Factorisation of Integral Domain

Divisibility in Integral Domain: An element $a (\neq 0)$ of an integral Domain R is said to be a divisor or factor of an element $b \in R$ if there exists $c \in R$ such that

$$b = ac$$

and we write $a|b$ to denote "a divides b".

Units: An element a of an integral domain R is called unit if it has multiplicative inverse in R

i.e. $\exists$ $b \in R$ such that

$$a.b = b.a = 1 \text{ (Unity)}.$$

Note: ① 1 & -1 are always units of Integral domain of integers.

② Every non-zero element of a field is unit.

③ If $a \in R$ is unit of R then a^{-1} is also a unit of R.

Associates: Two non zero elements of an Integral domain R are called associates if $a|b$ and $b|a$.

We write $a \sim b$ to denote "a and b are associates".

Proper Divisor: Let a be a non-zero element of integral domain R. We know that units of R and associates of a are always divisors of a. These are called improper divisors of a.

A divisor which is not improper divisor is called proper divisor of a. i.e. b is said to be a proper divisor of a if

(i) $b|a$

(ii) b is neither unit nor an associate of a

Prime Element: Let R be an integral domain. An element $p \in R$ is called a prime element if $p \neq 0$, p is non-unit and if $p|ab$ then either $p|a$ or $p|b$

Irreducible element: Let R be an integral domain. An element $a \in R$ is called an irreducible element if it is not a product of two non-units.

or

Let R be an integral domain. An element $a \in R$ is called an irreducible element if it is not unit and its only divisors are units of R and associates of a.

Greatest Common division: Let a and b be arbitrary elements of an integral domain R. An element $d \in R$ is said to be g.c.d of a and b if

① $d|a$, $d|b$

& ⓘⓘ if $c \in R$ such that $c|a$, $c|b$ then $c|d$.

We write (a, b) to denote "gcd of a & b".

Least Common Multiple: Let a and b be any two arbitrary elements of an integral domain R. An element $c \in R$ is said to be l.c.m of a and b if

① $a|c$, $b|c$

& ⓘⓘ if $m \in R$ such that $a|m$, $b|m$ then $c|m$

Unique Factorisation Domain:

An integral domain R is said to be a unique factorisation domain if

(i) any non-zero element of R is either a unit or it can be expressed as the product of a finite number of primes in R

(ii) The factorisation in ① is unique (i.e free from order & associates)

<u>Content</u>: Let $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ be be a polynomial over a unique factorisation domain R. Then content of $f(x)$ is greatest common divisor of coefficient $a_0, a_1, a_2 \ldots a_n$. It is denoted by $c(f(x))$.

<u>Primitive Polynomial</u>: A polynomial $f(x) \in R[x]$ is called primitive polynomial if its content is 1.

<u>Example</u>

$x^2 - 3x + 5$ is primitive $(\because \gcd(1, -3, 5) = 1)$

$2x^2 + 4x + 8$ is not primitive $(\because \gcd(2, 4, 8) = 2)$

$3x^2 + 12$ is not primitive $(\because \gcd(3, 12) = 4)$

<u>Note</u> ① An irreducible polynomial is necessary primitive

<u>Ex</u> Let us consider a non-primitive polynomial say $3x^2 + 12$

We have $3 \cdot (x^2 + 4)$ is product of two polynomials 3 & $x^2 + 4$ which are not associates of $3x^2 + 12$. {Note: 3 is ~~oth~~ zeroth degree polynomial}

Hence $3x^2 + 12$ is reducible.

② A primitive polynomial may or may not be reducible.

<u>Ex</u> Let us consider two polynomials

$x^2 + 3x + 2$ & $x^2 + 3x + 1$

Both are primitive as $\gcd(1,3,2) = 1$ & $\gcd(1,3,1) = 1$

Here $x^2 + 3x + 2 = (x+1)(x+2)$ (reducible)

where as $x^2 + 3x + 1$ is not reducible.

Thm. The relation of divisibility on an integral domain R is reflexive and transitive.

Proof Let R be any integral domain and let $a \in R$

Since $a = 1.a$

$\Rightarrow a|a$

$\Rightarrow$ The relation is reflexive

Let $a, b, c \in R$ such that $a|b$ & $b|c$

$\Rightarrow \exists\ x$ & $y \in R$ such that

$b = ax$ & $c = by$

Now $c = by$

$= (ax)y$

$= a.(xy)$

$= az$ where $z = xy \in R$

$\Rightarrow a|c$

$\Rightarrow$ The relation is transitive.

Proved

Thm If R is an integral domain and $a, b, c \in R$ then

(i) $a|b$, $a|c \Rightarrow a|b+c$

(ii) $a|b \Rightarrow a|bx \ \forall\ x \in R$

Proof (i) $a|b$ & $a|c$

$\Rightarrow \exists\ x$ and $y \in R$ such that

$b = ax$ & $c = ay$

$\Rightarrow b + c = ax + ay$

$\Rightarrow b+c = a(x+y)$

$\Rightarrow b+c = az$ where $z = x+y \in R$

$\Rightarrow a \mid b+c$

(ii) $a \mid b \Rightarrow \exists\ y \in R$ such that $b = ay$

$\Rightarrow bx = (ay)x$

$\Rightarrow bx = a(yx)$

$\Rightarrow bx = ap$ where $p = yx \in R$

$\Rightarrow a \mid bx$

__Thm.__ If R is an integral domain, the relation on R defined as "a is an associate of b" is an equivalence relation.

__Proof__ Let $a \in R$

since $a \mid a$ (& converse)

$\Rightarrow a \sim a$

So it is reflexive relation.

Let $a, b \in R$ and $a \sim b$

$\Rightarrow a \mid b$ & $b \mid a$

$\Rightarrow b \mid a$ & $a \mid b$

$\Rightarrow b \sim a$

So it is symmetric relation

Let $a, b, c \in R$ and $a \sim b$ & $b \sim c$

$\Rightarrow a \mid b$ & $b \mid a$ similarly $b \mid c$ & $c \mid b$

ie $a \mid b$, $b \mid c$ & $c \mid b$, $b \mid a$

$\Rightarrow a \mid c$ & $c \mid a$ ie $a \sim c$ Hence transitive

ie Equivalence.