Lecture 21

Last time: - Defined rings $(R, +, \cdot)$

$$\begin{cases} (R,+) \text{ abelian group} \\ (R,\cdot) \text{ monoid} \\ a\cdot(b+c) = a\cdot b + a\cdot c \;;\; (b+c)\cdot a = b\cdot a + c\cdot a \end{cases}$$

- Examples: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/n\mathbb{Z}, Mat_{2\times 2} \ldots$

- Defined polynomial ring $R[x]$ (arbitrary ring)

$$\{a_0 + a_1 x + \ldots + a_n x^n\}$$

- Discussed division with reminder in $R[x]$:

$$f(x), h(x) \in R[x], \quad h(x) \text{ monic}$$

$$\Downarrow$$

$$\exists!\ q(x), r(x) \in R[x] \quad \text{s.t.} \quad \deg r(x) < \deg h(x)$$

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

$(f(\alpha)=0)$

Lemma α — root of $f(x)$ iff

$$f(x) = (x-\alpha)\cdot q(x)$$

R for some $q(x) \in R[x]$

proof. if $f(x) = (x-\alpha)\cdot q(x)$

$$f(\alpha) = (\alpha-\alpha)\cdot q(\alpha) = 0 \checkmark$$

if $f(\alpha)=0$ then let's divide $f(x)$ by $x-\alpha$:

$$f(x) = (x-\alpha)\,q(x) + r(x)$$

r: polynomial of

$\deg r(x) < \deg(x-\alpha)$

$\deg r(x) = 0 \Rightarrow r(x) = r$

r: just an element of R

So $f(\alpha) = (\alpha - \alpha) \cdot q(\alpha) + r = r$

0 // $\Rightarrow$ $r = 0$

We get $f(x) = (x - \alpha) q(x)$ ✓

Definition R – ring has **no zero divisors** if $\forall a, b \in R \setminus \{0\}$, $a \cdot b \neq 0$.

Examples: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ – no zero divisors

In general: if R – division ring (in particular, field) $\Rightarrow$

$\Rightarrow$ R – has no zero divisors

Proof: if $a, b \in R \setminus \{0\} \Rightarrow a, b \in R^{\times} \Rightarrow$

$\Rightarrow ab \in R^\times \Rightarrow ab \neq 0$

Question: do we have zero divisors in

$\mathbb{Z}/6\mathbb{Z}$?

Answer: yes σ $2 \cdot 3 = 0$!

In general, if n is not prime

$\swarrow$

$\mathbb{Z}/n\mathbb{Z}$ σ has zero divisors

(take any $k \mid n$, $k \neq 1, n \Rightarrow k \cdot \frac{n}{k} = 0$)

How about $Mat_{2\times 2}(\mathbb{R})$?

$$\underset{R}{\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}} \cdot \underset{9}{\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

zero divisors

(for example, R = field)

Thm: assume R has no zero divisors.

Fix $f(x) \in R[x]$, then:

$$\#\text{roots of } f \leq \deg f$$

proof: Induction on $\deg f = n$.

Induction step: pick α = any root of f

Use Lemma above:

$$f(x) = (x-\alpha)\cdot q(x)$$

$\deg(q) = n-1$

Claim: $\{\text{roots of } f\} \overset{(*)}{=} \{\text{roots of } q\} \cup \{\alpha\}$

If $\beta \neq \alpha$ then $f(\beta) = (\beta-\alpha)\cdot q(\beta)$

$\neq 0$ $\quad$ $\neq 0$

Note: $\beta - \lambda \neq 0$ (our assumption)

$\parallel$

$q(\beta) = 0$ (use that R has no zero divisors)

q

i.e. $\beta \in \{\text{roots of } q\}$

(*) follows

(*) implies that (induction hypothesis)

$$\#\text{roots of } f \leq \#(\text{roots of } q) + 1 \leq$$

$$\leq (n-1) + 1 = n \quad \checkmark$$

Next time: will use Thm. above to prove that $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic

(more generally, $R^\times$ is cyclic for any finite field)

Another important example of a ring.

It turns out that starting with arbitrary monoid G and arbitrary ring R one can associate to this pair a ring RG

it's called monoid ring

(if G - group we call it group ring)

Definition

$$RG = \left\{ r_1 g_1 + r_2 g_2 + \dots + r_n g_n \;\middle|\; r_i \in R \right\}$$

(formal sums)

Let's define <u>ring structure</u> on RG:

any two elements of RG can be written in the form:

$$a_1 g_1 + \dots + a_n g_n, \quad b_1 g_1 + \dots + b_n g_n \quad \text{for some } g_1, \dots, g_n$$

(a_i, b_i can be zero!)

Then the sum of these elements is:

$$(a_1 + b_1) g_1 + \dots + (a_n + b_n) g_n$$

Product is defined as follows:

$$(a_1 g_1 + \dots + a_n g_n) \cdot (b_1 g_1 + \dots + b_n g_n) =$$

$$= \sum_{i,j} a_i g_i \cdot b_j g_j = \sum_{g \in G} \left(\sum_{g_i \cdot g_j = g} (a_i b_j) \right) g$$

($g_i \cdot b_j$: commute)

compare with what we did for $R[x]$!

Claim: $(RG, +, \cdot)$ is a ring

proof similar argument as the one you use to prove that $(R[x], +, \cdot)$ - ring

prove this in PSet 8

Example: $R[x]$ is a particular case of RG.

For which G?

Take $G = \mathbb{Z}_{\geq 0}$

Then $RG \leftarrow \{ r_0 0 + r_1 1 + \dots + r_{n-1} n \}$

is

$R[x] \leftarrow \{ r_0 + r_1 x^1 + \dots + r_{n-1} x^n \}$

product in $\mathbb{Z}_{\geq 0}$

is exactly the product

in $\{1, x, x^2, \dots\}$

(i.e. $\mathbb{Z}_{\geq 0} \xrightarrow{\sim} \{1, x, x^2, \dots\}$)

$n \longmapsto x^n$

isomorphism of monoids

Example of group algebra.

Take $G = D_8 = \langle r, s \rangle / \langle r^4 = s^2 = 1,\ rs = sr^{-1} \rangle$

$= \{ r^k s^m \mid k = 1, 2, 3, 4,\ m = 0, 1 \}$

Take $R = \mathbb{Z}$

Then elements:

$$\alpha = r + r^2 - 2s \quad ; \quad \beta = -3r^2 + rs$$

are typical elements of $\mathbb{Z}D_8$

Let's compute their sum and product:

$$\alpha + \beta = (r + r^2 - 2s) + (-3r^2 + rs) =$$

$$= r - 2r^2 - 2s + rs \quad \checkmark$$

$$\alpha \cdot \beta = (r + r^2 - 2s) \cdot (-3r^2 + rs) =$$

$$= r \cdot (-3r^2 + rs) + r^2 \cdot (-3r^2 + rs) -$$

$$- 2s \cdot (-3r^2 + rs) =$$

$$= -3r^3 + r^2s - 3 + r^3s + \underbrace{6sr^2}_{\| \; 6r^2s} - \underbrace{2srs}_{\| \; 2r^3}$$

$$\|$$

$$-3r^3 + r^2s - 3 + r^3s + 6r^2s - 2r^3$$

$$\|$$

$$-5r^3 - 3 + 7r^2s + r^3s$$

Remarks: get lots of examples of noncommutative rings:

if G noncommutative, $R = \mathbb{Z}$

$$\|$$

$\mathbb{Z}G$ noncommutative

Indeed: take $g_1, g_2 \in G$ s.t. $g_1 g_2 \neq g_2 g_1$

$$\|$$

g_1, g_2 considered as elements of RG do not commute

Also note that if G a group

$$G \subset (RG)^\times$$

embedding of groups

(indeed, if $g \in G$, then it's invertible in RG with inverse g^{-1})

Module over a ring

Remember that for groups G we had a (very useful) notion of G acting on some set X

It turn's out that there is a similar notion for rings.

This is called <u>module</u> over a ring.

<u>Definition</u> R a ring, a <u>module</u> over R is a set M together with:

(1) $+ : M \times M \to M$

(2) $\cdot : R \times M \to M$ a <u>action</u> s.t.

$(M, +)$ a <u>abelian</u> group

$\forall r, s \in R,\ m \in M$

$(r+s)\cdot m = r\cdot m + s\cdot m$

$(r\cdot s)\cdot m = r\cdot(s\cdot m)$

$r\cdot(m+n) = rm + rn$

$1\cdot m = m$

Example: $\mathbb{Z}$-modules are abelian groups