GOVERNMENT DEGREE COLLEGE, RAVULAPALEM
NAAC Accredited with 'B' Grade(2.61 CGPA)
(Affiliated to Adikavi Nannaya University)
Beside NH-16, Main Road, Ravulapalem-533238, East Godavari Dist., A.P, INDIA
E-Mail : jkcjyec.ravulapalem@gmail.com, Phone : 08855-257061
ISO 50001:2011, ISO 14001:2015, ISO 9001:2015 Certified College

GROUP THEORY

UNIT-1 GROUPS

B. SRINIVASARAO. LECTURER IN MATHS. GDC. RVPM.KONASEEMA

UNIT – 1: Syllabus

Binary Operation – Algebraic structure – semi group-monoid – Group definition and elementary properties Finite and Infinite groups – examples – order of a group. Compositiontables with examples.

Sets Relations

Definition (Set): A set is a collection of well-defined objects.

Examples:1 A = {1,2,3,4,5,6,7,} B = { a, b , c, d } are sets

Example:2 Collection of Mathematics books in the college library.

Example:3 Collection of those students in your college who secured more than 80% of marks in Annual examination.

Number system: The following sets are defined as:

1.The set of Natural numbers are defined by **N** = $\{1,2,3,4, \dots \dots \dots .., n, n+1, \dots ..\}$

2.The set of Integers are defined by **Z** = $\{\dots \dots \dots \dots \dots -3,-2,-1,0,1,2,3, \dots \dots \dots \dots\}$

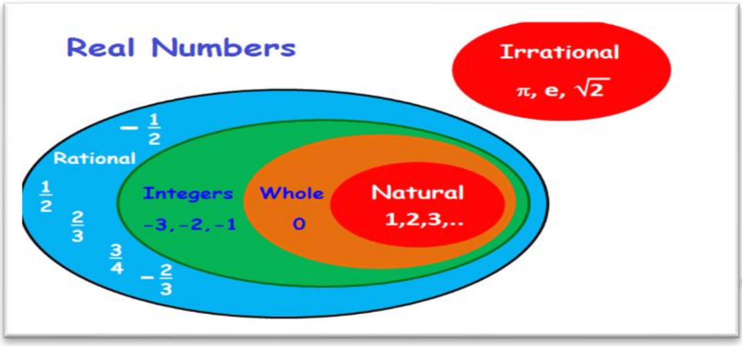
3.The set of rational numbers are defined by **Q** = $\{ \frac{p}{q} : p, q \in Z, q \neq 0 \}$

4.The set of Irrational numbers are **R - Q** = $\{ \sqrt{2}, \sqrt{3}, \sqrt{5}, \dots .. \pi, \dots \}$

5.The set of Real numbers are the union of set of Rationales and the set of Irrationals.

i.e., $\boldsymbol{R} = \boldsymbol{Q} \cup (\boldsymbol{R} - \boldsymbol{Q})$

6.The set of complex numbers are defined by $\mathbb{C} = \{x + iy : x, y \in R, i = \sqrt{-1} \}$



Complex Numbers

Real number system

Non-Empty set: A set A has at least one or more than one element is called a non-emptyset and is denoted by ≠φ.

Binary operation: An operation 0 is said to be binary on a non-empty set G if

for all a, b ∈ G then a 0 b ∈ G.

Example: Addition (+) is a binary operation on set of Naturals N but Subtraction (-) is not a binary operation on N.

Since for a = 5, b = 9 ∈ N then a + b = 5 + 9 = 14 ∈ N but a - b = 5 – 9 = -4 ∉ N

Algebraic Structure: -

A non-empty set together with one or more than one binary operation is called analgebraic structure.

Examples: -

1.**(R, +, × ·) .** is an Algebraic Structure where R is set of Real Numbers.

2.**(N, +) , (Z, +), (Q, +)** are algebraic structures but **(N, -) (Z, ÷)** are not an algebraic structures

Example: Division (÷) is not a binary operation on **Z**

Since for a = 2, b = 3 ∈ Z but 2 ÷ 3 = $\frac{2}{3}$ ∉ **Z.** Therefore < **Z, ÷ >** is not an Algebraic structure.

Therefore < **Z,** ÷ > is not an Algebraic Structure.

Example: Multiplication is a Binary operation on the set or Rational numbers Q

$$\textbf{For } a = \frac{2}{3} \quad b = \frac{5}{9} \ in\ Q\ then\ a.b = \frac{2}{3}.\frac{5}{9} = \frac{10}{27} \ \in Q$$

Therefore < Q, × > is an Algebraic Structure

Example: Division is a Binary operation on the set or Rational numbers Q Since

for $\boldsymbol{a = 7/9, b = 8/9\ then\ a \div b = 7/9 \div 8/9 = 7/9 \times 9/8 = 7/8 \in Q}$

Therefore < Q, ÷ > is an Algebraic Structure.

Definition (Group): A non-empty set $\boldsymbol{G}$ is said to be a Group w r t a Binary operation 0 if it satisfies the following properties

1.Closure Property : $\forall\ a, b \in$G $\Rightarrow$ $aob \in G$.

2.Associative Property : $a\ o\ (\ b\ o$ c) = $(a\ o\ b)\ o\ c\ \ \forall\ a, b, c \in G$

3 Identity Properties : For all a $\in G$ there exist an element e $\in G$ such that

$$a\ o\ e = e\ o\ a = a$$

' e ' is called identity w r t the operation o

4.Inverse Property : For all a $\in G$ there exist an element b $\in G$ such that

a 0 b = e = b 0 a

then b is the inverse element of a w r t operation 0

Note:1. In an additive Group the Identity is o (zero) and the multiplicative Identity is 1 (one)

Note :2. In the **Additive** Group G the **Inverse** element of $\boldsymbol{a}$ is – $\boldsymbol{a}$ and in the **Multiplicative** group G the inverse element of $\boldsymbol{a\ is\ a^{-1}}$

Example: The set of integers **Z** = $\{\ldots\ldots\ldots - 3, -2, -1, 0, 1, 2, 3, \ldots\ldots\ldots\ldots\}$ form a group with respect to addition (+) .

Solution: Given that **Z** = $\{\ldots\ldots\ldots - 3, -2, -1, 0, 1, 2, 3, \ldots\ldots\ldots\ldots\}$

1.Closure Property:

Clearly the addition of any two integers is also an integer therefore closure law exists.

That is for a = 5 b = - 8 in Z then a + b = 5 + (-8) = -3 $\in$ Z

2.Associative property:

For any a, b, c $\in Z\ then\ a + (b + c) = (a + b) + c$

3.Identity Property:

For all a $\in Z\ there\ exist\ 0 \in Z\ such\ that\ a + 0 = a = 0 + a$

and 0 is the additive identity in Z.

4.Inverse Property:

For all $a \in Z$ *there exist* $-a \in Z$ *such that* $a + (-a) = 0 = (-a) + a$

And $-a$ is the additive Inverse of a in Z.

Groupoid:

A non – empty set G is said to be Groupoid wrt to given binary operation o if it satisfies Closure law i.e for all $a, b \in G \Rightarrow a0b \in G$

Example: **Z= {. . . . . . -3, -2 ,-1, 0, 1, 2, 3 ,.........}** is a Groupoid w r t – (Subtraction).

Semi-Group:

A non – empty set G is said to be a semi-group wrt to given Binary operation o if it satisfies 1. Closure 2. Associative laws.

Example:

The set of Natural numbers **N** = $\{1,2,3,4, \ldots \ldots \ldots .., n, n+1, \ldots ..\}$is a semi group wrt addition. Since Identity o is not in N.

Monoid:

A non – empty set G is said to be a Monoid wrt to given Binary operation o if it satisfies1. Closure 2. Associative and 3. Identity laws.

Example: **N** = $\{1,2,3,4, \ldots \ldots \ldots .., n, \ldots ..\}$ is a Monoid wrt Multiplication.

Since Inverse property is not existed in N. for a = 3 then $a^{-1} = \frac{1}{3}$ is not in N.

Note: The stanard Groups in the Number system are < Z, + >, < Q, + >, < Q -{0}, ×>

$< R, +>$, $< R - \{0\}, \times >$ < C, + > and , $< C - \{0\}, \times >$

Abelian Group:

A Group G is said to be Abelian w r t 0 *if it satisfies commutative property that is*

for all a , b in G then $a \circ b = b\, 0\, a$

Theorem: 1 - (Uniqueness of identity) Prove that every group has unique Identity.

Proof: If possible, suppose that e and e' are two identity elements in a group G.

Case-1: Let e = Identity and e' = element

$\therefore \quad e'e = e' = e e' --- (1)$ (Since $a e = a = e a$)

Let $e' = Identity \ and \ e = Element$

$\therefore \quad e\,e' = e = e'e \quad ---(2)$

$From\ (1)\ and\ (2)\quad e' = e\,e' = e$

$\therefore\ e' = e$

$Hence\ the\ Identity\ element\ is\ unique.$

Theorem: 2 (Uniqueness of inverse)

Prove that the inverse of each element of a group is unique.

Proof: For all a ϵ G to show that it has unique inverse.

Suppose b, c are two inverse elements of a in G

$If\ b\ is\ inverse\ of\ a\ we\ get\ \ ab = e = b\,a \quad ----(1)$

$If\ c\ is\ inverse\ of\ a\ we\ get\ \ ac = e = c\,a \quad ----(2)$

$To\ show\ that\ b = c$

As $b = eb(\because\ e\ is\ the\ Identity\ )$

$= (ca)\,b(\because\ from\ (2)\ e = ca\ )$

$= c(ab) \because\ Associate\ property\ in\ G$

$= c(e) \because\ from\ (1)$

$= c \therefore\quad b = c\ .\ Therefore, inverse\ element\ is\ unique.$

Theorem:3 (Cancellation laws)

For any $a \neq 0, b, c$ in a group G. Prove that

1.If $a\,b = a\,c \Rightarrow b = c$ (Left cancellation)

2.If $b\,a = c\,a \Rightarrow b = c$ (Right cancellation)

Proof: Let $a\,b = a\,c$

$\Rightarrow\ a^{-1}$ (a b) = a^{-1} (a c) $(since\ a \in G\ by\ inverse\ law\ a^{-1} \in G)$

⇒ (a^{-1}a) b = (a^{-1}a) c (by Associative in G)

⇒ (e)b =(e) c (by Inverse property in G)

⇒ b = c since e is the identity

Also, if $ba = ca$

⇒ $(ba)\,a^{-1} = (ca)\,a^{-1}$ (since a ∈ G by inverse law a^{-1} ∈ G)

⇒ $b\,(a\,a^{-1}) = c\,(a\,a^{-1})$ (by Associative in G)

⇒ $be = ce$ (by Inverse property in G)

⇒ $b = c$

Hence cancellation laws hold in a group G

Theorem:4 (Reversion rule) :

In a Group G, Prove that $(ab)^{-1} = b^{-1}a^{-1}$. for all a, b in G.

Proof: Let $c = b^{-1}a^{-1}$. for all a, b in G

Consider $c(ab) = b^{-1}a^{-1}(ab)$

$= b^{-1}(a^{-1}a)b$ (By Associative in G)

$= b^{-1}(e)b$ (By Inverse property in G)

$= b^{-1}b$ (Since e is the identity)

$= e$

$\therefore c(ab) = e$ ----------(1)

Also $(ab)c = (ab)b^{-1}a^{-1}$

$= a(bb^{-1})a^{-1}$ (By Associative in G)

$= a(e)a^{-1}$ (By Inverse property in G)

$= aa^{-1}$ (Since e is the identity)

$= e$

$(ab)c = e$ -------------(2)

from (1) and (2)

$\therefore c(ab) = e = (ab)c \Rightarrow c = (ab)^{-1}$ ($\because ab = e = ba \Rightarrow b = a^{-1}$)

Hence $(ab)^{-1} = b^{-1}a^{-1}$

Theorem:5 Let G be a group and $a \in G$ then prove that $(a^{-1})^{-1} = a$.

Proof: - By the definition of the group G.

For all $a \in G$ by Inverse property in G $\exists\, a^{-1}$ in G such that

$aa^{-1} = e = a^{-1}a$ ------------(1)

Let $b = a^{-1} \in G$ by inverse property in G $\exists$ an element $b^{-1} \in G$ such that

$bb^{-1} = e = b^{-1}b$ But $b = a^{-1}$

$\therefore (a^{-1})(a^{-1})^{-1} = e = (a^{-1})^{-1}(a^{-1})$ --------(2)

From (1) & (2) $aa^{-1} = (a^{-1})^{-1}(a^{-1})$

Apply Right cancellation to a^{-1} We get $(a^{-1})^{-1} = a$.

Theorem: **If G is a group and $a, b \in G$ then the equations $ax = b$ ans $ya = b$ have unique solutions in G.**

Proof: As $ax = b \Rightarrow a^{-1}(ax) = a^{-1}b$ $\quad$ ($for\ a \in G \Rightarrow a^{-1} \in G$)

$\Rightarrow (a^{-1}a)x = a^{-1}b$ $\quad$ (by Associative in G)

$\Rightarrow e\,x = a^{-1}b$

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

Now LHS = $ax = a(a^{-1}b) = (aa^{-1})b = eb = b\ RHS$

It follows $x = a^{-1}b$ is the solution of $ax = b$

To show that $x = a^{-1}b$ is the unique solution of $ax = b$

Suppose $x_1\ and\ x_2$ are two such solutions of $ax = b$

$\therefore ax_1 = b \quad and \quad ax_2 = b$

$\Rightarrow ax_1 = ax_2$ and by left cancellation laws $x_1 = x_2$

Hence $x = a^{-1}b$ is the unique solution of $ax = b$

Similarly, to prove that $ya = b\ has\ y = ba^{-1}$ is the unique solution.

Theorem: **If G is a Semigroup and $a, b \in G$ the equations $ax = b\ and\ ya = b$ have solutions in G then prove that G is group.**

Proof: Assume that G is a Semigroup

Let $a \in G \Rightarrow a, a \in G$ $ax = a$ has a solution and $ae = a$ for some e $\in G$

Let $a, b \in G$ $ya = b$ has a solution and $e^1 a = b$ for some $e^1 \in G$

Now $be = (e'a)e = e'(ae) = e'a = b$

$\therefore e\ is\ the\ right\ identity\ in\ G$ Similarly, to find left identity.

For a$\in G\ and\ a, e \in G\ ax = e\ has\ a\ solution\ say\ a' \Rightarrow aa' = e\ for\ some\ a' \in G$

And hence $a' is\ the\ right\ inverse\ of\ a\ in\ G$

Similarly, to find left inverse in G

Hence G is a group

Problem:1 **Show that $G = \{a + b\sqrt{2} : a, b \in Q\}$ form an abelian group wrt Addition .**

Solution: Given $G = \{ a + b\sqrt{2} : a, b \in Q \}$

To show that $< G, + >$ form an abelian group.

1.Closure property: $\forall\ x = a_1 + b_1\sqrt{2}$ $\quad y = a_2 + b_2\sqrt{2} \in G$ then

$$x + y = (a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{2}$$

$= a' + b'\sqrt{2} \in G$ where $a' = (a_1 + a_2)$ and $b' = (b_1 + b_2) \in Q$ Closure property holds.

2.Associative property: Since all the elements in G are all Real numbers and $< R, + >$ is anAbelian Group.

Therefore, Associative holds in G . that is for all

$$x\, o\, (y\, o\, z) = (x\, o\, y)\, o\, z \qquad \forall\, x, y, z \in G$$

3.Identity Property : For all $x = a + b\sqrt{2}$ in $G\ \exists\ 0 = \mathbf{0 + 0\sqrt{2}} \in G$ such that

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

$$= a + b\sqrt{2} = x$$

Similarly $0 + x = x$ $\quad \therefore$ Identity element exist in G

4.Inverse Property: For all $x = a + b\sqrt{2}$ in $G\ \exists$ $\mathbf{-x = -a - b\sqrt{2}}$ $\in G$ such that

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

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

$$= 0 + 0\sqrt{2} = 0$$

Similarly $(-x) + x = 0$

5. Commutative Property : $\forall\ x = a_1 + b_1\sqrt{2}$ $\quad y = a_2 + b_2\sqrt{2}$ $\in G$ then

$$x + y = (a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{2}$$

$$= (a_2 + a_1) + (b_2 + b_1)\sqrt{2}$$

$$= y + x$$

$\therefore$ $< G, + >$ form an abelian group

Problem:2.

Show that the set of integers Z form a Group w r t the operation * defined by

$$\boldsymbol{a * b = a + b - 1} \text{ for all a, b in Z}$$

Solution: To show that $< Z, * >$ form a Group

1.Closure Property: For all $a, b \in Z \Rightarrow a + b \in Z$ and $-1 \in Z$

$$\Rightarrow a + b + (-1) \in Z$$

$$\Rightarrow a + b - 1 \in Z \quad (\text{Since } < Z, + > \text{ is a group })$$

$$\Rightarrow a * b \in Z.$$

2. Associative Property: For all a, b, c $\in Z$ then

To verify $a * (b * c) = (a * b) * c$.

$$LHS = a * (b * c) = a * (b + c - 1)$$
$$= a * x \quad where\ x = b + c - 1$$
$$= a + x - 1$$
$$= a + (b + c - 1) - 1$$
$$= a + b + c - 2$$

$$\boldsymbol{RHS = (a * b) * c = (a + b - 1) * c = y * c \ where\ y = a + b - 1}$$

$$= y + c - 1$$
$$= (a + b - 1) + c - 1$$
$$= a + b + c - 2$$
$$\therefore a * (b * c) = (a * b) * c$$

3. Existence of Identity: For all a $\in Z$ there is an element e $\in Z$ (to find) such that

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

If $\quad a * e = a \Rightarrow a + e - 1 = a$

$$\Rightarrow e - 1 = 0$$

$\Rightarrow e = 1 \in Z \quad is\ the\ Identity\ w\ r\ t\ \ *$

4. Existence of Inverse**:** For all a $\in Z$ there is an element x $\in Z$ (to find) such that

$$a * x = e = x * a$$

If $\quad a * x = e \Rightarrow a + x - 1 = 1$

$\Rightarrow x = 2 - a \in Z$ is the Inverse element of a w r t $*$ in Z

$< Z, * >$ form a Group.

Problem: 3 ***Show that the set of Rational numbers***

$Q_1 = Q - \{1\} form\ an\ abelian\ Group\ w\ r\ t\ the\ operation\ defined\ by$

$$a * b = a + b - ab\ for\ all\ a, b\ in\ Q_1$$

Solution: To show that $< Q_1, * >$ form an abelian Group

1.Closure Property: For all a, b $\in Q_1 \Rightarrow$ a + b $\in Q_1$ and ab $\in Q_1$

$\Rightarrow a + b \in Q_1$ and $- ab \in Q_1$

$\Rightarrow a + b + (-ab) \in Q_1$ (Since $< Q_1,+ >$ is a group)

$\Rightarrow a + b - ab \in Q_1$

$\Rightarrow a * b \in Q_1$

2.Associative Property: for all a,b,c $\in Q_1$ then to verify $a * (b * c) = (a*b) *c$

LHS $= a * (b * c) = a* (b + c - bc)$

$= a * x$ where $x = b + c - bc$

$= a + x - ax$

$= a + (b + c - bc) - a(b +c - bc)$

$= a + b + c -bc -ab -ac + abc.$

RHS $= (a * b)* c = (a + b - ab) * c$

$= y * c$ where $y = a + b - ab$

$= y + c - yc$

$= (a + b -ab) + c - (a + b -ab)c$

$= a + b + c - ab -ac-bc +abc$

$\therefore$ LHS = RHS

3.Existence of Identity: For all a $\in$ Q1 there is an element e $\in$ Q1 (to find) such thata $a * e = a = e * a$

If $a * e = a \Rightarrow a + e - a e = a$

$\Rightarrow e (1 - a) = 0$

$\Rightarrow e = 0 \in Q1$ is the Identity w r t $*$

4. Existence of Inverse: **For** all a $\in$ Q1 there is an element x $\in$ Z (to find) such thata

$$a * x = e = x * a$$

If $a * x = e \Rightarrow a + x - a x = 0$ (Since $e = 0$)

$\Rightarrow x(1 - a) = -a$

$\Rightarrow x = \frac{-a}{1-a}$ in Q1 is the Inverse element of a .

5. Commutative property: For all a , b $\in Q_1$ then

$$a * b = a + b - a b = b + a - b a = b * a$$

$< Q_1, * >$ form an Abelian Group

Problem:4 Show that the set of positive rational numbers Q^+ form an abelian group w r t a operation $*$ defined by $a * b = \frac{a\,b}{3}$ $for\ all\ a, b \in Q^+$

Solution: Given that $a * b = \frac{ab}{3}$ for all $a, b \in Q^+$

To show that $< Q^+, * >$ form an abelian group.

1. Closure property: for all $a, b \in Q^+$ and Q^+ is a group wrt multiplication

$\Rightarrow$ $a\,b \in Q^+$ and $\frac{1}{3} \in Q^+$

$\Rightarrow a\,b \,.\, \frac{1}{3} \in Q+$. since closure law in Q+.

$\Rightarrow \frac{ab}{3} \in Q+$

$\Rightarrow a * b \in Q^+$

$\therefore$ *Closure property exist.*

2.Associative property: for all a, b, c $\in Q^+$ then to verify $a * (b * c) = (a * b) * c$.

LHS $= a * (b * c) = a * \left(\frac{bc}{3} \right) = a * x$ where $x = \frac{bc}{3}$

$= \frac{ax}{3} = \frac{a\left(\frac{bc}{3}\right)}{3} = \frac{a(bc)}{9} = \frac{(ab)c}{9}$ since $a, b, c \in Q^+$

$= \frac{\left(\frac{ab}{3}\right)c}{3}$

$= \frac{(y)c}{3}$ where $y = \frac{ab}{3} = a * b$

$= y * c$

$= (a * b) * c =$ RHS $\therefore$ Associative property holds.

3. Identity property : for all $a \in Q^+$ we have an element (to find) $e \in Q^+$ such that

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

if $a * e = a \Rightarrow \frac{ae}{3} = a \Rightarrow$ $e = 3$ $\in Q^+$ is the identity wrt $*$

4.Inverse property: for all $a \in Q^+$ we have an element (to find) $x \in Q^+$ such that

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

if $a * x = e \Rightarrow \frac{ax}{3} = 3$ since $e = 3$

$\Rightarrow$ $x = \frac{9}{a}$ $\in Q^+$ is the inverse element of a wrt $*$

5. Commutative property : for all $a,b \in Q^+$

$a * b = \frac{ab}{3} = \frac{ba}{3} = b * a$ (since $a\,b = b\,a$ in Q^+).

Hence $< Q^+, * >$ form an abelian group.

Problem : Show that $G = \left\{A_{\alpha} = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} : \alpha \in Z\right\}$ is an abelian group wrt Matrix multiplication.

Solution:

To show that $G = \left\{A_{\alpha} = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} : \alpha \in Z\right\}$ is an abelian group wrt matrix multiplication.

1.Closure property: For all $A_{\alpha} = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$ $A_{\beta} = \begin{pmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{pmatrix}$ in G

Then $A_{\alpha} A_{\beta} = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}\begin{pmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{pmatrix}$

$$= \begin{pmatrix} \cos\alpha\cos\beta - \sin\alpha\sin\beta & -\cos\alpha\sin\beta - \sin\alpha\cos\beta \\ \sin\alpha\cos\beta + \cos\alpha\sin\beta & -\sin\alpha\sin\beta + \cos\alpha\cos\beta \end{pmatrix}$$

$$= \begin{pmatrix} \cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & \cos(\alpha+\beta) \end{pmatrix} = A_{\alpha+\beta} \in G$$

(Since $\alpha, \beta \in Z \Rightarrow \alpha + \beta \in Z$)

$\therefore$ $A_{\alpha} A_{\beta} = A_{\alpha+\beta}$.

2.Associative property: we know that in matrix multiplication for any three Matrices Associative property holds $\therefore$ Associative property exist.

3. Identity property: For all $A_{\alpha} = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$ there exist A_0 in G such that

$$A_{\alpha} A_0 = A_{\alpha+0} = A_{\alpha} \quad \text{and} \quad A_0 A_{\alpha} = A_{0+\alpha} = A_{\alpha}$$

$\therefore$ $A_0 = \begin{pmatrix} \cos 0 & -\sin 0 \\ \sin 0 & \cos 0 \end{pmatrix}$ is the identity

4.Inverse property: For all $A_{\alpha} = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$ there exist $A_{(-\alpha)}$ in G such that

$$A_{\alpha} A_{(-\alpha)} = A_{\alpha+(-\alpha)} = A_0 \quad \text{and} \quad A_{(-\alpha)} A_{\alpha} = A_{(-\alpha)+\alpha} = A_0$$

$\therefore$ $A_{(-\alpha)}$ is the inverse matrix of A_{α}.

5.Commutative property :

For all A_{α} , A_{β} in G then $A_{\alpha} A_{\beta} = A_{\alpha+\beta} = A_{\beta+\alpha} = A_{\beta} A_{\alpha}$

Hence $< G , . >$ is an abelian group

Problems: Show that the set of matrices $G = \left\{ \begin{pmatrix} x & x \\ x & x \end{pmatrix} : x \in Q - \{0\} \right\}$ is a group wrt matrix multiplication.

Solution:

1.Closure property: For all $A = \begin{pmatrix} a & a \\ a & a \end{pmatrix}$ $B = \begin{pmatrix} b & b \\ b & b \end{pmatrix}$ in G

Then

$$A\,B = \begin{pmatrix} a & a \\ a & a \end{pmatrix}\begin{pmatrix} b & b \\ b & b \end{pmatrix} = \begin{pmatrix} ab+ab & ab+ab \\ ab+ab & ab+ab \end{pmatrix} = \begin{pmatrix} 2ab & 2ab \\ 2ab & 2ab \end{pmatrix} \text{ in G}$$

(Since $a, b \in Q - \{0\} \Rightarrow a\,b \in Q - \{0\}$)

2.Associative property : We know that in matrix multiplication for any Three Matrices A, B, C in G $A (B C) = (A B) C$ holds

∴ Associative property exist.

3. Identity property:

For all $A = \begin{pmatrix} a & a \\ a & a \end{pmatrix}$ there exist $E = \begin{pmatrix} e & e \\ e & e \end{pmatrix}$ in G (to find) such that

$$A\,E = A = E\,A.$$

If $A\,E = A \Rightarrow \begin{pmatrix} a & a \\ a & a \end{pmatrix}\begin{pmatrix} e & e \\ e & e \end{pmatrix} = \begin{pmatrix} a & a \\ a & a \end{pmatrix}$

$$\Rightarrow \begin{pmatrix} 2ae & 2ae \\ 2ae & 2ae \end{pmatrix} = \begin{pmatrix} a & a \\ a & a \end{pmatrix}$$

$$\Rightarrow \mathbf{2ae = a \;\Rightarrow\; e = \tfrac{1}{2} \in Q - \{0\}}\;.$$

∴ Identity element $E = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$ in G Exist

4.Inverse property: For all $A = \begin{pmatrix} a & a \\ a & a \end{pmatrix}$ there exist $X = \begin{pmatrix} x & x \\ x & x \end{pmatrix}$ in G (to find)such that

$$A\,X = E = X\,A.$$

If $A\,X = E \Rightarrow \begin{pmatrix} a & a \\ a & a \end{pmatrix}\begin{pmatrix} x & x \\ x & x \end{pmatrix} = \begin{pmatrix} e & e \\ e & e \end{pmatrix}$

$$\Rightarrow \begin{pmatrix} 2ax & 2ax \\ 2ax & 2ax \end{pmatrix} = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$$

$$\Rightarrow 2\,ax = \tfrac{1}{2} \;\Rightarrow\; x = \tfrac{1}{4a} \in Q - \{0\}\,.$$

∴ Inverse of X is $X^{-1} = \begin{pmatrix} 1/4a & 1/4a \\ 1/4a & 1/4a \end{pmatrix}$ in G exist.

Hence < G, . > is a group .

Finite Groups

Definition: A group having finite number of elements then it is a finite group

Problem:1 Show that the set of cube roots of unity form a group wrt multiplication.

Solution: We know that the set of cube roots of unity

$$G = \{1, \omega, \omega^2\} \text{ where } \omega^3 = 1.$$

To Construct Multiplication Table For $G = \{1, \omega, \omega^2\}$

$\times$	**1**	$\boldsymbol{\omega}$	$\boldsymbol{\omega^2}$
1	**1**	ω	ω^2
$\boldsymbol{\omega}$	ω	ω^2	**1**
$\boldsymbol{\omega^2}$	ω^2	**1**	ω

1.Closure property: Using the composition table the multiplication of any two elements in G is also in G $\quad That\ is\ for\ all\ a, b \in G \Rightarrow a\,b \in G.$

Closure law exist.

2.Associative property: all the elements in G are complex numbers. But the set of complexnumbers satisfy associative.

$\therefore$ Associative exist in G.

3.Existence of Identity: Using the table

$1.1 = 1,\quad \omega.\ 1= \omega \quad$ and $\quad \omega^2\ .1= \omega^2$" 1"

is the identity in G.

4.Existence of Inverse: Using the table

$1.1 = 1 \quad \omega\ .\ \omega^2 =1 \quad$ and $\quad \omega^2 \cdot \omega = 1$Each element in G has inverse in G

Hence G is a group w r t multiplication.

Problems:2. Show that the set of 4^{th} roots of unity is a Group w r t multiplication

$$\mathbf{G} = \{ \mathbf{1}, -\mathbf{1}, \boldsymbol{i}, -\boldsymbol{i} \}$$

form a group wrt multiplication.

Solution: Given $G = \{1, -1, i, -i\}$ where $i^2 = -1$ and $i^3 = -i$ and $i^4 = 1$

To Construct Multiplication Table for G = $\{1, -1, i, -i\}$

$\times$	**1**	$-\mathbf{1}$	$\boldsymbol{i}$	$-\boldsymbol{i}$
1	**1**	-1	i	$-i$
$-\mathbf{1}$	-1	**1**	$-i$	i
$\boldsymbol{i}$	i	$-i$	-1	**1**
$-\boldsymbol{i}$	$-i$	i	**1**	-1

1. Closure property: Using the composition table the multiplication of any two elements in Gis also in G That is for all a, b $\in$ G $\Rightarrow$ a b $\in$ G.Closure law exist.
2. Associative property: All the elements in G are complex numbers.The set of complex numbers satisfies associative. $\therefore$ Associative exist in G.
3. Existence of Identity: Using the table

   1.1 = 1, (-1) 1= -1 $i.1 = i$ and $(-i).1 = -i$

   ' 1' is the identity in G.
4. Existence of Inverse: Using the table

   1.1 = 1 $(-1)(-1) = 1$, $i(-i) = 1$ and $(-i)(i) = 1$

   Each element in G has inverse in G

   Hence G is a group w r t multiplication.

Problem:3 In a Group G prove that if each element is inverse element of it self then it is abelian.

Solution: Let G is a group and for any $a \in G$ *then* $\boldsymbol{a\,a = e} \Rightarrow \boldsymbol{a = a^{-1}}$ **--------(1)**

And for any $b \in G$ *then* $\boldsymbol{b\,b = e} \Rightarrow \boldsymbol{b = b^{-1}}$ **--------(2)**

$\therefore$ *for any* $a, b \in G \Rightarrow$ *By closure law* $ab \in G$

Let $x = ab \in G$

From (1) $\boldsymbol{x = x^{-1}}$

$\Rightarrow ab = (ab)^{-1}$

$\Rightarrow ab = b^{-1}a^{-1}$

From (1) & (2) $ab = ba$ *and hence G is Abelian*

Problem:

Let G is a group then show that for all a, b $\in$ G $(ab)^2 = a^2b^2$ if and only if G isabelian.

Solution:

$\Rightarrow$ **Part** Suppose in a Group G for all a, b $\in$ G

$$(ab)^2 = a^2\ b^2$$

$$\Rightarrow (a\,b)(a\,b) = (a\,a)(bb)$$

$$\Rightarrow a\,(b\,a)\,b = a(a\,b)b \quad (\because\ Associativ\,e\,property)$$

$$\Rightarrow (b\,a)\,b = (a\,b)b \quad (\because\ by\ left\ cancellation)$$

$$\Rightarrow b\,a = (a\,b) \quad (\because\ by\ Right\ cancellation)$$

$$\Rightarrow G\ is\ abelian.$$

$\Leftarrow$ **Part**

Let G is abelian group. To show that for all a, b $\in$ G $(ab)^2 = a^2b^2$

LHS = $(ab)^2$ for all a, b $\in$ G

$= (a\,b)(a\,b)$

$= a\,(b\,a)\,b$ ($\because$ Associative)

$= a\,(a\,b)b$ ($\because$ G is abelian group)

$= (a\,a)(b\,b) = a^2b^2$ = RHS

Problem:

Prove that the set of n^{th} roots of Unity form a group w r t to multiplication of complex numbers.

Solution: $Let\quad x = \sqrt[n]{1} \Rightarrow x = 1^{1/n} = (\cos 0 + i\sin 0)^{1/n}$

$$= [\cos(2k\pi + 0) + i\sin(2k\pi + 0)]^{1/n} \quad for\ k = 0,1,2,3, \dots\dots\dots.$$

$$= [\cos 2k\pi + i\sin 2k\pi]^{1/n} \quad for\ k = 0,1,2,3, \dots\dots$$

$$x = [\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}] \quad for\ k = 0,1,2,3, \dots\dots$$

But $\cos\theta + \sin\theta) = e^{i\theta}$

$$\therefore\ x = e^{\frac{2k\pi i}{n}} \quad for\ k = 0,1,2,3, \dots$$

Put k = 0,1,2,3, ...$we\ get\ \ G = \{ e^{\frac{2(0)\pi i}{n}}, e^{\frac{2(1)\pi i}{n}}, e^{\frac{2(2)\pi i}{n}}, e^{\frac{2(3)\pi i}{n}} \dots\dots\dots\dots e^{\frac{2k\pi i}{n}} \}$

$$let\ \omega = e^{\frac{2\pi i}{n}}$$

$\therefore\ G = \{1, \omega, \omega^2, \omega^3, \dots\dots\dots.\omega^{n-1}\}\ \ where\ \omega^n = 1\ but\ \omega^3 \neq 1$ is the set of nth roots of unity

To show that $< G, . >$ *is an abelian group.*

By the definition of G *for all* $a \in G \quad a^n = 1$

1. Closure property:

By the definition of G For all $a, b \in G$ $\quad a^n = 1$ and $b^n = 1$

Now $(ab)^n = a^n b^n = 1.1 = 1 \Rightarrow ab \in G$.

$\therefore$ Closure property exist.

2. Associative Property: All the elements in G is complex numbers.

But the set of complex numbers satisfies associative.

$\therefore$ Associative exist in G.

3. Existence of Identity: By the definition of nth roots of unity $\mathbf{1 = \omega^0 = \omega^n}$ is the identity in G exist and for all $a \in G \Rightarrow a.1 = a = 1.a$

4. Existence of Inverse: For all $\omega^r \in G$ where $0 \le r \le n-1$ $\exists$ an element $\omega^{(n-r)} \in G$ where $n-r \ge 1 \Rightarrow n - r - 1 > 0$ such that $\omega^r \omega^{(n-r)} = \omega^n = 1$.

$\therefore \omega^{(n-r)} \in G$ is the inverse element of ω^r.

Hence G is a group wrt multiplication

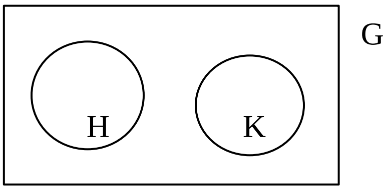
All the best

Unit-II Subgroups, Cosets & Lagrange's theorem

B. Srinivasa Rao. GDC RVPM

Definition (Complex of the Group)

If G is a Group, then any non-empty subset of G is called Complex of the Group.



Example: H= {2 ,3,4,5, 6,… } is a Complex of the Group of integers < Z,+ >

Example: H ={ $i, -i$ } is a complex of the Group G = { 1,-1,$i, -i$ }.

Properties: If H and K are complex of the group G then

$i)\ H^{-1} = \{ h^{-1} : h \in H \}$

$ii)\ HH^{-1} = \{ h_1 {h_2}^{-1} :\ h_1 \in H\ h_2 \in H\}$

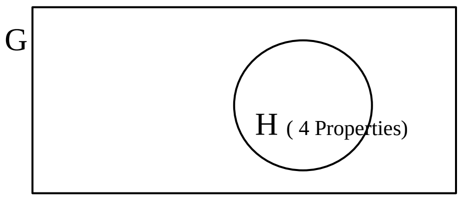
$iii) HH = \{ h_1 h_2 :\ h_1 \in H\ h_2 \in H\}$

$iv) HK = \{hk : h\ \in H, k \in K \}$

$v)\ H^{-1}\ K^{-1} \{ h^{-1}\ k^{-1} : h\ \in H, k \in K \}$

Definition (Sub group) :

A non-empty subset H of a group G is said to be subgroup of G if H satisfies all the four properties of the group or H itself is a group.



Example: H = {1, -1} is a sub group of G = {1 , -1, i , $-i$ }

Example: The set of Even Integers 2Z = {. . . . . .. -6, -4, -2,0,2,4,6, ...}

and the multiples of 3 i.e 3Z = { . . . . -9,-6,-3,0,3,6,9, ...} etc.

are the subgroups of Group of Integers Z w r t addition.

Result: Prove that if H is a sub group of G then H^{-1} = H.

Proof: Let H is a sub group of G, For all $h \in H$ and H is a subgroup of G

By inverse law in the sub group H $h^{-1} \in H$ $\Rightarrow (h^{-1})^{-1} \in H^{-1}$ $\Rightarrow h \in H^{-1}$

$\therefore$ $H \subseteq H^{-1}$ ------(1)

For all $h^{-1} \in H^{-1}$ where $h \in H$

But H is a subgroup of G As $h \in H$ By inverse law $h^{-1} \in H$.

$\therefore$ $H^{-1} \subseteq H$------- (2)

From (1) and (2) $H^{-1} = H$

Note: B u t converse is not true. since H={ $i, -i$ } is a subset of a Group G = {1,-1,$i, -i$ }.

Clearly H^{-1} = { $i^{-1}, (-i)^{-1}$} = { $-i, i$ } = H

But H is not a subgroup of G, Since $i \times -i = 1 \notin H$

Result: If H is a subgroup of a group G then prove that HH = H

Proof: Given that His a subgroup of G

To show that HH = H

Case – 1 HH $\subseteq$ H

By the definition of HH = { $h_1h_2 : h_1 \in H, h_2 \in H$}

For any $x \in HH \Rightarrow x = h_1h_2 \in HH$ $Where$ $h_1 \in H, h_2 \in H$

As $h_1 \in H, h_2 \in H$ and H is a $subgroup$ by $closure$ law $h_1h_2 \in H$

$\Rightarrow x \in H$ $\therefore HH \subseteq H$ --------(1)

Case-2 H $\subseteq$ HH

For any h$\in H \Rightarrow h = he \in HH$ ($\because$ $identity$ $element$ in H)

$\Rightarrow h \in HH$

$\therefore H \subseteq HH$ ----(2)

$From$ (1) & (2) HH=H

Theorem (Necessary and sufficient condition for sub group of a group)

Statement: **A non-empty subset H of a group G to be a subgroup if and only iff for all a, b $\in$ H $\Rightarrow$ a $b^{-1} \in$ H.**

Proof: $\Rightarrow$ **Part** Suppose H is a subgroup of G

for all a, b $\in$H

$\Rightarrow a \in H,\ b \in H$

$\Rightarrow a \in H,\ b^{-1} \in H$ ($\because$ H is subgroup inverse property in H)

$\Rightarrow a b^{-1} \in H$. (by closure property in H).

$\Leftarrow$ **Part** **Assume that H is a subset of G and for all a, b $\in$ H $\Rightarrow$ a $b^{-1} \in$ H.**

1.For all $a \in H \Rightarrow a \in H,\ a \in H \Rightarrow a a^{-1} \in H$ (given)

$\Rightarrow e \in H$. Identity element exist in H.

2.As $e \in H$ and for all $b \in H \Rightarrow e b^{-1} \in H$

$\Rightarrow b^{-1} \in H$

$\therefore$ for all $b \in H \Rightarrow b^{-1} \in H$ Inverse property exists in H

3.For all $a, b \in H \Rightarrow a \in H,\ b \in H$

$\Rightarrow a \in H,\ b^{-1} \in H$ (Since for all $b \in H \Rightarrow b^{-1} \in H$)

$\Rightarrow a (b^{-1})^{-1} \in H$ (for all $a, b \in H \Rightarrow a b^{-1} \in H$.)

$\Rightarrow ab \in H$

Closure property exist in H

4.As $H \subseteq G$ and G is a group and it satisfies associative property and hence H Satisfies associative.

Hence H is a subgroup of G

Theorem: **Let G is a group then prove that H is a subgroup of G $\Leftrightarrow$ H H^{-1} = H.**

Proof: $\Rightarrow$ Part Let H is a subgroup of G the $HH = H$ and $H^{-1} = H$ --------- (1)

LHS = H H^{-1} = H H = H = RHS (Since from (1))

⇐ Part Let H is a subset of G & H H^{-1} = H. To show than H is a subgroup

By the definition of HH^{-1} for all a, b ∊ H then

ab^{-1} ∊ H H^{-1}= H ⇒ ab^{-1} ∊ H.

Hence the theorem

Theorem:

The necessary and sufficient condition for a nonempty finite subset H of the groupG to be a subgroup is that for all a, b ∈ H then ab ∈ H.

Proof: ⇒ Part Suppose H is a subgroup of G

∴ By closure property in H for all a, b ∈ H then ab ∈ H.

⇐ Part Suppose H is finite subset of group G andfor all a, b ∈ H then ab ∈ H -----(1)

To show that H is a subgroup of G .

1.Identity property: From (1) for all a ∈ H ⇒ a, a ∈ H

⇒ aa ∈ H⇒ a^2 ∈ H⇒ again for a ∈ H, a^2 ∈ H

⇒ a a^2 ∈ H

⇒ a^3 ∈ H and so on . . . . .

We get $\{ a, a^2, a^3, a^4, \dots \dots \dots, a^n \dots \dots \}$ ⊆ H

But H is a **finite subset of G**. An infinite set is not a sub set of a finite set

$\therefore$ *some of the elements in the set* $\{ a, a^2, a^3, a^4, \dots \dots \dots, a^n \dots \dots \}$ are repeated

Suppose $a^r = a^s \quad for\ some\ r > s$

$\Rightarrow a^{r-s} = a^0 \quad for\ some\ r - s > 0$

, $\Rightarrow a^{r-s} = a^0 \in H \ \Rightarrow \ a^0 \in H \quad Since\ r - s\ is\ positive$

2.Inverse property: for all a ∈ H ∃ an element a^{r-s-1} ∈ H ($r - s - 1 > 1$ such that

$$aa^{r-s-1} = a^{r-s} = a^0 \in H \ \&\ a^{r-s-1}a = a^{r-s} = a^0 \in H$$

∴ Inverse property exists in H.

3.Closure property: Given that for all a, b ∈ H then ab ∈ H.

4 Associative property: As $H \subseteq G$ and is a group Associative holds in H.

Hence the theorem.

Example: **We know that H = $\{ \mathbf{1}, \mathbf{-1}, \boldsymbol{i}, \boldsymbol{-i} \}$ is a finite sub group of group of Complex numbers C.**

$As\ i \in H \Rightarrow i.i = i^2 \in H$ Also $i \in H\ and\ i^2 \in H \Rightarrow i.\ i^2 = i^3 \in H$

Again $i \in H\ and\ i^3 \in H \Rightarrow i.\ i^3 = i^4 \in H$ etc

$\Rightarrow \{ i, i^2, i^3, i^4, i^5, \ldots \ldots \ldots \ldots \} \subseteq H\ but\ H\ is\ finite.$ Elements are repeated.they are

$$i^3 = -i, i^4 = 1, i^5 = i^4.i = i \Rightarrow i^5 = i\ etc$$

Theorem: Let H and K are two subgroups of a group G then prove thatHK is a subgroup of G if and only is HK=KH.

Proof: ⇒ Part Let HK is a subgroup of G

$\Rightarrow (HK)^{-1} = HK$ (Since H is a subgroup $\Rightarrow H^{-1}=H$)

$\Rightarrow K^{-1} H^{-1} = HK$

$\Rightarrow K H = HK$ (Since H,K are a subgroups $\Rightarrow H^{-1} = H$ and $K^{-1} = K$)

⇐ Part : Suppose H and K are two subgroups of a group G and HK=KH

To show that HK is a subgroup of G

That is to show that $(HK)(HK)^{-1} = HK$ ($\because$H is a subgroup of G $\Leftrightarrow HH^{-1} = H$)

LHS= $(HK)(HK)^{-1} = (HK)K^{-1}H^{-1}$

$= H(K K^{-1})H^{-1}$ ($\because$ associative)

$= H(K)H^{-1}$ (K is a subgroup of G $\Leftrightarrow KK^{-1} = K$

$= (HK)H^{-1}$

$= (KH)H^{-1}$ ($\because$ HK = K H)

$= K(HH^{-1})$

$= KH = HK = RHS$ ($\because HH^{-1} = H$)

Theorem: Prove that the intersection of two subgroups is a subgroup of the group G .

Proof:

Let H_1 and H_2 are two subgroups of the group G.To show that $H_1 \cap H_2$ is also subgroup of G .

1. $H_1 \cap H_2 \neq \varphi$ As H_1 and H_2 are two subgroups of G by

Identity property $e \in H_1$ and $e \in H_2 \Rightarrow e \in H1 \cap H2 \Rightarrow H_1 \cap H_2$ is non-empty sub set of G

2. For all $a, b \in H_1 \cap H_2 \Rightarrow ab^{-1} \in H_1 \cap H_2$

For all $a, b \in H_1 \cap H_2 \Rightarrow a, b \in H_1$ and $a, b \in H_2$

But Let H_1 and H_2 are subgroups of G

$\therefore$ $ab^{-1} \in H_1$ and $ab^{-1} \in H_2$

$\Rightarrow ab^{-1} \in H_1 \cap H_2$

Hence $H_1 \cap H_2$ is subgroup of the group G

Theorem: Prove that the union of two subgroups is a subgroup of a group G if and only if one is contained in other.

Proof : Let H_1 and H_2 are two subgroups of the group G To prove that

$H_1 \cup H_2$ is a subgroup $\Leftrightarrow H_1 \subseteq H_2$ or $H_2 \subseteq H_1$

$\Leftarrow$Part Let H_1 and H_2 are two subgroups of the group G and $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$

To show that $H_1 \cup H_2$ subgroup

If $H_1 \subseteq H_2 \Rightarrow H_1 \cup H_2 = H_2$ subgroup of G

If $H_2 \subseteq H_1 \Rightarrow H_1 \cup H_2 = H_1$ subgroup of G

$\Rightarrow$ Part let H_1 and H_2 subgroups and $H_1 \cup H_2$ is a subgroup

to show that $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$

If $H_1 \not\subset H_2 \Rightarrow$ For all $a \in H_1 \not\subset H_2$ => $a \in H_1$ but $a \notin H_2$ ----- (1)

If $H_2 \not\subset H_1 \Rightarrow$ For all $b \in H_2 \not\subset H_1$ => $b \in H_2$ but $b \notin H_1$ ---------(2)

As $a \in H_1$, $b \in H_2$ => $a, b \in H_1 \cup H_2$

But $H_1 \cup H_2$ is a subgroup

$\therefore ab \in H_1 \cup H_2$

$\Rightarrow ab \in H_1$ or $ab \in H_2$ ---------------------------- (3)

From (1) and (3)

For $a \in H_1$, $ab \in H_1 \Rightarrow a^{-1} \in H_1$ (subgroup) $ab \in H_1$

$\Rightarrow a^{-1}(ab) \in H_1$ (Closure property in H_1)

$\Rightarrow (a^{-1}a)b \in H_1$

$\Rightarrow eb \in H_1$

$\Rightarrow$ $b \in H_1$ but from (2) $b \notin H_1$ it is Contradiction.

Also from (2) and (3)

$ab \in H_2$ $b \in H_2 \Rightarrow$ $ab \in H_2$ $b^{-1} \in H_2$ (Sub group of G)

$\Rightarrow (a\,b)\,b^{-1} \in H_2$ (Closure property in H_1)

$\Rightarrow a(b\,b^{-1}) \in H_2$

$\Rightarrow$ $ae \in H_2$

$\Rightarrow$ $a \in H_2$ but from (1) $a \notin H_2$ it is also a contradiction.

$\therefore H_1 \subseteq H_2$ or $H_2 \subseteq H_1$

COSETS

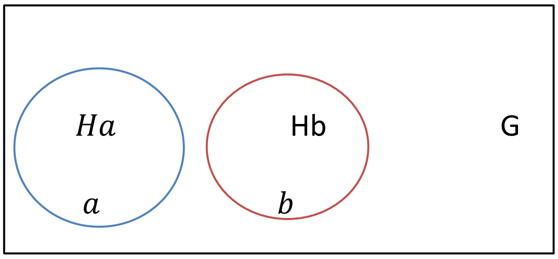
Definition (Cosets):

Let H is a subgroup of the group G then for any $a \in G$ to define a set

if $H = \{ h_1, h_2, h_3, ... h_n, ... \} = \{h: h \in H\}$

$aH = \{ ah_1, ah_2, ah_3, ... ah_n,\} = \{ah: h \in H\}$ is the left coset of H in G.

$Ha = \{h_1a, h_2a, h_3a, \dots \dots . . h_na, . .\} = \{ha: h \in H\}$ is the right coset of H in G



Example: We know that

$H = \{\dots .. -6, -4, -2, 0, 2, 4, 6, \dots \dots .\}$ is a sub group of additive group of Integers

Z = {. . . . . . .-6,-5,-4,-3,-2,-1,0,1,2,3,4,5,6,.......}

Then the right cosets of H for $3 \in Z$ but $3 \notin' H$

$$H + 3 = \{\dots -6+3, -4+3, -2+3, 0+3, 2+3, 4+3, 6+3,\}$$

$$= \{\dots\dots -3, -1, 1, 3, 5, 7, 9, \dots\dots\dots\}.$$

$$H+5 = \{......-6+5,-4+5,-2+5,0+5,2+5,4+5,6+5,.........\}$$

$$= \{......-1,1,3,5,7,9,11,\} \qquad for\ 5 \in Z\ but\ 5 \notin' H$$

$$H+\ 2 = \{......-6+2,-4+2,-2+2,0+2,2+2,4+2,6+2,\}$$

$$= \{.......-4,-2,0,2,4,6,8,......\} = H$$

$$\therefore\ for\ 2 \in H\ iff\ H+\ 2 = H$$

$Similarly\ for\ 4 \in H\ iff\ H+\ 4 = H$

Note: For a ∈ H if and only if Ha = H = a H

Theorem If H is a subgroup of the group G for any a, b ∈ G Prove that

i) Ha = Hb iff $ab^{-1} \in H$

ii)aH = bH iff $a^{-1}b \in H$

Proof: ⇒ par Suppose Ha = Hb ------- (1)

As a ∈ Ha ⇒ a∈ Hb since from (1)

⇒ $ab^{-1} \in Hb\,b^{-1}$

⇒ $ab^{-1} \in He$

⇒ $ab^{-1} \in H$

⇐ Part .

i) Suppose $ab^{-1} \in H \Rightarrow H\,ab^{-1} = H$ (Since a∈ H ⇔ Ha = H = aH)

⇒ $(H\,ab^{-1})\,b = Hb$

⇒ $Ha\,(b^{-1}b) = Hb$

⇒ H a (e) = Hb

⇒ H a = Hb

ii)Similarly, to prove second one also. $aH = bH\ iff$ $a^{-1}b \in H$

Theorem: If H is a subgroup of the group G for any a, b ∈ G Prove that

i) a ∈ Hb iff Ha = Hb

ii) b ∈ Ha iff a H = b H

Proof: i) ⇒ Part As a ∈ Hb ⇒ $ab^{-1} \in Hbb^{-1}$ ⇒ $ab^{-1} \in He$

⇒ $ab^{-1} \in H \Rightarrow H\,ab^{-1} = H$ (Since a ∈ H if and only if Ha = H)

$\Rightarrow$ (H ab^{-1}) b=Hb $\Rightarrow$ H a = Hb

$\Leftarrow$ **Part** Let H a=Hb clearly a $\in$ Ha $\Rightarrow$ a $\in$ Hb Since H a=Hb

Similarly, to prove b $\in$ a H iff a H = b H

Theorem:

Prove that in a group G any two right or left cosets are either identical or disjoint.

Proof: *Let H is a subgroup of the group G to show that*

for any a, b $\in$G theright cosets Ha and Hb are

either Ha = Hb (identical) or Ha $\cap$ Hb = φ (disjoint)

Part-1 suppose Ha $\cap$ Hb $\neq \varphi$

$\therefore$ *for any* $x \in Ha \cap Hb \Rightarrow x \in Ha$ *and* $x \in Hb$

$\Rightarrow x = h_1 a$ *and* $x = h_2 b$ *for* $h_1, h_2 \in H$

$\Rightarrow h_1 a = h_2 b$ *for* $h_1, h_2 \in H$

$$\Rightarrow {h_1}^{-1}(h_1 a) = {h_1}^{-1}(h_2 a) \ (\because \ h_1 \in H \Rightarrow \ {h_1}^{-1} \in H)$$

$\Rightarrow a \in Hb \Rightarrow Ha = Hb$ *identical*

Similarly, to prove left cosets also

Part-2 It is very clear if Ha $\neq$ Hb then Ha $\cap$ Hb = φ

Lagrange's Theorem for finite groups

Statement: The order of a subgroup H of a finite group G is a divisor of order of the group G that is O(H) is a factor of O(G)

Proof:

Let G be a group of finite order n. ie $O(G) = n$

Let H be a subgroup of G and let $o(H) = m$

Suppose $h_1, h_2, \ldots\ldots, h_m$ are the m members of H.

Let a $\in$G. Then Ha is a right coset of H in G and we have

Ha= $\{h1a, h2\,a, \ldots hm\,a\}$.

Ha has m distinct members, since $h_i a = h_j a \Rightarrow h_i = h_j$ *for* $i \neq j$

Therefore $O(Ha) = m$. *for all* $a \in G$

But any two distinct right cosets of H in G are disjoint or identical

ie , they have no element in common. Since G is a finite group, the number of distinct right cosets of H in G will be finite, say, equal to k.

The union of these k distinct right cosets of H in G is equal to G.

Thus $H_{a_1}, H_{a_2}, H_{a_3}, \ldots \ldots . . H_{a_k}$are the k distinct right cosets of H in G,

$$\therefore G = H_{a_1} \cup H_{a_2} \cup H_{a_3} \cup, \ldots \ldots . . \cup H_{a_k}$$

$$\Rightarrow \; O(G) = O(H_{a_1} \cup H_{a_2} \cup H_{a_3} \cup, \ldots \ldots . . \cup H_{a_k})$$

$$n \; = \; O(H_{a_1}) + (H_{a_2}) + (H_{a_3}) + \cdots \ldots . . + (H_{a_k}) =$$

Since $H_{a_1}, H_{a_2}, H_{a_3}, \ldots \ldots . . H_{a_k}$ are disjoint co-sets

$$= \; m \; + \; m + \; \ldots \ldots \ldots + m \; (\; k \; times \;) \qquad (Since \; O(\; Ha \;) \; = \; m \;)$$

$$n = km \; \Rightarrow m/n \quad (\text{Since } 12 \; = 3 \; \times \; 4 \; \Rightarrow 3/12)$$

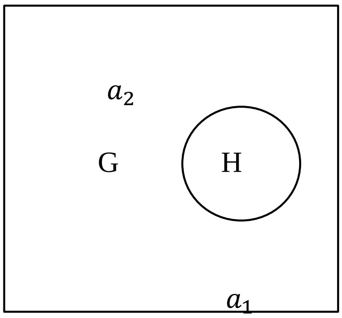
$$\Rightarrow \; O(H) \; / \; O(G) \; that \; is \; order \; of \; the \; subgroup \; is \; a \; divisor \; of \; order \; of \; the \; Group$$

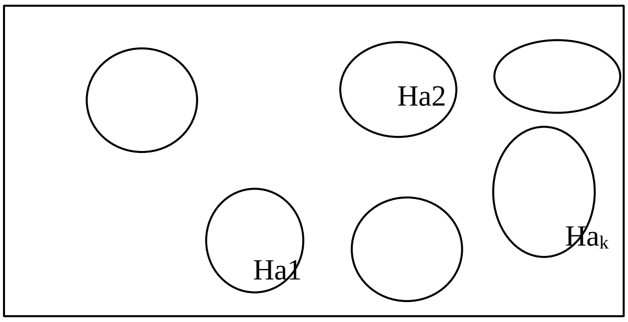
Note: $n \; (AU \; B) \; = \; n(\; A \;) \; + \; n(\; B) - \; n(\; A \cap B \;) \;$ *But if A and B are disjoint* .

$$i.e. A \cap B \; = \phi \; then \; n \; (AU \; B) \; = \; n(A \;) \; + \; n(\; B)$$

Note: $3 \times 5 = 15 \; \Rightarrow$ 3 is a factor of 15 and 5 is a factor of 15 i e 3/15 5/15

And $17 \times 4 \; = 68 \Rightarrow$ 17 is a factor of 68 and 4 is a factor of 68. ie 17/68 ,4/68





****

GOVERNMENT DEGREE COLLEGE, RAVULAPALEM
NAAC Accredited with 'B' Grade(2.61 CGPA)
(Affiliated to Adikavi Nannaya University)
Beside NH-16, Main Road, Ravulapalem-533238, Dr.B.R.Ambedkar Dist., A.P, INDIA
E-Mail : jkcjyec.ravulapalem@gmail.com, Phone : 08855-257061
ISO 50001:2011, ISO 14001:2015, ISO 9001:2015 Certified College

B. SRINIVASARAO. Lecturer in Maths GDC RVPM

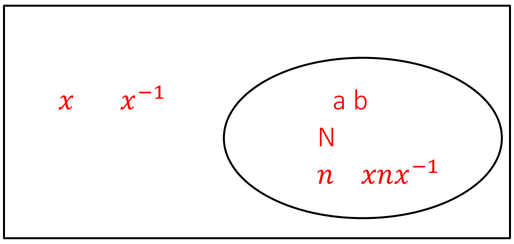
NORMAL SUBGROUPS

Definition (Normal subgroup):

A non-empty subset N of Group G is said to be a Normal subgroup of G

if 1. For all a, b ∈ N ⇒ ab^{-1} ∈ N (subgroup property)

2. For all x ∈ G, n ∈ N ⇒ xnx^{-1} ∈ N (Normal property)



Note : If N is Normal then $xNx^{-1} = \{ xnx^{-1} : x \in G, n \in N \} \subseteq N$

Example: H= { 1,-1 } is a Normal subgroup of G= $\{ 1, -1, i, -i \}$

let $x = i$, n = -1 ∈ H and $x^{-1} = i^{-1} = -I$ ∈ G

Now xnx^{-1}= i(-1)(-i) = -1 ∈ H

Simple Group: A group G having no proper normal subgroups is called simple group

ie { e } and G are only Normal subgroups of G

Theorem: -1

If N is a subgroup of a group G then prove that N is Normal if and only if xNx^{-1} = N ∀ x ∈ G.

Proof: ⇒ part. Suppose N is normal subgroup of G

$\forall x \in G. n \in N \Rightarrow xnx^{-1} \in N$

$\Rightarrow \{xnx^{-1} \in N : n \in N \} \subseteq N$

$\Rightarrow xNx^{-1} \subseteq N$ -------- (1)

From (1) for all x ∈ G. ⇒ x^{-1} ∈ G

Therefore $(x^{-1}) N (x^{-1})^{-1} \subseteq N$

$\Rightarrow x^{-1} N x \subseteq N$

$\Rightarrow x (x^{-1} N x) x^{-1} \subseteq x N x^{-1} \quad \forall x \in G.$

$\Rightarrow (x x^{-1}) N (x x^{-1}) \subseteq x N x^{-1} \quad \forall x \in G.$

$\Rightarrow (e) N (e) \subseteq x N x^{-1} \quad \forall x \in G.$

$\Rightarrow N \subseteq x N x^{-1} \quad \forall x \in G.$ --------- (2)

From (1) and (2) $xNx^{-1} = N \quad \forall x \in G.$

$\Leftarrow$ part Suppose $xNx^{-1} = N \quad \forall x \in G$ to show that N is normal

By the definition of xNx^{-1}

$\forall x \in G. n \in N \Rightarrow xnx^{-1} \in x N x^{-1} = N$

$\Rightarrow xnx^{-1} \in N$

Hence N is normal subgroup of G

Theorem: 2

If N is a subgroup of a group G then prove that N is Normal if and only if each left coset of N is the right coset of N in G .

Proof: $\Rightarrow$ part Suppose N is normal subgroup of G

$x N x^{-1} = N \quad \forall x \in G.$

$\Rightarrow (x N x^{-1}) x = N x$

$\Rightarrow x N (x^{-1} x) = N x \quad \forall x \in G.$ (by associative)

$\Rightarrow x N = N x \quad \forall x \in G.$

$\Rightarrow$ each left coset of N is the right coset of N in G .

$\Leftarrow$ part Suppose $x N = N y \quad \forall x, y \in G$ ----------- (1)

As $x \in x N = N y \quad \forall y \in G.$

$\Rightarrow x \in N y \quad \forall y \in G.$

$\Rightarrow N x = N y \quad \forall y \in G.$---------(2)

From (1) and (2) $x N = N x \quad \forall x \in G.$

$\Rightarrow x^{-1}(x N) = x^{-1} N x \quad \forall x \in G.$

$\Rightarrow (x^{-1} x) N = x^{-1} N x \quad \forall x \in G.$

$\Rightarrow e N = x^{-1} N x \quad \forall x \in G \Rightarrow N = x^{-1} N x \quad \forall x \in G.$

Hence N is normal subgroup of G.

Theorem: 3

If N is a subgroup of a group G then prove that N is Normal if and only if product of two right (left) cosets of N is again right(left) coset of N in G.

Proof: $\Rightarrow$ Part Suppose N is normal subgroup of G and N x, Ny are two right cosets of N .

To show that (N x Ny) = N x y $\forall$ x, y $\in$ G

LHS = (N x Ny)

= N(x N)y = N(N x)y (since N is normal subgroup$\Rightarrow$ x N = N x)

= N N x y

= N x y (Since H is subgroup $\Rightarrow$ H H = H)

= RHS

$\Leftarrow$ Part Let N is a subgroup of G and product of two right co sets of N is a right co set of N in G

ie (N x)(Ny) = N x y $\forall$ x, y $\in$ G ....(1)

To show that N is Normal ie for all $x \in G$ $n \in N \Rightarrow xnx^{-1} \in N$

Since $xnx^{-1} = e\,(xnx^{-1})$ since e is the identity in H

$=(ex)(nx^{-1}) \in (Hx)(Hx^{-1})$ since $e \in H$

$=(ex)(nx^{-1}) \in (Hxx^{-1})$ since from (1)

$=(x)(nx^{-1}) \in (He)$

$= x\,n\,x^{-1} \in H$

$\therefore$ for all $x \in G$ $n \in H \Rightarrow xnx^{-1} \in H$

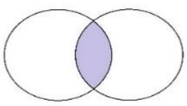
Hence H is normal subgroup of G

Theorem:4

Prove that the intersection of two normal subgroups is also a normal subgroup of group G.

Proof: Let N_1 and N_2 are two normal subgroups of the group G.

To prove that $N_1 \cap N_2$ is also a normal subgroup of G.



1) $N_1 \cap N_2$ is non empty.

As N_1 and N_2 are subgroups by Identity law $e \in N_1$ and $e \in N_2$

$\Rightarrow e \in N_1 \cap N_2$

$\Rightarrow N_1 \cap N_2$ is nonempty.

2) For all $a, b \in N_1 \cap N_2 \Rightarrow ab^{-1} \in N_1 \cap N_2$

As For all $a, b \in N_1 \cap N_2 \Rightarrow a, b \in N_1$ and $a, b \in N_2$

But N_1 and N_2 are subgroups of G

$\Rightarrow ab^{-1} \in N_1$ and $ab^{-1} \in N_2$

$\Rightarrow ab^{-1} \in N_1 \cap N_2$

3) For all $x \in G$, $n \in N_1 \cap N_2 \Rightarrow x\, n\, x^{-1} \in N_1 \cap N_2$

As for all $x \in G$, $n \in N_1 \cap N_2 \Rightarrow x \in G$, $n \in N_1$ and $n \in N_2$

$\Rightarrow x \in G$, $n \in N_1$ and $x \in G$, $n \in N_2$

But N_1 and N_2 are normal subgroups

$\Rightarrow x\, n\, x^{-1} \in N_1$ and $x\, n\, x^{-1} \in N_2$

$\Rightarrow x\, n\, x^{-1} \in N_1 \cap N_2$

Hence $N_1 \cap N_2$ is a normal subgroup of G

Definition (Index of subgroup): **In a group G the number of distinct right or left cosets of a subgroup H is called Index of H in G and is denoted by** [H : G]

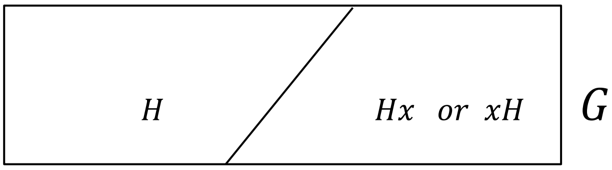
Theorem:5 **Prove that every subgroup of index 2 is normal.**

Proof: Let H is a sub group of a group G and index of H is 2.

To show that H is Normal.

As index of H is 2 $\therefore$ for any $x \in G \Rightarrow x \in H$ or $x \notin H$.

If $x \in H$ $\Rightarrow Hx = H = xH \Rightarrow$ H is normal.



If $x \notin H$ $\Rightarrow$ we get a right coset Hx or a left coset xH.

If Hx is a right coset of H in G and index of H is 2.

$\therefore G = H \cup Hx$ or $G = H \cup xH$

$\Rightarrow H \cup Hx = H \cup xH$

$\Rightarrow Hx = xH$ since H , Hx and x H are disjoint

$\Rightarrow$ H is normal.

Theorem :6

Let H is a subgroup and N is a normal subgroup of a group G then prove that $H \cap N$ is a normal subgroup of H.

Proof: As H and N are subgroups of G $\Rightarrow H \cap N$ is a sub group of G

But $H \cap N \subseteq H \Rightarrow H \cap N$ is a sub group of H.

ie to show that for all $x \in H$, $n \in H \cap N \Rightarrow x\, n\, x^{-1} \in H \cap N$

As for all $x \in H$, $n \in H \cap N \Rightarrow$ for all $x \in H$, $n \in H$ and $n \in N$

$\Rightarrow$ for all $x \in H$, $n \in H$ and $x \in G$, $n \in N$ $(\because H \subseteq G)$

As N is normal subgroup of G $\Rightarrow$ $x \in G$, $n \in N \Rightarrow x n x^{-1} \in N$ ------------------ (1)

As H is a subgroup of G $\Rightarrow$ for all $x \in H$, $n \in H \Rightarrow x, x^{-1} \in H$, $n \in H$

$\Rightarrow x n x^{-1} \in H$ ($\because$ H is a subgroup of G) -----------(2)

From (1) and (2) $x n x^{-1} \in H$ and $x n x^{-1} \in N$

$\Rightarrow x n x^{-1} \in H \cap N$.

Hence the theorem.

Theorem :7

Let N and M are two normal subgroups of a group G then prove that NM is also a normal subgroup of G.

Proof:

We know that any sub group is commutes with a complex of a group .

Therefore NM = MN (Here we are taking M is complex of G)

$\Rightarrow$ NM is a subgroup of G ($\because$ HK is subgroup of G iff HK = KH)

Now to find the normal property

For all $x \in G$, $nm \in NM \Rightarrow x(nm)x^{-1} \in NM$

As $x(nm)x^{-1} = x(n e m)x^{-1} = x[n(x^{-1}x)m]x^{-1}$

$= [x n x^{-1}][x m x^{-1}] \in NM$

Since N and M are normal subgroups of G

we get $[x n x^{-1}] \in N$ $[x m x^{-1}] \in M$

Hence NM is a normal subgroup of G

Theorem: 8 (Normalizer of a group)

If G is a group and for any $a \in G$ show that the set

$N(a) = \{ x \in G : a x = x a$ for $a \in G$ is a subgroup of G and is called normalize of G.

Proof: Given that for all $x \in N(a) \Leftrightarrow a x = x a$ for $a \in G$

1) N(a) is non empty: we know that $a e = e a \Leftrightarrow e \in N(a)$

$\Rightarrow$ N(a) is nonempty sub set of G

2) for all $x \in N(a) \Rightarrow x^{-1} \in N(a)$

As f or all $x \in N(a) \Rightarrow a x = x a$

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

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

$\Rightarrow (x^{-1}a)(e) = (e)(a x^{-1})$

$\Rightarrow x^{-1}a = a x^{-1} \Rightarrow x^{-1} \in N(a)$

3) for all $x, y \in N(a) \Rightarrow$ to show that $x y^{-1} \in N(a)$

That is to show that $a(xy^{-1}) = (xy^{-1})a$

LHS $= a(xy^{-1}) = (ax)y^{-1} = (xa)y^{-1}$ (since $x \in N(a) \Leftrightarrow ax = xa$ for $a \in G$)

$= x(ay^{-1})$

$= x(y^{-1}a)$ (since $y \in N(a) \Rightarrow y^{-1} \in N(a)$)

$= (xy^{-1})a =$ RHS

$\therefore$ N(a) is a normal subgroup of G

Note : N(e) = G where e is the identity and N(a) is not a normal subgroup of G

Theorem:9 **Let M and N are two normal subgroups of group G such that $M \cap N = \{e\}$ then prove that each element in M is commute with each element in N.**

Proof : Give that M,N are Normal subgroups of G and $M \cap N = \{e\}$

To show that for all $m \in M$, $n \in N$ then $mn = nm$

ie $(mn)(mn)^{-1} = (nm)(mn)^{-1}$

ie $e = (nm)(n^{-1}m^{-1})$

ie $nmn^{-1}m^{-1} = e$

Case -1 . Let M is Normal and N is a subgroup of G

$\therefore$ for all $m \in M$, $n \in N \subseteq G$

$\Rightarrow m \in M$, $n \in G$ and M is Normal

$\Rightarrow nmn^{-1} \in M$ but $m^{-1} \in M$

$\Rightarrow nmn^{-1}m^{-1} \in M$ by closure in M .... (1)

Case-2 . Let N is Normal and M is a subgroup of G

$\therefore$ for all $n \in N$, $m \in M \subseteq G$

$\Rightarrow n^{-1} \in N$, $m \in G$ and N is Normal

$\Rightarrow mn^{-1}m^{-1} \in N$ but $n \in N$

$\Rightarrow nmn^{-1}m^{-1} \in N$ by closure in N .... (2)

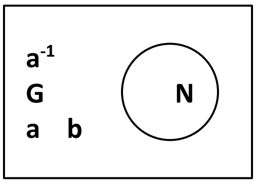
From (1),(2) $nmn^{-1}m^{-1} \in M \cap N = \{e\}$

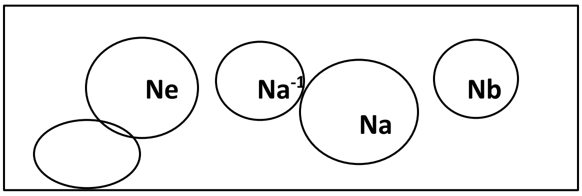
$\therefore nmn^{-1}m^{-1} = e$ It follows $mn = nm$

Quotient Group

Theorem:10 Prove that if N is a Normal subgroup of the group G then the set of cosets of N $G/N = \{Na : a \in G\}$ form a Group w r t coset multiplication

$$N\,a\,N\,b = Na\,b \quad \text{for all } a, b \in G$$





Proof: To show that < G/N, . > is a Group

1.Closure Property: For all Na, N b ∈ G/N then a, b ∈ G but G is a Group

$\Rightarrow$ a b ∈ G

$\Rightarrow$ N (a b) ∈ G/N (Since a∈ G $\Leftrightarrow$ Na ∈ G/N

$\Rightarrow$ (N a)(Nb) ∈ G/N

$\Rightarrow$ G/N is closed

2) Associative property: For all N a, N b, N c ∈ G/N where a, b, c ∈ G

Now (Na) [(Nb)(Nc)] = (N a) [N(b c)]

= N[a (b c)]

= N[(a b)c)] since [a (b c)] = [(a b)c)] in G

=[N(a b)](Nc)

=[(Na) (Nb)] (Nc)

Associative property exist.

3)Identity property: For all Na in G/N there exist a coset Ne in G/N (∵ e ∈ G)

Such that (N a) (Ne)= N(ae) = N a.

(Ne)(Na)= N(e a) = Na.

∴ Ne = N is the Identity in G/N.

4)Inverse property: For all Na in G/N there exist a coset Na^{-1} in G/N (since a∈ G $\Rightarrow$ a^{-1}∈ G

such that (Na)[Na^{-1}]= N[a (a^{-1})] = Ne = N.

[Na^{-1}] (Na) = N (a^{-1} a) = Ne = N

∴ [Na^{-1}] is the inverse element of Na in G / N.

∴ < G/N, . > is a Group

Theorem :11 **Let N is an normal subgroup of the group G then prove that**

If G is commutative group then G / N also commutative

Proof: For all Na, Nb ∈ G / N where a, b∈ G

(Na) (Nb) = N(a b)

= N (b a) (∵ a b = b a in G)

= (Nb) (N a) Commutative property holds.

GOVERNMENT DEGREE COLLEGE, RAVULAPALEM
NAAC Accredited with 'B' Grade(2.61 CGPA)
(Affiliated to Adikavi Nannaya University)
Beside NH-16, Main Road, Ravulapalem-533238, Dr.B.R.Ambedkar Dist., A.P, INDIA
E-Mail : jkcjyec.ravulapalem@gmail.com, Phone : 08855-257061
ISO 50001:2011, ISO 14001:2015, ISO 9001:2015 Certified College

Group Theory II BSC MATHS

UNIT- IV. HOMOMORPHISMS AND ISOMORHISMS

B. SRINIVASARAO. Lecturer in Mathematics, Government Degree College, Ravulapalem.

Definition (Homomorphisms) Let G and G ‘ are groups and a function f: G → G‘ is said to be homomorphism if for all a, b $\in$ G then $f\,(a\,b) = f(a)\,f(b)$.

Definition (Endomorphism): A homomorphism f from G into itself is called endomorphism

Definition (Isomorphism): A function f: G → G‘ is said to be Isomorphism if it is

1)One-one 2) onto 3) Homomorphism

And is denoted by **G ≅ G’**

Monomorphism: A function f from a group G into a group G’ is said to be Monomorphism if it is

1.one-one ie for all $a\,,b \in G\ If\ f(a) = f(b) \Rightarrow a = b.$

2.Homomorphism.

Epimorphism: A function f from a group G into a group G’ is said to be Epimorphism if it is

1) Onto $ie\ for\ all\ y \in G' \,\exists\, an\ element\ x \in G\ such\ that\ y = f(x).$

2) Homomorphism.

General properties of Homomorphism’s:

Let $f : G \to G'$ is a homomorphism then prove that

1) $f(e) = e'\ where\ e'\ is\ the\ identity\ in\ G'$

2) $f(a^{-1}) = [f(a)]^{-1}\quad for\ all\ a \in G$

Proof : 1) By identity law in G $a\,e = a = e\,a$

Now $f(a) = f(a\,e) = f(a)\,f(\,e\,)$ since f is homomorphism

$f(a)\ e\,' = f(a)\,f(\,e\,)$ where e’ is the identity in G’

$e' = f(\,e)$ since by left cancellation law .

2) We know by inverse law $e = aa^{-1} = a^{-1}a\quad for\ all\ a \in G$

$Since\ e' = f(\,e) = f(aa^{-1}\,) = f(\,a\,)\,f(\,a^{-1}\,)$ (∵ f is homomorphism)

$\therefore\ e' = f(a) f(a^{-1})$ -----------(1)

$Again\ e' = f(e) = f(a^{-1}a) = f(a^{-1})\ f(a)$ $(\because\ f\ is\ homomorphism)$

$e' = f(a^{-1})\ f(a)$ -------------- (2)

$from\ (1)\ and\ (2)\quad f(a) f(a^{-1}) = e' = f(a^{-1})\ f(a)$

$(\because\ xy = e = yx \Rightarrow y = x^{-1})$

It $follows\ \ f(a^{-1}) = [f(a)]^{-1}\quad for\ all\ a \in G$

Kernel of Homomorphism: Let f : G → G' is a homomorphism then to define Kernel of Homomorphism by

$$Ker\ f = \{ x \in G : f(x) = e'\ where\ \ e'\ is\ the\ identity\ in\ G' \}$$

and is denoted by K or Ker f.

Theorem: Let f: G → G' is a homomorphism then prove that Ker f is a normal subgroup of G.

Proof: By the definition of Ker f

$For\ all\ x \in Ker\ f\ \ if\ and\ only\ if\ \ f(x) = e'\ where\ e'\ \ is\ the\ identity\ in\ G'$

1) $\boldsymbol{Ker f\ \ is\ nonempty}$:

$By\ The\ General\ Property\ \ f(e) = e' \Rightarrow Ker\ f\ is\ non\ empty.$

2) $For\ all\ a, b \in Ker\ f \Rightarrow ab^{-1} \in Ker\ f$

$As\ f(ab^{-1}) = f(a) f(b^{-1})\quad \because\ f\ is\ homomorphism$

$= f(a)\,[f(b)]^{-1}\qquad \because\ f(a^{-1}) = [f(a)]^{-1}\quad for\ all\ a \in G$

$= e'[e']^{-1} = e'\qquad \because\ from\ (1)$

$\therefore\ f(ab^{-1}) = e' \Rightarrow ab^{-1} \in Ker\ f$

3) $For\ all\ x \in G, n \in Ker\ f \Rightarrow x\,n\,x^{-1} \in Ker\ f$

$Now\ f(x\,nx^{-1}) = f(x) f(n) f(x^{-1})\qquad \because\ f\ is\ homomorphism$

$= f(x) f(n)\ [f(x)]^{-1}\qquad \because\ f(a^{-1}) = [f(a)]^{-1}\quad for\ all\ a \in G$

$= f(x)\, e'\ [f(x)]^{-1}\quad (\because\ n \in Ker\ f \Rightarrow f(n) = e')$

$= f(x)\ [f(x)]^{-1} = e'$

$\therefore\quad f(x\,nx^{-1}) = e'\qquad it\ follows\quad x\,nx^{-1} \in Ker\ f.$

Hence Kernel of f is a normal subgroup of G

Theorem: *If $f : G \rightarrow G'$ is an onto homomorphism then prove that f is Isomorphism if and only if $Ker\, f = \{e\}$*

Proof: $\Rightarrow$ ***Part***

$Let\ f\ is\ isomorphism\ to\ show\ that\ \ Ker\, f = \{e\}$

For all x ∈ Ker f $\Leftrightarrow f(x) = e'$ where e' is the identity in G'

$\Leftrightarrow f(x) = f(e)$ since $f(e) = e'$

$\Leftrightarrow x = e$ since f is one-one function

$\Leftrightarrow x \in \{e\}$

$\therefore\ For\ all\ x \in Ker\, f \Leftrightarrow x \in \{e\}$

$\therefore\ Ker\, f = \{e\}$

$\Leftarrow$ ***part***

$Let\ f : G \rightarrow G'\ is\ an\ onto\ homomorphism\ and\ Ker\, f = \{e\}$

$to\ show\ that\ f\ is\ one - one\ function.$

$Let\ \ f(a) = f(b)\ for\ all\ a, b \in G$

$f(a)[f(b)]^{-1} = f(b)[f(b)]^{-1}\ \ for\ all\ a, b \in G$

$\Rightarrow f(a) f(b^{-1}) = e'$ $\qquad (since\ f(b)\ is\ in\ G')$

$\Rightarrow f(ab^{-1}) = e'$ $\qquad (\because f\ is\ Homomorphism)$

$But\ for\ all\ x \in Ker\, f\ \ if\ and\ only\ if\ \ f(x) = e'\ \ where\ e'\ \ is\ the\ identity\ in\ G')$

$\Rightarrow ab^{-1} \in Ker\, f = \{e\} \Rightarrow ab^{-1} = e \Rightarrow a = b$

$\therefore\ f\ is\ one -\ one\ function.$

Theorem:

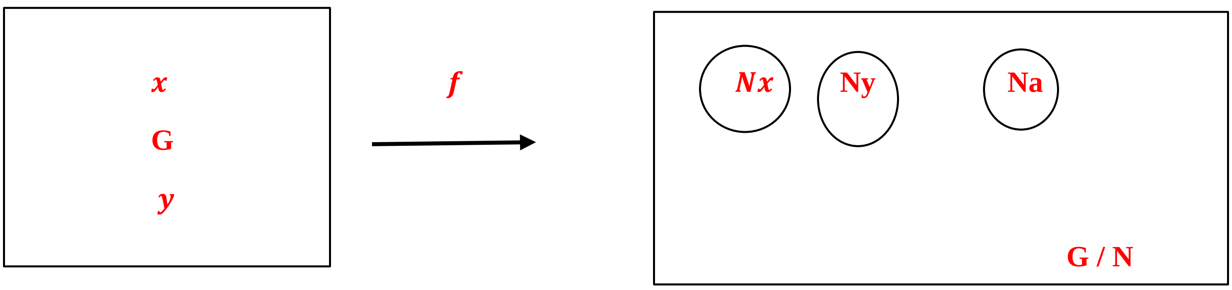
Let N is a normal subgroup of the group G and G/N is the Quotient group then prove that the mapping $f : G \rightarrow G/N$ defined by

$$f(x) = N x\ \ for\ all\ x \in G$$

is an onto homomorphism and $Ker\, f = N$

Proof: Given that $f : G \rightarrow G/N$ defined by

$$f(x) = N x\ \ for\ all\ x \in G$$



1.Clearly it is onto function

By the definition of f for any Na in G/N ∃ $a \in G$ such that $f(a) = Na$

2.f is Homomorphism:

For all x, y in G then

$f(xy) = Nxy = NxNy$ (Since N is normal subgroup of G)

$= f(x)f(y)$

$\therefore$ f *is Homomorphism.*

3.To show that Ker f = N.

$For\ all\ x \in Ker\, f \Leftrightarrow f(x) = N$ $(Since\ N\ is\ the\ Identity\ element\ in\ G/N)$

$\Leftrightarrow Nx = N$ $since\ by\ the\ definition\ of\ f$

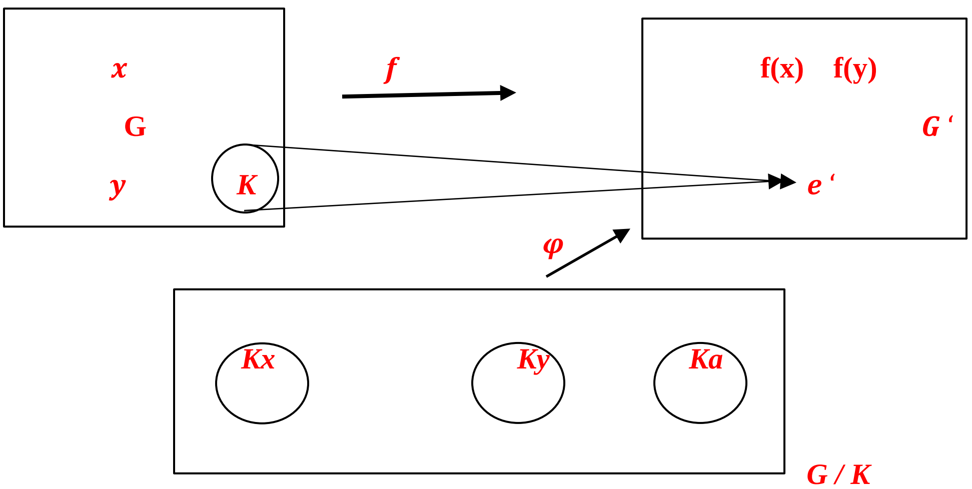
$\Leftrightarrow x \in N$ $since\ a \in H \Leftrightarrow Ha = H = aH$

$Hence\ Ker\, f = N$

**** State and prove Fundamental theorem of Homomorphisms of Groups.**

Every homomorphic image of the group is isomorphic to some quotient group of the group .

Proof :



Let G and G' are two groups and $f : G \to G'$ *is an onto homomorphism*

then $\mathbf{f(G) = G'}$ *is the homomorphic image of the group G.*

As $f : G \to G'$ *is a homomorphism*

$\therefore Ker\, f = \{ x \in G : f(x) = e'$ $where\ e'\ is\ the\ identity\ in\ G'\}$ $exist$

$Let\ Ker\, f = K$ *but kernel of homomorphism is a normal subgroup of G.*

$\therefore G/K = \{ Kx : x \in G \}$ *is a Quotient Group .*

To show that G / K is Isomorphic to G'

Define a function $\varphi : G/K \to G'$ *by* $\boldsymbol{\varphi(x) = Kx}$ *for all* $x \in G.$

1) First to show that $\boldsymbol{\varphi}$ is well defined function from G / K → G':

$For\ all\ Kx, Ky\ in\ G/K$

$Let\ Kx = Ky \Rightarrow xy^{-1} \in$ K (Ha = Hb ⇔ $ab^{-1} \in H$)

⇒ $xy^{-1} \in$ Ker f (Since Ker f = K)

⇒ f (xy^{-1}) = e'

$\Rightarrow f\ (x)\ f\ (y^{-1}) = e'$ $(since\ f\ is\ Homomorphism)$

$\Rightarrow f\ (x)\ [f\ (y)]^{-1} = e'$

$\Rightarrow f\ (x) = f\ (y)$

$\Rightarrow \varphi(Kx) = \varphi(Ky)$

$\therefore \varphi\ is\ well\ defined\ function$

2) $\varphi\ is\ one-one\ function\ G\ /\ K \rightarrow G'$:

$For\ all\ Kx, Ky\ in\ G/K$

$Let\ \varphi(Kx) = \varphi(Ky) \Rightarrow f\ (x) = f\ (y)$

$\Rightarrow f\ (x)\ [f\ (y)]^{-1} = f\ (y)\ [f\ (y)]^{-1}$

$\Rightarrow f\ (x)\ f(y^{-1}) = e'$ $since\ f\ (y)\ in\ G'\ and\ is\ Homomorphism$

$\Rightarrow f\ (x\,y^{-1}) = e'$

$\Rightarrow xy^{-1} \in Ker\ f$ $but\ Ker\ f = K$

$\Rightarrow xy^{-1} \in K$

$\Rightarrow Kx = Ky.$

$\therefore \varphi\ is\ one-one$

3) $\varphi\ is\ onto$:

$As\ \varphi : G/K \rightarrow G' = f(G)\ is\ the\ function\ for\ any\ y = f(x) \in G'\ and\ f\ is\ onto$

$\exists\, x \in G \Rightarrow K\ x \in G/K\ such\ that$

$\varphi\ (Kx) = y = f\ (x)$

$\Rightarrow \varphi\ is\ onto.$

4). $\boldsymbol{\varphi}$ is Homomorphism:

$For\ all\ K\,x, K\,y\ in\ G/K$

$To\ verify\ that\ \varphi\ [(K\,x)\ (K\,y)] = \varphi\ (K\,x)\ \varphi\ (K\,y)$

$LHS = \varphi\ [(K\,x)\ (K\,y)] = \varphi\ [K\,x\,y]$ $since\ K\ is\ Normal\ subgroup\ of\ G$

$= f(x\,y)$ $by\ the\ definition\ of\ \varphi$

$= f(x)\,f(y)$ $since\ f\ is\ homomorphism$

$= \varphi\ (K\,x)\ \varphi\ (K\,y) = RHS$

$Hence\ \varphi\ is\ an\ isomorphism\ and\ \boldsymbol{G\ /\ K} \cong \boldsymbol{G'}$

Result: $Show\ that\ the\ mapping\ a \to a^{-1}\ is\ Automorphism\ on\ G\ \ iff\ \ G\ is\ abelian.$

$Proof$:

$\Rightarrow\ part$ $\ suppose\ f: G \to G\ is\ an\ Automorphism\ defined\ by$

$$f(a) = a^{-1}\quad for\ all\ a \in G$$

$to\ show\ that\ G\ is\ abelian\ group$

$for\ all\ a, b \in G\ and\ f\ is\ Homomorphism$

$$\therefore\ f(a\,b) = f(a)\,f(b)$$

$$\Rightarrow (ab)^{-1} = a^{-1}\ b^{-1}$$

$$\Rightarrow (ab)^{-1} = (ba)^{-1}$$

$$\Rightarrow a\,b = b\,a$$

$$\therefore\ G\ is\ abelian\ group.$$

$\Leftarrow\ part$ $\ suppose\ G\ is\ abelian\ group\ \ To\ show\ that\ f\ is\ Automorphism$

1) $one-one$: $for\ all\ a, b \in G$

$$Let\quad f(a) = f(b) \Rightarrow a^{-1} = b^{-1}$$

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

$$\Rightarrow a = b$$

2)$onto$: $for\ all\ \ y \in G\ \ \exists\ x \in G \Rightarrow x^{-1} \in G(\,Group)\ such\ that\ y = f(x) = x^{-1} \in G.$

3) $Homomorphism$: $for\ all\ a, b \in G$

$$f(a\,b) = (ab)^{-1} = (ba)^{-1} = a^{-1}b^{-1} = f(a)f(b)\ \ (\,since\ G\ is\ abelian\ group\,)$$

$$Hence\ f\ is\ Automorphism$$

****

Permutation Groups

- B SRINIVASARAO.GDC RVPM

Definition: A one -one and onto function from a finite set S into S is called a permutation.

If S = {1,2,3,4,5,6} and f: S→ S is one-one and onto function then the permutation is denoted by

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 2 & 6 & 5 \end{pmatrix}$$

Product of two permutations:

If $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 1 & 3 & 6 & 2 \end{pmatrix}$ $\quad g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 2 & 6 & 4 & 1 \end{pmatrix}$

Then $fg = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 1 & 3 & 6 & 2 \end{pmatrix}$

$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 3 & 2 & 1 & 5 \end{pmatrix}$

$gf = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 2 & 6 & 4 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 1 & 3 & 6 & 2 \end{pmatrix}$

$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 4 & 2 & 3 & 5 \end{pmatrix}$

Clearly $fg \neq gf$

Identity Permutation: A permutation is in the form

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$ is called Identity permutation.

Inverse of a permutation:

If $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 1 & 3 & 6 & 2 \end{pmatrix}$ $then\ its\ inverse\ is$ $\begin{pmatrix} 5 & 4 & 1 & 3 & 6 & 2 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$ or

$$f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 2 & 1 & 5 \end{pmatrix}$$

Note that $f.f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 1 & 3 & 6 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 2 & 1 & 5 \end{pmatrix}$

$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$

Note: If a finite set S containing n elements, then the number permutations formed from S into S are n!

Note: The set of permutations form a group w r t permutation multiplication and is called permutation group.

Cyclic Permutation: A permutation is in the form

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix}$ of length 6 and is simply denoted by (1 2 3 4 5 6).

And $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 4 & 5 & 6 & 1 & 8 & 9 & 7 \end{pmatrix}$ Is also cyclic and is denoted by (1 2 3 4 5 6) (7 8 9)

Also $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 1 & 4 & 5 & 7 & 8 & 6 & 9 \end{pmatrix}$ *is cyclic denoted by* $(1\ 2\ 3)(4)(5)(6\ 7\ 8)(9)$

It's length $3 + 3 = 6$.

Cyclic permutations: There no common element between two cycles called disjoint cycles.

That is f = $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}\begin{pmatrix} 5 & 6 & 7 & 8 & 9 \\ 6 & 7 & 8 & 9 & 1 \end{pmatrix}$ are disjoint cycles.

Transposition: A transposition is cyclic permutation of length 2.

Example: $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = (1\ 2), \begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix} = (2\ \ 3)\ \ e\ t\ c$

Note: (1 2 3 4 5 6) = (1 2)(1 3)(1 4)(1 5)(1 6)

Even and Odd permutations:

A permutation f said to be Even if f can be expressed as even number of transpositions and it can be expresses as odd number of transpositions then it is Odd permutation.

Example:1 If f = (1 2 3 4 5 6 7) = (1 2) (1 3) (1 4) (1 5) (1 6) (1 7)

Number of transpositions = 6 so, it is even permutation

Example:2 If f = (1 2 3 4 5 6) = (1 2) (1 3) (1 4) (1 5) (1 6)

Number of transpositions = 5 so, it is Odd permutation.

Problems:

If write the permutations into disjoint cycles

1. (1 3 2)(5 6 7)(2 6 1)(4 5)
2. (1 3 6)(1 3 5 7)(6 7)(1 2 3 4)

Solution: 1. Given that f = (1 3 2)(5 6 7)(2 6 1)(4 5)

$$= \begin{pmatrix} 1 & 3 & 2 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 5 & 6 & 7 \\ 6 & 7 & 5 \end{pmatrix} \begin{pmatrix} 2 & 6 & 1 \\ 6 & 1 & 2 \end{pmatrix} \begin{pmatrix} 4 & 5 \\ 5 & 4 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 6 & 5 & 1 & 7 & 4 \end{pmatrix}$$

$$f = \begin{pmatrix} 1 & 3 & 6 & 7 & 4 & 5 \\ 3 & 6 & 7 & 4 & 5 & 1 \end{pmatrix} \begin{pmatrix} 2 \\ 2 \end{pmatrix} = (1\ 3\ 6\ 7\ 4\ 5)(2)\, disjoint\ cycles$$

2.Given that f = (1 3 6)(1 3 5 7)(6 7)(1 2 3 4)

$$= \begin{pmatrix} 1 & 3 & 6 \\ 3 & 6 & 1 \end{pmatrix} \begin{pmatrix} 1 & 3 & 5 & 7 \\ 3 & 5 & 7 & 1 \end{pmatrix} \begin{pmatrix} 6 & 7 \\ 7 & 6 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 3 & 7 & 1 & 6 & 4 & 2 \end{pmatrix}$$

$$f = \begin{pmatrix} 1 & 5 & 6 & 4 \\ 5 & 6 & 4 & 1 \end{pmatrix} \begin{pmatrix} 2 & 3 & 7 \\ 3 & 7 & 2 \end{pmatrix} = (1\ 5\ 6\ 4)(2\ 3\ 7)\, disjoint\ cycles$$

Note: The inverses of above permutations are

1.$f^{-1} = (5\ 4\ 7\ 6\ 3\ 1)(2)$ 2.$f^{-1} = (4\ 6\ 5\ 1)(7\ 3\ 2)$

If write the permutations into disjoint cycles and find whether they are Even or Odd

1. (1 3 2)(5 6 7)(2 6 1)(4 5)

2. (1 3 6)(1 3 5 7)(6 7)(1 2 3 4)

Solution: 1. Given that f = (1 3 2)(5 6 7)(2 6 1)(4 5)

$$= \begin{pmatrix} 1 & 3 & 2 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 5 & 6 & 7 \\ 6 & 7 & 5 \end{pmatrix} \begin{pmatrix} 2 & 6 & 1 \\ 6 & 1 & 2 \end{pmatrix} \begin{pmatrix} 4 & 5 \\ 5 & 4 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 6 & 5 & 1 & 7 & 4 \end{pmatrix}$$

$$f = \begin{pmatrix} 1 & 3 & 6 & 7 & 4 & 5 \\ 3 & 6 & 7 & 4 & 5 & 1 \end{pmatrix} \begin{pmatrix} 2 \\ 2 \end{pmatrix} = (1\ 3\ 6\ 7\ 4\ 5)(2)\, disjoint\ cycles$$

Again f = $(1\ 3\ 6\ 7\ 4\ 5)(2)$ = (1 3)(1 6)(1 7)(1 4)(1 5)(2)

Number of transpositions = 4 Even permutation

2.Given that f = (1 3 6)(1 3 5 7)(6 7)(1 2 3 4)

$$= \begin{pmatrix} 1 & 3 & 6 \\ 3 & 6 & 1 \end{pmatrix} \begin{pmatrix} 1 & 3 & 5 & 7 \\ 3 & 5 & 7 & 1 \end{pmatrix} \begin{pmatrix} 6 & 7 \\ 7 & 6 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 3 & 7 & 1 & 6 & 4 & 2 \end{pmatrix}$$

$$f = \begin{pmatrix} 1 & 5 & 6 & 4 \\ 5 & 6 & 4 & 1 \end{pmatrix} \begin{pmatrix} 2 & 3 & 7 \\ 3 & 7 & 2 \end{pmatrix} = (1\ 5\ 6\ 4)(2\ 3\ 7)\, disjoint\ cycles$$

Again f $=(1\ 5\ 6\ \ 4)(2\ \ 3\ \ 7) = (1\ \ 5)(1\ \ 6)(1\ \ 4)(2\ \ 3)(2\ \ 7)$

Number of transpositions = 5   Odd permutation

7.Show that f = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 4 & 5 & 6 & 7 & 1 \end{pmatrix}$ is Odd permutation.

Solution: Given that f = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 4 & 5 & 6 & 7 & 1 \end{pmatrix}$

$$= \begin{pmatrix} 1 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 5 & 6 & 7 & 1 \end{pmatrix}\begin{pmatrix} 2 \\ 2 \end{pmatrix} = (1\ \ 3\ \ 4\ \ 5\ \ 6\ \ 7)(2)$$

$$= (1\ \ 3)(1\ \ 4)(1\ \ 5)(1\ \ 6)(1\ \ 7)(2)$$

Number of Transpositions = 5   Therefore, it is Odd Permutation.

8. Show that f = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 3 & 1 & 8 & 5 & 6 & 2 & 4 \end{pmatrix}$ is Even permutation.

Solution: Given that f = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 3 & 1 & 8 & 5 & 6 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 7 & 2 & 3 \\ 7 & 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 4 & 8 \\ 8 & 4 \end{pmatrix}\begin{pmatrix} 5 \\ 5 \end{pmatrix}\begin{pmatrix} 6 \\ 6 \end{pmatrix}$

$$=(1\ \ 7\ \ 2\ \ 3)(4\ \ 8)(5)(6)$$

$$= (1\ \ 7)(1\ \ 2)(1\ \ 3)(4\ \ 8)(5)(6)$$

Number of Transpositions = 4   Therefore, it is Even Permutation.

9.If G = $\{1, \omega, \omega^2\}$ is a group then find all the regular permutations of G.

Solution: Given G = $\{1, \omega, \omega^2\}$ By Cayley's theorem $f_a(x) = ax$ $for\ all\ x \in G$

Now the regular permutations are $\{f_1, f_\omega, f_{\omega^2}\}$ where

$$f_1 = \begin{pmatrix} 1 & \omega & \omega^2 \\ 1.1 & 1.\omega & 1.\omega^2 \end{pmatrix} = \begin{pmatrix} 1 & \omega & \omega^2 \\ 1 & \omega & \omega^2 \end{pmatrix}$$

$$f_{\omega,} = \begin{pmatrix} 1 & \omega & \omega^2 \\ \omega.1 & \omega.\omega & \omega.\omega^2 \end{pmatrix} = \begin{pmatrix} 1 & \omega & \omega^2 \\ \omega & \omega^2 & 1 \end{pmatrix}$$

$$f_{\omega^2} = \begin{pmatrix} 1 & \omega & \omega^2 \\ \omega^2.1 & \omega^2.\omega & \omega^2.\omega^2 \end{pmatrix} = \begin{pmatrix} 1 & \omega & \omega^2 \\ \omega^2 & 1 & \omega \end{pmatrix}.$$

10 Marks Questions.

10.State and prove Cayley's theorem for permutation groups.

Statement: Every finite Group is Isomorphic to Permutation Group.

Proof: Let G is finite group.

Step:1 For any a $\in G$ Define a function

$$f_a : G \to G \text{ by } f_a(x) = ax \ \ for\ all\ x \in G$$

To show that f_a is both one-one and onto function

i) $\boldsymbol{f_a}$ ***is one-one*** : For all $x, y \in G$ f_a (x)= f_a (y)

$\Rightarrow$ ax = ay $\Rightarrow$ x = y (by cancellation law)

ii) $\boldsymbol{f_a}$ **is onto**: $for\ all\ y \in G(image)\ \exists\ x \in G\ such\ that$

$y = f_a\,(x) \Rightarrow$ y = ax $\Rightarrow$ x = a^{-1}y $\in G$.

Therefore f_a is a permutation.

Step-2 To collect all such permutations $G' = \{ f_a : a \in G \}$

To show that G' is a Group wrt composition of functions.

1.Closure property: for all f_a , f_b $\in$ G' then

$(f_a f_b)(x) = f_a\,[f_b\,(x)] = f_a\,(bx) = f_a\,(y) = ay = a(bx) = (ab)x = f_{ab}(x)$

$\Rightarrow f_a f_b = f_{ab} \in G'$

2)Associate property: For all $f_a, f_b, f_c \in G'$ then

$[\,f_a(f_b\,f_c)] = [\,f_a(f_{bc}\,)]$

$= [\,f_{a(bc)}]$

$=[\,f_{(ab)c}]$

$=[\,f_{(ab)}f_c]$

$=[\,(\,f_a f_b)\,f_c]$.

Therefore $[\,f_a(f_b\,f_c)] = [\,(\,f_a f_b)\,f_c]$.

3)Identity property: for all $f_a \in G'\ \exists\ a\ pemutation\ f_e$ (since e $\in G$) such that

$f_a f_e = f_{ae} = f_a$ and $f_e f_a = f_{ea} = f_a$.

Identity element exist.

4) Inverse Property: for all $f_a \in G'$ $\exists$ *a pemutation* $f_{a^{-1}} \in G'$ (since $a^{-1} \in G$) such that

$$f_a f_{a^{-1}} = f_{aa^{-1}} = f_e \text{ and } f_{a^{-1}} f_a = f_{a^{-1}a} = f_e.$$

$\therefore$ for all $f_a \in G'$ we get $f_{a^{-1}} \in G'$

Inverse property exists.

Hence G' is a group and is permutation group.

Step:3 Finally to show that G' $\cong$ G

Define a function $\varphi: G \to G'$ by $\varphi(a) = f_a$ for all a$\in G$

1.φ *is one − one* : For all a, b $\in G$

Let $\varphi(a) = \varphi(b) \Rightarrow f_a = f_b \Rightarrow f_a(x) = f_b(x) \Rightarrow$ ax = bx $\Rightarrow$ a = b

2. φ *is onto*: for all f_a in G' there exist a $\in G$ such that $\varphi(a) = f_a$.

3. φ *is homomorphism*: For all a, b $\in G$

$$\varphi(ab) = f_{ab} = f_a f_b = \varphi(a)\, \varphi(b)$$

$\therefore$ *φ is one − one, onto and homomorphism and hence Isomorphism*

11.If f = (1 2 3 4 5 8 7 6) and g = (4 1 5 6 7 3 2 8) then show that

$$(f\, g)^{-1} = g^{-1} f^{-1}$$

Solution: Given that f = (1 2 3 4 5 8 7 6) and g = (4 1 5 6 7 3 2 8)

That is f = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 8 & 7 & 6 \\ 2 & 3 & 4 & 5 & 8 & 7 & 6 & 1 \end{pmatrix}$ g = $\begin{pmatrix} 4 & 1 & 5 & 6 & 7 & 3 & 2 & 8 \\ 1 & 5 & 6 & 7 & 3 & 2 & 8 & 4 \end{pmatrix}$

Now f g = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 8 & 7 & 6 \\ 2 & 3 & 4 & 5 & 8 & 7 & 6 & 1 \end{pmatrix}\begin{pmatrix} 4 & 1 & 5 & 6 & 7 & 3 & 2 & 8 \\ 1 & 5 & 6 & 7 & 3 & 2 & 8 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 2 & 1 & 6 & 4 & 5 & 7 & 3 \end{pmatrix}$

$$(f\, g)^{-1} = \begin{pmatrix} 8 & 2 & 1 & 6 & 4 & 5 & 7 & 3 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 8 & 5 & 6 & 4 & 7 & 1 \end{pmatrix}$$

Also $f^{-1} = \begin{pmatrix} 2 & 3 & 4 & 5 & 8 & 7 & 6 & 1 \\ 1 & 2 & 3 & 4 & 5 & 8 & 7 & 6 \end{pmatrix}$ and $g^{-1} = \begin{pmatrix} 1 & 5 & 6 & 7 & 3 & 2 & 8 & 4 \\ 4 & 1 & 5 & 6 & 7 & 3 & 2 & 8 \end{pmatrix}$

$$g^{-1}f^{-1} = \begin{pmatrix} 1 & 5 & 6 & 7 & 3 & 2 & 8 & 4 \\ 4 & 1 & 5 & 6 & 7 & 3 & 2 & 8 \end{pmatrix}\begin{pmatrix} 2 & 3 & 4 & 5 & 8 & 7 & 6 & 1 \\ 1 & 2 & 3 & 4 & 5 & 8 & 7 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 8 & 5 & 6 & 4 & 7 & 1 \end{pmatrix}.$$

Hence $(f\,g)^{-1} = g^{-1}f^{-1}$

12.State Cayley's theorem for permutation group and if

$G = \{1, -1, i, -i\}$ is a group find all the regular permutations of G.

Solution: *Given $G = \{1, -1, i, -i\}$ By Cayley's theorem $f_a(x) = ax$ for all $x \in G$*

Now the regular permutations are $\{ f_1, f_{(-1)}, f_i f_{-i} \}$ were

$$f_1 = \begin{pmatrix} 1 & -1 & i & -i \\ 1.1 & 1(-1) & 1(i) & 1(-i) \end{pmatrix} = \begin{pmatrix} 1 & -1 & i & -i \\ 1 & -1 & i & -i \end{pmatrix}$$

$f_{(-1)} = \begin{pmatrix} 1 & -1 & i & -i \\ -1 & 1 & -i & i \end{pmatrix}$ $\quad f_i = \begin{pmatrix} 1 & -1 & i & -i \\ i & -i & -1 & 1 \end{pmatrix}$ *and* $\quad f_{(-i)} = \begin{pmatrix} 1 & -1 & i & -i \\ -i & i & 1 & -1 \end{pmatrix}$ *since* $i^2 = -1$ *and* $-i^2 = 1$

&&&&&&&&&&&

GOVERNMENT DEGREE COLLEGE:: RAVULAPALEM
(An outcome based Institution since 1981 Affiliated to
Adikavi Nannaya University)
East Godavari District, ANDHRA PRADESH, INDIA 533 238

RING THEORY

By B. Srinivas Rao. Lecturer in Mathematics.

RINGS-I

UNIT – 1

Definition of Ring and basic properties, Boolean Rings, divisors of zero and cancellation laws Rings, Integral Domains, Division Ring and Fields, The characteristic of a ring - The characteristic of an Integral Domain, The characteristic of a Field. Sub Rings, Ideals

Definition (Ring).

A non-empty ser R is said to be a ring w.r.t two binary operations (+) and multiplication(.) if it satisfies the following properties

I.R is an abelian group under addition

(1). For all a, b ∈R then a+ b ∈ R (Closure)

(2) (Associativity) For all a, b and c in R, (a + b) + c = a + (b + c).

(3) For any a ∈R There is an element 0 ∈ R(identity) such that for all a in R a + 0 = 0 + a = a.

(4) For all a in R, there exists b ∈ R such that a + b = b + a = 0. b will be denoted −a.

(5) For all a and b in R, a + b = b + a.

II Semi-Group w r t Multiplication.

(6) For all a, b ∈R then a . b ∈ R

(7) For all a, b and c in R, (a · b) · c = a · (b · c).

III (8) (Distributivity Properties)

For all a, b and c in R, we have a · (b + c) = a · b + a · c (Left Distributive law)

(b + c) · a = b · a + c · a (Right Distributive Law)

Example: The set of Integers Z = {. . . . . -3, -2, -1, 0, 1, 2, 3, ... } is a Ring w r t Addition and multiplication.

Example: The set of Rationales Q= $\{ p/q : p, q \in Z, q \neq 0 \}$ is also Ring w r t Addition and multiplication.

General properties on rings:

Let R is a ring then prove that for all a, b, c ∈ R then

1. $a\,0 = 0 = 0\,a$ 2. $a\,(-b) = -(a\,b) = (-a)\,b$

$3. (-a)(-b) = ab$ $4. a(b - c) = ab - ac$

Proof: $1. As\ a\,0 = a(0 + 0) = a0 + a\,0 \qquad (\because\ a (b + c) = a\,b + a\,c\ in\ R)$

$\therefore\ a\,0 = a0 + a\,0$

$\Rightarrow\ 0 + a\,0 = a0 + a\,0 \qquad \because\ a = a + 0\ in\ R$

$\Rightarrow$ 0 = a 0 $\qquad \because$ By cancellation.

$Similarly, to\ prove\ 0\,a = 0$

$2. As\ 0 = a0 = a[b + (-b)] = a\,b + a(-b)$

$\therefore\ 0 = a\,b + a(-b)$---(1)

Again $0 = a0 = a[(-b) + b] = a (-b) + a\,b$

$\therefore\ 0 = a(- b) + a\,b$ -----(2)

$From\ (1)\ and (2)\ a\,b + a(-b) = 0 = a(- b) + a\,b$

$\Rightarrow\ a (-b) = -(a\,b)$

$Similarly\ to\ prove\ (-a)b = -(a\,b) .$

3. $(-a)(-b) = (-a)x = -(a\,x) \qquad where\ x = -b\ and\ \because\ (-a) b = -(a\,b)$

$= -[a (-b)]$

$= -[-(a\,b)] (\because\ a (-b) = -(a\,b)$

$= a\,b$

$4. a (b - c) = a [b + (- c)] = a\,b + a (-c) (\because\ by\ left\ distributive\ law)$

$= a\,b - ac .$

$Definition: (Zero\ divisors)$

$A\ non\ zero\ element\ a \neq 0 \in R\ is\ said\ to\ be\ zero\ divisor\ if$

$\exists\ b \neq 0 \in R\ such\ that\ a\,b = 0.$

$Example: In\ the\ ring\ of\ 2 \times 2\ matrices\ R$

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \neq 0, B = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \neq 0\ such\ that\ AB = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = 0$$

$\Rightarrow$ A and B are Zero divisors.

$Definition: (Without\ Zero\ divisors):$

In a ring R for any a , b ∈ R if a b = 0 ⇒ either a= or b=0 then we say a, b are without zero divisors.or if a ≠ 0 and b≠ 0 then a b ≠ 0 in the ring R.

Example: In the ring of integers Z for any a = 5 ≠ 0, b=8 ≠ 0 then a b = 5× 8 = 40 ≠ 0.

Definition (Integral domain) :

$A \ ring \ < D,+,.> \ is \ said \ to \ be \ an \ Integral \ domain \ if \ it \ satisfies$

1. $Unity \ (1 \in D)$
2. $Commutative \ w \ r \ t \ multiplication \ i \ e \ ab = b \ a \ for \ all \ a,b \in D$

3. $Without \ zero \ devisors \ property \ ie \ for \ all \ a,b \in D \ if \ a \ b = 0 \ then$

$a = 0 \ or \ b = 0. or \ if \ a \neq 0, b \neq 0 \ then \quad ab \neq 0 \ for \ all \ a,b \in D$

$Example$: 1. $The \ ring \ of \ Integers \ Z = \{.....-3,-2,-1,0,1,2,3,\} \ form \ an \ Integral \ domain.$

$Example$: 2. $The \ ring \ of \ rational \ Q, The \ ring \ of \ Reals \ R \ are \ also \ Integral \ domains.$

Definition (Field) :

$A \ ring \ < F,+,.> \ is \ said \ to \ be \ a \ Field \ if \ it \ satisfies$

1. $Unity \ (1 \in D)$
2. $Commutative \ wrt \ multiplication \ i \ e \ ab = b \ a \ for \ all \ a,b \in D$

3. $Multiplicative \ Inverse \ Property \ for \ all \ a \neq 0 \in F \ there \ exist$ $a^{-1} \in F$ such that

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

Example:

1. The ring of Integers Z = {. . . . . -3, -2, -1, 0, 1, 2, 3, ... } is not a field since multiplicative inverse property does not exist. Since for a = 3 ∈ Z then $a^{-1} = \frac{1}{3} \notin Z$

2. The ring of rational Q , The ring of Real numbers R are Fields and the ring of Complex numbers form a field $i \ e \ \{x + iy \,/\, x,y \in R \ and \ i = \sqrt{-1}\}$.

$Division \ Ring \ or \ Skew \ field$:

$A \ ring \ < R,+,.> \ is \ said \ to \ be \ a \ skew \ Field \ if \ it \ satisfies$

1. Unity (1 ∈ R)

2. Multiplicative Inverse Property for all a ≠0 ∈ F there exist $a^{-1} \in R$ such that $a.a^{-1} = 1 = a^{-1}a$.

Example: The ring of Non-singular matrices forms a skew field

Boolean Ring: A Ring R is Said to be a Boolean Ring if it satisfies Idempotent property

$That \ is \ for \ all \ a \in R \ then \ a^2 = a$

Theorem:

Prove that in a ring R without zero divisors if and only if cancellation laws.

$Proof: \Rightarrow\ part$

$Let\ R\ has\ without\ zero\ divisors\ to\ find\ cancellation\ laws$

$For\ any\ a\ \neq 0, b, c\ \in\ R$

$If\ a\,b\ =\ a\,c\ \Rightarrow\ b = c\ (\,Left\ cancellation\ law)$

$If\ b\,a\ =\ c\,a\ \Rightarrow\ b = c\ (Right\ cancellation\ law)$

$$If\ a\,b\ =\ a\,c\ \Rightarrow\ a\,b\ -\ a\,c\ = 0$$

$$\Rightarrow\ a\,(\,b\ -\ c)\ = 0$$

$By\ Without\ Zero\ Divisors\ Property$

$Either\ a\ =\ 0\ or\ b\ -\ c\ =\ 0\ \ but\ a\ \neq 0 \therefore\ b - c\ =\ 0\ \Rightarrow\ b =\ c\,.$

$Similarly\ to\ prove\ Right\ cancellation\ law.$

$\Leftarrow\ Part$

$Suppose\ cancellation\ laws\ holds\ in\ the\ ring\ R.$

$To\ find\ without\ zero\ divisors\ property$

$for\ any\ a, b \in\ R\ Let\ a\,b\ =\ 0\ and\ a \neq 0, b \neq 0.$

$\Rightarrow\ a\,b\ =\ a0\ \Rightarrow\ b = 0\ (\because\ by\ Left\ cancellation\ law\,)$

$But\ b \neq 0\ it\ is\ a\ contradiction$

$\therefore\ a\ =\ 0\ or\ b\ =\ 0.$

Theorem:

$Prove\ that\ every\ field\ is\ an\ integral\ domain\ .also\ show\ that\ using\ an\ example\ converse\ is\ not\ true$

$Poof$: $Suppose\ F\ is\ a\ field\ ie\ It\ is\ a\ ring\ having$

1. $Commutative,$
2. $unity\ and$
3. $Multiplicative\ inverse\ property$

,

$To\ show\ that\ F\ is\ an\ Integral\ domain\ That\ is\ only\ to\ find\ without\ zero\ divisors\ property\ in\ F.$

$ie\ For\ all\ a\,, b\ \in\ F\ if\ a\,b\ = 0\ \Rightarrow\ a\ =\ 0\ or\ b\ =\ 0.$

$Case - 1$ $let\ a\,b\ = 0\ and\ a\ \neq\ 0\ \in\ F(\because\ a\ \neq\ 0\ \in\ F\ (\,field)\ \Rightarrow a^{-1}\ \in\ F\,)$

$\Rightarrow\ a^{-1}(a\,b\,)\ =\ a^{-1}\,0\ = 0$

$\Rightarrow\ (\,a^{-1}\,a\,)\,b\ =\ 0$

$\Rightarrow\ (\,1\,)\,b\ =\ 0$

$\Rightarrow\ b\ =\ 0.$

Case − 2 $let\ a\ b\ = 0\ and\ b\ \neq\ 0\ \in\ F$ (∵ b ≠ 0 ∈ F (field) ⇒ b^{-1} ∈ F)

⇒ (a b) b^{-1} = 0 b^{-1} =0

⇒ a (b b^{-1}) = 0

⇒ a (1) = 0

⇒ a = 0. ∴ For all a , b ∈ F if a b =0 ⇒ a = 0 or b = 0

$Hence\ F\ is\ an\ integral\ domain.$

Example: The ring of Integers Z = {. . . . . -3, -2, -1, 0, 1, 2, 3, ... } is an integral domain but not a field sincemultiplicative inverse property does not exist. Since for a= 3 ∈ Z then a^{-1} = 1/3 is not in Z

Theorem : Prove that every finite Integral domain is a Field.

Proof: Suppose D $= \{a_1,\ a_2,\ a_3, \dots \dots\ a_n\}\ where\ a_i \neq a_j\ for\ i \neq j$ ------(1)

$is\ a\ finite\ Integral\ domain\ containing\ exactly\ n\ elements$

$Therefore, D\ is\ a\ ring\ having\ Unity\ Commutative\ and\ Without\ zero\ devisors\ property$

$To\ Show\ that\ D\ is\ a\ field\ ie\ only\ to\ find\ the\ Multiplicative\ Inverse\ Property.$

ie for all a ≠ 0 ∈ D there exist a^{-1} ∈ D such that a.a^{-1} =1 = a^{-1} a .

Consider a set a D = { $a\,a_1, aa_2, a\,a_3 \dots\dots, a\,an$ } is also contained in D (∵ Closure in D)

Since for $a\,ai\ = a\,aj \quad for\ i\ \neq\ j$

$\Rightarrow\ a\,ai - a\,aj\ = 0\ \ for\ i\ \neq\ j$

$\Rightarrow\ a\,(a\,i - a\,j\,)\ =\ 0\ \ for\ i\ \neq\ j$

$\Rightarrow\ a\ =\ 0\ or\ (a\,i - a\,j\,) =\ 0\ for\ i\ \neq\ j$ (by Without zero devisors property)

$But\ a\ \neq 0\ \ \therefore\ (a\,i - a\,j\,) =\ 0\ for\ i\ \neq\ j$

$\Rightarrow\ a\,i\ =\ a\,j\ \ \ for\ i\ \neq\ j\ since\ (1)$

$\therefore\ a\,D\ and\ D\ containing\ exactly\ n\ elements\ \Rightarrow\ a\,D\ =\ D, but\ 1\ \in\ D\ \Rightarrow\ 1\ \in\ a\,D$

By the definition of a D ∃ a_k ∈ D such that $1 = aa_k = a_k a$

It follows a_k is the inverse of $a\ \in\ D$ Inverse property exist

Hence D is a Field.

Example: Let D = { $1, \omega, \omega^2$ } is a finite group wrt multiplication

Then D ω = { $1.\omega, \omega.\omega,, \omega^2.\omega$ } = { $\omega, \omega^2, \omega^3$ } = { $\omega, \omega^2, 1$ } = D

∴ D ω = D But 1 ∈ D ⇒ 1 ∈ D ω ⇒ 1 = $\omega^2.\omega$ ⇒ ω^2 *is the Inverse of* ω

Theorem: In a ring R for all $a \in R$, $a^2 = a$ (idempotent law) , prove that

1. $a + a = 0$ $\quad$ $for\ all\ a \in R$

2. $if\ a + b = o\ then\ a = b$ $\quad$ $for\ all\ a, b \in R$

3. $R\ is\ a\ commutative\ ring.$

Proof: 1. for all $a \in R \Rightarrow$ for all $a, a \in R \Rightarrow a + a \in R$

Let $a + a = x \in R$

By idempotent property $x^2 = x$

$$\Rightarrow (a + a)^2 = a + a$$

$$\Rightarrow (a + a)(a + a) = a + a.$$

$$\Rightarrow a(a + a) + a(a + a) = a + a.$$

$$\Rightarrow a^2 + a^2 + a^2 + a^2 = a + a.$$

$$\Rightarrow a + a + a + a = a + a + 0 \quad (\because for\ all\ a \in R, a^2 = a)$$

$$\Rightarrow a + a = 0 (\because Cancellation\ law)$$

2. $Given\ a + b = 0 = a + a (\because a + a = 0)$

$$\Rightarrow b = a\ i.e.\ a = b$$

2. R is a commutative ring.

for all $a, b \in R \Rightarrow a + b \in R$

Let $a + b = x \in R$

By idempotent property $x^2 = x$

$$\Rightarrow (a + b)^2 = a + b$$

$$\Rightarrow (a + b)(a + b) = a + b.$$

$$\Rightarrow a(a + b) + b(a + b) = a + b.$$

$$\Rightarrow a^2 + ab + ba + b^2 = a + b.$$

$$\Rightarrow a + ab + ba + b = a + b \quad (\because \text{for all } a \in R, a^2 = a)$$

$$\Rightarrow ab + ba = 0 (\because cancellation\ law)$$

$$\Rightarrow ab = ba (\because if\ a + b = o\ then\ a = b)$$

Problem:

Show that $R = \{ a + b\sqrt{2} : a, b \in Q \}$ form a field with respect to addition and multiplication.

Solution: Given $R = \{ a + b\sqrt{2} : a, b \in Q \}$ to show that R is field using Q is a field.1.for all $x = a_1 + b_1\sqrt{2}$ $\quad y = a_2 + b_2\sqrt{2}$ in R then

$$x + y = (a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2})$$

$$= (a_1 + a_2) + (b_1 + b_2)\sqrt{2}$$

$= a' + b'\sqrt{2} \in R$ where $a' = (a_1 + a_2)$, $b' = (b_1 + b_2) \in Q$

$x\,y = (a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2})$

$= (a_1 a_2 + 2 b_1 b_2) + (a_1 b_2 + b_1 a_2)\sqrt{2}$

$= a'' + b''\sqrt{2} \in R$ where $a'' = (a_1 a_2 + 2 b_1 b_2)$ $b'' = (a_1 b_2 + b_1 a_2) \in Q$

Closure property holds w r t addition and multiplication

2.A) For all $x = a + b\sqrt{2} \in R$ there is an element $\bar{0} = 0 + 0\sqrt{2} \in R$ ($\because$ $0 \in Q$) Such that

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

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

$\therefore$ $\bar{0} = 0 + 0\sqrt{2} \in R$ is the Identity wrt addition

B) for all $x = a + b\sqrt{2} \in R$ there is an element $\bar{1} = 1 + 0\sqrt{2} \in R$ ($\because 1, 0 \in Q$)

Such that $x\,.\bar{1} = (a + b\sqrt{2})(1 + 0\sqrt{2}) = (a\,1) + (b+0)\sqrt{2} = (a + b\sqrt{2}) = x$

$\bar{1}.\,x = (1 + 0\sqrt{2})(a + b\sqrt{2}) = (1.a) + (0 + b)\sqrt{2}$

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

$\therefore$ $\bar{1} = 1 + 0\sqrt{2} \in R$ is the Identity wrt Multiplication

3.A) for all $x = a + b\sqrt{2} \in R$ there is an element $-x = -a + (-b)\sqrt{2} \in R$ ($\because$ for all $a \in Q \Rightarrow -a \in Q$)

Such that $x + (-x) = (a + b\sqrt{2}) + [-a + (-b)\sqrt{2}] = [a + (-a)] + [b + (-b)]\sqrt{2}$

$= (0 + 0\sqrt{2}) = \bar{0}$

$(-x) + x = [-a + (-b)\sqrt{2}] + (a + b\sqrt{2}) = [(-a) + a] + [(-b) + b]\sqrt{2}]$

$= (0 + 0\sqrt{2}) = \bar{0}$

$-x = -a + (-b)\sqrt{2} \in R$ is the inverse of x w r t addition

B) for all $x = a + b\sqrt{2} \in R$ $\exists$ an element

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

$= \dfrac{1}{a + b\sqrt{2}} \times \dfrac{a - b\sqrt{2}}{a - b\sqrt{2}} = \dfrac{a - b\sqrt{2}}{a^2 - 2b^2} = \dfrac{(a)}{a^2 - 2b^2} + \dfrac{(-b)}{a^2 - 2b^2}\sqrt{2} \in R$ is the inverse

element of $x \in R$ since $\dfrac{a}{a^2 - 2b^2} \in Q$ and $\dfrac{(-b)}{a^2 - 2b^2} \in Q$

4) As R contain all Real numbers but the set of all real numbers form a field and hence the remaining properties of the field are all exist in R

ie Associative, Commutative and Distributive laws wrt addition and multiplication are exist.

$< R, +, . >$ is a field

Problem:

Show that $R = \{ a + b\sqrt{2} : a, b \in Z \}$ form an Integral domain with respect to addition and multiplication.

Solution: Given $R = \{ a + b\sqrt{2} : a, b \in Z \}$ to show that R is an Integral domain using Z is Integral domain.

1.A) for all $x = a_1 + b_1\sqrt{2}$ $y = a_2 + b_2\sqrt{2}$ in R then

$$x + y = (a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2})$$

$$= (a_1 + a_2) + (b_1 + b_2)\sqrt{2}$$

$$= a' + b'\sqrt{2} \in R \quad \text{where } a' = (a_1 + a_2), b' = (b_1 + b_2) \in Z$$

B) $xy = (a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2})$

$$= (a_1 a_2 + 2 b_1 b_2) + (a_1 b_2 + b_1 a_2)\sqrt{2}$$

$$= a'' + b''\sqrt{2} \in R \quad \text{where } a'' = (a_1 a_2 + 2 b_1 b_2),\ b'' = (a_1 b_2 + b_1 a_2) \in Z$$

Closure property holds wrt addition and multiplication

2.A) For all $x = a + b\sqrt{2} \in R$ there is an element $0 = 0 + 0\sqrt{2} \in R$ ($\because$ $0 \in Z$) Such that

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

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

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

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

$\therefore$ $0 = 0 + 0\sqrt{2} \in R$ is the Identity wrt addition

B) for all $x = a + b\sqrt{2} \in R$ there is an element $1 = 1 + 0\sqrt{2} \in R$ ($\because 1, 0 \in Z$) Such that

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

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

and $1.\, x = (1 + 0\sqrt{2})(a + b\sqrt{2}) = (1.a) + (0+b)\sqrt{2}$

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

$\therefore$ $1 = 1 + 0\sqrt{2} \in R$ is the Identity wrt Multiplication.

3.A) for all $x = a + b\sqrt{2} \in R$ there is an element $-x = -a + (-b)\sqrt{2} \in R$ ($\because$ for all $a \in Z \Rightarrow -a \in Z$)

Such that $x + (-x) = (a + b\sqrt{2}) + [-a + (-b)\sqrt{2}] = [a + (-a)] + [b + (-b)]\sqrt{2}$

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

$(-x) + x = [-a + (-b)\sqrt{2}] + (a + b\sqrt{2}) = [(-a) + a] + [(-b) + b]\sqrt{2}]$

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

$-x = -a + (-b)\sqrt{2} \in R$ is the inverse of x w r t addition

B) Without zero divisors property: For all $x = a_1 + b_1\sqrt{2}$ $y = a_2 + b_2\sqrt{2}$ in R then

if $xy = 0$

$\Rightarrow (a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = 0$

$\Rightarrow (a_1 a_2 + 2 b_1 b_2) + (a_1 b_2 + b_1 a_2)\sqrt{2} = 0 + 0\sqrt{2}$

$\Rightarrow (a_1 a_2 + 2 b_1 b_2) = 0$ and $(a_1 b_2 + b_1 a_2) = 0$.

But a_1, a_2, b_1, b_2 are positive integers

$\Rightarrow a_1 a_2 = 0,\ b_1 b_2 = 0$

$\Rightarrow a_1 = 0$ or $a_2 = 0,\ b_1 = 0$ or $b_2 = 0$.

$\Rightarrow (a_1 + b_1\sqrt{2}) = 0 + 0\sqrt{2}$, or $(a_2 + b_2\sqrt{2}) = 0 + 0\sqrt{2}$

$\Rightarrow x = 0$ or $y = 0$. Without zero divisors property exist.

4) As R contain all Real numbers but the set of all real numbers form an Integral domain and hence the remaining properties of the integral domain are all exist in R

ie Associative, Commutative and Distributive laws wrt addition and multiplication are exist.

Therefore < R,+,.> is an Integral domain. But it not a field

Since for any $x = 3 + 4\sqrt{2} \in R$ *then* $x^{-1} = \frac{1}{3+4\sqrt{2}} \times \frac{3-4\sqrt{2}}{3-4\sqrt{2}} = \frac{3-4\sqrt{2}}{9-32}$

$$= \frac{3}{-21} + \frac{4}{21}\sqrt{2} \notin R \quad \because \frac{-3}{21}, \frac{4}{21} \notin Z$$

Problem:

Show that the set of Gaussian Integers $J(\,i\,) = \{\, a + ib : \; a, b \in Z\,\}$ form an Integral domain withrespect to addition and multiplication.

Solution: Given $J(\,i\,) = \{\, a + ib : a, b \in Z\,\}$ to show that $J(\,i\,)$ is an Integral domain using Z is Integraldomain.

1.A) for all x = a_1 + I b_1 , y = a_2 + I b_2 in $J(\,i\,)$

then x + y = ($a_1 + ib_1$) + ($a_2 + ib_2$)

= ($a_1 + a_2$)+ i($b_1 + b_2$)

= a' +i b ' ∈ $J(\,i\,)$ where a' = ($a_1 + a_2$) ,b' = ($b_1 + b_2$) ∈ Z

B) x y=($a_1 + ib_1$)($a_2 + ib_2$) =($a_1 a_2 + 2 b_1 b_2$) + i($a_1 b_2 + b_1 a_2$)

= a'' + ib '' ∈ J(i) where a'' = ($a_1 a_2 + 2 b_1 b_2$), b'' =($a_1 b_2 + b_1 a_2$) ∈ Z

Closure property holds wrt addition and multiplication

2.A) For all x = a + ib∈ J(i) there is an element 0 = 0 + 0√2 ∈ J(i) (∵ 0 ∈ Z) Such that

x + 0 = (a + ib) + (0 + i0) = (a+0) + i(b + 0)

= (a + ib) = x

0 + x = (0 + i0)+ (a + ib)= (0+ a) + i(0+ b)

= (a + ib) = x

$\therefore\; 0 = 0 + i0 \in J(\,i\,)$ *is the Identity wrt addition*

B) For all x= a + ib ∈ J(i) there is an element 1 = 1 + i0∈ J(i) (∵ 1, 0 ∈ Z) Such that

x .1 = (a + ib)(1 + i0) = (a 1) + i(b+0)

= (a + ib) = x

and 1. x = (1 + i0) (a + ib) = (1.a) + i(0+ b)

= (a + ib) = x

$\therefore\; 1 = 1 + i0 \in J(i)$ *is the Identity(unity) wrt Multiplication*

3.A) for all x = a + ib ∈ J(i) there is an element – x = - a+ i(-b) ∈ J(i) (∵ for all a ∈ Z ⇒ - a ∈ Z)

Such that $x + (-x) = (a + ib) + [-a + i(-b)\,] = [\,a + (-a\,)\,] + i[\,b + (-b)\,]$

= (0 + i0) = 0

$(-x) + x = [-a + i(-b)] + (\,a + ib\,) = [(-a) + a\,) + i[(\,-b) + b\,]$

$= (\,0 + i0\,) = 0$

$-x = -a + i(-b) \in J(\,i\,)$ *is the inverse of x w r t addition*

B) Without zero divisors property: For all $x = a_1 + ib_1 \quad y = a_2 + ib_2$ in J(i) then

if x y =0

$\Rightarrow (a_1 + ib_1)(a_2 + ib_2) = 0$

$\Rightarrow (a_1 a_2 - b_1 b_2) + i(a_1 b_2 + b_1 a_2) = 0 + i0$

$\Rightarrow (a_1 a_2 - b_1 b_2) = 0$ and $(a_1 b_2 + b_1 a_2) = 0$ .Squaring on both sides

$(a_1 a_2 - b_1 b_2)^2 = 0$ and $(a_1 b_2 + b_1 a_2)^2 = 0$ Adding we get

$\Rightarrow (a_1^2 a_2^2 + b_1^2 b_2^2) + (a_1^2 b_2^2 + b_1^2 a_2^2) = 0$

$\Rightarrow (a_1^2 a_2^2 + b_1^2 b_2^2) = 0$ and $(a_1^2 b_2^2 + b_1^2 a_2^2) = 0$ $But\ a_1, a_2, b_1, b_2\ are\ positive\ integers$

$\Rightarrow a_1^2 a_2^2 = 0$, and $b_1^2 b_2^2 = 0$

$\Rightarrow a_1 = 0$ or $a_2 = 0$, $b_1 = 0$ or $b_2 = 0$.

$\Rightarrow (a_1 + ib_1) = 0 + i0, or\ (a_2 + ib_2) = 0 + i0 \Rightarrow$ x = 0 or y = 0. Without zero divisors property exist.

4) As J(i) contain all Complex numbers but the set of all complex numbers form an Integral domainand hence the remaining properties of the integral domain are all exist in J(i)

ie Associative, Commutative and Distributive laws wrt addition and multiplication are exist.

< J(i) , +, . > is Integral domain .

But It is not a field since for $x = 2 + 3i \in J(i)$ then $x^{-1} = \frac{1}{2+3i} \times \frac{2-3i}{2-3i}$

$$= \frac{2-3i}{4+9} = \frac{2}{13} - \frac{3}{13}\sqrt{2} \notin J(i) \text{ since } \frac{2}{13} \notin Z \text{ and } \frac{3}{13} \notin Z$$

Characteristic of a ring

Definition: Let R is a ring a least positive integer n is said to be the characteristic of the ring if for all a $\in$ R then $a + a + a + \ldots n\ times = n\,a = 0$

Example: In the ring of additive modulo 6

$Z_6 = \{0, 1, 2, 3, 4, 5\}$

$6(1) = 0\,, 6(2) = 0\,, 6(3) = 0, 6(4) = 0, 6(5) = 0$

$\therefore$ The characteristic of Z_6 is 6

Theorem: Prove that the characteristic of an integral domain is either 0 or prime number.

Proof: Suppose D is an Integral domain.

For any $a \neq 0 \in D$ and $o(a) = 0$ then the characteristic of D is zero.

If $o(a) = p \neq 0$ where p is least positive integer then to show that p is prime number.

Suppose p is not prime number ie it is composite number

Let $p = p_1 p_2$ where $0 < p_1 < p$ and $0 < p_2 < p$

As $a \neq 0 \in D \Rightarrow a^2 \neq 0 \in D$

Also $o(a) = p \Rightarrow o(a^2) = p$

$\Rightarrow p\,(a^2) = 0$

$\Rightarrow p_1 p_2 (a\,a) = 0$

$\Rightarrow (p_1 a)(p_2 a) = 0$

$\Rightarrow (p_1 a) = 0$ or $(p_2 a) = 0$

$\Rightarrow o(a) = p_1$ or $o(a) = p_2$ but $0 < p_1 < p$ and $0 < p_2 < p$.

But $o(a) = p \neq 0$ where p is least positive integer. It is contradiction

$\therefore$ The characteristic of R is prime.

SUBRINGS

Definition: A non-empty sub set S of a ring R is said to be a sub ring of R if S itself is a ring wrtaddition and multiplication that is S satisfies all the properties (8 proprieties) of the ring R.

Example: 1. The set of Even Integers

$2Z = \{\ldots\ldots -6, -4, -2, 0, 2, 4, 6, \ldots\ldots\}$ and the multiples of 3 i.e.

$3Z = \{\ldots\ldots -9, -6, -3, 0, 3, 6, 9, \ldots\ldots\}$ etc are the subrings of Ring of Integers Z.

Example: 2. The ring of Integers Z is a subring of ring of Rationales Q

Theorem: (Necessary and sufficient condition for sub ring of a Ring)

Statement: A non-empty subset S of a ring R to be a subring iff

i) For all $a, b \in S \Rightarrow a - b \in S$

ii) For all $a, b \in S \Rightarrow a\,b \in S$.

Proof: $\Rightarrow$ Part: Suppose S is a subring of the ring R

i) For all $a, b \in S \Rightarrow a \in S,\ b \in S \Rightarrow a \in S, -b \in S$ (S is a sub ring)

$\Rightarrow a + (-b) \in S$ (closure in S)

$\Rightarrow a - b \in S$

ii) for all $a, b \in S \Rightarrow a \in S, b \in S \Rightarrow ab \in S$ (closure wrt .)

$\Leftarrow$ Part: Suppose Sis a non-empty sub set of ring R

andi)For all $a, b \in S \Rightarrow a - b \in S$

ii) For all $a, b \in S \Rightarrow a\,b \in S$. To show that S is a subring of R.

1.For all $a \in S \Rightarrow a, a \in S \Rightarrow a - a \in S$ ($\because$ from)

$\Rightarrow 0 \in S$ **Additive Identity element exist in S.**

1. As $0 \in S$ For all $b \in S \Rightarrow 0 - b \in S$ ($\because$ from (i))

$\Rightarrow -b \in S$

Additive inverse exist .

2. For all $a, b \in S \Rightarrow a \in S,\ b \in S \Rightarrow a \in S, -b \in S$($\because$ from (A))

$\Rightarrow a - (-b) \in S$ ($\because$ from (i))

$\Rightarrow a + b \in S$.

Closure w r t addition exist.

3.From (ii) For all a, b $\in$ S $\Rightarrow$ a b $\in$ S. Closure Property w r t multiplication exist.

As S $\subseteq$ R the remaining properties of the ring are all exist in S.

Hence S is a sub ring of R

Theorem:

Prove that the intersection of two subrings is a subring of the Ring R

Proof: Let S_1 and S_2 are two subrings of the ring R.

To show that $S_1 \cap S_2$ is also subring of R .

1) As S_1 and S_2 are two subrings of the ring R by Identity property

$0 \in S_1$ and $0 \in S_2 \Rightarrow 0 \in S_1 \cap S_2$

$\Rightarrow S_1 \cap S_2$ is non-empty sub set of R

2) i) For all a , b $\in S_1 \cap S_2 \Rightarrow a - b \in S_1 \cap S_2$

For all a , b $\in S_1 \cap S_2 \Rightarrow$ a , b $\in S_1$ and a, b $\in S_2$

$\Rightarrow$ a - b $\in S_1$ and a - b $\in S_2$ (since S_1 and S_2 are subrings of R)

$\Rightarrow$ a - b $\in S_1 \cap S_2$

ii)For all a, b $\in S_1 \cap S_2 \Rightarrow ab \in S_1 \cap S_2$

For all a,b $\in S_1 \cap S_2 \Rightarrow$ a,b $\in S_1$ and a,b $\in S_2$

But Let S_1 and S_2 are subrings of the ring R

$\therefore$ ab $\in S_1$ and ab $\in S_2$

$\Rightarrow ab \in S_1 \cap S_2$

Hence $S_1 \cap S_2$ is subring of R

Problem :Show that the union of two sub rings of a ring R is not a subring of R using an example.

Solution: Let $S_1 = \{ . . . . . -4, -2, 0, 2, 4, ...\}$ and $S_2 = \{ . . . . .-6, -3, 0, 3, 6, ... \}$ are subrings of the ring of Integers Z ,but it's union

Ie $S_1 \cup S_2 = \{ . . . . -6,-4,-3,-2,0,2,3,4,6, ...\}$ not subring of Z

Since for a= 3, b= 4 $\in S_1 \cup S_2$ then a + b = 3+4 = 7 $\notin S_1 \cup S_2$

Theorem: Prove that the union of two subrings is a subring of a ring R if and only if one is contained in other.

Proof: Let S_1 and S_2 are two subrings of the ring R To prove that

$S_1 \cup S_2$ is a sub ring $\Leftrightarrow S_1 \subseteq S_2$ or $S_2 \subseteq S_1$

<= Part Let S_1 and S_2 are two subrings of the ring R and $S_1 \subseteq S_2$ or $S_2 \subseteq S_1$

To show that $S_1 \cup S_2$ subring

If $S_1 \subseteq S_2 \Rightarrow S_1 U S_2 = S_2$ subring of R If $S_2 \subseteq S_1 \Rightarrow S_1 U S_2 = S_1$ subring of R

$\Rightarrow$ Part let S_1 and S_2 subrings and $S_1 U S_2$ is a sub ring

To show that $S_1 \subseteq S_2$ or $S_2 \subseteq S_1$

If $S_1 \not\subset S_2 \Rightarrow$ For all $a \in S_1 \not\subset S_2$ => $a \in S_1$ but $a \notin S_2$.......(1)

If $S_2 \not\subset S_1 \Rightarrow$ For $b \in S_2 \not\subset S_1$ => $b \in S_2$ but $b \notin S_1$............(2)

$a \in S_1\ b \in S_2 \Rightarrow a, b \in S_1 U S_2$

But $S_1 U S_2$ is a subring $\therefore a + b \in S_1 U S_2$

$\Rightarrow a + b \in S_1$ or $a + b \in S_2$..(3)

From (1) and (3) $a \in S_1$ $a + b \in S_1 \Rightarrow -a \in S_1$ (subring) $a + b \in S_1$

$\Rightarrow -a + (a + b) \in S_1$ (Closure property in S_1)

$\Rightarrow b \in S_1$ I t is a contradiction to (2)

From (2) and (3) $b \in S_2$ $a + b \in S_2 \Rightarrow - b \in S_2$ (subring) $a + b \in S_2$

$\Rightarrow -b + (a + b) \in S_2$ (Closure property in S_2)

$\Rightarrow a \in S_2$ I t is a contradiction to (1)

$\therefore S_1 \subseteq S_2$ or $S_2 \subseteq S_1$

Theorem: Prove that an arbitrary intersection of subrings of a ring R is a subring of the ring R.

Proof: suppose S = $\{ S_i : i \in I \}$ is arbitrary collection of subrings of the ring R .

To show that $\bigcap_{i \in I} S_i$ is also a subring of R.

1. $\bigcap_{i \in I} S_i$ *is non − emty*: *As* S_i *for all* $i \in I$ *is a subring of* R

by Identity property $0 \in S_i$ for all $i \in I$

$$\Rightarrow 0 \in \bigcap_{i \in I} S_i \quad \Rightarrow \bigcap_{i \in I} S_i \neq \varphi$$

2. For all $a, b \in \bigcap_{i \in I} S_i \Rightarrow a - b \in \bigcap_{i \in I} S_i$

As For all $a, b \in \bigcap_{i \in I} S_i \Rightarrow$ For all $a, b \in S_i$ for all $i \in I$

As S_i *for all* $i \in I$ *is a subring of* R

$\Rightarrow a - b \in S_i$ *for all* $i \in I$
$\Rightarrow a - b \in \bigcap_{i \in I} S_i$.

3. For all $a, b \in \bigcap_{i \in I} S_i \Rightarrow a\, b \in \bigcap_{i \in I} S_i$

As For all $a, b \in \bigcap_{i \in I} S_i \Rightarrow$ For all $a, b \in S_i$ for all $i \in I$

As S_i *for all* $i \in I$ *is a subring of* R

$\Rightarrow a\, b \in S_i \quad for\ all\ i \in I$

$\Rightarrow a\, b \in \cap_{i \in I} S_i.$

Hence an arbitrary intersection of subrings of a ring R is a subring of the ring R

IDEALS

Definition : (Right Ideal)

A non-empty sub set S of a ring R is said to be Right Ideal if it satisfies the following conditions

1) For all a , b ∈ S ⇒ a – b ∈ S.

2) For all r ∈ R, s ∈ S ⇒ s r ∈ S.

Definition : (Left Ideal)

A non-empty sub set S of a ring R is said to be Left Ideal if it satisfies the following conditions

1) For all a , b ∈ S ⇒ a – b ∈ S.

2) For all r ∈ R, s ∈ S ⇒ r s ∈ S .

Definition : (Ideal)

A non-empty sub set S of a ring R is said to be an Ideal if it satisfies the following conditions

1) For all a , b ∈ S ⇒ a – b ∈ S.

2) For all r ∈ R, s ∈ S ⇒ r s ∈ S and s r ∈ S.

Example:

$The\ set\ of\ even\ integers\ S = 2Z = \{\ldots\ldots -6, -4, -2, 0, 2, 4, 6, \ldots \ldots ..\}\ is\ an$

$Ideal\ of\ Ring\ of\ Integers\ Z = \{\ldots\ldots -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots \ldots .\}$

Since 1) for a = 4, b = 6 then a - b = 4 - 6 = -2 ∈ S

2) for r = 5 ∈ R , s = 4 ∈ S then r s = 5 × 4 =20 ∈ S

Note: The ring of integers Z is not an ideal of ring of Rationales Q.

Since for r = 3/5 ∈ Q and s= 4 ∈ Z then s r = 4 .(3/5) = 12/5 not in Z.

Theorem:

Prove that the intersection of two Ideals is an Ideal of the Ring R .

Proof: Let S_1 and S_2 are two Ideals of the ring R.

To show that $S_1 \cap S_2$ is also an Ideal of R .

1) As S_1 and S_2 are two Ideals of the ring R by Identity property

$0 \in S_1$ and $0 \in S_2 \Rightarrow 0 \in S_1 \cap S_2$

$\Rightarrow S_1 \cap S_2$ is non-empty sub set of R

1) For all a , b $\in S_1 \cap S_2 \Rightarrow a - b \in S_1 \cap S_2$

For all a , b $\in S_1 \cap S_2 \Rightarrow$ a , b $\in S_1$ and a, b $\in S_2$

$\Rightarrow$ a - b $\in S_1$ and a - b $\in S_2$ ($\because S_1$ and S_2 are Ideals)

$\Rightarrow$ a - b $\in S_1 \cap S_2$

2)For all r $\in$ R, s $\in S_1 \cap S_2 \Rightarrow$ r s $\in S_1 \cap S_2$ and s r $\in S_1 \cap S_2$

For all r $\in$ R, s $\in S_1 \cap S_2 \Rightarrow$ r $\in$ R , s $\in S_1$ and s $\in S_2$

But Let S_1 and S_2 are Ideals of the ring R

$\therefore$ r s $\in S_1$ and s r $\in S_1$ and r s $\in S_2$ and s r $\in S_2$

$\Rightarrow$ r s $\in S_1 \cap S_2$ and s r $\in S_1 \cap S_2$

Hence $S_1 \cap S_2$ is also an Ideal of R.

Theorem:

Prove that the union of two Ideals is an Ideal of a ring R if and only if one is contained in other .

Proof: Let S_1 and S_2 are two Ideals of the ring R To prove that

$S_1 U S_2$ is an Ideal $\Leftrightarrow S_1 \subseteq S_2$ or $S_2 \subseteq S_1$

$\Leftarrow$ Part

Let S_1 and S_2 are two ideals of the ring R and $S_1 \subseteq S_2$ or $S_2 \subseteq S_1$

To show that S_1US_2 is an ideal of R

If $S_1 \subseteq S_2 \Rightarrow S_1US_2 = S_2$ ideal of R

If $S_2 \subseteq S_1 \Rightarrow S_1US_2 = S_1$ ideal of R

$\therefore$ S_1US_2 is an Ideal of R

$\Rightarrow$ Part

let S_1 and S_2 ideals and $S_1U S_2$ is an ideal of R

To show that $S_1 \subseteq S_2$ or $S_2 \subseteq S_1$ suppose $S_1 \not\subset S_2$ and $S_2 \not\subset S_1$

If $S_1 \not\subset S_2 \Rightarrow$ For all a $\in S_1 \not\subset S_2$ => a $\in S_1$ but a$\notin S_2$---- (1)

If $S_2 \not\subset S_1 \Rightarrow$ For b $\in S_2 \not\subset S_1$ => b $\in S_2$ but b$\notin S_1$ -----(2)

a $\in S_1$ b $\in S_2 \Rightarrow$ a, b $\in S_1US_2$

But S_1US_2 is an Ideal of R

$\therefore$ a + b$\in S_1U S_2$

$\Rightarrow$ a + b $\in S_1$ or a+ b $\in S_2$ --------(3)

From (1) and (3) a $\in S_1$ a + b $\in S_1 \Rightarrow$ - a $\in S_1$ (*Ideal*) a + b $\in S_1$

$\Rightarrow$ -a + (a + b) $\in S_1$ (Closure property in S_1)

$\Rightarrow$ b$\in S_1$ I t is a contradiction to (2)

$$From\ (2)\ and\ (3)\ b\ \in\ S_2\ a\ +\ b\ \in S_2\ \Rightarrow -b\ \in S_2\ (Ideal)\ a\ +\ b\ \in S_2$$

$\Rightarrow$ -b + (a + b) $\in S_2$ (Closure property in S_2)

$\Rightarrow$ a $\in S_2$ I t is a contradiction to (1)

$\therefore S_1 \subseteq S_2$ or $S_2 \subseteq S_1$

Example: Show that the set of 2×2 Matrices

$$S = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in Z \right\}$$

is Subring but neither right Ideal nor left ideal of R ring of 2×2 Matrices.

Solution:

For all $A = \begin{pmatrix} a_1 & 0 \\ 0 & b_1 \end{pmatrix}$ $B = \begin{pmatrix} a_2 & 0 \\ 0 & b_2 \end{pmatrix}$ in S then

i) $A - B = \begin{pmatrix} a_1 & 0 \\ 0 & b_1 \end{pmatrix} - \begin{pmatrix} a_2 & 0 \\ 0 & b_2 \end{pmatrix} = \begin{pmatrix} a_1 - a_2 & 0 \\ 0 & b_1 - b_2 \end{pmatrix}$ in S

ii) $AB = \begin{pmatrix} a_1 & 0 \\ 0 & b_1 \end{pmatrix}\begin{pmatrix} a_2 & 0 \\ 0 & b_2 \end{pmatrix} = \begin{pmatrix} a_1 a_2 & 0 \\ 0 & b_1 b_2 \end{pmatrix}$ in S.

S is a subring of R.

For all $X = \begin{pmatrix} x & y \\ p & q \end{pmatrix}$ in R and $A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ then

$XA = \begin{pmatrix} x & y \\ p & q \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} xa & yb \\ pa & qb \end{pmatrix}$ is not in S.

$AX = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\begin{pmatrix} x & y \\ p & q \end{pmatrix} = \begin{pmatrix} ax & ay \\ bp & bq \end{pmatrix}$ is not in S.

Hence S is Subring but neither right Ideal nor left ideal

Result: Let S is an ideal of a ring R with unity then prove that if 1 $\in$S then prove that S = R.

Proof : Given S is an ideal of a ring R with unity.

Clearly $S \subseteq R$------ (1)

To show that $R \subseteq S$

For any $r \in R$ given $1 \in S$ and S is an Ideal of R

$\Rightarrow r\,1 \in S \Rightarrow r \in S$

$\Rightarrow R \subseteq S$ ------------(2) from (1) and (2) R = S

Theorem: Prove that every field has no proper ideals.

Proof: Suppose F is a field to show that the only ideals of F are { 0 } and F .

Assume that S is an ideal of F and S $\neq$ { 0 } to show that S=F.

Clearly $S \subseteq F$ ------(1) To show that $F \subseteq S$

For any $a \neq 0 \in S \subseteq F \Rightarrow a \neq 0 \in F$ and F is a a field

$\Rightarrow a^{-1} \in F$ again $a \in S$ and is ideal of R $\Rightarrow a\, a^{-1} \in S$

$\Rightarrow 1 \in S$ and S is an Ideal of R for any $r \in F$

$\Rightarrow r\,1 \in S \Rightarrow r \in S \Rightarrow F \subseteq S$ ------------(2)

from (1) and (2) $F = S$

All the best