Nalanda Open University

M.sc (Mathematics)

Part-I

Paper I (Advanced Abstract Algebra)

UNIT II

EUCLIDEAN AND FACTORIZATION DOMAIN

CONTENTS—

From:-

Dr. L .K .SHARAN

Rtd. Professor & Head, Deptt. Of mathematics

V.K.S. University, ARA.

Mobile:- 9835228272

Email Id – lalitsharan9@gmail.com

Ring: - A system (R, +, .) containing a set R and two binary operations called addition and multiplication is said to be a ring if this system satisfies the following conditions :-

(1) (R, +) is an abelian group.

(2) (a.b) .c = a.(b.c) $\forall$ a, b, c $\in$ R

That is associative law is satisfied w.r.t multiplication

(3) (i) a. (b + c) = a.b + a.c $\forall$ a, b, c $\in$ R

(ii) (b+c) . a = b.a + c.a $\forall$ a, b, c $\in$ R

Note 1:- Since we have taken two binary operations ' + ' and ' . 'so closure property are naturally satisfied w.r.t both of the binary operations.

Note 2:- If there is no chance of confusion then in place of writing (R, +, .) we shall write simply R to mean a ring.

Commutative Ring-- ring R is said to be commutative

if a . b = b. a , $\forall$ a, b $\in$ R .

Ring with unity: - A ring R is said to be with unity if $\exists$ an element 1 in R such that

1 . a = a . 1 = a for every a $\in$ R.

A Commutative Ring with unity: - It means a ring R which is commutative and has a unity.

Inversible element or a unit: - An element a in a ring R is called inversible (or a unit) if $\exists$ an element b $\in$ R such that a.b = b.a = 1. In this situation we write b = a^{-1} and we speak that b is the multiplicative inverse of a.

Division Ring: - A ring R with unity is called a division ring if non zero elements of R form a group w.r.t multiplication clearly if non zero elements of R must have multiplicative inverse.

Some examples of Ring:-

(1) The set of integers w.r.t usual ‘ + ‘ and ‘ . ‘ is a commutative ring with unity

(2) The set of even integers is a commutative ring without unit element w.r.t ordinary ‘ + ‘ and ‘ **.**’

(3) The set of all real valued functions defined over the closed interval [0 ,1] forms a ring

w.r.t ‘+ and ‘ **.** ‘ defined as follows:-

$(f+g)(x)=f(x)+g(x)$

$(f.g)(x)=f(g(x))$.

(4) The set M of all 2×2 square matrices whose elements are real numbers a ring w.r.t addition and multiplication of matrices.

Zero –Divisor:- Let R be a commutative ring A non zero element a of R is called a zero divisor if we have another non zero element b in R such that ab = 0.

Proper Divisors of Zero :- If a.b =0 and a≠0 , b≠0 for a, b Є R then, a is called proper left zero divisor and b is called proper right zero divisor if we take them together they are said to be proper divisors of zero.

Integral Domain: - A commutative ring R with unity is called an integral domain if R has no zero divisors.

That is if ab = 0 in R then either a=0 or b=0.

That is the product of non zero elements in R is non zero.

Example 1:- The ring of integers is an integral domain w.r.t ‘ + ‘ and ‘ **.** ‘ .
Example 2:- The set E of all even integers with 0 is a commutative ring w.r.t usual ‘ + ‘ and ‘ **.** ‘ . But it is not an integral domain as 1 ∉ E for multiplication.

Example 3:- The ring I/(6) of residue class modulo 6 is a commutative ring with unity but it is not integral domain

Left Ideal: - A non empty subset I of a ring is called a left ideal of R if

(i) a, b Є I => a - b Є I

(ii) a Є I, r Є R => ra Є I

Right Ideal: - A non empty subset I of R is called a right ideal of R if

(i) a, b $\in$ I => a - b $\in$ I

(ii) a $\in$ I, r $\in$ R => ar $\in$ I

Ideal: - A subset I of a ring R is called simply ideal if it is both left and right ideals.

Maximal Ideal:- Let M be an ideal of a ring R such that M $\neq$ R, then M is called

Maximal ideal of R if whenever A is an ideal of R such that M $\subseteq$ A $\subseteq$ R then either

A = M or A = R.

NOTE: - A ring may have more than one maximal ideal.

Prime Ideal: - An ideal P of a ring R is called a Prime Ideal if

ab $\in$ P => a $\in$ P or b $\in$ P .

EXAMPLE 1: {o} in the ring Z of integers is a prime ideal as ab $\in${o}

=> ab = o => a = 0 or b = 0 => a $\in$ {0} or b $\in$ {0} .

EXAMPLE 2: H_4 = { 4n : n $\in$ Z, Z is the set of integers } then H_4 is a maximal ideal but not a prime ideal .

Observation: Let (E, +, .) be a ring of even integers.

By question H_4 = { 4n : n is an integer}.

Then H_4 is an ideal of E and as 2 $\notin$ H_4, $H_4 \neq$ E.

Let A be any ideal of E such that $H_4 \subseteq A \subseteq E$.

Sufficient to show that, A = H_4 or A = E.

If $H_4 \neq A$, we have A = E

Since $H_4 \subset A$, $\exists$ some x $\in$ A such that x $\notin$ H_4

By division algorithm, we can write that x = 4 q + r where 0 < r < 4.

Then clearly r $\neq$ 0 otherwise x = 4 q => x $\in$ H_4 which goes against assumption.

Now r = 1, 3 => x is odd => x does not belongs to E =><=

So r must be equal to 2

Thus x = 4 q + 2 => 2 = x - 4 q $\in$ A

Thus as x $\in$ A, 4 q $\in$ $H_4 \subseteq$ A => x- 4 q $\in$ A.

$2 \in A \Rightarrow$ multiples of 2 are in A (by the definition of ideal)

$\Rightarrow E \subseteq A$. But $A \subseteq E$. Hence $A = E$

Thus $H_4 = \{ 4n : n \text{ is an integer}\}$ is a maximal ideal in E.

However H_4 is not prime ideal as $2 \times 2 = 4 \in H_4$ but $2 \notin H_4$

Thus H_4 is maximal ideal but not a prime ideal

Principal Ideal: - An ideal M of a ring R is said to be principal ideal if it is generated by a single element of S. That is, if $a \in S$ then $S = \{a\}$.

NOTE 1 :- A ring R with unity is itself called the unit ideal because the ideal generated by 1 i.e, {1} is the ring R itself as $r. 1 = r, \forall r \in R$.

NOTE 2 :- The ideal generated by the zero element of R i.e, {0} is called null ideal.

Divisibility in an integral Domain: - Let a be a non zero element of a commutative ring R.

Then a divides $b \in R$, $\exists$ an element $c \in R$ such that $b = ca$.

We generally use the symbols a/b to represent the fact that " a divides b ". Here a is called a factor of b.

Clearly every non zero element of R is a divisor of its zero element.

Theorem 1:- If R is a commutative ring, then

(i) a/b and b/c => a/c

(ii) a/b and a/c => a/(b+c)

(iii) a/b => a/b x, $\forall x \in R$.

(iv) if R has unity then $1/x \ \forall x \in R$ and if a is a unit then $a / x \ \forall x \in R$.

Proof:-

(i) a/b => b = a m, for some $m \in R$

and b/c => c = b n, for some $n \in R$

Thus c = b n = (a m) n = a (m n)

=> a/c as m, $n \in R$ => m n $\in R$.

(ii) a/b => b = a m, for m Є R and

a/c => c = a n, for n Є R

Thus b + c = a m + a n = a (m+n)

=> a/(b+c) as m, n Є R => (m+n) Є R

(iii) a/b => b = a n, for some n Є R

=> b x = a n x, for all n Є R

=> a/b x,∀ n x Є R.

(iv) it can be easily verified.

Greatest common divisor or H.C.F:- Let R be a commutative ring and a, b Є R. Then an element d Є R is called greatest common divisor (G.C.D.) or highest common factor (H.C.F.) of a and b if

(i) d/a and d/b

(ii) whenever c/a, c/b then c/d

In this case we write d = g.c.d (a, b). It is also denoted by (a.b)

Least common multiple or L.C.M:- Let R be a commutative ring. A non zero Element l Є R is called least common multiple (L.C.M) of two non zero elements a, b Є R. if

(i) a/l and b/l

(ii) if a/x, b/x then l/x

We denote l by l.c.m (a, b) = [a, b].

Associates: - Let R be a commutative ring with unity. Then any two elements a, b Є R are called associates if b = ua for some unit u Є R. In this case we also write a~ b.

Principal ideal Domain:- An integral domain R with unity is called a principal ideal domain (P.I.D) if every ideal of R is a principal ideal.

Principal ideal ring :- A commutative ring with unity is called a principal ideal ring if every ideal of R is a principal ideal.

Prime element :- Let R be a commutative ring with unity an element p Є R is called prime element if:

(i) $p \neq 0$, p is not a unit

(ii) for any a, b, c Є R if p | ab then p|a and p|b

Irreducible element :- An element p of a commutative ring R with unity is called an irreducible element if

(i) $p \neq 0$, p is not a unit

(ii) whenever p = ab, then one of a and b must be a unit .

Theorem 2:- Let

(i) R be an integral domain (I. D)
(ii) a, b Є R be non zero elements

Then a/b and b/a iff a and b are associates.

Proof:- By question, R is an integral domain with unity and a, b Є R , a, b are non zero.

Suppose a/b and b/a

Since a/b => b = x a, for some x Є R

b/a => a = y b for some y Є R

Thus b = x a = x (y b) => b – x (y b) = 0 => b (1 – x y) = 0 => 1 – x y = 0 => x y = 1

=> y is a unit in R and a = y b.

Conversely let a, b are associates :

As we know that ∃ a unit u such that a = b u => b/a and a/b.

Theorem3:- Let R be an integral domain (I. D) with unity then

d_1 = g.c.d (a,b) in R then d_2 is also a g.c.d (a,b) iff $d_1 = d_2$ are associates.

Proof:- Let d_1, d_2 both are g.c.d (a,b)

Then as we know that, we can write d_1/a , d_1/b and d_2/a , d_2/b.

So by definition we get d_1/d_2 from which d_1 and d_2 are associates.

Conversely : let d_1 = g.c.d (a,b) and d_2 be an associates of d_1

then u $d_2 = d_1$, for some unit u.

=> d_2/d_1 and as d_1/a , d_1/b, we find d_2/a , d_2/b.

Let x/a , x/b then x/ d_1 as d_1 is g.c.d (a,b).

Also as $d_2 = d_1 u^{-1}$ so $d_1/d_2 \Rightarrow x/ d_2$.

Thus d_2 = g.c.d (a,b).

Theorem4:- In an integral domain if there exists a lowest common multiple (L.C.M) of any two elements, then it is unique apart from the distinction between the associates.

Proof:- Let a, b be any two non zero elements of an integral domain D.

Also let L.C.M of a and b exist.

if possible let for a moment that l_1 and l_2 are two L.C.M of a and b then

We see that: if l_1 is the L.C.M of a and b then we have a/ l_1 and b/ l_1

Similarly if l_2 is the L.C.M of a and b then we have a/ l_2 and b/ l_2

but then l_1/l_2 and Similarly l_2/l_1

Thus l_1/l_2 and l_2/l_1 => that l_1 and l_2 are associates.

Theorem 5:- Each pair of elements surely has a least common multiple in a principal ideal domain.

Proof:- Let a, b be any two non zero elements of a principal ideal domain (P.I. D.) D.

Also let (a) and (b) stand for principal ideal of D generated by a and b respectively.

Clearly (a) $\cap$ (b) is an ideal of D [since intersection of two ideals is again an ideal]

Also (a) $\cap$ (b) is principal ideal but then there will exist an element l in D

such that (a) $\cap$ (b) = (l).

It remains to show that l is the L.C.M.

For, since (a) $\cap$ (b) = (l) => (l) $\subset$ (a) and (l) $\subset$ (b)

=> l $\in$ (a) and l $\in$ (b) => l = a x_1 and l = b x_2 for some x_1, $x_2 \in$ D.

=> a/l and b/l

=> l is a common multiple of a and b

Now if m is a common multiple of a and b, then a/m and b/m.

Thus m = a y_1 and m = b y_2, for some y_1, $y_2 \in$ D.

Now x $\in$ (m) => x = m z_1, for some $z_1 \in$ D

=> $x = (a\ y_1)\ z_1$ => $x = a(y_1, z_1)$, $y_1, z_1 \in D$ => $x \in (a)$

That is $x \in (m)$ => $x \in (a)$ => $(m) \subseteq (a)$

In a similar style we can establish that $(m) \subseteq (b)$

=> $(m) \subseteq (a) \cap (b)$

=> $(m) \subseteq (l)$

=> $m \in (l)$ => $m = ly$, for some $y \in D$ => l/m

Thus a/l, b/l and if m/a and m/b, then l/m

Thus l is the least common multiple of a and b.

Theorem 6:- In every principal ideal domain (P.I. D.) each pair of non zero elements surely has a greatest common divisor.

Proof:- Let a, b be any two non zero elements of a principal ideal domain D.

Also let (a) and (b) be principal ideal generated by a and b respectively.

As we know that (a) + (b) is an ideal in D and every ideal of D is principal.

Thus (a) + (b) is principal ideal but then there exists $d \in D$,

Such that (a) + (b) = (d)

Our problem is to establish that d = greatest common divisor (a,b).

For, since (a) + (b) = (d) => $(a) \subset (d)$, $(b) \subset (d)$

Now $(a) \subset (d)$ => $a = d\ x_1$, for some $x_1 \in D$ => d/a

Also $(b) \subset (d)$ => $b = d\ x_2$, for some $x_2 \in D$ => d/b.

So d is the common divisor of a and b.

If possible, let for a moment that c is also a common divisor of a and b.

So that c/a and c/b => $a = c\ y_1$ and $b = c\ y_2$,for some $y_1, y_2 \in D$.

Thus $x \in (a)$ => $x = a\ z_1$ for some $z_1 \in D$.

=> $x = (c\ y_1)\ z_1 = c\ (y_1\ z_1)$, where $y_1\ z_1 \in D$

=> $x \in (c)$ => $(a) \subset (c)$

Similarly it can be shown that (b) $\subset$ (c)

Therefore (a) $\subset$ (c) and (b) $\subset$ (c) => (a) + (b) $\subset$ (c)

=> (d) $\subset$ (c) => d $\in$ (c) => d = c z, for some z $\in$ D => c/d.

Hence d/a and d/b and whenever c/a, c/b then c/d

Therefore d = greatest common divisor (a,b),,

Theorem 7:- In a principal ideal domain (P.I. D.), an element is prime if and only if it is irreducible.

Proof:- Let D be a principal domain. Let p $\in$ D be a prime element

To prove that if p = a b then a or b is a unit.

For, let p = a b then p/ab => p/a or p/b, where p is prime.

If p/a then a = px, for some x. Then p = ab = (px) b => p (1- xb) = 0

But p $\neq$ so 1- xb = 0 => xb = 1 => b is a unit.

Similarly it can be shown that if p/b then 'a' will be a unit

Conversely: let p is irreducible element and p/ab

To show p/a or p/b

if possible let p/a.

Also p and a are members of a P.I. D. So by a theorem they must have a greatest common divisor. Let this G.C.D be d.

To show d is a unit.

For, d/p and d/a => there exists u and v such that p = du, a = dv

If d is not a unit, then as p is irreducible and p = du, u will be a unit.

=> u^{-1} exists => p u^{-1} = d

Thus a = p u^{-1} v => p/a which is a contradiction

Thus d is a unit.

d is g.c.d. so d can be expressed as d = λ a + μ p which gives us

$d\, d^{-1} = d^{-1} \lambda a + d^{-1} \mu p \Rightarrow b \cdot 1 = \lambda d^{-1} a\, b + \mu d^{-1} b\, p$

But p/ab, $p/ \mu d^{-1} bp$.

Therefore, $p/ (ab \lambda d^{-1} + \mu d^{-1} bp) \Rightarrow p/b$. ,,

Euclidean Rings or Euclidean Domain: - Let R be an integral domain then R is called Euclidean ring (or Euclidean Domain) if for every non zero element $a \in R$ there exists a non negative integers d (a) such that :

(i) For all non zero elements $a, b \in R$, $d(a) \leq d(ab)$ [or $d(b) \leq d(ab)$]

(ii) For each $a, b \in R$ with $b \neq 0$, there exists $q , r \in R$ such that
$a = bq + r$ where either $r = 0$ or $d(r) < d(b)$

Note 1 :- The above property (ii) is known as division algorithm.

d is known as Euclidean norm function. We do not assign a value to d (0)

Example of Euclidean Rings:- The ring Z of all integers is an Euclidean ring.

Solution:- Let Z = the set of all integers and

N = set of non-negative integers

We define a mapping $d : z \rightarrow N$ given by $d (a) = | a |$, $\forall\ a \in Z$ and $a \neq 0$.

Since $| a |$ is non-negative as $a \neq 0$.

It means for every non zero integer a, d (a) is non-negative integer of Z.

We now consider :

(i) If a, b are any two non zero elements of I then
$d(a) = |ab| = |a|\, |b| \geq |a|$ (since $|b| \geq a$, $\forall$ non zero $b \in Z$)
$\Rightarrow$ $d (ab) \geq d(a) \Rightarrow d(a) \leq d(ab)\ \forall\ a, b \in Z$.

(ii) If a, b are any two non zero elements of Z, then by algorithm $\exists\ q, r \in Z$ such that $a = bq + r$ where $0 \leq r |b|$,
So that $0 \leq r < |b| \Rightarrow$ either $r = 0$ or $0 < r < |b|$
$\Rightarrow$ either $r = 0$ or $|r| < |b|$ (since $0 < r \Rightarrow |r| = r$)

$\Rightarrow$ either $r = 0$ or $d(r) < d(b)$

So we find that the mapping d is a Euclidean valuation on Z and accordingly Z is a Euclidean ring.

Theorem 8:- Every Euclidean ring is a principal ideal ring.

Proof:- Let R be an Euclidean ring and S be an arbitrary ideal of R.

To show that S is a principal ideal

If S = (0) i.e, S is generated by 0 then S is a principal ideal.

If $S \neq (0)$ then there must exist a non zero element say $b \in S$ i.e, $b \neq 0$

Let d (b) be minimal so we cannot get c in S such that $d(c) < d(b)$

We show that S = (b) that is S is generated by b.

Clearly for any $a \in S \exists$ q and r in R such that

$A = bq + r$ where either $r = 0$ or $d(r) < d(b)$

As S in an ideal so,

$q \in R$ and $b \in S \Rightarrow bq \in S$

Also $q \in R$ and $bq \in S \Rightarrow a - bq \in S \Rightarrow r \in S$

But we have either $r = 0$ or $d(r) < d(b)$ contradict that d (b) is generated by b.

i.e, S = (b) so that S is a principal ideal.

Also S is an arbitrary ideal in R.

Thus R is a principal ideal ring.

Hence a = bq. => that every element of S can we expressed as a multiple of b.

Thus S = (b) => S is a principal ideal.

Hence R is a principal ideal ring.

Theorem 9:- An Euclidean ring possesses a unit element.

Proof:- Let R be an Euclidean ring. But we know that every Euclidean ring is a principal ideal ring.

Clearly R is itself an ideal of R so it is principal ideal.

Let $R = (u_0)$ for $u_0 \in R$.

So every element in R is a multiple of u_0.

In particular $u_0 = u_0\, c$, for some c in R.

Let a be any element of R, then $a = x\, u_0$, for some $x \in R$.

So $ac = (x\, u_0)\, c = x\, (u_0\, c)$. Also R is a commutative ring.

Thus $ac = a = c\, a$, $\forall\ a \in R$.

Thus c is unit element of R.

Theorem 10 :- The necessary and sufficient that the non zero element a in the Euclidean ring R is a unit is that d(a) = d(1).

Proof:- Let R be an Euclidean ring.

Also let a be a non zero element of R and a is a unit then by definition of Euclidean ring.

$d(a) = d(1.\ a) \geq d(1)$ or $d(a) \geq d(1)$ ----------(1)

a is unit in R => a^{-1} exists in R then $1 = a\, a^{-1}$ => $d(1) = d(a\, a^{-1}) \geq d(a)$

⇨ $d(1) \geq d(a)$ ----------(2)

Thus from (1) and (2) d (a) = d (1)

Conversely: let d (a) = d (1). To show a is a unit in R.

If possible, let for a moment that a is not unit in R

Then by a theorem d (1,a) > d (1) => d (a) > d (1) which is a contradiction

$\therefore$ a is unit in R.

Theorem 11 (Unique Factorization theorem) :- Statement let R be a Euclidean ring and $a \neq 0$ a non unit in R. Suppose

$a = p_1\, p_2 \ldots\ldots\ldots\ldots p_m = q_1\, q_2 \ldots\ldots\ldots\ldots q_n$, where each p_i and q_i are prime elements of R then m = n and each p_i $(1 \leq i \leq m)$ is an associate of some q_i $(1 \leq i \leq n)$ and each q_i is an associative of some p_i.

Proof:- Since given $a = p_1\, p_2 \ldots\ldots\ldots\ldots p_m = q_1\, q_2 \ldots\ldots\ldots\ldots q_n$ ----------(1)

Also $p_1 \mid p_1\, p_2 \ldots\ldots\ldots\ldots p_m$ => $p_1 \mid q_1\, q_2 \ldots\ldots\ldots\ldots q_n$ => p_1 must divide at least one of

q_1 , q_2 ,....., q_n (since R is commutative)

By left cancellation law, we have

$P_2\, p_2 \ldots\ldots\ldots\ldots p_m = u_1\, q_2\, q_3 \ldots\ldots\ldots\ldots q_n$ ----------(2)

We repeat the above argument on (2) with p_2 , p_3 and so on

If m < n then after m steps, the left side becomes 1 and

the right side reduces to a product of some units in R and certain

numbers of q_j's. But q_j's are not units in R, so that the product of

some units are some q_j's cannot be equal to 1.

This shows that m < n.

Thus we obtain $m \geq n$ ----------(3)

Now interchanging the role of q_i's and q_j's, we get $n \geq m$ ----------(4)

Thus from (3) and (4) , we obtain m = n.

Clearly the above process shows the fact that every p_i has some p_j as an

associate and conversely.

Theorem 12 : An ideal S of the Euclidean ring R is maximal if and only if

S is generated by some prime element of R.

Proof:- Let a be an element of an Euclidean ring and S = (a) be an ideal generated by a.

Also every Euclidean ring => principal ideal ring .

So S is a principal ideal. Let S is maximal ideal.

We have show that a is a prime element in R .

We claim that a is a prime element.

If not a is a composite number but then a = bc ----------(1)

Where b , c are non zero units in R.

(1) implies that b/a then for some $x \in R$, $ax \in (a)$, then

$ax = (bc)\, x = b\,(x) \in (b)$

Thus $(a) \subset (b) \subset R$ => $S \subset (b) \subset R$ => either S = (b) or S = R (since S is maximal)

When S = (b) then (a) = (b) => $(b) \subseteq (a)$ => $b \in (a)$ => b = ay for some $y \in R$.

- ⇨ $b = (bc)\, y$ => $b = b\,(cy)$ => $b - b\,(cy) = 0$ => $b\,(1 - cy) = 0$ but $b \neq 0$
- ⇨ $1 - cy = 0$ => $cy = 1$ => c is a unit in R which is a contradiction.

Thus supposing that a is not prime we arrived at a contradiction .

However if S = R then (a) = R => $1 \in (a)$ => $1 = az$ for some $z \in R$ => a is a unit in R,

which contradicts the fact that a is not a unit in R.

Thus letting a not to be a prime number we arrived at a contradiction .

Thus our supposition was wrong .

Therefore a is prime element in R .

Conversely : Let S = (a) and a is prime element in R .

To show S is maximal.

For , let T be an ideal of R such that $S \subset T \subset R$.

Since every Euclidean ring is a principal ideal ring so R is principal ideal ring so T is principal ideal.

Let T = (b) , for $b \in R$.

But $S \subset T$ => $(a) \subset (b)$ => a = bx for some $x \in R$.

- ⇨ b is either a unit in R or an associate of a
- ⇨ either (b) = R or (b) = (a)
- ⇨ either T = R or T = S
- ⇨ S is maximal ideal of R.

EXERCISES

Problem 1:- Give an example to show that it is possible to have more than one g.c.d for the same pair of elements.

Solution:- Consider the ring R = { 0 ,1 , 2 ,....., 7 } modulo 8

If there is no chance of confusion then by ordinary sign of multiplication '×' we shall mean a modified form of multiplication on the set of remainders.

Thus $2 \times 3 = 6$ then 2|6

$2 \times 2 = 4$ then 2|4

Again , if c|4 , c|6 than c|6 – 4 =>c|2

Thus g.c.d (4,6) = 2 ----------(1)

Also $6 = 6 \times 1$

$4 = 6 \times 6$

So we find 6|6 and 6|4

Now c|6 , c|4

Then as c|6 , we get g.c.d (4,6) = 6 ----------(2)

Thus from (1) and (2) it is possible to have more than one g.c.d for the same pair of elements.

Problem 2:- Verify whether in the ring E of even integers 4 and 6 have a g.c.d or not ?

Solution : The only possibility that 2 is not a g.c.d of 4, 6 as 2 does not divides 6 in E.

In fact $6 = 2 . 3$ but $3 \notin E$.

Problem 3:- Let R be an integral domain with unity and $a , b \in R$ be non zero elements such that a/b and b/a , then a and b are associates.

Solution : Since $a/b \Rightarrow b = xa$ for some $x, y \in R$

$b/a \Rightarrow a = yb$

Thus $b = xa = x (yb) \Rightarrow b (1 – xy) = 0 \Rightarrow 1-xy = 0$ (as $b \neq 0$)

⇨ y is a unit in R and $a = yb$.

Problem 4:- Construct an example of Euclidean domain.

Solution : We consider the integral domain (Z, +, .) of integers.

For any non zero integer a in Z , we define $d (a) = |a|$ then d (a) is non negative integer.

Again , let $a, b \in Z$ be any two non zero elements ,

Then $d (a) = |a|$, $d (ab) = |ab| = |a| |b|$

$\therefore d (a) \leq d (ab)$ [since $|a| \leq |a| . |b|$]

Again $a, b \in Z$ $(a, b \neq 0)$

Suppose $b > 0$ then it is possible to write $a = tb + r$ where $0 \leq r < b$, $t, r \in Z$

If $r \neq 0$ then $r < b \Rightarrow |r| < |b| \Rightarrow d (r) < d (b)$.

Also if $b < 0$ then $(-b) > 0$ so there exists $t, r \in Z$ such that

$a = (-b) t + r$ where $0 \leq r < -b$

or, $a = (-t)\, b + r$.

If $r \neq 0$, $r < -b \Rightarrow |r| < |b| \Rightarrow d(r) < d(b)$

Thus the system $(Z, +, .)$ is a Euclidean domain.

Problem 5:- Show that in a P.I.D every non zero prime ideal is maximal .

Solution : Let $P = (p)$, $p \neq 0$ be a non zero prime ideal in a P.I.D R.

Let $P \subseteq Q = (q) \subseteq R$ then $p \in P \subseteq Q = (q) \Rightarrow p = qr \Rightarrow q\, r \in P$.

$\Rightarrow$ $q \in P$ or $r \in P$.

If $q \in P$ then all multiples of q are in $P \Rightarrow Q \subseteq P$.

Thus $Q = P$.

If $r \in P$ then $r = pt \Rightarrow r = q\, r\, t \Rightarrow r(1- qt) = 0 \Rightarrow 1 = qt$ $(r \neq 0)$

But $q \in Q$, $t \in R \Rightarrow q\, t \in Q \Rightarrow 1 \in Q \Rightarrow Q = R$.

Problem 6:- Show that an element x in a Euclidean domain is a unit if and only if d(x) =d(1)

Solution : Let $d(x) = d(1)$; to show x is a unit.

Let for a moment x is not a unit then by a theorem $d(1) < d(1.\, x)$

That is $d(1) < d(x)$ which is a contradiction.

Thus x is a unit.

Conversely : Let x is a unit, to prove $d(x) = d(1)$

But x is a unit in R then there exists y in R such that $xy = 1$

Since by definition $d(x) \leq d(xy) \Rightarrow d(x) \leq d(1)$ ----------(1)

Also $d(1) \leq d(1.x) \Rightarrow d(1) \leq d(x)$ ----------(2)

Thus from (1) and (2)

$D(x) = d(1)$

Hence the problem.

Problem 7:- Show by an example that it is possible to find two elements a , b in a Euclidean domain such that $d(a) = d(b)$ but a , b are not associates.

Solution : Consider $D = \{ a + ib: a, b \in Z \}$. Also let $d(a + ib) = a^2 + b^2$

Then D is a Euclidean domain .

Here d (2 + 3i) = 13 = d (2 – 3i) but 2 + 3i and 2 – 3i are not associates.

We note here that units of D are ± 1 , $\pm i$ and thus an associate of 2 + 3i can be

(2 + 3i) 1, (2 + 3i) (-1), (2 + 3i) i, (2 + 3i) (-i)

That is 2 + 3i, -2 -3i, 2i – 3, 3 – 2i,

Which are all different from 2 + 3i.

Problem 8:- Show that whenever a, b are relatively prime in a Euclidean domain R, then g.c.d (a, b) = 1.

Solution : Since by a theorem any associate of a g.c.d is a g.c.d.

Also since 1 is associate of any unit.

So 1 will be an associate of d = g.c.d (a, b) = a unit => 1 = g.c.d (a, b).

Problem 9:- Find all the units of Z ($\sqrt{-5}$)

Solution : Assume that $a + \sqrt{-5}\, b$ is unit in Z ($\sqrt{-5}$)

Then $(a +\sqrt{-5}\, b) (c + \sqrt{-5}\, b) = 1 + \sqrt{-5} . 0$, for some $c, d \in Z$

Therefore $(a - \sqrt{-5}\, b) (c - \sqrt{-5}\, b) = 1 \Rightarrow a^2 + 5 b^2 = 1 \Rightarrow a = \pm 1, b = 0$

Thus $a + \sqrt{-5}\, b = \pm 1$ are the units.

Problem 10:- Consider the ring $Z (\sqrt{-5}) = \{ a +\sqrt{-5}\, b : a, b \in Z\}$

Under the operation defined by

$\{ a +\sqrt{-5}\, b \} + \{ c + \sqrt{-5}\, d \} = (a + c) + \sqrt{-5} (b+d)$

and $(a +\sqrt{-5}\, b) . (c + \sqrt{-5}\, d) = (ac – 5 bd) + \sqrt{-5} (ad + bc)$

Then (1) $\sqrt{-5}$ is a prime element

(2) 3 is an irreducible element which is not prime

Solution : Since $\sqrt{-5} \neq 0$

If it is not a unit then $\exists$ $a + \sqrt{-5}\, b$ such that

$\sqrt{-5}(a +\sqrt{-5}\, b) = 1 \Rightarrow \sqrt{-5} = 1 + 5b$ is not possible because R.H.S is an integer where as it is not an integer.

Let $\sqrt{-5}$ divides $(a + \sqrt{-5}\, b)(c + \sqrt{-5}\, d)$ then $\exists$ $(x + \sqrt{-5}\, y)$

Such that $\sqrt{-5}\,(x + \sqrt{-5}\, y) = (a + \sqrt{-5}\, b)(c + \sqrt{-5}\, d)$

On comparison we get $-5y = ac - 5bd \Rightarrow 5(bd - y) = ac \Rightarrow 5 \mid ac$.

But 5 being a prime number, therefore either $5 \mid a$ or $5 \mid c$

If $5 \mid a$ then $(\sqrt{-5})(\sqrt{-5}) \mid a \Rightarrow \sqrt{-5} \mid a \Rightarrow \sqrt{-5} \mid (a + b\sqrt{-5})$

Similarly, if $5 \mid c$, then $\sqrt{-5} \mid c + \sqrt{-5}\, d$.

Thus $\sqrt{-5}$ is a prime element.

Thus first part is done.

For the (2) part:-

Since $3 = (a + \sqrt{-5}\, b)(c + \sqrt{-5}\, d)$, $a, b, c, d \in Z$

- $\Rightarrow$ $\ddot{3} = (a - \sqrt{-5}\, b)(c - \sqrt{-5}\, b) \Rightarrow 3.\ddot{3} = (a^2 + 5b^2)(c^2 + 5d^2)$
- $\Rightarrow$ $9 = (a^2 + 5b^2)(c^2 + 5d^2) \Rightarrow a^2 + 5b^2 = 1, 3 \text{ or } 9$

Thus $a^2 + 5b^2 = 3$ is not possible as $a, b \in Z$.

If $a^2 + 5b^2 = 1$ then $a = \pm 1$ and $b = 0$

If $a^2 + 5b^2 = 9$, then $a^2 + 5d^2 = 1$, then $c = \pm 1$ and $d = 0$

Thus, if $a^2 + 5b^2 = 1$ then $a^2 + \sqrt{-5}\, b = \pm 1$, which is a unit and if

$a^2 + 5b^2 = 9$, then $c + \sqrt{-5}\, d = \pm 1$, which is also a unit.

Thus, 3 is an irreducible element of $Z(\sqrt{-5})$

Further, we have $(2 + \sqrt{-5})(2 - \sqrt{-5}) = 9$ so $3 \mid (2 + \sqrt{-5})(2 - \sqrt{-5})$

We show here that it does not divide anyone of these

Suppose $3 \mid (2 + \sqrt{-5})$ in $Z(\sqrt{-5})$

Then $(2 + \sqrt{-5}) = 3(a + \sqrt{-5}\, b)$, $a, b \in Z$.

$2 - \sqrt{-5} = 3(a - \sqrt{-5}\, b) \Rightarrow 9 = 9(a^2 + 5b^2) \Rightarrow 1 = a^2 + 5b^2$ i.e, $a = \pm 1$, $b = 0$

$2 + \sqrt{-5} = \pm 3$ which is not possible.

Thus $3 \mid (2 + \sqrt{-5})$

Similarly we can show that $3 \mid (2 - \sqrt{-5})$

Thus 3 is not a prime element of Z ($\sqrt{-5}$).

Problem 11:- An example of a prime element but not a irreducible.

Solution : Let us consider a ring $Z_6 = \{ 0, 1, 2, 3, 4, 5\} \bmod 6$

Then 2 is a prime element in Z_6 but is not irreducible. 2 is in fact non zero , non unit.

Let $2 | a \times b$ (here $\times$ is modified sign of multiplication on the set of remainders)

Since $ab = 6q + a \times b$ for some q and as $2 | 6q$, $2 | a \times b$, we find $2|ab$.

⇨ $2|a$ or $2|b$ => $2|a$ or $2|b \in Z_6$.

Thus 2 is prime element.

Again as $2 \times 4 = 2$, where neither 2 nor 4 is a unit.

We find 2 is not irreducible.