

$$\int (\cos^5 x) dx$$

MA 839

## Advanced Commutative Algebra

---

Notes By: Aryaman Maithani

Spring 2020-21

## A Quick Intro.

**Setup:** A ring is commutative with 1.

Let  $M$  be an  $R$ -module.

**Observation:** ① If  $M$  is cyclic, (say  $M = \langle x \rangle = \{ax : a \in R\}$ ),  
we get an  $R$ -linear map  $R \rightarrow M$  which is onto.  
 $a \mapsto ax$

Then,  $M \cong R/I$  where  $I$  is the kernel.  
In this case,  $I = \text{ann}_R(x)$ .

Thus, if  $M$  is cyclic, then  $M$  is a quotient of  $R$ .

② Suppose  $\exists x, y \in M$  s.t.  $M = \langle x, y \rangle = \{ax + by \mid a, b \in R\}$ .  
 $= \{ax + by \mid (a, b) \in R^{\oplus 2}\}$

Then, we get an onto  $R$ -linear map  $R \oplus R \xrightarrow{\varphi} M$   
 $e_1 \mapsto x$   
 $e_2 \mapsto y$  } extend this  
 $\{e_1, e_2\}$  is a basis  
→ this lets us extend the map

In particular,  $M \cong R^2 / \ker \varphi$ .

Q. Is it necessary that we can actually write

$$M \cong \frac{R}{\langle \rangle} \oplus \frac{R}{\langle \rangle} ?$$

This has a positive answer: ①  $R$  is a field  
②  $R$  is a PID

**CAUTION:** We won't include fields as PID.  
That is, when we say "PID", we exclude fields.

③ Suppose  $M$  is a finitely generated (f.g.)  $R$ -module.

(That is, suppose  $M = \langle x_1, \dots, x_n \rangle$ .)

Then,  $M$  is a quotient of  $R^{\oplus n}$ .  
→  $R^n$

Then,  $M$  is a quotient of  $R^n$ .

way to get this

Define  $R^n \xrightarrow{\varphi} M$  by  $e_i \mapsto x_i$ .

$$M \cong R / \ker \varphi.$$

④ In general, consider a free module with " $M$  as basis", call it  $F(M)$ . Then  $F(M)$  maps onto  $M$ .

Slightly more general: If  $A \subset M$  is a generating set, i.e.,  $M = \langle A \rangle$ ,

then  $F(A)$  maps onto  $M$ .

Thus,  $M$  can be written as a quotient of a free-module.

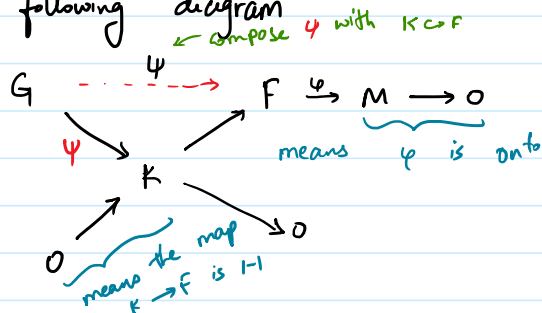
To Summarise: If  $M$  is an  $R$ -module, then  $M$  can be written as a quotient of a free  $R$ -module. Moreover, if  $M$  is fg, then the free module can be assumed to have finite rank.

Free resolution of  $M$  (over  $R$ ):

Let  $F$  be a free  $R$ -module mapping onto  $M$  with kernel  $K$ . That is,  $\varphi: F \rightarrow M$  is onto  $R$ -linear and  $\ker \varphi = K$ .

Now,  $\exists$  a free  $R$ -module  $G$  and an onto map  $\psi: G \rightarrow K$

We capture this in the following diagram



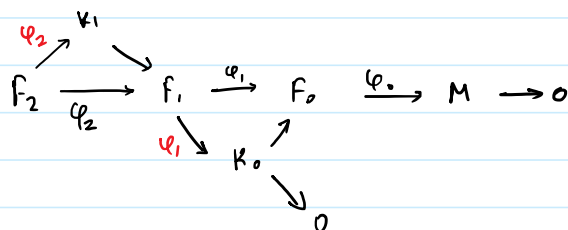
Note that  $\text{im } \psi = K = \ker \varphi$ .

Thus, we have  $G \xrightarrow{\psi} F \xrightarrow{\varphi} M \rightarrow 0$ .

- ①  $\varphi$  is onto and  $\ker \varphi = \text{im } \psi$ .
- ②  $G$  and  $F$  are free  $R$ -modules.

Note that we can repeat the above process with  $K$  instead of  $F$ .

Change notation:  $F_0 := F$ ,  $F_1 := G$ ,  $K_0 := K$ ,  $\varphi_0 := \varphi$ ,  $\varphi_1 := \psi$ .



Thus, we get free modules  $\{F_n, \varphi_n: F_n \rightarrow F_{n-1}\}$  such that  $\ker \varphi_{n-1} = \text{im } \varphi_n$  written as

$$\dots \rightarrow F_n \xrightarrow{\varphi_n} F_{n-1} \xrightarrow{\varphi_{n-1}} \dots \rightarrow F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \rightarrow 0$$

$F_i$ s are free,  $\varphi_0$  is onto &  $\ker \varphi_{n-1} = \text{im } \varphi_n$ ,  $n \geq 1$

Often, we drop the 'n' and call

$$F: \dots \rightarrow F_n \xrightarrow{\varphi_n} F_{n-1} \rightarrow \dots \rightarrow F_1 \xrightarrow{\varphi_1} F_0 \rightarrow 0 \text{ as an}$$

$R$  free resolution of  $M$ .

$\text{im } \varphi_1 = K$ , this is not exact here.  
 $\varphi_1$  not onto (rec.)

Q: ① If  $M$  is f.g.:

Can we get  $F_i$ s so that  $\text{rank}(F_i) < \infty \forall i$ .

② If yes, are  $\text{rank}(F_i)$ s independent of construction?

③ Can you describe the maps?

④ Give explicit bases for  $F_i$ s s.t. the maps are "described nicely".

Q: If two modules have "isomorphic" free resolutions, are they isomorphic?

$$\begin{array}{ccccccc}
 \dots & \xrightarrow{\varphi_3} & F_2 & \xrightarrow{\varphi_2} & F_1 & \xrightarrow{\varphi_1} & F_0 \rightarrow 0 \\
 & & \downarrow \varphi_2' & & \downarrow \varphi_1' & & \downarrow \varphi_0' \\
 \dots & \xrightarrow{\varphi_3'} & F_2' & \xrightarrow{\varphi_2'} & F_1' & \xrightarrow{\varphi_1'} & F_0' \rightarrow 0
 \end{array}$$

$$M \cong F_0 / \text{im } \varphi_1$$

$$M' \cong F_0' / \text{im } \varphi_1'$$

$$\varphi_1' \varphi_1 = \varphi_0 \varphi_1 \quad (*)$$

Claim.  $\gamma_0(\text{im } \varphi_1) = \text{im } \varphi'_1$

( $\subseteq$ ) clear by (\*)

( $\supseteq$ ) clear again since  $\varphi'_1 = \gamma_0 \varphi_1 \gamma_1^{-1}$

$$\text{Thus, } M_0 \cong \frac{F_0}{\text{im } \varphi_0} \cong \frac{\varphi_0(F_0)}{\varphi_0(\text{im } \varphi)} = \frac{F_0'}{\text{im } \varphi'_1} \cong M'_0$$

# Lecture 1 (11-01-2021)

11 January 2021 11:07

## Free modules:

As usual :  $R$  is a (commutative) ring (with 1).  
 $M$  is an  $R$ -module.

Def<sup>n</sup>. ① Let  $A \subset M$ .  $A$  is said to be a **generating set** of  $M$  (as an  $R$ -module) if  
 $\forall x \in M, \exists x_1, \dots, x_n \in A$  and  $(a_1, \dots, a_n) \in R^n$  s.t.  
 $x = a_1 x_1 + \dots + a_n x_n$ .

(Note that  $A$  need not be finite.)

Notation :  $M = \langle A \rangle$

If  $A = \{x_1, \dots, x_n\}$  is finite, then  $M = \langle x_1, \dots, x_n \rangle$   
and  $M$  is said to be **finitely generated**.

②ⓐ Let  $x_1, \dots, x_n \in M$ . We say  $\{x_1, \dots, x_n\}$  is **linearly independent** (over  $R$ ) if for  $(a_1, \dots, a_n) \in R^n$ ,

$$a_1 x_1 + \dots + a_n x_n = 0 \Rightarrow (a_1, \dots, a_n) = 0 \text{ in } R^n.$$

ⓑ A subset  $A \subset M$  is **linearly independent** <sup>(over  $R$ )</sup> if every finite subset of  $A$  is linearly independent <sub>(over  $R$ )</sub>.

③ A subset  $A \subset M$  is a **basis** of  $M$  (over  $R$ ) if  $M = \langle A \rangle$  <sub>(over  $R$ )</sub> and  $A$  is linearly independent <sub>(over  $R$ )</sub>.

④  $M$  is **free** <sub>(over  $R$ )</sub> if  $M$  has a basis <sub>(over  $R$ )</sub>.

## REMARKS

- ① Not every  $R$ -module has a basis.
- ② A minimal generating set need not be lin. indep.
- ③ A maximal lin indep. set need not be a gen. set.

Q. If every  $R$ -module has a basis, is  $R$  a field?

(Yes. Take a non-field ring  $R$  and any non-trivial ideal  $I \subsetneq R$ .  
Then,  $R/I$  has no lin. indep. set over  $R$ .)

Q. If an  $R$ -module  $M$  has a basis, does every basis have the same cardinality?

Ans. Yes. This is called the Invariant Basis Number (IBN) property of  $R$ .

Remark. This is not true if  $R$  is non-commutative. (That is, we can find a counterexample of a non-commutative ring.)  
If  $R$  is a division ring, then again we have IBN.

Def<sup>n</sup> If  $M$  has a finite basis, say  $B$ , then we define  $\text{rank}(M) := |B|$ . } \text{well-defined by IBN}

If  $M$  is free with an infinite basis,  $\text{rank}(M) := \infty$ .

(When we do say "rank", we will usually mean "finite rank".)

EXAMPLES. ①  $R^{(n)}$  is a free  $R$ -module of rank  $n$   
 $M_{m \times n}(R)$  of rank  $mn$   
 $R[x]$  of rank  $\infty$

② Let  $A$  be a non-empty set and

$$F_0(A, R) = \{f: A \rightarrow R \mid f(a) = 0 \text{ for all but fin. many } a \in A\}.$$

Then,  $F_0(A, R)$  is an  $R$ -module under pointwise operations.

In fact,  $F_0(A, R)$  is a free  $R$ -module with basis  $\{\chi_a\}_{a \in A}$ , where

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

To see where the above set is generating, given any  $f \in F_0(A, R)$ , we can write

$$f = \sum_{a \in A} f(a) \chi_a.$$

↑ the sum is actually finite since  $f(a) = 0$  for all but finitely many  $a$ .  
(it is to be understood that 0s are ignored.)

Q. What if we take  $F(A, R)$ ? (All functions.)

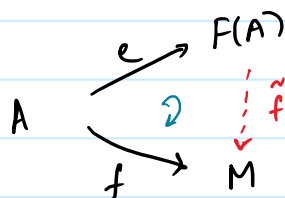
Universal Property of free modules:

Defn:

Given a non-empty set  $A$ , a free  $R$ -module on  $A$  is a pair  $(F(A), e)$  where (i)  $F(A)$  is an  $R$ -module, (ii)  $e: A \rightarrow F(A)$  is a (set) function

satisfying:

Given an  $R$ -module  $M$  and a function  $f: A \rightarrow M$ , there exists a unique  $R$ -linear  $\tilde{f}: F(A) \rightarrow M$  making the following diagram commute.



(That is,  $\tilde{f}e = f$ .)

REMARKS. ① Given  $A = \emptyset$ , a free  $R$ -module on  $A$  exists, and is unique up to isomorphism.

Moreover,  $e: A \rightarrow F(A)$  is one-one and  $F(A)$  is free with basis  $\{e_a\}_{a \in A}$ , where  $e_a := e(a)$ .



② If  $M$  is a free  $R$ -module, then  $M \cong F(B)$ , where  $B$  is any basis of  $M$ .

Thus, an  $R$ -module  $M$  is free iff  $M \cong F(A)$  for some  $A$ .

What the universal property is really saying is that:  
given a free  $R$ -module  $M$  with basis  $A$ , every  $R$ -linear  
 $M \rightarrow N \rightarrow R\text{-module}$

is completely determined by its action on  $A$ .

(The above is in the sense that given any assignment of values on  $A$ , we do get an  $R$ -linear map.)

EXAMPLE: Given an  $R$ -module  $M$ , such that  $M = \langle A \rangle$ , we can write  $M$  as a quotient of  $F(A)$ .  
(What we did last lec.)