THEORY

1. RING - The structure $(R,+,\cdot)$ consisting of a non-void set R and two binary operⁿ, denoted by $+$ and $\times$ is s.t.b a ring if
$(R,+)$ is an abelian group
$(R,\cdot)$ is a semi group
$\forall a,b,c \in R$

$a(b+c) = ab+ac$ (Left distributive law)
$(a+b)c = ac+bc$ (Right distributive law)

$(R,+)$ is called the additive group $(R,\cdot)$ is called the multiplicative grp.
Identity element of additive group is called additive identity / zero element
Identity element of multiplicative group is called multiplicative identity / unity

RING WITH UNITY - A ring $(R,+,\cdot)$ is s.t.b a ring with unity if its multiplicative identity exists i.e if $\exists\, e \in R$
$ea = ae = a \quad \forall a \in R$

COMMUTATIVE RING - If multiplicative composition is also commutative i.e if
$ab = ba$

COMMUTATIVE RING WITH UNITY → CR + RU
Identity element + commutative.

PROPERTIES OF A RING

Theorem 1) For any elements a, b, c of a ring R:

$a0 = 0a = 0$
$b = b+0$
$0 + \cancel{ab} = \cancel{ab} + a0$
$0 = a.0$

$b = b+0$
$ba = (b+0)a$
$0 + \cancel{ba} = \cancel{ba} + 0.a$
$0 = 0.a$

$a(-b) = -(ab) = (-a)(b)$
$a0 = 0$
$a(-b+b) = 0$
$a(-b) + ab = 0$
$a(-b) = -(ab)$
$(-a+a)b = 0$
$(-a)b + ab = 0$
$(-a)b = -(ab)$

$(-a)(-b) = ab$
$(-a)(-b) = -[a(-b)]$
$= -[-(ab)]$
$= ab$

$a(b-c) = ab - ac$
$a(b-c)$
$= a[b+(-c)]$
$= ab + a(-c)$
$= ab - ac$

ZERO DIVISOR IN A RING - An element $a(\neq 0)$ of a ring R is s.t.b a zero divisor if $\exists$ a non-zero b in R such that $a \times b = 0$

Eg- $[\{0,1,2,3,4,5\}, +_6, \times_6]$
2, 3 and 4 are zero divisors
$2 \times_6 3 = 0 \quad 3 \times_6 2 = 0 \quad 4 \times_6 3 = 0.$

RING WITHOUT ZERO DIVISOR - A ring is s.t.b a ring without zero divisor if it has no zero divisor i.e $a,b \in R$
$ab = 0 \Rightarrow a = 0$ or $b = 0$.

Eg $(\mathbb{Z},+,\times), (\mathbb{Q},+,\times), (\mathbb{R},+,\times)$

RING WITH ZERO DIVISOR - A ring is s.t.b a ring with zero divisor if $\exists\, a,b \in R$ such that $a \neq 0$ $b \neq 0$ yet $a.b = 0$.

BOOLEAN RING – A ring $(R,+,\times)$ is called a Boolean ring if all $\forall a \in R$ are idempodent i.e $a^2 = a$
for eg $\{0,1\}$ is a boolean ring

Theorem 2 A ring R is without zero divisors iff the cancelation law holds in R

considering them to be zero divisors

suppose $a \neq 0$ $ab = ac$,

$$ab = ac \Rightarrow ab - ac = ac - ac$$
$$ab - ac = 0$$
$$a(b-c) = 0$$
$$b - c = 0 \quad [\because a \neq 0]$$
$$b = c$$

cancellation law holds

$$ab = 0$$
$$\cancel{a}b = \cancel{a}0$$
$$b = 0$$

INTEGRAL DOMAIN – A ring D is s.t.b an integral domain if it is a commutative ring with unity and without 0 divisor

Ring R is
(i) commutative
(ii) with unity
(iii) without 0 divisors

Eg → $(\mathbb{Z},+,\times)$, $(\mathbb{Q},+,\times)$, $(\mathbb{C},+,\times)$, $(\mathbb{R},+,\times)$

Theorem → Ring $(\mathbb{Z}_p = \{0,1,2,\ldots(p-1)\}, +_p, \times_p)$ is an integral domain iff p is prime

FIELD – A ring F is called a field if it is
i) commutative
ii) with unity
iii) its every non-zero element is invertible
iv) Distributive law

$(R,+)$ is an abelian group + $(R,\times)$ is an abelian group (Multiplicative inverse of every non-zero number)

Eg $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$, $(\mathbb{C},+,\times)$

UNIT ELEMENT IN A RING – Let R be a ring with unity and 1 be the identity of the 2nd composition, then any $a \in R$ is called a unit element if $\exists$ $b \in R$ such that $ab = 1$
(Inverse hai matlab)

Eg $(\mathbb{Z},+,\times) \to 1$ and -1 are unit elements

Theorem The set of all units in a ring with unity forms a multiplicative group.

DIVISION RING → Field – commutativity in $(R,\times)$
SKEW FIELD

A ring is called a division ring or a skew field if
1) It is a ring with unity
2) Each of its non-zero element has an inverse

Eg → $n \times n$ non singular matrices over real numbers.

Theorem Every field is necessarily an integral domain but converse of it is not true

C.R + R.U + Distributive + Non zero divisors

F is without zero divisor prove and to ajayega

$a, b \in F$ such that $a \neq 0$

$ab = 0$

If $a \in F, a^{-1} \in F$

$ab = 0$

$a^{-1}(ab) = a^{-1} 0$

$b = 0$

$\therefore$ F is without zero divisor.

F is integral domain

Theorem A finite commutative ring without zero divisor is a field

$(R, +, \times)$ — $(R, +)$ abelian, $(R, \times)$ semi + commutative

field: $(R, +) \to$ abelian, $(R, \times) \to$ abelian

Let us suppose R has n elements $a_1, a_2 \dots a_n$ and $a_i \in R$ $a_i \neq 0$

consider n products $a_1 . a_i, a_2 a_i, \dots, a_n . a_i$

All these products belong to R (closed)

$a_r a_i = a_s a_i$

$a_r a_i - a_s a_i = 0$

$(a_r - a_s) a_i = 0$ $(\because a_i \neq 0)$

$a_r = a_s$ R is without zero divisor

So No two elements are =

Thus we see that

$R = \{a_1, a_2 \dots a_n\} = \{a_1 a_i, a_2 a_i, \dots, a_n a_i\}$

But $a_i \in R$ so there exists a_k in R such that

$a_k a_i = a_i$

R is commutative $a_k a_i = a_i a_k = a_i$

Let any element $b \in R$ then $a_m \in R$

$b = a_m a_i$

$a_k b = b a_k = (a_m a_i) a_k$

$= a_m (a_i . a_k)$

$= a_m . a_i = b$

a_k is unity in R

Every non zero element has multiplicative inverse

$e \in R \Rightarrow \exists a_j \in R$

$a_j . a_i = a_i . a_j = e$

a_i is any arbitrary non-zero element in R

which implies that multiplicative inverse exits

... Let $(R,+,\times)$ be a ring. If there exists a +ve integer n such that $na=0$, $\forall a \in R$, R is s.t.b a ring with finite characteristic. If no such +ve integer exists, then R is s.t.b characteristic zero

Eg The characteristic of Ring $(Z_4, +_4, \times_4)$ is 4 because $n \times = 0$ $n \in Z_4 \Rightarrow n(\text{least}) = 4$

Rings with characteristic zero $(Q,+,\times), (R,+,\times), (C,+,\times), (Z,+,\times)$

No. of times any element is added to obtain 0

CHARACTERISTIC OF AN INTEGRAL DOMAIN AND FIELD

The characteristic of an integral domain or a field D is the least integer n for which $n.e=0$

If no such +ve integer exists then D is s.t.b of characteristic 0

No. of times identity element is added to obtain 0

Eg in $(Z_7, +_7, \times_7)$ is 7 because $o(1)=7$ in $(Z_7, +_7)$

Theorem → The characteristic of an integral domain is either 0 or a prime no.

SUBRING → A nonvoid subset of a Ring $(R,+,\times)$ is called a subring of R iff S itself is a ring for induced compositions

IMPROPER OR TRIVIAL SUBRINGS → Every ring has min. 2 subrings R itself and $\{0\}$.

PROPER SUBRING → A subring which is not an improper subring

If $(S,+,\cdot)$ is a subring of $(R,+,\cdot)$ then $(S,+)$ is a subgroup of the commutative group $(R,+)$

Eg ring $(mZ,+,\times)$ $m \in Z$ is a subring of $(Z,+,\times)$

Theorem → The necessary and sufficient condn for a non-void subset S of a ring R to be a subring of R are $a \in S$, $b \in S \Rightarrow (a-b), ab \in S$.

To prove subring $a \in S$ $b \in S$ $(a-b), ab \in S$

suppose S is a subring of ring R

$a, b \in S$

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

$a+(-b) \in S$

$a \in S$, $b \in S \Rightarrow ab \in S$

Now considering condn only

$S \neq \phi$ Let $a \in S$

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

$a-a \in S \Rightarrow 0 \in S$ (Additive identity)

$0 \in S$ $a \in S$

$0-a \in S \Rightarrow -a \in S$ (Additive inverse)

$a \in S$ $b \in S \Rightarrow a \in S$ $-b \in S$

$a-(-b) \in S$ $a+b \in S$ (closed)

Associativity and commutation must hold in S as they hold in R

Moreover by condn $ab \in S$, S is closed in multiplication

Also associativity and distributivity of multiplicn over addn must hold in S since they hold in R

Theorem 2 The intersec^{n} of two subrings is again a subring

Let S_1 and S_2 be two subrings

$0 \in S_1, \quad 0 \in S_2$

$\Rightarrow 0 \in S_1 \cap S_2$

$S_1 \cap S_2 \neq \phi$

Let $a, b \in S_1 \cap S_2$ then

$a, b \in S_1 \quad a, b \cap S_2$

$a-b \in S_1, ab \in S_1 \quad a-b \cap S_2 \quad ab \in S_2$

$a-b \in S_1 \cap S_2 \quad ab \in S_1 \cap S_2$

$S_1 \cap S_2$ is a subring