Lecture 13: Prime and maximal ideals

Wednesday, May 2, 2018 11:03 AM

In the previous lecture we defined

$I \underset{\neq}{\trianglelefteq} R$ is prime if $ab \in I \Rightarrow (a \in I$ or $b \in I)$.

<u>Proposition</u>. $I \trianglelefteq R$ is prime $\Longleftrightarrow$ R/I is an integral domain.

<u>Pf.</u> ($\Rightarrow$) • $I \neq R \Rightarrow R/I$ is not the zero ring

• $(a+I)(b+I) = 0+I \Rightarrow ab+I = 0+I$

$\Rightarrow ab \in I \Rightarrow a \in I$ or $b \in I$

$\Rightarrow a+I = 0+I$ or $b+I = 0+I$

Hence R/I does not have a zero divisor.

($\Leftarrow$). R/I is not the zero ring $\Rightarrow I \neq R$

. $ab \in I \Rightarrow ab+I = 0+I \Rightarrow (a+I)(b+I) = 0+I$

$\Rightarrow$ either $a+I = 0+I$ or $b+I = 0+I$

$\Rightarrow$ either $a \in I$ or $b \in I$. $\blacksquare$

<u>Def.</u> $I \underset{\neq}{\trianglelefteq} R$ is called a <u>maximal ideal</u> if

$I \subseteq J \trianglelefteq R$ implies $I = J$ or $J = R$.

Again the factor ring R/I can help us to find out if I is maximal or not.

<u>Proposition</u>. $I \lhd R$ is maximal $\Leftrightarrow$ R/I is a field.

<u>Pf</u>: ($\Rightarrow$) Since $I \neq R$, R/I is not the zero ring. Now we need to show $\forall\, a+I \neq 0+I$, $a+I$ has a multiplicative inverse.

Let $J = I + \langle a \rangle := \{ b + ar \mid b \in I \text{ and } r \in R \}$.

<u>Claim 1</u> $J \lhd R$.

<u>Pf of claim</u>. Using the ideal criterion we need to show

$$x_1, x_2 \in J \Rightarrow x_1 - x_2 \in J \quad \text{and} \quad r \in R,\, x \in J \Rightarrow rx \in J$$

- $x_1, x_2 \in J \Rightarrow \left.\begin{cases} x_1 = b_1 + a r_1 \\ x_2 = b_2 + a r_2 \\ b_i \in I,\ r_i \in R \end{cases}\right\} \Rightarrow x_1 - x_2 = \underbrace{(b_1 - b_2)}_{\text{in } I} + a\underbrace{(r_1 - r_2)}_{\text{in } R}$

  $\Rightarrow x_1 - x_2 \in J$.

- $x \in J \Rightarrow \left.\begin{array}{l} x = b + ar' \\ b \in I,\ r' \in R \end{array}\right\} \Rightarrow rx = \underbrace{rb}_{\text{in } I} + a\underbrace{(rr')}_{\text{in } R} \Rightarrow rx \in J$.

<u>Notice</u> $I \neq J$ as $a \in J \setminus I$.

As I is maximal, $J = R$. Hence $1 \in J$, which implies

Lecture 13: Prime and maximal ideals

Wednesday, May 2, 2018 11:24 AM

$1 = b + ar$ for some $b \in I$ and $r \in R$. Hence

$1 + I = ar + I = (a+I)(r+I)$. Therefore $a+I$ is

a unit.

$(\Leftarrow)$ Suppose $I \subsetneq J$ and $J \lhd R$. So $\exists\, a \in J \setminus I$.

Then $a + I \neq 0 + I$ in R/I. As R/I is a field,

$\exists\, a' \in R$ s.t. $(a+I)(a'+I) = 1 + I$. Hence

$1 = aa' + b$ for some $b \in I$.

$$\left.\begin{array}{l} a \in J \Rightarrow aa' \in J \\ b \in I \subseteq J \end{array}\right\} \Rightarrow 1 \in J \Rightarrow J = R.$$ And so I is

maximal. (Notice since R/I is not the zero ring, $I \neq R$.) ∎

Corollary. $I \lhd R$ maximal $\Rightarrow$ $I \lhd R$ prime.

Pf. $I \lhd R$ maximal $\Rightarrow$ R/I field

$\Rightarrow R/I$ integral domain $\Rightarrow$ $I \lhd R$ prime. ∎

Ex. $I \lhd \mathbb{Z}$ is maximal $\Leftrightarrow$ $I = p\mathbb{Z}$ where p is prime.

Ex. Suppose $a^2 + b^2 = p$ is prime; then $\langle a + ib \rangle \lhd \mathbb{Z}[i]$ is maximal

Lecture 13: Irreducible elements and maximal

Wednesday, May 2, 2018 11:32 AM

Pf. $\mathbb{Z}[i]/\langle a+bi\rangle \simeq \mathbb{Z}/p\mathbb{Z}$ as we proved in the previous lecture, and so it is a field. Hence $\langle a+bi\rangle$ is a maximal ideal. ■

Next definition help us to understand maximal ideals of a PID.

Def. • Let R be (as before) a unital commutative ring. $0\neq a\in R$ is called irreducible if a is not a zero-divisor and a is not a unit and

$$a=bc \Rightarrow \text{either } b\in U(R) \text{ or } c\in U(R).$$

Lemma. Suppose D is a PID, which is not a field. Then

$$a\in D \text{ is irreducible} \Leftrightarrow \langle a\rangle \text{ is a maximal ideal.}$$

Pf. ($\Rightarrow$) Suppose $\langle a\rangle \subsetneq J \trianglelefteq D$. Since D is a PID, $J=\langle a'\rangle$ for some $a'\in D$. As $a\in\langle a\rangle \subseteq \langle a'\rangle$,

$$a=a'd \text{ for some } d\in D.$$ Since a is irreducible, either $a'\in U(D)$ or $d\in U(D)$.

If $d\in U(D)$, then $\langle a'\rangle = \langle a'd\rangle = \langle a\rangle$ which is a contra.

Lecture 13: Irreducible and maximal

Wednesday, May 2, 2018 11:43 AM

Therefore $a' \in U(D)$; and so $\langle a' \rangle = D$.

Notice that, since $a \notin U(D)$, $\langle a \rangle \neq D$. And so $\langle a \rangle$ is a maximal ideal.

$(\Leftarrow)$. if $a=0$, then $D/_{\langle a \rangle} = D/_{\langle 0 \rangle} \simeq D$ is a field which is a contradiction. So $a \neq 0$. Since D is an integral domain, a is not a zero-divisor.

. if a is a unit, then $\langle a \rangle = D$ as you had it in your HW; this contradicts the assumption that $\langle a \rangle$ is a maximal ideal.

. if $a = bc$, then $\langle a \rangle \subseteq \langle b \rangle$. Hence either $\langle b \rangle = \langle a \rangle$ or $\langle b \rangle = D$. As you had it in your HW,

* $\langle b \rangle = \langle a \rangle$ implies $a = bu$ for some $u \in U(D)$; and so $bu = bc$ which implies $c = u \in U(D)$ (D is an integral domain, and so it has the cancellation property.)

* $\langle b \rangle = D$ implies $b \in U(D)$.

Hence either $b \in U(D)$ or $c \in U(D)$. ■