Lecture – 53

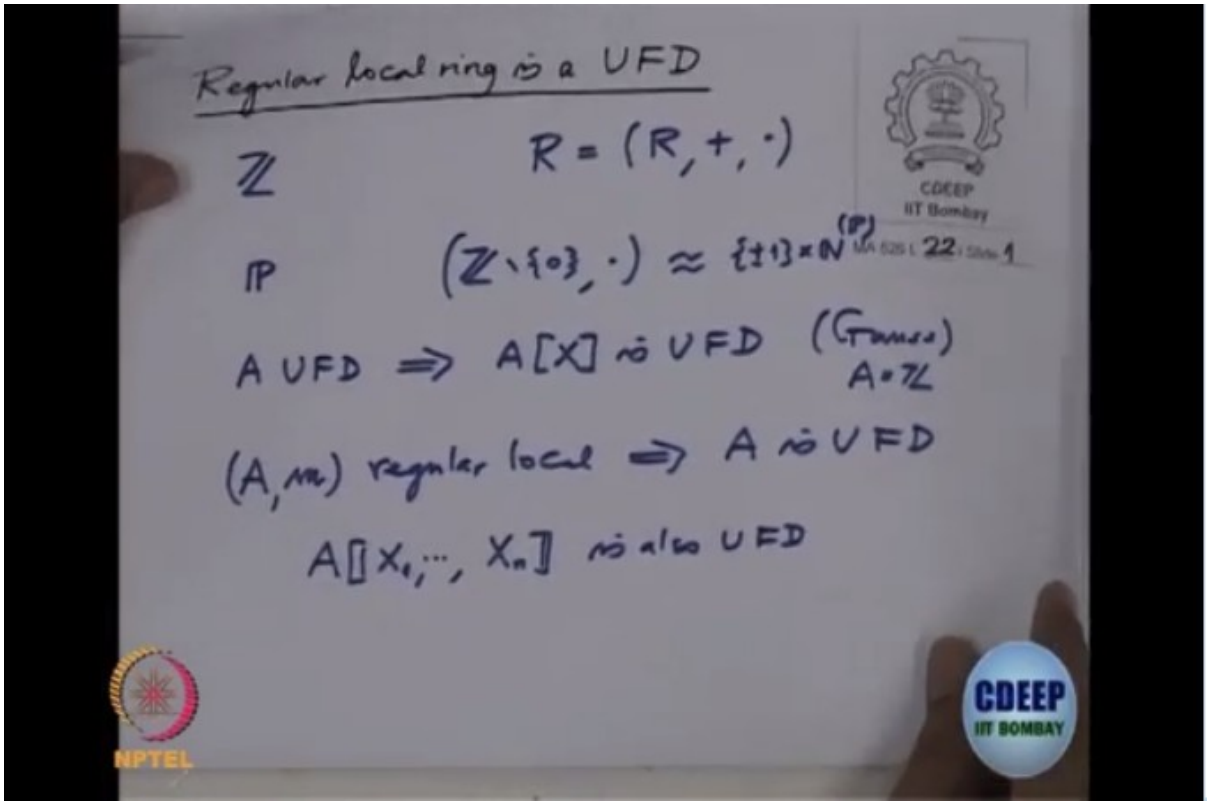
Regular Local Rings are UFD

GnanamParamamDhyeyam. Knowledge is supreme.

Good afternoon. We continue our study of regular local rings. And today I will prove that regular local rings are UFD's. This is a good application of the last theorem we proved that regular local rings can be characterized through the finiteness if the global dimension. I will assume that your familiar with UFD's, except I will recall some results which you have already proved and with some motivation. So the first ring which is a UFD's ring of integers. And this is actually proved the time of Euclid now and I guess the motivation was-- basically two motivations. One is, of course, the need or solving the Diophantine equations. Right. So, for example, solving Fermat's last theorem was also one of the problem in the solution, et cetera. And it would have been very convenient if we have a prime decomposition. Then if we have two prime decomposition, then you can compare and say the exponents are equal and so on. So that was very important and also this actually gives you a description of a multiplicative monoid. See, if you have a ring R, ring R as a structure, it's a set with two binary operations plus and dot. Right. And with respective plus it is an abelian group, so cancelation, et cetera happens and everything is neatly as like the equations also solutions and so on. With respect to the product, when it is an integral domain then I can remove zero and then it's still a monoid. It's a multiplicate to monoid. And what would like to understand this multiplicate to monoid in terms of the additive monoid. So for example, for $\mathbb{Z}$, if you look at set of prime numbers then give with the multiplicative monoid of $\mathbb{Z}$ which is $\left(\mathbb{Z} \setminus \{0\}, .\right)$. This can be described, this is a free monoid on this P basis. So this is isomorphic too.We can write down it is the sign which is plus minus one group under multiplication and cross N power this round bracket P. So this gives a good description for the multiplicative monoid. If we want to understand a ring better, you like to understand multiplicative mono orbit. And this understand is done with the UFD property.

So these are done by Euclid time and then the Gause proved this again and also noted that generally if I have a UFD, A is a UFD, then the polynomial ring over that is also UFD. These are gauss. Gauss actually proved it for A equal $\mathbb{Z}$. And therefore for finitely mini variables we can repeat this argument and we can create for the finitely mini variables. However for a power series ring it is not proved this way.Power series ring this is little bit more tedious. And in generally it is not truth. If you have a in generally UFD then the power series ring over a UFD may not be UFD. So this is strange, normally for power series ring the results are better but in this particular thing the result is not so good. Okay, so, with this now we will assume today A is our regular local ring.And we want to prove that A is a UFD. In particular, ifI take this polynomial, if I take a power series ring over a regular local ring. A power series $X_1, \ldots, X_n$ and finitely mini variables, this is also UFD. If R is a regular local, r is not a UFD, it's more than that. See, in general this false UFD's.So this will follow because if R is regular local then the power series ring over that is also regular local.

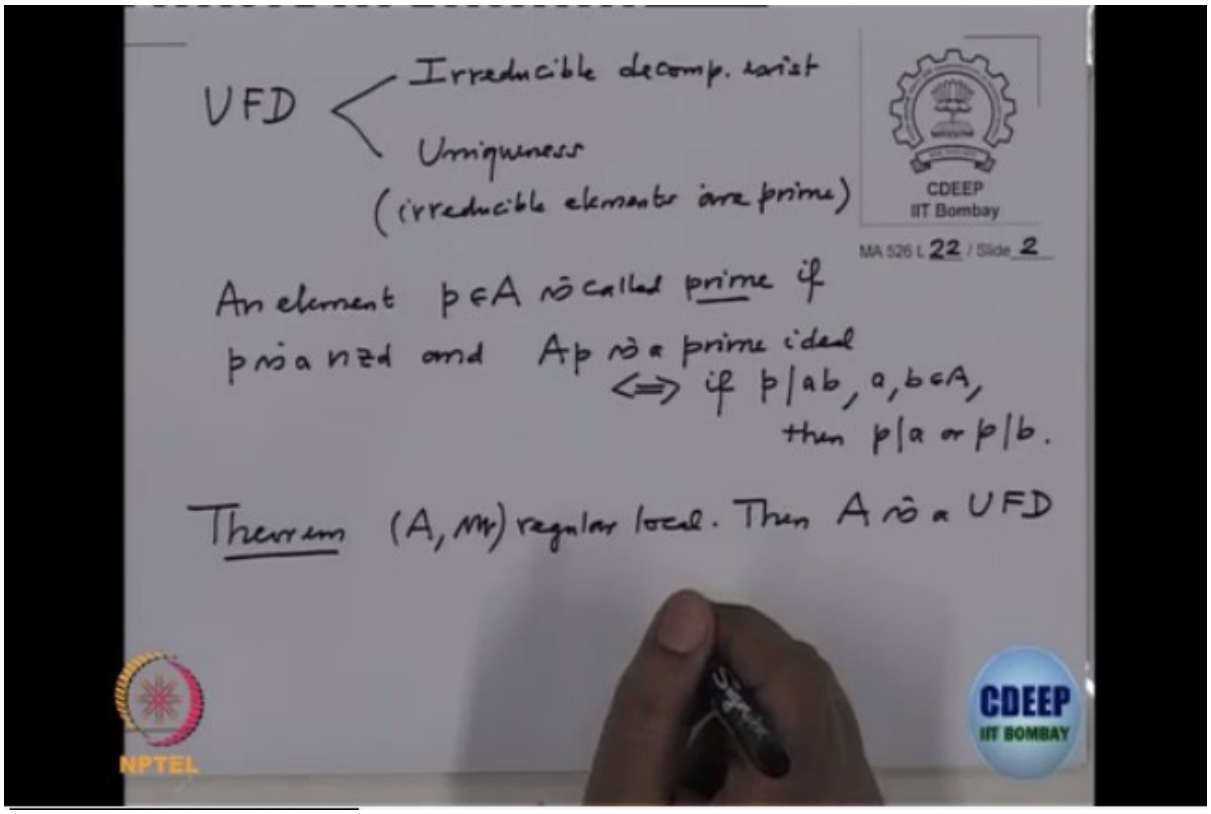
(Refer Slide Time: 06:13)



Okay, so, you will be use this the homological dimension of any module over A is either final finite homological dimension. This is what the main ingredient. Oaky, so, we have notice that regular local rings by definition. They're Neotherian. So, to prove UFD, we have to prove two things. Irreducible decomposition exist. That means every element, every nonzero, every non-zero is a product of irreducible elements. And second part is uniqueness. That means we have two irreducible decomposition, then up to a permutation, up to a unit they're equal. So, because the ring is Noetherianfor every element have the irreducible decomposition is clear because sending chain of ideals become stationary. And divisibility can be rewritten in terms of the ideal in ascending chain.So irreducible decomposition exist, this is immediate from the Noetherianess. So we have to prove the uniqueness. And uniqueness is well proved by proving irreducible elements are prime elements. So this is usually proved by proving irreducible elements and prime elements. They are equivalent in this set up or R'. So, we will also be concentrating proving that the irreducible elements are prime or which is equivalent to saying again that every height one prime ideals are principle. So because if you have a high-- if we have a prime ideal,then it will have an element in that and that non unit you can [express in a way] irreducible decomposition and therefore because aideal is prime it will contain one of the element. And because height is one ,it has to be equal. And that will be therefore generator will be a prime elements and that's how the proof is go. So therefore we have to concentrate on proving every height one prime ideal in a regular local ring principle. So that is a main step. Okay, now, before I gone, I just want to also recall you what is the definition of a prime element in general in a ring. So, an element p in the ring A, general, not in a domain is called prime. If first of all p has to be non-zero deviser. Normally, when assumes when you talk about this concept when I assumes were in integral domain but you may not in generally you not be an integral domain in that case. And element is called prime. If p a nonzero divisor and ideal generated by p is a prime ideal or equivalently if p divides ab, a b are element in A then $p \vee a$ or $p \vee b$. So,the theorem actually we will prove is -- this is the theorem will prove, (A, m) regular local then A is a UFD. As you will see this proof is also

difficult now because the major work has gone into the earlier theorem. Then homological characterization of the regular local ring.

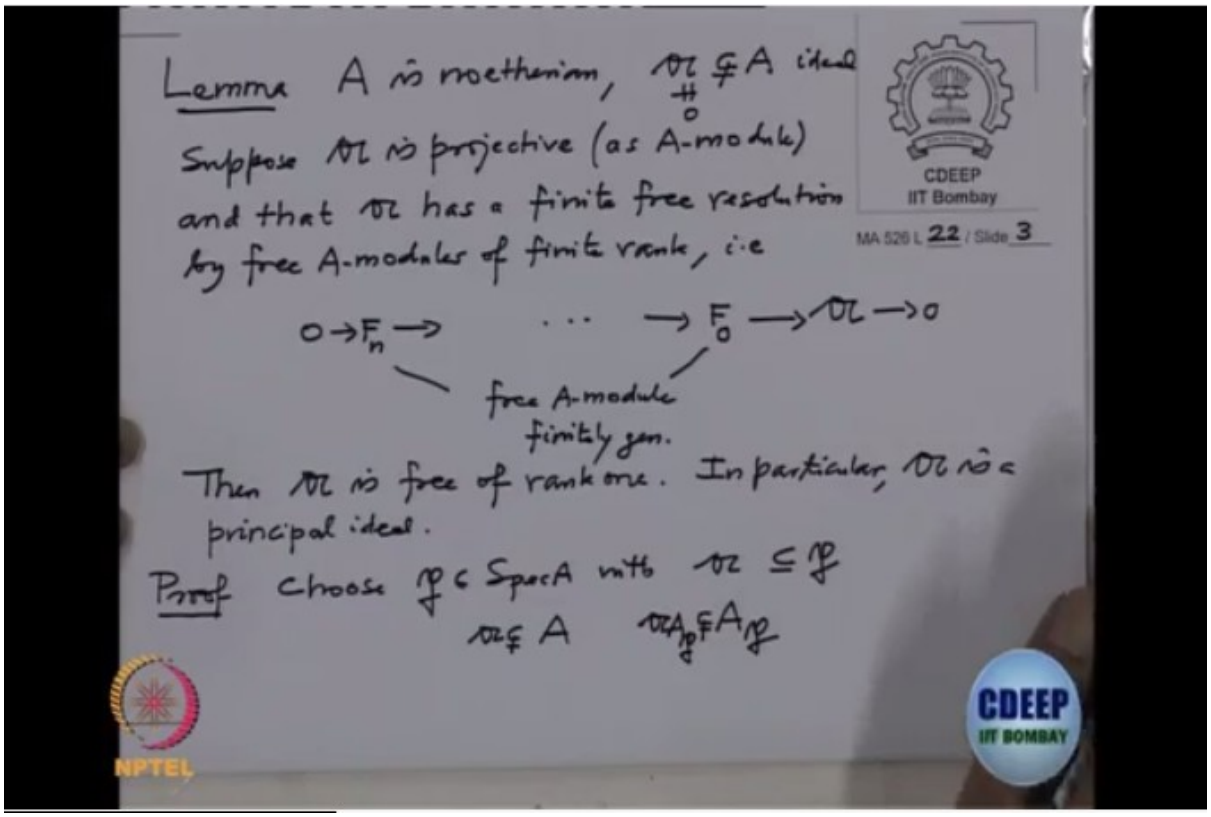
(Refer Slide Time: 11:00)



Okay, so, first let just note the Lemma,which I've used and this Lemma is valid for not necessary local ring. It is valid for any Noetherianring. So, I will state in that generality, so Lemma, A is Noetherianand A, is an ideal, nonzero ideal. Suppose,A is projective of A-modale, and thatA has a finite free resolutionby free modules of finite rank. This means, so that is let us fill out what does it means, this means you have an ideal A here, we can have resolution like this. Finite, finite length,the resolution and all these modules are free. A-modulesor finite rank. That mean, they're finitely generated free modules. They have the basis of finite cardinalities that is what given. Then-- the conclusion is then the ideal A is free of rank one.In particular, A is principle. Proof is very simple. Let's finish off the proof. I want to show it is free of rank one, and what is given? So, let A is a nonzero ideal and also if A is equal to a, there's nothing to prove. So we might as well assume A is a proper ideal. So then I can always find a prime ideal, choose a prime ideal, choose P' with A is contained in p. It's a proper ideal, it's containing some maximal ideals, in particular prime ideal. Once it is contain there and then when I localize, now from the ring A,I go to the localization, A localize at P. We had an ideal A here, proper ideal. Now you get aideal A, A localize at P. This will also be proper ideal. Because A is contain in P. and now what we had given was A is a projective module. So

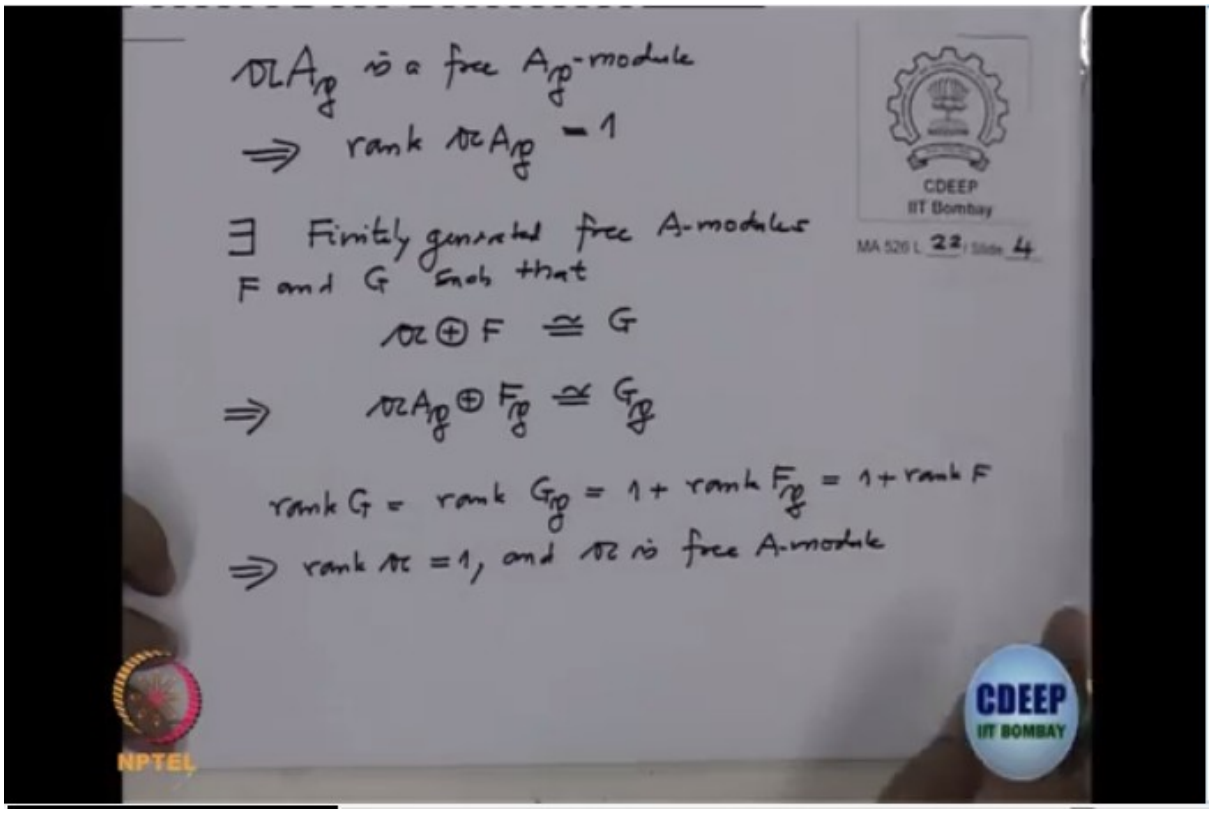
locally it is free, projective modules or local rings are free. So in particular this A localize at A P is a free…

(Refer Slide Time: 15:05)



So,A this module, this ideal is a free, A localize at P module. But this is an ideal in the local ring which is free. Therefore,it actually haverank one, because any two elements in ideal they will be linearly dependent. Therefore, if the rank is more than one it will have basis consisting of more than one element, but that is not possible because any subset which has more than one cardinality has to be lineally dependent. So therefore, rank of this module has to be one. Okay.And what is that we want to prove? We wanted to prove that A is free of rank one, but locally we proved A is free of rank one. Okay, and we have a finite free resolution.So that will tell you there exist finitely generated free A modules F and G such that A directs some F is isomorphic to G. This you've prove it by induction on the length of the free resolution we're given, because the module is projective, therefore,you can add something so that it become free, but you can the other component may not be free but you can add more and then make it free. So therefore you keep doing this. So, by adding a free module you will get a free module. But when you localize this, the localization come within the direct sum et cetera. So, A this direct sum F localize at P is isomorphic to G localize at P, therefore, rank of G which will be rank of the localization. So write down, the rank of G which is rank of G localize at P,which is from here, this is rank one, this is whatever rank. So, this is one plus rank of F F which is one plus rank of F. So, therefore, A has to be up rank one. So that implies a rank of A is one. And it is-- once it is rank one and it is free. And once it is freeit is principle. And the delay is free.

(Refer Slide Time: 19:06)



Okay, this is I will use it, I may not be use in the generality, I mean, you may use it in a even with more special case of this Lemma which will be even more easier than proving what we have proved it down. Now, we will start with regular local ring.They are assuming it is regular. And as we saw enough to prove that,if we have prime module P height of P is one, then P is principle. And this I am going to do it by induction on the ring, dimension of the ring.We will prove this by induction on d equal to dimension A. We know dimension A finite because A is a local ring. So,let us for d equal to one-- we have a regular local ring of dimension d, therefore this d is also same as minimal number of generators for the maximum ideal,which is the dimension of the vector space $\frac{m}{m^2}$, which is also called embedding dimension of A. Suppose d is zerothat means what? That means this vector space is zero dimensional vector space. That means it's a zero vector space. So then $\frac{m}{m^2}$ is zero, which means m equal to m^2. But that means m is zero by Nakayama's Lemma. But,once the maximum ideal is zero, you are in local ring, therefore, actually A is a field, is a field and they know prime ideal, they're nothing to prove. Okay, so, I assume now dimension is act least one and let P be a prime ideal height p equal to one. Height P definitely contains zero, zero is a prime ideal because regular local rings are domains. So, this is not. And because this is local ring, this P is containing the maximum ideal m. So, if and also we know that a d is act least one,so m cannot be m^2.

Because this d the dimension of this $\frac{m}{m^2}$, so it cannot be zero at a space. So, definitely I can choose, so choose $T \in m \setminus m^2$. And we have seen that when I to more t now $\frac{A}{AT}$, this ring is again regular. Because we have gone modular part of a regular system of parameters. So, this T can always extended to a generating set for m, because it's a non-zero element in vector space always can always be extended to a basic. So this $T\left[X_1, \ldots, X_d \right]$, this is a minimal set of generators for m. And it's about irregular local ring again. Alright. So, therefore in particular is AT is a prime ideal? Because this is a regular local ring, it's a integral domain, therefore AT will generate a prime ideal. This is a prime ideal in A. And therefore it cannot be containing-- if it is containing P, then P has to be equal to height P is one. So, if AT is containing P then PA to AT is principle. And we are finished your proof to prove that P is principle.

So, we may assume T is not in P. okay, we have assume T is not in P therefore if I take this multiplicative set S generated by T that is one T, T square et cetera. This multiplicand is said will not interested with P. so S intersection P is empty, therefore when I go from A to S inverse A this P here will survive here. What do I call that, okay, I just called it S inverse P. this will not be equal to S inverse A. let's called this ring as B, so this P will be a-- this is a image of P, this is a prime ideal in B, okay, so instead of writing I will write B and this one therefore P B. so we are in this situation like this now, A was our original regular local ring. We have localized that at this multiplicative set, and remember that this may not be local now, but what we know is if we have a prime ideal here that remains prime here. Okay, and now if I want to prove P is-- okay. Our aim is to prove P is principle, remember that. Okay. So I will prove this in three steps. So, how will I prove it? I will prove it like that. Step one, I will first prove that this ideal PB is a projective B module. Alright.So, to prove somebody that projective B module, it's enough to prove that it is locally free. It's a finitely generated. Or it's enough to prove that it's locally free. So enough to prove that PB is locally free.That is I have to prove that if I localize this at any prime ideal of B it is free. So that is I have to prove that PB and localize at P this is free BP module for every prime ideal P of B. but we know the prime ideal structure of this B, they are coming from A, those who don't intersect with S. so, therefore, this P look like $P^{'}B$ where $P^{'}$, this is a prime ideal of A and don't intersect with this with $P^{'}$ intersection S is empty. Here now, all prime ideals of this B, they are coming from the prime ideals of A who don't intersects with this. So I've taken P, I have written prime ideal of B which will be $P^{'}$, where $P^{'}$ is actually prime ideal in A which don't intersect with S. But such a $P^{'}$ cannot contain T, note that. T cannot be contain in prime because $P^{'}$ don't intersect with S and as it is generated by T. So $P^{'}$ cannot be in-- T cannot be $P^{'}$. So, $P^{'}$ cannot be M because M contains T. So, once, so, therefore, $P^{'}$ is a prime ideal of A which is not the maximal id. That means that dimension of A localize at $P^{'}$, this will be strictly less than dimension of A. which is D. This is height of $P^{'}$ and height of $P^{'}$ cannot be full dimension. Height of D is height of M. And remember we have proved that if A is regular local then all localizations are regular local. So, therefore, a localize at $P^{'}$ is again regular local, this is by the corollary to the earlier theorem that global dimension is finite. This you cannot directly prove from the definition of, okay. So, and what is it? And this P, p small p A localize at $P^{'}$, this is capital, this is what we wanted to prove it is principle, right. Our aim was to prove that P is principle. But when I prove that P is principle, I'm proving it as a localization, it is principle. So therefore, this is principle by induction. No, I don't even want to note that. So, you look at this prime ideal this is same as P B localize at P. so here B was S inverse of A and this $P^{'}$ don't intersect with this and so whether you

localize at B localize at P and A localize at P' they are same. See because this P' is a… see you remember this capital P was P' B. so when I localize, further localization that is same as this. So this prime ideal is same as this. So, therefore, this is principle by induction, so, P A localize at P' is principle by induction on D. because this dimension are drop. Since dimension of A localize at P' is strictly smaller than D. once it is principle if is free and hence free. And hence P A localize at P' is free. But then this is free. And that is we wanted to prove, we wanted to prove it is locally free. So, the-- what we proved is, therefore we've concluded that if I take this P and extended to B this is a projective model. This is want we wanted to prove it step one.

(Refer Slide Time:33:26)