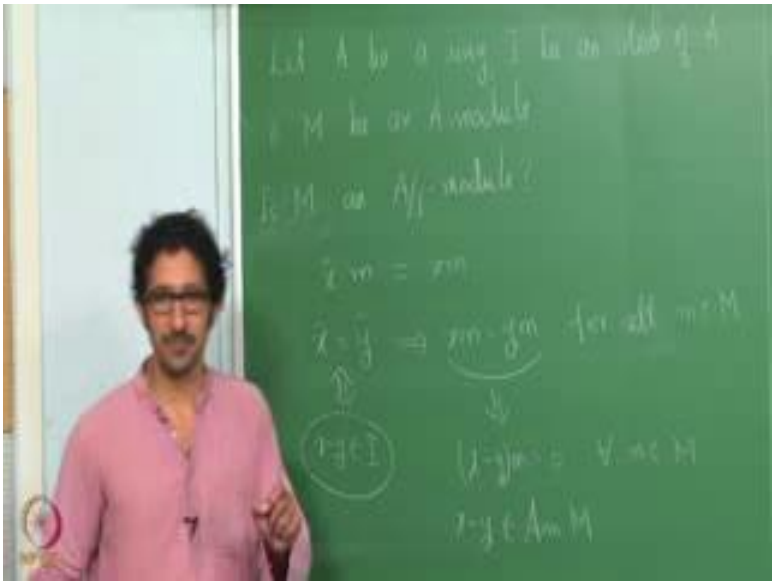
Commutative Algebra
Prof. A.V. Jayanthan
Department of Mathematics
Indian Institute of Technology, Madras

Lecture - 10
Operation and Modules (Continued)

Let us begin with the question that we addressed last time.

(Refer Slide Time: 00:28)



Suppose I have a an ideal; let A be a ring I be an ideal of A and M be an A module. When can is M an A mod (Refer Time: 01:12) module. Can we think of M as an A mod I module, in a natural way; that is how do you expect the natural way? See this is an abelian group; basically we need to define a scalar multiplication. So, how do you define scalar multiplication here? X bar m, this is the natural way of defining. But then, if I take two representatives of x bar then may not be equal. So, what is the condition that is required?

So, what I want is if I take any two representatives that should imply that xm is ym for any M in M or for all M in M. Then only this definition will make sense. But what does this mean? Does this mean x equal to y? So, this would imply that x minus y times M is 0 for all.

Student: M belongs to M.

M belongs to M; or in other words.

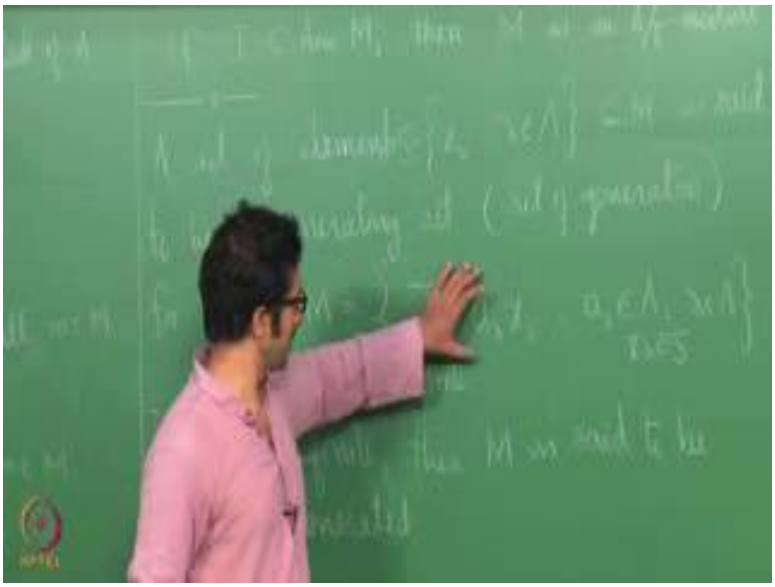
Student: X minus y should be (Refer Time: 02:59).

X minus y should be in the annihilator of M. See here we have started with x bar equal to y bar and we have concluded that for this to be a M to be naturally A mod I module we need x minus y to be in the annihilator of M. This says that x minus y belongs to I. And what indeed we want is x minus y should be in the annihilator. So, what condition would you like to impose?

Student: (Refer Time: 03:52).

See this is the condition that we started with, right x minus y belongs to I which is same as say x bar equal to y bar. And then we said that from here I want this property, so ultimately we got x minus y belongs to annihilator. Or in other words what we want is I is contained in annihilator.

(Refer Slide Time: 04:26)



So, therefore, the observation that we have made here is if I is contained in the annihilator of M then M is an A mod I module.

As I said earlier, see if you look for example, if you take Z and Z let us say Z 5. We cannot really say that Z is a Z 5 module. So, start with Z n z, Z is a Z module, but Z is not a Z mod 5 Z module, naturally. You can of course define all scalar multiplication to

be 0; that will define a null structure on the module, but the natural definition is this. With this we do not have a module structure on Z over Z mod 5 Z. So, you have A module M over a ring A does not mean that you can have A module structure on M over A mod I. For that what we have found is I should be contained in the annihilator, and then only it is possible.

So, now let us look at some more properties of modules. So, a set of elements x lambda, lambda belong to ok; M is said to be a generating set or set of generators for M if, when would you say a set is a generating set?

Student: (Refer Time: 07:27).

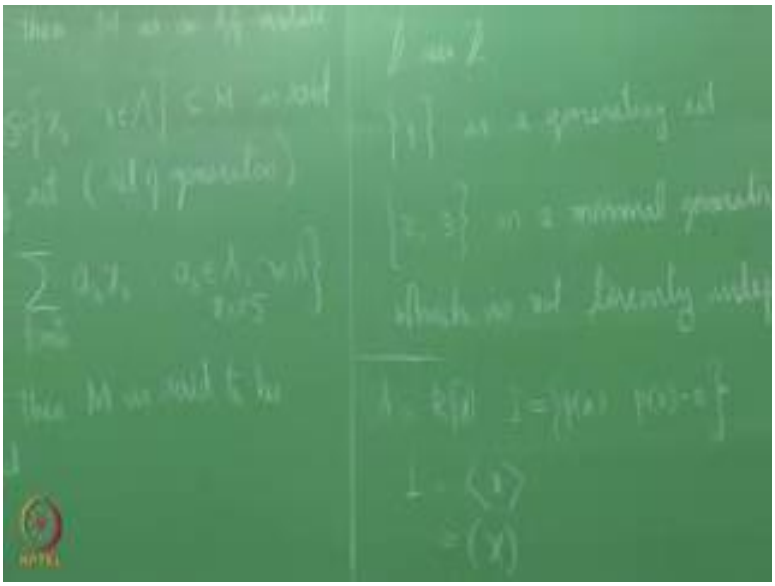
So, think of the vector space you must have gone through that; to start with.

Student: (Refer Time: 07:31).

Every element can be expressed as a finite linear combination of elements coming from here. Or in other words if M is equal to summation a lambda x lambda, I will just write finite here a lambda belongs to A; lambda belongs to A. So maybe I will write this call the set S x lambda in S. And if S is finite then M is said to be finitely generated. So now, taking ideas from the linear algebra course that you have gone through one may you know tend to talk about linear independence and basis and so on. So, one of the linear independence of course you can define the same way. Like this finite linear combination is 0 if and only if all the coefficients are 0. A set is said to be linearly independent if you take any finite linear combination nonzero finite linear combination cannot be 0.

In this case one can define to be the same, now the question is the: first question is can we have a generating set which is linearly independent? You start with any generating set can we reduce it to a linearly independent, I mean maximal linearly independent set which is a span of whose span is the whole module and so on. So, the module theory is not as fortunate as the vector space theory.

(Refer Slide Time: 10:16)



For example, if you take Z, take one of the nicest example; Z over Z. If you take the module Z over Z itself, can you give me generating set? 1 right, this is a generating set. And this is linearly independent right, alpha times 1 is 0 if and only if alpha is 0. But now in vector space theory we have much more. You take any generating set from that you can throw out if needed few vectors and get a generating set which is linearly independent. In this case suppose you take the generator taking set 2, 3; this is certainly a generating set.

Now, is this linearly independent? Minus 3 times 2 plus 2 times 3 is 0, therefore this is not linearly independent. But can you throw away one of them? Still generate whole Z, no. So therefore, this is a generating set; in fact this is a minimal generating set which is not linearly independent.

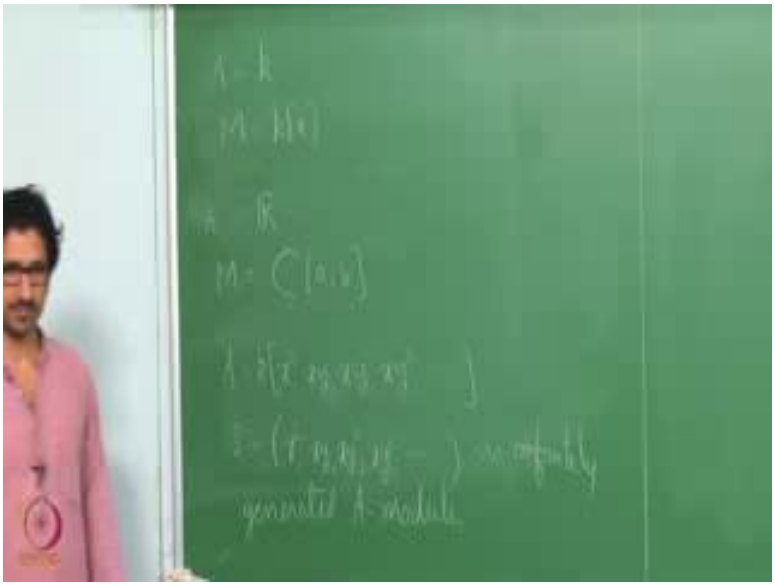
So, unlike in the case of vector spaces here minimal generating set need not be linearly independent. And similarly a maximal linearly independent set need not be a generating set, for example 2. If you take simply 2 that is a maximal linearly independent set. In fact, you take any integer single integer that is going to be maximal linearly independent set, but that is not a basis unless that integer is 1 or minus 1. So therefore, the theory of modules is no slightly more general, and it is does not behave as nice as in the case of vector spaces over fields. So, let us look at one or two more examples of generating set.

Suppose, your ring A is let us take k x k a field and I to be all polynomials with constant terms 0, is this an ideal? There is certainly A module over A. Can you tell me what a generating set for this? What is a generating set for this?

Student: X.

X right. So, ideal I is generated by x, I will write. Usually either this or another notation, both the notations will be used. Can you think of A module which is infinitely generated? Think of vector space theory; if you borrow the example from vector space theory you can always cook up infinite dimensional vector space over a field.

(Refer Slide Time: 15:03)



Here itself if you take A to be, A to be?

Student: (Refer Time: 15:11).

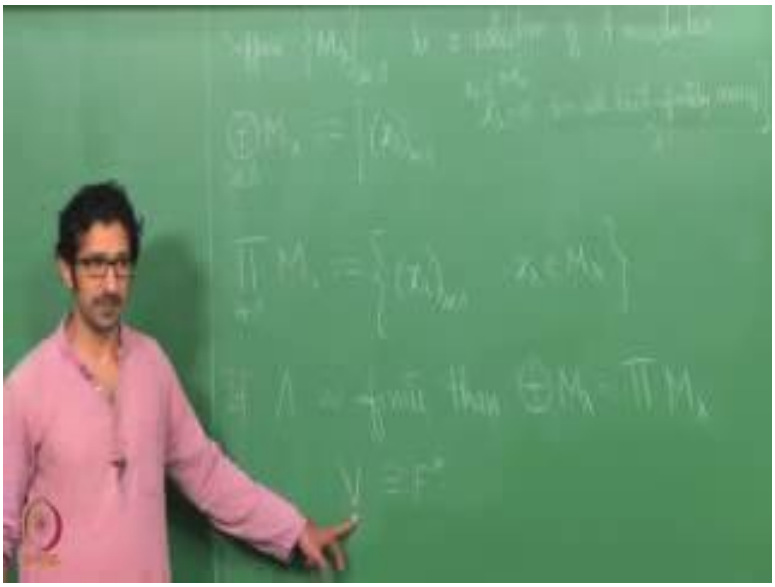
Well, A to be C ab; this is what you mean, and then what is M then?

Student: (Refer Time: 15:25).

Well, that will require some; M cannot be c dash, can it be c dash? Will it be A module over, but how do you? I guess you are thinking too complex, let me just then; I will take A to be k and M to be k x, it is a infinite dimensional vector space over k rights that is a natural infinite dimensional infinitely generated module over k. And if you take A to be R and M to be C ab; again example coming from the vector space theory.

Suppose, I take A to be; so here you will see some sub rings of k x k xy and so on. So, if I take A to b k M to be; let me take the A to be not k x square, xy, xy square, xy cube, and so on. So, this is a ring and if I take I to be this ideal x square, xy, xy square, xy cube and so on. Can you see that this is infinitely generated? Can you get this from here? How do you get this from here? The only possibility is to multiply by y, but in the ring it is not there; y is not there in the ring. I mean no pure power of y is there in the ring. So, none of these can be obtained from previous nevertheless. Therefore, this is infinitely generated A module.

(Refer Slide Time: 18:54)



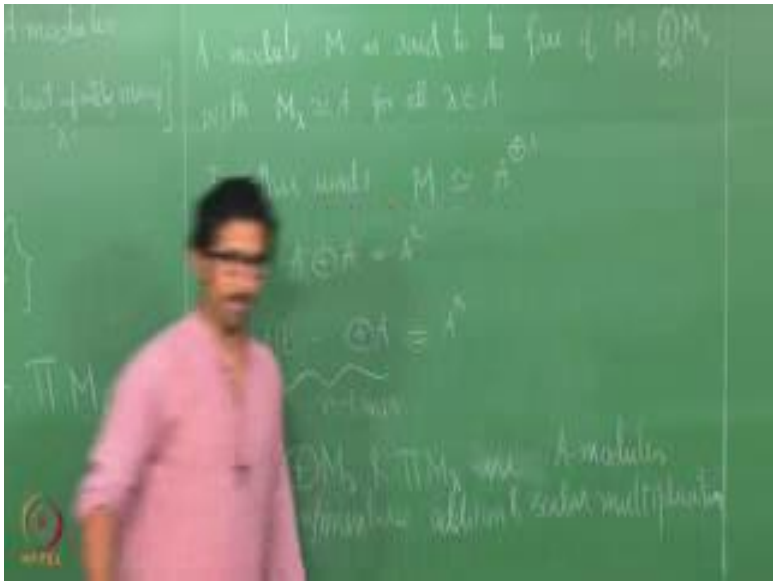
Suppose I have a; see in the case of rings, in the case of vector spaces, in the case of groups you have studied, now if you have a collection of vector spaces V 1, V 2 and so on of vector spaces over a field F then you can form its product right: Cartesian product. Have you seen direct product direct? Some direct product, there is a difference between these two. So, suppose I have a collection of A modules be a collection of A modules, then we can form what is called direct sum of M lambda, lambda belonged to lambda. This is set of all sequences x alpha, I mean x lambda lambda and lambda, such that x lambda is 0 for all but finitely many. This is all tuples where it is a 0 after a finite stage.

And I can form the product. So, this x lambda in M lambda and x lambda is 0 for all but finitely many lambdas. Product M lambda lambda n lambda this is defined as x lambda sequence with no restriction; that is the only. So, if lambda is finite then?

Student: (Refer Time: 21:38).

Then the direct some M lambda is same as a product M lambda. And otherwise they are not the same, I mean if your modules are nonzero modules and the indexing set is infinite then they are not the same; product and directs sum they are not the same. Because in this one there would be an infinite nonzero sequence, while here there are none like that.

(Refer Slide Time: 22:26)



A module M is said to be free if; so this is somewhat similar to the case of vector spaces, we do not really have. Again as I said see in the vector space theory, once you say it is a vector space over A module over a field F there is a unique either infinity or a unique integer assigned to it which is the cardinality of minimal generating set or a maximal linearly independent set. But in the case of modules we have already seen that there is nothing like that. In general there is no dimension in some sense.

But in for a certain subclass of modules one can, one has this. These classes of modules are called Free modules. So, what is free modules? We define free module to be the way exactly that a vector space looks like, in the case of linear or in the case of vector spaces over fields. If you take any finite dimensional vector space or you take any vector space it is a direct sum of phi. If you take any vector space V over a field F, if it is finite dimensional then we know that this is isomorphic to F n where n is the dimension of V. And this is true in general aspect; it is a direct sum of. If you take any infinite dimensional vector space also it is product of F.

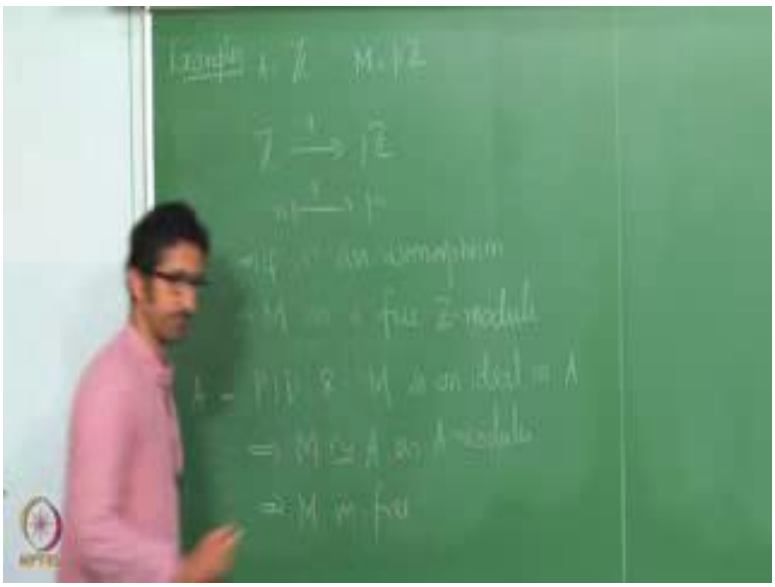
So, here we will define A module to be free module if it is exactly of this form. Or in other words if M is equal to direct some M lambda with M lambda isomorphic to A for all: each M lambda is isomorphic to A. Or in other words we can say that M is isomorphic to; this is the notation for you know direct sum of as many copies of A as the cardinality of lambda: this is a notation. For example I have, if I take M to be M direct sum M; sorry A direct some A. So, this is we usually denote this by A. And A direct sum A n times is denoted by A power n, if the lambda is finite then we denote it like this instead of this.

So, just to take examples from; ok sorry I forgot to mention one thing. See again this is something that you have already seen in the case of rings and module vector spaces and groups and so on. This is again in A module, remark direct sum M lambda and the product M lambda is an A module or A modules. So, when you say they are A modules you need to specify what should be the operations; the addition and the scalar multiplication.

Student: (Refer Time: 27:49).

Component wise right: with component wise addition and scalar multiplication. Let us look at one or two examples: can you give me an example.

(Refer Slide Time: 28:18)



So, a module over Z which is not free gives me an example.

Student: (Refer Time: 28:33).

P Z, why is this not free? Is this free or not free? As a module over, so this is A, this is M, is M free A module? How do you check whether M is a free A module or not? The question is. So, here we are saying it is a direct sum of like this with each M isomorphic to M lambda isomorphic to A. So, here it is kind of obvious that it has to be.

Student: Isomorphic (Refer Time: 29:28).

Isomorphic to Z if at all; so how do you check whether it is isomorphic to Z or not?

Student: (Refer Time: 29:38).

You have to define a map right, you have to define a homomorphism a map which is a homomorphism injective and subjective. If you are able to do this then, it is an isomorphism they are isomorphic. Now looking at this can you think of a map to start with, from Z to here or from here to Z.

Student: (Refer Time: 30:02).

So, from Z to?

Student: P z.

P z.

Student: N going to p n.

n going to p n, is this an A module homomorphism? N 1 plus n 2 is mapped to p n 1 plus p n 2. Similarly p I mean M n is mapped to p times M n which is M times p n which is M times phi, if I call this to be phi. So, then phi is, is this injective? It is injective right. This is an integral domain and you are doing a multiplication map, that can never be nonzero image element cannot be taken to a 0 element. So therefore, this is injective. Is it surjective?

Student: Yes sir.

Yes, so this is an isomorphism. So therefore, what does that say?

Student: (Refer Time: 31:19).

And what did we start with? We wanted to check whether M is?

Student: Free or not.

Free or not; so what does it say?

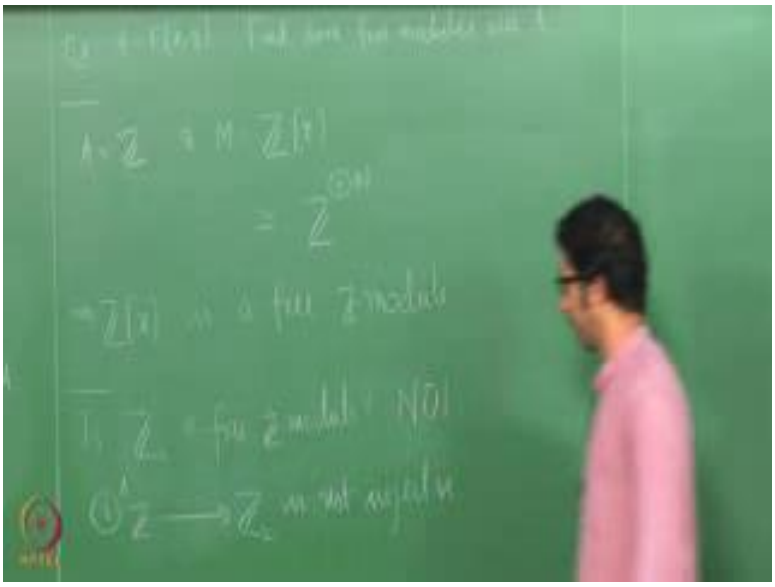
Student: (Refer Time: 31:33).

M is a free Z module. So, what can you; I mean can you more generally say can you generalize this statement? That is if you take any n that is going to be a free Z module, every ideal is a free Z module. Can you say this more generally? Suppose instead of Z can you replace Z by some special kind of ring and any integral domain.

Student: (Refer Time: 32:21).

If you take any principle ideal domain and take any ideal in the principal ideal domain that will be a free A module. So, A is a PID and M is an ideal in A, then M is isomorphic to a as A modules. So, that implies M is free.

(Refer Slide Time: 33:04)



So, let me give you an exercise to think about. Take A equal to F xy. Find some free modules over A? Well, do not give me examples like A direction A A direction A direction, you know that is by definition they are free models. What I am asking for

some ideals of A or some modules over A which are free. Think about it; now give me some examples which are not free.

Student: (Refer Time: 34:14).

Z x this is; so your A is Z and M is Z x. This is free, not free? It is not finite that is.

Student: (Refer Time: 34:38).

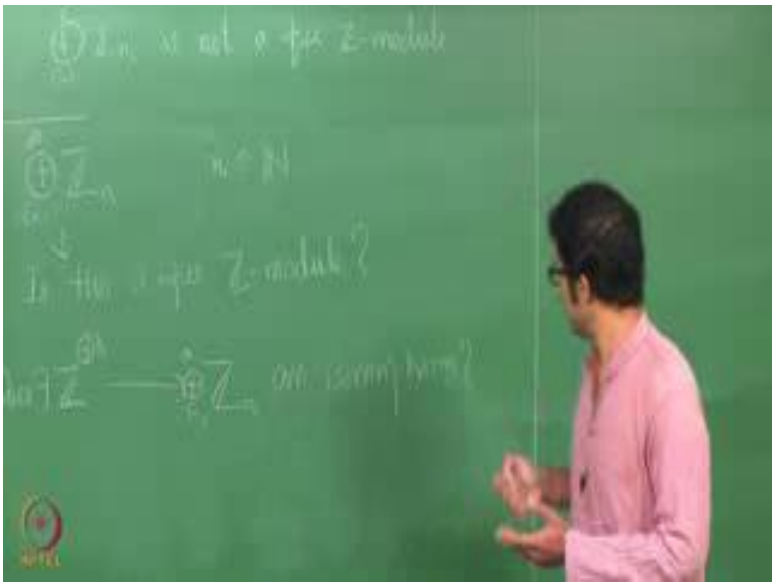
So, see there is one way that to say it is not free you have to say that M cannot be isomorphic to something of this form.

Student: (Refer Time: 35:03).

In this case this is isomorphic to right. See every element is a finite tuple in some sense right. So, one can define this map A naught plus A 1 plus etcetera up to A n; A naught plus A 1 x plus etcetera A n x power n is mapped to A naught comma A 1 comma a n and then 0 everywhere else. That will be A module isomorphism between these two modules. So, again this is Z x is a free Z module. So let me ask you; how about is Z 5, let us start with Z 2 free A module.

Can we say Z 2 be a free A module. Z 2 if I have any map from an infinite set to a finite set it cannot be injective, as simple as that. So, any homomorphism from some direct sum of that form; direct some lambda of Z this any map to Z 2 is not injective. This is pure set theory, there is homomorphism or not any map from direct sum like this to Z 2 cannot be injective, because of properties of finite sets; basic properties of finite sets. So therefore, this is Z 2 is not a free module. So, can you make a general statement? Any finite abelian group.

(Refer Slide Time: 38:04)



Student: (Refer Time: 38:02).

Is not; And if you take Z ni, i from 1 to R let us say is they are all see the any abelian group is in Z module. So, they are all Z modules, but this is not a free Z module.

Now, what if I take infinitely many of them? Up to here we did not need any group theory, we only needed the definition of free modules and to say that a basic set theory from an infinite set you cannot give a injective mapped to a finite set. But what if I take direct sum Z ni i from 1 to infinity, ni in Z well Z n maybe. So, you shall with the usual notation, yes we will expect it to be natural numbers. I can even exclude 0 and 1. Therefore, is this free Z module? Think about this. Why it cannot be a well; so let me reveal the answer it cannot be a free Z module. Now think about why this cannot be a?

Student: (Refer Time: 40:16).

So, the question is whether we have an isomorphism like this. There is an isomorphism, does there exist an isomorphism?

Student: (Refer Time: 40:45).

Yes.

Student: And each component is finite.

Yes.

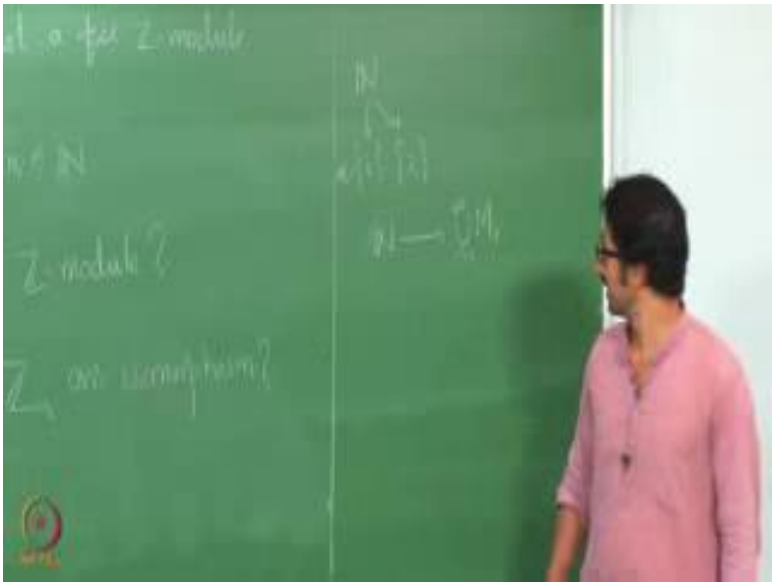
Student: So how (Refer Time: 40:53).

That is exactly you have to prove right. See earlier arguments say that you cannot have a injective map from here to here, because of properties of finite sets. But you have here it is, this is an infinite set. Why we cannot have? Again Z is infinite.

Student: (Refer Time: 41:27).

That is ok, that does not follow from the basic set theory.

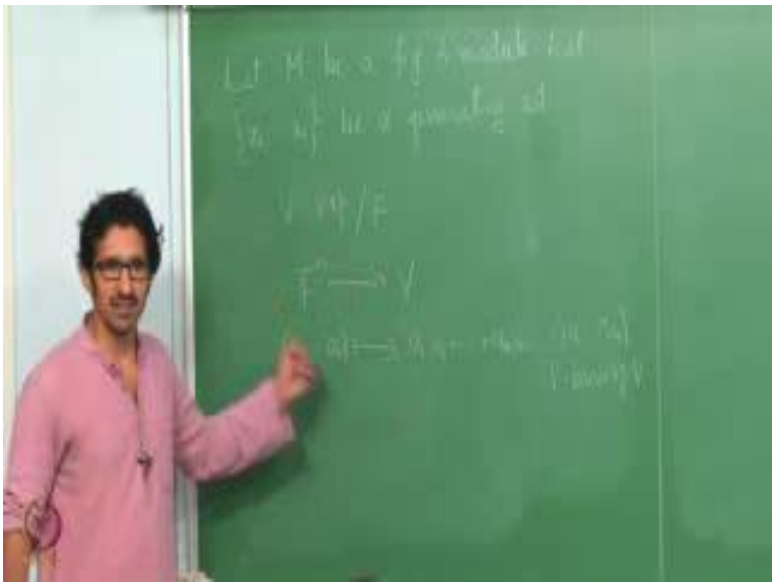
(Refer Slide Time: 41:39)



See for example, if you take natural number take N from N to 1. Is there an injective map? No, N to 2; no. Now this is my M i this is M i, but from n to union M i i from 1 to infinity there is an 1 1 on 2 map. So, we cannot really say, but the idea is there from what you said. Each Z ni is a finite Z module. That Z ni sits inside here, you can think of it as a sub module of this module.

So, I will probably leave it at that point you know, you should now be able to complete it. So, what are these? You know we will just explore more properties of modules and then come back to this question later maybe. I mean does not need any more theory it is straight forward from here.

(Refer Slide Time: 43:12)



Suppose I have a finitely generated M be a finitely generated A module. Let x 1 up to x n be a generating set. In the case of vector spaces if I have a generating set then we have. So, the same in fact in the case of vector spaces there is one result that we proved during the linear algebra course, that if you take a basis of a vector space V and you take that many number of vectors from another vector space w then there exists a unique linear map from V to w which maps each of these V i's to corresponding w i's. We did not really use any specific properties of vector spaces there, except for the case of uniqueness.

So, in the case of modules also one can prove that there exists a linear map, there exists a homomorphism from M to N taking a generating set and corresponding set of elements, we will not need that for the time being. But then how did we prove the same method to say that V has dimension n n is uniquely determined where V is isomorphic to F n. We define the map from. So, if V is a vector space over F then we define the map from F n to V by a 1 up to a n going to a 1 b 1 plus etcetera a n v n. Where, this is a basis of F basis of V. And one showed that this is a homomorphism, I mean it is a linear map 1 1 on 2 and so on.

So in the case of modules, suppose I have a generating set can you think of something similar? Will it be 1 1 on 2 and so on? We will take it up in the next class.