Midterm = April 8 $\Rightarrow$ covers Chapter 16, 17

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

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

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

Proof: very similar to proof for $p, q \in \mathbb{Z}$.
th 17.10, 2.10

Irreducible Polynomials

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

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

i.e. f irreducible iff f does not factor.

↑ like prime numbers for poly. ring.

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 $\mathbb{Z}_3[x]$

Suppose $p(x)$ were reducible over $\mathbb{Z}_3[x]$

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

$\therefore \quad p(x) = (x-a)\,q(x)$ $\qquad \mathbb{Z}_3 = \{0,1,2\}$

for this a $\quad p(a) = 0$

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

$\therefore$ $p(x)$ is irreducible since $0, 1, 2$ are not roots.

<u>Lemma</u> 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 $\gcd(r,s) = 1$, $\gcd(a_0, \ldots, a_n) = 1$.

<u>proof:</u>

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

rewrite

$$p(x) = \frac{1}{c_0 \cdots c_n}\left(d_0 + \cdots + d_n x^n\right)$$

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

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

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

writing $\frac{d}{c_0 \cdots c_n}$ in lowest terms as $\frac{r}{s}$ this gives

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

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

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

Then $p(x) = a(x)\, b(x)$ where a, b are <u>monic</u> polynomials in $\mathbb{Z}[x]$ with $\deg(\alpha(x)) = \deg(a(x))$
$\deg(\beta(x)) = \deg(b(x))$

simple version: If poly in $\mathbb{Z}[x]$ factors in $\mathbb{Q}[x]$ it also factors in $\mathbb{Z}[x]$.

<u>Proof:</u> By last lemma may assume

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

$$\beta(x) = \frac{c_2}{d_2}(b_0 + b_1 x + \cdots + b_n x^n) = \frac{c_2}{d_2}\beta_1(x)$$

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

$$p(x) = \alpha(x)\beta(x) = \frac{c_1 c_2}{d_1 d_2}\alpha_1(x)\beta_1(x) = \frac{c}{d}\alpha_1(x)\beta_1(x)$$

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

Case $d = 1$, since $p(x)$ is monic $\Rightarrow c\, a_m b_n = 1$

$c, a_m, b_n \in \mathbb{Z} \Rightarrow c = 1$ or $c = -1$
$\hookrightarrow a_m = b_n = 1 \longrightarrow p(x) = \alpha_1(x)\beta_1(x)$ monic

& $a_m = b_n = -1 \Rightarrow p(x)\ (\underbrace{-\alpha_1(x)}_{\text{monic}})(-\beta_1(x))$

$c = -1$ similar

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

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

and also $\exists$ some a_i s.t. $q \nmid a_i$, and 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 $q \mid d \Rightarrow \overline{\alpha_1(x)} \cdot \overline{\beta_1(x)} = 0$ in $\mathbb{Z}_q[x]$.

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

$\overline{\beta_1(x)} \neq 0$ $\mathbb{Z}_q[x]$

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

$\therefore$ this is a contradiction $\therefore$ $d = 1$. ∎

Corol Let $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$, $a_0 \neq 0$

If $p(x)$ has a zero in $\mathbb{Q}$ then $p(x)$ also has a zero $\alpha \in \mathbb{Z}$. Furthermore $\alpha \mid a_0$.

Proof:

Let $a \in \mathbb{Q}$ s.t. $p(a) = 0 \Rightarrow p(x)$ a liner factor $x - a$

By Gauss's Lemma since $p(x) = (x - a)q(x)$ in $\mathbb{Q}[x]$

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

$\therefore$ $\alpha \mid a_0$. ∎