Math 128A, Wed Nov 18

- 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 Wed: Ch. 12. Reading for Mon Nov 30: Ch. 14.
- Outline for PS10 due Fri Nov 20; full version due Mon Nov 30.
- Problem session/exam review, Fri Nov 20, **9:00–11:00am** on Zoom. 128A 10:00am
- **EXAM 3, MON NOV 23.**

PS07-09

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 $-a$.

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

Note: In any ring, the + operation is always commutative, i.e., a+b=b+a.

But the multiplication may not be: ab may not be equal to ba.

Examples

polys

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

numbers

- $\mathbf{R}(X)$ (X any set)
- $\mathbf{Z}[i]$

fns

- $\mathbf{H}$
- $\mathbf{Z}_n$

(non-comm)

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

Units

(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**.

Let R be a ring with unity 1 (and therefore, $1 \neq 0$).

Definition

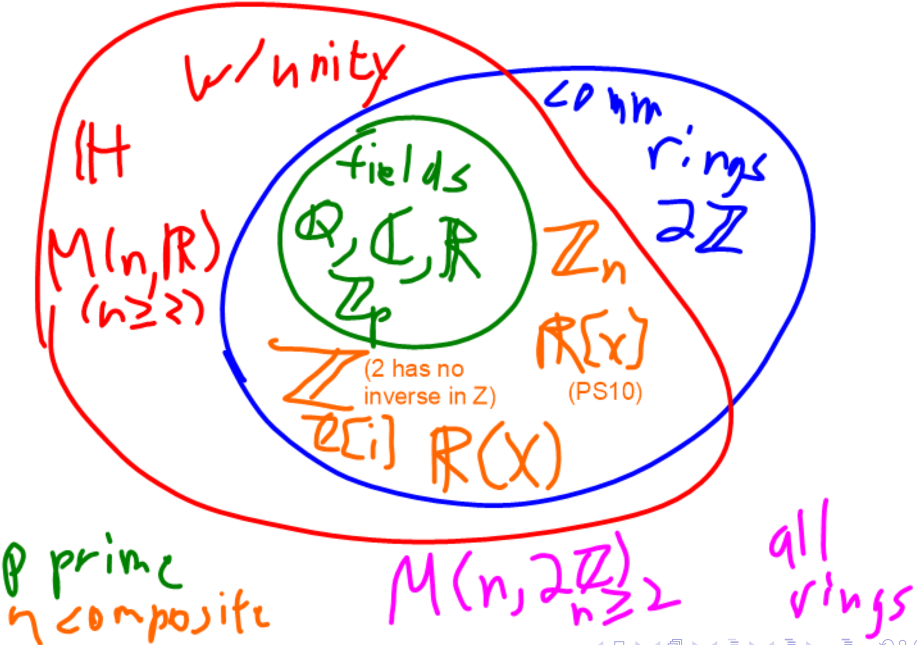
To say that $a \in R$ is a **unit of** R means that a is multiplicatively invertible in R, i.e., there exists some $b \in R$ such that $ab = 1 = ba$.

Definition

To say that R is a **field** means that R is a commutative ring with unity and every nonzero element of R is a unit of R.

Ex $\mathbb{R}$ is a field.

Venn diagram of examples of rings



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 $q \in R$. (q for quotient)

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

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

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

12: $6 = 12\left(\frac{1}{2}\right)$ $\quad 18$: $6 = 18\left(\frac{1}{3}\right)$ $\quad \pi$: $6 = \pi\left(\frac{6}{\pi}\right)$

$\boxed{\text{not } 0}$ $\quad 6 \neq 0a = 0$

Example: Let $R = \mathbf{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbf{Z}\}$.
How can we factorize 6 in R?

$6 = 2 \cdot 3$

$$6 = (1+\sqrt{-5})(1-\sqrt{-5})$$

Turns out that both of these factorizations of 6 cannot be broken down any further. In other words, 6 does *not* have unique factorization in R.

$$\begin{array}{ccc} & 6 & \\ \swarrow & & \searrow \\ 2 & & 3 \end{array} \qquad \begin{array}{ccc} & 6 & \\ \swarrow & & \searrow \\ 1+\sqrt{-5} & & 1-\sqrt{-5} \end{array}$$

UF: $6 = 2\cdot 3$ is "only" factor

In $\mathbb{Z}$ $\quad = 3\cdot 2$ into irreducibles

$\quad = (-2)\cdot(-3)$

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* $(b - c)a = ba - ca.$

$b - c = b + (-c)$

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

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

Job interview

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

$(-a)(-b) + a(-b)$

$= ((-a) + a)(-b)$ (DL)

$= 0(-b)$ (defn -a)

$= 0$ (prop. 1)

So (-a)(-b) is an additive inverse of a(-b) = -ab (prop. 2).

But ab is also an additive inverse of -ab, and since additive inverses are unique (Ch. 2!!), we must have that (-a)(-b)=ab.

Subrings

Definition

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

Subring test:

Theorem (Subring Test)

*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.,*

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

  (Alt: closed $+$ closed $-$)

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

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

Examples of subrings

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

$$
\begin{tikzcd}
\mathbb{C} \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{R} \arrow[d, dash] & \mathbb{Z}[i] \arrow[ddl, dash] \\
\mathbb{Q} \arrow[d, dash] & \\
\mathbb{Z} &
\end{tikzcd}
$$

Prove:

$S = \mathbb{Z}[\sqrt{-5}] =$

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

$\{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$

subring of $\mathbb{C}$.

$\boxed{\begin{aligned} \delta^2 &= -5 \\ \delta &= \sqrt{-5} \end{aligned}}$

Pf $0 \in S$, so $S \neq \emptyset$

Closed −

(A) $a+b\delta,\ c+d\delta \in S$

$(a,b,c,d \in \mathbb{Z})$

(You try)

(C) $(a+b\delta)-(c+d\delta) \in S$

Closed ·

(A) $a+b\delta,\ c+d\delta \in S$

$(a,b,c,d \in \mathbb{Z})$

$$(a+b\delta)(c+d\delta)$$

$$= ac+(bc+ad)\delta + bd\delta^2$$

$$= \underbrace{(ac-5bd)}_{\in\mathbb{Z}} + \underbrace{(bc+ad)}_{\in\mathbb{Z}}\delta$$

(C) $(a+b\delta)(c+d\delta) \in S$

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?