Algebra - I

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

## Lecture 69 [Problem Solving]

Let us do some problems today. So, here is problem number 1. So, suppose I have a homomorphism of free modules, so let us take $R$. In this case let us say $R$ is a commutative ring. Let us take a commutative ring $R$. And let us take a homomorphism $\phi : R^n \to R^n$, ok and this $n$ is greater than equal to 1. And so, this is an $R$ module homomorphism, $R$ module homomorphism and let this be given by a matrix $A$, ok. So, let this correspond to $A$, by which we mean suppose I take $e_i$ to be the standard basis element of $R^n$ with all 0s and 1, in one of the places, one in the i-th place.

Then, this map $\phi$ maps $e_i$ to, let us let us call it $e_j$, $e_j$ to summation $\sum_{i=1}^{n} a_{ij}\ e_i$, i equals from 1 to n, ok. Now, $a_{ij}$'s are some elements of the ring $R$. And recall this is how we associate a matrix to a homomorphism ij goes from 1 to n, ok. So, the homomorphism $\phi$ corresponds to the matrix $A$. And recall also that we we have talked about this in the lectures that this map $\phi$ is an isomorphism or an automorphism of $R^n$ is the same as saying that the the matrix $A$ here, has determinant which is a unit in the ring $R$, ok.

Problems

1. $R$ commutative ring $\quad \varphi : R^n \to R^n \quad$ R-module homomorphism

$$e_i = \begin{bmatrix} 0 \\ \vdots \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \qquad \varphi(e_j) = \sum_{i=1}^{n} a_{ij}\, e_i \qquad a_{ij} \in R$$

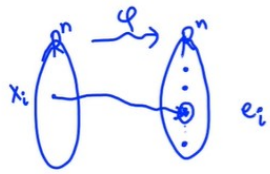
$$A = [a_{ij}]_{i,j=1}^{n}$$

$\varphi$ isom $\iff$ det $A$ is a unit in $R$

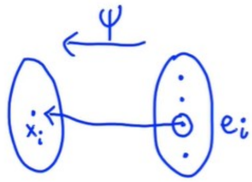
$\iff \exists\, B \in Mat_n(R)$ st $AB = BA = I$

(Q) If $\varphi$ is ONTO, PT it is also one-to-one.

1/1




For each $1 \leq i \leq n$, $\exists\, x_i \in R^n$ st $\varphi(x_i) = e_i$




Define a $R$-homomorphism $\psi : R^n \to R^n$

via $\psi(e_i) = x_i \quad \forall i$

Observe: $\varphi\psi(e_i) = e_i \quad \forall i \Rightarrow \varphi\psi = I$

Let $B$ denote the matrix of $\psi$

$A$ " s " " " $\varphi$

2/2

This was special for commutative rings. And of course, the definition of isomorphism is that there is really an inverse map, such that the compositions the identity and this in terms of matrices says that there exists a matrix $B$, matrices $n \times n$ with entries in $R$ such that the product $A$ into $B$ is equal to $B$ into $A$ equals the $n \times n$ identity matrix, ok. So, this is just something to recall. Now, here is the the problem itself. So, the question problems as if $\phi$ is an onto map, if $\phi$ is onto show that it is also one-to-one prove that it is also one-to-one, and hence an automorphism, ok. So, this is the thing that we need to prove. If I have a homomorphism from $R^n \to R^n$ which is onto, then it is automatically one-to-one, ok.

So, let us let us prove this. So, recall that I mean what does on to mean. So, let us draw a picture of this module $R^n$ to $R^n$, I have got this homomorphism phi. And what I am given is that it is on to. In particular, it means that if I take these $e_i$'s these basis elements $e_i$ each $e_i$ has, so let us call this element as as $e_i$, then each $e_i$ has some element of $R^n$ which maps to it under a phi, ok. So, there exists an element $X_i$ in $R^n$ which maps to $e_i$ under this isomorphism phi, ok. So, remove this arrow here, so that that little element here is $e_i$, ok. So, for each i, we know that there is an element of this module $R^n$ such that $\phi$ maps $X_i$ to $e_i$, ok that is what surjectivity in particular implies.

Now, what that allows us to do is the following. Let us define a map in the reverse direction, ok. So, I am going to define a homomorphism $\psi$ which maps sort of which goes in the opposite direction you think of it as going in the opposite way, going the opposite way. Now, what it does is the following it takes each $e_i$ to $X_i$ here remember $X_i$ is somewhat arbitrary here there may be many different elements of $R^n$ which map to to $e_i$, I pick any one pre image, ok call it $X_i$ and I claim I can use those excise to define a map $\psi$ , ok.

So, define $R$ module homomorphism or $R$ homomorphism $\psi$ from $R^n \to R^n$ by the following recipe by prescribing its value is on the $e_i$. So, recall if I tell you what a homomorphism does to $e_i$, then its uniquely determined in this case I want the $e_i$'s to map to $X_i$, ok. And that now, defines homomorphism uniquely. Now, what is the property of $\psi$ with respect to phi? Well, observe by construction. If you first apply $\psi$ and then you apply $\phi$ on any of the $e_i$'s what you get back is $e_i$ again, ok. So, it maps each basis element back to itself therefore, the composition $\phi\psi$ is nothing, but the identity map, ok. Let me call it i, it is the identity homomorphism of $R^n$, ok.

So, now let us let us take this I mean let us do this in terms of matrices. Let $B$ denote the matrix of $\psi$ , ok. Just like we had $A$ which denote it. So, recall $A$ already denotes the matrix of phi, ok. Now, what do we know the composition of $\phi\phi$ and $\psi$ and remember $R$ is commutative, so the opposite ring here is the same as the original. So, recall this was $RR$ key observation if I am looking at endomorphisms of $R^n$. Then, to each endomorphism I can associate a matrix, but I should really think of the matrix entries as coming from $R$ op, the opposite ring rather than the the original. If I do this, then these two spaces are isomorphic as rings, ok. In other words, composition of endomorphisms maps to multiplication of matrices, ok.

And that is where that that multiplication involved the opposite map. But now here we are in the commutative ring case where everything is nice. So, we do not need to worry about this op business, in this case $R$ op is the same as $R$. So, now, what do we know because $\phi$ and $\psi$ , so the the the matrix of $\phi\psi$ . So, let me use this notation for the matrix of $\phi\psi$ is nothing but the product of the matrices, ok of $\phi$ and $\psi$ which is $A$ and $B$, ok. So, the matrix is just $AB$. And on the other hand, $\phi\psi$ is the identity homomorphism whose matrix is the identity you know the $n \times n$ identity matrix, ok. So, what does that mean? It implies therefore, that the matrix $A$ times the matrix $B$ is the identity matrix and therefore, if you take determinants on both sides and recall determinant of $AB$ is determinant of $A$ determinant of $B$, even though they have, I mean this is true for all matrices with entries in any commutative ring.

This is just the determinant of the right hand side, the determinant of the identity is 1. So, what this therefore gets us is the fact that the determinant of $A$ is a unit because it has an inverse determinant $B$, And well what does this mean? This means that $\phi$ is an isomorphism. So, recall this automatically means that $\phi$ is an isomorphism. In other words, it is also 1-to-1; i e, it is also 1-to-1, ok. So, on to is enough to to ensure 1-to-1 and therefore, thereby an isomorphism. So, this brings us to the the obvious second question; is the same true if I knew that $\phi$ was 1-to-1, ok. Could I conclude that $\phi$ is on to?

So, I I give you the same question. Phi is a homomorphism, $R$ module homomorphism from $R^n \to R^n$, $\phi$ is 1-to-1, ok. So, the question is does that imply ontoness. In other words, is is $\phi$ an isomorphism, ok. ah Observe the same proof will not work anymore because how did the the earlier proof work, we constructed sort of an inverse, a one sided inverse in some sense are map in the opposite direction the same same idea will not work here, ok. So, I mean you you should try that to see that you cannot quite do the same thing and in fact, this this statement is false, ok. So, the answer here is no, not quite true. And the examples are very easy to construct. So, for example, if I just take $R$ to be the integers $n$ to be 1, then I am just looking at homomorphisms from $\mathbb{Z} \to \mathbb{Z}$ and I am asking if I give you an injective module homomorphism is it automatically surjective, ok.

And that is of course, not true because here is an example. Each $n$ maps to 2 $n$ is an injective module homomorphism of $\mathbb{Z} \to \mathbb{Z}$ ok. But, of course this is not surjective because the image is only the set of even numbers, ok. So, that is an interesting thing. If you are given it is on to then it is automatically 1-to-1. If you are given its 1-to-1 it is not necessarily

$$\mathrm{End}_R(R^n) \xrightarrow{\sim} \mathrm{Mat}_n(\underset{R}{\overset{\shortparallel}{R^{op}}})$$

$$[\varphi\psi] = AB$$
$$\shortparallel$$
$$[I] = I_n$$

$$AB = I_n \Rightarrow \det(A)\det(B) = 1$$

$\Rightarrow \det(A)$ is a unit

$\Rightarrow \varphi$ is isomorphism

$\Rightarrow \varphi$ is 1-1 ∎

onto, ok. But the important thing here is that all this only holds if $R$ is a commutative ring, ok. So, recall we use the the fact that you you know you can you can talk about determinants and so on and all of that really only works for commutative rings, ok.

You cannot really make sense out of a determinant of $A$ matrix where the entries are from some non-commutative ring, because the determinant involves you know the expanding the the entries in some ways you have to take products of the various entries. And if you do not quite know, what order to take them in then we are in trouble, ok. All the nice properties of determinants will not be true anymore.

But the question can still be asked over non-commutative rings. So, here is my question is question 1; that is is question 1 true over non-commutative rings, ok. In other words, if I give you a surjective map between you know from $R^n \to R^n$, if does that automatically imply that the map is injective, ok. And again, here we cannot use the same proof definitely because the proof there involved realizing that you can construct an inverse in one direction. And being able to construct an inverse tells you something about the determinant, the determinant has a unit and so on. So, we we really make very essential use of the determinant there. So, well, it turns out the answer is no, ok. So, we really do essentially use the fact that the ring $R$ is commutative.

And let us look at, I mean several different counter examples could probably be constructed, so I am going to describe one of them for you. So, here is the the counter example. So, let us first look at; so, I will tell you what the ring is in just a minute. Before I tell you what the ring is let me define a vector space, ok. So, let me call this. So, it is a vector space of the real numbers. This is I call it $R$ infinity, the elements are just infinite sequences of real numbers, ok. I think of it like this $X_i$ ranging over $R$, it is just sequences of real numbers $X_1$ , $X_2$, $X_3$, dot, dot, dot. It is an infinite dimensional vector space, ok. So, it is like I mean an infinite dimensional analog if you wish of the finite dimensional vector spaces $R^n$, ok.

(2) $\varphi : R^n \to R^n$ $\varphi$ is 1-1 (Q) Is $\varphi$ onto ?

(A) NO

$R = \mathbb{Z}$ $n=1$ $\mathbb{Z} \to \mathbb{Z}$

$n \to 2n$

(3) Is (Q1) true over non-commutative rings ?

NO

So, I think of this as a vector space over $R$ over the real numbers. And let me define the ring for you. Let us take the ring $R$. So, remember I am looking to construct a non-commutative ring, the ring is just the set of all linear operators on this infinite dimensional vector space. ok By this I mean it is just all linear maps $T$ from $V \to V$, it is a linear transformation $T$ is it is a $R$ linear operator, ok. So, the set of all linear operators on a vector space whose dimension is at least two, this this collection of linear operators, they are a ring under composition. It is like if this where a finite dimensional vector space this would be like the set of all $n \times n$ matrices, where $n$ is the dimensional vector space.

Here it is an infinite dimensional vector space, so you you actually have lots and lots of operators, but this ring $R$ is definitely non-commutative, ok just like just like matrices in some sense. And let me let me sort of demonstrate that explicitly for you. So, I will look at two special operators which I will also use for my example. So, one of them is called $A$, it is a following operator, it takes ($X_1$ , $X_2$,.... )dot, dot, dot and moves everything one step forward, ok,( 0, $X_1$ , $X_2$,.... )etcetera.

So, this is the forward shift operator if you wish. It is called the forward shifting operator. It pushes everything one step to the right and puts a 0 in the first place. And does a backward shift operator which pushes everything one step back, and when it does that it pops out the $X_4$, blah blah blah there is a backward shift, ok. Now, observe that if I first do the forward shift and then the backward shift on a tuple, an infinite tuple like this. Then, well it shifts one step forward and then one step backward, the 0 sort of gets added on first and then removed in the second step. So, that is just the identity map gives me back what I started out here.

But if I do it in the other order then I do not quite get the same answer because the backward shift will will sort of throw the $X_1$ , out and the forward shift will put a 0 in its place. So, this is like the $X_1$ , goes away and I have a 0 in its place, ok. So, observe that these are not in general equal, right. I mean if $X_1$ , is nonzero they are not going to be equal

(Eg) $V = \mathbb{R}^\infty = \{(x_1, x_2, x_3, \dots) : x_i \in \mathbb{R}\}$

$R = \mathrm{End}_{\mathbb{R}}(V) = \{T : V \to V \mid T \text{ is } \mathbb{R}\text{-linear opr}\}$

(eg) $A(x_1, x_2, \dots) = (0, x_1, x_2, \dots)$ forward shift

$B(x_1, x_2, \dots) = (x_2, x_3, x_4, \dots)$ backward shift

$BA(x_1, x_2, \dots) = (x_1, x_2, x_3, \dots)$

$AB(x_1, x_2, \dots) = (0, x_2, x_3, \dots)$

$AB \neq BA$

to each other. So, the operator $AB$ is not the same as the operator $BA$, ok. ah Now, here is the, here is a counter example. So, what does it that we want to construct? We wanted to construct a map. So, let us let us review what is it that we are trying to do.

We are trying to find, so this $R$ is now this ring of endomorphisms we are trying to find a surjective homomorphism which is not injective, ok. So, what is it that I want? I want $\phi$ to be surjective, but not injective, ok. This cannot happen if $R$ is commutative as we just saw. But if $R$ is non-commutative in this particular, I mean in particular in this example we will construct such a fact, ok. So, let us do this. So, let us it is; in fact, enough to take $n$ equals one we will just construct a counter example right there.

So, look at $R$ the ring at of endomorphisms. Think of it as just a free module over itself. Now, let me construct a map $\phi$ as follows The definition is the following each $X \in R$ each endomorphism of this infinite dimensional vector space I map it to $XA$, ok, $A$ remember is the forward shift operator. So, each $X \to XA$, ok, this is my map. This is a $R$ linear homomorphism. So, recall that the the endomorphisms of $R$ are nothing but the right multiplication operators, right, and that is exactly what is happening here we are we are right multiplying by some fixed element of $R$, ok the element $A$ in this case. So, I claim that this map $\phi$ has exactly the properties we want, that it is surjective but not injective, ok.

So, let us prove prove this. So, first why is it surjective? To show it is surjective let us first look for what what element maps to the identity, ok of this ring $R$. So, observe that if I look at $B$ here, if I apply $\phi$ to this backward shift operator $B$ and that is just going to be $BA$, ok. And $BA$ remember is just the identity map, ok that is the thing that we looked at first. $BA$ is just the identity map, ok.

So, in particular; that means, that if I apply $\phi$ to $XB$, ok take any x in your ring $R$ apply $\phi(XB) = XBA$, then by definition this is $XBA$, but $BA$ is the identity, so this is $X$, ok. So, what does that mean? Any element $X$ in your ring here take any $X$, it is got a preimage, ok. The element $XB$ maps to $X$, so that means, $X$ is in the image of $\phi$ and this is true for every $X$ in my module, ok in my module $R$ power 1. Therefore, it means that my map $\phi$ is a

$R^n \xrightarrow{\varphi} R^n$ want $\varphi$ surjective, not injective.

$\underline{n=1}$ $R \xrightarrow{\varphi} R$ R-homomorphism.

$X \longrightarrow XA$

(a) $\varphi(B) = BA = I \Rightarrow \varphi(\underline{XB}) = XBA$
$= \underline{X}$

$\Rightarrow X \in \text{Image-}\varphi$
$\forall X \in R^1$.

(b) $C(X_1, X_2, \dots) = (X_1, 0, 0, \dots)$

surjection. Let us show it is not an injection. To show it is not an injection we need to show it is got some kernel right that it kills some element. So, here is the the element it kills, let me define an operator $C$ as follows $C(X_1\ , X_2,....)$ etcetera is $(X_1\ , 0, 0, 0,....)$ So, here is my operator C, ok. It is sort of the projection onto the first content, ok. Keep x 1, make all the other 0.

Now, observe that, so $C$ is clearly a nonzero operator, right, $C$ is not the 0 operator, ok. And on the other hand, if I apply $\phi(C) = CA$. Now, what is $CA$? $A$ was the forward shift operator, ok which is basically it you know; so, when I first apply let us let us apply to an actual element and check if I apply $CA(X_1\ , X_2,...)$, dot, dot, dot. This is $C(\ 0, X_1\ , X_2,...)$. But what does $C$ do. It keeps a first component as it is and makes all the other component 0, ok. So, in other words, this composition $CA$ maps everybody to 0, ok. So, what does that mean? Phi of $C$ is 0, whereas $C$ itself is a nonzero element of the module, ok. In other words, the kernel $C$ belongs to the kernel of this homomorphism $\phi$ therefore, $\phi$ is not 1-to-1, ok. So, I hope the example itself is clear. So, what this demonstrates is is various things that the surjectivity implies injectivity over commutative rings for free modules. Injectivity does not imply surjectivity, even if you are over a commutative ring. And if you are over a non-commutative ring then you do not get anything, I mean injectivity does not imply surjectivity, surjectivity does not imply injectivity and so on.

So, this sort of underscores the key role played by this determinant somehow. You know it it over a commutative ring the fact that you have got this determinant map is is very key, ok. It really helps us in many situations.

$C \neq 0 \qquad \varphi(C) = CA = 0$

$$CA(x_1, x_2, \dots) = C(0, x_1, x_2, \dots)$$

$$= (0, 0, 0, \dots)$$

$\Rightarrow C \in \ker \varphi \Rightarrow \varphi$ not 1-1.