Math 128B, Mon Feb 08

- Use a laptop or desktop with a large screen so you can read these words clearly.
- In general, please turn off your camera and mute yourself.
- Exception: When we do groupwork, please turn both your camera and mic on. (Groupwork will not be recorded.)
- Please always have the chat window open to ask questions.
- Reading for today and Wed: Ch. 14.
- PS01 due tonight.
- PS02 outline due Wed, full version due Mon Feb 15.
- Next problem session Fri Feb 12, 10:00–noon on Zoom.
- **Exam 1** in 2 weeks from today.

The characteristic of a ring

If we think of n*1 as the integer n, then the char(R) is the smallest n>0 such that n=0 in R. (Unless no such n, in which case char(R)=0.)

R a ring. If $n > 0$, $nx = x + \cdots + x$ (n times).

Definition

Characteristic of R is smallest positive integer n such that $nx = 0$ for all $x \in R$. If no such n, **characteristic 0**.

Theorem

Suppose R has multiplicative identity 1.
If additive order of 1 is $n < \infty$, characteristic n; if additive order of 1 is ∞, characteristic 0.

$\mathbb{Z}_n$ char n

$\mathbb{Z}$ " 0.

An integral domain has characteristic 0 or p (prime)

Contrapositive:

Theorem

If R is a commutative ring with unity and characteristic $n = ab$ $(1 < a, b < n)$, then R has zero-divisors.

Proof:

Observe:

$$(a \cdot 1)(b \cdot 1) = (ab)1$$

mult id.

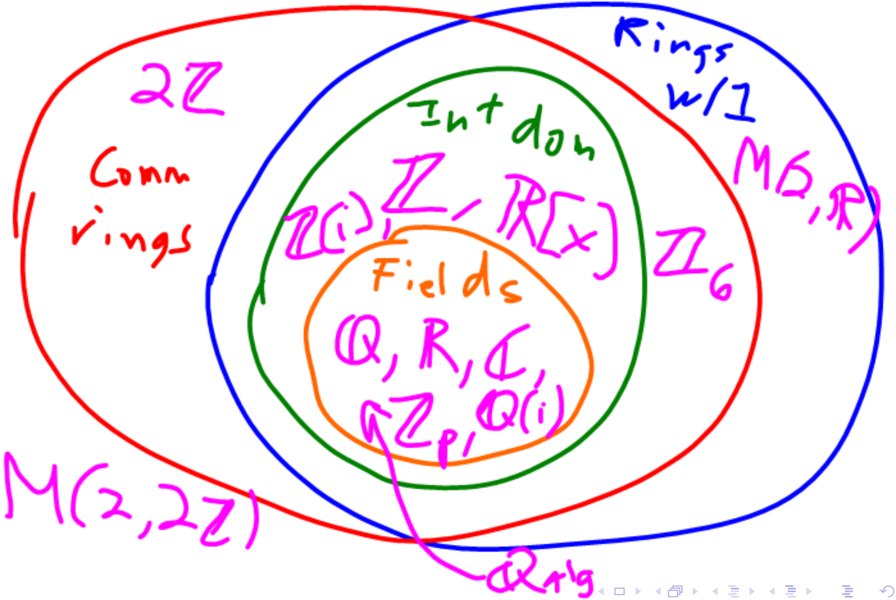
Proof: Induction (not super-interesting)

i.e. $$\underbrace{(1 + \cdots + 1)}_{a \text{ times}} \underbrace{(1 + \cdots + 1)}_{b \text{ times}} = \underbrace{1 + \cdots + 1}_{ab \text{ times}}$$

Then, since neither a*1 nor b*1 is = 0, since a,b <n, we have that the product of the two nonzero elements a*1 and b*1 is ab*1 = n*1 = 0.

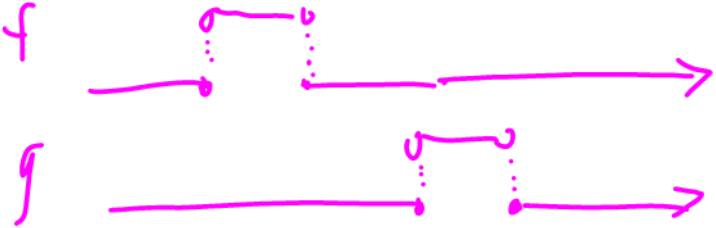
Classes of rings we have seen so far

Commutative rings. Rings with unity. Integral domains and fields.



$\mathbb{F}(\mathbb{R})$: all $f: \mathbb{R} \to \mathbb{R}$

This is a ring with unity (the constant function 1) that has zero-divisors.



Review: What are the main problems of group theory?

- **Structure:** Understand subgroups and cosets.
- **Homomorphisms and factor groups:** Understand homomorphisms, factor groups (i.e., normal subgroups), and relationship between them (1IT).
- **Classification:** Find a list of all possible groups of a given order (or: all abelian groups of a given order).

What are the main problems of ring theory?

comm

Main problems of ring theory:

- **Structure:** Understand subrings.
- **Homomorphisms and factor groups:** Understand homomorphisms, factor rings (i.e., **ideals**), and relationship between them (1IT).
- **Number theory:** Motivated by number theory:
  - **Factorization:** When do elements of a ring factor uniquely into "primes"?
    (Leads to solutions of integer equations.) $a^2+b^2=c^2$
  - **Field extensions:** If we start with (say) $\mathbf{Q}$, what is the structure of the smallest field containing some particular **algebraic number(s)** (e.g., $\sqrt{2}$, $\sqrt[3]{-5}$)?
    (Leads to solutions of polynomial equations.)

K-12!

Ideals

Definition

Let A be a sub**ring** of a ring R. To say that A is an **ideal** of R means that:

for every $r \in R$, **and not just every** $r \in A$

and every $a \in A$, both ra and ar are in A.

That is, A is closed not just under multiplication by elements of A (as is any subring), A is closed under multiplication by elements of the bigger ring R. (So when we talk about ideals, we have to be clear what the bigger ring R is.)

Ideal test

Recall that a nonempty $A \subseteq R$ is a subring of R if and only if A is closed under subtraction and multiplication. Combining this with the definition of ideal:

See, in linear algebra: subspace test

Theorem

step 0

Let $A \neq \emptyset$ be a subset of a ring R. Then A is an **ideal** *of R if and only if the following conditions all hold:*

- *(Closed under subtraction) For all $a, b \in A$, we have $a - b \in A$.*
- *(Closed under R-multiplication) For all $a \in A$ and $r \in R$, we have that $ra \in A$ and $ar \in A$.*

A/C: (A) $a, b \in A$

Closure under subtraction

(C) $a - b \in A$

(A) $a \in A$, $\boxed{r \in R}$

Closure under R-multiplication

(C) $ra, ar \in A$

Examples

- For any fixed $n \in \mathbf{Z}$, we have the ideal

$$n\mathbf{Z} = \{kn \mid k \in \mathbf{Z}\}$$

  of $R = \mathbf{Z}$.

One case: The even numbers 2Z are an ideal of Z.

- For $R = \mathbf{Z}[x]$, the set

ring of polys w/ integer coeffs

$$A = \{f(x) \mid f(0) \in 2\mathbf{Z}\}$$

  (i.e., polynomials with even constant term) is an ideal of $\mathbf{Z}[x]$.

Check:
* A closed under subtraction b/c if const terms of f(x), g(x) are even, so is the const term of f(x)-g(x).
* A closed under multiplication by R=Z[x] b/c if f(x) has an even constant term c, and g(x) is *any* poly in Z[x] with const term d (maybe not even), then f(x)g(x) has an even constant term cd.

Finitely generated ideals

Even more generally:

Theorem

Let R be a commutative ring, and let a be a fixed element of R. Then

$$A = \langle a \rangle = \{ra \mid r \in R\}$$

is an ideal of R, called the **principal ideal generated by** a.

Even more generally,

$$\langle a_1, \dots, a_k \rangle = \overbrace{\{r_1 a_1 + \cdots + r_k a_k \mid r_i \in R\}}^{\text{span!}}$$

is an ideal of R, called the **ideal generated by** $a_1, \dots, a_k$.

Proof that $\langle a \rangle$ is an ideal:

$\boxed{\neq \emptyset}$ $0a = 0 \in A$, so $A \neq \emptyset$

$\boxed{\text{closed -}}$

A) $x, y \in A$, so $x = ra$, $y = sa$ $\quad r, s \in R$

So $x - y = ra - sa$

$= \underbrace{(r-s)}_{\in R} a \in A$

C) $x - y \in A$

cl $-$

A) $x \in A$, $\boxed{s \in R}$

So $x = ra$ for $r \in R$

$\Rightarrow sx = sra = \underbrace{(sr)}_{\in R} a \in A$

C) $sx \in A$ (R comm)

cl R mult

Examples and non-examples

- Let $R = \mathbf{C}$ and let $A = \mathbf{R}$. Then A is a subring of R, but A is not an ideal of R because:
- Let $R = \mathbf{R}[x]$ and
$$A = \{f(x) \mid f(0) = 0\}.$$
Then $A = \langle x \rangle$, which means that A is a principal ideal (i.e., generated by a single element). It is true but very much not obvious that **every** ideal of $R = \mathbf{R}[x]$ is principal.
- Let $R = \mathbf{Z}[x]$, and let
$$A = \{f(x) \mid f(0) \in 2\mathbf{Z}\},$$
(again, all polynomials with even constant term). Then $A = \langle 2, x \rangle$, but A is not principal (again, true but very much not obvious).

Factor rings

Given an ideal A of a ring R, we can define the factor ring R/A as follows.

- **Set:** We define R/A to be the set of (additive) cosets of A in R, i.e.,
$$R/A = \{r + A \mid r \in R\}.$$
- **Operations:** For $r, s \in R$, we define
$$(r + A) + (s + A) = (r + s) + A$$
$$(r + A)(s + A) = (rs) + A.$$

As with groups, we might worry that these operations are not well-defined. However:

Theorem

The above operations are well-defined, and give R/A the structure of a ring.

Proof that factor rings are well-defined

As with groups, the hard part is to prove that the operations are well-defined.

$$(r + A) + (s + A) = (r + s) + A$$
$$(r + A)(s + A) = (rs) + A$$

An example that turns out to be familiar

Example: $R = \mathbf{Z}$, $A = 3\mathbf{Z}$. Then $R/A = \mathbf{Z}/3\mathbf{Z}$ has:

- **Elements:**

- **Addition:**

- **Multiplication:**

Another example that turns out to be familiar

Example: $R = \mathbf{R}[x]$, $A = \langle x^2 + 1 \rangle$. $R/A = \mathbf{R}[x]/\langle x^2 + 1 \rangle$ has:

- **Elements:**
- **Addition:**
- **Multiplication:**

In general: For $a \in R$, $R/\langle a \rangle$ is "R after setting $a = 0$".