Assignment - 01

Name - Siddharth Jha
Roll no - 23/mc/151

(modern algebra)

Q.1 To Prove $n \cdot ab = (n \cdot a)b = a(n \cdot b)$

Proof:- when $n = 1$ we have

$ab = ab$, $(1 \cdot a)b = ab$, $a(1 \cdot b) = ab$

So the equality holds for some positive integer k, i.e assume

$k \cdot ab = (k \cdot a)b = a(k \cdot b)$.

now we need to show that it holds for $k+1$, meaning we want to prove.

$(k+1)ab = ((k+1) \cdot a)b = a((k+1) \cdot b)$.

By using the definition of multiplication in rings and the distributive property, we write;

$(k+1)ab = (k \cdot ab) + ab$

By the inductive hypothesis $k \cdot ab = (k \cdot a)b = a(k \cdot b)$, so;

$(k+1) \cdot ab = ((k \cdot a) + a)b = (k \cdot a)b + ab = ((k+1) \cdot a)b$

similarly

$a((k+1) \cdot b) = a((k \cdot b) + b) = a(k \cdot b) + ab = (k \cdot ab) + ab = (k+1) \cdot ab$

Since both $(k+1) \cdot ab = (k+1) \cdot a)b$ and $(k+1) \cdot ab = a(k+1) \cdot b$ hold, the result follows by induction

thus we have shown that $n \cdot ab = (n \cdot a)b = a(n \cdot b)$ for any +ve integers

Q.2 Let

(i) $a^2-b^2=(a+b)(a-b)$ holds $\forall\ a,b\in R$ ~~then R is~~

(ii) let $a,b\in R$

Expanding $(a+b)(a-b) = a^2-ab+ba-b^2$ (distributive property)

$a^2-b^2 = a^2-ab+ba-b^2$

$0 = -ab+ba$

$\Rightarrow ab = ba$ So R is commutative

Converse :-

let R is commutative

then $ab=ba\ \forall\ a,b\in R$

$(a+b)(a-b) = a^2-ba+ab-b^2 = a^2-b^2$

thus $a^2-b^2=(a+b)(a-b)$

Hence proved

Q.3

Proof :-

$A=\begin{pmatrix} a & a \\ b & b \end{pmatrix}$ and $B=\begin{pmatrix} c & c \\ d & d \end{pmatrix}$ where $a,b,c,d\in Z$

then,

$A+B=\begin{pmatrix} a & a \\ b & b \end{pmatrix}+\begin{pmatrix} c & c \\ d & d \end{pmatrix}=\begin{pmatrix} a+c & a+c \\ b+d & b+d \end{pmatrix}$

Since ~~a~~ ac+ad and bc+bd are integers

~~A.B is of the form $\begin{pmatrix} e & e \\ f & f \end{pmatrix}$ where $e=ac+ad$, $f=bc+bc$~~

A+B is also in S. therefore S is closed under addition.

Now checking S is closed under multiplication or not

Consider the product A·B

$$A \cdot B = \begin{pmatrix} a & a \\ b & b \end{pmatrix}\begin{pmatrix} c & c \\ d & d \end{pmatrix} = \begin{pmatrix} ac+ad & ac+ad \\ bc+bd & bc+bd \end{pmatrix}$$

Since ac+ad and bc+bd are integers,

A·B is of the form $\begin{pmatrix} e & e \\ f & f \end{pmatrix}$; where e = ac+ad and f = bc+bd

thus A·B is in S and S is closed under multiplication.

→ Now check if S contains the additive identity.

The additive identity in $M_2(2)$ is the zero matrix

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

we can see that the matrix is in S because it can be written as $\begin{pmatrix} a & a \\ b & b \end{pmatrix}$ with a=0 & b=0.

Hence, proved

Q.4 Take any two elements $x, y \in A+B$. By definition of A+B we can write

$x = a_1+b_1$ and $y = a_2+b_2$
where $a_1, a_2 \in A$ and $b_1, b_2 \in B$

then,

$x+y = (a_1+b_1)+(a_2+b_2) = (a_1+a_2)+(b_1+b_2)$

Since A and B are ideals, they are closed under addition
So $a_1+a_2 \in A$ & $b_1+b_2 \in B$. therefore $x+y \in A+B$,
Showing that A+B is closed under addition.

Consider now we will show that A+B is closed under multiplication

Let $r \in R$ and any $x \in A+B$. then $x = a+b$ for some $a \in A$ and $b \in B$.

Consider rx & xr

$rx = r(a+b) = ra+rb$ (since A and B are ideals of R they are closed under multiplication by elements of R. thus $ra \in A$ and $rb \in B$, so $rx = ra+rb \in (A+B)$)

Similarly

$ar \in A$ & $br \in B$ we have $xr = ar+br \in A+B$

$xr = (a+b)r = ar+br$

therefore, A+B is closed under multiplication by elements of R.

Q.6 Take two elements $z_1, z_2 \in Z(R)$

By def z_1 & z_2 commute with every element in R

$(z_1+z_2)r = z_1r+z_2r = rz_1+rz_2 = r(z_1+z_2)$

thus z_1+z_2 commute with every $r \in R$

So $z_1+z_2 \in Z(R)$ therefore, Z(R) is closed under addition.

now we are checking that Z(R) is closed under multiplication or not

Let $z_1, z_2 \in Z(R)$ since z_1 & z_2 commute with every element in R $\forall r \in R$

$(z_1z_2)r = (z_1(z_2r)) = z_1(rz_2) = (z_1r)z_2 = (rz_1)z_2 = r(z_1z_2)$

thus $z_1 z_2$ also commutes with every $r \in R$, so $z_1 z_2 \in Z(R)$. Therefore $Z(R)$ is closed under multiplication.

Checking that $Z(R)$ contains the additive identity 0

the additive identity 0 of R satisfies $0 \cdot r = r \cdot 0 = 0$ $\forall$ $r \in R$ so $0 \in Z(R)$.

Now check that $Z(R)$ is closed under additive inverse

if $z \in Z(R)$ then z commutes with every $r \in R$. The additive inverse $-z$ also commutes with every r

Since:

$(-z)r = -(zr) = -(rz) = r(-z)$

thus $-z \in Z(R)$, so $Z(R)$ is closed under additive inverse.

Since $Z(R)$ is closed under addition, multiplication, contains the additive identity, and is closed under additive inverses, $Z(R)$ is a subring of R.

→ Why $Z(R)$ may not be an ideal??

for $Z(R)$ to be an ideal of R it must satisfy that for any $z \in Z(R)$ and any $r \in R$, both $rz \in Z(R)$ and $zr \in Z(R)$. However $Z(R)$ only guarantees that z commutes with every element of R but doesn't require elements of R to commute with each other.

Q.7 ⇒ Let's consider an example with the ring $R = 2\mathbb{Z}$

$$R = \{2n \mid n \in \mathbb{Z}\}$$

where
- R is closed under addition & multiplication
- The additive identity of R is 0 but there is no multiplicative identity in R because there is no element $e \in R$ such that $e \cdot 2 = 2 \ \forall \ 2 \in R$

thus $R = 2\mathbb{Z}$ is a ring without a unity element.

Now Consider $S = \mathbb{Z}$ the set of all integers which is a subring of R;

- $S \subseteq R$ because every int is an int multiple of 2
- S has unity element: the number 1

$$1 \cdot a = a \cdot 1 = a \ \forall \ a \in S$$

Q.8 ⇒ No, the unity of a subring doesn't have to be the same as the unity of the whole ring. However if the subring and the whole ring both have a unity, the unity of the subring must act as the unity within the subring itself, but it may not necessarily be the same as the unity of the whole ring.

for ex:-

Consider $R = 2\mathbb{Z}$ with no unity and its subring $S = \mathbb{Z}$ which has unity 1 (since $1 \cdot n = n \ \forall \ n \in \mathbb{Z}$)

R has no unity but S has its own unity, 1, which is not a unity in R since $1 \notin R$.

Q.9

let $x, y \in \mathbb{Q}[\sqrt{d}]$,

$x = a+b\sqrt{d}$ & $y = c+e\sqrt{d}$ $\quad a, b, c, e \in \mathbb{Q}$

Addition

$x+y = (a+b\sqrt{d}) + (c+e\sqrt{d}) = (a+c) + (b+e)\sqrt{d}$.

Since $a+c \in \mathbb{Q}$ & $b+e \in \mathbb{Q}$ we have

$x+y \in \mathbb{Q}[\sqrt{d}]$. therefore $\mathbb{Q}[\sqrt{d}]$ is closed under addition

Subtraction

$x-y = (a+b\sqrt{d}) - (c+e\sqrt{d}) = (a-c) + (b-e)\sqrt{d}$

Since $a-c \in \mathbb{Q}$ & $b-e \in \mathbb{Q}$, we have

$x-y \in \mathbb{Q}[\sqrt{d}]$. therfore $\mathbb{Q}[\sqrt{d}]$ is closed under Subtraction

closure under multiplication

consider $x \cdot y = (a+b\sqrt{d})(c+e\sqrt{d}) = ac + ae\sqrt{d} + bc\sqrt{d} + be \cdot d$

$x \cdot y = (ac + be \cdot d) + (ae+bc)\sqrt{d}$.

Since $ac + be \cdot d \in \mathbb{Q}$ & $ae+bc \in \mathbb{Q}$, it follows that $x \cdot y \in \mathbb{Q}[\sqrt{d}]$ therfore $\mathbb{Q}[\sqrt{d}]$ is closed under multiplication..

check for multiplicative inverse

To show that $\mathbb{Q}[\sqrt{d}]$ is a field, we must also show that every nonzero element $x = a+b\sqrt{d}$ (where $a, b \in \mathbb{Q}$ and $x \neq 0$) has a multiplicative inverse in $\mathbb{Q}[\sqrt{d}]$

thus multiplicative inverse of $x = a+b\sqrt{d}$

$$\frac{1}{x} = \frac{1}{a+b\sqrt{d}}$$

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

Since $a, b \in \mathbb{Q}$ $a^2-b^2d \in \mathbb{Q}$ and assuming $u \neq 0$ we have $a^2-b^2d \neq 0$

therefore $\frac{1}{a+b\sqrt{d}} = \frac{a-b\sqrt{d}}{a^2-b^2d} \in \mathbb{Q}[\sqrt{d}]$

Q.10 Consider two matrices $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$ in $M_2(\mathbb{Z})$

the Sum A and B is

$$A+B = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}$$

Now applying ϕ to $A+B$

$$\phi(A+B) = a+e$$

on the other hand

$$\phi(A) + \phi(B) = a+e$$

thus $\phi(A+B) = \phi(A) + \phi(B)$ so ϕ preserves addition

Now the product of A & B is

$$A \cdot B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae+bg & af+bh \\ cg+dg & cf+dh \end{pmatrix}$$

applying ϕ to $A \cdot B$

$$\phi(A \cdot B) = ae+bg$$

on the other hand, applying ϕ to A and B separately the multiplying

$$\phi(A) \cdot \phi(B) = a \cdot e = ae$$

Since $ac+bg \neq ac$ (in general when b and g are non-zero) we see that $\phi(A \cdot B) \neq \phi(A) \cdot \phi(B)$

Q.11 ~~Let S = {a}~~

Verifying if S is a subring of $\mathbb{Z}[i]$

(1) Containment of 0;
the element 0 can be written as $0+i \cdot 0$ where $a=0$ & $b=0$ therefore $0 \in S$

(2) closed under addition
Consider two elements $x = a+ib$ & $y = c+id$ in S where $a, c \in \mathbb{Z}$ & $b, d \in \mathbb{Z}$ are even then

$x+y = (a+c)+i(b+d)$

Since $a+c \in \mathbb{Z}$ & $b+d \in \mathbb{Z}$ (and is even as the sum of two even integers is even). $x+y \in S$ thus S is closed under addition.

(3) closed under subtraction :-

Consider $x = a+ib$ & $y = c+id$ in S

then
$x-y = (a-c)+i(b-d)$

Since $a-c \in \mathbb{Z}$ & $b-d \in \mathbb{Z}$ (and is even as the diff of two even int is even) $x-y \in S$. thus S is closed under subtraction.

(4) closed under multiplication

$x = a+ib$ & $y = c+id$ in S

$x \cdot y = (a+ib)(c+id) = (ac-bd)+i(ad+bc)$

Since b & d are even so both bd & ad+bc are even

$\therefore$ $ac-bd \in \mathbb{Z}$
$ad+bc \in \mathbb{Z}$ (and is even

thus $x \cdot y \in S$, so S is closed under multiplication.

Now to be an ideal of $\mathbb{Z}[i]$, S must satisfy the property that for any $s \in S$ and any $z \in \mathbb{Z}[i]$, the product $z \cdot s$ must be in S.

Consider $s = 1+2i \in S$ (with $a=1$ & $b=2$ so b even)

Now let $z = i \in \mathbb{Z}[i]$

then

$z \cdot s = i \cdot (1+2i) = i + 2i^2 = 1 + 2(-1) = i - 2 = -2 + i$

the result $-2+i$ is not in S because its imaginary part 1 is not even.

So $\mathbb{Z}[i]$ is not an ideal of $\mathbb{Z}[i]$.

Q.12 Idempotent of $\mathbb{Z}_{10}$

(a) for $x = 0$ $\quad x^2 = 0 \equiv x \pmod{10}$

$x = 0$ is idempotent

for $x = 1$: $x^2 = 1 \equiv x \pmod{10}$

$x = 1$ idempotent

for $x = 2$: $x^2 = 4 \not\equiv 2 \pmod{10}$

for $x = 3$ $x^2 = 9 \not\equiv 3 \pmod{10}$

$x = 4$ $x^2 = 16 \not\equiv 4 \pmod{10}$

$x = 5$ $x^2 = 25 \equiv 5 \pmod{10}$

$x = 6$ $x^2 = 36 \not\equiv 6 \pmod{10}$

$x = 7$ $x^2 = 49 \not\equiv 7 \pmod{10}$

$x = 8$ $x^2 = 64 \not\equiv 8 \pmod{10}$

$x = 9$ $x^2 = 81 \not\equiv 9 \pmod{10}$

thus the idempotent elements in $\mathbb{Z}_{10}$ are $\{0, 1, 5\}$

Idempotent elements in $\mathbb{Z}_{12}$

for $n=0$ $n^2=0 \equiv n \pmod{12}$
$n=1$ $n^2=1 \equiv n \pmod{12}$
$n=2$ $n^2=4 \not\equiv 2 \pmod{12}$
$n=3$ $n^2=9 \not\equiv 3 \pmod{12}$
$n=4$ $n^2=16 \equiv 4 \pmod{12}$
$n=5$ $n^2=25 \not\equiv 5 \pmod{12}$
$n=6$ $n^2=36 \equiv 6 \pmod{12}$
$n=7$ $n^2=49 \not\equiv 7 \pmod{12}$
$n=8$ $n^2=64 \not\equiv 8 \pmod{12}$
$n=9$ $n^2=81 \equiv 9 \pmod{12}$
$n=10$ $n^2=100 \not\equiv 10 \pmod{12}$
$n=11$ $n^2=121 \not\equiv 11 \pmod{12}$

thus the idempotentent element in $\mathbb{Z}_{12}$ are $\{0,1,4,6,9\}$

Q.1.3 let $A = \langle 4 \rangle = \{4n \mid n \in \mathbb{Z}\}$ and
$B = \langle 8 \rangle = \{8n \mid n \in \mathbb{Z}\}$

then $A/B = \{0+B, 4+B, 8+B, 12+B\}$

define $\phi : A/B \to \mathbb{Z}_4$ by $\phi(4k+B) = k \pmod 4$

- ϕ is well defined, bijective & preserves addition
- Hence $A/B \cong \mathbb{Z}_4$ as groups

for A/B

- $(4+B)(4+B) = 16+B = 0+B$

in $\mathbb{Z}_4$

- $1 \cdot 1 = 1 \neq 0$

thus $A/B \cong \mathbb{Z}_4$ as rings

Q.14 let $\phi: R \to S$ be a ring homomorphism

$Im(\phi) = \{\phi(r) \mid r \in R\}$ is subring of S

(1) addition closure

for $a, b \in Im(\phi)$ $a = \phi(r_1)$, $b = \phi(r_2)$

then $a+b = \phi(r_1+r_2) \in Im(\phi)$

(2) multiplication closure

$ab = \phi(r_1 r_2) \in Im(\phi)$

(3) Additive Identity

$0_S = \phi(0_R) \in Im(\phi)$

thus $Im(\phi)$ is a subring of S.

Q.15 Proof :-

let S be a non empty subset of a ring R

(1) Non-emptiness

S has at least one element a.

(2) Additive identity

for $a \in S$, $a-a = 0 \in S$

(3) closed under addition

for $a, b \in S$ $a-(-b) = a+b \in S$.

(4) closed under Substraction:

given $a, b \in S$ $a-b \in S$

(5) closed under multiplication

given $a, b \in S$ $a \cdot b \in S$.

Q. 16 Let $\{S_i\}_{i \in I}$ be a collection of subrings of R.
define $S = \bigcap_{i \in I} S_i$

(1) Non-emptiness
S contains 0 (since $0 \in S_i$ for all i).

(2) closed under subtraction :-
if $a, b \in S$, then $a, b \in S_i$ for all i so $a - b \in S_i$. thus $a - b \in S$

(3) closed under multiplication
If $a, b \in S$ then $ab \in S_i$ for all i. thus, $ab \in S$

So S is a subring

Union of subrings

Let S_1 & S_2 be subrings of R define $S = S_1 \cup S_2$
Counter ex :-
Let $S_1 = 2$ & $S_2 = 2Z$ in Z
then $S_1 \cup S_2 = \{n \in Z \text{ or } n \equiv 0 \mod 2\}$

1. $1 \in S_1$, $1 \notin S_2$
2. $1 + 1 = 2 \in S_2$, $1 + 1 \notin S_1$

thus $S_1 \cup S_2$ is not closed under addition and is not a subring.

Q. 17 Let R be an integral domain and let $a, b, c \in R$ with $a \neq 0$ & $ab = ac$

(1) Rewrite the eqn
$ab - ac = 0$

(2) factor out a
$a(b - c) = 0$

(3) use integral domain property

Since R is an integral domain (no zero divisors) $a \neq 0$, implies $b - c = 0$

Conclusion $b = c$;

thus the Cancellation law holds in R.

Q.18 Let R be a Commutative ring without zero divisors we want to show that the characteristics of R is either 0 or a prime number

the characteristic of R is the smallest $n > 0$ such that $n \cdot 1 = 0$, or 0 if no such n exists.

Assume $n \neq 0$;

Suppose $n = ab$ (with $1 < a, b < n$). then $n \cdot 1 = (a \cdot 1)(b \cdot 1) = 0$

Since R has no zero divisors $a \cdot 1 = 0$ or $b \cdot 1 = 0$

contradicting the minimality of n

hence the characteristic is 0 or a prime

Q.19 To show that the characteristic of R is 2 we need to prove that $a + a = 0$ for any $a \in R$ which implies $2 \cdot a = 0$

Since R is Boolean $\forall a \in R \; a^2 = a$

$\Rightarrow (a+a)^2 = a^2 + 2a^2 + a^2 = a + a$

Since $a^2 = a$

$a + a = 0$

$\therefore 2 \cdot a = 0 \; \forall a \in R$ So characteristic of R is 2.

Q.20

To show that a Boolean ring R is commutative we need to prove that $ab = ba \quad \forall \quad a, b \in R$

→ in Boolean ring every element is idempotent
So $a^2 = a$ & $b^2 = b \quad \forall \quad a, b \in R$

→ consider $(a+b)^2$

$$(a+b)^2 = a^2 + ab + ba + b^2$$

→ Since $a^2 = a$ & $b^2 = b$

$$a + ab + ba + b = a + b$$

Subtract $a+b$ from both sides

$$ab + ba = 0$$

this shows $ab = -ba$ But in a Boolean ring $a+a=0$ so $-ba = ba$, Hence $ab = ba$ proving that R is commutative.