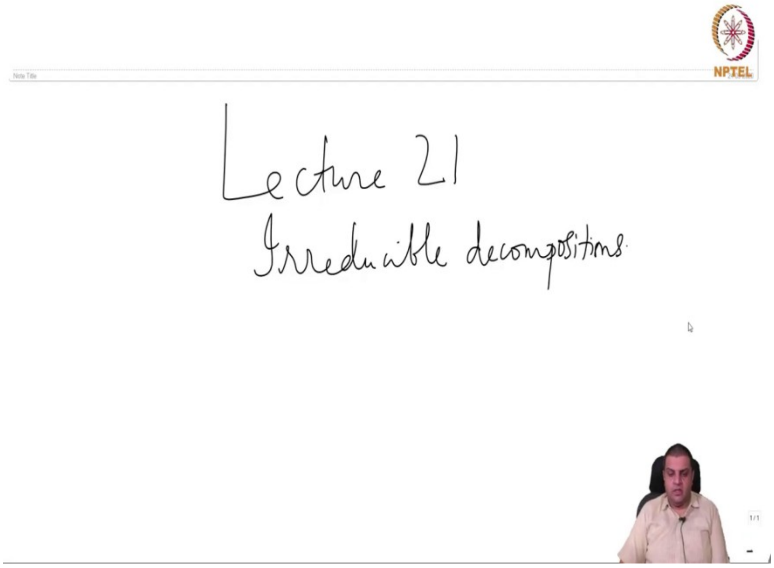
Computational Commutative Algebra
Prof. Manoj Kummini
Department of Mathematics
Chennai Mathematical Institute
Indian Institute of Technology, Madras

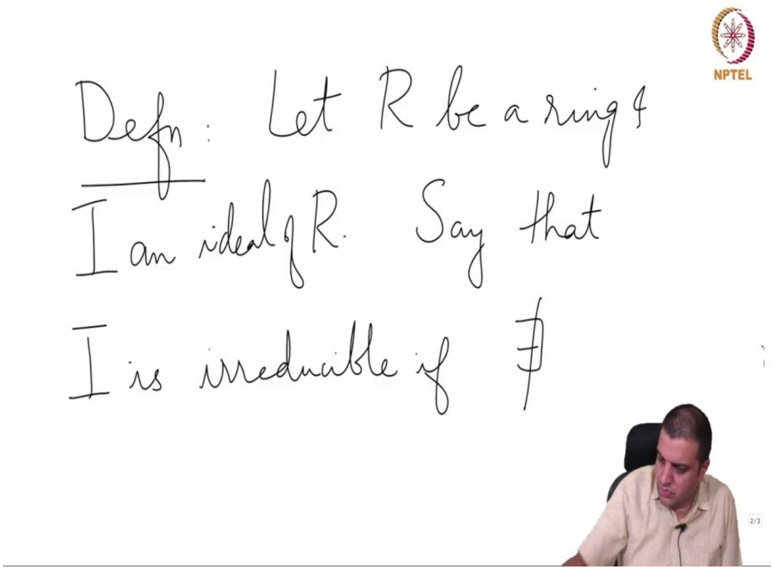
Lecture – 21
Associated primes

(Refer Slide Time: 00:17)



So, this is lecture 21 and we continue our discussion about irreducible decomposition.

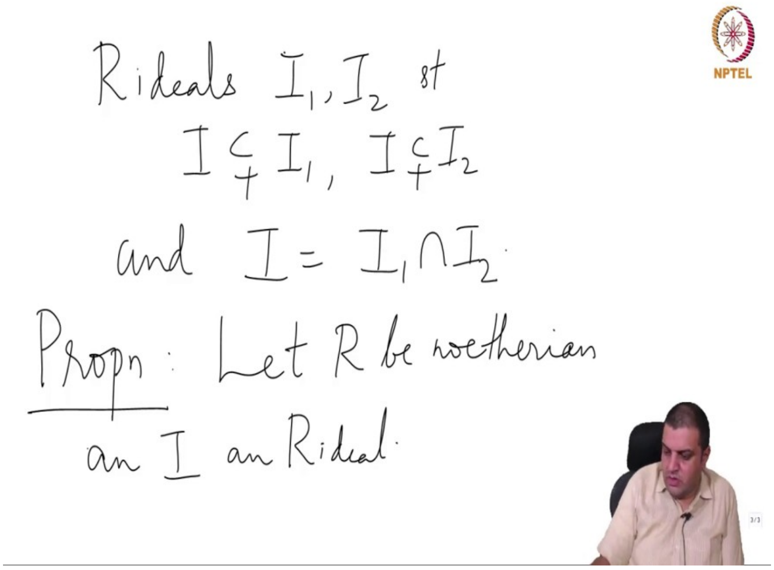
(Refer Slide Time: 00:23)



So, definition. So, now, we want to slowly shift to discussing irreducible decompositions of ideals as opposed to spectrum of a ring. The reason is that if you have to work with arbitrary rings, we need this notion and not just for spectrum.

One important reason is that we have not yet defined it, but we will come to it the irreducible decomposition of an ideal and irreducible decomposition of its radical would be different, but the spectra are the same. So, there if you take the irreducible decomposition, it is going to it will be the same.

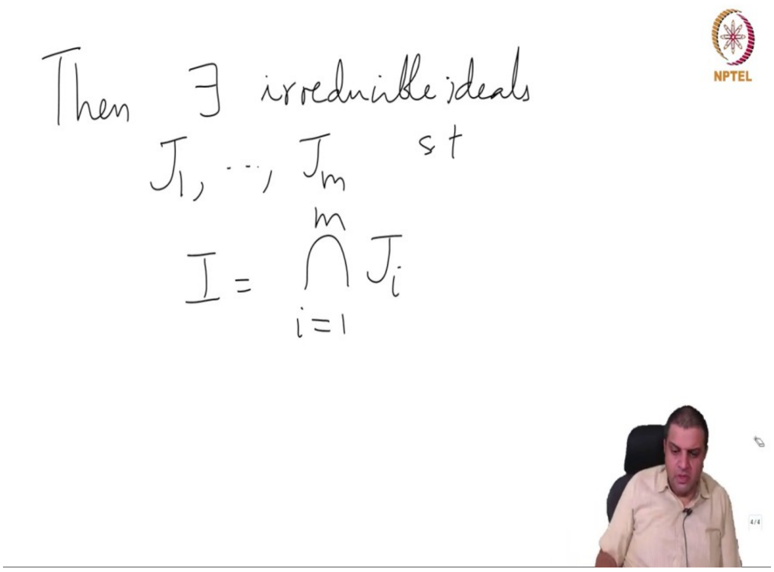
(Refer Slide Time: 01:43)



So, let R be a ring and I an ideal. Say that I is irreducible if there does not exist R ideals I_1 and I_2 such that, I is a proper subset of I_1, and I is a proper subset of I_2 and I is the intersection of these two. So, this is a non-trivial intersection.

So, I mean $I = I_1 \cap I_2$ is a non-trivial intersection and if there is no such decomposition of I, then we say that I is irreducible. We are just defining this term I is irreducible if there does not exist such a decomposition. So, this is an important notion. It sort of generalizes the notion that we just talk for spec. So, here is a proposition, let R be an Noetherian ring and I an R ideal.

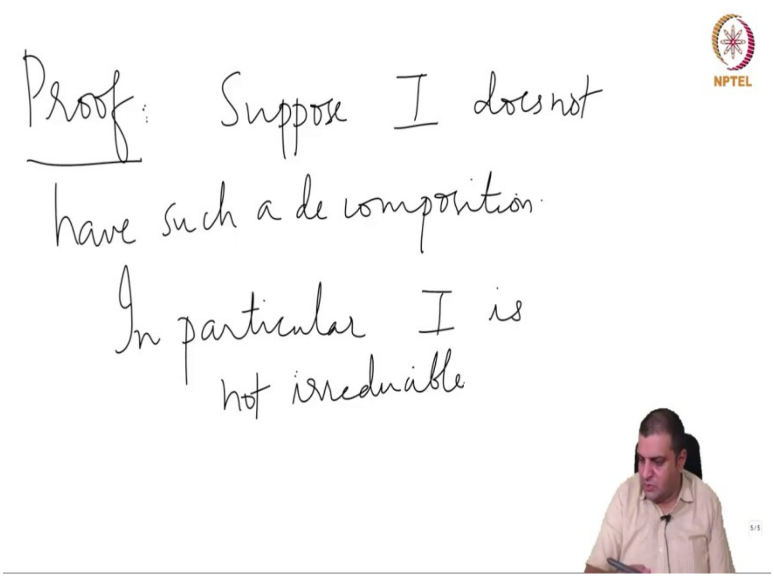
(Refer Slide Time: 03:21)



Then, there exist finitely many irreducible ideals $J_1, J_2, \ldots, J_m$ such that $I = \cap J_i$. So, any ideal can be written as a finite intersection of irreducible ideals in a Noetherian ring.

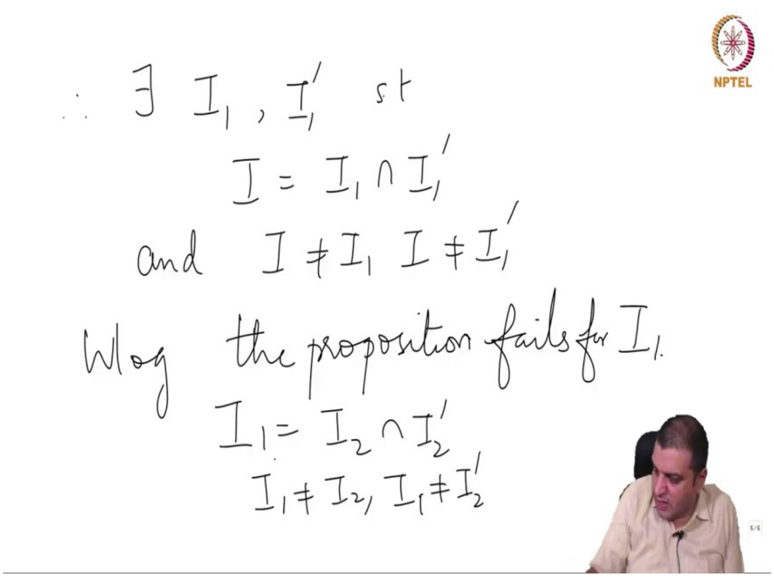
So, we will use this as a starting point and try to get more understanding of this decomposition and this will take us a few lectures and it is going to be more abstract than what we have discussed so far, and eventually, after a while we will come back to computational aspects of this question what are how do we try to find this decomposition.

(Refer Slide Time: 04:31)



So, the proof is sort of a typical proof in an Noetherian case. So, suppose this is not true, suppose I cannot be written that way, suppose I does not have a such a decomposition. What does that mean? Well I cannot be written as a finite intersection of irreducible ideals. In particular, I is not irreducible. Irreducible ideals themselves can be written as just I equals I that would satisfy.

(Refer Slide Time: 05:27)



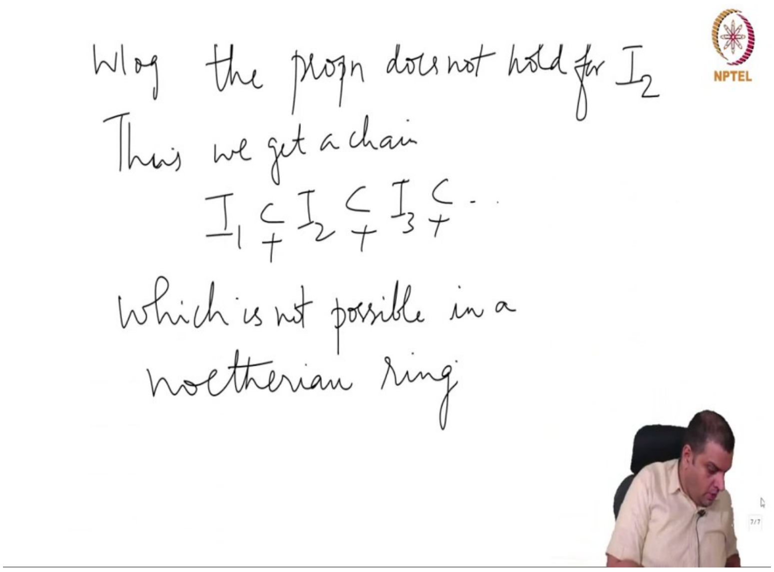
Therefore, there exist some I_1 and some $I_1^{'}$ such that $I = I_1 \cap I_1^{'}$ and $I \neq I_1$ and $I \neq I_1^{'}$. So, these are strictly bigger ideals which contain I, but their intersection is I.

Now, the proposition cannot hold for one of these. Suppose the proposition holds for both, then this is an intersection of finitely many irreducibles, this is an intersection of finitely many irreducibles and one can just put them together and that is a finite intersection of irreducibles.

So, without loss of generality the proposition fails for I_1, it is just whatever we just discussed. If the proposition holds for both, it will also hold for an intersection because in intersection of two finite intersections is a finite intersection.

And now, we can ask I_1 can be written as some $I_2 \cap I_2^{'}$ where again $I_1 \neq I_2$ and $I_1 \neq I_2^{'}$ by the same reason. So, same argument and again without loss of generality.

(Refer Slide Time: 07:23)

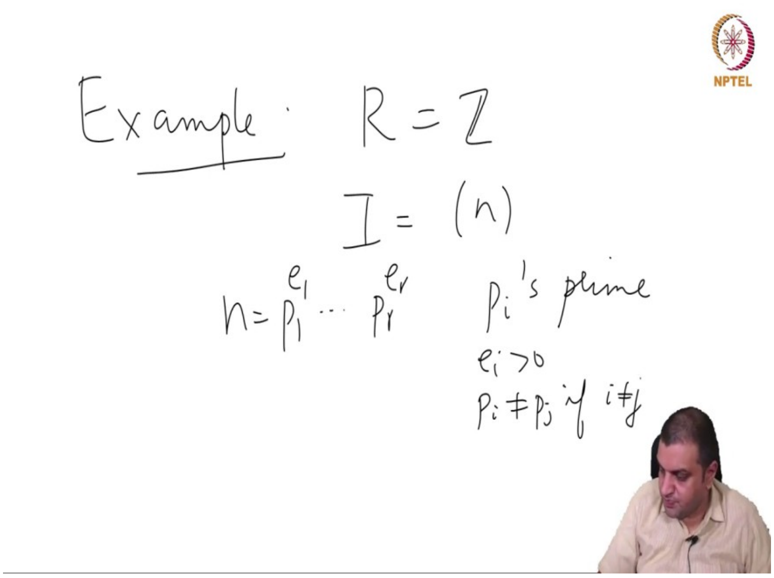


The proposition does not hold for I_2. Thus, we get a chain $I_1 \subset I_2 \subset I_3 \subset \ldots$ but this is not possible in a Noetherian ring.

Another way to argue is that we had some three equivalence conditions for Noetherian ring. Among all such ideals pick one that is maximal, then same way it is not irreducible so, it can be written like this, but these are strictly bigger. So, the proposition therefore, will work for them and that is one way of proving.

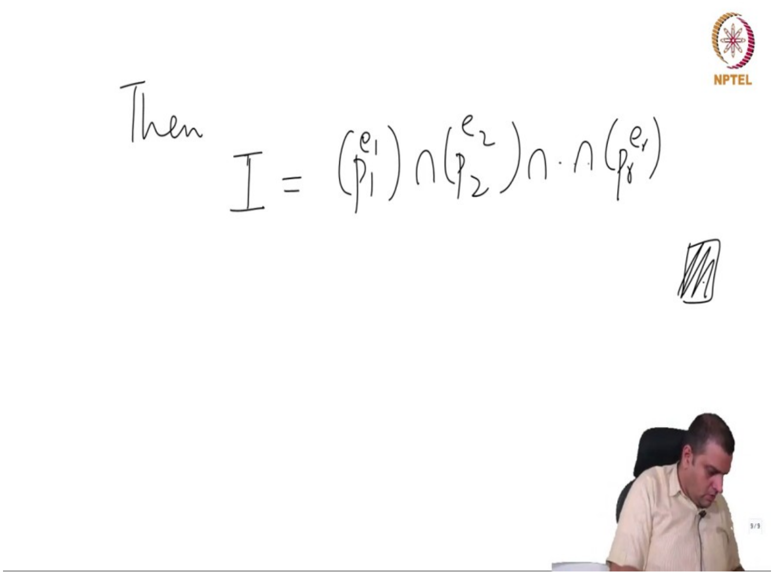
So, among the three equivalents, among the two conditions that are equivalent to ideal being finitely generated one can use either one of them to prove this. So, now, as I mentioned, I mean what we are going to work is to understand what this decomposition looks like. How do we determine this? What extra properties do these ideals J_i have and how unique is it and so on.

(Refer Slide Time: 09:11)



So, let us quickly look at it in Z or $k[X]$ or something. So, let us look at an example. If you take R to be Z and I to be some ideal. Every ideal is principle so I to be generated by some n where $n = p_1^{e_1} \ldots p_r^{e_r}$; p_i's are prime, let us say e_i are positive and p_i different from p_j if i is different from j. So, we have this. Then what is the irreducible decomposition?

(Refer Slide Time: 09:53)

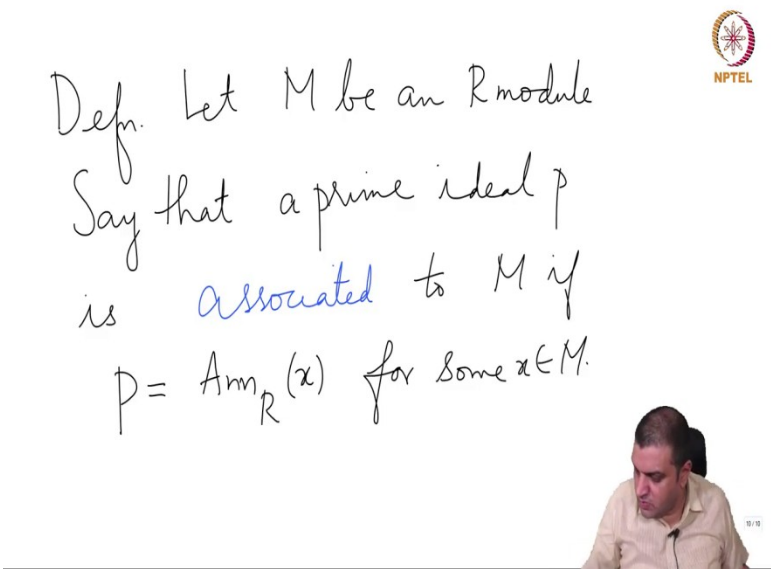


Then I so, one needs to check this a little bit, but after we discuss all these things, it will become clear that this is $I = \left(p_1^{e_1}\right) \cap \left(p_2^{e_2}\right) \cap \ldots \cap \left(p_r^{e_r}\right)$. So, it is easy to check that so, n is in all these ideals.

So, n is divisible by this, by this, by this etc and by no higher powers so, that is just for unique factorization one would get this equality of this I equals this one. What one needs to check is that these ideals are irreducible, but that again one can write out explicitly saying if p is a prime and $(p^e) = J_1 \cap J_2$ then one of them must be equal. So, this is an example.

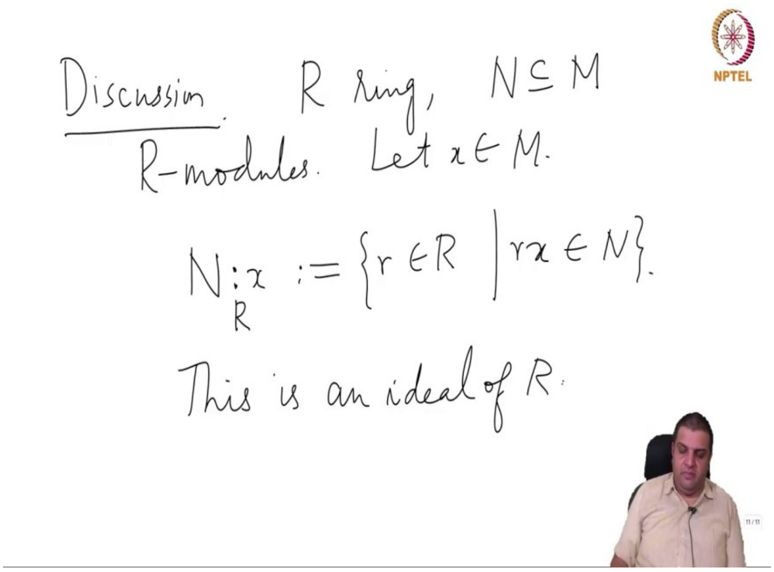
So, we would like to extend this to various other rings, larger number of variables, abstract rings etc.

(Refer Slide Time: 11:27)



So, first of all we will have to switch to the language of modules at this point and we have to introduce some notation, some new language etc. Definition: let M be an R module. Say a prime ideal P is associated to M if $P = Ann_R(x)$ for some $x \in M$. We just need to define what this is.

(Refer Slide Time: 12:39)

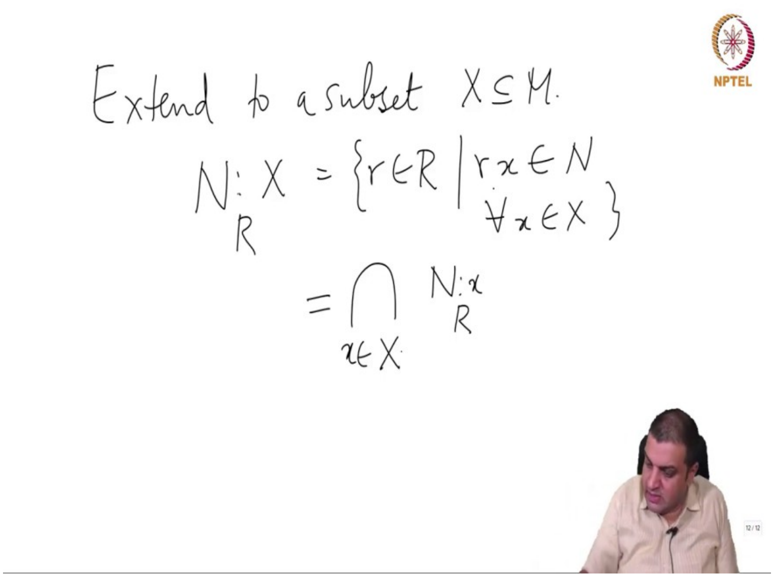


So, a small discussion and will come back to that. So let R is a ring and M is an R module and $N \subseteq M$ is an R module. So N is a sub module of M. Let $x \in M$ Then we can define the following: $N :_R x$.

We write this to mean $N :_R x = \{r \in R | rx \in N\}$. So, this is read as N colon x and if you want to be specific N colon x over R. So, this is a notation.

So, now it is easy to check that this is an ideal of R. So, these are all the elements in R that multiply x into N and one can observe that this is an ideal and that ideal is a proper ideal if and only if $x \notin N$. If $x \in N$, then 1_R will belong to the set so, it will be all of the ring and if $x \notin N$, 1_R cannot belong to this set. So, it is a proper ideal. So, this is an ideal.

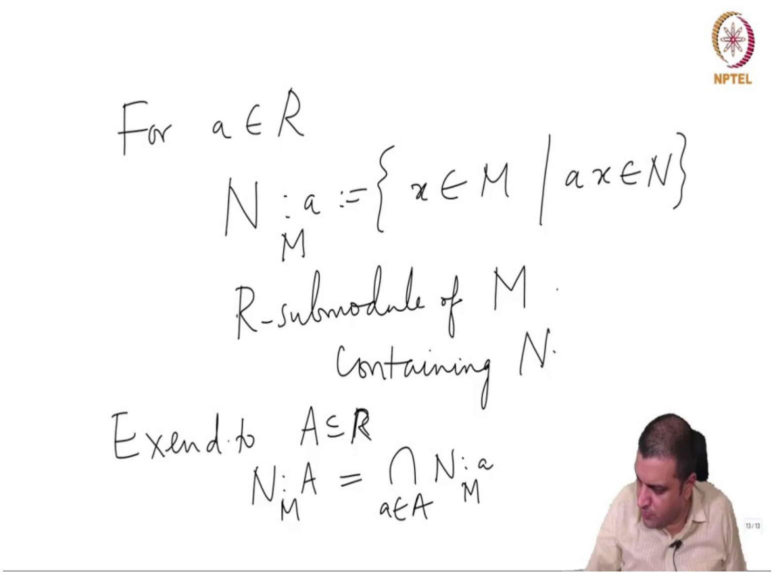
(Refer Slide Time: 14:47)



One can extend this to also a subset X of M not necessarily sub module. So, we can write $N:_R X$, this is a set. So, this is the set $N:_R X = \{r \in R | rx \in N, \forall x \in X\}$ and it is then easy to see that this condition on every x. So, this is the same thing as $\cap_{x\in X} N:_R x$. So, this is just an observation.

We can underlying first thing we have to get this multiplication. Now, we can also reverse the role of R and M in this case.

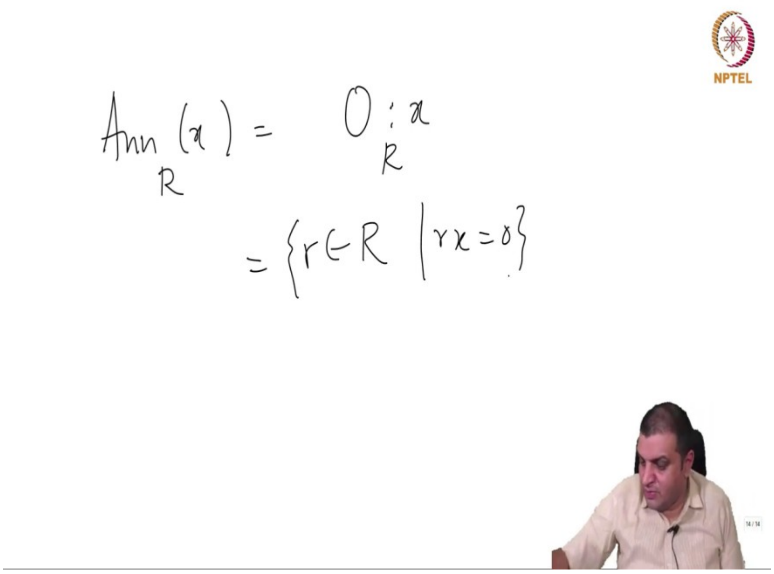
(Refer Slide Time: 15:45)



We can ask for $a \in R$ we can write $N :_M a$ but now the it would be over M and that is just $N :_M a = \{x \in M \mid ax \in N\}$. So, these are the elements of M that multiply a into N. So, this is a R sub module of M. M is a bigger module. If $x \in N$, then $ax \in N$ also. So, this containing N.

And we can also do this for an arbitrary subset. So, I will not write it. It is the same idea to the subset A of R so, then we can write $N :_M A$ defined as like this, this is $\cap_{a \in A} N :_M a$. So, so this is just multiplying and this is just what multiplies some element to a subset.

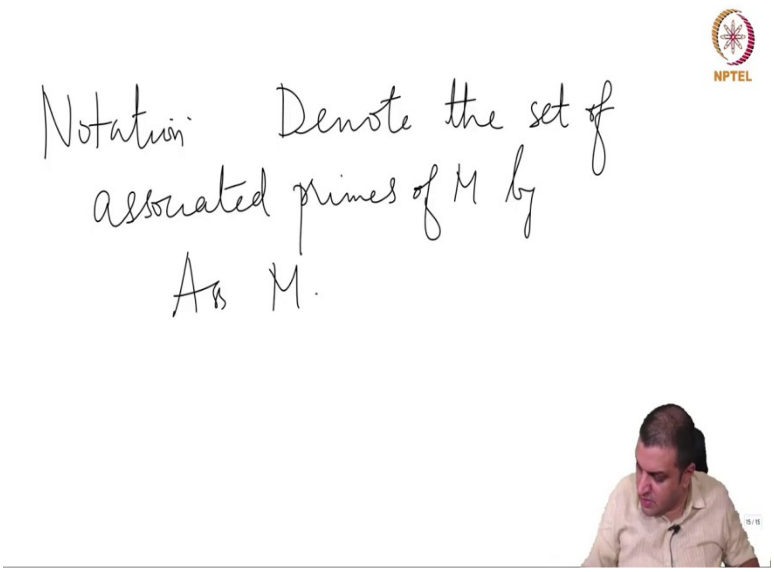
(Refer Slide Time: 17:29)



So, then annihilator of x in R is just precisely $Ann_R(x) = 0 :_R x$. So, that is the set $\{r \in R \mid rx = 0\}$. So, the reason why we introduce the colon notation more than just writing annihilator is that quite often we will have to work with things of this kind N colon some other sub module quite often this X will also be a sub module.

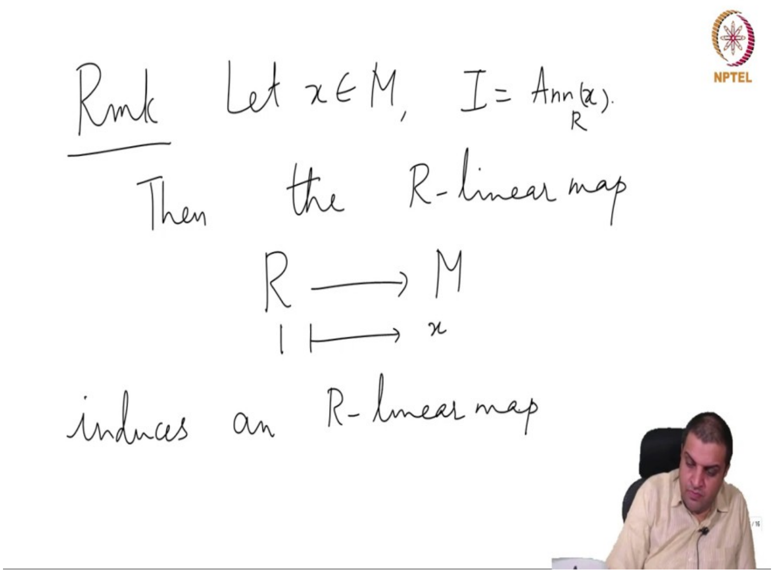
So, N colon some subset over R or one of these like this. So, which is the reason why we introduce this notation. It is just notation not nothing much I mean we will need this later. So, that that explains what annihilator is. This is just this annihilator.

(Refer Slide Time: 18:35)



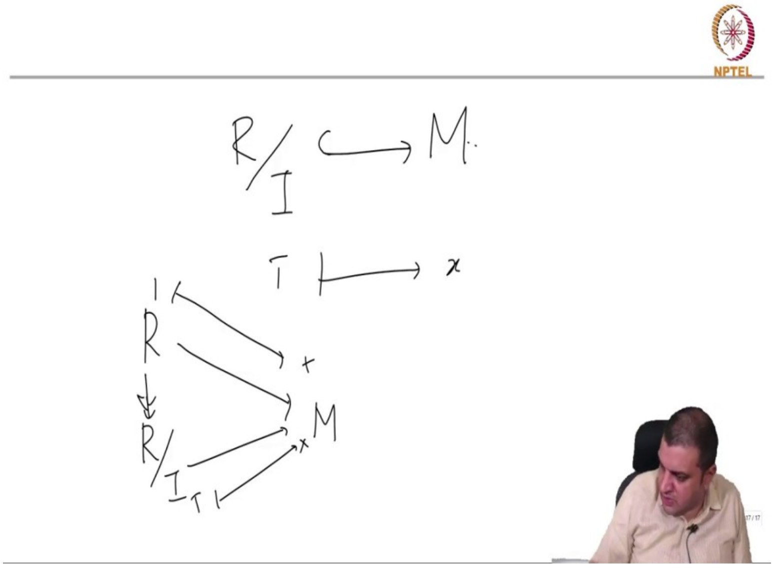
And one more piece of notation. We denote the set of associated primes by $Ass\,M$.

(Refer Slide Time: 19:17)



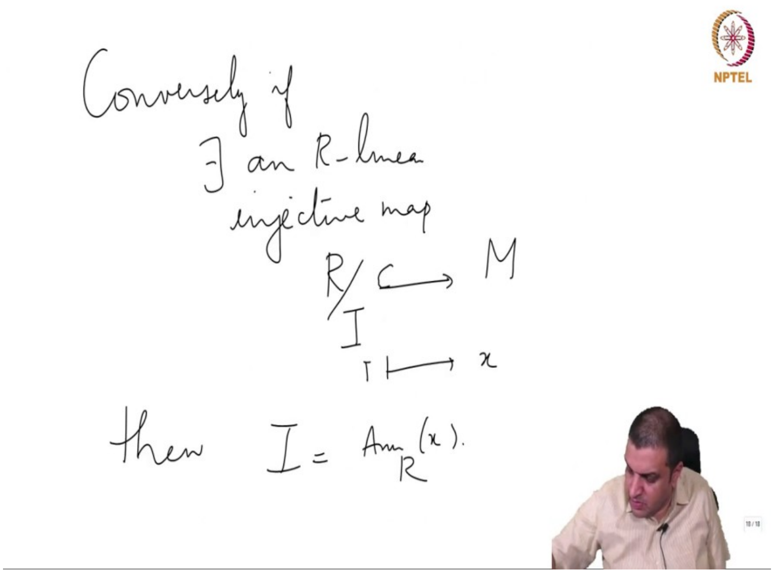
So, one observation about associated primes or in general about annihilators. Remark: let $x \in M$ and $I = Ann_R(x)$. We observe that annihilator is an ideal. Then the R-linear map R to M. Given any R module M and an element inside the module there is a natural R-linear map which takes 1 to that element. So this element induces an R-linear map. So, this is a map from $\frac{R}{I} \to M$ an injective map to M.

(Refer Slide Time: 20:15)



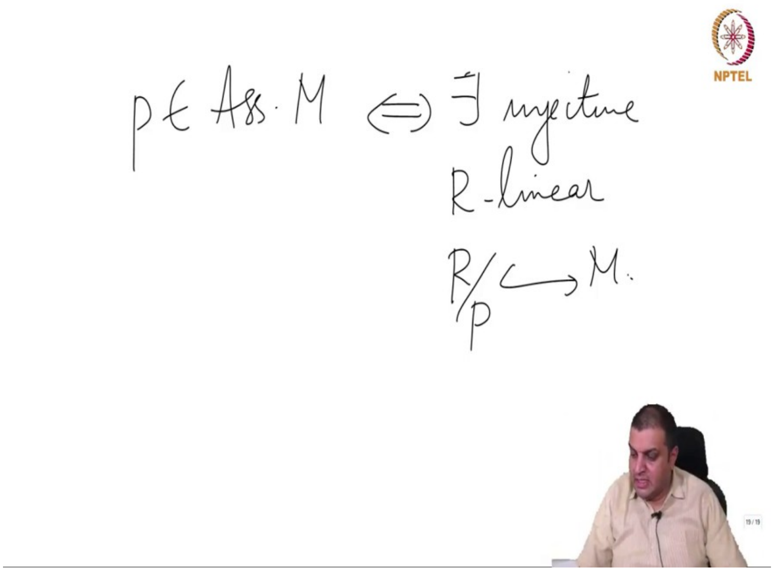
Again $\bar{1}$ here will go to x. So, what we are really saying is that there is the map from R to M and then there is a natural quotienting map and then 1 goes to x here and from here $\bar{1}$ goes to x. So, in other words we say this arrow is a composite of these two arrows. So, this is an observation.

(Refer Slide Time: 21:07)



Conversely, if there exists an R-linear injective map $\frac{R}{I} \rightarrow M$, $\bar{1}$ goes to x then, I is the annihilator of x. Here is injective.

(Refer Slide Time: 22:17)

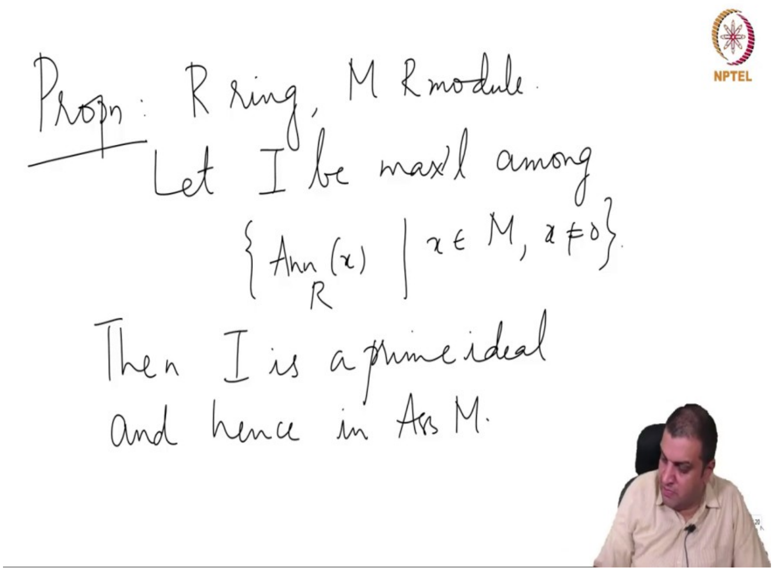


So, why did we say all these things we were discussing associated primes and what was the definition of associated primes? Say that P is an associated prime, if P is the annihilator of some $x \in M$ and now we can rewrite.

Therefore P is associated to M if and only if there exists an injective R-linear map from $\frac{R}{P} \rightarrow M$ and quite often this is how we will probably use it. So, this is what we mean by an associated prime.

And remember we are trying to refine the idea of an irreducible decomposition and we are sort of slowly progressing to set.

(Refer Slide Time: 23:21)

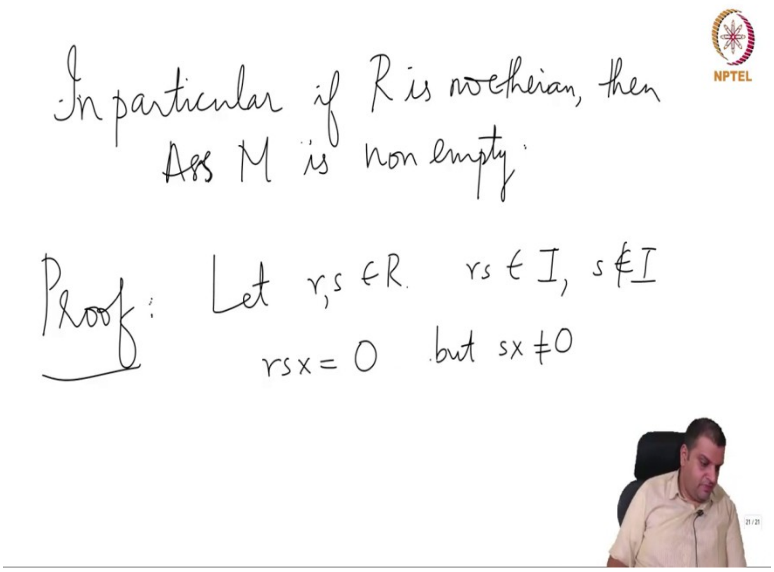


So, now how do we know that a ring has a module has associated prime or do modules have associated primes. So, that is not in general, it is not very easy to answer so, but here is one proposition.

So, right now R is just a ring and M is an R module. Let I be maximal among the set $\{Ann_R(x) | x \in M, x \neq 0\}$. If you put $x=0$ then the annihilators is of full ring and we do not want that in the set because then that will automatically be the maximal.

So, proper annihilators of non-zero elements, there are of proper ideals and I be maximal among these things, then I is a prime ideal and hence it is an associated prime. So, this is one way of proving, one way of looking for associated prime primes, but of course, this is not guaranteed that such set we have maximal elements except.

(Refer Slide Time: 24:47)

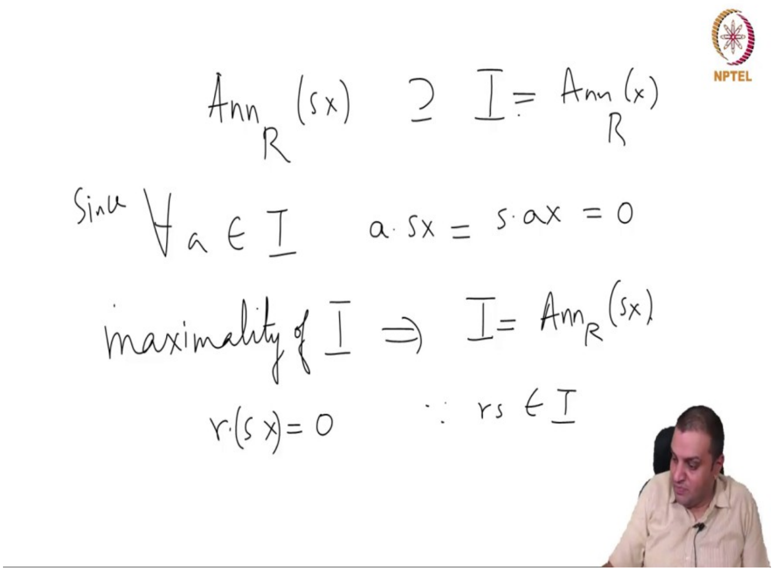


Therefore, in particular, if R is Noetherian, then the set of associated primes is non-empty. So, modules over Noetherian rings have associated primes.

Proof: so, the last part is just an immediate consequence that any non-empty collection of ideals have a maximal element that is the property of Noetherian rings. So, the last part is immediate from the first part itself. So, will just prove the first part and last part is immediate because R is Noetherian. So, we will just prove the first part.

So, let $r, s \in R$, the product $rs \in I$ and $s \notin I$. So, we want to show that $r \in I$. So, what does that say? So, the product $rsx = 0$ because rs is in the annihilator of x, but $sx \neq 0$ because s is not in the annihilator we are just rewriting this condition.

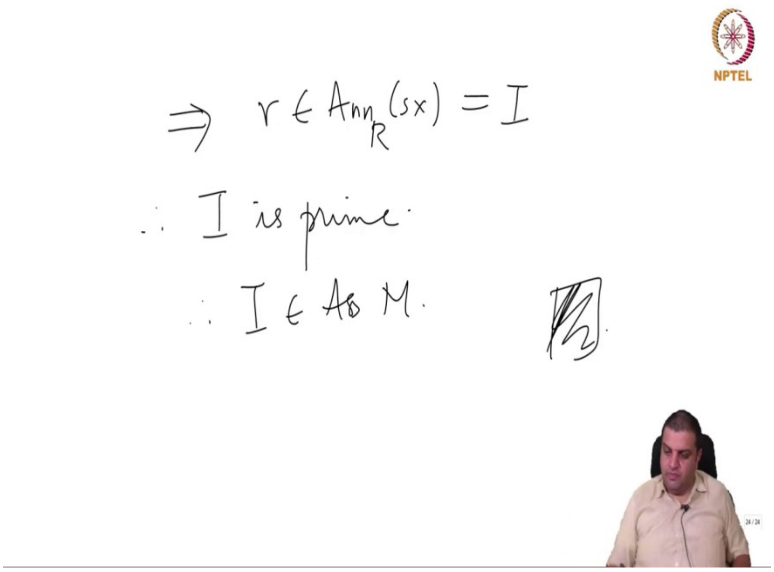
(Refer Slide Time: 26:41)



So, we want to consider the $Ann_R(sx)$. This contains I why? Because $\forall\, a \in I$, $asx = sax = 0$. So, remember this is the annihilator of x. So, this is 0. But I is maximal in that family of annihilators of elements. Maximality of I implies that I is equal to that. So, this is equal to this.

But on the other hand by the same property $rsx = 0$ right because rs is in the ideal I.

(Refer Slide Time: 28:03)



So, then this now implies that this set here contains r, but that is also equal to I. So, this implies that $r \in Ann_R(sx) = I$ which is inside annihilator of sx which is equal to I and therefore, I is prime and therefore, by definition of what an associated prime is any prime ideal which is an annihilator of some element is what is called an associated prime.

So, therefore, I is in associated M and if R is Noetherian that family of ideals is non-empty therefore, it has a maximal element and therefore, those are max primary associated primes. So, this is the end of this proposition.