Unit I — Group Theory

Objectives: Understand the fundamental algebraic structure “Group”; study Groups – Examples – Cyclic Groups – Permutation Groups – Lagrange’s theorem –Normal subgroups – Homomorphism – Cayley’s theorem – Cauchy’s theorem –Sylow’s theorems – Finite Abelian Groups.

Concepts Overview

Concept	Description	Note	Example
Group	Non-empty set with a binary operation satisfying closure, associativity, identity, and inverse properties.	Algebraic structure	$(\mathbb{Z},+)$, $(\mathbb{R}^*,\cdot)$
Subgroup	Non-empty subset closed under operation and inverses.	Contains identity	$2\mathbb{Z}$ in $\mathbb{Z}$
Cyclic Group	Generated by a single element a.	Every element $= a^k, k \in \mathbb{N}$	$(\mathbb{Z}_n,+)$
Permutation Group	Set of all bijections on $\{1,2,\ldots,n\}$.	Order $= n!$	S_3, S_4
Normal Subgroup	$aN = Na$ for all $a \in G$.	Needed for quotient group	$A_n \trianglelefteq S_n$
Quotient Group	Set of cosets G/N when $N \trianglelefteq G$.	Operation $(aN)(bN) = abN$	$\mathbb{Z}/2\mathbb{Z}$
Homomorphism	Map preserving operation.	$\ker f$ normal, $\mathrm{Im} f$ subgroup	$\phi:\mathbb{Z}\to\mathbb{Z}_n$, $\phi(k)=k \bmod n$
Isomorphism	Bijective homomorphism.	Structure preserving	$\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$
Automorphism	Isomorphism from $G \to G$.	Symmetry of structure	In $\mathbb{Z}_n$, each automorphism is $x \mapsto kx$ with $\gcd(k,n)=1$

Important Examples of Groups

No.	**Group**	Description	Cyclic	Abelian	Normal Subgroups	Abelian Subgroups	Cyclic Subgroups	Key Point
1	$(\mathbb{Z}, +)$	Integers under addition	✓	✓	All $n\mathbb{Z}$	All	All	Infinite cyclic
2	$\mathbb{Z}_n$	Integers mod n	✓	✓	All	All	All	Finite cyclic
3	S_3	Permutations of 3 elements	–	–	A_3	A_3	$\langle(12)\rangle$, $\langle(123)\rangle$	Smallest non-abelian
4	D_4	Symmetries of square	–	–	$\langle r^2\rangle$	Some	$\langle r\rangle$, $\langle r^2\rangle$	Dihedral (order 8)
5	Q_8	Quaternion group	–	–	$\langle -1\rangle$	$\langle -1\rangle$, $\langle i\rangle$	$\langle i\rangle$, $\langle j\rangle$, $\langle k\rangle$	All subgroups normal
6	V_4	Klein four group	–	✓	All	All	All	Not cyclic, abelian
7	A_4	Even permutations of 4 elements	–	–	V_4	Few	Some	Order 12
8	$\mathbb{Z}_2 \times \mathbb{Z}_3$	Direct product	✓	✓	All	All	All	$\cong \mathbb{Z}_6$
9	$GL(n, \mathbb{R})$	Invertible $n \times n$ matrices	–	–	Infinitely many	Infinitely many	Infinitely many	$\text{SL}_n(\mathbb{R}) \trianglelefteq GL_n^+(\mathbb{R}) \trianglelefteq GL_n(\mathbb{R})$
10	$SL(n, \mathbb{R})$	$n \times n$ real matrices with $\det(A) = 1$	–	–	Infinitely many	Infinitely many	Infinitely many	Subgroup of $GL(n, \mathbb{R})$
11	D_n	Symmetry group of regular n-gon	–	–	$\langle r^k\rangle$	Some	Some	Non-abelian for $n > 2$
12	$(\mathbb{R}, +)$	All real numbers under addition	✓	✓	All subgroups of the form $r\mathbb{Z}$ ($r \in \mathbb{R}$)	All	All	No proper finite subgroups
13	C_n	Complex nth roots of unity	✓	✓	All	All	All	$\langle e^{2\pi i/n}\rangle$, cyclic of order n

Legend: ✓ = yes; "–" = no/limited. $\langle x\rangle$ is the cyclic subgroup generated by x.

Named Theorems

- **Lagrange's Theorem:** If G is a finite group and H is a subgroup of G, then the order of H divides the order of G. In particular, the order of every element of G divides $|G|$.
- **Cauchy's Theorem:** If a prime p divides the order of a finite group G, then G contains an element of order p.
- **First Isomorphism Theorem:** If $\phi : G \to H$ is a homomorphism, then $G/\operatorname{Ker}\phi \cong \operatorname{Im}\phi$.
- **Second Isomorphism Theorem:** If A is a subgroup and N a normal subgroup of G, then $AN/N \cong A/(A \cap N)$.
- **Third Isomorphism Theorem:** If N and K are normal subgroups of G with $K \subseteq N$, then $(G/K)/(N/K) \cong G/N$.
- **Cayley's Theorem:** Every group G is isomorphic to a subgroup of the symmetric group on G.
- **First Sylow Theorem:** If p^k divides $|G|$, then G has a subgroup of order p^k.
- **Second Sylow Theorem:** Any two Sylow p-subgroups of G are conjugate in G.
- **Third Sylow Theorem:** The number n_p of Sylow p-subgroups divides $|G|$ and satisfies $n_p \equiv 1 \pmod{p}$
- **Structure Theorem for Finite Abelian Groups:** Every finite abelian group is a direct product of cyclic groups of prime-power order.

Key Theorems

- Subgroups of a cyclic (Abelian) group are cyclic (Abelian); number of elements of order d in a cyclic group is $\varphi(d)$. Every cyclic group is Abelian.
- $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic $\iff$ $\gcd(m, n) = 1$; then $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$.
- For $|G| = p$ (prime), G is cyclic; V_4 is the smallest non cyclic group. S_3 is the smallest non-abelian group.
- If $a \in$ a group G & $\operatorname{ord}(a) = m$, then $\operatorname{ord}(a^k) = \dfrac{m}{\gcd(m,k)}$. If H and K are finite subgroups of a group G, then $|HK| = \dfrac{|H|\,|K|}{|H \cap K|}$.
- In any group, the intersection of normal subgroups is normal, but their union need not be a subgroup.
- If a group has exactly one subgroup of a given order, that subgroup is always normal in G.