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: Ch. 12. Reading for Mon: Ch. 13.
- PS00 due Mon Feb 01.
- PS01 outline due Wed Feb 03, full version due Mon Feb 08.
- Problem session Fri Jan 29, 10:00–noon on Zoom.

Tour of the course website

The course website is:

`http://www.timhsu.net/courses/128b/`

Breakout room activity 1

In a minute, I'll send everyone into breakout rooms in groups of 3–4 to answer the following question:

What is a notable fact about yourself?

(If nothing comes to mind, make something up!)

In each breakout room:

- Share your notable facts with each other.
- Learn each others' names.

Get ready to turn on your cameras and mics. (I'll pause the recording.)

Breakout room activity 2

Next, in breakout rooms, you'll answer the following question:

What is one important event in your mathematical life?

In each breakout room:

- Learn **someone else's** name and important event. (I'll visit each room to help you organize cyclically.)
- Be ready to share that person's important event when we get back to the main room. (Take notes!)

Get ready to turn on your cameras and mics again.

Some things you'll need to know from 128A

- Fundamentals of groups
- Subgroups and cosets
- Normal subgroups and factor groups
- Homomorphisms
- Examples: $\mathbf{Z}_n$, D_n, S_n, A_n, $G \oplus H$, finite abelian groups.

Rings

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 $a, b, c \in R$:

gp: Assoc: $(a+b)+c = a+(b+c)$
Identity: $0+a = a = a+0$
Inverse: $a+(-a) = 0 = (-a)+a$

Ab: Comm: $a+b = b+a$

(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 $(a+b)c = ac + bc$.

Other 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**.

Examples

- $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{C}$, $\mathbf{R}$
- $\mathbf{R}[x]$
- Ideals
- $\mathbf{F}(X)$, the real-valued functions on X
- $\mathbf{Z}[i]$
- $\mathbf{H}$
- $\mathbf{Z}_n$
- $M(n, \mathbf{R})$
- Operator algebras. . . .

Rings that are sets of numbers

- **Z** integers
- **Q** rationals
- **C** complexes
- **R** reals

later: polynomials (Ch 16), ideals (Ch 14)

- $\mathbf{Z}[i]$ $= \mathbb{Z}[\sqrt{-1}]$

  = { a+bi | a,b in Z } = Gaussian integers

  $i^2 = -1$; e.g. $3-4i \in \mathbb{Z}[i]$

  We'll see that arithmetic in Z[i] is just like arithmetic in Z (integers), but we'll also see that there are very similar rings in which arithmetic doesn't work as well. $\mathbb{Z}[\sqrt{-5}]$

- $\mathbf{Z}_n$ $\rightarrow$ $\mathbb{Z}/n\mathbb{Z}$

  integers mod n
  + mod n
  * mod n

Real-valued functions

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 $g(x)$:
- **Multiplication:** To multiply $f(x)$ and $g(x)$:

Noncommutative rings

"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.

Units

Let R be a ring with unity 1.

Definition

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

Examples: Units of $\mathbf{Z}$ are:

Units of $\mathbf{R}$ are:

Divisibility

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 $\mathbf{Z}$?

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

Facts that are true inside any ring

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,

- $(-1)a = -a$.
- $(-1)(-1) = 1$.

Proof of $(-a)(-b) = ab$, given previous two identities:

Subrings

Definition

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

Subring test:

Theorem

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

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

Examples of subrings

$\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{C}$, $\mathbf{R}$, $\mathbf{Z}[i]$:

$$\left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \middle| \, a, b \in \mathbf{R} \right\} \text{ in } M(2, \mathbf{R})$$

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"?
  - **Field extensions:** If we start with (say) $\mathbf{Q}$ and add in some **algebraic numbers** (e.g., $\sqrt{2}$, $\sqrt[3]{-5}$), what is the structure of the resulting ring?