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.

(日本本語を本書を本書を入事)の(の)

EXAM 3, MON NOV 23. On PS7-9 CL.7-10

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. (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.

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**.

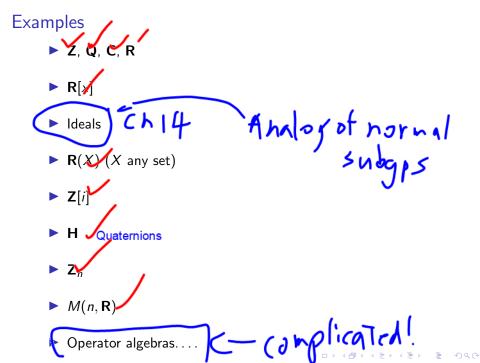
Axioms of an additive abelian group:

1. + associative: (a+b)+c = a+(b+c)

2. Additive identity: there exists $0 \operatorname{such} 0 + a = a = a + 0$

3. Negatives: There exists (-a) such that a+(-a) = 0 = (-a)+a

4. Commutative: a+b = b+a



Rings that are tets of number 4 > ystehs timals Sa+5: 4,60 (R) Q >reda R ► **Z**[*i*]

Gaussian integers:

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

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

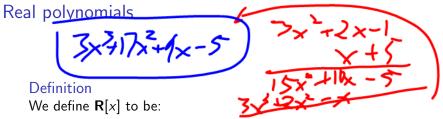
イロト 不得 トイヨト イヨト

3

► **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 $Z_n = Z/nZ$.



- 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 **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.

▲□▶ ▲□▶ ▲□▶ ▲□▶ □ のQで

In Z2[2]: Coeffs are in Z2= {0,1,2} ZX+X+1 $2.2x^{2} = 4x^{2}$ 7+2 =χ² $x^{2} + 2x + 2$ $2x^{2} + x^{2} + x$ 2x+x=3x = () 2x2+2x2 +2 Math 127 $Z_2(x) \rightarrow 4$

Real-valued functions

Definition

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

(X=IR)

Set: Functions $f : X \to \mathbf{R}$.

• Addition: To add f(x) and g(x):

Defn ftg X > R bx

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

Note: all functions in a ring

HX6X

< ロ > < 同 > < 回 > < 回 >

of fns must have same

domain and codomain

∀*x* €X (++)(x) = +(x) + q(x)

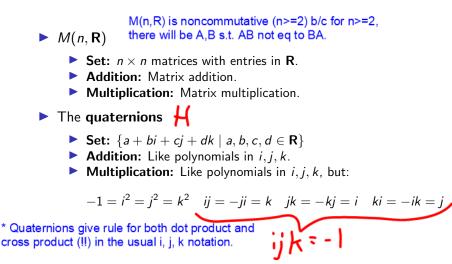
• Multiplication: To multiply f(x) and g(x): $Pefp + g : X \rightarrow \mathbb{R}$

(fy)(x)=f(x) g(x)

not compositior Even larger generalization: R(X) where R is any ring

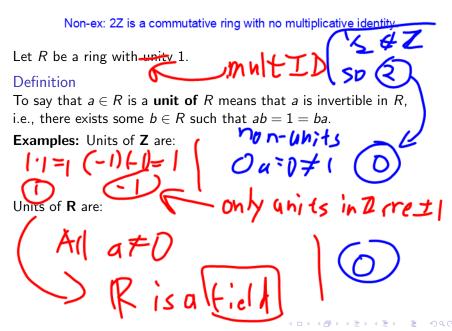
All functions with domain X, codomain R.

Examples of noncommutative rings



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

Units



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 $q \in R$.

▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ ●の00

Example: What are the factors of 6 in Z?

Example: What are the factors of 6 in R?

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

Facts that are true inside any ring

Theorem

$$R \text{ a ring, } a, b, c \in R.$$
 Then:
 $\bullet a0 = 0a = 0.$
 $\bullet a(-b) = (-a)b = -ab.$
 $\bullet (-a)(-b) = ab.$
 $\bullet a(b-c) = ab - ac \text{ and } (b-c)a = ba - ca.$
And if $1 \in R$ is a unity element,
 $\bullet (-1)a = -a.$
 $\bullet (-1)(-1) = 1.$

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 subring of R if and only if

▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ ●の00

► S closed under subtraction, i.e.,



S closed under multiplication, i.e.,

Examples of subrings

Z, **Q**, **C**, **R**, **Z**[*i*]:

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

▲□▶ ▲□▶ ▲ 三▶ ▲ 三▶ 三三 - のへぐ

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) Q and add in some algebraic numbers (e.g., √2, ³√-5), what is the structure of the resulting ring?