Welcome to Math 128B

- 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. 13.
- PS00 due Mon Feb 01.
- PS01 outline due Wed Feb 03, full version due Mon Feb 08.
- Problem session Fri Feb 05, 10:00–noon on Zoom.

Rings (review)

A **ring** is a set R with binary operations $+$ and $\cdot$ (multiplication) such that:

(Abelian group, 4 axioms) The operation $+$ gives R the structure of an abelian group, with (additive) identity 0 and the inverse of a written $-a$. ~~So for $a, b, c \in R$.~~

(Associativity of multiplication) For all $a, b, c \in R$, $(ab)c = a(bc)$.

(Distributive) For all $a, b, c \in R$, $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.

Two particular types of rings:

(Rings with unity) If there exists $1 \in R$ such that $1a = a1 = a$ for all $a \in R$, and $1 \neq 0$, we say that 1 is a **unity** (or **multiplicative identity**) in R.

(Commutative rings) If $ab = ba$ for all $a, b \in R$, we say that R is **commutative**.

Real-valued functions

$\mathbb{F}(\mathbb{R}) =$ ring of R-valued fns w/ domain R.

Definition

Suppose X is any set. We define $\mathbf{F}(X)$, the **ring of real-valued functions on** X, to be:

- **Set:** Functions $f : X \to \mathbf{R}$.
- **Addition:** To add $f(x)$ and $g(x)$:

  To define f+g : X -> R, we declare that for all x in X:

  (f+g)(x) = f(x) + g(x)

  I.e., output of the sum is the sum of the outputs.
- **Multiplication:** To multiply $f(x)$ and $g(x)$:

  To define fg : X -> R, we declare, for all x in X:

  (fg)(x) = f(x)g(x)

  I.e., output of the product is the product of the outputs.

Can check that all of the axioms of a commutative ring with unity are satisfied. In particular:

* Additive identity element for F(X)

Additive identity is the *zero function*.

$$0(x) = 0$$

* Unity element (multiplicative) for F(X).

This is the constant function 1:

$$1(x) = 1$$

Particular case: X = real numbers

So F(X) is the ring of real-valued functions with domain R.

Examples of elements of F(X) include f(x) = x^2, g(x) = sin x.

The additive identity of $F(X)$ is the constant function 0. (AKA $f(x) = 0$.)

The unity element of $F(X)$ is the constant function 1.

Noncommutative rings

$n \geq 2$

"The" example of a noncommutative ring is $M(n, \mathbf{R})$:

- **Set:** $n \times n$ matrices with entries in $\mathbf{R}$.
- **Addition:** Matrix addition.
- **Multiplication:** Matrix multiplication.

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

Noncommutative ring with unity: Unity element is (multiplicative) identity matrix.

Units

Let R be a ring with ~~unity~~ multiplicative identity 1.

Definition

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

Examples: Units of $\mathbf{Z}$ are: $1, -1$

Every other element of Z is a non-unit in Z. E.g., 2 is not a unit in Z.

Units of $\mathbf{R}$ are: every real number except 0.

For any $a \in \mathbb{R}$, $\frac{1}{a}$ exists unless $a = 0$.

Note: When we ask "Is b a unit?" we have to specify which ring R we're working in, because answer depends on R.

Divisibility

d divides a in R $\Leftrightarrow a = dq, q \in R$

Let R be a commutative ring.

Definition

For $a, b \in R$, to say that a **divides** b in R, or that a is a **factor** of b in R, means that $b = aq$ for some $q \in R$.

Example: What are the factors of 6 in $\mathbf{Z}$?

$1, 2, 3, 6, -1, -2, -3, -6$

$\Rightarrow \pm 1, \pm 2, \pm 3, \pm 6$

Example: What are the factors of 6 in $\mathbf{R}$?

All nonzero real numbers in R are divisors of 6.

So questions of divisibility are much more interesting in rings like Z than in rings like R.

Ex. $\underset{a}{6} = \underset{d}{\pi}\underset{q}{\left(\frac{6}{\pi}\right)}$, so π divides 6 in $\mathbb{R}$.

Facts that are true inside any ring

Overall theme of the initial facts that are true in every ring:

* In any ring, we can use the manipulations of high school algebra, as long as we remember that mult might not be commutative.

* In any commutative ring, the formal manipulations of HS algebra work.

Theorem

R a ring, $a, b, c \in R$. Then:

- $a0 = 0a = 0$.
- $a(-b) = (-a)b = -ab$.
- $(-a)(-b) = ab$.
- $a(b-c) = ab - ac$ and $(b-c)a = ba - ca$.

And if $1 \in R$ is a unity element,

- $(-1)a = -a$.
- $\boxed{(-1)(-1) = 1.}$

Proving/explaining this is a good job interview question for community college teaching jobs.

See text and HW and practice problems.

Subrings

A sub(foo) is a subset of a (foo) that itself is a (foo) under same operation(s).

Definition

$S \subseteq R$ is a **subring** of R if S is a ring under the operations of R.

Subring test:

0

Theorem

*Suppose $S \subseteq R$ and $S \neq \emptyset$. Then S is a sub***ring** *of R if and only if*

1
- *S closed under subtraction, i.e.,*

  If $a, b \in S$ then $a - b \in S$

  A $a, b \in S$

  C $a - b \in S$

2
- *S closed under multiplication, i.e.,*

  If $a, b \in S$ then $ab \in S$.

  A $a, b \in S$

  C $ab \in S$

Applying the Subring Theorem

$$2\mathbf{Z} = \{ n \in \mathbf{Z} \mid n = 2k \text{ for some } k \in \mathbf{Z} \}.$$

Thm: $2\mathbf{Z}$ is a subring of $\mathbf{Z}$.

Outline:

0 ✓

$0 = 2(0)$, so

$0 \in 2\mathbb{Z}$.

C So $\exists x \in 2\mathbb{Z}$

1

A $a, b \in 2\mathbb{Z}$

$a = 2k$, $b = 2l$

for $k, l \in \mathbb{Z}$

⋮

$a - b = 2m$ $(m \in \mathbb{Z})$

C $a - b \in 2\mathbb{Z}$

2

A $a, b \in 2\mathbb{Z}$

C $ab \in 2\mathbb{Z}$

More vocabulary

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 $ab = 0$.

I.e., if $ab = 0$ in a ring R, doesn't mean 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: $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{C}$, $\mathbf{R}$.

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

Being an integral domain is equivalent to cancellation

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 $b = c$.
2. R is an integral domain.

Proof:

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 $ab = 1$.

Definition

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

Definition

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

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.)