Math 128A, Mon Nov 30

- 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.
- Last reading in the course: Ch. 14.
- PS10 due tonight; outline for PS11 due Wed Dec 02.
- Problem session, Fri Dec 04, 10:00am–noon on Zoom.
- ~~**EXAM 3,**~~ **TUE DEC 15.** 7:15-9:30 AM!!!!!
  FINAL EXAM

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

(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**.

Think: Rings axiomatize the properties of a number system.

Question: What is the difference between the ring of polynomials with coefficients in R and the ring of real-valued functions on R?

Surface answer: Every real polynomial defines a function on R, but not every function on R comes from a polynomial (e.g., exponential function).

Deeper answer: In 128B, we look at polynomials not just as functions, but also (and more importantly) as abstract algebraic expression in their own right. It turns out to be important to think of $p(x) = x^2 + 4x + 5$ as an algebraic expression independently of plugging something into it.

Review: What are the fundamental problems of group theory?

From 30,000 ft:

- **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).

Classifications that we've done (or at least understood):
* All finite abelian groups
* Groups of order p, order 2p (not necessarily abelian), order p^2
* Orders 1, 2, 3, 4, 5, 6, 7, (not 8), 9, 10, 11. 8 has additional complications, and 12 has new types of groups.

What are the fundamental problems of ring theory?

Gps	Rings
$N \trianglelefteq G$	A ideal of R

- **Structure:** Understand subrings.
- **Homomorphisms and factor ~~groups~~ rings:** Understand homomorphisms, factor rings (which are defined by **ideals**, as we'll see), 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?

Background motivation: Solving equations!!

In $\mathbb{Z}[\sqrt{-5}]$: $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$

Ideals

Subring Test:

* (A nonempty)
* A closed under subtraction
* A closed under multiplication

Definition

Let A be a sub**ring** of a ring R. To say that A is an **ideal** of R means that:

$$\text{for every } r \in R, \textbf{ and not just every } r \in A$$

and every $a \in A$, both ra and ar are in A.

That is, A is closed not just under multiplication by elements of A (as is any subring), A is closed under multiplication by elements of the bigger ring R. (So when we talk about ideals, we have to be clear what the bigger ring R is.)

Note: Ideals are very different from subgroups in several ways.
E.g., every subgroup of a group G contains the identity e.
But even though every subring contains 0, and therefore every ideal contains 0, if an ideal A of R contains 1, then A must contain *all* of R.

Ideal test

Recall that a nonempty $A \subseteq R$ is a subring of R if and only if A is closed under subtraction and multiplication. Combining this with the definition of ideal:

Theorem

Let $A \neq \emptyset$ be a subset of a ring R. Then A is an **ideal** *of R if and only if the following conditions all hold:*

- *(Closed under subtraction) For all $a, b \in A$, we have $a - b \in A$.*
- *(Closed under R-multiplication) For all $a \in A$ and $r \in R$, we have that $ra \in A$ and $ar \in A$.*

A/C: (A) $a, b \in A$ | (A) $a \in A$, $\boxed{r \in R}$

(A closed under subtraction) | (A closed under R-mult)

(C) $a - b \in A$ | (C) $ra \in A$, $ar \in A$

Examples

Even numbers are:
* closed under subtraction
* closed under mult by *any* integer, even or odd

- For $R = \mathbf{Z}$, we have the ideal

$$A = 2\mathbf{Z} = \{2k \mid k \in \mathbf{Z}\}$$ even #s!

  of $R = \mathbf{Z}$.
- More generally, for any fixed $n \in \mathbf{Z}$, we have the ideal

$$n\mathbf{Z} = \{kn \mid k \in \mathbf{Z}\}$$

  of $R = \mathbf{Z}$. (all multiples of that fixed n)
- For $R = \mathbf{R}[x]$, the set

$$A = \{f(x) \mid f(0) = 0\}$$

  (i.e., polynomials with constant term 0) is an ideal of $\mathbf{R}[x]$.

Finitely generated ideals

Even more generally:

Theorem

Let R be a commutative ring, and let a be a fixed element of R. Then

$$\langle a \rangle = \{ra \mid r \in R\}$$

is an ideal of R, called the **principal ideal generated by** a.

Even more generally,

all R-linear combinations of a_1,...,a_k

$$\langle a_1, \ldots, a_k \rangle = \{r_1 a_1 + \cdots + r_k a_k \mid r_i \in R\}$$

is an ideal of R, called the **ideal generated by** $a_1, \ldots, a_k$.

Proof that $\langle a \rangle$ is an ideal:

$A = \langle a \rangle = \{ra \mid r \in R\}$

$\forall x, y \in \langle a \rangle$

So $x = ra$, $y = sa$ for $r, s \in R$.

$x - y = ra - sa = (r-s)a$ (DL)

Let $t = r - s \in R$ b/c R ring

So $x - y = ta$ for some $t \in R$.

C $x - y \in \langle a \rangle$ ☺

A $x \in \langle a \rangle$ $\boxed{r \in R}$

So $x = as$ for some $s \in R$

So $rx = ras = (rs)a$ (R comm)

Let $t = rs \in R$ b/c R ring

So $rx = at$ for some $t \in R$

C $rx \in \langle a \rangle$

Examples and non-examples

- Let $R = \mathbf{R}$ and let $A = \mathbf{Z}$. Then A is a subring of R, but A is not an ideal of R because:

  $2 \in A, \pi \in R$, but $2\pi \notin A$.

- Let $R = \mathbf{R}[x]$ and

  $$A = \{f(x) \mid f(0) = 0\}.$$

  Then $A = \langle x \rangle$, which means that A is a principal ideal (i.e., generated by a single element). It is true but very much not obvious that **every** ideal of $R = \mathbf{R}[x]$ is principal.

- Let $R = \mathbf{R}[x, y]$ (real polynomials in two variables, and let

  $$A = \{f(x, y) \mid f(0, 0) = 0\},$$

  which is again the set of all (two-variable) polynomials with constant term 0. Then $A = \langle x, y \rangle$, but A is not principal (again, true but very much not obvious).

Factor rings

Given an ideal A of a ring R, we can define the factor ring R/A as follows.

- **Set:** We define R/A to be the set of (additive) cosets of A in R, i.e.,
$$R/A = \{r + A \mid r \in R\}.$$
- **Operations:** For $r, s \in R$, we define
$$(r + A) + (s + A) = (r + s) + A$$
$$(r + A)(s + A) = (rs) + A.$$

As with groups, we might worry that these operations are not well-defined. However:

Theorem
The above operations are well-defined, and give R/A the structure of a ring.

Proof that factor rings are well-defined

As with groups, the hard part is to prove that the operations are well-defined.

$$(r + A) + (s + A) = (r + s) + A$$
$$(r + A)(s + A) = (rs) + A$$