MAS439 Lecture 4
Ideals

October 6th

Motivation for ideals: kernels

Let $\varphi : R \to S$ be a ring homomorphism, we have $\mathrm{Im}(\varphi) \subset S$ and $\ker(\varphi) \subset R$.

Our study of subrings was motivated by $\mathrm{Im}(\varphi)$:

- The image of φ is a subring
- Every subring $S \subset R$ is the image of a homomorphism: the inclusion $i : S \to R$

What about the kernel of φ?

The kernel $\ker \varphi$ is “almost” a subring

- $\ker(\varphi)$ is closed under addition:

$$\varphi(k_1 + k_2) = \varphi(k_1) + \varphi(k_2) = 0_R + 0_R = 0_R$$

- $\ker(\varphi)$ is closed under multiplication:

$$\varphi(k_1 \cdot k_2) = \varphi(k_1) \cdot \varphi(k_2) = 0_R \cdot 0_R = 0_R$$

- $\ker(\varphi)$ will almost never contain the identity:

$$\varphi(1_R) = 1_S \neq 0_S$$

But it satisfies a stronger property:

If $k \in \ker(\varphi)$, and $r \in R$ an arbitrary element, then $r \cdot k \in \ker(\varphi)$:

$$\varphi(r \cdot k) = \varphi(r)\varphi(k) = \varphi(r)0_S = 0_S$$

Ideals abstract away those properties of the kernel

Definition

An ideal $I \subset R$ is a nonempty subset that is

- Closed under addition: $I + I \subset I$
- Closed under multiplication by elements of R: $rI \subset I$.

Remarks:

- Ideals are additive subgroups. Closed under addition, and if $r \in I$, then $(-1) \cdot r = -r \in I$.
- If $1 \in I$, then $I = R$, since $r = r \cdot 1 \in I$.

First examples of ideals

- In any ring R, the set $\{0_R\}$ is an ideal
- In any ring R, the set R is an ideal
- The set $n\mathbb{Z} = \{k \in \mathbb{Z} | n \,\mathrm{divides}\, k\}$
- The even numbers in $\mathbb{Z}/12\mathbb{Z}$ form an ideal
- The set $\{0\} \times R \subset S \times R$ is an ideal in $S \times R$
- The set $I \subset R[x]$ of polynomials whose constant term is 0 is an idea

Another set of examples

Let X be any set; $x \in X$ any element. The set of all functions vanishing at x is an ideal:

$$I_x = \{f \in Fun(X, \mathbb{R}) : f(x) = 0\}$$

The ideal $I_x = \ker \mathrm{ev}_x$.
The same holds true for rings of continuous functions, or polynomial functions.

The ideals of $\mathbb{Z}$

Lemma

Any ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some n.

Proof.

Let $I \subset \mathbb{Z}$ be an ideal; assume $I \neq \{0\}$, and let n be the smallest nonnegative element of I. We claim that $I = n\mathbb{Z}$.
We have $n\mathbb{Z} \subset I$.
To prove that $I \subset n\mathbb{Z}$, suppose not, and let $x\ inI, x \notin n\mathbb{Z}$. We have $x = qn + r$, for some $0 \leq r < n$. $r \neq 0$, as $x \notin n\mathbb{Z}$. But $r = x - qn \in I$, which contradicts n being the smallest positive element of I.

$\square$

♫ Let's all go to the lobby ♫
♫ Let's all go to the lobby ♫
(2 minute intermission)

Generating Ideals

Parallel to what we did yesterday with subrings, we now want to discuss generating ideals.

Definition ideal

Let $T \subset R$ a subset. The *ideal generated by* T, denoted (T), should be the smallest ideal of R containing T.

It's not clear that this is defined, and it's not how we normally think of generators as "mashing things together". Hopefully you can see what's coming next..

Intersections of ideals are ideals

Lemma

Suppose that I_j, for $j \in J$ an index set, is set of ideals of R. Then $\bigcap_{j \in J} I_j$ is an ideal.

Proof.

Let I denote the intersection of all the I_j.

- I is nonempty since $0 \in I_j$ for each j, so $0 \in I$.
- I is closed under addition: $r, s \in I$ means $r, s \in I_j$ for all j, so $r + s \in I_j$ for all j, so $r + s \in I$.
- I is closed under multiplication by arbitrary elements of R: if $i \in I$ and $r \in R$, then $i \in I_j$ for all j, so $ri \in I_j$ for all j since $_j$ an ideal, so $ri \in I$

$\square$

The elegant definition

Definition

The ideal generated by T, denoted (T), is the intersection of all ideals of R containing T.

Again, this is a nice definition and easy to prove things with, but doesn't tell us what elements of (T) look like. So, we now find another description of (T) in terms of "mashing" elements of T and R together.

This description is easy for ideals than rings

Lemma

The ideal (T) consists of all finite sums of the form

$$r = r_1 \cdot t_1 + \cdots + r_k t_k, k \geq 0; r_j \in R, t_j \in T$$

Proof.

Let X be the set of such elements.

- $X \subset (T)$: since the $t_i \in (T)$, and T is closed under addition and multiplication by elements of R.
- $(T) \subset X$: clearly X contains T, so by the definition of (T) it is enough to show that X is an ideal. X is nonempty, is closed under addition, and by the distributive property is closed under multiplication by elements of R.

$\square$

Generating subrings vs. generating ideals

Consider the subset $T = \{2, x\} \subset \mathbb{Z}[x]$

- The subring generated by T, $\langle T \rangle$, consists of all of $\mathbb{Z}[x]$; in fact, we already have $\langle x \rangle = \mathbb{X}[x]$, and including the two does nothing.
- The ideal generated by T, $(T) = (2, x)$ consists of all polynomials with even constant term, i.e., those of the form

$$2a_0 + a_x + \cdots + a_n x^n, a_i \in \mathbb{Z}$$

Note that here the inclusion of the two is essential; the ideal generated by just x, (x), consists of all polynomials with *vanishing* constant term.

Two Analogies

1. Yesterday, we saw the subring generated by T looked like *polynomials* in $T, \mathbb{Z}[T]$.
2. In contrast, the ideal generated by T looks like a *vector space* over R with T as a generating set.

Both of these rough observations will be made more formal. The observations about subrings will be developed this semester when we talk about polynomial rings and quotient rings. Next semester, the similarity of ideals and vector spaces will be fit into a larger concept of *modules*

Generating ideals

Definition

If $I = (T)$, we say that T generates I. We say that I is *finitely generated* if $I = (T)$ for T a finite set. If $T = \{t_1, \ldots, t_n\}$ is a finite set, we write $(t_1, \ldots, t_n)$ instead of (T).

Definition

An ideal generated by a single element,

$$I = (t) = \{r \cdot t : r \in R\}$$

is called *principal*. If every ideal in R is principal, we call R an *principal ideal domain*.

Are you a principal ideal domain?

Examples of principal ideal domains:

- We saw the $\mathbb{Z}$ is a principal ideal domain
- Any quotient ring $\mathbb{Z}/n\mathbb{Z}$ is a P.I.D.
- For any field k, $k[x]$ is a principal ideal domain.

For last two, why?

Rings that aren't principal ideal domains:

- $\mathbb{Z}[x]$
- For k a field, $k[x, y]$

Why?

Random notation needed for the homework

Union of ideals isn't an ideal:

For example, consider $(2) \cup (3) \in \mathbb{Z}$; it contains 2 and 3 but not 2+3=5

If course, we could look at the ideal generated by $I_1 \cup I_2$.

Lemma

$$(I_1 \cup I_2) = \{r_1 + r_2 : r_i \in I_i\}$$

For obvious reasons, we will denote this ideal $I_1 + I_2$.