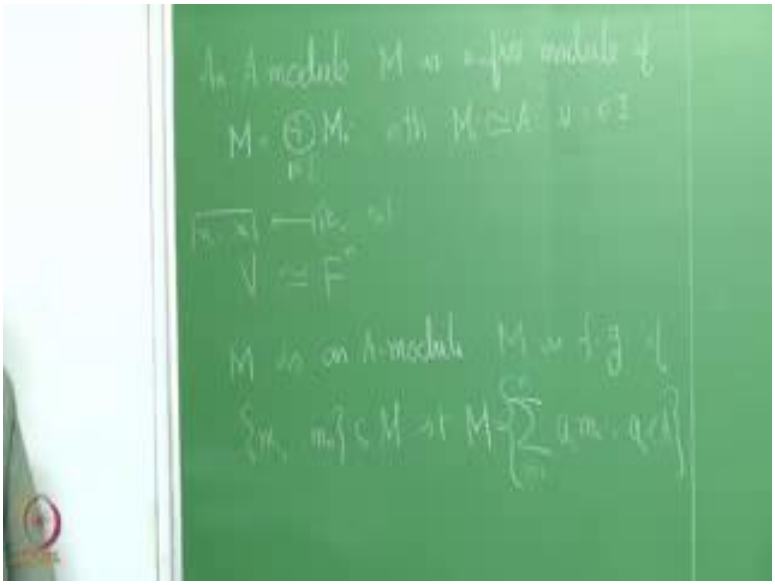
Commutative Algebra
Prof. A.V. Jayanthan
Department of Mathematics
Indian Institute of Technology, Madras

Lecture – 11
Module Homomorphism and Determinant Trick

(Refer Slide Time: 00:28)



We were talking about free modules last time. So, an A module M is a free module, if M is equal to the direct sum of M i, i in some indexing set I with M i isomorphic to A for all i in I. So, we know that see if you take a vector space [vocalized-noise]; finite dimensional vector space then we know this is isomorphic to F n, V is a finite dimensional vector space or a field F then V is isomorphic to F n where n is the dimension of V.

Now, I take a module M, M is an A module, what is meant by this being finitely generated?

Student: (Refer Time: 02:00).

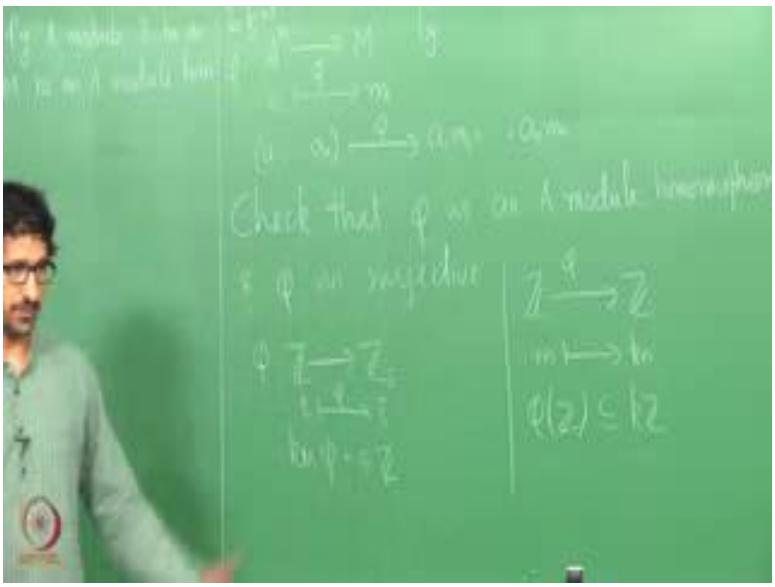
M is finitely generated if I can find some m 1 up to m n such that M is equal to summation a i, m i, i from 1 to n, a i belong to A. You can write every element of M as a linear combination like this of course, we have already seen that you know one does not have analogues of.

Student: Basis.

Basis.

Right, we need not have any I mean any finitely any generating set need not be you know reduced to any linearly independent finitely, I mean generating set. So, we might not be able to expect something like this, but still looking at this can you think of some linear maps or you know homomorphism.

(Refer Slide Time: 03:26)



Student: (Refer Time: 03:18) the coefficient.

From where to where?

Student: (Refer Time: 03:20).

From, so here we could think I mean given a basis V 1 up to V n we usually define a map from F n to here, e i the standard basis being map to the spaces. So, here again similarly one can think of a map from

Student: A n to M.

A n to M right, n e i being map to.

Student: M i.

M i or in other words if you take any n tuple this is being map to a 1 m 1 plus etcetera a n m n. This is a homomorphism define phi from a n to M by or phi of any a 1 up to a n is a 1 m 1 plus etcetera a n m n this is again inspired by the definition of you know linear transformation in the case of vector spaces in a similar situation. But now, so what we have obtained is that homomorphism, an A module, so this is check that phi is an A module homomorphism. What more can we say about this homomorphism?

Student: (Refer Time: 05:34).

This is onto and phi is surjective, is this injective? Need not necessarily be injective, for example, if you have, if you take map from Z to Z n I mean Z 5, this is a finitely generated Z module, a generator of this is 1 to any one of them is a generator here. So, if you take 1 going to 1 bar then there is a kernel here, kernel phi is what does kernel phi here?

Student: 5 Z.

5 Z, this is Z mod 5 Z the natural map from a to a mod i the kernel of the natural map from a to a mod i is i kernel is i. So, therefore, this is, this has a kernel. So, this in general need not be injective, but what we can say is that there exists if M is finitely generated there exists an A module homomorphism from A n to M a finitely generated free module this is a finitely generated.

Student: Free Module.

Free module and there exists a onto homomorphism from A n to M.

(Refer Slide Time: 07:30)

Suppose conversely suppose there exists a finitely generated free A module say F and an A module homomorphism phi from F to M which is onto, what can you say about M?

Student: M finitely generated.

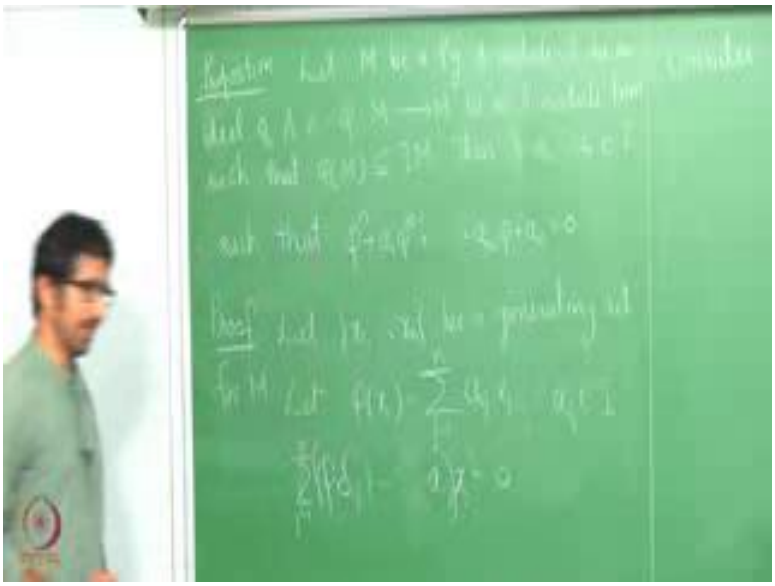
M has to be finitely generated. In fact, you can very specifically mention what I mean get a finite generating set.

Student: (Refer Time: 08:37).

So, let F be isomorphic to A power n then and let, this is isomorphic (Refer Time: 09:00) psi and let you know f i be psi i of e i then and M i be equal to psi e i and phi of f i then m 1 up to m n is a generating set for M. So, what we have proved now is let M be an A module then M is finitely generated, if and only if there exists finitely generated free A module F and a surjective homomorphism phi from F to M. For the converse part we do not need the free condition here, if I have a finitely generated module M; finitely generated module F and a surjective homomorphism then M is also finitely generated.

Now, finitely generated modules are very special they behave very well, I mean as in the case of finite dimensional vector spaces, particularly when the ring is also nice which we will see later when the ring is Noetherian.

(Refer Slide Time: 11:40)



So, first of all let us look at one important property of modules finitely generated A modules. So, let me state the result let M be a finitely generated A module, I be an ideal of A and phi be an A module homomorphism such that phi of M is contained in IM, phi of M is contained in IM. What does this mean? Say for example, if I have Z to Z, M going to some k n fixing a k this is a Z module homomorphism and this if I call this phi then phi of Z is contained in k Z. So, if you take I to be the ideal generated by k then this is you know phi Z is contained in phi of M is contained in IM that is the condition that we are looking at here.

Suppose there exists an ideal I with this property then there exists a naught a 1 up to a n in I such that phi power n plus a 1 phi power n minus 1 a n minus 1 phi plus a n is 0. So, this is as a.

Student: (Refer Time: 14:15).

As an element in.

Student: N.

No, what is phi? Phi is a homomorphism. So, what is meant by phi square?

Student: (Refer Time: 14:30).

What does phi square?

Student: (Refer Time: 14:33).

Exactly, so this as an element in Hom A M M this has another name called set of all endomorphism of M as an element of the endomorphism. This, see we have seen that Hom for any modules M and M, Hom A M comma M is A module, A module; if you know if I look at this Hom M M this has a natural multiplication, what is that?

Student: (Refer Time: 15:27).

The composition, if I take f and g, f times g is?

Student: (Refer Time: 15:36).

Their composition that is again a homomorphism that will again be an endomorphism of M, but now this ring is not commutative f times g is not equal to g times f, but this is indeed a ring with respect to the addition and multiplication this is indeed a ring.

Now, what this says? What this says is that I can you know I get a linear combination of identity phi square up to phi power n in the endomorphism ring whose linear combination is a 0 map. Does this look somewhat familiar you know, put this in the situation of in the vector spaces or does this look somewhat familiar?

Student: Sir, I have a question.

Yes.

Student: In the previous position you said that (Refer Time: 16:58).

Yeah.

Student: But then we used (Refer Time: 17:03).

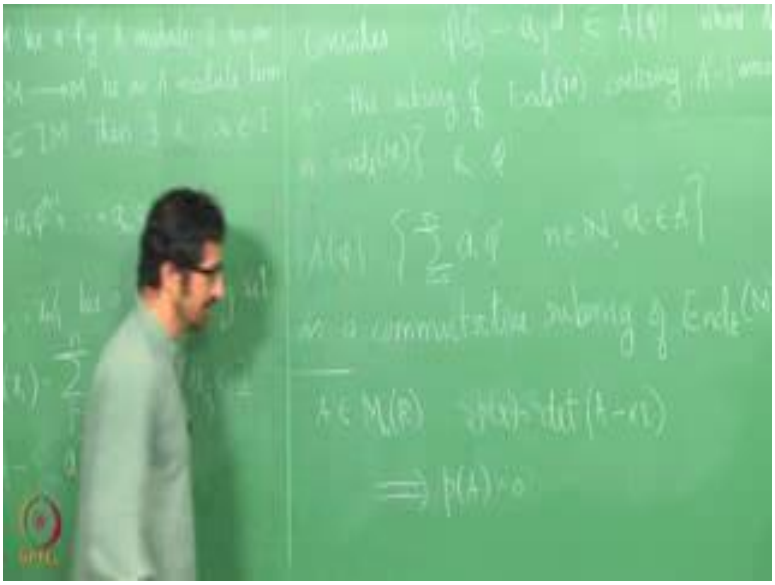
So, if I have a i mean what we have ultimately done here we have taken a generating set of this module and map to corresponding generating, I mean map to the corresponding generating set in M. So here if I have a generating set let it be some module f 1 up to f m suppose this is a generating set then every element is a linear combination of a i, I mean linear combination of the form a i f i. Now, look at you know I am sending a f i to I mean look at the images of f i then if I take any element here in M look at the preview, I mean pre image of that that will be some a i f i. So, therefore, phi of that will be sigma a i mi.

So, therefore, this every element in M is a linear combination of m 1 up to m n therefore, it is finitely generated.

So, let us try to prove this. So, here M is contained in phi of M is contained in IM M is finitely generated so let us start with the generating set x 1 up to x n be a generating set for M. Therefore, I can write phi of x i this is equal to summation j from 1 to n a i j x j and where are these a i j is coming from? Phi of x i is contained in IM every element of IM looks like summation some a i j, I mean alpha i j y j where alpha i j come from I and y j come from M, but every element of M is linear combination of x 1 up to x n. So, each y j can I can you know expand and then write it in this form ultimately. So, this can be written you know I collect all these expressions and write this as phi delta i j minus summation j from 1 to n a i j x j this is summation is 0.

Now, look at this, this is again consider phi delta i j minus a i j. So, I am writing this as a summation outside this I am sorry. So, this should be here j from 1 to n.

(Refer Slide Time: 21:03)



Consider the elements phi delta i j minus a i j I mean delta i j is the Kronecker's delta I mean x 0 if i is not equal to j and this 1 if i is equal to j or in other words here phi will be I mean in this summation when j runs from 1 to n this will be non 0 only when x j is i. So, phi x i phi x i will come from this part and from this part the whole thing will come. So, I have just written a compact form.

So, look at this, this is an element of, so you can think of this as a i j as a i j times identity or a or else you can think of a i j as the constant multiplication map from M to M, a i j can be thought of as the homomorphism sending x to a i j times x. So, you can think of this as an element in A prime phi, what is a prime phi? Where a prime phi is the subring of the endomorphism ring containing A prime this is image of A in; and phi. That is I consider the smallest subring containing all these constant maps, constant multiplication maps and the homomorphism phi.

So, every element in phi looks like summation a i phi power i, i from 0 to n, n in N, a i in a this is what my I mean I am denoting it A prime because it is not really A, it need not necessarily be 1 isomorphic to a because the multiplication map can be 0. If you take a if your module M has an annihilator and if you take an element from the annihilator multiplication by that would be 0. So, therefore, that in this ring that element will be everything in the annihilator is same as 0. So, that is why I am denoting it by a different notation; A prime phi this is a subring of endomorphism. It is not clear to you, do you understand this notation? Sorry, this is the collection of all elements of this form, one can.

Student: Sir how this (Refer Time: 25:32).

That is what I said see every element a i, a i is a multiplication map right from M to M is the map a i of x is a i x. So, every constant can be seen as the constant multiplication map, multiplication by that constant. So, that way I have a image of a inside endomorphism.

Now, a ring endomorphism of A, End M this is not a commutative ring right, in most cases in the general case this is not commutative. What can you say about this ring? What can you say about this ring?

Student: (Refer Time: 26:41).

Take any 2 elements f and g.

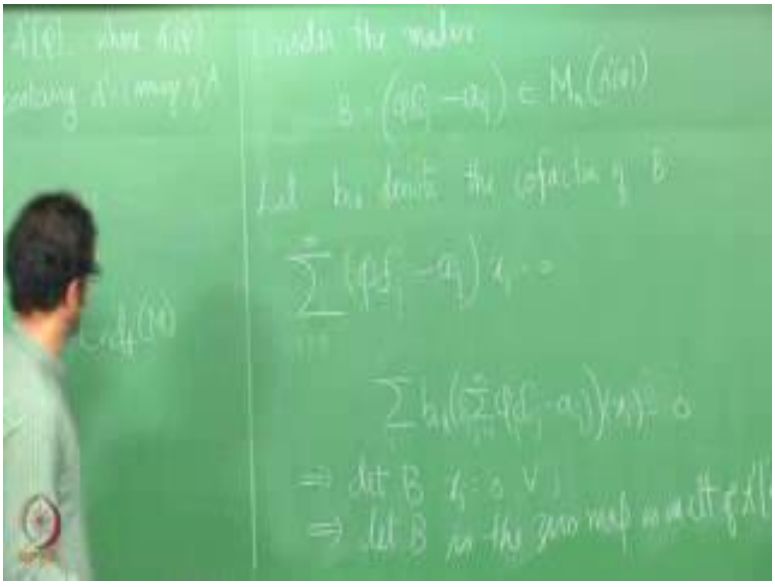
Student: Because (Refer Time: 26:49).

Come phi always commutes right phi n composition phi m is same as phi M composite phi N. So, therefore, this is a commutative subring of.

Now, we will have to talk about a theorem that is you have seen in the case of vector spaces over fields and I will take the freedom to ask you to go through the proof again and see that the theorem is true for modules over commutative rings. That is or you know it is over commutative rings there is no module involved here. So, it is basically the Cayley Hamilton theorem. What does Cayley Hamilton theorem say? The Cayley Hamilton theorem says that if I take a matrix A in M and F and look at determinant of, and I right p x as determinant of A minus X I or X I minus a either way if p x is this then p A is 0. So, here we are looking at elements matrices A with entries coming from the field.

Now how would you prove this? What you do is look at this take this matrix multiply look at this matrix containing the cofactors basically the adjoin and then multiply and see that this gives you the determinant and that gives you another 0. So, if you look at the proof, proof does not use anything that this is you know the ring or the elements need to have a multiplicative inverse what is needed is commutativity. You need to you know multiply elements switch them accordingly, see when you take the determinant and expand for that you need commutativity. So, the only assumption needed for this statement to be true is commutative ring, ring should be commutative. So, here I am if I replace this by a commutative ring R the statement is still true.

(Refer Slide Time: 30:24)



Now, let us come back to this, these are all elements in a commutative ring and I look at this matrix, the matrix; consider the matrix let me call it B to be equal to phi delta i j minus a i j. So, a i j as I said thought of as the multiplication map this is a an M by n matrix in with entries coming from A prime phi matrix over a commutative ring. Now let b ik denote the cofactors of B that is b ik is the determinant of the matrix obtained by removing the ith row and kth column and we are just preceding in the manner that we that one proves the Cayley Hamilton theorem there is nothing more to it.

So, now, I have this system of linear equations i from 1 to n phi delta i j minus a i j x j is 0 sorry j from 1 n if I look at this. So, I take this cofactors if I take b ik phi i j sorry phi delta i j a i j, j from 1 to n and take the summation over or i this will turn out to be equal to the determinant. So, this will be. So, this acting on any x j is 0 and that will say that. So, this if you expand what you get is the determinant of B acting on x j is 0 for all j and that would imply that determinant of B as a function in, as an element in a prime phi is 0; this is the 0 map as an element of. But what is determinant phi? If you expand this what you get is a degree n equation here, I mean phi power n. Now, look at each a i j, each A i j come from?

Student: (Refer Time: 34:39).

From the ideal i, not only from the ring because you know phi of M is contained in

Student: IM.

IM. So, therefore, each a i j come from?

Student: i.

i. Now look at the expansion of determinant of B. Determinant of B look at the highest power that will be phi power n and then. So, this, your matrix looks like this.

(Refer Slide Time: 35:21)

Phi a 11, phi minus a 11, minus a 12, minus a 1n; a 21 minus a 21, phi minus a 22, minus a 2n; minus a n1, minus a n2 to phi minus a nn and this is how the matrix B look like. Determinant of B will be again an element of A prime phi and as an endomorphism from M to M it is 0. But what is determinant of B? It will be no, this times determinant of this minus plus determinant of the rest and so on. But that will be again some phi power n plus the coefficient of phi power n minus 1 will have 1 I mean some a i js, some linear combination of a i js. So, this will be a 1 phi power n minus 1 a n minus 1 phi plus a n.

Student: (Refer Time: 37:02).

Right, each a i see they are all coming from here all these a is are linear combinations of some linear or you know combinations of all these a i js they are all in either the ideal i. So, a i belongs to I and that is precisely what we were trying to prove.

So, here in the proof there are only 2 things that we have used, we have not really used the Cayley Hamilton theorem one can use Cayley Hamilton theorem and get this, what we have done is we have just gone through the proof of Cayley Hamilton theorem we take B, take the cofactors multiply with the cofactors correct cofactors and sum it over all of them; what you get is determinant and this applied on x j is 0 implies the determinant applied on x j is 0 for all j. That is precisely, I mean as an element of or as a map from M to M it is 0 and determinant of B once you express it in this form what you get is the required form.

In the statement of the proposition we have mentioned a i belong to I, but one can see that it is not only this it is little more. One can see that a i belong to in fact I power i. See if you look at coefficient of phi power n minus 1 it will be some n minus 1 product times one a i j coming from here. So, therefore, that a i j will come from I. So, a 1 belongs to I.

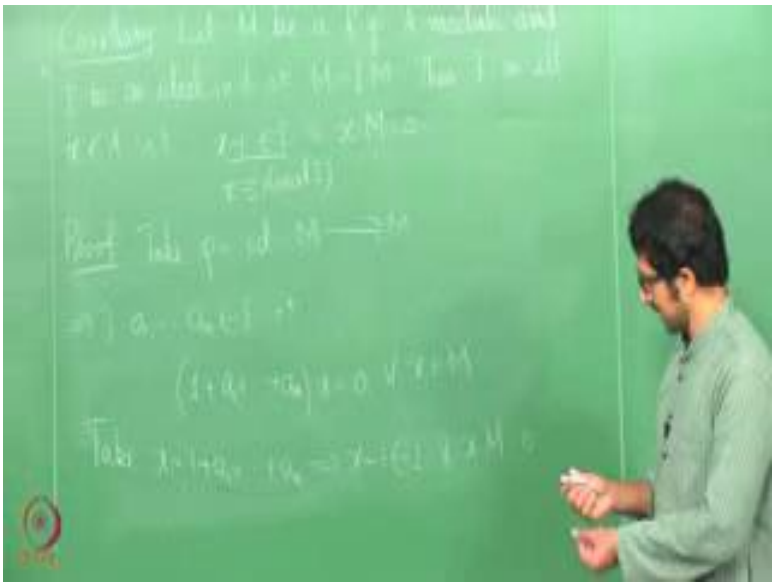
Now let us look at phi power n minus 2 phi power n minus 2 will be, there will be phi power n, I mean n minus 2 of them and then you know there will be several you know power of phi power n minus 2 you get in several ways not only one way. But in all these ways you will have n minus 2 of these terms involved and 2 a i j products. So, each a i j belongs to.

Student: I.

I; therefore, these 2 will give the element in I square and so on. I mean it is basic you know counting in some sense. So, one can obtain that a i is in I power i.

This has a very important corollary.

(Refer Slide Time: 40:12)



Suppose I take let M be finitely generated A module and I be an ideal in A such that M is equal to IM then there exists an element x in A, x in A such that x minus 1 belongs to I and x M is 0 or x is in the.

Student: (Refer Time: 41:16).

Annihilator of M and this can also be written as x congruent to 1 mod I or in other words there is an element which is a unit in a mod I and annihilating M. This is straightforward from the previous theorem, if I take phi to be identity map from M to M then what do you get there exists you know a 1, a 2 up to a n in I such that, so there exists a 1, a n in I such that phi power n, if phi is identity phi power n is identity. So, you can write it 1 plus a 1, so you can you know this can be thought of as phi can be thought of as constant multiple like 1, constant multiple of 1, 1 plus a 1 up to a n; this is 0 which means this acting on M any element in M is 0.

Now, this is an element in a and what can you say about. So, this if I take x to be equal to 1 plus a 1 plus etcetera a n, what can you say about x minus 1?

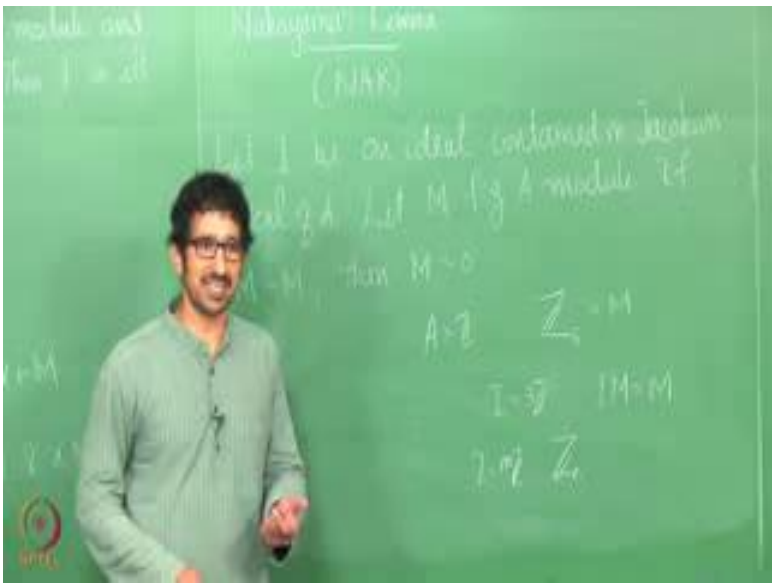
Student: (Refer Time: 43:34).

X minus 1 is in i.

Student: (Refer Time: 43:39).

Right, so, then x minus 1 belongs to I and x M is 0. So, now, there is this gives one of the most important basic results in commutative algebra called Nakayama's lemma.

(Refer Slide Time: 44:03)



So, in the paper of map, in the book of Matsumura there is this a book commutative ring theory by Hideki Matsumura in that book there is something interesting written about

Nakayama's lemma. It seems Nakayama claims that this is not his contribution it is, it should I mean according to him it should be attributed to Azumaya and Krull. So, in Nakayama's in Matsumura's book he writes it as, he writes theorem and in bracket he writes NAK and many places it is used like this Nakayama, Azumaya and Krull, but we always refer to it as Nakayama's lemma, it is been like that for a while now.

So, what does this theorem say? Let I be an ideal contained in Jacobson radical of A let M be a finitely generated A module if IM is M then M is 0. Think of this situation in the local ring suppose you have a local ring every ideal is contained in the Jacobson radical because there is only one maximal ideal, every ideal is contained in the Jacobson radical. So, what it says is that in a local ring if you take a nonzero module then IM can never be equal to M, but this is not true in general. Say for example, if you take Z n or Z 5 over Z, can you think of an ideal I such that Z 5 is Z 5?

Student: (Refer Time: 46:59).

If you take 5 Z then it will be 0 right, I times I take M to be this and A to be Z, now my question is can you tell me an ideal I such that IM is equal to M.

Student: (Refer Time: 47:19), 3 Z.

3 Z, will this be satisfied?

Student: 3 Z (Refer Time: 47:33).

Yeah, 3?

Student: 3 is a generator in M.

3 is a generator in M, so what? One can, so if you think of this, now this is 3 is a unit as well. So, 1 will be here right, 1 will be in IM, as a module, if a sub module contains that generator it will contain (Refer Time: 47:16). Now, can you generalize this if you take Z n, can you give me an ideal I such that IM is M?

Student: (Refer Time: 48:29).

You take any I equal to m Z where m is co prime to n then IM will be equal to M. So, this is not true in general I mean this statement, see in this case note that all these ideals

are not, if it this is not a local ring, but this a commutative ring. None of these ideals, none of these ideals are in the Jacobson radical. What is the Jacobson radical of A?

Student: (Refer Time: 49:13).

Intersection of all maximal ideals; what is Jacobson radical of A?

Student: (Refer Time: 49:21).

Hm?

Student: 0.

0, right there cannot be any n Z there. If you take any n Z you can always find a maximal ideal n which skips a maximal ideal. So, intersection of all maximal ideals, therefore, this is I mean this is not a counterexample to the Nakayama lemma. What I am saying is if you remove this hypothesis this is no longer true. We will prove Nakayama lemma in the next class.