Q.1. Show that the groups $(\mathbb{Z}, +)$ and $(\mathbb{Q}, +)$ are not isomorphic

Ans:- $(\mathbb{Z}, +)$ can be generated from one element and hence is cyclic. On the other hand $\mathbb{Q}$ is not cyclic nor can it be finitely generated. In any case being cyclic is a structural property that is preserved by any isomorphism.

Thus $(\mathbb{Z}, +)$ and $(\mathbb{Q}, +)$ are not isomorphic.

Q.3. Show that $8\mathbb{Z}/72\mathbb{Z} \cong \mathbb{Z}_9$

Ans:- let $\phi : 8\mathbb{Z} \to \mathbb{Z}_9$, where it is defined by

$$\phi(8a) = [a] \; \forall a \in \mathbb{Z}$$

$$\phi(8a + 8b) = [a+b] = [a] +_9 [b]$$

$$= \phi(8a) +_9 \phi(8b)$$

$\therefore \phi$ is an epimorphism.

Now, let $8\mathbb{Z}/\ker\phi \cong \mathbb{Z}_9$

$$\ker\phi = \{ 8a \in 8\mathbb{Z} : \phi(8a) = [0] \}$$

$$= \{ 8a \in 8\mathbb{Z} : [a] = [0] \}$$

$$= \{ 8a \in 8\mathbb{Z} : a = 9q \}$$

$$= \{ 72q : q \in \mathbb{Z} \}$$

$$= 72\mathbb{Z}$$

$$\therefore 8\mathbb{Z}/72\mathbb{Z} \cong \mathbb{Z}_9$$

Q.5. Prove that the cancellation law holds in a ring R if and only if R has no divisor of zero.

Ans:- let R be a ring in which cancellation law holds.

let $a, b \in R$ and $a \cdot b = 0$ where $a \neq 0$.

$\therefore a \cdot b = 0 = a \cdot 0$

Since the cancellation law holds in R; $a \cdot b = a \cdot 0$ which implies $b = 0$.

This proves that a is not a left divisor of zero.

Let $a, b \in R$, and $a.b = 0$ where $b \neq 0$

Then $a.b = 0 = 0.b$

Since the cancellation law holds in R,

$a.b = 0.b$ implies $a = 0$

This prove that b is not a right divisor of zero.

Thus R has neither a left nor a right divisor of zero.

Conversely

Let R be a ring containing no divisor of zero.

Let $a, b, c \in R$ and $a.b = a.c$, where $a \neq 0$

Then $a.(b-c) = 0$

Since R contains no divisor of zero, $b-c = 0$

That is $b = c$.

So the left cancellation law holds in R.

Similarly the right cancellation law also holds in R.

Thus cancellation law holds in a ring R if and only if R has no divisor of zero.

Q.6. Show that the ring of matrices $\left\{ \begin{pmatrix} 2a & 0 \\ 0 & 2b \end{pmatrix} : a, b \in \mathbb{Z} \right\}$ contains divisors of zero and does not contain the unity.

Ans: — Let S be the ring and let $E = \begin{pmatrix} 2x & 0 \\ 0 & 2y \end{pmatrix}$ in S be the unity.

Then $AE = EA = A \;\forall\; A$ in S.

Let $A = \begin{pmatrix} 2a & 0 \\ 0 & 2b \end{pmatrix}$, then

$$AE = \begin{pmatrix} 2a & 0 \\ 0 & 2b \end{pmatrix}\begin{pmatrix} 2x & 0 \\ 0 & 2y \end{pmatrix} = \begin{pmatrix} 4ax & 0 \\ 0 & 4by \end{pmatrix}$$

Since, $AE = A$, $4ax = 2a$, $4by = 2b$.

$$\therefore x = \frac{1}{2},\ y = \frac{1}{2}$$

and $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \notin S$

$\therefore S$ does not contain unity.

$\begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 \\ 0 & 4 \end{pmatrix}$ are the non-zero elements of S and

$$\begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 4 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

This shows that S contains divisors of zero.

Q.7. Examine if the ring of matrices $\left\{ \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} : a, b \in R \right\}$ contains divisors of zero.

Ans:— Let S be the ring and $A = \begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$ be a non-zero element of S. Then $a, b \in \mathbb{R}$ and $(a,b) \neq (0,0)$

Let $AB = O$, where $B = \begin{pmatrix} p & q \\ 2q & p \end{pmatrix}$

This gives $ap + 2bq = 0$ and

$bp + aq = 0$

This is a homogeneous system of equations giving non-zero solutions for p, q if $\begin{vmatrix} a & 2b \\ b & a \end{vmatrix} = 0$, i.e. if $a^2 - 2b^2 = 0$

Since a and b are real, $a^2 - 2b^2$ may be zero for nonzero a, b.
Example :- $a = \sqrt{2}$ and $b = 1$, then $a^2 - 2b^2 = 0$ In this case a non-zero matrix B exists such that $AB = O$.

$$\begin{pmatrix} \sqrt{2} & 1 \\ 2 & \sqrt{2} \end{pmatrix} \begin{pmatrix} -\sqrt{2} & 1 \\ 2 & -\sqrt{2} \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$\therefore S$ contains divisors of zero.

Q.8. Prove that the ring $\mathbb{Z}[x]$, the ring of all polynomials with integer coefficients, is an integral domain.

Ans:- The ring $\mathbb{Z}[x]$ is a commutative ring with unity, the constant polynomial 1 being the identity element.

The zero element in the ring is the constant polynomial 0.

Let $f(x), g(x)$ be non-zero polynomials in $\mathbb{Z}[x]$ of degree m, n respectively.

Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m$, and

$g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_nx^n$, where a_i, b_i are integers

and $a_m \neq 0$, $b_n \neq 0$

Then $f(x)g(x)$ is a polynomial in $\mathbb{Z}[x]$ with a non-zero term $a_mb_nx^{m+n}$, since $a_mb_n \neq 0$ and therefore $f(x)g(x)$ is a non zero polynomial in $\mathbb{Z}[x]$.

This proves that the ring $\mathbb{Z}[x]$ contains no divisor of zero and therefore it is an integral domain.

Q.9. Prove that the ring of matrices $\left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R}\right\}$ is a field.

Ans:- Let $S = \left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R}\right\}$

$(S, +, \cdot)$ is a ring with unity, the matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ being the unity.

Let $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, $B = \begin{pmatrix} p & q \\ -q & p \end{pmatrix} \in S$, then.

$$A \cdot B = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} p & q \\ -q & p \end{pmatrix} = \begin{pmatrix} ap - bq & aq + bp \\ -bp - aq & -bq + ap \end{pmatrix}$$

$$B \cdot A = \begin{pmatrix} p & q \\ -q & p \end{pmatrix}\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} pa - qb & pb + qa \\ -qa - pb & -qb + pa \end{pmatrix}$$

$\therefore A\cdot B = B\cdot A \ \forall A, B \in S$.

Hence $(S, +, \cdot)$ is a commutative ring with unity.

Let $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ be a non zero element of S.

Then $(a,b) \neq (0,0)$ and $|A| = a^2+b^2 \neq 0$.

Hence A^{-1} exists and $A^{-1} = \dfrac{1}{a^2+b^2}\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in S$

$\therefore$ Each non zero element of the ring is a unit.

Hence $(S, +, \cdot)$ is a field.

Q.10. Prove that the ring of matrices $\left\{\begin{pmatrix} a & b \\ 2b & a \end{pmatrix} : a, b \in \mathbb{Q}\right\}$ is a field.

Ans:- Let $S = \left\{\begin{pmatrix} a & b \\ 2b & a \end{pmatrix} : a, b \in \mathbb{Q}\right\}$

$(S, +, \cdot)$ is a ring with unity, $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ being the unity

Let $A = \begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$, $B = \begin{pmatrix} p & q \\ 2q & p \end{pmatrix} \in S$, then

$$A\cdot B = \begin{pmatrix} ap + 2bq & ap + bp \\ \cancel{2bp} + 2aq & 2bq + ap \end{pmatrix}$$

$$B\cdot A = \begin{pmatrix} pa + 2qb & pb + qa \\ 2qa + 2qb & 2qb + pa \end{pmatrix}$$

$\therefore A\cdot B = B\cdot A \ \forall A, B \in S$.

Hence $(S, +, \cdot)$ is a commutative ring with ~~to~~ unity.

Let $A = \begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$ be a non-zero element of S, then

$(a,b) \neq (0,0)$

$|A| = a^2 - 2b^2 \neq 0$ since $(a,b) \neq (0,0)$ and a, b are rational

$\therefore A^{-1}$ exists.

$$A^{-1} = \frac{1}{a^2-2b^2}\begin{pmatrix} a & -b \\ -2b & a \end{pmatrix} \in S.$$

$\therefore$ Each non-zero element of S is a unit.

Hence $(S, +, \cdot)$ is a field.

Q.11. Examine if the ring of matrices $\left\{ \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} : a, b \in \mathbb{R} \right\}$ is a field.

Ans:- Let $S = \left\{ \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} : a, b \in \mathbb{R} \right\}$

$(S, +, \cdot)$ is a commutative ring with unity.

Let $A = \begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$ be a nonzero element of S.

Then $(a,b) \neq (0,0)$

A^{-1} exists if and only if $|A| \neq 0$

$|A| = a^2 - 2b^2$.

There exists non-zero real numbers a, b such that

$a^2 - 2b^2 = 0$

For example $a = \sqrt{2}, b = 1$

$\therefore$ The non-zero matrix $\begin{pmatrix} \sqrt{2} & 1 \\ 2 & \sqrt{2} \end{pmatrix}$ has no inverse

Hence $(S, +, \cdot)$ is not a field.

Q.12. Prove that the set S of matrices $\left\{\begin{pmatrix} a & 0 \\ b & c\end{pmatrix} : a,b,c \in \mathbb{Z}\right\}$ is a subring of the ring $M_2(\mathbb{Z})$.

Ans:– Let $A = \begin{pmatrix} a_1 & 0 \\ b_1 & c_1\end{pmatrix}$ and $B = \begin{pmatrix} a_2 & 0 \\ b_2 & c_2\end{pmatrix}$, where

$a_1, b_1, c_1, a_2, b_2, c_2 \in \mathbb{Z}$

The $A-B = \begin{pmatrix} a_1-a_2 & 0 \\ b_1-b_2 & c_1-c_2\end{pmatrix} \in S$ as

$a_1-a_2,\ b_1-b_2,\ c_1-c_2 \in \mathbb{Z}$

Again $AB = \begin{pmatrix} a_1 & 0 \\ b_1 & c_1\end{pmatrix}\begin{pmatrix} a_2 & 0 \\ b_2 & c_2\end{pmatrix}$

$= \begin{pmatrix} a_1a_2 & 0 \\ b_1a_2+c_1b_2 & c_1c_2\end{pmatrix} \in S$, as

$a_1a_2,\ b_1a_2+c_1b_2,\ c_1c_2 \in \mathbb{Z}$

$\therefore$ S is a subring of the ring $M_2(\mathbb{Z})$

Q.13. Prove that the ring $(\mathbb{Z}_n, +, \cdot)$ is an integral domain if and only if n is a prime.

Ans:– Let $(\mathbb{Z}_n, +, \cdot)$ be an integral domain. Then it is a non-trivial commutative ring with unity having no divisor of zero. Since it is non trivial $n \neq 1$. We prove that n is a prime.

Let n be a composite number and $n = pq$ where p and q are positive integers and $1 < p < n$, $1 < q < n$.

Then $\bar{p} \in \mathbb{Z}_n$, $\bar{q} \in \mathbb{Z}_n$ and $\bar{p}\bar{q} = \bar{n} = \bar{0}$

This implies that the ring $(\mathbb{Z}_n, +, \cdot)$ contains divisors of zero, a contradiction to the hypothesis

$\therefore$ n is a prime.

Conversely

Let n be a prime. The ring $(\mathbb{Z}_n, +, \cdot)$ is a commutative ring with unity, $\bar{1}$ being the unity.

Let $\bar{m}$ be a non-zero element in $\mathbb{Z}_n$.

Then $0 < m < n$.

Since n is a prime, $\gcd(m, n) = 1$. Therefore, there exist integers u and v such that $um + vn = 1$.

Consequently $um \equiv 1 \pmod{n}$.

Clearly $u \not\equiv 0 \pmod{n}$

Let $u \equiv r \pmod{n}$, where $0 < r < n$.

$\Rightarrow um \equiv rm \pmod{n}$

$\Rightarrow 1 \equiv rm \pmod{n}$.

$\Rightarrow \bar{r}\bar{m} = \bar{1}$

Since the ring is commutative $\bar{r}.\bar{m} = \bar{m}.\bar{r} = \bar{1}$

This proves that $\bar{m}$ is a unit and therefore $\bar{m}$ is not a divisor of zero.

Hence the ring contains no divisor of zero and thus is an integral domain.

Q.14. Prove that the ring $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$, the ring of Gaussian integers is an integral domain.

Ans :- The ring of Gaussian integers is a commutative ring with unity. $(1 + 0i)$ being the unity.

Let $(a+bi)(c+di) = 0$ and let $a + bi \neq 0$

Then $(a, b) \neq (0, 0)$

$(a+bi)(c+di) = 0$ gives $ac - bd = 0$, $ad + bc = 0$.

This is a homogeneous system of equations in a, b having non-zero solutions.

$\therefore$ The coefficient determinant of the system, $c^2 + d^2 = 0$.

This gives $c = 0$, $d = 0$

Thus $(a+bi)(c+di)=0$ with $a+bi=0$ implies $c+di=0$. This proves that the ring contains no divisor of zero. Hence it is an integral domain.

Q.15. Prove that Z_{11}, the ring of integers modulo 11 is a field. State any theorem that you use. Find the multiplicative inverses of all non-zero elements of Z_{11}.

Ans:- i. Z_{11} is closed w.r.t. addition modulo 11.

ii. Addition modulo 11 is associative in Z_{11}

Ex:- $(\bar{3}+\bar{9})+\bar{6} = \bar{1}+\bar{6} = \bar{7}$

$\bar{3}+(\bar{9}+\bar{6}) = \bar{3}+\bar{4} = \bar{7}$

iii. $\bar{0}$ is the additive identity.

iv. The inverse of each element exist.

The inverse of $\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5},\bar{6},\bar{7},\bar{8},\bar{9},\bar{10}$ are $\bar{0},\bar{10},\bar{9},\bar{8},\bar{7},\bar{6},\bar{5},\bar{4},\bar{3},\bar{2},\bar{1}$ respectively.

v. The operation addition modulo 11 is commutative.

Ex:- $\bar{2}+\bar{8} = \bar{10} = \bar{8}+\bar{2}$

vi. Z_{11} is closed w.r.t multiplication modulo 11.

vii. Multiplication modulo 11 is associative in Z_{11}

Ex:- $(\bar{2}\times\bar{5})\times\bar{3} = \bar{10}\times\bar{3} = \bar{8}$

$\bar{2}\times(\bar{5}\times\bar{3}) = \bar{2}\times\bar{4} = \bar{8}$

$\therefore (\bar{2}\times\bar{5})\times\bar{3} = \bar{2}\times(\bar{5}\times\bar{3})$

viii. Inverse of each element exist and $\bar{1}$ is the multiplicative identity.

ix. The operation multiplication is commutative.

Ex:- $\bar{3}\times\bar{6} = \bar{7} = \bar{6}\times\bar{3}$.

x. The distributive property holds in Z_{11}

$\bar{2}\times(\bar{6}+\bar{7}) = \bar{2}\times\bar{2} = \bar{4}$, $\bar{2}\times\bar{6}+\bar{2}\times\bar{7} = \bar{1}+\bar{3} = \bar{4}$.

Hence $(Z_{11},+,\cdot)$ is a field.

The multiplicative inverse of $\bar{1},\bar{2},\bar{3},\bar{4},\bar{5},\bar{6},\bar{7},\bar{8},\bar{9},\bar{10}$ are $\bar{10},\bar{9},\bar{8},\bar{7},\bar{6},\bar{5},\bar{4},\bar{3},\bar{2},\bar{1}$ respectively.

Q.16. Let R be a ring. The centre of R is set $\{x \in R : ax = xa\} \ \forall a \in R$. Prove that the centre of the ring is a subring.

Ans:- i. Associativity of both addition and multiplication is inherited from R. Distributivity of multiplication over addition is inherited from R. Hence it is associative over R.

ii. Let a, b ~~$\in R$~~ in the centre and x in R. Then

$$x(a+b) = ax + bx = xa + xb = (a+b)x.$$

Hence it is closed under addition.

The additive identity exists and it is 0.

$$0 = 0 \cdot x = x \cdot 0$$

So 0 is in the centre.

The inverse of an element also exists.

if $a \in R$, then

$$a + (-a) = 0 = (-a) + a \quad \text{, then } -a \in R.$$

Now let us show $-a$ is in the centre.

Let x in R.

$$0 = 0 \cdot x = (a + (-a))x = ax + (-a)x \text{, and}$$

$$0 = x \cdot 0 = x(a + (-a)) = xa + x(-a)$$

As $xa = ax$, it follows that $(-a)x = x(-a)$.

Hence inverses exist in the centre. So the centre is a group under $+$.

Now for multiplication,

For a, b in the centre and x in R,

$$(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab)$$

Thus multiplication is closed.

1 is the multiplicative identity.

$$1 \cdot x = x \cdot 1 = x$$

Hence x is in the centre.

So the centre is a subring of R.

Scanned by CamScanner

Q.17. In a ring $(\mathbb{Z}_n, +, \cdot)$, $[m]$ is a unit if and only if $\gcd(m,n)=1$

Ans:- The ring is a commutative ring with unity, $[1]$ being the unity.

Let $[m]$ be a unit in the ring, then $[m]$ is a non-zero element and there exists a non-zero element $[u]$ in the ring such that $[m][u] = [1]$.

$[m]\cdot[u] = [1]$

$\Rightarrow mu \equiv 1 \pmod n$.

So $mu - 1 = vn$ for some integer v.

$\Rightarrow mu - nv = 1$, where u and v are integers.

This proves that $\gcd(m,n) = 1$.

<u>Conversely</u>

Let $[m]$ be an element in the ring such that the $\gcd(m,n)=1$

Then for some integers u & v, $um + vn = 1$

So $um \equiv 1 \pmod n$.

Then $u \neq 0$.

Let $u \equiv r \pmod n$, where $0 < r < n$

$u \equiv r \pmod n$

$\Rightarrow um \equiv rm \pmod n$

$\Rightarrow 1 \equiv rm \pmod n$

$\Rightarrow [r][m] = [1]$

$\therefore [r][m] = [m][r] = [1]$, since the ring is commutative.

This shows that $[m]$ is a unit.

Q.18. In a ring R with unity $(xy)^2 = x^2y^2$ $\forall x, y \in R$, then show that R is commutative.

Ans:- Since the unity of ring $1 \in R$, $\forall x, y \in R$.

By given conditions.

$[x(y+1)]^2 = x^2(y+1)^2$

$\Rightarrow [x(y+1)][x(y+1)] = x^2 (y+1)(y+1)$

$\Rightarrow (xy+x)(xy+x) = x^2 [y(y+1) + (y+1)]$ [Distributive law]

$\Rightarrow xy(xy+x) + x(xy+x) = x^2 [y^2 + y + y + 1]$

$\Rightarrow (xy)^2 + xyx + xxy + x^2 = x^2y^2 + x^2y + x^2y + x^2$

$\Rightarrow x^2y^2 + xyx + x^2y + x^2 = x^2y^2 + x^2y + x^2y + x^2$

$\Rightarrow xyx + x^2y = x^2y + x^2y$

$\Rightarrow xyx = x^2y$.

Replacing x with $(x+1)$, we get.

$(x+1)y(x+1) = (x+1)^2 y$

$\Rightarrow (xy+y)(x+1) = (x+1)(x+1)y$

$\Rightarrow (xy+y)x + (xy+y)1 = \{x(x+1) + 1(x+1)\} y$

$\Rightarrow xyx + yx + xy + y = (x^2 + x + x + 1)y$

$\Rightarrow x^2y + yx + xy + y = x^2y + xy + xy + y$

$\Rightarrow yx + xy = xy + xy$

$\Rightarrow \cancel{xy = yx}\; yx = xy$.

$\therefore$ R is commutative.

Q.19. Prove that in a Field, $a^2 = b^2$ implies either $a = b$ or $a = -b$ for $a, b \in F$.

Ans:- By Right distribution law,

$(a-b)(a+b) = (a-b).a + (a-b).b$

$\Rightarrow a.a - b.a + a.b - b.b$ [By left distributive law].

$\Rightarrow a^2 - a.b + a.b - b^2$ [$\because a.b = b.a, \forall a, b \in F$]

$\Rightarrow a^2 - b^2 = a^2 - a^2$ [$\because a^2 = b^2$]

$= 0$

$\therefore$ Either $a - b = 0$ or $a + b = 0$

$\therefore$ Either $a = b$ or $a = -b$.

Q.20. Find all the solutions of the equation $x^2+x-6=0$ in the ring $\mathbb{Z}_{14}$ by factoring the quadratic polynomial.

Ans:- By factorising we get $(x+3)(x-2)$

For x, y in $\mathbb{Z}14$, we have $x*y=0$.

This can happen if and only if

$x*y$ is a multiple of 14.

$\therefore$ Either x is a multiple of 7 or y is a multiple of 7.

The only two multiples of 7 in $\mathbb{Z}_{14}$ are 0 and 7 so

$x+3=0$

or

$x+2=0$

or

$x+3=7$

or

$x-2=7$.

$\therefore$ Solutions of x are 2, 4, 9, 11.

Q.21. Find all solutions of the equation $x^3-2x^2-3x=0$ in the ring $\mathbb{Z}_{12}$

Ans:- Factoring $x^3-2x^2-3x=0$ gives.

$$x(x+1)(x-3)=0$$

In $\mathbb{Z}_{12}$, the product of two non-zero elements may be 0.

We have to find all elements of x, where $x \in \mathbb{Z}_{12}$ and $0 \leq x \leq 11$

Thus zero occurs in $\mathbb{Z}_{12}$ when $x=0, 3, 5, 8, 9, 11$ in

$$x(x+1)(x-3)=0$$

$\therefore$ Solutions of the equation $x^3-2x^2-3x=0$ in $\mathbb{Z}_{12}$ is

0, 3, 5, 8, 9, 11

Q.22. An element a of a ring R is idempotent if $a^2 = a$.

i. Show that the set of all idempotent elements of a commutative ring is closed under multiplication.

Ans: — If $a \in R$, $a+a \in R$.

$\Rightarrow (a+a)^2 = a+a$, by the given condition

$\Rightarrow (a+a)\cdot(a+a) = a+a$

$\Rightarrow (a+a)\cdot a + (a+a)\cdot a = a+a$

$\Rightarrow (a^2+a^2) + (a^2+a^2) = a+a$ $\quad [\because a\cdot a = a^2]$

$\Rightarrow (a+a) + (a+a) = (a+a) + 0$ $\quad [\because a+0 = a]$

$\Rightarrow a+a = 0$ [LCL]

Now let $a+b = 0$

$\therefore a+b = a+a.$

[$b = a$ by LCL]

$\therefore (a+b)^2 = a+b$

$\Rightarrow (a+b)\cdot(a+b) = a+b$

$\Rightarrow (a+b)\cdot a + (a+b)\cdot b = a+b.$

$\Rightarrow a^2 + ba + ab + b^2 = a+b.$

$\Rightarrow (a+ba) + (ab+b) = a+b$

$\Rightarrow (a+b) + (ba+ab) = a+b)$

$\Rightarrow ba+ab = 0$ [LCL]

$\Rightarrow ab = ba.$

$\therefore R$ is commutative.

6. Find all idempotents in $\mathbb{Z}_6 \times \mathbb{Z}_{12}$

Ans: — The idempotents of this ring are the ordered pairs (a,b) such that a is an idempotent of Z_6 and b is an idempotent of Z_{12}.

$\therefore$ Idempotent of $Z_6 = \{0,1,3,4\}$

$\therefore$ Idempotent of $Z_{12} = \{0,1,4,9\}$

$\therefore$ Idempotent of $Z_6 \times Z_{12} = \{0,1,3,4\} \times \{0,1,4,9\}$

Q.21. Prove that the intersection of two subrings is a subring.

Ans: — Let S & T be two subrings of a ring R. Then $S \cap T$ is non-empty as $0 \in S \cap T$.

Let $S \cap T = \{0\}$.

Then obviously $S \cap T$ is a trivial subring of R.

Now,

Let $S \cap T \neq \{0\}$ and $a, b \in S \cap T$.

Then $a \in S$, $a \in T$, $b \in S$, $b \in T$

Now $a - b \in S$, $\because a \in S, b \in S$.

and $a \cdot b \in S$, as S is a subring of R.

Similarly

$a - b \in T$ and $a \cdot b \in T$ as T is also a subring of R.

Hence $a - b \in S \cap T$, and $a \cdot b \in S \cap T$.

$\therefore$ $S \cap T$ is a subring of R.