1$) forms a group under multiplication.

1.3.1 Group of integers modulo n

Definition 1.12 (Congruence class). For $n \in \mathbb{Z}$ define the congruence relation R as $aRb \iff n|(a-b)$. This is an equivalence relation.

Definition 1.13 ($\mathbb{Z}/n\mathbb{Z}$ or \mathbb{Z}_n). Let $\mathbb{Z}/n\mathbb{Z}$ be defined as the $\{x \in \mathbb{Z} \mid xRn\}$.

$$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$$

Addition $\bar{a} + \bar{b} = \overline{a+b}$ and multiplication $\bar{a} \cdot \bar{b} = \overline{ab}$.

$(\mathbb{Z}_n, +)$ forms a group for all n , while (\mathbb{Z}_n^*, \cdot) forms a group only when n is prime.

Theorem 1.14. \mathbb{Z}_n^* forms a group under multiplication iff n is prime.

Proof. The proof is trivial. □

1.3.2 Klein-4 group (Vierergruppe)

Denoted by V_4 the Klein-4 group is the smallest non-cyclic group. It is abelian. It is a group with 4 elements such that the square of all elements is identity. And product of two distinct elements gives a distinct element. The symmetry group of a rectangle is isomorphic to V_4 .

1.3.3 Symmetric group

The symmetric group is the group whose elements are all the bijections from the set to itself. The order of the n^{th} Symmetric group (S_n) is equal to $n!$.

Two-Line to Cycle notation for permutations

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix} = (125)(34) = (34)(125) = (34)(512) = (15)(25)(34)$$

Here, the last form is a case of 2-cycle (transposition).

The parity of any permutation σ is given by the parity of the number of its 2-cycles (transpositions). In the above example it is odd.

1.3.4 Alternating group

The group of all even permutations from S_n is called the alternating group A_n .

1.3.5 Dihedral group

This is the group of symmetries of a regular polygon. Denoted by $D_n, n \geq 3$.

- Order of $D_n = 2n$.
- $D_n = \{e, x, x^2, \dots, x^{n-1}, y, yx, yx^2, \dots, yx^{n-1}\}$. Here we can interpret x as rotation by $2\pi/n$ and y is reflection about vertical axis.

1.4 Common properties of groups

1.4.1 Abelian group

If a group is commutative it is called Abelian.

- If $a^2 = e \forall a \in G$ then it is Abelian.

1.4.2 Order of a group

If there are a finite number of elements in a group then the group is called a finite group and the number of elements is called the group order of the group.

1.4.3 Order of element

The smallest natural number n such that $a^n = e$ is called the order of a group element a .

Chapter 2

Cyclic groups and cyclic subgroups

Chapter 3

Lagrange's theorem and group homomorphisms

