Let F be a field. A monic polynomial $d(x)$ is a greatest common divisor of $p(x), q(x) \in F[x]$ if $d(x) \mid p(x)$ and $d(x) \mid q(x)$ and if for any other $\hat{d}(x)$ which divides $p, q \Rightarrow \hat{d}(x) \mid d(x)$

$$d(x) = \gcd(p(x), q(x))$$

- $p(x), q(x)$ are relitivley prime if $\gcd(p(x), q(x)) = 1$

17.10

Prop | Let F be a field, $q(x), p(x) \in F[x]$. There exists $r(x), s(x)$ s.t

$$d(x) = \gcd(p(x), q(x)) = r(x)p(x) + s(x)q(x)$$

Further more $\gcd(p(x), q(x))$ is unique.

Proof: very similar to th. 2.10 where $p, q \in \mathbb{Z}$

Remark | we could define an ideal in $F[x]$

$$I = \langle f(x), g(x) \rangle = \{ f(x)r(x) + g(x)s(x) \mid r(x), s(x) \in F[x] \}$$
$$= \langle \gcd(f(x), g(x)) \rangle$$

Irreducible polynomials

A non-constant poly. $f(x) \in F[x]$ is irreducible over a field F if $f(x)$ cannot be expressed

$$f(x) = g(x)\,h(x) \quad \text{with} \quad 0 < \deg(g(x)) < \deg(f)$$
$$0 < \deg(h(x)) < \deg(f)$$

i.e. f is irreducible if ~~f~~ f does not factor (Neglecting constant factors)

Ex| $x^2 - 2 \in \mathbb{Q}[x]$ is irreducible

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

Ex| $p(x) = x^3 + x^2 + 2$ is irreducible over $\mathbb{Z}_3[x]$

If $p(x)$ were reducible By the div. alg $(x-a)$ is a factor for some $a \in \mathbb{Z}_3$

$\mathbb{Z}_3 = \{0, 1, 2\}$

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

for this $a \in \mathbb{Z}_3 \Rightarrow p(a) = 0$

$p(0) = 2$, $p(1) = 1$, $p(2) = 2$

$\therefore$ no elements of $\mathbb{Z}_3$ are roots of $p(x)$

$\therefore$ it has no linear factors.

Lemma| Let $p(x) \in \mathbb{Q}[x]$. Then

$$p(x) = \frac{r}{s}\left(a_0 + a_1 x + \cdots + a_n x^n\right)$$

where $r, s, a_0, \ldots, a_n \in \mathbb{Z}$ and $\gcd(r, s) = 1$, $\gcd(a_0, \ldots, a_n) = 1$.

proof:

Suppose $p(x) = \frac{b_0}{c_0} + \frac{b_1}{c_1}x + \cdots + \frac{b_n}{c_n}x^n$

Take common denom. $p(x) = \frac{1}{c_0 \cdots c_n}(d_0 + d_1 x + \cdots + d_n x^n)$

$d_i \in \mathbb{Z}$

set $d = \gcd(d_0, \ldots, d_n)$, set $a_i = \frac{d_i}{d} \in \mathbb{Z}$

then $\gcd(a_0, \ldots, a_n) = 1$

$$p(x) = \frac{d}{c_0 \cdots c_n}(a_0 + a_1 x + \cdots + a_n x^n)$$

let $\frac{r}{s}$ be $\frac{d}{c_0 \cdots c_n}$ in lowest terms. $\blacksquare$

Theorem (Gauss's Lemma) Let $p(x) \in \mathbb{Z}[x]$, monic

suppose $p(x) = \alpha(x)\beta(x) \in \mathbb{Q}[x]$ with $\deg(\alpha(x)) < \deg(p(x))$
$\deg(\beta) < \deg(p)$

Then $p(x) = a(x)\,b(x)$ where $a, b \in \mathbb{Z}[x]$ and are monic with $\deg(\alpha) = \deg(a)$, $\deg(\beta) = \deg(b)$.

Simple ver: factoring in $\mathbb{Z}[x]$ is equivalent to factoring in $\mathbb{Q}[x]$.

Proof: By last Lemma may assume

$$\alpha(x) = \frac{c_1}{d_1}(a_0 + a_1 x + \cdots + a_m x^m) = \frac{c_1}{d_1}\alpha_1(x)$$

$$\beta(x) = \frac{c_2}{d_2}(b_0 + b_1 x + \cdots + b_n x^n) = \frac{c_2}{d_2}\beta_2(x)$$

$$\gcd(a_0, \ldots, a_m) = \gcd(b_0, \ldots, b_n) = 1$$

$$p(x) = \alpha(x)\,\beta(x) = \frac{c_1c_2}{d_1d_2}\,\alpha_1(x)\,\beta_1(x) = \frac{c}{d}\,\alpha_1(x)\,\beta_1(x)$$

$$\therefore \quad d\,p(x) = c\,\alpha_1(x)\,\beta_1(x)$$

Case $d=1$: Since $p(x)$ is monic $\Rightarrow$ $c\,a_m b_n = 1$ and, $a_m, b_n, c \in \mathbb{Z}$

$c=1 \Rightarrow c = 1 = a_m = b_m$

$\Downarrow$

$c = d = a_m = b_m = 1$ hence $\alpha_1 \cdot \beta_1 = p(x)$ monic, in $\mathbb{Z}[x]$

or $c = 1$ and $a_m = b_n = -1$

$c = d = 1$, $p(x) = \underbrace{(-\alpha_1(x))}_{\text{monic}}\underbrace{(-\beta_1(x))}_{\text{in } \mathbb{Z}[x]}$

$c=-1$ similar...

look for contradiction

Suppose $d \neq 1$, $\gcd(c,d) = 1$

since $\gcd(a_1, \dots, a_n) = 1$, etc.

$\Rightarrow \exists$ a prime q s.t. $q \mid d$, and $q \nmid c$

and $\exists$ some a_i s.t $q \nmid a_i$, some b_i s.t. $q \nmid b_i$

Let $\overline{\alpha_1(x)} \in \mathbb{Z}_q[x]$, $\overline{\beta_1(x)} \in \mathbb{Z}_q[x]$

Since $q \mid d$ and $\underset{\substack{\parallel \\ 0}}{d \cdot p(x)} = c\,\alpha_1\,\beta_1 = 0$ in $\mathbb{Z}_q[x]$

$$\therefore \quad \overline{\alpha_1(x)} \cdot \overline{\beta_1(x)} = 0 \quad \text{in } \mathbb{Z}_q[x]$$

but since $q \nmid a_i$ and $q \nmid b_i$ $\Rightarrow \overline{\alpha_1(x)} \neq 0$, $\overline{\beta_1(x)} \neq 0$

But $\mathbb{Z}_q[x]$ is an integral domain (since $\mathbb{Z}_q$ is a field)

$\therefore$ this is a contradiction.

$\therefore$ $d = 1$ ∎

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

Proof: Let $\beta \in \mathbb{Q}$ s.t. $p(\beta) = 0 \Rightarrow p(x)$ has a linear factor $x - \beta \in \mathbb{Q}[x]$. By Gauss's Lemma

since $p(x) = (x-\beta)\, q(x)$ in $\mathbb{Q}[x]$

$$\Rightarrow \quad p(x) = (x-\beta)\left(x^{n-1} + \cdots - \frac{a_0}{\beta}\right) \in \mathbb{Z}[x]$$

$\therefore$ $\beta \in \mathbb{Z}$ and $\alpha = \beta$ and $\alpha \mid a_0$. ∎

Ex $p(x) = x^4 - 2x^3 + x + 1$ is irreducible in $\mathbb{Q}[x]$

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

$\Rightarrow$ $\alpha \in \mathbb{Z}$ is a zero of $p(x)$ and $\alpha \mid 1$

$\Rightarrow$ $\alpha = \pm 1$, But $p(1) = 1$, $p(-1) = 3$

$\therefore$ $p(x)$ has no linear factors.

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

$$= x^4 + \underset{-2}{\underset{\shortparallel}{(a+c)}}\,x^3 + \underset{0}{\underset{\shortparallel}{(ac+b+d)}}\,x^2 + \underset{1}{\underset{\shortparallel}{(ad+bc)}}\,x + \underset{1}{\underset{\shortparallel}{bd}}$$

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

$$\Rightarrow \quad b = d$$

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

$$\Rightarrow \quad -2b = 1$$

This is a contradiction of Guass's lemma ($b \in \mathbb{Z}$).

$\therefore$ p is irreducible

Thm (Eisensenstern'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 is irreducible in $\mathbb{Q}[x]$.

Proof: By Guasses lemma it is sufficent to show irr. in $\mathbb{Z}[x]$.

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

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

$p^2 \nmid a_0 = b_0 c_0 \quad \therefore$ Either $p \nmid b_0$ or $p \nmid c_0$.

Assume $\quad p \nmid b_0, \quad p \mid c_0$

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

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

$$a_m = \underbrace{b_0 c_m}_{\text{Not divisible by } p} + \overbrace{\underbrace{b_1 c_{m-1} + \cdots + b_m c_0}_{\text{all divisible by } p}}^{\text{by expansion}}$$

$\therefore \quad p \nmid a_m$

By assumtion of Thm. $p \mid a_m$ for $m < n$

$\Rightarrow \quad m = s = n$

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

$\therefore$ f is irreducible. ∎

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

is irr by Eisenstein with $p = 3$

since 3 divides $9, 3, 6, 21$, $3^2 = 9 \nmid 21$

$3 \nmid 16$

Ideals in $F[x]$

Let R be an ~~integral domain~~ ring, an ideal I is called principal

if $I = \langle f \rangle = \{ f \cdot r \mid \forall r \in R \}$

An Integral domain where every ideal is principal is called is called a principle ideal domain.

Thm] Let F be a field. Every ideal I in $F[x]$ is principal, i.e. $F[x]$ is a principal ideal domain.

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

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

Suppose I is a non-trivial ideal, let $f(x) \in I$ be a nonzero poly. in I of minimal degree.

If $\deg(f(x)) = 0 \Rightarrow f(x) = c \in F[x]$, $c \in F$

$\therefore 1 \in I \therefore I = \langle c \rangle = \langle 1 \rangle = F[x]$

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

By the div. alg. $\exists\, q, r$ s.t

$$\underbrace{g(x)}_{\in I} = \overbrace{f(x)\,q(x)}^{\in I} + r(x) \quad , \deg(r) < \deg(f)$$

$\therefore r(x) \in I$

$\Rightarrow$

but $f(x)$ has minimal degree in I.

$\therefore r(x) = 0 \quad \therefore \forall\, g(x) \in I \quad g(x) = f(x)\,q(x)$

$\therefore I = \langle f(x) \rangle$. $\blacksquare$