Lecture 8 (01-09)

01 September 2020 10:29 AM

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

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

called the prime spectrum of R.

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

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

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

Okay, assume $R \neq 0$.

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

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

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

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

② Λ is a poset by $\subseteq$.

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

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

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

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

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

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

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

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

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

WLOG ↗

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

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

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

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

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

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

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

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

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

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

Corollaries: ($R \neq 0$)

① Every proper ideal is contained in a maximal ideal.

② Let $a \in R$. Then,

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

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

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

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

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

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

Max ideals are prime

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

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

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

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

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

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

$\Rightarrow mb + rab = b$

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

$\therefore b \in m$.

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

Proof of Cor.

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

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

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

(2) Let $a \in R$.

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

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

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

$\Leftrightarrow$

a is cont. in a max ideal

Lecture 9 (03-09)

03 September 2020 11:27 AM

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

Also, 0 is not an integral domain.

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

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

Comm:

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

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

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

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

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

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

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

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

Jacobson radical

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

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

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

Max. ideals are prime

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

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

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

↳ any equality?

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

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

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

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

Does this converse hold now?

Yes!

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

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

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

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

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

$\Rightarrow 1 + ra$ is a unit.

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

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

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

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

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

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

Thus, our assumption was incorrect. In other words,

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

Thus, $a \in J(R)$. ☺

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

Sol^n: Disproof: We construct a counterexample.

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

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

↳ maximal!

Thus, $J(R) = \{0,2\} \neq \{0\}$. ☹

(Prime ideal Exercise solution)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Leads to the following defn.

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

Co-maximal, comaximal ideals

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

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

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

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

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

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

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

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

$= (\bar{a}, \bar{b})$. ∎

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

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

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

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

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

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

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

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

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

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

↓

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

↳ Such a ring is called **local.**

↳ Notation: $(R, \mathfrak{y})$.

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

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

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

Choose two distinct maximal ideals!

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

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

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

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

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

↳ often called the "diagonal map"

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

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

↑ j^{th} pos.

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

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

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

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

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

Lecture 11 (08-09)

08 September 2020 10:29 AM

Recall the following q.

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

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

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

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

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

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

Proof. Same as above.

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

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

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

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

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

We can now prove the result by induction.

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

Base: $n = 2$ done.

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

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

Assume claim for now.

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

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

Moreover, this iso was induced by φ.

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

Using this, we get that

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

is onto.

Now, we prove the claim.

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

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

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

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

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

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

Thus, we have proved the Chinese Remainder Theorem.

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

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

Then,

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

Note that we also proved:

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

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

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

Prime Ideals.

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

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

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

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

Claim. $A \subset B$.

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

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

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

Consider the collection

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

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

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

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

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

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

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

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

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

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

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

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

↳ Now what?

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

To be continued...

Lecture 12 (10-09)

10 September 2020 11:14 AM

Changing the prev. proof.

Consider the collection

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

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

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

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

(still goes through)

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

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

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

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

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

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

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

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

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

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

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

Thus, we have proven.

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

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

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

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

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

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

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

Prime Avoidance

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

Nope!

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

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

Still nope!

Ex. Find a counterexample.

However, the statement is true for prime ideals.

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

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

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

We prove $n \geq 3$ by induction.

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

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

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

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

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

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

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

Counter example for non-prime ideals.

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

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

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

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

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

Lecture 13 (14-09)

14 September 2020 09:35 AM

Thm. (Prime avoidance)

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

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

Proof. $n=1$. Nothing.

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

Then, $a_1 + a_2 \in I$.

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

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

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

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

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

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

here is where we used primality

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

Let $b \in I$ be defined as

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

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

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

Proof. We phrase the theorem as follows:

Let $n \geq 2$.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Lecture 14 (15-09)

15 September 2020 10:32 AM

Localisation : Create "more" units

E.g. $R = \mathbb{Z}[1/2] = \left\{ \frac{m}{2^k} : m \in \mathbb{Z},\ k \in \mathbb{N} \cup \{0\} \right\} \hookrightarrow \mathbb{Z}$ → ring containing $\mathbb{Z}$ as a subring

Observed that 2 is a unit in R.

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

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

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

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

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

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

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

Expect : $\mathbb{Q}$

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

③ $R = \mathbb{Z}$. Invert 2.

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

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

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

↑ set exclusion

↑ set exclusion

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

↓ recall

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

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

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

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

① $\forall a, b \in A$: $a, b \in A$

② $1 \in A$

③ $0 \notin A$

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

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

2) Define a relation on $R \times A$ as

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

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

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

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

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

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

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

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

Solutions.

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

Sol'n: Reflexive (a=1) and symm. (same a) is clear.

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

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

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

mult. with $a_3 a$

mult. with $a_2 a'$

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

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

add

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

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

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

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

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

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

$\frac{x}{a} = \frac{x'}{a'}$ $\qquad b \in A$

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

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

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

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

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

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

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

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

add

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

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

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

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

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

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

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

$\Downarrow$

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

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

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

as desired.

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

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

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

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

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

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

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

(2) We have shown $I_A = IR_A$.

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

(Extension ideal)

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

$$\{\text{some ideals in } R\} \rightleftarrows \{\text{ideals in } R_A\}$$

$\{\text{some ideals in } R\} \to \{\text{ideals in } R_A\}$: ? ↷

$\{\text{ideals in } R_A\} \to \{\text{some ideals in } R\}$: ↷ id

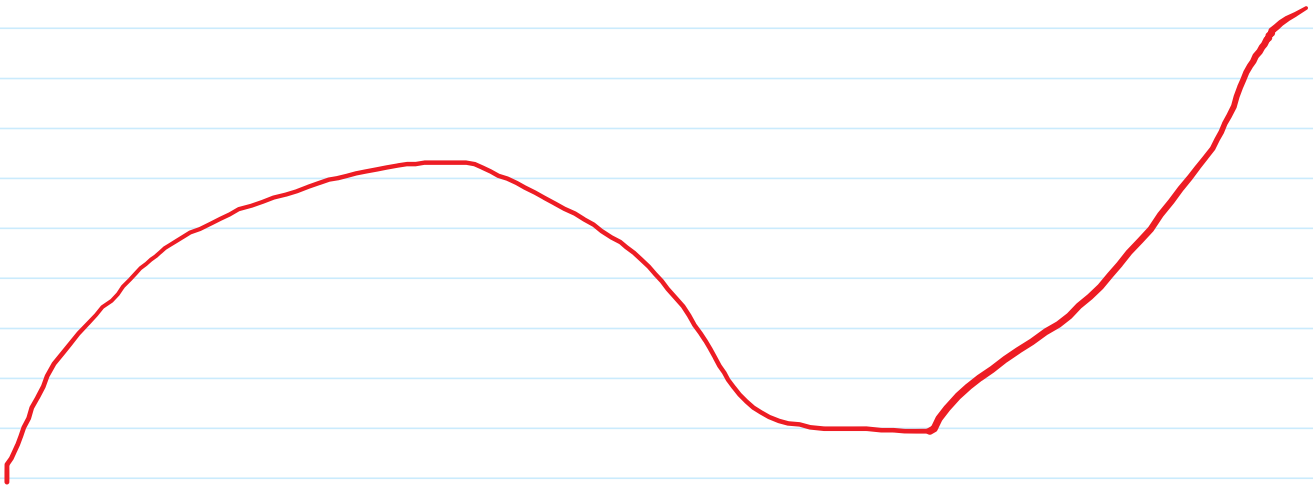
Q. a) When is $I_A = 0$? $\quad I_A = 0 \Leftrightarrow \forall x \in I\ (\exists a \in A\ (ax = 0))$

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 $\mathrm{Spec}(R_A)$ and $\mathrm{Max}(R_A)$?



Lecture 16 (21-09)

21 September 2020 09:27 AM

Some examples of m.c.s.:

① Let $a \in R \setminus N(R)$. Then $A = \{1, a, a^2, \dots\}$ is an 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 $p \in \operatorname{Spec}(R)$. Then, $A = R \setminus p$ is an m.c.s.
R_A is denoted R_p.
↳ R localised at 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. $\varphi_A(x) = 0$.
$\varphi_A(x) = \frac{x}{1}$ and $0 = \frac{0}{1}$

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

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

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

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: 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 $Q(R)$).

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

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

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

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

Moreover, $I_A = IR_A = J$

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

↳ contradicts primality

Consider the collection

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

We showed that $\text{Spec}(R_A)$ //

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

(Note: If $\mathfrak{p} \cap A = \emptyset$, 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: $\operatorname{Spec}(R_A) \longleftrightarrow \{\mathfrak{p} \in \operatorname{Spec}(R) : \mathfrak{p} \cap A = \emptyset\}$.

Lecture 17 (22-09)

22 September 2020 10:29 AM

Ex. If $\mathfrak{p}_A \in \mathrm{Spec}(R_A)$ 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

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

$\mathfrak{p}_A \longleftarrow \mathfrak{p}$

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

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

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

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

Proof. ($\to$) Let $I \in \Lambda$ be maximal. We want to prove: $I_A \in \mathrm{Max}(R_A)$.
Let $I_A \subset J \subsetneq R_A$. (We want to prove $I_A = J$.)

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

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

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

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

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

($\leftarrow$) Let $J \in \text{Max}(R_A)$. 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, ($\rightarrow$) & ($\leftarrow$) prove the corresponding since composition in both directions is id.

Note Let $p \in \text{Spec}(R)$. 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, $\text{Max}(\Lambda) = \{p\}$.
↖ exactly one.

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

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

Lecture 18 (24-09)

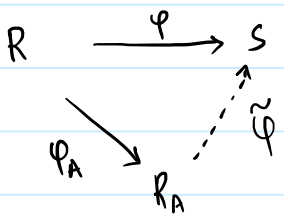
24 September 2020 11:24 AM

Universal Property of Localisation

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

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

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



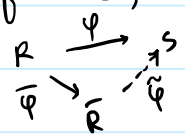
$\exists ! \tilde{\varphi} : R_A \to S$ s.t. $\tilde{\varphi} \circ \varphi_A = \varphi$.

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

↑ this makes sense since $\varphi(a) \in U(S)$

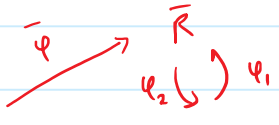
↑ Verify that this is well-defined.

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. $\bar{\varphi}(R) \subset U(\bar{R})$.

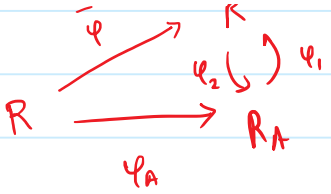
Furthermore, assume that $(\bar{R}, \bar{\varphi})$ also satisfies ②, i.e., given (S, φ) as in ②, φ factors as 

uniquely

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

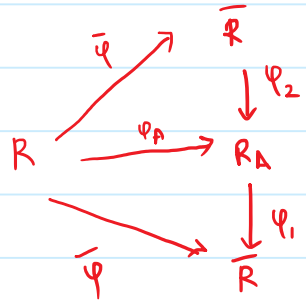


Using ② & ③ & $\bar{\varphi}(A) \subset U(\bar{R})$, $\varphi_A(A) \subset U(R_A)$,

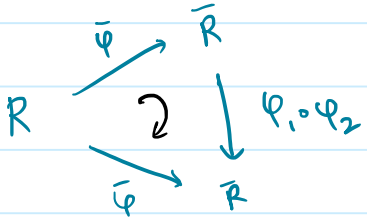


$\bar{\varphi}(A) \subset \mathcal{U}(\bar{R})$, $\varphi_A(A) \subset \mathcal{U}(R_A)$,
we get φ_1 & φ_2 as shown.

rewrite



Both triangles commute and thus,



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 (module $\mathbb{Z}$ not being a field.)

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

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

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 $R[x]$: $a \cdot (a_0 + a_1 x + \dots + a_n x^n) = (a + 0x + \dots + 0x^n)(a_0 + \dots + a_n x^n)$

④ $R[[x]]$: similar

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

Thus, they are all actually R-algebra

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

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 $\Bbbk$ be a field. What are $\Bbbk$-modules?
Precisely $\Bbbk$-vector spaces.

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

Precisely abelian groups.

R-module is abelian group is clear by defn.

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

$\cdot : \mathbb{Z} \times G \to G$ 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 $R = k[x]$, V a vector space over 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: $X \cdot (u+v) = X \cdot u + X \cdot v$ $\quad u, v \in V$

$X \cdot (au) = (Xa) \cdot u = (aX) \cdot u = a \cdot (Xu)$ $\quad a \in k \subset k[x]$

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

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

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

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

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

(dot on RHS is the vspace scalar mult.)

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

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

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

ⓐ $0 \in N$,

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

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

(submodule)

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

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

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

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

Given a subset $S \subset M$,

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

(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

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

M is indecomposable otherwise. (indecomposable)

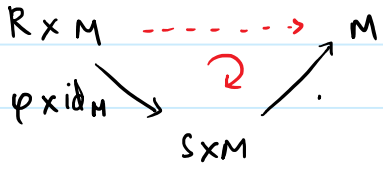
Q. What are $\mathbb{k}$-submodules of V? $\mathbb{k}[x]$-submodules of V (via T)?
What are $\mathbb{Z}$-submodules of an abelian group G?
What are submodules of a ring R?
If M is an S-module, $\varphi: R \to S$ is a ring map, then M is an R-module. (via φ)

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



V is a k-vector space, $T: V \to V$ is linear.
V is a $k[x]$-module via T.
(!! R)

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., $\forall w \in W: T(w) \in W$.)
↳ 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.: $\forall p \in k[x], u \in W (p \cdot u \in W)$

Let $p \in k[x]$ and $u \in W$ be arbitrary.
Write $p = a_0 + a_1 x + \cdots + a_n x^n$. $n \geq 0$, $a_i \in k$

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

↳ think of this as the function which is multiplication by a_0

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

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 $k[x]$ module, W_1 & W_2 have to be T-inv.

Q. When is V simple as a $k[x]$ 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!

Defn ① Let $N \subset M$ be a R-module. Then M/N is an (abelian group to start with) ...

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

(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

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

(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 $N_1 \subset M$, $N_2 \subset M_2$, 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 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.

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

Proof. Lin indep:

Suppose $a_1, \dots, a_n \in k$ & $v_1, \dots, v_n \in B_2$ are s.t. $a_1 \bar{v}_1 + \dots + a_n \bar{v}_n = 0$.

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

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

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

$b_i \in F$, $v_i \in B_1$

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 $M \to M$

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

↑ product.

This is a ring as well as a module (over R).

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

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

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

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

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

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

$\Uparrow$

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

$id = 1.$

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!

$\forall f, g \in \mathcal{F}(A, N)$ $\forall r \in R$, we define

$(f+g)(a) = f(a) + g(a)$,

$(r \cdot f)(a) = r \cdot (f(a))$.

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

↳ 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 $\mathrm{id}: M \to M$ is R-linear

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

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 $\ker \mu$.

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

ideal

(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

$\mathrm{Hom}_{\mathbb{Z}}(G_1, G_2)$ = 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: $\mu_1 = \mathrm{id}$ ✓ 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, $\langle \{x : y \in S\} \cup S' \rangle = M$.

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

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

Take $y_1, \dots, y_n \in^{CM}$ 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 $a \in \operatorname{ann}_R(M)$. 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, $a \in \operatorname{ann}_R(\operatorname{Hom}_R(M,N))$. In other words

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

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

Therefore,

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

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

② If $M = 0$ module, then $\operatorname{ann}_R(M) = R$.
Conversely, if $\operatorname{ann}_R(M) = R$, then $1\cdot x = 0 \ \forall x \in M$.
(1 · x = x)

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

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

(faithful module)

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

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

② What can we say about $\varphi \in \operatorname{Hom}_R(M,N)$ 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).

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

$\pi_i^2 = \pi_i$ (idempotent) & $\pi_i \pi_j = 0$ $(i \neq j)$ (orthogonal)

$\mathrm{id}_M = \pi_1 + \pi_2$. (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 $M = \mathrm{im}\ \pi \oplus \ker \pi$?

Yes!

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

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. $\mathrm{im}\ \pi + \ker \pi = M$.

Proof. Let $a \in M$.

$$a = \underbrace{\pi a}_{\in \operatorname{im}\pi} + \underbrace{a - \pi a}_{\in \ker\pi \text{ since } \pi(a-\pi a) = \pi a - \pi^2 a = 0.}$$

□

Note: $\ker \pi \neq 0$ since $x - \pi(x) \in \ker \pi \ \forall x$ & $\exists x$ s.t. $\pi(x) = x$. $(\pi \neq 0)$

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

Lecture 24 (15-10)

15 October 2020 11:41 AM

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

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

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

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

Q. ① How are I & J related to R_1 and R_2?

② If $R \cong R_1 \times R_2$, identifying R_1 with $R_1 \times \{0\}$, is it an ideal or subring of R?

Other constructions

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

We would 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 $I \subset \mathrm{ann}_R(M/IM)$.)

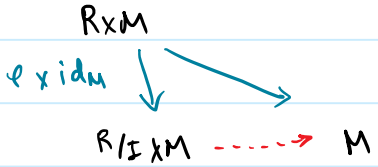
Also note: if $I \subset \operatorname{ann}_R(M)$, then $IM = 0$ & thus, $M/IM = M/0 \cong M$.

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

(And we know vector spaces.)

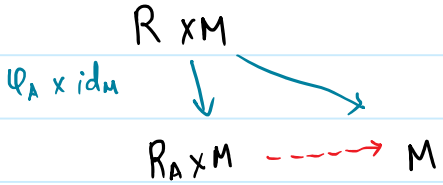
↳ will be useful in local rings (Nakayema Lemma)

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



(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:



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 $\Leftrightarrow$ $I \subset \text{ann}_R(M)$
  $\Leftrightarrow \forall a \in I,\ \mu_a = 0$
- M is R_A-module $\Leftrightarrow \forall a \in A,$ μ_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

$(x, a) \sim (y, b)$ iff

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

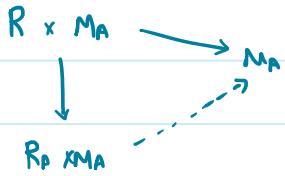
$\sim$ is then an equiv. rel^n. Define $\frac{x}{a} := [(x, a)]$.

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.



We have an R-linear map

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

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 $\Leftrightarrow Z_R(M) \cap A = \emptyset$

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

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

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

[$\Rightarrow$ 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, $ax = 0$.]

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

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

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

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

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

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

$\Leftrightarrow \forall\, \mathfrak{p} \in \mathrm{Spec}(R),\ M_{\mathfrak{p}} = 0$ (M_A with $A = R/\mathfrak{p}$)

$\Leftrightarrow \forall\, \mathfrak{m} \in \mathrm{Max}(R),\ M_{\mathfrak{m}} = 0$

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

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

Proof. We show: $M \neq 0 \Rightarrow \exists\, \mathfrak{m} \in \mathrm{Max}(R)$ 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 $I = \mathrm{ann}_R(x)$.

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

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

($I = \mathrm{ann}_R(x)$)

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

(Proof. $\frac{x}{1} = 0 \Rightarrow a \cdot x = 0$ for some $a \in A = R/\mathfrak{m}$
$\Rightarrow \mathrm{ann}_R(x) \cap (R/\mathfrak{m}) \neq \emptyset$
$\Rightarrow \mathrm{ann}_R(x) \not\subset \mathfrak{m}$ $\rightarrow\leftarrow$)

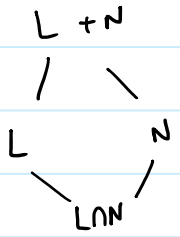
R_A-submodules of M_A: Given $N \overset{\text{submod.}}{\leq} M$, N_A is an R_A-module.
Then, $N_A \hookrightarrow M_A$ as a submodule and
$N_A = \langle \varphi_A(x) : x \in N \rangle$.

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



$$\frac{L+N}{L} \simeq \frac{N}{L \cap N}$$

$L+N$ 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,

$$x_1 = a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n$$
$$x_2 = a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n$$
$$\vdots$$
$$x_n = a_{n1}x_1 + \cdots + a_{nn}x_n$$

for $a_{ij} \in I$

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

Draw conclusion! Get something that annihilates M.

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

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

$\Rightarrow (\text{adj } B)BX = 0$

$\Rightarrow (\det B)X = 0$

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

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

Lecture 27 (29-10)

29 October 2020 11:34 AM

Same notation from earlier:

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

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

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

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

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

1. If we know $\operatorname{ann}_R(M) = 0$ (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 $1+a \in V(R)$, then $M = 0$. (Nakayama Lemma) (NAK)

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

3. If $(R, \mathfrak{m})$ is local, M f.g., $IM = M$ for a proper ideal $I \subsetneq R$, then $M = 0$.

   (If $a \in I$, then $1+a \notin \mathfrak{m}$, then $1+a \notin$ any ideal, then $1+a \in V(R)$.)

   (Recall Global-Local which said that if $M_{\mathfrak{m}} = 0 \ \forall \mathfrak{m} \in \operatorname{Max}(R)$, 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: $\frac{M}{N} = I\left(M/N\right)$, then we are done by 2.

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

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)
$\Rightarrow M = IM + \langle x_1, \ldots, x_n \rangle$ (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

$$M = \langle x_1, \ldots, x_n \rangle \Leftrightarrow M/\mathfrak{m}M = \langle x_1 + \mathfrak{m}M, \ldots, x_n + \mathfrak{m}N \rangle.$$

↓

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

Can talk about bases!!

Ex) ① $x_1, \ldots, x_n$ is a minimal (in terms of inclusion) generating set of M $\Leftrightarrow$ $\{\bar{x}_1, \ldots, \bar{x}_n\}$ 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

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

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

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

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

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

What's the next best thing to hope for?

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

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

(Non-) Examples of Free Modules

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

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

0 is free with empty basis.

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

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 elements 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.

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

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

(Assuming Choice, of c)

Lecture 29 (03-11)

03 November 2020 10:31 AM

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

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

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

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

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

Proof. ① Generating

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

Linear independence (be distinct)

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

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

$$\Rightarrow \quad a_1x_1 + \cdots + a_nx_n \in IM \quad \text{(in } M \text{ as } R\text{-mod)}$$

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

$$a_1x_1 + \cdots + a_nx_n = b_1y_1 + \cdots + b_my_m$$

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

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

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

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

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

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

(for $x, y \in B$)

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

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

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

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

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

$x - y \in IM$

$\Rightarrow x - y = b_1 z_1 + \cdots + b_n z_n$ $\quad b_i \in I$, $z_i \in B$, 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, $\text{Max}(R) \neq \emptyset$. Pick $m \in \text{Max}(R)$.

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, $|B_1| = |B_2|$.

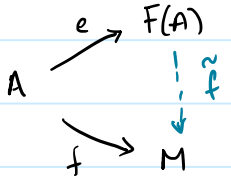
If $R = 0$, then $M = 0$ and the only basis is $\emptyset$. ∎

Universal property of free R modules

Let R be a ring.

Defn. Let A be a non-empty set. A free module on the set A is a pair $(F(A), e: A \to F(A))$ 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



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