Ring

$G \to m$

$\parallel \quad G \to n \qquad m\%n$

Def Ring:

Let R be a non-empty set on which we have two closed binary operations denoted by $+$ and $\cdot$

Then $(R, +, \cdot)$ is a ring if for all $a, b, c \in R$, the following conditions are satisfied.

(a) $a+b = b+a$ — commutative law of $+$

(b) $a+(b+c) = (a+b)+c$ — Associative law of $+$

(c) There exists $z \in R$ such that $a+z = z+a = a$ for every $a \in R$ — Existence of an identity for $+$

(d) For each $a \in R$ there is an element $b \in R$ with $a+b = b+a = z$. — Existence of inverse under $+$

(e) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ — Associative law of $\cdot$

(f) $a \cdot (b+c) = a \cdot b + a \cdot c$

$(b+c) \cdot a = b \cdot a + c \cdot a$ — Distributive Laws of $\cdot$ over $+$

Definition : Integral domain, field

Let R be a commutative ring with unity. Then identity

(a) R is called an integral domain if R has no proper divisor of zero.

(b) R is called a field if every non-zero element of R is a unit. identity

NOTE: The ring R is said to have no proper divisors of zero if for all $a, b \in R \Rightarrow ab = 0 \Rightarrow a = 0$ (or) $b = 0$ (or)

Definition : Sub ring

$a, b \in R \Rightarrow a, b = Z$

$\Rightarrow a = Z, b = Z$

For ring $(R, +, \cdot)$, a non-empty subset S of R is called a subring of R if $(S, +, \cdot)$. that is S under the addition and multiplication of R, restricted to S is a ring.

Def: Ideal

A non-empty subset I of a ring R is called a subring of R if $(S, +, \cdot)$ - that is, S under the addition and multiplication of R, restricted to S - is a ring.

*/. Theorem : 2 PART-A, B

Every field is an integral domain.

Proof: Let R be a field

To prove R is an integral domain, it is enough to prove that it has no zero divisors suppose.

$a, b \in R$ with $ab = 0$, $a \neq 0$ then there exists $a^{-1} \in R$ such that $aa^{-1} = 1$

$ab = 0$

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

$ab = 0 \Rightarrow a = 0$ or $b = 0$

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

$\therefore$ R has no zero divisors

$b = 0 \quad a \neq 0$

Hence R is an integral domain.

$a = 0 \quad b \neq 0$

Theorem 3 :

*/. Every finite integral domain is a field.

Proof: Let $(R, +, \cdot)$ be a finite integral domain

$\therefore$ R is a commutative ring with identity and without zero divisors.

Claim :

To prove R is a field, it is enough to prove that every non-zero element in R has multiplicative inverse.

Let $R = \{0, \overset{\text{identity}}{1}, a_2, a_3 \dots a_n\} : a \in R$

and $a \neq 0$

Multiplying the non-zero and they are distinct.

Suppose $a \cdot a_j = a, a_k, j \neq k$ then

$aa_j = aa_k$ | $a(a_j - a_k) = 0$

$aa_j - aa_k$

$a.(a_j - a_k) = 0$ since $a \neq 0, a_j = a_k,$

which is a contradiction to the fact that a_k are distinct elements in R.

$\therefore a \cdot a_j \neq a \cdot a_k$

Since R is finite, these n elements are same as the n non-zero elements in R in some order by pigeon hole principle.

$\therefore 1 = a \cdot a_i$ for some $a_i \in R$. since R is commutative, $a \cdot a_i = a_i \cdot a = 1$

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

Hence any finite integral domain is a field.

∗ Theorem 1:

The fundamental theorem of homomorphism

Let R and R' rings and $f : R \to R'$ an epimorphism. Let K be the kernel of f. Then $R/K \cong R'$

R and R' and $f : R \to R'$ an epimorphism

Proof: Define $\phi : R/K \to R'$ by $\phi(K+a) = f(a)$

(i) To prove ϕ is well defined Let $K+b = K+a$

Then $b \in K+a$,

∴ $b = k+a$, where $k \in K$.

$f(b) = f(k+a) = f(k) + f(a) = 0 + f(a) = f(a)$

$\phi(K+b) = f(b) = f(a) = \phi(K+a)$

(ii) claim : ϕ is 1-1

for, $\phi(K+a) = \phi(K+b) \Rightarrow f(a) = f(b)$

$\Rightarrow f(a) - f(b) = 0 \Rightarrow f(a) + f(-b) = 0$

$f(a-b) = 0 \Rightarrow a-b \in K$,

$a \in K+b \Rightarrow K+a = K+b$

(iii) claim : ϕ is onto

for, let $a' \in R'$,

Since f is onto, there exists $a \in R$

Such that $f(a) = a'$

Hence, $\phi(k+a) = f(a) = a'$

iv) $\phi[(k+a)+(k+b)] = \phi[k+(a+b)] =$

$f(a+b) = f(a) + f(b)$

$\therefore \phi[(k+a)+(k+b)] = \phi(k+a) + \phi(k+b)$

$\phi[(k+a)(k+b)] = \phi[k+(ab)] =$

$f(ab) = f(a) + f(b)$

$\therefore \phi[(k+a)(k+b)] = \phi(k+a)\phi(k+b)$

Hence, ϕ is an isomorphism