Lecture March 19

Midterm #6:

$a^{(n)} = 0_R$, $b^{(k)} = 0_R$

$(a+b)^{(m)} \Rightarrow$ binomial thm

$(a + -a)\, a^{n-1}$ — $(-a)^n = 0_R$

$= \underbrace{a^n}_{0_R} + \underbrace{(-a)\cdot a^{n-1}}_{-a^n}$

Today: Homomorphisms

Def: Let R, S be rings. A function $f: R \to S$ is called a homomorphism if

$$f(a+b) = f(a) + f(b),$$
$$f(ab) = f(a)f(b)$$

for all $a, b \in R$.

We've seen homomorphisms before:

all isomorphisms are homomorphisms. They just also need to be injective and surjective.

Examples:

(1) zero map $z: R \to S$

for any $a \in R$,

$$z(a) = 0_S$$

This is a homomorphism:

Let $a, b \in R$. Then:

- $z(a+b) = 0_S$.

$$z(a) + z(b) = 0_S + 0_S = 0_S \checkmark$$

$$\Rightarrow z(a+b) = z(a) + z(b)$$

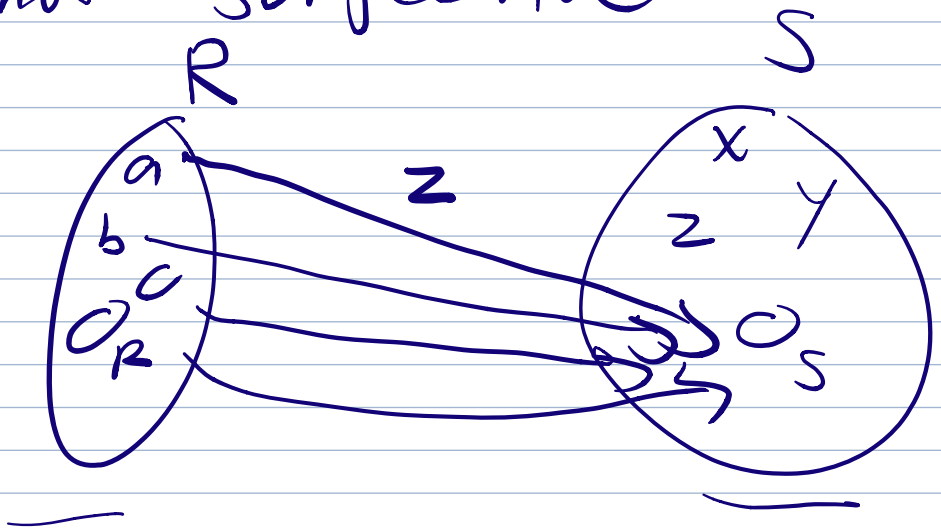
- $z(ab) = 0_S = 0_S \cdot 0_S$

$$= z(a) \cdot z(b) \checkmark$$

$\Rightarrow$ zero map is a homomorphism.

Clearly, this is not an isomorphism.

Why? z is neither injective nor surjective.



(2) Define $\pi : \mathbb{Z} \to \mathbb{Z}_5$

$n \mapsto [n]_5$

So $\pi(1) = [1]_5$

$\pi(7) = [7]_5 = [2]_5$

$\pi(20) = [20]_5 = [0]_5$.

Show π is a homomorphism:

Let $n, m \in \mathbb{Z}$. Then,

$$\pi(n+m) = [n+m]_5 = [n]_5 + [m]_m$$
$$= \pi(n) + \pi(m) \checkmark$$

$$\pi(nm) = [nm]_5 = [n]_5 \cdot [m]_5$$
$$= \pi(n) \cdot \pi(m) \checkmark$$

$\Rightarrow \pi$ is a homomorphism.

But, π is not an isomorphism:

π is not injective:

for instance, $\pi(0) = \pi(5) = [0]_5$.

In general, the function

$$\pi: \mathbb{Z} \longrightarrow \mathbb{Z}_k$$
$$a \longmapsto [a]_k$$

is a homomorphism, but not

an isomorphism.

(3) $M_2(\mathbb{Z})$ = ring of 2×2 matrices with integer entries

$$L = \left\{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} : a, b, c \in \mathbb{Z} \right\}$$

Define a function $f: L \to \mathbb{Z}$ by

$$f\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} = a$$

So

$$f\begin{pmatrix} 3 & 0 \\ -2 & 6 \end{pmatrix} = 3.$$

This is a surjective homomorphism:

$$f\left(\begin{pmatrix} a_1 & 0 \\ b_1 & c_1 \end{pmatrix} + \begin{pmatrix} a_2 & 0 \\ b_2 & 0 \end{pmatrix} \right)$$

$$= f\begin{pmatrix} a_1 + a_2 & 0 \\ b_1 + b_2 & c_1 + c_2 \end{pmatrix}$$

$$= a_1 + a_2$$

$$= f\begin{pmatrix} a_1 & 0 \\ b_1 & c_1 \end{pmatrix} + f\begin{pmatrix} a_2 & 0 \\ b_2 & c_2 \end{pmatrix} \checkmark$$

$$f\left(\begin{pmatrix} a_1 & 0 \\ b_1 & c_1 \end{pmatrix}\begin{pmatrix} a_2 & 0 \\ b_2 & c_2 \end{pmatrix}\right)$$

$$= f\begin{pmatrix} a_1a_2 & 0 \\ a_2b_1 + c_1b_2 & c_1c_2 \end{pmatrix}$$

$$= a_1a_2 = f\begin{pmatrix} a_1 & 0 \\ b_1 & c_1 \end{pmatrix} f\begin{pmatrix} a_2 & 0 \\ b_2 & c_2 \end{pmatrix} \checkmark$$

$\Rightarrow f$ is a homomorphism.

Check f is surjective:

Let $a \in \mathbb{Z}$. find matrix $A \in L$

s.t. $f(A) = a$

Set $A = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$. Then

$f(A) = f\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = a \checkmark \Rightarrow$ surjective

However, f is not injective:

$$f\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = 1 = f\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

$\Rightarrow$ f is not an isomorphism.

Nice Properties of Homomorphisms:

Thm 3.10: Let $f: R \to S$ be a homomorphism of rings. Then,

(1) $f(0_R) = 0_S$.

(homomorphisms map zero elements to zero elements)

(2) for any $a \in R$,

$$f(-a) = -f(a).$$

(3) $\forall\, a, b \in R$,

$$f(a-b) = f(a) - f(b)$$

If R has identity and f is surjective, then

(4) S is a ring w/ identity $f(1_R)$

(5) Whenever u is a unit in R, $f(u)$ is a unit in S, and $f(u^{-1}) = f(u)^{-1}$.

Pf:

(1) $f(0_R) = f(0_R + 0_R)$

$= f(0_R) + f(0_R)$

$\Rightarrow f(0_R) = 0_S$.

(2)

$0_S = f(0_R) = f(a-a) = f(a+(-a))$

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

$\Rightarrow$ $f(-a)$ solves the equation

$$\underbrace{f(a) + x = 0_S}.$$

But, this has a unique solution $-f(a)$.

$\Rightarrow$ $f(-a) = -f(a)$.

(3) by (2)

$$f(a-b) = f(a + (-b)) = f(a) + f(-b) = f(a) - f(b)$$

(4) Now, we assume R has identity 1_R and f is surjective.

Let $s \in S$, want to show

$$f(1_R) \cdot s = s.$$

Since f is surjective, $\exists\, r \in R$ s.t. $f(r) = s$. So,

$$f(1_R)\cdot s = f(1_R)\cdot f(r)$$
$$= f(1_R \cdot r)$$
$$= f(r)$$
$$= s. \checkmark$$

(5) By 4, S has identity $1_S = f(1_R)$. Let u be a unit in R. Want to show $f(u)$ is a unit w/ inverse $f(u^{-1})$:

$$1_S = f(1_R) = f(u\cdot u^{-1}) = f(u)f(u^{-1})$$
$$\Rightarrow f(u)f(u^{-1}) = 1_S$$

$\Rightarrow f(u)$ is a unit w/ inverse $f(u^{-1})$

$\Rightarrow f(u)^{-1} = f(u^{-1})$. ∎

Chapter 4 - Polynomials

Let R be a ring, and x an <u>indeterminate</u>. Define the set

$$R[x] = \{a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n : a_0, a_1, \ldots, a_n \in R, n \geq 0\}$$

The elements of this set are called <u>polynomials</u>, and the a_i are called <u>coefficients</u>.

Ex:

(1) $\mathbb{Z}[x]$ = polynomials with integer coefficients.

Some elements: $1 + x$, $x^2 + 3x + 2$, $17x - 5$, $33x^{17}$.

(2) $\mathbb{Q}[x]$ = polys w/ rational coefficients.

Some elements: $\frac{3}{4}x + 5$

$\frac{22}{7}x^3 + \frac{1}{3}x^2 + 4x - \frac{2}{5}$.

(3) $\mathbb{Z}_5[x]$ - coefficients are in $\mathbb{Z}_5$.

(4) $M_2(\mathbb{R})[x]$ - coefficients are 2×2 matrices.

An element: $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} x^2 + \begin{pmatrix} 3 & 2 \\ 1 & 0 \end{pmatrix}$

We usually denote a poly. as $f(x)$, $g(x)$, $h(x)$, etc.

Defining operations:

Let R be a ring. Then, $R[x]$ is also a ring w/ the following operations:

If $f(x) = a_0 + a_1 x + \cdots + a_n x^n$,

$g(x) = b_0 + b_1 x + \cdots + b_n x^n$,

then,

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots + (a_n + b_n)x^n$$

$$f(x) \cdot g(x) = (a_0 + a_1 x + \cdots a_n x^n) \cdot (b_0 + b_1 x + \cdots + b_n x^n)$$

$$= \sum_{k=0}^{n+m} c_k x^k$$

where $c_k = \sum_{i=0}^{k} a_i b_{k-i}$.

(typical polynomial multiplication)

We'll just work with $R[x]$ where R is commutative, so $+$ and $\cdot$ will be what we're used to.

Ex:

(1) Consider $\mathbb{Z}[x]$

$f(x) = x+3, \quad g(x) = 2x+1$

Then,

$$f(x)+g(x) = (x+3)+(2x+1)$$
$$= 3x+4$$

$$f(x)g(x) = (x+3)(2x+1)$$
$$= 2x^2+7x+3$$

(2) Consider $\mathbb{Z}_4[x]$

Let $f(x) = 2x^2+2x+3, \quad g(x) = 2x+1$

Then,

$$f(x) + g(x) = (2x^2 + 2x + 3) + (2x + 1)$$
$$= 2x^2 + 4x + 4$$
$$= 2x^2 + 0x + 0$$
$$= 2x^2$$

$$f(x)g(x) = (2x^2 + 2x + 3)(2x + 1)$$
$$= 4x^3 + 4x^2 + 6x + 2x^2 + 2x + 3$$
$$= 0x^3 + 0x^2 + 2x + 2x^2 + 2x + 3$$
$$= 2x^2 + 4x + 3 = 2x^2 + 3$$

- $R[x]$ is a ring w/ the above addition and mult.
- The elements of R form a subring of $R[x]$; in this context we call the elements of R the <u>constant polynomials</u>

The zero element of $R[x]$ is just the constant poly 0_R.

If R has identity, then so does $R[x]$, and its identity is just 1_R.

for a poly $f(x) \in R[x]$, we call its <u>degree</u>, denoted $\deg f(x)$, the largest exponent of x that appears in $f(x)$.

So, if $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, then its degree is n, and we write $\deg f(x) = n$.

Ex: in $\mathbb{Q}[x]$,

$$\deg\left(x^3 + \frac{3}{4}x^2\right) = 3$$

we say constant polys have degree 0, but the zero element 0_R does not have a degree.

we say two polynomials are equal iff all of their coefficients are the same and they have the same degree. That is,

$$a_0 + a_1 x + \cdots + a_n x^n = b_0 + b_1 x + \cdots + b_m x^m$$

iff $n = m$ and $a_0 = b_0$, $a_1 = b_1$, $a_2 = b_2$, $\ldots$, $a_n = b_n$.

Thm 4.2: If R is an integral domain and $f(x), g(x)$ are nonzero polys in $R[x]$, then,

$$\deg[f(x)\cdot g(x)] = \deg f(x) + \deg g(x)$$

Pf: $f(x) = a_n x^n + \cdots + a_1 x + a_0 \quad (\deg f(x) = n)$

$g(x) = b_m x^m + \cdots + b_1 x + b_0, \quad (\deg g(x) = m)$

where $a_n, b_m \neq 0_R$. Then,

$$f(x)\,g(x) = (a_n x^n + \cdots + a_0)(b_m x^m + \cdots + b_0)$$

$$= a_n b_m x^{n+m} + \cdots + a_0 b_0$$

↖ we don't care about rest

Since R is an integral domain and $a_n, b_m \neq 0_R$, then $a_n b_m \neq 0_R$.

$\Rightarrow x^{n+m}$ is the largest-degree term in $f(x)\cdot g(x)$, so

$$\deg\left(f(x)\cdot g(x)\right) = n+m$$
$$= \deg f(x) + \deg g(x)$$

$\blacksquare$