April20

Monday, April 19, 2021 10:01 PM

Maximal & Prime ideals

Prop HW 11 #5

R is a unital ring. $I \subseteq R$ an ideal

a) $I = R \iff I \cap R^{\times} \neq \emptyset$

↑ unit ideal

b) R is commutative.

R a field $\iff$ Only ideals are (0) & R

Corollary F a field, and $F \xrightarrow{\phi} R$

a nonzero ring homomorphism

Then ϕ is injective.

proof

HW 11 #1

$\ker\phi \subseteq F$ is an ideal.

So either (0) or F

↑ ϕ injective

↑ ϕ 0 map

Def^n^ (Maximal Ideals)

Let S be an arbitrary ring.

An ideal $M \subseteq S$ is maximal if

1) $M \neq S$

2) If $M \subseteq I \subseteq S$ I also an ideal then $I = S$ or $I = M$.

Existence uses following result from set theory.

Zorn's Lemma (Set Theory)

Let $(A, \leq)$ a partially ordered set. If every chain $x_1 \leq x_2 \leq \dots$ has an upper bound in A, then A has a maximal element.

(Equivalent to axiom of choice).

Prop Let R be a unital ring. Then every ideal $I \neq R$ is contained in a maximal ideal of R.

Proof

$$\mathcal{G} = \{ J : J \text{ an ideal } \& \ I \subseteq J \subsetneq R \}$$

Ordered by $\subseteq$.

Consider a chain

$$J_1 \leq J_2 \leq J_3 \leq \dots \quad \text{in } \mathcal{G}$$

Let $J = \bigcup J_i$

1) ideal of R ← HW 11 or 10

2) Contains I

3) $J \neq R$. If it were, then

$1 \in J$ so $1 \in J_i$

so $J_i = R$. ↯

So J is an upper bound for our chain in $\mathcal{G}$

Zorn $\Longrightarrow \exists\ \mathfrak{M} \in \mathcal{G}$. This is a maximal ideal.

If $\exists\ \mathfrak{M} \subseteq \mathfrak{N} \subsetneq R \Longrightarrow \mathfrak{N} \in \mathcal{G}$

$\Longrightarrow \mathfrak{M} = \mathfrak{N}$ by maximality. ⊘

There is a very nice characterization of maximal ideals in terms of quotients. (in case R commutative)

Prop Let R be a commutative unital ring. $I \subseteq R$ an ideal.

I is maximal $\Longleftrightarrow$ R/I is a field.

Proof 4th iso thm HW11 #2

$$\left\{ \begin{array}{l} \text{Ideals } J \\ \text{w/ } I \subseteq J \subseteq R \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \bar{J} \subseteq R/I \\ \uparrow \text{ideals.} \end{array} \right\}$$

I max'l $\Longleftrightarrow$ LHS is $\{I, R\}$

$\Longleftrightarrow$ RHS is $\{0, R/I\}$

$\Longleftrightarrow$ R/I a field. ⊘

$\uparrow$ HW 11 #5

Examples

1) Maximal ideals in $\mathbb{Z}$.

Directly

$$(a) \subseteq (b) \iff a \in (b) \iff a = nb \iff b \mid a$$

Being maximal

$\Updownarrow$

Having few divisors $(\pm 1, \pm p)$

$\Updownarrow$

a is prime.

Using Characterization

$(n) = n\mathbb{Z} \subseteq \mathbb{Z}$ is maximal

$\iff \mathbb{Z}/n\mathbb{Z}$ is a field

$\iff n$ is prime.

2) $(2, x) \subseteq \mathbb{Z}[x]$.

$$\overset{\shortparallel}{(2,x)} = \ker\Big(\mathbb{Z}[x] \xrightarrow{\varepsilon_0} \mathbb{Z} \xrightarrow{\pi} \underbrace{\mathbb{Z}/2\mathbb{Z}}_{\text{Field.}}\Big)$$

So $\dfrac{\mathbb{Z}[x]}{(2,x)} \simeq \mathbb{Z}/2\mathbb{Z}$ is a field

$\longrightarrow (2, x)$ is maximal.

3) $(x) \subseteq \mathbb{Z}[x]$. Not maximal

1) $(x) \subseteq (2, x)$ ← not principle.

2) $\dfrac{\mathbb{Z}[x]}{x} \simeq \mathbb{Z}$ not a field.

---

4) $\mathrm{Maps}(X, \mathbb{R})$.

Let $M_x := \ker(\varepsilon_x : \mathrm{Maps}(X, \mathbb{R}) \to \mathbb{R})$

$$f \longmapsto f(x).$$

Show M_x is a principle $\underline{\text{maximal ideal}}$.

Maximal

F.I.T. $\Rightarrow \dfrac{\mathrm{Maps}(X,\mathbb{R})}{M_x} \simeq \mathbb{R}$. ✓

Have injective function principle.

$$\begin{tikzcd} X \arrow[r] & \left\{ \begin{matrix} \text{Max'l ideals in} \\ \mathrm{Maps}(X,\mathbb{R}) \end{matrix} \right\} \\ x \arrow[r, mapsto] & M_x \end{tikzcd}$$

Given $x \in X$, define characteristic function

$$\chi_x : X \longrightarrow \mathbb{R}$$

$$\chi_x(z) = \begin{cases} \underline{0} & x = z \\ 1 & \text{else.} \end{cases}$$

Claim $M_x = (\chi_x) = \{ f \cdot \chi_x : f \in \mathrm{Maps}(X,\mathbb{R}) \}$

Proof $\supseteq$ $f \cdot \chi_x(x) = f(x) \cdot \chi_x(x) = 0$

$\subseteq$ $f \in M_x \leftarrow$

Then $f = f \cdot \chi_x \underset{=}{:} f(x)$

$$f(z) \cdot \chi_x(z) = \begin{cases} 0 & x = z \\ f(z) & \text{else} \end{cases}$$

Prime Ideals

Motivation

E.g. In $\mathbb{Z}[\sqrt{-5}]$ we lost the notion of

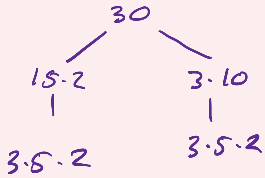
Unique factorization.

$$6 = 2\cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$$

This is problematic if you want a good arithmetic theory.

Kummer: Conjectured that some sort "ideal numbers" serve as sort of missing factors.

Ex



ok

keep factoring & arrive @ the prime factorization.

Dedekind formalized this dream.

Idea:

Ideals in $\mathbb{Z}$ $\longleftrightarrow$ $n\mathbb{Z}$ $\longleftrightarrow$ nonnegative integers.

$$(a)(b)=(c) \xleftrightarrow{\text{exercise.}} ab=c$$

Maybe instead of looking @ & factoring #s, do it for ideals?

Ex Replace 6 by (6). in $\mathbb{Z}[\sqrt{-5}]$.

Let $\mathfrak{p} = (2, 1+\sqrt{-5})$
$\mathfrak{q} = (3, 2+\sqrt{-5})$
$\mathfrak{r} = (3, 2-\sqrt{-5})$ $\Big\} \leftarrow$

Exercise

$\mathfrak{p}^2 = (2) \qquad \mathfrak{q}\mathfrak{r} = (3)$

$\mathfrak{p}\mathfrak{q} = (1+\sqrt{-5}) \qquad \mathfrak{p}\mathfrak{r} = (1-\sqrt{-5}).$

$$\begin{tikzcd}
& (6) \arrow[dl, dash] \arrow[dr, phantom, "="] & \\
(2)(3) \arrow[d, phantom, "\parallel"] & & (1+\sqrt{-5})(1-\sqrt{-5}) \arrow[d, phantom, "\parallel"] \\
\mathfrak{p}^2\mathfrak{q}\mathfrak{r} & = & \mathfrak{p}\mathfrak{q}\mathfrak{p}\mathfrak{r}
\end{tikzcd}$$

✓

There is now hope of recovering unique factorization, into prime ideals instead of prime #s.

↑ What is this?

Need: A good notion of prime ideals.

(commutative unital rings)

First Attempt: (not correct).

$n\mathbb{Z}$ max'l
$\iff n$ prime.

(works for $\mathbb{Z}[\sqrt{-5}]$)

Maybe maximal ideals??

⚠ Saw $(x) \subseteq \mathbb{Z}[x]$ not maximal....
Feels like should be prime. (x irreducible).

Second attempt

Principly generated by irreducible elts.

Bad doesn't work for $\mathbb{Z}[\sqrt{-5}]$.

Observation (+ motivation for (x) being prime).

Model: Euclid's Lemma

p prime.

$$\begin{tikzcd} p \mid ab \arrow[d, Rightarrow] \arrow[r, leftrightsquigarrow] & ab \in (p) \arrow[d, Rightarrow] \\ p \mid a \text{ or } p \mid b & a \in (p) \text{ or } b \in (p). \end{tikzcd}$$

Does this work for $x \in \mathbb{Z}[x]$?

$$\begin{tikzcd} x \mid fg \arrow[d, Rightarrow] \arrow[r, leftrightsquigarrow] & fg \in (x) \arrow[d, Rightarrow] \\ x \mid f \text{ or } x \mid g & f \in (x) \text{ or } g \in (x) \end{tikzcd}$$

$f = f_0 + f_1 x + \cdots$

$g = g_0 + g_1 x + \cdots$

$fg = \underset{\Uparrow}{f_0 g_0} + x(\cdots)$

$= 0$ then f_0 or $g_0 = 0$.

Def^n R a commutative unital ring.

An ideal $\mathfrak{P} \leq R$ is called a prime ideal if $\mathfrak{P} \neq R$ & $\forall\ a, b \in R$

if $ab \in \mathfrak{P}$ then $a \in \mathfrak{P}$ or $b \in \mathfrak{P}$.

Example $I, J \leq R$. $I \not\subseteq J$ & $J \not\subseteq I$.

Then IJ not prime.

HW !!

$a \in I \setminus J$ $\quad b \in J \setminus I$. $\quad a, b \notin IJ \subseteq I \cap J$

But $ab \in IJ$.

Characterization in terms of quotients

Prop R a unital commutative ring.
$P \subseteq R$ an ideal.

P is prime $\Longleftarrow$ R/P an integral domain.

Recall
An integral domain is a commutative unital ring w/ $1 \neq 0$ & no zero divisors.

Proof Unwinding definitions.
For $a \in R$, $\bar{a} \in R/P$ is $0 \iff a \in P$.

$$\begin{tikzcd}
ab \in P \arrow[rr, leftrightarrow] \arrow[d, Rightarrow, "P \text{ prime}"] & & \overline{ab} = \bar{a}\bar{b} = 0 \arrow[d, Rightarrow, "R/P \text{ int domain}"] \\
a \in P \text{ or } b \in P \arrow[rr, leftrightarrow] & & \bar{a} = 0 \text{ or } \bar{b} = 0
\end{tikzcd}$$

Corollary
R commutative unital ring.
A maximal ideal in R is prime.

Proof M max'l

$\Longrightarrow$ R/M is a field, thus an integral domain

$\Longrightarrow$ M prime.

Corollary R commutative unital.

R int. domain $\iff$ (0) is prime.

Examples

1) $(p) \subseteq \mathbb{Z}$ is prime & maximal

$(0) \subseteq \mathbb{Z}$ is prime & not maximal.

$(0) \subseteq (p)$ chain of prime ideals.

2) $(x) \subseteq \mathbb{Z}[x]$ prime not max'l

$(\mathbb{Z}[x]/(x) \simeq \mathbb{Z}$ an. int dom.

$(2, x) \subseteq \mathbb{Z}[x]$ prime & max'l

$(0) \subseteq \mathbb{Z}[x]$ prime & not max'l.

$(0) \subseteq (x) \subseteq (2, x)$ longer chain of primes.

Fractions in Ring Theory

Recall

Let R be a unital subring of a field.

Then R is an integral domain.

The converse is true as well!

Idea Do it formally using fractions.

Example

$$\mathbb{Z} = \left\{\frac{n}{1} \mid n \in \mathbb{Z}\right\} \subseteq \left\{\frac{n}{m} ,\ \underset{m \neq 0}{n, m \in \mathbb{Z}}\right\} = \mathbb{Q}$$

Formally build $\mathbb{Q}$ as fractions of elts of $\mathbb{Z}$.

Start w/ $\{(a,b) \le \mathbb{Z}\times\mathbb{Z} \quad b \neq 0\}$ ← equiv classes

Have equiv relation

relation

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

$\frac{a}{b}+\frac{c}{d} = \frac{ad+bc}{bd}$ $\qquad$ $\frac{a}{b}\,\frac{c}{d} = \frac{ac}{bd}.$

$\frac{a}{1}\in\mathbb{Z}$ now has inverse $\frac{1}{a}$

$\frac{a}{1}\cdot\frac{1}{a} = \frac{a}{a}$ $\qquad$ $\frac{a}{a} = \frac{1}{1}$

$\rightsquigarrow a\cdot 1 = a\cdot 1.$

Goal: Do this for more general (commutative) rings.

fractions in R

$$\begin{tikzcd} R \arrow[r, hook, "c"] & \mathrm{Frac}(R) \\ r \arrow[r, mapsto] & \frac{r}{1} \end{tikzcd}$$

Obstructions

① If $b\in R$ a zero div. $d\neq 0$ & $bd=0$.

$$d = \frac{d}{1} = \frac{bd}{b} = \frac{0}{b} = 0$$

Lose injectivity. of c.

Maybe pick & choose what I divide by.

② If I invert b & d, must invert bd.

$$\frac{1}{b}\cdot\frac{1}{d} = \frac{1}{bd}$$

Def^{n} A subset $S \subseteq R$ is called a good multiplicative subset if

1) S contains no zero divisors or 0.
2) $a, b \in S \quad ab \in S$.

Theorem R a commutative ring & $S \subseteq R$ a good multiplicative subset. Then, $\exists$ a commutative unital ring $Q = S^{-1}R$ s.t.

1) $R \leq Q$ is a subring.
2) $\forall\, s \in S \subseteq Q$, $s \in Q^{\times}$.
3) All elts of Q are $r \cdot s^{-1}$ some $r \in R$ & $s \in S$.

Furthermore. Q is universal for satisfying (1) - (3).

In particular, given s.t. $\forall\, s \in S$ $\phi(s) \in (Q')^{\times}$

$$\begin{tikzcd}
R \arrow[r, "\phi"] \arrow[d] & Q' & {} \arrow[l] \\
\underline{\underline{Q}} \arrow[ur, dashed, "\exists!\, \underline{\Phi}"'] & &
\end{tikzcd}$$

exist unique $\Phi : Q \to Q'$ a homomorphism s.t. $\Phi|_{R} = \phi$.

If ϕ is injective, $\underline{\Phi}$ is.

Beginning of Proof: Q as a set.

Let $\mathcal{F} = \{(a, b) \in R \times R : b \in S\}$

Define an equivalence relation on $\mathcal{T}$

$$(a,b) \sim (c,d)$$

if $ad = bc$.

Show this is an equivalence relation.

1) Reflexive. ✓
2) Symmetric ✓
3) Transitive.

$$\begin{tikzcd}
(a,b)\sim(c,d) & & (c,d)\sim(e,f) \\
ad-bc=0 \arrow[d, "\times f"] & & cf-de=0 \arrow[d, "\times b"] \\
adf-\underline{bcf}=0 \arrow[dr] & \underline{\text{add}} & \underline{bcf}-bde=0 \arrow[dl] \\
& adf-bde=0 \arrow[d, equal] & \\
& d(af-be) &
\end{tikzcd}$$

$d \in S \implies$ not a zero divisor.

$\implies af - be = 0$

$\implies af = be$

$\implies (a,b) \sim (e,f)$

Take equiv. classes $\mathcal{F}/\sim$

$$[(a,b)] = \frac{a}{b} = \left\{ (x,y) \;\middle|\; \begin{matrix} x\in R \\ y \in S \end{matrix} \quad ay = bx \right\}$$

$$Q = \left\{ \frac{a}{b} \;\middle|\; a\in R,\ b\in S \right\}$$

Next time Rest.

Define

$$+ : \quad \frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$$

$$\times : \quad \frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}.$$

1) well defined

2) Makes Q into a commutative unital ring.