19 May

Euclidean domain :

Defn: Let R be a comml- ring without zero divisors. R is called an "Euclidean domain" or an "Euclidean ring" if for every non-zero element $a \in R$, there is defined a 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 $a, b \in R$, $\exists\ q, r \in R$ such that $a = qb + r$ where either $r = 0$ or $d(r) < d(b)$.

Theorem: 4.36. Let R be an eucl- domain & I be an ideal of R; then $\exists$ an element $a \in I$ such that $I = aR$. ie) Every ideal of an eucl- domain is a principal ideal.

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

Let $a \in I$ be a non-zero element such that $d(a)$ is minimum. (This is possible since d takes only non-negal- integer values).

Now, we claim that $I = aR$.

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

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

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

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

$\therefore r$ is an element of I such that

$d(r) < d(a)$ which is a contradiction to the choice of a & hence $r = 0$

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

Theorem:

Any Euclidean domain R has an identity element.

Pf: Since R is an ideal of R, $\exists\, c \in R$ 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

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

$\therefore e$ is the required identity element

unique factorization domain (U.F.D) ③

Defn: Let R be a commut ring. Let $a, b \in R$ & $a \neq 0$. a divides b and $a|b$ if $\exists$ an element $c \in R$ such that $b = ac$. If $a|b$ we say that a is a "divisor" or a "factor" of b.

Ex: In a field F every non-zero element is a unit & hence every non-zero element divides every element of F.

Defn: Let R be a commut ring. Let a, b be two non-zero elements of R. Then a & b are said to be "associates" if $a|b$ and $b|a$.

Defn: Let R be a commut ring with identity. Let $a \in R$ & $a \neq 0$. 'a' is called a "prime" or an "irreducible element" if a is not a unit & its only divisors are units in R & associates of a.

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

i) any non-zero element in R which is not 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 order & associates of the prime elements

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

Unique factorization domain (U.F.D) 3

(12) Defn: Let R be a commt ring. Let $a, b \in R$ & $a \neq 0$. a divides b and $a|b$ if $\exists$ an element $c \in R$ such that $b = ac$. If $a|b$ we say that a is a "divisor" or a "factor" of b.

Ex: In a field F every non-zero element is a unit & hence every non-zero element divides every element of F.

Defn: Let R be a commut ring. Let a, b be two non-zero elements of R. Then a & b are said to be "associates" if $a|b$ and $b|a$.

Defn: Let R be a comm ring with identity. Let $a \in R$ & $a \neq 0$. 'a' is called a "prime" or an "irreducible element" if a is not a unit & its only divisors are units in R & associates of a.

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

i) any non-zero element in R which is not 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 order & associates of the prime elements

ie) 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 pr. elements, then $r = s$ & each p_i is an associate of some q_j.

6

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

$\therefore d|a$ & $d|b$.

Now suppose $l \in R$ & $l|a$ & $l|b$

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

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

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

Theorem: 4.43: Let R be an Euclidean domain. Let $a, b, c \in R$. Then $a|bc$ & $(a,b)=1 \Rightarrow a|c$

15

Pf since $(a,b)=1$, $\exists$ $x, y \in R \ni ax+by=1$.

$\therefore acx + bcy = c$.

Now, $a|acx$. Also $a|bc \Rightarrow a|bcy$.

$\therefore a|(acx+bcy)$.

Hence $a|c$.

Theorem: 4.45

Any Euclidean domain R is a U.F.D.

Pf: first we shall pr. th 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 pr. this by induction on d(a)

If $d(a) = d(1)$ then 'a' is a unit in R [by theorem 4·40].

Hence the assertion is true. Now, we assume that the result is true $\forall\, x \in R$ $\ni d(x) > d(a)$ & pr. th the result is true for 'a'.

If 'a' is a prime there is nothing to prove.

If not, $a = bc$ where neither b nor c is a unit in R.

$\therefore d(b) < d(a)$ & $d(c) < d(a)$ $\because$ by theorem 4·39.

Now, by induction hypothesis b & c can be written as the product of finite number of prime elements.

Hence a can be expressed as a product of finite no. of prime elements.

We now prove the uniqueness.

Let $a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ where p_i's & q_j's are prime elements of R.

$\because p_1 \mid q_1 q_2 \cdots q_s$

$p_i | q_i$ for some i. without loss of generality ~~of~~ we assume that $p_1 | q_1$.

Since p_1 & 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

$\therefore p_1 p_2 \cdots p_r = u_1 p_1 q_2 q_3 \cdots q_s$

$\therefore p_2 p_3 \cdots p_r = u_1 q_2 q_3 \cdots q_s$

Now, if $r < s$, repeating the above argument r times the left side becomes 1 & the ~~side~~ right side contains a product of some prime elements which is impossible.

17 Hence $r \geq s$.

Ill'y, $s \geq r$ & Hence $r = s$.

further we have shown that every p_i is an associate of some q_j & conversely.

Hence the Theorem.