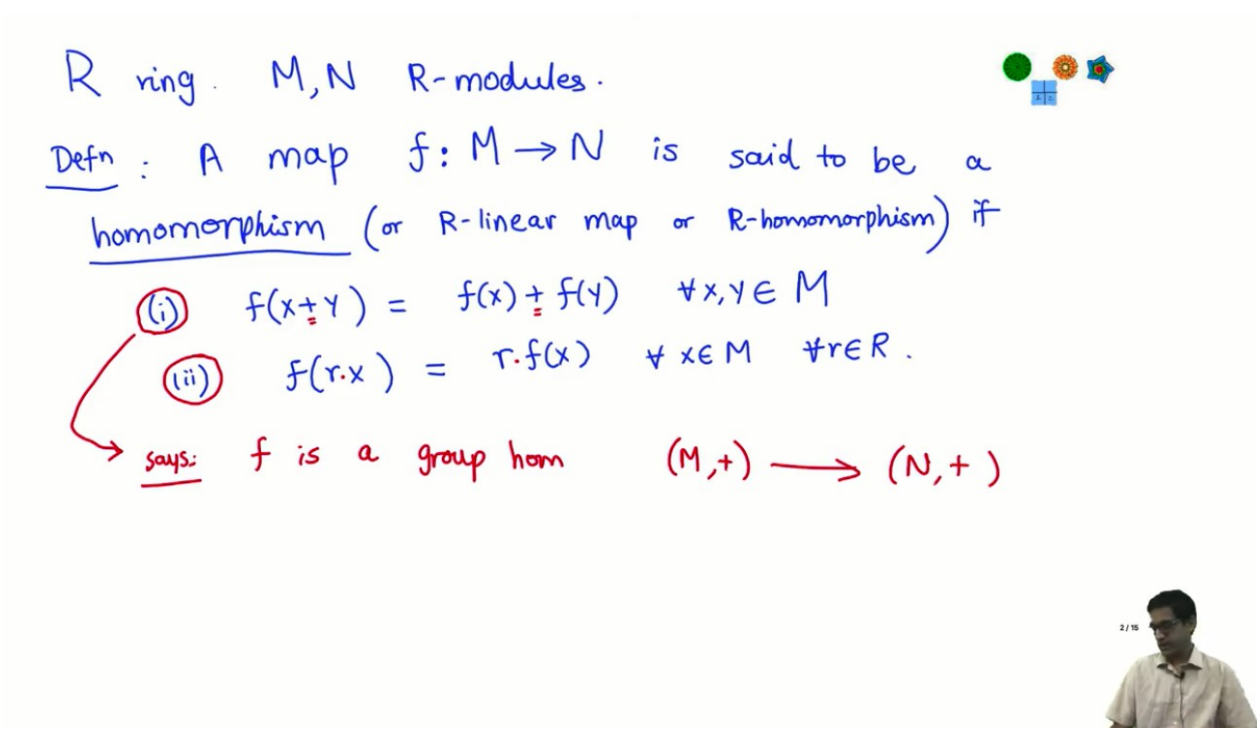
Algebra - I

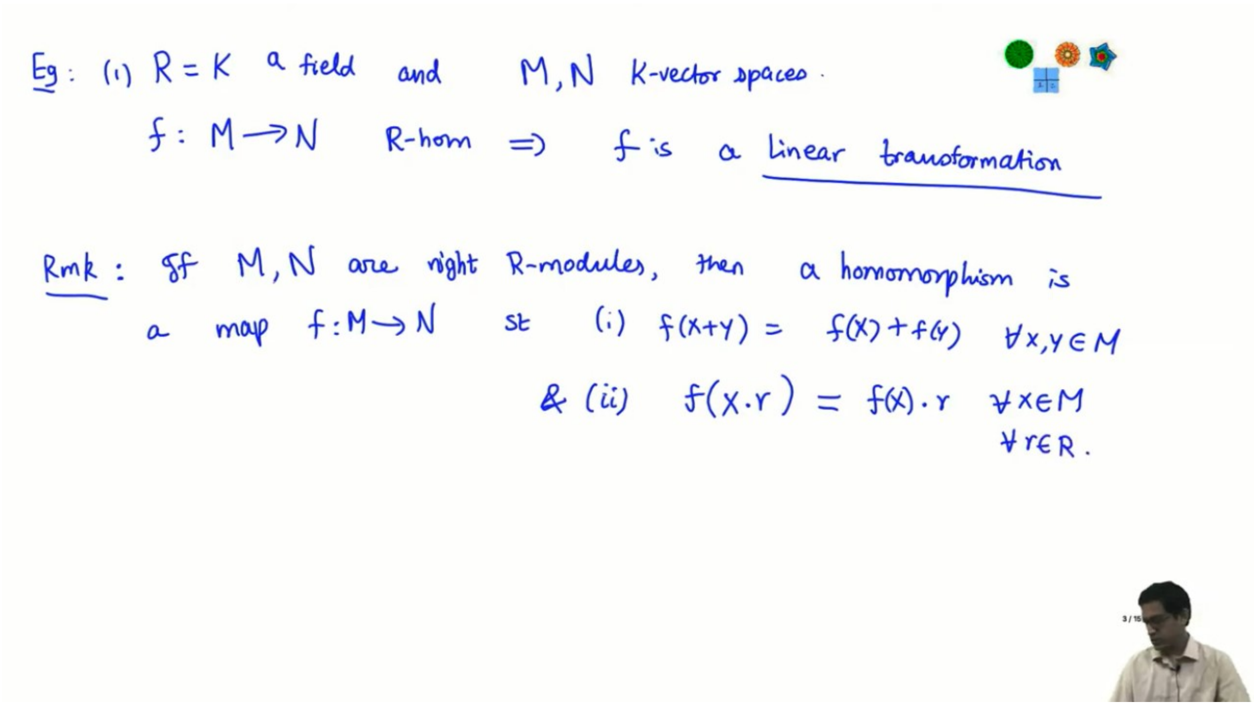
Prof. S. Viswanath & Prof. Amritanshu Prasad
Department of Mathematics
Indian Institute of Technology, Madras

Lecture 59 [Homomorphisms]

Let us talk about Homomorphisms of Modules . So, suppose R is a ring and M and N are two R modules. So, they need to be modules out the same ring R, then a map a function from $f : M \to N$ is said to be a homomorphism and sometimes we call it by other names we sometimes say it is an R linear map it is another word for homomorphism or if we want to emphasize the ring R we sometimes call it an R - homomorphism ok.

So, the there are sort of many different words we use for this. So, homomorphism of R modules is a map satisfying the following two properties; one that $f(x+y)$ equals $f(x)+f(y)$ for all x and y in the set M and property two is that $f(rx)$ should be $r \cdot f(x)$. So, this is the for all x in M and for all ring elements R in R ok. So, in other words a module remember has two important operations the that of addition and scalar multiplication by the ring R and homomorphism is a map which preserves these two operations ok. Now so, what are you know if you sort of look carefully at this definition notice that this + here is the addition in the space M this + on the right is the addition in the space N.



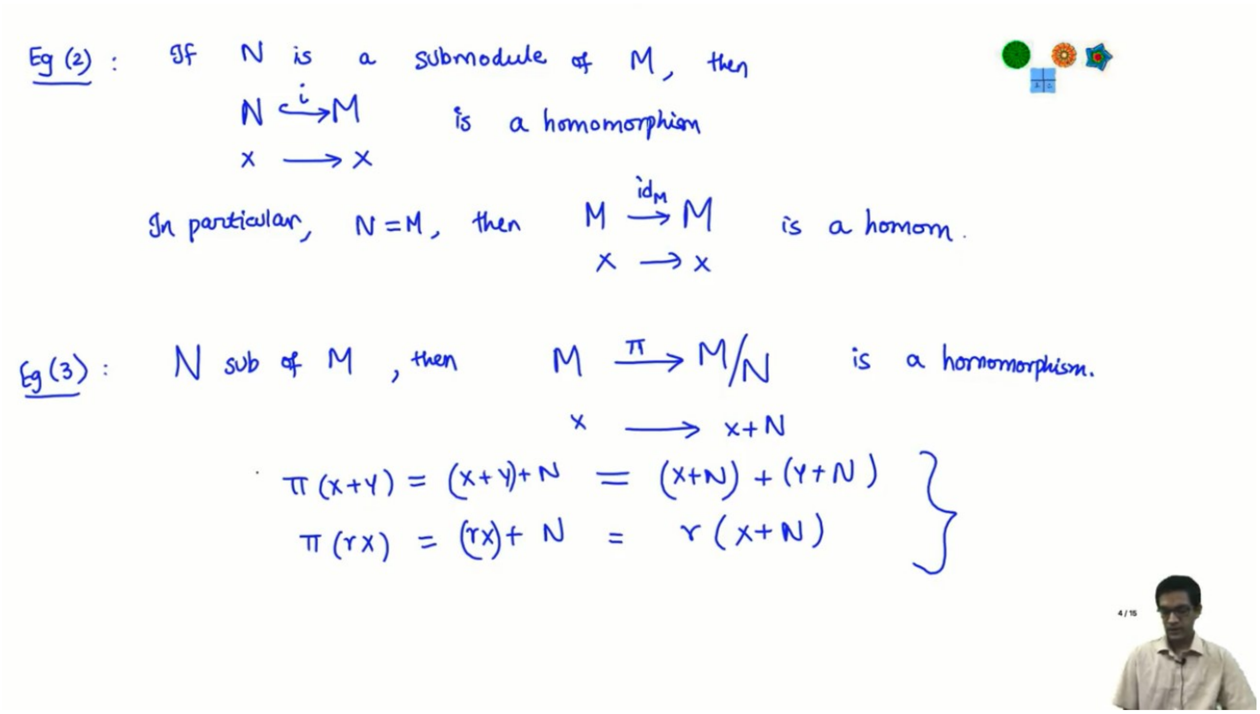


Similarly, if I take this scalar multiplication here $r \cdot x$ this $\cdot$ is scalar multiplication in M and the right hand side is scalar multiplication in N ok. Now one quick observation if you forgot for the moment that the modules had a scalar multiplication just think of them as Abelian groups under addition. Then a homomorphism if you just look at property 1 alone here in particular a homomorphism of R modules is in fact, a homomorphism of the underlying abelian groups M and N ok. So, observe that this property 1 says exactly that f is a group homomorphism of the group abelian group $(M+)$ to the abelian group $(N+)$ ok is a group homomorphism from $(M+) \to (N+)$ ok. Now, property 2 of course, says that in addition to being a group homomorphism it also respects the scalar multiplication ok.

Now let us look at examples. So, this is must be a familiar notion from linear algebra a map which preserves addition and scalar multiplication. So, this is what we call a linear transformation right. So, if $R = K$ a field and if M and N are . So, R modules therefore, they are K vector spaces , then homomorphism is exactly what we would call a linear transformation $f : M \to N$ is an R homomorphism means that f is a linear transformation of these two vector spaces ok .

So, it is just that familiar notion sort of imported to the context of modules over any ring . So, that is the the first example now here is a quick remark . So, of course, all these were defined for left modules ah, but there is it is not surprising how one defines homomorphisms for right modules ah, you just demand that it preserves the scalar multiplication on the right ok.

So, remark if M and N are right R modules , then a homomorphism a homomorphism is a map such that it preserves addition as before and it preserves sort of the right scalar multiplication . So, so recall I sort of spoke about this notational convention for right modules we often think of it as the the scalar sort of multiplying on the right ok. So, $f(x \cdot r) = f(x) \cdot r$. So, if you have a map satisfying these conditions then you would call it a homomorphism of



right modules ok. Now let us look at more examples. So, I talked about example 1 which is that of vector spaces and linear transformations . Example 2 so, a general class of examples if N is a sub module of M if N is a sub module of M then the inclusion map. So, from $N \to M$ there is what is called the inclusion map it is called I which does the following it takes each element to itself ok. So, it is just N is after all a subset of M. So, any element of N is necessarily an element of M as well. So, the inclusion map is; obviously, a homomorphism in fact, it is sort of trivially a homomorphism .

Because the you know $x + y$ of course, goes to $x + y$, rx goes to rx . So, the properties are are obvious. So, in particular if I take N equals M then the inclusion map becomes what is called the identity map right which takes every element to itself . So, this is usually denoted as id or id sub M this is of course, a homomorphism 2 ok. So, the identity homomorphism or the inclusion homomorphisms now example 3 let us take the same setting as before if N is a sub module of M if N is a sub of M by which I mean sub module then I consider the quotient. So, recall we talked about the quotient M by N which is the set of all cosets of N and M, now from M to the quotient I have what is called the projection map ok which is what does it do it takes each element x of M and maps it to its corresponding coset $x + N$ ok.

So, this projection map is a homomorphism ok, let us check this quickly this just follows from the way the addition and the scalar multiplication are defined on the right hand side on the quotient . So, let us check that $\pi(x + y)$. So, what is $\pi(x + y) = (x + y) + N$ it is just the coset of the the element $(x + N) + (y + N)$, but if you recall the definition this is exactly how addition is defined in the quotient module ok.

Now, $\pi(rx)$ similarly is just the it is the the coset of $rx + N$, but again by definition that is exactly how scalar multiplication was defined on the quotient module ok. So, these two equations here establish that this map π is in fact, a R module homomorphism. So, we have these natural classes of examples the inclusion and the projection maps .

Now, let us look for other examples. So, example 4 if we have a ring if we take our ring R to be the the ring of integers then recall that if I have two R modules . So, $\mathbb{Z}$ modules are the same as abelian groups ok this is the same as saying that M and N are really abelian groups ok. And what is a homomorphism now from $f : M \to N$ ok. So, homomorphism supposed to satisfy two properties $f(x+y) = f(x)+f(y)$. In other words it is a group homomorphism and it should satisfy this compatibility with respect to for all x and M compatibility with respect to scalar multiplication by elements of Z, but observe that this second property is superfluous we do not really need this one .

If the function satisfies the first property that $f(x + y) = f(x) + f(y)$ then the second property is automatically true ok this implies the second one automatically for $\mathbb{Z}$ modules and why is that because recall that f of. So, if r is an integer . So, let us say for the moment let us suppose r is a positive integer then recall that this scalar multiplication was just repeated addition.

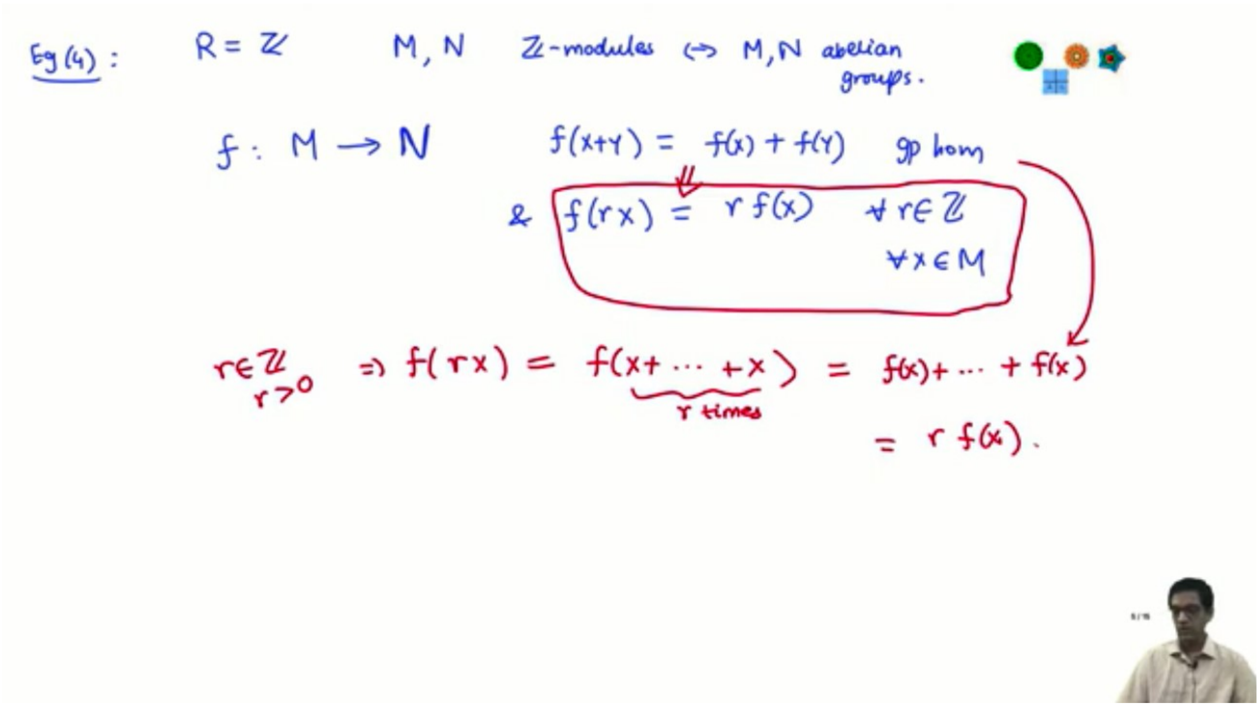
So, you just had to add x with itself $r \cdot x$ right, this is how we defined it and if the first property is true it means $f(x + x + ... + x) = f(x) + f(x) + ... + f(x)$ those many $\cdot$. This is just by using the first property alone that it is a group group homomorphism this implies this, but that is exactly the definition of how the element $rf(x)$ ok.

So, of course, I will just leave it for you to check that the same sort of thing holds if r is negative or 0. So, what this really says is recall we said if you a $\mathbb{Z}$ module is essentially the data of just the abelian group ok, the scalar multiplication is defined in terms of the addition and for homomorphisms a similar thing holds a homomorphism of $\mathbb{Z}$ modules is just a homomorphism of the underlying abelian groups the compatibility with respect to scalar multiplication just follows naturally as a corollary ok.

So, that is the fourth example . Let us do our other standard example which is the ring $K[X]$ of polynomials in one variable x. So, where K is a field and here again we know what. So, let us say M is an R module and recall that modules over the polynomial ring $K[X]$ are the same as well what is it it is like having a vector space V together with a linear operator on it ok.

So, where V is a some vector space over the field K. So, it is a K vector space where V is the K vector space and $T : V \to V$ is a linear operator ok and recall again from all our previous lectures that the element x the polynomial x acts as the linear operator T ok . Now, similarly let us take N that is also given to be an R module . So, let us assume that N corresponds to the pair (W, S) where W again is a K vector space and S is a linear operator on W ok. So, now, what we are going to do is to try and figure out what it means for a map $f : M \to N$ to be a homomorphism. So, suppose I give you a homomorphism of R modules of $K[X]$ module. So, suppose f from $M \to N$ is a homomorphism of $K[X]$ modules ok.

So, what does that mean ok. So, let us check what it means now let us go to the next page . So, observe that it just means that I have the additivity property. So, this means two things number 1 $f(v_1 + v_2)$ for all $v_1, v_2 \in V$. So, notice that you know when I say M and N are given by V and W. So, V and W recall are the underlying spaces. So, I should probably just replace M and N by the underlying vector spaces V and W ok. So, I the the set is V and W and I have a map between them which satisfies these two axioms number 1 $f(v_1 + v_2) = f(v_1) + f(v_2)$. So, this is the additivity .



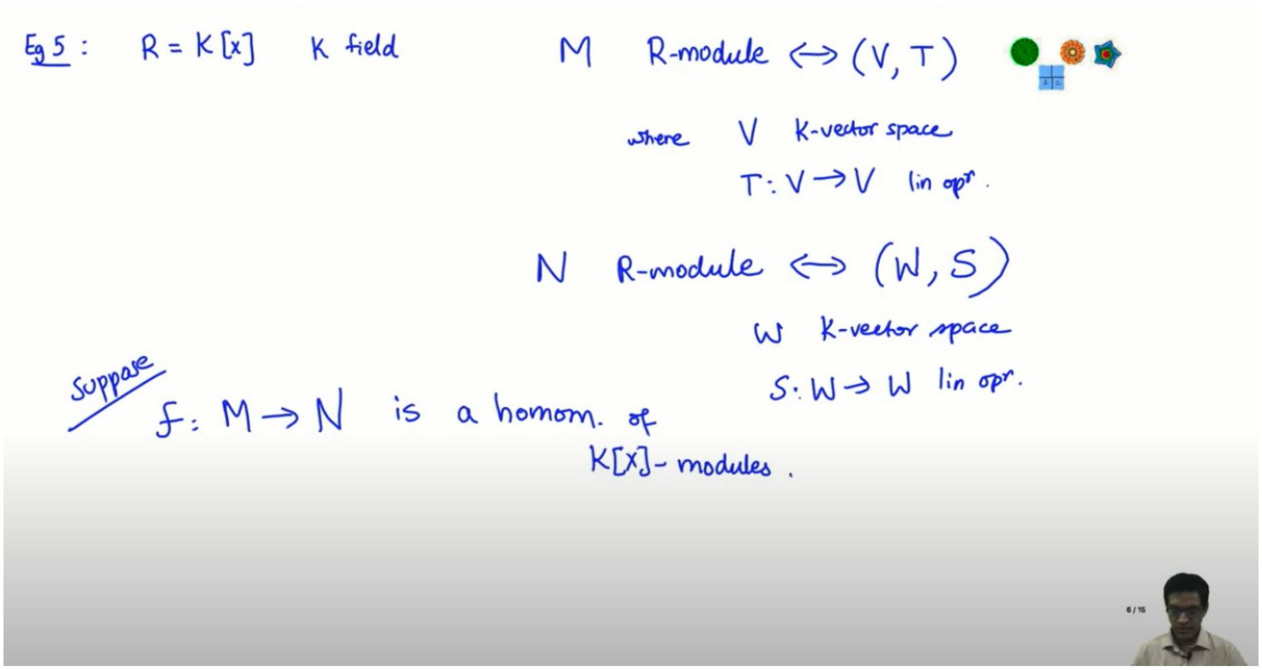
Second property is $f(rv) = rf(v)$ ok. So, let us try and analyze what the the second property means. So, we will try and understand this. So, let us do the following we will start out by so first let us take. So, case a let me take r to be an element of the field K itself ok r in general it can be any polynomial it is an element. So, remember this is $K[X]$. So, I should put in all polynomials in x there, but for a start I will just take the constant polynomials ok.

So, take r to be a constant polynomial . So, in this case the I know that this is true that $f(rv)$. So, which implies I conclude from property 2 . So, property 2 in particular implies that $f(rv) = rf(v)$ for all constant polynomials ok. Now, what does this mean this says that if I multiply v by a scalar from the field K that scalar can be pulled out ok . Now let us analyze this property so, I have this guy together with the additivity with the first property . So, now, put these two together and let us stare hard at it what does it tell us about f.

It says that f is a linear transformation of the vector spaces V and W ok. So, this the the 2 properties I marked in green are exactly the definition of $f : V \to W$ is a linear transformation ok of these vector spaces. So, linear transformation of the K vector spaces V and W ok or $V \to W$ really ok. So, that is only part of the data we have not use the full force of the hypothesis, we have concluded that at the very least f is a linear transformation from $V \to W$.

Now, let us do still more let us also take the polynomial x here. So, far we have taken r to only be the constant polynomial. So, case b let me take for r I will take the polynomial x^1 or x this is of course, a valid choice of scalar it is an element of the ring . So, now, I will plug this in and see what I get. So, remember $f(rv) = rf(v)$ for all $v \in V$. So, this again is for all $v \in V$.

Now, what does this imply since r is x this means that $f(x)$ acting on v should be x acting on $f(v)$ and recall that the action of x is exactly given by the action of the polynomial by the operator T . So, this is the same as S acting on $f(v)$ ok. So, this last equation comes



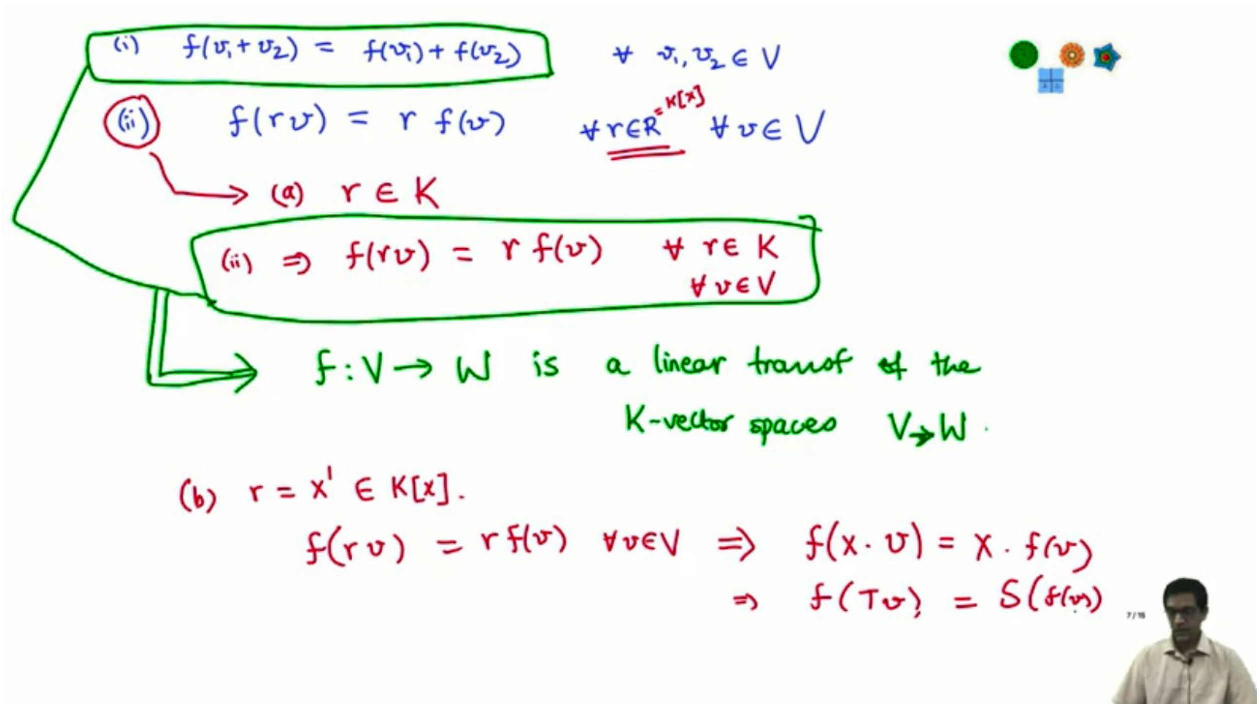
from realizing that the actions. So, this this data here exactly says that the polynomial x acts as T and the polynomial x acts as S on V and W respectively ok.

So, now, let us unravel this a little bit more. So, we have concluded the following that I have this operator f it is a linear operator from. So, f is a linear sorry linear transformation and second property I have conclude is that f composition T is the same as S composition f ok. So, that is what this this last equation says $f(T)v$ is the same as . So, this equation here you just saying that $f \circ T = S \circ f$.

Now, let us try to figure out where these compositions really live. So, remember $T : V \to V$ and $S : W \to W$. So, what does this say it says that $f \circ T = S \circ f$ ok. So, let me think of it as follows that let me draw T in the in the opposite direction it is a map from $V \to V$. So, let me think of it as going like this.

So, now observe what I am saying, I am saying that whether I you know. So, if I look at . So, maybe I should put the f here ok good. So, let me now draw it in the same direction. So, that this diagram is slightly more symmetrical. So, I would draw the diagram in this way. So, let me just put one more additional f on the bottom. So, what I have drawn is a diagram of these vector spaces V and W a little square of maps.

Now, let us observe what this this equality says about this diagram. So, it is says that if I look at $f \circ T$ means I first come along T and then go along f. So, it is it is this way I come from V and go down to W the other side $S \circ f$ is the other path I first do f and then I do S ok. So, what this identity is telling me is that whether I go along this this L here or this inverted L I get the same answer ok. So, this particular diagrammatic way of understanding such compositions. So, we usually say that this "diagram commutes." So, we draw this diagram and when we say this diagram commutes it just means that whether you go along one path or the other path the answer is the same ok and we usually put this little arrow here to say the diagram commutes ok .

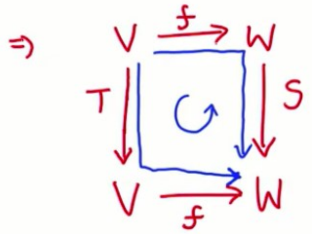


So, this is really what a homomorphism is between two $K[X]$ modules we have concluded that it must be a linear transformation which makes this diagram commute which such that $f \circ T = S \circ f$ok.

And of course, you can say that we still have not used the full force of the hypothesis we only plugged in r to be a constant and we took r equals x power 1 what about other polynomials what about r equals x square x cube what about $x+x+x$ square and so on . Now it turns out all of those do not really add any more information to this to this mix ok. So, if a function f satisfies these two properties that it is a linear transformation makes the diagram commute then it automatically ensures that it is a r linear map or a or a homomorphism ok meaning all the other r' s can also be pulled out.

So, let me just state that as my final conclusion ok. So, f from $V \to W$ is a $K[X]$ linear map . So, I am now using the alternate terminology for homomorphism. So, I will keep going switching back and forth between these various terminologies f from $V \to W$ is a $K[X]$ linear map if and only if f satisfies two properties number 1 f from $V \to W$ is K linear . In other words it is a linear transformation of i e is a linear transformation of these vector spaces and property 2 it makes the diagram commute the diagram commutes what diagram the one that I just do ok $V \to W$, $V \to W$ f, T, S this diagram commutes ok.

So, I claim that this is if and only if. So, I have shown one direction now I leave it as an exercise for you to show that the reverse is also true just having these two properties is enough to ensure that this map will actually be $K[X]$ linear ok and to do that you really have to show if x you know you can sort of pull the x out, then you can also pull out $x^2, x^3, x^4, ..$ and so on ok, it is the same sort of theme we have seen before ok .



f linear transf

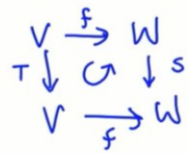
$f \circ T = S \circ f$

"diagram commutes"

Conclusion: $f : V \to W$ is a $K[x]$-linear map

⟺ (1) $f : V \to W$ is K-linear (i.e is a lin transf)

and (2) The dig commutes



8 / 15