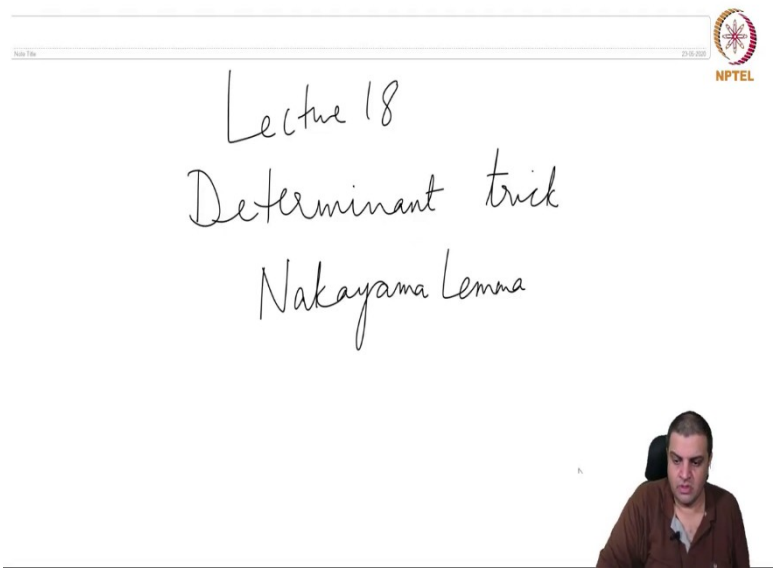
Computational Commutative Algebra
Prof. Manoj Kummini
Department of Mathematics
Chennai Mathematical Institute
Indian Institute of Technology, Madras

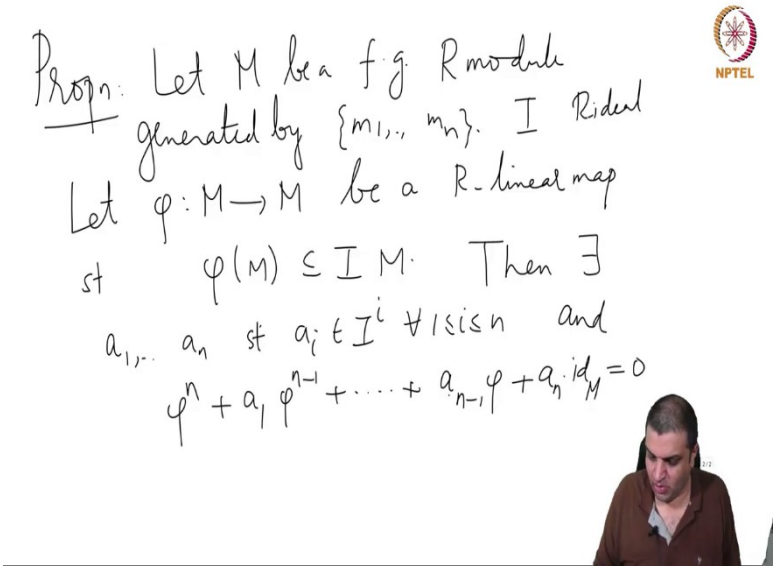
Lecture – 18
Nakayama Lemma

(Refer Slide Time: 00:17)



This is lecture 18. In this, we study the determinant trick and prove important result that gets used all the time called Nakayama's Lemma.

(Refer Slide Time: 00:29)



Proposition: let M be a finitely generated R-module, generated by $\{m_1,\ldots,m_n\}$.Let $\varphi: M \to M$ be a R-linear map and let I be an ideal of R, φ such that φ. So, both these are submodules of M.

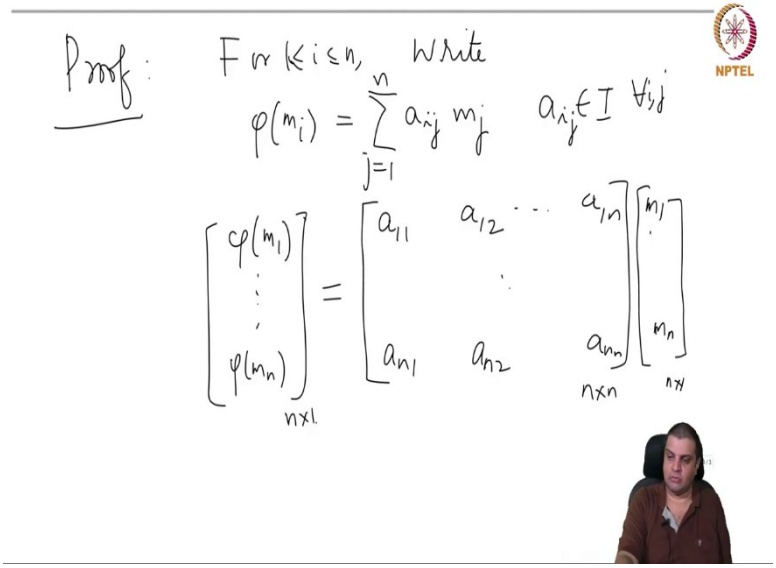
So, this suppose there is a containment. Then, there exist $a_1,\ldots,a_n$ such that, $a_i \in I^i \ \forall\, i$and $\varphi^n + a_1\varphi^{n-1} + \ldots + a_n + id_M = 0$.

So, let us just make sure we understand what the statement means. Notice that, φ is a homomorphism from M itself. So, we can compose it multiple times and we can talk about powers of φ. And, this is just zero times identity just the identity matrix. This is ones and this is the identity matrix.

Now, where does this expression live? Well, this is also because these are R linear maps we can talk about a 1 times I mean a 1 is an element of the ring. So, you can talk about a 1 times a map and we can talk about sums of such maps, because maps form a module, so that is where this is expression lives.

So, this is a statement about certain map being 0. Proof is very elementary linear algebra except that, we have never thought about these things for modules that is it. We have done this many times for variations of this for vector spaces.

(Refer Slide Time: 03:49)



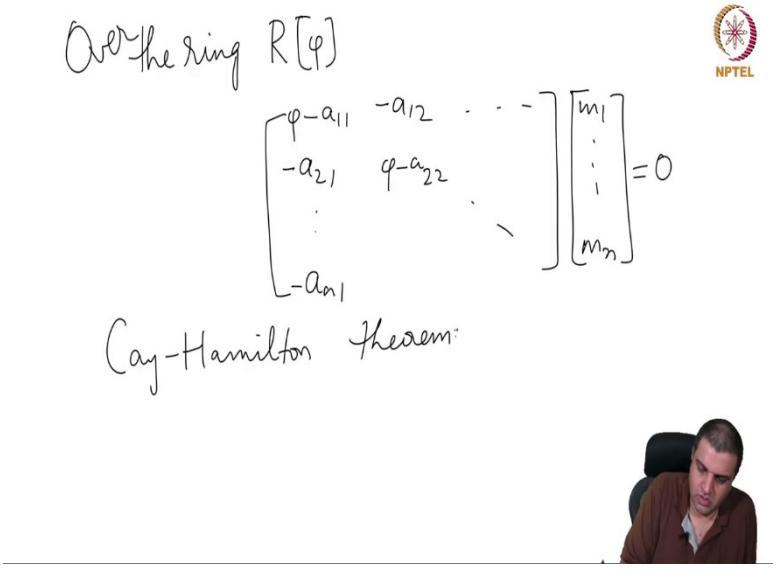
Proof: We know the hypothesis is that $\varphi(M) \subseteq IM$. So $1 \leq i \leq n$, write $\varphi(m_i) = \sum_{j=1}^{n} a_{ij} m_j$, $a_{ij} \in I \; \forall \, i, j$. So, let me just explain why this is possible $\varphi(m_i)$ is an element inside here.

So, we can take some ideal generator of the ideal times m_1 plus something in I ,1 times m_2 and so on. And, when we combine it we will get an expression like this. So, $a_{ij} \in I$. So, this is the observation that such a thing can be written for each i.

So, this can be expressed in terms of a matrix, $\begin{pmatrix} \varphi(m_1) \\ \cdots \\ \cdots \\ \varphi(m_n) \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix} = \begin{pmatrix} m_1 \\ \cdots \\ \cdots \\ m_n \end{pmatrix}$; we get a matrix expression like this.

Then, so here is the trick that we have done for vector spaces, but not or when you study eigenvalues etc., we have done this. But, so now, we have thinking about these as these elements as not just the elements of R, but elements of the R of a larger ring which also includes the endomorphism φ.

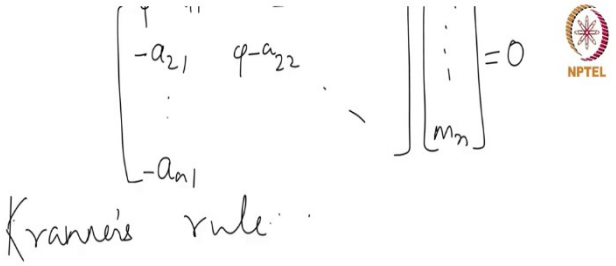
(Refer Slide Time: 06:55)



So, in that ring which is a commutative ring because every element of R commutes with that is the linearity R linearity of φ, and then multiples of φ commute with each other because this is just the same, I mean same map. So, if you have a single map this is a commutative ring.

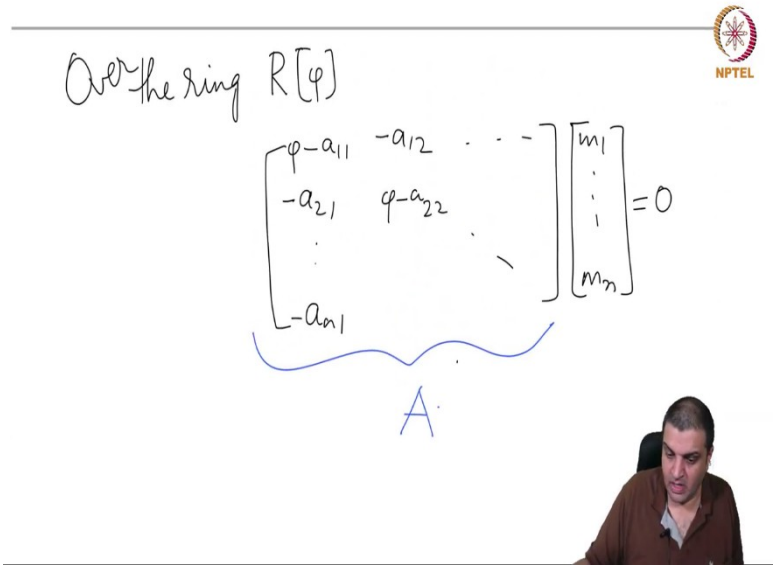
And, so in this ring what we have is that, $\begin{pmatrix} \varphi - a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & \varphi - a_{22} & \dots & \dots \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & \varphi - a_{nn} \end{pmatrix} = \begin{pmatrix} m_1 \\ \dots \\ \dots \\ m_n \end{pmatrix}$. So, M is also module over that, and in that over that we get this expression. So, this expression this matrix has entries in ring $R[\varphi]$ and not in R. But, what does that say?

(Refer Slide Time: 08:41)



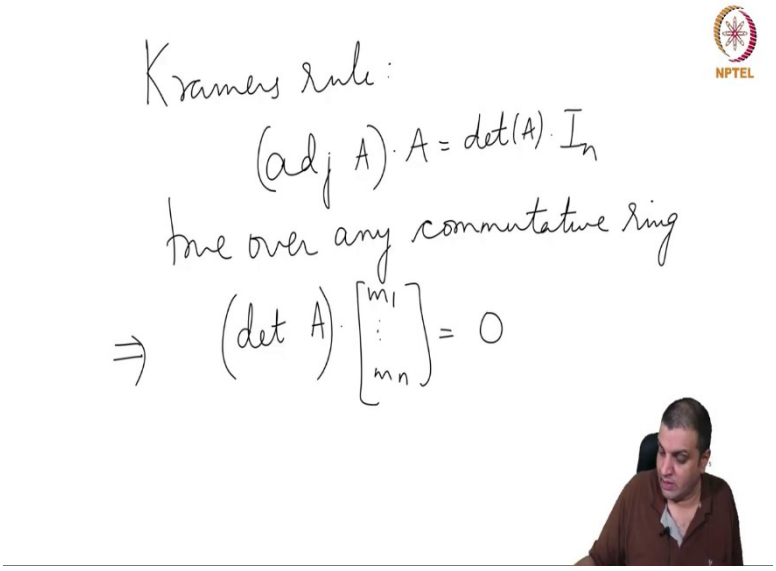
they are Kramer's rule. We use it to find a inverse of a invertible square matrix by taking the adjoint and dividing by the dividing by the determinant. But, if you do not do that, the statement is the follow if you do not try to divide by the determinant the statement is the following.

(Refer Slide Time: 09:19)



So, first of all let us call this matrix A.

(Refer Slide Time: 09:25)



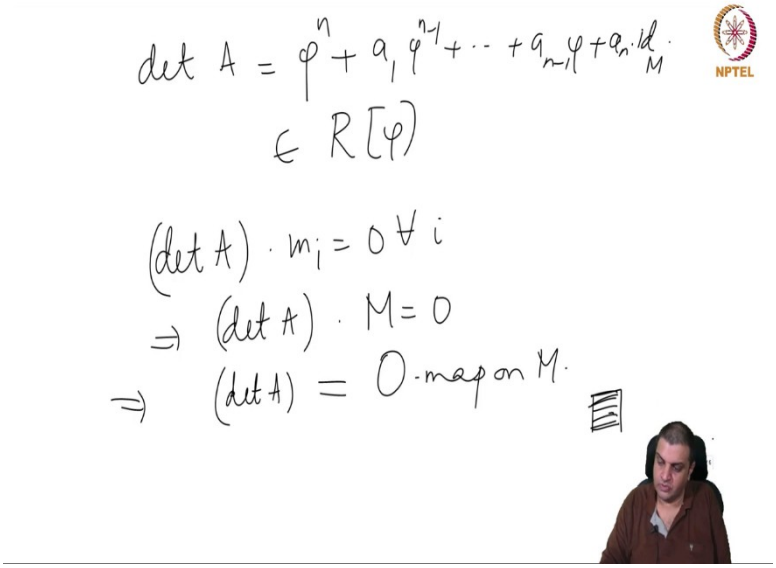
So, now Kramer's rule, it says adj(A) the way it is usually defined in a linear algebra over fields of course, $adj(A)A = det(A)I_n$. This is true. The only problem trying to find inverse using this is if determinant of A is not invertible we would not be able to divide it, but this statement is true over any commutative ring. This is the n by n. So, this is what we have.

So, now let us multiply both sides by adj(A). So, now this one says. So, if you multiply both

sides by adj(A), we get that $det(A)\begin{pmatrix} m_1 \\ \cdots \\ \cdots \\ m_n \end{pmatrix}=0$. But, what does determinant of A look like? This

is where the expression looks exactly like the way we would construct the characteristic polynomial. It is just a polynomial in the, in phi where the entries will be will come the way we compute

(Refer Slide Time: 10:55)



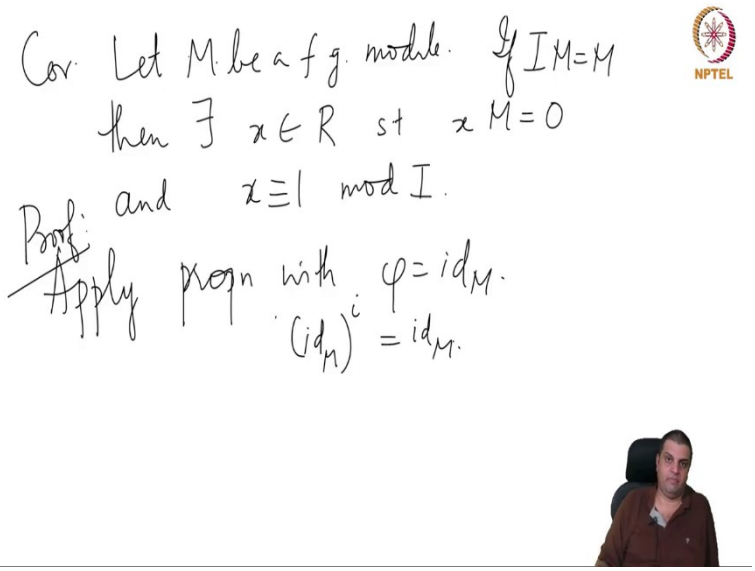
So, the determinant of A has a form $\varphi^n+a_1\varphi^{n-1}+\ldots+a_n id_m$where id_M identity map on M. So, this is form. So, this is an element of R adjoint φ; it is not an element of R. But, what this is say? It says $det(A)m_i=0$ for all i; in other words, $det(A)M=0$

. In other words, this is a 0 map.

Remember, this is an element of this is thought of as some powers of φ, which are endomorphism's and R linear combinations that is an endomorphism. So, this implies that determinant of A is the 0 map .I mean a function is 0 is the 0 map.

So, this is the proof of the, and then by one can check that the coefficients have this property that they are in increasingly larger powers of φ that it is a property of the determinants. So, this is what this is a proof of the theorem of this determinant trick.

(Refer Slide Time: 12:35)

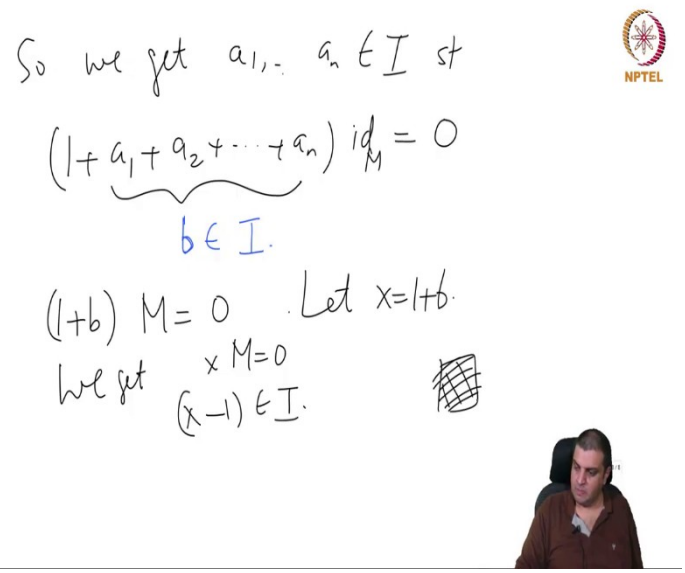


So, now there are many applications of this. So, corollary. M finite, corollaries of always will apply for finitely generated modules. Let M be a finitely generated module , if IM = M, then there exists some $x \in R$ such that, x M =0 and x is congruent to 1 modulo I. In other words, in the ring R/I , x = 1, that is what x is want to into . So, x-1 ∈ I .

So, proof. So, we need to understand this condition $M = \varphi(M)$ in terms of the determinant trick. So, this result this proposition is called determinant trick. So, we need to understand M = IM in this context. Well, the map that we have to consider is identity. So, $\varphi = id$.

So, then we are saying $M \subseteq I\,M$, but which means M= IM. So, we need to understand this. So, apply proposition with $\varphi = id_M$, this is a proof I am sorry. So, apply the proposition with this. So, now what do we get? so, notice that if you take a identity map and raise it to any i^{th} power, this is same; this is just the identity map itself.

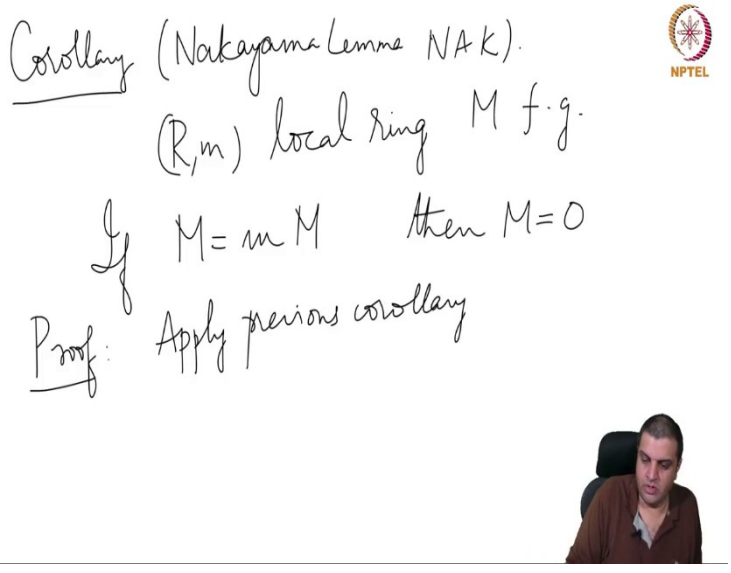
(Refer Slide Time: 14:43)



So, we get $a_1, \ldots, a_n \in I$ such that $(1 + a_1 + \ldots + a_n)\, id_M = 0$ So, notice that this element is inside; so, call this element b ; and b $\in$ I .

So, now, what do we know (1+ b) M = 0 because (1+ b) M is just I mean it does not change M at all. So, if you take this composite, I mean this whole map and apply to an element of M, it is just this element multiplying that element of M. So, this is just(1+ b) M = 0 . And, let us define x= 1+ b. So, that therefore, we get xM = 0, and $x - 1 \in I$. So, this is what we are asserted.

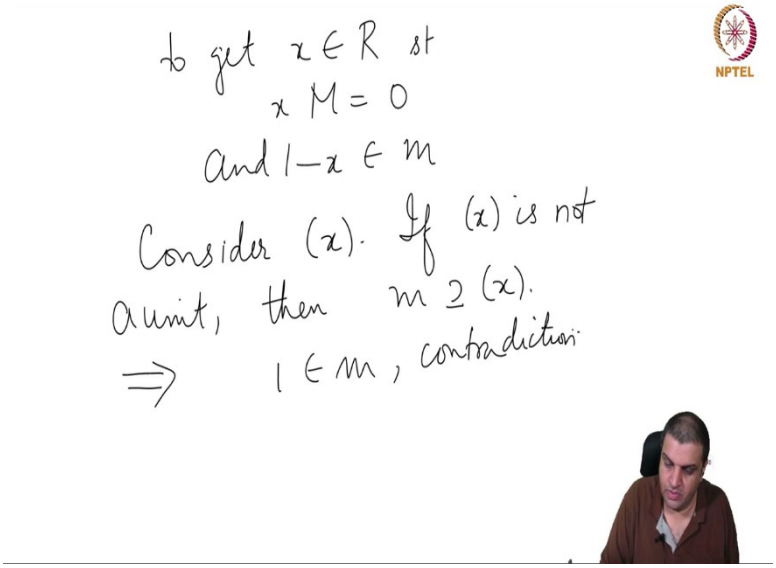
(Refer Slide Time: 16:21)



Another important corollary. so any version of this is called Nakayama's Lemma, but maybe the only the local version we will you say Nakayama's Lemma.

And, we will usually write NAK to abbreviate this in these lectures. So, what does that, what does the statement say? Suppose that (R, m) is a local ring, M finitely generated. If M = mM the maximal ideal times the module itself. So, this is a submodule of M. If M equals the sub module, then M =0. So, proof apply previous corollary.

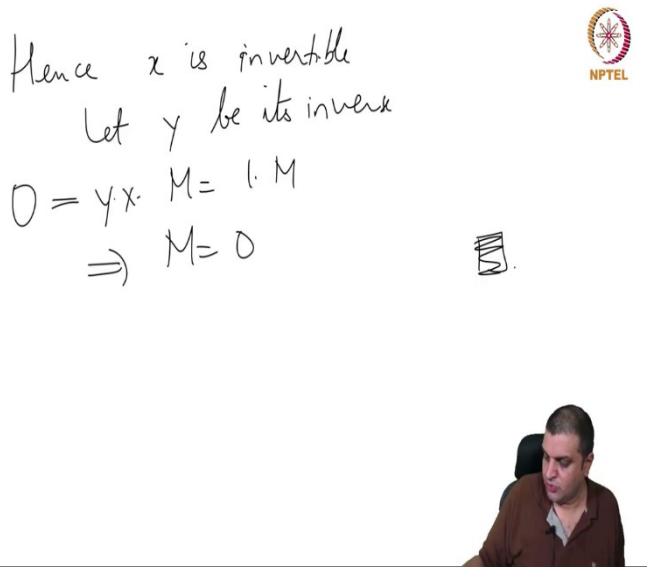
(Refer Slide Time: 17:49)



To get $x \in R$ such that x M=0, and 1-x is in the maximal ideal, but let us see what x is. So, is, we claim that x is a unit. So, consider the ideal generator by x. If x is not a unit,then $(x) \subseteq m$.

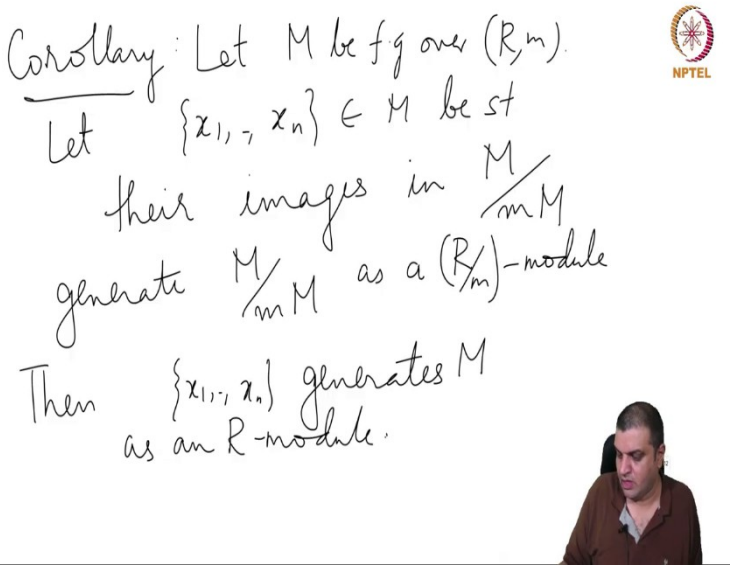
And, this implies that $1 \in m$. Every proper ideal is contained in a maximal ideal. If x is not a unit, then x is not invertible, then this is a proper ideal and it must be inside the maximal ideal; therefore, the unique maximal ideal. And therefore, 1 by from this expression, we get 1 is inside m; this is a contradiction.

(Refer Slide Time: 19:25)



Hence, x is invertible. Let y be its inverse. When we say invertible for multiplication and here we mean its multiplicative inverse. So, then y.x.M = 1.M on this side it is 0. So, M=0. So, it is this version that we often use as Nakayama's Lemma in many applications. So, if you have a local ring finitely generated module if it is, if M = mM, then M = 0.

(Refer Slide Time: 20:21)



Just one more corollary. So, this is another application of the same, same result; it is just a variation of Nakayama's Lemma or we can call this the Nakayama's Lemma. So, let again M

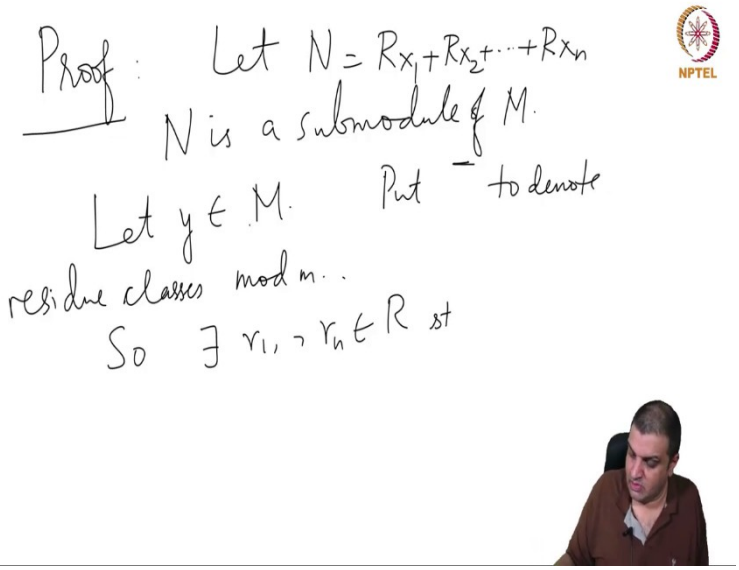
be finitely generated over local ring (R, m). Let $x_{1,\ldots}, x_n$ inside M be such that, their images such that, their images in $\frac{M}{mM}$ generate $\frac{M}{mM}$ as a $\frac{R}{m}$ module.

This is a vector space if this is a R/m is a field, therefore, M/mM is a finitely generated module over it, so it is a finite dimensional vector space. So, then we can talk about some elements. And, elements of here R residue classes of elements of M. So, let us just pick n elements in M; whose residue classes will generate this finite dimensional vector space. Then, $x_1, \ldots, x_n$ generates M as an R-module,.

So, this is how. So, let me just read this once more. Let M be a finitely generated module over R mod R, m local R, m. And, we have a finite generating so we take some finitely many elements inside M; whose images in the quotient generate the quotient, but the quotient module over R/m. So, this is a; this is a field.

So, this and since M is finitely generated the quotient is also finitely generated over the quotient ring. So, this is a finite dimensional vector space. And, we are just saying pick a spanning set, but pick a spanning pick elements in M whose images form a spanning set, then those elements generate M as an R-module.

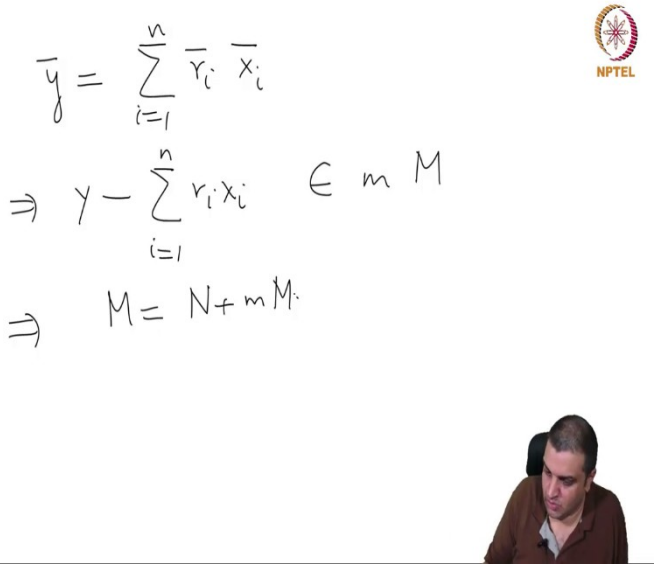
(Refer Slide Time: 23:03)



Proof: let $N = Rx_1 + \ldots + Rx_n$. N is a sub module of; sub module of M. What do we know about this module? So, let y $\in$ M, then so we will put bar to denote residue classes mod mM.

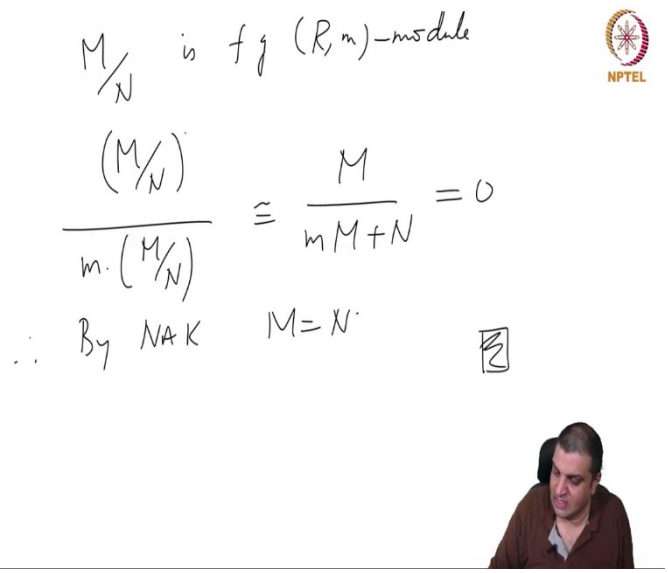
So, now what do we get? so, there exists. So, we get there exists some elements in $\frac{R}{m}$, but . So, we could just take elements in R itself and there exist $r_1,\ldots,r_n \in R$ such that; so, $y \in M$.

(Refer Slide Time: 24:31)



So, if you look at it is $\acute{y}$ image in M/mM, this is $\bar{y} = \sum_{i=1}^{n} \bar{r}_i \bar{x}_i$. This is the hypothesis that M/mM is generated by these elements n elements. But, what does this mean? So, this means that $y - \sum_{i=1}^{n} r_1 x_i \in mM$. So, every element can be written as a sum as an element of N plus an element here. So, this implies that, $M = N + mM$. So, this is what we have. So, where does Nakayama's Lemma come into picture?

(Refer Slide Time: 25:31)



So, now let us consider $\frac{M}{N}$. This is finitely generated (R, m) - module. And, if you multiply this by m, if you write $\frac{(M/N)}{m(M/N)} = \frac{M}{(mM+N)} = 0$. Therefore, by Nakayama's Lemma M = N this is what we wanted to prove, that those elements x generate M . So, this is what we want, M is equal to the sub module which is what we wanted to proof.

So, this is the end of this lecture. And in the next lecture, we will discuss a little bit about spectrum and some topology on spectrum called Zariski topology. And, so the what we wanted to understand I mean how we will proceed that, is to understand the what is behind primary prove the results about primary decomposition and associated primes, and how it fits in, what is I mean why is it relevant in this when we study solving equations v of i looking at zero sets of ideals etc.