Lecture 4

January 30, 2008
6:12 PM

Annoying properties

$\varphi: R \to S$ a hom., $A \subset R$ subring, $B \subset S$ ideal

1. $\varphi(nr) = n\varphi(r)$
   $\varphi(r^n) = \varphi(r)^n$
2. $\varphi(A)$ is a subring, and so is $\varphi(R) = \operatorname{im}\varphi$
3. If A is an ideal and φ is onto, then $\varphi(A)$ is an ideal
4. $\varphi^{-1}(B) = \{r \in R : \varphi(r) \in B\}$ is an ideal if B is an ideal. In particular, $\varphi^{-1}(\{0\}) = \ker\varphi$ is an ideal.

Ex: Let $f(x) = x^2$ f^{-1} does not make sense on $\mathbb{R}$.

$$f^{-1}(\{4\}) = \{2, -2\}, \quad f^{-1}(\{-4\}) = \emptyset$$

Proof: Assume $a \in \varphi^{-1}(B)$, i.e. $\varphi(a) \in B$. Assume $r \in R$. Does $ra \in \varphi^{-1}(B)$?

Indeed, $\varphi(ra) = \underbrace{\varphi(r)}_{\in S}\underbrace{\varphi(a)}_{\in B} \Rightarrow \varphi(ra) \in B$ (B is an ideal)

$\Rightarrow ra \in \varphi^{-1}(B)$

5. If R is commutative, $\varphi(R)$ is too.
6. Suppose R has a unity and φ is onto, then S has a unity, $\varphi(1)$.
7. If $\ker\varphi = \{0\}$, then φ is 1-1,
8. if also $\operatorname{im}\varphi = S$, then φ is an isomorphism.

Proof: Assume $\varphi(a) = \varphi(b)$. Then $\varphi(a) - \varphi(b) = 0$
$\Rightarrow \varphi(a-b) = 0 \Rightarrow a - b = 0 \Rightarrow a = b \Rightarrow$ 1-1

Thm: Every ideal $A \subset R$ is the kernel of some homomorphism.

homomorphism.

Proof: Given A, consider $\pi : R \to R/A$ defined by $\pi(r) = [r]$. (easy to check that this is a hom.)

$[r]$ = all $r' \in R$ s.t $r' \sim r$ i.e $r' - r \in A$

$$\ker \pi = \{r : [r] = [0]\}$$
$$= \{r : r - 0 \in A\} = \{r : r \in A\}$$
$$= A$$

In general, if $\varphi : R \to S$ is a hom., then

$$R/\ker\varphi \underset{\text{isom.}}{\cong} \varphi(R) = \operatorname{im}\varphi$$

Analogy 1: Rank-nullity thm of vector spaces.

$T : V \to W$

$$\dim V = \underbrace{\text{nullity}\, T}_{\dim\ker T} + \underbrace{\text{rank}\, T}_{\dim \operatorname{im} T}$$

$$\dim V - \dim\ker T = \dim\operatorname{im} T$$

Proof: Let $\psi : R/\ker\varphi \to \operatorname{im}\varphi$ defined

$$\psi[r] \longrightarrow \varphi(r)$$

1. well-defined $[r] = [r'] \Rightarrow \varphi(r) = \varphi(r')$

$\Updownarrow$ $\Updownarrow$

$r - r' \in \ker\varphi \Leftrightarrow \varphi(r - r') = 0$

2. $\operatorname{im}\psi = \operatorname{im}\varphi$ ✓

3. ψ is 1-1 checked

3. ψ is 1-1 ——— checked
4. ψ is a hom.

$$\psi([r]+[r']) = \psi([r+r']) = \varphi(r+r')$$

$$\psi([r])+\psi([r']) = \varphi(r)+\varphi(r')$$

but $\varphi(r+r') = \varphi(r)+\varphi(r')$ by the fact that φ is a homomorphism.

Ex: if R has a unity 1, then $\varphi: \mathbb{Z} \to R$ by $n \mapsto n\cdot 1$ is a hom! Therefore, if char$R = n$, ($n\cdot 1 = 0$, $k\cdot 1 \neq 0$ if $k<n$) then $\ker\varphi = n\mathbb{Z}$
(indeed $n \in \ker\varphi$, therefore $n\mathbb{Z} \subset \ker\varphi$)
Suppose $l \in \ker\varphi$. Then write $l = nq + r$ with $0 \le r < n$ and then

$$\begin{aligned} 0 = l\cdot 1 = (nq+r)\cdot 1 &= q\cdot n\cdot 1 + r\cdot 1 \\ &= 0 + r\cdot 1 \\ &= r \end{aligned}$$

$\Rightarrow r = 0 \Rightarrow l = nq$ so $l \in n\mathbb{Z}$

$\Rightarrow \mathbb{Z}/\ker\varphi \cong \operatorname{im}\varphi$

$\Rightarrow \mathbb{Z}/n\mathbb{Z} \cong \operatorname{im}\varphi$ a subring of R

Cor: Every ring of char n contains a subring which is isomorphic to $\mathbb{Z}/n\mathbb{Z}$

Cor: if char$R = 0$, R contains $\mathbb{Z}$.

Likewise for fields, if char$F = p$, $F \supset \mathbb{Z}/p$
char$F = 0$, $F \supset \mathbb{Q}$

Thm: Let D be a domain (avoid div. by 0).

Then $\exists$ a field F_D "The field of fractions of D" that contains D as a subring.

Pf-def: $F = \{(a,b) : a,b \in D\} /$

$\{ \frac{a}{b} \quad b \neq 0 \} / \sim$

Where $\frac{a}{b} \sim \frac{c}{d} \iff a \cdot d = b \cdot c$

Claim: This makes sense as $\sim$ is an equiv. relation.

1. $\frac{a}{b} \sim \frac{a}{b}$

2. $\frac{a}{b} \sim \frac{c}{d} \Rightarrow \frac{c}{d} \sim \frac{a}{b}$

3. $\frac{a}{b} \sim \frac{c}{d}, \frac{c}{d} \sim \frac{e}{f} \Rightarrow \frac{a}{b} \sim \frac{e}{f}$

Pf: 1 & 2 are easy

3. Assume $\frac{a}{b} \sim \frac{c}{d} \Rightarrow ad = bc$

$\frac{c}{d} \sim \frac{e}{f} \Rightarrow cf = de$

Want $\frac{a}{b} \sim \frac{e}{f}$ $(af = be)$

$adf = bcf$ & $cfb = deb$

$adf = deb \Rightarrow af = be$ ✓
$(d \neq 0)$

Next, define how to do: $\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right] = \left[\frac{ad+bc}{bd}\right]$

check well-definedness ✓

$\left[\frac{a}{b}\right] \cdot \left[\frac{c}{d}\right] = \left[\frac{ac}{bd}\right]$

$0 := \left[\frac{0}{b}\right]$

$1 := \left[\frac{1}{1}\right]$

$\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$

Claim: This is a field

Check all axioms.

Finally, let $\varphi: D \to F_D$ by

$$a \longrightarrow \left[\frac{a}{1}\right]$$

$\ker\varphi$: $\left[\frac{a}{1}\right] = \left[\frac{0}{1}\right]$

$\iff a\cdot 1 = 1\cdot 0 \iff a = 0$

$\ker\varphi = \{0\}$

So $D = D/\{0\} \cong \operatorname{im}\varphi \subset F_D$

So F_D contains D.

Ex: Let $D = \mathbb{R}[x]$

$F_D = \left\{ \frac{ax^3+bx^2+cx+d}{x^{17}-x^{16}+\pi x-7} \right\}$ "rational functions"

Given any commutative ring R, define

$$R[x] = \left\{ \sum_{x=0}^{n} a_k x^k : \begin{array}{l} a_k \in R \\ a_n \neq 0 \end{array} \right\}$$

addition & multip. (0 & 1) are defined (in the obvious way)

$$\sum_{k=0}^{n_1} a_k x^k + \sum_{k=0}^{n_2} b_k x^k = \sum_{k=0} (a_k+b_k)\, x^k$$

$$\left(\sum a_i x^i\right)\left(\sum b_j x^j\right) = \sum \Big(\sum_{\substack{i,j \\ i+j=k}} a_i a_j \Big) x^k$$

Claim: $R[x]$ is a ring.

Def: 1. If $f \in R[x]$, define the "degree" of

<u>Def</u>: 1. if $f \in R[x]$, define the "degree" of f: $\deg f = \begin{cases} \text{maximal } k \text{ for which } a_k \neq 0 & f \neq 0 \\ -\infty & f = 0 \end{cases}$

2. "Evaluation" if $f = \sum a_k x^k \in R[x]$ & if $r \in R$.

$$f(r) = \sum a_k r^k \in R$$

<u>Claim</u>: $ev_r : R[x] \to R$ is a ring hom.
$f \to f(r)$

$$ev_r(f+g) \overset{?}{=} ev_r(f) + ev_r(g)$$
$$\parallel$$
$$(f+g)(r) \overset{?}{=} f(r) + g(r)$$

<u>Claim</u>: If D is a domain and $f, g \in D[x]$

Then $\deg(f \cdot g) = \deg f + \deg g$ $\begin{cases} -\infty + 7 = -\infty \\ -\infty + -\infty = -\infty \\ 7 + 8 = 15 \end{cases}$

Proof: if f or $g = 0$, true by summation convention

otherwise, $0 \leq \deg f = n$

$0 \leq \deg g = m$

$f = a_n x^n +$ lower power terms

$(a_n \neq 0)$

$g = b_m x^m +$ lower terms

$(b_m \neq 0)$

$f \cdot g = (a_n x^n + \ldots)(b_m x^m \ldots)$
$= \underbrace{a_n b_m}_{\neq 0} x^{n+m} + \ldots$

So $\deg f \cdot g = n + m$ ∎

Cor: $D[x]$ is a domain

Cor: $D[x]$ is a domain

Indeed, $f\cdot g = 0 \Rightarrow \deg f\cdot g = -\infty \Rightarrow \deg f + \deg g = -\infty$

$\Rightarrow \deg f = -\infty$ or $\deg g = -\infty \Rightarrow f = 0$ or $g = 0$

Thm (long division for poly's)

Let F be a field & $f, g \in F[x]$, $g \neq 0$. Then $\exists$ unique poly's q & r s.t. "$\frac{f}{g} = q\,\frac{r}{g}$"

q ↓ quot. $\qquad r$ ↓ rem.

i.e. $f = g\cdot q + r$

$\deg r < \deg g$

Proof: Uniqueness.

Assume

$gq_1 + r_1 = f = g\cdot q_2 + r_2$

$\deg r_1 < \deg g$, $\deg r_2 < \deg g$

$gq_1 + r_1 = gq_2 + r_2$

$g(q_1 - q_2) = r_2 - r_1$

$\Rightarrow \deg g + \deg(q_1 - q_2) = \deg(r_2 - r_1)$

if both sides ≥ 0, $\deg g + \deg(q_1 - q_2) \geq \deg g >$

$> \deg(r_2 - r_1)$

$\deg(r_2 - r_1) =$

$\Rightarrow$ both sides are $-\infty$ $\Rightarrow r_2 - r_1 = 0 \Rightarrow r_1 = r_2$

$q_1 - q_2 = 0 \Rightarrow q_1 = q_2$

Existence of q & r: by induction on $\deg f$.

Existence of q & r: by induction on $\deg f$.

if $\deg f < \deg g$, take $q=0$, $r=f$ & everyth. works

$$\boxed{\begin{array}{l} f = g \cdot q + r \\ \deg r < \deg g \end{array}}$$

Assume thm is true if $\deg f < n$ for some $n \geq \deg g$

Assume $\deg f = n \geq \deg g = m$

$b \neq 0 \quad g = b \cdot x^m + \dots$

$a \neq 0 \quad f = a x^n + \dots$

$$\frac{f}{g} = \frac{ax^n}{bx^m} \quad \frac{a}{b} \cdot x^{n-m}$$

$$q = \frac{a}{b} x^{n-m} + \dots$$

Let $f_1 = f - \frac{a}{b} x^{n-m} g$

$$f_1 = (\cancel{a}x^n + \dots) - \cancel{\frac{a}{b}} x^{n-\cancel{m}} \cancel{b}\, \cancel{x^m}$$

$\Rightarrow \deg f_1 < \deg f$

by induction, find q_1 and r_1 s.t

$$f_1 = q_1 g + r_1 \quad , \deg r_1 < \deg g$$

So $f - \frac{a}{b} x^{n-m} g = q_1 g + r_1$

$$f = \underbrace{\left(\frac{a}{b} x^{n-m} + q_1 \right)}_{q} g + \underbrace{r_1}_{r}$$

$f = q \cdot g + r \quad \Rightarrow \deg r < \deg g$