Ring Theory – II

Sem – 6th

Polynomial Rings :– Let R be a ring and x be an indeterminate or a variable over R.
Let $R[x]$ be the set of all polynomials in x over R,
i.e., $R[x] = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \mid a_i \in R, n \in Z^+\}$;
a_i are called coefficients of the polynomials.

Definitions:

① If for some $n > 0$, $a_n \neq 0$ and $a_i = 0$ for all $i > n$, then a_n is called the leading coefficient of the polynomial; n is called the degree of the polynomial.

② If no such n exists, then the polynomial is of the form $a_0 + 0x + 0x^2 + \cdots$. It is said to be a constant polynomial of degree 0.

③ If $a_i = 0 \ \forall i = 0, 1, 2, \cdots$, the polynomial is said to be the zero polynomial of no degree assigned to it.

④ Equality in $R[x]$:–
Two polynomials $f(x) = a_0 + a_1x + a_2x^2 + \cdots$ and $g(x) = b_0 + b_1x + b_2x^2 + \cdots$ in $R[x]$ are said to be equal, i.e., $f(x) = g(x)$ if $a_i = b_i \ \forall i$.
Two equal polynomials have the same degree.

⑤ Addition in $R[x]$:–
$f(x) + g(x) = c_0 + c_1x + c_2x^2 + \cdots$; $c_i = a_i + b_i \in R$.
$f(x) \in R[x], g(x) \in R[x] \Rightarrow f(x) + g(x) \in R[x]$.
It may easily be verified that $(R[x], +)$ is a commutative group, where the identity element is the zero polynomial.

⑥ Multiplication on $R[x]$:–
$f(x) \cdot g(x) = c_0 + c_1x + c_2x^2 + \cdots$, where $c_k = a_0b_k + a_1b_{k-1} + \cdots + a_kb_0$

It can be verified that $(R[x], +, \cdot)$ is a ring, and is said to be the polynomial ring over the ring R.

⑦ If R be a ring with unity 1, then the ring $(R[x], +, \cdot)$ is also a ring with unity which is the constant polynomial 1 in $R[x]$.

⑧ If R be a commutative ring, then the ring $(R[x], +, \cdot)$ is also a commutative ring.

Theorem: If R be a ring with no divisor of zero, then the ring $(R[x], +, \cdot)$ is a ring with no divisor of zero.

Proof: Let $f(x) = a_0 + a_1 x + \cdots + a_m x^m$, and $g(x) = b_0 + b_1 x + \cdots + b_n x^n$ be non-zero elements in $R[x]$ with degree m & n respectively, (i.e, with leading coeffs. a_m, b_n respectively) where all $a_i, b_i \in R$.

Let us consider the product $f(x) \cdot g(x)$.

The coefficient of x^{m+n} in $f(x) \cdot g(x)$ is $a_m b_n \neq 0$, since $a_m \neq 0$, $b_n \neq 0$ and R contains no divisors of zero.

$\therefore$ $f(x) \cdot g(x)$ is a non-zero polynomial in $R[x]$.

This proves that the ring $(R[x], +, \cdot)$ contains no divisor of zero.

Corollary 1. If D be an I.D., then the polynomial ring $(D[x], +, \cdot)$ is an I.D.

If D be an I.D., D is a commutative ring with unity containing no divisor of zero, then the ring $(D[x], +, \cdot)$ is a commutative ring with unity containing no divisor of zero. Therefore $(D[x], +, \cdot)$ is an I.D.

Corollary 2. If F be a field, then the polynomial ring $(F[x], +, \cdot)$ is an I.D.

Because, every field is an I.D.

Theorem: If R be a ring and $f(x), g(x)$ be polynomials in $R[x]$, then $\deg(f(x)\,g(x)) \leq \deg(f(x)) + \deg(g(x))$.

Equality sign holds if R be an I.D.

Proof: From the previous theorem,

$\deg(f(x)) = m$, $\deg(g(x)) = n$.

$f(x)\,g(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + \cdots + a_m b_n x^{m+n}$

If $a_m b_n = 0$, then $\deg(f(x)\,g(x)) < m+n$.

If $a_m b_n \neq 0$, then $\deg(f(x)\,g(x)) = m+n$.

$\therefore$ $\deg(f(x)\,g(x)) \leq \deg(f(x)) + \deg(g(x))$.

Second part. If R be an I.D., then $a_m \neq 0$, $b_n \neq 0$

$\Rightarrow a_m b_n \neq 0$, since R contains no divisor of zero.

$\therefore$ $\deg(f(x)\,g(x)) = m+n = \deg(f(x)) + \deg(g(x))$.

Theorem: If R be a ring with unity, then the units in the ring R are the only units of the ring $R[x]$.

Proof: Let $f(x)$ be a unit in $R[x]$. Then $f(x) \neq 0$ and $\exists$ some $g(x) \neq 0$ in $R[x]$ s.t.

$f(x)\,g(x) = g(x)\,f(x) = 1$, 1 being the unity in $R[x]$.

$\therefore \deg(f(x)g(x)) = \deg(1) = 0$

or $\deg(f(x)) + \deg(g(x)) = 0 \longrightarrow (1)$

Since $f(x) \neq 0$, $g(x) \neq 0$, $\deg(f(x)) \geq 0$, $\deg(g(x)) \geq 0$

$\therefore$ the equality (1) holds only when

$\deg(f(x)) = 0$, $\deg(g(x)) = 0$, i.e., only when $f(x)$, $g(x)$ are non-zero constant polynomials in $R[x]$.

The non-zero constant polynomials in $R[x]$ are the " elements of R.

Thus a non-zero element $a \in R$ is a unit in $R[x]$ if there exists a non-zero element $b \in R$ s.t. $ab = ba = 1$, i.e., if a is a unit in R.

$\therefore$ the units in R are the only units in $R[x]$.

Corollary 1. If D be an I.D. then the units of D are the only units in the domain $D[x]$.

Corollary 2. If F be a field, then the non-zero elements of F are the only units in the domain $F[x]$.

Note: ① If R be a ring, then $R[x]$ is also a ring

② " R " an I.D., " $R[x]$ " " an I.D.

③ The polynomial ring $F[x]$ over a field F is not a field.

Because, if $p(x)$ be a non-constant polynomial in $F[x]$, then there is no polynomial $q(x) \in F[x]$ s.t. $p(x) \cdot q(x) = 1$, 1 being the unity in $F[x]$ and if is a constant polynomial.

For example, the polynomial $p(x) = x \in F[x]$ has no multiplicative inverse in $F[x]$.

$\therefore$ $F[x]$ is not a field.

Division algorithm for polynomials :-

Statement → Let F be a field and $f(x), g(x) \in F[x]$ with $g(x) \neq 0$. Then there exist unique polynomials $q(x), r(x) \in F[x]$ such that

$$f(x) = g(x) \cdot q(x) + r(x), \text{ where either } r(x) = 0, \text{ or } \deg(r(x)) < \deg(g(x)).$$

Proof: Existence of $q(x)$ & $r(x)$:

If $f(x) = 0$, then $0 = 0 \cdot g(x) + 0$; hence both $q(x)$ & $r(x)$ must also be the zero polynomial.

If $f(x) \neq 0$ and let $\deg(f(x)) = n$ and $\deg(g(x)) = m$.

Case I. $m > n$. Then we can let $q(x) = 0$ and $r(x) = f(x)$.

Case II. $m \leq n$. We use the 2nd principle of induction on n.

Let us assume that the theorem holds for all polynomials $f(x)$ of degree less than n and all $g(x) \neq 0$ s.t. $m \leq n$.

Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, [$a_n$ is leading coeff.]

$g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0$, [$b_m$ " " "]

Then the polynomial

$$f_1(x) = f(x) - a_n b_m^{-1} x^{n-m} g(x) \text{ in } F[x] \text{ has}$$

the degree $< n$, or, is the zero polynomial.

By induction hypothesis, there exists polynomials $q_1(x), r(x) \in F[x]$ s.t.

$$f_1(x) = q_1(x) \cdot g(x) + r(x), \text{ where either } r(x) = 0, \text{ or, } \deg(r(x)) < \deg(g(x)).$$

or, $f(x) - a_n b_m^{-1} x^{n-m} \cdot g(x) = q_1(x) \cdot g(x) + r(x)$.

or, $f(x) = [a_n b_m^{-1} x^{n-m} + q_1(x)]\, g(x) + r(x)$

Let us set $q(x) = a_n b_m^{-1} x^{n-m} + q_1(x) \in F[x]$.

Then $f(x) = q(x) \cdot g(x) + r(x)$, where either $r(x) = 0$, or, $\deg(r(x)) < \deg(g(x))$.

This shows that the theorem holds for all polynomials $f(x)$ of degree n and all polynomials $g(x) \neq 0$ s.t. $\deg(g(x)) \leq \deg(f(x))$.

By the 2nd principle of induction, the theorem holds for all polynomials $f(x), g(x) \in F[x]$ with $g(x) \neq 0$.

Uniqueness of $q(x)$ & $r(x)$:-

Suppose that there exist two other polynomials $q_1(x)$ and $r_1(x)$ s.t. $f(x) = g(x)\cdot q_1(x) + r_1(x)$ with $r_1(x)=0$, or, $\deg(r_1(x)) < \deg(g(x))$.

So that $f(x) = g(x)\cdot q(x) + r(x) = g(x)\cdot q_1(x) + r_1(x)$.

$\Rightarrow g(x)[q(x) - q_1(x)] = r_1(x) - r(x)$.

If $q(x) - q_1(x) \neq 0$ (zero polynomial), then

$\deg\big(g(x)[q(x)-q_1(x)]\big) = \deg\big(r_1(x) - r(x)\big) \geq \deg g(x)$

However, $\deg(r_1(x)) < \deg(g(x))$, and $\deg(r(x)) < \deg(g(x))$.

$\therefore$ $r_1(x) - r(x)$ must be a zero polynomial

i.e., $r_1(x) = r(x)$

$\Rightarrow q_1(x) = q(x)$

Examples of polynomial rings $R[x]$ over a ring $(R,+,\cdot)$.

① Let $(R,+,\cdot)$ be a ring of Gaussian integers.
$f(x) = x^3 + (1+2i)x^2 - ix + (3+4i)$ is a polynomial over $R = \{a+bi : a,b \in \mathbb{Z}\}$.
Then $R[x]$ forms a polynomial ring over $(R,+,\cdot)$, where $R[x] = \{f(x) = a_0 + a_1x + \cdots + a_nx^n,\ a_j \in R\ \forall j\}$

② $\mathbb{Z}[x] = \{f(x) = \sum_{i=0}^{n} a_i x^i : a_i \in \mathbb{Z}, \forall i\}$. Then $(\mathbb{Z}[x],+,\cdot)$ forms a polynomial ring over the ring of integers $(\mathbb{Z},+,\cdot)$.

③ $Z_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$. $(Z_5, \oplus_5, \odot_5)$ forms a ring.
$Z_5[x] = \{f(x) = \sum_{i=0}^{n} a_i x^i : a_i \in Z_5\ \forall i\}$ forms a polynomial ring over the ring Z_5.

In $Z_5[x]$, $f(x) = \bar{2}x^2 +_5 \bar{4}x +_5 \bar{4}$

$g(x) = \bar{3}x^2 +_5 \bar{1}x$

$h(x) = \bar{2}x +_5 \bar{2}$

Then $f(x) + g(x) = (\bar{2} +_5 \bar{3})x^2 + (\bar{4} +_5 \bar{1})x + (\bar{4} +_5 \bar{0})$

$= \bar{0}x^2 + \bar{0}x + \bar{4} = \bar{4}$

$\deg\big(f(x)+g(x)\big) = 0$.

Definition: Let F be a field. An element $a \in F$ is said to be a zero or a root of a polynomial $f(x)$ in $F[x]$ if $f(a) = 0$ in F.

example: ① Let $f(x) = \bar{4} +_6 \bar{4}x^2 +_6 \bar{1}x^4 \in Z_6[x]$. $\bar{2}, \bar{4}$ are the zeros of $f(x)$ in Z_6.

② Let $\phi(x) = x^2 + 1 \in \mathbb{R}[x]$, has no zero in $\mathbb{R}$.

Theorem: Let F be a field. An element $a \in F$ is a zero of $p(x) \in F[x]$ if and only if $x-a$ is a factor of $p(x)$ in $F[x]$

Proof: Suppose $a \in F$ and $p(a)=0$.

By D.A., $\exists$ two polynomials $q(x)$ & $r(x)$ s.t.

$$p(x) = (x-a)\cdot q(x) + r(x) \quad \text{where}$$

$\deg(r(x)) < \deg(x-a) = 1$.

$\therefore \deg(r(x)) = 0 \Rightarrow r(x)$ is a constant polynomial.

Let $r(x) = \alpha$ for $\alpha \in F$.

$\therefore p(x) = (x-a)\cdot q(x) + \alpha$.

But $0 = p(a) = 0 \cdot q(a) + \alpha = \alpha \Rightarrow r(x) = 0$

$\therefore p(x) = (x-a)q(x)$.

$\therefore (x-a)$ is a factor of $p(x)$.

Conversely, suppose $(x-a)$ is a factor of $p(x)$, say $p(x) = (x-a)\cdot q(x)$

Then $p(a) = 0 \cdot q(a) = 0$.

$\therefore a \in F$ is a zero of $p(x) \in F[x]$.

Theorem: Let F be a field. A non-zero polynomial $p(x)$ of degree n in $F[x]$ can have at most n distinct zeros in F.

Proof: We use induction on the degree of $p(x)$.

If $\deg p(x) = 0$, then $p(x)$ being a constant polynomial has no zeros.

Let $\deg p(x) = 1$. Then $p(x) = ax+b$; $a, b \in F$

If α_1, α_2 are zeros of $p(x)$, then $a\alpha_1 + b = a\alpha_2 + b$

$\Rightarrow \alpha_1 = \alpha_2$. Hence $p(x)$ has one zero in F.

Now assume that $p(x) > 1$. If $p(x)$ does not have a zero in F, then done.

On the otherhand, if α is a zero of $p(x)$, then $p(x) = (x-\alpha)\,q(x)$ for some $q(x) \in F[x]$

$\deg(q(x)) = n-1$ [$\because \deg p_1(x) + \deg q(x) = \deg(p_1(x)\cdot q(x))$]

Let $p(\beta) = 0$ s.t. $\alpha \neq \beta$. Then $0 = p(\beta) = (\beta-\alpha)q(\beta)$

Since $\alpha \neq \beta$ & F is a field, $q(\beta) = 0$. (***) continued in the next page

A polynomial of degree n over a field has at most n zeros, counting multiplicity.

Proof: (by induction)

A polynomial of degree 0 over a field has no zero.

Now suppose that $f(x)$ is a polynomial of degree n over a field and a is a zero of $f(x)$ of multiplicity K.

Then $f(x) = (x-a)^K q(x)$, $q(a) \neq 0$;

Since $\deg f(x) = n = \deg\{(x-a)^K q(x)\} = K + \deg q(x)$

$\Rightarrow K \leq n$.

If $f(x)$ has no zeros other than a, then $K = n$.

If $b \neq a$ and $f(b) = 0$, then $0 = f(b) = (b-a)^K q(b)$

$\Rightarrow q(b) = 0 \Rightarrow b$ is also a zero of $q(x)$ with the same multiplicity as it has for $f(x)$

By the 2nd principle of induction, we know that $q(x)$ has at most $\deg q(x) = n-K$ zeros, counting multiplicity.

Thus $f(x)$ has at most $K + n - K = n$ zeros, counting multiplicity.

Note: The above is not true for arbitrary polynomial rings.

For example, the polynomial $x^2 + 3x + 2$ has four zeros in $\mathbb{Z}_6$.

(***). (Continued from the previous page)

By the 2nd induction hypothesis, $q(x)$ can have at most $(n-1)$ zeros in F which are distinct from α.

$\therefore p(x)$ has at most n distinct zeros in F.

Irreducible Polynomial :-

A nonconstant polynomial $f(x)$ in $F[x]$ is irreducible ~~polynomial~~ over a field F if $f(x)$ cannot be expressed as the product $g(x)h(x)$ of two polynomials $g(x)$ and $h(x)$ in $F[x]$ both of lower degree than the degree of $f(x)$.

Every linear polynomial $ax+b$, $a \neq 0$ in $F[x]$ is clearly irreducible.

Irreducible polynomials function as the "prime numbers" of polynomial rings, since F is a field and $F[x]$ is a UFD.

Example: The polynomial $x^2-2 \in \mathbb{Q}[x]$ is irreducible over $\mathbb{Q}$.

The polynomial $x^2+1 \in \mathbb{R}[x]$ is irreducible over $\mathbb{R}$.

A polynomial $f(x) \in F[x]$ may be irreducible over the field F, but it may not be irreducible over a larger field K containing F as a subfield. For example, the polynomial x^2-2 is irreducible over $\mathbb{Q}$ but is not so over the field $\mathbb{R}$, because $x^2-2 = (x-\sqrt{2})(x+\sqrt{2})$ in $\mathbb{R}$.

Theorem: Let $f(x) \in F[x]$ of degree 2 or 3. Then $f(x)$ is reducible over F iff it has a zero in F.

Proof: Let $f(x)$ be reducible over F. Then $f(x) = g(x) \cdot h(x)$, where $\deg(g(x)) < \deg(f(x))$ and $\deg(h(x)) < \deg(f(x))$.

Since $\deg(f(x))$ is either 2 or 3, one of $g(x)$ and $h(x)$ must be of degree 1. Let $g(x) = ax+b$; $a, b \in F$ and $a \neq 0$. $g(x)$ has a zero, $-a^{-1}b \in F$ and consequently $-a^{-1}b$ is a zero of $f(x)$.

Conversely, let $a \in F$ be a zero of the polynomial $f(x) \in F[x]$. Then $x-a$ is a factor of $f(x)$ and this proves that $f(x)$ is reducible over F.

Example: The polynomial $f(x) = x^3 + x^2 + 2$ is irreducible over $\mathbb{Z}_3[x]$.

Suppose that $f(x)$ is reducible over $\mathbb{Z}_3[x]$. By the D.A. there exist a factor of the form $x-a$, where $a \in \mathbb{Z}_3$. Hence $f(a) = 0$ should be. However, $f(\bar{0}) = \bar{2}$, $f(\bar{1}) = \bar{1}$, $f(\bar{2}) = \bar{2}$.
$\therefore$ $f(x)$ has no zeros in $\mathbb{Z}_3$ and must be irreducible.

Lemma 1. Let $f(x) \in \mathbb{Q}[x]$. Then $f(x) = \frac{r}{s}(a_0 + a_1 x + \cdots + a_n x^n)$ where r, s, a_i's are integers. The a_i's are relatively prime, and r, s are also so.

Gauss's Lemma: Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial (leading coeff. $= 1$) such that $f(x)$ factors into a product of two polynomials $\alpha(x)$ and $\beta(x)$ in $\mathbb{Q}[x]$, where the degrees of both $\alpha(x)$ & $\beta(x)$ are less than the degree of $f(x)$. Then $f(x) = a(x)\,b(x)$, where $a(x)$ & $b(x)$ are monic polynomials in $\mathbb{Z}[x]$ with $\deg a(x) = \deg a(x)$ and $\deg f(x) = \deg b(x)$.

Cor: Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ (with $a_0 \neq 0$) in $\mathbb{Z}[x]$. If $f(x)$ has a zero in $\mathbb{Q}$ then $f(x)$ also has a zero α in $\mathbb{Z}$. Furthermore $\alpha \mid a_0$.

Proof: Let $f(x)$ have a zero $a \in \mathbb{Q}$. Then $f(x)$ must have a linear factor $x-a$.
By Gauss's lemma, $f(x)$ has a factorization with linear factor in $\mathbb{Z}[x]$
for some $\alpha \in \mathbb{Z}$,

$$f(x) = (x-\alpha)(x^{n-1} + \cdots - a_0/\alpha) \in \mathbb{Z}[x]$$

Hence $a_0/\alpha \in \mathbb{Z} \Rightarrow \alpha \mid a_0$.

Example: Let $f(x) = x^4 - 2x^3 + x + 1$. Show that $f(x)$ is irreducible over $\mathbb{Q}[x]$.

Solution: Let $f(x)$ be reducible in $\mathbb{Q}[x]$. Then either $f(x)$ has a linear factor, say $f(x) = (x-\alpha)\,q(x)$ where $q(x)$ is a polynomial of degree 3, or

$p(x)$ has two quadratic factors.

If $p(x)$ has a linear factor in $\mathbb{Q}[x]$ then it has a zero in $\mathbb{Z}$ by corollary (previous). And any zero must divide $(a_0 =) 1$, and hence must be ± 1. However, $p(1) = 1$, $p(-1) = 3$.

$\therefore \nexists$ any zero in $\mathbb{Z}$ and hence an impossibility to have $p(x)$ any linear factors.

If $p(x) = (x^2 + ax + b)(x^2 + cx + d)$

$= x^4 + x^3(a+c) + x^2(ac+b+d) + x(ad+bc) + bd$

where each factor is in $\mathbb{Z}[x]$ by Gauss's Lemma. Hence, $a+c = -2$, $ac+b+d = 0$, $ad+bc = 1$, $bd = 1$.

Since $bd = 1$, either $b = d = 1$ or $b = d = -1$.

$\therefore ad + bc = ab + bc = b(a+c) = 1$.

Since $a+c = -2$, $-2b = 1 \nRightarrow b \in \mathbb{Z}$.

$\therefore p(x)$ cannot be reducible over $\mathbb{Q}[x]$.

$\therefore p(x)$ must be irreducible over $\mathbb{Q}$.

Eisenstein's Criterion:

Let p be a prime and suppose that $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$. If $p \mid a_i$ for $i = 0, 1, \cdots, n-1$ but $p \nmid a_n$ and $p^2 \nmid a_0$ then $f(x)$ is irreducible over $\mathbb{Q}$.

Proof: By Gauss's Lemma, we need only to show that $f(x)$ does not factor into polynomials of lower degree in $\mathbb{Z}[x]$.

Let $f(x) = (b_r x^r + \cdots + b_0)(c_s x^s + \cdots + c_0)$ be a factorization in $\mathbb{Z}[x]$ with $b_r \neq 0$, $c_s \neq 0$ and $r, s < n$.

Since $p^2 \nmid a_0 = b_0 c_0$ and $p \mid a_0 = b_0 c_0$, either b_0 or c_0 is not divisible by p.

Suppose $p \nmid b_0$ and $p \mid c_0$. Since $p \nmid a_n = b_r c_s$, then $p \nmid b_r$ and $p \nmid c_s$ also.

Let m be the smallest value of k s.t. $p \nmid c_k$. Then $a_m = b_0 c_m + b_1 c_{m-1} + \cdots + b_m c_0$ is not divisible by p, since each term on the R.H.S. is divisible by p except for $b_0 c_m$. Therefore, $m = n$ since $p \mid a_i$ for $m < n$.

Hence, $f(x)$ cannot be factored into polynomials of lower degree and thereby must be irreducible.

Divisibility [Factorization] in Integral Domains:

If F be a field, then irreducible polynomials in F[x] may be considered as the building blocks in the ring of integers; that is very similar to the building blocks (prime numbers) of the integers.

Given an arbitrary I.D., we are led to the following series of definitions :-

(i) Let D be an I.D. and $a, b \in D$ with $a \neq 0$. We say that a divides b, and write $a|b$, if there exists an element $c \in D$ such that $b = ac$.

(ii) A non-zero element a in D is said to be a unit in D if $a|1$, 1 being the multiplicative identity in D.
i.e., $\exists$ an element $b \in D$ s.t. $1 = a \cdot b = b \cdot a$ [$\because$ D is commutative]
$\Rightarrow$ a has a multiplicative inverse in D.

(iii) Two non-zero elements a and b in D are said to be associates in D if there exists a unit u in D s.t. $a = ub$. [i.e., $b|a$]
Now $a = u \cdot b \Rightarrow u^{-1} a = (u^{-1}u) \cdot b \Rightarrow u^{-1} a = 1 \cdot b$
$\Rightarrow b = u^{-1}a \Rightarrow b = v \cdot a$,
where $v = u^{-1}$, is also a unit, as $u \cdot u^{-1} = u^{-1} \cdot u = 1$
$\Rightarrow u^{-1} | 1$.

(iv) A non-zero element p in an I.D. D that is not a unit is said to be irreducible provided that whenever $p = a \cdot b$, either a or b is a unit.

(v) A non-zero element p in an I.D. that is not a unit is said to be prime if whenever $p|ab$ either $p|a$ or $p|b$.

Example: It is important to notice that primes and irreducible elements do not always coincide.
Let R be the subring (with identity) of $\mathbb{Q}[x, y]$ generated by x^2, y^2 and xy. Each of these elements is irreducible in R; however, xy is not prime, since $xy | x^2y^2$ but does not divide either x^2 or y^2.

Note:

(i) The only divisors of an irreducible in D are units in D and the associates of it.

(ii) An associate of an irreducible element in D is also an irreducible

(iii) There is no irreducible element in a field, because a field is an I.D. where every non-zero element is a unit.

Theorem: In an I.D., every prime element is an irreducible.

Proof: Let p be a prime in an I.D. D.

Then $p \neq 0$ and p is not a unit in D.

Let $p \mid ab$ for some $a, b \in D$. Then either $p \mid a$ or $p \mid b$.

If $p \mid a$, then ~~$\exists$ some $c \in D$ s.t. $a = pc$~~

Let $a \in D$ and $a \mid p$. Then $\exists\ b \in D$ s.t. $p = a \cdot b$

Now $p = a \cdot b \Rightarrow p \mid a \cdot b$.

Since p is a prime & $p \mid a \cdot b \Rightarrow$ either $p \mid a$ or $p \mid b$.

(i) If $p \mid a$, then we have $a \mid p$ & $p \mid a \Rightarrow a$ is an associate of p.

(ii) If $p \mid b$, then $b = p \cdot K$ for some $K \in D$.

$\therefore p = a \cdot b = a \cdot pK \Rightarrow p(1 - aK) = 0$

Since $p \neq 0$ & D contains no divisor of zero,

$\therefore a \cdot K = 1 \Rightarrow a$ is a unit in D.

$\therefore a \mid p \Rightarrow$ either a is an associate of p or a is a unit in D.

$\therefore p$ is an irreducible in D.

Note: In an I.D., an irreducible element may not be a prime — give example.

In an I.D. $\mathbb{Z}[\sqrt{-3}]$, $4 = 2 \cdot 2 = (1+\sqrt{-3})(1-\sqrt{-3})$.

2 is an irreducible in $\mathbb{Z}[\sqrt{-3}]$. Because;

If we take $2 = (a+b\sqrt{-3})(c+d\sqrt{-3})$, and let us define a norm function N on $\mathbb{Z}[\sqrt{-3}]$ by $N(a+b\sqrt{-3}) = a^2+3b^2$,

then $N(2) = N(a+b\sqrt{-3})\,N(c+d\sqrt{-3}) \Rightarrow (a^2+3b^2)(c^2+3d^2) = 4$,

$a, b, c, d \in \mathbb{Z}$.

$\therefore$ either (i) $a^2+3b^2=1$ and $c^2+3d^2=1$; gives $\begin{cases} a=\pm1, b=0 \\ c=\pm1, d=0 \end{cases}$

or (ii) $a^2+3b^2=4$ and $c^2+3d^2=1$; gives $\begin{cases} c=\pm1, d=0 \\ a=\pm2, b=\pm1. \end{cases}$

or (iii) $a^2+3b^2=2$ and $c^2+3d^2=2$; Cannot happen.

From (i), $a=\pm1, b=0 \Rightarrow a+b\sqrt{-3}$ is a unit

But $c=\pm1, d=\pm1 \Rightarrow c+d\sqrt{-3}$ is not a unit

From (ii), $c=\pm1, d=0 \Rightarrow c+d\sqrt{-3}$ is a unit.

$a=\pm1, b=\pm1 \Rightarrow a+b\sqrt{-3}$ is not a unit.

$\therefore$ if $2=(a+b\sqrt{-3})(c+d\sqrt{-3})$ then

either $a+b\sqrt{-3}$, or $c+d\sqrt{-3}$ is a unit

This proves that 2 is an irreducible in $\mathbb{Z}[\sqrt{-3}]$.

Now $2 \mid (1+\sqrt{-3})(1-\sqrt{-3})$. But 2 is neither a divisor of $1+\sqrt{-3}$ nor a divisor of $1-\sqrt{-3}$.

So 2 is not a prime in $\mathbb{Z}[\sqrt{-3}]$.

Note: $2 \nmid (1+\sqrt{-3})$. Since if $2 \mid (1+\sqrt{-3})$, then

$(1+\sqrt{-3})$ $= 2K$; $K \in \mathbb{Z}[\sqrt{-3}]$

i.e., $(2K-1)^2+3=0$ or, $K^2-K+1=0$

$\Rightarrow K=\frac{1\pm\sqrt{1-4}}{2}=\frac{1}{2}\pm\frac{1}{2}\sqrt{-3}$

$\notin \mathbb{Z}[\sqrt{-3}]$.

Multiplicative norm function on an I.D.

A norm function N on an I.D. D is a mapping $N: D \to \mathbb{Z}$ satisfying the following conditions—

(i) $N(\alpha) \geq 0 \quad \forall \alpha \in D$,

(ii) $N(\alpha)=0$ iff $\alpha=0$,

(iii) $N(\alpha\beta)=N(\alpha)N(\beta), \quad \forall \alpha, \beta \in D$.

Th: $N(u)=1$ for every unit $u \in D$.

$1.1=1$.

$\Rightarrow N(1.1)=N(1)\cdot N(1)=N(1)$

$\Rightarrow N(1)[1-N(1)]=0 \Rightarrow N(1)=1$, since $N(1)\neq 0$ and D contains no divisors of zero.

Let u be a unit, $\in D$

$\therefore u^{-1} \in D$ & $uu^{-1}=1$

$\Rightarrow N(1)=N(u)\cdot N(u^{-1}) \Rightarrow 1=N(u)\cdot N(u^{-1})$

$\Rightarrow \underline{N(u)=1, N(u^{-1})=1}$.

G.C.D. in an I.D. D. An element $d \in D$ is said to be a gcd of two non-zero elements a, b in D if
(i) $d|a$ and $d|b$,
(ii) if $c|a$ and $c|b$, then $c|d$, for some $c \in D$.

Note:
① If $d = \gcd(a,b)$, then $du = \gcd(a,b)$, where u is a unit in D.
eg. In the I.D. $\mathbb{Z}$, $4 = \gcd(8,12)$, $-4 = \gcd(8,12)$, where (-1) is a unit in $D = \mathbb{Z}$.
② In an I.D. D, any two gcd's of two elements, if they exist, are associates.
Because, if $d = \gcd(a,b)$, $c = \gcd(a,b)$, then $c|d$ and $d|c \Rightarrow$ c & d are associates.
③ In an I.D., two elements may not have a gcd.
But in a UFD, " " must have a gcd.
④ If $\gcd(a,b)$ is a unit, then two non-zero elements $a, b \in D$ are said to be prime to each other.

L.C.M. An element $l \in D$ (I.D.) is said to be a lcm of two non-zero elements a, b in D, if
(i) $a|l$ and $b|l$
(ii) if $a|m$ and $b|m$, then $l|m$.

Note: Any two lcm's of a and b in an I.D. are associates.

Note: If some two elements in a I.D. D have no gcd, the domain D is not a UFD.
For example, the domain $\mathbb{Z}[\sqrt{-5}]$ is not a UFD, since the elements 21 and $3(1+2\sqrt{-5})$ have no gcd. [Done in Ex. 22/⑤].

Note: If in a UFD D, $au + bv = 1$ for two non-zero elements $a, b \in D$ and for some $u, v \in D$, then a and b are prime to each other.
But, the converse is not true.

Unique Factorisation Domain (UFD).

The Fundamental Theorem of Arithmetic can be extended from positive integers to the integers. The question arises of whether or not such factorisations are possible in other rings. Generalizing this definition, we say:

An integral domain D is a UFD, if D satisfies the following criteria —

(i) Let $a \in D$ such that $a \neq 0$ and a is not a unit. Then a can be written as the product of a finite number of irreducible elements in D, and

(ii) the decomposition is unique upto the order and associates of the irreducibles. that is, if $a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$, where p_i's and q_i's are irreducibles, then $r = s$ and p_i, q_j are associates for some i, j.

Examples:

1. The I.D. $\mathbb{Z}$ is a UFD. → by the Fundamental theorem of Arithmetic. Because, every non-zero element other than 1 and −1 (only units) in $\mathbb{Z}$ can be expressed as the product of a finite number of irreducible elements in $\mathbb{Z}$ and the factorization is unique except for the orders ~~of the factors~~ and the associates of the irreducibles.

   eg. $18 = 2 \cdot 3 \cdot 3 = (-2) \cdot (-3) \cdot 3$. Here 3 and −3 are associates.

Important Theorem:

If D be a UFD then the polynomial ring D[x] is a UFD.

So since the domain $\mathbb{Z}$ is a UFD, the integral domain $\mathbb{Z}[x]$ is a UFD.

Theorem: In a UFD, every irreducible element is a prime.

Proof: Let p be an irreducible element in a UFD D.
Then $p \neq 0$ and p is not a unit in D.
Let $p \mid ab$; $a, b \in D$. Then $\exists\, k \in D$ s.t. $ab = pk$.
Since p is irreducible, and $p \mid ab$, at least one of a and b must be non-unit, as p being a non-unit.

Case 1. Let one of a and b be non-unit.
Let a be a unit, then $a^{-1} \in D$ and $b = a^{-1}(pk)$
$= p(ka^{-1})$.
$\therefore p \mid b$.
If b be a unit, then $b^{-1} \in D$ and $a = (pk)b^{-1} = p(kb^{-1})$
$\therefore p \mid a$
$\therefore p \mid a$ or $p \mid b$

Case 2. Let both of a and b be non-units.
Let $a = p_1 p_2 \cdots p_r$ and $b = q_1 q_2 \cdots q_s$ where $p_1, p_2, \cdots, p_r$; $q_1, q_2, \cdots, q_s$ are irreducibles in D.
If k be a unit, then $ab = pk$ or $(ab)k^{-1} = p \Rightarrow ab \mid p$, again we have $p \mid ab \Rightarrow ab$ is an associate of p.
$\therefore ab$ is an irreducible, but it is not true.
$\therefore k$ is a non unit.
Let $k = t_1 t_2 \cdots t_K$; t_i's are irreducibles in D.
$ab = pk$ gives, $p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s = p t_1 t_2 \cdots t_K$.
By uniqueness of the factorisation of ab into irreducibles, it follows that p must be an associate of one of $p_1, p_2, \cdots, p_r$ or one of $q_1, q_2, \cdots, q_s$.
$\therefore p \mid a$ or $p \mid b$.
$\therefore p$ is a prime element in D.

Note: In a UFD there is no distinction between a prime element and an irreducible element.

Note: If an irreducible element in an I.D. be not a prime element, D is not a UFD.