Lecture 8

More on Maximal Ideals

Recall: $(x) \subset \mathbb{Z}[x]$ is prime, but $(x) \subsetneq (2, x)$, so it not maximal. $(x) \in \mathbb{R}[x]$ is maximal because $\mathbb{R}[x]/(x) \cong \mathbb{R}$ is a field

Example 8.1 Let $a \in \mathbb{R}$. We defined the evaluation homomorphism before:

$$\operatorname{Ev}_a \colon \mathbb{R}[x] \to \mathbb{R}$$

$$p(x) \mapsto p(a)$$

Observe that Ev_a is in fact surjective. Then

$$\mathbb{R}[x]/\operatorname{Ker}(\operatorname{Ev}_a) \cong \mathbb{R} \implies \operatorname{Ker}(\operatorname{Ev}_a)$$
 is a maximal ideal

Denote $M_a := Ker(Ev_a)$

<u>Claim:</u> $M_a = (x - a)$ (e.g $M_0 = (x)$)

Proof.

If $p(x) \in (x-a)$ then we may write $p(x) = q(x) \cdot (x-a)$, $q(x) \in \mathbb{R}[x]$, then

$$\operatorname{Ev}_a(p(x)) = p(a) = q(a) \cdot (a - a) = 0 \implies p(x) \in M_a \implies (x - a) \subset M_a$$

Conversely, suppose $p(x) \in M_a = \text{Ker}(\text{Ev}_a)$. Let $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, then you can check with polynomial division that x - a divides p(x) with remainder exactly p(a) which is 0, hence x - a is a factor of p(x) [obviously, if p(x) is a polynomial with a root at x = a, then x - a is a factor], and we can write

$$\frac{p(x)}{x-a} = q(x)$$

therefore,

$$p(x) = q(x) \cdot (x - a) \implies p(x) \in (x - a) \implies M_a \subset (x - a)$$

and hence $M_a = (x - a)$.

Q: Is every maximal ideal of $\mathbb{R}[x]$ of the form M_a ?

For example, in \mathbb{Z} , the {maximal ideals} = {prime ideals} but we saw above that in $\mathbb{Z}[x]$ there exist prime ideals that are not maximal.

Two standard questions:

- (1) What are the primes?
- (2) What are the maximal ideals?

Claim: Consider $I = (x^2 + 1)$, then $I \subset \mathbb{R}[x]$ is a maximal ideal.

Proof. We have that

$$\mathbb{R}[x] = \{a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \dots + a_n x^n | a_k \in \mathbb{R}, k = 0, 1, 2, \dots n\}$$

What does $\overline{x^n}$ look like in $\mathbb{R}[x]/(x^2+1)$? We can deduce from the zero coset of the

1

ideal:

$$x^2 + 1 \in (x^2 + 1) \implies \overline{x^2 + 1} = \overline{0} \implies \overline{x^2} = \overline{-1} \in \mathbb{R}[x]/I$$

Furthermore

$$x^{3} = x \cdot x^{2} \implies \overline{x^{3}} = \overline{x} \cdot \overline{(-1)} \in \mathbb{R}[x]/I$$

$$x^{4} = x^{2} \cdot x^{2} \implies \overline{x^{4}} = \overline{(-1)} \cdot \overline{(-1)} \in \mathbb{R}[x]/I$$

Therefore, since all powers of x greater than 2 can be deconstructed into products of -1 and x, we can collapse the cosets of the quotient to a convenient form:

$$\mathbb{R}[x]/I = \{ \overline{a_0 + a_1 x} \mid a_0, a_1 \in R \}$$

with the rule $\overline{x} \cdot \overline{x} = \overline{-1}$.

This should be familiar and there is a ring isomorphism

$$\mathbb{R}[x]/I \to \mathbb{C}$$
$$\overline{1} \mapsto 1$$
$$\overline{x} \mapsto i$$

and since the quotient ring is isomorphic to the field \mathbb{C} , I is maximal.

Claim: $(x^2 + 1)$ is **not** maximal in $\mathbb{C}[x]$

Proof. We know that $x+i, x-i \in \mathbb{C}[x]$ and

$$(x+i)(x-i) = x^2 + 1 \in (x^2 + 1)$$

But $x + i, x - i \notin (x^2 + 1)$ therefore $(x^2 + 1)$ is not prime in $\mathbb{C}[x]$ and consequently is not maximal.

Observe if $a \in R \subset S$ Then

$$(a)_R = \{r \cdot a | r \in R\}$$

$$\cap$$

$$(a)_S = \{s \cdot a | s \in S\}$$

can have different properties as ideals, e.g.

$$\underbrace{(x) \subset \mathbb{Z}[x]}_{\text{prime}} \longrightarrow \underbrace{(x) \subset \mathbb{R}[x]}_{\text{maximal}}$$

$$\underbrace{(x^2+1) \subset \mathbb{R}[x]}_{\text{maximal}} \longrightarrow \underbrace{(x^2+1) \subset \mathbb{C}[x]}_{\text{not prime, not maximal}}$$

The Ring of Fractions

Q: How do we build \mathbb{Q} out of \mathbb{Z} ?

We want to add in multiplicative inverses like $\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots$ but we can't just add them in and get a ring.

Consider

$$\mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) = \{(m, n) \mid m, n \in \mathbb{Z}, n \neq 0\}$$

and think of the elements of this set as the fractions $\frac{m}{n}$.

There are some repeats if we care about multiplication and addition like

$$\frac{1}{2} = \frac{2}{4} = \frac{3}{6}$$

We should define an equivalence relation

$$\frac{a}{b} \sim \frac{c}{d} \Longleftrightarrow ad = bc$$

e.g $\frac{4}{6} \sim \frac{6}{9}$ because $4 \cdot 9 = 36 = 6 \cdot 6$.

Definition 8.1: Field of Rational Numbers

The field of rational numbers is

$$\mathbb{Q} := \left\{ \frac{m}{n} \middle| \ m, n \in \mathbb{Q}, \ n \neq 0 \right\} / \sim$$

and this is a field with operations given by

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$
$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

We can also see that there is an injective ring homomorphism

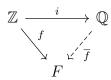
$$\mathbb{Z} \to \mathbb{Q}$$
$$n \mapsto \frac{n}{1}$$

Claim: If F is a field and there is an injective ring homomorphism

$$f: \mathbb{Z} \to F$$

Then it factors through \mathbb{Q} , i.e there is a ring homomorphism

$$\overline{f} \colon \mathbb{Q} \to F \text{ such that } f(n) = \overline{f}\left(\frac{n}{1}\right)$$



This is basically saying that if you have an injective homomorphism from Z to a field F, then under the homomorphism the integers will have inverses $f(2) \cdot \frac{1}{2} \in F$ and one should

see that this is exactly the rationals $\mathbb Q$ existing inside F.

Suppose R is any commutative ring with $1 \neq 0$.

Q: Can we do something similar with general rings R? i.e

$$R \times (R \setminus \{0\}) = \{(r, s) \mid r, s \in R, s \neq 0\}$$

(again, we will write (r,s) as $\frac{r}{s}$). We want to define $r^{-1} = \frac{1}{r}, r \neq 0$.

However, if r is a zero divisor, $r \cdot s = 0$ then in this case we want to exclude

$$\frac{1}{r} \cdot \frac{1}{s} = \frac{1}{r \cdot s} = \frac{1}{0}$$

Definition 8.2: Field of Fractions

Let R be an integral domain with $1 \neq 0$. Consider

$$R \times (R \setminus \{0\}) = \{(r, s) \mid r, s \in R, s \neq 0\}$$

Define an equivalence relation (exercise to show it is) by

$$\frac{a}{r} \sim \frac{b}{s} \Longleftrightarrow a \cdot s = b \cdot r$$

There is no ambiguity in the equality of products since R is integral there are no zero divisors, $s, r \neq 0$.

The field of fractions of R is

$$Q(R) := R \times (R \setminus \{0\}) / \sim = \left\{ \left\lceil \frac{a}{b} \right\rceil \middle| a, b \in R, \ b \neq 0 \right\}$$

Theorem 8.1

Q(R) is a field with operations

$$\frac{a}{r} + \frac{b}{s} = \frac{as + br}{rs}, \qquad \frac{a}{r} \cdot \frac{b}{s} = \frac{ab}{rs}$$

The map

$$i \colon R \to Q(R)$$

 $r \mapsto \frac{r}{1}$

is an injective ring homomorphism (we say R is a subring of its field of fractions). Moreover, if F is any field such that $R \subset F$ is a subring (i.e there exists an injective ring homomorphism $f: R \to F$), then there is a ring homomorphism

$$\overline{f} \colon Q(R) \to F \text{ such that } f(x) = \overline{f} \circ i(x)$$

$$R \xrightarrow{i} Q(R)$$

$$\downarrow f \qquad \qquad \downarrow f \qquad \qquad \downarrow$$

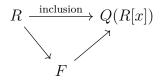
Proof. Think about it.....

Example 8.2 $Q(\mathbb{Z}) = \mathbb{Q}$

Example 8.3 $R = \mathbb{R}[x]$ is an integral domain. The fractional field of R is the field of rational functions

$$Q(R) = \mathbb{R}(x) := \left\{ \frac{p(x)}{q(x)} \middle| p, q \in \mathbb{R}[x], q \neq 0 \right\}$$

Example 8.4 If R is any integral domain with field of fractions Q(R) = F. Consider the integral domain R[x]. Then in particular $R \subset R[x]$, and $R[x] \subset Q(R[x])$ which tells us that



e.g $\mathbb{Z} \subset \mathbb{Z}[x]$, so in particular $\mathbb{Q} \subset Q(\mathbb{Z}[x])$.

In fact, since in $Q(\mathbb{Z}[x])$ you've added inverses to the coefficients but you also inverses to the polynomials, so you will get the field of rational functions

$$Q(\mathbb{Z}[x]) = \mathbb{R}(x)$$

Furthermore, this is generally true, as the field of fractions of R[x] is going to be the rational functions with coefficients in the field of fractions of R, i.e

$$Q(R[x]) = F(x)$$