Math 3032 Lecture 6 (Jan 28, 2021)

Office hours next week: Tues 12-2

HW 2 due end of today.

In your homework:

- sentences are good.

bad

Today: More on polynomials.

Recall: Given any ring R, build a ring $R[x]$.

As an additive gp, $R[x] = \bigoplus_{n\geq 0} Rx^n$ $\Rightarrow (a_0, a_1, \dots)$ where $\sum_{n\geq 0} a_n x^n$

Rx^n $\uparrow$ notation for a copy of $(R,+)$.

Sequence which is eventually zero.

$$(a_0, a_1, \dots)\cdot(b_0, b_1, \dots)$$

$$:= (a_0b_0,\ a_0b_1 + a_1b_0,\ a_0b_2 + a_1b_1 + a_2b_0,\ \dots)$$

$$\left(\sum_i a_i x^i\right)\left(\sum_j b_j x^j\right)$$

$$= \sum_n \left(\sum_{i\leq n} a_i b_{n-i}\right) x^n$$

If R is
- unital
- com
- domain

then so is $R[x]$.

If R is a domain (in particular, unital com)
then so is $R[x]$, and so we have its field
of fractions $R(x)$. The field of "rational functions"

↑ not functions!

Intermediate between $R[x] \subsetneq R[x^{\pm 1}] \subsetneq R(x)$

$$R[x^{\pm 1}] \cong R[x][x^{-1}]$$

"Laurent polynomials"

every element can be written as

$$\frac{a(x)}{x^i} = a_0 x^{-i} + a_1 x^{1-i} + \dots + a_n x^{n-i}$$

where $a(x) = a_0 x^0 + a_1 x^1 + \dots + a_n x^n$

$i \in \mathbb{N}$.

Find: $(R[x^{\pm 1}], +) \cong \coprod_{n \in \mathbb{Z}} R x^n$.

Aside: $(R[\![x]\!], +) \cong \prod_{n \geq 0} R x^n$.

$R(\!(x)\!) = R[\![x]\!][x^{-1}] \ni \sum_{n \geq i} a_n x^n$.

the whole field of fractions of $R[\![x]\!]$ if R was already a field.

for some $i \in \mathbb{Z}$

Every polynomial $a(x) \in R[x]$ gives a function

$R \to R$.

Namely, $r \mapsto a(r)$ (the value of evaluating a at r).

In other words, take the formal expression $\sum a_i x^i$ to the element $\sum a_i r^i \in R$.

Fix $r \in R$ and consider the map

$$ev_r : R[x] \longrightarrow R$$
$$a(x) \mapsto a(r).$$

Lemma: ev_r is additive, i.e. a hom of additive gps.

(because of the distributive law)

Proposition: If R is commutative, then

$$ev_r : R[x] \to R \quad \text{is a ring homomorphism.}$$

$ev_r\left(\sum a_i x^i + \sum b_i x^i\right) \stackrel{?}{=} ev_r\left(\sum a_i x^i\right) + ev_r\left(\sum b_i x^i\right)$

$\sum (a_i + b_i) x^i$

$\sum (a_i + b_i) r^i \stackrel{?}{=} \sum a_i r^i + \sum b_i r^i$ (Yes).

Pf:

$$ev_r\left(\left(\sum_i a_i x^i\right)\left(\sum_j b_j x^j\right)\right) \stackrel{?}{=} \left(\sum_i a_i r^i\right)\left(\sum_j b_j r^j\right)$$

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

$$ev_r\left(\sum_k \left(\sum_{i=0}^{k} a_i b_{k-i}\right) x^k\right) \qquad \sum_{i,j} a_i r^i b_j r^j$$

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

$$\sum_k \left(\sum_i a_i b_{k-i}\right) r^k \qquad \sum_k \sum_{i+j=k} a_i r^i b_j r^{k-i}$$

(if r commutes w/ b_j's.)

$$\sum_k \sum_{i=0}^{k} a_i r^i b_{k-i} r^{k-i}$$

There is a ring "R^R" or "functions (R, R)" which is the set of all functions $R \to R$.
addition and multiplication are "pointwise":

$f, g \in R^R$ then $(f+g) : r \longmapsto f(r)+g(r)$

$(f \cdot g) : r \longmapsto f(r) \cdot g(r)$.

$ev_* : R[x] \to R^R$ is a ring hom if R is commutative.

POLYNOMIALS ARE NOT FUNCTIONS.

In particular: ev_* can have a kernel!

- When $R = \mathbb{R}$ or $\mathbb{C}$, then

$$ev_* : R[x] \hookrightarrow R^R.$$

For these coeffs, two polys are equal if their functions are equal.

- If $R = \mathbb{Z}/p \cong \mathbb{F}_p$,

then $R[x]$ has ∞ many elements

but R^R has only $p^p < \infty$ many elements.

So ev_* has no chance to be injective.

Fermat's little theorem:

x^1 and $x^p \in \mathbb{F}_p[x]$ are different as polys, but they have the same values as functions.

$-x + x^p \in \mathbb{F}_p[x]$

$\wedge \Leftarrow$ FLT

$\ker(ev_*)$ i.e. $ev_*(-x+x^p) = 0 \in (\mathbb{F}_p)^{(\mathbb{F}_p)}$.

$\mathbb{F}_2 \cong \mathbb{Z}/2 \subseteq \mathbb{F}_4 = \{0, 1, \omega, \bar{\omega}\}$.

$\| \quad (\mathbb{F}_4, +) \cong (\mathbb{Z}/2)^2$. $\omega + \omega = 0$

$\{0,1\}$ $\bar{\omega} = 1 + \omega$.

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

$\omega^2 = \bar{\omega}$. $\bar{\omega}^2 = \omega$.

×	0	1	ω	$\bar{\omega}$
0	0	0	0	0
1	0	1	ω	$\bar{\omega}$
ω	0	ω	$\bar{\omega}$	1
$\bar{\omega}$	0	$\bar{\omega}$	1	ω

$\mathbb{F}_2[x] \subseteq \mathbb{F}_4[x]$

$\cup$

$\boxed{-x + x^2}$

$0 \neq -\omega + \omega^2 = 1$

↑ the values of this poly on inputs in $\mathbb{F}_2$ all vanish

Vocab: If $f \in R[x]$ and $r \in R$ s.t.

$$0 = ev_r(f) = f(r)$$ i.e. if $f \in \ker(ev_r)$

then r is called a zero of f.

E.g:

- Every element of $\mathbb{F}_p$ is a zero of $x^p - x$.
- No element of $\mathbb{R}$ is a zero of $x^2 + 1$.
- In $\mathbb{F}_5$, no element is a zero of $x^2 + 2$.
- In $\mathbb{F}_5$, 2 is a zero of $x^2 + 1$.

What are the homomorphisms with domain $R[x]$?

i.e. what is $\hom(R[x], S)$? (R, S commutative).

When $S = R$, $\hom(R[x], R) \ni ev_r$ for each $r \in R$.

Punchline Slogan: "ev_r's are all the homs."

$$\varphi : r_0 + r_1 x + \cdots \in R[x] \longrightarrow S$$

$$r \in R \hookrightarrow R[x] \xrightarrow{\varphi} S, \qquad f|_R : R \to S$$

$$\varphi(x) \in S$$

$$x \in R[x]$$

So any $\varphi : R[x] \to S$ includes in its data

- $\varphi|_R : R \to S$.
- $\varphi(x) \in S$.

We just described a map of sets

$$\hom(R[x], S) \longrightarrow \hom(R,S) \times S$$

$$\varphi \longmapsto (\varphi|_R, \varphi(x))$$

Thm: If S is commutative, then φ is a bijection.

$$\hom(R,S) \longleftarrow (\phi, s)$$

$$\left(\sum a_i x^i\right) \mapsto \left(\sum \phi(a_i)\, s^i\right)$$

$\phi \in \hom(R,S)$, $s \in S$

Need to check:

- is indeed a ring hom $R[x] \to S$.
- are indeed inverse to each other.

In particular, $S = R$ and decide to use

$$\begin{array}{c} id \\ \uparrow \\ \hom(R,R) \end{array} \qquad \hom(R[x],R) = \hom(R, R) \times R$$
$$\Psi$$
$$id$$

Find: Iff $\varphi : R[x] \to R$ is a ring homomorphism s.t. $\varphi|_R = id$, then $\varphi = ev_r$ where $r = \varphi(x)$.

"All homomorphisms w/ domain $R[x]$ are (twisted) evaluation maps"
$\subset$ by a hom w/ domain R.

Example:

Start w/ ring R $\rightsquigarrow$ $R[x]$.

$R[x]$ is a ring $\rightsquigarrow$ $(R[x])[y] =: R[x,y]$

polynomial ring w/ variable y and coeffs $\in R[x]$.

$R[y] \rightsquigarrow R[y][x]$.

lls dif letter.

$R[x]$

$\Downarrow$

$$\sum_i \underbrace{a_i(x)}_{\in} y^i$$

$$\left(\sum_j a_{ij} x^j\right)$$

$\mathrm{Hom}\left[\, R[x,y] \xrightarrow{\Phi} R[y,x] \,\right]$ is an iso.

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

$R[x][y] \qquad R[y][x]$

$\Phi|_{R[x]}$ and $\Phi(y)$

$\| \qquad\qquad \|$ decide

$\varphi \qquad\qquad y \cdot x^0$

$\varphi : R[x] \to R[y,x]$

$\varphi|_R := \text{inclusion } R \hookrightarrow R[y,x]$

$\varphi(x) := x.$

Warning:

$R[\![x]\!][\![y]\!]$

Φ is a y that $x \mapsto x$, $y \mapsto y$

$R[\![y]\!][\![x]\!]$.

What are homs w/ domain R domain

$R[x^{\pm 1}] = R[x][x^{-1}]$?

$R(x)$?

$$\hom(R[x][x^{-1}], S) = \{\varphi : R[x] \to S \text{ s.t. } \varphi(x) \text{ is invertible}\}$$

$$\cong \hom(R, S) \times S^{\times}.$$