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

Pf:- Let $f(x)$ be reducible over F. To show $f(x)$ has a zero in F.

Since $f(x)$ is reducible over F so $\exists$ two polynomials $g(x)$ and $h(x)$ in $F[x]$ with degrees less than $f(x)$ such that

$$f(x) = g(x) \cdot h(x).$$

$\Rightarrow \deg f(x) = \deg [g(x) \cdot h(x)]$

$\Rightarrow \deg f(x) = \deg g(x) + \deg h(x)$ [$\because F(x)$ is a field]

Since $\deg f(x) = 2$ or 3, so atleast one of $g(x)$ and $h(x)$ has degree 1, say

$g(x) = ax + b$, $a \neq 0$ — ① Now $a \neq 0$, $a \in F$

$\Rightarrow a^{-1} \in F$. So $-a^{-1}b \in F$.

Putting $x = -a^{-1}b$ in ①, we get

$$g(-a^{-1}b) = a(-a^{-1}b) + b = -(aa^{-1})b + b$$
$$= -b + b = 0$$

$\therefore -a^{-1}b$ is a zero of $g(x)$

Scanned with CamScanner

Now, $f(x) = g(x)\,h(x)$

$\Rightarrow f(-a^{-1}b) = g(-a^{-1}b)\,h(-a^{-1}b)$

$= 0 \cdot h(-a^{-1}b)$

$= 0$

$\therefore -a^{-1}b$ is zero of $f(x)$.

Conversely let $f(x)$ has a zero say a in F. Then $f(a) = 0$, $a \in F$.

$\Rightarrow x - a$ is a factor of $f(x)$

$\Rightarrow \exists\ q(x) \in F[x]$ such that

$f(x) = (x-a)\,q(x)$,

~~$\deg q(x) < \deg$~~

and $\deg f(x) = \deg(x-a) + \deg q(x)$

$\Rightarrow \deg f(x) = 1 + \deg q(x)$

$\Rightarrow \deg q(x) = \deg f(x) - 1 < \deg f(x)$

Thus $f(x)$ is expressible as product of two polynomials in $F[x]$ whose degrees are less than $f(x)$. Hence $f(x)$ is reducible over F.

Scanned with CamScanner

Ex. Show that the polynomial $f(x) = x^4 + 2x^2 + 1$ is reducible over $\mathbb{Q}[x]$.

Sol^n.

$$f(x) = x^4 + 2x^2 + 1$$

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

$$\Rightarrow f(x) = (x^2 + 1)(x^2 + 1)$$

$$= g(x) \cdot h(x)$$

where $g(x) = x^2 + 1 \in \mathbb{Q}[x]$

$h(x) = x^2 + 1 \in \mathbb{Q}[x]$.

And $\deg g(x) = 2 < \deg f(x) = 4$

$\deg h(x) = 2 < \deg f(x) = 4$

Since $\mathbb{Q}$ is a field so $f(x)$ is reducible over $\mathbb{Q}$.

Ex. Let F be a field and let a be a non-zero element of F. Show that

(a) If $a f(x)$ is irreducible over F, prove that $f(x)$ is irreducible over F.

(b) If $f(ax)$ is irreducible over F, prove that $f(x)$ is irreducible over F.

(c) If $f(x+a)$ is irreducible over F, prove that $f(x)$ is irreducible over F.

Scanned with CamScanner

Sol: (a) Let $a f(x)$ be irreducible over F.

To show $f(x)$ is irreducible over F.

Suppose $f(x)$ is reducible over F.

Then $\exists$ two polynomials $g(x)$ and $h(x)$ with degrees less than $f(x)$ such that

$$f(x) = g(x) \cdot h(x)$$

$$\Rightarrow a f(x) = [a g(x)] \cdot h(x)$$

But $\deg [a g(x)] = \deg g(x) < \deg f(x)$

and $\deg h(x) < \deg f(x)$

$\therefore a f(x)$ is reducible over F, which is a contradiction. So $f(x)$ must be irreducible over F. #

HW

(b) Hint: if $f(x) = g(x) h(x)$

Then $f(ax) = g(ax) h(ax)$

(c) Hint: if $f(x) = g(x) h(x)$

Then $f(x+a) = g(x+a) h(x+a)$

Scanned with CamScanner

Definition 4.3.1

Let $f(x) = a_0 + a_1 x + \cdots + a_m x^m$ be a poly. in $Z^*[x]$

[i.e. $a_0, a_1, \ldots, a_m \in Z^*$]

If $\gcd(a_0, a_1, \ldots, a_m) = 1$ then $f(x)$ is called a primitive polynomial.

Eg.

$2 + 3x + 5x^2$ is a primitive poly.

$3 + 6x + 12x^2$ is not a primitive polynomial.

Theorem 4.3.2. ~~If $f(x)$ and $g(x)$ are two primitive polynomials~~

Th^m 4.3.2. If $f(x)$ is a poly. in $Z^*[x]$ Then $f(x)$ can be expressed as $d\,p(x)$ where $d \in Z^*$ and $p(x)$ is a primitive polynomial.

Pf. Let

$f(x) = a_0 + a_1 x + \cdots + a_n x^n$

If $f(x)$ is a primitive polynomial Then there is nothing to prove because

[$f(x) = 1 f(x)$, where $d = 1$]

Suppose $f(x)$ is not primitive polynomial then $\gcd(a_0, a_1, \ldots, a_n) \neq 1$

Let $d = \gcd(a_0, a_1, \ldots, a_n)$

Then $d \mid a_0$, $d \mid a_1$, $\ldots$, $d \mid a_n$

$\Rightarrow a_0 = d b_0$, $a_1 = d b_1$, $\ldots$, $a_n = d b_n$

$b_0, b_1, \ldots, b_n \in Z^*$

$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$

$= d b_0 + (d b_1)x + (d b_2)x^2 + \cdots + (d b_n)x^n$

$= d(b_0 + b_1 x + b_2 x^2 + \cdots + b_n x^n)$

$= d\, P(x)$

where $P(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_n x^n$

(*) $d' \mid b_i \Rightarrow d' \mid d b_i$

$\Rightarrow d' \mid a_i$

and $d \mid a_i$

~~but d is gcd~~ $\Rightarrow d' \mid a_i$

$\Rightarrow dd' \mid a_i$

$d' \mid b_i$

$d \mid a_i = d b_i$

$d' \mid a_i = d b_i$

$\Rightarrow d' \mid d$

$b_i = d' m$

$d \mid a_i \Rightarrow a_i = dn$

$d \mid d'$

$\Rightarrow d = d' n \Rightarrow \frac{m}{n} =$

$d \mid a_i \Rightarrow a_i = dn$

$d' \mid b_i \Rightarrow b_i = d' n$

$\Rightarrow$

$dd' \mid b_i$

$d\, d \mid a_i = d b_i$

$\gcd(b_0, b_1, \ldots, b_n) = 1$ (otherwise it contradicts the fact that $\gcd(a_0, \ldots, a_n) = d$)

Theorem 3.2 : If $f(x)$ and $g(x)$ are two primitive polynomials then $f(x)g(x)$ is also a primitive polynomial.

Pf Let

$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_m x^m$

$g(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_n x^n$

be two primitive polynomials. then $f(x)g(x)$ is also a primitive polynomial.

$\Rightarrow \gcd(a_0, a_1, \cdots a_m) = 1$

and $\gcd(b_0, b_1, \cdots b_n) = 1$

$f(x)g(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{m+n} x^{m+n}$

where $c_k = \sum_{i+j=k} a_i b_j$

Here we have to prove that $f(x)g(x)$ is a primitive polynomial. Here we use the method of contradiction.

Scanned with CamScanner

On the contrary, we assume $f(x)\,g(x)$ is not a primitive polynomial.

$\Rightarrow gcd(c_0, c_1, \ldots c_{m+n}) \neq 1$

Let $d = gcd(c_0, c_1, \ldots c_{m+n})$, $d > 1$

$\therefore d|c_0,\ d|c_1, \ldots d|c_{m+n}$

Since $d > 1$, d has a prime factor p

$\Rightarrow p|c_i \ \forall\ i = 0, \ldots m+n$

$(\because p|d, d|c_i \Rightarrow p|c_i)$

Also $gcd(a_0, a_1, \ldots a_m) = 1$

$\Rightarrow$ **p** can not divide all $a_i\ \forall\ i = 0, \ldots m$

Let t be the smallest suffix such that $p \nmid a_t \quad \forall\ t = 0, \ldots m+n$

i.e., $p|a_0, p|a_1, \ldots p|a_{t-1}, p \nmid a_t$

Similarly u be the smallest suffix, such that $p \nmid b_u$.

Scanned with CamScanner

$\cancel{P \nmid b_u}$ $P \nmid b_u$.

i.e. $P \mid b_0$, $P \mid b_1$, ... $P \mid b_{u-1}$, $P \nmid b_u$

We consider c_{t+u}

$$c_{t+u} = \sum_{i+j=t+u} a_i b_j$$

$$= \underline{a_0 b_{t+u} + a_1 b_{t+u-1} + a_2 b_{t+u-2}} + \cdots$$

$$+ \underline{a_{t-1} b_{u+1}} + a_t b_u + \underline{a_{t+1} b_{u-1}} \cancel{+ a_{t+1}} + \cdots +$$

$$\underline{a_{t+u} b_0}$$

$\Rightarrow P \mid c_{t+u}$, $P \mid a_0$, $P \mid a_1$, ... $P \mid a_{t-1}$, $P \mid b_0$,

... $P \mid b_1$ ... $P \mid b_{u-1}$

Scanned with CamScanner

$\Rightarrow P \mid a_0 b_{t+u} + a_1 b_{t+u-1} + \cdots + a_{t-1} b_{u+1}$

and ~~$P \mid b_{u+t}$~~ a

$P \mid a_{t+1} b_{u-1} + \cdots + a_{t+u} b_0$

Then $P \mid a_t b_u$

$[\ P \mid ab \Rightarrow P \mid a$ or $P \mid b\ ]$.

$\Rightarrow$ eTheir $P \mid a_t$ or $P \mid b_u$

which is a contradiction.

which contradicts our assumption that $P \nmid a_t$, $P \nmid b_u$.

Hence our assumption that $\gcd(c_0, c_1, \cdots, c_{m+n}) = d > 1$ is incorrect.

Then $\gcd(c_0, c_1, \cdots, c_{m+n}) = 1$

$\Rightarrow f(x) g(x)$ is a primitive polynomial.

Scanned with CamScanner