Math 128A, Mon Nov 16

- 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. 12.
- PS09 due today. Outline for PS10 due Fri Nov 20.
- Problem session/exam review, Fri Nov 20, **9:00–11:00am** on Zoom.
- **EXAM 3, MON NOV 23.** on PS7-9
  Ch. 7-10

Rings

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

$(R,+)$ gp

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

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

$(R,\cdot)$ not gp

Other types of rings include:

(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**.

Axioms of an additive abelian group:

1. + associative: $(a+b)+c = a+(b+c)$
2. Additive identity: there exists 0 such $0+a = a = a+0$
3. Negatives: There exists $(-a)$ such that $a+(-a) = 0 = (-a)+a$
4. Commutative: $a+b = b+a$

Examples

- $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{C}$, $\mathbf{R}$
- $\mathbf{R}[x]$
- Ideals

Ch 14

Analog of normal subgps

- $\mathbf{R}(X)$ (X any set)
- $\mathbf{Z}[i]$
- $\mathbf{H}$ Quaternions
- $\mathbf{Z}_n$
- $M(n, \mathbf{R})$
- $\boxed{\text{Operator algebras. . .}}$

complicated!

Rings that are ~~sets of~~ number~~s~~ systems

- **Z** integers
- **Q** rationals
- **C** complex #s → $\{a+bi \mid a,b \in \mathbb{R}\}$ $\boxed{i^2=-1}$
- **R** reals
- $\mathbf{Z}[i]$

Gaussian integers:

Z[i] = {a+bi | a,b in Z}

Punchline: A ring is an axiomatic generalization of a system of numbers.

- $\mathbf{Z}_n$

Integers mod n:
Set = {0,...,n-1}
+ is addition (mod n)
* is multiplication (mod n)

Note: We only really rigorously proved Z_n is ab gp b/c Z_n = Z/nZ.

Real polynomials

$3x^3+17x^2+1x-5$

$$
\begin{array}{r}
3x^2+2x-1 \\
x+5 \\
\hline
15x^2+10x-5 \\
3x^3+2x^2-x
\end{array}
$$

Definition

We define $\mathbf{R}[x]$ to be:

- **Set:** Expressions of the form $a_n x^n + \cdots + a_1 x + a_0$, where $a_i \in \mathbf{R}$.
- **Addition:** Polynomial addition.
- **Multiplication:** Polynomial multiplication.

Can replace $\mathbf{R}$ with any commutative ring R, works the same, but coefficients multiplied in R. E.g., $\mathbf{Z}_2[x]$ is ring of polynomials with coefficients in integers mod 2, and all coefficient arithmetic is done mod 2.

In $\mathbb{Z}_3[x]$: Coeffs are in $\mathbb{Z}_3 = \{0,1,2\}$

$$
\begin{array}{r}
2x^2+x+1 \\
x+2 \\
\hline
x^2+2x+2 \\
2x^3+x^2+x \\
\hline
2x^3+2x^2 +2
\end{array}
$$

$2\cdot 2x^2 = 4x^2$
$= x^2$

$2x+x = 3x$
$= 0$

Math 127 $\quad \mathbb{Z}_2[x] \Longrightarrow \$$

Real-valued functions

$(X = \mathbb{R})$

Note: all functions in a ring of fns must have same domain and codomain

Definition

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

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

See: precalculus/calc textbook, "getting new functions from old" or "algebraic combinations of functions"

<u>Defn</u> $f+g : X \to \mathbb{R}$ by

$$(f+g)(x) = f(x) + g(x) \quad \forall x \in X$$

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

<u>Defn</u> $fg : X \to \mathbb{R}$

$$(fg)(x) = f(x)\, g(x) \quad \forall x \in X$$

not composition

Even larger generalization: $R(X)$ where R is any ring

All functions with domain X, codomain R.

Examples of noncommutative rings

- $M(n, \mathbf{R})$

M(n,R) is noncommutative (n>=2) b/c for n>=2, there will be A,B s.t. AB not eq to BA.

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

- The **quaternions** $\mathbb{H}$
  - **Set:** $\{a + bi + cj + dk \mid a, b, c, d \in \mathbf{R}\}$
  - **Addition:** Like polynomials in i, j, k.
  - **Multiplication:** Like polynomials in i, j, k, but:

$$-1 = i^2 = j^2 = k^2 \quad \underbrace{ij = -ji = k \quad jk = -kj = i \quad ki = -ik = j}_{ijk = -1}$$

* Quaternions give rule for both dot product and cross product (!!) in the usual i, j, k notation.

* You can make $ from quaternions b/c they make computations in rotations simpler.

Units

Non-ex: 2Z is a commutative ring with no multiplicative identity

$1 \notin Z$

so 2

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

multID

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 **Z** are:

$1 \cdot 1 = 1$ $(-1)(-1) = 1$

1 -1

non-units

$0a = 0 \neq 1$

0

only units in Z are ± 1

Units of **R** are:

All $a \neq 0$

R is a $\boxed{\text{field}}$

0

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 $\mathbf{R}$?

Example: Let $R = \mathbf{Z}[\sqrt{-5}] = \left\{a + b\sqrt{-5} \mid a, b \in \mathbf{Z}\right\}$.
What are the factors of 6 in 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?