L8: Maximal Ideals and Ring of Fractions

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:

$$\begin{aligned} \mathrm{Ev}_a \colon \mathbb{R}[X] &\to \mathbb{R} \\ p(X) &\mapsto p(a) \end{aligned}$$

Observe that Ev_a is in fact surjective. Then

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

Denote the set of polynomials with real coefficients which have a as a root as

$$M_a := \mathrm{Ker}(\mathrm{Ev}_a)$$

Claim: $M_a = (X - a) \quad$ (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
>
> $$\mathrm{Ev}_a(p(X)) = p(a) = q(a) \cdot (a - a) = 0 \implies p(X) \in M_a \implies (X - a) \subset M_a$$
>
> Conversely, suppose $p(X) \in M_a = \mathrm{Ker}(\mathrm{Ev}_a)$. 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
>
> $$\mathbb{R}[X] = \{a_0 + a_1X + a_2X^2 + a_3X^3 + \cdots + a_nX^n | a_k \in \mathbb{R},\ k = 0, 1, 2, \ldots n\}$$
>
> What does $\overline{X^n}$ look like in $\mathbb{R}[X]/(X^2 + 1)$? We can deduce from the zero coset of the 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:

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

with the rule $\overline{X} \cdot \overline{X} = \overline{-1}$.
This should be familiar and there is a ring isomorphism

$$\begin{aligned} \mathbb{R}[X]/I &\to \mathbb{C} \\ \overline{1} &\mapsto 1 \\ \overline{X} &\mapsto i \end{aligned}$$

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

$$\begin{aligned} &(a)_R = \{r \cdot a | r \in R\} \\ &\cap \\ &(a)_S = \{s \cdot a | s \in S\} \end{aligned}$$

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 $\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots$ 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

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

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

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

<u>Claim:</u> If F is a field and there is an injective ring homomorphism

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

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

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

$$\begin{tikzcd}
\mathbb{Z} \arrow[rr, "i"] \arrow[dr, "f"'] & & \mathbb{Q} \arrow[dl, dashed, "\overline{f}"] \\
& F &
\end{tikzcd}$$

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, $r \bullet s = 0$ then in this case we want to exclude

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

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

$$\frac{a}{r} \sim \frac{b}{s} \iff a \bullet s = b \bullet r$$

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

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

Theorem 8.3

$Q(R)$ is a field with operations

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

The map

$$\begin{aligned} i\colon R &\to Q(R) \\ r &\mapsto \frac{r}{1} \end{aligned}$$

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 $f\colon R \to F$), then there is a ring homomorphism

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

$$\begin{tikzcd} R \arrow[rr, "i"] \arrow[dr, "f"'] & & Q(R) \arrow[dl, dashed, "\overline{f}"] \\ & F & \end{tikzcd}$$

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

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

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

$$\begin{tikzcd} R \arrow[rr, "\text{inclusion}"] \arrow[dr] & & F = Q(R) \arrow[dl] \\ & Q(R[X]) & \end{tikzcd}$$

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

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