

Algebra – II
Professor Amritanshu Prasad
Mathematics
Indian Institute of Mathematical Sciences
Lecture 82
The Endomorphism Ring of an Indecomposable Module

(Refer Slide Time: 0:14)

Endomorphisms of an indecomposable module

R ring, $M : R$ -module ◀

$\text{End}_R M = \text{Hom}_R(M, M)$ is a ring.

Example: $\text{End}_R R = \{ \varphi_a : r \mapsto ra \mid a \in R \}$.

$$\varphi_a \varphi_b(r) = \varphi_b(r)a = (rb)a = r(ba)$$

$$= \varphi_{ba}(r)$$

So $\text{End}_R R = R^{\text{opp}}$.



In the next lecture, we will be proving the Krull-Schmidt theorem which says that the decomposition of a module that satisfies the ascending chain condition and the descending chain condition into indecomposable, into sum of indecomposables is essentially unique.

In that proof there is a certain technical lemma that is required and that basically involves understanding the endomorphism ring of any indecomposable module, and that is what I am going to do in this lecture. We are going to study the endomorphism ring of indecomposable module.

So if R is a ring, M an R -module, we have seen that we can think of this $\text{End}_R M$ which is nothing but R module homomorphisms from M to M , which we can think of is the arrows from M to M in the category of R -Modules. And this is in fact a ring because we can add two homomorphisms point wise and we can also compose them giving rise to associative product on this ring.

So for example simplest example, well may be not simplest, but the most very interesting example is that if you take any ring R and you look at R itself as a left R module, then this is isomorphic to $\text{Hom}_R(R, R)$, which is the, this is the same actually as, so endomorphism is given by $\text{Hom}_R(R, R)$ which gives r to r times a for every a and r .

You can check that $\text{Phi } a$ is in R module endomorphism and conversely given any r module endomorphism of r , the moment you know where it takes one it takes one to some element a , you can show that is actually equal to $\text{Phi } a$.

And here we have $\text{Phi } a$ composed with $\text{Phi } b$ of r , well that turns out to be $\text{Phi } b$ of r multiplied by a , but $\text{Phi } b$ of r is r times b so this is r times b times a . But that is $r b a$ by associativity, and that is just Phi of $b a r$. So $\text{End}R$ is not exactly R , it is very opposite to R , where the order of multiplication is reversed.

So now we will be interested in the endomorphism ring of an indecomposable R module, and the property that we will be interested is the fact that it is what is called a local ring. So for our purposes we will take the following as the definition of a local ring. I am sure most of you are familiar with some of you are familiar with notion of a local ring for a commutative ring, may be you are not all familiar with the local ring which is non-commuting.

(Refer Slide Time: 3:30)


So $\text{End}_R R = R^{\text{op}}$.

Defn: A ring R is called a local ring if its set m of non-units is a two-sided ideal.

Recall: $I \subset R$ is called an ideal if

- $(I, +) \subset (R, +)$ is a subgroup
- $a \in I, r \in R \Rightarrow ar \in I$ and $ra \in I$.

Example: $\mathbb{Z}/p^k\mathbb{Z}$ is local.
 \mathbb{Z} is not local
 $M_n(K)$ (K a field) is not local.



But we will just give a very simple definition a ring R and this we will be applying not to the original ring R whose module we are looking at but whose endomorphism ring, but this definition is general. A ring R is called a local ring if its set m of non-units that means elements which do not have an inverse, is a two sided ideal.

What is the meaning of an ideal? You can recall from Algebra 1, I is called an ideal if firstly I is a sub group of the additive group. Then secondly, it is closed under left and right multiplication by arbitrary elements of R . So if a belongs to I , r belongs to R then that implies that ar belongs to I and ra belongs to I .

And that is it, so these are the two conditions. And sometimes we would ask for a left ideal which only satisfies the second condition or a right ideal which only satisfies the first condition, but here we are looking at two sided ideals.

So let us just look at some examples to fix this portion. $Z \text{ mod } P$ to the k Z is local. The non-units are precisely the elements which are multiples of P , and so they form an ideal here. Z is not local, and matrices, let us just stick to fields for now. Is this local or not?

Well you can show that if you take any non-0 element of any non-0 matrix then the two sided ideal, the smallest two sided ideal that contains it is the entire matrix. So there is lots of non-units in M and k that is matrices which are not of full rank, but they do not unfortunately form an ideal. So this is not local.

(Refer Slide Time: 6:46)

Theorem: Let M be an indecomposable R -module satisfying the ACC and the DCC. Then $\text{End}_R M$ is a local ring.

Lemma (Fitting): If M is as above, and $g \in \text{End}_R M$, then either g is a unit, or g is nilpotent. ($g^n = 0$ for some $n \in \mathbb{N}$)

Pf: Take $g \in \text{End}_R M$
 $M \supseteq g(M) \supseteq g^2(M) \supseteq \dots$
 By the DCC $g^n(M) = g^{n+i}(M) \forall i \geq 0$ for some $n \in \mathbb{N}$.

And now for the main theorem of this lecture, so theorem is let M be an indecomposable R module satisfying the ACC and the DCC, then $\text{End}_R M$ is a local ring. So before proving this, we will prove a certain lemma, and this lemma is due to a mathematician called Fitting.

And it says that if M is as above or maybe we just need if M satisfies the DCC in fact. Well, let us just keep it M is as above, and g belongs to $\text{End}_R M$, then either g is a unit, or g is nilpotent. Recall that nilpotent means that, nilpotent means that g to the n is equal to 0 for some n belonging to \mathbb{N} . Some power of g vanishes.

So let us prove Fitting's lemma, and so what you do is consider, take any g in $\text{End}_R M$, and you consider M , well it contains as a sub module the image of g under M which in turn contain g squared M and so on. Now because of the descending chain condition there is some

stage after which this sequence stabilizes. So by the DCC, g to the n M is equal to g to the n plus i M for all i greater than or equal to 0, for some natural number n in N .

(Refer Slide Time: 10:05)


$M - g^{2n}M = 0$
 By the DCC $g^n(M) = g^{n+i}(M) \forall i \geq 0$ for some $n \in \mathbb{N}$.
 In particular, $g^n(M) = g^{2n}(M)$,
 i.e., $g^n : g^n(M) \rightarrow g^{2n}(M)$ is an isomorphism.
 $\forall x \in M, \exists y \in M$ such that $g^n(x) = g^{2n}(y)$
 $x = \underbrace{g^n(y)}_m + \underbrace{x - g^n(y)}_n$ $g^n(x - g^n(y)) = g^n(x) - g^{2n}(y) = 0$
 $\text{Im}(g^n) \quad \text{Ker}(g^n)$
 also, $\text{Im}(g^n) \cap \text{Ker}(g^n) = \{0\}$.

And what this means is that in particular, g to the n M is equal to the g to the power $2n$ M . Or another words, g to the power n is an isomorphism from g to the power n M to g to the power $2n$ M . So now let us proceed further, so if x is in M then there exists y in M such that g to the power n x is g to the power $2n$ y . Just because g to the power n M is g to the power $2n$ M . So I can write x as g to the power n y plus x minus g to the power n y .

Now let us look at this these two parts of the sum, this belongs to the image of g to the power n and this, well if I apply g to the power n to this, so I take g to the power n x minus g to the power n y then I will get g to the power n x minus g to the power $2n$ y , which is 0 because g to the power $2n$ y is equal to g to the power n x . So this belongs to the kernel of g to the power n .

So I have written x as the sum of two thing, one in the image of g to the power n and the other in the kernel of g to the power n . Moreover, g to the power n when restricted to g to the power n M is an isomorphism and therefore it has no kernel in g to the power n M . So, also we have that g to the power, image of g to the power n intersection with the kernel of g to the power n is 0.

(Refer Slide Time: 12:30)

$$\begin{aligned} & \text{also, } \text{Im}(g^n) \cap \text{ker}(g^n) = (0). \\ & \therefore M = \text{Im}(g^n) \oplus \text{ker}(g^n). \\ & \text{Since } M \text{ is indecomposable. So either} \\ & \cdot M = \text{Im}(g^n) \\ & \cdot M = \text{ker}(g^n) \quad [g \text{ is nilpotent}] \\ \hline & \text{If } \text{Im}(g^n) = M \quad g \text{ is surjective.} \\ & g: M/\text{ker}(g) \rightarrow M \text{ is an iso.} \\ & \Rightarrow l(M/\text{ker}(g)) = l(M) \end{aligned}$$


Theorem: Let M be an indecomposable R -module satisfying the ACC and the DCC. Then $\text{End}_R M$ is a local ring.

Lemma (Fitting): If M is as above, and $g \in \text{End}_R M$, then either g is a unit, or g is nilpotent. ($g^n = 0$ for some $n \in \mathbb{N}$)

Pf: Take $g \in \text{End}_R M$

$$M \supset g(M) \supset g^2(M) \supset \dots$$

By the DCC $g^i(M) = g^{n+i}(M) \forall i \geq 0$ for some $n \in \mathbb{N}$.

So what we get is the direct sum decomposition of M . So, but M is indecomposable so there are only two possibilities, one of the summands is the whole thing. So either M is the image of g to the power n or M is the kernel of g to the power n . Now M is the kernel of g to the power n means that g is nilpotent, and that was a one of options in Fitting's lemma, in Fitting's dichotomy so to speak. And so we just need to check that if M is the image of g to the power n , then g is in fact an isomorphism, a unit in $\text{End}_R M$.


So let us just look at that, so if image of g to the power n is equal to M for some n , then what we have is that g is surjective. Therefore, what we have is that g , if you take from M mod kernel of g to M , is an isomorphism. But that means that the length of M mod kernel of g

remember M satisfies both the ascending chain condition and the descending chain condition, and therefore it is a finite length, it has a Jordan-Holder series and it is a finite length.

(Refer Slide Time: 14:48)

$M = \text{Ker}(g^n)$ [g is nilpotent]


 If $\text{Im}(g^n) = M$ g is surjective.
 $g: M/\text{ker}(g) \rightarrow M$ is an iso.
 $\Rightarrow l(M/\text{ker}(g)) = l(M)$
 $\Rightarrow \text{ker}(g) = 0$
 $\Rightarrow g$ is also injective and hence an iso.



Theorem: Let M be an indecomposable R -module satisfying the ACC and the DCC. Then $\text{End}_R M$ is a local ring.

Lemma (Fitting): If M is as above, and $g \in \text{End}_R M$, then either g is a unit, or g is nilpotent. ($g^n = 0$ for some $n \in \mathbb{N}$)

Pf: Take $g \in \text{End}_R M$
 $M \supseteq g(M) \supseteq g^2(M) \supseteq \dots$
 By the DCC $g^n(M) = g^{n+i}(M) \forall i \geq 0$ for some $n \in \mathbb{N}$.

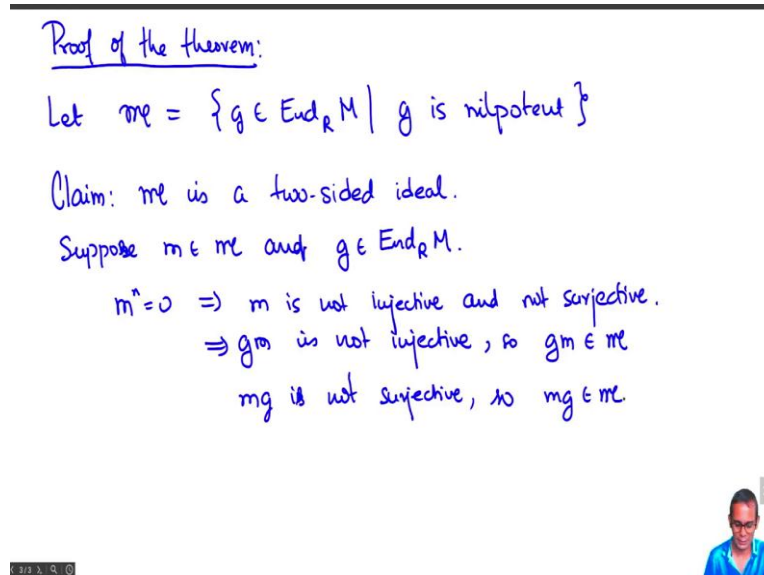


So the length of $M \text{ mod kernel } g$ is the same as the length of M , but this is only possible if a kernel of g is 0 because you could take a Jordan-Holder series for M and then pull it back here via this isomorphism and get a composition series of length 1 greater by adding kernel g to it. The only way this can happen is that kernel g equals 0 which implies that g is also injective and hence an isomorphism.


So we have completed the proof of Fitting's lemma that if g is an endomorphism of n then either it is a unit, i.e. it is an isomorphism or it is nilpotent. That lemma was the most

technical part of the proof of the main theorem and now we can proceed with the proof of the theorem.

(Refer Slide Time: 15:44)



Proof of the theorem:
Let $\mathfrak{m} = \{g \in \text{End}_R M \mid g \text{ is nilpotent}\}$
Claim: \mathfrak{m} is a two-sided ideal.
Suppose $m \in \mathfrak{m}$ and $g \in \text{End}_R M$.
 $m^n = 0 \Rightarrow m$ is not injective and not surjective.
 $\Rightarrow gm$ is not injective, so $gm \in \mathfrak{m}$
 mg is not surjective, so $mg \in \mathfrak{m}$.



So, proof of the theorem. Well we will take \mathfrak{m} to be the set of all nilpotent elements in $\text{End}_R M$, i.e. g to the power n is 0 for some n , and we will show that \mathfrak{m} is a two sided ideal. And of course we know that the complement of \mathfrak{m} consists of units and so we will have to prove the theorem.

First we will show that \mathfrak{m} is closed under left and right multiplication by elements of $\text{End}_R M$. So suppose m is in \mathfrak{m} and g is in $\text{End}_R M$. Now since m is in \mathfrak{m} , m is nilpotent. So m to the power n equals 0, implies firstly that m is not injective. It also implies that m is not surjective, it is also not surjective.

So that means that if you take g times m , this is not injective. So it is not a unit, but we saw that every element is not a unit is in \mathfrak{m} . And this also implies that mg , the original statement here, is not surjective, because m is not surjective. So mg again belongs to \mathfrak{m} , because the complement of \mathfrak{m} consists only of units. So \mathfrak{m} is closed under left and right multiplications, multiplication by elements of $\text{End}_R M$. Now it only remains to show that the sum of two elements of \mathfrak{m} is in \mathfrak{m} .

(Refer Slide Time: 18:25)

To prove: $m_1, m_2 \in m \Rightarrow m_1 + m_2 \in m$.

Suppose $m_1 + m_2 \notin m$. Then $(m_1 + m_2)g = \text{id}_M$ for some $g \in \text{End}_R M$.

Let $n_1 = m_1 g$, $n_2 = m_2 g$.

$n_1, n_2 \in m$,

And $n_1 + n_2 = \text{id}_M$.


So $n_2 = \text{id}_M - n_1$, $n_2^k = 0$ for some $k \in \mathbb{N}$.

$$n_2 (\text{id}_M + n_1 + \dots + n_1^{k-1})$$

$$= (\text{id}_M - n_1) (\text{id}_M + n_1 + \dots + n_1^{k-1}) = \text{id}_M$$

contradicting $n_2 \in m$.

Conclusion: $\text{End}_R M$ is a local ring.



Now to prove that, m_1, m_2 are in m then m_1 plus m_2 is in m . We will prove this by contradiction. Suppose m_1 plus m_2 is not in m , then it is a unit. So I can find some element m such that m_1 plus m_2 times m is the identity for some let us not say m , for some g in $\text{End}_R M$.

And let us call this n_1 equals $m_1 g$, n_2 be $m_2 g$ then because m is closed under left and right multiplication by arbitrary elements of $\text{End}_R M$, this n_1 and n_2 again belong to m . And moreover, n_1 plus n_2 is the identity element. So what we have is that n_2 equals identity minus n_1 , and let us say, since n_2 is in m , n_2 is nilpotent, n_2 to the power k equals 0 for some k .

So let us say that this also holds, then what we have is that n_2 times 1 plus n_1 , no I want n_1 to the power k , plus n_1 plus n_1 to the power k minus 1, well that is equal to a identity. Here this is not 1; this is identity of M , minus n_1 into identity of M plus n_1 plus n_1 to the power k minus 1.

Now when you multiply these two out, the sum will telescope and terms will cancel out. And you will only be left with identity of M minus n_1 to the power k which is 0. So then what happened, n_2 has become a unit but that is a contradiction, because we assume that, we know that n_2 is in m , so it is nilpotent. And so m_1 plus m_2 must again be an element of m . And so $\text{End}_R M$ is a local ring as acquired because all non-units form a two sided ideal.