SC421: Introduction to Modern Algebra **Course content**

DA-IICT, B.Tech,

Objective:
To introduce the rich field of groups, rings and fields in algebra. To look at the set of polynomials as rings and their roots in extensions of field. To get introduced to Galois Theory.

Pre-requisite
Number systems: Integers, rational numbers, Real numbers and Complex numbers.
Groups, Linear Algebra.
Evaluation:
Two Midsemester Test 20% + 20%
Endsemester Test 50%
Attendance 10%

Outcome:
Students learn the intersting process of creating a field through quotient rings of polynomial rings. The beautiful connection between roots of polynomials and the group of automotphisms on the fields. This is the essence of Galois theory.

P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12
	X								X		X

Course Outline

1. Groups:
   Basic Definitions, Subgroups, Cosets, Normal Subgroups, Lagrange's Theorem, Isomorphism, Homomorphism, Quotient groups.

2. Rings:
   Definition, types of rings , zero divisors , integral domains, Fields, Characteristic of a field.

3. The number system:
   Examples of Rings and Fields in the number systems.

4. Polynomials:
   Definition, The division Algorithm, Factorization.

5. Quotient Rings:
   Homomorphisms, Ideals, Quotient rings, Quotient rings of Polynomial Rings, Factorization and Ideals.

6. Field Extensions:
   Simple Extensions, Degree of Extension, Splitting Fields, Finite Fields.

7. Galois Theory:
   Galois Group, Separability and Normality, Fundamental Theorem of Galois Theory, Solvability by radicals.

8. Geometric Constructions:
   Doubling of a cube, trisecting an angle, squaring a circle, constructible numbers.

Books

1. Topics in Algebra
   I.N. Herstein

2. Abstract Algebra, An Introduction
   Thomas W. Hungerford

Groups:

Natural numbers. $\{1, 2, 3, \ldots\}$.

Binary operation $+$

$4 + 3 = 7$. $7 \in N$.

$4, 3, 2$

$(4+3) = 7 + 2 = 9$

$4 + (3+2) = 4 + 5 = 9$.

$4 + x = 4$? Include $0 \rightarrow$

$x = 0$.

The idea of removing an object is called the inverse of a number

Introduce the idea of inverse of a number.

$0 + (-4) = -4$ We include -ve natural number.

Group: A set G with a binary operation $*$ that satisfies the following:

1) G is closed under $*$
   $\forall\ a, b \in G$, $a * b = c \in G$.
2) $\forall\ a, b, c \in G$, $(a * b) * c = a * (b * c)$
   $*$ is associative in G.
3) $\exists\ e \in G$ such that $a * e = a$ and $e * a = a$.
   e is the $*$ identity in G.
4) $\forall\ a \in G$ $\exists\ b \in G$ such that
   $a * b = e$, and $b * a = e$.

There are the Group axioms.

Groups: A group G is a set, together with a binary operation $*$, satisfying:

1) G is closed under $*$,
2) $*$ is associative.
3) G has a $*$ identity $\quad a * e = e * a = a$
4) Every element in G has a $*$ inverse. $\quad a * b = b * a = e$

$a * b \equiv ab.$

Eg: $\langle \mathbb{Z}, + \rangle$, $\langle \mathbb{Q}, + \rangle$ Groups.

$\langle \mathbb{Z}, \times \rangle$ Not a group.

Every element doesn't have an inverse.

$\langle \mathbb{Q}, \times \rangle$ Mult. inverse of $\frac{p}{q}$ is $\frac{q}{p}$.

If $p = 0$ then inverse doesn't exist.

This is not a group.

$\mathbb{Q}^* = \mathbb{Q} - \{0\}$: $\langle \mathbb{Q}^*, \times \rangle$ is a group.

Is it possible that $\frac{p_1}{q_1} \times \frac{p_2}{q_2} = 0$ where $\frac{p_1}{q_1}, \frac{p_2}{q_2} \neq 0$.

Not possible

$\therefore \langle \mathbb{Q}^*, \times \rangle$ is a group.

$G = \{ a + b\sqrt{2} \; ; \; a, b \in \mathbb{Q} \}$

$\langle G, + \rangle$; $(a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{2}$.

Addn. is closed : (follows from $\langle \mathbb{Q}, + \rangle$ is a gmp)

Associativity : (- - -)

Identity : $0 + 0\sqrt{2}$: $(a + b\sqrt{2}) + (0 + 0\sqrt{2}) = a + b\sqrt{2}$.

$(0 + 0\sqrt{2}) + (a + b\sqrt{2}) = a + b\sqrt{2}$

$(a + b\sqrt{2}) \xrightarrow{\text{Inverse.}} \underbrace{(-a) + (-b)\sqrt{2}}_{\in G}$.

This set is denoted as $\mathbb{Q}(\sqrt{2})$

$G = \mathbb{Q}(\sqrt{2})$. $\langle \mathbb{Q}(\sqrt{2})^*, \times \rangle$ $\mathbb{Q}(\sqrt{2})^* = \mathbb{Q}(\sqrt{2}) - \{0\}$

$\langle \mathbb{Q}(\sqrt{2})^*, \times \rangle$?

$(a+b\sqrt{2}) \times (c+d\sqrt{2}) = (ac+2bd) + (ad+bc)\sqrt{2}$

Closed!

Mult^n is associative (because of $\mathbb{R}$).

Identity ? $1 + 0\sqrt{2} = 1$

$(a+b\sqrt{2}) * (1+0\sqrt{2}) = a+b\sqrt{2}$.

Inverse? $(a+b\sqrt{2}) * (c+d\sqrt{2}) = 1 + 0\sqrt{2}$.

Doesn't exist if $a+b\sqrt{2} = 0$, i.e $a=b=0$.

$(a+b\sqrt{2}) \cdot (c+d\sqrt{2}) = 1$

$(a+b\sqrt{2})^{-1} = \frac{1}{a+b\sqrt{2}} \cdot \frac{a-b\sqrt{2}}{a-b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2}$

$\frac{a}{a^2-2b^2} + \frac{(-b)}{a^2-2b^2}\sqrt{2}$.

$a^2 - 2b^2 = 0$? $\Rightarrow \frac{a^2}{b^2} = 2 \Rightarrow \frac{a}{b} = \sqrt{2}$. ✗

$\therefore (\mathbb{Q}(\sqrt{2}))^*$ is group under multiplication

$a * e = a = e * a$.

$\longrightarrow$ $a * a^{-1} = e = a^{-1} * a$.

In most number system $a * b = b * a$.

Set of all permutations on 3 elements : S_3

$A = \{1, 2, 3\}$, $S_3 = \left\{ \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}, \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} \right\}$

$e \quad \tau_1 \to \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$ $\quad \sigma$ $\quad \sigma^2 = \sigma \circ \sigma$

$\tau_3 \quad \tau_2$.

Set of permutation: S_3, is closed under composition.

Permutation is a one-one onto function on A.

$\therefore$ Composition is possible

$$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} \qquad \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$$

$$\sigma \circ \tau_3 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = \tau_1$$

$\sigma^2 \circ \tau_3 = \tau_2$.

Call $\tau_3 \equiv \tau$ then $\sigma\tau = \tau_1$, $\sigma^2\tau = \tau_3$

$S_3 := \{ e, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau \}$

$\tau^2 = e$ $\quad (\sigma\tau)^2 = e$.

$\sigma\tau \neq \tau\sigma$ But $\sigma\tau = \tau\sigma^2$.

$(\sigma\tau)^2 = (\sigma\tau)(\sigma\tau) = (\tau\sigma^2)(\sigma\tau) = \tau \cdot \tau = \tau^2 = e$.

$\mathbb{Z}_4$: $\{0, 1, 2, 3\}$ with $\oplus_4$ (addition mod. 4).

$1 \oplus_4 2 = 3$, $1 \oplus 3 = 0$, $3 \oplus 2 = 1$ - - -

0 is the identity 1 is the a.d.d. inverse of 3.

This is a group. Group table.

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Z_4 $\oplus_4$.

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

0 - identity 1 & 3 are inverses of each other.

2 is its own inverse.

$K_4 = \{e, a, b, c\}$

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

There are the only two groups with 4-elements.

Rotations about x, y, z axis by 180°.

Operations are commutative.

Def: Abelian Group:
If $ab = ba$ $\forall$ $a, b \in G$ then. G is called an abelian group.

Set of all. real $m \times n$ matrices and the operation is matrix addition.

$$A + B = B + A .$$

This is an. abelian Group.

Under multiplication we can only have $n \times n$. (square) matrices in our set.:
We should also have. multiplicative inverses.
So determinant of the - matrices. must not be zero.
Associative. but not commutative
This is a. non- abellian. Grp.: General linear grp. of order n.
with real entries. $GL_n(\mathbb{R})$, $GL_n(\mathbb{C})$

Lemma 1: If $\langle G, * \rangle$ be a group, then.

(i) The identity element in $\langle G, * \rangle$ is unique.

(ii) Every $a \in G$ has a unique inverse.

(iii) $\forall\ a \in G$; $(a^{-1})^{-1} = a$.

(iv) $\forall\ a, b \in G$; $(ab)^{-1} = b^{-1} a^{-1}$

-2 in additive group. is 2^{-1}

Lemma 1. Let $\langle G, * \rangle$ be a group. Then the following statements are true

(i) The identity element in $\langle G, * \rangle$ is unique.

(ii) Every $a \in G$ has a unique inverse

(iii) $\forall a \in G, \quad (a^{-1})^{-1} = a$

(iv) $\forall a, b \in G, \quad (ab)^{-1} = b^{-1} a^{-1}$

Proof (i): Let e and e' be two identities in G.

Then $e * e' = e'$ (since e is the identity)

and $e * e' = e$ (since e' is the identity)

$\therefore \quad e = e'$

Lemma 2: Let $a, b \in G$. Then $\exists$ a unique solution to $a * x = b$ and $y * a = b$ in G.

Also $\forall\ a, x, y \in G$

$a * x = a * y \Rightarrow x = y$ (left cancellation law)

and $x * a = y * a \Rightarrow x = y$ (right cancellation law)

Proof: (Exercise)

$a * x = b$

a^{-1} exists in G

$\therefore\ a^{-1} * (a * x) = a^{-1} * b$

$(a^{-1} * a) * x = a^{-1} * b.$

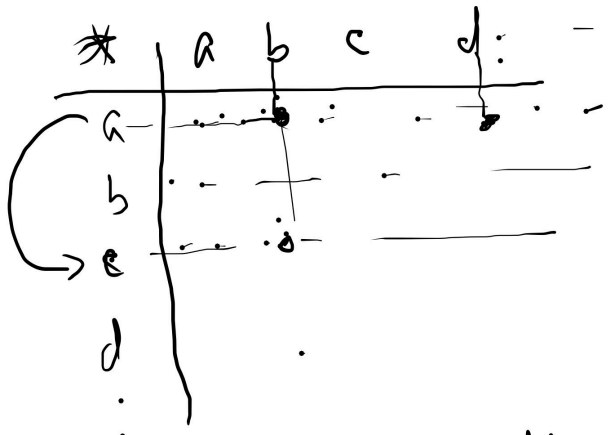
$\therefore\ e * x = a^{-1} * b.$

$\therefore\ x = a^{-1} * b.$

$a * x = a * y$

$\Rightarrow\ a^{-1} * (a * a) = a^{-1} * (a * y)$

$\Rightarrow\ x = y$



$a * b = a * d$

$\Rightarrow b = d$

Every row in the group table doesn't have any group element more than once.

All elements of the group must occur in every row.

Same for columns.

Every row and column of a group table is a permutation of the group elements.

Def: Order of a group: The number of elements in a finite group. is called the order of the grp.

$o(\mathbb{Z}_4) = 4$, $o(K_4) = 4$.

$o(S_3) = 6$

Consider an element $a \in G$.

Construct $a * a = a^2$, $a * a * \cdots * a$ (i times) $= a^i$

After a finite step (say m), $a^m = e$.

Then m is called the order of a.

$a * a * \dots * a$ (n times) $= a^n$.

If the group is $\langle \mathbb{Z}, + \rangle$ then.

$3 + 3 + \dots + 3$ (8 times) = denoted as 3^8

Denote the inverse of an element a. by a^{-1}

In $\langle \mathbb{Z}, + \rangle$ 2^{-1} is -2.

$a^i = (a * a \dots * a)$ (i times)

$(a^i)^{-1} = ?$ $\qquad (a * b)^{-1} = b^{-1} * a^{-1}$.

$(a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1}$.

$= a * e * a^{-1} = a * a^{-1} = e$.

$(b^{-1} * a^{-1}) * (a * b) = e$.

$(a * a \dots * a) * (a^{-1} * a^{-1} * \dots * a^{-1}) = e$.

$(a^{-1})^i = a^{-i}$

$\therefore$ Inverse of a^i in a group is a^{-i}.

$a^i * (a^j)^{-1} = a^{i-j} = (a * a \dots * a) * (a^{-1} * a^{-1} \dots * a^{-1})$

(i times) (j times)

2). Subgroups. Let $\langle G, * \rangle$ be a group.

A non-empty subset H of G is called a subgroup of $\langle G, * \rangle$ if $\langle H, * \rangle$ is a group.

Eg. 1 Group $\langle \mathbb{Z}, + \rangle$

Consider the set $2\mathbb{Z} = \{\ldots -6, -4, -2, 0, 2, 4, 6, \ldots\}$

Thm is a subgroup of $\langle \mathbb{Z}, + \rangle$

$\langle 2\mathbb{Z}, + \rangle$

Eg. 2 : Let $S = \{0, 1, 2, \ldots\}$.

Not a subgroup of $\langle \mathbb{Z}, + \rangle$.

$S = \{\ldots -5, -3, -1, 0, 1, 3, 5, \ldots\}$.

Not closed under addition.

$\langle \mathbb{Z}, + \rangle$ is a subgroup of $\langle \mathbb{Q}, + \rangle$ is a subgroup of $\langle \mathbb{R}, + \rangle$.

$\langle \mathbb{R}, + \rangle$ is a subgroup of $\langle \mathbb{C}, + \rangle$.

Eg: M be the set of 2×2 real matrices with determinant 1.

M is a subgroup of $GL_2(\mathbb{R})$

$$\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$$

Lemma 3: A non-empty subset H of a group $\langle G, * \rangle$ is a subgroup of G iff
(i) H is closed under $*$
(ii) $a \in H \Rightarrow a^{-1} \in H$.

Eg: Consider $\langle \mathbb{Z}, + \rangle$. $n \in \mathbb{Z}$
$n\mathbb{Z} = \{ nz \mid z \in \mathbb{Z} \}$ is a subgroup of $\langle \mathbb{Z}, + \rangle$.

$4\mathbb{Z} = \{ \ldots -12, -8, -4, 0, 4, 8, 12, \ldots \}$.

$\{ \ldots, -9, -6, -3, 0, 3, 6, 9, \ldots \}$

(i) Consider $nk_1, nk_2 \in n\mathbb{Z}$
$nk_1 + nk_2 = n \cdot (k_1 + k_2) \in n\mathbb{Z}$
$\because k_1 + k_2 \in \mathbb{Z} \Rightarrow n(k_1 + k_2) \in n\mathbb{Z}$
$\therefore n\mathbb{Z}$ is closed under $+$

(ii) Consider $nk \in n\mathbb{Z}$.
Then $n(-k) \in n\mathbb{Z}$
$nk + n(-k) = n(k + (-k)) = n \cdot 0 = 0$.
$\therefore n(-k)$ is the add. inv. of nk.

$\therefore n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$

Consider $\{\ldots -10, -8, -7, -6, -4, -2, 0, 2, 4, 5, \ldots\}$

All subgroups of $\langle \mathbb{Z}, + \rangle$ are of the type $n\mathbb{Z}$.

Cyclic groups: $\langle \mathbb{Z}, + \rangle$ is a cyclic group. (infinite)

All subgroups of a cyclic group is cyclic.

$\langle \mathbb{Z}_5, \oplus \rangle = \{\underline{1}, \underline{1} \oplus \underline{1} = 2, 3, 4, 5 \equiv 0, \underline{1}\}$

This is finite cyclic group. $\{1, 2, 3, 4, 0\}$.

$\langle \mathbb{Z}, + \rangle$ is an infinite cyclic group

$\ldots \quad a^{-2}, a^{-1}, e, a, a^2, a^3 - - - - -$

$\ldots$ This is an infinite cyclic group

Lemma 4: If H is a non-empty finite subset of a group $\langle G, * \rangle$ and H is closed under $*$ then H is a subgroup of G.

Proof: H is non-empty.

$\exists\ a \in H$.

$\therefore a^2, a^3, \ldots \in H$

But H is finite. $\Rightarrow \exists\ p > r$ such that

$a^p = a^r \Rightarrow a^{p-r} = e$

$\therefore e \in H \Rightarrow a^{(p-r)-1} = a^{-1}$

$\therefore a^{-1} \in H$

By Lemma 3. this is a subgroup.

Lagrange's Theorem.

$\mathbb{Z}_{12} = \{0, 1, 2, \ldots, 11\}$ $\quad \langle \mathbb{Z}_{12}, \oplus \rangle$

Consider subgroup : $\{3, 6, 9, 0\} \longrightarrow \langle 3 \rangle$

$1 \notin \langle 3 \rangle$

$1 \oplus \langle 3 \rangle = \{4, 7, 10, 1\}$

$2 \oplus \langle 3 \rangle = \{5, 8, 11, 2\}$

$\langle 3 \rangle$, $1 \oplus \langle 3 \rangle$, $2 \oplus \langle 3 \rangle$. are disjoint sets.

$|\langle 3 \rangle|$ divides $|\mathbb{Z}_{12}|$

This is true. in general.

Let G be a finite group. and H be a subgroup of G.
If H is a proper subgroup. $\exists$ a in G such that $a \notin H$.

Consider aH

Let $x \in H \cap aH$ $\qquad H = \{h_1, h_2, \ldots, h_k\}$

$\Rightarrow$ $x = h_1 \in H$ also $x = ah_2 \in aH$

$\therefore h_1 = ah_2 \Rightarrow h_1 h_2^{-1} = a$

$\therefore a \in H$ since $h_1 h_2^{-1} \in H$.

$\Rightarrow\Leftarrow$

$\therefore H \cap aH = \phi$ $\qquad (ah_1 = ah_2 \Rightarrow h_1 = h_2.)$

$\therefore$ If $\exists$ $b \in G$ such that $\underline{b \notin H}$ & $\underline{b \notin aH}$.

Consider bH.

Let $x \in aH \cap bH$.

Then $\exists$ $h_1, h_2 \in H$ such that $x = ah_1 = bh_2$

$\Rightarrow ah_1h_2^{-1} = bh_2h_2^{-1} = b$

$\therefore b = ah_1h_2^{-1} = ah_3 \in \underline{aH}$ $\Rightarrow\Leftarrow$.

$\therefore H, aH, bH$ are disjoint.

This construction continues till all elements in G are exhausted.

$\therefore |G| = |H| \times m$ where m is a +ve integer.

$|H| \mid |G|$. $\qquad o(H) \mid o(G)$. Lagrange's theorem.

For infinite grp. $G = \langle \mathbb{Z}, + \rangle$

$H = 3\mathbb{Z} = \{ \ldots -6, -3, 0, 3, 6, \ldots \}$

$1 + 3\mathbb{Z} = \{ \ldots, -5, -2, 1, 4, 7, \ldots \}$

$2 + 3\mathbb{Z} = \{ \ldots -4, -1, 2, 5, 8, \ldots \}$

Lagrange's Theorem: If H is a subgroup of a finite group G. then $o(H) \mid o(G)$.

We define the index of H in G. denoted as $[G:H]$ as

$$[G:H] = \frac{o(G)}{o(H)}$$

This is the number of left (right) cosets of H in G.

Even if G is infinite we can define the index as the number of distinct cosets. (right or left) of H in G.

G is $\langle \mathbb{R}, + \rangle$ Infinite.

H is $\langle \mathbb{Z}, + \rangle$

$\mathbb{Z} = \{ \ldots -5, -4, -3, -2, -1, 0, 1, 2, 3, \ldots \}$

$0.1 + \mathbb{Z} = \{ \ldots -4.9, -3.9 \ldots 0.1, 1.1, 2.1, \ldots \}$.

Infinite number of distinct cosets.

$\{ x + \mathbb{Z} \mid 0 \leq x < 1 \}$

So index $[G : H]$ can be infinite.

Cyclic groups: (we know)

$\mathbb{Z}_4$: $\{0, 1, 2, 3\}$ 1 generates $\mathbb{Z}_4$. $\langle 1 \rangle$

$\langle 2 \rangle = \{2, 0\}$ not a generator of $\mathbb{Z}_4$.

BW a sub group.

$\langle 3 \rangle = \{3, 2, 1, 0\} = \mathbb{Z}_4$

$\langle 3 \rangle$ is also a generator of $\mathbb{Z}_4$.

In $\mathbb{Z}_n$, an element a is a generator of $\mathbb{Z}_n$ if.

g.c.d $(a, n) = 1$.

Consider a group G:

Let $a \in G$. Construct: $\{a, a^2, a^3, \ldots, \underline{a^k = e}\} = H$.

Then H is closed under the group operation.

H is called the subgroup generated by a.

This is a cyclic subgroup. denoted as $\langle a \rangle$

$$o(\langle a \rangle) = k.$$

By Lagrange's Theorem $k \mid o(G)$

$a^k = e \Rightarrow$ $\boxed{a^{o(G)} = e}$ → corollary to Lagrange's theorem.

If $k = o(G)$, then G is a cyclic group and a is a generator of G.

Corollary 1: Let $a \in G$. Then $a^{o(G)} = e$.

Corollary 2: If $o(G) = p$ (a prime) then G is cyclic.

Reason: If G has a subgrp H such that

$$1 < o(H) < (o(G) = p)$$

Then $o(H) \mid p$. $\Rightarrow\Leftarrow$ since p is prime.

So order of every element in G is p and.

G is cyclic.

$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$.

Only subgroup of $\mathbb{Z}_5$ are $\{0\}$ and $\mathbb{Z}_5$

(Trivial subgroups)

Normal Subgroups:

Given a subgroup H of G. the cosets are.

aH. $\longrightarrow$ left multiplication.

We can also consider right multiplication.

If G is non-abelian then. $aH \neq Ha$. in general.

Permutation group $S_3 = \{ e, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau \}$

$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ $\quad \tau\sigma^2$. $\quad \tau\sigma$

$H = \{ e, \tau \}$ is a subgroup of G.

Left cosets of $H = \{e, \tau\}$: $\left\{ \begin{pmatrix} e \\ \tau \end{pmatrix}, \begin{pmatrix} \sigma \\ \sigma\tau \end{pmatrix}, \begin{pmatrix} \sigma^2 \\ \sigma^2\tau \end{pmatrix} \right\} = \{ H, \sigma H, \sigma^2 H \}$.

Right Cosets of H : $\left\{ \begin{pmatrix} e \\ \tau \end{pmatrix}, \begin{pmatrix} \sigma \\ \tau\sigma \end{pmatrix}, \begin{pmatrix} \sigma^2 \\ \tau\sigma^2 \end{pmatrix} \right\} = \left\{ \begin{pmatrix} e \\ \tau \end{pmatrix}, \begin{pmatrix} \sigma \\ \sigma^2\tau \end{pmatrix}, \begin{pmatrix} \sigma^2 \\ \sigma\tau \end{pmatrix} \right\}$

The set of left cosets are different from right cosets.

Consider $N = \{e, \sigma, \sigma^2\} \longrightarrow$ subgroup of S_3

$$\{(e, \sigma, \sigma^2); (\tau, \tau\sigma, \tau\sigma^2)\} = \{(e, \sigma, \sigma^2); (\tau, \sigma^2\tau, \sigma\tau)\}.$$

Left Cosets of N :

Right Cosets of N :

$$\{(e, \sigma, \sigma^2); (\tau, \sigma\tau, \sigma^2\tau)\}$$

The left and right Cosets are same.

Subgroups where left and right sets of Cosets are same. are called normal subgroups.

Let N be subgroup of G.
Construct the set $aN.a^{-1}$ → Prove that this is also a subgroup of G.

In general aNa^{-1} may be a different subgroup than N.

If $aNa^{-1} = N$ then ⇒ $aN = N.a$
This happens $\forall a \in G$ i.e. left cosets are equal to the right cosets.
Such subgroups are called normal subgroups

Def: (normal subgroups)
A subgroup N of G is called a normal subgroup if:
$aNa^{-1} \subseteq N$. $\forall\ a \in G$.

Eg (Trivial) For any G, the trivial subgroups.
$\{e\}$ and G are normal subgroups.

Lemma: N is a normal subgroup of G if and only if:
$aNa^{-1} = N$. $\forall\ a \in G$.

Proof: if part (easy)
$aNa^{-1} = N \Rightarrow aNa^{-1} \subseteq N$.
So N is normal.

Only if: Given $aNa^{-1} \subseteq N$. (N is normal)

Tne. $\forall a \in G$. $\therefore N \subseteq a^{-1}Na$. (Mult a^{-1} from left & a from right)

$\therefore a^{-1}Na \subseteq N$.

$\therefore N \subseteq aNa^{-1}$

$\therefore aNa^{-1} = N$. $\leftarrow$

Also the defining statement for normal subgroups.

Def: N is a normal subgroup of G. if $aNa^{-1} \subseteq N \ \forall a \in G$

Lemma: $aNa^{-1} = N$.

Lemma: A subgroup. N of G is normal if and only if every left coset of N is also a right coset of N.

Proof: (only if part) Let N be normal

$\therefore aNa^{-1} = N \quad \forall a \in G$.

$\therefore aN = Na$

(if part): Every left coset is also a right coset:

$\therefore aN = Nb$ ←

$a \in aN \Rightarrow a \in Nb$.

Does $a \in Na$. ? Yes.

$\therefore N_a$ and N_b are not disjoint.

$\therefore N_a = N_b$.

$\therefore aN = Na$.

$\therefore aNa^{-1} = N$.

$\therefore N$ is a normal subgroup of G.

If H and K are two subgroups of G
Is HK also a subgroup of G ?

$HK = \{ h * k \mid h \in H, k \in K \}$.

If $HK = KH$ then HK is a subgroup of G.
(If and only if) (Exercise.)

If one of the subgroups (H & K) is normal then.
$HK = KH \Rightarrow$ HK is a subgroup of G.

Is HK a normal subgroup ?
Yes. if both H and K are normal.

Structure in the set of cosets

Lemma: N is a normal subgroup of G iff the product of two left (right) cosets is also a left (right) coset.

Lemma.: N is a normal subgroup of G iff the product of two right (left) cosets of N in G. is also a right (left) coset of N in G.

Proof: (only if) part: Given N is a normal subgroup of G.

Consider two right cosets Na and Nb

Consider $Na \cdot Nb = N(aN)b = N(Na)b$.

(N is Normal)

$= (NN)ab = N(ab)$

This is also a right coset.

Left cosets are also right cosets since N is normal.

∴ It is proved also for Left cosets.

(if part): Product of two right cosets is a right coset.

$\therefore \quad Na \cdot Nb = Nc = (Nab)$ to be shown

$a \in Na \cdot \; b \in Nb. \Rightarrow ab \in Na\,Nb = Nc.$

$\therefore ab \in Nc.$

$ab \in N(ab) \Rightarrow Nab = Nc.$

$\therefore \quad Na \cdot Nb = Nab.$

Consider $b = a^{-1}$. Then.

$Na\,Na^{-1} = N$ (We will show $aNa^{-1} \subset N.$)

Let $x \in aNa^{-1}$. then.

$Nx \subseteq N.$

$x \in Nx \Rightarrow x \in N.$

$\therefore \quad aNa^{-1} \subseteq N. \Rightarrow$ N is a normal subgroup of G.

The collection of cosets of a normal subgroup is closed under set multiplication.
We denote this collection as G/N.

Proposition 6: If N is a normal subgroup of G, then G/N forms a group under multiplication of cosets.
This group is called the quotient group of G by N.

Proof: Closed is done.
Mult. is associative: $(N_a N_b)\cdot N_c = N_a (N_b N_c)$.

$N_{ab}\cdot N_c$ $\qquad$ $N_a \cdot N_{bc}$.

$N_{(ab)c} = N_{a(bc)}$

$N \cdot N_a = N_e \cdot N_a$.

$= N_{(e\cdot a)} = N_a$.

$\therefore$ G/N forms a group.

$$o(G/N) = \frac{o(G)}{o(N)}.$$

Lemma: N is a normal subgroup of a group G iff.

$aN \cdot bN = \in N. = (ab)N.$

Proposition: The set of all cosets of a normal subgroup. forms a group under set multiplication. This group is denoted as G/N. called the quotient group.

$x + \mathbb{Z}$ $\quad 0 \leq x < 1$ is a coset of $\mathbb{Z}$ in $\langle \mathbb{R}, + \rangle$

$(x_1 + \mathbb{Z}) + (x_2 + \mathbb{Z}) = (x_1 + x_2) + \mathbb{Z}$ $\quad (aN) \cdot (bN) = (ab) \cdot N.$

$(\mathrm{mod}\ 1).$

Identity $= \mathbb{Z}$, Inverse of $x + \mathbb{Z}$? is $(1 - x) + \mathbb{Z}$

$\in [0, 1)$

$G = \mathbb{Z}$, $N = n\mathbb{Z}$ → is a subgroup of $\mathbb{Z}$

N is a normal

$4\mathbb{Z} = \{ \ldots -8, -4, 0, 4, 8, \ldots \}$.

$1 + 4\mathbb{Z} = \{ \ldots -7, -3, 1, 5, 9 \ldots \}$

$2 + 4\mathbb{Z} =$

$3 + 4\mathbb{Z} =$ }

Isomorphism: $\{4\mathbb{Z}, 1+4\mathbb{Z}, 2+4\mathbb{Z}, 3+4\mathbb{Z}\} \longrightarrow G/N$.

$\mathbb{Z}_4$. addition modulo 4.

Def: $\underline{b}$ is conjugate of $\underline{a}$ if $\exists\ x \in G$ such that

$$x a x^{-1} = b$$

If a basis transform through a matrix U

$B = \{e_1, e_2 - - -, e_n\} \rightarrow B' = \{e_1', e_2', - -, e_n'\}$.

$e_1' = U e_1$, $e_2' = U e_2$.

$$[A]_B \longrightarrow [A]_{B'}$$

$$U^{-1} [A]_B U = [A]_{B'}$$

If a is conjugate to b we represent this as a relation $a \sim b$.

This is an equivalence relation. (prove this).

The group elements gets partitioned into several equivalence classes $\longrightarrow$ conjugacy class.

Conjugacy class of an element a is $C(a)$

$$C(a) = \{ b \in G \mid \exists\, x,\ xax^{-1} = b \}.$$

$C(a)$ (conjugacy classes) are disjoint

These are not always of same size.

$C(e)$.

$\uparrow$

identity.