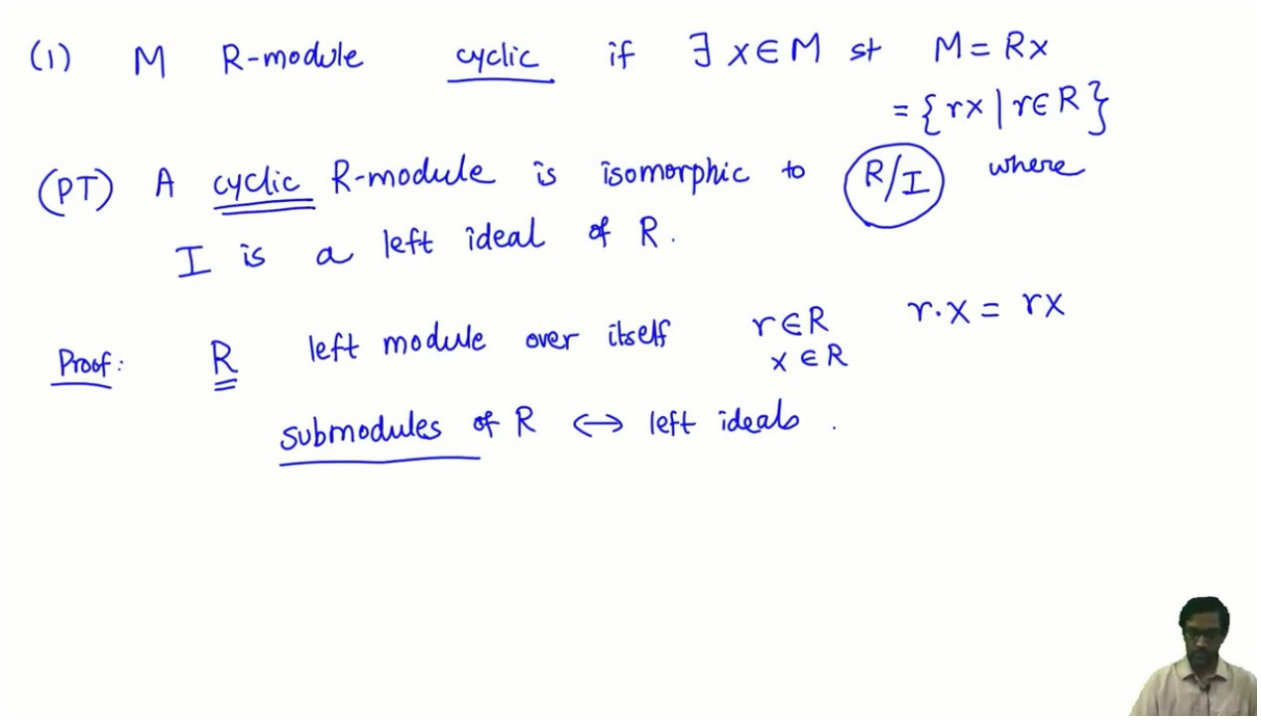
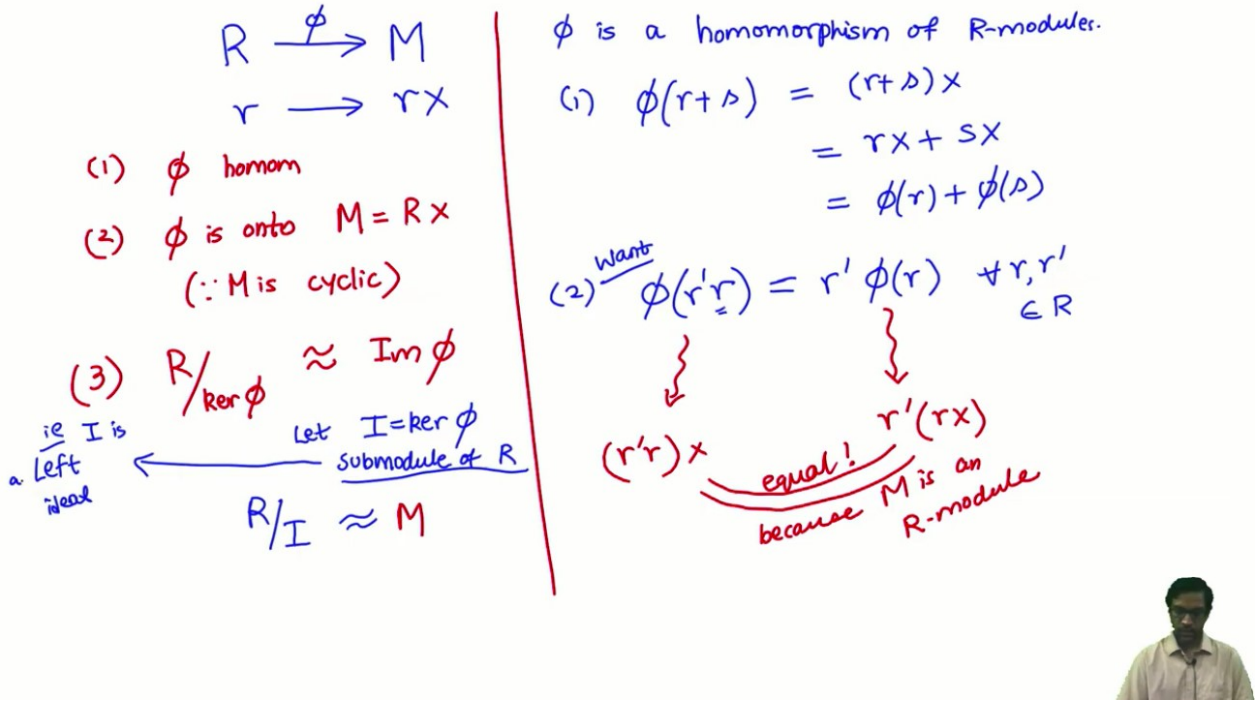
Algebra - I
Prof. S. Viswanath & Prof. Amritanshu Prasad
Department of Mathematics
Indian Institute of Technology, Madras

Lecture 65 [Problem Solving]

Let us do some problems on quotients, and homomorphisms, and so on. So, recall, so problem 1. So, recall the following definition M and R-module is said to be cyclic, so we call M a cyclic module if it is generated by a single element. So, there exists a single $x \in M$, such that M is just the submodule generated by x, ok. In other words, it is all multiples of x, scalar multiples of x, $\{rx | r \in R\}$ So, if this happens, then we call M cyclic or singly generated, ok.

So, here is the question problem. Prove that, a cyclic R-module a cyclic R-module is isomorphic to to a special module $\frac{R}{I}$ the quotient, the quotient module $\frac{R}{I}$, where I is a left ideal where I is some left ideal, ok. Let us prove this proof. So, firstly, let us ensure we understand the definitions here. Recall that if you have a left ideal of R then you can think of it. So firstly, R can be thought of as a left module over itself how is this by sort of left multiplication, other words I take a scalar $r \in R$ I think of the module also as being R itself. So, let suppose I have $x \in R$ then how does $r \cdot x$? Well, the scalar multiplication is just the usual multiplication in the ring R ok.





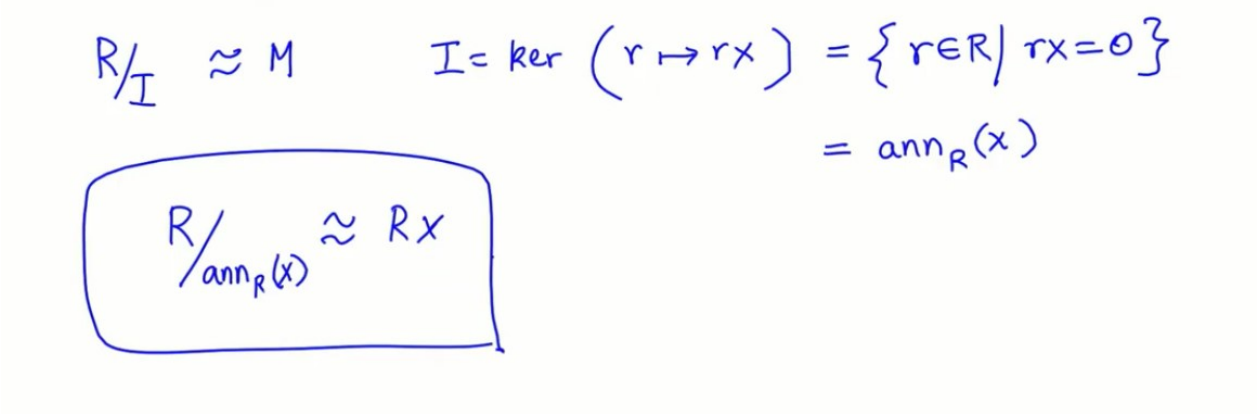
So, R is the left module over itself. And what are the submodules for this? Module, they are exactly what we call the left ideals. So, the submodules of R under the left action are just the left ideals, ok. Left ideal just mean there are additive subgroup and if you multiply them on the left by any element of the ring, then it still belongs to the same left ideal, ok.

Sub modules are the same as left ideals. And what we therefore can do? You have a module R you have a submodule, which is a left ideal um and you can therefore, take their quotient. So, what is being asked to prove is that if I take every possible left ideal of R consider the quotient $\frac{R}{I}$ this collection exhausts the possible cyclic R-modules up to isomorphism, ok. Every cyclic R-module is isomorphic to a module of the form $\frac{R}{I}$.

So, let us prove this ah. So, what what if we say a cyclic module was. So, so the best way to prove this really is to set up a homomorphism. So, what what do we have? We have a module M which is known to be cyclic which means there is a single generator x, ok. Now, let us do the following. Let us define a map from $R \to M$, let us call this map ϕ . What does this map do? To each element r of the ring it associates the element rx, ok. So, recall x is the fixed generator of M, So, define this map r going to rx.

So, the first thing to observe is that this map is actually a, so both sides R and M are R-modules, this is a module homomorphism, this is a homomorphism of R-modules, ok. Let us verify the properties. We need to check on the one hand that if I take a sum of two elements on the left. Well, what does that give me? It is $(r + s)x$.

But the fact that M is an R-module means I have this distributive property its $rx + sx$ and therefore, that is just $\phi(r) + \phi(s)$, ok. So, that is 1. We need to check that if I take ϕ of; so, I take an element of r and multiply it on the left by something, right. So, I need to now take let us give this a name, so I take an element r of the ring and suppose I multiply it on the left by r' , ok.



So, I want this answer to be; so, let us write down what we want. So, this is the second property of being a module homomorphism, that if I hit the module element on the left by r' , the r' should be I should be able to pull it out, ok. I want this to be true for all rr' and R ok. This slightly confusing because the ring is also a module now in this case over itself, but you should convince yourself that this is exactly the second axiom of a homomorphism, ok.

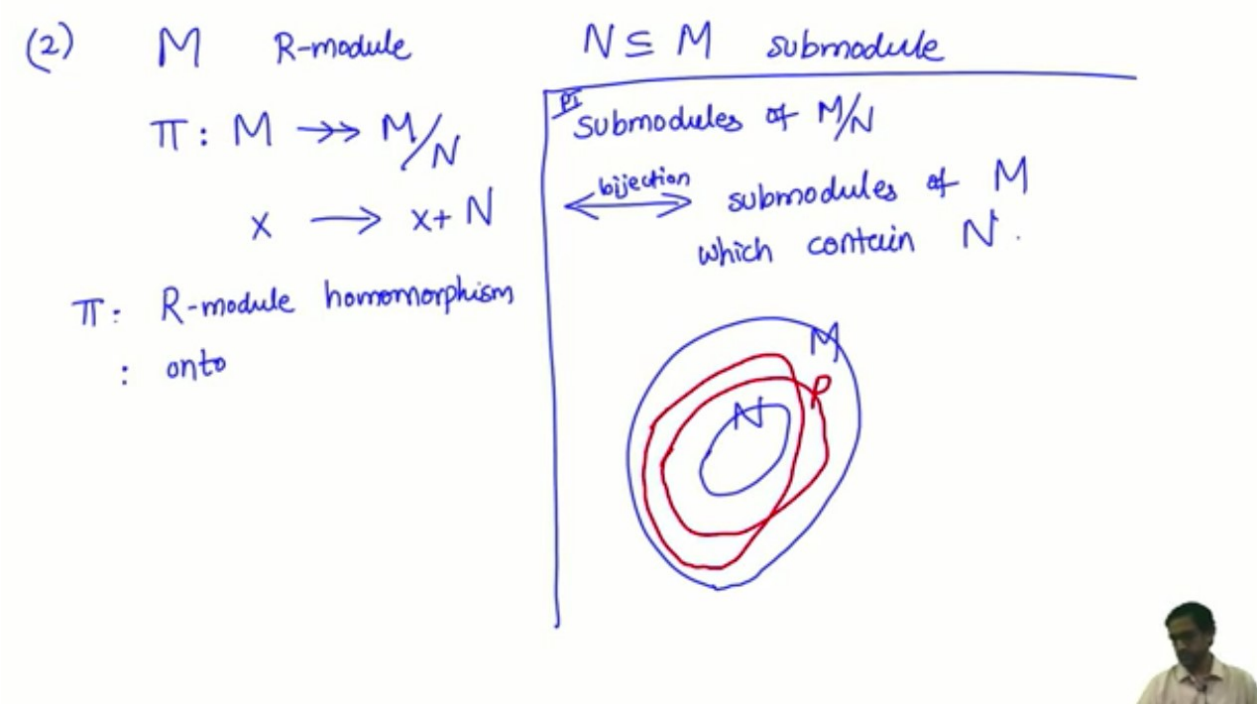
Now, let us check that this is true. So, $\phi(r'r)$, so let us compute the left hand side. So, what is this? By definition this is $r'r$ acting on x. Now, let us do the right hand side. This is $r'\phi(r)$, $\phi(r) = rx$, ok. But observe that these two are actually equal to each other because of the module axiom because M is a R-module, because M is an R-module. So, the R-module axiom says when I have a product of two scalars, r' and r when that acts on a on an element of the module, I can think of it as a two repeated actions, right. First apply the first scalar, then apply the second scalar, ok. So, what we actually have is that this map ϕ that we have defined is a homomorphism, ok.

Now, what what else can we conclude about this? So, first property of ϕ , ϕ is a R-module homomorphism. Second property ϕ is onto. Why is that? Because M was given to be cyclic we were given this property, right. That every element of M is of the form rx for some Rx is the fixed element remember, ok. So, the the fact that; so, this is since M is cyclic, ok.

So, now, we are in good shape because we can sort of apply the first isomorphism theorem which says that when I have an homomorphism, then T modulo the kernel of this map is isomorphic to the image of this map, ok. Now, in this case, what is the image? The image is M, And let us call the kernel as I.

So, what is the kernel in general? Remember, if I have a homomorphism between two modules the kernel is always a submodule, ok. So, let us let us call this fellow as I. So, let I be the kernel of this map, then that is no you know we we already know it is a submodule, submodule of R but submodule remember is the same as left ideal, ok. So, it says R modulo the kernel is actually isomorphic to M and that is exactly what we needed to prove, ok. So, we just have to realize that submodules are the same as left ideals, i.e left ideal. I is a left ideal, ok. In fact this this this ideal, we we have actually proved a little more. We have said what was I. So, we said $\frac{R}{I} \cong M$, where I is exactly the kernel of the map. The kernel of what map? The map which sends each element $r \to rx$, ok.

So, which means what? This is exactly the set of all $r \in R$ such that $rx = 0$, right. And this is usually I mean this has a name this usually called the annihilator in $Ann_R(x)$, ok. It



is all elements, all scalars which annihilate that element x. So, $\frac{R}{ann_R(X)} \cong Rx$. So, this is sometimes another form in which you will see this R modulo the annihilator is isomorphic to the submodule generated by that element x, ok.

So, all this I mean this assuming that x is inside some module. In this case, we have we have assumed that Rx itself is M, ok. So, let us move on to the second problem. So, again is about quotients and and submodules. In fact it is about submodules of quotients. So, here is the problem broadly speaking. So, suppose I have a module M, M is an R-module, when R is not necessarily commutative and suppose I have a submodule N sub of M, ok. So, um recall; that means, that I have the quotient $\frac{M}{N}$ and in fact I have a quotient map from $M \to \frac{M}{N}$, ok. So, this double arrow just means that this map is, it is a surjection.

So, what is this map do? It takes each element $x \in M$ and maps it to the coset $x + N$, ok. So, this is this this is the, this map is it is an R-module homomorphism, it is a surjection, π is an R-module homomorphism, π is onto, ok. Sometimes called the quotient map, ok. So, the problem is the following ah. Determine what the submodules of $\frac{M}{N}$ look like, ok. So, prove that. The submodules of this module $\frac{M}{N}$ are in one-to-one correspondence. They are in bijection. Show that there is a bijection between the submodules of M mod N and the submodules of M which contain N, ok.

So, sometimes it is nice draw a picture. So, I have M the ambient module, I have N the submodule. And what we are saying here is that to understand the quotient $\frac{M}{N}$ or understand the the submodules of the quotient, it is the same as understanding what are the submodules of M which lie between M and N. So, these P's you know there could be several of them. These different submodules which lie between M and N, to each of them their corresponds a submodule of $\frac{M}{N}$, ok.

So, this is an equivalent way of thinking about submodules of the quotient, ok. So, let us just set up the the bijection itself. So, proving it is is easy. So, let me just tell you what

what the bijection is here. So, here is the bijection. So, on one side let us write down the submodules of $\frac{M}{N}$ and on the other side let us take the collection of all submodules of M which contain N, ok.

So, I want to establish a bijection between these two. So, I will give you maps in both directions. So, here is the first thing. Suppose I have a submodule. So, let us go in the forward direction, if I have a submodule of $\frac{M}{N}$ then here is what I can do. So, let for the moment just go back to the quotient map. So, the quotient map is a map from $M \to \frac{M}{N}$. So, what I could do is um the following. So, let us just move this, ok. Let us move this down.

Now, look at the submodule here. So, let us take. So, suppose I have a submodule of M mod N, ok. So, that something which lives on this side, B is a sub of M by N. Now, what I can do is I have this map pi, I can look at its inverse image under π, ok. Inverse image just means I mean π is not a one-to-one onto I means, it is an onto map, not a one-to-one map, but inverse image just means I take all the elements. So, if B looks like this, ok, here is the ambient module M by N, here is the ambient module M, the inverse image of B just means I take all elements of M which map to B, right. The pre-images of all elements of B. So, that is going to be my map.

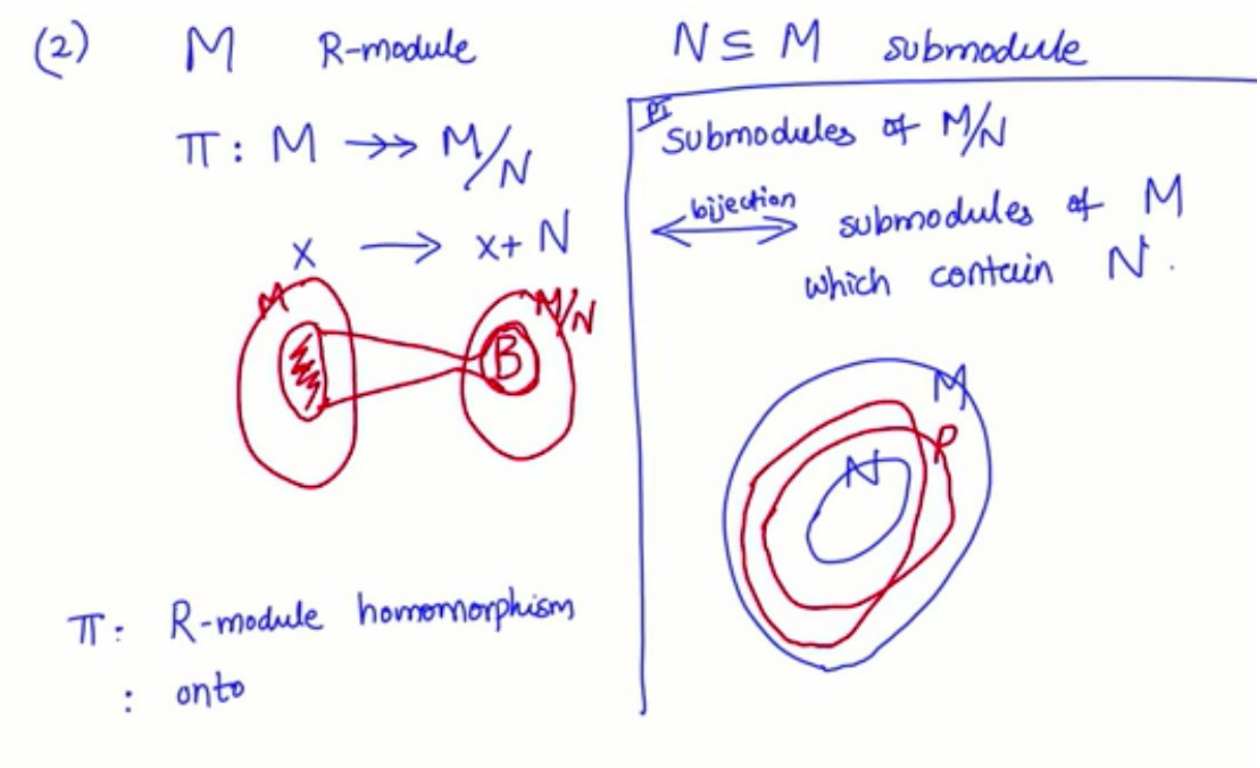
So, this this pre-image is what is usually denoted as $\pi^{-1}(B)$, so to each B let associate. So, if this is my B then to B I associate its inverse image under the projection map, ok by which I mean take all elements of M such that $\pi(x)$ belongs to B, ok. ah It is easy to check that this is a submodule of M, And it contains N necessarily because observe that B is a submodule of $\frac{M}{N}$, so B must have the 0 element of $\frac{M}{N}$, ok. So, the first observation to make here is that this map is well defined. So, let us just record this somewhere. So, observe the inverse image of B um is is a submodule of M, That is easy to check. I believe that for you to verify. But the key property that we need is because B contains the 0 element, the the pre-image of the 0 element which is.

Well, what is the pre-image of the 0 element? It is all elements of M whose cosets give you the 0 coset and that is of course, N by definition, ok. So, the the inverse image of the 0 coset is N. So, N is certainly contained in every $\pi^{-1}(B)$. So, therefore, π inverse B is a submodule of M which contains N that bit is fine.

So, now, let us define a map in the other direction. So, suppose I give you a submodule P of M which contains N then this map is just $\pi(P)$. So, I just map this to all the cosets. So, I define take P and I just map it to, its image under pi, by which I mean all cosets $x \in P$, ok. So, these are the two maps. And I claim that you know these two maps are inverses of each other that they they give you the bijection that you want, ok. Or equivalently you could say that you know you can take any one of the two maps let us say the red map and show that it is a one-to-one and onto, ok.

So, I mean the verification itself is very easy, and I hope you can you can do it. So, let me just do one of them. So, let us check for example, that the red map is one-to-one. So, I claim that, so I mean here is one way of proceeding you prove that this this red map is both one-to-one and onto. Show both its properties. So, let us check that this map is one-to-one or on to whichever is. So, let me do one of them. Let me show its one-to-one maybe you can show it is onto, ok.

So, to show it is one-to-one, what do we need? I need to take two different elements B_1 and B_2, two submodules of M mod N and show if they are distinct, I need to show that their images are distinct. So, if take two fellows B_1 and B_2, so let us write like this I take B_1 and B_2 which are two different submodules of M mod N and then I claim that their images



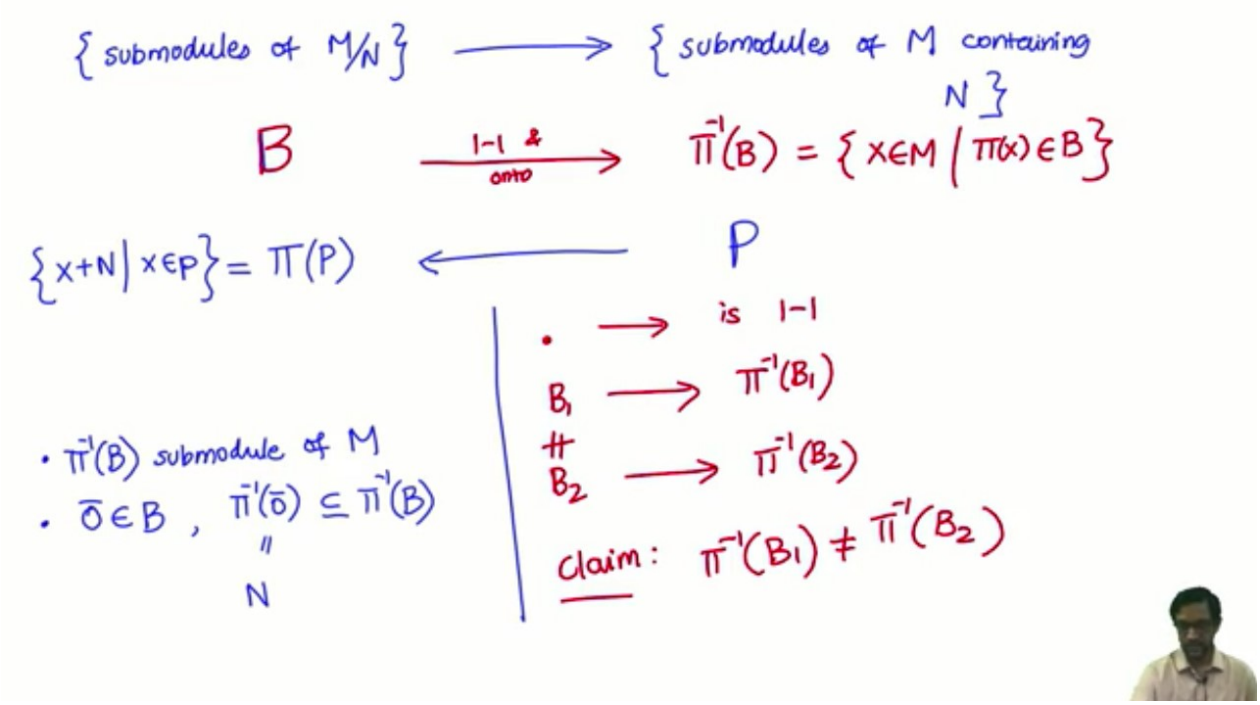
are also distinct. So, look at $\pi^{-1}B_1$, $\pi^{-1}B_2$, the claim is that $\pi^{-1}B_1$ is also not the same as $\pi^{-1}B_2$. And in fact, this is this is just trivial fact about I mean we do not really need the fact that π is a homomorphism or anything, it is just a fact about set maps, maps between sets.

So, let me just give you a diagrammatic argument. So, if M and M mod N, I have a projection map π which is onto, right, the key point is that π is an onto map. And what I am doing is taking two different subsets here. I mean there are submodules, but let just say they are subsets for now. So, we just use two different colors.

So, here are two different submodules B_1 and B_2, ok. So, here is B_1 here is B_2. And I claim that if B_1 and B_2 are not equal to each other, then their inverse images they are you know under π inverse cannot be equal, ok. Why is that? Well, observe that and given B_1 not equal to B_2 means either there is an element in B_1 which is not in B_2 or there is an element in B_2 which is not in B_1. So, let us assume one of them.

So, this means that you know B_1 minus B_2 is not empty or B_2 minus B_1 is not empty, ok. So, let us assume it is a former say the first one. So, let us pick an element x which is in B_1 minus B_2, ok. So, maybe not to confuse with the earlier x and so on let me call it $\mathbb{Z}$. So, $\mathbb{Z}$ is actually a coset in this example because it is an element of M mod N. So, let us take $\mathbb{Z} \in B_1 - B_2$ and observe that, so if $\mathbb{Z}$ is here because π is onto, so I know that $\mathbb{Z}$ must have some pre-image, right. So, let us call this pre-image something. So, let us look at there is an element $x \in M$ which must map to $\mathbb{Z}$, ok. So, since π is onto there exists an element $x \in M$ such that $\pi(x)$ maps to $\mathbb{Z}$.

Now, observe that this x is certainly in π inverse of B_1, because it is the inverse image of an element $\mathbb{Z} \in B_1$, but it is not in $\pi^{-1}(B_2)$, but x is not in $\pi^{-1}(B_2)$ because what is the



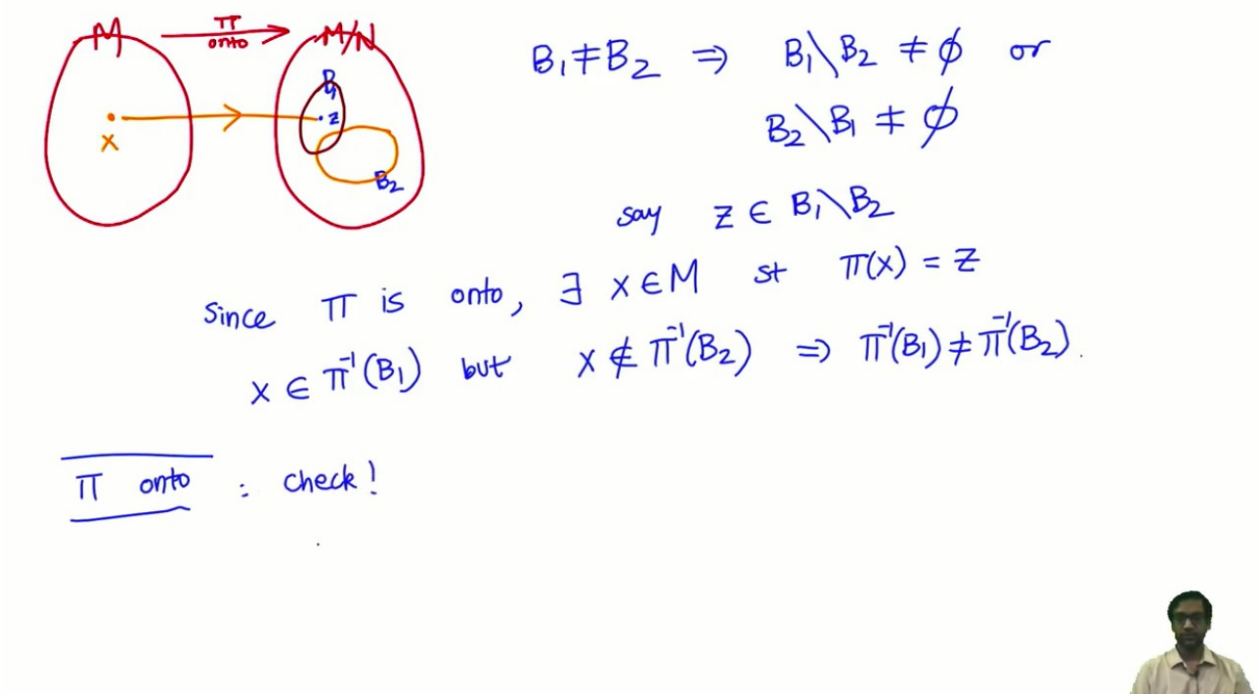
definition of $\pi^{-1}(B_2)$ its all elements of M which map to some element of B_2, right. But in this case x is not I mean x maps to $\mathbb{Z}$ and $\mathbb{Z}$ is not in B_2, ok. So, this shows that $\pi^{-1}(B)$, we have produced an element in $\pi^{-1}(B_1)$ which is not in $\pi^{-1}(B_2)$. So, actually observe for this we we did not really use anything about modules and so on. This is a general fact about onto maps between two sets and their inverse images, ok.

So, this is the first part. The other part which I leave you to check. So, I check π is one-to-one, check that π is onto, ok. Again, a straight forward verification. So, the the result is worth remembering, which finally says that submodules of a quotient are really nothing, but submodules of M which contain N, ok which lie between M and N in some sense, ok.

Now, let us do one last problem which sort of uses this submodules of a quotient business. So, let let me take a specific module. So, suppose I have $\mathbb{Z}$ modulo some power of a $'$. So, consider the following $\mathbb{Z}$ modulo the ideal generated by a single element p^n. And what is a n here? Well, n is at least 1, p is a' . So, this is an ideal. So, of course, it is a left ideal as well if you wish and therefore, a submodule of $\mathbb{Z}$, ok.

So, think of this as a $\mathbb{Z}$ module, $\frac{\mathbb{Z}}{(p^n)}$ is a $\mathbb{Z}$ module, ok. The claim is that, prove that $\mathbb{Z}$ mod p to the N cannot be written, cannot be written as the direct sum as the, well the internal direct sum if you wish of two submodules, of two nonzero submodules . So, everything here is a submodule, modulo over $\mathbb{Z}$. So, two nonzero $\mathbb{Z}$ submodules, ok. So, in some sense it says you cannot split it into the direct sum of two two submodules, ok with both nonzero. So, let us prove this um.

So, first observation is that what we are dealing with is really a quotient module it $\mathbb{Z}$ modulo something. So, it it fits into the framework of the previous problem. So, let us call this M, let us call this N, they are both $\mathbb{Z}$ modules, N is a submodule of M, And what we are trying to do is to understand whether we can decompose this guy into a direct sum of two submodules, right. I want to see whether I can do this or not, ok. To do this, I need to



understand what are the possible submodules B_1 and B_2, right. What do submodules of my quotient look like?

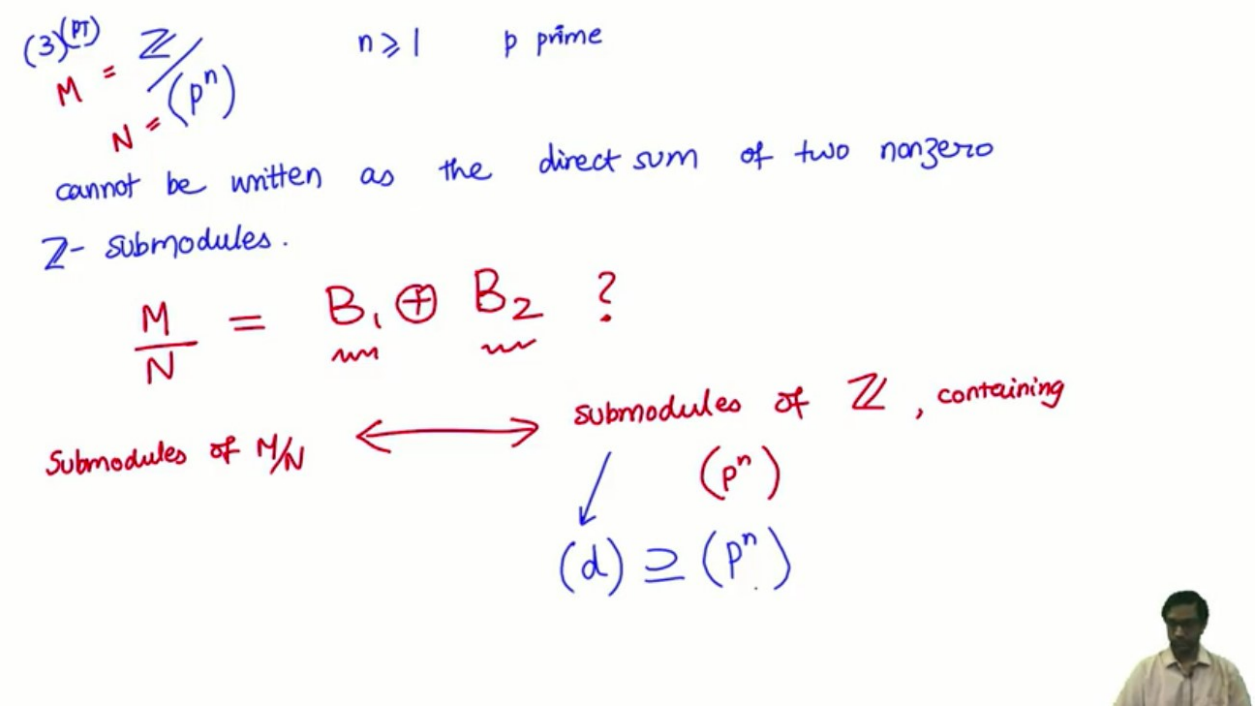
If I can figure that out first, then I can then try and prove that you can never decompose in this way. So, first step is to understand the submodules of M/N, and recall by the previous problem we know what submodules of M/N look like. Submodules of M/N are really in bijection you can think of them, as being in bijection with submodules of M, ok M in this case is $\mathbb{Z}$, containing N and N in this case is the ideal p^n or the submodule p^n, ok, ok.

Now, let us understand the right hand side what do submodules of $\mathbb{Z}$ look like. So, recall submodules of $\mathbb{Z}$ are really the ideals or the left ideals of $\mathbb{Z}$. So, what is a typical submodule? Well, $\mathbb{Z}$ remember is a pid therefore, all ideals are singly generated. So, the submodules of $\mathbb{Z}$ are exactly the ideals generated by just a single integer d, ok. So, any submodule looks like this. And we want to know when does this submodule contain the submodule p^n, ok.

Now, containment is again very easy to figure out for ideals in in $\mathbb{Z}$ as we have seen before. So, if I have an ideal (a) it contains (b) that is the same as saying that one of them divides the other, right, so which divides which. Well, if (a) contains (b) then a divides b, ok. So, this is for integers a and b, ok.

So, what is that mean? So, in our case therefore, we should say, so I had (d) contains (p^n) means that d has to divide p^n and we assume that well p is a' , and so if I have a' power therefore, a divisor of a $'$ power has very few choices really. What can it look like? It is again a', p^m, where the power m.is a number between 0 and n, ok.

So, we are we have already understood quite a bit what are the submodules of $\mathbb{Z}$ modulo p to the n. They are just the submodules, so on the side it is $\mathbb{Z}$ modulo of p to the n. The submodules are exactly submodules of the form p^m, you know they are in there in bijection if you wish with submodules of the form p^n, ok. So, let us just write down that final conclusion. So, the submodules of $\mathbb{Z}$ modulo p^n are therefore, exactly; what are they? They are all the

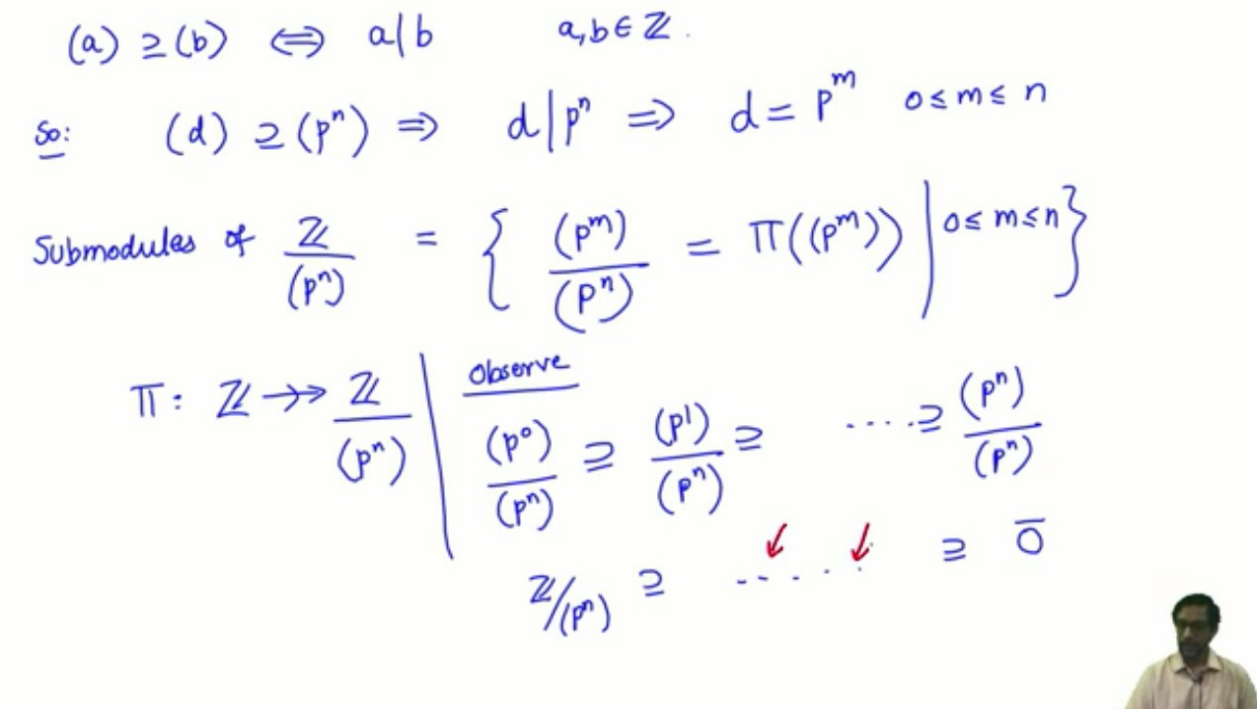


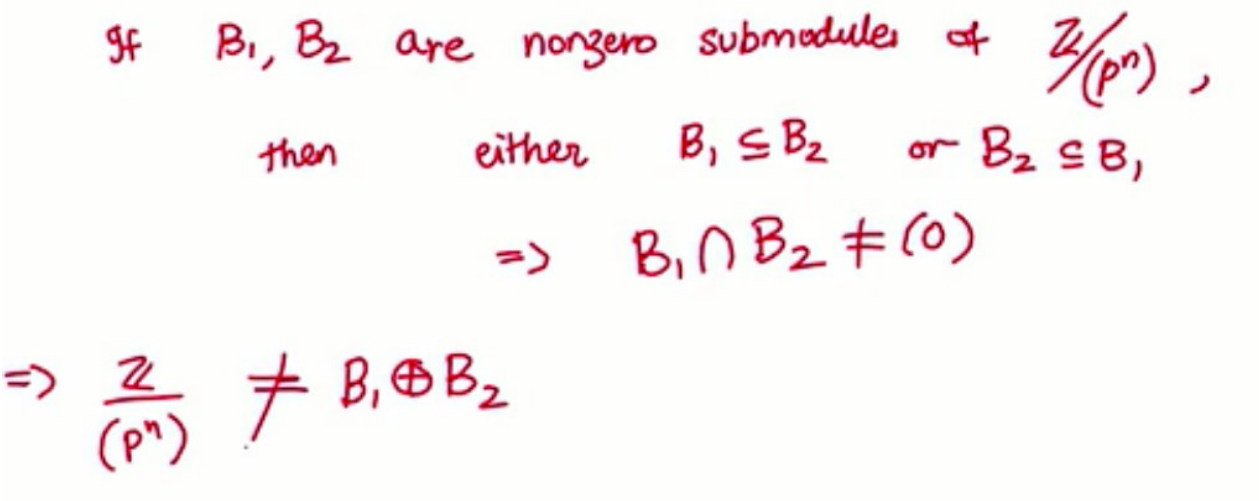
submodules they are the following form. So, take p^m and look at its quotient, ok, where m. So, what is this? Another notation for this is what we used earlier π of p^m, ok where π is the projection map from $\mathbb{Z}$ to.

So, all cosets of all elements coming from $p^m$and $m$is now a number between 0 and n. So, the submodules look exactly like this, ok. Now, here is the interesting observation. These submodules actually form sort of a chain, ok with one contained in the other, ok. So, that is the the interesting thing which is having $'$ powers. So, the key observation here observe that if I look at you know what do the submodules look like I can look at $\pi(p^0)$.

So, as p^0 by p^n or p^1 by p^n, all the way till p^n by pp^n this is just the trivial submodule of the quotient if you wish. And they are all contained one in the other in this way. This is the largest, this contains an x guy, it is contains an x guy and so on. So, on this side is the 0 submodule, and on this side this is the whole p^0 is just $\mathbb{Z}$. So, this is $\mathbb{Z}$ mod p^n, ok. So, observe that all the submodules behave in the following way, ok. The quotient module $\mathbb{Z}$ mod pn has the 0 module and the full module. They are of course, submodule s. But every other submodule occurs as part of a chain which goes from the bottom to the top, ok.

In particular, what it says is that these B_1s and B_2s that I am looking for, right. So, I am I am trying to say can I write this as some $B_1 \oplus B_2$. Well, B_1 and B_2, but must both occur somewhere in this chain, right. If I could write it as B_1 and B_2, B_1 must be one of them, B_2 must be you know another both occurring inside this chain. But observe that will mean that either B_1 is contained in B_2 or B_2 is contained in B_1, right. They both occur as part of this chain somewhere. So, if B_1 and B_2 are any two nonzero submodules, if B_1, B_2 are nonzero submodules, the observation now is that of $\mathbb{Z}$ mod p to the n, then the observation is that either B_1 is inside B_2 or B_2 is inside B_1, ok. In particular, it means that their intersection is not 0 because the intersection is one of them its either B_1 or B_2 whichever is smaller, right and I have assumed I have two nonzero submodules. So, what does that mean? It





means that you know these two guys are not are not independent in the sense that you know remember to say that the whole thing is a direct sum of these two. What I need is that their intersection must be 0, right and their sum must give me the whole module.

Now, in this case the intersection itself is not is not 0, ok. So, this automatically proves that my whole module is definitely not, you know it does not make sense to say that it is their internal direct sum at all, ok. So, I mean this is this is again, it demonstrates the utility of uh trying to understand submodules of a quotient in terms of modules of the ambient module.