MAS439 Lecture 7
Maximal, Prime, Radical

October 129h

Last week, we defined quotient rings, and proved the universal property of quotient rings and the isomorphism theorems.

Today, we ask the following question: what conditions on I make R/I nice? Specifically, when is R/I a field/integral domain/reduced?

Tomorrow we will introduce the notion of *algebras*.

$$R/I \text{ is a field} \iff I \text{ is maximal}$$
$$R/I \text{ is a domain} \iff I \text{ is prime}$$
$$R/I \text{ is a reduced} \iff I \text{ is radical}$$

An observation about fields

Lemma

A ring R is a field if and only if the only ideals are $\{0\}$ and R.

Proof.

Suppose R a field, and $I \neq \{0\}$ an ideal. We must show $I = R$.

- $\exists 0 \neq r \in I$.
- Since R a field, $\exists s \in R$ s.t. $rs = 1$.
- Since I ideal, $r \in I$, we have $1 = s \cdot r \in I$
- But then $I = R$

$\square$

Lemma

A ring R is a field if and only if the only ideals are $\{0\}$ and R.

Proof.

Suppose the only ideals of R are $\{0\}$ and R, and let $0 \neq r \in R$.
We must show r is a unit.
Consider (r), the ideal generated by r.

- Since $r \in (r), (r) \neq \{0\}$.
- Hence $(r) = R$.
- Hence $1 \in (r)$
- So $1 = r \cdot s$

$\square$

Maps out of fields are injective[1]

Lemma

Let R be a field, and $\varphi : R \to S$ a homomorphism. Then either

1. *φ is injective*
2. *S is the trivial ring*

Proof.

We have $\ker(\varphi)$ is either $\{0\}$, in which case φ is injective, or $\ker(\varphi) = R$, in which case $1_S = 0_S$. $\square$

[1] Terms and conditions may apply

Now we can prove what we wanted

By the second isomorphism theorem, ideals in R/I are of the form J/I, with $I \subset J \subset R$ an ideal.

Definition

A proper ideal I is *maximal* if there are no ideals J with $I \subsetneq J \subsetneq R$

Lemma

Let R/I is a maximal ideal if and only if R/I is a field.

Note: maximal ideals are often written $\mathfrak{m}$ (`\mathfrak{m}`)

Maximal ideals of $\mathbb{Z}$

- Ideals of $\mathbb{Z}$ are of the form (n).
- $(n) \subset (m)$ if and only if m divides n
- So (n) is maximal if and only if the element n is prime

Indeed, we have seen $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is prime.

Maximal ideals always exist

Lemma

Let $r \in R$ not be a unit. Then r is contained in some maximal ideal $\mathfrak{m} \subset I$

Proof.

Consider the set of all proper ideals of R that contain r, ordered under inclusion. Suppose

$$r \in I_1 \subset I_2 \subset \cdots I_n \subset \cdots$$

is a chain of ideals. Then we can see $\cup I_n$ is a proper ideal containing r. We now apply Zorn's lemma. $\square$

$$R/I \text{ is a field} \iff I \text{ is maximal}$$
$$R/I \text{ is a domain} \iff I \text{ is prime}$$
$$R/I \text{ is a reduced} \iff I \text{ is radical}$$

Once you define prime ideals, it's obvious

Definition

An ideal $I \subset R$ is *prime* if $ab \in I$ implies $a \in I$ or $b \in I$

Lemma

An ideal I is prime if and only if R/I is an integral domain.

Proof.

For $a \in R$, let $[a]$ denote the image of a in R/I.

Then $a \in I \iff [a] = 0$. And $a \cdot b \in I \iff [a] \cdot [b] = 0$.

So the definition of I being prime is exactly equivalent to R/I being an integral domain.

$\square$

Two little comments

1. Note that R being an integral domain is equivalent to $\{0\} \subset R$ being a prime ideal.
2. Sometimes you'll see a prime ideal denote $\mathfrak{p}$, (i.e., \mathfrak{p}), but it's a bit old-school now, in contrast to $\mathfrak{m}$ for a maximal ideal, which is still commonplace

Example: Prime ideals in $\mathbb{Z}$

Remember all ideals in $\mathbb{Z}$ are principal, hence of the form (n).

An element $m \in \mathbb{Z} \in (n)$ if and only if $m = an$.
That is, if and only if n divides m.

So asking (n) to be prime is asking for $n|ab \implies n|a$ or $n|b$.
That is, asking for n to be prime.

Wait! In $\mathbb{Z}$ nearly all prime ideals are maximal?

Note that since all fields are integral domains, we have that all maximal ideals are prime.

In $\mathbb{Z}$, the converse is nearly true – the maximal ideals are the ideals (p), with p prime; the prime ideals in $\mathbb{Z}$ are (p) and (0).

Essentially the same proof holds true in any principal ideal domain...

R/I is a field $\iff$ I is maximal

R/I is a domain $\iff$ I is prime

R/I is a reduced $\iff$ I is radical

Some pun about radical ideals

Recall that if I is an ideal, the *radical* of I was

$$\sqrt{I} = \{a : a^n \in I \text{ for some } a\}$$

Definition

We call an ideal *radical* if $I = \sqrt{I}$. That is, I is radical if and only if $a^n \in I \implies a \in I$.

Lemma

I is radical if and only if $\sqrt{I}$ is reduced

Note: R/I being reduced is equivalent to $\{0\}$ being radical.

Radical ideals in $\mathbb{Z}$

Lemma

The ideal (n) is radical if and only if n is square-free – that is, n has no repeated prime factors.

Proof.

We have that $a \in \sqrt{(n)}$ if and only if n divides a^k for some k, if and only if a contains all the prime factors of n.

For (n) to be radical, this needs to be equivalent to a dividing n, i.e., every prime factor of n occuring exactly once.

$\square$