UNIT-V

Maximal and Prime Ideal

Def/:-

Let R be a ring An ideal M of R is said to be a Maximal ideal of R if whenever U is an ideal of R such that $M \subseteq U \subseteq R$ then either $U = M$ or $U = R$. That is, there is no Proper ideal of R Properly containing M.

Eg:-

Let P be any Prime. Then (P) is maximal ideal in Z.

Let U be any ideal of Z such that $P \subseteq U$.

$\because$ every ideal of Z is a Principal ideal

$U = (n)$ for some $n \in Z$.

Now, $P \in (P) \subseteq U \Rightarrow P \in U = (n)$.

$\therefore P = nm$ for some integer m.

$\because$ P is Prime either $n = 1$. Then $U = Z$. $n = P$.

Suppose $n = P$. Then $U = Z$.

Suppose $n = P$ Then $U = (P)$.

$\therefore$ There's no Proper ideal of Z Properly containing (P). Hence (P) of a maximal ideal in Z.

Theorem 5.1

Let R be a Commutative ring with identity. An ideal M of R is maximal iff R/M is a field.

Let M be a maximal ideal in R.

$\therefore$ R is a Commutative ring with identity and $M \neq R$, R/M is also a Commutative ring with identity.

Now, let M+a be a non-zero element in R/M So that $a \notin M$. We shall Prove that M+a has a multiplicative inverse in R/M.

Let $U = \{ra + m / r \in R \text{ and } m \in M\}$.

W.C.T U in an ideal of R.

$(r_1a + m_1) - (r_2a + m_2) = (r_1 - r_2)a + (m_1 - m_2) \in U$.

Also, $r(r_1a + m_1) = (rr_1)a + rm_1 \in U$ ($\because rm_1 \in M$).

$\therefore$ U is an ideal of R.

Now, let $m \in M$. Then $m = 0a + m \in U$.

$\therefore M \subseteq U$.

Also, $a = 1a + 0 \in U$ & $a \notin M$.

$\therefore M \neq U$.

$\therefore$ U is an ideal of R Properly containing M.

But M is a maximal ideal of R.

$\therefore U = R$. Hence $1 \in U$.

$\therefore$, $1 = ba + m$ for some $b \in R$.

Now,

$M+1 = M + ba + m = M + ba$ ($\because$, $m \in M$)

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

Hence $M+b$ is the inverse of $M+a$.

Thus every non-zero element of R/m has an inverse.

Hence R/M is a field.

Conversely, suppose R/M is a field.

Let U be any ideal of R properly containing M.

$\therefore$, There exists an element $a \in U$ such that $a \notin M$.

$\therefore$, $M+a$ is a non-zero element of R/M.

$\therefore$, R/M is a field $M+a$ has an inverse,

Say $M+b$.

$\therefore$, $(M+a)(M+b) = M+1$.

$\therefore$, $M+ab = M+1$.

$\therefore$, $1-ab \in M$.

But $M \subseteq U$. Hence $1-ab \in U$.

Also $a \in U \Rightarrow ab \in U$.

$\therefore$, $1 = (1-ab)+ab \in U$. Thus $1 \in U$.

$\therefore$, $U = R$. Thus there is no proper ideal of R properly containing in M. Hence M is a maximal ideal in R.

Definition:

Let R be a commutative ring. An ideal $P \neq R$ is called a Prime ideal if $ab \in P \Rightarrow$ either $a \in P$ or $b \in P$.

eg:-

Let R be an integral domain. Then (0) is a Prime ideal of R.

For, $ab \in (0) \Rightarrow ab = 0$.

$\Rightarrow a = 0$ or $b = 0$ ($\because$ R is an I.D.)

$\Rightarrow a \in (0)$ or $b \in (0)$.

Theorem 5.2:

Let R be any Commutative ring with identity. Let P be an ideal of R. Then P is a Prime ideal $\Leftrightarrow R/P$ is an integral domain.

Let P be a Prime ideal.

$\because$ R is a commutative ring with identity R/P is also commutative ring with identity.

Now, $(P+a)(P+b) = P+0$

$\Rightarrow P+ab = P$

$\Rightarrow ab \in P$.

$\Rightarrow a \in P$ or $b \in P$ ($\because$ P is a Prime ideal)

$\rightarrow P+a = P$ or $P+b = P$.

Thus R/P has no zero divisors.

$\therefore R/P$ is integral domain.

Conversely, Suppose R/P is an integral domain.

w.r.t., P is a Prime ideal of R

Let $ab \in P$. Then $P+ab=P$.

$\therefore (P+a)(P+b)=P$.

$\therefore P+a=P$ or $P+b=P$. ($\because$ R/P has no. zero-div

$\therefore a \in P$ or $b \in P$.

$\therefore P$ is Prime ideal of R.

Corollary:

Let R be a Commutative ring with identity. Then every maximal ideal of R is a Prime ideal of R.

Let M be a maximal ideal of R.

$\therefore$, R/M is a field. ($\because$ by theorem 5.1)

$\therefore$, R/M is an integral domain

Note:-

The Converse of the above statement isn't true. For eg., (0) is a Prime ideal of Z but not a maximal ideal of Z.

Homomorphism of Rings

Defn/:-

Let R and R' be rings. A function $f: R \to R'$ is called a homomorphism if

$$f(a+b) = f(a) + f(b) \text{ and}$$
$$f(ab) = f(a)f(b) \quad \forall\, a, b \in R.$$

If f is 1-1, then f is called a monomorphism. If f is onto, then f is called an epimorphism. A homomorphism of a ring onto itself is called an endomorphism.

Note:

1, Obviously an isomorphism of a ring is a homomorphism and a 1-1, onto homomorphism is an isomorphism.

2, The name homomorphism is used for mapping between groups and between rings. In groups, a homomorphism preserves the binary operation of the group. Since rings have two binary operations, a ring homomorphism is defined as a mapping preserving the two binary operations in a ring.

3, Condition (i) of a ring homomorphism says that f is a group homomorphism from the additive group $(R,+)$ to the additive group $(R',+)$.

eg:-

1, $f: R \to R'$ defined by $f(a)=0 \ \forall a \in R$ is obviously a homomorphism. f is called the trivial homomorphism.

2, Let R be any ring. The identity map $f: R \to R$ is obviously a homomorphism.

3, Let R be any ring. $f: R \times R \to R$ given by $f(x,y)=x$ is a ring homomorphism.

For,

$$f[(a,b)+(c,d)] = f(a+c, b+d) = a+c$$
$$= f(a,b)+f(c,d).$$

Also, $f[(a,b)(c,d)] = f(ac, bd) = ac$
$$= f(a,b) f(c,d).$$

4, $f: Z \to Z_n$ defined by $f(x)=r$ where $x = qn+r$, $0 \le r < n$ is a homomorphism.

For, let $a, b \in Z$.

Let, $a = q_1 n + r_1$ where $0 \le r_1 < n$,

$b = q_2 n + r_2$ where $0 \le r_2 < n$,

$r_1 + r_2 = q_3 n + r_3$, where $0 \le r_3 < n$, and

$r_1 r_2 = q_4 n + r_4$ where $0 \le r_4 < n$.

Now,

$(a+b) = (q_1+q_2)n + r_1 + r_2 \quad (\because r_1 + r_2 = q_3 n + r_3)$

$= (q_1+q_2+q_3)n + r_3$

$\therefore f(a+b) = r_3$

$= r_1 \oplus r_2$

$= f(a) \oplus f(b)$.

Also, $ab = (q_1 n + r_1)(q_2 n + r_2)$

$= n(q_1 q_2 n + r_1 q_2 + r_2 q_1) + r_1 r_2$.

$= n(q_1 q_2 n + r_1 q_2 + r_2 q_1 + q_4) + r_4$.

$\therefore f(ab) = r_4$

$= r_1 \odot r_2$

$= f(a) \odot f(b)$.

Hence f is a homomorphism.

5, Let R be a ring and I be an ideal of R. Then $\phi : R \to R/I$ defined by $\phi(x) = I + x$ is a ring homomorphism. ϕ is called the natural homomorphism.

$\phi(x+y) = I + (x+y)$

$= (I+x) + (I+y)$

$= \phi(x) + \phi(y)$.

$$\phi(xy) = I + xy$$
$$= (I+x)(I+y)$$
$$= \phi(x)\phi(y).$$

Hence ϕ is a ring homomorphism.

Theorem 5.3:

Let R & R' be a rings and $f: R \to R'$ be a homomorphism. Then,

(i) $f(0) = 0'$.

(ii) $f(-a) = -f(a)$ $\forall a \in R$.

(iii) If S is a subring of R, then $f(S)$ is a subring of R'. In Particular $f(R)$ is a Subring of R'.

(iv) If S is an ideal of R, then $f(S)$ is an ideal of $f(R)$.

(v) If S' is a subring of R', then $f^{-1}(S')$ is a Subring of R.

(vi) If R is a ring with identity 1 and $f(1) \neq 0'$, then $f(1) = 1'$ is the identity of $f(R)$.

(vii) If R is a commutative ring then $f(R)$ is also commutative.

Proof:- Since f is a homomorphism of the group $(R,+)$ to $(R',+)$, the results (i) & (ii) follow from $[f(e) = e' \text{ & } f(a^{-1}) = [f(a)]^{-1}]$ by the theorem

(iii) ∵, S is a subring of R, (S,+) is a sub group of (R,+) and hence f(S) is a subgroup of (R',+).

Now, let a', b' ∈ f(S).

Then a' = f(a) and b' = f(b) for some a, b ∈ S.

∴, a'b' = f(a) f(b)

= f(ab) ∈ f(S).

Hence f(S) is a subring of R'.

(iv) Let S be an ideal of R.

To. P.t., f(S) is an ideal of f(R) it's enough if we P.t., r' ∈ f(R) and a' ∈ f(S) ⇒ r'a' and a'r' ∈ f(S).

Let r' = f(r) and a' = f(a) where r ∈ R and a ∈ S.

Now ∵, S is an ideal of R, ra and ar ∈ S.

Hence f(ra) = f(r) f(a) = r'a' ∈ f(S).

Similarly a'r' ∈ f(S).

Hence f(S) is an ideal of f(R).

(v) Let S' be a subring of R'. Since $(S',+)$ is a subgroup of $(R',+)$, $f^{-1}(S')$ is a subgroup of $(R,+)$.

Now, let $a,b \in f^{-1}(S')$.

Then $f(a), f(b) \in S'$.

$\therefore f(ab) = f(a)f(b) \in S'$ ($\because S'$ is a subring of R')

$\therefore ab \in f^{-1}(S')$.

Hence $f^{-1}(S')$ is a subring of R.

(vi) Proof is III^{rly} to (v) above theorem.

(vii) Let R be a ring with identity 1. Let $a' \in f(R)$.

Then $a' = f(a)$ for some $a \in R$.

Now, $a'f(1) = f(a)f(1)$

$= f(a1) = f(a) = a'$.

III^{rly} $f(1)a' = a'$. Also $f(1) \neq 0$.

Hence $f(1)$ is the identity of $f(R)$.

(viii) Proof is left to the reader.

Defn/:-

The Kernel of a homomorphism f of a ring R of a ring R' is defined by

$\{a / a \in R \text{ \& } f(a) = 0\}$.

Theorem 5.4:

Let $f: R \to R'$ be a homomorphism. Let K be the kernel of f. Then K is an ideal of R.

By definition, $K = f^{-1}(\{0\})$.

$\because \{0\}$ as an ideal of $f(R)$, by (v) of theorem S' is an ideal of $f(R)$, then $f^{-1}(S')$ is an ideal of R.

The fundamental theorem of homomorphism

Theorem 5.5:

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

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

(i) ϕ is well-defined, for let $K+b = K+a$.

Then $b \in K+a$.

$\therefore b = K+a$ where $k \in K$.

$\therefore f(b) = f(k+a) = f(k) + f(a)$

$= 0 + f(a) = f(a)$.

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

(ii) ϕ is 1-1

For, $\phi(k+a) = \phi(k+b) \Rightarrow f(a) = f(b)$

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

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

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

$\Rightarrow a - b \in k$

$\Rightarrow a \in k + b$

$\Rightarrow k + a = k + b$

(iii) ϕ is onto

For, let $a' \in R'$

$\therefore$ for only those exists $a \in R$ such that $f(a) = a'$

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

(iv) ϕ is homomorphism.

For,

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

$$= f(a+b)$$

$$= f(a) + f(b) \quad (\because f \text{ is homomorphism})$$

$$= \phi(k+a) + \phi(k+b)$$

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

$$= f(ab)$$

$$= f(a) f(b) \quad (\because f \text{ is homomorphism})$$

$$= \phi(k+a)\phi(k+b).$$

Hence ϕ is an isomorphism and

hence $R/k \cong R'$.

Solved Problem

Problem 01:

The homomorphic image of an integral domain need not be an integral domain.

$f: Z \to Z_4$ defined by $f(a) = r$ where $a = 4q + r, 0 \leq r < 4$ is a homomorphism of Z onto Z_4. Here Z is an integral domain and Z_4 isn't an integral domain.

$\because 2 \odot 2 = 0$.

Problem 02:

Any homomorphism of a field to itself is either one-one or maps every element to 0.

Let F be a field and $f: F \to F$ be a homomorphism. Let K be the kernel of f. Then K be the kernel of f. Then K is an ideal of F. $K = \{0\}$ or $K = F$.

If $K = \{0\}$ then f is 1-1.

If $K = F$, then $f(a) = 0 \ \forall \ a \in F$.

Field of quotients of an integral domains

If D is an integral domain, the non-zero elements in D may or may not have multiplicative inverses. for eg in Z all the non-zero elements except 1 & -1 don't have multiplicative inverses. w.k.t., an integral domain in which every non-zero element has a multiplicative inverse is a field. In this section we construct a field F which contain the given integral domain D. The field will be the smallest field containing D. For eg, Z is contained in the field Q and all the elements of Q can be expressed as quotients of integers. The construction of the quotient field of an integral domain is motivated at every step by the well known behaviour of the field of rational numbers.

We note that every element of Q can be expressed as a quotient p/q where $p, q \in Z$ & $q \neq 0$. Further the 2 fractions $2/3$ & $4/6$ represent the same rational number iff $ad = bc$. Also $(a/b) + (c/d) = (ad+bc)/bd$ and $(a/b)(c/d) = ac/bd$. The elements of Z can be thought of as fractions of the form $a/1$.

The construction of the field of quotients F of an integral domain D is carried out in the following four stages:

Specify the elements of F.

Define (+) and (×) in F.

S.t., F is a field under these operations.

D can be embedded in F.

Stage(i):

Let D be an integral domain.

Let $S = \{(a,b) / a,b \in D \text{ and } b \neq 0\}$.

We are going to think of the ordered pair(a,b) as one representing a formal quotient a/b. for eg, if D=Z, the pair (1,2) will eventually represent the fraction 1/2.

Definition:

Two elements (a,b) and (c,d) ∈ S are defined to be equivalent : iff ad=bc. If (a,b) is equivalent to (c,d) - we write (a,b) ~ (c,d).

Lemma 1:

$\sim$ is an equivalence relation in S.

Proof:

Let $(a,b) \in S$.

$(a,b) \sim (a,b)$ $\because ab = ba = ab$.

Hence $\sim$ is reflexive.

Now, $(a,b) \sim (c,d) \Rightarrow ad = bc$.

$\Rightarrow cb = da$

$\Rightarrow (c,d) \sim (a,b)$.

Hence $\sim$ is Symmetric.

Now, Let $(a,b) \sim (c,d)$ and $(c,d) \sim (e,f)$.

Now to P.T., $(a,b) \sim (e,b)$ we must Prove that $af = be$.

Case(i): Let $c = 0$. Now, $ad = bc$ & $cf = de$.

$\therefore, ad = 0$ & $de = 0$.

But $d \neq 0$. Hence $a = 0$ & $e = 0$.

$\therefore, af = be = 0$.

Case(ii): Let $c \neq 0$.

we have $ad = bc$ and $cf = de$.

$\therefore, adcf = bcde$.

$\therefore, af = be$ (by Cancellation law).

$\therefore, \sim$ is transitive.

Here $\sim$ is an equivalence relation on S.

Consider the equivalence relation class containing (a,b).

Let it be denoted by $\frac{a}{b}$.

Let $F = \{\frac{a}{b} | (a,b) \in S\}$.

Step (ii)

Let $\frac{a}{b}, \frac{c}{d} \in F$. We now define

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \text{ and } \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

$\because$ D is an integral domain and $b, d \neq 0$, we have $bd \neq 0$.

$\therefore \frac{ad+bc}{bd}$ and $\frac{ac}{bd} \in F$.

Lemma 2:

Addition and multiplication defined above are well defined.

Proof:

Let $(a_1, b_1) \in \frac{a}{b}$ and $(c_1, d_1) \in \frac{c}{d}$.

$\therefore a_1 b = b_1 a$ & $c_1 d = d_1 c$ $\longrightarrow$ (1)

$\therefore a_1 b d d_1 = b_1 a d d_1$ and $c_1 d b b_1 = d_1 c b b_1$

$\therefore (a_1 d_1 + b_1 c_1) bd = (ad + bc) b_1 d_1$

$\therefore \frac{ad+bc}{bd} = \frac{a_1 d_1 + b_1 c_1}{b_1 d_1}$

$\therefore \frac{a}{b} + \frac{c}{d} = \frac{a_1}{b_1} + \frac{c_1}{d_1}$.

Addition is well defined.

Also from (1), $a_1 b c_1 d = b_1 a d_1 c$.

$\therefore (ac, bd) \sim (a_1 c_1, b_1 d_1)$.

$\therefore \frac{a}{b} \cdot \frac{c}{d} = \frac{a_1}{b_1} \cdot \frac{c_1}{d_1}$.

$\therefore$ Multiplication is well defined.

Lemma 3:

stage (iii):

F is a field with the addition and multiplication defined above.

Proof:-

It can easily be verified that addition is commutative and associative.

$\frac{0}{1}$ is the zero of F and $\frac{-a}{b}$ is the additive inverse of $\frac{a}{b}$.

$\therefore (F, +)$ is an abelian group.

Clearly Multiplication is commutative and

associative. $\frac{1}{1}$ is the identity of F.

If $\frac{a}{b}$ is a non-zero element of F, then $a \neq 0$.

$\therefore \frac{b}{a} \in F$ and the inverse of a/b.

Now, $\frac{a}{b}\left(\frac{c}{d}+\frac{e}{f}\right) = \frac{a}{b}\left(\frac{cf+de}{df}\right)$

$$= \frac{acf+ade}{bdf}$$

$$= \frac{acfb+adeb}{bdfb}$$

$$= \frac{ac}{bd} + \frac{ae}{bf}$$

$$= \frac{a}{b}\frac{c}{d} + \frac{a}{b}\frac{e}{f}.$$

$\therefore$ F is a field.

Stage (iv):

The field F contains a subring R which is isomorphism of D onto $f(D)$.

Lemma 4:

The map $f: D \to F$ given by $f(a) = a/1$ is an isomorphism of D onto $f(D)$.

Proof:

Let $a, b \in D$.

Then $f(a+b) = \frac{a+b}{1}$

$= \frac{a}{1} + \frac{b}{1}$

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

and $f(ab) = \frac{ab}{1}$

$= \frac{a}{1} \cdot \frac{b}{1}$

$= f(a) \cdot f(b)$.

Also f is 1-1. For, $f(a) = f(b)$

$\Rightarrow \frac{a}{1} = \frac{b}{1}$

$\Rightarrow (a,1) \sim (b,1)$

$\Rightarrow a1 = 1b$

$\Rightarrow a = b$.

$\therefore f$ is an isomorphism.

Thus we have Proved the following.

Theorem 5.6:

Any integral domain D can be embedded to a field F and every element of F can be expressed as a quotient of two elements of D.

The field F which we have constructed above is called the field of quotients of D.

Theorem 5.7:

The field of quotients F of an integral domain D is the smallest field containing D. (i.e.) If F' is any other field containing D then F' contains a subfield isomorphic to F.

Let $a, b \in D$ & $b \neq 0$.

Then $a, b \in F'$ and since F' is a field $ab^{-1} \in F'$.

Now, let F be the quotient field of D.

~~we define: for, let $(a|b) = ab^{-1}$.~~

we define $f: F \to F'$ by $f(a|b) = ab^{-1}$.

f is well defined: for, let $(a_1, b_1) \sim (a, b)$.

Then $a_1 b = b_1 a$. Hence $a_1 b_1^{-1} = ab^{-1}$.

f is 1-1.

$\because f(a|b) = f(c|d) \Rightarrow ab^{-1} = cd^{-1}$

$f(a/b) = f(c/d) \Rightarrow ad = bc$

$\Rightarrow (a/b) = c/d.$

Now, let $a/b, c/d \in F$.

Then $f[(a/b)+(c/d)] = f[(ad+bc)/bd]$

$= (ad+bc)(bd)^{-1}$

$= (ad+bc)d^{-1}b^{-1}$

$= ab^{-1} + cd^{-1}$

$= f(a/b) + f(c/d).$

Also, $f[(a/b)(c/d)] = f[(ac)/(bd)]$

$= (ac)(bd)^{-1}$

$= acd^{-1}b^{-1}$

$= ab^{-1}.cd^{-1}$

$= f(a/b)\, f(c/d)$

Thus F is isomorphically embedded in F'.

Problem 01:

Describe the quotient field of an integral domain $D = \{a+b\sqrt{2} \mid a, b \in Z\}$.

The set of real numbers R is a field containing the given integral domain D.

Hence R contains a subfield isomorphic to the field of quotiens of D.

This subfield is Precisely of all real numbers of the form $(a+b\sqrt{2}) / (c+d\sqrt{2})$ where $c+d\sqrt{2} \neq 0$.

$(a+b\sqrt{2}) / (c+d\sqrt{2})$ is of the form $p+q\sqrt{2}$ where p & q are rational numbers. Thus the quotient field of D is $\{p+q\sqrt{2} \mid p, q \in Q\}$.

Problem 02:

If D & D' are isomorphic integral domains then their quotient fields are also isomorphic.

Let $f: D \to D'$ is an isomorphism. Let F & F' be the quotient fields of D & D' respectively. Consider $\phi: F \to F'$ given by $\phi(a/b) = f(a)/f(b)$. ϕ is an isomorphism of F onto F' (verify).

Unique Factorization Domain

[U.F.D.]

Defn:

Let $a, b \in R$ and $a \neq 0$. We say that a divides b and write $a|b$ if there exists an element $c \in R$ such that $b = ac$. If $a|b$ we say that a is a divisor or a factor of b.

Examples:

1, In $\mathbb{Z}$, $2|6$, since $6 = 2 \times 3$. However in $2\mathbb{Z}$, 2 doesn't divide 6. since there is no element $c \in 2\mathbb{Z}$. such that $6 = 2c$.

2, In $\mathbb{Z}_5$, $2|3$ since $3 = 2 \cdot 4$.

3, Let R be commutative ring with identity. Let u be a unit in R. Then u divides any element a of R.

For, since u is a unit, u^{-1} exists and

$u^{-1}u = uu^{-1} = 1$.

$\therefore, a = 1a = (uu^{-1})a = u(u^{-1}a) = uc$.

where $c = u^{-1}a \in R$. $\therefore, u|a$.

4, In a field F every non-zero element is a unit and hence every non-zero element divides every element of F.

Defn1:-

Let R be a commutative ring. let a, b be two non-zero elements of R. Then a and b are said to be associates if $a|b$ and $b|a$.

eg:

1, In Z, for any non-zero integer a, a and $-a$ are associates. In general in any commutative ring R with identity, for any non-zero element of R, a and $-a$ are associates.

2, In $2\mathbb{Z}$, 2 doesn't divide 2. Hence 2 isn't an associate of 2.

3, In Z_8, 2 & 6 are associates.

· For, $2 = 6 \cdot 3$ and hence $6|2$,

Also, $6 = 2 \cdot 3$ & hence $2|6$.

Theorem 5.8:-

Let R be an integral domain. Let a & b be two non-zero element of R. Then a & b are associates iff $a = bu$ where u is a unit in R.

Let a and b be associates. Then $a|b$ & $b|a$. Hence there exist element $c, d \in R$ such that $b = ac$ & $a = bd$.

$\therefore a = bd = (ac)d = a(cd)$.

Now, since R is an integral domain cancellation law is valid in R.

$\therefore 1 = cd$ & hence c & d are units

$\therefore a = bd$ where d is a unit.

Conversely, let $a = bu$ where u is a unit in R.

Then $b|a$.

Also, $au^{-1} = b$ ($\because$ u is a unit)

$\therefore a|b$ & hence a and b are associates.

Defn/:

Let R be a commutative ring with identity. Let $a \in R$ & $a \neq 0$. a is called Prime or an irreducible element if a isn't a unit & it's only divisors are units in R and associates of a.

UFD:

An integral domain R is said to be a unique factorization domain (U.F.D) if

(i) any non-zero element in R which isn't a unit can be expressed as the Product of a finite number of Prime elements.

(ii) The factorization in (i) is unique up to the other Order and associates of the Prime elements.

(a) If $a = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$ where the p_i's & q_j's are Prime elements, then $r = s$ and each p_i is an associate of some q_j.

for eg Z is a U.F.D.

GCD

Let R be a U.F.D. Let $a, b \in R$. Then an element $d \in R$ is said to be greatest common divisor (g.c.d) of a & b if

(i) $d|a$ & $d|b$
(ii) $c|a$ & $c|b \Rightarrow c|d$.

The g.c.d of a & b is denoted by (a, b).

Euclidean domain

Let R be a Commutative ring without zero-divisors. R is called the Euclidean domain or an Euclidean ring if for every non-zero element $a \in R$. There is defined as the non-negative integer $d(a)$ satisfying the following conditions

(i) For any two non-zero elements $a, b \in R$, $d(a) \leq d(ab)$.

(ii) For any two non-zero elements $a, b \in R$, there exist $q, r \in R$ such that $a = qb + r$ where either $r = 0$ or $d(r) < d(b)$.

Examples:

1, Z is an Euclidean domain where $d(a)=|a|$.

$d(ab)=|ab|=|a||b|\geq|a|=d(a)$.

Let a,b be two non-zero element of Z. Let q be the numbers of the quotient and r be the remainder when a is divided by b.

Then $a=qb+r$ and $0\leq r<|b|$.

Hence Z is a Euclidean domain.

2, Any field F is an Euclidean domain where $d(a)=1\ \forall\ a\in F=\{0\}$.

$d(a)=d(ab)=1\ \forall\ a\in F-\{0\}$.

Hence $d(a)\leq d(ab)$.

Also, $a=(ab^{-1})b+0$ so that $q=ab^{-1}$ and $r=0$.

∴, Condition (ii) is satisfied. Hence F is an Euclidean domain.

3, The ring of Gaussian integers $R=\{a+bi/a,b\in z\}$ is an Euclidean domain where we define $d(a+ib)=a^2+b^2$.

Let $x=a+ib$ and $y=c+id$ be two non-zero elements in R. Then

$$d(xy) = d[(a+ib)(c+id)]$$

$$= d[(ac-bd)+i(ad+bc)]$$

$$= (ac-bd)^2 + (ad+bc)^2$$

$$= (a^2+b^2)(c^2+d^2)$$

$$\geq a^2+b^2$$

$$= d(x)$$

$$\therefore d(xy) \geq d(x)$$

Now to Prove condition (ii), let

$$\frac{a+bi}{c+di} = p+iq.$$

Then $p = \frac{ac+bd}{c^2+d^2}$ and $q = \frac{bc-ad}{c^2+d^2}$ and hence $p, q \in Q$

Now, let $m, n \in z$ be such that $|p-m| \leq \frac{1}{2}$ and $|q-n| \leq \frac{1}{2}$.

Let $p-m = \alpha$ and $q-n = \beta$ so that $|\alpha| \leq \frac{1}{2}$ and $|\beta| \leq \frac{1}{2}$.

Now,

$$a+bi = (c+di)(p+qi)$$

$$= (c+di)[(\alpha+m)+(\beta+n)i]$$

$$= (c+di)(m+ni)+r$$

where $r = [(c+di)(\alpha+\beta i)]$

Now,

$a+bi, c+di, m+ni \in R$ and hence $r \in R$.

If $r \neq 0$, then

$$d(r) = (c^2+d^2)(\alpha^2+\beta^2)$$
$$\leq (c^2+d^2)\left(\tfrac{1}{4}+\tfrac{1}{4}\right)$$
$$< c^2+d^2$$
$$= d(y)$$

$\therefore d(r) < d(y)$.

$\therefore R$ is an Euclidean domain.

Theorem 59:

Let R be an Euclidean domain and I be an ideal of R. Then there exists an element $a \in I$ such that $I = aR$. (ie) Every ideal of an euclidean domain is a Principal ideal.

If $I = \{0\}$, then we take $a = 0$. Hence we assume that $I \neq \{0\}$.

Let $a \in I$ be non-zero element such that $d(a)$ is minimum. ($\because$ d take non-(-ve) values)

w.c.t., $I = aR$.

Let $x \in I$. Then there exist $q, r \in R$ such that $x = qa + r$ where $r = 0$ or $d(r) < d(a)$.

$\therefore$ Now, $a \in I \Rightarrow qa \in I$ ($\because$ I is an ideal).

Also $x \in J$. Hence $r = x - qa \in I$.

Now, we suppose $r \neq 0$. Then $d(r) < d(a)$.

$\therefore$ r is an element of I such that $d(r) < d(a)$ which is contradiction to the choice of a and hence $r = 0$.

$\therefore$ $x = qa$ and hence $I = aR$.

Theorem 5.10:

Any Euclidean domain R has an identity element.

$\therefore$ R is an ideal of R, there exist $c \in R$ such that $R = cR$.

$\therefore$ Every element of R is a multiple of c.

In particular $c = ec$ for some $e \in R$.

Now, let $x \in R$. Then $x = cy$ for some $y \in R$.

$\therefore$ $ex = e(cy) = (ec)y = cy = x$.

$\therefore$ e is the required identity element.

Theorem 5.11:

Any Euclidean domain R is a Principal ideal domain

By defn of Euclidean domain R is a Commutative ring without zero-divisors. we known that R has an identity element. Hence R is an integral domain. Also every ideal of R is a Principal ideal. Hence R is a Principal ideal domain

Theorem 3.12:

Let R be an Euclidean domain. Let a and b be two non-zero elements of R. Then

b is not a unit in R $\Rightarrow d(a) < d(ab)$.

b is unit in R $\Rightarrow d(a) = d(ab)$.

1) Suppose b isn't a unit in R.

By definition of Euclidean domain there exist elements $q, r \in R$ such that

$a = q(ab) + r \longrightarrow (1)$

where either $r = 0$ or $d(r) < d(ab)$

Now, suppose $r = 0$ then $a = q(ab)$.

$\therefore a - q(ab) = 0$.

$a(1 - qb) = 0$.

Now, R has a no-zero-divisors and $a \neq 0$.

$\therefore 1 - qb = 0$. Hence $qb = 1$.

$\therefore$ b is a unit in R which is a contradiction.

$\therefore r \neq 0$. Hence $d(r) < d(ab) \longrightarrow (2)$

Now, $r = a(1 - qb)$ (by 1)

$\therefore d(r) = d[a(1 - bq)] \geq d(a) \longrightarrow (3)$

$\therefore d(a) \leq d(r) < d(ab)$ (by (2) & (3))

$\therefore d(a) < d(ab)$.

(ii) Suppose b is a unit in R.

Now, $d(a) \leq d(ab)$.

Also $d(a) = d[(ab)b^{-1}] \geq d(ab)$

$\therefore, d(a) \geq d(ab)$.

$\therefore, d(a) = d(ab)$.

Theorem 5.13:

Let a be a non-zero element of an Euclidean domain R. Then a is a unit in R iff $d(a) = d(1)$.

Suppose a is a unit in R.

$\therefore, d(a) = d(aa^{-1})$

$= d(1)$.

Conversely, let $d(a) = d(1)$.

Suppose a is not an unit in R.

Then $d(1) > d(1)$

$\therefore, d(a) > d(1)$ which is contradiction.

$\therefore, a$ is a unit.

Theorem 5.14:

Let a be a non-zero element of an Euclidean domain R. If $d(a)=0$, then a is a unit in R.

Suppose a isn't a unit in R.

Then $d(1)<d(1a)$

$\therefore, d(1)<d(a)=0$. Hence $d(1)<0$ which is a contradiction.

$\therefore$ d takes only a non-negative values.

Theorem 5.15:

Let R be an Euclidean domain. Then any two elements, $a, b \in R$ have a g.c.d and it's of the form $ax+by$ where $x, y \in R$.

Let $A=\{ax+by \mid x, y \in R\}$.

w.c.t., A is an ideal of R,

let $u, v \in A$. Then $u=ax_1+by_1$ and $v=ax_2+by_2$.

$\therefore, u-v=a(x_1-x_2)+b(y_1-y_2) \in A$

Now, let $c \in R$. Then

$uc=(ax_1+by_1)c$

$=a(x_1c)+b(y_1c) \in A$

$\therefore, A$ is an ideal of R.

Now, since R is an Euclidean domain it's a Principal ideal domain. Hence A is a Pricipal

ideal of R.

Now, let $d \in A$ be such that $A = (d)$.

$\therefore$, $d = ra + sb$ where $r, s \in R$.

Now, $a = 1a + 0b \in A$ and $b = 0a + 1b \in A$.

$\therefore$, $a = da_1$ and $b = db_1$ for some $a_1, b_1 \in R$.

$\therefore$, $d \mid a$ & $d \mid b$.

Now, Suppose $l \in R$ and $l \mid a$ and $l \mid b$.

Then $l \mid (ra + sb)$ so that $l \mid d$.

$\therefore$, d is the required g.c.d of a & b.

Defn1:

Two elements a & b of an Euclidean domain R are said to be relatively prime if their g.c.d is a unit in R.

Theorem 5.16

Let R be an Euclidean domain. Let $a, b, c \in R$.

Then $a \mid bc$ and $(a,b) = 1 \Rightarrow a \mid c$.

$\because$, $(a,b) = 1$, there exist $x, y \in R$ such that $ax + by = 1$.

$\therefore$, $acx + bcy = c$.

Now, $a \mid acx$. Also, $a \mid bx \Rightarrow a \mid bcy$.

$\therefore$, $a \mid (acx + bcy)$. Hence $a \mid c$.

Theorem 5.17

Let p be a Prime element in an Euclidean domain R. Let $a, b \in R$.

Then $p \mid ab \Rightarrow p \mid a$ or $p \mid b$.

Let P be a Prime element in Euclidean domain R. Let $a_1, a_2, \ldots, a_n \in R$.

Then $P \mid a_1 a_2 \ldots a_n \Rightarrow P$ divides at least one a_i.

Theorem 5.18:

Any Euclidean domain R is a U.F.D

First we shall P.t., any element a in R is either a unit or can be expressed as the Product of a finite number of Prime elements of R.

We Prove this by induction on $d(a)$.

If $d(a) = d(1)$ then a is a unit in R.

Hence by assertion is true. Now, we assume that the result is true for all $x \in R$ such that $d(x) < d(a)$ and Prove that the result is true for a.

If a is a Prime there is nothing to Prove.

If not, $a = bc$ where neither b or c is a unit in R.

$\therefore d(b) < d(a)$ and $d(c) < d(a)$.

Now, by induction hypothesis b and c is a unit in R. $\therefore d(b) \geq d(a)$ and $d(c) \geq d$

written as the Product of a finite number Prime elements.

Hence a can be expressed as a Product of a finite number of prime elements.

We now Prove the uniqueness:

Let $a = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$ where p_is and q_is are Prime elements of R.

$\therefore, p_1 | q_1 q_2 \dots q_s$.

$p_1 | q_i$ for some i. Without loss of generality we assume that $p_1 | q_1$. Since p_1 and q_1 are both Prime elements of R. p_1 & q_1 must be associates.

$\therefore, q_1 = u_1 p_1$ where u_1 is a unit in R.

$\therefore, p_1 p_2 \dots p_r = u_1 p_1 q_2 q_3 \dots q_s$.

$\therefore, p_2 p_3 \dots p_r = u_1 q_2 q_3 \dots q_s$.

Now, if $r < s$, repeating the above argument r times the left side becomes 1 and the right side contains a Product of some Prime elements which is impossible.

Hence $r \geq s$.

Similarly $s \geq r$ and hence $r = s$.

Further we have shown that every p_i is an associate of some q_j and conversely. Hence the theorem.

Example 01:

St $1+i$ is a Prime element in the ring R of Gaussian integers.

Suppose $(a+bi) \mid (1+i)$.

Then there exist an element $c+id \in R$ such that $(a+bi)(c+di) = 1+i$.

$\therefore, d[(a+bi)(c+di)] = d(1+i)$.

$\therefore (a^2+b^2)(c^2+d^2) = 2$ and $a, b, c, d \in Z$.

$\therefore, a^2+b^2 = 1$ or $c^2+d^2 = 1$

$\therefore, d(a+ib) = d(1)$ or $d(c+id) = d(1)$.

$\therefore,$ Either $a+ib$ or $c+id$ is a unit in R.

Hence $1+i$ is a Prime element of R.

Example 02:

Prove that 5 isn't prime element in the ring R of Gaussian integers.

$5 = (2+i)(2-i)$

and $d(2+i) = d(2-i) = 5 > d(i)$

Hence neither $2+i$ nor $2-i$ is a unit in R.

Hence 5 is not a Prime element of R.

Example 03:

Find the g.c.d of $16+7i$ and $10-5i$ in the ring R of Gaussian integers

Let $a = 16+7i$ and $b = 10-5i$

$$\therefore \frac{a}{b} = \frac{16+7i}{10-5i}$$

$$= \frac{(16+7i)(10+5i)}{(10-5i)(10+5i)}$$

$$= 1 + \frac{6i}{5} = 1 + i + i/5$$

$$\therefore a = (1+i)b + (1+2i)$$

Let $q_1 = 1+i$ and $r_1 = 1+2i$.

Now, $b/r_1 = \frac{10-5i}{1+2i} = 4-3i$

$$\therefore b = (4-3i)(1+2i) + 0$$

Hence g.c.d of a and b is $r_1 = 1+2i$.