

VU LEARNING HUB

vulearninghub.xyz

HIGHLIGHTED HANDOUT

MTH5210

Group Theory

MTH5210 by VU Learning HUB

Prepared for VU students • Free study resources

<https://vulearninghub.xyz>

MTH5210

Group Theory

Lecture-Wise Study Handout
Virtual University of Pakistan

11 lectures • prepared for exam study 

Table of Contents

1. Binary Operations and the Group Axioms
2. Elementary Properties: Identity, Inverses, Order
3. Subgroups and the Subgroup Test
4. Cyclic Groups
5. Permutation Groups: S_n and A_n
6. Cosets and Lagrange's Theorem
7. Normal Subgroups and Factor Groups
8. Homomorphisms and Isomorphisms
9. The Isomorphism Theorems
10. Group Actions and the Class Equation
11. Direct Products, Classification and Sylow Preview

About This Course

Group theory is the mathematical study of symmetry. A group is a set equipped with an operation satisfying a few simple axioms — yet this spare structure governs the symmetries of crystals, the solvability of equations, and the conservation laws of physics.

This handout builds the subject step by step: binary operations, the group axioms, subgroups, cyclic groups, permutations, cosets and Lagrange's theorem, normal subgroups and factor groups, homomorphisms and the isomorphism theorems, and an introduction to group actions. Definitions, theorems with proof sketches, worked examples and exam pointers accompany each lecture. 

Lecture 1: Binary Operations and the Group Axioms

Learning Objectives

- Define binary operations
- Verify the group axioms

A binary operation $*$ on a set G assigns to each pair (a, b) a result $a * b$ in G — closure is built into the definition. Familiar examples: addition on integers, multiplication on non-zero reals, composition of functions, matrix multiplication. Non-examples: subtraction on natural numbers ($1 - 3$ is not natural), division on integers.

A group is a set G with a binary operation satisfying four axioms: closure (already in the operation), associativity $((a*b)*c = a*(b*c))$, identity (an element e with $a*e = e*a = a$ for all a), and inverses (for each a , an element a^{-1} with $a*a^{-1} = a^{-1}*a = e$). An abelian group additionally satisfies commutativity ($a*b = b*a$).

Checking the axioms is the basic skill: $(\mathbb{Z}, +)$ is an abelian group; $(\mathbb{Q}^*, \times)$ is abelian; the set of $n \times n$ invertible matrices $GL(n, \mathbb{R})$ under multiplication is non-abelian for $n \geq 2$ — matrix multiplication does not commute. Very important: always verify all four axioms; most student errors come from assuming inverses exist.

Key Definitions

Group is defined as a set with a binary operation satisfying closure, associativity, identity and inverses

Abelian group is defined as a group whose operation commutes: $a*b = b*a$ for all a, b

Key Points — very important for exams

Binary operation: pairs $\rightarrow$ element of the set (closure included).

Four axioms: closure, associativity, identity, inverses; abelian adds commutativity.

Examples: $(\mathbb{Z}, +)$, $(\mathbb{Q}^*, \times)$ abelian; $GL(n, \mathbb{R})$ non-abelian; $(\mathbb{N}, +)$ fails inverses.

Review Questions

- ? Is subtraction a binary operation on $\mathbb{Z}$? On $\mathbb{N}$?
- ? Show matrix multiplication is associative but not commutative.

Section Summary

Four axioms define a group — check all four, every time.

Exam Pointers

- $\rightarrow$ Verify the group axioms for $(\mathbb{Z}, +)$ and explain why $(\mathbb{N}, +)$ fails.

Lecture 2: Elementary Properties: Identity, Inverses, Order

Learning Objectives

- Prove elementary group properties
- Compute element orders

Elementary consequences follow from the axioms alone. The identity is unique: if e and e' both act as identities, $e = e * e' = e'$. Each element's inverse is unique, and $(a^{-1})^{-1} = a$. Cancellation holds: $a * b = a * c$ implies $b = c$ (multiply by a^{-1} on the left) — and the one-sided version gives that equations $a * x = b$ have the unique solution $x = a^{-1} * b$.

Powers are defined naturally: $a^n = a * a * \dots * a$ (n times), $a^0 = e$, $a^{-n} = (a^{-1})^n$; the laws $a^m * a^n = a^{m+n}$ and $(a^m)^n = a^{mn}$ hold. The order of an element a is the smallest positive n with $a^n = e$ (infinite if none exists): in $(\mathbb{Z}_6, +)$, the element 2 has order 3 since $2+2+2 = 0 \pmod 6$.

These facts are the working toolkit: uniqueness of identity/inverses, cancellation, and order computations appear in nearly every proof. A very important exam habit: when stuck, return to the axioms — most elementary results are two lines from cancellation. 

Key Definitions

Order of an element is defined as the smallest positive n with $a^n = e$; infinite if no such n exists

Key Points — very important for exams

Identity and inverses are unique; cancellation holds; $a * x = b$ solves uniquely.

Powers: $a^m * a^n = a^{m+n}$; order = smallest n with $a^n = e$.

In $(\mathbb{Z}_6, +)$: $\text{ord}(2) = 3$, $\text{ord}(5) = 6$ — compute via repeated addition.

Review Questions

- ? Prove $(a * b)^{-1} = b^{-1} * a^{-1}$.
- ? Find all elements of order 2 in $\mathbb{Z}_8$ under addition.

Section Summary

Uniqueness, cancellation and order — the toolkit for everything that follows.

Exam Pointers

→ Prove uniqueness of identity and inverses; compute orders in $\mathbb{Z}_6$.

Lecture 3: Subgroups and the Subgroup Test

Learning Objectives

- Test subsets for subgroup status
- Describe centres and centralizers

A subgroup H of G is a non-empty subset closed under the operation and inverses — equivalently, a group in its own right under the same operation. The subgroup test: H is a subgroup iff $a*b^{-1}$ is in H for all a, b in H (one step). Finite non-empty subsets need only closure: in a finite set, closure forces inverses.

Examples: $(\mathbb{Z}, +)$ sits inside $(\mathbb{Q}, +)$ inside $(\mathbb{R}, +)$; the even integers $2\mathbb{Z}$ form a subgroup of $\mathbb{Z}$; the rotations form a subgroup of the symmetries of the square; the trivial subgroup $\{e\}$ and G itself are always subgroups. Non-examples: the odd integers are not a subgroup of $(\mathbb{Z}, +)$ — odd + odd = even breaks closure.

The centre $Z(G) = \{z : zg = gz \text{ for all } g\}$ and the centralizer of an element are important subgroups: the centre measures how abelian a group is ($Z(G) = G$ iff G is abelian). Intersections of subgroups are subgroups; unions generally are not — a favourite true/false trap.

Key Definitions

Subgroup is defined as a non-empty subset H of G forming a group under the same operation

Key Points — very important for exams

Subgroup test: $a*b^{-1}$ in H for all a, b in H ; finite sets need only closure.

Examples: $2\mathbb{Z} < \mathbb{Z}$; rotations $<$ symmetries of square; $\{e\}$ and G always.

Centre $Z(G)$ measures abelianness; intersections of subgroups are subgroups.

Review Questions

? Is $\{\text{odd integers}\}$ a subgroup of $(\mathbb{Z}, +)$? Why?

? Prove the intersection of two subgroups is a subgroup.

Section Summary

Subgroups are groups-within-groups — test with one step, watch closure.

Exam Pointers

→ State and apply the subgroup test; give subgroup and non-subgroup examples.

Lecture 4: Cyclic Groups

Learning Objectives

- Recognize cyclic groups
- Find subgroups and generators

A group G is cyclic if some element g generates it: $G = \langle g \rangle = \{g^n : n \in \mathbb{Z}\}$. The integers $(\mathbb{Z}, +)$ are infinite cyclic, generated by 1 (and by -1); $\mathbb{Z}_n$ is cyclic of order n , generated by 1. Every cyclic group is abelian — but not conversely: $\mathbb{Z}_2 \times \mathbb{Z}_2$ (the Klein four-group) is abelian yet no single element generates all four.

The structure theorem: every infinite cyclic group is isomorphic to $\mathbb{Z}$; every finite cyclic group of order n is isomorphic to $\mathbb{Z}_n$. So cyclic groups are completely classified — there is essentially one of each size. Subgroups of cyclic groups are cyclic: the subgroups of $\mathbb{Z}_n$ correspond to divisors of n — $\mathbb{Z}_{12}$ has subgroups of orders 1,2,3,4,6,12.

Generators are characterized: in $\mathbb{Z}_n$, the element k generates iff $\gcd(k,n) = 1$. Thus $\mathbb{Z}_{12}$ is generated by 1, 5, 7, 11 — four generators, matching Euler's $\phi(12) = 4$. Counting generators via the ϕ function is a standard exam computation. ☰

Key Definitions

Cyclic group is defined as a group generated by a single element: $G = \{g^n : n \in \mathbb{Z}\}$

Key Points — very important for exams

Cyclic = one generator; $\mathbb{Z}$ and $\mathbb{Z}_n$ are the models; cyclic implies abelian.

Classification: infinite cyclic $\cong \mathbb{Z}$; order- n cyclic $\cong \mathbb{Z}_n$; subgroups of cyclic are cyclic.

$\mathbb{Z}_n$ generated by k iff $\gcd(k,n)=1$; count = $\phi(n)$.

Review Questions

? Is $\mathbb{Z}_2 \times \mathbb{Z}_2$ cyclic? Justify.

? List all subgroups of $\mathbb{Z}_{18}$.

Section Summary

Cyclic groups are fully classified — one per size — with divisor-linked subgroups.

Exam Pointers

→ Classify cyclic groups; find all subgroups and generators of $\mathbb{Z}_{12}$.

Lecture 5: Permutation Groups: S_n and A_n

Learning Objectives

- Compute with permutations
- Describe alternating groups

A permutation of $\{1, \dots, n\}$ is a bijection of the set; the set S_n of all permutations under composition forms the symmetric group of degree n , of order $n!$. Every permutation factors into transpositions (2-cycles): e.g. $(1\ 3\ 2) = (1\ 3)(3\ 2)$. A permutation is even or odd according as its transposition count is even or odd — parity is well-defined.

The sign is a homomorphism: $\text{sign}(\sigma \tau) = \text{sign}(\sigma) \cdot \text{sign}(\tau)$. The even permutations form the alternating group A_n , a subgroup of S_n of order $n!/2$. A_3 is cyclic of order 3; A_4 (order 12) famously has no subgroup of order 6 — the classic counterexample to the converse of Lagrange's theorem.

Permutations model symmetry concretely: the symmetries of an equilateral triangle form $D_3 \cong S_3$ (order 6); the Cayley theorem (later) shows every group sits inside some S_n . Cycle notation, parity and A_n are computational essentials — practise multiplying permutations until fluent.

Key Definitions

Symmetric group S_n is defined as the group of all permutations of n objects under composition, of order $n!$

Alternating group A_n is defined as the subgroup of even permutations in S_n , of order $n!/2$

Key Points — very important for exams

S_n : $n!$ permutations under composition; every permutation = product of transpositions.

Parity is well-defined; even permutations form A_n of order $n!/2$.

A_4 has no subgroup of order 6 — converse of Lagrange is false.

Review Questions

? Write $(1\ 2\ 3)(2\ 4)$ as transpositions; is it even or odd?

? Why does A_4 refute the converse of Lagrange?

Section Summary

Permutations concretize symmetry; parity splits S_n into the alternating half.

Exam Pointers

→ Multiply permutations in cycle notation; determine parity; describe A_4 's anomaly.

Lecture 6: Cosets and Lagrange's Theorem

Learning Objectives

- Work with cosets
- Prove and apply Lagrange

For $H \leq G$, the left coset $aH = \{ah : h \text{ in } H\}$ partitions G : distinct cosets are disjoint, all have $|H|$ elements, and their union is G . The number of cosets is the index $[G:H] = |G|/|H|$. Cosets are the tool for counting — they turn subgroup structure into arithmetic.

Lagrange's theorem: if G is finite and $H \leq G$, then $|H|$ divides $|G|$. Proof sketch: the cosets partition G into equal-sized blocks, so $|G| = [G:H] \cdot |H|$. Corollaries: every element's order divides $|G|$ (apply to $\langle a \rangle$); every group of prime order is cyclic; $a^p = e$ for all a implies structure constraints.

Applications are immediate: a group of order 15 must have elements of orders dividing 15 — and in fact is cyclic; S_3 (order 6) can have subgroups only of orders 1,2,3,6. But as A_4 shows, divisors need not occur as subgroup orders — Lagrange gives necessity, not sufficiency.

Key Definitions

Index $[G:H]$ is defined as for finite $H \leq G$, the number of cosets of H in G , equal to $|G|/|H|$

Lagrange's theorem is defined as $|H|$ divides $|G|$ for finite groups — proved via coset partitioning

Key Points — very important for exams

Cosets aH partition G into equal blocks of size $|H|$; index = $|G|/|H|$.

Lagrange: $|H|$ divides $|G|$ — counting via partitions.

Corollaries: element orders divide $|G|$; prime-order groups are cyclic; converse false (A_4).

Review Questions

? List possible subgroup orders of a group of order 30.

? Prove every group of order p (prime) is cyclic.

Section Summary

Cosets count: subgroup sizes must divide the group — arithmetic constraining structure.

Exam Pointers

→ Prove Lagrange's theorem and deduce that groups of prime order are cyclic.

Lecture 7: Normal Subgroups and Factor Groups

Learning Objectives

- Test normality
- Build quotient groups

A subgroup N is normal ($N \triangleleft G$) if $gNg^{-1} = N$ for all g — equivalently, left and right cosets coincide. Normal subgroups are exactly the kernels of homomorphisms and the subgroups by which we can quotient. All subgroups of abelian groups are normal; subgroups of index 2 are always normal.

The factor (quotient) group G/N consists of cosets with operation $(aN)(bN) = abN$ — well-defined precisely because N is normal. Examples: $\mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}_2$; the quotient collapses N to the identity, measuring G modulo N . The natural map $\pi: G \rightarrow G/N$ is a surjective homomorphism with kernel N .

Normality is the gateway to structure theory: simple groups (no non-trivial proper normal subgroups) are the atoms — A_n is simple for $n \geq 5$, and the classification of finite simple groups is one of mathematics' great theorems. Exam skill: test normality via conjugation or index-2.

Key Definitions

Normal subgroup is defined as a subgroup N with $gNg^{-1} = N$ for all g — equivalently, cosets multiply consistently

Factor (quotient) group G/N is defined as the group of cosets of a normal subgroup under $(aN)(bN) = abN$

Key Points — very important for exams

Normal: invariant under conjugation; all subgroups of abelian groups; index-2 always normal.

G/N : cosets as elements; well-defined iff N normal; $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

Simple groups (e.g. A_n , $n \geq 5$) are the atoms of group theory.

Review Questions

? Why is every subgroup of an abelian group normal?

? Describe the elements of $\mathbb{Z}/4\mathbb{Z}$ as cosets.

Section Summary

Normal subgroups let us divide groups — quotients measure structure modulo the subgroup.

Exam Pointers

→ Test subgroups for normality; construct $\mathbb{Z}/6\mathbb{Z}$'s quotient by $\langle 2 \rangle$.

Lecture 8: Homomorphisms and Isomorphisms

Learning Objectives

- Work with homomorphisms
- Test isomorphism

A homomorphism $\phi: G \rightarrow H$ satisfies $\phi(ab) = \phi(a)\phi(b)$ — it preserves the operation. The kernel $\ker \phi = \{g : \phi(g) = e\}$ is a normal subgroup; the image is a subgroup of H . The determinant map $GL(n, \mathbb{R}) \rightarrow \mathbb{R}^*$ and the sign map $S_n \rightarrow \{\pm 1\}$ are canonical examples; $\phi(n) = n \bmod m$ maps $\mathbb{Z}$ onto $\mathbb{Z}_m$.

An isomorphism is a bijective homomorphism — groups are isomorphic ($G \cong H$) when they have identical structure under relabelling. Invariants distinguish non-isomorphic groups: order, abelianness, element orders, centre size. $\mathbb{Z}_4$ is not isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$: $\mathbb{Z}_4$ has an element of order 4, the Klein group does not.

Cayley's theorem: every group G is isomorphic to a subgroup of S_G (permutations of its own elements) — via left multiplication. So permutation groups are universal: studying subgroups of S_n studies all groups. This is why S_n mastery pays off everywhere.

Key Definitions

Homomorphism is defined as an operation-preserving map: $\phi(ab) = \phi(a)\phi(b)$; its kernel is normal

Isomorphism is defined as a bijective homomorphism — a structure-preserving relabelling of groups

Key Points — very important for exams

Homomorphism preserves operation; kernel normal; image a subgroup.

Isomorphic = structurally identical; invariants (order, abelianness, element orders) test it.

Cayley: every group embeds in a symmetric group — permutations are universal.

Review Questions

? Find kernel and image of $\det: GL(2, \mathbb{R}) \rightarrow \mathbb{R}^*$.

? Prove any two groups of order 3 are isomorphic.

Section Summary

Homomorphisms compare groups; isomorphisms identify them; Cayley embeds all in permutations.

Exam Pointers

→ Define homomorphism, kernel, isomorphism; prove $\mathbb{Z}_4$ not $\cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Lecture 9: The Isomorphism Theorems

Learning Objectives

- State the isomorphism theorems
- Identify quotients via homomorphisms

The fundamental theorem of homomorphisms (first isomorphism theorem): if $\phi: G \rightarrow H$ is surjective with kernel K , then $G/K \cong \text{im } \phi$ — the quotient by the kernel is exactly the image. It is the bridge between quotients and maps: $\mathbb{Z}/\langle n \rangle \cong \mathbb{Z}_n$ via reduction mod n ; the sign map gives $S_n/A_n \cong \mathbb{Z}_2$.

The second (diamond) isomorphism theorem: for $H \leq G$ and $N \trianglelefteq G$, $HN/N \cong H/(H \cap N)$. The third: for $K \trianglelefteq G$, $N \trianglelefteq G$ with $K \leq N$, $(G/K)/(N/K) \cong G/N$ — quotients of quotients collapse. The correspondence theorem completes the picture: subgroups of G/N correspond bijectively to subgroups of G containing N .

These theorems are the working machinery of classification: to identify a mysterious quotient, find a surjective map with the right kernel. Exam strategy: when asked to prove $G/N \cong H$, define $\phi: G \rightarrow H$, prove homomorphism, compute kernel = N , apply the first isomorphism theorem.

Key Definitions

First isomorphism theorem is defined as $G/\ker \phi \cong \text{im } \phi$ — the quotient by the kernel equals the image

Key Points — very important for exams

First: $G/\ker \phi \cong \text{im } \phi$ — identify quotients via surjective maps.

Second (diamond): $HN/N \cong H/(H \cap N)$; third: quotients of quotients collapse.

Correspondence: subgroups of $G/N \leftrightarrow$ subgroups of G containing N .

Review Questions

- ? Use the first isomorphism theorem on $\phi: Z \rightarrow Z_n$.
- ? State the correspondence theorem.

Section Summary

The isomorphism theorems turn quotient puzzles into homomorphism constructions.

Exam Pointers

- State the three isomorphism theorems; prove $S_n/A_n \cong Z_2$.

Lecture 10: Group Actions and the Class Equation

Learning Objectives

- Work with group actions
- Apply the class equation

A group action is a homomorphism $G \rightarrow S_X$ — G permuting a set X . The orbit of x is $\{g \cdot x\}$; the stabilizer is $\{g : g \cdot x = x\}$; orbits partition X , and the orbit–stabilizer theorem gives $|\text{orbit}| = [G : \text{stabilizer}]$. The regular action (G on itself by multiplication) proves Cayley's theorem.

The class equation applies the conjugation action: $|G| = |Z(G)| + \sum [G : C(g)]$ over non-central representatives. Since each index divides $|G|$, this forces structure: every non-trivial p -group has non-trivial centre — the key lemma for classifying groups of order p^2 (all abelian) and p^3 .

Burnside's lemma counts orbits under symmetry — e.g. distinct necklaces under rotation: average the fixed points over group elements. Group actions thus connect abstract groups to counting, geometry and chemistry (molecular symmetry). Very important: actions make groups concrete — always ask what the group permutes.

Key Definitions

Orbit is defined as the set $\{g \cdot x : g \in G\}$ — the points reachable from x under the action

Class equation is defined as for the conjugation action, $|G| = |Z(G)| + \sum [G : C(g)]$ — forcing p -group structure

Key Points — very important for exams

Action = homomorphism to permutations; orbits partition; $|\text{orbit}| = [G : \text{stabilizer}]$.

Class equation constrains finite groups: non-trivial p -groups have non-trivial centres.

Burnside's lemma counts symmetric configurations; actions concretize groups.

Review Questions

? What are the orbits of D_4 acting on a square's vertices?

? Why must a group of order p^2 be abelian?

Section Summary

Groups act by permuting — and the class equation turns actions into structure theorems.

Exam Pointers

→ State orbit–stabilizer; prove p -groups have non-trivial centre via the class equation.

Lecture 11: Direct Products, Classification and Sylow Preview

Learning Objectives

- Classify finite abelian groups
- Preview Sylow theory

Direct products combine groups: $G \times H$ with componentwise operation; $Z_2 \times Z_2$ is the Klein four-group. Finite abelian groups are completely classified: every finite abelian group is a product of cyclic p -groups — e.g. abelian groups of order 12 are Z_{12} and $Z_2 \times Z_6$ (equivalently $Z_2 \times Z_2 \times Z_3$). The invariant-factor and elementary-divisor decompositions are the two standard forms.

Semidirect products generalize: $N \rtimes H$ where H acts on N by automorphisms — dihedral groups D_n = rotations $\rtimes$ reflection. This builds all the small non-abelian groups and is the language of group extensions.

Sylow's theorems (preview): for $|G| = p^n \cdot m$ (p not dividing m), subgroups of order p^n exist, are all conjugate, and their number n_p satisfies $n_p \equiv 1 \pmod{p}$ and $n_p \mid m$. Sylow theory classifies groups of many orders — e.g. groups of order 15 are cyclic — and is the natural next course after this one.

Key Definitions

Fundamental theorem of finite abelian groups is defined as the classification: finite abelian groups are products of cyclic p -groups

Key Points — very important for exams

$G \times H$ componentwise; Klein four = $Z_2 \times Z_2$; finite abelians = products of cyclic p -groups.

Semidirect products (D_n) build non-abelian groups via actions.

Sylow: p -subgroups exist, are conjugate, counted by $n_p \equiv 1 \pmod{p}$, $n_p \mid m$.

Review Questions

? List abelian groups of order 8 up to isomorphism.

? Show a group of order 15 is cyclic using Sylow.

Section Summary

Products and quotients assemble and disassemble groups — classification is the payoff.

Exam Pointers

→ Classify abelian groups of order 36; state Sylow's theorems' conclusions for order 15.

Glossary of Key Terms

Group — a set with a binary operation satisfying closure, associativity, identity and inverses

Abelian group — a group whose operation commutes: $a*b = b*a$ for all a, b

Order of an element — the smallest positive n with $a^n = e$; infinite if no such n exists

Subgroup — a non-empty subset H of G forming a group under the same operation

Cyclic group — a group generated by a single element: $G = \{g^n : n \in \mathbb{Z}\}$

Symmetric group S_n — the group of all permutations of n objects under composition, of order $n!$

Alternating group A_n — the subgroup of even permutations in S_n , of order $n!/2$

Index $[G:H]$ — for finite $H \leq G$, the number of cosets of H in G , equal to $|G|/|H|$

Lagrange's theorem — $|H|$ divides $|G|$ for finite groups — proved via coset partitioning

Normal subgroup — a subgroup N with $gNg^{-1} = N$ for all g — equivalently, cosets multiply consistently

Factor (quotient) group G/N — the group of cosets of a normal subgroup under $(aN)(bN) = abN$

Homomorphism — an operation-preserving map: $\phi(ab) = \phi(a)\phi(b)$; its kernel is normal

Isomorphism — a bijective homomorphism — a structure-preserving relabelling of groups

First isomorphism theorem — $G/\ker \phi \cong \text{im } \phi$ — the quotient by the kernel equals the image

Orbit — the set $\{g \cdot x : g \in G\}$ — the points reachable from x under the action

Class equation — for the conjugation action, $|G| = |Z(G)| + \sum [G:C(g)]$ — forcing p -group structure

Fundamental theorem of finite abelian groups — the classification: finite abelian groups are products of cyclic p -groups