Lecture 8 (01-09)

01 September 2020 10:29 AM

If $R \to R/I \times R/J$ is onto, then $(0,1)$ & $(1,0)$ must have preimage.

Notation: Given a ring R, we denote the set of maximal ideals in R by $\mathrm{Max}(R)$, and if R is commutative, then the set of prime ideals is denoted $\mathrm{Spec}(R)$.

called the prime spectrum of R.

[We shall consider R to be comm. when talking about prime ideals.]

[Natural q. after defining a set → is it non-empty?]

[Is $\max(R) \neq \emptyset$? Well, no, if $R = 0$.]

Okay, assume $R \neq 0$.

Claim: $\max(R) \neq \emptyset$.

Proof. We prove this by using Zorn's Lemma.

Let Λ be the set of all proper ideals in R.

① $\Lambda \neq \emptyset$ since $\{0\} \in \Lambda$.

② Λ is a poset by $\subseteq$.

③ Let $\{I_j\}_{j \in \gamma} \subseteq \Lambda$ be a chain (totally ordered).

We claim that $\{I_j\}_{j \in \gamma}$ has an upper bound in Λ,

i.e., $\exists\, I \in \Lambda$ s.t. $\forall j \in \gamma$, $I_j \subset I$.

Indeed, define $I := \bigcup_{j \in \gamma} I_j$.

[Of course, we clearly have that $I_j \subset I$ $\forall j$.]

Claim. $I \in \Lambda$. That is, I is an ideal which is proper (in R).

Proof. Let $a, b \in I$.

$a \in I_{j_1}$ & $b \in I_{j_2}$ for some $j_1, j_2 \in \gamma$.

Since $\{I_j\}_{j \in \gamma}$ was a chain, either $I_{j_1} \subset I_{j_2}$ or $I_{j_2} \supset I_{j_1}$.

WLOG ↗

Thus, $a \in I_{j_2}$ as well. Then, $a + b \in I_{j_2} \subset I$.

Similarly, given $r \in R$, we have $a_j, ra \in I_j \subset I$.

Thus, I is actually an ideal. ($I \neq \emptyset$ is obvious.)

Lastly, to see that I is proper, note that $1 \notin I_j \ \forall j$ since each I_j was proper.

Thus, $1 \notin I$. $\therefore I$ is proper. ☺

Now, by ①, ② and ③, we see that Λ satisfies the hypothesis of Zorn's Lemma. Thus, Λ has a maximal element m.

Claim. m is a maximal ideal in R. (That is, $m \in \text{Max}(R)$.)

Proof. Let $I \subset R$ be an ideal such that $m \subsetneq I$.

If $I \subsetneq R$, then $I \in \Lambda$ which contradicts maximality of m.

Thus, $I = R$, proving that m is maximal. ☺

Corollaries: ($R \neq 0$)

① Every proper ideal is contained in a maximal ideal.

② Let $a \in R$. Then,

a is not a unit $\iff \exists\, m \in \text{Max}(R)$ s.t. $a \in m$.

} Commutative ring. Otherwise "left max." or "right max."

Ex. $\text{Max}(\mathbb{Z}) = \{p\mathbb{Z} : p \text{ is prime}\}$

$\text{Spec}(\mathbb{Z}) = \{p\mathbb{Z} : p \text{ is prime or } p = 0\}$.

In general, $\text{Max}(R) \subset \text{Spec}(R)$.

That is, if m is a maximal ideal in R, then m is prime.

Max ideals are prime

Recall: $\mathfrak{p}$ is prime if (if $ab \in \mathfrak{p}$, then $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$).

Working rule: $ab \in \mathfrak{p}$, $a \notin \mathfrak{p} \Rightarrow b \in \mathfrak{p}$.

$\ldots$ $b \in R$ be such that

Proof. Let m be a maximal ideal and $a, b \in R$ be such that $ab \in m$ and $a \notin m$.

$a \notin m \Rightarrow m \subsetneq m + \langle a \rangle \Rightarrow m + \langle a \rangle = R$

$\Rightarrow \exists m \in m, r \in R$ s.t. $m + ra = 1$

$\Rightarrow mb + rab = b$

($mb \in m$, $rab \in m$, so $mb + rab \in m$)

$\therefore b \in m$.

Remark. Corollary (2) is not necessarily true if R not comm. Take $R = M_n(\mathbb{Q})$ $(n \geq 2)$

Proof of Cor.

(1) Let $I \subsetneq R$ be an ideal. Then, R/I is a ring which is not the zero ring.

Let m be a max. ideal in R/I.

Then, $\pi_I^{-1}[m]$ is a max. ideal in R containing I.

(2) Let $a \in R$.

a is not a unit $\Leftrightarrow \langle a \rangle \neq R$

$\Updownarrow$ ↓ we proved ↑ obvious since max ideals are proper

$\langle a \rangle$ is conta. in max ideal

$\Leftrightarrow$

a is cont. in a max ideal

Lecture 9 (03-09)

03 September 2020 11:27 AM

Note: A prime ideal has to be proper.
(Commutative ring is also assumed.)

Also, 0 is not an integral domain.

Ex. Let $\mathfrak{p} \subset R$ be prime, $I, J \subset R$ be ideals in R.
(Prime ideal Exercise) If $IJ \subset \mathfrak{p}$, then $I \subset \mathfrak{p}$ or $J \subset \mathfrak{p}$.

Q. Let $\mathfrak{m} \in \operatorname{Max}(R)$, $a \in \mathfrak{m}$. What can you say about $1+a$?

Comm:

- $1 + a \notin \mathfrak{m}$. (Otherwise $1 \in \mathfrak{m}$ and $\mathfrak{m} = R$. $\rightarrow\leftarrow$)
- $1 + a \in V(R)$? No. Take $R = \mathbb{Z}$, $\mathfrak{m} = 2\mathbb{Z}$, $a = 2$.

Recall: $u \in V(R)$ iff $u \notin \mathfrak{m}$ for any $\mathfrak{m} \in \max(R)$.

Q. What conditions can you put on $a \in R$ so that $1+a$ is a unit?

$$\bigcup_{\mathfrak{m} \in \operatorname{Max}(R)} \mathfrak{m} = R \setminus V(R)$$

What if we take $J = \bigcap_{\mathfrak{m} \in \operatorname{Max}(R)} \mathfrak{m}$ and $a \in J$.

Is $1+a$ a unit? Yes. If $1+a \notin V(R)$, then $1+a \in \mathfrak{m} \in M(R)$, then $1 \in \mathfrak{m}$ ($\because a \in \bigcap \mathfrak{m}$).
$\rightarrow\leftarrow$

Def'n Let R be a commutative ring. The Jacobson radical $J(R)$ of R is defined as

$$J(R) = \bigcap_{\mathfrak{m} \in \operatorname{Max}(R)} \mathfrak{m}.$$

Jacobson radical

Prop. $\mathcal{N}(R) \subset J(R)$. That is, if a is nilpotent, then $a \in m$ for all $m \in \mathrm{Max}(R)$.

Proof: If $a \in N(R)$, then $a^k = 0$ for so—

$\Rightarrow a^k \in m \quad \forall\, m$ max.

max. ideals are prime

$\Rightarrow a \in m \quad \forall\, m$

$\Rightarrow a \in J(R)$.

In fact, $N(R) \subset \bigcap_{p \in \mathrm{Spec}(R)} p \subset J(R)$.

↳ any equality?

Thm. In fact, $J(R)$ is a radical ideal, by (almost) the same argument.

Q. If $1+a$ is a unit, does $a \in J(R)$?

No. Take, $R = \mathbb{Z}$, $1 + a = -1$.

Note: $a \in J(R) \Rightarrow \forall r \in R\,(1 + ra \in U(R))$

Does this converse hold now?

Yes!

Prop $a \in J(R) \Leftrightarrow \forall r \in R\ (1 + ra \in U(R))$

Proof: ($\Rightarrow$) Let $a \in J(R)$ and $r \in R$ be arbitrary.

$ra \in J(R)$ since $J(R)$ is an ideal

Thus, $ra \in m$ for every max. ideal m.

$\Rightarrow 1 + ra \notin m$ for any max ideal m

$\Rightarrow 1 + ra$ is a unit.

($\Leftarrow$) Fix $a \in R$.

Assume that $1+ra$ is a unit for every $r \in R$.

Assumption: Suppose that $\exists y \in \mathrm{Max}(R)$ s.t. $a \notin y$.

Then, $y + \langle a \rangle = R$.

$\Rightarrow m - ra = 1$ for some $r \in R$, $m \in y$.

$\Rightarrow m = 1+ra \in y$ is a unit $\rightarrow\leftarrow$

Thus, our assumption was incorrect. In other words,

$a \in y$ for all $y \in \mathrm{Max}(R)$.

Thus, $a \in J(R)$. ☺

Q: Prove or disprove: $J(R) = 0$ for any $0 \neq R$ comm.

Sol^n: Disproof: We construct a counterexample.

$R = \mathbb{Z}/4\mathbb{Z}$.

Ideals of $R = \{\{0\}, \{0,2\}, R\}$

↳ maximal!

Thus, $J(R) = \{0,2\} \neq \{0\}$. ☹

(Prime ideal Exercise solution)

Let R be a comm. ring and $I, J \subset R$ be ideals. Let $\mathfrak{p} \in \mathrm{Spec}(R)$ s.t.

$IJ \subset \mathfrak{p}$ and $I \not\subset \mathfrak{p}$.

We show that $J \subset \mathfrak{p}$.

Proof. Let $j \in J$ be arbit.

Since $I \not\subset \mathfrak{p}$, $\exists\, i \in I$ s.t. $i \notin \mathfrak{p}$. $ij \in IJ \subset \mathfrak{p}$.

$\Rightarrow ij \in \mathfrak{p}$ and $i \notin \mathfrak{p}$.

$\therefore j \in \mathfrak{p}$ since $\mathfrak{p}$ is prime.

$\Rightarrow J \subset \mathfrak{p}$ (j was arbit) ☺

From this point on, unless otherwise mentioned, we shall assume rings to be commutative

Q Consider the natural map $\varphi : R \to R/I \times R/J$. Is this onto?

A. Well, if φ is onto, then $(\bar{1}, \bar{0})$ must have a preimage.

$\therefore \varphi(a) = (\bar{1}, \bar{0})$ for some $a \in R$.

$\Rightarrow a \equiv 1 \mod I$ & $a \equiv 0 \mod J$

$\Rightarrow 1 - a \in I$ and $a \in J$

$\Rightarrow 1 = (1-a) + a \in I + J$.

Leads to the following defn.

Def. Let $I, J \subsetneq R$ be ideals. We say (I, J) is co-maximal if $I + J = R$.

Co-maximal, comaximal ideals

Thus, if $\varphi : R \to R/I \times R/J$ is onto, then (I, J) is co-max. [Assuming they are proper.]

Q. Is the converse true? That is, if (I, J) is co-max, then is $\varphi : R \to R/I \times R/J$ surjective?

A. Yes! Note that $\exists i \in I, j \in J$ s.t. $i + j = 1$. $(\because I + J = R)$

Now, let $(\bar{a}, \bar{b}) \in R/I \times R/J$ be arbitrary. Fix some pre-im. $a \in R$, $b \in R$.

Consider $r = bi + aj \in R$.

Then, $\varphi(r) = (bi + aj + I, bi + aj + J)$

$= (aj + I, bi + J) = (a - ai + I, b - bj + J)$

$= (a + I, b + J)$

$= (\bar{a}, \bar{b})$. ∎

Q. Is φ one-one? **Ans.** Note that $\ker \varphi = I \cap J$.
Thus, $1\text{-}1 \iff I \cap J = 0$.

Thus, we see that for proper ideals I, J in R

$$R/I\cap J \xhookrightarrow{\tilde{\varphi}} R/I \times R/J,$$

which is an isomorphism if the pair (I, J) is co-max.

$$\begin{array}{ccc} R/I\cap J & \xhookrightarrow{\tilde{\varphi}} & R/I \times R/J \\ \pi \uparrow & \nearrow_{\varphi} & \\ R & & \end{array}$$

① **Observation:** If (I, J) is comaximal, then $IJ = I \cap J$.

Proof. ($\subseteq$) Always.
($\supseteq$) Let $a \in I \cap J$. $\quad i + j = 1$

$$a = ai + aj$$
$$\in JI \quad \in IJ$$
$$IJ =$$

② **Examples:** Let $\mathfrak{y} \in \mathrm{Max}(R)$ and $I \nsubseteq \mathfrak{y}$ be a proper ideal.
Then, $(I, \mathfrak{y})$ is comaximal.

↳ However, this will not work if every proper ideal is contained in $\mathfrak{y}$.

↓

This means that $\mathrm{Max}(R) = \{\mathfrak{y}\}$.

↳ Such a ring is called **local.**

↳ Notation: $(R, \mathfrak{y})$.

③ A local ring does not contain a pair of comaximal ideals.

If I, J are prop. ideals, then $I, J \subseteq \mathfrak{y}$ & thus, $I + J \subseteq \mathfrak{y} \subsetneq R$.

Conversely, a non-local ring always contains a comaximal pair.

Choose two distinct maximal ideals!

$$\mathfrak{y}_1, \mathfrak{y}_2 \subsetneq \mathfrak{y}_1 + \mathfrak{y}_2. \quad \therefore \mathfrak{y}_1 + \mathfrak{y}_2 = R.$$

Q. Let $m, n \in \mathbb{Z}$. When is $m\mathbb{Z}$ maximal, prime or radical?
When is $(m\mathbb{Z}, n\mathbb{Z})$ comaximal?

Do the same for $\mathbb{K}[x]$.

Q. Let $I_1, \dots, I_n \subsetneq R$. What can we say about

$$\varphi : R \longrightarrow R/I_1 \times \cdots \times R/I_n \ ?$$

↳ often called the "diagonal map"

(Note that $\ker \varphi = \bigcap_{i=1}^{n} I_i$)

Notation: $\overline{e_j} \leftarrow (\bar{0}, \dots, \bar{0}, \bar{1}, \bar{0}, \dots, \bar{0})$

↑ j^{th} pos.

If φ is onto, $\exists a_j \in R$ s.t. $\varphi(a_j) = \overline{e_j}$.

$\Rightarrow 1 - a_j \in I_j$ & $a_j \in I_k$ for $k \neq j$.

$\Rightarrow I_j$ & $\bigcap_{\substack{k=1 \\ k \neq j}}^{n} I_k$ are comaximal

Q. Suppose I_1 and $\bigcap_{j=2}^{n} I_j$ are comaximal.

Is (I_1, I_j) comaximal for all $j \neq 1$?

Lecture 11 (08-09)

08 September 2020 10:29 AM

Recall the following q.

Q. Suppose I_1 and $\bigcap_{j=2}^{n} I_j$ are coximal. Is (I_1, I_j) comax $\forall j \geq 2$?

Ans. Yes. Let $2 \leq j \leq n$. Then

$$R = I_1 + \bigcap_{j=2}^{n} I_j \subseteq I + I_j \subseteq R.$$

$\Rightarrow I + I_j = R$ showing (I, I_j) is comax.

(we had assumed $I_j \subsetneq R$.)

★ In fact, if (I, J) is co-max, then so is (I, K) for all proper ideals $K \supsetneq J$.

Proof. Same as above.

Thus, if $\varphi : R \longrightarrow R/I_1 \times \cdots \times R/I_n$ is onto,

then for all $j \neq k$, (I_j, I_k) is comax.

In other words: $I_1, \ldots, I_n$ are pairwise comax.

Q. Is converse true? That is, if $I_1, \ldots, I_n \subsetneq R$ are comax, is φ onto?

A Recall we had seen in the last class that if (I, J) is comax, then the induced map $\tilde{\varphi} : R/(I \cap J) \longrightarrow R/I \times R/J$ is an iso.

We can now prove the result by induction.

Suppose the result is true for $m < n$. (Induc. hyp.)

Base: $n = 2$ done.

Let $I_1, \ldots, I_n$ be pairwise comaximal.

Claim: I_1 and $\bigcap_{j=2}^{n} I_j$ are comaximal.

Assume claim for now.

Then, $\varphi: R \longrightarrow R/I_1 \times R/\bigcap_{j=2}^{n} I_j$ is onto (by $n=2$)

By induction, $R/\bigcap_{j=2}^{n} I_j \simeq R/I_2 \times \cdots \times R/I_n$. (and the iso thm.)

Moreover, this iso was induced by φ.

$$(a + \textstyle\bigcap I_j) \longmapsto (a+I_2, \ldots, a+I_n).$$

Using this, we get that

$$R \twoheadrightarrow R/I_1 \times R/(\textstyle\bigcap I_j) \longrightarrow R/I_1 \times \cdots \times R/I_n$$

is onto.

Now, we prove the claim.

Claim: I_1 and $\bigcap_{j=2}^{n} I_j$ are comaximal.

Proof: $a_2 \in I_2, \ldots, a_n \in I_n$ $\quad b_2 \in I_1, \ldots, b_n \in I_1$

$a_2 + b_2 = 1, \quad a_3 + b_3 = 1, \ldots, a_n + b_n = 1$

$$1 = (a_2 + b_2)\cdots(a_n + b_n)$$
$$= a_2 a \cdots a_n + b_2(\ ) + b_3(\ ) + \cdots + b_n(\ )$$

$a_2 a \cdots a_n \in \bigcap I_j$, $\quad b_2(\ ) + \cdots + b_n(\ ) \in I_1$

$\Rightarrow (I_1, \bigcap_{j=2}^{n} I_j)$ is comaximal. □

Thus, we have proved the Chinese Remainder Theorem.

Thm. (Chinese Remainder Theorem)
Let R be a non-zero commutative ring.
Let $I_1, \ldots, I_n \subsetneq R$ be pairwise comaximal ideals.
Then,

$$R/\quad \simeq R/\quad \times \cdots \times R/\quad .$$

Then,

$$\frac{R}{I_1 \cap \cdots \cap I_n} \simeq R/I_1 \times \cdots \times R/I_n .$$

Note that we also proved:

① The natural map $R \longrightarrow \prod R/I_j$ is onto.

② $I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$.

Ex. Write a text book proof of CRT. → Assignment, due before class on Thursday.
The statement

Prime Ideals.

How do you find prime ideals?
How do you find prime but not maximal?

1 Q: Is $N(R) = \bigcap_{P \in \mathrm{Spec}(R)} P$? ($R \neq 0$, comm.)

We had observed $(\subseteq)$.
What about $(\supseteq)$?

Let $A = \bigcap P$ and $B = N(R)$.

Claim. $A \subset B$.

Proof We show $B^c \subset A^c$.

Let $a \in R \setminus N(R)$. We show that $a \notin P$ for some $P \in \mathrm{Spec}(R)$.

Idea in general: Take some collection of proper ideals
Show it has a max.
Show it is prime.

Consider the collection

$$\Lambda = \{ I \subsetneq R \mid I \text{ is an ideal, } a \notin I \}.$$

$\Lambda \neq \emptyset$ since $N(R) \in \Lambda$. Λ is a poset by $\subseteq$.

Given a chain $\{I_i\}_{i \in I}$, take $I = \bigcup I_i$.

$I \in \mathcal{A}$, clearly. By Zorn, $\exists$ maximal $\mathfrak{p} \in \mathcal{A}$.

Claim. $\mathfrak{p}$ is prime.

Let $b, c \in R$ s.t. $b \notin \mathfrak{p}$ and $c \notin \mathfrak{p}$. (want to show $bc \notin \mathfrak{p}$.)

By maximality of $\mathfrak{p}$ in $\mathcal{A}$, we get

$$\mathfrak{p} + \langle b \rangle \notin \mathcal{A} \not\ni \mathfrak{p} + \langle c \rangle.$$

Thus, $a \in \mathfrak{p} + \langle b \rangle$ and $a \in \mathfrak{p} + \langle c \rangle$.

$\Rightarrow$ $a = p_1 + r_1 b = p_2 + r_2 c$, $p_1, p_2 \in \mathfrak{p}$, $r_1, r_2 \in R$

$$a^2 = p + r_1 r_2 bc$$

$bc \in \mathfrak{p} \iff a^2 \in \mathfrak{p}$

↳ Now what?

Well, we didn't use the full power of $a \notin \mathcal{N}(R)$.

To be continued...

Lecture 12 (10-09)

10 September 2020 11:14 AM

Changing the prev. proof.

Consider the collection

$$\Lambda = \{ I \subsetneq R \mid I \text{ is an ideal, } a^n \notin I \text{ for any } n \in \mathbb{N} \}$$

$\Lambda \neq \emptyset$ since $N(R), \langle 0 \rangle \in \Lambda$. Λ is a poset by $\subseteq$.

Given a chain $\{I_i\}_{i \in I}$, take $I = \bigcup I_i$.

$I \in \Lambda$, clearly. By Zorn, $\exists$ maximal $\mathfrak{p} \in \Lambda$.

(still goes through)

Claim. $\mathfrak{p}$ is prime.

Let $b, c \in R$ s.t. $b \notin \mathfrak{p}$ and $c \notin \mathfrak{p}$. (want to show $bc \notin \mathfrak{p}$.)

By maximality of $\mathfrak{p}$ in Λ, we get

$$\mathfrak{p} + \langle b \rangle \notin \Lambda \supsetneq \mathfrak{p} + \langle c \rangle.$$

Thus, $a^n \in \mathfrak{p} + \langle b \rangle$ and $a^m \in \mathfrak{p} + \langle c \rangle$. for some $n, m \in \mathbb{N}$

$\Rightarrow$ $a^n = p_1 + r_1 b$, $a^m = p_2 + r_2 c$, $p_1, p_2 \in \mathfrak{p}$, $r_1, r_2 \in R$

$$a^{n+m} = p + r_1 r_2 bc$$

$bc \in \mathfrak{p} \Rightarrow a^{n+m} \in \mathfrak{p}$

↳ not possible by def^n of $\mathfrak{p}$

Thus, $bc \notin \mathfrak{p}$.

Hence, $\mathfrak{p}$ is a prime and $a \notin \mathfrak{p}$. ∎

Thus, we have proven.

Thm. Let R be a non-zero commutative ring. Then,

$$\mathcal{N}(R) = \bigcap_{\mathfrak{p} \in \operatorname{Spec}(R)} \mathfrak{p}.$$

Cor. Let $I \subsetneq R$ be a proper ideal. Then,

$$\sqrt{I} = \bigcap_{\substack{\mathfrak{p} \in \operatorname{Spec}(R) \\ I \subset \mathfrak{p}}} \mathfrak{p}.$$

Proof. ① Either go mod I.
② Re-write earlier theorem with new 1.

Notation: For an ideal $I \subset R$,

$$V(I) = \{\mathfrak{p} \in \operatorname{Spec}(R) : I \subset \mathfrak{p}\}.$$

Prime Avoidance

Set Theoretic Q. Let $A, A_1, \dots, A_n$ be sets. If $A \subset \bigcup_{i=1}^{n} A_i$, is it necessary that $A \subset A_i$ for some i?

Nope!

Take ($n=2$) $A = \{0, 1\}$, $A_1 = \{0\}$, $A_2 = \{1\}$.

Is the above true if each A and A_i is an ideal in some (comm.) ring R?

Still nope!

Ex. Find a counterexample.

However, the statement is true for prime ideals.

Thm. (Prime Avoidance) Let $I \subset P_1 \cup \cdots \cup P_n$ for $P_i \in \operatorname{Spec}(R)$.

Then, $I \subset P_j$ for some j.

Proof. Note that $n=2$ is true in general. (Even if $P_1, P_2 \notin \operatorname{Spec}(R)$.)

We prove $n \geq 3$ by induction.

$n=3$: Suppose $I \not\subset P_j$; $j = 1, 2, 3$.

We show $I \not\subset P_1 \cup P_2 \cup P_3$.

$\rightarrow \exists\, a_j \in I$ but $a_j \notin P_j$.

Verify that $a = a_1 a_2 + a_3 a_1 + a_2 a_3 \in I$ but not in union.

This actually WON'T work. (Or at least, we don't see why it should.)

The point is that we did not use the full info.

That is, $I \not\subset P_1 \cup P_2$, etc. (induction)

Counter example for non-prime ideals.

Take the ring $R = \dfrac{\mathbb{F}_2[x,y]}{\langle x^2, xy, y^2 \rangle}$ and the ideal $I = \langle \bar{x}, \bar{y} \rangle \subset R$.

$$= \{ 0, 1, \bar{x}, \bar{y}, \bar{x}+1, \bar{y}+1, \bar{x}+\bar{y}, \bar{x}+\bar{y}+1 \}$$

$I = \{ 0, \bar{x}, \bar{y}, \bar{x}+\bar{y} \}$ ← this is not principal. (Check manually.)

But $I \subset \langle \bar{x} \rangle \cup \langle \bar{y} \rangle \cup \langle \bar{x}+\bar{y} \rangle$ and not contained in any individual one.

But $I \subset \langle \bar{x} \rangle \cup \langle \bar{y} \rangle \cup \langle \bar{x} + \bar{y} \rangle$ and not contained in any individual one. □

Lecture 13 (14-09)

14 September 2020 09:35 AM

Thm. (Prime avoidance)

Let $I \subset R$ be an ideal and $\mathfrak{p}_1, \dots, \mathfrak{p}_n \in \operatorname{Spec}(R)$.

If $I \subset \bigcup \mathfrak{p}_i$, then $I \subset \mathfrak{p}_i$ for some $1 \le i \le n$.

Proof. $n=1$. Nothing.

$n=2$. Suppose not. Take $a_1 \in I \setminus \mathfrak{p}_1$ & $a_2 \in I \setminus \mathfrak{p}_2$.

Then, $a_1 + a_2 \in I$.

But $a_1 + a_2 \notin \mathfrak{p}_1 \cup \mathfrak{p}_2$ $\to \leftarrow$

$n \ge 3$. By induction. Suppose not.

we know $I \not\subset \bigcup_{\substack{i=1 \\ i \neq k}}^{n} \mathfrak{p}_i$ for each k, by induc.

Choose $a_k \in I \setminus \bigcup_{\substack{i=1 \\ i \neq k}}^{n} \mathfrak{p}_i$.

Then, $b_k = \prod_{\substack{j=1 \\ j \neq k}}^{n} a_j \notin \mathfrak{p}_k$ since $\mathfrak{p}_k$ is prime.

$\in \mathfrak{p}_j$ for all $j \neq k$.

here is where we used primality

Thus, $b_k \in \bigcup_{\substack{j=1 \\ j \neq k}}^{n} \mathfrak{p}_j \setminus \mathfrak{p}_k$, also $b_k \in I \setminus \mathfrak{p}_k$.

Let $b \in I$ be defined as

$$b = b_1 + \dots + b_n.$$

Then, $b \in I \setminus \bigcup_{j=1}^{n} \mathfrak{p}_j$. $\to \leftarrow$

Thm. (More general prime avoidance) In the above hypothesis, we can assume two are not necessarily prime.

Proof. We phrase the theorem as follows:

Let $n \geq 2$.

Let $I_1, \dots, I_n \subset R$ be ideals s.t. $I_n \in \operatorname{Spec}(R)$ for $n \geq 3$.

Let $I \subset R$ be an ideal such that

$$I \subset \bigcup_{i=1}^{n} I_i.$$

Then, $I \subset I_i$ for some $1 \leq i \leq n$.

Proof. For $n=2$, we know by earlier.

Assume true for $n-1$ for some $n \geq 3$.

Now, let $I_1, \dots, I_n$ be as in the theorem.

Assumption: Suppose $I \not\subset I_i$ for any $1 \leq i \leq n$ but $I \subset \bigcup_{i=1}^{n} I_i$.

By induction, $I \not\subset \bigcup_{\substack{i=1 \\ i \neq k}}^{n} I_i$ for any $1 \leq k \leq n$.

↳ each such has at most 2 ideals which are possibly not prime

Thus, we may choose $a_k \in I \setminus \bigcup_{\substack{i=1 \\ i \neq k}}^{n} I_i$ for each $k = 1, \dots, n$.

Then, $a_k \in I_k$ for each $1 \leq k \leq n$.

Define $a = \underbrace{a_1 a_2 \cdots a_{n-1}}_{\in I_1, \dots, I_{n-1}} + \underbrace{a_n}_{\in I_n \setminus (I_1 \cup \dots \cup I_{n-1})}$.

This does not belong to I_n since I_n is prime, whereas each factor $\notin I_n$

Thus, $a \notin \bigcup_{i=1}^{n} I_i$, contradiction!

Lecture 14 (15-09)

15 September 2020 10:32 AM

Localisation : Create "more" units

E.g. $R = \mathbb{Z}[1/2]$ → ring containing $\mathbb{Z}$ as a subring

$$\mathbb{Z}[1/2] = \left\{ \frac{m}{2^k} : m \in \mathbb{Z},\ k \in \mathbb{N} \cup \{0\} \right\} \hookleftarrow \mathbb{Z}$$

Observed that 2 is a unit in R.

Note: If $a \in R$ becomes a unit, so do a^n for all $n \in \mathbb{N}$.
Also, if $ab \in U(R)$, then $a, b \in U(R)$.
Conversely, if $a, b \in U(R)$, then $ab \in U(R)$.

Example. ① Take $R = \mathbb{Z}/6\mathbb{Z}$. What happens if we "invert 2"?

Then, $2 \cdot 3 = 0 \Rightarrow 2 = 0$. 2 becomes 0.

$3 = 2 + 1 = 1$, $4 = 2 + 2 = 0$, $5 = 1 + 4 = 1$.

Looks like the ring has become $\mathbb{Z}/2\mathbb{Z}$.

(Haven't yet defined what "invert" means)

② $R = \mathbb{Z}$. What if we invert all non-zero elements?

Expect : $\mathbb{Q}$

(In fact, that's how we defined the field of fractions of an ID.)

③ $R = \mathbb{Z}$. Invert 2.

Expect: $\mathbb{Z}[1/2]$

④ $R = \mathbb{Z}$. Invert whatever possible except 2.

(Invert $\mathbb{Z} \setminus 2\mathbb{Z}$)

↑ set exclusion

↑ set exclusion

Expect: $\left\{ \frac{m}{n} : m \in \mathbb{Z},\ n \in \mathbb{Z} \setminus 2\mathbb{Z} \right\}$.

↓ recall

When constructing field of fracs, these were equiv classes. This was $\sim$ on $R \times (R \setminus \{0\})$.

Q. Given R, $A \subset R$, we "invert" elements in A to get a ring R_A. ($A^{-1}R$ sometimes)

1. How do we do this? (Idea: $\mathbb{Q}$ from $\mathbb{Z}$)
2. What properties must A have?

Def. A subset $A \subset R$ is called multiplicatively closed set (m.c.s.) if

① $\forall a, b \in A$: $a, b \in A$

② $1 \in A$

③ $0 \notin A$

Given an m.c.s. $A \subset R$, we create a new ring R_A as follows:

1) Take the set $R \times A$.

2) Define a relation on $R \times A$ as
$(x_1, a_1) \sim (x_2, a_2)$ iff $\exists a \in A$ s.t. $a(x_1 a_2 - x_2 a_1) = 0$.

Verify that this is an equivalence relation. (Ex. 1)

3) The equivalence class of (x_1, a_1) is denoted by $\frac{x}{a}$.

4) $R_A := \left\{ \frac{x}{a} : (x, a) \in R \times A \right\}$.

Questions to think: ① When is $\frac{x}{a} = \frac{y}{b}$? ② When is $\frac{x}{a} = 0$?

Questions to think: ① When is $\frac{x}{a} = \frac{y}{b}$? ② When is $\frac{x}{a} = 0$? $\in U(R_A)$?

5) Define $+$ and $\cdot$ on R_A as:

$$\frac{x}{a} + \frac{y}{b} = \frac{xb + ya}{ab} \quad ; \quad \frac{x}{a} \cdot \frac{y}{b} = \frac{xy}{ab}.$$

(Ex. 2) Verify that these operations are well-defined. Show that R_A is then a ring.

Solutions.

(Ex. 1) Show that $\sim$ is an equiv. relation.

Soln: Reflexive ($a=1$) and symm. (same a) is clear.

Transitivity: Let $(x_1, a_1) \sim (x_2, a_2)$ and $(x_2, a_2) \sim (x_3, a_3)$.

Then, $\exists\, a, a' \in A$ s.t. $a(x_1 a_2 - x_2 a_1) = 0$

$a'(x_2 a_3 - x_3 a_2) = 0$

mult. with $a_3 a$

mult. with $a_2 a$

$x_1 a_3 (a a' a_2) - x_2 a a' a_1 a_3 = 0$

$x_2 a a' a_1 a_3 - x_3 a_1 (a' a_2 a) = 0$

add

$x_1 a_3 a a' a_2 - x_3 a_1 a' a_2 a = 0$

$\Rightarrow a a' a_2 (x_1 a_3 - x_3 a_1) = 0$

$a a' a_2 \in A$, since A is an m.c.s.

$\therefore (x_1, a_3) \sim (x_3, a_1)$, as desired.

(Ex. 2) To show: well-defined.

Let $\frac{x}{a} = \frac{x'}{a'}$ and let $\frac{y}{b} \in R_A$.

Let $\frac{x}{a} = \frac{x'}{a'}$ and let $\frac{y}{b} \in R_A$.

It suffices to show that: $\frac{xb+ya}{ab} = \frac{x'b+ya'}{a'b}$. (Note that the fractions make sense because $ab \in A$.)

We know that $\exists a_1 \in A$ s.t.

$$a_1(xa' - x'a) = 0$$

Observe: $\frac{x}{a} = \frac{x'}{a'} \Rightarrow \frac{xb}{ab} = \frac{x'b}{a'b}$. ①

Also, $\frac{y}{b} = \frac{ya}{ab} = \frac{ya'}{a'b}$. ②

$\exists a_1 \in A$: $a_1(xa' - x'a) = 0 \Rightarrow \exists a_1 \in A$: $a_1((xb)(a'b) - (x'b)(ab)) = 0$

① : $\exists a_1 \in A$: $a_1(xb\,a'b - x'b\,ab) = 0$ $\times a_2$

② : $\exists a_2 \in A$: $a_2(ya\,a'b - y'a\,ab) = 0$ $\times a_1$

add

$$\underbrace{a_1 a_2}_{\in A}\{(xb+ya)(a'b) - (x'b+y'a)(ab)\} = 0$$

$$\Rightarrow \frac{xb+ya}{ab} = \frac{x'b+y'a}{a'b}.$$

Thus, if $\frac{x}{a} = \frac{x'}{a'}$ and $\frac{y}{b} = \frac{y'}{b'}$, then

$$\frac{xb+ya}{ab} = \frac{x'b+ya'}{a'b} = \frac{x'b'+y'a'}{a'b'}$$

use above thing again and swap roles of x & y.

Now, we prove $\cdot$ is well defined.

Let $\frac{x}{a} = \frac{x'}{a'}$ and $\frac{y}{b} \in R_A$ as before

$\Downarrow$

$\exists a_1 \in A$: $a_1(xa' - ax') = 0$

$$a_1\big((xa')(yb) - (ax')(yb)\big) = 0$$

$$a_1\big((xy)(a'b) - (x'y)(ab)\big) = 0 \Rightarrow \frac{xy}{ab} = \frac{x'y}{a'b},$$

as desired.

That it is a commutative ring is now easily verified using the fact that R was a commutative ring.