

Lecture 8 (01-09)

01 September 2020 10:29 AM

If $R \rightarrow R/I \times R/J$ 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 $\text{Max}(R)$, and if R is commutative, then the set of prime ideals is denoted $\text{Spec}(R)$.
 called the prime spectrum of R .

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

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

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

Okay, assume $R \neq 0$.

Claim: $\text{max}(R) \neq \emptyset$.

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 $I_j \subset I \quad \forall j$.]

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 \nearrow

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

Similarly, given $r \in R$, we have $ar, ra \in I_j$. CI.

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

Lastly, to see that I is proper, note that

$I \neq I_j$ $\forall j$ since each I_j was proper.

Thus, $I \neq I$. $\therefore I$ is proper. \square

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

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

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 $\Leftrightarrow \exists m \in \text{Max}(R)$ 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.

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

Working rule: $ab \in P, a \notin P \Rightarrow b \in P$.

Max ideals
are
prime

... be such that

L

o

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

$$ab \in m \text{ and } a \notin m.$$

$$a \notin m \Rightarrow m \subsetneq m + \langle a \rangle \Rightarrow m + \langle a \rangle = R$$
$$\Rightarrow \exists m \in m, r \in R \text{ s.t. } m + ra = 1$$

$$\Rightarrow mb + rab = b$$
$$\underbrace{\begin{matrix} mb \\ \in m \end{matrix}}_{\in m} + \underbrace{\begin{matrix} rab \\ \in m \end{matrix}}_{\in m} = b$$

$$\therefore b \in m.$$

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 $\Rightarrow \langle a \rangle \neq R$

\Updownarrow we proved

↑ obvious since
↑ max ideals are
proper

a is cont. in \Rightarrow

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

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

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

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

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

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

$$\left[\bigcup_{m \in \text{Max}(R)} m = R \setminus \mathcal{V}(R) \right]$$

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

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

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

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

Jacobson radical

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

Proof. If $a \in N(R)$, then $a^k = 0$ for some k .

$\Rightarrow a^k \in \mathfrak{m}_y \text{ for every max}$
 $\text{max. ideals are prime}$

$\Rightarrow a \in \mathfrak{m}_y \text{ for every max}$
 $\Rightarrow a \in J(R)$.

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

$p \in \text{Spec}(R)$

\hookrightarrow 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: $a \in J(R) \Rightarrow \forall r \in R (1+ra \in N(R))$

\leftarrow
Does this converse hold now?
Yes!

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

Prop. (\Rightarrow) Let $a \in J(R)$ and $r \in R$ be arbitrary.
 $ra \in J(R)$ since $J(R)$ is an ideal.

Thus, $ra \in \mathfrak{m}_y$ for every max. ideal \mathfrak{m}_y .

$\Rightarrow 1+ra \notin \mathfrak{m}_y$ for any max. ideal \mathfrak{m}_y

$\Rightarrow 1+ra$ is a unit.

\Leftarrow Fix $a \in R$.

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

Assumption: Suppose that $\exists m \in \text{Max}(R)$ s.t. $a \notin m$.
Then, $m + \langle a \rangle \subseteq R$.

$$\Rightarrow m - ra = 1 \quad \text{for some } r \in R, m \in m.$$

$$\Rightarrow m = 1+ra \in m \text{ is a unit} \rightarrow \Leftarrow$$

Thus, our assumption was incorrect. In other words,
 $a \in m$ for all $m \in \text{Max}(R)$.

Thus, $a \in J(R)$. \square

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

Sol. Disproof. We construct a counterexample.

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

Ideals of $R = \{\{0\}, \{0, 2\}, R\}$
 \hookrightarrow maximal!

Thus, $J(R) = \{0, 2\} \neq \{0\}$. \square

(Prime ideal
Exercise solution)

Let R be a comm. ring and $I, J \subset R$
be ideals. Let $p \in \text{Spec}(R)$ s.t.
 $IJ \subset p$ and $I \not\subset p$.

We show that $J \subset p$.

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

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

$\Rightarrow ij \in p$ and $i \notin p$.

$\therefore j \in p$ since p is prime.

$\Rightarrow J \subset p$ (j was arbit) \square

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

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

A: Well, if φ is onto, then (\bar{r}, \bar{s}) must have a preimage.

$$\therefore \varphi(a) = (\bar{r}, \bar{s}) \text{ for some } a \in R.$$

$$\Rightarrow a \equiv r \pmod{I} \quad \& \quad a \equiv s \pmod{J}$$

$$\Rightarrow 1-a \in I \text{ and } a \in J$$

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

Leads to the following def?

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

Co-maximal, comaximal ideals

Thus, if $\varphi: R \rightarrow R/I \times R/J$ 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

$$\varphi: R \rightarrow R/I \times R/J \text{ surjective?}$$

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. $a \in R, b \in R$.

$$\text{Consider } r = bi + aj \in R.$$

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

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

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

$$= (\bar{a}, \bar{b}).$$

□

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

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

$$R/I \cap J \xrightarrow{\tilde{\varphi}} R/I \times R/J, \text{ which is an isomorphism}$$

$\uparrow \pi \quad \uparrow \varphi$

if the pair (I, J) is comax.

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

Proof. (1) Always.

(2) Let $a \in I \cap J$. $i+j=1$

$$a = \underset{I}{\overset{i}{\underset{\uparrow}{a_i}}} + \underset{J}{\overset{j}{\underset{\uparrow}{a_j}}}$$

$$IJ = JI \quad IS$$

□

② Examples : Let $m \in \text{Max}(R)$ and $I \neq m$ be a proper ideal.

Then, (I, m) is comaximal.

However, this will not work if every proper ideal is contained in m .



This means that $\text{Max}(R) = \{m\}$.

Such a ring is called local.
 Notation : (R, m) .

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

If I, J are prop. ideals, then $I, J \subseteq m$ & thus, $I+J \subseteq m \neq R$.

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

Choose two distinct maximal ideals!

$$m_1, m_2 \subsetneq m_1 + m_2. \therefore m_1 + m_2 = R.$$

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 $I_1, \dots, I_n \subset R$. What can we say about

$$\varphi: R \rightarrow R/I_1 \times \dots \times R/I_n ?$$

↳ often called the "diagonal map"

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

Notation: $\bar{e}_j = (\bar{0}, \dots, \bar{0}, \underset{\uparrow j\text{th pos.}}{\bar{1}}, \bar{0}, \dots, \bar{0})$

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

$\Rightarrow 1 - a_j \in I_j \quad \& \quad a_j \in I_k \text{ for } k \neq j$.

$\Rightarrow I_j \quad \& \quad \bigcap_{\substack{k=1 \\ k \neq j}} I_k$ 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 co-maximal. Is (I_1, I_j) comax $\forall j \geq 2$?

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

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

$\Rightarrow I_1 + I_j = R$ showing (I_1, 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 $K > J$.

Proof. Same as above.

Thus, if $\varphi: R \rightarrow R/I_1 \times \dots \times R/I_n$ is onto,

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

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

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

A: Recall we had seen in the last class that if (I, J) is comax, then the induced map $\tilde{\varphi}: R/(I \cap J) \rightarrow R/J \times R/J$ 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, \dots, I_n be pairwise comaximal.

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

Assume claim for now.

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

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

Moreover, this iso was induced by φ .

$$(a + \bigcap_{j=2}^n I_j) \mapsto (a + I_2, \dots, a + I_n).$$

Using this, we get that

$$R \rightarrow R/I_1 \times R/\bigcap_{j=2}^n I_j \rightarrow R/I_1 \times \dots \times R/I_n$$

is onto.

Now, we prove the claim.

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

Proof:

$a_2^{e_{I_2}}, \dots, a_n^{e_{I_n}}$	$b_2^{e_{I_2}}, \dots, b_n^{e_{I_n}}$
$a_2 + b_2 = 1, a_3 + b_3 = 1, \dots, a_n + b_n = 1$	
$1 = (a_2 + b_2) \dots (a_n + b_n)$	
$= a_2 a \dots a_n + \underbrace{b_2 (\quad)}_{\bigcap_{j=2}^n I_j} + b_3 (\quad) + \dots + b_n (\quad)$	$\underbrace{\quad}_{I_1}$

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

Thus, we have proved the Chinese Remainder Theorem.

Thm. (Chinese Remainder Theorem)

Let R be a non-zero commutative ring.

Let $I_1, \dots, I_n \subsetneq R$ be pairwise comaximal ideals.

Then,

$$\cancel{R} \cong R/I_1 \times \dots \times R/I_n.$$

Then,

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

Note that we also proved:

- ① The natural map $R \rightarrow \prod R/I_j$ is onto.
- ② $I_1 \cap \dots \cap I_n = I_1 \dots I_n$.

Ex- Write a text book proof of CRT. \rightarrow 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 $N(R) = \bigcap_{\mathfrak{p} \in \text{Spec}(R)} \mathfrak{p}$? ($R \neq 0$ comm.)

We had observed (\subseteq).

What about (\supseteq)?

Let $A = \bigcap_{\mathfrak{p}} \mathfrak{p}$ 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 $a \notin \mathfrak{p}$ for some $\mathfrak{p} \in \text{Spec}(R)$.

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 $I = \bigcup I_i$.

$I \in A$, clearly. By Zorn, \exists maximal $\mathbb{P} \in A$.

Claim: \mathbb{P} is prime.

Let $b, c \in R$ s.t. $b \notin \mathbb{P}$ and $c \notin \mathbb{P}$. (Want to show $bc \notin \mathbb{P}$.)

By maximality of \mathbb{P} in A , we get

$$\mathbb{P} + \langle b \rangle \neq A \neq \mathbb{P} + \langle c \rangle.$$

Thus, $a \in \mathbb{P} + \langle b \rangle$ and $a \in \mathbb{P} + \langle c \rangle$.

$$\Rightarrow a = p_1 + r_1 b = p_2 + r_2 c, \quad p_1, p_2 \in \mathbb{P}, \quad r_1, r_2 \in R$$

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

$$bc \in \mathbb{P} \Leftrightarrow a^2 \in \mathbb{P}$$

Now what?

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

To be continued...

Changing the prev. proof.

Consider the collection

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

$\mathcal{I} \neq \emptyset$ since $N(R), \langle 0 \rangle \in \mathcal{I}$. \mathcal{I} is a poset by \subseteq .

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

$I \in \mathcal{I}$, clearly. By Zorn, \exists maximal $\mathbb{P} \in \mathcal{I}$.
still goes through

Claim: \mathbb{P} is prime.

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

By maximality of \mathbb{P} in \mathcal{I} , we get
 $\mathbb{P} + \langle b \rangle \notin \mathcal{I} \Rightarrow \mathbb{P} + \langle b \rangle$.

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

$$\Rightarrow a^n = p_1 + r_1 b ; a^m = p_2 + r_2 c , \quad p_1, p_2 \in \mathbb{P}, \quad r_1, r_2 \in R$$

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

$bc \in \mathbb{P} \Rightarrow a^{n+m} \in \mathbb{P}$
not possible by def" of \mathbb{P}

Thus, $bc \notin \mathbb{P}$.

Hence, \mathbb{P} is a prime and $a \notin \mathbb{P}$. □

Thus, we have proven.

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

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

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

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

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

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

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

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 $A = \{0, 1\}$, $A_1 = \{0\}$, $A_2 = \{1\}$.

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 $I \subset \mathbb{P}_1 \cup \dots \cup \mathbb{P}_n$ for $\mathbb{P}_i \in \text{Spec}(R)$.

Then, $I \subset \mathbb{P}_j$ for some j .

Proof. Note that $n=2$ is true in general. (Even if $\mathbb{P}_1, \mathbb{P}_2 \notin \text{Spec}(R)$.)

We prove $n \geq 3$ by induction.

$n=3$: Suppose $I \not\subset \mathbb{P}_j$; $j = 1, 2, 3$.

We show $I \not\subset \mathbb{P}_1 \cup \mathbb{P}_2 \cup \mathbb{P}_3$.

$\rightarrow \exists a \in I$ but $a \notin \mathbb{P}_j$.

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, $I \not\subset \mathbb{P}_1 \cup \mathbb{P}_2$, etc.
(induction)

Counter example for non-prime ideals.

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

\parallel

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

$I = \{ 0, \bar{x}, \bar{y}, \bar{x}+\bar{y} \}$ ← 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. \square

Lecture 13 (14-09)

14 September 2020 09:35 AM

Thm.

(Prime avoidance)

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

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

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 $a_1 + a_2 \notin \mathfrak{p}_1, \mathfrak{p}_2 \rightarrow$

$n \geq 3$.

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

Here is where we used primality

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 $j \neq k$.

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

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

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.) $R = \mathbb{Z}[\frac{1}{2}]$ → ring containing \mathbb{Z} as a subring

$$\left\{ \frac{m}{2^k} : m \in \mathbb{Z}, k \in \mathbb{N} \cup \{0\} \right\} \hookrightarrow \mathbb{Z}$$

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 3"?

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: $\mathbb{Z}[\frac{1}{2}]$

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

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

set exclusion

^{set exclusion}

$$\text{Expect: } \left\{ \frac{m}{n} : m \in \mathbb{Z}, n \in \mathbb{Z} \setminus \{0\} \right\}.$$

↓
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 .
 $(A^{-1}R \text{ sometimes})$

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
 $(x_1, a_1) \sim (x_2, a_2) \text{ iff } \exists a \in A \text{ s.t. } a(x_1 a_2 - x_2 a_1) = 0.$

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

- 3) The equivalence class of (x_1, a_1) is denoted by $\frac{x_1}{a_1}$.
- 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 $\frac{x}{a} = 0$?
When is $a \in V(R_A)$?

5) Define + and . on R_A as:

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

(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 and symm. is clear.
(some a)

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.

$$\begin{aligned} & a(x_1 a_2 - x_2 a_1) = 0 \\ & a'(x_2 a_3 - x_3 a_2) = 0 \end{aligned}$$

mult. with $a_3 a'$

$$\begin{aligned} & x_1 a_3 (aa' a_2) - x_2 a a' a_1 a_3 = 0 \\ & x_2 a a' a_1 a_3 - x_3 a_1 (a' a_2 a) = 0 \end{aligned}$$

add

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

$$\Rightarrow \underbrace{a a' a_2}_{\in A} (x_1 a_3 - x_3 a_1) = 0$$

$\in A$, 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 $\frac{y}{b} \in R_A$.

It suffices to show that: $\frac{xb+ya}{ab} = \frac{x'b+y'a'}{a'b}$. (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, $\frac{y}{b} = \frac{ya}{ab} = \frac{y'a'}{a'b}$. ②

\downarrow \uparrow

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

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

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

} add

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

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

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

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

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

Now, we prove . is well defined.

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

↓

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

$$a, \left(\underset{\Downarrow}{(xa')(yb)} - (ax')(yb) \right) = 0$$

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

as desired.

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

Lecture 15 (17-09)

17 September 2020 11:32 AM

① When is $\frac{x}{a} = 0$ in R_A ?

Precisely when $a' \cdot x = 0$ for some $a' \in A$.

② $\frac{0}{1} = 0 \quad \forall a \in A.$

$$\textcircled{3} \quad \frac{xa'}{aa'} = \frac{x}{a} \quad \forall x \in R, \forall a, a' \in R$$

We have a function $\varphi_A : R \rightarrow R_A$
 $x \mapsto \frac{x}{1}$

Is this a ring homomorphism? Yes, because of our def
of + and \cdot .

Q. Let $J \subset R_A$ be an ideal. How is J related to $I = \varphi_A^{-1}(J)$?

Note: $x \in I$ iff $\frac{x}{1} \in J$.

$$\varphi_A(I) = \left\{ \frac{x}{1} \in R_A : x \in I \right\}$$

$$\langle \varphi_A(I) \rangle = \left\langle \frac{x}{1} : x \in I \right\rangle \subset J$$

?
✓ Yes

$$\text{Let } \frac{x}{a} \in J. \text{ Then, } \varphi_A(x) = \frac{a}{1} \cdot \frac{x}{a} \in J \Rightarrow x \in \varphi_A^{-1}(J)$$

$$\Rightarrow \frac{x}{a} = \frac{x}{1} \cdot \frac{1}{a} \in \left\langle \frac{x}{1} : x \in I \right\rangle$$

The above ideal is denoted by $IR_A = \langle \varphi_A(I) \rangle \subset R_A$.

① Conclusion: If $I = \varphi_A^{-1}(J)$, then $J = IR_A$.

* Define $I_A = \left\{ \frac{x}{a} \in R_A : x \in I, a \in A \right\} \subset R_A$.

② We have shown $I_A = IR_A$.

General: $\varphi: R \rightarrow S$ is a ring, $I \subset R$ an ideal, then
(Extension ideal) $IS := \langle \varphi(I) \rangle \subset S$.

Def.: If every ideal of R is finitely generated, we say
 R is Noetherian.
(Noetherian ring)

If every ideal of R is principal, we say R is a principal ideal ring. (PIR)

Ex. Let R be Noetherian, $I \subset R$ an ideal

Prove or disprove: R/I is Noetherian.

These give us many examples.

Thm. (Hilbert Basis Theorem) If R is Noetherian, then so is $R[x]$.

Q. If R is Noetherian and $A \subset R$ is an m.c.s., is R_A Noetherian?

Q. How are ideals in R_A related to ideals in R ?

More precisely: given an ideal $J \subset R_A$, \exists ideal $I \subset R$ s.t. $J = IR_A$?

Yes. Take $I = \varphi_A^{-1}(J)$.

$$\left\{ \begin{array}{c} \text{some ideals} \\ \text{in } R \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{ideals in } R_A \\ \text{id} \end{array} \right\}$$

Q. a) When is $I_A = 0$? $I_A = 0 \Leftrightarrow \forall x \in I \ (\forall a \in A \ (ax = 0))$

b) When is $I_A = R_A$? $I_A = R_A \Leftrightarrow \frac{1}{1} \in I_A \Leftrightarrow I \cap A \neq \emptyset$

$$\downarrow \\ \exists x \in I, a \in A \text{ s.t. } \frac{1}{1} = \frac{x}{a}$$

Q. What about $\text{Spec}(R_A)$ and $\text{Max}(R_A)$?



Lecture 16 (21-09)

21 September 2020 09:27 AM

Some examples of m.c.s.:

① Let $a \in R \setminus N(R)$. Then $A = \{1, a, a^2, \dots\}$ is an m.c.s.

In this case, R_A is denoted by R_a . $\hookrightarrow 0$ isn't here

$$R_a = \left\{ \frac{r}{a^m} : r \in R, m \in \mathbb{N} \cup \{0\} \right\}.$$

② Let $p \in \text{Spec}(R)$. Then, $A = R \setminus p$ is an m.c.s.

R_A is denoted R_p .

$\hookrightarrow R$ localised at p .

\hookrightarrow This turns out to be a local ring.

Note: \mathbb{Z}_2 is $\mathbb{Z}[Y_2] = \left\{ \frac{m}{2^n} \in \mathbb{Q} : n \in \mathbb{N} \cup \{0\} \right\}$.

$$\mathbb{Z}_{(2)} = \left\{ \frac{m}{n} \in \mathbb{Q} : 2 \nmid n \right\}$$

Primes and Maximal Ideals in R_A .

Q. What can we say about φ_A ?

onto: No, we don't expect this to be onto. E.g. $\mathbb{Z} \rightarrow \mathbb{Q}$
 $(A = \mathbb{Z} \setminus \{0\})$

One-one: $A \cap Z(R) = \emptyset \Rightarrow \varphi_A$ is one-one

Proof-

Converse?

\hookrightarrow Suppose φ_A is not 1-1. Then, $\exists x \in R \setminus \{0\}$ s.t. $\varphi_A(x) = 0$.

$$\begin{array}{ccc} \parallel & & \parallel \\ x & & 0 \end{array}$$

$$\begin{array}{c} \parallel \\ \times \\ \hline \end{array} \quad \begin{array}{c} \parallel \\ 0 \\ \hline \end{array}$$

$\Rightarrow \exists a \in A \text{ s.t. } ax = 0.$

$$\Rightarrow a \in A \cap Z(R) \Rightarrow A \cap Z(R) \neq \emptyset$$

Conversely, if $A \cap Z(R) \neq \emptyset$, then φ_A is not H.

Let $a \in A \cap Z(R)$ and $x \neq 0$ be s.t. $ax = 0$

$$\Rightarrow \varphi_A(x) = 0$$

$\Rightarrow \varphi_A$ is not H.

Thus, φ_A is one-one $\Leftrightarrow A \cap Z(R) = \emptyset$.

Eg3. Let $A = R \setminus Z(R)$. Then A is an m.c.s. and R_A is called the total ring of quotients of R (denoted $Q(R)$).

$\frac{a}{1}, \frac{b}{1} =$ elements of $R \setminus Z(R)$ become units under φ_A .

Q. let $J \in \text{Spec}(R_A)$? What can you say about $\varphi_A^{-1}(J) = I$?

$I \in \text{Spec } R$.

Moreover, $I_A = IR_A = J$

Also, $I \cap A = \emptyset$. (Otherwise $J = R_A$.)

contradict primality

Consider the collection

$$\{ P_A : P \in \text{Spec}(R) \text{ and } P \cap A = \emptyset \}$$

We showed that

$$\text{Spec}(R_A) \cup$$

Is this the reverse true? That is, if $P \in \text{Spec}(R)$, then is $P \cap A = \emptyset \Rightarrow P_A \in \text{Spec}(R_A)$?

(Note: If $\mathfrak{p} \cap A = \emptyset$, then)
 $\mathfrak{p} \subseteq R$.

let $\frac{x}{a}, \frac{y}{b} \in R_A$ be s.t. $\frac{xy}{ab} \in \mathfrak{p}_A$.

Then, $\frac{xy}{ab} = \frac{z}{c}$ for some $z \in \mathfrak{p}$, $c \in A$.

$$\Rightarrow \exists u \in A : u(xy_c - zab) = 0$$

$$\Rightarrow uxyc = (uab)z \in \mathfrak{p}$$

But $u, c \notin \mathfrak{p}$. Thus, $xy \in \mathfrak{p}$.

$$\Rightarrow x \in \mathfrak{p} \text{ or } y \in \mathfrak{p}$$

$$\Rightarrow \frac{x}{a} \in \mathfrak{p}_A \text{ or } \frac{y}{b} \in \mathfrak{p}_B. \quad \square$$

Thus, $\mathfrak{p}_A \in \text{Spec}(R_A)$

Conclusion: $\text{Spec}(R_A) \hookrightarrow \{\mathfrak{p} \in \text{Spec}(R) : \mathfrak{p} \cap A = \emptyset\}$.

Lecture 17 (22-09)

22 September 2020 10:29 AM

Ex: If $P_A \in \text{Spec}(R_A)$ and $\frac{x}{a} \in P_A$, then $x \in P$.

Q: Is the above true if we do not assume P_A is prime.
Ans! Take $R = \mathbb{Z}$, $A = \mathbb{Z} \setminus \{0\}$, $P = \langle 2 \rangle$, $\frac{x}{a} = \frac{3}{1}$.

Yesterday, we proved a 1-1 correspondence between $\text{Spec}(R_A)$ and $\{P \in \text{Spec}(R) : R \cap A\}$.

$$\begin{array}{ccc} P_A & \longleftrightarrow & P \\ \downarrow & \longmapsto & \varphi_A^{-1}(P) \end{array}$$

• We know $\text{Max}(R_A) \subset \text{Spec}(R_A)$.

Q: Which subset of RHS corresponds to $\text{Max}(R_A)$?

Claim: Let $\Lambda = \{I \subset R : I \text{ is an ideal and } I \cap A = \emptyset\}$.

The maximal elements of Λ are in one-one correspondence with maximal ideals of R_A .

Proof: (\rightarrow) Let $I \in \Lambda$ be maximal. We want to prove: $I_A \in \text{Max}(R_A)$.

Let $I_A \subset J \subsetneq R_A$. (We want to prove $I_A = J$.)

let $K = \varphi_A^{-1}(J) \subset R$. Then $I \subset K$.

Moreover, $K \cap A \neq \emptyset$ since $J \neq R_A$.

$\Rightarrow I = K$, by maximality (we know K is an ideal)

Thus, $I = \varphi_A^{-1}(J)$.

$$\Rightarrow I_A = (\varphi_A^{-1}(J))_A = J.$$

□

(\leftarrow) Let $J \in \text{Max}(R_A)$. We claim that $\varphi_A^{-1}(J)$ is a maximal elt. of A .

First note that $\varphi_A^{-1}(J) \cap A = \emptyset$ since $(\varphi_A^{-1}(S))_A = J \neq R$.

Let $I = \varphi_A^{-1}(J)$. Then, $I \in A$.

Now, let $I' \in A$, $I \subset I'$. (Want to prove $I = I'$.)

Observe: $I_A = J$.

Since $I \subset I'$, we have $J = I_A \subset I'_A$.

$I' \in A \Rightarrow I'_A \neq R_A$

By maxim. of J , we get $J = I'_A$.

$$\Rightarrow I' \subset \varphi_A^{-1}(I'_A) = \varphi_A^{-1}(J) = I.$$

Thus, $I = I'$, proving maximality of I in A .

Along with our earlier observation for Spec, (\rightarrow) & (\leftarrow) prove the correspondence since composition in both directions is id.

Note. Let $p \in \text{Spec}(R)$. Then $A = R/p$ is an m.c.s.

Moreover A as above is $\{I \subset R : I \subset p\}$.

$p \in A$. Thus, $\text{Max}(A) = \{p\}$.

exactly one.

Thus, $R_p = R_p$ is a local ring.

Q.

Find $\text{Max}(R_A)$ when $A = R \setminus (p_1 \cup \dots \cup p_n)$, $p_i \in \text{Spec}(R)$.

Lecture 18 (24-09)

24 September 2020 11:24 AM

Universal Property of Localisation

- ① $(R_A, \varphi_A: R \rightarrow R_A)$ is a pair such that R_A is a ring,
 φ_A is a ring map and $\varphi_A(A) \subset \mathcal{V}(R_A)$.
- ② Let $(S, \varphi: R \rightarrow S)$ be a pair such that S is a ring,
 φ is a ring map and $\varphi(A) \subset \mathcal{V}(S)$.

Then, φ factors through R_A via φ_A , ^{uniquely} i.e.,

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ & \searrow \varphi_A & \nearrow \tilde{\varphi} \\ & R_A & \end{array} \quad \exists! \tilde{\varphi}: R_A \rightarrow S \text{ s.t. } \tilde{\varphi} \circ \varphi_A = \varphi.$$

In this case, $\tilde{\varphi}\left(\frac{x}{a}\right) = \varphi(x) \cdot [\varphi(a)]^{-1}$.

[↑] this makes sense since $\varphi(a) \in \mathcal{V}(S)$

[↑] Verify that this is well-defined.

- ③ Suppose $(\bar{R}, \bar{\varphi}: R \rightarrow \bar{R})$ is a pair s.t. \bar{R} is a ring,
 $\bar{\varphi}$ is a ring map s.t. $\varphi(R) \subset \mathcal{V}(\bar{R})$.

Furthermore, assume that $(\bar{R}, \bar{\varphi})$ also satisfies ②, i.e., given

(S, φ) as in ②, φ factors as $R \xrightarrow{\varphi} S$ ^{uniquely} $\bar{\varphi} \xrightarrow{\varphi} \bar{R}$.

We would like to claim $R_A \cong \bar{R}$.

$$\bar{\varphi} \xrightarrow{\varphi} \bar{R} \xrightarrow{\varphi_1} \varphi_2 \xrightarrow{\varphi_1} \varphi_2$$

Using ② & ③ &
 $\bar{\varphi}(A) \subset \mathcal{V}(\bar{R})$, $\varphi_A(A) \subset \mathcal{V}(R_A)$,

$$\begin{array}{ccc} & \bar{\varphi} & \\ R & \xrightarrow{\quad \varphi \quad} & R_A \\ & \varphi_A & \end{array}$$

$\bar{\varphi}(A) \subset \bar{V(R)}$, $\varphi_A(A) \subset V(R_A)$, we get φ_1 & φ_2 as shown.

rewrite

$$\begin{array}{ccc} & \bar{\varphi} & \\ R & \xrightarrow{\quad \varphi_A \quad} & R_A \\ & \bar{\varphi} & \downarrow \varphi_2 \\ & \bar{\varphi} & \end{array}$$

Both triangles commute and thus,

$$\begin{array}{ccc} & \bar{\varphi} & \\ R & \xrightarrow{\quad \varphi_A \quad} & R_A \\ & \bar{\varphi} & \downarrow \varphi_1 \\ & \bar{\varphi} & \end{array}$$

Thus, $\varphi_1 \circ \varphi_2$ is a lift. However $\text{id}_{\bar{R}}$ is also such a lift. By uniqueness, $\text{id}_{\bar{R}} = \varphi_1 \circ \varphi_2$.

Similarly, $\text{id}_{R_A} = \varphi_2 \circ \varphi_1$. This shows that φ_1 & φ_2 are isomorphisms.

Modules

over a ring (possibly non-commutative)
(but soon we'll go to comm.)

Q. Is $M_2(\mathbb{R})$ a v-space over \mathbb{R} ? Yes

Is $M_2(\mathbb{Z})$ a v-space over \mathbb{Z} ? Well, \mathbb{Z} is not a field but $M_2(\mathbb{Z})$ satisfies all the axioms of v-space (modulo \mathbb{Z} not being a field.)

We say that $M_2(\mathbb{Z})$ is a module over \mathbb{Z} .

Defn. Given a ring R , an R -module M is an abelian group under + with a "scalar multiplication" $\cdot : R \times M \rightarrow M$

left

~~V~~

(left
modules)

under + with a "scalar multiplication" $\therefore R \times M \rightarrow M$

satisfying

$$\left. \begin{array}{l} \textcircled{1} \quad (a+b) \cdot x = a \cdot x + b \cdot x \\ \textcircled{2} \quad (ab) \cdot x = a(b \cdot x) \\ \textcircled{3} \quad a \cdot (x+y) = a \cdot x + a \cdot y \\ \textcircled{4} \quad 1 \cdot x = x \end{array} \right\} \text{for all } x, y \in M, a, b \in R$$

Ex $R^{(\oplus^n)}, M_n(R), R[x], R[[x]], \mathcal{F}(A, R) \quad (A \neq \emptyset)$

In fact, if S is an R -algebra via $\varphi: R \rightarrow S$, then S is an R -module via φ , i.e., for $r \in R, s \in S$, define $r \cdot s := \varphi(r)s$.

Q1 What are modules over a field \mathbb{K} ? Over \mathbb{Z} ?

Q2. Verify if the usual properties hold:

- ① $0 \cdot x = 0$
- ② $0 \cdot 0 = 0$
- ③ $(-1) \cdot x = -x$
- ④ $a \cdot x = 0 \Rightarrow a = 0 \text{ or } x = 0.$

Writing assignment (due 9:30 AM, coming Saturday)

either one

$$\left\{ \begin{array}{l} \textcircled{1} \quad IR_A = I_A \quad \rightarrow \text{define the two sets and show they are equal} \\ \textcircled{2} \quad (I \cap J)_A = I_A \cap J_A \rightarrow \end{array} \right.$$

Lecture 19 (28-09)

28 September 2020 09:26 AM

Examples of modules : $R^{\oplus n}$, $M_n(R)$, $R[x]$, $R[[x]]$, $\mathcal{F}(A, R)$ ($A \neq \emptyset$).

① $R^{\oplus n}$: multiplication is $a \cdot (r_1, \dots, r_n) = (ar_1, \dots, ar_n)$.

$R^{\oplus n}$ is already a ring. The above can be seen as the product $(a, \dots, a)(r_1, \dots, r_n)$ in $R^{\oplus n}$.

② $M_n(R)$: $a \cdot \begin{bmatrix} r_1 & r_2 \\ r_3 & r_4 \end{bmatrix} = \begin{bmatrix} \quad & \quad \\ \quad & \quad \end{bmatrix} = \begin{bmatrix} a & a \\ a & a \end{bmatrix} \begin{bmatrix} r_1 & r_2 \\ r_3 & r_4 \end{bmatrix}$

③ $R[x]$: $a \cdot (a_0 + a_1x + \dots + a_nx^n) = (a + a_1 + \dots + a_n)x^n$

④ $R[[x]]$: similar

⑤ $\mathcal{F}(A, R)$: $a \cdot f = e_a \cdot f$ where e_a is the const f^n .

Thus, they are all actually R -algebra

① $\Psi: R \rightarrow R^{\oplus n}$, $a \mapsto (a, \dots, a)$

② $R \rightarrow M_n(R)$, $a \mapsto \begin{bmatrix} a & & \\ & \ddots & \\ & & a \end{bmatrix}$

③, ④ $a \mapsto a$
↳ const poly/ pow series

⑤ $a \mapsto (x \mapsto a)$
↳ const function

(Verify that these are indeed ring homomorphisms.)

Q. Let \mathbb{k} be a field. What are \mathbb{k} -modules?
Precisely \mathbb{k} -vector spaces.

Q. Let $R = \mathbb{Z}$. what are R -modules?

Precisely abelian groups.

R -module is abelian group is clear by defⁿ.

Conversely, let G be an abelian group. Define scalar mult.
 $\cdot: \mathbb{Z} \times G \rightarrow G$ as

$$n \cdot a = \begin{cases} \underbrace{a + \dots + a}_n & n > 0 \\ 0 & n = 0 \\ \underbrace{(-a) + \dots + (-a)}_{-n} & n < 0 \end{cases}$$

This defines a \mathbb{Z} module structure on G .

In fact, this is the only way to define a \mathbb{Z} -module structure on G .

Thus, things we say about modules will be true for vector spaces and abelian groups (interpreted appropriately).

Ex. Let $R = k[x]$, V a vector space over k , $T: V \rightarrow V$ be linear.
 Then, V is an R -module as follows : Let $u \in V$

How should we define $X \cdot u$?

Things we want : $X \cdot (u+v) = X \cdot u + X \cdot v$ $u, v \in V$
 $X \cdot (au) = (Xa) \cdot u = (ax) \cdot u = a \cdot (Xu)$ $a \in k \hookrightarrow k[x]$

Thus, multiplication by X gives a linear transformation $V \rightarrow V$.

Define $X \cdot u = T(u)$.

In general, for $p \in k[x]$, $u \in V$, define

$$p \cdot u = p(T) \cdot u.$$

Explicitly : $(a_0 + a_1 x + \dots + a_n x^n) \cdot u = a_0 \cdot u + a_1 \cdot Tu + \dots + a_n \cdot T^n u$.

(dot on RHS is the vspace.)

Verify that V is a $\mathbb{k}[x]$ -module. This is called the module structure on V over T .

Note that \mathbb{Z} and $\mathbb{k}[x]$ are PIDs. Thus, understanding modules over PID tells us about abel. groups and V over T .

- Def. ① Let M be an R -module and $N \subseteq M$. Then N is an R -submodule of M if
- Ⓐ $0 \in N$,
 - Ⓑ $x, y \in N \Rightarrow x+y \in N$, and
 - Ⓒ $a \in R, x \in N \Rightarrow ax \in N$.

- ② Let $x \in M$. The submodule generated by x is

$$\langle x \rangle = \{ ax : a \in R \} = Rx.$$

Given $x_1, \dots, x_n \in M$, $\langle x_1, \dots, x_n \rangle = \{ a_1x_1 + \dots + a_nx_n \mid a_i \in R \}$.

$$y \in \langle x_1, \dots, x_n \rangle \Leftrightarrow \exists (a_1, \dots, a_n) \in R^n \text{ s.t. } y = a_1x_1 + \dots + a_nx_n.$$

Given a subset $S \subseteq M$,

$$\langle S \rangle = \left\{ x \in M : \exists n \in \mathbb{N}, (a_1, \dots, a_n) \in R^n, x_1, \dots, x_n \in S \right\} \\ x = a_1x_1 + \dots + a_nx_n.$$

- ③ M is cyclic if $\exists x \in M$ s.t. $M = \langle x \rangle$.
- ④ M is finitely generated if $\exists n \in \mathbb{N}, \exists x_1, \dots, x_n \in M$ s.t. $M = \langle x_1, \dots, x_n \rangle$.
- ⑤ M is simple if the only submodules of M are 0 and M .
- ⑥ M is decomposable if \exists submodules M_1, M_2 s.t. $M_1 \neq 0 \neq M_2$ and

$$M = M_1 \oplus M_2. \quad (\text{That is, } M = M_1 + M_2, M_1 \cap M_2 = 0)$$

M is indecomposable otherwise.

Q.

What are \mathbb{k} -submodules of V ? $\mathbb{k}[\alpha]$ -submodules of V (via T)?

What are \mathbb{Z} -submodules of an abelian group G ?

What are submodules of a ring R ?

If M is an S -module, $\varphi: R \rightarrow S$ is a ring map, then M is an R -module.
(via φ)

Lecture 20 (29-09)

29 September 2020 10:21 AM

Recall If M is an S -module, $\varphi: R \rightarrow S$ is a ring map, then M is an R -module.
(via φ)

We want a function $R \times M \rightarrow M$.

We already have $S \times M \rightarrow M$ and $\varphi: R \rightarrow S$. This gives

$$\begin{array}{ccc} R \times M & \xrightarrow{\quad \varphi \times \text{id}_M \quad} & M \\ & \curvearrowright & \nearrow \end{array}$$

V is a k -vector space, $T: V \rightarrow V$ is linear.

V is a $\mathbb{k}[x]$ -module via T .

\mathbb{k}

Q What are its R -submodules?

Ans. These are precisely the T -invariant subspaces of V .
(A subspace $W \subset V$ is T -invariant if $T(w) \in W$, i.e.,)
 $\forall w \in W: T(w) \in W$.
 $\hookrightarrow W$ is closed under the action of T

(One direction) Let W be a T -inv. subspace of V . We show that W is an R -submodule of V .

① $0 \in W$ is true because W is a subspace

② $\forall u, v \in W (u + v \in W)$ is true because W is a subspace

③ T.S: $\forall p \in \mathbb{k}[x], u \in W (p \cdot u \in W)$

Let $p \in \mathbb{k}[x]$ and $u \in W$ be arbitrary.

Write $p = a_0 + a_1x + \dots + a_nx^n, n \geq 0, a_i \in \mathbb{k}$

Then, $p \cdot u = (a_0 + a_1 T + \dots + a_n T^n)(u)$

\hookrightarrow think of this as the function which is multiplication by a_0

$$= a_0 \cdot u + a_1 \cdot T(u) + \dots + a_n \cdot T^n(u) \in W$$

each $a_i \cdot T^i(u) \in W$ by
invariance

[Thus, we have shown that if W is T invariant, it is $p(T)$
invariant.]

Hence, W is an R -submodule of V (via T).

or simply: W is a submodule of V (via T).

(Other direction) If W is an R -submodule of V , then W is an T -inv. subspace of V .

WRITING ASSIGNMENT, 'ERE THURSDAY 11:30!

Q. What does it mean to say V is decomposable as a $\mathbb{k}[x]$ -submodule.

Note that $V = W_1 \oplus W_2$ says the following:

Given any bases B_1 and B_2 of W_1 and W_2 , we have
that $B_1 \cup B_2$ is a basis of V .

For decomposability as $\mathbb{k}(x)$ module, W_1 & W_2 have to be T -inv.

Q. When is V simple as a $\mathbb{k}[x]$ module?

When V has no T -inv. Subspace other than 0 and V

If T has an eval and $\dim V \geq 2$, then you have $\overset{\text{non-trivial}}{\text{non-inv.}}$ subspace.
Hence, cannot be simple!

abelian group to start with

Def: ① Let $N \subset M$ be an R -submodule. Then, M/N is an R -module with scalar multiplication

$$a \cdot \bar{x} = \overline{a \cdot x}.$$

(Verify this is well defined.)

② Given R -modules M_1, M_2 , a function $\varphi: M_1 \rightarrow M_2$ is an R -module homomorphism (or an R -linear map) if $\forall a \in R \ \forall x, y \in M_1 : \varphi(ax + y) = a\varphi(x) + \varphi(y)$.

E.g. $\pi: M \rightarrow M/N$ given by $x \mapsto \bar{x}$ is R -linear.

Given R -linear $\varphi: M_1 \rightarrow M_2$ and submodules $N_1 \subset M_1, N_2 \subset M_2$, ask and answer questions about $\varphi(N_1)$ and $\varphi^{-1}(N_2)$. Use this to conclude that the submodules of M/N are in 1-1 correspondence with the submodules of M containing N_1 .

Q. Let V be a k -vector space and let $W \subset V$ be a subspace. What is V/W ?

Ex. Let $\text{Hom}_R(M, N) = \{\varphi: M \rightarrow N \mid \varphi \text{ is } R\text{-linear}\}$.

Then, $\text{Hom}_R(M, N)$ is an R -module under point-wise operations.

In fact, one can show that $\mathcal{F}(A, N)$ is a module for $A \neq \emptyset$ and N an R -module. Then, $\text{Hom}_R(M, N) \subset \mathcal{F}(M, N)$ is an R -submodule.

$\text{End}_R(M, M) = \text{Hom}_R(M, M)$ is a (possibly non-comm.)
ring (of endomorphisms).
↓
Composition

Lecture 21 (01-10)

01 October 2020 11:34 AM

Let A be a non-empty set, R a ring. Then, $F(A, R)$ is

- ① a ring, ② an R -module (under pointwise op.)

(The proofs here boiled down to the fact that R had the analogous properties.)

An identical proof shows that: if N is an R -module, then $F(A, N)$ is an R -module under pointwise op.

$$\left\{ \begin{array}{l} \text{if } f, g \in F(A, N) \text{ & } r \in R, \text{ we define} \\ (f+g)(a) = f(a) + g(a), \\ (r \cdot f)(a) = r \cdot (f(a)). \end{array} \right\}$$

only module.
not ring!

In particular, if M is an R -module, then $F(M, N)$ is an R -module under pointwise operation.

Then $\text{Hom}_R(M, N)$ is a submodule of $F(M, N)$.

↳ R-linear functions from M to N
this wasn't said b4!
to be a ring tho!

- Verify:
- ① $D: M \rightarrow N$ is R -linear
 - ② $\varphi_1, \varphi_2: M \rightarrow N$ R -lin $\Rightarrow \varphi_1 + \varphi_2$ is R -linear
 - ③ $a \in R, \varphi: M \rightarrow N$ R -lin $\Rightarrow a\varphi$ is R -linear

Some more observations:

- ① $\text{id}: M \rightarrow M$ is R -linear
- ② If $\varphi: M \rightarrow N$ is an isomorphism (R -linear + bij.), then so is $\varphi^{-1}: N \rightarrow M$. $(\varphi^{-1}(r_{n+m}) = \varphi^{-1}(r\varphi(\varphi^{-1}(n)) + \varphi(\varphi^{-1}(m))) = \varphi^{-1}(\varphi(r\varphi^{-1}(n) + \varphi^{-1}(m))) = r\varphi^{-1}(n) + \varphi^{-1}(m))$
- ③ If $\varphi: M \rightarrow N$ is R -linear, $\psi: L \rightarrow M$ is R -linear; then $\varphi \circ \psi: L \rightarrow N$ is R -linear.

- ① - ③ tell us that "is isomorphic to" is an equivalence relation.
(Using the fact that id is a bij. & so is composition)

We also get $\text{End}_R(M) (= \text{Hom}_R(M, M))$ forms a ring under pointwise addition and composition.

didn't ↴ (Mostly non-comm.)

pointwise addition and composition.
 we didn't talk about ring in general (Mostly non-comm.)
 in general $\text{Hom}(M, N)$

Note: ① M is a module over $\text{End}_R(M)$ with "scalar" multiplication given by $\forall \varphi \in \text{End}_R(M), \forall x \in M, \varphi \cdot x = \varphi(x)$.
 (Verify!)

② Given $a \in R, \forall x \in M (ax \in M)$.

This gives us a function $x \mapsto ax$.

For $a \in R$, define $\mu_a: M \rightarrow M (x \mapsto ax)$ is a function.

Moreover, this is R -linear. That is, $\mu_a \in \text{End}_R(M)$.

Thus, we get a function

$$\mu: R \rightarrow \text{End}_R(M)$$

$$a \mapsto \mu_a$$

Verify that μ is a ring homomorphism. Identify $\ker \mu$.

$$\ker \mu = \{a \in R : \forall x \in M (ax = 0)\} = \text{ann}_R(M) \stackrel{\text{ideal}}{\subset} R.$$

(Annihilator of M)

Q: Is the R -module structure on M the same as the one induced via μ ?

Eg ① Let V, W be vector spaces over \mathbb{k} . Then, what is $\text{Hom}_{\mathbb{k}}(V, W)$?
 Ans: Linear trans. from V to W .

② Let G_1, G_2 be \mathbb{Z} -modules. Then
 $\text{Hom}_{\mathbb{Z}}(G_1, G_2) =$ group homomorphisms $G_1 \rightarrow G_2$.

③ Let V be a $\mathbb{k}[x]$ -module via T .
 If $\varphi \in \text{End}_{\mathbb{k}[x]}(V)$, what can you say about φ ?
 • When will φ be \mathbb{k} -onto?
 • Is φ \mathbb{k} -linear?
 • What will $\ker \varphi$ be?
 • What relation does φ have with T ?

