Ex $p(x) = x^4 - 2x^3 + x + 1$ is irreducible

- suppose $p(x) = (x-\alpha)\,q(x)$

$\Rightarrow \alpha \in \mathbb{Z}$ is a zero of $p(x)$

$\alpha \mid 1 \Rightarrow \alpha = \pm 1$

But $p(-1) = 3$, $p(1) = 1$

$\therefore$ No linear factors

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

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

$(a+c) = -2$, $(ac + b + d) = 0$, $(ad + bc) = 1$, $bd = 1$

$\Rightarrow b = d = 1$ or $b = d = -1$

$\Rightarrow b = d$

$ad + bc = b(a+c) = 1$

$\Rightarrow -2b = 1$

$\therefore$ a contradiction

$\therefore$ $p(x)$ is irreducible.

Thm (Eisenstein's Criterion)

Let p be a prime and

$$f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$$

If $p \mid a_i$, $i = 0, \ldots, n-1$ but $p \nmid a_n$ and $p^2 \nmid a_0$ then $f(x)$ is irr. over $\mathbb{Q}$.

Proof: By Gauss Lemma it is sufficient to show that $f(x)$ does not factor over $\mathbb{Z}$.

Suppose

$$f(x) = (b_r x^r + \cdots + b_0)(c_s x^s + \cdots + c_0) \in \mathbb{Z}[x]$$

$b_r \neq 0$, $c_s \neq 0$, $r, s < n$

$p^2 \nmid a_0 = b_0 c_0 \Rightarrow$ Either $p \nmid b_0$ OR $p \nmid c_0$

Assume $p \nmid b_0$, $p \mid c_0$ $(p \mid a_0)$

$p \nmid a_n = b_r c_s$ $\therefore$ $p \nmid b_r$ and $p \nmid c_s$

Let m be the smallest value s.t. $p \nmid c_m$ (know $p \mid c_0$)

$$a_m = b_0 c_m + b_1 c_{m-1} + \cdots + b_m c_0$$

$b_0 c_m$: Not divisible by p; $b_1 c_{m-1} + \cdots + b_m c_0$: all divisible by p

we know (by assumption of thm) $p \mid a_m$ for $m < n$

$\Rightarrow$ $m = n$, $m = s = n$

$$f(x) = b_0 (c_n x^n + \cdots + c_0)$$

$\therefore$ f is irreducible. ∎

Ex] $f(x) = 16x^5 - 9x^4 + 3x^2 + 6x - 21$

is irr. by Eisenstein using $p = 3$

3 divides $9, 3, 6, 21$, $3^2 = 9 + 21$, $3 \nmid 16$.

Ideals in $F[x]$

Let F be a field

$$\langle p(x) \rangle = \{ p(x) q(x) \mid q(x) \in F[x] \}$$

$\langle p(x) \rangle$: Principal ideal

Integral domain where every ideal is principal is called a principal ideal domain

Thm If F is a field then every ideal in $F[x]$ is principal.

Proof: I - ideal of $F[x]$

- $I = \{0\} \Rightarrow I = \langle 0 \rangle$

Suppose I is non-trivial, let $f(x) \in I$ be an element of minimal degree.

- If $\deg(f(x)) = 0 \Rightarrow f(x) = c \in F \Rightarrow 1 \in I$

$\langle c \rangle = \langle 1 \rangle = F[x]$

- Assume $\deg(f) \geq 1$. Let $g(x)$ be any element of I

By the div. alg $\exists$

$$g(x) = f(x) q(x) + r(x) \qquad \deg(r) < \deg(f)$$

($g(x) \in I$, $f(x) q(x) \in I$)

$\Rightarrow r(x) \in I$ but $f(x)$ has minimal degree in I

$\therefore r(x) = 0 \therefore \forall g(x) \in I$ are s.t. $g(x) = f(x) q(x)$

$\therefore \quad I = \langle f(x) \rangle$

Thm Let F be a field and suppose $p(x) \in F[x]$
$I = \langle p(x) \rangle$ is maximal iff $p(x)$ is irreducible.