27-April 2022

PAGE NO.
DATE: / /

UNIQUE FACTORIZATION DOMAIN UFD

An ID (Rt.) is UFD if

$a \in R$, a is non zero and non unit element in R s.t.

$$a = u P_1 P_2 P_3 \cdots P_n$$
$$= u q_1 q_2 q_3 \cdots q_m$$

all q_i, P_j are irreducible, then

(i) $m = n$

(ii) P_i is <u>associate</u> to some q_j

$a, b \in R \Rightarrow a/b$ or b/a

EX: Set of Integers $\rightarrow$ FD.

$$2 = 1 \cdot 2$$
$$= (-1)(-2)$$

$1/-1$, $-1/1$
$2/-2$ $-2/2$

Associates: $a, b \in R$

$a \sim b$ if a/b or b/a

$$8 = 1 \cdot 2^3$$

Every F.D need not be UFD

Counter: $\mathbb{Z}\sqrt{-5}$ is F.D $\quad \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5}, a, \ldots$
$= \{a + \sqrt{5}bi$

$$21 = 1 \cdot 3 \cdot 7$$
$$21 = 1 \cdot (4 - \sqrt{-5})(4 + \sqrt{-5})$$

so not UFD

Factorization Theorem (FD)

If $(R,+,\cdot)$ is ID and let $a \in R$ be non zero and non unit element in R then ID $(R,+,\cdot)$ is FD if

$a = UP_1P_2P_3 \cdots P_n$, where $P_1, P_2, P_3 \cdots P_n$ are irreducible elements

$\forall a \in (R,+,\cdot)$

x is irred.

if $x = ab$ then either a is unit or b is unit

Ex: Set of integers $(\mathbb{Z},+,\cdot)$ is FD

$2 = 1 \cdot 2$

$6 = 1 \cdot 2 \cdot 3$

$= (-1) \cdot 2 \cdot 3$

$= 1 \cdot (-2) \cdot 3$

$= 1 \cdot 2 \cdot (-3)$

$= (-1)(2)(-3)$

$= 1(-2)(-3)$

PAGE NO.
DATE: / /

Unique Factorization Theorem :-

Prime element :- An element p of a CR R is prime if it is not zero element in R and not a unit element and

if p/ab for some $a, b \in R$
then p/a or p/b.

Unique Factorization Domain & Theorem

Let R be a Euclidian ring R and a be non zero, non unit in R.
If

$a = p_1 p_2 \cdots p_m$, p_i are prime
$a = q_1 q_2 \cdots q_n$, q_j are prime

then (1) $m = n$

(2) each p_i and q_j are associates, $1 \le i \le m$, $1 \le j \le n$
i.e p_i / q_j or q_j / p_i

$6 = 1 \cdot 2 \cdot 3$
$= 2(-1)(-2)3$

Proof :-

Given that $a = p_1 p_2 p_3 \cdots p_m$
$a = q_1 q_2 q_3 \cdots q_n$

since $p_1 / p_1 p_2 \cdots p_m$
$\Rightarrow p_1 / q_1 q_2 \cdots q_n$
Let p_1 / q_1 ∵ p_1 and q_1 are prime elements in R
$\Rightarrow q_1 = p_1 u_1$
where u_1 is unit ele in R
$\therefore p_1 p_2 p_3 \cdots p_m = p_1 u_1 q_2 q_3 \cdots q_n$
$\Rightarrow p_2 p_3 \cdots p_m = u_1 q_2 q_3 \cdots q_n$ (by left cancellation law)

Since $p_2 / p_2 p_3 p_4 \cdots p_m$

$\Rightarrow p_2 / u_1 q_2 q_3 \cdots q_n$

$\Rightarrow$ ⊛

$\therefore$ Let p_2 / q_2

$\because p_2$ and q_2 are prime elements in R

$\Rightarrow p_2$ and q_2 are associates

$\Rightarrow q_2 = p_2 u_2$, u_2 is unit in R.

$\Rightarrow$

$p_2 p_3 \cdots p_m = u_1 p_2 u_2 q_3 q_4 \cdots q_n$

(III) $p_3 p_4 \cdots p_m = u_1 u_2 q_3 q_4 \cdots q_n$ (Left Cancellation)

if $m < n$ then after a finite no of steps LHS of (III) becomes 1 and RHS becomes the product of some units and some non units of R which can not be equal to 1 in LHS.

$\Rightarrow \Leftarrow$

$\therefore m \not< n$

only $m \not> n$ (interchanging the role of p_i and q_j)

$\therefore \boxed{m = n}$

$\Rightarrow$ each p_i is some associate of some q_j

$\Rightarrow$