MATH 403/503 L23

Polynomials. (Judson §17)

$\mathbb{F}$ field, $\mathbb{F}[x] = \left\{ \sum_{k=0}^{n} c_k x^k \mid \substack{c_k \in \mathbb{F} \\ n \geq 0} \right\}$ the ring of polynomials in x over $\mathbb{F}$.

$\mathbb{F}[x]$ is a comm ring, in fact an integral domain.

Theorem (Division Algorithm)

Let $f(x), g(x) \in \mathbb{F}[x]$, $g(x) \neq 0$.
Then there is a unique pair $(q(x), r(x))$ of poly's s.t.

$$f(x) = g(x) \cdot q(x) + r(x)$$

and $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

Proof: Long division. (See Judson §17.2)

Def i) $f \mid g \iff \exists h : fh = g$

ii) The gcd of f, g is a pol d s.t. a) $d \mid f$, $d \mid g$
b) $e \mid f, e \mid g \Rightarrow e \mid d$

The gcd exists for any f, g and is unique up to nonzero scalar. Usually we pick the monic gcd.

Proposition (§17.10 Judson) (Bezout's Thm)
If d is the gcd of $f, g \in \mathbb{F}[x]$
then $d = af + bg$
for some $a, b \in \mathbb{F}[x]$.

Remark
Using that if

$$f = gq + r$$

then $\gcd(f,g) = \gcd(g,r)$
we can find d, a, b above
(Euclid's Algorithm).

§17.3 Irreducible poly's

Thm If $f \in \mathbb{F}[x]$ has degree 2 or 3 then TFAE

i) f is irreducible

ii) $f(\alpha) \neq 0 \quad \forall \alpha \in \mathbb{F}$.

Proof f reducible $\iff f = ab$ where a, b are nonconstant. Then

$\{2,3\} \ni \deg f = \underbrace{\deg a}_{\geq 1} + \underbrace{\deg b}_{\geq 1}$

So a or b must have degree 1.

So f reducible $\iff f$ has a linear factor

$\iff f$ has a root $\alpha \in \mathbb{F}$.

(factor thm)

∎

If $R \subseteq S$ are comm rings and $f(x) \in R[x]$, sometimes $f(x)$ can be factored in $S[x]$ but not in $R[x]$.

Ex x^2+1 is irreducible in $\mathbb{R}[x]$ but is reducible in $\mathbb{C}[x]$:

$$x^2+1 = \underbrace{(x+i)}_{\in \mathbb{C}[x]}(x-i)$$

We often say "over R" instead of "in $R[x]$", and abbreviate this with "$/R$":

- x^2+1 is irr$/\mathbb{R}$ and irr$/\mathbb{R}$ but red$/\mathbb{C}$
- x^3+2 is irr$/\mathbb{Z}$

$f(x) = x^2+3x+2$ is red$/\mathbb{Z}$ since

$$f(x) = (x+1)\underbrace{(x+2)}_{\in \mathbb{Z}[x]}.$$

Gauss Lemma

Thm If a monic pol $f(x) \in \mathbb{Z}[x]$ can be factored over $\mathbb{Q}$:

$$f(x) = a(x)\, b(x)$$

$a, b \in \mathbb{Q}[x]$ nonconstant, then there is a nonzero $k \in \mathbb{Q}$ such that $k \cdot a(x)$, $\frac{1}{k} b(x)$ are monic pol's in $\mathbb{Z}[x]$

Proof Suppose $f(x)$ is red/$\mathbb{Q}$.

That means

$\mathbb{Z}[x] \ni f(x) = a(x)\,b(x)$, where $a(x) \in \mathbb{Q}[x]$, $b(x) \in \mathbb{Q}[x]$. are nonconstant.

By factoring out lcm of denominators, can write

$$a(x) = \frac{s}{t}(a_0 + a_1 x + \cdots + a_m x^m) = \frac{s}{t}\tilde{a}(x)$$

$$b(x) = \frac{u}{v}(b_0 + b_1 x + \cdots + b_n x^n) = \frac{u}{v}\tilde{b}(x)$$

where $s, t, u, v, a_i, b_i \in \mathbb{Z}$ and $\{s, t\}$ relatively prime, as is $\{a_0, \ldots, a_m\}$, $\{u, v\}$, $\{b_0, \ldots, b_n\}$.

So $f(x) = \frac{su}{tv}\tilde{a}(x)\tilde{b}(x)$,

Canceling common factors,

$$\frac{su}{tv} = \frac{c}{d} \quad \text{where } c, d \in \mathbb{Z},\ \gcd(c,d) = 1.$$

If $d = 1$, then $f(x) = c\,\tilde{a}(x)\cdot\tilde{b}(x)$ shows $f(x)$ is reducible over $\mathbb{Z}$.

If $d \neq 1$, there exists a prime p dividing d but not c.

Also (since $n, m \geq 1$) $\exists i : p \nmid a_i$ and $\exists j : p \nmid b_j$

Let $a'(x)$, $b'(x)$ be the polys in $\mathbb{Z}_p[x]$ obtained by reducing coeffs of $\tilde{a}(x)$, $\tilde{b}(x)$ mod p. Then, since $p \mid d$,

$$\underbrace{a'(x)}_{\neq 0}\,\underbrace{b'(x)}_{\neq 0} = 0 \quad \text{in } \mathbb{Z}_p[x]$$

contradicting $\mathbb{Z}_p[x]$ is an integral domain.

∎

Corollary

If $p(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$ is a monic pol in $\mathbb{Z}[x]$ and if $p(x)$ has a rational root ~~$\alpha \in \mathbb{Q}$~~, then $p(x)$ has an integer root $\alpha \in \mathbb{Z}$.

Furthermore $\alpha \mid a_0$.

Proof If $p(\lambda) = 0$ for some $\lambda \in \mathbb{Q}$ then $(x - \lambda) \mid p(x)$ in $\mathbb{Q}[x]$ so $p(x)$ is red/$\mathbb{Q}$.

By Gauss Lemma, ~~$p(x)$ is red.~~

$\lambda \in \mathbb{Z}$. Lastly

$(x-\lambda)q(x) = p(x) \Rightarrow \lambda \mid a_0$ ∎

Eisenstein's Criterion

Let $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$

Suppose $\exists$ a prime number p such that

i) $p \mid a_0, p \mid a_1, \ldots, p \mid a_{n-1}$

ii) $p^2 \nmid a_0$

iii) $p \nmid a_n$

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

Proof By Gauss' Lemma, it suffices to show $f(x)$ is irreducible over $\mathbb{Z}$.

Suppose

$$f(x) = (b_r x^r + \cdots + b_1 x + b_0)(c_s x^s + \cdots + c_1 x + c_0)$$

where $b_i, c_i \in \mathbb{Z}$, $b_r \neq 0, c_s \neq 0$, and $r < n, s < n$. Since $p^2 \nmid a_0$ but $p \mid a_0$, WLOG $p \nmid b_0$, $p \mid c_0$.

Since $p \nmid a_n$, we have $p \nmid b_r, p \nmid c$

Let $m > 0$ be smallest integer s.t. $p \nmid c_m$

Then, equating coeffs of x^m we have

$$a_m = \underbrace{b_0 c_m}_{\text{not divisible by } p} + \underbrace{b_1 c_{m-1} + \cdots + b_m c_0}_{\text{divisible by } p}$$

This contradicts that $p \mid a_m$, (unless $m = n$ but that's impossible since $s < n$). ∎

Example $f(x) = 16x^5 - 9x^4 + 3x^2 + 6x - 21$ is irreducible over $\mathbb{Q}$ by Eisenstein with $p = 3$. Therefore $\frac{\mathbb{Q}[x]}{(f(x))}$ is a field.

Example $g(x) = x^3 + 3x + 2$

Cannot apply Eisenstein directly.

Trick: Consider

$h(x) = g(x+1) = (x+1)^3 + 3x + 2 = x^3 + 3x^2 + 6x + 6$

$h(x)$ is irr/$\mathbb{Q}$ by Eisenstein with $p = 3$

Therefore $g(x)$ is also irreducible/$\mathbb{Q}$.