

## 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  $\Lambda$  be the set of all proper ideals in  $R$ .

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

②  $\Lambda$  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  $\Lambda$ ,

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  $\Lambda$  satisfies the hypothesis of Zorn's Lemma. Thus,  $\Lambda$  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

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

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

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

$$\therefore b \in m.$$

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

$\Updownarrow$  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  $k$ .

$\Rightarrow a^k \in \mathfrak{m}_y \text{ for } \mathfrak{m}_y \text{ max}$

max. ideals are prime

$\Rightarrow a \in \mathfrak{m}_y \text{ for } \mathfrak{m}_y$

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

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  $\varphi$  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  $\varphi$  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  $\varphi$  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  $\varphi$  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  $\varphi$ .

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

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  $I_1, \dots, I_n \subset R$  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  $N(R) \in \Lambda$ .  $\Lambda$  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,  $b \in I \setminus \bigcup_{j=1}^n \mathfrak{p}_j \rightarrow$

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.

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

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

$\nwarrow \searrow$

$\nearrow$  set exclusion

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  $R_A$ .  
( $A \cap R$  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  $\forall a, b \in A : a \cdot b \in A$
- 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  
 $(x_1, a_1) \sim (x_2, a_2) \quad \text{iff} \quad \exists a \in A \text{ s.t. } a(x_1 a_2 - x_2 a_1) = 0.$

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

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

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 ·.

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

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

$$\Rightarrow \frac{x}{a} = \frac{x_1}{1} \cdot \frac{1}{a} \in \left\langle \frac{x_1}{1} : x_1 \in I \right\rangle$$

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.

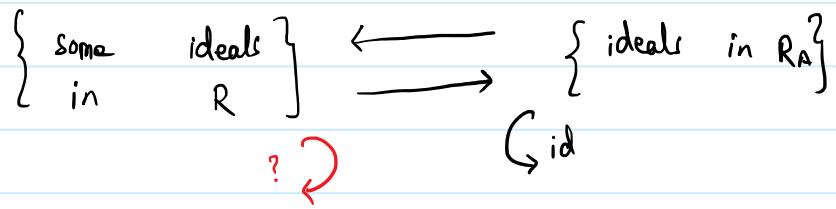
These give us many examples.

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

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



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

b) When is  $I_A = R_A$ ?  $I_A = R_A \Leftrightarrow \frac{1}{1} \in I_A \Leftrightarrow I \cap A \neq \emptyset$   
 $\uparrow$   
 $\exists x \in I, a \in A \text{ s.t. } \frac{1}{1} = \frac{x}{a}$

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  $\varphi_A$ ?

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  $\varphi_A$  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  $\varphi_A$  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,  $\varphi_A$  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  $\varphi_A$ .

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

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

Proof: ( $\rightarrow$ ) Let  $I \in I$  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,  
 $\varphi_A$  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,  
 $\varphi$  is a ring map and  $\varphi(A) \subset \mathcal{V}(S)$ .

Then,  $\varphi$  factors through  $R_A$  via  $\varphi_A$ , <sup>uniquely</sup> 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,  $\tilde{\varphi}\left(\frac{x}{a}\right) = \varphi(x) \cdot [\varphi(a)]^{-1}$ .

<sup>↑</sup> this makes sense since  $\varphi(a) \in \mathcal{V}(S)$

<sup>↑</sup> 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

$(S, \varphi)$  as in ②,  $\varphi$  factors as  $R \xrightarrow{\varphi} S$  <sup>uniquely</sup> via  $\bar{\varphi}: R \rightarrow \bar{R}$ .

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

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

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  $\varphi_1$  &  $\varphi_2$  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  $\varphi_1$  &  $\varphi_2$  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

~~Very~~ Under + with a "scalar multiplication"  $\therefore R \times M \rightarrow M$

(left modules)

Satisfying

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

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

In fact, if  $S$  is an  $R$ -algebra via  $\varphi: R \rightarrow S$ , then  $S$  is an  $R$ -module via  $\varphi$ , 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 :  $R^{\oplus n}$ ,  $M_n(R)$ ,  $R[x]$ ,  $R[[x]]$ ,  $F(A, R)$  ( $A \neq \emptyset$ ).

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

④  $R[[x]]$  : similar

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

Thus, they are all actually  $R$ -algebra

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

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

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.

$$\cdot : \mathbb{Z} \times G \rightarrow G \text{ as}$$

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

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

How should we define  $x \cdot u$ ?

Things we want :  $x \cdot (u+v) = x \cdot u + x \cdot v$   $u, v \in V$   
 $x \cdot (au) = (xa) \cdot u = (ax) \cdot u = a \cdot (xu)$   $a \in \mathbb{k} \hookrightarrow R$

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

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

In general, for  $p \in \mathbb{k}[x]$ ,  $u \in V$ , 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 scalar mult.)

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  $T$ .

Dof. ① Let  $M$  be an  $R$ -module and  $N \subseteq M$ . Then  $N$  is an  $R$ -submodule of  $M$  if

- (a)  $0 \in N$ ,
- (b)  $x, y \in N \Rightarrow x+y \in N$ , and
- (c)  $a \in R, x \in N \Rightarrow ax \in N$ .

(submodule)

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

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

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

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

Given a subset  $S \subseteq M$ ,

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

(cyclic) ③  $M$  is cyclic if  $\exists x \in M$  s.t.  $M = \langle x \rangle$ .

(finitely generated) ④  $M$  is finitely generated if  $\exists n \in \mathbb{N}, \exists x_1, \dots, x_n \in M$  s.t.  $M = \langle x_1, \dots, x_n \rangle$ .

(simple) ⑤  $M \neq 0$  is simple if the only submodules of  $M$  are  $0$  and  $M$ . ( $0$  is not simple.)

(decomposable) 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. (indecomposable)

- Q. What are  $\mathbb{K}$ -submodules of  $V$ ?  $\mathbb{K}[x]$ -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  $\varphi$ )

## 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  $\varphi$ )

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  $\text{non-trivial}$  inv. subspace.  
Hence, cannot be simple!

Def:

- ① Let  $N \subset M$  be an  $R$ -submodule. Then,  $M/N$  is an  $R$ -module with scalar multiplication  
(quotient)  $a \cdot \bar{x} = \overline{ax}$ .

(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  $\forall a \in R \ \forall x, y \in M_1 : \varphi(ax + y) = a\varphi(x) + \varphi(y)$ .

(module homomorphism or  $R$  linear map)

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.  
(not ring)

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).  
put product as composition

(endomorphisms)

Verification of quotient: First we show  $a \cdot \bar{x} = \bar{ax}$  is well defined.

Let  $x, y \in M$  be s.t.  $\bar{x} = \bar{y}$ .

Then,  $x - y \in N$ .

Then,  $a \cdot (x-y) \in N$ . ( $N$  is a sub-module).

$$\Rightarrow a \cdot x - a \cdot y \in N$$

$$\Rightarrow \bar{ax} = \bar{ay}.$$



To show:  $M/N$  so defined is an  $R$ -module.

It is an abelian group ✓

Let  $a, b \in R$  &  $x, y \in M$ . Then,

$$\begin{aligned}(a+b) \cdot \bar{x} &= \overline{(a+b) \cdot x} = \overline{a \cdot x + b \cdot x} \\ &= \overline{a \cdot x} + \overline{b \cdot x} \\ &= a \cdot \bar{x} + b \cdot \bar{x}\end{aligned}$$

$$\text{Similarly, } a \cdot (\bar{x} + \bar{y}) = a \cdot \bar{x} + a \cdot \bar{y}$$

$$a \cdot (b \cdot \bar{x}) = a \cdot (\bar{b \cdot x}) = \overline{a \cdot (b \cdot x)} = \overline{(a \cdot b) \cdot x} = (ab) \cdot \bar{x}$$
$$1 \cdot \bar{x} = \overline{1 \cdot x} = \bar{x}.$$

Since an arbitrary elt. of  $M/N$  can be written as  $\bar{x}$  for some  $x \in M$ , we are done!

---

V/W: Let  $W \subset V$  be v-spaces (not necessarily finite dim.)

Let  $B_1$  be a basis of  $W$ .

Extend it to a basis  $B = B_1 \cup B_2$  of  $V$ .  
(Need choice.)

Then,  $B_2/W$  is a basis of  $V/W$ .

$$\{ v + w : v \in B_1 \}$$

Proof. Lin indep:

Suppose  $a_1, \dots, a_n \in k$  &  $v_1, \dots, v_n \in B_1$

$$\text{are s.t. } a_1 \bar{v}_1 + \dots + a_n \bar{v}_n = 0.$$

$$\Rightarrow a_1 v_1 + \dots + a_n v_n = 0$$

$$\Rightarrow a_1 v_1 + \dots + a_n v_n \in W$$

$$\Rightarrow a_1 v_1 + \dots + a_n v_n = b_1 w_1 + \dots + b_m w_m$$

$$b_i \in F, w_i \in B,$$

But  $\{v_i\} \cup \{w_j\} \subset B$  is lin indep. Thus,

$$a_i = 0 \ \forall i \ \& \ b_j = 0 \ \forall j.$$

.. Lin indep!

Spanning: Let  $v \in V$ , then  $v = \sum a_i v_i + \sum b_j w_j$   
 $\Rightarrow \bar{v} = \sum a_i \bar{v}_i \quad \checkmark$

$$\text{End}_R(M) = \text{Hom}_R(M, M)$$

$$= \{ \varphi : M \rightarrow M \mid \varphi \text{ is } R\text{-linear} \}$$

If  $\varphi, \psi \in \text{End}_R(M)$ , then  $\varphi \circ \psi$  is also  $R$ -linear from  $M \rightarrow M$ .  
 Then,  $\varphi \circ \psi \in \text{End}_R(M)$ .  
product.

This is a ring as well as a module.  
over  $R$

$$\begin{aligned} [\varphi \circ (\psi_1 + \psi_2)](a) &= \varphi [(\psi_1 + \psi_2)(a)] \\ &= \varphi [\psi_1(a) + \psi_2(a)] \\ &= \varphi(\psi_1(a)) + \varphi(\psi_2(a)) \\ &= (\varphi \circ \psi_1)(a) + (\varphi \circ \psi_2)(a) \\ &= [(\varphi \circ \psi_1) + (\varphi \circ \psi_2)](a) \end{aligned}$$

$$\therefore \varphi \circ (\psi_1 + \psi_2) = \varphi \circ \psi_1 + \varphi \circ \psi_2$$

//

$$(\psi_1 + \psi_2) \circ \varphi = \psi_1 \circ \varphi + \psi_2 \circ \varphi.$$

$$id = 1.$$

## 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.

only module  
not ring!

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

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  $F(M, N)$ .

this wasn't said  
to be a ring, btw!

- Verify:
- ①  $0: M \rightarrow N$  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  $\varphi^{-1}: N \rightarrow M$ .  $(\varphi^{-1}(r_n+m) = \varphi^{-1}(r\varphi(\varphi^{-1}(n)) + \varphi(\varphi^{-1}(m))) = \varphi^{-1}(\varphi(r\varphi^{-1}m + \varphi^{-1}n)) = r\varphi^{-1}n + \varphi^{-1}m)$
- 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  $\text{id}$  is a bij. & so is composition)

(endomorphisms)

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

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

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,  $\mu_{a+b} \in \text{End}_R(M)$ .

Thus, we get a function

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

$$a \mapsto \mu_a.$$

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

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

ideal

(Annihilator of  $M$ )

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

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

$\text{Hom}_{\mathbb{Z}}(G_1, G_2) = \text{group homomorphisms } G_1 \rightarrow G_2$ .

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  $\varphi$ ?

• When will  $\varphi$  be 1-1? onto?

• Is  $\varphi$   $\mathbb{k}$ -linear? Yes ✓

• What will  $\ker \varphi$  be?

• What relation does  $\varphi$  have with  $T$ ?  $\varphi \circ T = T \circ \varphi$

$\mu$  is a ring homo.: To show:  $\mu_1 = \text{id}$  ✓ true

$$\mu_{a+b} = \mu_a + \mu_b$$

$$\mu_{ab} = \mu_a \circ \mu_b$$

Let  $x \in M$ .

$$\begin{aligned} \text{Then, } \mu_{a+b}(x) &= (a+b) \cdot x \\ &= a \cdot x + b \cdot x \\ &= \mu_a(x) + \mu_b(x) \\ &= (\mu_a + \mu_b)(x) \end{aligned}$$

Let  $x \in M$ .

$$\begin{aligned} \mu_{ab}(x) &= (ab) \cdot x \\ &= a \cdot (b \cdot x) \\ &= \mu_a(b \cdot x) \\ &= \mu_a(\mu_b(x)) \\ &= ((\mu_a \circ \mu_b)(x)) \end{aligned}$$

## Lecture 22 (12-10)

12 October 2020 09:24 AM

Setup.

$\varphi: M \rightarrow N$  is  $R$ -linear. ( $M$  and  $N$  are  $R$ -linear.)

What is  $\varphi^{-1}(N)$ ?  $M$ .

Suppose  $\langle S \rangle = \varphi(M)$ . For each  $y \in S$ , choose  $x \in \varphi^{-1}(y)$ .

Suppose  $\langle S' \rangle = \ker \varphi$ .

Then,  $\langle \{x: y \in S\} \cup S' \rangle = M$ .

Thus, ① If  $\varphi(M)$  and  $\ker \varphi$  are f.g., then so is  $M$ .

E.g. Let  $\varphi(M) = \langle z_1, \dots, z_n \rangle^{CN}$ ,  $\ker \varphi = \langle x_1, \dots, x_k \rangle^{CM}$ .

Take  $y_1, \dots, y_n \in M$  s.t.  $\varphi(y_i) = z_i$ .

Then,

$$M = \langle x_1, \dots, x_k, y_1, \dots, y_n \rangle.$$

② Suppose  $\langle S \rangle = M$ . Then,  $\varphi(M) = \langle \varphi(S) \rangle$ .

## Lecture 23 (13-10)

13 October 2020 10:34 AM

- ① Let  $\varphi: M \rightarrow N$  be a module homomorphism and  $a \in \text{ann}_R(M)$ . Then,  $a \cdot \varphi = 0$ . ( $(a \cdot \varphi)(m) := a \cdot \varphi(m)$  or  $a\varphi = \mu_a \circ \varphi$ .)  
Proof-  $a \cdot \varphi(x) = a\varphi(x) = \varphi(ax) = \varphi(0) = 0$ .

That is,  $a \in \text{ann}_R(\text{Hom}_R(M, N))$ . In other words

$$\text{ann}_R(M) \subset \text{ann}_R(\text{Hom}_R(M, N)).$$

- Q. What about  $\text{ann}_R(N)$ ? Easy check again that there's containment.  
Therefore,

$$\text{ann}_R M + \text{ann}_R N \subset \text{ann}_R(\text{Hom}_R(M, N)).$$

(Recall that  $\text{ann}_R(-)$  is an ideal.)

- ② If  $M = 0$  module, then  $\text{ann}_R(M) = R$ .  
Conversely, if  $\text{ann}_R(M) = R$ , then  $1 \cdot x = 0 \quad \forall x \in M$ .  
Thus,  $M = 0 \iff \text{ann}_R(M) = R$ .

Def. If  $\text{ann}_R(M) = 0$ , then  $M$  is a faithful  $R$ -module.

(faithful module)

More about  $\text{End}_R(M)$ : ①  $\text{End}_R(R) \stackrel{\text{pos rings}}{\cong} R$ . (think about 1.)

- ①  $\text{End}_R(M) = 0 \iff M = 0$ . ( $x \mapsto 0$  and  $x \mapsto x$  are always two endos.)

- ② What can we say about  $\varphi \in \text{Hom}_R(M, N)$  if  
③  $M$  is simple? Either  $\varphi = 0$  or  $\varphi$  is 1-1.

(b)  $N$  is simple? Either  $\varphi = 0$  or  $\varphi$  is onto.

② Both are simple?  $\varphi = 0$  or bijective.

Thus, if  $M$  is simple, then  $\text{End}_R(M)$  is a division ring.

Q. Is converse true?

(3) Suppose  $M$  is decomposable, i.e.,  $\exists O \neq L, N$  submodules s.t.  
 $M = L \oplus N$ .

Consider the projections  $T_{l_1} : M \rightarrow M$  and  $T_{l_2} : M \rightarrow M$   
 (onto  $l$ ) (onto  $N$ )

$$\ker \pi_1 = N, \quad \text{im } \pi_1 = L \quad ; \quad \ker \pi_2 = L, \quad \text{im } \pi_2 = N.$$

$$\underbrace{\pi_i^2}_{\text{idempotent}} = \pi_i; \quad \& \quad \underbrace{\pi_i \pi_j}_{{(i \neq j)}} = 0 \quad \text{orthogonal}$$

$$id_M = T_1 + T_2.$$

complete

Thus  $M$  is decomposable  $\Rightarrow \text{End}_R(M)$  has a pair of complete orthogonal idempotents

Note:  $\pi_1$  and  $\pi_2$  cannot be 0 or id.

Q. Is the converse true?

Note: If  $a \in R$  is idemp., then so is  $1-a$ .

→ Suppose  $\text{End}_R(M)$  has a non-trivial idempotent  $\pi$ , i.e.,  $0 \neq \pi \neq 1$ , is  $M$  decomposable.

Try: Is  $M = \text{im } \pi \oplus \ker \pi$ ?

Yes!

Proof. Claim!  $\text{im } \pi \cap \ker \pi = 0$ .

Proof - let  $a \in \text{LHS}$ .

Then,  $a = \pi b$  &  $\pi a = 0$ .

$$\Rightarrow \pi^2 b = 0 \quad \text{but} \quad \pi^2 b = \pi b = a. \quad \therefore a = 0.$$

Claim 2.  $\text{im } \pi + \ker \pi = M$ .

Proof. Let  $a \in M$ .

$$a = \underbrace{\pi a}_{\text{im } \pi} + \underbrace{a - \pi a}_{\text{ker } \pi}$$

$$\text{since } \pi(a - \pi a) = \pi a - \pi^2 a = 0.$$

□

Note:  $\ker \pi \neq 0$  since  $x - \pi(x) \in \ker \pi \quad \forall x$

&  $\exists x \text{ s.t. } \pi(x) = x$ . ( $\pi \neq 0$ )

$\text{im } \pi \neq 0$  since  $\pi \neq 0$ .

## Lecture 24 (15-10)

15 October 2020 11:41 AM

Recap:  $M$  is decomposable as  $R$ -module  
 $\Leftrightarrow \text{End}_R(M)$  has a non-trivial idempotent

Thus,  $R$  is decomposable as an  $R$ -module  $\Leftrightarrow R$  has non-trivial idempotents.  
↓  
i.e.  
 $\exists$  non-zero ideals  $I, J \subset R$   
s.t.  $I \oplus J = R$   
thus, comaximal

$\Leftrightarrow \exists R_1, R_2 \neq 0$  s.t.  
 $R \cong R_1 \times R_2$   
(as rings)

- Q.
- ① How are  $I$  &  $J$  related to  $R_1$  and  $R_2$ ?
  - ② If  $R \cong R_1 \times R_2$ , identifying  $R_1$  with  $R_1 \times \{0\}$ , is it an ideal or subring of  $R$ ?

### Other constructions

- ① Let  $M$  be an  $R$ -module,  $I \subset R$  an ideal. Is  $M$  an  $R/I$  module with the "same" structure?  
We would like to define

$$(a + I) \cdot x := a \cdot x.$$

Is this well-defined?

Not in general. Take  $R = M = \mathbb{Z}$  &  $I = 2\mathbb{Z}$ .

Then,  $0 \cdot 1 = 0$  and  $2 \cdot 1 = 2 \neq 0$  but  $0 + I = 2 + I$ .

In fact:

The induced multiplication is well-defined iff  $I \subset \text{ann}_R(M)$ .  
(and makes it a module)

In particular,  $M/IM$  is always an  $R/I$ -module.  
(Verify that  $I \subset \text{ann}_R(M/IM)$ )

Also note: if  $I \subset \text{ann}_R(M)$ , then  $IM = 0$  & thus,  $M/IM = M/0 \cong M$ .

Thus, if  $\mathfrak{m} \in \text{Max}(R)$ , then  $M/\mathfrak{m}M$  is a vector space over  $R/\mathfrak{m}$ .

(And we know vector spaces.)

↳ will be useful in local rings (Nakayama Lemma)

A different perspective:

We had the blue maps. Did there exist a red map making it commute?

$$\begin{array}{ccc} R \times M & & \\ \downarrow \varphi \times \text{id}_M & \searrow & \\ R/I \times M & \dashrightarrow & M \end{array}$$

- ② Let  $A \subset R$  be an m.c.s.,  $M$  an  $R$ -module. Is  $M$  an  $R_A$ -module under the "same" structure?

Same as earlier:

$$\begin{array}{ccc} R \times M & & \\ \downarrow \varphi_A \times \text{id}_M & \searrow & \\ R_A \times M & \dashrightarrow & M \end{array}$$

General question:  $R \xrightarrow{\varphi} S$  ring map,  $M$  an  $R$ -module.  
Can we make  $M$  an  $S$ -module via  $\varphi$ ?

## Lecture 25 (26-10)

26 October 2020 09:14 AM

$M$  is a  $R$ -module,  $I \subset R$  an ideal,  $A \subset R$  a m.c.s.

- $M$  is  $R/I$ -module  $\Leftrightarrow I \subset \text{ann}_R(M)$   
 $\Leftrightarrow \forall a \in I, \mu_a = 0$
- $M$  is  $RA$ -module  $\Leftrightarrow \forall a \in A, \mu_a$  is an isomorphism  
(Verify!)

(Recall:  $\mu_a : M \rightarrow M$  was  $x \mapsto a \cdot x$ .)  
(↳ This was an  $R$ -linear map)

Note: When  $M$  was not an  $R/I$ -module, we had  $M/IM$  which was.  
 We now do a similar thing for  $M$  and  $RA$ .

Making  $M$  into an  $R_A$  module (localisation of a module):

Define a relation  $\sim$  on  $M \times A$  as

$$(x, a) \sim (y, b) \quad \text{iff} \\ \exists c \in A \text{ s.t. } c(bx - ay) = 0.$$

$\sim$  is then an equiv. reln. Define  $\frac{x}{a} := [(x, a)]$ .

Then,  $M_A := \left\{ \frac{x}{a} : (x, a) \in M \times A \right\}$  is a  $R$ -module

with addition and scalar multiplication defined as:

$$\frac{x}{a} + \frac{x'}{a'} = \frac{ax' + ax'}{aa'}, \quad c \cdot \left(\frac{x}{a}\right) = \frac{cx}{a}.$$

We then see that this extends to an  $R_A$  module in the obvious way.

$$\begin{array}{ccc} R \times M_A & \xrightarrow{\quad} & M_A \\ \downarrow & & \nearrow \\ R_A \times M_A & & \end{array}$$

We have an  $R$ -linear map

$$\varphi_A : M \longrightarrow M_A \quad \text{given as} \\ x \mapsto \frac{x}{1}.$$

$$\text{Then, } \ker \varphi_A = \{x \in M \mid \exists a \in A \ (ax = 0)\} = \bigcup_{a \in A} \ker \mu_a.$$

$$\text{Let } Z_R(M) := \{a \in R \mid \exists x \in M \setminus \{0\} \ (ax = 0)\}.$$

$$\varphi_A \text{ is injective} \Leftrightarrow Z_R(M) \cap A = \emptyset$$

$$\boxed{M_A = 0 \Leftrightarrow \forall x \in M, \exists a \in A \ (ax = 0)}$$

Suppose  $M$  is f.g. Write  $M = \langle x_1, \dots, x_n \rangle$

$$M_A = 0 \Leftrightarrow \forall i \in \{1, \dots, n\}, \exists a_i \in A \ (a_i x_i = 0)$$

$\Leftrightarrow$  obvious

$\Leftrightarrow$  Take  $a = a_1 \dots a_n \in A$ .

Let  $x \in M$ . Then,  $x = r_1 x_1 + \dots + r_n x_n$ ;  $r_i \in R$ .  
Then,  $a x = 0$ .

$$\Leftrightarrow \exists a \in A, \forall x \in M \ (ax = 0)$$

$$\Leftrightarrow \text{ann}_R(M) \cap A \neq \emptyset$$

For finite gen.,  $\Rightarrow$  is not true. That is,

$$M_A = 0 \not\Rightarrow \text{ann}_R(M) \cap A = \emptyset$$

Observation:  $M = 0 \Leftrightarrow \forall A \subset R \text{ m.c.s.}, M_A = 0$

$\Leftrightarrow A \text{ is a proper } M_{\text{fin}} \text{ with } M_{\text{fin}} = 0$

$$\begin{array}{l} \Leftrightarrow \forall p \in \text{Spec}(R), M_p = 0 \\ \Leftrightarrow \exists m \in \text{Max}(R), M_m = 0 \end{array} \quad (\text{M}_A \text{ with } A = R \setminus p)$$

$(\Rightarrow)$ s are trivial. Really have to show:

$$\forall m \in \text{Max}(R), M_m = 0 \Rightarrow M = 0. \quad \begin{array}{l} \text{Local-Global} \\ \text{principle} \end{array}$$

(Local-Global principle)

Proof. We show:  $M \neq 0 \Rightarrow \exists m \in \text{Max}(R) \text{ s.t. } M_m \neq 0.$

Recall:  $M_m = 0 \Leftrightarrow \forall x \in M, \exists a \notin m (a \cdot x = 0)$

Since,  $M \neq 0, \exists x \in M, x \neq 0$

Consider the ideal  $I = \text{ann}_R(x).$

$$x \neq 0 \Rightarrow I \neq I \Rightarrow I \subsetneq M.$$

Thus,  $\exists m \in \text{Max}(R) \text{ s.t. } I \subset m.$

$$\text{ann}_R^{(m)}$$

Put  $A := R \setminus m.$  Then,  $\frac{x}{1} \in M_A$  is not zero. True

$$\left( \begin{array}{l} \text{Prof. } \frac{x}{1} \Rightarrow a \cdot x = 0 \text{ for some } a \in A = R \setminus m \\ \Rightarrow \text{ann}_R(x) \cap (R \setminus m) \neq \emptyset \\ \Rightarrow \text{ann}_R(x) \not\subset m \end{array} \right)$$

$R_A$ -submodules of  $M_A:$  Given  $N \subseteq M,$   $N_A$  is an  $R_A$ -module.  
Then,  $N_A \subseteq M_A$  as a submodule and  
 $N_A = \langle \varphi_A(x) : x \in N \rangle.$

Further more,

$$(M/N)_A \cong M_A/N_A$$

## Lecture 26 (27-10)

27 October 2020 10:20 AM

Given an  $R$  module  $M$  and submodules  $N, L$ , we have

$$\begin{array}{c} L+N \\ / \quad \backslash \\ L \qquad N \\ \backslash \quad / \\ LN \end{array} \quad \frac{L+N}{L} \cong \frac{N}{LN}$$

$L+N$  is the smallest submodule containing  $L$  and  $N$ .

$LN$  is the largest submodule contained in  $L$  and  $N$ .

We have :  $L \hookrightarrow L+N \xrightarrow{\frac{L+N}{N}}$  as a map from  $L$  to  $\frac{L+N}{N}$ .

If it is surjective with kernel  $LN$ , we are done.

If  $L$  and  $N$  are f.g., then so is  $L+N$ .

$$L = \langle l_1, \dots, l_m \rangle, \quad N = \langle n_1, \dots, n_k \rangle \Rightarrow L+N = \langle l_1, \dots, l_m, n_1, \dots, n_k \rangle$$

Remarks:

(Notation:  $N \leq M$  means submodule.)

① Let  $M$  be f.g.,  $N \leq M$ . Then  $M/N$  is f.g. but  $N$  need not be.

(If  $M = \langle x_1, \dots, x_n \rangle$ , then  $M/N = \langle \bar{x}_1, \dots, \bar{x}_n \rangle$ .)

② In general:

Let  $M$  be f.g.,  $\varphi: M \rightarrow M'$  be  $R$ -linear. Then,  $\varphi(M')$  is f.g.

(If  $M = \langle x_1, \dots, x_n \rangle$ , then  $\varphi(M) = \langle \varphi(x_1), \dots, \varphi(x_n) \rangle$ )

However,  $\ker \varphi$  need not be so.

③ Let  $N \leq M$ . If  $N$  and  $M/N$  are f.g., then so is  $M$ .

(If  $N = \langle n_1, \dots, n_k \rangle$ ,  $M/N = \langle \bar{x}_1, \dots, \bar{x}_m \rangle$ , then  
 $M = \langle n_1, \dots, n_k, x_1, \dots, x_m \rangle$ )

④ Let  $\varphi: M \rightarrow M'$  be  $R$ -linear. If  $\varphi(M)$  and  $\ker \varphi$  are f.g., so is  $M$ .

⑤ Let  $M$  be f.g.,  $A \subset R$  m.c.s. Then  $M_A$  is f.g. as an  $R_A$  module but not necessarily as an  $R$  module.

If  $M = R\langle x_1, \dots, x_n \rangle$ , then  $M_A = R_A\langle \frac{x_1}{1}, \dots, \frac{x_n}{1} \rangle$ .

⑥ Can you give a gen. set of  $M_A$  as an  $R_A$ -module?  
 (other than  $M_A$  itself.)

$$M_A = R_A \left\langle \frac{x}{1} : x \in M \right\rangle.$$

⑦ (Determinant trick)

Suppose  $M$  is f.g.,  $I \subset R$  an ideal and  $IM = M$ .

Write  $M = \langle x_1, \dots, x_n \rangle$ . Then,

$$x_1 = a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n$$

$$\begin{aligned} x_2 &= a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n \\ &\vdots \end{aligned} \quad \text{for } a_{ij} \in I$$

$$x_n = a_{n1}x_1 + \dots + a_{nn}x_n$$

$$\therefore \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = A \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}, \quad \text{where } A = [a_{ij}]$$

Draw conclusion! Get something that annihilates  $M$ .

Put  $B = A - I$  and  $x = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$ .  
Then,  $Bx = 0_{n \times 1}$   
 $\Rightarrow (\text{adj } B)Bx = 0$

$$\Rightarrow (\det B)x = 0$$
$$\Rightarrow (\det B)x_i = 0 \quad \forall i$$
$$\Rightarrow \det B \in \text{ann}_R(M)$$

## Lecture 27 (29-10)

29 October 2020 11:34 AM

Same notation from earlier:

$$I - A = \begin{bmatrix} 1-a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & 1-a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & 1-a_{nn} \end{bmatrix}$$

$$\Rightarrow \det(I - A) = 1 + a, \quad a \in I.$$

Thus,  $\exists a \in I$  s.t.  $1+a \in \text{ann}_R(M)$ .

(This was assuming:  $M$  is f.g.,  $IM = M$ )

Special Cases: (Assuming  $M$  is f.g. &  $IM = M$ )

1. If we know  $\text{ann}_R(M) = 0$  (i.e.,  $M$  is faithful), then  $I = R$ .  
(since  $1+a = 0 \Leftrightarrow a = -1 \Leftrightarrow I = R$ )

Thus, if  $M$  is faithful, then  $IM = M \Leftrightarrow I = R$ .

2. If  $I \subset J(R)$ , then  $1+a \in \mathcal{V}(R)$ , then  $M = 0$ . (Nakayama Lemma)  
(NAK)

NAK: Let  $M$  be f.g.,  $IM = M$ . If  $I \subset J(R)$ , then  $M = 0$ .

3. If  $(R, \mathfrak{m})$  is local,  $M$  f.g.,  $IM = M$  for a proper ideal  $I \subsetneq R$ , then  $M = 0$ .  
(If  $a \in I$ , then  $1+a \notin \mathfrak{m}$ , then  $1+a \notin \text{any ideal}$ , then  $1+a \in \mathcal{V}(R)$ .)

(Recall Global-Local which said that if  $M_{\mathfrak{m}} = 0 \forall \mathfrak{m} \in \text{Max}(R)$ , then  $n = 0$ .  $R$  then is local.)

4. Let  $M$  be f.g. and  $M/IM = 0$ . If  $I \subset J(R)$ , then  $M = 0$

$$(M/IM = 0 \Leftrightarrow M = IM \text{ and use NAK 2.)}$$

5. Let  $N \subset M$  be a submodule s.t.  $N + IM = M$ .

Assume  $M$  is f.g.,  $I \subset J(R)$ . ( $IM = M$  not assumed.)

Then  $M = N$ .

Proof. We show, by (2), that  $M/N = 0$ .

First, note that  $M/N$  is f.g. since  $M$  is.

Want to show:  $\frac{M}{N} = I(M/N)$ , then we are done by 2.

Proof. (2) Duh.

$$(2) \text{ Let } \bar{x} \in M/N. \quad x = n + (i_1 m_1 + \dots + i_k m_k) \quad (\because M = N + IM) \\ \bar{x} = i_1 \bar{m}_1 + \dots + i_k \bar{m}_k \in I(M/N).$$

Obs. Suppose  $M = \langle x_1, \dots, x_n \rangle$ ,  $I \subset R$  is an ideal.

Then  $M/IM = \langle \bar{x}_1, \dots, \bar{x}_n \rangle$ .

Q Is converse true? That is,

if  $x_1, \dots, x_n \in M$  are s.t.  $M/IM = \langle \bar{x}_1, \dots, \bar{x}_n \rangle$ , is it necessary that  $M = \langle x_1, \dots, x_n \rangle$ ?

(No! Counter example?)

Note:  $M/IM = \langle x_1 + IM, \dots, x_n + IM \rangle$  (in  $M/IM$ )

$$\Rightarrow M = IM + \langle x_1, \dots, x_n \rangle \quad (\text{in } M)$$

6. Thus: If  $M$  is f.g.,  $I \subset J(R)$  and  $\exists x_1, \dots, x_n \in M$  s.t.

$$M/\mathfrak{m}M = \langle \bar{x}_1, \dots, \bar{x}_n \rangle,$$

$$\text{then } M = \langle x_1, \dots, x_n \rangle.$$

(This is by ⑤.  $N = \langle x_1, \dots, x_n \rangle$  with the above obs.)

7. Let  $(R, \mathfrak{m})$  be local and  $M$  f.g.; then for  
 $x_1, \dots, x_n \in M$  we have

$$M = \langle x_1, \dots, x_n \rangle \Leftrightarrow \underbrace{M/\mathfrak{m}M}_{\downarrow} = \langle x_1 + \mathfrak{m}M, \dots, x_n + \mathfrak{m}M \rangle.$$

This is a vector space over  $R/\mathfrak{m}$ !

Can talk about bases!!

Ex) ①  $x_1, \dots, x_n$  is a minimal (in terms of inclusion) generating set of  $M \Leftrightarrow \{\bar{x}_1, \dots, \bar{x}_n\}$  is a basis of  $M/\mathfrak{m}M$ .

② Every minimal gen. set of  $M$  has the same no. of elements, namely  $\dim_{R/\mathfrak{m}}(M/\mathfrak{m}M)$ .

## Lecture 28 (02-10)

02 November 2020 09:33 AM

Note: Linear independence defined in the usual way. (No non-trivial relations.)  
Basis  $\rightarrow$  lin indep + generating

Def. (free module) An  $R$ -module which admits a basis is called a free  $R$ -module.

(relation) If  $x_1, \dots, x_n \in M$ , an  $n$ -tuple  $(a_1, \dots, a_n) \in R^{\oplus n}$  s.t.  $a_1 x_1 + \dots + a_n x_n = 0$  is called a relation on  $x_1, \dots, x_n$ .

Remark:  $(0, \dots, 0)$  is always a relation. Other relations are called non-trivial relation.

Eg. If  $a, b \in R$ , then  $(-b, a)$  is a relation on  $a, b$ .

Note. Fix  $x_1, \dots, x_n$ . Then, the set of relations on  $(x_1, \dots, x_n)$  forms a submodule of  $R^{\oplus n}$ .

What's the next best thing to hope for?

"Def."  $(a, b)$  is "special" if the set of relation on  $a, b$  is generated by  $(-b, a)$  in  $R^{\oplus 2}$ .

Q. If  $a_1, \dots, a_n \in R$ , when would you call them special?

### (Non-) Examples of Free Modules

①  $R^{\oplus n}$  is a free  $R$ -module with basis  $\{e_1, \dots, e_n\}$ .  
 $(e_i = (0, \dots, \underset{i^{\text{th}} \text{ place}}{1}, \dots, 0))$

Note, if  $n = 1$ , then  $R$  is a free  $R$ -module with basis  $\{1\}$ .  
 (thus, each ring is a free module over itself.)  
 $0$  is free with empty basis.

②  $R[x]$  admits a basis  $\{1, x, x^2, \dots\}$ .

③  $M_n(R)$  has basis  $\{E_{ij} \mid 1 \leq i, j \leq n\}$ .

In general,  $M_{n \times m}(R)$  works.

④ An ideal which is not principal is not free.

(Any two elements in a ring are indep.)

⑤ If  $0 \neq I \subsetneq R$ , then  $R/I$  is not free.  
 (as an  $R$ -mod)

Note:  $R/I$  is free as an  $R/I$ -module!

⑥ Converse of ④ : If an ideal is not free, then it is not principal.

That is : Principal  $\Rightarrow$  Free ?

No. Take  $\{\bar{0}, \bar{2}\}$  in  $\mathbb{Z}/4\mathbb{Z}$ .

## The Invariant Basis Number (IBN) Property

(Invariant Basis Number (IBN))

A ring  $R$  is said to have the IBN property if the following holds:

Given two bases  $B_1$  and  $B_2$  of a free  $R$ -module  $M$ ,  $B_1$  and  $B_2$  have the same cardinality.  
 (card. depends on  $M$ .)

E.g.  
Ex. Any field.

Find a ring which does not have IBN.

Remark: Every commutative ring has the IBN property.

Def<sup>n</sup>. (Rank) Let  $R$  be commutative,  $M$  is a free  $R$ -module.

Then  $\text{rank}_R(M)$  is the cardinality of any basis of  $M$ .

In this course:  $\text{rank}_R(M) = \begin{cases} \text{no. of elements if finite basis} \\ \infty ; \text{ otherwise} \end{cases}$

(Assuming choice, of c)

## Lecture 29 (03-11)

03 November 2020 10:31 AM

Prop: Let  $M$  be a free  $R$ -module,  $I \subsetneq R$  an ideal.  
Then,  $M/IM$  is a free  $R/I$ -module.

In fact, ① if  $B$  is an  $R$ -basis of  $M$ , then

$$\bar{B} = \{x + IM : x \in B\}$$

is an  $R/I$ -basis of  $M/IM$ .

②  $|B| = |\bar{B}|$ . *(This is what required)  
 $I \subsetneq R$ .*

Proof. ① Generating

Since  $M = \langle B \rangle$ , we see that  $M/IM = \langle \bar{B} \rangle$  as an  $R$ -mod  
and hence, as an  $R/I$ -module.

Linear independence (be distinct)

Let  $\bar{x}_1, \dots, \bar{x}_n \in \bar{B}$  and  $(\bar{a}_1, \dots, \bar{a}_n) \in (R/I)^{\oplus n}$  be s.t.

$$\bar{a}_1 \bar{x}_1 + \dots + \bar{a}_n \bar{x}_n = 0 \quad (\text{in } M/IM \text{ as } R/I\text{-mod})$$

$$\Rightarrow a_1 x_1 + \dots + a_n x_n \in IM \quad (\text{in } M \text{ as } R\text{-mod})$$

Thus, there exist  $b_1, \dots, b_m \in I$ ,  $y_1, \dots, y_m \in B$  s.t.

$$a_1 x_1 + \dots + a_n x_n = b_1 y_1 + \dots + b_m y_m$$

Since  $B$  is a basis and both sides above represent the same element. Thus,  $m=n$ , and

$$\{x_1, \dots, x_n\} = \{y_1, \dots, y_n\} \text{ with}$$

$$\{a_1, \dots, a_n\} = \{b_1, \dots, b_n\}. \text{ Thus,}$$

each  $a_i \in I$  and  $\bar{a}_i = 0$  in  $R/I$ .

*(Not technically correct, we could have  $m \neq n$  if there are some  $b_i = 0$  or  $a_i = 0$ .)*

② We need to show that  $x \neq y \Rightarrow \bar{x} \neq \bar{y}$ .

(for  $x, y \in B$ )

Consider  $\pi: M \rightarrow M/IM$ .

Then,  $\bar{B} = \pi(B)$ .

We need to show that  $\pi|_B$  is 1-1. Then,

$$|B| = |\bar{B}|.$$

$(\pi|_B: B \rightarrow \bar{B} \text{ is onto by defn.})$

Suppose  $x \neq y$  and  $\bar{x} = \bar{y}$ . Then,

$$x - y \in IM$$

$$\Rightarrow x - y = b_1 z_1 + \dots + b_n z_n \quad \begin{matrix} b_i \in I \\ z_i \in B, \text{ distinct} \end{matrix}$$

$$z_i = x, z_j = y, b_i = 1, b_j = -1 \text{ for } 1 \leq i \neq j \leq n$$

$$\Rightarrow 1 \in I.$$

Thus,  $I = R$ . A contradiction!

---

Using the above, we prove the IBN property of comm. rings.

Proof: Let  $R \neq 0$  be a commutative ring.

Thus,  $\text{Max}(R) \neq \emptyset$ . Pick  $\mathfrak{m} \in \text{Max}(R)$ .

Then,  $\mathfrak{m} \subsetneq R$ .

Now, let  $M$  be a free-module over  $R$ .

Let  $B_1, B_2$  be bases for  $M$ .

Then,  $\bar{B}_1, \bar{B}_2$  are  $R/\mathfrak{m}$ -bases for  $M/\mathfrak{m}M$ .

Since  $\mathfrak{m}$  is maximal,  $R/\mathfrak{m}$  is a field and thus

$|\bar{B}_1| = |\bar{B}_2|$ . By the earlier note,  $|B_1| = |B_2|$ .

If  $R=0$ , then  $M=0$  and the only basis is  $\emptyset$ .  $\square$

---

## Universal property of free $R$ modules

Let  $R$  be a ring.

Defn. Let  $A$  be a non-empty set. A free module on the set  $A$

is a pair  $(F(A), e: A \rightarrow F(A))$  where  $F(A)$  is an  $R$ -mod.

$e$  is a function satisfying the following UMP:

Given a pair  $(M, f: A \rightarrow M)$  where  $M$  is an  $R$ -mod and  $f$  a function, there is a unique  $R$ -linear map  $\tilde{f}: F(A) \rightarrow M$  s.t. the following diagram commutes

$$\begin{array}{ccc} & e \nearrow & \\ A & & F(A) \\ & f \searrow & \downarrow \tilde{f} \\ & & M \end{array}$$

Thm. A free  $R$ -module on the set  $A$  exists and is unique up to isomorphism.

## Lecture 30 (03-11)

05 November 2020 11:20 AM

Free module on set  $A$ :

Uniqueness: A free module on the set  $A$ , if it exists, is unique up to isomorphism.

Suppose  $(F, e)$  and  $(F', e')$  are free modules on set  $A$ .

Since  $(F, e)$  is a universal object,  $\exists$  R-linear map

$$\varphi: F \rightarrow F' \text{ s.t.}$$

$$\begin{array}{ccc} & \overset{e}{\nearrow} & F \\ A & \underset{e'}{\searrow} & \downarrow \varphi \\ & \overset{e'}{\nearrow} & F' \end{array} \quad \text{commutes.}$$

Similarly,  $\exists$  R-lin.  $\psi: F' \rightarrow F$  s.t.

$$\begin{array}{ccc} & \overset{e'}{\nearrow} & F' \\ A & \underset{e}{\searrow} & \downarrow \psi \\ & \overset{e}{\nearrow} & F \end{array}$$

Thus,

$$\begin{array}{ccc} & \overset{e}{\nearrow} & F \\ A & \underset{e'}{\searrow} & \downarrow \psi \circ \varphi \\ & \overset{e'}{\nearrow} & F \end{array} \quad \text{but} \quad \begin{array}{ccc} & \overset{e}{\nearrow} & F \\ A & \underset{e}{\searrow} & \downarrow \text{id}_F \\ & \overset{e}{\nearrow} & F \end{array}$$

Thus, uniqueness forces  $\psi \circ \varphi = \text{id}_F$ .

Similarly,  $\varphi \circ \psi = \text{id}_{F'}$ .

Thus,  $\varphi$  and  $\psi$  are isomorphisms!  $\square$

Existence! (<sup>Idea:</sup> Construct a free R-module with basis  $A$ )

Given  $A$ , and  $a \in A$ , consider the function

$e_a: A \rightarrow R$  defined as

$$e_a(b) = \begin{cases} 1 & ; b = a, \\ 0 & ; b \neq a. \end{cases}$$

Consider the submodule of  $F(A, R)$  generated by  $\{e_a \mid a \in A\}$ .

This is precisely the set of functions in  $F(A, R)$

which take all but finitely many points of  $A$  to 0.

Denote this by  $F_0(A, R)$ .

(Ex. verify that

$$\langle ea \mid a \in A \rangle = F_0(A, R) \text{ is actually true.)}$$

[Note that the above doesn't say anything about the finite set taking non-zero values.]

In particular,  $F_0(A, R)$  is a submodule of  $F(A, R)$ .

Verify that  $\{ea \mid a \in A\}$  is linearly independent.

Thus,  $\{ea\}$  is a basis for  $F_0(A, R)$ . (Generating by construction.)

Define  $e: A \hookrightarrow F_0(A, R)$  as  $a \mapsto ea$ .

(Note  $e$  is 1-1.)

Thus, we may identify  $a \in A$  with  $ea \in F_0(A, R)$ .

What remains:

$(F_0(A, R), e)$  satisfies the UMP.

(Ex!  
Writing as.  
'ere Saturday!

# Lecture 31 (07-11)

07 November 2020 09:34 AM

We have existence and uniqueness of free R-modules over a set A. We call it  $F(A)$ .

Ex. If A and B are in bijection, then  $F(A) \cong F(B)$  as R-modules.

$$\begin{array}{ccc} A & \xrightarrow{e_1} & F(A) \\ f \uparrow \downarrow f^{-1} & \psi \uparrow \downarrow \psi & \text{id}_{F(A)} \uparrow \downarrow \text{id}_{F(A)} \\ B & \xrightarrow{e_2} & F(B) \end{array}$$

$$\begin{array}{ccc} A & \xrightarrow{e_1} & F(A) \\ f \downarrow & \Rightarrow & \downarrow \psi \\ B & \xrightarrow{e_2} & F(B) \\ f^{-1} \downarrow & \Rightarrow & \downarrow \psi \\ A & \xrightarrow{e_1} & F(A) \end{array} \quad \begin{array}{ccc} A & \xrightarrow{e_1} & F(A) \\ \text{id}_A \downarrow & \Rightarrow & \downarrow \psi \circ \varphi \\ A & \xrightarrow{e_1} & F(A) \end{array}$$

Is the converse true? Yes!

Observation: Let  $M \neq 0$  be a free R-module.

Then,  $M \cong F(A)$  for some A.

(Which A? Pick your favourite basis.)

Two ways: ① Let  $i: A \hookrightarrow M$  be incl. Then, we get a  $\xrightarrow{\text{R-lin.}}$  map  
 $i$  as:  $A \xrightarrow{e} F(A) \xrightarrow{\cong} M$  using UMP of  $F(A)$ .

Show  $\cong$  is a bij.

② Show that  $(M, i)$  satisfies the universal property of a free R-module on A.

Note: ① Suppose  $M$  is a cyclic  $R$ -module, i.e.,  $\exists x \in M$  s.t.  
 $M = \langle x \rangle$ .

We get a map  $\varphi: R \rightarrow M$  by extending  
 $1 \mapsto x$ .

(Extension possible because  $\{1\}$  is a basis.)

Moreover, it is onto, since  $M = \langle x \rangle$  and  $r \mapsto rx$ .

$$\ker \varphi = \text{ann}_R(x).$$

Thus,  $M \cong R/\text{ann}_R(x)$ .  $\leftarrow$  Thus,  $M$  is a quotient of  $R$ .

Thus, every cyclic module is iso. to some  $R/I$  for  $I \subset R$  a submodule. Converse is clearly true.

The size of  $\text{ann}$  tell how far from being free.

Aside: Let  $M = \langle x \rangle$ ,  $N$  an  $R$ -module,  $y \in N$ .

Does "  $x \mapsto y$  and extend linearly" (always) make sense?

No.  $\text{ann}_R(x) \subset \text{ann}_R(y)$  should be true.

② Suppose  $M = \langle x, y \rangle$ .

As earlier, we get an onto  $R$ -linear map

$$\begin{aligned} \varphi: R^2 &\rightarrow M \quad \text{by sending} \\ e_1 &\mapsto x \\ e_2 &\mapsto y \end{aligned}$$

[Since  $\{e_1, e_2\}$  is a basis, the extension exists and is unique.]

$$\begin{aligned} \ker \varphi &= \{(a, b) \in R^{(2)} : ax + by = 0\} \\ &= \text{relations on } (x, y). \end{aligned}$$

$$\text{Thus, } M \cong R^{(2)}/\ker \varphi.$$

③ If  $M = \langle x_1, \dots, x_n \rangle$ , then  $M \cong R^{(n)}/I$  for some submodule  $I \subset R^{(n)}$ .

$\hookrightarrow$  all  $\dots$   $\rightsquigarrow$  note:  $R^{(n)}$  is free!

submodule  $I \subset R^{\oplus n}$

↳ all relations on  $(x_1, \dots, x_n)$

note:  $R^{\oplus n}$  is free!

⑩ General case: Let  $M$  be an  $R$ -module.

Then,  $\exists$  a free  $R$ -module  $F$  and an onto  $R$ -linear map  $\varphi: F \rightarrow M$ . In particular,  $M$  is a quotient of  $F$ .

Pf.  $F = F(M)$  will work. (Consider  $M$  as a set)  
 $\langle e_n \mid n \in M \rangle$

$\varphi: F(M) \rightarrow M$  as  $e_n \mapsto x$  works.

Observation: If  $M = \langle S \rangle$  for some  $S \subseteq M$ , one can take  $F = F(S)$ .

Conclusion: Every module can be written as a quotient of a free-module.

E.g. Let  $R = \mathbb{Z}$ ,  $M = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ .

Then,  $M = \langle (\bar{1}, \bar{0}), (\bar{0}, \bar{1}) \rangle$

[an onto map  $\mathbb{Z}^{\oplus 2} \rightarrow M$ . What is  $\ker \varphi$ ?  
 $e_1 \mapsto x$   
 $e_2 \mapsto y$

$$\begin{aligned}\ker(\varphi) &= \{(a, b) \in \mathbb{Z}^{\oplus 2} : ax + by = 0\} \\ &= \{(a, b) \in \mathbb{Z}^{\oplus 2} : a \in 2\mathbb{Z}, b \in 3\mathbb{Z}\} \\ &= 2\mathbb{Z} \times 3\mathbb{Z} \\ &= \langle (2, 0), (0, 3) \rangle\end{aligned}$$

Consider  $\mathbb{Z}^{\oplus 2}$  with kernel  $\{f_1, f_2\}$  and consider

$$\begin{array}{rcl}\psi: \mathbb{Z}^{\oplus 2} &\rightarrow &\ker \varphi \\ f_1 &\mapsto &u \\ f_2 &\mapsto &v\end{array}$$

$\psi$  is onto with  $\ker \psi = \{(a, b) \in \mathbb{Z}^{\oplus 2} : a(2, 0) + b(0, 3) = 0\}$   
in  $\mathbb{Z}^{\oplus 2}$

$$= 0$$

Thus,  $\ker \psi$  is free

Thus,  $M \cong \mathbb{Z}^{\oplus 2}$  both free!  
 $\ker \psi$

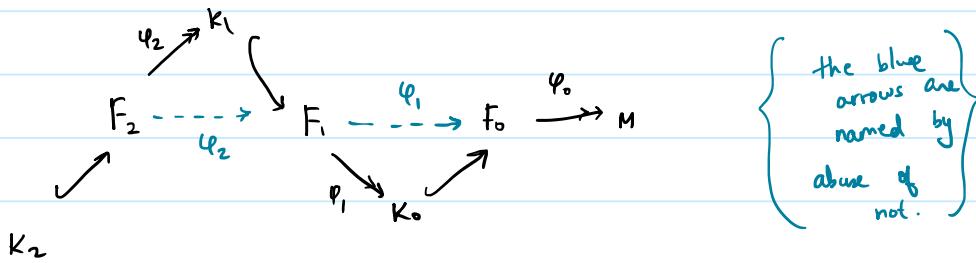
More general:

Let  $M$  be an  $R$ -module. Then  $\exists$  free  $R$ -mod.  $F_0$  mapping onto  $M$  (via  $\varphi_0$ ). Let  $K_0 = \ker(\varphi_0)$ .

( " set of relations on a suitable  
gen. set of  $M$  )

Note that  $K_0$  is again an  $R$ -module.

Let  $F_1$  be a free  $R$ -mod. mapping onto  $K_0$  via  $\varphi_1$ ,  
with  $\ker(\varphi_1) = k_1$ .



Thus, we get a sequence of free  $R$ -modules  
and  $R$ -linear maps

$$M \leftarrow F_0 \leftarrow F_1 \leftarrow F_2 \leftarrow \dots \quad \text{where}$$

$\varphi_0$  is onto and  $\forall i \geq 1, \text{im}(\varphi_i) = \ker(\varphi_{i-1})$ .

The above is called a free resolution of  $M$  over  $R$ .

Q: Does this process stop? ← bad question, we could choose

$F_i$  very big

Q: Can we choose  $F_0, F_1, \dots$  such that the process stops?

In this case,  $M$  has a finite free resolution over  $R$ .

- Note
- ① If  $M$  is f.g., we may choose  $F_i$  to be of finite rank.
  - ②  $K_0$  may not be f.g. even if  $F_0$  has finite rank.

Def. If  $M$  is f.g.,  $F_0 \xrightarrow{\varphi_0} M$ , where  $F_0$  is a free  $R$ -module with finite rank and  $K_0 = \ker(\varphi_0)$  is f.g., then we say that  $M$  is finitely presented.

Remark. Suppose  $M$  is f.g. Then  $\exists$  free  $R$ -modules of finite rank  $F_0$  and  $F_1$  with maps

$$\varphi_1: F_1 \rightarrow F_0, \quad \varphi_0: F_0 \rightarrow M \quad \text{s.t.}$$

$\varphi_0$  is onto and  $\text{im}(\varphi_1) = \ker(\varphi_0)$ .

This can be written as  $F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M$ .

Fix an ord. basis  $(u_1, \dots, u_n)$  of  $F_0$  and an ordered basis  $(v_1, \dots, v_m)$  of  $F_1$ . Then  $\varphi_1$  can be written as a matrix in  $M_{n \times m}(R)$ .

↳ called a presentation matrix of  $M$

Ex. ① Find "the" pres. matrix of  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$  over  $\mathbb{Z}$  as in the example.

② Note that  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$ .

⑤ Note that  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$ .  
find a diff  
pres. matrix

⑥ If  $(v_1, \dots, v_m)$  is a basis of  $F_1$ , so are

$$(v_2, v_1, \dots, v_m), \quad (v_1 + v_2, v_2, \dots, v_m),$$

$$(cv_1, v_2, \dots, v_m) \quad \text{where } c \in V(R).$$

How does the matrix change with these changes?

Do the same with  $F_0$ .

## Lecture 32 (09-11)

09 November 2020 09:25 AM

Unfinished business:  $(\mathcal{F}_0(A, R), e)$  has the univ. property of  
a free  $R$ -module on the set  $A$ .

- Step
- ① Construct a well-defined function  $\tilde{f}: \mathcal{F}_0(A, R) \rightarrow M$ .
  - ② Show  $\tilde{f} \circ e = f$
  - ③  $\tilde{f}$  is  $R$ -linear
  - ④  $\tilde{f}$  is unique

- ① Let  $\varphi \in \mathcal{F}_0(A, R)$ . Then,  $\exists a_1, \dots, a_n \in A, r_1, \dots, r_n \in R$  s.t.

$$\varphi = r_1 e_{a_1} + \dots + r_n e_{a_n}.$$

Define  $\tilde{f}(\varphi) = r_1 f(a_1) + \dots + r_n f(a_n)$ .

This is well-defined since  $\{ea\}_{a \in A}$  is a basis of  $\mathcal{F}_0(A, R)$ .

- ②  $\tilde{f}(e(a)) = \tilde{f}(e_a) = f(a) \quad \forall a \in A.$   
 $\therefore \tilde{f} \circ e = f$

- ③ Let  $\varphi_1, \varphi_2 \in \mathcal{F}_0(A, R), r \in R$ .

Let  $\varphi_1 = r_1 e_{a_1} + \dots + r_n e_{a_n}$ ,

$$\varphi_2 = s_1 e_{a_1} + \dots + s_n e_{a_n}.$$

( $a_1, \dots, a_n$  same)

( $r_i, s_i$  are allowed to be 0)

Now,  $\tilde{f}(r\varphi_1 + \varphi_2)$   
 $= \tilde{f}((rr_1 + s_1)e_{a_1} + \dots + (rr_n + s_n)e_{a_n})$   
 $= (rr_1 + s_1)f(a_1) + \dots + (rr_n + s_n)f(a_n)$   
 $= r\tilde{f}(\varphi_1) + \tilde{f}(\varphi_2)$

- ④ Let  $\tilde{g}: \mathcal{F}_0(A, R) \rightarrow M$  be  $R$ -linear s.t.  $\tilde{g} \circ e = f$ , i.e.,  
 $(\tilde{g} \circ e)(a) = \tilde{g}(ea) = f(a) \quad \forall a \in A. (*)$

Claim:  $\tilde{f} = \tilde{g}$ , i.e., for all  $\varphi \in \mathcal{F}_0(A, R)$ :  $\tilde{f}(\varphi) = \tilde{g}(\varphi)$ .

Claim:  $\tilde{f} = \tilde{g}$ , i.e., for all  $\varphi \in S_r(A, R) : \tilde{f}(\varphi) = \tilde{g}(\varphi)$ .

Proof: Write  $\varphi = r_1 e_{a_1} + \dots + r_n e_{a_n}$  for  $r_i \in R, a_i \in A$

$$\text{Then, } \tilde{f}(\varphi) = r_1 f(a_1) + \dots + r_n f(a_n) \quad (\text{defn of } \tilde{f})$$

$$\tilde{g}(\varphi) = r_1 \tilde{g}(e_{a_1}) + \dots + r_n \tilde{g}(e_{a_n}) \quad (\text{linearity of } \tilde{g})$$

By  $(*)$ ,  $\tilde{f} = \tilde{g}$ .

Objects satisfying universal properties:

Let  $\{M_i\}_{i \in \Gamma}$  be a family of  $R$ -modules.

(Direct product)

① A (direct) product of  $\{M_i\}_{i \in \Gamma}$  is a pair  $(P, \{\pi_i\}_{i \in \Gamma})$ , where  $P$  is an  $R$ -module and for all  $i \in \Gamma$ ,  $\pi_i : P \rightarrow M_i$  is  $R$ -linear such that the following holds:

Given any  $(M, \{\varphi_i\}_{i \in \Gamma})$  where  $M$  is an  $R$ -module and

$\varphi_i : M \rightarrow M_i$  is  $R$ -linear for all  $i \in \Gamma$ ,

there exists a unique  $R$ -linear map  $\tilde{\varphi} : M \rightarrow P$  s.t.

$$\begin{array}{ccc} \tilde{\varphi} & \rightarrow & P \\ \downarrow & \pi_i & \downarrow \pi_i \\ M & \longrightarrow & M_i \end{array} \quad \text{commutes for all } i \in \Gamma.$$

(In other words,  $\pi_i \circ \tilde{\varphi} = \varphi_i$  for all  $i \in \Gamma$ .)

Thm. Direct products of  $R$ -modules exist and are unique up to isomorphism.

Not<sup>n</sup> Denoted by  $\prod_{i \in \Gamma} M_i$ .

Proof. Uniqueness: Same idea as seen before!

Existence:

Let  $P$  be the set of functions of the following type:

disjoint union

we can think of function  $f$  in form of sets.

$f: P \rightarrow \bigcup_{i \in M} M_i$  s.t.  
 $f(i) \in M_i$  for all  $i \in M$ .

Notation: For  $f \in P$ , we write  $f = (f_i)_{i \in P}$  where  $f_i = f(i)$   
and call  $f_i$  the  $i^{\text{th}}$  coordinate of  $f$ .

## Lecture 33 (10-11)

10 November 2020 10:27 AM

Recall:  $\{M_i\}_{i \in \Gamma}$  was given. We defined

$$P = \left\{ f : P \rightarrow \bigsqcup_{i \in \Gamma} M_i \mid f(i) \in M_i \quad \forall i \in \Gamma \right\}$$

Note that  $P$  is an  $R$ -module under pointwise operations:

$$(f+g)(i) = f(i) + g(i), \quad (r \cdot f)(i) = r \cdot f(i)$$

(Think about in terms of coordinate notation.)  
We're adding & mult. coordinate wise.

For each  $i \in \Gamma$ , we have a natural function

$$\pi_i : P \rightarrow M_i \text{ given by}$$

$$f \mapsto f(i).$$

$$(\pi_i(f) = f(i) = f_i)$$

called the projection  
onto the  $i^{\text{th}}$  coordinate

Note:  $\pi_i$  is  $R$ -linear for all  $i$ . (Follows directly from our def' of + and  $\cdot$  in  $P$ .)

Now, we prove that  $(P, (\pi_i))$  satisfies the universal property.

Suppose  $M$  is an  $R$ -module and  $\forall i \in \Gamma$ ,  $\varphi_i : M \rightarrow M_i$  is  $R$ -lin.

We want to construct a (unique)  $R$ -linear

$$\tilde{\varphi} : M \rightarrow P.$$

Define  $\tilde{\varphi}$  as follows: Let  $x \in M$ . Define  $\tilde{\varphi}(x) \in P$  by

$$\tilde{\varphi}(x)(i) = \varphi_i(x) \quad \forall i \in \Gamma,$$

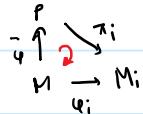
$$\text{i.e., } \tilde{\varphi}(x)_i = \varphi_i(x),$$

$$\text{i.e., } \tilde{\varphi}(x) = (\varphi_i(x))_{i \in \Gamma}.$$

Moreover,  $\tilde{\varphi}$  is  $R$ -linear. (Verify!)

Moreover, for each  $i \in \Gamma$ , we have

$$\pi_i \circ \tilde{\varphi} = \varphi_i.$$



Now, we show uniqueness of  $\tilde{\varphi}$ . Suppose

$\psi: M \rightarrow P$  is R-linear s.t.

$$\pi_i \circ \psi = \varphi_i \quad \forall i \in \Gamma.$$

Then, for all  $x \in M$ ,

$$(\psi(x))_i = \varphi_i(x) = (\tilde{\varphi}(x))_i \quad \forall i \in \Gamma$$

Thus,  $\psi(x)$  and  $\tilde{\varphi}(x)$  are functions which agree on  $\Gamma$ . Thus,  $\psi(x) = \tilde{\varphi}(x)$ .

Since this is true for all  $x \in M$ ,  $\psi = \tilde{\varphi}$ .  $\square$

Remark: By uniqueness of products, any way of defining "the" product gives us the same object.

Q. Do direct products of rings exist?

② (Direct sum) Given  $\{M_i\}_{i \in \Gamma}$ , a family of R-modules, a direct sum of  $\{M_i\}_{i \in \Gamma}$  is a pair

$$(S, (e_i)_{i \in \Gamma})$$

where  $S$  is an R-module and  $e_i: M_i \rightarrow S$ , R-linear  $\forall i \in \Gamma$  satisfying:

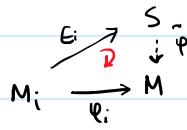
Given any  $(M, (\varphi_i)_{i \in \Gamma})$ ,  $M$  an R-module,  $\varphi_i: M_i \rightarrow M$

R-linear for all  $i \in \Gamma$ , there exists a unique

R-linear  $\tilde{\varphi}: S \rightarrow M$  s.t.

$$\tilde{\varphi} \circ e_i = \varphi_i$$

for all  $i \in \Gamma$ .



Thm. Direct sums of R-modules do exist and are unique up to isomorphism.

Proof.

Uniqueness : Exercise

Existence :

Let  $P$  be the product that we explicitly constructed earlier.

for  $i \in I$ :

Consider the natural  $\epsilon_j : M_j \rightarrow P$  defined by

$$\epsilon_j(x_j) = x \quad \text{where}$$

$$x \in P \quad \text{is} \quad (x)_i = \begin{cases} x_j & i=j, \\ 0 & i \neq j. \end{cases}$$

$\epsilon_j$  is  $R$ -linear. all except  $j^{\text{th}}$  coordinate is zero

Let  $S = \langle \epsilon_j(M_j) : j \in I \rangle$   
 $= \left\{ x \in P \mid x_j = 0 \text{ for all but finitely many } j \in I \right\}.$

Verify that the universal property is satisfied.

Q. Does a direct sum of rings exist?

③ (Tensor products) Given  $R \xrightarrow{\varphi} S$  a ring map. (That is,  $S$  is an  $R$ -alg via  $\varphi$ .)

$M$  is an  $R$ -module.

Want: to create an  $S$ -module "like"  $M$ .

General construction: Tensor product of  $M$  and  $N$  over  $R$ .

(Converts bilinear maps from  $M \times N$  to  $L$  into a linear map  $M \otimes N \rightarrow L$ .)

## Lecture 34 (12-11)

12 November 2020 11:32 AM

Def<sup>n</sup>

(Tensor product) Given  $R$ -modules  $M$  and  $N$ , a tensor product of  $M$  and  $N$  over  $R$  is a pair  $(T, \theta)$  where

- $T$  is an  $R$  module and
- $\theta : M \times N \rightarrow T$  is  $R$ -bilinear, satisfying:

Given any pair  $(L, \varphi)$  where  $L$  is an  $R$ -module and  $\varphi : M \times N \rightarrow L$  is bilinear,  $\exists! \tilde{\varphi} : T \rightarrow L$   $R$ -linear which makes the following diagram commute:

$$\begin{array}{ccc} M \times N & \xrightarrow{\theta} & T \\ & \searrow \varphi & \downarrow \sim \tilde{\varphi} \\ & & L \end{array}$$

$\tilde{\varphi} \circ \theta = \varphi.$

Ex of bilinear maps: Inner product (over  $\mathbb{R}$ ),

$$\det : \mathbb{R}^2 \times \mathbb{R}^2 \rightarrow \mathbb{R},$$

scalar mult. of any ring:  $\cdot : R \times R \rightarrow R$

similarly  $\cdot : R \times M \rightarrow M$

$$R[x] \times R[y] \rightarrow R \quad (f, g) \mapsto f(0) \cdot g(0)$$

$$M_{m \times n}(R) \times M_{n \times p}(R) \rightarrow M_{m \times p}(R), \quad (A, B) \mapsto AB$$

Q. Can you identify some elements forced to map to 0?

*haven't proven this yet*

Q. What is "the" tensor product of  $\mathbb{Q}[x]$  and  $\mathbb{Q}[y]$  over  $\mathbb{Q}$ ?

(Can do in general:  $R^{\leftarrow \text{comm. ring}} \text{ instead of } \mathbb{Q}.$ )

Guess:  $R[x, y]$ . We have  $R[x] \times R[y] \rightarrow R[x, y]$   
 $(f, g) \mapsto f \cdot g.$

We also had  $R[x] \times R[y] \rightarrow R$  earlier.

Is  $R$  the tensor product? Is  $R[x, y]$ ?

Is  $R$  the tensor product? Is  $R[x, y]$ ?

Q. We also saw  $R \times M \rightarrow M$  was bilin. Is  $M$  the tensor product of  $R$  and  $M$  over  $R$ ? If not, then what?

Thm. Given  $R$ -modules  $M$  and  $N$ , a tensor product of  $M$  and  $N$  over  $R$  exists, and is unique up to isomorphism.

This is denoted as  $M \otimes_R N$ .

Proof. Uniqueness. (Exercise!)

Existence.

Vague (but improper) idea : Given an  $R$ -bilin. map  $M \times N \xrightarrow{\Phi} L$ , we want an  $R$ -mod  $T$  &  $R$ -bi map  $M \times N \xrightarrow{\Phi} T$ , an  $R$ -lin. map  $\tilde{\Phi}: T \rightarrow L$  satisfying some conditions.

(Improper because it looks like  $(T, \Phi)$  depends on  $(L, \Phi)$ )

$$\begin{array}{ccc} M \times N & \xrightarrow{\Phi} & T \\ \varphi \downarrow & \swarrow \tilde{\Phi} & \\ L & & \end{array}$$

Denote  $\Phi(x, y)$  by  $\langle x, y \rangle$ . We want

$$\langle x, y \rangle + \langle x', y \rangle = \langle x+x', y \rangle, \quad a \langle x, y \rangle = \langle ax, y \rangle$$

$$\langle x, y \rangle + \langle x, y' \rangle = \langle x, y+y' \rangle \quad \langle x, ay \rangle.$$

Thus, we want  $\langle x, y \rangle + \langle x', y \rangle - \langle x+x', y \rangle = 0, \dots$

Quotient!

But on what module?

On  $M \times N$  with usual operations? Nah!

↳ This already has relations

Actual  
construction

Let  $F = F(M \times N)$  be the free  $R$ -module on the set  $M \times N$ .

Then,  $\{e_{(x,y)} : (x,y) \in M \times N\}$  is a basis of  $F$ .

Let  $G$  be the submodule of  $F$  generated by

*there are all relations we want. To get mod. we need the submodule.*

$$\left\{ \begin{array}{l} \cdot e_{(x_1+x_2, y)} - e_{(x_1, y)} - e_{(x_2, y)} \\ \cdot e_{(x, y_1+y_2)} - e_{(x, y_1)} - e_{(x, y_2)} \\ \cdot e_{(ax, y)} - ae_{(x, y)} \\ \cdot e_{(x, ay)} - ae_{(x, y)} \end{array} \right.$$

where  $x, x_i \in M, y, y_i \in N, a \in R$ .

Define  $T = F/G$ . Let  $\pi: F \rightarrow T$  be the natural map,  $e: M \times N \rightarrow F$  the usual "inclusion".

Denote  $e(x, y)$  by  $e_{(x, y)}$  and  $\pi(e_{(x, y)})$  by

*this was just a map*

$$M \times N \xrightarrow{e} F \xrightarrow{\pi} T$$

$x \otimes y$

Is  $\theta$  bilinear?

$\theta = \pi \circ e$  and now check if bilinear.

Note that  $e$  is just a function!

$$\begin{aligned} \theta(x_1 + x_2, y) &= \pi(e_{(x_1 + x_2, y)}) \\ &= (x_1 + x_2) \otimes y \end{aligned}$$

Note  $e_{(x_1 + x_2, y)} - e_{(x_1, y)} - e_{(x_2, y)} \in G = \ker \pi$

$$\begin{aligned} \Rightarrow \pi(e_{(x_1 + x_2, y)}) &= \pi(e_{(x_1, y)} + e_{(x_2, y)}) \\ &= \pi(e_{(x_1, y)}) + \pi(e_{(x_2, y)}) \end{aligned}$$

$$\begin{aligned} &= x_1 \otimes y + x_2 \otimes y \\ &= \theta(x_1, y) + \theta(x_2, y) \end{aligned}$$

Similarly the other relations in  $G$  give us

$$x \otimes (y_1 + y_2) = x \otimes y_1 + x \otimes y_2, \quad a(x \otimes y) = (ax) \otimes y \\ = x \otimes (ay)$$

# Lecture 35 (12-11)

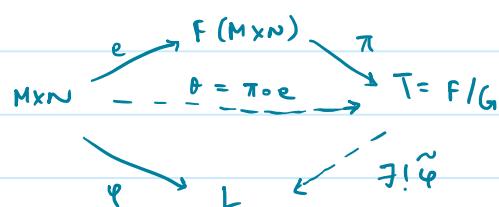
12 November 2020 19:03

Observations / Notations:

- ①  $\pi(e(x,y)) = \pi(e_{(x,y)}) = x \otimes y$
- ②  $x \otimes y$  is "linear in each coordinate"
- ③  $\{x \otimes y \mid x \in M, y \in N\}$  is a generating set for  $T$  over  $R$ .

In fact, any element of  $T$  can be written as a finite sum  $\sum x_i \otimes y_i$ . (Don't need scalars.)

Coming back:



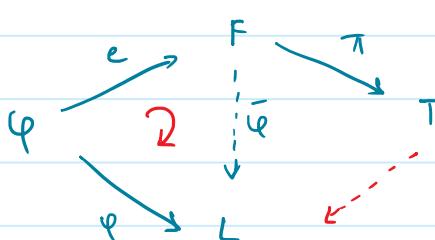
Constructing  $\tilde{\varphi}$ :

$$\begin{aligned} \text{We would like } \tilde{\varphi}(x \otimes y) &= \varphi(x,y), \quad \tilde{\varphi}\left(\sum x_i \otimes y_i\right) \\ &= \sum \varphi(x_i, y_i) \end{aligned}$$

BUT WE DON'T KNOW IF WELL-DEFINED! :-

Note that  $\varphi$  is a function. Then, by the Univ. property of  $F$  (on the set  $M \times N$ ),  $\exists! \bar{\varphi}: F \rightarrow L$   
 $\bar{\varphi}(e(x,y)) = \varphi(x,y)$

$R$ -lin ear



We have  $R$ -linear

$$\bar{\varphi}: F \rightarrow L.$$

We want it to factor through  $T (= F/G)$ .

What do we need?

Well,  $\ker \bar{\varphi} \cap G$  is what!

(universal) property  
of kernels

{

✓ This is true because  $\varphi$  is  $R$ -bilinear!

Take any one of the four type of gen. of

G. for example:  $z = \varphi(x, y_1 + y_2) - \varphi(x, y_1) - \varphi(x, y_2)$

$$\begin{aligned}\bar{\varphi}(z) &= \bar{\varphi}(- - -) \\ &= \bar{\varphi}(-) - \bar{\varphi}(-) - \bar{\varphi}(-) \\ &= \varphi(x, y_1 + y_2) - \varphi(x, y_1) - \varphi(x, y_2) \\ &= 0\end{aligned}$$

2.  $\bar{\varphi}$  is additive  
def "of"  
 $\bar{\varphi}$  on basis  
D-bilinear

Thus,  $G \subset \ker \bar{\varphi}$ . Thus, the map factors.

Thus, we have

$$\begin{array}{ccc} & F & \\ \nearrow & & \searrow \\ M \times N & \xrightarrow{\quad} & T \\ \downarrow & & \downarrow \\ L & & \end{array}$$

The red triangle

commutes too now.

(Check!)

use that the other triangles do.

Now, we have to show uniqueness of  $\tilde{\varphi}$ .

Claim. Suppose  $\exists \psi : T \rightarrow L$  R-linear s.t.  $\psi \circ \theta = \varphi$ , then  $\psi = \tilde{\varphi}$ .

Proof. Commutativity gives:  $\varphi(x, y) = \psi \circ \theta(x, y) = \psi(x \otimes y)$

but we also have  $\tilde{\varphi}(x \otimes y) = \varphi(x, y)$

thus,  $\tilde{\varphi}(x \otimes y) = \psi(x \otimes y)$  for all  $x \in M, y \in N$

Since  $\{x \otimes y\}_{\substack{x \in M \\ y \in N}}$  generates  $T$ , we are done!

Q: ① Suppose  $z \in T$  s.t.  $\tilde{\varphi}(z) = 0$ .

Write  $z = x_1 \otimes y_1 + \dots + x_n \otimes y_n$ .

What does this tell us about  $x_i$ 's and  $y_i$ 's?

② Suppose  $z = 0$ . Can we say anything about  $x_i$  and  $y_i$ ?

Caution.

$x = 0$  or  $y = 0 \Rightarrow x \otimes y = 0$

Converse is not true!

$$R = \mathbb{Z}, M = \mathbb{Z}, N = \mathbb{Z}/2\mathbb{Z}.$$

$$x = 2, y = 1.$$

Then,  $x \neq 0$  &  $y \neq 0$ . But  $x \otimes y = 2 \otimes 1$

$$= (2 \cdot 1) \otimes 1$$

$$= 2 \cdot (1 \otimes 1) = 1 \otimes (2 \cdot 1)$$

$$= 0$$

Example:

① Find  $M, N$  non-zero s.t.  $M \otimes_R N = 0$

Q. Suppose  $K \leq M$ . Is  $K \otimes_R N \leq M \otimes_R N$ ?

② What is  $R \otimes M$ ?

A more precise question: Is  $R \otimes M \cong M$ ?

Strategy 1: Show that  $(M, \cdot : R \times M \rightarrow M)$  satisfies universal property.

Strategy 2: Given  $(M, \cdot : R \times M \rightarrow M)$ ,  $\exists ! \tilde{\psi} : R \otimes M \rightarrow M$  s.t. ...

Show  $\tilde{\psi}$  is an isomorphism.

Proof. Let's try Strat. 1!

Note that  $M$  is an  $R$ -module and

$$\theta : R \times M \rightarrow M, (r, m) \mapsto r \cdot m$$

is bilinear.

Given a pair  $(N, \psi)$ ,  $\psi : R \times M \rightarrow N$   $R$ -bilinear, we

want to show existence of a unique  $R$ -linear

$$\tilde{\psi} : M \rightarrow N \text{ s.t. } \tilde{\psi} \circ \theta = \psi.$$



Define  $\tilde{\psi} : M \rightarrow N$  as  $\tilde{\psi}(x) = \psi(1, x)$ .

Verify it's linear.

$$\text{Also, } \tilde{\psi} \circ \theta(a, n) = \tilde{\psi}(ax) = \psi(1, ax) = \psi(a, n) \text{ by }$$

The uniqueness is clear since

$$\tilde{\psi}(x) = \tilde{\psi} \circ \theta(1, x) = \psi(x) \text{ is forced.}$$

Ex. Prove this using Strat. 2.

Ex2. If  $I \subset R$ , do you have a guess for  $R/I \otimes_R M$ ?

Yes,  $M/IM$  with  $\theta: R/I \times M \rightarrow M/IM$  as  
 $(\bar{a}, x) \mapsto \bar{ax}$ .

Using same strategy. What would  $\tilde{\varphi}$  be?

---

E.g.  $R[x] \otimes_R R[y] \cong R[x,y]$

Define  $\theta: R[x] \times R[y] \rightarrow R[x,y]$ .  $\theta$  is bilin.  
 $(f,g) \mapsto fg$

Suppose  $(M, \varphi)$  is a pair,  $M \xrightarrow{\text{R-bilin}} R[x,y] \rightarrow M$   
R-bilinear

Want: unique  $\tilde{\varphi}: R[x,y] \rightarrow M$  s.t.

$$\tilde{\varphi} \circ \theta = \varphi$$

$$R[x] \times R[y] \xrightarrow{\theta} R[x,y]$$

$$\varphi \downarrow_M \tilde{\varphi}$$

Note that  $R[x,y]$  is free with  
 $B = \{x^i y^j : i, j \in \mathbb{N}_{\geq 0}\}$  as basis.

Thus, sufficient to define on  $B$ .

Define  $\tilde{\varphi}(x^i y^j) = \varphi(x^i, y^j)$ .

Moreover, the above is forced since  $\tilde{\varphi}(x^i y^j)$   
by comm.  $= \tilde{\varphi}(\theta(x^i, y^j))$   
 $= \varphi(x^i, y^j)$ .

This proves existence and uniqueness.

---

(Base change)

Let  $M$  be an  $R$ -module, and  $R \xrightarrow{\varphi} S$  a ring map.

Then,  $S \otimes_R M$  is an  $S$ -module with multiplication

defined by:

For  $a, b \in S$ ,  $x \in M$ , define  $a \cdot (b \otimes x) := (ab) \otimes x$ .

# Lecture 36 (16-11)

16 November 2020 09:26

Example.

①  $M \otimes_R N \cong N \otimes_R M$

Want:  $x \otimes y \mapsto y \otimes x$ . why well-defined, though?

$$\begin{array}{ccc} M \times N & \longrightarrow & N \times M \\ (x, y) & \mapsto & (y, x) \end{array} \xrightarrow{\sigma} N \otimes_R M$$

This is bilinear

②  $L \otimes (M \oplus N) \longrightarrow (L \otimes M) \oplus (L \otimes N)$

$$\begin{aligned} L \times (M \oplus N) &\longrightarrow (L \times M) \oplus (L \times N) \\ (x, (y, z)) &\mapsto ((x, y), (x, z)) \end{aligned}$$

③  $L \otimes (M \otimes N) \longrightarrow (L \otimes M) \otimes N$

$$\begin{aligned} L \times (M \otimes N) &\longrightarrow (L \times M) \otimes N \\ (x, (y, z)) &\mapsto ((x, y), z) \end{aligned}$$

Modules over a PID:

Recall.  $M = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \xleftarrow{\quad \text{F} \quad} \mathbb{Z}_{e_1} \oplus \mathbb{Z}_{e_2}$

$$\begin{aligned} (\bar{1}, \bar{0}) &\longleftrightarrow e_1 \\ (\bar{0}, \bar{1}) &\longleftrightarrow e_2 \end{aligned}$$

$$K := \ker \psi = \langle 2e_1, 3e_2 \rangle$$

$$K := \ker \psi = \langle 2e_1, 3e_2 \rangle$$

↑ lin indep.

Thus,  $K$  is free.

$$\begin{array}{ccc} \text{Map } & \mathbb{Z}_{f_1} \oplus \mathbb{Z}_{f_2} & \xrightarrow{\psi} K \\ & f_1 \mapsto 2e_1 & \\ & f_2 \mapsto 3e_2 & \end{array}$$

Since  $K$  is free with basis  $\{2e_1, 3e_2\}$ , we get that  $\psi$  is an isomorphism.

$$G \xrightarrow{\psi} F \rightarrow M \text{ where}$$

$$\psi = \begin{bmatrix} e_1 & e_2 \\ f_1 & f_2 \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix}$$

Note that  $M \cong \mathbb{Z}/6\mathbb{Z}$ .

How can we write  $\mathbb{Z}/6\mathbb{Z}$  as a quotient of  $F$ ?

$$\text{Write } M \cong \mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/\mathbb{Z}.$$

Now we wish to do a change of basis.

Need a basis  $\{u_1, u_2\}$  s.t.

$\ker \psi$  has basis  $\{6u_1, u_2\}$ .

Q: What are  $u_1, u_2$ ? (In terms of  $e_1, e_2$ )

Exercise!

(Want:  $u_1 = e_1 + e_2$  since  $e_1 + e_2$  maps to  $\sim$   
gen. of  $\mathbb{Z}/2 \times \mathbb{Z}/3$ )

Recall: If  $G$  is a fin. gen abelian group, then  

$$G \cong \mathbb{Z}^r \oplus \mathbb{Z}/p_1^{k_1} \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_n^{k_n} \mathbb{Z}$$

where  $p_i$ 's are prime.

Thm.

(Structure theorem)

Let  $R$  be a PID,  $M$  a finitely generated module over  $R$ .

Then,

$$M = R^s \oplus \left( \bigoplus_{i=1}^k R/\langle p_i^{k_i} \rangle \right)$$

where each  $p_i$  is prime.

(Elementary divisor form)

Proof. We first show: (Decomposition theorem)

$\exists a_1, \dots, a_n \in R$  s.t.

$$M \cong R^s \oplus R/\langle a_1 \rangle \oplus \cdots \oplus R/\langle a_n \rangle$$

(Call this the decomposition theorem.)

One: WLOG, assume that each  $a_i \neq 0$  and  
 $a_i \notin V(R)$ .

↳ can check  $R/\langle a_i \rangle \neq 0$

↑ can absorb  
in  $R^s$

Suppose  $a$  is a non-zero non-unit.

Then  $0 \neq \langle a \rangle \subsetneq R$ . Then  $\exists$  primes  $p_1, \dots, p_r$

s.t.

$$a = p_1^{k_1} \cdots p_r^{k_r}. \quad (p_i \neq p_j \text{ for } i \neq j)$$

Then,  $(\langle p_i^{k_i} \rangle, \langle p_j^{k_j} \rangle)$  is comax  $\forall i \neq j$ .

Then,

$$\frac{R}{(a)} \cong \frac{R}{\langle p_1^{k_1} \rangle} \times \cdots \times \frac{R}{\langle p_r^{k_r} \rangle} \text{ by CRT.}$$

From this, it follows that  
decomposition  $\Rightarrow$  elementary.

Two: To prove decomposition, we prove:

Let  $R$  be a PID and  $F$  a free  $R$ -module of finite rank. If  $K$  is a submodule of  $F$ , then  $K$  is free of rank at most  $\text{rank}_R(F)$ .

Moreover,  $\exists$  a basis  $\{y_1, \dots, y_n\}$  of  $F$  s.t.

$\exists a_1, \dots, a_m$  s.t.  $\{a_1 y_1, \dots, a_m y_m\}$  is a basis of  $K$ .  $(m \leq n)$

## Lecture 37 (17-11)

17 November 2020 10:07 AM

(Submodule theorem)

Thm.: Let  $R$  be a PID,  $F$  a free  $R$ -module of finite rank  $m$ . Let  $K$  be a submodule of  $F$ . Then,

- ①  $K$  is free
- ②  $\text{rank}_R(K) \leq m$
- ③  $\exists$  a basis  $\{y_1, \dots, y_m\}$  of  $M$ ,  $a_1, \dots, a_n \in R$  s.t.  $\{a_1y_1, \dots, a_ny_n\}$  is a basis of  $K$ .

Claim. Submodule thm  $\Rightarrow$  Decomposition Thm

Proof: Suppose  $M$  is gen. by  $m$  elements.

By earlier class, we can write  $M \cong F/K$ , where  $F$  is free with  $\text{rank}_R(F) = m$ .

By submodule thm ③,  $K = \langle a_1y_1, \dots, a_ny_n \rangle$  where  $\{y_1, \dots, y_m\}$  is a basis of  $F$  and  $\{a_1y_1, \dots, a_ny_n\}$  of  $K$  and  $a_1, \dots, a_n \in R$ .

Verify that  $F/K \cong R/\langle a_1 \rangle \oplus \dots \oplus R/\langle a_m \rangle \oplus R^{m-n}$ .

Proof of submodule thm.

Induction on  $\text{rank}_R(F)$ . (to prove ① and ②)

•  $\text{rank}_R(F) = 1$ , then  $F \cong R$  and  $I \subset R$  is an ideal in  $R$ .

Fact: every ideal in PID is free and if  $I \neq 0$ ,  $\text{rank}_R(I) = 1$ , else  $\text{rank}_R(I) = 0 \leq 1$ .

• Assume true for  $\text{rank}_R(F) \leq m-1$  &  $m > 1$ .

Suppose  $\text{rank}_R(F) = m$ .

If  $K = 0$ , then nothing to prove.

Assume  $K \neq 0$ . Let  $\pi_i$  be the  $i^{\text{th}}$  projection of  $F$  onto  $R$  (w.r.t. a fixed basis  $(e_1, \dots, e_m)$ ).

$\exists i$  s.t.  $\pi_i(K) \neq 0$ . wlog, let  $i = 1$ .

Then,  $\text{ker } \pi_i(K)$  is a non-zero ideal in  $R$ .

Thus,  $\text{ker } \pi_i(K) = \langle a \rangle$  for some  $a \in R \setminus \{0\}$ .

Let  $x \in K$  be such that  $\pi_i(x) = a$ .

Let  $y \in K$ . Then  $\pi_i(y) = b\pi_i(x)$  for some  $b \in R$ .  
 $(\because \text{ker } \pi_i(K) = \langle \pi_i(x) \rangle)$

$$\begin{aligned} \Rightarrow y - bx &\in (\text{ker } \pi_i) \cap K \\ \Rightarrow y &= bx + (\text{something}) \\ \Rightarrow K &= Rx + (\text{ker } \pi_i \cap K) \end{aligned}$$

Is it a direct sum?

Let  $y \in Rx \cap (\text{ker } \pi_i \cap K)$ .

$$\Rightarrow y = bx \quad \text{for some } b \in R,$$

$$\pi_i(y) = 0.$$

$$\hookrightarrow \pi_i(bx) = 0 \Rightarrow b\pi_i(x) = 0 \xrightarrow{a \neq 0, \text{ in an ID}} b = 0.$$

$$\therefore y = 0 \quad \text{and} \quad K = Rx \oplus (\text{ker } \pi_i \cap K)$$

By induction,

$\text{ker } \pi_i \cap K$  is free of rank at most  $m-1$ ,  
say with basis  $x_2, \dots, x_n$ .  
 $\left( \begin{array}{l} \text{since } \text{ker } \pi_i \\ \text{is free with} \\ \text{rank } m-1. \end{array} \right)$

Verify that  $\{x, x_2, \dots, x_n\}$  is a basis of  $K$ .

This proves ① and ②.

Proof of ③:

$$③ \text{ Let } \mathcal{I} = \{ \varphi(K) \mid \varphi \in \text{Hom}_R(F, R) \}$$

$\langle 0 \rangle \in \mathcal{I}$ . ( $R \in \mathcal{I}$  if  $F \neq 0$ .)

$\mathcal{I} \neq \emptyset$ .  $\mathcal{I}$  is ordered by inclusion.

If  $\{I_j\}_{j \in \Gamma}$  is a chain,  $I = \bigcup_{j \in \Gamma} I_j$  is

an ideal. (Seen before.)

$I = \langle a \rangle$ , since  $R$  is PID.

Then,  $a \in I_j$  for some  $j \in \Gamma$  & thus,  $I_j = I \in \mathcal{I}$ .

Thus, by Zorn's Lemma,  $\mathcal{I}$  has a maximal element,

say  $\varphi_0(k) = \langle a_0 \rangle$ .