Math 128B, Wed Feb 10

- 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. 14. Reading for Mon: Ch. 15
- PS02 outline due tonight, full version due Mon Feb 15.
- Next problem session Fri Feb 12, 10:00–noon on Zoom.
- **Exam 1** in 12 days.

Ideals and the ideal test

Definition

Let A be a sub**ring** of a ring R. To say that A is an **ideal** of R means that: A closed under R-multiplication, not just A-multiplication

for every $r \in R$, **and not just every** $r \in A$

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

Theorem (Ideal test)

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 $ar \in A$.*

Examples and non-examples

$\mathbb{R}$ $\mathbb{C}$ $\mathbb{R}$

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

  $\mathbb{C}$

  $1 \in \mathbb{R}$

  $i \in \mathbb{C}$

  $i \cdot 1 = i \notin \mathbb{R}$

  polys w/ R coeffs

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

  const term = 0

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

  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 $R = \mathbf{Z}[x]$, and let

  (integer coeffs) const term even

  $$A = \{f(x) \mid f(0) \in 2\mathbf{Z}\},$$

  (again, all polynomials with even constant term). Then $A = \langle 2, x \rangle$, but A is not principal (again, true but very much not obvious).

In R[x], how did we know that A = {f(x) | f(0)=0} is <x>?

* Right now, experimentation and hard work.
  - Experimentation shows that the "simplest" element in A is x
  - Once you guess that A = <x>, you can prove that by set equality proof

* Eventually, we'll prove that every ideal of R[x] is principal, and as part of that proof, we'll prove that any nonzero ideal A of R[x] is generated by any nonzero element of lowest possible degree.

Norm subgps : Factor gps
as
Ideal : Factor rings

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

Define +, * of two cosets by +, * of their coset reps

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

Defn of add gp R/A.

also mult

We might worry that these operations are not well-defined, but:

Theorem

The above is well-defined, and R/A is a ring.

Note that if R is a ring with unity, then the additive and multiplicative identities of R/A are $0 + A$ and $1 + A$, respectively.

Proof that factor rings are well-defined

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

$$\left.\begin{array}{c}(r+A)+(s+A)=(r+s)+A\end{array}\right\} \text{already done}$$

$$\boxed{(r+A)(s+A)=(rs)+A}$$

S'pose $r' \in r+A$, $s' \in s+A$

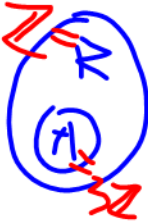
so $r' = r+a$, $s' = s+b$ $a,b \in A$.

$(r'+A)(s'+A)$

$= r's'+A$

$= (r+a)(s+b)+A$

$$= rs + \underbrace{\underbrace{\overset{\in A}{a}\,\overset{\in R}{s}}_{\in A} + \overbrace{\underset{\in R}{r}\,\underset{\in \cancel{A}}{b}}^{\in A} + \underbrace{ab}_{\in A}}_{\in A} + A$$



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

An example that turns out to be familiar

$0+A, 1+A, 2+A$ partition $\mathbb{Z}$

Example: $R = \mathbf{Z}$, $A = 3\mathbf{Z}$. Then $R/A = \mathbf{Z}/3\mathbf{Z}$ has:

$\mathbb{Z}_3 =$

- **Elements:** $A = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$

R/A

$0+A = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$
$1+A = \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\}$
$2+A = \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\}$

3 elts

- **Addition:**

$(2+A)+(1+A) = 3+A$
$= 0+A$

Note: $r+A = s+A \iff r \equiv s \pmod 3$

- **Multiplication:**

"$2+1=0$ in $\mathbb{Z}/3\mathbb{Z}$"

$(2+A)(2+A) = 4+A = 1+A$ (b/c 1, 4 in same coset)

Since addition in any ring is commutative ($r+s=s+r$), we see that
$r+A = A+r$
$s+A = A+s$

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

But we don't necessarily have $rs+A$ equal to $sr+A$, b/c mult need not be commutative.

$$(-1+A)(-1+A) = 1+A$$
$$= (2+A)(2+A)$$

(as in pf)

$$(1+A)(r+A) = 1\cdot r + A = r+A$$

Another example that turns out to be familiar

Example: $R = \mathbf{R}[x]$, $A = \langle x^2+1 \rangle$. $R/A = \mathbf{R}[x]/\langle x^2+1\rangle$ has:

- **Elements:** $x^2 + A = -1 + A$, $x^3 + A = -x + A$, ...

So for any f(x) = R[x], we can reduce f(x) + A to ax+b + A.

So $\mathbb{R}/A = \{ax+b+A \mid a,b \in \mathbb{R}\}$.

- **Addition:** $(ax+b)+A + (cx+d)+A$
  $= (a+c)x + (b+d) + A$
- **Multiplication:** $((ax+b)+A)((cx+d)+A)$
  $= acx^2 + (ad+bc)x + bd + A$

In general: For $a \in R$, $R/\langle a\rangle$ is "R after setting $a = 0$".

$$x^2+1 \in \langle x^2+1\rangle = A$$

$$\Rightarrow \; x^2+1+A = A$$

$$x^2+A = -1+A$$

So: In R/A, "x^2+1 = 0", i.e., in R/A, we set x^2+1 = 0.

So in R/A, "x^2 = -1" i.e., the element x+A of R/A is what we usually call i.

$$= (ad+bc)x + (bd-ac) + A$$

ex: $\mathbb{Z}_3[i]$, $\mathbb{Z}_p[i]$

Point: If you remove +A and replace x with i, we see that R[x]/<x^2+1> is isomorphic to the ring of complex numbers.

Prime and maximal ideals

Let R be a commutative ring, and let A be an ideal of R.

Defn: To say that A is **prime** means that if $a, b \in R$ and $ab \in A$, then either $a \in A$ or $b \in A$.

$R = \mathbb{Z}, A = p\mathbb{Z}$

Defn: To say that A is **maximal** means that $A \neq R$ and if B is an ideal of R and $A \subseteq B \subseteq R$, then either $A = B$ or $B = R$.

lattice of ideals

Examples of prime and maximal ideals

Ex: Let $p \in \mathbf{Z}$ be prime. Then $\langle p \rangle = p\mathbf{Z}$ is a prime ideal of $\mathbf{Z}$ because:

Ex: But $\langle p \rangle = p\mathbf{Z}$ is also maximal: Suppose $p\mathbf{Z} \subseteq B \subseteq \mathbf{Z}$, B is an ideal, and suppose $b \in B$ is not contained in $p\mathbf{Z}$. Then b is not a multiple of p, and so $\gcd(b, p) = 1$. So by "GCD is a linear combination":

But not every prime ideal is maximal

Ex: Let $R = \mathbf{Z}[x]$ and let $A = \langle x \rangle = \{f(x) \in \mathbf{Z}[x] \mid f(0) = 0\}$.
Then A is a prime ideal:

But A is not maximal, since $A \subset \langle 2, x \rangle \subset \mathbf{Z}[x]$.

A is prime if and only if R/A is an integral domain

Let R be a commutative ring with unity and let A be an ideal of R. TFAE:

1. A is prime.
2. R/A is an integral domain.

A is maximal if and only if R/A is a field

Let R be a commutative ring with unity and let A be an ideal of R. TFAE:

1. A is maximal.
2. R/A is a field.