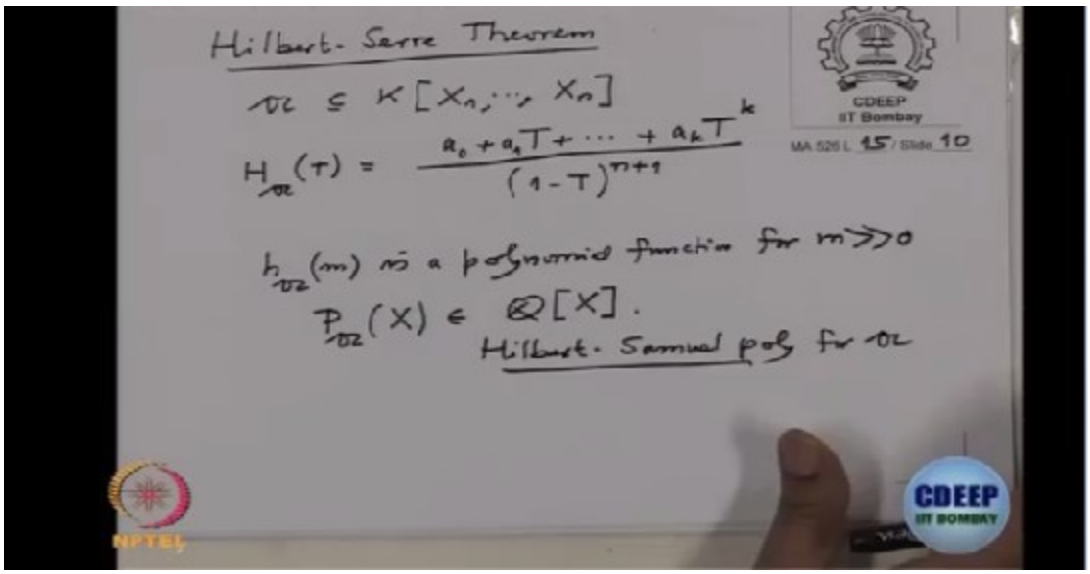
Lecture – 40

Hilbert-Serre Theorem

GyanamParamamDhyeyam: Knowledge is supreme.

This is the theorem that we proved also earlier, the same proof here also, Hilbert-Serre theorem. That say that this for any ideal A in the polynomial ring, this Hilbert-Serre is a rational function, the denominator is $(1-T)^{n+1}$, and up is the polynomial is integer coefficients $a_k T^k$. And therefore h a is m either polynomial function for large m. And that polynomial will denotes by p suffix a and this is the polynomial in with rational coefficients. This polynomial called Hilbert polynomial or Hilbert Samuel polynomial for a.

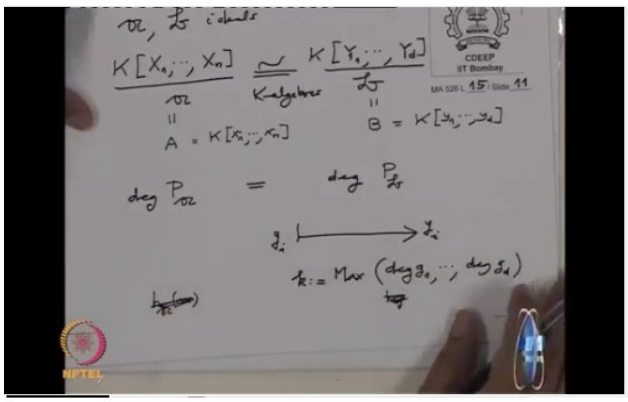
(Refer Slide Time: 01:54)



Alright. Now, the most important fact, this is only observations and recalled all these things. So suppose now, I have two ideals A and B, such that this two algebra that isomorphic $\frac{K[X_1,\ldots,X_n]}{a}$ and $\frac{K[Y_1,\ldots,Y_d]}{b}$. Suppose these are isomorphic K-algebras. This is then we are denoting by A, this is we're denoting by B and this $K[y_1,\ldots,y_d]$ and this was $K[x_1,\ldots,x_n]$. And then what we need to prove is P, the polynomial, P_a we've associated polynomial P_a here, here P_b and then we've seen in earlier example that they are not same polynomials. But we want to prove that they're the same degree, so degree of this equal to degree of

this. This is what we need to prove. So, we have is isomorphism, that mean this small y they're coming from some polynomial, right. Therefore, let us called the small y_i , they're coming from from g_i. And let us take these are gis are polynomials. So let us look at their degrees. Degree of g_1 , degree of g_d . and let us take their maximum. Call it K. Then what do we want to check? Actually how are you going to check these two polynomials have the same degree. What one will prove is, this is polynomial for large n, this polynomial for large m. And so we have to look at $h_a(m)$ and h_b at somebody so let me use the next page.

(Refer Slide Time: 04:30)

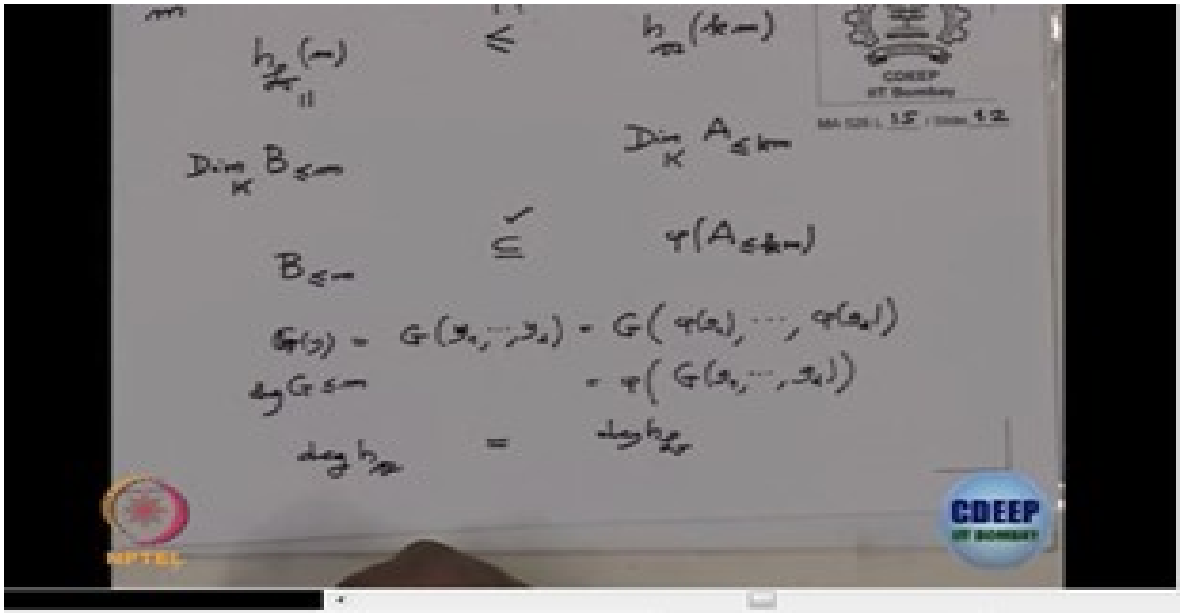


So, let us take any m and I want to now prove direct the relation between $h_b(m)$ and h_a of this k is a fix coefficient here km. I want to find the relation between these two numbers. And I will prove this is less equal to. So for large m and again interchange the roles. So one will be less than other and that will be the equality on the degree. So how do approve this? So what was this? So this is what I'm trying to prove. So what is this by definition? This is by definition, what involved is $B_{\leq m}$. This is a dimension of $B_{\leq m}$. That was the definition. If you remember when B is the finite type algebra generated by y_1 to y_d, $B_{\leq m}$ means,

you take all polynomials in y's of degree up m and you collect them. So that was you elute them at small y and collect them.

So this was the definition, and here it was dimension of K over K, $A_{\leqslant km}$, these are the definition. And I want to prove this. So I should be proving that-- so it enough to prove that these vector space $B_{\leqslant m}$ is a subspace of $\phi(A_{\leqslant km})$. So if ϕ isomorphism that was ϕ. These are isomorphism is ϕ. So whenever I have somebody here I just pushed there. And that's an isomorphism. So if I prove that this is a subspace of this then this dimension will be less equal to these dimension but because ϕ is an isomorphism, this dimension will be equal to this dimension. So I've only prove that this is contained here, right. This image of this is, it's containing B, so that contains this subspace. So if I've prove that then we are done. So what do we have to prove? That means, if I've any element here, any element will look like what, any element will like h of y, or maybe I should use some another letter. $G(y)$, where G is a polynomial of degree less equal to m Then we have eluted at y means, we have read the image of G in B. So this polynomial and-- so this is same as G y, yd but this $y_1,\ldots,y_d$ they're coming from the g's, small g's. Right. So this is same as $G(y_1)$ is coming as ϕ image of g_1. So that is $\phi(g_1),\ldots,\phi(g_d)$, correct? Because you remember this we have lifted this y's, this y we've lifted here. So y_1 is coming from g_1 under ϕ. So therefore, this is correct. But now this ϕ is an algebra homomorphisms. So I can take ϕ outside. So this is same as $\phi(G(g_1,\ldots,g_d))$. So here is the polynomial of degree less equal to m and in that the variable we've substituted at $g_1,\ldots,g_d$ and $g_1,\ldots,g_d$ are polynomials of some degrees and k is the maximum. So, these polynomial cannot have degree more than k times that original, so that it is. So that proves this increase it. So therefore we're done. So all together we have done that-- what we have proved is degree of h_a and degree of h_b , they're same. So we have proved that this degree doesn't depend on a algebra generating said for the finite tape algebra. Okay. The next is now we're almost done.

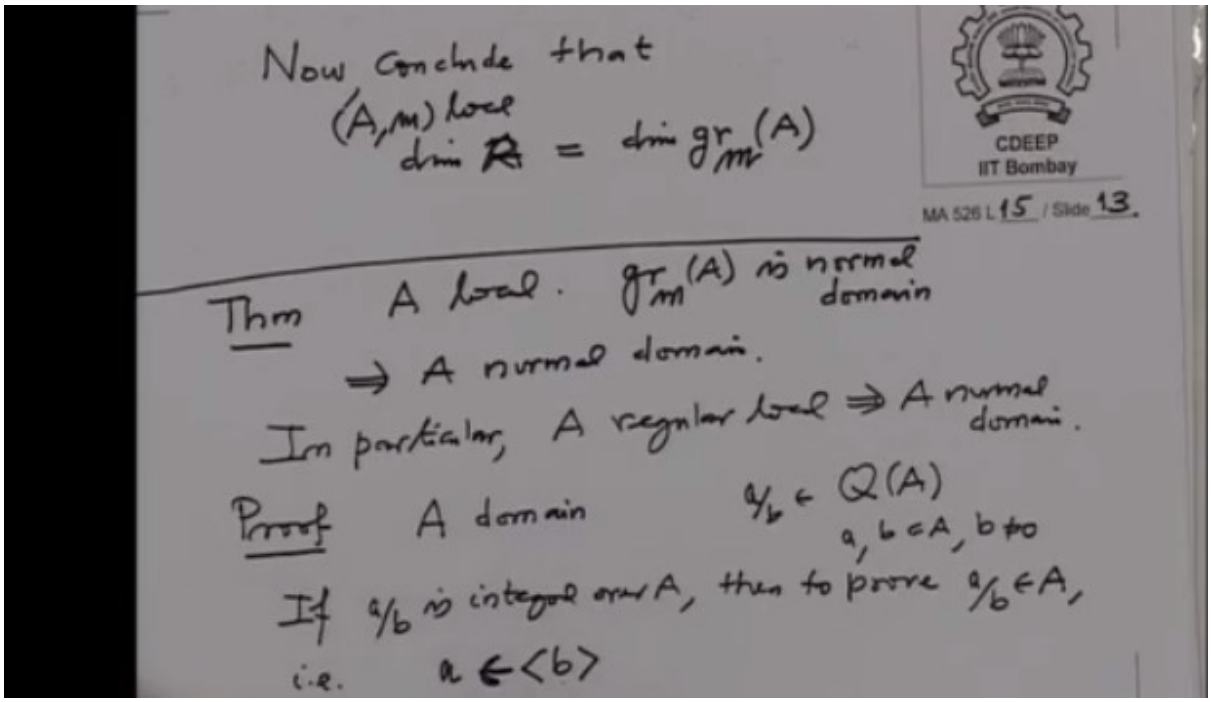
(Refer Slide Time: 09:17)



Now use this degree. So, this degree gives one hand the dimension A and the other hand dimension of graded ring. So now I would just live it for you to tie it up. So now conclude little checking in the end, but that I live it to you, conclude that dimension of A, when A is local, (A,m) local. Then dimension of A and dimension of $gr_m(A)$ they're same. Okay, now that proves one of the thing and now I will prove, this is also very important to prove that normality. Because normality is usually prove by a lot of complicated theorem. And later on we will use more complicated when we have machinery to deduce it easily. So the theorem now I want to prove is, A local and suppose grm is normal domain then A normal domain. In particular it will be regular local rings are normal. A regular local implies A normal. Because we have seen a regular means graded ring is polynomial ring, therefore polynomial is normal, therefore A is normal. Okay, so proof. Proof is not difficult, but it's little tricky. So first note A is a domain, because we have seen last time if graded ring, associated graded ring is a domain then A is a domain. This is we have seen last time. So what do we want to prove now, here you have a quotient field $Q(A)$ and here you have an element $\frac{a}{b}$, where a and b are elements in A, $b \neq 0$. And suppose this is integral over A then I have to prove it is in A. So if $\frac{a}{b}$ is integral over A, then I want to prove, then to prove $\frac{a}{b}$ belongs to A. What does that mean? That is you want to prove that the element a belongs to the ideal generated by b, this is what we want to. Because if it is ideal generated by

b, then a is the multiple of b and then you can cancel b. So we want to prove this.

(Refer Slide Time: 12:51)



But proving this, it's enough to prove that the element a belongs to powers of m, $m^n+\langle b\rangle$ for all m. That is where I will use krull's intersection theorem. It say that in a noetherian local ring, if we take the powers of m and intersect them, it is 0. Okay. So we want to prove this. So I want to prove this for all n. All right, this I'm going to prove it by induction i n. If m equal to 0 it's clear. Because $n=0, m^0$ is ideal the ring itself and nothing to prove. So, I assume n is bigger than equal to 1. And then by induction hypothesis, I can certainly write this a as m power n minus1 plus ideal generated by b. This is by induction hypothesis. So that means a I can write it as some element in m^{n-1} that is $\tilde{a}+rb$, where $\tilde{a}$ belongs to m^{n-1} and r belongs to A. All right, now if this $\tilde{a}$ is already in the next power we are done. So, if $\tilde{a}$ is in m power n then we are done. Otherwise what? Otherwise, it is exactly here. So that means, otherwise, the order of $\tilde{a}$ is $n-1$, now let me explain these term order of $\tilde{a}$. So we have graded ring here, $gr_m(A)$ and we have ring is here and when you have an element here let's say x, element is x here, how do you read it here? You have to first go to the highest power of m that x belong to. And then read mode the next power. See, if this belongs to m^{n+1} then you will read, the x will read in $\bar{x}$

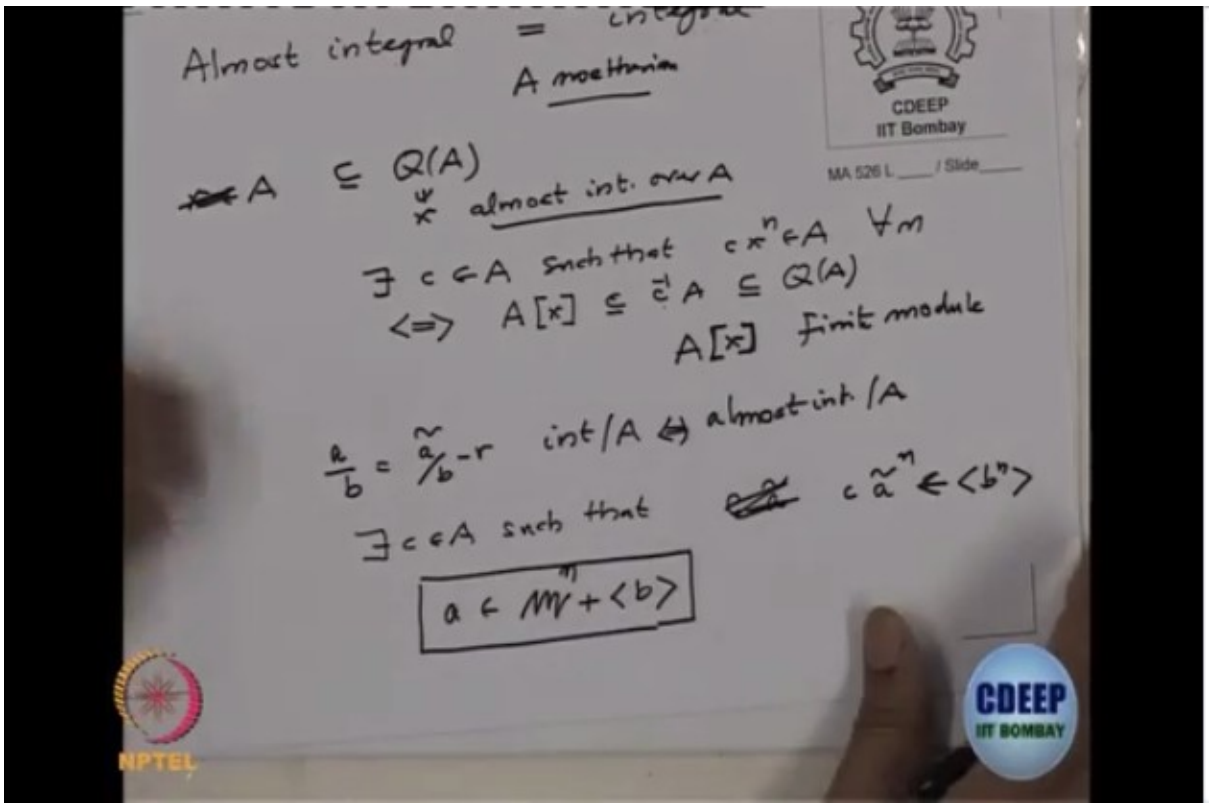
will be in $\frac{m^n}{m^{n+1}}$ and that-- this is the-- it's going to $\bar{x}$. That is how you read elements of a in the graded ring but then this n either property this, n as a property that x belongs to m^n but not the one. So this n is called the order of x.

So that is what I've written, order of $\tilde{a}$ with $n-1$ that means it belongs to m^{n-1} , that's okay. But it doesn't belong to the next one because if it belonging to the next one we are already done anyway. So that is the notation, okay. In that case what happens? Now if you look at these equation and divide this equation by b. That means, $\frac{a}{b}$ will be equal to $\frac{\tilde{a}}{b}+r$, but this is same as saying rewrite it, that means $\frac{\tilde{a}}{b}=\frac{a}{b}-r$, and a and b were integral, r is an element in it, so it's integral over A. So therefore the difference is integral over A. So this is integral over. You see from $\frac{a}{b}$, I'm making some process so that the numerator becomes less and lesser degree, no? So module this. So this is integral over A. Have you heard the concept of almost integral? That two concept almost integral and integral, in case of integral domain. And both are same if the ring is noetherian, so I will recall that. Both are same if the ring is noetherian, if the integral domain is noetherian. So integral you know, integral means, it satisfies the monic polynomial with coefficients in a. Almost integral means, so an element $x\in Q(A)$, this is the quotient field of a, x is an element here. We call it almost integral over A, if there exist an element c in a such that c times x power n belongs to A or all m. that is almost integral. Now what is always two is, integral implies almost-- so, you want to say, they're equal. This concepts are equal in case when A is noetherian. So how do it test somebody is integral, that means we have to check that we should take the algebra generated by that elements it is the finite module, right. So $A[x]$ should be finite module. This is integral, that was one of the equivalent condition from the definition of integral t. But if it is almost integral then what is the condition? If we want to rewrite this condition is what? That means, this condition equivalent saying, look at this $A[x]$, that is contained in $c^{-1}A$ which is contained in $Q(A)$.

You see, if this is in A that means all powers of x will belong to A, if we invert c. This condition is obviously this contains and if everything is noetherian, this

is noetherian because its generated by noetherian module and therefore this will be noetherian. So both this conditions in case of noetherian they're equivalent. So now-- because we have concluded that this $\frac{a}{b}$, which is a tilde by b minus r. This is integral over A, so in particular it is almost integral. So that is that is equivalent to saying almost integral over A. But that will mean that there exist c in A such that-- this is my element x, right? This will mean that there exist a c such that $c\tilde{a}$ so from here I wanted to prove that, see what if that we want to prove? We want to prove that-- we want to prove this equation, no? a belonging to m^n+b , this is what we're heading to prove. This is what we need to prove. So almost integral means, there is a c so that $c\tilde{a^n}$ will belong to $\langle b^n \rangle$. See, they knew this one times sum c power this but when you calculate that will mean that it belongs to b^n .

(Refer Slide Time: 22:12)



But then now read this equations in a graded ring, in a associated graded ring we have to read that. So that means, if I take-- so let me write for an element x in a in grma its image I want to write it $gr(x)$. What is the $gr(x)$? That means, you find the power of m, where x belongs to the highest power and read

mod the next power, that is the $gr(x)$. So when I have this equation, so $gr(c)gr(\tilde{a})^n$ that will belong to gr ideal generated by $gr(b)^n$, but $gr(b)^n$ is this. This is true for every n. That will mean that when I go mod $gr(\tilde{a})$ mod divide by $gr(b)$. This element power of this times the $gr(c)$, this will belongs to the ring and this will belongs to the quotient field. Quotient field of $gr(A)$. See, therefore this element is almost integral. So $gr(A)$ tilde this proof is not difficult but it is-- we have to use some calculations. This one is almost integral because this element exist, so that the all powers belongs to this quotient field. So this is integral, almost integral and therefore integral over $gr(A)$ but we know our assumption this is normal, so this belongs to $gr(A)$. So $gr(\tilde{a})$ belong to-- divided by $gr(b)$, this actually belongs to $gr(A)$ since $gr(A)$ is normal. But what did that mean? That mean, that where do this element by definition $gr(\tilde{a})$, this is by definition it is in the nth component of this ring, and an nth component means? The order of this $\tilde{a}$. So this belongs to, therefore $gr(A)_{n-1}$ and this $gr(b)$, this belongs to $gr(A)_{ord(b)}$.

And therefore this fraction is therefore homogeneous. So these are homogeneous element of degree $n-1$. This homogeneous element of degree order b and therefore this fraction is homogeneous of degree $n-1+ord(b)$. So that means this element is of the forum $gr(\tilde{a})$ divided by $gr(b)$, these of the form gr of some element s. Where s is of order this order $n-1+ord(b)$. That is belongs to therefore this belongs to $m^{n-1+ord(b)}$, what the next power? $m^{n+ord(b)}$. Its homogeneous elements loop are coming from a. But this means look at $gr(\tilde{a})$ - $gr(s)$, you just multiply $gr(b)$ which is equal to $gr(\tilde{a})$ - $gr(sb)$ because that is how the product is defined in the graded ring. But this is same as $\tilde{a}-sb$, this belong to the next power. So this is plus or this is the image of this element in $\frac{m^{n-1}}{m^n}$. This is the image of this element in this coefficient. So that will mean that $\tilde{a}$ is equal to $\tilde{a}-sb$. This - sb which is + sb. This is $\tilde{a}$ is equal to this + sb. This belongs to m^n look at the difference. And this one belongs to b. So we are done, right. So just what I just say that we just, this is just an interplay between how do read the graded ring. The structure of the graded ring is very important. How the element from a go there and how do you read their degrees and so on. So that will, the Krulls whatever you want and then Krulls by passing from a to $\bar{a}$ which is $\bar{a}$ is A by ideal generated by b. Then the Krulls intersection theorem will tell you what we want to get the result. But this doesn't use high powered machinery that

again I will prove this regular local in the normal when I would have hired some more vocabulary from algebra. But this is the first principle proof. Okay.