Prime and Maximal Ideals

Thursday, 24 March 2022 12:04

Recap: R ring. $I \subseteq R$ is an ideal if (1) $a, b \in I \Rightarrow a+b \in I$

(2) $a \in R, h \in I \Rightarrow ah, ha \in I$.

$$\underbrace{\text{Ideals} \Leftrightarrow \text{Kernels of ring morphisms}}_{\text{Quotient rings}}$$

Example: $R = \{ f : \mathbb{R} \to \mathbb{R} \}$

$I = \{ f(2) = 0 \mid f : \mathbb{R} \to \mathbb{R} \}$.

Method 1: Check from def

$f, g \in I$ $(f+g)(2) = f(2) + g(2) = 0$

$\Rightarrow f+g \in I$

$f \in R, g \in I$ $(fg)(2) = f(2)\underbrace{g(2)}_{0}$

$= 0$

$\Rightarrow f \cdot g \in I$

Method 2: $I = \ker(ev_2)$ a ring homomorphism

Prop: $\varphi: R \to R'$ I is an ideal of R'. Then $\varphi^{-1}(I)$ is an ideal.

Proof: $a, b \in \varphi^{-1}(I) \Rightarrow a+b \in \varphi^{-1}(I)$ follows from (iv) yesterday.

$a \in R$, $h \in \varphi^{-1}(I)$. Want to show $ah \in \varphi^{-1}(I)$

$$\varphi(ah) = \overset{\in R'}{\varphi(a)}\,\overset{\in I}{\varphi(h)} \in I$$

$\Rightarrow ah \in \varphi^{-1}(I)$ $\square$

Alternative method: Check that $\varphi^{-1}(I)$ is the kernel of the ring homomorphism $\psi: R \to R'/I$, given by $\psi(r) = \varphi(r) + I$

Non-example: $\iota: \mathbb{Z} \to \mathbb{Q}$

$\iota(n) = \frac{n}{1}$. $6\mathbb{Z}$ is an ideal $\mathbb{Z}$

$\iota(6\mathbb{Z}) = \{\frac{6n}{1} : n \in \mathbb{Z}\}$.

Now $\underset{\in \mathbb{Q}}{\frac{1}{12}} \cdot \underset{\in \iota(6\mathbb{Z})}{6} = \frac{1}{2} \notin \iota(6\mathbb{Z})$

So $\iota(6\mathbb{Z})$ is not an ideal.

$\circledast$: The image of an ideal might not be an ideal.

R is a ring with unity 1

Lemma: $I \subseteq R$ is an ideal.

$I = R \iff I$ contains a unit (e.g. 1)

Proof: "$\Rightarrow$" $I = R \ni 1$

"$\Leftarrow$": Suppose $a \in I$ is a unit.

So there exists $b \in R$ s.t. $ab = 1$

$\Rightarrow 1 = ab \in I$

$\Rightarrow$ For every $r \in R$, $r \cdot 1$ is in I

$\Rightarrow$ $R = I$ $\square$

Corollary: The ideals of a field F are $\{0\}$, F

Def: $\{0\}$ is the <u>trivial</u> ideal of R, R is the <u>improper</u> ideal of R. Everything else is (proper) non-trivial.

Recall: Want to reverse engineer

$$\mathbb{R}[x]/\ker(ev_i) \cong im(ev_i) = \mathbb{C}.$$

When is a quotient ring a field?

Example: $R = \mathbb{Z}$ (is an ID, not a field)

(1) $\mathbb{Z}/\{0\} \cong \mathbb{Z}$ ID but not a field

(2) $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_p$ Field

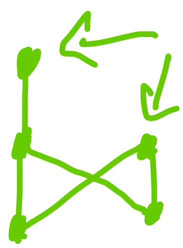
(3) $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ Not even an ID

$n = ab,\ a,b \geq 1$ $\quad$ $a \cdot b = 0$ in $\mathbb{Z}_n$

Def: An ideal $I \subsetneq R$ is <u>maximal</u> if there are no proper ideal J s.t. $I \subsetneq J \subsetneq R$.

Maximal: Nothing is larger than it

Maximum: Larger than everything else



Maximal not maximum

Example: $R = \mathbb{Z}$

$\{0\}$ is not maximal b/c $6\mathbb{Z} \supsetneq \{0\}$ $\quad$ $\mathbb{Z} \neq$

$6\mathbb{Z}$ is not maximal b/c $3\mathbb{Z} \supsetneq 6\mathbb{Z}$

$2\mathbb{Z}, 3\mathbb{Z}$ are maximal.

F is a field. Then $\{0\}$ is maximal.

R commutative with unity 1.

Lemma: $I \subseteq R$ an ideal. $a \in R$ (say $a \notin I$). Then $J = \{ar + h \mid r \in R, h \in I\}$ is an ideal containg a and I.

Proof: $ar_1 + h_1, ar_2 + h_2 \in J$

$$(ar_1 + h_1) + (ar_2 + h_2) = a\overset{\in R}{(r_1 + r_2)} + \overset{I \ni}{(h_1 + h_2)} \in J$$

$r \in R$, $ar_1 + h_1 \in J$

$$r(ar_1 + h_1) = a\overset{\in R}{(rr_1)} + \overset{\in I}{rh_1} \in J$$

Set $r = 0 \Rightarrow I \subseteq J$

Set $r = 1, h = 0 \Rightarrow a \in J$ $\square$

Theorem: Let $I \subseteq R$ be an ideal. Then I is maximal $\Leftrightarrow$ R/I is a field.

Quick example: $2\mathbb{Z}, 3\mathbb{Z}$ are maximal b/c $\mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}_2$, $\mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}_3$ are fields

Proof: "$\Rightarrow$" Need to check every non-zero element of R/I has a multiplicative inverse.

Let $a+I$ be a non-zero element of R/I, i.e., $a \notin I$.

Consider $J = \{ar + h : r \in R, h \in I\}$ which is an ideal properly contains I.
$(a \in J, a \notin I)$

Since I is maximal, $J = R \ni 1$

So $1 = ar + h$ for some $r \in R$, $h \in I$

$\in ar + I$

$\Rightarrow$ $\underset{\text{Unity in } R/I}{1 + I} = ar + I$

$= (a+I)(r+I)$

$\Rightarrow r+I$ is an inverse of $a+I$.

"$\Leftarrow$": Suppose R/I is a field, but $I \subsetneq J \subsetneq R$. Then pick any $a \in J$ but $a \notin I$, i.e. $a+I$ is non-zero in R/I. Since R/I is a field $\underline{(a+I)(b+I) = 1+I}$ for some b.

$ab \in ab + I = (a+I)(b+I) = 1 + I$.

$\Rightarrow ab = 1 + h$ for some $h \in I$.

Now, $a \in J$ means $ab \in J$,

which means $1 = ab - \underset{\in I \subseteq J}{h}$ is in J.

This means $J = R$, a contradiction. $\square$

Def: An ideal $I \subseteq R$ is <u>prime</u> if $ab \in I \Rightarrow$ either $a \in I$ or $b \in I$.

Example: $p\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$ for prime p. Suppose $ab \in p\mathbb{Z}$

$ab = pm$ for some $m \in \mathbb{Z}$

$\Rightarrow$ either a is a multiple of p

or b " " " "

$\Rightarrow$ either $a \in p\mathbb{Z}$, or $b \in p\mathbb{Z}$.

Lemma: $\{0\}$ is a prime ideal of an integral domain.

Proof: Suppose $ab \in \{0\}$.

$ab = 0$

$\Rightarrow a = 0$ or $b = 0$ as ID has no zero divisors.

$\Rightarrow a \in \{0\}, b \in \{0\}$ $\square$

Theorem: I is a prime ideal of $R \Leftrightarrow R/I$ is an integral domain.

Proof: "$\Rightarrow$" If $(a+I)(b+I) = I$, then $ab + I = (a+I)(b+I) = I$.

So $ab \in I$, which means either $a \in I$ or $b \in I$ as I is prime.

i.e. $a+I=I$ or $b+I=I$ in R/I,

Therefore R/I has no zero divison.

"$\Leftarrow$": Exer $\square$

Example: $p\mathbb{Z}$ and $\{0\}$ are prime ideals b/c $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}/\{0\} \cong \mathbb{Z}$ are IDs.

Corollary: Every maximal ideal is a prime ideal.

Proof: I is maximal

$\Rightarrow$ R/I is a field

$\Rightarrow$ R/I is an ID

$\Rightarrow$ I is prime. $\square$