Math 128B, Mon Feb 15

- 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. 15.
- PS02 due tonight; PS03 outline due Wed, full version due Mon Feb 22.
- Next problem session Fri Feb 19, 10:00–noon on Zoom.
- **Exam 1 now on Wed Feb 24**, in 9 days.

Extra office time today: 1-1:30pm; regular time 2-3.

Struggle

Paul Zeitz: Problems and exercises

PS01 wasn't meant to be easy, and PS02 even more so.

- The problem sets are challenging because everyone learns through struggle.
- If you don't get all of the problems the first time around, or even after trying many times — that's OK! I'm not expecting that you get 100% on the homework, even after revision.
- Remember: The most productive learning experiences are **problems**, where your method of solution may not be clear, and you may not even know how to get started. That's where you really start to understand the material.
- Corollary: You need to do the homework **yourself**, without outside "help". Think: There are two times you can choose to try a class of problems for the very first time, on the problem sets, or on an exam.

Prime and maximal ideals

Non-example: 6Z = <6> is an ideal of Z.

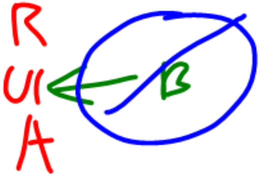
2, 3 in Z and 2*3 is in 6Z, but neither 2 nor 3 are in 6Z.

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 $b \in A$.

A proper

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 $B = R$.



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:

If a,b in Z and ab in pZ
=> ab = kp for some integer k

=> p divides ab
=> Either p divides a or p divides b

Defn of prime ideal imitates this.

=> Either a is in pZ or b is in pZ.

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":

There exist x,y in Z such that bx + py = 1.

But b, p are in the ideal B, so bx, py are in B, so 1 = bx + py is in B.

Since 1 is in B, every multiple r*1 of 1 is in B, so B=Z.

So there exists no ideal B strictly between pZ and Z.

$6\mathbb{Z}$ not max'l in $\mathbb{Z}$:

$$6\mathbb{Z} \subset 3\mathbb{Z} \subset \mathbb{Z}$$

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:

If $f(x)g(x) \in A$
$\Rightarrow f(0)g(0) = 0$
$\Rightarrow$ one of $f(0), g(0) = 0$
$\Rightarrow$ " " $f(x), g(x) \in A$.

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

0 const

any const.

All integer polynomials with even constant term.

$\mathbb{Z}[x]$ "Z bracket x"

$$= \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \mid \text{each } a_i \in \mathbb{Z}\}$$

$\mathbb{Z}_2[x]$ "Z two bracket x"

$$= \{(\text{same}) \mid a_i \in \mathbb{Z}_2\}$$

$$\mathbb{R}[x] = \{(\text{same}) \mid a_i \in \mathbb{R}\}$$

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 A prime ideal

A $r+A, s+A \in R/A$

$(r+A)(s+A) = 0+A$

$rs+A = 0+A$

$\Rightarrow rs \in A$

$\Rightarrow r \in A$ or $s \in A$

C $r+A = 0+A$ or $s+A = 0+A$

ID in R/A

A R/A is ID.

A $r, s \in R$

$rs \in A$

So $(r+A)(s+A)$

$= rs + A$

$= 0 + A$

b/c $rs \in A$

$\Rightarrow r+A = 0+A$ or $s+A = 0+A$

C $r \in A$ or $s \in A$

Big takeaway:

$r+A = 0+A \iff r \in A$

More generally:

$r+A = s+A \iff r \in s+A$

See Chapter 7 for reviewing this point!

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.

(Assuming R is a ring with unity)
Since every field is an ID,
A max'l => A prime.

See Gallian for details.

One useful fact on PS02: Suppose R is a ring with unity
If <a>=R

then 1 is in <a> = {ax | x in R}

so ax = 1 for some x in R

so a has a multiplicative inverse.

Ring homomorphisms

Definition

Let R and S be rings. To say that $\varphi : R \to S$ is a **homomorphism** (of rings) means that for all $a, b \in \cancel{\mathbf{R}}$ R

$$\varphi(a+b) = \varphi(a) + \varphi(b), \qquad \varphi(ab) = \varphi(a)\varphi(b).$$

If φ is also bijective, we say that φ is an **isomorphism** (of rings).

I.e., ring homomorphisms preserve **both** ring operations, $+$ and $\cdot$.

Now: We'll do the analogue of everything in Ch 10, but for rings and ring homomorphisms.

“Natural” examples

(complex conjugation)

Example: $\varphi : \mathbf{C} \to \mathbf{C}$ defined by $\varphi(a + bi) = a - bi$.
Then φ is a ring homomorphism: a+bi, c+di in C.

$$\varphi((a+bi)(c+di))$$
$$= \varphi((ac-bd)+(ad+bc)i)$$
$$= (ac-bd)-(ad+bc)i$$

multiply, then apply phi

$= \checkmark$

$$\varphi(a+bi)\varphi(c+di)$$
$$= (a-bi)(c-di) = (ac-bd) + (-ad-bc)i$$

Example: Let $R = \mathbf{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbf{Q}\}$.
Define $\varphi : R \to R$ by $\varphi(a + b\sqrt{2}) = a - b\sqrt{2}$.
Same kind of calculation shows that φ is a ring homomorphism.

Also need to check + preserved; not as interesting.

A class of examples

Example: Find all ring homomorphisms $\varphi : \mathbf{Z}_{20} \to \mathbf{Z}_{30}$.

S'pose $\varphi : \mathbb{Z}_{20} \to \mathbb{Z}_{30}$ homom.

Then $\varphi(n \cdot 1) = n\varphi(1)$. So just need $\varphi(1)$.

$$0 = \varphi(0) = \varphi(\underset{\text{mod } 20}{20} \cdot 1) = \underbrace{20\,\varphi(1)}_{\text{mod } 30}.$$

So $\varphi(1) \in \{0, 3, 6, 9, 12, 15, 18, 21, 24, 27\}$

Also $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1)\varphi(1)$.

So if $\varphi(1) = r$ in $\mathbb{Z}_{30}$,

$a^2 = a$ in $\mathbb{Z}_{30}$.

Sol'ns: $0^2 = 0$, $6^2 = 6$, $15^2 = 15$, $21^2 = 21$

So $\varphi(1) = 0, 6, 15,$ or 21.

Check: If $\varphi(1) = 6$, $\varphi(x) = 6x$.

So $\varphi(xy) = 6xy$

$\varphi(x)\varphi(y) = (6x)(6y)$ in $\mathbb{Z}_{30}$

$= 36xy = 6xy$ ✓

$20\varphi(1) = 0$ in $\mathbb{Z}_{30}$.

$\varphi(1) = 1$? $\quad 20 \cdot 1 \neq 0$ in $\mathbb{Z}_{30}$ $\quad$ NO

$\varphi(1) = 2$? $\quad 20 \cdot 2 = 10 \neq 0$ $\quad$ "

$\varphi(1) = 3$? $\quad 20 \cdot 3 = 0$ in $\mathbb{Z}_{30}$ $\quad$ Yes

$\varphi(1) = 4$?

$\vdots$

We can also use Gallian Ch 4 to find all elements of Z_30 that have additive order dividing 20.

Homomorphism preserve ring-theoretic properties

Just like Ch. 10 and groups!
Suppose $\varphi : R \to S$ is a ring homomorphism, A an ideal of R, and B an ideal of S.
Defn: $\varphi^{-1}(B) = \{r \in R \mid \varphi(r) \in B\}$, and $\ker \varphi = \varphi^{-1}(\{0\})$.
Thm:

- $\varphi(nx) = n\varphi(x)$ and $\varphi(x^n) = \varphi(x)^n$.
- $\varphi(A)$ is an ideal of:
- $\varphi^{-1}(B)$ is an ideal of:
- If $1 \in R$, $S \neq \{0\}$, and φ is onto, then $\varphi(1)$ is the multiplicative identity of S.
- φ is injective if and only if $\ker \varphi = \{0\}$.

Important facts about group homomorphisms

Suppose $\varphi : G \to H$ is a group homomorphism. Recall that:

- **Kernels are normal subgroups:** $\ker \varphi \lhd G$.
- **Normal subgroups are kernels:** If $N \lhd G$, define $\gamma : G \to G/N$ by $\gamma(a) = aN$. Then $\ker \gamma = N$.
- **First isomorphism theorem:**

Important facts about ring homomorphisms

Suppose $\varphi : R \to S$ is a right homomorphism. Then:

- **Kernels are ideals:** $\ker \varphi$ is an ideal of R.
- **Ideals are kernels:** If A is an ideal of R, define $\gamma : R \to R/A$ by $\gamma(r) = r + A$. Then $\ker \gamma = A$.
- **First isomorphism theorem:**