Lecture 8 (01-09)

01 September 2020 10:29 AM

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

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

called the prime spectrum of R.

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

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

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

Okay, assume $R \neq 0$.

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

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

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

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

② Λ is a poset by $\subseteq$.

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

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

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

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

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

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

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

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

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

WLOG

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

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

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

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

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

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

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

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

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

Thus, $I = R$, proving that $\mathfrak{m}$ is maximal. ☺

Corollaries: ($R \neq 0$)

① Every proper ideal is contained in a maximal ideal.

② Let $a \in R$. Then,

a is not a unit $\iff \exists\, \mathfrak{m} \in \mathrm{Max}(R)$ s.t. $a \in \mathfrak{m}$. } Commutative ring. Otherwise "left max." or "right max."

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

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

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

That is, if $\mathfrak{m}$ is a maximal ideal in R, then $\mathfrak{m}$ is prime.

Max ideals are prime

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

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

$b \in R$ be such that

Proof. Let $\mathcal{M}$ be a maximal ideal and $a, b \in R$ be such that $ab \in \mathcal{M}$ and $a \notin \mathcal{M}$.

$a \notin \mathcal{M} \Rightarrow \mathcal{M} \subsetneq \mathcal{M} + \langle a \rangle \Rightarrow \mathcal{M} + \langle a \rangle = R$

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

$$\Rightarrow \underbrace{\underset{\in \mathcal{M}}{mb} + \underset{\in \mathcal{M}}{rab}}_{\in \mathcal{M}} = b$$

$\therefore b \in \mathcal{M}$.

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 $\mathcal{M}$ be a max. ideal in R/I.

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

② let $a \in R$.

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

$\Updownarrow$ $\Downarrow$ we proved $\Uparrow$ obvious since max ideals are proper

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

a is cont. in a max ideal $\Longleftrightarrow$

Lecture 9 (03-09)

03 September 2020 11:27 AM

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

Also, 0 is not an integral domain.

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

(Prime ideal Exercise)

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

Comm.

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

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

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

$$\bigcup_{\mathfrak{m} \in \mathrm{Max}(R)} \mathfrak{m} = R \setminus \mathcal{U}(R)$$

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

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

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

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

Jacobson radical

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

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

$\Rightarrow a^k \in \mathfrak{m} \quad \forall \mathfrak{m}$ max

max. ideals are prime

$\Rightarrow a \in \mathfrak{m} \quad \forall \mathfrak{m}$

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

In fact, $\underbrace{\mathcal{N}(R) \subset \bigcap_{\mathfrak{p} \in \mathrm{Spec}(R)} \mathfrak{p} \subset J(R)}_{\text{any equality?}}$.

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

Q. If $1+a$ is a unit, does $a \in J(R)$?
No. Take, $R = \mathbb{Z}$, $1+a = -1$.

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

Does this converse hold now?
Yes!

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

Proof: $(\Rightarrow)$ Let $a \in J(R)$ and $r \in R$ be arbitrary.
$ra \in J(R)$ since $J(R)$ is an ideal.
Thus, $ra \in \mathfrak{m}$ for every max. ideal $\mathfrak{m}$.
$\Rightarrow 1 + ra \notin \mathfrak{m}$ for any max ideal $\mathfrak{m}$
$\Rightarrow 1 + ra$ is a unit.

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

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

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

Then, $\mathfrak{m} + \langle a \rangle = R$.

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

$\Rightarrow m = 1 + ra \in \mathfrak{m}$ is a unit $\rightarrow\leftarrow$

Thus, our assumption was incorrect. In other words,

$a \in \mathfrak{m}$ for all $\mathfrak{m} \in Max(R)$.

Thus, $a \in J(R)$. ☺

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

Sol^n. Disproof: We construct a counterexample.

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

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

↳ maximal!

Thus, $J(R) = \{0, 2\} \neq \{0\}$. ☹

(Prime ideal Exercise solution)

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

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

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

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

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

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

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

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

Lecture 10 (07-09)

07 September 2020 09:22 AM

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

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

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

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

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

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

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

Leads to the following def^n.

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

Co-maximal, comaximal ideals

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

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

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. $a \in R$, $b \in R$.
Consider $r = bi + aj \in R$.

Then, $\varphi(r) = (bi + aj + I,\ bi + aj + J)$
$= (aj + I,\ bi + J) = (a - ai + I,\ b - bj + J)$
$= (a + I,\ b + J)$
$= (\bar{a}, \bar{b})$. $\square$

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

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

$$\begin{tikzcd} R/I\cap J \arrow[r, hook, "\tilde{\varphi}"] & R/I \times R/J \\ R \arrow[u, "\pi"] \arrow[ur, "\varphi"'] & \end{tikzcd}$$

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

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

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

$$a = \underset{\substack{\uparrow \\ JI}}{ai} + \underset{\substack{\uparrow \\ IJ}}{aj}$$

$IJ =$ ☺

② Examples : Let $m \in Max(R)$ and $I \not\subseteq m$ 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 $Max(R) = \{m\}$.

↳ 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, $I + J \subseteq m \subsetneq R$.

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

Choose two distinct maximal ideals!

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

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

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

often called the "diagonal map"

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

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

jth pos.

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

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

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

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

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

Lecture 11 (08-09)

08 September 2020 10:29 AM

Recall the following q.

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

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

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

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

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

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

Proof. Same as above.

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

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

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

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

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

We can now prove the result by induction.

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

Base: $n = 2$ done.

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

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

Assume claim for now.

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

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

Moreover, this iso was induced by φ.

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

Using this, we get that

$$\begin{tikzcd} R \arrow[r, two heads] \arrow[rr, bend right, "\text{is onto}"'] & R/I_1 \times R/(\bigcap I_j) \arrow[r, two heads] & R/I_1 \times \cdots \times R/I_n \end{tikzcd}$$

Now, we prove the claim.

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

Proof. $\overset{\in I_2}{a_2}, \ldots, \overset{\in I_n}{a_n}$. $\quad \overset{\in I_1}{b_2}, \ldots, \overset{\in I_1}{b_n}$

$a_2 + b_2 = 1$, $a_3 + b_3 = 1$, ..., $a_n + b_n = 1$

$$1 = (a_2 + b_2) \cdots (a_n + b_n)$$
$$= \underbrace{a_2 a_3 \cdots a_n}_{\cap I_j} + \underbrace{b_2(\ ) + b_3(\ ) + \cdots + b_n(\ )}_{I_1}$$

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

Thus, we have proved the Chinese Remainder Theorem.

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

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

Then,

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

Note that we also proved:
1. The natural map $R \longrightarrow \prod R/I_j$ is onto.
2. $I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$.

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

Prime Ideals.

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

1 Q: Is $\mathcal{N}(R) = \bigcap_{\mathfrak{p} \in \operatorname{Spec}(R)} \mathfrak{p}$? ($R \neq 0$ comm.)

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

Let $A = \bigcap \mathfrak{p}$ and $B = \mathcal{N}(R)$.

Claim. $A \subset B$.
Proof We show $B^c \subset A^c$.
Let $a \in R \setminus \mathcal{N}(R)$. We show that $a \notin \mathfrak{p}$ for some $\mathfrak{p} \in \operatorname{Spec}(R)$.

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

Consider the collection

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

$\Delta \neq \emptyset$ since $\mathcal{N}(R) \in \Delta$. Δ is a poset by $\subseteq$.

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

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

<u>Claim</u>. $\mathfrak{p}$ is prime.

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

By maximality of $\mathfrak{p}$ in Λ, we get
$$\mathfrak{p} + \langle b \rangle \notin \Lambda \not\ni \mathfrak{p} + \langle c \rangle.$$

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

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

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

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

$\hookrightarrow$ Now what?

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

To be continued.--

Lecture 12 (10-09)

10 September 2020 11:14 AM

Changing the Prev. proof.

Consider the collection

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

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

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

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

still goes through

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

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

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

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

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

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

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

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

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

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

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

Thus, we have proven.

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

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

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

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

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

Notation: For an ideal $I \subset R$,
$$V(I) = \{\mathfrak{p} \in \operatorname{Spec}(R) : I \subset \mathfrak{p}\}.$$

Prime Avoidance

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

Nope!

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

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

Still nope!

Ex. Find a counterexample.

However, the statement is true for prime ideals.

Thm. (Prime Avoidance) Let $I \subset \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_n$ for $\mathfrak{p}_i \in \operatorname{Spec}(R)$.

Then, $I \subset \mathfrak{p}_j$ for some j.

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

We prove $n \geq 3$ by induction.

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

We show $I \not\subset \mathfrak{p}_1 \cup \mathfrak{p}_2 \cup \mathfrak{p}_3$.

$\Rightarrow \exists a_j \in I$ but $a_j \notin \mathfrak{p}_j$.

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

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

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

That is, $I \not\subset \mathfrak{p}_1 \cup \mathfrak{p}_2$, etc. (induction)

Counter example for non-prime ideals.

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

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

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

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

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

Lecture 13 (14-09)

14 September 2020 09:35 AM

Thm. (Prime avoidance)

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

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

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

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

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

Here is where we used primality

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

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

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

Let $b \in I$ be defined as

$b = b_1 + \dots + b_n$.

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

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

Prof. We phrase the theorem as follows:

Let $n \geq 2$.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Lecture 14 (15-09)

15 September 2020 10:32 AM

Localisation : Create "more" units

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

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

Observed that 2 is a unit in R.

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

Example. ① Take $R = \mathbb{Z}/6\mathbb{Z}$. What happens if we "invert 3"?
Then, $2 \cdot 3 = 0 \Rightarrow 2 = 0$. 2 becomes 0.
$3 = 2 + 1 = 1$, $4 = 2 + 2 = 0$, $5 = 1 + 4 = 1$.
Looks like the ring has become $\mathbb{Z}/2\mathbb{Z}$.
(Haven't yet defined what "invert" means)

② $R = \mathbb{Z}$. What if we invert all non-zero elements?
Expect : $\mathbb{Q}$
(In fact, that's how we defined the field of fractions of an ID)

③ $R = \mathbb{Z}$. Invert 2.
Expect: $\mathbb{Z}[1/2]$

④ $R = \mathbb{Z}$. Invert whatever possible except 2.
(Invert $\mathbb{Z} \setminus 2\mathbb{Z}$)
set exclusion

set exclusion

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

recall

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

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

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

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

① $\forall a, b \in A$: $a, b \in A$
② $1 \in A$
③ $0 \notin A$

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

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

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

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

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

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

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

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

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

Verify that these operations are well-defined. Show that R_A is then a ring.

(Ex. 2)

Solutions.

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

Sol^n: Reflexive and symm. is clear.
$(a=1)$ (same 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. $a(x_1 a_2 - x_2 a_1) = 0$
$a'(x_2 a_3 - x_3 a_2) = 0$

mult. with $a_3 a'$ mult. with $a_1 a$

$$x_1 a_3 (a a' a_2) - x_2 a a' a_1 a_3 = 0$$
$$x_2 a a' a_1 a_3 - x_3 a_1 (a' a_2 a) = 0$$

add

$$x_1 a_3 a a' a_2 - x_3 a_1 a' a_2 a = 0$$
$$\Rightarrow \underbrace{a a' a_2}_{\in A,\text{ since } A \text{ is an m.c.s.}} (x_1 a_3 - x_3 a_1) = 0$$

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

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

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

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

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

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

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

Observe: $\frac{x}{a} = \frac{x'}{a'} \Rightarrow \frac{xb}{ab} = \frac{x'b}{a'b}$. — ① Also, $\underbrace{\frac{y}{b} = \frac{ya}{ab} = \frac{ya'}{a'b}}_{②}$.

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

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

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

add

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

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

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

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

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

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

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

$\Downarrow$

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

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

$$\Downarrow$$

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

as desired.

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

Lecture 15 (17-09)

17 September 2020 11:32 AM

① When is $\frac{x}{a} = 0$ in R_A?

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

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

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

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

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

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

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

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

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

$\supset$? ✓ Yes

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

$\Rightarrow x \in \varphi_A^{-1}(J) = I$

$\Rightarrow \frac{x}{a} = \frac{x}{1}\cdot\frac{1}{a} \in \langle \frac{x}{1} : x \in J \rangle$

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 $I_A = \left\{ \frac{x}{a} \in R_A : \begin{matrix} x \in I \\ a \in A \end{matrix} \right\} \subset R_A$.

② We have shown $I_A = IR_A$.

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

Def^n. 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.

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

These give us many examples.

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

$$\begin{tikzcd} \{\text{some ideals in } R\} \arrow[r, shift right] \arrow[loop below, "?"] & \{\text{ideals in } R_A\} \arrow[l, shift right] \arrow[loop below, "id"] \end{tikzcd}$$

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

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

$\Updownarrow$

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

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

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 $A = \{1, a, a^2, \ldots\}$ is an mcs.
In this case, R_A is denoted by R_a. ↖ 0 isn't here

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

② Let $\mathfrak{p} \in \operatorname{Spec}(R)$. Then, $A = R \setminus \mathfrak{p}$ is an m.c.s.
R_A is denoted $R_\mathfrak{p}$.
↳ R localised at $\mathfrak{p}$.
↳ This turns out to be a local ring.

Note: $\mathbb{Z}_2$ is $\mathbb{Z}[1/2] = \{ m/2^n \in \mathbb{Q} : n \in \mathbb{N} \cup \{0\} \}$.
$\mathbb{Z}_{\langle 2 \rangle} = \{ m/n \in \mathbb{Q} : 2 \nmid n \}$

Primes and Maximal Ideals in R_A.

Q. What can we say about φ_A?

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

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

Converse?

Proof.

Suppose φ_A is not 1-1. Thus, $\exists x \in R \setminus \{0\}$ s.t. $\underset{\substack{\| \\ \underline{x}}}{\varphi_A(x)} = \underset{\substack{\| \\ 0}}{0}$.

$\frac{x}{1} \quad \frac{0}{1}$

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

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

Conversely, if $A \cap Z(R) \neq \phi$, then φ_A is not 1-1.

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 1-1.

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

Eg 3. 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 $Q(R)$).

$\frac{a}{1} \cdot \frac{b}{1} =$

- elements of $R \setminus Z(R)$ become units under φ_A.
- elements of $Z(R) \longrightarrow$?

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

$I \in Spec\, R$.

Moreover, $I_A = IR_A = J$

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

$\hookrightarrow$ contradicts primality

Consider the collection

$$\{ \mathfrak{p}_A : \mathfrak{p} \in Spec(R) \text{ and } \mathfrak{p} \cap A = \phi \}$$

We showed that $\quad Spec(R_A)$ $\cup$

Is this the reverse true? That is, if $\mathfrak{p} \in Spec(R)$, & $\mathfrak{p} \cap A = \phi$ then is $\mathfrak{p}_A \in Spec(R_A)$?

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

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 $z \in \mathfrak{p}$, $c \in A$.

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

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

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

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

$\Rightarrow \frac{x}{a} \in \mathfrak{p}_A$ or $\frac{y}{b} \in \mathfrak{p}_b$. ☺

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

Conclusion: $\operatorname{Spec}(R_A) \longleftrightarrow \{\mathfrak{p} \in \operatorname{Spec}(R) : \mathfrak{p} \cap A = \phi\}$.

Lecture 17 (22-09)

22 September 2020 10:29 AM

Ex. If $\mathfrak{p}_A \in \operatorname{Spec}(R_A)$ and $\frac{x}{a} \in \mathfrak{p}_A$, then $x \in \mathfrak{p}$.

Q. Is the above true if we do not assume $\mathfrak{p}_A$ is prime.

No! Take $R = \mathbb{Z}$, $A = \mathbb{Z} \setminus \{0\}$, $\mathfrak{p} = \langle 2 \rangle$, $\frac{x}{a} = \frac{3}{1}$.

Yesterday, we proved a 1-1 correspondence between

$$\operatorname{Spec}(R_A) \quad \text{and} \quad \{\mathfrak{p} \in \operatorname{Spec}(R) : R \cap A\}.$$

$$\mathfrak{p}_A \longleftarrow\!\shortmid \; \mathfrak{p}$$

$$\mathfrak{q} \longmapsto \varphi_A^{-1}(\mathfrak{q})$$

- We know $\operatorname{Max}(R_A) \subset \operatorname{Spec}(R_A)$.

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

Claim. Let $\Lambda = \{I \subset R : I \text{ is an ideal and } I \cap A = \phi\}$.
The maximal elements of Λ are in one-one correspondence with maximal ideals of R_A.

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

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

$\varphi_A(I) \subset I_A \subset J$

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

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

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

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

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

($\Leftarrow$) Let $J \in Max(R_A)$. We claim that $\varphi_A^{-1}(J)$ is a maximal elt. of Λ.
First note that $\varphi_A^{-1}(J) \cap A = \phi$ since $(\varphi_A^{-1}(J))_A = J \neq R$.

Let $I = \varphi_A^{-1}(J)$. Then, $I \in \Lambda$.
Now, let $I' \in \Lambda$, $I \subset I'$. (Want to prove $I = I'$.)

Observe: $I_A = J$.
Since $I \subset I'$, we have $J = I_A \subset I'_A$.
$I' \in \Lambda \Rightarrow I'_A \neq R_A$
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 Λ.

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

Note Let $p \in Spec(R)$. The $A = R \setminus p$ is an m.c.s.

Moreover Λ as above is $\{I \subset R : I \subset p\}$.
$p \in \Lambda$. Thus, $Max(\Lambda) = \{p\}$. ← exactly one.

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

Q. Find $Max(R_A)$ when $A = R \setminus (p_1 \cup \cdots \cup p_n)$, $p_i \in Spec(R)$.

Lecture 18 (24-09)

24 September 2020 11:24 AM

Universal Property of Localisation

① $(R_A, \varphi_A : R \to R_A)$ is a pair such that R_A is a ring, φ_A is a ring map and $\varphi_A(A) \subset \mathcal{U}(R_A)$.

② Let $(S, \varphi : R \to S)$ be a pair such that S is a ring, φ is a ring map and $\varphi(A) \subset \mathcal{U}(S)$.

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

$$\begin{tikzcd} R \arrow[rr, "\varphi"] \arrow[dr, "\varphi_A"'] & & S \\ & R_A \arrow[ur, dashed, "\tilde{\varphi}"'] & \end{tikzcd}$$

$\exists ! \, \tilde{\varphi} : R_A \to S$ s.t. $\tilde{\varphi} \circ \varphi_A = \varphi$.

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

this makes sense since $\varphi(a) \in \mathcal{U}(S)$

Verify that this is well-defined.

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

Furthermore, assume that $(\bar{R}, \bar{\varphi})$ also satisfies ②, i.e., given (S, φ) as in ②, φ uniquely factors as

$$\begin{tikzcd} R \arrow[rr, "\varphi"] \arrow[dr, "\bar{\varphi}"'] & & S \\ & \bar{R} \arrow[ur, dashed, "\tilde{\varphi}"'] & \end{tikzcd}.$$

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

$$\begin{tikzcd} & \bar{R} \arrow[loop right, "\varphi_1"] \arrow[loop left, "\varphi_2"'] \\ R \arrow[ur, "\bar{\varphi}"] & \end{tikzcd}$$

Using ② & ③ &

$\bar{\varphi}(A) \subset \mathcal{U}(\bar{R})$, $\varphi_A(A) \subset \mathcal{U}(R_A)$,

$$\begin{tikzcd} R \arrow[r, "\bar\varphi"] \arrow[dr, "\varphi_A"'] & \bar R \arrow[d, shift left, "\varphi_2"] \\ & R_A \arrow[u, shift left, "\varphi_1"] \end{tikzcd}$$

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

rewrite

$$\begin{tikzcd} & \bar R \arrow[d, "\varphi_2"] \\ R \arrow[ur, "\bar\varphi"] \arrow[r, "\varphi_A"] \arrow[dr, "\bar\varphi"'] & R_A \arrow[d, "\varphi_1"] \\ & \bar R \end{tikzcd}$$

Both triangles commute and thus,

$$\begin{tikzcd} & \bar R \arrow[dd, "\varphi_1 \circ \varphi_2"] \\ R \arrow[ur, "\bar\varphi"] \arrow[dr, "\bar\varphi"'] \arrow[r, phantom, "\circlearrowright"] & \\ & \bar R \end{tikzcd}$$

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

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

Modules over a ring (possibly non-commutative)

(but soon we'll go to comm.)

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

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

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

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

(left

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

(left modules)

1. $(a+b)\cdot x = a\cdot x + b\cdot x$
2. $(ab)\cdot x = a(b\cdot x)$
3. $a\cdot(x+y) = a\cdot x + a\cdot y$
4. $1\cdot x = x$

for all $x, y \in M$, $a, b \in R$

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

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

$$r\cdot s := \varphi(r)s.$$

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

Q2. Verify if the usual properties hold:

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

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

either one

1. $IR_A = I_A$ → define the two sets and show they are equal
2. $(I \cap J)_A = I_A \cap J_A$ →

Lecture 19 (28-09)

28 September 2020 09:26 AM

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

① $R^{\oplus n}$: multiplication is $a\cdot(r_1, \dots, r_n) = (ar_1, \dots, ar_n)$.
$R^{\oplus n}$ is already a ring. The above can be seen as the product $(a, \dots, a)(r_1, \dots, r_n)$ in $R^{\oplus n}$.

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

③ $R[x]$: $a\cdot(a_0 + a_1x + \dots + a_nx^n) = (a + 0x + \dots + 0x^n)(a_0 + \dots + a_nx^n)$

④ $R[[x]]$: similar

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

Thus, they are all actually R-algebra

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

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

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

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

(Verify that these are indeed ring homomorphisms.)

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

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

Precisely abelian groups.

R-module is abelian group is clear by def^n.

Conversely, let G be an abelian group. Define scalar mult.

$\cdot : \mathbb{Z} \times G \to G$ as

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

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 $\mathbb{k}$, $T: V \to V$ be linear.

Then, V is an R-module as follows: Let $u \in V$

How should we define $x \cdot u$?

Things we want: $x \cdot (u + v) = x \cdot u + x \cdot v$ $\quad u, v \in V$

$x \cdot (au) = (xa) \cdot u = (ax) \cdot u = a \cdot (xu)$ $\quad a \in \mathbb{k} \subseteq \mathbb{k}[x]$

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

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: $(a_0 + a_1 x + \cdots + a_n x^n) \cdot u = a_0 \cdot u + a_1 \cdot Tv + \cdots + a_n T v^n$.

(dot on RHS is the vspace scalar mult.)

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

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

Def^n. ① Let M be an R-module and $N \subset M$. Then N is an R-submodule of M if

(submodule)

ⓐ $0 \in N$,

ⓑ $x, y \in N \Rightarrow x+y \in N$, and

ⓒ $a \in R,\ x \in N \Rightarrow ax \in N$.

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

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

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

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

Given a subset $S \subset M$,

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

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

Lecture 20 (29-09)

29 September 2020 10:21 AM

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

We want a function $R \times M \to M$.
We already have $S \times M \to M$ and $\varphi : R \to S$. This gives

$$\begin{tikzcd} R \times M \arrow[rr, dashed] \arrow[dr, "\varphi \times id_M"'] & & M \\ & S \times M \arrow[ur] & \end{tikzcd}$$

V is a $\mathbb{k}$-vector space, $T : V \to V$ is linear.
V is a $\underbrace{\mathbb{k}[x]}_{=:R}$-module via T.

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 $T(W) \subset W$, i.e., $\forall w \in W$: $T(w) \in W$.)
$\rightsquigarrow$ 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 $p = a_0 + a_1 x + \cdots + a_n x^n$. $n \geq 0$, $a_i \in \mathbb{k}$

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

↳ 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 a non-trivial inv. subspace. Hence, cannot be simple!

---

abelian group to start with

Def^n ① Let $N \subset M$ be a R-module. Then M/N is an

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

(quotient)

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

(Verify this is well defined.)

② Given R-modules M_1, M_2, a function $\varphi: M_1 \to M_2$ 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. $\pi: M \to M/N$ given by $x \mapsto \bar{x}$ is R-linear.

- Given R-linear $\varphi: M_1 \to M_2$ 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.

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

Ex. Let $\mathrm{Hom}_R(M,N) = \{\varphi: M \to N \mid \varphi \text{ is } R\text{-linear}\}$.
Then, $\mathrm{Hom}_R(M,N)$ 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, $\mathrm{Hom}_R(M,N) \subset \mathcal{F}(M,N)$ is an R-submodule.]

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

(put product as composition)

(endomorphisms)

Verification of quotient: First we show $a\cdot\bar{x} = \overline{a\cdot x}$ 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)

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

$\Rightarrow \overline{a\cdot x} = \overline{a\cdot y}$. ✓

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,

$$(a+b)\cdot\bar{x} = \overline{(a+b)\cdot x} = \overline{a\cdot x + b\cdot x}$$
$$= \overline{a\cdot x} + \overline{b\cdot x}$$
$$= a\cdot\bar{x} + b\cdot\bar{x}$$

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

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

$$1\cdot\bar{x} = \overline{1\cdot x} = \bar{x}.$$

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 $B = B_1 \sqcup B_2$ of V.

(Need choice.)

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

$\{ \bar{v} + W : v \in B_2 \}$

Proof. Lin indep:

Suppose $a_1, \ldots, a_n \in \mathbb{k}$ & $v_1, \ldots, v_n \in B_2$

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

$\Rightarrow \overline{a_1 v_1 + \cdots + a_n v_n} = 0$

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

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

$b_i \in \mathbb{F}, \; w_i \in B_1$

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

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

$\therefore$ Lin indep!

Spanning: Let $v \in V$, then $v = \sum a_i v_i + \sum b_j w_j$

$\Rightarrow \bar{v} = \sum a_i \bar{v}_i$ ✓

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

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

If $\varphi, \psi \in \mathrm{End}_R(M)$, then $\varphi \circ \psi$ is also R-linear from $M \circlearrowleft$

Then, $\varphi \circ \psi \in \mathrm{End}_R(M)$.

↖ product.

This is a ring as well as a module.

↳ over R

$[\varphi \circ (\psi_1 + \psi_2)](a) = \varphi[(\psi_1 + \psi_2)(a)]$

$= \varphi[\psi_1(a) + \psi_2(a)]$

$= \varphi(\psi_1(a)) + \varphi(\psi_2(a))$

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

$= [(\varphi \circ \psi_1) + (\varphi \circ \psi_2)](a)$

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

$$\overset{\text{M}}{\parallel} \qquad (\psi_1 + \psi_2) \circ \varphi = \psi_1 \circ \varphi + \psi_2 \circ \varphi.$$

$id = 1.$

Lecture 21 (01-10)

01 October 2020 11:34 AM

Let A be a non-empty set, R a ring. Then, $\mathcal{F}(A, R)$ 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 $\mathcal{F}(A, N)$ is an R-module under pointwise op.

only module! not ring!

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

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

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

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

$\hookrightarrow$ R-linear functions from M to N

Verify: 1. $0 : M \to N$ is R-linear

2. $\varphi_1, \varphi_2 : M \to N$ R-lin $\Rightarrow$ $\varphi_1 + \varphi_2$ is R-linear

3. $a \in R$, $\varphi : M \to N$ R lin $\Rightarrow$ $a\varphi$ is R-linear

Some more observations:

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

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

(endomorphisms)

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

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

Note: ① M is a module over $\mathrm{End}_R(M)$ with "scalar" multiplication given by

$$\forall \varphi \in \mathrm{End}_R(M),\ \forall x \in M, \quad \varphi \cdot x = \varphi(x).$$

(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 $\mu_a : M \to M$ $(x \mapsto ax)$ is a function.
Moreover, this is R-linear. That is, $\mu_a \in \mathrm{End}_R(M)$.
Thus, we get a function

$$\mu : R \to \mathrm{End}_R(M)$$
$$a \mapsto \mu_a.$$

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

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

(Annihilator of M)

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

Eg. ① Let V, W be vector spaces over $\mathbb{k}$. Then, what is $\mathrm{Hom}_{\mathbb{k}}(V,W)$?

Ans: Linear trans. from V to W.

② Let G_1, G_2 be $\mathbb{Z}$-modules. Then

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

③ Let V be a $\mathbb{k}[x]$-module via T.

If $\varphi \in \mathrm{End}_{\mathbb{k}[x]}(V)$, what can you say about φ?

- When will φ be 1-1? onto?
- Is φ $\mathbb{k}$-linear? Yes ✓
- what will $\ker\varphi$ be?
- what relation does φ have with T? $\varphi \circ T = T \circ \varphi$

μ is a ring homo.: To show: $\mu_1 = id$ ✓ true

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

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

Let $x \in M$.

Then, $\mu_{a+b}(x) = (a+b)\cdot x$

$= a\cdot x + b\cdot x$

$= \mu_a(x) + \mu_b(x)$

$= (\mu_a + \mu_b)(x)$ ✓

Let $x \in M$.

$\mu_{ab}(x) = (ab)\cdot x$

$= a\cdot(b\cdot x)$

$= \mu_a(b\cdot x)$

$= \mu_a(\mu_b(x))$

$= (\mu_a \circ \mu_b)(x)$ ✓

Lecture 22 (12-10)

12 October 2020 09:24 AM

Setup. $\varphi : M \longrightarrow N$ 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, $\langle \{x : y \in S\} \cup S' \rangle = M$.

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

Ex. Let $\varphi(M) = \langle z_1, \dots, z_n \rangle^{\subset N}$, $\ker \varphi = \langle x_1, \dots, x_k \rangle^{\subset M}$.

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 $\varphi: M \to N$ be a module homomorphism and $a \in \text{ann}_R(M)$.
Then, $a \cdot \varphi = 0$. $\left((a\cdot\varphi)(m) := a\cdot\varphi(m) \text{ or } a\varphi = \mu_a \circ \varphi.\right)$

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 $\underset{\overset{\shortparallel}{x}}{1\cdot x} = 0 \ \forall x \in M$.

Thus, $M = 0 \iff \text{ann}_R(M) = R.$

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

(faithful module)

More about $\text{End}_R(M)$: ⓪ $\text{End}_R(R) \overset{\text{as rings}}{\cong} R$. (think about 1.)

① $\text{End}_R(M) = 0 \iff M = 0$. $\left(\begin{matrix} x \mapsto 0 \\ x \mapsto x \end{matrix} \text{ are always two endo.s}\right)$

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

(b) N is simple? Either $\varphi = 0$ or φ is onto.
(c) Both are simple? $\varphi = 0$ or bijective.

Thus, if M is simple, then $\mathrm{End}_R(M)$ is a division ring.
Q. Is converse true?

(3) Suppose M is decomposable, i.e., $\exists\ 0 \neq L, N$ submodules s.t.
$$M = L \oplus N.$$

Consider the projections $\pi_1 : M \to M$ (onto L) and $\pi_2 : M \to M$ (onto N).

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

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

$$id_M = \underbrace{\pi_1 + \pi_2}_{\text{complete}}.$$

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

Note: π_1 and π_2 cannot be 0 or id.
Q. Is the converse true?

Note: If $a \in R$ is idemp, then so is $1-a$.
Suppose $\mathrm{End}_R(M)$ has a non-trivial idempotent π,
i.e., $0 \neq \pi \neq 1$, is M decomposable.
Try: Is $M = \operatorname{im} \pi \oplus \ker \pi$?
Yes!
Proof. Claim 1. $\operatorname{im} \pi \cap \ker \pi = 0$.
Proof. Let $a \in$ LHS.
Then, $a = \pi b$ for some $b \in M$ & $\pi a = 0$.
$\Rightarrow \pi^2 b = 0$ but $\pi^2 b = \pi b = a$. $\therefore a = 0$.

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

Proof. Let $a \in M$.

$$a = \underset{\substack{\cap \\ \mathrm{im}\,\pi}}{\pi a} + \underbrace{a - \pi a}_{\substack{\cap \\ \ker \pi}}$$

since $\pi(a - \pi a) = \pi a - \pi^2 a = 0$. $\square$

Note: $\ker \pi \neq 0$ since $x - \pi(x) \in \ker \pi \; \forall x$
& $\exists x$ s.t. $\pi(x) \neq x$. $(\pi \neq \mathrm{id})$

$\mathrm{im}\, \pi \neq 0$ since $\pi \neq 0$.

Lecture 24 (15-10)

15 October 2020 11:41 AM

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

Thus, R is decomposable as an R-module $\iff$ R has non-trivial idemps.

i.e. $\exists$ non-zero ideals $I, J \subset R$ s.t. $I \oplus J = R$
thus, comaximal

$\iff \exists$ rings $R_1, R_2 \neq 0$ 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 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 $I \subset \mathrm{ann}_R(M)$.
(and makes it a module)

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

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

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

(And we know vector spaces.)

will be useful in local rings (Nakayema Lemma)

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

$$\begin{tikzcd} R \times M \arrow[d, "\varphi \times \mathrm{id}_M"'] \arrow[dr] & \\ R/I \times M \arrow[r, dashed] & M \end{tikzcd}$$

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:

$$\begin{tikzcd} R \times M \arrow[d, "\varphi_A \times \mathrm{id}_M"'] \arrow[dr] & \\ R_A \times M \arrow[r, dashed] & M \end{tikzcd}$$

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

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 $\Leftrightarrow I \subset \mathrm{ann}_R(M)$
  $\Leftrightarrow \forall a \in I, \ \mu_a = 0$

- M is R_A-module $\Leftrightarrow \forall a \in A, \ \mu_a$ is an isomorphism
  (Verify!)

(Recall: $\mu_a : M \to M$ 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 R_A.

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

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

$$(x, a) \sim (y, b) \quad \text{iff}$$

$\exists c \in A$ s.t. $c(bx - ay) = 0$.

$\sim$ is then an equiv. rel^n. 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:

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

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

$$\begin{tikzcd} R \times M_A \arrow[r] \arrow[d] & M_A \\ R_A \times M_A \arrow[ur, dashed] & \end{tikzcd}$$

We have an R-linear map

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

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

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

φ_A is injective $\Leftrightarrow Z_R(M) \cap A = \phi$

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

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

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

$(\Rightarrow)$ obvious

$(\Leftarrow)$ Take $a = a_1 \cdots a_n \in A$.
Let $x \in M$. Then, $x = r_1 x_1 + \cdots + r_n x_n$; $r_i \in R$.
Then, $ax = 0$.

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

$\Leftrightarrow \operatorname{ann}_R(M) \cap A \neq \phi$

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

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

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

$\Updownarrow$ $\forall \mathfrak{p} \in \operatorname{Spec}(R)$ $M_{\mathfrak{p}} = 0$ (M_A with $A = R \setminus \mathfrak{p}$)

$$\Updownarrow \; \forall \mathfrak{p} \in \operatorname{Spec}(R), \; M_{\mathfrak{p}} = 0 \qquad (M_A \text{ with } A = R \setminus \mathfrak{p})$$

$$\Updownarrow \; \forall \mathfrak{m} \in \operatorname{Max}(R), \; M_{\mathfrak{m}} = 0$$

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

$$\forall \mathfrak{m} \in \operatorname{Max}(R), \; M_{\mathfrak{m}} = 0 \Rightarrow M = 0. \qquad \text{(Local-Global principle)}$$

(Local-Global principle)

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

Recall: $M_{\mathfrak{m}} = 0 \Leftrightarrow \forall x \in M, \exists a \notin \mathfrak{m} \; (a \cdot x = 0)$

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

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

$1 \cdot x \neq 0 \Rightarrow 1 \notin I \Rightarrow I \subsetneq M$.

Thus, $\exists \mathfrak{m} \in \operatorname{Max}(R)$ s.t. $\underbrace{I}_{\operatorname{ann}_R(x)} \subset \mathfrak{m}$.

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

(Proof. $\frac{x}{1} = 0 \Rightarrow a \cdot x = 0$ for some $a \in A = R \setminus \mathfrak{m}$

$\Rightarrow \operatorname{ann}_R(x) \cap (R \setminus \mathfrak{m}) \neq \phi$

$\Rightarrow \operatorname{ann}_R(x) \not\subset \mathfrak{m} \quad \rightarrow\leftarrow$)

R_A-submodules of M_A: Given $N \overset{\text{submod.}}{\leq} M$, N_A is an R_A-module.

Then, $N_A \hookrightarrow M_A$ as a submodule and

$N_A = \langle \varphi_A(x) : x \in N \rangle$.

Furthermore, $(M/N)_A \cong M_A / N_A$.

Lecture 26 (27-10)

27 October 2020 10:20 AM

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

$$\begin{tikzcd} & L+N \arrow[dl, dash] \arrow[dr, dash] & \\ L \arrow[dr, dash] & & N \arrow[dl, dash] \\ & L \cap N & \end{tikzcd} \qquad \frac{L+N}{L} \simeq \frac{N}{L\cap N}$$

$L+N$ is the smallest submodule containing L and N.
$L \cap N$ is the largest submodule contained in L and N.

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

If it is surjective with kernel $L\cap N$, we are done.

If L and N are f.g., then so is $L+N$.
$L = \langle l_1, \dots, l_m \rangle$, $N = \langle n_1, \dots, n_k \rangle \Rightarrow L+N = \langle l_1, \dots, l_m, n_1, \dots, n_k \rangle$

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., $\varphi : M \to M'$ 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 $\varphi : M \to M'$ 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,

$$x_1 = a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n$$
$$x_2 = a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \qquad \text{for } a_{ij} \in I$$
$$\vdots$$
$$x_n = a_{n1}x_1 + \cdots + a_{nn}x_n$$

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

Draw conclusion! Get something that annihilates M.

Put $\quad B = A - I \quad$ and $\quad x = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$.

Then, $\quad Bx = 0_{n \times 1}$

$\Rightarrow \quad (\operatorname{adj} B) B x = 0$

$\Rightarrow \quad (\det B) x = 0$

$\Rightarrow \quad (\det B) x_i = 0 \quad \forall\, i$

$\Rightarrow \quad \det B \in \operatorname{ann}_R(M)$

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. $1+a \in \mathrm{ann}_R(M)$.

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

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

1. If we know $\mathrm{ann}_R(M) = 0$ (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 $1+a \in \mathcal{U}(R)$, 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 $1+a \notin$ any ideal, then $1+a \in \mathcal{U}(R)$.)

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

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

($M/IM = 0 \Leftrightarrow M = IM$ 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.
($\subseteq$) Let $\bar{x} \in M/N$. $\quad x = n + (i_1 m_1 + \cdots + i_k m_k) \quad$ ($\because M = N + IM$)
$\bar{x} = i_1 \bar{m}_1 + \cdots + i_k \bar{m}_k \in I(M/N)$.

Obs. Suppose $M = \langle x_1, \ldots, x_n \rangle$, $I \subset R$ is an ideal.
Then $M/IM = \langle \bar{x}_1, \ldots, \bar{x}_n \rangle$.

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

(No! Counter example?)

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

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

$$M/IM = \langle \bar{x}_1, \ldots, \bar{x}_n \rangle,$$

then $M = \langle x_1, \ldots, x_n \rangle$.

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

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

$$M = \langle x_1, \ldots, x_n \rangle \iff \underbrace{M/\mathfrak{m}M}_{\text{This is a vector space over } R/\mathfrak{m}\text{! Can talk about bases!!}} = \langle x_1 + \mathfrak{m}M, \ldots, x_n + \mathfrak{m}N \rangle.$$

Ex) ① $x_1, \ldots, x_n$ is a minimal (in terms of inclusion) generating set of M $\iff$ $\{\bar{x}_1, \ldots, \bar{x}_n\}$ 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^n. (free module) An R-module which admits a basis is called a free R-module.

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

Remark: $(0, \ldots, 0)$ 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 $x_1, \ldots, x_n$. Then, the set of relations on $(x_1, \ldots, x_n)$ forms a submodule of $R^{\oplus n}$.

What's the next best thing to hope for?

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

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

(Non-) Examples of Free Modules

① $R^{\oplus n}$ is a free R-module with basis $\{e_1, \ldots, e_n\}$.
($e_i = (0, \ldots, 1, \ldots, 0)$) $\uparrow$ ith place

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 $\{E_{ij} \mid 1 \le i, j \le n\}$.
In general, $M_{n \times m}(R)$ works.

(4) An ideal which is not principal is not free.
(Any two element in a ring are indep.)

(5) If $0 \subsetneq I \subsetneq R$, 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. Any field.

Ex. Find a ring which does not have IBN.

Remark Every commutative ring has the IBN property.

Def^n. (Rank) Let R be commutative, M is a free R-module. Then $\mathrm{rank}_R(M)$ is the cardinality of any basis of M.

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

(Assuming Choice, ofc)

Lecture 29 (03-11)

03 November 2020 10:31 AM

Prop^n 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

Let $\bar{x}_1, \ldots, \bar{x}_n \in \bar{B}$ (be distinct) and $(\bar{a}_1, \ldots, \bar{a}_n) \in (R/I)^{\oplus n}$ be s.t.
$$\bar{a}_1 \bar{x}_1 + \cdots + \bar{a}_n \bar{x}_n = 0 \qquad (\text{in } M/IM \text{ as } R/I\text{-mod})$$
$$\Rightarrow \quad a_1 x_1 + \cdots + a_n x_n \in IM \qquad (\text{in } M \text{ as } R\text{-mod})$$

Thus, there exist $b_1, \ldots, b_m \in I$, $y_1, \ldots, y_m \in B$ s.t.
$$a_1 x_1 + \cdots + a_n x_n = b_1 y_1 + \cdots + b_m y_m$$

Since B is a basis and both sides above represent the same element. Thus, $m = n$, an
$$\{x_1, \ldots, x_n\} = \{y_1, \ldots, y_n\} \text{ with}$$
$$\{a_1, \ldots, a_n\} = \{b_1, \ldots, b_n\}. \text{ Thus,}$$
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 $\pi: M \to M/IM$.

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

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

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

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

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

$x - y \in IM$

$\Rightarrow x - y = b_1 z_1 + \dots + b_n z_n$ $\quad$ $b_i \in I$, $z_i \in B$, distinct

$z_i = x$, $z_j = y$, $b_i = 1$, $b_j = -1$ 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, $\mathrm{Max}(R) \neq \phi$. Pick $m \in \mathrm{Max}(R)$.

Then, $m \subsetneq R$.

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/m-bases for M/mM.

Since m is maximal, R/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 ϕ. ∎

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 $(F(A), \iota : A \to F(A))$ where $F(A)$ is an R-mod,

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

$$\begin{tikzcd} & F(A) \arrow[d, dashed, "\tilde{f}"] \\ A \arrow[ur, "e"] \arrow[r, "f"'] & M \end{tikzcd}$$

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
$\varphi : F \to F'$ s.t.

$$\begin{tikzcd} & F \arrow[d, dashed, "\varphi"] \\ A \arrow[ur, "e"] \arrow[r, "e'"'] & F' \end{tikzcd}$$

commutes.

Similarly, $\exists$ R-lin. $\psi : F' \to F$ s.t.
$$\begin{tikzcd} & F' \arrow[d, dashed, "\psi"] \\ A \arrow[ur, "e'"] \arrow[r, "e"'] & F \end{tikzcd}$$

Thus,
$$\begin{tikzcd} & F \arrow[d, "\psi \circ \varphi"] \\ A \arrow[ur, "e"] \arrow[r, "e"'] & F \end{tikzcd}$$
but
$$\begin{tikzcd} & F \arrow[d, dashed, "id_F"] \\ A \arrow[ur, "e"] \arrow[r, "e"'] & F \end{tikzcd}$$

Thus, uniqueness forces $\psi \circ \varphi = id_F$.
Similarly, $\varphi \circ \psi = id_{F'}$.
Thus, φ and ψ are isomorphisms! $\square$

Existence! (Idea: Construct a free R-module with basis A.)

Given A, and $a \in A$, consider the function
$e_a : A \to R$ defined as

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

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

This is precisely the set of functions in $\mathcal{F}(A, R)$

which take all but finitely many points of A to 0.
Denote this by $\mathcal{F}_0(A, R)$.

(Ex. verify that
$\langle e_a \mid a \in A \rangle = \mathcal{F}_0(A, R)$ is actually true.)

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

In particular, $\mathcal{F}_0(A, R)$ is a submodule of $\mathcal{F}(A, R)$.
Verify that $\{e_a \mid a \in A\}$ is linearly independent.

Thus, $\{e_a\}$ is a basis for $\mathcal{F}_0(A, R)$. (Generating by construction.)

Define $e: A \hookrightarrow \mathcal{F}_0(A, R)$ as $a \mapsto e_a$.
(Note e is 1-1.)

Thus, we may identify $a \in A$ with $e_a \in \mathcal{F}_0(A, R)$.

What remains: $(\mathcal{F}_0(A, R), e)$ satisfies the UMP

(Ex!
Writing assⁿ.
'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.

$$\begin{tikzcd} A \arrow[r, "e_1"] \arrow[d, shift right, "f"'] & F(A) \arrow[loop right, "id_{F(A)}"] \arrow[d, dashed, shift right, "\varphi"'] \\ B \arrow[r, "e_2"'] \arrow[u, shift right, "f^{-1}"'] & F(B) \arrow[u, dashed, shift right, "\psi"'] \end{tikzcd} \qquad \begin{tikzcd} & F(A) \arrow[d, bend right, "\psi\circ\varphi"'] \arrow[d, phantom, "="] \arrow[d, bend left, "id_{F(A)}"] \\ A \arrow[ur, "e_1"] \arrow[dr, "e_1"'] & \\ & F(A) \end{tikzcd}$$

$$\begin{tikzcd} A \arrow[r, "e_1"] \arrow[d, "f"'] \arrow[dr, phantom, "\circlearrowright"] & F(A) \arrow[d, "\varphi"] \\ B \arrow[r, "e_2"] \arrow[d, "f^{-1}"'] \arrow[dr, phantom, "\circlearrowright"] & F(B) \arrow[d, "\psi"] \\ A \arrow[r, "e_1"'] & F(A) \end{tikzcd} \qquad \begin{tikzcd} A \arrow[r, "e_1"] \arrow[d, "id_A"'] \arrow[dr, phantom, "\circlearrowright"] & F(A) \arrow[d, "\psi\circ\varphi"] \\ A \arrow[r, "e_1"'] & F(A) \end{tikzcd}$$

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.)

Proofs

Two ways: ① Let $i : A \hookrightarrow M$ be incl. Then, we get a R-lin. map $\tilde{i}$ as:

$$\begin{tikzcd} A \arrow[r, "e"] \arrow[dr, "i"'] & F(A) \arrow[d, dashed, "\tilde{i}"] \\ & M \end{tikzcd}$$

using UMP of $F(A)$.

Show $\tilde{i}$ 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 $\varphi : R \longrightarrow M$ by extending $1 \longmapsto x$.

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

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

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

Thus, $M \simeq R/\operatorname{ann}_R(x)$. ← 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 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. $\operatorname{ann}_R(x) \subset \operatorname{ann}_R(y)$ should be true.

② Suppose $M = \langle x, y \rangle$.

As earlier, we get an onto R-linear map $\varphi : R^2 \longrightarrow M$ by sending

$$e_1 \longmapsto x$$
$$e_2 \longmapsto y$$

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

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

Thus, $M \simeq R^{\oplus 2}/\ker \varphi$.

ⓝ If $M = \langle x_1, \ldots, x_n \rangle$, then $M \simeq R^{\oplus n}/I$ for some submodule $I \subset R^{\oplus n}$.

↳ all relati… $(x_1, \ldots, x_n)$

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

submodule $I \subset R^{\oplus n}$.
↳ all relations on $(x_1, \dots, x_n)$

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

(∞) General case: Let M be an R-module. Then, $\exists$ a free R-module F and an onto R-linear map $\varphi: F \to M$. In particular, M is a quotient of F.

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

$\varphi: F(M) \twoheadrightarrow M$ as $e_x \mapsto x$ works.

Observation: If $M = \langle S \rangle$ for some $S \subset M$, 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, $M = \langle (\bar{1}, \bar{0}), (\bar{0}, \bar{1}) \rangle$, $x = (\bar{1}, \bar{0})$, $y = (\bar{0}, \bar{1})$

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

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

$u = (2,0)$, $v = (0,3)$

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

$\psi: \mathbb{Z}^{\oplus 2} \to \ker \varphi$
$f_1 \mapsto u$
$f_2 \mapsto v$

Ψ 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, $\ker \varphi$ is free

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

More general: Let M be an R-module. Then $\exists$ free R-mod. F_0 mapping onto M (via φ_0). Let $K_0 = \ker(\varphi_0)$.

$\Big($ $\overset{\shortparallel}{\text{set}}$ of relations on a suitable gen. set of M $\Big)$

Note that K_0 is again an R-module.
Let F_1 be a free R-mod. mapping onto K_0 via φ_1 with $\ker(\varphi_1) = K_1$

$$\begin{tikzcd}
& K_1 \arrow[dr] & & & & \\
F_2 \arrow[ur, "\varphi_2"] \arrow[rr, dashed, "\varphi_2"'] & & F_1 \arrow[rr, dashed, "\varphi_1"] \arrow[dr, "\varphi_1"'] & & F_0 \arrow[r, "\varphi_0"] & M \\
K_2 \arrow[u] & & & K_0 \arrow[ur] & &
\end{tikzcd}$$

$\Big\{$ the blue arrows are named by abuse of not. $\Big\}$

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

$$M \xleftarrow{\varphi_0} F_0 \xleftarrow{\varphi_1} F_1 \xleftarrow{\varphi_2} F_2 \leftarrow \cdots$$ where

φ_0 is onto and $\forall i \geq 1$, $\operatorname{im}(\varphi_i) = \ker(\varphi_{i-1})$.

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

Q. Does this process stop? $\leftarrow$ bad question, we could choose

F_0 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_0 to be of finite rank.

② K_0 may not be f.g. even if F_0 has finite rank.

Def^n. If M is f.g., $F_0 \xrightarrow{\varphi} M$, 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

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

φ_0 is onto and $\operatorname{im}(\varphi_1) = \ker(\varphi_0)$.

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 φ_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 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/6\mathbb{Z}$.

I. F I.C

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

find a diff pres. matrix

③ If $(v_1, \dots, v_m)$ is a basis of F_1, so are $(v_2, v_1, \dots, v_m)$, $(v_1 + v_2, v_2, \dots, v_m)$, $(cv_1, v_2, \dots, v_m)$ where $c \in \mathcal{U}(R)$.

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 $\tilde{f} : \mathcal{F}_0(A,R) \longrightarrow M$.
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 $\{e_a\}_{a \in A}$ 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 $\varphi_1 = r_1 e_{a_1} + \dots + r_n e_{a_n}$,

$\varphi_2 = s_1 e_{a_1} + \dots + s_n e_{a_n}$. (Yes, same $a_1, \dots, a_n$.)

(r_i, s_i are allowed to be 0.)

Now, $\tilde{f}(r\varphi_1 + \varphi_2)$

$= \tilde{f}\left((rr_1 + s_1) e_{a_1} + \dots + (rr_n + s_n) e_{a_n} \right)$

$= (rr_1 + s_1) f(a_1) + \dots + (rr_n + s_n) f(a_n)$

$= r \tilde{f}(\varphi_1) + \tilde{f}(\varphi_2)$

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

$(\tilde{g} \circ e)(a) = \tilde{g}(e_a) = f(a) \quad \forall a \in A. \quad (*)$

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

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

Then, $\tilde{f}(\varphi) = r_1 f(a_1) + \cdots + r_n f(a_n)$ (def^n of $\tilde{f}$)

$\tilde{g}(\varphi) = r_1 \tilde{g}(e_{a_1}) + \cdots + r_n \tilde{g}(e_{a_n})$ (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 $i \in \Gamma$, $\pi_i : P \to M_i$ is R-linear such that the following holds:

Given any $(M, \{\varphi_i\}_{i \in \Gamma})$ where is an R-module and $\varphi_i : M \longrightarrow M_i$ is R-linear for all $i \in \Gamma$, there exists a unique R-linear map $\tilde{\varphi} : M \to P$ s.t.

$$\begin{tikzcd} & P \arrow[d, "\pi_i"] \\ M \arrow[ur, dashed, "\tilde{\varphi}"] \arrow[r] & M_i \end{tikzcd}$$

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^n 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

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

$$f : P \longrightarrow \overset{\text{disjoint union}}{\bigsqcup} M_i \quad \text{s.t.}$$
$$f(i) \in M_i \qquad \text{for all } i \in M.$$

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

Lecture 33 (10-11)

10 November 2020 10:27 AM

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

$$P = \{ f : P \longrightarrow \bigsqcup_{i\in\Gamma} M_i \mid f(i) \in M_i \ \forall i \in \Gamma\}$$

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 co-ordinate notation. We're adding & mult. co-ordinate wise.)

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

$$\pi_i : P \longrightarrow M_i \quad \text{given by}$$
$$f \mapsto f(i).$$

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

called the projection onto the i^{th} co-ordinate

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

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

Suppose M is an R-module and $\forall i \in \Gamma$, $\varphi_i : M \longrightarrow M_i$ is R-lin.
We want to construct a (unique) R-linear

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

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

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

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

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

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

$$\begin{tikzcd} & P \arrow[d, phantom, "\circlearrowleft"] \arrow[dr, "\pi_i"] & \\ M \arrow[ur, "\tilde{\varphi}"] \arrow[rr, "\varphi_i"'] & & M_i \end{tikzcd}$$

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

$\psi : M \to P$ 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 from Γ which agree on Γ. Thus, $\psi(x) = \tilde{\varphi}(x)$.

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

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

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

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

Given any $(M, (\varphi_i)_{i\in\Gamma})$, M an R-module, $\varphi_i : M_i \to M$ R-linear for all $i \in \Gamma$, there exists a unique R-linear $\tilde{\varphi} : S \to M$ s.t.

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

for all $i \in \Gamma$.

$$\begin{tikzcd} & S \arrow[d, dashed, "\tilde{\varphi}"] \\ M_i \arrow[ur, "\epsilon_i"] \arrow[r, "\varphi_i"'] \arrow[ur, phantom, shift right=3, "\circlearrowleft"] & M \end{tikzcd}$$

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 $j \in \Gamma$: Consider the natural $\epsilon_j : M_j \longrightarrow P$ defined by $\epsilon_j(x_j) = x$ where $x \in P$ is

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

i_j is R-linear.

Let $S = \langle \epsilon_j(M_j) : j \in \Gamma \rangle$ (all except j^{th} coordinate is zero)

$$= \{ x \in P \mid x_j = 0 \text{ for all but finitely many } j \in \Gamma \}.$$

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 φ.)

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 $M \otimes N \to L$.)

Lecture 34 (12-11)

12 November 2020 11:32 AM

Def^n. (Tensor product) Given R-modules M and N, a tensor product of M and N over R is a pair (T, θ) where
- T is an R module and
- $\theta : M \times N \to T$ is R-bilinear, satisfying :

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

$$\begin{tikzcd} M \times N \arrow[r, "\theta"] \arrow[dr, "\varphi"'] & T \arrow[d, dashed, "\tilde{\varphi}"] \arrow[d, phantom, "?" near start, shift right=3ex] \\ & L \end{tikzcd}$$

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

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

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

Scalar mult. of any ring : $\cdot : R \times R \to R$

Similarly $\cdot : R \times M \to M$

$R[x] \times R[y] \longrightarrow R \qquad (f, g) \longmapsto f(0) \cdot g(0)$

$M_{m \times n}(R) \times M_{n \times p}(R) \longrightarrow M_{m \times p}(R), \qquad (A, B) \longmapsto AB$

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

Q. What is "the" tensor product of $\mathbb{Q}[x]$ and $\mathbb{Q}[y]$ over $\mathbb{Q}$?
haven't proven this yet

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

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

We also had $R[x] \times R[y] \longrightarrow R$ earlier.
Is R the tensor product? Is $R[x, y]$?

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

Q. We also saw $R \times M \to M$ 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 $M \times N \xrightarrow{\varphi} L$, we want an R-mod T & R-bi map $M \times N \xrightarrow{\theta} T$, an R-lin. map $\tilde{\varphi} : T \to L$ satisfying some conditions.

(Improper because it looks like (T, θ) depends on (L, φ))

$$\begin{tikzcd} M \times N \arrow[r, dashed, "\theta"] \arrow[dr, "\varphi"'] & T \arrow[d, dashed, "\tilde{\varphi}"] \\ & L \end{tikzcd}$$

Denote $\theta(x, y)$ by $\langle x, y \rangle$. We want
$\langle x, y \rangle + \langle x', y \rangle = \langle x + x', y \rangle$, $\quad a\langle x, y \rangle = \langle ax, y \rangle$
$\langle x, y \rangle + \langle x, y' \rangle = \langle x, y + y' \rangle \qquad\qquad = \langle x, ay \rangle.$

Thus, we want $\langle x, y \rangle + \langle x', y \rangle - \langle x + x', y \rangle = 0, \ldots$
Quotient!
↳ But on what module?
On $M \times N$ with usual operations? Nah!
↳ This already has relations

Actual Construct

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

these are all relations we want. To go mod, we need the submod.

- $e_{(x_1+x_2,\, y)} - e_{(x_1,\, y)} - e_{(x_2,\, y)}$
- $e_{(x,\, y_1+y_2)} - e_{(x,\, y_1)} - e_{(x,\, y_2)}$
- $e_{(ax,\, y)} - a e_{(x,y)}$
- $e_{(x,\, ay)} - a e_{(x,y)}$

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

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

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

this was just a set map

$$\begin{tikzcd} M \times N \arrow[r, "e"] \arrow[rr, bend right, "\theta"'] & F \arrow[r, "\pi"] & T \end{tikzcd}$$

Is θ bilinear?

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

Note that e is just a function!

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

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

$\Rightarrow \pi(e_{(x_1+x_2,\, y)}) = \pi(e_{(x_1,y)} + e_{(x_2,y)})$
$= \pi(e_{(x_1,y)}) + \pi(e_{(x_2,y)})$

$$= x_1 \otimes y + x_2 \otimes y$$
$$= \theta(x_1, y) + \theta(x_2, y)$$

Similarly the other relations in G give us

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

$= x \otimes (ay)$

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:

$$\begin{tikzcd}
 & F(M \times N) \arrow[dr, "\pi"] & \\
M \times N \arrow[ur, "e"] \arrow[rr, dashed, "\theta = \pi \circ e"] \arrow[dr, "\varphi"'] & & T = F/G \arrow[dl, dashed, "\exists! \tilde{\varphi}"] \\
 & L &
\end{tikzcd}$$

Constructing $\tilde{\varphi}$:

We would like $\tilde{\varphi}(x \otimes y) = \varphi(x,y)$, $\tilde{\varphi}(\sum x_i \otimes y_i) = \sum \varphi(x_i, y_i)$

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

Note that φ is a function. Thus, by the Univ. property of F (on the set $M \times N$), $\exists!\ \bar{\varphi} : F \to L$ R-linear

$\bar{\varphi}(e_{(x,y)}) = \varphi(x,y)$

$$\begin{tikzcd}
 & F \arrow[dr, "\pi"] \arrow[dd, dashed, "\bar{\varphi}"] & \\
\varphi \arrow[ur, "e"] \arrow[dr, "\varphi"'] & & T \arrow[dl, dashed] \\
 & L &
\end{tikzcd}$$

We have R-linear $\bar{\varphi} : F \to L$.

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

What do we need?

(universal) property of kernels

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

This is true because φ is R-bilinear!

Take any one of the four type of gen. of G. for example: $z = e(x, y_1+y_2) - e(x,y_1) - e(x,y_2)$

$$\bar{\varphi}(z) = \bar{\varphi}(\quad - \quad - \quad)$$

$$= \bar{\varphi}(\quad) - \bar{\varphi}(\quad) - \bar{\varphi}(\quad)$$ ∵ $\bar{\varphi}$ is additive

$$= \varphi(x, y_1+y_2) - \varphi(x,y_1) - \varphi(x,y_2)$$ defⁿ of $\bar{\varphi}$ on basis

$$= 0$$ R-bilinear

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

Thus, we have

$$\begin{tikzcd} & F \arrow[dr, dashed] \arrow[dd, dashed] & \\ M \times N \arrow[ur] \arrow[rr] \arrow[dr] & & T \arrow[dl] \\ & L & \end{tikzcd}$$

The red triangle commutes too now. (Check!)

use that the other triangles do.

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

Claim. Suppose $\exists\, \psi : T \to L$ 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 $\{x \otimes y\}_{x \in M, y \in N}$ generates T, we are done!

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

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

What does this tell us about x_is and y_is?

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!

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

$x = 2, \quad y = \bar{1}.$

Then, $x \neq 0$ & $y \neq 0$. But
$$x \otimes y = 2 \otimes \bar{1} = (2\cdot 1)\otimes \bar{1} = 2\cdot(1\otimes\bar{1}) = 1\otimes(2\cdot\bar{1}) = 0$$

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

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

② What is $R \otimes M$?

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

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

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

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

Proof. Let's try Strat. 1!

Note that M is an R-module and
$$\theta : R \times M \to M, \quad (r, m) \mapsto r\cdot m$$
is bilinear.

Given a pair (N, ψ), $\psi : R \times M \to N$ R-bilin., we want to show existence of a unique R-linear $\tilde{\psi} : M \to N$ s.t. $\tilde{\psi}\theta = \psi$.

$$\begin{tikzcd} R\times M \arrow[r, "\theta"] \arrow[dr, "\psi"'] & M \arrow[d, dashed, "\tilde{\psi}"] \\ & N \end{tikzcd}$$
$(a, x) \mapsto ax$

(keep picture in mind)

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

Verify it's linear.

Also, $\tilde{\psi} \circ \theta(a, x) = \tilde{\psi}(ax) = \psi(1, ax) = \psi(a, x)$ bil.

The uniqueness is clear since $\tilde{\psi}(x) = \tilde{\psi}\,\theta(1, x) = \psi(x)$ 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 $\theta : R/I \times M \to M/IM$ as

$(\bar{a}, x) \mapsto \overline{ax}$.

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

Eg. $R[x] \otimes_R R[y] \cong R[x,y]$

Define $\theta : R[x] \times R[y] \to R[x,y]$. θ is bilin.

$(f, g) \mapsto f \cdot g$

Suppose (M, φ) is a pair, $M \to$ R-mod, $\varphi : R[x] \times R[y] \to M$
R-bilinear

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

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

$$\begin{tikzcd} R[x] \times R[y] \arrow[r, "\theta"] \arrow[dr, "\varphi"'] & R[x,y] \arrow[d, dashed, "\tilde{\varphi}"] \\ & M \end{tikzcd}$$

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

Examples.

① $M \otimes_R N \simeq N \otimes_R M$

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

$$\begin{array}{ccccc} M \times N & \longrightarrow & N \times M & \xrightarrow{\otimes} & N \otimes_R M \\ (x, y) & \longmapsto & (y, x) & \longmapsto & y \otimes x \end{array}$$

This is bilinear

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

$$\begin{array}{ccc} L \times (M \oplus N) & \longrightarrow & (L \times M) \oplus (L \times N) \\ (x, (y, z)) & \longmapsto & ((x, y), (x, z)) \end{array}$$

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

$$\begin{array}{ccc} L \times (M \times N) & \longrightarrow & (L \times M) \times N \\ (x, (y, z)) & \longmapsto & ((x, y), z) \end{array}$$

Modules over a PID:

Recall. $M = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \overset{\varphi}{\twoheadleftarrow} \underbrace{\mathbb{Z}e_1 \oplus \mathbb{Z}e_2}_{F}$

$$(\bar{1}, 0) \longleftarrow e_1$$
$$(0, \bar{1}) \longleftarrow e_2$$

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

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

lin indep.

Thus, K is free.

Map $\mathbb{Z} f_1 \oplus \mathbb{Z} f_2 \overset{\psi}{\twoheadrightarrow} K$

$$f_1 \longmapsto 2e_1$$
$$f_2 \longmapsto 3e_2$$

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

$$G \xrightarrow{\psi} F \twoheadrightarrow M \quad \text{where}$$

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

Note that $M \cong \mathbb{Z}/6\mathbb{Z}$.
How can we write $\mathbb{Z}/6\mathbb{Z}$ as a quotient of F?

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 a gen. of $\mathbb{Z}/2 \times \mathbb{Z}/3$

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

$$G \cong \mathbb{Z}^r \oplus \mathbb{Z}/p_1^{i_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_n^{i_n}\mathbb{Z}$$

where p_is are prime.

Thm. (Structure theorem)

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

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

where each p_i is prime.
(Elementary divisor form)

Proof. We first show: (Decomposition theorem)
$\exists\, a_1, \ldots, a_n \in R$ 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 $a_i \notin \mathcal{U}(R)$.
can chuck $R/\langle a_i \rangle \cong 0$
can absorb in R^s

Suppose a is a non-zero non-unit.
Then $0 \subsetneq \langle a \rangle \subsetneq R$. Then $\exists$ primes $p_1, \ldots, p_r$

s.t.

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

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

Then,

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

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. $\{a_1 y_1, \dots, a_n y_n\}$ 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, $K = \langle a_1 y_1, \dots, a_n y_n \rangle$ where $\{y_1, \dots, y_m\}$ is a basis of F and $\{a_1 y_1, \dots, a_n y_n\}$ 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 th^m.

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

- $\text{rank}_R(F) = 1$, then $F \xrightarrow[\varphi]{\sim} R$ and $I \overset{\varphi}{\leftarrow} K$ 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 π_i be the i^{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, $\pi_1(K)$ is a non-zero ideal in R.

Thus, $\pi_1(K) = \langle a \rangle$ for some $a \in R\setminus\{0\}$.

Let $x \in K$ be such that $\pi_1(x) = a$.

Let $y \in K$. Then $\pi_1(y) = b\,\pi_1(x)$ for some $b \in R$.

($\because \pi_1(K) = \langle \pi_1(x) \rangle$.)

$\Rightarrow y - bx \in (\ker \pi_1) \cap K$

$\Rightarrow y = bx + (\text{something})$

$\Rightarrow K = Rx + (\ker \pi_1 \cap K)$.

Is it a direct sum?

Let $y \in Rx \cap (\ker \pi_1 \cap K)$.

$\Rightarrow y = bx$ for some $b \in R$,

$\pi_1(y) = 0$.

$\hookrightarrow \pi_1(bx) = 0 \Rightarrow ba = 0 \xRightarrow{a \neq 0,\ \text{in an ID}} b = 0$.

$\therefore y = 0$ and $K = Rx \oplus (\ker \pi_1 \cap K)$

By induction,

$\ker \pi_1 \cap K$ is free of rank at most $m-1$, (since $\ker \pi_1 \cap K \leq \ker \pi_1$ is free with rank $m-1$.)

say with basis $x_2, \dots, x_n$.

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

This proves ① and ②.

Proof of ③:

ⓐ Let $\Lambda = \{ \varphi(K) \mid \varphi \in \mathrm{Hom}_R(F, R) \}$

$\langle 0 \rangle \in \Lambda$. ($R \in \Lambda$ if $F \neq 0$.)

$\Lambda \neq \phi$. Λ 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, $I_j = I \in \Lambda$.

Thus, by Zorn's Lemma, Λ has a maximal element, say $\varphi_0(k) = \langle a_0 \rangle$.

Lecture 38 (19-11)

19 November 2020 11:18

Recall: $R \leftarrow$ PID

$F \leftarrow$ free R-module

3 $0 \neq K \subseteq F$ submodule

To show: $\exists$ a basis $\{y_1, \ldots, y_m\}$ of F, $\exists a_1, \ldots, a_n \in R$ s.t. $\{a_1 y_1, \ldots, a_n y_n\}$ is a basis of K. ($n \leq m$)

Had shown: K is free, has finite rank, $\mathrm{rank}_R(K) \leq m$.

(a) The collection of ideals

$$\Lambda = \{\varphi(K) \mid \varphi \in \mathrm{Hom}_R(F, R)\}$$

has a maximal element, say $\varphi_0(K) = \langle a_0 \rangle$.

Note that $a_0 \neq 0$ since $\pi_i(K) \neq 0$ for some i.

(Thus, $a_0 \mid \varphi_0(x) \quad \forall x \in K$.)

(b) $\forall \varphi \in \mathrm{Hom}_R(F, R)$, $\varphi(x_0) \in \langle a_0 \rangle$, where $x_0 \in K$ is s.t. $\varphi_0(x_0) = a_0$

Proof: Let $\varphi(x_0) = b$ and $d = \gcd(a_0, b)$.

Then, $\exists r, s \in R$ s.t.

$ra_0 + sb = d$.

Consider $\psi = r\varphi_0 + s\varphi$.

Thus, $\psi(x_0) = d$.

$\Rightarrow \psi(K) \supset \langle d \rangle \supset \langle a_0 \rangle$.

By maximality of $\langle a_0 \rangle$ in Λ, we get $\langle a_0 \rangle = \langle d \rangle$ or $a_0 \mid d$ and hence, $\boxed{a_0 \mid b}$.

This tells us that $\varphi_0(x_0) \mid \varphi(x_0)\ \forall \varphi \in \mathrm{Hom}$.

(c) $\exists y_0 \in F$ such that $a_0 y_0 = x_0$.
(and hence, $\varphi_0(y_0) = 1$)

Let $\{e_1, \dots, e_m\}$ be a basis of F.
$x_0 = \alpha_1 e_1 + \dots + \alpha_m e_m$ for $\alpha_i \in R$.
$\pi_i(x_0) = \alpha_i$. Also, $\pi_i \in \mathrm{Hom}_R(F, R)$
$\Rightarrow a_0 \mid \alpha_i$. (by (b))
Thus, $\exists \beta_1, \dots, \beta_m$ s.t. $a_0 \beta_i = \alpha_i\ \forall i$.
Put $y_0 = \beta_1 e_1 + \dots + \beta_m e_m$. (*)

Thus, $\varphi_0(a_0 y_0) = \varphi_0(x_0) = a_0$
$$\varphi_0(a_0 y_0) = a_0 \cdot \varphi_0(y_0)$$

$\Rightarrow a_0 \cdot \varphi_0(y_0) = a_0$ in an ID with $a_0 \neq 0$

$\Rightarrow \varphi_0(y_0) = 1$.

This also gives us that $\varphi_0(e_1), \dots, \varphi_0(e_m)$ have $\gcd = 1$. (Apply φ_0 to (*).)

(d) (i) $F = Ry_0 \oplus \ker \varphi_0$ and

(ii) $K = Rx_0 \oplus (\ker \varphi_0 \cap K)$.

Proof (i) Let $y \in F$. Put $r = \varphi_0(y)$. Then,

$$y = \underbrace{r y_0}_{\in Ry_0} + \underbrace{(y - r y_0)}_{\in \ker \varphi_0 \text{ since } \varphi_0(y_0) = 1}.$$

$\cup$ $\quad$ $\Cap$ $\cup$ $\quad$ $\Cap$

Ry_0 $\quad$ $\ker \varphi_0$ since $\varphi_0(y_0) = 1$

Easy to check that $Ry_0 \cap \ker \varphi_0 = 0$.
Thus,
$$F = Ry_0 \oplus \ker \varphi_0.$$

(ii) Similar argument as above.

(e) Now we use induction to prove (3).

Suppose $m = 1$. Then, (3) is true since R is a P.I.D. Assume $m > 1$. Then, $\ker \varphi_0$ is a free module (from (1) & (2)) of rank $= m-1$ (by (d) and IBN of R).

By induction, $\ker \varphi_0$ has a basis $\{y_2, \ldots, y_m\}$ with $a_2, \ldots, a_n \in R$ $(n \leq m)$ s.t. $\{a_2 y_2, \ldots, a_n y_n\}$ is a basis for $\ker \varphi_0 \cap K$.

Verify that $\{y_0, y_2, \ldots, y_m\}$ is a basis of F and $\{a_0 y_0, a_2 y_2, \ldots, a_m y_m\}$ of K.

To summarise:

If M is a f.g. R-module, then we have the following:
Write $M = \langle x_1, \ldots, x_m \rangle$. Suppose the relations on the x_is are given by
$$a_{11} x_1 + \cdots + a_{m1} x_m = 0$$
$$\vdots$$
$$a_{n1} x_1 + \cdots + a_{mn} x_m = 0$$

Let $F = Re_1 \oplus \cdots \oplus Re_m$. Map F onto M as $e_i \mapsto x_i$.

Then, $\ker \varphi = \left\langle \begin{bmatrix} a_{11} \\ \vdots \\ a_{m1} \end{bmatrix}, \ldots, \begin{bmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{bmatrix} \right\rangle = K.$

(K being finitely generated is by Noetherian property.
Freeness is what we really needed.
Both are implied by submodule theorem.)

Then, $M \cong F/K$.

By the submodule theorem, $\exists$ a basis $\{y_1, \ldots, y_m\}$ of F and $a_1, \ldots, a_n \in R$ s.t.

$K = \langle a_1 y_1, \ldots, a_n y_n \rangle$. Thus, in this new basis,

$$K = \left\langle \begin{bmatrix} a_1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \ldots \begin{bmatrix} 0 \\ \vdots \\ 0 \\ a_n \\ 0 \\ \vdots \\ 0 \end{bmatrix} \right\rangle.$$

Conclusion $M \cong \dfrac{F}{K} = \dfrac{Ry_1 \oplus Ry_2 \oplus \cdots \oplus Ry_m}{Ra_1y_1 \oplus \cdots \oplus Ra_ny_n \oplus 0 \oplus \cdots \oplus 0}$

$$\cong R/\langle a_1 \rangle \oplus \cdots \oplus R/\langle a_n \rangle \oplus R^{m-n}$$