Observation:- Let $f(x) \in \mathbb{Q}[x]$

Then $f(x)$ can be expressed as follows:

$$f(x) = \frac{a}{b} P(x)$$

where $a, b \in \mathbb{Z}$, $b \neq 0$ and $P(x)$ is a primitive polynomial.

Let us suppose

$$f(x) = \frac{a_0}{b_0} + \frac{a_1}{b_1} x + \frac{a_2}{b_2} x^2 + \cdots + \frac{a_m}{b_m} x^m$$

$\forall\ b_i \neq 0$

Let $b = LCM(b_0, b_1, b_2, \ldots, b_m)$

$b_0 \mid b \Rightarrow b = b_0 b_0'$

$b_1 \mid b \Rightarrow b = b_1 b_1'$

$\vdots$

$b_m \mid b \Rightarrow b = b_m b_m'$

~~$bf(x) =$~~

Scanned with CamScanner

$$bf(x) = \left(b_0, b_0'\right)\frac{a_0}{b_0} + \left(b_1, b_1'\right)\frac{a_1}{b_1}x + \cdots + \left(b_m, b_m'\right)\frac{a_m}{b_m}x^m$$

$$= c_0 + c_1 x + \cdots + c_m x^m$$

where $c_i \in Z^+$, $i = 0, 1, \ldots, m$.

$$\Rightarrow bf(x) = a\,p(x)$$

where $a = \gcd(c_0, c_1, \ldots, c_m)$ and $p(x)$ is a primitive polynomial.

$$\Rightarrow f(x) = \frac{a}{b}p(x)$$

//

Defination 4.3.4. Let $f(x) = a_0 + a_1 x + \cdots + a_m x^m$ be a polynomial in $Z'[x]$.

Then the content of $f(x)$ is the gcd of $a_0, a_1, \ldots, a_m$.

$\Rightarrow$ content of $f(x) = \gcd(a_0, a_1, \ldots, a_m)$

for a primitive poly. content $= 1$

(Gauss Lemma)

Theorem 4.3.5. If the primitive polynomial $f(x)$ can be factored as the product of the polynomials $p(x)$ and $q(x)$ with rational coefficient then it can be factored as the product of polynomial $p_1(x)$ and $q_1(x)$ with integer coefficients.

OR

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

Scanned with CamScanner

Pf: The primitive polynomial $f(x)$ can be expressed as $f(x) = P(x)Q(x)$

where $P(x), Q(x) \in \mathbb{Q}[x]$

Now we have to show that

$f(x) = P_1(x) Q_1(x)$

where $P_1(x), Q_1(x) \in \mathbb{Z}'[x]$

Since $P(x) \in \mathbb{Q}[x]$ $P(x)$ can be expressed as $\frac{a}{b} P_1(x)$ where $a, b \in \mathbb{Z}'$ and $P_1(x) \in \mathbb{Z}'$

for $P(x) = \frac{a_0}{b_0} + \frac{a_1}{b_1} x + \cdots + \frac{a_m}{b_m} x^m$

then $b\,P(x) = c_0 + c_1 x + \cdots + c_m x^m$

where $b = Lcm(b_0, b_1, \ldots, b_m)$

and $c_i \in \mathbb{Z}' \ \forall i = 0, \ldots, m$

$\therefore b\,c\,P(x) = a\,P_1(x)$ where $a = gcd(c_0, c_1, \ldots, c_m)$

$\Rightarrow P(x) = \frac{a}{bc} P_1(x)$, $P_1(x)$ is a primitive poly.

Similarly $Q(x) = \frac{e}{d} Q_1(x)$, $Q_1(x)$ is a primitive poly.

where $e, d \in \mathbb{Z}'$ and $Q_1(x) \in \mathbb{Z}'[x]$

Now $f(x) = P(x) Q(x)$

$\Rightarrow f(x) = \left[\frac{a}{bc} P_1(x)\right]\left[\frac{e}{d} Q_1(x)\right]$

$= \left(\frac{ae}{bcd}\right) P_1(x) Q_1(x)$

$\Rightarrow f(x) = ae\,[P_1(x) Q_1(x)]$ ——— (1)

By the given condition $f(x)$ is a primitive poly.

Also $P_1(x)$ and $Q_1(x)$ both are primitive poly.

so $P_1(x) Q_1(x)$ is also a primitive poly.

Scanned with CamScanner

Then content of bd $f(x)$ is ~~bd~~ bd and the content of ac $p_1(x)\, q_1(x) \in Q[x]$ is ac

From ① we get

$$bd = ac$$

$$\Rightarrow f(x) = p_1(x)\, q_1(x)$$

Defn 4.3.6. A polynomial in $Z[x]$ is called an (integer) monic polynomial if the leading coeff. of the polynomial is 1.

eg. $4 - 6x + 2x^2 + x^3$ is a monic polynomial. (Note:- A monic poly is always primitive

Corrolary of Gauss lemma) If a monic poly $f(x)$ can be factored as product of $p(x)$, $q(x)$ with rational coeff. Then it can be factored as product of monic polynomials $p_1(x)$ and $q_1(x)$

4.3.8. Defn:- A polynomial $f(x)$ in $R[x]$ is said to be an irreducible polynomial over R (as in $R[x]$) if whenever $f(x) = g(x)\, h(x)$

$g(x), h(x) \in R[x]$ then one of $g(x)$ or $h(x)$ has degree zero.

[If $f(x) = g(x)\, h(x)$

$\Rightarrow$ either $\deg g(x) = 0$ or $\deg h(x) = 0$

then $f(x)$ is an irreducible polynomial in $R[x]$

i.e. $f(x)$ cannot be factored as product of non constant polynomials.

eg. ① $f(x) = x^2+1$ is an irreducible polynomial in $\mathbb{Z}[x]$

② $f(x) = 2x^2+2$ is an irreducible poly. in $\mathbb{Z}[x]$

But $f(x) = x^2+1$ is not an irreducible poly. in $\mathbb{C}[x]$ where $\mathbb{C}$ is the field of complex numbers.

$$x^2+1 = (x+i)(x-i)$$

4.3.9. Theorem:

(Eisenstein's irreducibility criterion)

Statement:- Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ be a polynomial with integer coefficients. If there is a prime number p such that $p \mid a_0, a_1, \cdots a_{n-1}$ and $p \nmid a_n$ and $p^2 \nmid a_0$ then $f(x)$ is irreducible over $\mathbb{Q}$ ($\mathbb{Q}$: the field of rational numbers)

Ex. Examine the irreducibility of the polynomial $x^3+6x+12$ over $\mathbb{Q}$.

Soln $f(x) = x^3+6x+12$

$= 12 + 6x + x^3$

$a_0 = 12,\ a_1 = 6,\ a_2 = 0,\ a_3 = 1$

$p = 3$ $\quad 3 \mid 12,\ 3 \mid 6,\ 3 \mid 0$ but $3 \nmid 1$

Also $3^2 \nmid 12$

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

Pf. Without loss of generality we can assume $f(x)$ is a primitive polynomial [because if $f(x)$ is not primitive then $f(x) = df_1(x)$ where $f_1(x)$ is a primitive polynomial and d is the content of $f(x)$. This means that if the theorem hold for $f_1(x)$ it holds for $f(x)$.]

Scanned with CamScanner

Let $f(x) = p(x)q(x)$ where $p(x), q(x) \in \mathbb{Q}[x]$ are non constant polynomial.

Then by Gauss lemma, There exist $g(x), h(x) \in \mathbb{Z}[x]$ s.t. $f(x) = g(x)h(x)$

where $p(x) = \frac{a}{b} g(x)$ & $q(x) = \frac{c}{d} h(x)$

for some $a, b, c, d \in \mathbb{Z}'$

Here $g(x)$ and $h(x)$ are non constant polynomials over $\mathbb{Z}$.

Let $g(x) = b_0 + b_1 x + \cdots + b_r x^r$

$h(x) = c_0 + c_1 x + \cdots + c_s x^s$

b's and c's are integers.

Also $r > 0$, $s > 0$

Since $f(x) = g(x)h(x)$, we have

$a_0 = b_0 c_0$ and $a_n = b_r c_s$.

Now $p \mid a_0 \Rightarrow p \mid b_0 c_0 \Rightarrow p \mid b_0$ or $p \mid c_0$

But $p^2 \nmid a_0$, so p can not divide both b_0 & c_0.

Let $p \mid b_0$ and $p \nmid c_0$

$p \nmid a_n \Rightarrow p \nmid b_r c_s \Rightarrow p \nmid b_r$ and $p \nmid c_s$

Let k be the smallest suffix such that $p \nmid b_k$.

Then $k > 0$ and $k \leq r < n$

and $p \mid b_0, b_1, \ldots, b_{k-1}$, $p \nmid b_k$

Now $a_k = \sum_{i+j=k} b_i c_j$

$= b_0 c_k + b_1 c_{k-1} + b_2 c_{k-2} + \cdots + b_{k-1} c_1 + b_k c_0$

Since $p \mid a_k$, $p \mid b_0, b_1, \ldots, b_{k-1}$

we get $p \mid b_k c_0$

But $p \nmid b_k \Rightarrow p \mid c_0$. This is a contradiction

Scanned with CamScanner

This means that $g(x)$ and $h(x)$ both cannot be non constant polynomials.

$\Rightarrow$ $p(x) - r(x)$ can not be non constant polynomial

$\Rightarrow$ either $p(x) = 0$ or $\deg r(x) = 0$

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

Note: $f(x) = g(x)\,h(x)$

iff $f(x+a) = g(x+a)\,h(x+a)$

$f(x)$ is irreducible iff $f(x+a)$ is irreducible.

Ex. Examine the irreducibility of the following polynomials over $\mathbb{Q}$.

(1) $3x^3 + 6x^2 + 2x + 6$

(2) $x^3 + 3x + 2$

Sol. (1) $f(x) = 3x^3 + 6x^2 + 2x + 6$

$= 6 + 2x + 6x^2 + 3x^3$

$a_0 = 6,\ a_1 = 2,\ a_2 = 6,\ a_3 = 3$

$p = 2$, $2 \mid a_0, a_1, a_2$, $2 \nmid a_3$

Also $2^2 = 4 \nmid 6 = a_0$

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

(2) $f(x) = x^3 + 3x + 2 = 2 + 3x + x^3$

Now $x \to x+1$

$f(x+1) = 2 + 3(x+1) + (x+1)^3$

$= 2 + 3x + 3 + x^3 + 3x^2 + 3x + 1$

$= 6 + 6x + 3x^2 + x^3$

$a_0 = 1,\ a_1 = 6,\ a_2 = 3,\ a_3 = 1$

$p = 3$, $3 \mid a_0, a_1, a_2$, $3 \nmid a_3$

Also $3^2 = 9 \nmid a_0$

$\therefore f(x+1)$ is irreducible over $\mathbb{Q}$ $\Rightarrow f(x)$ is irreducible over $\mathbb{Q}$.

Scanned with CamScanner