Lecture 5

February 6, 2008
6:12 PM

Thm: If F is a field, $f, g \in F[x]$, $g \neq 0$, then there are unique $q, r \in F[x]$ s.t. $f = gq + r$ and $\deg r < \deg g$

Ex: $f = x^5 - 2$ $\quad g = x^2 - x - 1$

$$\begin{array}{r|l} x^5 + 0x^4 + 0x^3 + 0x^2 + 0x - 2 & x^2 - x - 1 \\ \hline x^5 - x^4 - x^3 & x^3 + x^2 + 2x + 3 = q \\ \hline \quad x^4 + x^3 & \\ \quad x^4 - x^3 - x^2 & \\ \hline \quad 2x^3 + x^2 & \\ \quad 2x^3 - 2x^2 - 2x & \\ \hline \quad 3x^2 + 2x - 2 & \\ \quad 3x^2 - 3x - 3 & \\ \hline \quad 5x + 1 = r & \end{array}$$

Cor: $f \in F[x]$, then $f(a)$ is the remainder for $f / x - a$

Pf: $f = q(x-a) + r$ Subst. $x = a$

But $\deg r < \deg (x-a)$

$\Rightarrow \deg r = 0 \Rightarrow r =$ constant, so $r = f(a)$.

$f(a) = q(a)(a-a) + r$

$f(a) = r$

Cor: a is a root of $f \in F[x]$ (i.e. $f(a) = 0$) iff $x - a$ divides f with no remainder

$(x - a \mid f)$

a is a root $\Leftrightarrow x - a \mid f$

Pf: $f(a)$ is the remainder

$\quad \| \qquad\qquad \|$

$0 \quad \Leftrightarrow \quad 0$

Def: We say that a is a root of multiplicity k

Def: We say that a is a root of order k (multiplicity) of $f \in F[x]$ if

$$(x-a)^k \mid f \quad \& \quad (x-a)^{k+1} \nmid f$$

ex: consider $f = x^3 + x^2 - x - 1$
$= (x+1)^2(x-1)$

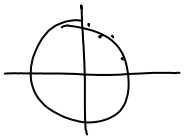
roots: 1 $(x+1)^k \mid f$
-1 $(x-1)^k$

	1	-1	-1
1	1	2	1	0
-1	1	1	0
	-1	1	0

Thm: A $\neq 0$ polynomial $f \in F[x]$ with $\deg f = n$ has at most n roots counting with multiplicities.

Ex1: Consider $x^{27} - 1 = 0$
in $\mathbb{R}[x]$, one root, $x = 1$
multiplicity: $(x-1)^2 \nmid x^{27} - 1$
$\Rightarrow$ mult. is 1
in $\mathbb{C}[x]$, has 27 roots

$$x_j = e^{\frac{2\pi i \cdot j}{27}}$$



Ex2: $x^2 + 3x + 2$ over $\mathbb{Z}/6[x]$
0 ✗ 2 ✓ 4 ✓
1 ✓ 3 ✗ 5 ✓
$\deg = 2$, 4 roots.
But $\mathbb{Z}/6[x]$ is not a field

Pf: By induction on $\deg f$.
if $\deg f = 1$, $f = ax + b$
Assume Thm is true for poly's of deg $< n$
Assume $\deg f = n$
If f has no roots, nothing to check
Otherwise, assume a is a root of mult. k
So $(x-a)^k \mid f$, but $(x-a)^{k+1} \nmid f$
So $f = (x-a)^k g$, but $(x-a) \nmid g$
$\Rightarrow \deg g = n - k$, g has at most $n-k$ roots (by induction)
Thus f has those $n-k$ roots plus a with mult. k, so f has at most $n - k + k = n$ roots.

Exercise for $\uparrow$: if b is a root of g, its

multiplicity as a root of g is the same as its order as a root of f.

Def: An ideal is called principal if it is generated by a single element.
$A \subset R$ is an ideal if $A = \langle a \rangle = aR$

Def: A domain is called a principal ideal domain (PID) if every ideal in it is principal.

Thm: $F[x]$ is a PID.; if $A \subset F[x]$ is a nonzero ideal in $F[x]$, then A is generated by any non-zero polynomial in A which has a minimal degree within A.

Application: Consider $\varphi : \mathbb{R}[x] \to \mathbb{C}$ defined by $f \longmapsto f(i) \in \mathbb{C}$ by the FIT.

$\mathbb{R}[x]/\ker\varphi \cong \operatorname{im}\varphi \subset \mathbb{C} \Rightarrow = \mathbb{C}$

$bx + a \to bi + a$

$\ker\varphi$ is an ideal in $\mathbb{R}[x]$
by thm, generated by any (non-zero) minimal degree poly in it.
Constants do not "kill" i.
linears ——— " ———

$bx + a \xrightarrow{\varphi} a + ib = 0$ iff $a, b = 0$

But $x^2 + 1 \in \ker\varphi$
So $x^2 + 1$ is of min-deg, so $\ker\varphi = \langle x^2 + 1 \rangle$

Ex: $\mathbb{Z}[x] = \langle 2, x \rangle$ not PID
Ex2: $R = F[x, y]$

Pf of Thm: Let $A \subset F[x]$ be an ideal, let $f \neq 0$ be a min. deg. poly. in A
Claim: $A = \langle f \rangle$
$\langle f \rangle \subset A$ obvious
Take $g \in A$, want to show it is a mult. of f.
Consider g/f. Find q, r s.t. $g = f \cdot q + r$, $\deg r < \deg f$

$\Leftrightarrow r = g - f \cdot q \in A \Rightarrow r \in A$. So $r = 0$, $g = f \cdot q$
($g \in A$, $f \cdot q \in A$)
$\Rightarrow g \in \langle f \rangle$

Def: A unit in a ring R is an invertible

Def: A unit in a ring R is an invertible element.

Ex: 1. In $F[x]$, the units are the non-zero constants.
2. In $\mathbb{Z}[x]$ the units are

Def: A non-zero, non-unit poly $f \in D[x]$ is "reducible" if $f = gh$ for some nonunits g & $h \in D[x]$. If f is $\neq 0$ and not reducible we say it is irreducible.

Ex: $2x^2+4$ is irred. in $\mathbb{Q}[x]$
(otherwise $2x^2+4 =$ linear $\cdot$ linear)
(linear: has root; linear: has root)

But $2x^2+4$ has no roots over $\mathbb{Q}$

Lemma: If $f \in F[x]$, $\deg f = 2$ or 3, then f is red. iff f has a root

Pf: $f = gh$ $\deg g = 1$ or $\deg h = 2$ or opposite

g is linear, so has root. So f has root
On the other hand, if f has a root a, then $(x-a) \mid f$. So f is red.

Only works for deg 2, 3.

Back to example: $2x^2+4$ is red. in $\mathbb{Z}[x]$ (2 is unit in $\mathbb{R}$, not in $\mathbb{Z}$)
$2x^2+4 = 2(x^2+2)$
irred in $\mathbb{R}[x]$
red. in $\mathbb{C}[x]$

Ex: x^2-2 irred. in $\mathbb{Q}[x]$
red. in $\mathbb{R}[x]$
x^2+1 irred. over $\mathbb{Z}/3$
red. over $\mathbb{Z}/5$
$x^2+1 = (2x+1)(3x+1)$ in $\mathbb{Z}/5[x]$
$= (x-2)(x-3)$
$= (x+3)(x+2)$

$= (x+3)(x+2)$

Thm: Let $f \in \mathbb{Z}[x]$. If it is reducible in $\mathbb{Q}[x]$, then it is reducible in $\mathbb{Z}[x]$ (alt, if f is irred. in $\mathbb{Z}[x]$, it is irred over $\mathbb{Q}[x]$)

consider: $x^5 - 3x + 6 = (-x^3 + -x^2 + \ldots)(-x^2 + \ldots)$
$= (\ldots 2)(\ldots 3)$
$(\ldots 6)(\ldots 1)$

irred. over $\mathbb{Z}[x]$ $\Rightarrow$ irred. over $\mathbb{Q}[x]$

Consider $6x^2 + x - 2 = (3x - \frac{3}{2})(2x + \frac{4}{3})$

$= (2x-1)(3x+2)$

Def: $f \in \mathbb{Z}[x]$ is called "primitive" if the greatest common factor of its coefficients is 1. That is if no prime divides all of its coeffs.

Ex: $30x^2 + 8x + 9$

Claim: The product of two primitive polys is primitive.

Proof: Assume $f = g \cdot h$ isn't primitive, i.e. some prime p divides all coeffs of f.

$\varphi : R \to S$
$\downarrow$
$\varphi : R[x] \to S[x]$
$\sum a_i x^i \to \sum \varphi(a_i) x^i$

Use this with $\varphi : \mathbb{Z} \to \mathbb{Z}/p$

$f = g \cdot h$ $\quad \bar{f} = \varphi(f)$
$\downarrow$ $\quad \bar{g} = \varphi(g)$
$\bar{f} = \bar{g} \cdot \bar{h}$ $\quad \bar{h} = \varphi(h)$

$\Rightarrow \bar{g} = 0$ or $\bar{h} = 0$

But if $\bar{g} = 0 \Rightarrow$ all coeffs. of g are div. by p. So g isn't primitive. Done (shown the contrapositive).

Prop/def2 Let $f \in \mathbb{Q}[x]$. Then there is a unique positive constant $c \in \mathbb{Q}$ s.t. f/c is primitive.

("c is the content of f" and denoted $c(f)$)
($f = c(f)\cdot f'$, f' is primitive)

Prop 3: $c(fg) = c(f)c(g)$

Proof of Thm: Assume $f = gh$ in $\mathbb{Q}[x]$; wlog, $c(f) = 1$ (f is primitive)

So write $f = c(g)g' \cdot c(h)h' = c(g)c(h)g'h'$

(g' primitive, h' primitive, $\mathbb{Z}[x]$)

$= c(gh)gh' = c(f)g'h'$

$= g'h'$

Pf of 2: If $f = \sum \frac{a_i}{b_i} = \frac{1}{\pi b_i} \sum c_i x^i = \frac{\text{common factors of } c_i\text{'s}}{b_i}$

$\to \sum d_i x^i$

primitive

Assume $f = c_1 f_1 = c_2 f_2$ where $c_1 = \frac{a_1}{b_1}$, $c_2 = \frac{a_2}{b_2}$

$a_1, a_2, b_1, b_2 \in \mathbb{Z}_+$, f_1 & f_2 are primitive.

$\Rightarrow \frac{a_1}{b_1} f_1 = \frac{a_2}{b_2} f_2 \Rightarrow b_2 a_1 f_1 = b_1 a_2 f_2$

Claim $b_2 a_1 \mid b_1 a_2$, $b_1 a_2 \mid b_2 a_1$

Assume $p^k \mid b_2 a_1$ $\quad$ p prime, $k \geq 1 \in \mathbb{Z}$

$\Rightarrow p^k \mid$ all coeff. of $b_1 a_2 f_2 \Rightarrow$ must div. $b_1 a_2$

By primitivity of f_2, $p^k \mid b_1 a_2$

$\Rightarrow b_2 a_1 \mid b_1 a_2$

Likewise $b_1 a_2 \mid b_2 a_1$. Hence they are equal.

$\Rightarrow \frac{a_1}{b_1} = \frac{a_2}{b_2} \Rightarrow c_1 = c_2$ ∎

Proof of 3: $h = fg$ $\quad$ $h = c(h)\cdot h_1$, h_1 prim.
$f = c(f)\cdot f_1$, f_1 —"—
$g = c(g)\cdot g_1$, g_1 —"—

$c(h)\cdot h_1 = h = f\cdot g = c(f)c(g) f_1 g_1$

$$c(h)\cdot h_1 = h = f\cdot g = c(f)c(g)\, f_1 g_1$$

(h_1: prim; $f_1 g_1$: prim.)

$$\Downarrow$$

$$c(h) = c(f)c(g)$$

∎