Math 3032 Lecture 7 (Feb 4)

OH Tues 12-2

Main event: a few noncommutative rings.

FYI: Problem sets will be out of ~14 or 15 range depending on difficulty.

There will be a discussion board on Brightspace.

↳ discuss

↳ exchange contact info.

1. We begin by showing the forward direction.

   Suppose R is a unital ring with characteristic $n \in \mathbb{N}$. Let $r \in R$. Then

$$n \cdot r = r + r + \ldots + r = \sum_1^n r.$$

   Since $1 \in R$ and $1 \cdot r = r$, we have

$$n \cdot r = \sum_1^n (1 \cdot r).$$

   By distributivity,

$$\sum_1^n (1 \cdot r) = \left(\sum_1^n 1\right) \cdot r.$$

   But

$$\left(\sum_1^n 1\right) \cdot r = (n \cdot 1) \cdot r = 0 \cdot r$$

   since R has characteristic n. Therefore,

$$n \cdot r = 0 \cdot r = 0.$$

   To show the backward direction, suppose that R is a unital ring and $n \in \mathbb{N}$ is such that $n \cdot r = 0$ for every $r \in R$. Then, since $1 \in R$,

$$n \cdot 1 = 0.$$

   So, by definition, R has characteristic n.

Highly recommend

"On proof and progress in mathematics"

W. Thurston

Bull of AMS

1994.

This course is mostly geared towards factorization in commutative rings — alg. geo
— number thy.

Noncom rings and their "representations" are fun + important
modules

A main example: Let R is a "ground ring"
(most of the time in applications $R = \mathbb{Z}, \mathbb{C}$)

Let G be a group. (write G multiplicatively)

Construct a ring RG, $R \cdot G$ $R[G]$ "the group ring"

As an additive gp

mean the same thing for ab. gps.

$$(RG, +) = \coprod_{g \in G} Rg = \bigoplus_{g \in G} Rg$$

$(Rg, +)$ is a copy of $(R, +)$

g is a label

elements of Rg are "$r \cdot g$" = "rg" where and $r \in R$.

An element of RG is

- a list of elements in R indexed by G s.t. only finitely many nonzero elts.
- a (formal) sum of finitely many elements of form $r_i g_i$ $\quad g_i \in G$, $r_i \in R$

E.g. $R = \mathbb{R}$, $G = C_2 = \{e, z\}$ $z^2 = e$.

e : identity element

e^{th} entry z^{th} entry

$$\mathbb{R}C_2 \ni a := (7, 3) \longleftrightarrow 7e + 3z.$$

$$b = (\pi, -1) \longleftrightarrow \pi e + (-1) z.$$

$$a + b = (7+\pi, 3+-1) = (7+\pi)e + 2z$$

multiplication is not componentwise. Uses the multiplication in G. $(r_1 g_1)\cdot(r_2 g_2) := \underbrace{r_1 r_2}_{\in R} \cdot \underbrace{g_1 g_2}_{\in G}$

E.g. $\mathbb{R}C_2$

compare: in $\mathbb{C}$, would have been $-$.

$$a \cdot b = (7\pi - 3)e + (3\pi - 7)z$$

Why is RG a ring?

- $(RG, +)$ is by construction an additive gp.
- multiplication is defined first on monomials and then extended to all of RG by distributivity

  ↪ every elt in RG is a sum of monomials in a canonical way.

  So closure and distributivity are automatic.
- to check associativity, it is enough to check on monomials.

  because $\left(\left(\sum_i a_i\right)\left(\sum_j b_j\right)\right)\left(\sum_k c_k\right) = \sum_{ijk} (a_i b_j) c_k$

For monomials, it just uses assoc in R and in G.

$1 = e \in G$ is the identity.

Basic observations:

(0) $R \hookrightarrow RG \qquad r \mapsto r \cdot e$

$\hookrightarrow$ means injection. mix of $\to$ and $\subset$.

$\hookrightarrow$ if R is not com, then RG is not com.

(1) If R is unital, then so is RG with unit $\underbrace{1 \cdot e}_{= 1}$

(2) If R and G both com, then RG is com.

$\hookrightarrow$ if $R \ni 1$, then $G \hookrightarrow \underline{(RG)^\times}$ gp of inv. elements in any RG.

$g \longmapsto 1 \cdot g$

So if G is not com, then neither is RG.

RG typically fails "niceness" properties.

e.g. $\mathbb{R} C_2$ has zero div. $\quad (1+z)(1-z) = 0$.

<u>Notation:</u> Assuming $R \ni 1$, then

$$1 \cdot g = (0, \dots, 0, \underset{g}{1}, 0, \dots, 0) \in \coprod_{g \in G} Rg$$

$$\begin{array}{c} \| \\ \text{“}g\text{”} \end{array}$$

So I can think of $G \subseteq RG$.

$e \Leftrightarrow 1e \in RG$

$\uparrow$

G

$G = \cancel{\{e, z\}}$ $\{1, z\}$.

<u>N.B:</u> To construct RG, you never use inverses in G.

It would have worked even if G were merely a <u>monoid</u>.

set w/ associative (unital) multiplication.

e.g. $G \simeq (\mathbb{N}, +)$ as a monoid.

$$\begin{array}{ccc} G & & \mathbb{N} \\ \| & & n \\ & & \updownarrow \\ x^{\mathbb{N}} & & x^n \end{array} \qquad x^n \cdot x^m := x^{n+m}$$

$$R\, x^{\mathbb{N}} = R[x]$$

$$\begin{array}{ccc} G & \simeq & (\mathbb{Z}, +) \\ \| & & n \\ & & \updownarrow \\ x^{\mathbb{Z}} & & x^n \end{array} \qquad R\, x^{\mathbb{Z}} = R[x^{\pm 1}]$$

E.g.: Q_8 quaternion gp of order $8 = 2^3$

a gp of order 8.

There are (up to iso) 5 gps of order 8. (p^3 for any prime p).

$C_2 \times C_2 \times C_2$, $C_2 \times C_4$, C_8 } commutative

D_8 dihedral — syms of a square

Q_8

D_8, Q_8 } non comm.

$$e_+ \quad i_+ = i \quad j_+ = j \quad k_+ = k$$

$$\underbrace{e_+ \; e_-}_{\pm 1} \quad \underbrace{i_+ \; i_-}_{\pm i} \quad \underbrace{j_+ \; j_-}_{\pm j} \quad \underbrace{k_+ \; k_-}_{\pm k}$$

- id is e_+.
- $e_- x_+ = x_- = x_+ e_-$
  $e_- x_- = x_+ = x_- e_-$ $\quad \forall x \in \{e, i, j, k\}$
- $x_+^2 = x_-^2 = e_-$ for $x \in \{i, j, k\}$
- $i_+ j_+ = k_+$, $j_+ k_+ = i_+$, $k_+ i_+ = j_+$.

$ij = k$

$$ji = j(ij)j^{-1} = \underbrace{jk}_{i}\underbrace{j^{-1}}_{j_-} = ij e_- = k_-$$

$\mathbb{R}Q_8$ gp ring.

$Q_8 \supset C_2 = \{e_+, e_-\}$

$\mathbb{R}Q_8 \supset \mathbb{R}C_2$ has zero divisors

$0 = (1+z)(1-z)$

elements look like sums of eight terms.

$$\boxed{\alpha e_+ + \beta e_- + \gamma i_+ + \delta i_- + \ldots + \eta k_-}$$

build from this a quotient ring where we impose $\underbrace{}_{= \mathbb{H}}$

an equiv relation

$-x_+ = x_-$ for all $x \in \{e, i, j, k\}$

In the quotient, we'll have a basis $\{\overset{1}{\text{"}e\text{"}}, i, j, k\}$

$[e_+]$ $[i_+]$

$(\alpha - \beta)\cdot 1 + (\gamma - \delta)\cdot i + \ldots$

An elt of $\mathbb{H}$ is $(a \cdot 1 + b \cdot i + c\, j + d \cdot k)$.

$(\mathbb{H}, +) \cong \mathbb{R}^4$ just like $(\mathbb{C}, +) \cong \mathbb{R}^2$

$$(a + bi + cj + dk)(a' + b'i + c'j + d'k)$$
$$= \text{sum (by distributivity)}$$

so if there is a natural ring str, then it is determined by basic monomials. $bi \cdot cj = \underbrace{(b \cdot c)}_{\in \mathbb{R}} i \cdot j$

$$\boxed{i^2 = j^2 = k^2 = ijk = -1} \,\star \;.\; \Rightarrow \; ij = k, \; ji = -k \text{ and so on.}$$

Not too hard to see that this is a ring.

↳ would have to check
- every product follows from $\star$
- associativity.

$\mathbb{H}$ is called the ring of quaternions.

$\mathbb{C}$ 4d over $\mathbb{R}$

invented by Hamilton.

actually noncom.

com.

non com. "strictly skew field"

ring in which every non-zero elt is inv.

"strictly skew division ring".

Given $x = a + bi + cj + dk$

define $\bar{x} := a - bi - cj - dk$. "~~complex~~ quaternionic conjugate"

If $x \neq 0$ then $x\bar{x} = a^2 + b^2 + c^2 + d^2$ is a sum of real squares, at least of which is not zero, and so $x\bar{x} \neq 0$.

$\mathbb{R}$.

So $x\bar{x}$ is invertible. So x is invertible.

Closing comments:

- You can certainly repeat construction of $\mathbb{H}$ w/ $\mathbb{R} \rightsquigarrow \mathbb{Q}$ or $\mathbb{Z}$

  get versions of e.g. Gaussians $\mathbb{Z}[i]$.

- $Re(x) = \frac{x + \bar{x}}{2} \in \mathbb{R}$, $Im(x) = \frac{x - \bar{x}}{2} \in \mathbb{R}^3_{ijk}$

if $x \in \mathbb{H}$

$$Re(x \cdot y) = Re(x) \cdot Re(y) \pm Im(x) \bullet Im(y)$$

$$Im(x \cdot y) = Re(x)\, Im(y) + Im(x) \cdot Re(y)$$
$$\pm Im(x) \times Im(y).$$

Remark:

- Wedderburn's little theorem:

there are no strictly skew fields of finite order.

↳ I'll post a proof on Brightspace