Algebra - I

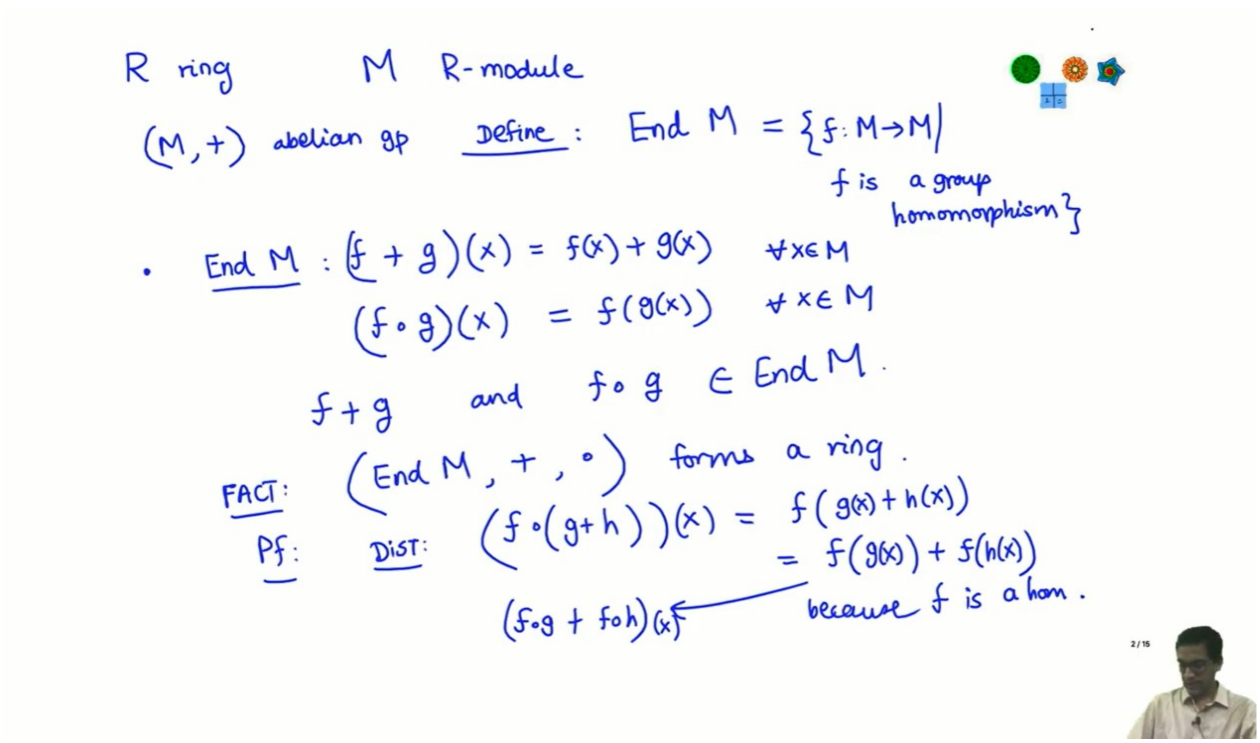
Prof. S. Viswanath & Prof. Amritanshu Prasad
Department of Mathematics
Indian Institute of Technology, Madras

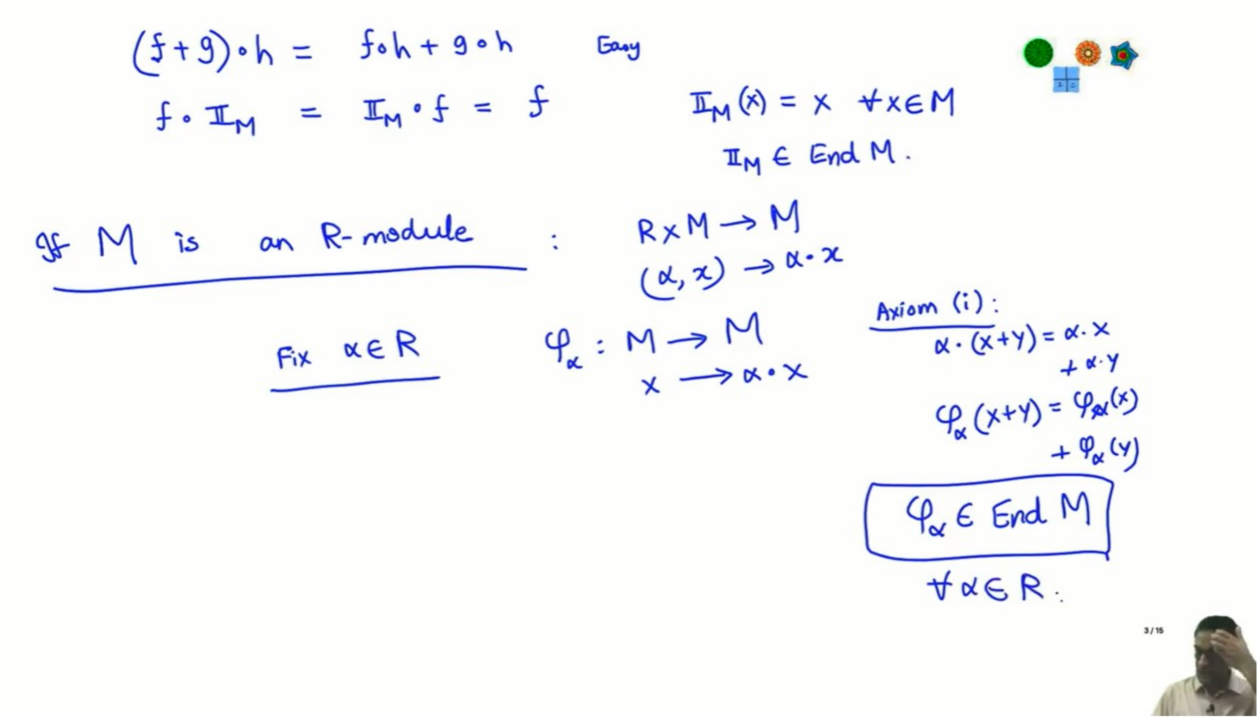
Lecture 53 [Modules:Alternative definitions]

Today, we will talk about an Alternative Definition of the Notion of Modules. So, we have seen the followingwe need a ring R and what is a module? So, M is suppose an R-module, then what does that mean? It means that M is an abelian group and it is got a scalar multiplication by scalars coming from the ring R ok . So, now, let us rephrase the axioms that scalar multiplication satisfies in a more compact form, ok. That is going to be our our goal for this lecture . So, let us first make some observations, that if M is an abelian group. So, recall $(M+)$ is in abelian group. Now, let me define something called End$(M.)$ So, where End stands for endomorphism's, by which we mean homomorphism's from the the group M to itself.

$$End(M) = \{f : M \to M | fis\ a\ group\ homomorphism\}$$

So, this is something that I can I can consider given in abelian group, I can look at the set of all homomorphism's from the group to itself . Now, the key observation is that, this this





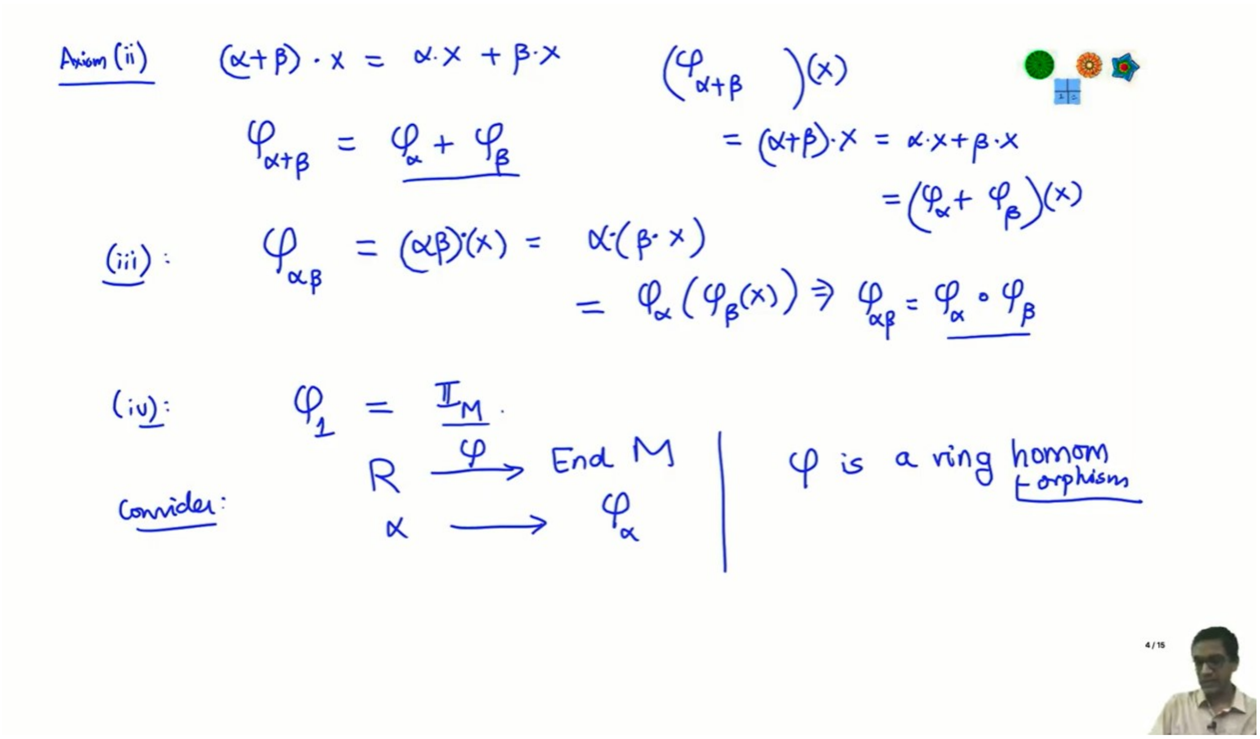
set End$M$ actually has some additional structure. So, what can I do End M itself has an addition operation. So, it has an addition what is the definition of addition? If, I take two homomorphism's f and g, then I can add them as follows. This is called point wise addition I can look at $(f+g)x = f(x) + g(x)$, this is for all $x \in M$ and this would of course, be also homomorphism as you can check easily. The second important observation is that I have a composition of maps.

So, I can look at $(f \circ g)(x) = f(g(x))$, this is for all $x \in M$. Now, $f \circ g$ is also a homomorphism. So, $f + g$ and $f \circ g$ are in fact, both elements of End$M$. In other words they are both homomorphisms from $M \to M$ ok . So, it is an easy verification which I will leave you to do . So, what does this mean? It means that the set End$M$ actually has two operations an addition and well a sort of multiplication, which is composition here .

And, the key fact here key observation is that with respect to these operations the set of all homomorphism's under point wise addition and composition forms a ring ok. So, this is a ring. Now, what does that entail? You need to check all the axioms of a ring .

So, addition of course, is commutative is easy to check. Ah. Composition of maps is an associative operation as you have no doubt seen before. And, what else is required the identity map? Ok. So, we need to show well distributivity as well . So, let us just check those two axioms . So, let us check the distributivity axiom that multiplication distributes over addition. So; that means, if I look at $f \circ (g + h)$, then that is got to give me $f \circ g + f \circ h$. So, let us compute what is this homomorphism on x? This is by definition $(f(g + h))x$.

But, the key key thing here is that f is a homomorphism. Therefore, f of a sum of two things is just going to be f of the first guy $+f$ of the second guy ok . So, this is because f is a homomorphism . So, that is the that is the first distributivity axiom, because well what is on the right hand side is exactly $f \circ g + f \circ h$. So, it is this guy evaluated at x by definition ok .

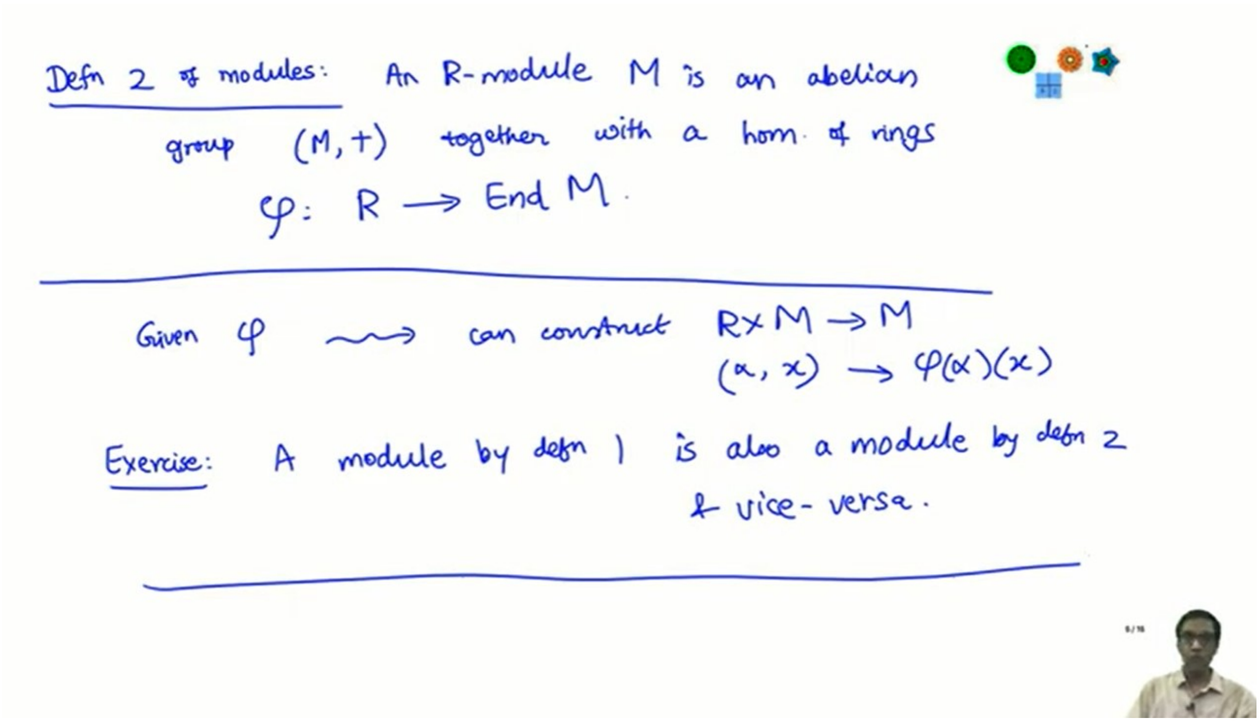


So, that is the first distributivity axioms you can check the the other one similarly if I take $f + g$ of x, $(f + g) \circ h$, this is in fact, simpler this is just directly by definition $f \circ h + g \circ h$ ok. Now, this is easy lastly let us check the identity axiom . So, I need to have an identity for the multiplication. And, of course, it is clear what the identity should be it is just the identity operator on M ok .

So, let us look at I_M which is the identity operator. Now, I_M is well it satisfies this property if you compose the identity operator, in either direction of course, it gives you back the original function ok. So, I_M is the identity map, it sends $x \to x$ for all $x \in M$, ok and that is a homomorphism. So, the key property here again is that the identity is in fact a group homomorphism , ok .

So, what that completes is the proof that the the set of endomorphisms forms a ring under these two operations, the point wise addition and the composition of maps ok. Now, let us try to well let us let us try to see what we can get out of this this new structure. So, suppose M is a so, if M is an R-module ok, that is given . So, what does that mean in addition to my additive group structure on M I am given this this map from $R \times M \to M$ right that is the scalar multiplication . So, what do I have? I have a map from $R \times M \to M, (\alpha\ , x\ )$ mapping to what we will call $\alpha \cdot x$, the the scalar multiplication of x by α. Now, this map let us try and and encode it in the following manner So, it is it is the very same information, but written slightly differently. So, let us do the following let us fix the α ok .

So, I fix a certain scalar in the ring and when I do that what it defines for me is a map from $\phi_\alpha M \to M$ ok. What map is this? It takes each element of M to $\alpha \cdot x$. So, α is fixed. So, this map of course, is dependent on α , but this is the scalar multiplication by α map ok. So, it is a map from $M \to M$. So, let us check what are it is properties? So, observe axioms so remember we have axioms for the scalar multiplication. So, axiom number 1 of modules



says that, if I take the scalar multiple of that is $\alpha \cdot (x + y) = \alpha \cdot x + \alpha \cdot y$ ok. In other words if I look at ϕ_α this map scalar multiplication map on $x + y$, it just gives me $\phi_\alpha x + \phi_\alpha y$. In other words ϕ_α is a group homomorphism .

So, this belongs to this set end M that we just constructed ok . So, ϕ_α belongs to end M for all α in R . So, that is the first observation that we are making. Now, the second observation is so the first axiom in is in some sense taken care of the first axiom just says that this map ϕ_α is a group homomorphism. Now, let us encode the remaining 3 axioms . So, let us look at axiom number 2 so, it said that so, this is axiom 2 of modules said that, if I take $\alpha + \beta$ and scalar multiplied by x the answer is same as $\alpha x + \beta x$ ok.

Now, in terms of this map ϕ_α this is what it says if I take the map ϕ_α, which is scalar multiplication by α, take the map ϕ_β. And, I construct their sum ok, this is now the sum in endomorph in the endomorphism ring of$M$, remember this just means it is the point wise addition . So, consider $\phi_\alpha +$ sorry consider $\phi_{\alpha+\beta}$ that is the left hand side, scalar multiplication by $(\alpha + \beta)x$. ; is the same as scalar multiplication by $\alpha +$ the scalar multiplication by β. In other words it is the pointwise sum of these two endomorphisms. And, this is true for all x . So, another way of of restating axiom ii is to say, that this map $\phi_{\alpha+\beta}$ is the sum of these two maps $\phi_\alpha + \phi_\beta$ ok, it is it is the pointwise sum ok .

Now, axiom iii similarly, you can already start seeing where this is going, the scalar multiplication by the product $\phi_{\alpha\beta}$, by the product $\alpha\beta$, this by definition is $\alpha\beta$ acting on x . But, that remember is the same as α acting on β acting on x , but that just means it is ϕ_α composed with $\phi_\beta(x)$.

So, this axiom 3 can be restated as follows $\phi_{\alpha\beta} = \phi_\alpha \circ \phi_\beta$ ok. And, axiom iv finally, just says that the identity map the identity element the scalar multiple multiplication by the identity just gives me the identity map ok. This just says 1 multiplied by x is x. So, what I have done is to recast the 4 axioms in terms of this map ϕ_αs that I define ok .

Now, all all of this can now further be recast as follows consider the map. So, let me now consider the following map. So, remember I had fixed α so far. Now, let me let α also vary. In other words let me look at the map . So, let us call this ϕ now. It takes each α to this scalar multiplication by α map ok. So, consider this map α going to ϕ_α .

Now, what we have shown is that axioms so the the foregoing discussion, axiom 1 says that ϕ_α is in the endomorphism axioms 2, 3 and 4 say exactly that ϕ is a ring homomorphism. Why is that? Well, because the the operation of addition in this ring End M is exactly this point wise addition the operation of multiplication in this ring is exactly this operation of composition, and the identity in this ring is exactly this this map I_M, ok .

So, these 3 axioms here just say say that this map ϕ is actually a ring homomorphism ok . So, and as you can easily check you can sort of go back the other way around as well. In other words if you are given a ring homomorphism you can from that construct a module in the usual sense of the word. So, here is the definition 2 of modules. So, let me give you the second definition of modules you can simply say an R module or this is all so; I am always talking about left modules So, like I said last time if I do not say anything I always mean left.

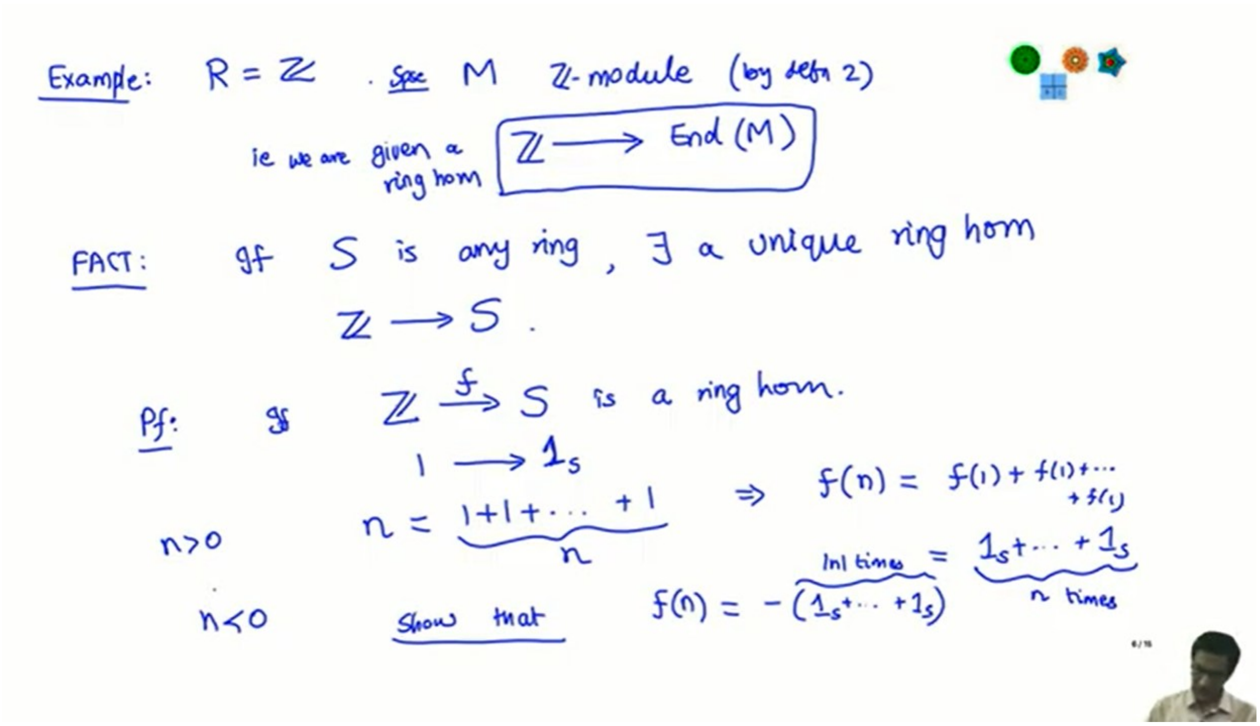
And, R-module M is an abelian group is an abelian group $(M+)$ together with a map, together with a homomorphism of rings, homomorphism of rings. Let us call it $\phi : R \rightarrow$ End$M$. This is an other way of defining a module, ok . So, what we have just seen is that if you use the first definition of modules, then from that you can construct this map ϕ ok. The map ϕ is just each α going to the scalar multiplication by ϕ_α map.

Conversely if I give you a module according to definition 2, it satisfies definition 2, then you can show that it it it satisfies definition 1 as well ok. In other words given this map phi, given such a map phi, you can construct, can construct the scalar multiplication map $R \times M \rightarrow M$ as follows, if I give you an (α, x).

Since, I am I I sort of know what my ϕ should be doing. So, I will just do the following I take ϕ I evaluate it on α. So, that gives me sort of the scalar multiplication map. So, it is an element of end M and I evaluate it on x ok . So, I can construct my scalar multiplication map in this way, ok . So, I am I am going to leave the details for you to check, check that a module by definition 1 is also module by definition 2 ok. In other words definitions 1 and 2 are equivalent ok, is also a module by definition 2 and vice-versa. These two definitions are equal.

And, the second definition is is sometimes convenient it is important to know this way of thinking as well , it is it is definitely far more compact right. It it sort of encapsulates all the axioms into one single statement, that you should have a map from $R \rightarrow$ End$M$ which is a ring homomorphism, ok. Now, let us look at some of our previous examples of modules and see how they they match up in this point of view? . So, let us do one particular example let us look at the case of the $\mathbb{Z}$ modules .

Example suppose my ring $R = \mathbb{Z}$ the ring of integers, then recall that a $\mathbb{Z}$ module by definition 1, we we more or less figured out that there is only one possible scalar multiplication that you can define on a module. And, that turns out to be just the you know the map which sends $(n\ ,\ x) \rightarrow x + x + ... + x$, n times ok . So, look back on the lecture the one of the previous lectures, but now I just want to see what I will get if I apply definition 2 ok. So, let us take R equals $\mathbb{Z}$ and let me say I I want to look at M, which is a module over $\mathbb{Z}$ according to my 2nd definition ok. So, by say the 2nd definition, what does that mean?

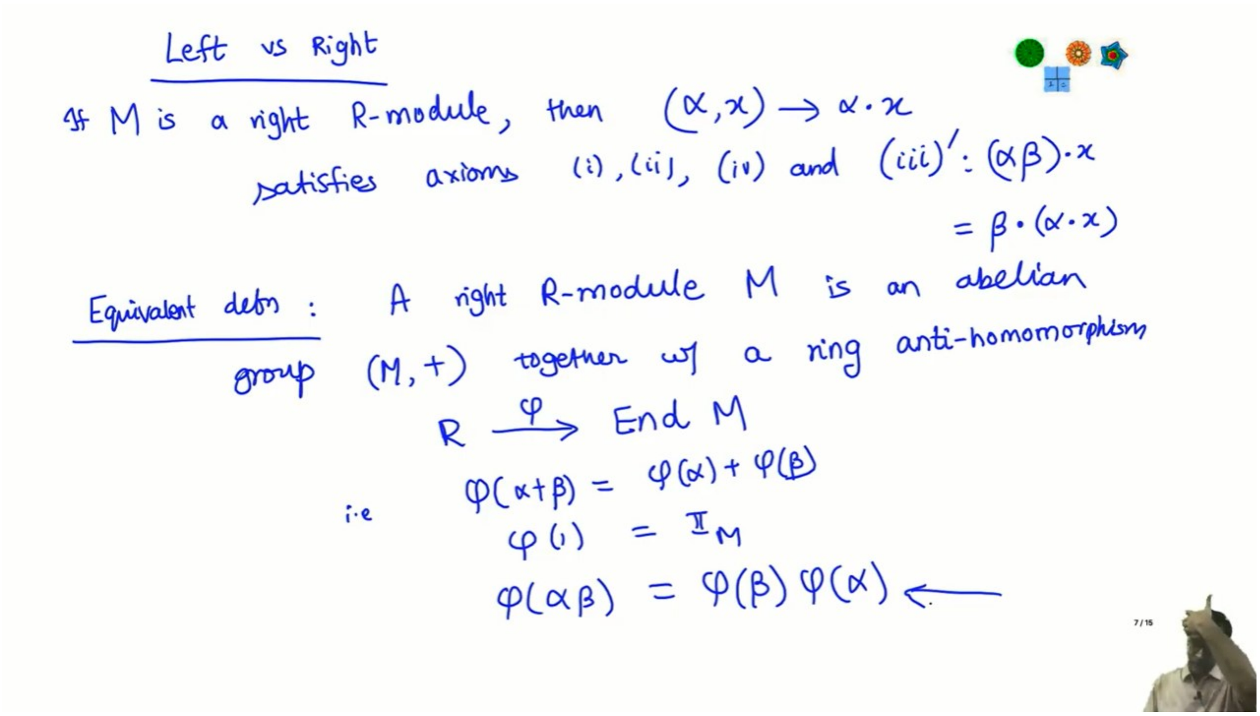


Suppose suppose M is a $\mathbb{Z}$ module according to my 2nd definition i e that just means what am I given we are given a map from so, we are given a a ring homomorphism, from the ring R to the ring of endomorphisms of M , ok. And, R here is just $\mathbb{Z}$, it is just the the the abelian group $\mathbb{Z}$ ok. Now, this is this is sort of the scalar multiplication map right, it keeps track of the scalar multiplication, i e we are given a ring homomorphism like this. Now , observe last time we we figured out that according to definition 1 there is just 1 module structure $\mathbb{Z}$ module structure you can give on an abelian group. You can not really make it a $\mathbb{Z}$ module in in any other way ok. Now, what that translates to here is that if you are trying to construct a ring homomorphism from the ring $\mathbb{Z}$,

To the ring End M well, then there is actually a unique ring homomorphism, ok. You cannot find two different ring homomorphisms from the ring $\mathbb{Z}$ to the ring End M, ok . So, claim or little fact, in fact, not just to the to the ring End M, if S is any ring, if S is any ring what is over in particular I can take S to be End$M$, there always exists a unique ring homomorphism from $f : \mathbb{Z} \to S$ ok. So, let us prove this, well the ring homomorphism from $\mathbb{Z}$ suppose I have a ring homomorphism f. So, suppose if f is a ring homomorphism .

So, observe that it has to satisfy many important properties in particular by definition the ring homomorphism sends identity to identity ok. So, the identity element so, let me call this multiplicative identity of S as 1_S. So, the integer 1 has to map to 1_S ok. That is one of the properties that a homomorphism should satisfy, but as we have seen before I mean this is sort of the calculation we did earlier. If, you know what 1 maps to then more or less everything is fixed ok, why? Because any other number $n = 1 + 1 + ... + 1$ n times ok .

So, this is just I take suppose n is positive then, I can write $n = 1 + 1 + ... + 1$. So, many times which means that this homomorphism f must map $f(\ n) \to= f(1) + f(1) + ... + f(1)$ so many times. In other words it has to map it to $1_S + 1_S + ... + 1_S$ added n times ok, $f(n)$ has to be this there is no other choice for n positive ok. So, similarly if n is negative. Now,



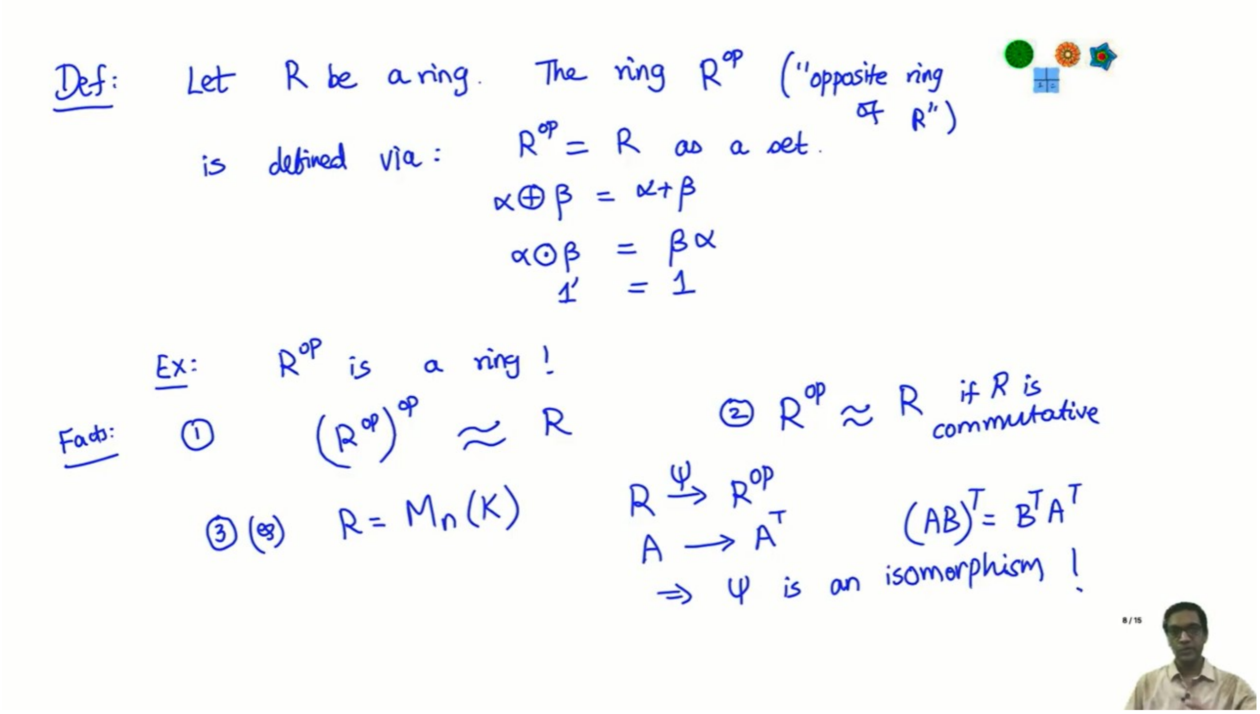
you you just have to do the same sort of calculation we did before f of 0 is 0 and therefore, $f(-n)$ ok. So, when n is negative show that .

So, let me leave this little step for you if n is negative show that f of n is just going to be minus of $f(n) = -(1_S + 1_S + ... + 1_S)$, n times, this is modulus of n times ok. And, and if n is 0 then of course, $f(0) = 0$. So, that is also one of the first things that one should have done if $n = 0$ then f has to map it to the additive identity of S ok .

So, if you are trying to construct a ring homomorphism from the ring $\mathbb{Z}$ to any other ring in some sense you have no choice everything is forced on you ok. And, that is really a reflection of the fact that there are if I give you an abelian group I can not really make it into a $\mathbb{Z}$ module in in any other way that is just one way of making it into a $\mathbb{Z}$ module um. So, so that is sort of very very clear from this this second definition from this way of thinking about it ok.

Now, let us look at left versus right modules. So, remember the axioms I had mentioned for modules. I also included axiom 3 dash if it were to be a right module, we said that it should satisfy axiom 3 dash, which says that ϕ I mean the α, so, recall so, suppose if M is right. If, M is a right module, if M is a right R module, then the scalar multiplication map $(\alpha, x) \to \alpha \cdot x$ satisfies axioms i, ii, iv . But, instead of iii, it satisfies axiom iii dash. And, if you recall what this was this says the product $(\alpha\beta)x$ should be $\beta(\alpha x)$ ok. So, the question is what does it become in you know from the second definition point of view? Ok.

So, let me just state it it should be more or less clear equivalent definition is the following analogous to the definition we gave for left modules . So, M is a right ok, what is the right module? A right module is an abelian group together with right module M is an abelian group, it is called the operation as + together with well what are we given we are given a map from $R \to End(M)$, let us call this map ϕ as before . Now, the property that ϕ has to satisfy is the following that, this is what is called a ring not a homomorphism, but what



sometimes called an anti homomorphism, $\phi : R \to End(M)$. In other words ϕ is well it is almost a homomorphism $\phi\ (\alpha + \beta\ ) = \phi(\alpha) + \phi(\beta)\phi(1) = I_M$. In this case the identity these two are ok, but $\phi(\alpha\beta) = \phi(\beta)\phi(\alpha)$.

So, it just goes in reverse ok. So, this is really what the axiom 3 dash now becomes that $\phi(\alpha\beta) = \phi(\beta)\phi(\alpha)$ ok. So, what this again means is that, you know right modules are almost the same as left modules instead of being given homomorphism to End M you are given a anti homomorphism you are given a map, which switches the order of these two numbers of of those two elements, ok .

So, this this switching of order of elements can sort of be again you know formulated as a as a new notion . So, this is what is called the opposite of a ring. So, let R be a ring, then the ring we define the ring are opposite . So, this is called the opposite ring of R . So, what is the opposite ring? Well, it is to say that this ring I must tell you what the operations are the ring R^{op} is defined via the following R^{op} is the same as R as a set, ok .

The underlying elements are the same as the elements before. What is the addition operation in this in this ring? So, let me now put a circle around it. So, this is a new operation. The new addition operation is the same as the old addition operation. The new multiplication operation is the same as the old multiplication operation, but carried out in reverse ok. So, this is the thing and the identity element will turn out to be the same as the the identity element of R, ok. So, this is the new identity same as the old identity. So, check that this makes R^{op} into a ring ok. So, here is an exercise, if I am given a ring I can consider or construct the opposite ring. So, exercise prove that R^{op} is in fact a ring ok.

Now, you know observe some obvious facts here, that if I take a ring R I construct it is opposite ring and I construct the opposite of the opposite ring. Then, it is just isomorphic to the original ring ok. Why? Because, the opposite ring involves interchanging the order and you interchange the order twice . So, that is the first property. Property 2 is that if the ring is commutative then this this opposite ring business is really not required. The opposite of ring is the same or is isomorphic to the original ring if R is commutative ok. So, for commutative rings the opposite is the same or isomorphic to the original. But, the converse is not necessarily true you can have if a ring is non commutative it can still be isomorphic to it is opposite ok .

And, a standard example of that is if I take the ring to be the ring of so, this is an example if I take the ring of $n \times n$ matrices. Then, the the so, what is the opposite ring mean, it means, if I give you two matrices A and B their new product is defined to be BA instead of AB ok. Observe that from the ring to it is opposite I can actually define a very natural nice map. This is a matrix going to it is transpose ok. And, this map psi observe the property of transposes that if you take AB and transpose it it is the same as B transpose A transpose right .

It switches the the transpose operations which is the order, what is this mean this just says that this map psi is in fact, a homomorphism of rings I mean you have to check it also satisfies the additivity and so on . So, let me leave you to check this that psi is in fact not just a homomorphism; it is actually a bijective homomorphism . So, it is an isomorphism of these 2 rings ok. So, the matrix ring is in fact, isomorphic to it is opposite ring by means of this nice map which is the transpose ok . So, you know what is the reason for wanting to construct the opposite of a ring.

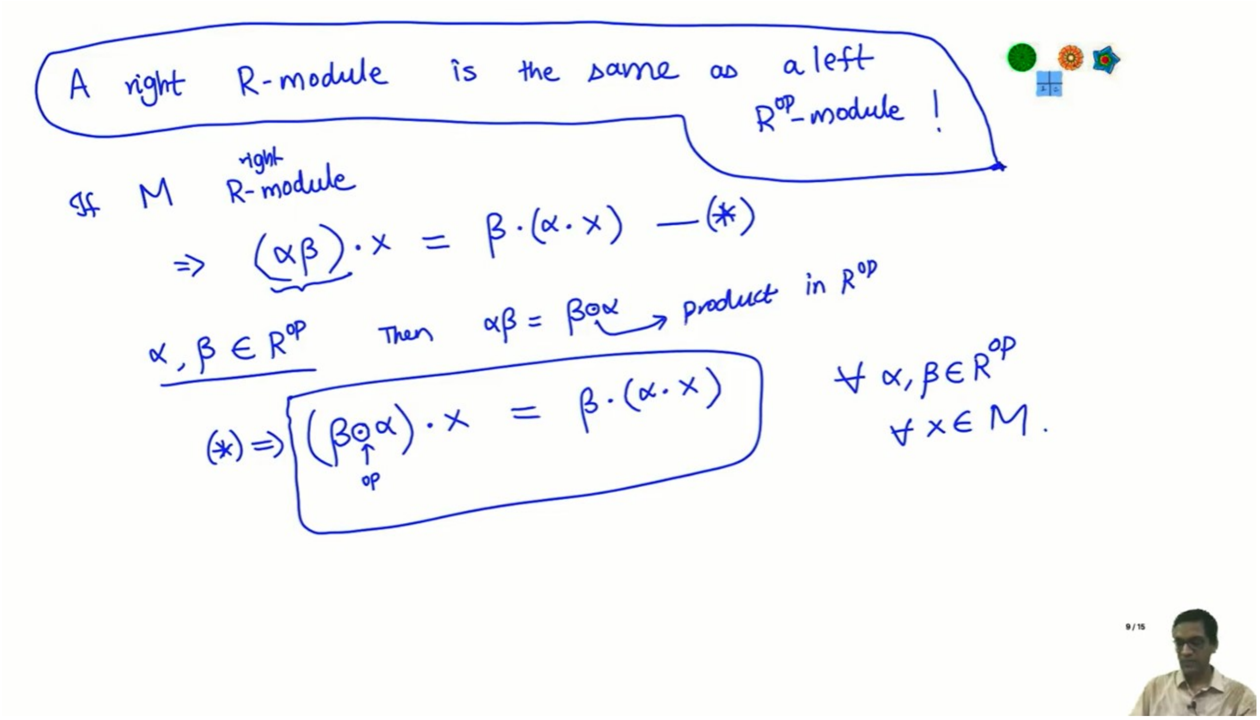
So, observe again that a right R module . So, here is the final important fact is the same as well or it becomes a left $R\ ^{op}$ module ok. Why is this? Because observe if I had a write module so if M were a right. So, it is a right R-module, if M is a right R-module which means let us look only at the axiom 3 which is the key difference . If, I take the product of $\alpha\beta$ and then act it on x, then the answer is just β acting on α acting on x right. So, that is the third that is axiom 3 prime this is what right module satisfy. But, this product $\alpha\beta$ that I have here, this is the product and the ring R. If, I think of α and β as being elements of the ring R^{op} now I mean R and R^{op} are really the same underlying set .

So, think of the elements α and β is coming from the opposite ring, then observe that this product $\alpha\beta$ that occurs here is actually in in the opposite ring it is the it is the product of of β with α ok . So, this is the product of the opposite ring product operation R^{op} ok. So, what does that mean? It means that if I rewrite this this identity this equation or axiom star .

Star can be rewritten as follows take β and multiply it with α, but do the multiplication in the opposite ring . So, this is the R^{op} [FL] multiplication, then multiply it with x. Then, the answer is the same as the right hand side just β acting on α acting on x ok. And, now this axiom as you can see is is axiom 3 right this is now in the correct order. So, remember this holds for all $\alpha\beta$ in the ring R .

So, I can like I said R and R^{op} are the same set and for all x in the module M ok . So, this new identity just means that if I consider M as an R^{op} module rather than as an R module, then it becomes a left module over R^{op} ok. So, this is the key key statement here right modules over the ring are the same as left modules over the opposite opposite ring .

And, so, in some sense whatever we prove for left modules will automatically hold for right modules with sort of the appropriate modification in notation and so on ok. So, we will usually only talk about left modules for this reason, that you can quickly convert any result about left modules right modules by just looking at this opposite ring construction, but that is not to say that right modules are not important.



In fact, they will turn out to be extremely important in many things that come up. In fact, what is also very important is modules, which have both I mean what are called bi modules modules which are both left and right modules and so on ok. So, it is it is equally important to keep thinking about left and right modules, ok. We will stop .