Welcome to Math 128B, Wed Feb 03

- 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: Ch. 13.
- Reading for Mon: Ch. 14.
- PS01 outline due tonight, full version due Mon Feb 08.
- Problem session Fri Feb 05, 10:00–noon on Zoom.

Zero-divisors and integral domains

Definition

Let R be a commutative ring. A **zero-divisor** is some $a \neq 0$ in R such that there exists some $b \neq 0$ in R such that $ab = 0$.

> So if $ab = 0$ in a random ring R, it doesn't follow that $a = 0$ or $b = 0$.

Definition

An **integral domain** is a commutative ring with unity that has no zero-divisors.

Many familiar number-like rings are integral domains: $\mathbf{Z}$, $\overbrace{\mathbf{Q}, \mathbf{C}, \mathbf{R}}^{\text{fields}}$.

$\mathbf{Z}_6$ is **not** an integral domain because:

$2 \neq 0$
$3 \neq 0$ but $2 \cdot 3 = 0$ So $2, 3$ zero-divs

$\mathbb{Z} \oplus \mathbb{Z}$ not int dom:

$$\underbrace{(0,1)}_{\neq 0}\underbrace{(1,0)}_{\neq 0}=\underbrace{(0,0)}_{=0}$$

$$(a,b)(c,d)=(0,0)$$

Zero Factor Property: To say that R has ZFP means that for a,b in R, if ab=0, then either a=0 or b=0. → H $ab=0$

Having ZFP = being an integral domain.

C $a=0$ or $b=0$

Being an integral domain is equivalent to cancellation

TFAE = The Following Are Equivalent

Thm: Let R be a ring with unity. Then TFAE:

1. For $a, b, c \in R$, if $a \neq 0$ and $ab = ac$, then $b = c$. (Cancellation)
2. R is an integral domain.

Proof.

(A) Cancellation

(A) $a, b \in R$, $a \neq 0$, $ab = 0$

So $ab = 0 = a0$

By Cancellation (with c=0):

(C) $b = 0$

(C) ZFP

(A) ZFP

(A) $a, b, c \in R$, $a \neq 0$, $ab = ac$

So ab-ac = 0, so a(b-c)=0.
ZFP => a=0 or (b-c)=0.

But we assumed a is not = 0, so b-c=0.

(C) $b = c$

(C) Cancellation

Units and idempotents

Let R be a ring with unity. Recall:

Definition

To say that $a \in R$ is a **unit** of R means that there exists some $b \in R$ such that $ab = 1 = ba$.

Definition

To say that $a \in R$ is an **idempotent** means that $a^2 = a$.

Ex

$R = M(5, \mathbb{R})$ $a = \begin{bmatrix} 1 & & & & 0 \\ & 1 & & & \\ & & 1 & & \\ & & & 0 & \\ 0 & & & & 0 \end{bmatrix}$, $a^2 = a$

Fields

Definition

A **field** is a commutative ring R with unity such that every $a \neq 0$ in R is a unit.

Thm: If F is a field, then F is an integral domain.

A: $a, b \in F$, $\boxed{ab = 0}$, $a \neq 0$.

Mult by a^{-1}:

$\underbrace{a^{-1}a}_{1}b = a^{-1}0 = 0$

$1b = 0$

C: $b = 0$.

Given $ax = 0$, $a \neq 0$

Divide both sides by a, get x=0.

Solve for x

Converse false, as one integral domain that is not a field is: $\mathbb{Z}$

Z not a field b/c 2 has no mult inverse in Z
Z an integral domain b/c (axioms of the integers).

Finite integral domains are fields

Proof by Pigeonhole!

Suppose R is an finite ID, $a \in R$, $a \neq 0$.

(A) Consider $a, a^2, a^3, \ldots$

(B) By PP, $\exists\, k < n$ s.t. $1a^k = a^n = a^k a^{n-k}$

Cancel $\Rightarrow a^{n-k} = 1$. So $a \cdot (a^{n-k-1}) = 1$

(C) a is a unit.

B/c n>k, n-k>0, so n-k-1 >= 0, so a^{n-k-1} exists.

Cor: For p prime, the ring $\mathbf{Z}_p$ is a field.

Alt: By "GCD is a linear combination" (Ch 0 of Gallian), for 1 <= a <= p-1, b/c gcd(a,p)=1, we know that ax + py = 1 has an integer solution x, y in Z.

Mod p, we get ax = 1, i.e., a is a unit in Z_p.

$\rightarrow \mathbb{Z}$: ID, not field

$\rightarrow p$ prime: $\mathbb{Z}_p$ field

$\left(\text{set: } \{0, 1, \ldots, p-1\}, \text{ op'n } \begin{array}{l} + \pmod{p} \\ \cdot \pmod{p} \end{array}\right)$

$\rightarrow n$ not prime: $\mathbb{Z}_n$ not ID

$\Rightarrow \mathbb{Z}_n$ not field.

Example of a finite field that isn't $\mathbf{Z}_p$

A field of order 4:

$$\mathbf{Z}_2[\omega] = \{a + b\omega \mid a, b \in \mathbf{Z}_2\} = \{0, 1, \omega, \omega + 1\},$$

all mod 2

where $\omega^2 = \omega + 1$.

Multiplication table:

	0	1	w	$w+1$
0	0	0	0	0
1	0	1	w	$w+1$
w	0	w	$w+1$	1
$w+1$	0	$w+1$	1	w

$$w(w+1) = w^2 + w = w + 1 + w = 2w + 1 = 1$$

$$(w+1)^2 = w^2 + \cancel{2w} + 1$$

$$(w+1)^2$$

$$= w^2 + \cancel{2w} + 1$$

$$= w + 1 + 1 = w + 2 = w.$$

Two rules:

$$w^2 = w + 1$$

$$2 = 0.$$

The characteristic of a ring

$3x = x + x + x$

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**.

Examples:

- The most familiar systems of numbers ($\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$) have characteristic 0. I.e., you're used to working in rings with characteristic 0, so finite characteristic is the place where rings deviate from HS algebra most dramatically.
- $\mathbf{Z}_n$ has characteristic n.
- $\mathbf{Z}_2[\omega]$ (field of order 4) has characteristic 2.

Characteristic of a ring with unity

R a ring with multiplicative identity 1.

Theorem

If additive order of 1 *is* $n < \infty$*, characteristic* n*; if additive order of* 1 *is* ∞*, characteristic 0.*

Recall: Additive order of 1 is smallest $n > 0$ such that $n \cdot 1 = 0$. If no such n, order ∞.

Proof:

If additive order of 1 is infinite, can't have n>0 such that nx = 0 for all x in R, so char 0.

Spose order(1) = n. Then:

$k<n$: Not true $kx=0$ for all $x \in R$

For any $x \in R$, $nx = n1x = (n1)x = 0x$
$= 0$.

So char $= n$.

An integral domain has characteristic 0 or p

Contrapositive:

Theorem

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

Proof:

Classes of rings we have seen so far

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

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?

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.)
  - **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.)