STUDY MATERIALS

(RING THEORY-II)

TOPIC: FACTORIZATION OF POLYNOMIALS

Mathematics Honours
Semester – 6

Paper – C14 T Unit - 1

Dr. Sangita Chakraborty
Associate Professor
Department of Mathematics
Kharagpur College

** FACTORIZATION OF POLYNOMIALS **

Irreducible Polynomials.

Definition: Let F be a field. A non-constant polynomial $f(x) \in F[x]$ is said to be irreducible over F if $f(x) \neq g(x) \cdot h(x)$, where $g(x), h(x) \in F[x]$ and $\deg(g(x)) < \deg(f(x))$ and $\deg(h(x)) < \deg(f(x))$.
Otherwise, i.e., if $f(x) = g(x) \cdot h(x)$, then $f(x)$ is said to be reducible over F.

Remark: Irreducible polynomials function as the "prime numbers" of polynomials rings, since F is a field and $F[x]$ is a Unique Factorization Domain (UFD).

Examples:

① Every linear polynomial $ax+b$, $a \neq 0$ in $F[x]$, where F ~~is~~ a field, is irreducible over F.
Let us suppose $ax+b$ is not irreducible, then $ax+b = f(x) \cdot g(x)$, where $f(x), g(x) \in F[x]$.
Then $\deg(f(x) \cdot g(x)) = \deg(ax+b) = 1$
or, $\deg(f(x)) + \deg(g(x)) = 1$.
We may assume that $\deg(f(x)) = 0$, $\deg(g(x)) = 1$.
Now $\deg(f(x)) = 0 \Rightarrow f(x)$ is a non-zero constant polynomial and thus a unit in F.
Hence $ax+b$ is irreducible over F.

BUT, a linear polynomial over a UFD D may not be irreducible in $D[x]$.
For example, $2x+4 = 2(x+2)$ is not irreducible in $\mathbb{Z}[x]$, because, neither 2 nor $(x+2)$ is a unit in $\mathbb{Z}[x]$.

② The polynomial x^2-5 is irreducible in $\mathbb{Q}[x]$ and reducible in $\mathbb{R}[x]$.

If x^2-2 is reducible in $\mathbb{Q}[x]$, then there would exist $a, b, c, d \in \mathbb{Q}$ such that
$$x^2-2 = (ax+b).(cx+d) = acx^2+(ad+bc)x+bd.$$
$$\Rightarrow ac=1, \quad ad+bc=0, \quad bd=-2.$$
Now $(ad)^2 = (ad).(ad) = (ad).(-bc) = (ac).(-bd)$
$$= 1.2 = 2.$$
$\Rightarrow ad = \sqrt{2} \notin \mathbb{Q}$. This is a contradiction
$\therefore x^2-2$ is irreducible in $\mathbb{Q}[x]$.
However, $x^2-2 = (x-\sqrt{2})(x+\sqrt{2})$ in $\mathbb{R}[x]$.
$\therefore x^2-2$ is reducible in $\mathbb{R}[x]$.

(3) The polynomial x^2+1 is irreducible in $\mathbb{R}[x]$, but reducible in $\mathbb{C}[x]$.

If x^2+1 is reducible in $\mathbb{R}[x]$, then there would exist $a, b, c, d \in \mathbb{R}$ such that
$x^2+1 = (ax+b).(cx+d) \Rightarrow ac=1, ad+bc=0, bd=1.$
$\therefore (ad)^2 = (ad).(ad) = (ad).(-bc) = (ac).(-bd) = 1.(-1)$
$$= -1$$
$\Rightarrow ad = i$ or $-i \notin \mathbb{R}$. which is a contradiction.
$\therefore x^2+1$ is irreducible in $\mathbb{R}[x]$.
However, $x^2+1 = (x+i)(x-i)$ in $\mathbb{C}[x]$.

(4) The polynomial x^2+1 is irreducible over $\mathbb{Z}_3$, but reducible over $\mathbb{Z}_5$.

$x^2+1 \equiv x^2-4 \pmod 5$
$\equiv (x-2)(x+2)$ in $\mathbb{Z}_5[x]$
$\therefore x^2+1$ is reducible in $\mathbb{Z}_5[x]$.
However, $x^2+1 \equiv x^2-2 \pmod 3$, which cannot be expressible as the product of two polynomials of lower degree in $\mathbb{Z}_3[x]$.
OR, polynomial x^2+1 of degree 2 has no root in $\mathbb{Z}_3$.
Because, if $f(x) = x^2+1$, then
$f(0)=1$, $f(1)=2$, $f(2) = 4+1 = 5 \pmod 3 = 2$.

Reducibility Test for Degrees 2 and 3.

Let F be a field. If $f(x) \in F[x]$ and $\deg f(x)$ is 2 or 3, then $f(x)$ is reducible over F iff $f(x)$ has a zero in F.

Proof: Let $f(x) \in F[x]$ be reducible over F.
Then $f(x) = g(x) \cdot h(x)$, where $g(x), h(x) \in F[x]$ and $\deg g(x) < \deg f(x)$, $\deg h(x) < \deg f(x)$.
Since $\deg f(x)$ is 2 or 3, one of $g(x)$ and $h(x)$ must be polynomial of degree 1.
Let us suppose that $g(x) = ax + b$, $a \neq 0$; $a, b \in F$.
$\Rightarrow -a^{-1}b$ be a zero of $f(x)$ and hence a zero of $f(x)$.

Conversely, let us suppose $f(x)$ has a zero at $x = a \in F$. So that $f(a) = 0$. Then by the Factor Theorem, we have $(x-a)$ is a factor of $f(x)$, and this proves that $f(x)$ is reducible over F.

Examples:

① Let us consider the polynomial $f(x) = x^2+1 \in \mathbb{Z}_p[x]$.
Since $\bar{2}$ is a zero of x^2+1 over $\mathbb{Z}_5$,
x^2+1 is reducible over $\mathbb{Z}_5$.
On the other hand, neither $\bar{0}$, $\bar{1}$, nor $\bar{2}$ is a zero of x^2+1 over $\mathbb{Z}_3$, x^2+1 is irreducible over $\mathbb{Z}_3$.

② Show that the polynomial $f(x) = x^3 + x^2 + 2$ is irreducible over $\mathbb{Z}_3$.

Let us suppose that $f(x)$ is reducible over $\mathbb{Z}_3$, and let $(x-a)$ be a factor of $f(x)$, for $a \in \mathbb{Z}_3$.
$\therefore$ a is a zero of $f(x)$ $\Rightarrow f(a) = 0$.
However, $f(\bar{0}) = \bar{2}$, $f(\bar{1}) = \bar{4} \equiv \bar{1}$, $f(\bar{2}) = \overline{14} \equiv \bar{2}$.
$\therefore f(x)$ has no zeros in $\mathbb{Z}_3$, a contradiction.
$\therefore$ $f(x)$ is irreducible over $\mathbb{Z}_3$.

NOTE:- Polynomials of degree > 3 may be reducible over a field even though they do not have zeros in the field. eg. In $\mathbb{Q}[x]$, $x^4 + 2x^2 + 1 = (x^2+1)^2$, but has no zeros in $\mathbb{Q}$. [it has zeros in $\mathbb{C}$].

Definition: Content of a Polynomial, Primitive Polynomial.

The Content of a non-zero polynomial $\sum_{i=0}^{n} a_i x^i$, where a_i's are integers, is the gcd of the integers a_i $(i = 0, 1, 2, \cdots, n)$.

A primitive polynomial is an element of $\mathbb{Z}[x]$ with content 1.

Gauss's Lemma:- The product of two primitive polynomials is primitive.

PROOF:- Let $f(x)$ and $g(x)$ be primitive polynomials, and let us suppose that $f(x) \cdot g(x)$ is NOT primitive. Let p be a prime divisor of the content of $f(x) \cdot g(x)$.

Let $\bar{f}(x)$, $\bar{g}(x)$ and $\overline{f(x) \cdot g(x)}$ be the polynomials obtained from $f(x)$, $g(x)$, and $f(x) \cdot g(x)$ by reducing the coefficients modulo p.

$\therefore$ $\bar{f}(x), \bar{g}(x) \in \mathbb{Z}_p[x]$, the I.D.

$\bar{f}(x) \cdot \bar{g}(x) = \overline{f(x) \cdot g(x)} = \bar{0} \in \mathbb{Z}_p[x]$; since p divides the content of $f(x) \cdot g(x)$.

$\Rightarrow \bar{f}(x) = \bar{0}$ or $\bar{g}(x) = \bar{0}$ [$\because \mathbb{Z}_p[x]$ is an I.D.]

$\Rightarrow$ p divides every coefficient of $f(x)$,
or, p " " " $g(x)$.

$\Rightarrow$ either $f(x)$ is not primitive or $g(x)$ is not primitive.

This contradicts our assumption that $f(x) \cdot g(x)$ is not primitive.

$\therefore$ $f(x) \cdot g(x)$ is a primitive.

Theorem:- Reducibility over $Q \Rightarrow$ Reducibility over Z.

Let $f(x) \in Z[x]$. If $f(x)$ is reducible over Q, then show that $f(x)$ is reducible over Z.

PROOF:- Let $f(x) \in Z[x]$ be reducible over Q.
And let $f(x) = g(x) \cdot h(x)$, where $g(x), h(x) \in Q[x]$.
We may assume that $f(x)$ is primitive, because the content of $f(x)$ divides both $g(x)$ and $h(x)$.
Let $g(x) = \frac{r_1}{s_1}(a_0 + a_1 x + \cdots + a_n x^n) \in Q[x]$, and
$h(x) = \frac{r_2}{s_2}(b_0 + b_1 x + \cdots + b_m x^m) \in Q[x]$; where
r_1, s_1, r_2, s_2, a_i's, b_i's $\in Z$ and r_1, s_1 are relatively prime; r_2, s_2 are so, also a_i's are so, and b_i's are so.
Let a be the l.c.m of the denominators of the coeffs. of $g(x)$;
and b " " " " " " " " $h(x)$.
Then $a.b\, f(x) = a g(x) \cdot b h(x)$, where $a g(x), b g(x) \in Z[x]$.
Let c_1 be the content of $a g(x)$, and
c_2 " " " " $b h(x)$
Then $a g(x) = c_1 g_1(x)$, $g_1(x)$ is a primitive.
and $b h(x) = c_2 h_1(x)$, $h_1(x)$ " " "
Since $f(x)$ is primitive, the content of $a b\, f(x) = ab$.
Also $g_1(x) \cdot h_1(x)$ is primitive [$\because$ product is primitive]
$\therefore$ the content of $c_1 c_2 g_1(x) \cdot h_1(x)$ is $c_1 c_2$.
$\therefore$ $ab = c_1 c_2 \Rightarrow f(x) = g_1(x) \cdot h_1(x)$, where $g_1(x), h_1(x) \in Z[x]$
And $\deg g_1(x) = \deg g(x)$; $\deg h_1(x) = \deg h(x)$.

IRREDUCIBILITY TEST FOR POLYNOMIALS.

There are many tests for irreducibility →

- Some tests depend on the degree of the polynomial we are testing;
- Some tests depend on the domain that the polynomial lives in: $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{Z}_n[x]$, etc.

① Brute Force Method :-

Sometimes we can show that a polynomial is irreducible by showing that any of the polynomials that could be factored can not be factored.

For example,

Consider the polynomial $f(x) = x^4 + x + 1$ in $\mathbb{Z}_2[x]$.

Can $f(x) = g(x) \cdot h(x)$?? , where $\deg(g(x)) < 4$ & $\deg(h(x)) < 4$.

Now $\deg f(x) = \deg \cdot g(x) + \deg \cdot h(x)$

$$\therefore \quad 4 = 1 + 3 \text{ (or, } 3 + 1)$$
$$= 2 + 2$$

So $g(x)$ can have degree 1 or 2.

Does $f(x)$ have a degree 1 or degree 2 factor?

deg. 1	deg. 2
$x + 0 \in \mathbb{Z}_2[x]$	$x^2 + x + 1 \in \mathbb{Z}_2[x]$
$x + 1 \in \mathbb{Z}_2[x]$	$x^2 + 1 \in \mathbb{Z}_2[x]$
	$x^2 + x \in \mathbb{Z}_2[x]$
	$x^2 \in \mathbb{Z}_2[x]$

Now $x \in \mathbb{Z}_2[x]$ cannot be a factor since $f(x)$ has a constant term 1.

Similarly $x^2 + x$, x^2 in $\mathbb{Z}_2[x]$ can not be a factor of $f(x)$.

Now we have to check whether $x+1$, x^2+x+1 and x^2+1 in $\mathbb{Z}_2[x]$ can be factors of $f(x)$.

For deg. 1 polynomial $x+1$ in $\mathbb{Z}_2[x]$, we have $-1\,[\equiv 1 \pmod 2]$, i.e., 1 in $\mathbb{Z}_2$ is a root of $x+1$, however 1 is not a root of $f(x) = x^4+x+1$ over $\mathbb{Z}_2$.

$\therefore$ $x+1$ can not be a factor of $f(x)$.

Now let us consider x^2+x+1 and x^2+1 are the factors of $f(x)$ over $\mathbb{Z}_2$.

Then $f(x) = (x^2+x+1)(ax^2+bx+c)$; $f(x) = (x^2+1)(ax^2+bx+c)$

where $a, b, c \in \mathbb{Z}_2$.

$\therefore$ $x^4+x+1 = (x^2+x+1)(ax^2+bx+c)$

$\Rightarrow x^4+x+1 = ax^4+(a+b)x^3+(a+b+c)x^2+(b+c)x+c$

$\Rightarrow a=1,\ a+b=0,\ a+b+c=0,\ b+c=1,\ c=1$

$\Rightarrow$ If $a=1,\ b=1,\ c=1$, then $a+b+c=0$ is not satisfied in $\mathbb{Z}_2$.

$\therefore$ x^2+x+1 is NOT a factor of $f(x)$ in $\mathbb{Z}_2[x]$

$x^4+x+1 = (x^2+1)(ax^2+bx+c)$

$\Rightarrow x^4+x+1 = ax^4+bx^3+(a+c)x^2+bx+c$.

$\Rightarrow a=1,\ b=0,\ a+c=0,\ b=1,\ c=1$

$b=0,\ b=1$ is not possible.

$\therefore$ x^2+1 is not a factor of $f(x)$.

$\therefore$ $f(x)$ is irreducible in $\mathbb{Z}_2[x]$.

② $\boxed{\text{ROOTS}}$

- If a polynomial has no roots and its degree is 2 or 3, then it is irreducible.

Because, "Has a root $\Leftrightarrow$ Has a deg. 1 factor.

Since deg. 2 = deg. 1 + deg. 1

& deg. 3 = deg. 1 + deg. 2

For example, consider $f(x) = 2x^2+x+1$ in $\mathbb{Z}_3[x]$. Here we see that $f(0)=1$, $f(1)=4\equiv 1 \pmod 3$, and $f(2)=11\equiv 2 \pmod 3$.

$\therefore$ $f(x)$ has no roots in $\mathbb{Z}_3$. Further, deg. $f(x) = 2$, So $f(x)$ is irreducible in $\mathbb{Z}_3[x]$.

If a polynomial $f(x) \in F[x]$ has a root $a \in F \Rightarrow f(a) = 0 \Rightarrow (x-a)$ is a factor of $f(x)$ $\Rightarrow f(x)$ is reducible over F.

The converse is NOT true. That is — If a polynomial $f(x) \in F[x]$ is reducible, it may not have a root in F.

For example, consider $f(x) = x^4 + 2x^3 + 3x + 1 \in \mathbb{Z}_5[x]$.
Here $f(0) = 1$, $f(1) = 2$, $f(2) = 4$, $f(3) = 0$, $f(4) = 2$, in $\mathbb{Z}_5$.
$\therefore$ 3 is a root of $f(x)$ over $\mathbb{Z}_5$.
$\Rightarrow (x-3)$ is a factor of $f(x)$
$\Rightarrow f(x)$ is reducible over $\mathbb{Z}_5[x]$.

Example for converse part.

Consider $f(x) = x^4 + 5x^2 + 4 \in \mathbb{R}[x]$.
$= (x^2+1)(x^2+4)$ having roots at $x = \pm i, \pm 2i \notin \mathbb{R}[x]$.
$\therefore$ $f(x)$ is reducible over $\mathbb{R}$, but it has no roots in $\mathbb{R}$.
Because, deg. $f(x) = 4$ here, for which $f(x)$ can ~~be fact~~ have two quadratic (deg. 2) factor, if it does not have a linear (deg. 1) factor (i.e., no roots).

Therefore, the question arises —
If a polynomial has no roots, does that mean it is irreducible ??
Answer is — Not necessarily. eg. $x^4 + 5x^2 + 4 \in \mathbb{R}[x]$.

③ Rational Root Test :-

Given a polynomial $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ with integer coefficients, any rational number $\frac{r}{s}$ ($s \neq 0$, $\gcd(r,s)=1$) that is a root of $f(x)$ must have $r | a_0$ and $s | a_n$; where $a_0 \neq 0, a_n \neq 0$.

<u>Proof</u>:- Since $\frac{r}{s}$ is a root of $f(x)$,

$$0 = f\left(\frac{r}{s}\right) = a_n\left(\frac{r}{s}\right)^n + \cdots + a_1 \cdot \frac{r}{s} + a_0$$

$$\Rightarrow a_n r^n + \cdots + a_1 r s^{n-1} + a_0 s^n = 0$$

$$\Rightarrow s\left(a_{n-1} r^{n-1} + a_{n-2} r^{n-2} s + \cdots + a_1 r s^{n-2} + a_0 s^{n-1}\right) = -a_n r^n.$$

$$\Rightarrow s | a_n r^n \Rightarrow \underline{s | a_n}, \text{ since } \gcd(r,s)=1.$$

On the otherhand,

$$0 = f\left(\frac{r}{s}\right) = a_n\left(\frac{r}{s}\right)^n + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + \cdots + a_1 \cdot \frac{r}{s} + a_0$$

$$\Rightarrow a_n r^n + a_{n-1} r^{n-1} s + \cdots + a_1 r s^{n-1} + a_0 s^n = 0$$

$$\Rightarrow r\left(a_n r^{n-1} + a_{n-1} r^{n-2} s + \cdots + a_1 s^{n-1}\right) = -a_0 s^n.$$

$$\Rightarrow r | a_0 s^n \Rightarrow \underline{r | a_0}, \text{ since } \gcd(r,s)=1.$$

<u>Examples:</u>

① Consider $f(x) = 3x^3 - 2x^2 + 12x - 8$.

Let r/s be a rational root of $f(x)$.

Then by Rational root test, we have

$r | (-8)$ and $s | 3$ $\Rightarrow r = \pm 1, \pm 2, \pm 4, \pm 8$;

and $s = \pm 1, \pm 3$.

$\therefore$ The potential roots (rational) are:

$\frac{r}{s} = \pm 1, \pm 2, \pm 4, \pm 8, \pm 1/3, \pm 2/3, \pm 4/3, \pm 8/3$.

We get $f(2/3) = 0 \Rightarrow (x - 2/3)$ is a linear factor of $f(x)$

$\Rightarrow f(x)$ is reducible in $\mathbb{Q}[x]$

Ex. ② Consider $f(x) = x^4 - 3x + 6$. Examine its reducibility over $\mathbb{Q}[x]$.

Imp: Let r/s be a rational root of $f(x)$.
Then by Rational Root test, we have
$r | 6$ and $s | 1 \Rightarrow r = \pm 1, \pm 2, \pm 3, \pm 6$;
and $s = \pm 1$.
$\therefore$ The potential rational roots are:
$r/s = \pm 1, \pm 2, \pm 3, \pm 6$.
And we find that $f(x) \neq 0$ for any of r/s.
$\Rightarrow f(x)$ has no rational roots.
BUT, $\deg. f(x) = 4\ (> 3)$, so we are not sure yet whether $f(x)$ is irreducible or not in $\mathbb{Q}[x]$.
We have to depend on some other tests,
We will use Eisenstein criterion for this $f(x)$.
And we will do it later.

④ Eisenstein's Criterion :-

Given a polynomial $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, if there exists a prime p for which
(i) $p | a_i$ for $i = 0, 1, \cdots, n-1$;
(ii) $p \nmid a_n$;
(iii) $p^2 \nmid a_0$, then $f(x)$ is irreducible over $\mathbb{Q}$.

PROOF: Let $f(x)$ be reducible over $\mathbb{Q}$. Then $f(x)$ is reducible over $\mathbb{Z} \Rightarrow f(x) = g(x) \cdot h(x)$, where $g(x), h(x) \in \mathbb{Z}[x]$, and $\deg. g(x) < \deg. f(x)$, $\deg. h(x) < \deg. f(x)$.
Let $g(x) = \sum_{j=0}^{r} b_j x^j$ and $h(x) = \sum_{j=0}^{s} c_j x^j$
then $a_0 = b_0 \cdot c_0$. Since $p | a_0$, $p^2 \nmid a_0$, it follows that p divides one of b_0 and c_0, but not the both.

Suppose $p | b_0$ and $p \nmid c_0$.
Also since $p \nmid a_n = b_r c_s \Rightarrow p \nmid b_r$
So $\exists$ a least integer t s.t. $p \nmid b_t$.
Now consider $a_t = b_t c_0 + b_{t-1} c_1 + \cdots + b_0 c_t \longrightarrow (1)$.
By assumption of Eisenstein's Criterion,
$p | a_t$.
By the choice of t, we can have the every term except the first in the R.H.S. of (1) is divisible by p. Then it follows that $p | b_t c_0$ as well.
This is impossible, since $p \nmid b_t$, $p \nmid c_0$ and p is a prime.
$\therefore f(x)$ is irreducible in $\mathbb{Q}[x]$.

Irreducibility of pth cyclotomic Polynomial :-

For any prime p, the pth cyclotomic polynomial

$$\phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

is irreducible over $\mathbb{Q}$.

PROOF: Let $f(x) = \phi_p(x+1) = \dfrac{(x+1)^p - 1}{(x+1) - 1}$

$$= x^{p-1} + {}^pc_1 x^{p-2} + {}^pc_2 x^{p-3} + \cdots + {}^pc_1.$$

Since every term on the R.H.S. except x^{p-1} is divisible by p and the constant term is not divisible by p^2, by Eisenstein's Criterion, $f(x)$ is irreducible over $\mathbb{Q}$.
Therefore, if we consider that $\phi_p(x)$ is reducible over $\mathbb{Q}$ s.t. $\phi_p(x) = g(x) \cdot h(x)$, then $f(x) = \phi_p(x+1) = g(x+1) \cdot h(x+1)$ will be a factorization over $\mathbb{Q}$. This is a contradiction,
$\therefore \phi_p(x)$ is irreducible over $\mathbb{Q}$.

Example: Consider the polynomial in Ex. (2).
$f(x) = x^4 - 3x + 6$. Examine its reducibility over $\mathbb{Q}$.

Apply Eisenstein's criterion by taking $p = 3$.
$f(x) = x^4 + 0.x^3 + 0.x^2 - 3.x + 6$, where all the coefficients except the coefficient of x^4 are divisible by p; moreover $p^2 \nmid 6 (= a_0)$
$\therefore$ $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Example: Consider $f(x) = 3x^3 + 4x^2 - 6x + 18$;
Apply Eisenstein's criterion by taking $p = 2$.
Here all the coefficients except the coefficient of x^3 (which is 3) are divisible by $p = 2$
Also $p^2 \nmid 18 (= a_0)$.
$\therefore$ $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Example: Consider $f(x) = x^{10} + 50$.
Apply Eisenstein's criterion by taking $p = 2$.
$f(x)$ is irreducible over $\mathbb{Q}$.

(5) **Mod p Irreducibility Test:-**

Let $f(x) \in \mathbb{Z}[x]$ and p be a prime.
Let $\bar{f}(x) \in \mathbb{Z}_p[x]$ obtained from $f(x)$ by reducing all the coefficients of $f(x)$ mod p.
If $\bar{f}(x)$ is irreducible over $\mathbb{Z}_p$ and $\deg.\bar{f}(x) = \deg.f(x)$, then $f(x)$ is also irreducible over $\mathbb{Q}$.

Example: Consider $f(x) = 4x^3 + x^2 - x + 3$.
Consider its reducibility over $\mathbb{Q}$.
Test its reducibility over $\mathbb{Q}$.

If we apply Eisenstein's criterion by

taking $p=2$, then the conditions are not satisfied
$\therefore$ We cannot apply Eisenstein Criterion.
Again similarly we cannot apply Eisenstein Criterion by taking $p=3$, $p=5$, ... so on.

So we take "Mod p Irreducibility Test".

Let us take $p=5$.

Then in $\mathbb{Z}_5[x]$, $\bar{f}(x) = 4x^3 + x^2 + 4x + 3$ $[\because -1 \equiv 4 \pmod 5]$

Now $\bar{f}(0) = 3$, $\bar{f}(1) = 12 \equiv 2 \pmod 5$, $\bar{f}(2) = 32+4+8+3 \equiv 2 \pmod 5$

$\bar{f}(3) = 68+9+12+3 \equiv 2 \pmod 5$, $\bar{f}(4) = 256+16+16+3 \equiv 1 \pmod 5$

So $\bar{f}(x)$ has no roots in $\mathbb{Z}_5$ and the $\deg \bar{f}(x) = 3$,

$\therefore$ $\bar{f}(x)$ is irreducible over $\mathbb{Z}_5$;

$\Rightarrow f(x)$ " " over Q.

NOTE: The CONVERSE IS NOT TRUE ↓

Example: Consider $f(x) = x^4 + 1 \in \mathbb{Z}[x]$.

We apply "Rational Root Test" by taking a rational number r/s; where $r|1$, $s|1$

$\Rightarrow r = \pm 1$; $s = \pm 1 \Rightarrow r/s = \pm 1$

But $f(\pm 1) = 2 \neq 0$. $\Rightarrow f(x)$ has no roots in Q.
$\Rightarrow f(x)$ has no linear factor in $Q[x]$

However, $\deg f(x) = 4\ (>3)$, $f(x)$ may have two quadratic factors. Let $f(x) = (x^2+ax+b)(x^2+cx+d)$

$\Rightarrow x^4+1 = x^4 + (a+c)x^3 + (b+ac+d)x^2 + (ad+bc)x + bd$

$\Rightarrow a+c=0$, $b+ac+d=0$, $ad+bc=0$, $bd=1$; where $a, b, c, d \in \mathbb{Z}$.

Now $bd = 1 \Rightarrow$ either $b=d=1$ or $b=d=-1$.

From $ad+bc=0$, $ab+bc=0 \Rightarrow b\cdot(a+c)=0$

$\therefore$ $a+c=0 \Rightarrow c=-a$.

From $b+ac+d=0 \Rightarrow 2b-a^2=0 \Rightarrow a^2=2b$, which is not true for every $a, b \in \mathbb{Z}$.

$\therefore$ $f(x)$ is irreducible over Q.

BUT $f(x)$ is reducible over $\mathbb{Z}_p$ for every prime p.

Example:- Consider the polynomial

$$f(x) = \frac{5}{7}x^3 - \frac{1}{2}x + 1 \text{ in } Q[x].$$

$\Rightarrow 14 f(x) = 10x^3 - 7x + 14 \equiv f_1(x)$, say.

Reducing $f_1(x)$ in $Z_3[x]$, we obtain

$\bar{f_1}(x) = x^3 + 2x + 2$; $\bar{f_1}(0) = 2$, $\bar{f_1}(1) = 2$, $\bar{f_1}(2) = 2$ in Z_3.

$\therefore$ $\bar{f_1}(x)$ has no root in $Z_3[x]$, and deg. $\bar{f_1}(x) = \deg f(x) = 3$,

hence $\bar{f_1}(x)$ is irreducible in $Z_3[x]$, and

consequently $f_1(x)$ is irreducible in $Q[x]$.

As a result $f_1(x) = 14 f(x)$ is irreducible in $Q[x]$.

But 14 is a unit in $Q[x]$. Hence $f(x)$ is irreducible in $Q[x]$.

Theorem:- Let F be a field and $f(x) \in F[x]$. Then $\langle f(x) \rangle$ is a maximal ideal in $F[x]$ iff $f(x)$ is irreducible over F.

Proof: (Necessary Part) $\rightarrow$

Let $\langle f(x) \rangle$ be a maximal ideal in $F[x]$.

Then $f(x)$ is neither the zero polynomial nor a unit in $F[x]$, because, neither $\{0\}$ nor $F[x]$ is a maximal ideal in $F[x]$.

If $f(x) = g(x) \cdot h(x)$ is reducible over F, then

$\langle f(x) \rangle \subset \langle g(x) \rangle \subset F[x]$

$\langle f(x) \rangle = \langle g(x) \rangle$ or, $F[x] = \langle g(x) \rangle$.

$\Rightarrow$ deg. $f(x)$ = deg. $g(x)$; or, $\Rightarrow$ deg. $g(x) = 0$,

And hence deg. $h(x)$ = deg. $f(x)$.

$\therefore$ $f(x)$ cannot be written as a product of two polynomials in $F[x]$ of lower degree.

(Sufficient Condition) $\rightarrow$ Let $f(x)$ be irreducible over F.

Let U be any ideal of $F[x]$ s.t. $\langle f(x) \rangle \subset U \subset F[x]$

Since $F[x]$ is a PID, $U = \langle g(x) \rangle$ for some $g(x) \in F[x]$.

$\because f(x) \in \langle g(x) \rangle \Rightarrow f(x) = g(x) \cdot h(x)$, " " $h(x) \in F[x]$

$\Rightarrow$ either $g(x)$ is a constant or $h(x)$ is a constant [$\because$ $f(x)$ is irred.]

$\Rightarrow$ " $U = F[x]$ or $\langle f(x) \rangle = \langle g(x) \rangle = U$ $\Rightarrow \langle f(x) \rangle$ is maximal in $F[x]$.

Example: Examine whether the polynomial $f(x) = x^4 - 2x^3 + x + 1$ is irreducible over $\mathbb{Q}$.

If $f(x)$ is reducible in $\mathbb{Q}[x]$, then either $f(x)$ has a linear factor (i.e., a rational root) or $f(x)$ has two quadratic factors in $\mathbb{Q}[x]$, since $\deg f(x) = 4$.

To examine for its linear factor, let us consider a rational ~~root~~ number r/s where $r|1$, $s|1$

$\therefore$ Possible rational roots are $\pm 1 \ (= r/s)$.

But $f(1) = 1$, $f(-1) = 3$.

$\therefore$ There does not exist any rational root.

So, $f(x)$ does not have any linear factor.

This may not imply that $f(x)$ is irred. over $\mathbb{Q}$, as $\deg f(x) = 4$.

Next, to examine for its quadratic factors,

let $f(x) = x^4 - 2x^3 + x + 1 = (x^2 + ax + b) \cdot (x^2 + cx + d)$,

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

$\Rightarrow a + c = -2, \quad ac + b + d = 0, \quad ad + bc = 1, \quad bd = 1$.

Now $b.d = 1 \Rightarrow$ either $b = d = 1$, or, $b = d = -1$.

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

$\Rightarrow b.(-2) = 1 \quad [\because a + c = -2]$

$\Rightarrow b = -\frac{1}{2} \notin \mathbb{Z}$.

$\therefore f(x)$ cannot have quadratic factors too.

$\therefore f(x)$ is irreducible over $\mathbb{Q}$.

Ex 9. Find all irreducible polynomials of degree 3 in $\mathbb{Z}_2[x]$.

A polynomial of deg 3 over $\mathbb{Z}_2$ is of the form ax^3+bx^2+cx+d, where $a,b,c,d \in \mathbb{Z}_2$ and $a \neq \bar{0}$.

$\therefore$ $a = \bar{1}$, since $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$.

b, c, d can take up 2 elements each.

$\therefore$ Total number of such polynomials is $1 \times 2 \times 2 \times 2 = 8$.

They are: x^3, $x^3+\bar{1}$, x^3+x, $x^3+x+\bar{1}$, x^3+x^2, $x^3+x^2+\bar{1}$, x^3+x^2+x, $x^3+x^2+x+\bar{1}$ (8 polynomials).

The irreducible polynomials, i.e., the polynomials which do not have roots in $\mathbb{Z}_2$ are:

$x^3+x+\bar{1}$, $x^3+x^2+\bar{1}$.

Ex. 10. Show that the polynomial x^2+x+1 is irreducible in $\mathbb{Z}_2[x]$. Show that the quotient ring $\frac{\mathbb{Z}_2[x]}{\langle x^2+x+1 \rangle}$ is a field of 4 elements.

Let $p(x) = x^2+x+1$. If $p(x)$ be reducible in $\mathbb{Z}_2[x]$, then $p(x) = f(x) \cdot g(x)$, where $\deg f(x) = 1$; $\deg g(x) = 1$.

Let $f(x) = x - a$ for some $a \in \mathbb{Z}_2$. Then $p(a) = 0$.

However, $p(\bar{0}) = \bar{1}$, $p(\bar{1}) = \bar{3} = \bar{1}$ $\Rightarrow$ $p(x) = x^2+x+1$ has no zero in $\mathbb{Z}_2$. So x^2+x+1 is irreducible in $\mathbb{Z}_2[x]$.

Since $\mathbb{Z}_2$ is a field, the ideal $\langle x^2+x+1 \rangle$ is a maximal ideal in $\mathbb{Z}_2[x]$.

$\Rightarrow$ the quotient ring $\frac{\mathbb{Z}_2[x]}{\langle x^2+x+1 \rangle}$ is a field, since $\mathbb{Z}_2[x]$ is a ring with unity.

Any element of the quotient ring is of the form $h(x) + \langle x^2+x+1 \rangle$, where $h(x) \in \mathbb{Z}_2[x]$.

By Division algorithm, $h(x) = (x^2+x+1)q(x) + r(x)$; where either $r(x) = \bar{0}$ or $\deg(r(x)) = 1$ or 0.

In both the cases, $r(x)$ can be chosen as $r(x) = ax+b$, for $a, b \in \mathbb{Z}_2$; when $(a,b) = (\bar{0}, \bar{0})$, then $r(x) = \bar{0}$, otherwise $\deg(r(x)) = 0$ or 1.

$$\therefore \quad h(x) + \langle x^2+x+1 \rangle$$
$$= (x^2+x+1)q(x) + ax+b + \langle x^2+x+1 \rangle$$
$$= ax+b+\langle x^2+x+1 \rangle \quad [\because (x^2+x+1)q(x) \in \langle x^2+x+1 \rangle]$$

Since each of a and b can independently be chosen in 2 ways, the total number of elements of the quotient ring $\frac{\mathbb{Z}_2[x]}{\langle x^2+x+1 \rangle}$ is $2 \times 2 = \underline{4}$.