Def" :-

Subring :- Any nonempty subset S of a ring $(R, +, \cdot)$ is called a subring if $(S, +, \cdot)$ is itself a ring.

NOTE :-

Each ring has trivial subrings $\{0\}$ and R.

Eg :-

(1) Under usual add^n & multip^n

$E = \{0, \pm 2, \pm 4, \pm 6, \dots\}$

Z = set of integers

Q = set of Rationals

R = set of Reals

C = set of complex.

are all rings.

From this we can say that E is a subring of each of these rings

$\mathbb{Z}$ is a subring of each ring $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ and etc.

(2) Denote $M_n = M_n(R)$, the set of $n \times n$ matrices over the real field R. Then M_2 is a non commutative ring under matrix add^n and matrix multip^n so that $M_2(R)$ is a subring of $M_n(R)$.

In general $M_n(R)$ is a subring of $M_n(\mathbb{C})$.

Theorem

Q.13) Prove that a non-empty subset S of a ring R is a subring of $R (=) x-y, xy \in S \ \forall x, y \in S$?

Proof:- Given that S is a non-empty subset of ring $(R, +, \cdot)$

Part I :-

Suppose that S is a subring of R
$\Rightarrow$ S is itself a ring
$\because x, y \in S$
$\Rightarrow x, -y \in S$ — By G_4 of R_1 in S.
$\Rightarrow x + (-y) \in S$ — By G_1 of R_1 in S.
$\Rightarrow x - y \in S$
Also $x, y \in S \Rightarrow xy \in S$ — By G_1 of R_2 of S

Thus $x-y, xy \in S, \forall x, y \in S$
This proofs necessary condition.

Part II :-

Conversely suppose that $x-y, xy \in S \quad \forall x, y \in S$
we want to prove that S is subring of R.

(i) S is a non-empty subset of group $(R, +)$ together with
$x + (-y) = x - y \in S, \forall x, y \in S$
∴ By a theorem of subgroup,
$(S, +)$ is a subgroup of $(R, +)$.
But $(R, +)$ is commutative group.
∴ $(S, +)$ is also a commutative group
i.e R_1 holds for S.

(ii) We have $xy \in S, \forall x, y \in S$
Also associativity for multip^n is satisfied for element of S because of G_2 of R_2 in R.
⇒ $(S, \cdot)$ is a semigp i.e R_2 holds for S

(iii) Let $a, b, c \in S \subseteq R$
∴ By R_3 of R we have $a(b+c) = ab + ac$
Also $(b+c) \cdot a = b \cdot a + c \cdot a$
$\forall a, b, c \in S$
i.e R_3 holds for S.

Hence $(S, +, \cdot)$ is a ring but S is a non-empty subset of R.
$\therefore$ S is a subring of R.
This proofs sufficient conditions
Hence follows the theorem.

[SET]

Q.(4) Let S_1 & S_2 be subrings of a ring R, then prove that $S_1 \cap S_2$ is a subring of R?

Sol^{n} :- Given that S_1 & S_2 are subrings of R
$\Rightarrow$ S_1 & S_2 are non-empty subsets of R. Also $0 \in S_1$, $0 \in S_2$
$\Rightarrow$ $0 \in S_1 \cap S_2$
$\therefore$ $S_1 \cap S_2$ is a non-empty subset of R (A)
let $x, y \in S_1 \cap S_2$.
$\Rightarrow$ $x, y \in S_1$ & $x, y \in S_2$
But S_1 & S_2 are subrings of R.
$\therefore$ By a theorem
$x-y, xy \in S_1$ & $x-y, xy \in S_2$.
$\Rightarrow$ $x-y, xy \in S_1 \cap S_2$

$\therefore$ $x-y, xy \in S_1 \cap S_2$ $\forall x, y \in S_1 \cap S_2$ (B)
From (A) & (B), a standard thm on subring implies that
$S_1 \cap S_2$ is a subring of R.

In general intersection of any 2 subring of a ring R is a subring of R.

NOTE :-
Intersection of any family of subring of a ring R is a subring of R.

15/12

[W7] Ideals :-

Def^n :- A nonempty subset U of a ring R is called

(1) left ideal of R if
(i) U is a subgroup of (R, +)
(ii) $r \in R$, $u \in U \Rightarrow ru \in U$

(2) Right ideal of R if
(i) U is a subgroup of (R, +)
(ii) $r \in R$, $u \in U \Rightarrow ur \in U$

(3) An ideal or two sided ideal of R if
(i) U is a subgroup of (R, +)
(ii) $r \in R$, $u \in U \Rightarrow ru, ur \in U$.

REMARK :-
(1) U is an ideal of R if and only if $x, y \in U$, $r \in R \Rightarrow x - y \in U$, ru & $ur \in U$

(2) Every ring R has 2 trivial ideals, $\{0\}$ and R. These are called improper ideals. Other ideals are called non-trivial or proper ideals.

(3) A ring which has only trivial ideals is called a simple ring.

Ex

(8) If V is a left or right or two sided ideal of a ring R. Then prove that V is a subring of R?

Proof:- Given that V is a left or right or two sided ideal of ring R.

Then we have

(i) V is a subgroup of $(R, +)$

i.e $x - y \in V \ \forall \ x, y \in V$

(ii) For $r \in R$, $u \in V$, we have

$ru \in V$ or $ur \in V$ or both $ru, ur \in V$.

For $x \in V \subseteq R$ and $y \in V$

we get $xy \in V$ because of left ideal

OR For $y \in V \subseteq R$ and $x \in V$

we get $xy \in V$ because of right ideal

OR $xy, yx \in V$ because of two sided ideal.

Thus,
$x-y \in U$, $xy \in U$ $\forall x, y \in U$
$\Rightarrow$ U is a subring of R.

[W6] Ex
6.(S) Let R be a ring then prove that intersection of 2 left ideals of R is a left ideal of R?

Proof:- Let U & V be 2 left ideals of a ring R. Then $0 \in U$ & $0 \in V$
$\Rightarrow 0 \in U \cap V$
$\therefore U \cap V$ is a nonempty subset of R. ①
Let $x, y \in U \cap V$ and $r \in R$
$\Rightarrow x, y \in U$ and $x, y \in V$ with $r \in R$.
$\Rightarrow x-y \in U$, $rx \in U$ as U is left ideal of R.
Also $x-y \in V$, $rx, ry \in V$ as V is left ideal of R
$\Rightarrow x-y \in U \cap V$ and $rx, ry \in U \cap V$
$\therefore x-y \in U \cap V$ and $rx \in U \cap V$ $\left.\begin{matrix} \forall x, y \in U \cap V \\ \forall r \in R \end{matrix}\right\}$ ②
$\therefore$ From ① & ② we obtain $U \cap V$ is left ideal of R.
Thus intersection of 2 left ideals of R is again a left ideal.

[105]

Q.(7) Prove that if an ideal U of a ring R contain unity of R then U = R? OR

If U is an ideal of R with unity 1 and $1 \in U$, prove that U = R?

Proof:- Given that U is an ideal of ring R.

$\Rightarrow x-y,\ xr,\ rx \in U \ \forall\ x, y \in U$ ... (1)
$\forall\ r \in R$

Also given that R is with unity 1 and $1 \in U$

we want to prove that U = R

Obviously $U \subseteq R$

we show that $R \subseteq U$

Let $r \in R$

Then $r \cdot 1,\ 1 \cdot r \in U$ for $1 \in U$ - using (1)

$\Rightarrow r \in U$ $\{\because$ 1 is unity of R
$\Rightarrow r \cdot 1 = r = 1 \cdot r$

$\therefore R \subseteq U$

Hence U = R

Hence proved.

[56]

5(e) If F is a field, then prove that its only ideals are $\{0\}$ and F itself?

Proof :- Let F be a field

$\Rightarrow$ F is a commutative division ring we want to prove that $\{0\}$ and F are the only (improper) ideals of F. On the contrary we assume that S is any proper ideal of F.

$\Rightarrow$ S is neither $\{0\}$ nor complete F.

Let $0 \neq a \in S \subseteq F$.

Then $a^{-1} \in F$ s.t

$aa^{-1} = 1 = a^{-1}a$ — By Gen of Rs of F

where 1 is unity of F.

Now; $a^{-1} \in F$ (ring), $a \in S$ (ideal)

$\Rightarrow a^{-1}a, aa^{-1} \in S$ — By def^n

$\Rightarrow 1 \in S$

$\Rightarrow S = F$ — By a result

which contradicts our assumption that S is a proper ideal (subset) of F.

Hence a field F has only trivial ideals $\{0\}$ and F.

NOTE :-
A field F is thus a simple ring.

[S5, S7] Theorem :-
S.(9) Let R be a commutative ring with unit element whose only ideals are {0} and R itself. Then prove that R is a field?

Proof :- We are given that R is a commutative ring with unit element 1. Also R has only trivial ideals {0} and R.
We want to prove that R is a field For this it is sufficient to prove that non-zero element form a group under multiplication.
Clearly we have $G_1, G_{12}, G_{3,4,5}$ for multiplication in R.
We show that every non-zero element of R possess its inverse in R.
Let $0 \neq a \in R$
Rem We define $Ra = \{xa / x \in R\}$.
Clearly for $1 \in R$ we have
$1 \cdot a \in Ra$
$\Rightarrow a \in Ra$
$\therefore$ Ra is a non-empty subset of R
↳ (1)

we prove that Ra is an ideal of R

(i) Let $u, v \in Ra$

$\Rightarrow u = xa$, $v = ya$ for some $x, y \in R$

Then $u - v = xa - ya$

$= xa + (-ya)$

$= xa + [(-y)a]$ - By a result in R

$= [x + (-y)]a$ - By right distr.

$= (x - y)a$

For $x, y \in R$ we have $x - y \in R$.

$\{\because (R, +)$ is a group

$\therefore (x - y)a \in Ra$

i.e $u - v \in Ra$

$\therefore u - v \in Ra$, $\forall u, v \in Ra$ — (2)

i.e Ra is a subgroup of R under addition.

(ii) Let $u \in Ra$ and $r \in R$

$\Rightarrow u = xa$ for some $x \in R$

Then $ru = r(xa)$

$= (rx)a$ - by G_2 of R_2 of R

For $r, x \in R$ we have $rx \in R$ - By G_1 of R_2.

$\therefore (rx)a \in Ra$

i.e $ru \in Ra \subseteq R$.

But R is commutative ring

$\therefore ru = ur \in Ra$

Thus $xa, ax \in Ra \ \forall x \in R$, $\forall u \in Ra$ → (3)

From (1), (2) and (3) we obtain Ra is an ideal of R.

But we are given that R has only two trivial ideals, $\{0\}$ and R itself.

∴ We must have

either $Ra = \{0\}$ or $Ra = R$.

But $a \in Ra$ and $a \neq 0$

∴ $Ra \neq \{0\}$

∴ $\boxed{Ra = R}$

We have R is with unit element 1.

⇒ Ra also has 1.

i.e $1 \in Ra$

⇒ $1 = ba$ for some $b \in R$ - By def^n of Ra

∴ $1 = ba = ab$ → ∵ R is commutative

Thus for $a \neq 0$ in R, ∃ some $b \in R$ s.t. $ab = 1 = ba$.

⇒ b is a multiplicative inverse of a in R.

∴ Every non-zero element of R has multiplicative inverse in R.

Hence proved.

i.e R is a field.

16/12

Def" :-

Maximal ideal :-

An ideal $M \neq R$ in a ring R is said to be the maximal ideal of R if whenever U is an ideal of R s.t $M \subset U \subset R$, then either $M = U$ or $U = R$.

REMARK :-

An ideal M different from ring R is maximal of R if there is no ideal betn M & R.

[56] Theorem :-

11. (8) If R is a commutative ring with a unit element and M is an ideal of R. Then prove that M is a maximal ideal of R iff R/M is a field?

Proof :- We are given that

(1) R is a commutative ring with unit element 1.

(2) M is an ideal of R.

Then $R/M = \{M+a / a \in R\}$ is a quotient ring under the operations of the form

Addition :- $(M+a) + (M+b) = M + (a+b)$

Multip" :- $(M+a) \cdot (M+b) = M + (a \cdot b)$

Here the identity element w.r.t addition is $M+0=M$, where 0 is zero element of ring R.

Also,

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

$= M+(b\cdot a)$ {∵ R is commu

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

$\therefore (M+a)\cdot(M+b) = (M+b)\cdot(M+a)$ $\forall M+a,$

$M+b \in R/M$

$\Rightarrow R/M$ is a commutative ring.

And $(M+a)\cdot(M+1) = M+(a\cdot 1)$

$= M+a$ — By G_{13} of R_2 in R

$\therefore (M+a)\cdot(M+1) = M+a = (M+1)\cdot(M+a)$

↳ By commutivity in R/M $\forall M+a \in R/M$

$\Rightarrow (M+1)$ is unity of R/M.

★ Now by a result there is one to one correspondance bet^n the set of ideals of R/M to the set of ideals of R which contain M.

Part I :-

Given :- M is a maximal ideal of R

Claim :- R/M is a field

Since M is maximal ideal of R, there is no ideal of R bet^n M and R.

∴ By result ⊛, R/M has only 2 ideals $\{0\}$ of R/M i.e $\{M+0\}$ and

R/M itself.
Thus R/M is a commutative ring with unity having only 2 ideals $\{M+0\}$ and R/M itself.
$\Rightarrow$ R/M is a field — By a result.
This proves necessary condition.

Part II :-
Given :- R/M is a field.
Claim :- M is a maximal ideal of R.
Since R/M is a field, it has only two ideals $\{0\}$ of R/M i.e $\{M+0\}$ and R/M itself.
$\therefore$ By result (*) R has exactly 2 ideals which contain M.
$\Rightarrow$ R has only two ideals M and R itself.
$\therefore$ By def^n, M is maximal ideal of R as there is no ideal of R bet^n M and R.
This proves sufficient condition.
Hence follows the theorem.