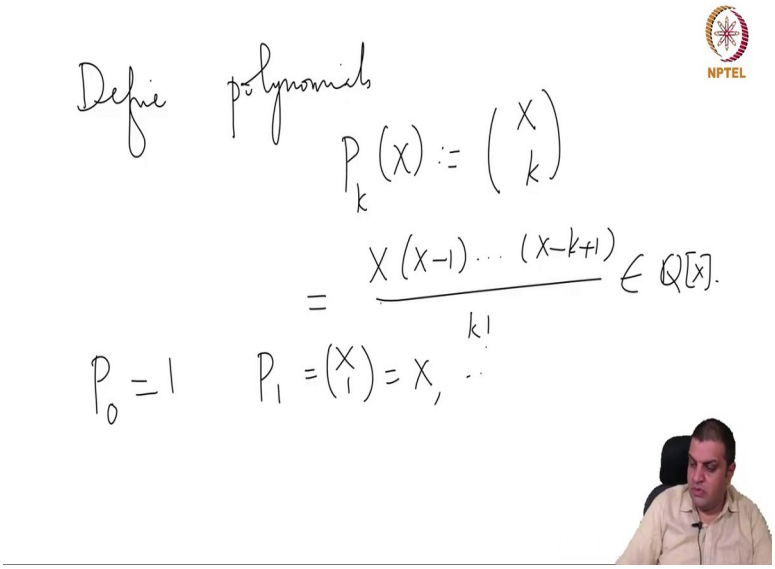
Computational Commutative Algebra
Prof. Manoj Kummini
Department of Mathematics
Chennai Mathematical Institute
Indian Institute of Technology, Madras

Lecture – 38
Hilbert polynomial

This is lecture 38 and in this, we wanted to understand if you look if you have a graded module over the polynomial ring over an Artinian local ring like in the last lecture. How the length of the module; so, we know that we saw that each M_j is finitely generated R module.

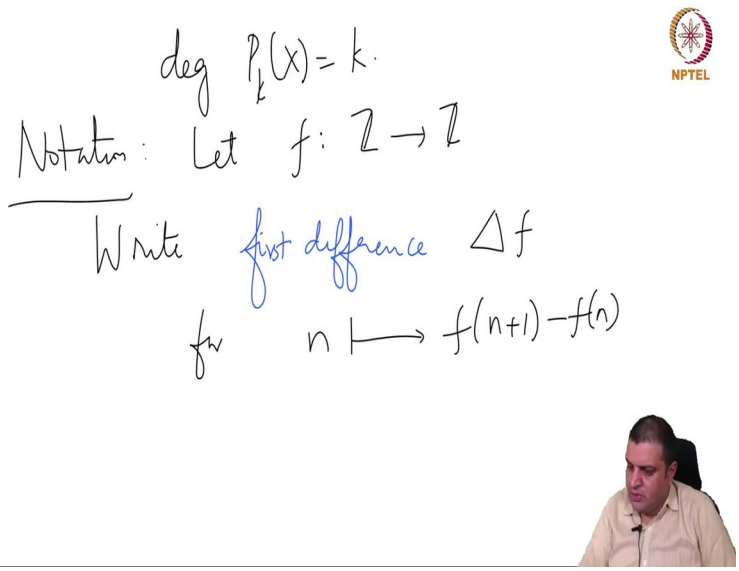
R is an Artinian local ring. Hence, M_j itself is an Artinian module. So, it has finite length and we would like to understand how it varies with j. So, the function j goes to length of M_j. This is what we would like to understand.

(Refer Slide Time: 00:56)



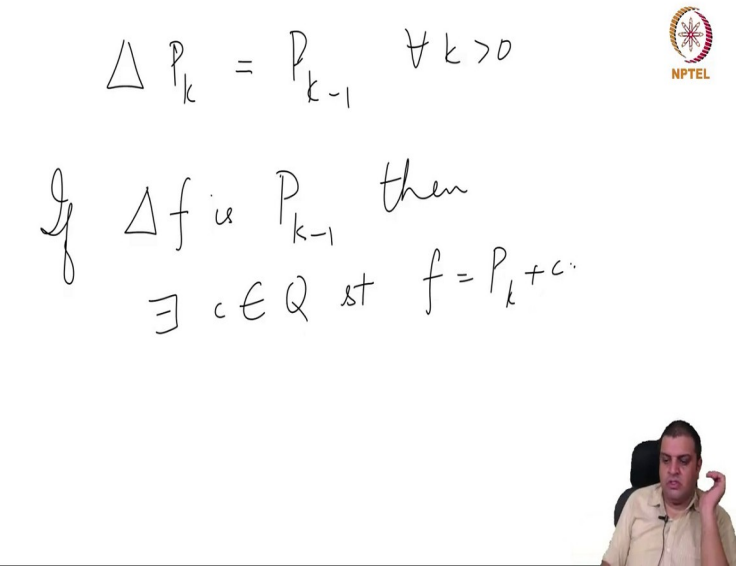
So, we want to define polynomials; $P_k(X) = X \text{ choose } k = \frac{X(X-1)\ldots(X-k+1)}{k!}$ and this is a polynomial with rational coefficients. We can take a quick look at what this is; $P_0 = 1$, constant polynomial 1; $P_1 = X \text{ choose } 1 = X$ and then and so on.

(Refer Slide Time: 01:47)



So, $deg(P_k) = k$ notation. Let $f: Z \to Z$ be a function, write the first difference, Δf for the function, the function which takes $n \to f(n+1) - f(n)$. So, this is what M.

(Refer Slide Time: 02:54)

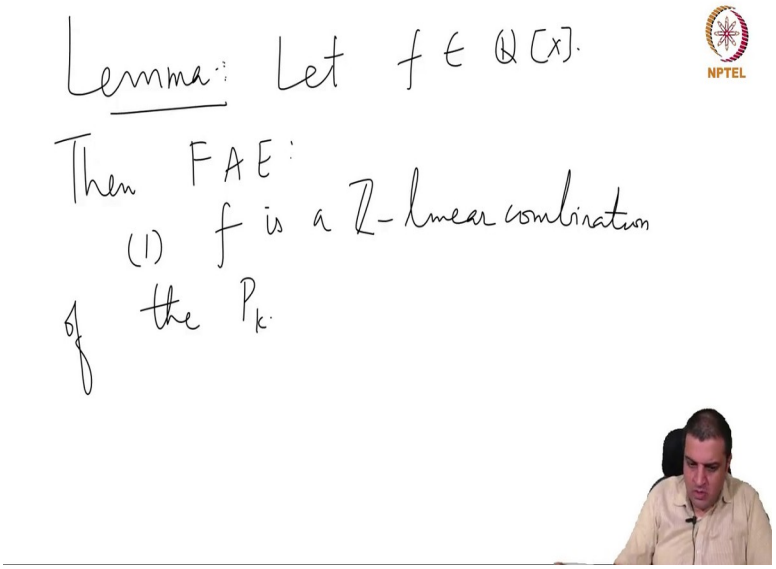


So, we would need to what do. So, if you take $\Delta P_k = P_{k-1}$ for all k > 0 that is just like Pascal's triangle . So, what we are saying is (n + 1) choose k - n choose k = n choose (k+ 1) ;

This follows from the Pascal's triangle and also, if Δf is P, so maybe one should not just one should think of f(x) as a polynomial in Q[X]. So, we would like to talk about delta f for; if Δf is P_{k-1} then there exist a $c \in Q$ such that $f = P_k + c$.

So, this is slightly loose. What we are saying is f is a function from Z to Z, it agrees with P_k at every point of Z. So, this is a polynomial. So, Δ as a function from Z to Z these two things are the same; f is a function from Z to Z. It is the same thing is implied there also.

(Refer Slide Time: 04:39)

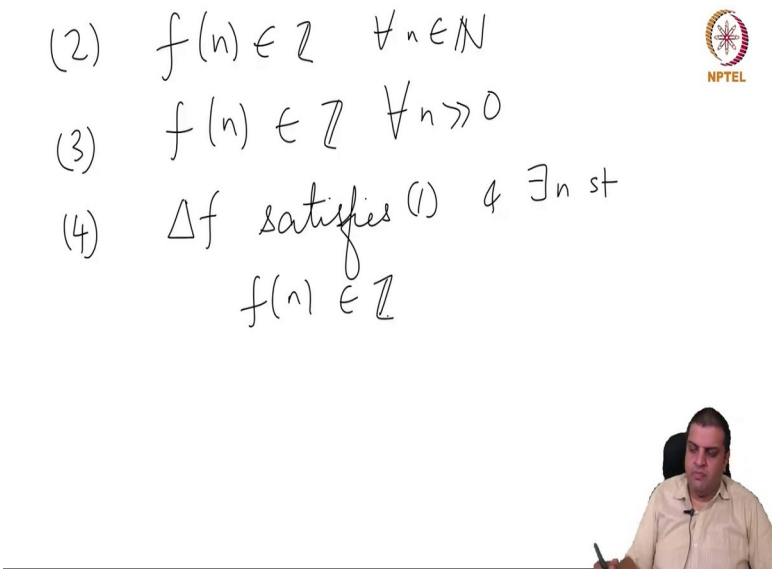


So, this is just two observations. So, here is a lemma. Let $f \in Q[X]$, then the following are equivalent;

1) f is a Z-linear combination of the polynomials P_k .

2) f(n) is an integer for all $n \in N$.

(Refer Slide Time: 05:23)

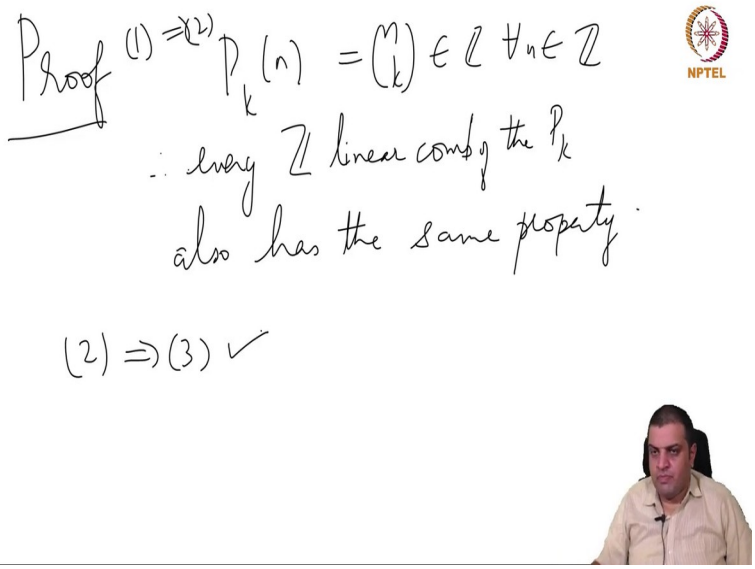


3) f (n) is an integer for all n >>0; and

4) the function Δf satisfies (1) and there exist an n such that $f(n) \in Z$. So, the conditions are f itself is the linear; so, we are talking about rational polynomial; f itself is a linear combination of the P_k .

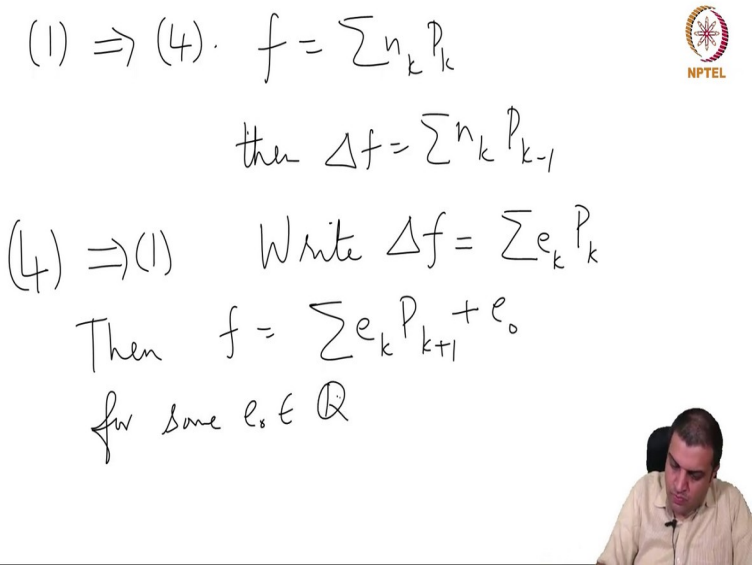
Then, it is equivalent to f(n) is an integer for every N and this is a weaker statement and as far as this is concerned this is a weak, this just says that they are existing with this property but on the other hand, one also needs a Δf is satisfies 1.

(Refer Slide Time: 06:39)



So, let us quickly prove this lemma. Notice that P_k satisfies this. $P_k(n) = n \text{ choose } k$ which is an integer for all $n \in Z$. Therefore, every Z-linear combination of the P_k also has the same property. So, this is 1 implies 2; 2 implies 3 is immediate.

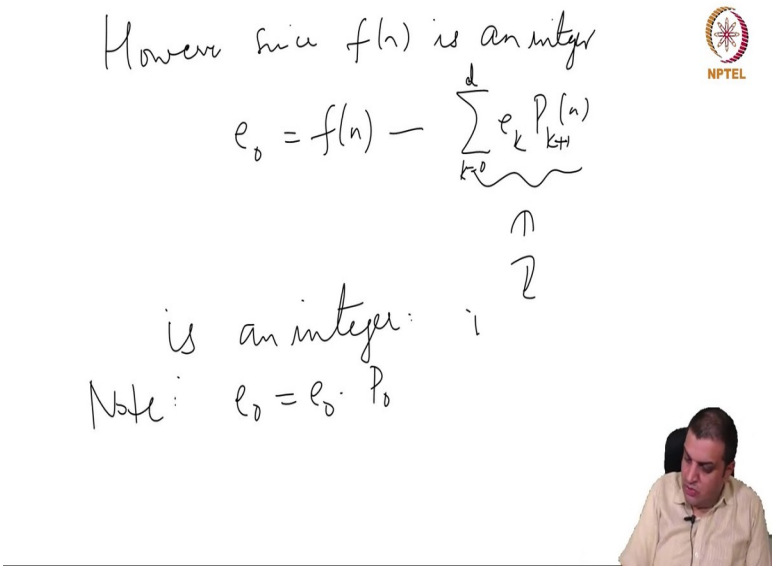
(Refer Slide Time: 07:34)



Now, let us prove 1 implies 4, that is also immediate because if $f = \sum n_k P_k$, then $\Delta f = \sum n_k P_{k-1}$. So, this is it is also true that 1 implies 4, Δf satisfies this and f of course satisfies Z-linear combination, its true; I mean f satisfies 2, condition 2. So, it also satisfies 4 the final part of 4.

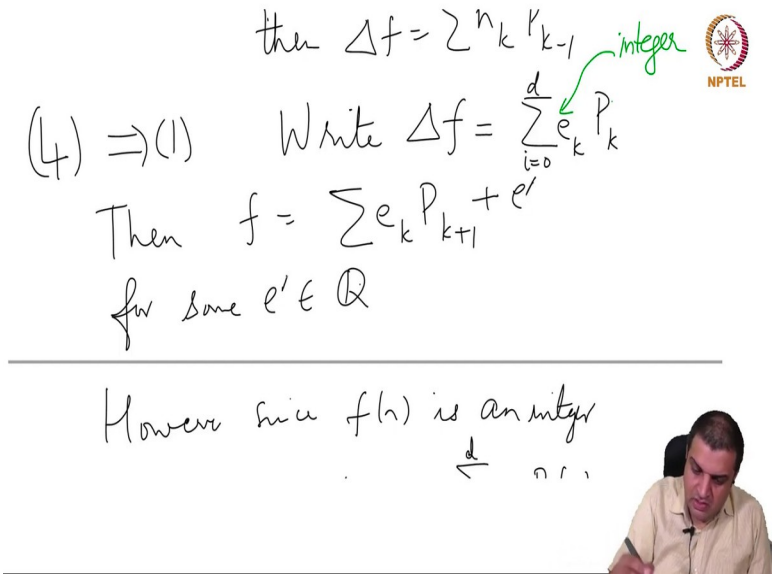
So, now let us imply let us prove that 4 implies 1. So, this is to say that if Δf satisfies satisfies 1 and it has this property, then f itself satisfies 1. write $\Delta f = e_k P_k$ where $e_k \in Z$, then f we have seen this earlier $f = \sum e_k P_{k+1} + e'$; P_k goes to P_{k+1} , e_k does not change in any way , for some $e' \in Q$.

(Refer Slide Time: 09:24)



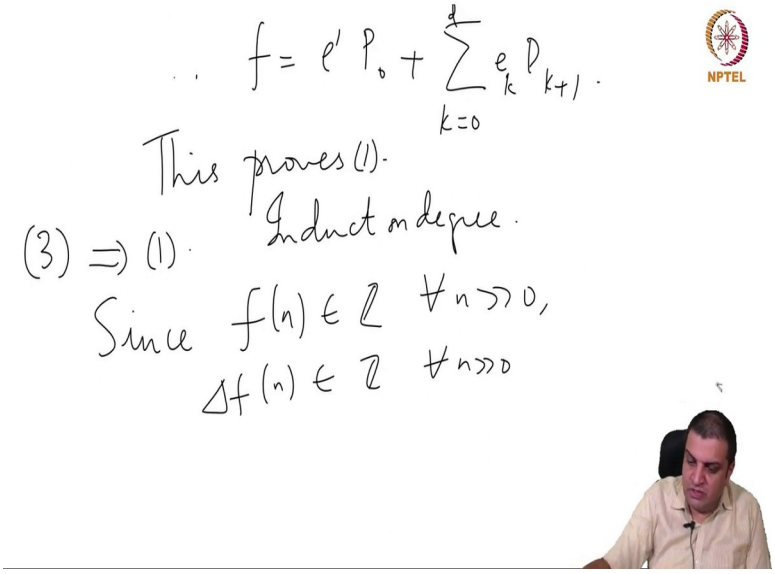
However, since f (n) is an integer, , for the f(n) satisfies 1 as to say e_k are integers ; so, f (n) is an integer ; $e' = f(n) - \sum_{k=0}^{d} e_k P_{k+1}(n)$ in Z ;

(Refer Slide Time: 09:40)



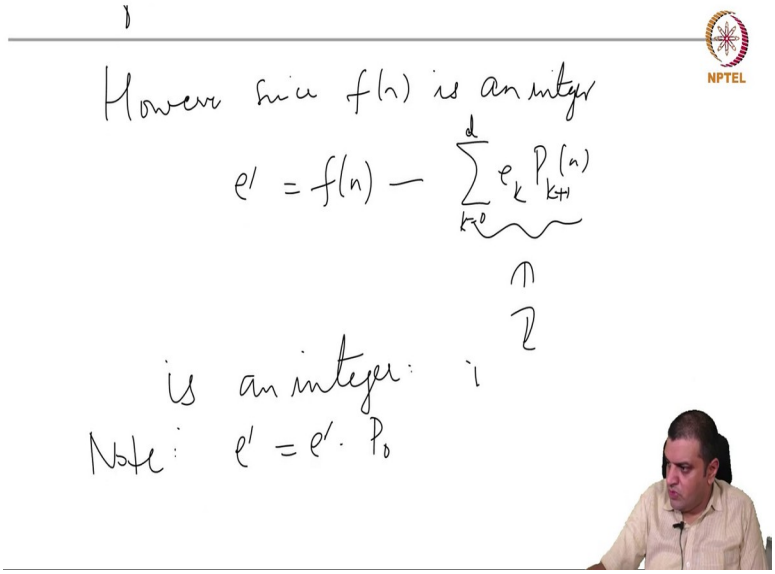
So, we can rewrite it as $e' P_1 + i$ this condition. So, it is so this proves 1. maybe I should just write it notice that, here we only start with P_1 onwards. So, $e' = e' P_0$.

(Refer Slide Time: 10:56)



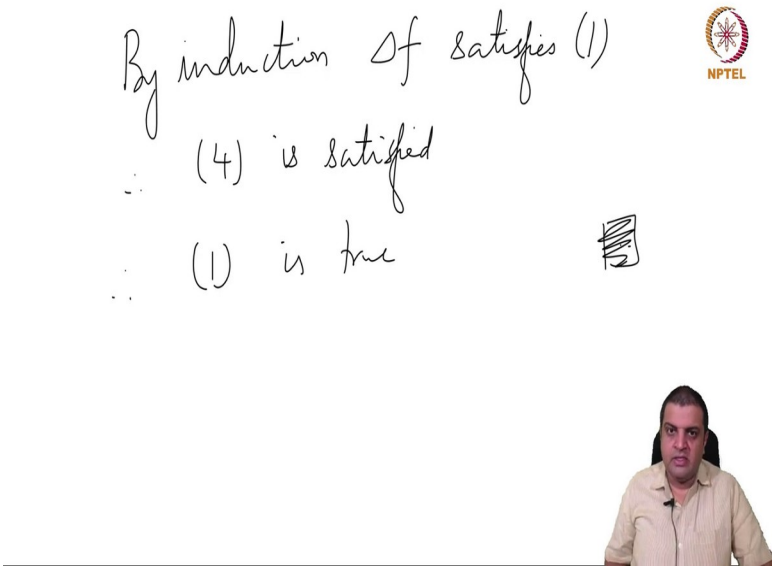
So, therefore, $f = e' P_0 + \sum_{k=0}^{d} e_k P_{k+1}(n)$

(Refer Slide Time: 11:30)



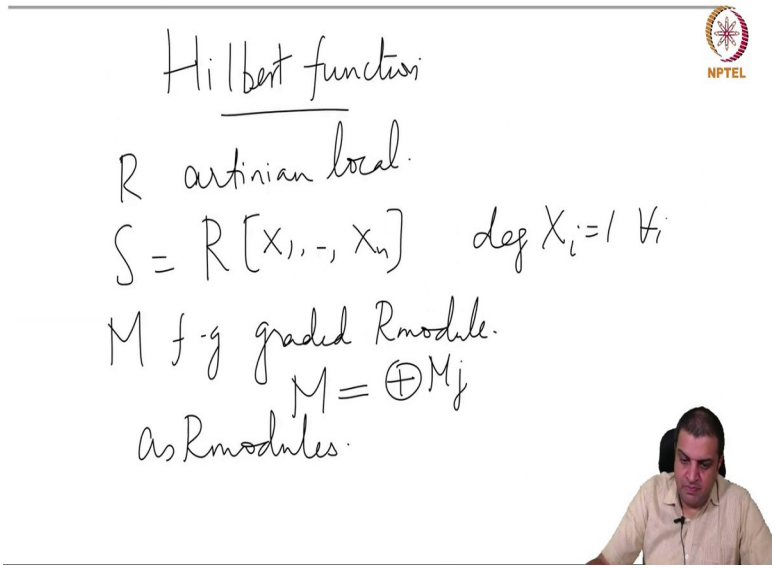
So, this is this proves 1. So, now, we prove that 3 implies 1. So, this is done by induction on degree. since $f(n) \in Z$ for all n >> 0. $\Delta f(n)$ is an integer for all n >>0.

(Refer Slide Time: 12:48)



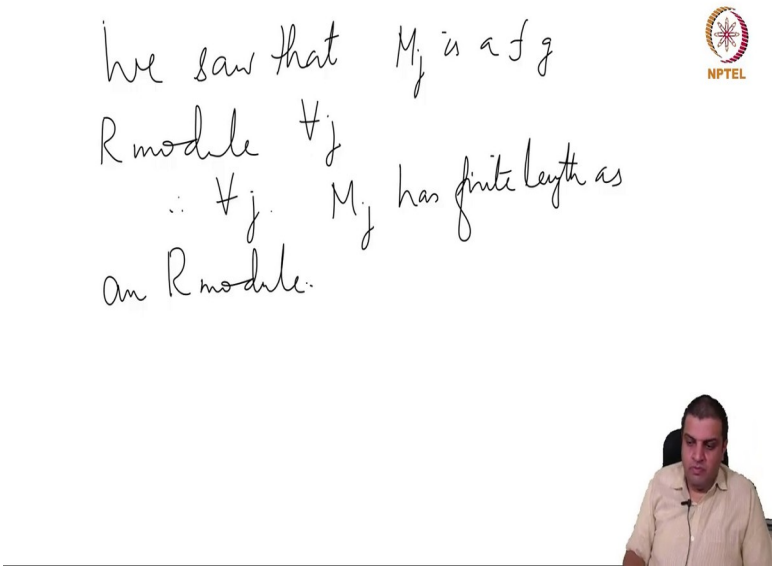
So, by induction Δf satisfies 1 and of course, so therefore, 4 is satisfied . Δf satisfies 1 and f (n) = 0 is an integer for some integer. So, 4 is satisfied, but we have already proved that 4 implies 1; therefore, 1 is true. So, next, we want to apply this to the study of what is called the Hilbert function of graded modules over Artinian rings.

(Refer Slide Time: 13:52)



So, this is the setup that we want. So, let us call let us say Hilbert functions. So, we go back to the setup that we had earlier. So, R is an Artinian local ring; $S = R[X_1, \ldots, X_n]$ graded with $deg(X_i) = 1$ for all i and M is a finitely generated graded R-model.

(Refer Slide Time: 14:45)

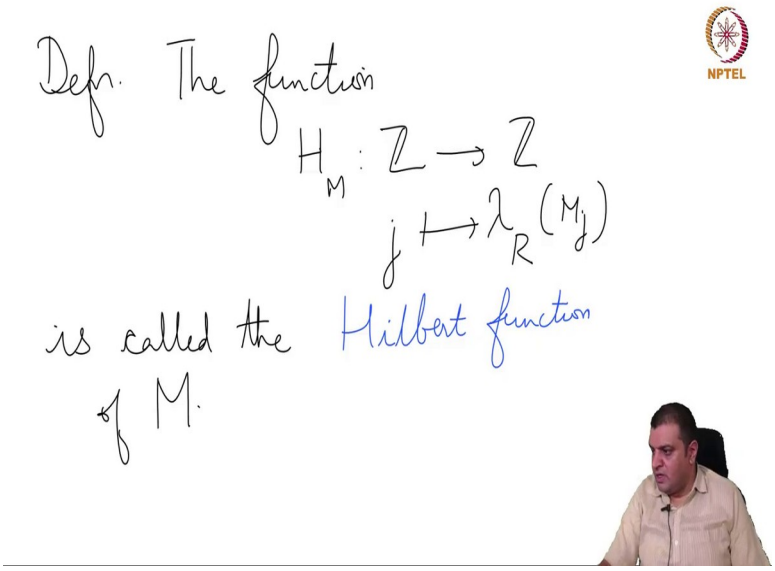


I mean we can decompose $M = \oplus M_j$ as R-modules. Notice that this decomposition is R-modules. Similarly, direct sum of S_j as is as R-modules. So, we saw that M_j is a finitely generated R_module for all j.

So far we did not use that R is Artinian, we used that M is Noetherian for which we use that S is Noetherian to say that M_j is a finitely generated, we have to take submodules and then, their quotients. So, we need all of them finitely generated.

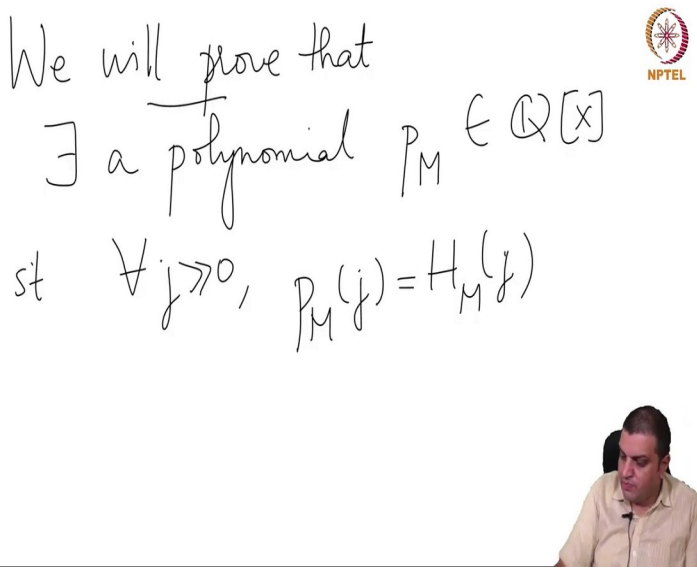
So, we needed finite M is Noetherian. For M to be Noetherian, with this hypothesis S has to be Noetherian for which all that we need is R is Noetherian. So, we are not yet used that R is Artinian. So, here we set that up. Therefore, for all j, M_j has finite length as an R module. definition.

(Refer Slide Time: 16:28)



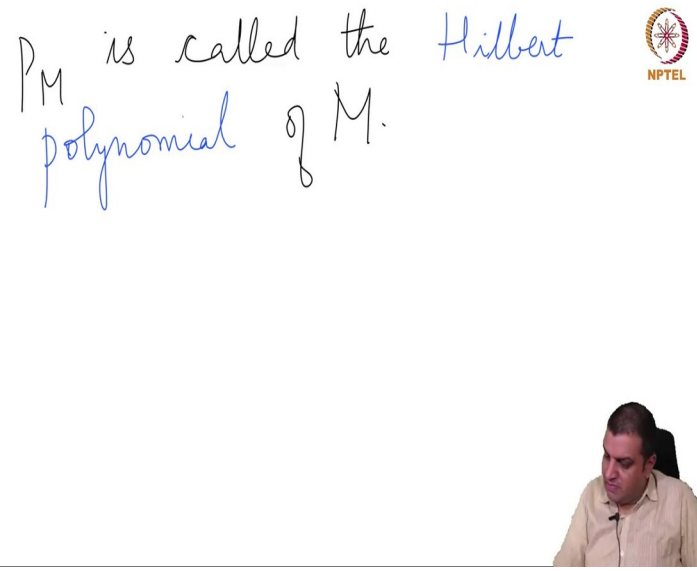
The function let us denote it by $H_M : Z \to Z$ which $j \to \lambda_R(M_j)$ is called the Hilbert function of M.

(Refer Slide Time: 17:24)



So, what we wanted to prove is that; so, we will prove that there exists a polynomial $P_M \in Q[X]$ such that for all j >>0, $P_M(j) = H_M(j)$. So, this is what we want to prove. So, we will prove this statement.

(Refer Slide Time: 18:13)

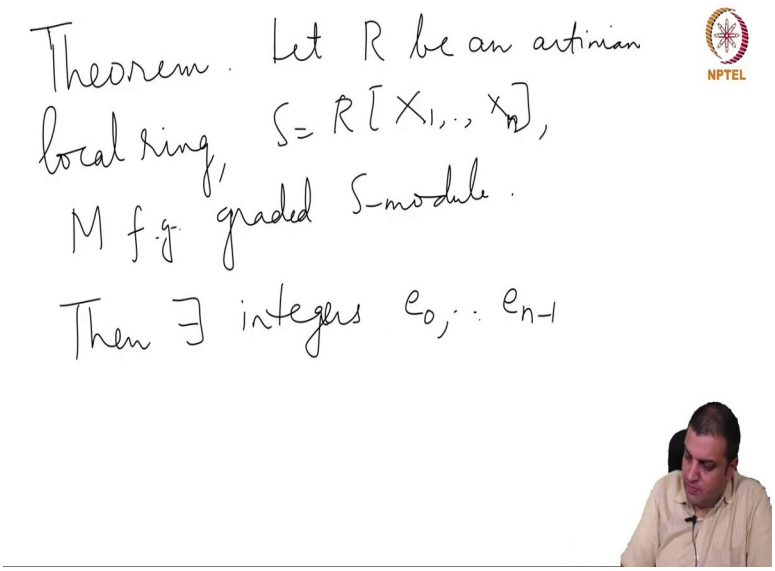


P_M the polynomial is called the Hilbert polynomial of M. in the little this lecture maybe a little bit of the next, we will prove that. So, Hilbert function is what is defined that there is a polynomial which gives a value for sufficiently large M.

So, we will see example where and it is not at all difficult to generate them. We will see examples, where the polynomial would not agree with it right at the beginning itself. So, that is one thing we will have to that is we only that this is for all sufficiently large ok.

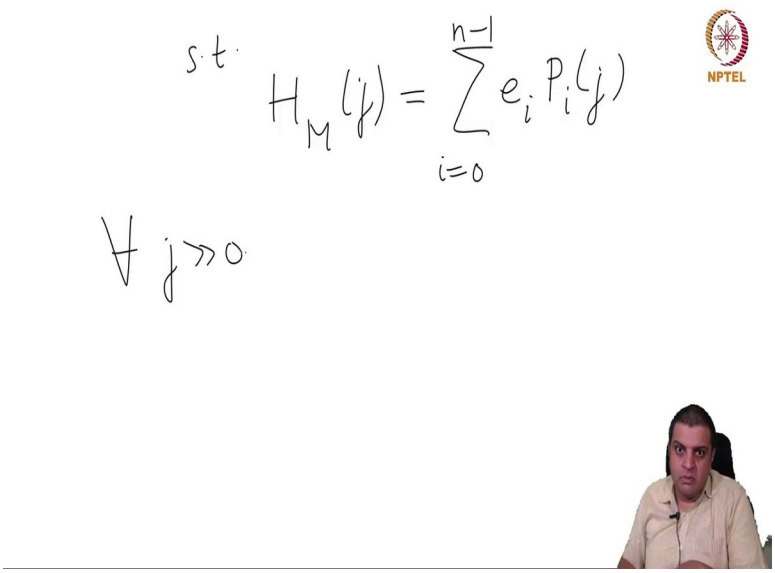
So, we will prove something a little stronger, we will say that we will prove that the Hilbert polynomial is actually a combination; integral combination of the of these here; that is the context of this lemma that the Hilbert polynomial is Z-linear combination of the P k that is what we will prove in the theorem. The full strength of theorem will not be used a lot, but it is better to see it this way itself .

(Refer Slide Time: 20:11)



So, let us prove that statement theorem. Let R be an Artinian local ring, $S = R[X_{1,\ldots}, X_N]$, M finitely generated graded S-module; then, there exists integers $e_{0,\ldots}, e_{n-1}$

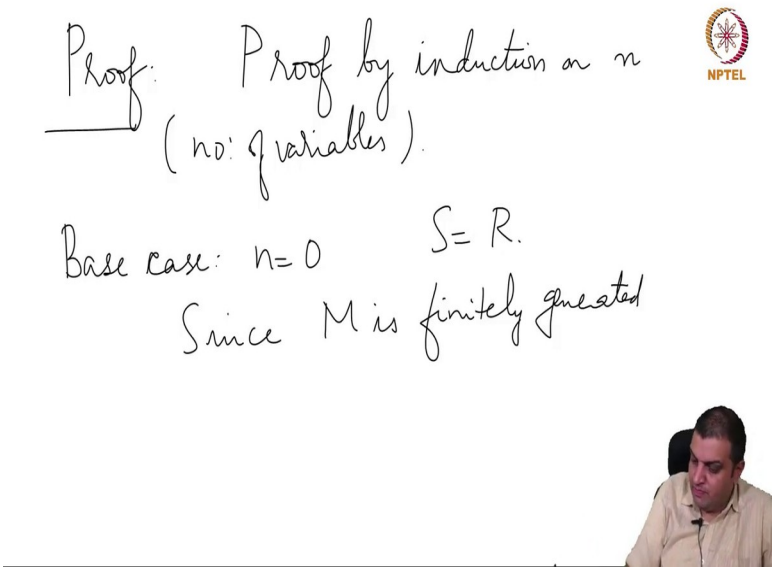
(Refer Slide Time: 21:18)



such that the $H_M(j) = \sum_{i=0}^{n-1} e_i P_i$ for all j>>0. So, this is this is the stronger version of this theorem.

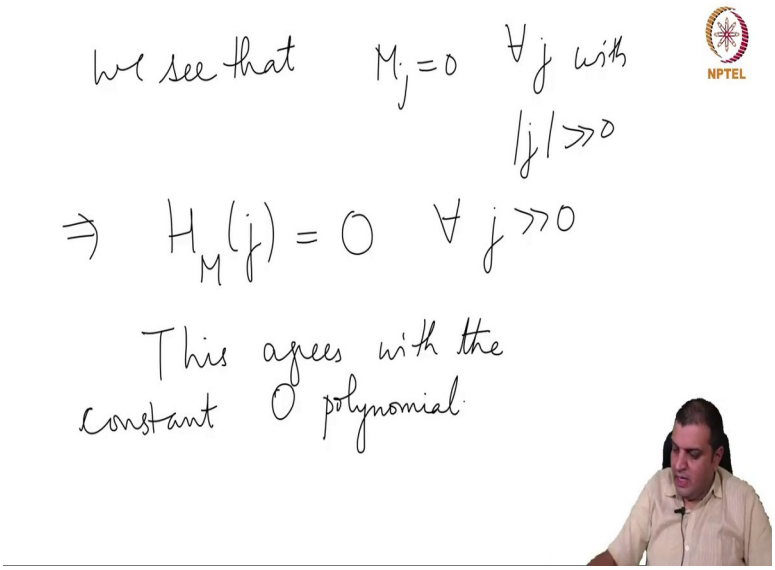
In other words, the Hilbert polynomial is an integral linear combination of these special binomial polynomials that we just defined. So, this is what we will prove. So, we will set up the basic part today in this lecture and in the next lecture, we will finish the proof.

(Refer Slide Time: 22:19)



So, this proof; so, this is just set up of the basic part of the proof will be done; we will do it now. So, this is proof by induction on n; n the number of variables. The base cases n = 0. In other words, S = R and M is a graded module, it is finitely generated by as an S-module means that it has generators living only in finitely many degrees.

(Refer Slide Time: 23:27)

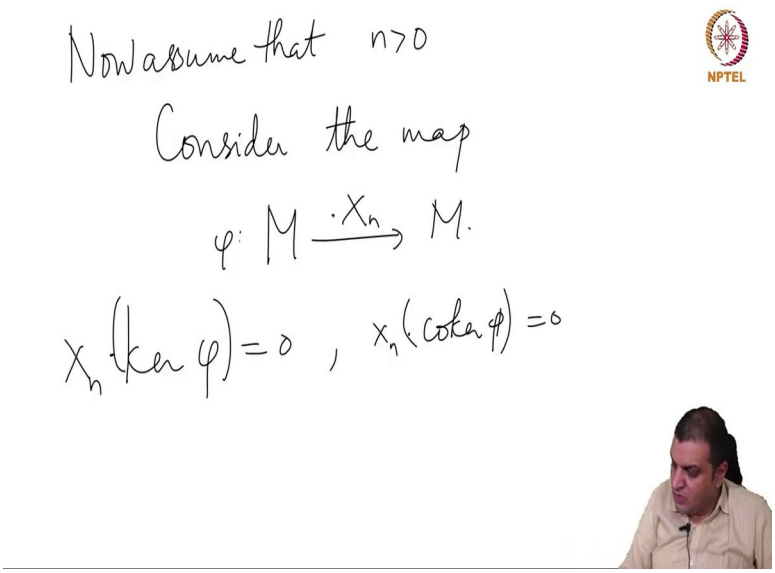


We see that $M_j = 0$ for all | j | >>0 ; going in either direction M_j must be 0 ok. In other words, $H_M(j) = 0$ for all j >>0. So, we just leave this part because assertion is only about this and we treat this as a polynomial as the empty sum on that side.

.So, for this we take. So, this is a constant 0 polynomial. So, this agrees with them. that is all. Here, the summation is empty. So, this is. So, it this proves in the 0 case. So, let us just look if there is this thing says that if there is 1 variable, you will only see P_0 which is the constant; constant polynomial.

If there are 2 variables, we will see P_0 and P_1 which is constant and linear, if there are no variables; then, we will not see anything here and we get this I mean convention sum of an empty set is 0. So, this is this takes care of the base case .

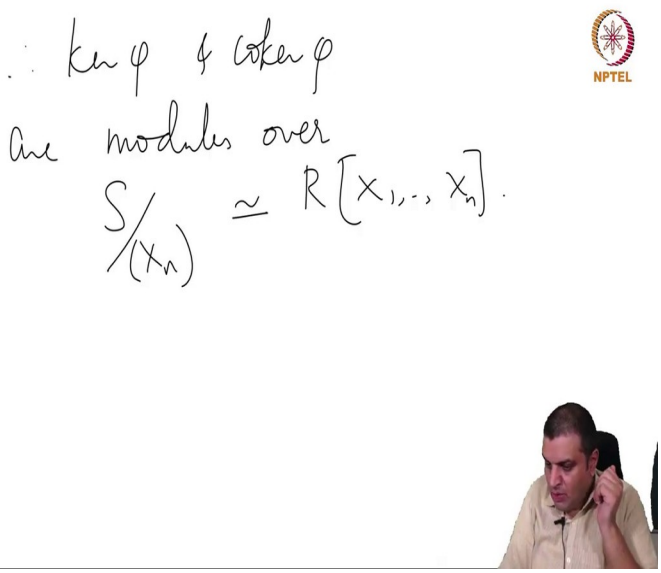
(Refer Slide Time: 25:19)



Now, assume that n > 0 , now consider the map $\varphi : M \to M$ multiplication by X_n . Let us look at the kernel and co kernel. Notice that $X_n ker(\varphi)=0$ that is why it is a kernel of multiplication by X_n .

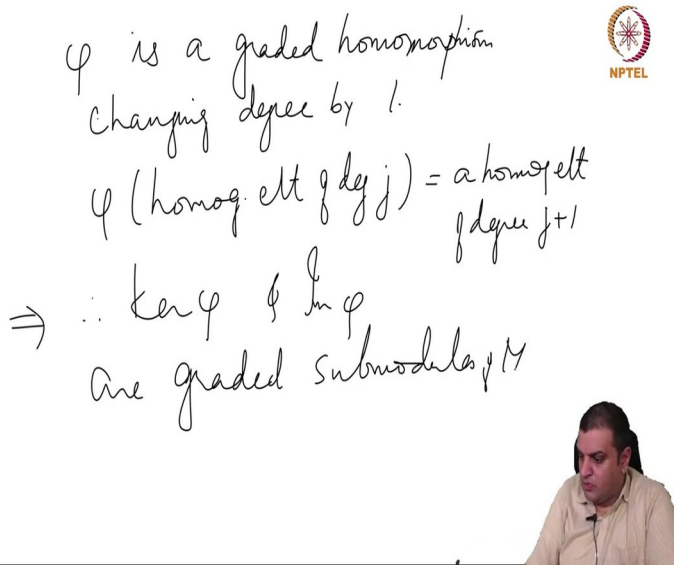
And similarly, $X_n(coker\,\varphi)=0$. cokernel means M modulo the image of this map. But anything that is in M will get multiplied by X_n precisely into the image of this. So, it will go to 0; co kernel will be 0.

(Refer Slide Time: 26:34)



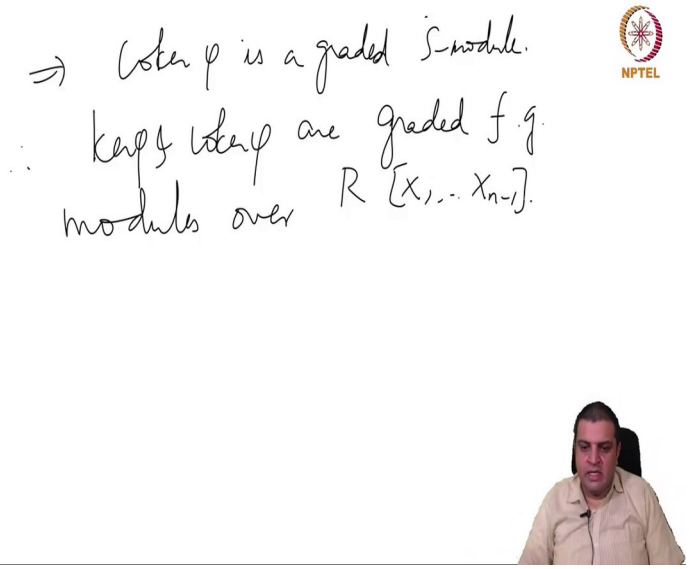
So, in other words, $ker(\varphi)$ and $coker(\varphi)$ are modules over $\frac{S}{X_n}$ which is isomorphic to the subring $R[X_1, \ldots, X_{n-1}]$. So, this is both the subring of S and also, quotient ring of S and we will identify these two things, we will not fuss about this. So, we get this.

(Refer Slide Time: 27:21)



Now φ is a graded homomorphism changing degree by 1. So, that is φ (homogeneous element of degree j) = a homogeneous element of degree j + 1; therefore, $ker(\varphi)$ and $\Im(\varphi)$ are graded submodules of M.

(Refer Slide Time: 28:26)



Which now implies that $coker(\varphi)$ is a graded S-module and all of these are finitely generated because we are in Noetherian situation. So, therefore, $ker(\varphi)$ and $coker(\varphi)$ are graded finitely generated modules over $R[X_1, \ldots, X_n]$.

So, we will end this lecture here, but so, there is a little bit more argument using induction to now conclude the proof, which we will do first thing in the next lecture.