ROHINI COLLEGE OF ENGINEERING & TECHNOLOGY
Near Anjugramam Junction, Kanyakumari Main Road, Palkulam, Variyoor P.O - 629401
Kanyakumari Dist, Tamilnadu., E-mail : admin@rcet.org.in, Website : www.rcet.org.in

DEPARTMENT OF MATHEMATICS

NAME OF THE SUBJECT: ALGEBRA AND NUMBER THEORY

SUBJECT CODE : MA8551

REGULATION : 2017

UNIT – I : GROUPS AND RINGS

UNIT–I GROUPS AND RINGS

1. **Prove that $G=\left\{\begin{bmatrix}1&0\\0&1\end{bmatrix},\begin{bmatrix}-1&0\\0&1\end{bmatrix},\begin{bmatrix}1&0\\0&-1\end{bmatrix},\begin{bmatrix}-1&0\\0&-1\end{bmatrix}\right\}$ forms an abelian group under matrix multiplication.**

Solution:

Let $I=\begin{bmatrix}1&0\\0&1\end{bmatrix}$, $A=\begin{bmatrix}-1&0\\0&1\end{bmatrix}$, $B=\begin{bmatrix}1&0\\0&-1\end{bmatrix}$ and $C=\begin{bmatrix}-1&0\\0&-1\end{bmatrix}$

The matrix multiplication table is,

$\times$	I	A	B	C
I	I	A	B	C
A	A	I	C	B
B	B	C	I	A
C	C	B	A	I

Claim 1: Closure property

Since all the elements inside the table are the elements of G.

Hence G is closed under multiplication.

Claim 2: Associative property

We know that matrix multiplication is always associative

Claim 3: Identity property

From the above table we observe that the matrix $I \in G$ is the Identity matrix.

Claim 4: Inverse property

From the above table we observe that all the matrices are inverse to each other.

Hence Inverse element exists.

Claim 5: Commutative property

From the table we have

$$A\times B = C = B\times A, A\times C = B = C\times A, B\times C = A = C\times B$$

Therefore commutative property exists.

2. **Prove that the necessary and sufficient condition for a non-empty subset H of a group (G, *) to be a subgroup is $a, b \in H \Rightarrow a * b^{-1} \in H$. (Nov/Dec 2012)**

Solution:

<u>Necessary Condition:</u>

Let us assume that H is a subgroup of G. Since H itself a group, we have if $a,b\in H$ implies $a*b\in H$

Since $b\in H$ then $b^{-1}\in H$ which implies $a*b^{-1}\in H$

<u>Sufficient Condition:</u>

Let $a*b^{-1}\in H$, for $a*b\in H$

Claim 1: Identity property

If $a \in H$, which implies $a*a^{-1}=e \in H$

Hence the identity element $e\in H$.

	Claim 2: Inverse property Let $a,e \in H$, then $e*a^{-1} = a^{-1} \in H$ Hence a^{-1} is the inverse of a . **Claim 3: Closure property** Let $a, b^{-1} \in H$, then $a*\left(b^{-1}\right)^{-1} = a*b \in H$ Therefore H is closed. **Claim 4: Associative property** Clearly * is associative. Hence H is a subgroup of G.
3.	**Prove that intersection of two subgroups of a group G is again a subgroup of G, but their union need not be a subgroup of G.**
	Solution: **Claim 1: Intersection of two subgroups is again a subgroup.** Let A and B be two subgroups of a group G. we need to prove that $A \bigcap B$ is a subgroup. (i.e.) It is enough to prove that $A \bigcap B \neq \phi$ and $a,b \in A \bigcap B \Rightarrow a* b^{-1} \in A \bigcap B$. Since A and B are subgroups of G, the identity element $e \in A$ and B. $\therefore \ A \bigcap B \neq \phi$ Let $a,b \in A \bigcap B \Rightarrow a,b \in A$ and $a,b \in B$ $\Rightarrow a* b^{-1} \in A$ and $a* b^{-1} \in B$ $\Rightarrow a* b^{-1} \in A \bigcap B$ Hence $A \bigcap B$ is a subgroup of G. **Claim 2: Union of two subgroups need not be a subgroup** Consider the following example, Consider the group $(Z,+)$,where Z is the set of all integers and the operation + represents usual addition. Let $A = 2Z = \{0, \pm 2, \pm 4, \pm 6, \ldots\}$ and $B = 3Z = \{0, \pm 3, \pm 6, \pm 9, \ldots\}$. Here $(2Z,+)$ and $(3Z,+)$ are both subgroups of $(Z,+)$ Let $H = 2Z \bigcup 3Z = \{0, \pm 2, \pm 3, \pm 4, \pm 6, \ldots\}$ Note that $2, 3 \in H$, but $2 + 3 = 5 \notin H \Rightarrow 5 \notin 2Z \bigcup 3Z$ (i.e.) $2Z \bigcup 3Z$ is not closed under addition. Therefore $2Z \bigcup 3Z$ is not a group Therefore (H, +) is not a subgroup of (Z, +).
4.	**Prove that intersection of any two normal subgroups of a group (G, *) is a normal subgroup of a group (G, *).**
	Solution: Let G be the group and H and K are the normal subgroups of G. Since H and K are normal subgroups of $\Rightarrow H$ and K are subgroups of G

	$\Rightarrow H \cap K$ is a subgroup of G. Now we have to prove $H \cap K$ is normal Since $e \in H$ and $e \in K \Rightarrow e \in H \cap K$. Thus H $\cap$ K is nonempty. Let $x \in G$ and $h \in H \cap K$ $x \in G$ and $h \in H, h \in K$ $x \in G$, $h \in H$ and $x \in G$, $h \in K$ So, $x * h * x^{-1} \in H$ and $x * h * x^{-1} \in K$ $\therefore\ x * h * x^{-1} \in H \cap K$ Thus $H \cap K$ is a Normal subgroup of G.
5.	Let f : G $\rightarrow$ H be a homomorphism from the group (G,$*$) to the group (H, Δ). Prove that the kernel of f is a normal subgroup of G.
	Proof: Let K be the Kernel of the homomorphism g. That is $K = \{x \in G \mid g(x) = e'\}$ where e' the identity element of H. is Let x, y $\in$ K. Now $g(x * y^{-1}) = g(x)\ \Delta\ g(y^{-1}) = g(x)\ \Delta [g(y)]^{-1} = e' \Delta (e')^{-1} = e' \Delta\ e' = e'$ $x * y^{-1} \in K$ Therefore K is a subgroup of G. Let $x \in K$, $f \in G$ $g(f * x * f^{-1}) = g(f) * g(x) * g(f^{-1}) = g(f)\ e'\ [g(f)]^{-1} = g(f)\ [g(f)]^{-1} = e'$ $\therefore\ \ f * x * f^{-1} \in K$ Thus K is a normal subgroup of G.
6.	**Let** $(G,)$, **(H,*) be groups with respective identities** e_G , e_H **.If** f **:G$\rightarrow$H is a homomorphism, then show that** $(a)\ f(e_G) = e_H$ $(b)\ f(a^{-1}) = [f(a)]^{-1} \forall a \in G$ $(c)\ f(a^n) = [f(a)]^n \forall a \in G and\ all\ n \in Z$ (d) f(S)isasubgroupof Hfor eachsubgroup Sof G. **Proof:** (a) $e_H * f(e_G) = f(e_G) = f(e_G\ e_G) = f(e_G) * f(e_G)$ $\therefore e_H = f(e_G)$, by right cancellation law *(b)* Let $a \in G$, since G is a group, $a^{-1} \in G$ Since G is a group, $a * a^{-1} = e_G$ By homomorphism $f(a * a^{-1}) = f(e_G)$ $f(a) \circ f(a^{-1}) = e_H$ Hence $f\left(a^{-1}\right)$ is the inverse of $f(a)$ *i.e.*, $f(a^{-1}) = [f(a)]^{-1} \forall a \in G$

(c) $\forall a \in G \text{ and all } n \in Z$

Case(i): if n=0 then $a^n = a^0 = e$

$$f(a^0) = f(e_G) = e_H = [f(a)]^0$$

$$\Rightarrow f(a^n) = [f(a)]^n$$

Case(ii): if n is a positive integer then

$$a^n = a \circ a \circ a \circ \cdots \circ a \ (n \text{ times})$$

$$f(a^n) = f(a \circ a \circ a \circ \cdots \circ a) \text{ (n times)}$$

$$= f(a) * f(a) * f(a) * \cdots * f(a)$$

$$= [f(a)]^n$$

Case(iii): if n is a negative integer , then n=-r, r>0.

$$f(a^n) = f(a^{-r}) = f[(a^{-1})^r] = [f(a^{-1})]^r = [f(a)]^{-r} = [f(a)]^n$$

$\therefore f(a^n) = [f(a)]^n \ \forall a \in G \text{ and all } n \in Z$

(d) If S is a subgroup of G , then $S \neq \phi$, so $f(S) \neq \phi$. Let x,y ∈ f(S).

Then x = f(a), y = f(b) for some a,b∈S. Since S is a subgroup of G, it follows that

$\therefore a \circ b \in S,$

$$f(a) * f(b) = f(a \circ b) \in f(S)$$

$\Rightarrow x * y \in f(S), \text{ so } f(S) \text{ is closed}$

Finally, $x^{-1} = [f(a)]^{-1} = f[a^{-1}]$

$\because \ a \in S \Rightarrow a^{-1} \in S \ \& \ f[a^{-1}] \in f(S)$

$x^{-1} \in f(S)$

$\therefore f(S) \text{ is a subgroup of H for each subgroup S of G.}$

7. **Show that $(M, \bullet)$ is an abelian group where M={A,A^2,A^3,A^4} with $A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ and $\bullet$ is the ordinary matrix multiplication. Further prove that $(M, \bullet)$ is isomorphic to the abelian group $(G, \bullet)$ where G={1, -1, *i*, -*i*} and $\bullet$ is the ordinary multiplication.**

Solution:

$$A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}; \ A^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}; A^3 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}; \ A^4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

For all 1≤ m, n ≤ 4, $A^m . A^n = A^{m+n} = A^r$ where 1< r < 4 and m + n ≅ r (mod 4).

Thus . is a closure. Thus . is a closure operation. Since matrix multiplication is associative so is '.'.

$A^4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$ is the identity.

$A^{-1} = \frac{1}{1}\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = A^3$

$\left(A^2\right)^{-1} = \frac{1}{1}\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = A^2$

$\left(A^3\right)^{-1} = \frac{1}{1}\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = A$

$\left(A^4\right)^{-1} = \frac{1}{1}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I = A^4$

For all $1 \le m, n \le 4$, $A^m . A^n = A^{m+n} = A^{n+m} = A^n . A^m$, so '.' is communicative.

$\therefore (M, \bullet)$ is an abelian group .

Define f: M → G such that $f(A) = i$, $f(A^2) = -1 = i^2$, $f(A^3) = -i = i^3$, $f(A^4) = 1 = i^4$

$\therefore$ f is 1-1 and onto

Since $i^3 = -i = f(A^3) = f(A \bullet A^2) = f(A) f(A^2) = i \cdot i^2 = i^3 = -i$

Hence f is isomorphic from M to G.

8. **State and Prove Lagrange's theorem on finite groups *(or)* Prove that in a finite group, order of any subgroup divides the order of the group.**

The order of each subgroup of a finite group is divides the order of the group.

Proof:

Let G be a finite group and $O(G) = n$ and let H be a subgroup of G and $O(H) = m$

Let $h_1, h_2, h_3, ..., h_m$ are the m distinct elements of H

For $x \in G$, the right coset of H is defined by $Hx = \{h_1 x, h_2 x, h_3 x, ... h_m x\}$.

Since there is a one to one correspondence between H and Hx , the members of Hx are distinct.

Hence, each right coset of H in G has m distinct members.

We know that any two right cosets of H in G are either identical or disjoint.

The number of distinct right cosets of H in G is finite (say k)

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

(i.e.) $G = Hx_1 \cup Hx_2 \cup Hx_3 \cup ... \cup Hx_k$

$O(G) = O(Hx_1) + O(Hx_2) + O(Hx_3) + ... + O(Hx_k)$

$n = m + m + m + ... + m$ (k times)

$\frac{O(G)}{O(H)} = k$

Hence $O(H)$ divides $O(G)$

9. **Prove that every subgroup of a cyclic group is cyclic.**

Proof:

Let (G,*) be the cyclic group generated by an element a ∈G and let H be the subgroup of G.

Claim: H is cyclic

If H = G or {e} then trivially H is cyclic.

If not the elements of H are non-zero integral powers of a, Since if $a^r \in H$, its inverse $a^{-r} \in H$.

Let "m" be the smallest positive integer such that $a^m \in H$. → **(1)**

Let a^n be any arbitrary element of H. Let q be the quotient and r be the remainder when n is divided by m.

Then n = qm + r where $0 \le r < m$. → **(2)**

Now $a^n = a^{qm + r} = (a^m)^q . a^r$

	$a^r = (a^m)^{-q}. a^n = a^{n-mq}$. Since $a^m \in H$, $(a^m)^q \in H$ by closure property $a^{mq} \in H$ $(a^{mq})^{-1} \in H$, by existence of inverse, as H is a subgroup $a^{-mq} \in H$ Since $a^n \in H$ and $a^{-mq} \in H$ $a^{n-mq} \in H$ $\therefore\ a^r \in H$ By **(1) & (2),** we get r=0, $\therefore$ n=mq $a^n = a^{mq} = \left(a^m\right)^q$. Thus every element of $a^n \in H$ is of the form $\left(a^m\right)^q$ Hence H is a cyclic subgroup generated by a^m.
10.	**Prove that every group of prime order is cyclic.** Proof: Let O(G)=p, where p is a prime number. Let $a(\neq e) \in$ G. Consider a subgroup generated by a. Let $H = \langle a \rangle$ $\Rightarrow O(H) > 1 \left[\because H = \langle a \rangle \Rightarrow a \in H \ \&\ also\ e \in H \Rightarrow O(H) > 1\right]$ Since H is a subgroup of G, then by Lagrange's theorem, O(H)/O(G) $\Rightarrow$ O(H)/p $\Rightarrow O(H) = 1\ or\ p\ [\because p\ is\ prime]$ $But\ O(H) > 1,\ \therefore O(H) \neq 1.$ $Thus\ O(H) = p = O(G)$ $\therefore G = H$ But H is a cyclic group, $\therefore$ G is a cyclic group.
11.	**Prove that the set R of numbers of the form $a + b\sqrt{2}$, where a and b are integers, is a ring with respect to ordinary addition and multiplication.** **Proof:** 1. Closure : Let $x_1 = a_1 + b_1\sqrt{2}$, $x_2 = a_2 + b_2\sqrt{2} \in R$ where $a_1, a_2, b_1, b_2 \in Z$ $x_1 + x_2 = \left(a_1 + b_1\sqrt{2}\right) + \left(a_2 + b_2\sqrt{2}\right) = \left(a_1 + a_2\right) + \left(b_1 + b_2\right)\sqrt{2} \in R$ $\text{where}\left(a_1 + a_2\right) \& \left(b_1 + b_2\right) \in Z.$ $\therefore$ R is closed under +. 2. Associative: Let $x_1 = a_1 + b_1\sqrt{2}$, $x_2 = a_2 + b_2\sqrt{2}$, $x_3 = a_3 + b_3\sqrt{2} \in R$ where $a_1, a_2, a_3, b_1, b_2, b_3 \in Z$ $\left(x_1 + x_2\right) + x_3 = \left[\left(a_1 + b_1\sqrt{2}\right) + \left(a_2 + b_2\sqrt{2}\right)\right] + \left(a_3 + b_3\sqrt{2}\right)$ $= \left[\left(a_1 + a_2\right) + \left(b_1 + b_2\right)\sqrt{2}\right] + \left(a_3 + b_3\sqrt{2}\right)$ $= \left[\left(a_1 + a_2\right) + a_3\right] + \left[\left(b_1 + b_2\right) + b_3\right]\sqrt{2}$ $= \left[a_1 + \left(a_2 + a_3\right)\right] + \left[b_1 + \left(b_2 + b_3\right)\right]\sqrt{2}$ $= \left(a_1 + b_1\sqrt{2}\right) + \left[\left(a_2 + a_3\right) + \left(b_2 + b_3\right)\sqrt{2}\right]$

$$= \left(a_1 + b_1\sqrt{2}\right) + \left[\left(a_2 + b_2\sqrt{2}\right) + \left(a_3 + b_3\sqrt{2}\right)\right] = x_1 + (x_2 + x_3)$$

3. Identity: $0 + 0\sqrt{2} \in R$

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

4. Inverse: $a + b\sqrt{2}, -a - b\sqrt{2} \in R$

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

$(-a) + (-b)\sqrt{2}$ is the identity inverse of $a + b\sqrt{2}$

5. Commutative law:

$$x_1 + x_2 = \left(a_1 + b_1\sqrt{2}\right) + \left(a_2 + b_2\sqrt{2}\right) = (a_1 + a_2) + (b_1 + b_2)\sqrt{2}$$
$$= (a_2 + a_1) + (b_2 + b_1)\sqrt{2}$$
$$= \left(a_2 + b_2\sqrt{2}\right) + \left(a_1 + b_1\sqrt{2}\right) = x_2 + x_1$$

Under Multiplication

6. Closure Axioms:

$$x_1x_2 = \left(a_1 + b_1\sqrt{2}\right).\left(a_2 + b_2\sqrt{2}\right) = (a_1a_2 + 2b_1b_2) + (a_2b_1 + a_1b_2)\sqrt{2}$$

$a_1a_2 + 2b_1b_2 , a_2b_1 + a_1b_2 \in Z$

$\therefore x_1x_2 \in R$

7. Associative:

$$(x_1 \cdot x_2) \cdot x_3 = \left[\left(a_1 + b_1\sqrt{2}\right) \cdot \left(a_2 + b_2\sqrt{2}\right)\right] \cdot \left(a_3 + b_3\sqrt{2}\right)$$
$$= \left[(a_1a_2 + 2b_1b_2) + (a_2b_1 + a_1b_2)\sqrt{2}\right] \cdot \left(a_3 + b_3\sqrt{2}\right)$$
$$= \left[(a_1a_2 + 2b_1b_2)a_3 + 2(a_2b_1 + a_1b_2)b_3\right] + \left[(a_1a_2 + 2b_1b_2)b_3 + (a_2b_1 + a_1b_2)a_3\right]\sqrt{2}$$
$$= x_1 \cdot (x_2 \cdot x_3)$$

8. Distributive Laws :

$$x_1 \cdot (x_2 + x_3) = \left(a_1 + b_1\sqrt{2}\right) \cdot \left[\left(a_2 + b_2\sqrt{2}\right) + \left(a_3 + b_3\sqrt{2}\right)\right]$$
$$= \left(a_1 + b_1\sqrt{2}\right) \cdot \left[(a_2 + a_3) + (b_2 + b_3)\sqrt{2}\right]$$
$$= \left[a_1(a_2 + a_3) + 2(b_2 + b_3)b_1\right] + \left[b_1(a_2 + a_3) + (b_2 + b_3)a_1\right]\sqrt{2}$$
$$= \left(a_1 + b_1\sqrt{2}\right) \cdot \left(a_2 + b_2\sqrt{2}\right) + \left(a_1 + b_1\sqrt{2}\right) \cdot \left(a_3 + b_3\sqrt{2}\right)$$
$$= a_1a_2 + a_1a_3 + 2b_1b_2 + 2b_1b_3 + \sqrt{2}a_2b_1 + \sqrt{2}a_3b_1 + \sqrt{2}a_1b_2 + \sqrt{2}a_1b_3$$
$$= \left[(a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2}\right] + \left[(a_1a_3 + 2b_1b_3) + (a_1b_3 + a_3b_1)\sqrt{2}\right]$$

$x_1 \cdot (x_2 + x_3) = x_1 \cdot x_2 + x_1 \cdot x_3$

$(x_2 + x_3) \cdot x_1 = x_2 \cdot x_1 + x_3 \cdot x_1$

Hence the given set is a ring.

12. **Prove that the set $Z_4 = \{0,1, 2, 3\}$ is a commutative ring with respect to the binary operation $+_4$ and x_4. [Nov/Dec -2017]**

Answer:

Composition table for additive modulo 4.

$+_4$	*[0]*	*[1]*	*[2]*	*[3]*
[0]	*0*	*1*	*2*	*3*
[1]	*1*	*2*	*3*	*0*
[2]	*2*	*3*	*0*	*1*
[3]	*3*	*0*	*1*	*2*

Composition table for multiplicative modulo 4.

x_4	*[0]*	*[1]*	*[2]*	*[3]*
[0]	*0*	*0*	*0*	*0*
[1]	*0*	*1*	*2*	*3*
[2]	*0*	*2*	*0*	*2*
[3]	*0*	*3*	*2*	*1*

From tables, we get

(i) all the entries in both tables belongs to Z_4

Therefore Z_4 is closed under the both operations addition and multiplication.

(ii) From the both tables, entries in the first, second, third and fourth row is equal to entries in the first, second, third and fourth columns respectively.

Hence the operations are commutative.

(iii) Modular addition and Modular multiplications are always associative.

(iv) 0 is the additive identity and 1 is the multiplicative identity.

(v) Additive inverse of 0, 1, 2, 3 are respectively 0, 3, 2, 1. Multiplicative inverses of the non-zero elements 1, 2 and 3 are 1, 2 and 3 respectively.

(vi) If $a,b,\ c \in Z_4$ then

$$a\times(b+c)=(a\times b)+(a\times c)$$

$$(a+b)\times c=(a\times c)+(b\times c)$$

The operation multiplication is distributive over addition

Hence $(Z_4, +_4, \times_4)$ is a commutative ring with unity.

13. **Let** $A=\left\{\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} / a \in R\right\}$ **(a) Show that A is a ring under matrix addition and multiplication (b) Prove that R is isomorphic to A.**

Proof:

(a) For any $B=\begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix}$ and $C=\begin{bmatrix} c & 0 \\ 0 & c \end{bmatrix}$, we have

$$B+C=\begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix}+\begin{bmatrix} c & 0 \\ 0 & c \end{bmatrix}=\begin{bmatrix} b+c & 0 \\ 0 & b+c \end{bmatrix}\in A \text{ and},$$

$$B\cdot C=\begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix}\cdot\begin{bmatrix} c & 0 \\ 0 & c \end{bmatrix}=\begin{bmatrix} bc & 0 \\ 0 & bc \end{bmatrix}\in A$$

Also for any $B=\begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix}$, the additiveinverse $-B=\begin{bmatrix} -b & 0 \\ 0 & -b \end{bmatrix}$ exists such that

$$B+(-B)=\begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix}+\begin{bmatrix} -b & 0 \\ 0 & -b \end{bmatrix}=\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}\in A.$$

Distributive Laws:

$$A.(B+C)=\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}.\left\{\begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix}+\begin{bmatrix} c & 0 \\ 0 & c \end{bmatrix}\right\}=\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}.\left\{\begin{bmatrix} b+c & 0 \\ 0 & b+c \end{bmatrix}\right\}$$

$$A.(B+C)=\begin{bmatrix} a.(b+c) & 0 \\ 0 & a.(b+c) \end{bmatrix}=\begin{bmatrix} (a.b+a.c) & 0 \\ 0 & (a.b+a.c) \end{bmatrix}$$

$$=\begin{bmatrix} a.b & 0 \\ 0 & a.b \end{bmatrix}+\begin{bmatrix} a.c & 0 \\ 0 & a.c \end{bmatrix}$$

$$=\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}\cdot\begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix}+\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}\cdot\begin{bmatrix} c & 0 \\ 0 & c \end{bmatrix}=A.B+A.C$$

Similarly, (B+C).A=B.A+C.A

Thus Ais a ring.

(b) To prove isomorphism, consider a one-to-one and onto function f from R onto A defined as follows

For all $r\in R, f:R\to A$ where $f(r)=\begin{bmatrix} r & 0 \\ 0 & r \end{bmatrix}$ i.e., for any realnumber we associatea 2nd order scalar matrix.

Now for any $r, s \in R$

$$f(r+s)=\begin{bmatrix} r+s & 0 \\ 0 & r+s \end{bmatrix}=\begin{bmatrix} r & 0 \\ 0 & r \end{bmatrix}+\begin{bmatrix} s & 0 \\ 0 & s \end{bmatrix}=f(r)+f(s)$$

$$f(r\cdot s)=\begin{bmatrix} rs & 0 \\ 0 & rs \end{bmatrix}=\begin{bmatrix} r & 0 \\ 0 & r \end{bmatrix}\cdot\begin{bmatrix} s & 0 \\ 0 & s \end{bmatrix}=f(r)\cdot f(s)$$

Thus twooperations+,·arepreservedandf is 1–1andonto.

∴ f is an isomorphism from R to A.

14. **Show that a finite integral domain is a field**

Proof:

Let {D, +, · } be a finite integral domain.

Then D has a finite number of distinct elements, say $\{a_1, a_2, a_3, \ldots a_n\}$.

Let a(≠ 0) be any element of D.

Then the elements $a\cdot a_1, a\cdot a_2, a\cdot a_3, \ldots a\cdot a_n \in D$, since D is closed under multiplication.

The elements $a\cdot a_1, a\cdot a_2, a\cdot a_3, \ldots a\cdot a_n$ are distinct, because if

$a\cdot a_i = a\cdot a_j \in D$, then $a\cdot(a_i - a_j)=0$.

But a ≠0. Hence $a_i - a_j = 0$, since D is an integral domain i.e., $a_i = a_j$, which is not true because $a_1, a_2, a_3, \ldots a_n$ aredistinct elements of D.

Hence the sets $\{a\cdot a_1, a\cdot a_2, a\cdot a_3, \ldots a\cdot a_n\}$ and $\{a_1, a_2, a_3, \ldots a_n\}$ are thesame.

Since $a \in D$ is in both sets,

let $a\cdot a_k = a$, forsomek → **(1)**

Then a_k is theunityof D, detailed as follows:

	Let $a_j = a \cdot a_i,\ a_j \in D \quad \rightarrow$ **(2)** Now $a_j \cdot a_k = a_k \cdot a_j$, bycommutative property $= a_k \cdot (a \cdot a_i)$, by(2) $= (a_k \cdot a) \cdot a_i$ $= (a \cdot a_k) \cdot a_i$, bycommutative property $= a \cdot a_i$, by (1) $= a_j$, by(2) Since a_j is an arbitrary element of D, a_k is theunityof D Let it be denoted by 1. Since $1 \in D$, there exits a($\neq 0$) and $a_i \in D$ such that $a \cdot a_i = a_i \cdot a = 1$ $\therefore$ a has an inverse. Hence {D, +, · } be a finite integral domain.
15.	**Prove that Z_n is a field if and only if n is a prime.** **Proof:** We have $Z_n = \{[0],[1],[2];\cdot\cdot[n-1]\}$ We know $(Z_n, +, \cdot)$ is a commutative ring with identity $[1]$. Let n be a prime, and suppose that 0 < a < n then gcd (a , n)=1 $\therefore$ there exists integers s, t such that as + tn = 1 $\Rightarrow$ sa – 1= (- t) n $\therefore$ sa-1 is divisible by n $\Rightarrow$ $sa \equiv 1 (\mathrm{mod}\, n)$ $\Rightarrow$ $[s][a] = [1]$ $\therefore [s]$ is themultiplicativeinverseof $[a]$. Thus $[a]$ isa unit of Z_n, which is consequently a field Conversely, let Z_n be a field. So Z_n is a commutative ring with identity and without zero divisions of zero. To prove n is a prime. if n is not a prime, then n= $n_1 n_2$, where 1 < n_1 ,n_2 <n. So $[n_1] \neq [0]$ and $[n_2] \neq [0]$ But $[n_1][n_2] = [n_1 n_2] = [n] = [0]$ $\therefore$ $[n_1],[n_2]$ aredivisorsof zero which contradicts thefact Z_n is a field. Hence n is a prime.