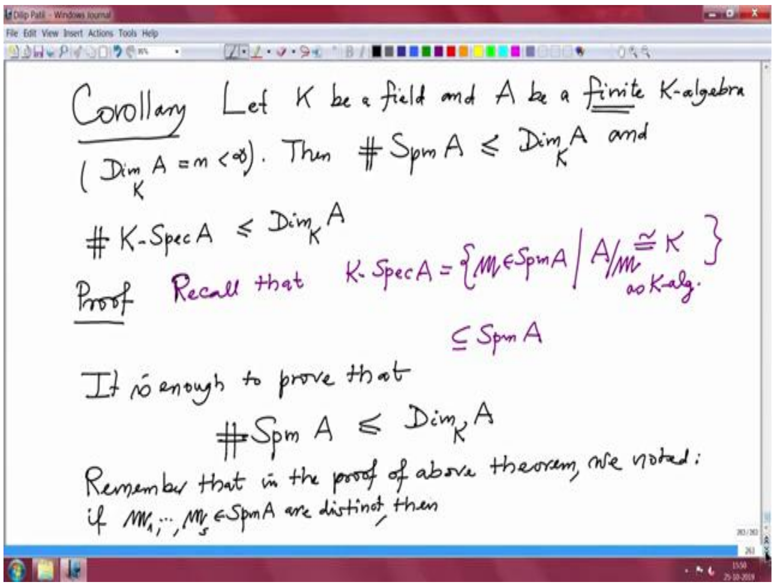
Introduction to Algebraic Geometry and Commutative Algebra
Professor Doctor Dilip P. Patil
Department of Mathematics
Indian Institute of Science, Bengaluru
Lecture 40
Krull Nakayama Lemma

Welcome back to this second half of today's lecture. Just now I proved a theorem, the artinian imply Noetherian, the Jacobson radical is nilpotent and the number of maximal ideals in artinian ring is finite.

(Refer Slide Time 0:51)



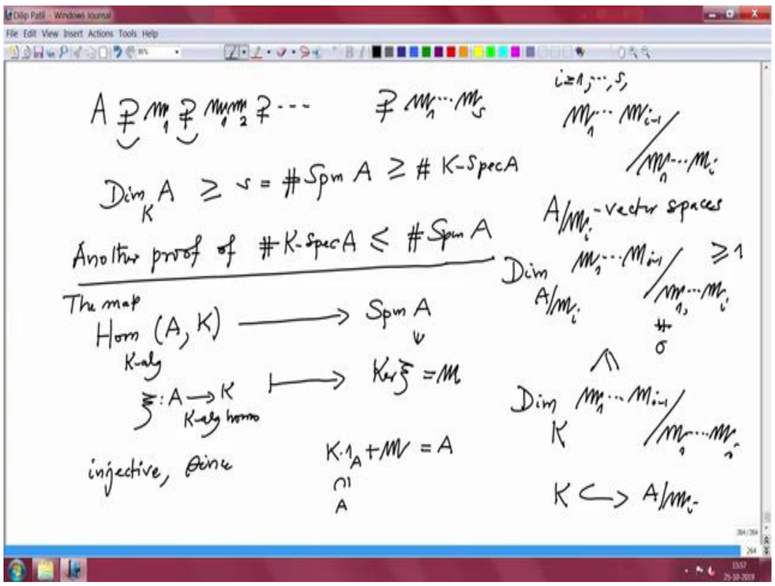
So, I want to note one important corollary. So, let K be a field and A be a finite K algebra. Remember when I write finite K algebra that means A as a module over this ring A, this ring K is a finitely generated and because in this case K is a field, this finite A algebra will simply means dimension of A as a K vector space is finite so let us call it n. In this case, then the cardinality of the set of maximal ideals is less equal to this dimension.

Dimension of K as a vector space over K and K spectrum I hope you are not forgotten because it is for a while we have not talked about it. This is also less equal to dimension of A over K. What was the K spectrum? So, proof, recall that K spectrum of a K algebra is precisely all those maximal ideals in A such that the residue field is isomorphic to the field K as K algebras. Therefore, this set is contained in Spm and we have seen example where it may not be equal.

So, therefore if I have to proof both these inequalities, I will only have to prove one of them. I will only prove this one and because this cardinality will be big or equal to this that we will also follow. So, it is enough to prove that, it is enough to prove that cardinality of the set of all maximal ideals is less equal to dimension of A over K.

So, how do we prove this? Remember in while proving the above theorem, so remember that in the proof of above theorem we noted the following, if I have if m1 to mr, m1 to ms are different maximal ideals are distinct then we have constructed. I will write on the next page then we have constructed a strictly descending chain.

(Refer Slide Time: 4:49)



So, A contained in not equal to m1 contained in not equal to m1m2 and so on. At least till m1 to ms and therefore, and each stage the residues that m1 mi minus 1 mod m1 mi this is for i equal to 1 to s this residues modules, this they are A by mi vector spaces. Because they are analyted by mi therefore and because it is strict here this has to one dimension at least and hence dimension over A by mi m1 to mi minus 1 by m 1 to mi this is big or equal to 1 because its strict here this is non zero and therefore dimension of the non zero vector spaces at least 1, so at each stage dimension is 1.

If this dimension is 1, then the dimension over K is even bigger because this dimension is big or equal to dimension of over K of this m1 to mi minus 1, m1 to mi this because K is contained in

A by mi. So, if the dimension of a bigger so it is, these are vector spaces over K also by restriction and this dimension will be more.

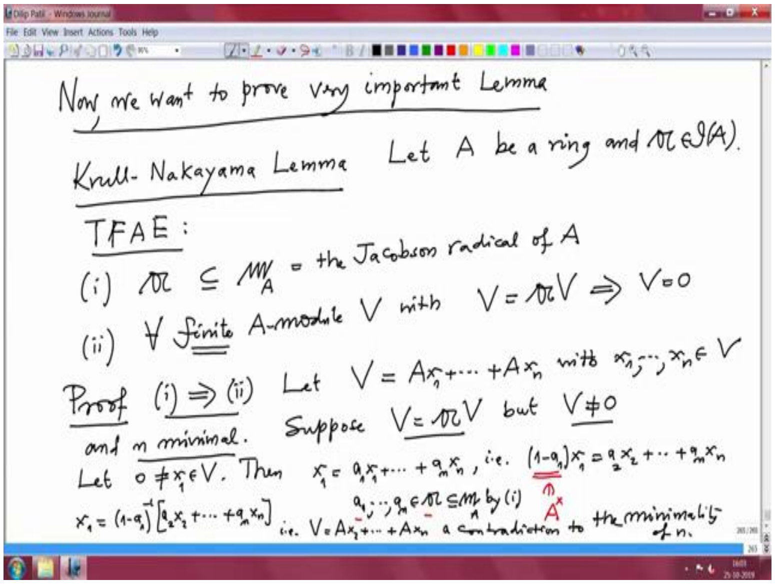
This dimension, I wrote the other way, so this dimension is more because K is a smaller field. For example, real dimension is more than the complex dimension. So, therefore these are also not big or equal to 1, so at each stage is big or equal to 1 from this and from this observation we get dimension of K over A is big or equal to the number of steps here so that is s.

So, which is what we have called cardinality of this maximal ideals of A. So, this, so and for the other assertion so this proved this one but I wanted to prove for more I wanted to prove, I did not have to prove because this cardinality is always big or equal to the cardinality of the K spectrum but also we can prove directly this, so direct proof, so another proof if you like, proof of this inequality, this directly proof of cardinality of K spectrum of A is small or equal to dimension of A.

I write another proof, so K spectrum you know that, that is also same as hom K algebras from A to K from here to Spm A, I give a map so the map, what is the map? Take any homomorphism K algebra homomorphism Psi from A to K. K algebra homomorphism and map this to kernel of Psi, kernel of Psi is a maximal ideal, so therefore it makes sense and I want to claim that this map is injective that is because how do you get back. So, since if I take K is, K times 1 A this is sub of A. So, all element this is copy of K contained in A and if I add this kernel, this, what do I get? This is the maximal ideal before any element if I add it, I get A, so this is A.

So, because of this the map is injective, because to, Psi and, Psi and Psi prime we cannot go to the same m, because if they do then this happens and therefore the map is injective and therefore we have actually proved that this cardinality is small or equal to this cardinality. So, what we have proved is not, so I have proved the fact that this cardinality is small or equal to cardinality of Spm of A. But this already we have proved one is the subset of other, so we did not have to prove that but anyway this was also interesting fact, so I mentioned it.

(Refer Slide Time: 11:30)



Now, I want to switch back to modules and generating systems and I want to study ultimately modules over a local ring and prove, and very important Lemma called Nakayama Lemma. So, let me start right away with what I want to prove. Now, we want to prove very important Lemma, this is called, actually it is called Krull Nakayama Lemma.

So, let A be a ring and a be a ideal in the ring A. Then the following are equivalent, one, a is contained in the Jacobson radical mA, this is the Jacobson radical of A. And two, for every finite A module V, remember finite means there exist a finite set of generators for V, it is finitely generated module over A with V equal to a times V that implies V is 0.

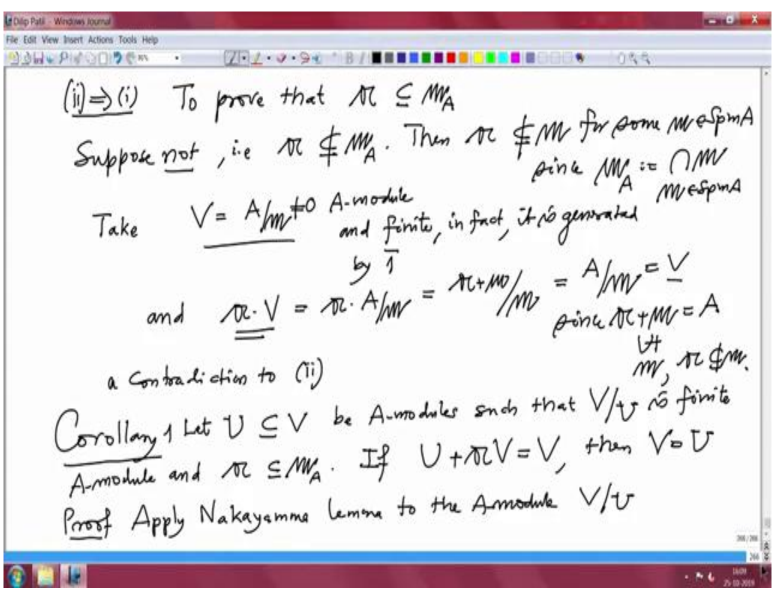
So, proof is very simple and I will deduce some consequences from this Lemma. I want to prove first one implies two. So, we have given it is a finite module, that means there is a finite generating system for V. So, let V equal to Ax1 plus plus plus plus Axn with these elements x1 to xn in V, that is a set of generators for re-finite set of generators for V. That means every element of V is finite a linear combination of x1 to xn and choose n minimal, and n minimal. That means there is no generating system for V which has lesser number of elements than V, lesser number of elements than n.

So, what does this mean? So, and I want to prove that if V equal to a V then v is 0. So, since, so suppose, V equal to a V but V is not 0 then we should get a contradiction. So, V is non-zero, so therefore there is at least one non-zero element there, so let 0 which is not equal to x be an element in V. Then this x, actually I can take that to be x1 only, see all none of these guys are 0 because n is minimal, if anyone of them is 0 then you do not need and that mean the n is not the minimal. So, x1 has to be non-zero.

And in fact all other has to be non-zero because if they, any one of them is 0 then you do not need that any generating system. So, x1 is non-zero but xn is in V and V have this equality, that means this x1 I can write a combination of x1 to xn but element, the coefficients are not only in capital A but in the ideal a. So, this I can write it as a1 x1 plus plus plus plus an xn which is same thing as saying, so that is I will rearrange this equation, I will bring this 1 minus a1 x1 on one side and the other side I will keep it the same x2 plus an xn.

But now look at this side, this element, this element because where is a1, so all the elements this when I wrote this a1 an all of them are in the ideal a and this ideal a we are assuming it is contained in the Jacobson radical by assumption 1. Therefore, this 1 minus a1 is actually unit in the ring A because this a1 is in A, therefore this is unit and therefore I can multiply this equation by inverse of that and then we get x1 equal to 1 minus a1 inverse a2 x2 etcetera, etcetera an xn. That means this generating element I can write in terms of the others. So, that means we have proved that V is generated by x2 up to xn, but this contradicts the minimality of n, a contradiction to the minimality of n. So, that proves one implies two.

(Refer Slide Time: 18:03)



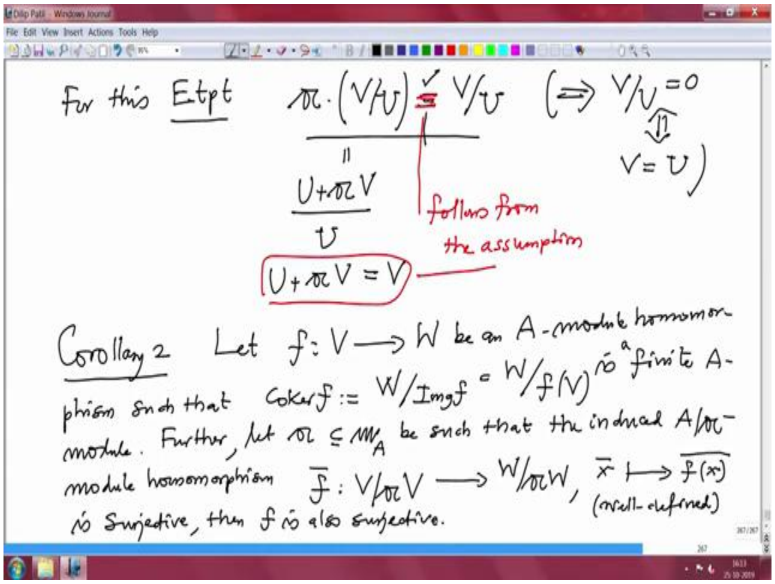
Now, let us move two implies one. Two implies one. So, what do I have given, so I want to prove that one is, so to prove that a is contained in the Jacobson radical. So, suppose not, that is a is not contained in the Jacobson radical then I want to contradict two. That means I want to produce a module which is a finite module where V equal to this ideal a times V but V is non-zero. So, if this is not contained then a will not be contained in at least one of them maximal ideals, for some m in Spm A. Because if a is contained in all of them then a will be contained in the Jacobson radical because since mA is by definition intersection m, m belong to Spm A.

So, therefore it is not contained in that maximal ideal and now take, V equal to A by m, this is obviously an A module and finite also in fact, it is generated by 1 bar which is the image of 1 under the residue map. So, it is actually a cyclic module and what is this is obviously non-zero because maximal ideal never a unit ideal and what is now a times V, this is a times A by m and a is not contained in m.

Therefore, this is, so this is precisely a plus m, module m. But a plus m is because a is not contained in m, this has to be the whole ring because this is m is maximal and this is something which is not contained there. Therefore, this is A by m since a plus m is the whole ring A because this contains properly m, this is because A is not contained in m therefore and this is V.

Therefore, I have checked that a V equal to V but we know V is non-zero, so a contradiction, contradiction to two. So, that proves two implies one also. So, some corollaries I will deduce, corollary one, so suppose U is contained in V be A modules, let this be A modules such that the residue class module V by U is finite. V may not be finite but V by U is finite, finite mean finitely generated, finite A module and suppose A is an ideal which is contained in the Jacobson radical of A if U plus a V equal to V then V equal to U. Proof, apply Nakayama Lemma to the module, to the A module V by U. I want to show this is 0, this is 0 equal to saying that this equality. So, to show that it is 0, I will check the condition, second condition there which is so enough for this.

(Refer Slide Time: 23:13)

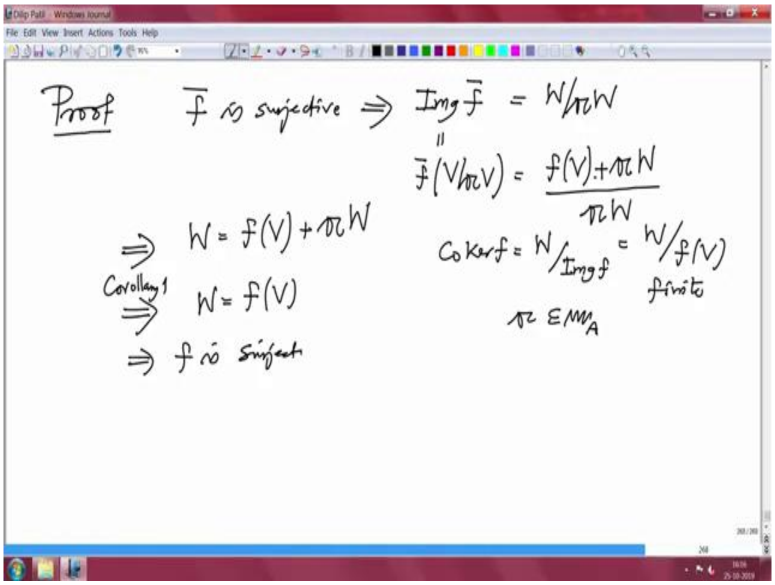


For this enough to proof that a times V by U is same thing as V by U and then that will imply by Nakayama Lemma V by U is 0 and that is equivalent to saying V equal to U. So, how do we check this? So, this is because how do you write this question. So, this is same thing as because this a times V may not contain U. So, the numerator will be now U plus a V modulo V. And these two modules are equal, now this is contained here, this contains U, this contains U and therefore by correspondence theorem, by correspondence theorem on sub modules, so I will not write more.

We get, already implies I have written, so this by correspondence theorem, the numerators are equal, so U plus a V equal to V, that is what we have given. So, therefore this equality. So, because of this I should correct myself, not because of the correspondence theorem, this equality, this equality follows from the assumption this. This is assumption, therefore I have therefore this equality and therefore by Nakayama Lemma then I can conclude V by a is, V by U is 0 that is equivalent to saying V is equal to U. So, that proves the corollary. So, corollary two, let f from V to W be an A module homomorphism such that co-kernel of f, which is by definition V mod W, modulo the image of f, that is W modulo f of V is finite, that means it is finite A module that is given.

Further, let this is a be an ideal contained in the Jacobson radical of A be such that the induce A by a module homomorphism f bar from V by a V to W by a W. So, what is this defined by? This is x bar going to f of x and then bar and then note that this should be well defined, this is well defined, this is the induced homomorphism from this f, this is A by, both are A by a modules such that, so we have assumption that a is contained in the Jacobson radical and this induce homomorphism is surjective, then f is already surjective, f is also surjective.

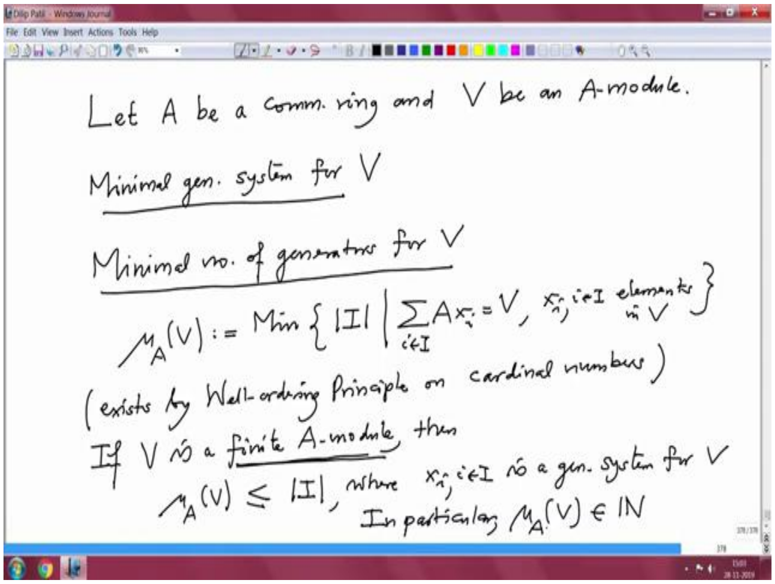
(Refer Slide Time: 28:01)



So, we will write down the proof and we will use, we will have to use Nakayama Lemma in the proof. So, proof, so f bar is surjective that is given. So, therefore image of f bar is equal to W by aW. On the other hand, this image of f bar is precisely by definition is f bar of the whole V by a, V by a V but this is same thing as f V plus a times V, not these are in W, so a times W, modulo a W. See, this I have to write this because this f V may not contain aW. Therefore, we have to always write, if you want to write the sub module of the quotient module then it is of this form.

So, these are equal, therefore the numerators are equal, so therefore W equal to f v plus aW but then because a is contained in the Jacobson radical by and this is co-kernel is co-kernel f is by definition W modulo the image of g, image of f which is W by f of V. So, this is finite, finite that is given and a is contained in the Jacobson radical given, therefore by earlier corollary, this what do you conclude? You conclude W equal to f V. This is U and this is, and I am applying to this sub module of W, so this is by corollary one. So, this, but what does this mean? This means f is surjective.

(Refer Slide Time: 30:41)

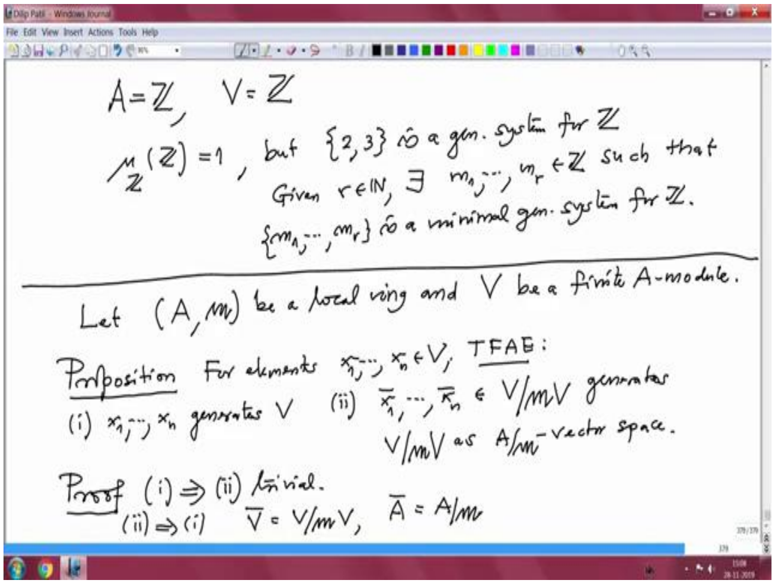


So, we will apply a Nakayama Lemma to say something about minimal number of generators for a module over a commutative ring. So, let us recall, so as usual our notation is let, A be a commutative ring and V be an A module. Then we have defined earlier what is a minimal generating system for V. That is a generating system for V from where we cannot drop any element of that system, that means no proper sub set of that generating system should generate V, such a system is called minimal generating system for V.

That we have used this term earlier also and now this is the minimal number of generators for V, that means among all the system of generators you take all system of generators and take their number, number in that and that is you take the minimum amount. So, therefore what I am saying is put mu AV by definition Min of all the cardinalities such that V should be generated by this system xi, where this xi's they are elements of V. And note that this cardinal, this minimum exist I will just note here this exists by well-ordering principle on cardinal numbers.

This case occurs when your module is not finite over A, then only the problem comes. So, for us if V is a finite A module then mu AV is always bounded by the cardinality of any generating system. So, cardinality I where xi i in I is a generating system for V, that is clear because you have taken the minimum over this. So, this is, so in case where V is a finite A module this number is always a finite number. This is an integer; this is a natural number. So, in particular, in this case mu AV is a natural number in this case of course V is a finite module. And now I want to compute this number precisely when A is a local ring and V is the finite module.

(Refer Slide Time: 35:08)



So, before I do that just to get a little feeling what you observe that this, for example if you take a ring, base ring to be Z and V is also Z, then we know that mu Z Z is 1, because 1 is a generating system and Z has to need at least 1 generator. So, this is 1 is clear but also note that if I look at the set 2, comma 3 this is a generating system for Z.

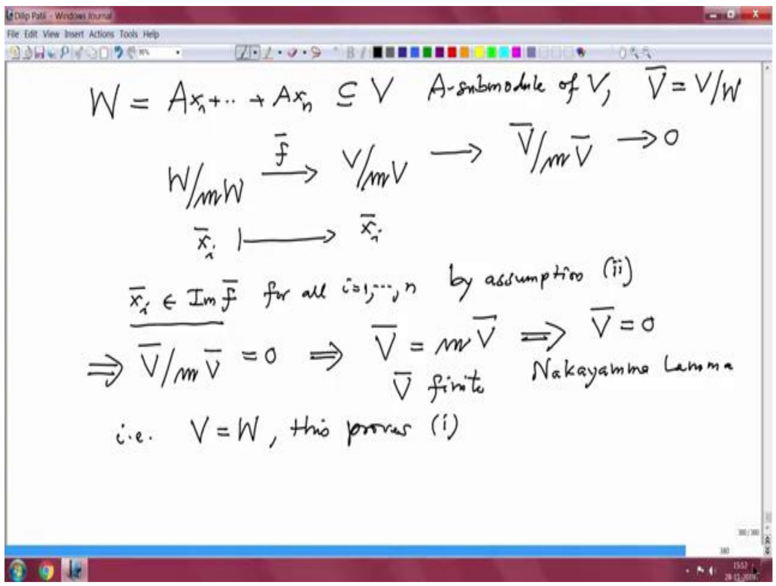
So, it has two elements, so the above inequality is crude. Because I said that mu Z, Z is less equal to 2. If I would have taken some other generating system in fact in this case, you can find out given any natural number r there exist m1 to mr integers such that, m1 to mr is a minimal generating system for Z.

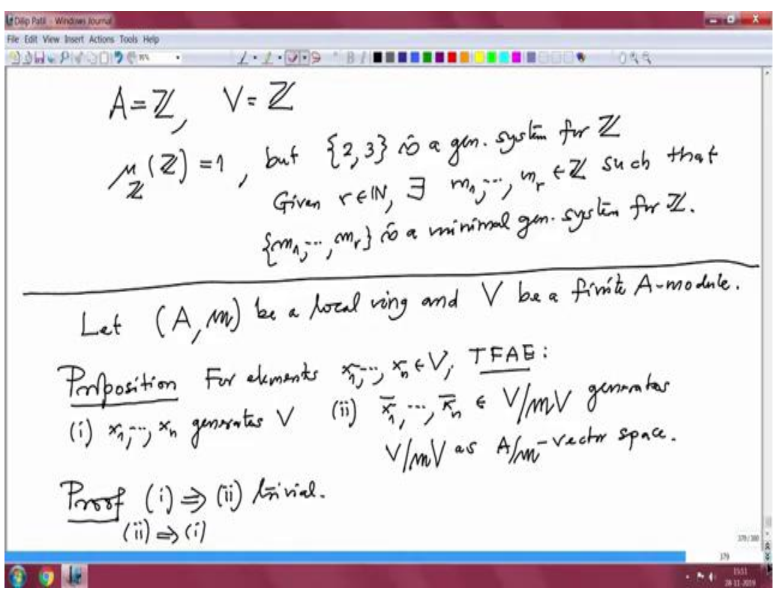
So that is very, this is very probably one has to be with an exercise, so but now I want to be little bit more specific and therefore these examples also show that we have to put some condition on the ring, then only we are going to get better result. So, our assumption now is let A, comma m be a local ring and V be a finite A module.

Then first I want to prove this proposition which will be a consequence of Lemma of Nakayama which I had proved in this lecture earlier, so which says that, so given, so we have this assumption. So, for elements x1 to xn in V, the following are equivalent, the following are equivalent.

So, one, x1 to xn generates V and two, x1 bar, xn bar where these are the images of x1 to xn in the residue class module V by mV, this generates V modulo mV as A by m vector space. So, if you want to check some system generates V, we have to check that the modulo m times V degenerate. So, let us see the proof, proof is really very simple. So, first of all one implies two is trivial, conversely two implies one we need to prove. For two implies one let us put V bar equal to V by mV and let us also put A bar is this A by m. These are the residue class structures.

(Refer Slide Time: 39:50)



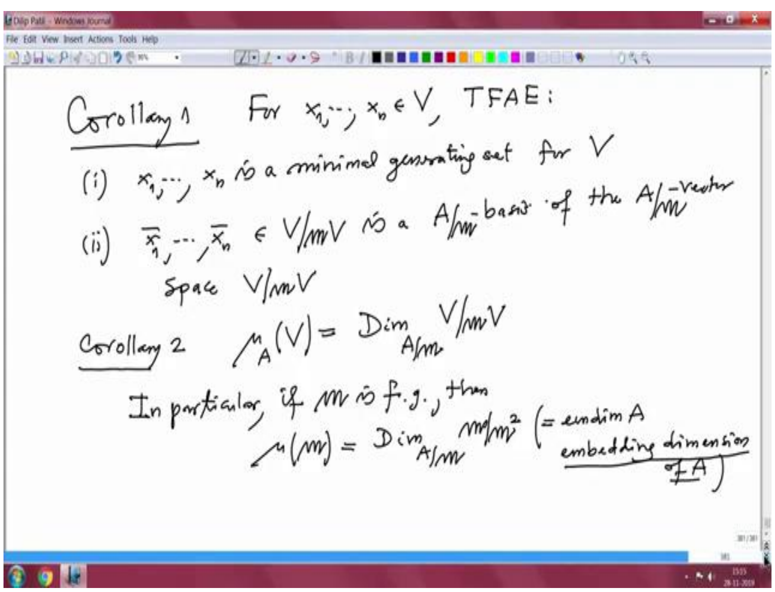


Now, what we have given, we also look at the map and W, let us put W is a submodule of V generated by this x1 to xn, this is a submodule, A submodule of V. And now we will look at the exact sequence W by mW to V by mW and to the mod now, this mod this. So, that will be precisely V bar by m V bar to 0. This is the exact sequence and this map is what? What is this map? This is of course, this is the co-kernel of this map and this map is, this is f bar, this map only I only have to prove, send where xi goes, xi bar that goes to xi bar.

So, that means image of xi mod mW that goes to image of the same xi mod this, this is the map and the fact that this module is generated by xi bar that is given to us by two, so that will simply mean that this xi bar belongs to the image of f bar for all i from 1 to n. That is because by two, by assumption two. That mean this f bar is already surjective, so therefore this has to be 0. So, that implies V bar by mV bar is 0 but this V bar is a finite module, so this means V bar is finite and this equality holds.

But we are over a local ring, V bar is finitely generated, V bar is finite and local so that will imply by Nakayama Lemma V bar is 0. This is by Nakayama Lemma, but V bar is 0 means what? So, that is V equal to W, maybe I have made an, I will just want to check that, I think I want to this definition, so I want to erase this. So, V bar is V by W, so note that this sequence is exact where this map f bar is given by just image of xi goes to the image of xi in appropriate residue class module and then that proves this is 0. So, that means V, so this is, that is, this proves one. So, that proves the equivalence of one and two. But I want to write important consequences of this which are very, very important and often used so it is better to record them.

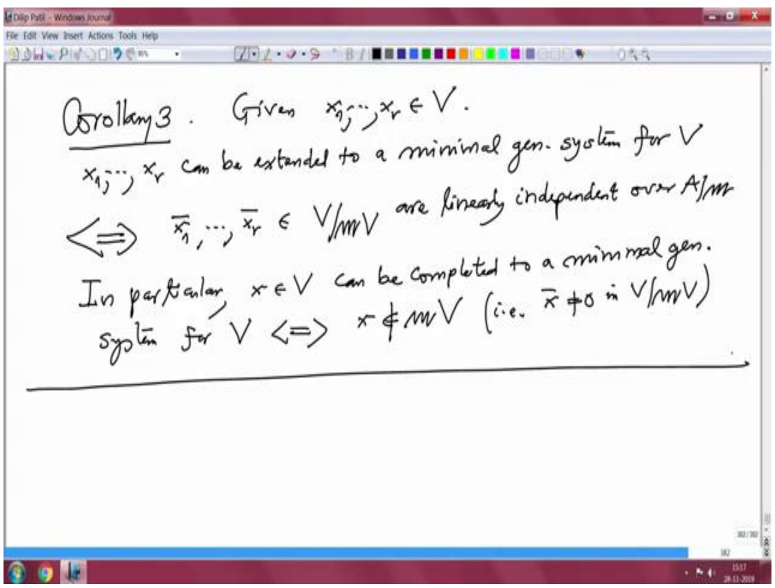
(Refer Slide Time: 43:40)



So, corollary 1, for elements x1 to xn in the module V as earlier notation V is finite and ring is local, the following are equivalent. One, x1 to xn is a minimal generating set for V. And two, x1 bar xn bar, these are elements in V by mV, images of x1 to xn modulo m times V is a A by m basis of the A by m vector space V by mV. So, this is obvious from the earlier one, so let me write another corollary. Corollary two, mu times, the minimal number of generators for V is precisely the dimension of the vector space V by mV as a A by m vector space.

This is what we proved in the earlier corollary. In particular, if m the ideal is finitely generated then the minimal number of generators for the maximal ideal of the ring A is dimension of the vector space A by m m by m square. This is also called embedding dimension of the ring, embedding dimension of the ring A, this is the notation, this is the term is for this. So, that was corollary two, one more and then we will stop.

(Refer Slide Time: 46:28)



Corollary 3, so given r elements in finite module over a local ring as the same notation. They can be extended to minimal generating set, so the statement is x1 to xr can be extended to a minimal generating system for V if and only if the residue classes x1 bar xr bar in v by mV are linearly independent over A by m over the residue field of the local ring. So, this is also immediately follows from the earlier one, in particular if you have one element x in V that can be extended or can be completed to a minimal generating system for V if and only if this x should not be 0 in modulo V by mV.

So, that means this x should not be in m times V because this is equivalent to saying that is x bar is not 0 in the vector space V by mV and then we know if you have a non-zero vector in a vector space that you can always complete it to a basis. So, that proves, so with this I will stop this and from the next lecture onwards I will prepare for proving a very important connection between commutative algebra and algebraic geometry, namely Hilbert's Nullstellensatz. So, thank you very much, we will continue in the next week. Thank you.