Algebra - I

Prof. S. Viswanath & Prof. Amritanshu Prasad
Department of Mathematics
Indian Institute of Technology, Madras

Lecture 66 [Free Modules (finitely generated)]

We will talk about Free Modules today. So, this is and for us we will only be talking about free modules of finite rank or finitely generated free modules. These are the ones which resemble finite dimensional vector spaces, but they are just over arbitrary rings. So, the definitions are all very very familiar. So, this should look like vector spaces.

So, suppose I take a ring R not necessarily commutative, it can be anything. What is the free module? So, let us define this to be R to the n. So, the free module well, any such thing is called a free module ok. What does it look like? Looks like R to the n which is all n tuples. So, this is all elements of the form $(a_1, a_2, ..., a_n)$ where a_i's come from ring R ok.

And, we think of this as an R module ok what is the R module structure well we do component wise addition and component wise scalar multiplication. So, this becomes a left R module under the component wise operations component wise addition and scalar multiplication ok. And, this is of course, since we have talked about direct sums and so on as you can see this is actually nothing, but another way of saying look at just R thought of as a module over itself.

R ring $\quad$ Free module : $R^n = \{ (a_1, a_2, \ldots, a_n) : a_i \in R \}$

R-module under componentwise $+$ & scalar mult

$$R^n \approx \underbrace{R \oplus \cdots \oplus R}_{n \text{ copies}}$$

Define : $e_i = (0, 0, \ldots, \underset{i}{1}, 0, \ldots, 0) \quad i = 1 \ldots n$

Every $R^n \ni x$ can be uniquely written $x = \sum_{i=1}^{n} c_i e_i$ $\quad (c_i \in R)$

2/2

Homomorphisms $\quad R^n \xrightarrow{\varphi} M$ $\quad$ A hom φ is uniquely determined by $\varphi(e_i)$ $\quad i=1 \dots n$

$$\varphi\left(\sum_{i=1}^{n} c_i e_i\right) = \sum_{i=1}^{n} c_i \boxed{\varphi(e_i)} \in M$$

Given $m_i \in M$, $\exists!$ hom $\varphi : R^n \to M$ st $\varphi(e_i) = m_i \ \forall i$

And, this is just isomorphic to the direct sum of R with itself n times ok you take n copies of of the ring R thought of as a module over itself. And, that direct sum is exactly what we we are thinking of in this way ok and of course, these share a lot of properties with vector spaces over a field or with n-dimensional vector spaces, but there are also some important differences ok. So, we need to sort of be a little vary these ah.

So, let us look at the standard basis in some sense. So, let us define the element e_i which is 0 everywhere else except 1 in the i-th position. So, this is the i-th place 0s ok. So, we we define this as e_i; i goes from 1 to n and as is clear every element of the ring R because the operations are component wise if I give any element of this module sorry, if I take an element X in R^n then this element can be uniquely written. So, every element $X \in R^n$ can be uniquely expressed . As a linear combination of this e_is summation $\sum_{i=1}^{n} c_i e_i$ ok it is more or less from definition where the c i's come from the ring R ok. So, that is like vector spaces again and the key point is free modules are especially good when you are trying to define homomorphisms from it to other modules.

So, how do you define homomorphisms from a free module. So, suppose I give you a free module R^n and I want to define a homomorphism to any other R module M ok I want a homomorphism the way to define it is just by stipulating it is values on a basis ok. So, homomorphism is uniquely determined by its values on a basis. So, a homomorphism ϕ to any module M is uniquely determined once you tell me what the basis elements go to by the values $\phi(\sum_{i=1}^{n} c_i e_i)$ ok and why is that? Because once you know it on the basis on any other element you will just use the fact that that element can be written as summation $\sum_{i=1}^{n} c_i e_i$ and therefore, the property of homomorphism says I can pull all the c_i's out write it as a linear combination.

So, this just by the definition of a homomorphism and since I have stipulated these values there are some elements of M summation c i times those elements is some well defined element of n. So this is how you would define the homomorphism ok. So, this is this is also well defined. So, this is like if I pick arbitrary. So, ok. So, there is actually a existence and uniqueness statement that is hidden in this which is that if you give me some elements m_i then I can find a homomorphism such that $\phi(e_i) = m_i$ and there is only a unique such homomorphism ok.

So, maybe one should just make this slightly more precise so, let me just make the precise statement and you know you can just prove it from what I just said ah. So, here is the statement given $m_i \in M$ there exists a unique homomorphism ϕ from $R^n \to M$ which maps $e_i \to m_i$. So this is really the key statement. This is the statement I am trying to make ok and the proof is more or less obvious ok. So, this is how you define homomorphisms from R^n.

And, so it sort of interesting to study homomorphisms from $R^n \to R^m$ ok. So, by the same token suppose I wanted to understand what homomorphisms from $R^n \to R^m$ look like. So, what am I supposed to do? To specify this homomorphism what I should do is for each e_i I should give you some element m_i ok in this module R^m ok. Now, what does R^m look like? Ah Where there are too many m, so, maybe I will just give this some other name let me call it X_i. So, I need to specify an element X_i in R^m, but R^m remember itself is again a free module. So, any element of R^m can be uniquely written as a linear combination of it is basis elements right. So, let let let me give the basis elements of R^m and m let me call them f_j's now.

So, what is f_j? This is 0, 0, 0, 1 in the j-th place ok 0, 0, 0. So, I am thinking of it as an element of the free module R^m ok. So, so observe that f_1, f_2, f_m will form a sort of a basis for R^m if you wish ok. So, each X_i since it is an R^m it can be uniquely written as a linear combination of the f_j's ok. So, let us do that let us write X_i as some linear combination and now I will use a_{ij}'s to denote the linear combination the elements of R which occur in the linear combination. So, this is now the sum j goes from 1 to m ok and what are the a_{ij}'s they are some elements of R. So, what are a_{ij}'s ok? So, our previous discussion then says that to specify a homomorphism from $R^n \to R^m$ you just need to tell me what are all these X_i's these nX_i's on equivalently you just need to tell me what these scalars a_{ij} are. Now, here how many of them are there? i is from 1 to n, j is from 1 to m and the appropriate way to arrange this is in the form of a matrix ok just like we do for vector spaces. So, a homomorphism ϕ is uniquely determined by a matrix. So, I I want to say let us take an $m \times n$ matrix this is like in the convention for vector spaces. So, this is an $m \times n$ matrix ah.

So, to to be very precise I mean for it to match our usual conventions what I should do is to change these these i's and j's around. So, let me just do one little thing here. So, that it matches with vector spaces. So, let me say let me take e j. So, j will go from 1 to n. So, I am going to switch the roles of i and j here ah. So, e_j maps to X_j ok. Now, i which is this other variable now will go from 1 to m ok. So, i goes from 1 to m.

And, observe that what I am doing here is what we do for vector spaces which is that we put these scalars along the columns ok. So, what does this mean? So, what have I done I am saying e_j maps to X_j; X_j is summation $a_{ij}f_i$ ok. So, in other words the if I wanted to know what is ϕ acting on e j, then the scalars which occur are in the j-th column of A ok. So, this is our usual convention arrange along the columns rather than along the rows ok. So, I hope that definition is clear there. So, I just need to tell you what these scalars are. These I need to tell you this $m \times n$ matrix a_{ij}. Now, let us sort of look at one little difference. Now, so far it is it is looking a lot like vector spaces but, there is one little twist to the tl.

So, let just see suppose I give you this matrix. So, given this matrix A given given A. So, what is A now? It is an element of. So, let me use this notation matrices $m \times n$ whose entries are not in a field necessarily, but in the ring R. So, given a matrix $Am \times n$ with entries in R, we define the homomorphism ϕ as before using this matrix by saying that the value on e_j is the scalars in the j-th column. So, $a_{ij}f_i$ i goes from 1 to m ok and this is for all j between

$$R^n \xrightarrow{\varphi} R^m \qquad f_j = (0,0,\ldots,\underset{j^{th}}{1},0,\ldots,0)$$

$$\begin{array}{ccc} & & \rotatebox{90}{$\in$} \\ e_j & \longrightarrow & X_j = \sum_{i=1}^{m} a_{ij} f_i \end{array} \qquad \in R^m$$

$$a_{ij} \in R. \qquad \begin{array}{l} 1 \le i \le m \\ 1 \le j \le n \end{array}$$

$$A = \begin{array}{c} \varphi(e_j) \\ \downarrow \\ \begin{bmatrix} \vdots \end{bmatrix}_{m \times n} \end{array}$$

1 and n . So, if we do this then what does the value become on a general element ok. So, suppose I I pick a on a general element of on a general element X in R^n . So, what does that mean? I I can write this element X as some linear combination $X_j e_j$ ok.

On a general element how does ϕ act? So, let us compute $\phi\phi$ acting on X now we have to be very careful when we do this. So, ϕ acting on summation $X_j e_j$ by definition is I can pull the X_j's out j goes from 1 to $nX_j \phi e_j$ ok and ϕe_j remember is what is written on top. So, there is a double summation here, but since R is not a commutative ring, I have to be careful with the order in which I multiply my scalars ok.

So, $\phi(e_j)$ I am just going to use this equation on top it says this is $\sum_{i=1}^{m} X_j \cdot a_{ij} \cdot f_i$ ok and I can switch the order of summation here. I can think of it as summing first over i then over j that is that is fine. I am just doing the same sum in a different order. So, this is summation i goes from 1 to m, summation j goes from 1 to n now and what I have here is $X_j a_{ij}$ ok $\cdot f_i$ ok. So, this is my this is my final formula.

So, observe so, I am I am sort of doing this slowly to point out that you know in the case of vector spaces you still get the same formula, but the ring there is a field ok which is commutator. So, these in the case of vector spaces we would tend to write this formula as $\sum a_{ij} X_j$ rather than $\sum X_j a_{ij}$, but in this case you are not allowed to commute these two things. The X has to come before the entries of A ok. So, this is the this is the key point to note here that we are used to writing it in the other order for vector spaces because they commute, but when you are trying to do this for general rings we have to be a little careful ok. So, anyway that is the; that is the formula here.

Now, observe this is ah. So, we we should really think of this as well if if we were able to commute these two guys you would write this as the product of the matrix A with the column vector X and this is the i-th element in that product in this case you cannot quite do that ok. So, let us just look at one more such case where it will become clearer. So, if I take for example, $R^n \to R^m \to R^p$. So, I will take three such free modules and I sort of do

Given $A \in \mathrm{Mat}_{m\times n}(R)$, define $\varphi : R^n \to R^m$ by

$$\varphi(e_j) = \underline{\underline{\sum_{i=1}^{m} a_{ij} f_i}} \qquad 1 \le j \le n.$$

<u>on a general element</u> $x \in R^n$, $x = \sum_{j=1}^{n} x_j e_j$

$$\varphi(x) = \varphi\left(\sum x_j e_j\right) = \sum_{j=1}^{n} x_j \, \varphi(e_j)$$

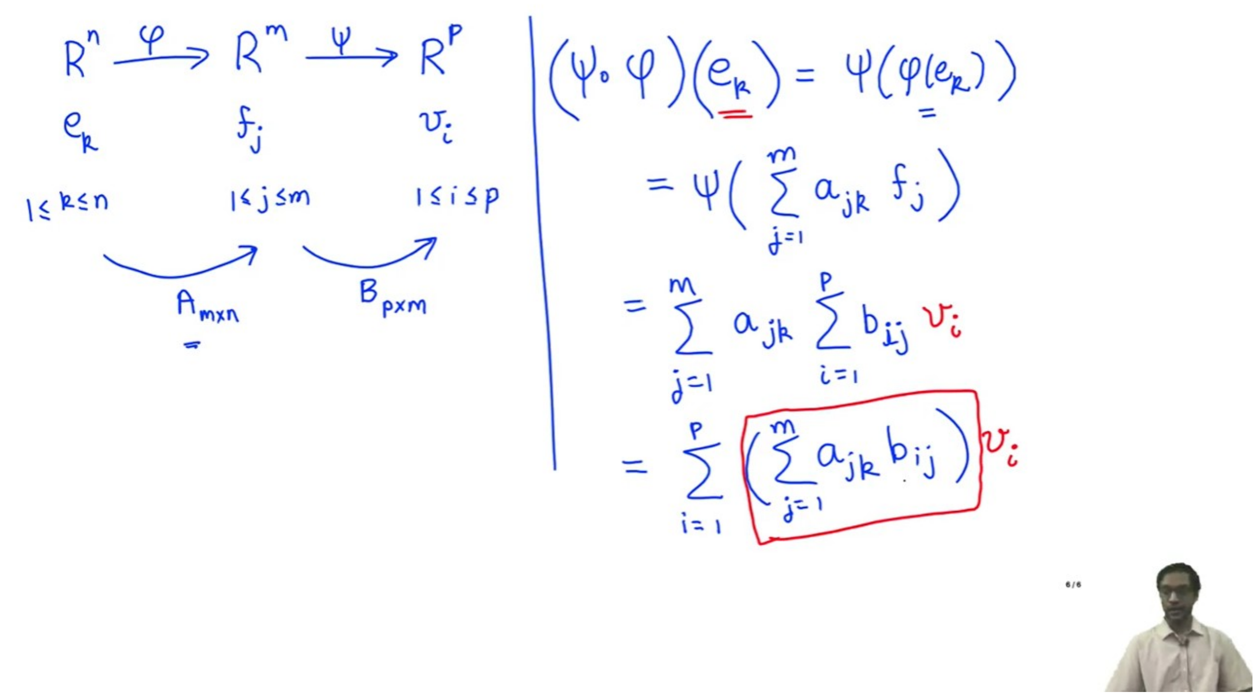
$$= \sum_{j=1}^{n} \sum_{i=1}^{m} x_j a_{ij} f_i = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} x_j \underset{\ast}{\underline{\underline{a_{ij}}}} \right) f_i$$

a similar thing. I take a basis of this free module call it e_k this free module call it f_j let us call these v_i 's ok.

So, this is now k going from 1 to n, j going from 1 to m and i going from 1 to p ok. So, I take three three basis and now I I have two homomorphisms ϕ and ψ. Each homomorphism is determined by the knowledge of an appropriate matrix right. So, suppose I call those two matrices which determine this homomorphism and this homomorphism let us call the corresponding matrices A and B. A will be whatever $m \times n$ and B will be $p \times m$, right. So, this is $m \times n$ and this is going to be $p \times m$. So, I have two matrices and now, if I compute what the matrix of their composition is ok this is again something which we are used to do in the case of vector spaces.

So, if you compute ψ composition ϕ and I need to figure out what the the matrix of the composition looks like which means I should just figure out what the what this composition does to the basis vectors e_k right to these elements e_k. So, I need to compute the value on e_k. So, let us just do that that is just ψ evaluated on ϕe_k ok. Now, I am given that this matrix is A; that means, I know what ϕe_k is this is just ψ of summation A let us call this j k f_j . Now, j is being summed over 1 to m. Now, when I apply ψ to this what am I supposed to do I pull the a out j goes from 1 to m this becomes a j k and I need to evaluate ψf_j ok. So, this is ψf_j and in the last step what am I supposed to do ψf_j has to be replaced by whatever it is it is equal to right.

So, let me let me just do it right there. So, let me erase this ψf_j is summation, it is given by the matrix b summation i from ah. So, this is $b_{ij} e_i$ ok. So, I have just use the definition of ψf_j and the matrix b ok. So, now, you will already start seeing a problem. So, I I just change the order of summation this i goes from 1 to p and inside is $\sum_{j=1}^{m} a_{jk} b_{ij} \cdot e_i$ ok. And, now, we are done that is the the end of the computation because I am trying to find out



what is the the compass the composed map acting on e_k um sorry this should have been v's here.

So, this should have been v_i it is an element of R^p. So, now, the composed map is again given by a matrix right the entries of that matrix are exactly what I get when I write ψ composition ϕe_k as a linear combination of the v_i 's, but now these therefore, are the entries of that matrix ok.

So, what this means is that ψ composition ϕ suppose this is given by a matrix C ok and this is now a $p \times n$ matrix right ah. $p \times n$ would be this full composition here ok. Now, in the in the case of if you remember how things work in the case of vector spaces we would just say oh that matrix C is known it is just a product of the two matrices B and A, right.

This is how it works when you compute matrices of linear transformations in the case of vector spaces, but now observe that our answer is not quite that because a and b I mean it is almost it is looking like that if the ring were commutative then of course, you could change the order of b and a and rewrite this this term here as $b_{ij}a_{jk}$ sum over j ok and then it would exactly be the product of b and a ok.

Now, the trouble is here it you know things do not commute. So, this matrix C that you have the elements of this matrix are the following C ik the k-th column i-th entry is the sum j going from 1 to n ok and it is almost what you would expect in the case of vector spaces you would have expected the following it is $b \cdot$ a.

So, you would have written $b_{ij}\cdot$ a a_{jk} this is what you would have wanted to write in the case of vector spaces, but in this case it does not occur like that it occurs in the other order ok. So, which means that this this a actually occurs on the other side. So, I need to push this a over to the other side ok. So, that is the that is the form of the answer here ok. So, let us just erase this make it slightly neater. So, this is $a_{jk}b_{ij}$ and that sort of seems rather unfortunate that we can not quite think of it the same way as vector spaces, but what we do is something rather interesting here recall that we talked about something called the opposite ring of ring R ok.

So, recall I once talked about something called R^{op}, what is this? It is the same ring it is the same set R with the same addition, but the multiplication alone is is different. So, what is the new multiplication in the opposite ring if I have to multiply two elements a and b, I just take the usual multiplication in the ring, but in the opposite order ok. So, given a ring that is this opposite ring in which the multiplication is just the the product in the other order and so, what we can do now is to think of this as instead of $a_{jk}b_{ij}$ well, I will do the following I will think of it as well it is just $b_{ij} \cdot a_{jk}$ except that this product is is taken in the opposite ring ok.

So, now, I am going to take the opposite product ok. So, now that that is already nicer it brings things into the same setup as vector spaces the matrix C is actually the product $b \cdot$ a, but we should just take care to to use not the usual ring multiplication, but the multiplication in the opposite ring ok. So, what we have really shown so far is the the following statement um. That, if you want to look at module homomorphisms from $R^n \to R^m$, then the sort of the correct formulation the correct way to think of it is the following. Each homomorphism gives rise to a matrix ok so, this gives rise to an $m \times n$ matrix and the elements are well they are elements of R of course, but the correct way to think about it is that they are elements of R^{op}.

So, if you think of each homomorphism as giving you a matrix $m \times n$ matrix with entries in R^{op}, then the composition takes on this rather nice thing which is that if I compose two such homomorphisms from $R^n \to R^m \to R^p$. So, this is ϕ and ψ, then as we just saw if this if the matrix or the first guy is an A this is an A and this matrix is B then the matrix of $\psi\phi$ will just turn out to be. So, this matrix will turn out to be BA, but remembering that the elements are a's and b's; the elements of a and b are elements of $R^{op}$and not elements of R ok.

And, in fact, this is we can also do the special case when n equals m. So, this is so, recall we call these the space of endomorphisms. So, if I just take n equals m then End of R^n just means all module homomorphisms from R^n to itself ok and now this is every such homomorphism to to every such homomorphism we can associate an $n \times n$ matrix. So, let me just say mat n meaning $n \times n$ matrix whose elements are in R^{op}. So, this is called the matrix of this homomorphism and now the beauty is that the space nR^n is it is it is it is actually a ring ok. So, here is a little exercise exercise observe that end R^n is a ring under composition of maps. So, this is a ring under point wise addition and composition ah. So, addition is point wise addition and the multiplication is the composition of maps ok.

On the other hand, mat the space of matrices with over with entries in a ring R is also ring ok under the usual matrix addition and matrix multiplication. So, observe that the right hand side is also a ring mat n . Entries in any ring is ring under matrix addition and matrix multiplication and check that this association ah. So, here is the exercise check that ϕ going to matrix of ϕ is actually a ring homomorphism ok.

So, we we actually checked some bits of this which is I mean the the the only thing really to check is that the multiplication is respected on the two sides, but that was really the point that we spent a lot of time over which is that when I take two homomorphisms ϕ and ψ, the composition of of $\psi \circ \phi$ goes to the product of the two matrices except that I should think that the entries come from R^{op} and not from R ok.

$$\mathrm{Hom}(R^n, R^m) \longrightarrow \mathrm{Mat}_{m\times n}(\underline{\underline{R}}^{op})$$

$$\varphi \longrightarrow A$$

$$R^n \xrightarrow{\varphi} R^m \xrightarrow{\psi} R^p$$

$$\underset{A}{\frown} \qquad \underset{B}{\frown}$$

$$[\psi \circ \varphi] = (BA)$$

And, recall also that we have sort of seen an instance of this before in in one of the problem sessions which is that if I take n equals 1 which means I just think of R as a module over itself ok and I ask what are all the endomorphisms of R right which means what are all the homomorphisms of R I mean homomorphisms from $R \to R$, then we we sort of had done this before that this is actually isomorphic to the ring R^{op} ok and what was the map?

Each homomorphism looks like a sort of a right multiplication ok. So, each homomorphism ϕ here ah. So, what are the homomorphisms? Well, maybe I should say the map in the opposite directions what we looked at given any element of R or R^{op}, it induces a homomorphism here ϕ_b as follows $\phi_b X = X_b$ the right multiplication by b map ok and that is exactly this I mean this is the the thing we are looking at here is a generalization of that to to arbitrary values of n ok ok .

$$\mathrm{End}(R^n) = \mathrm{Hom}(R^n, R^n) \longrightarrow \mathrm{Mat}_n(R^{op})$$
$$\varphi \longrightarrow [\varphi]$$

Ex: $\mathrm{End}(\underline{\underline{R^n}})$ is a ring, under $+$ & composition

$\mathrm{Mat}_n(R^{op})$ is a ring.

$\varphi \longrightarrow [\varphi]$ is a ring homomorphism.

Recall: $n = 1$ $\qquad \mathrm{End}(R) \xrightarrow{\sim} R^{op}$

$$\varphi_b(x) = xb \longleftarrow b$$