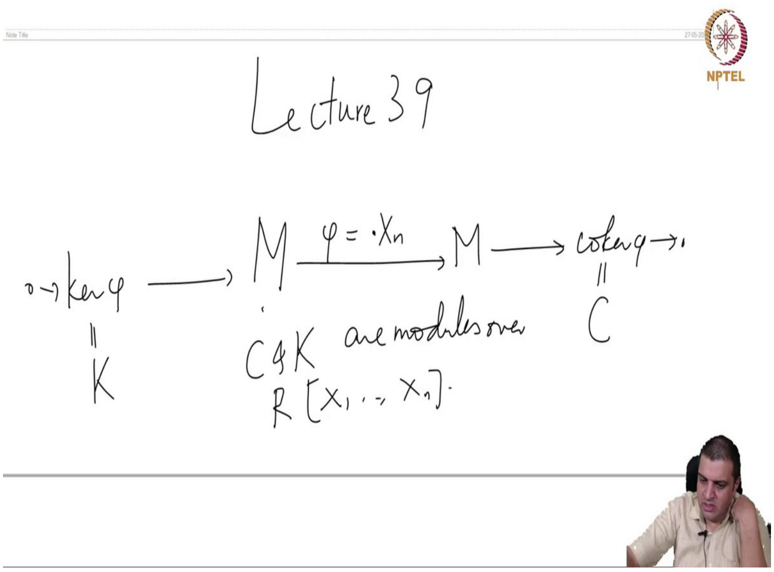
Computational Commutative Algebra
Prof. Manoj Kummini
Department of Mathematics
Chennai Mathematical Institute
Indian Institute of Technology, Madras

Lecture – 39
Hilbert-Samuel polynomial

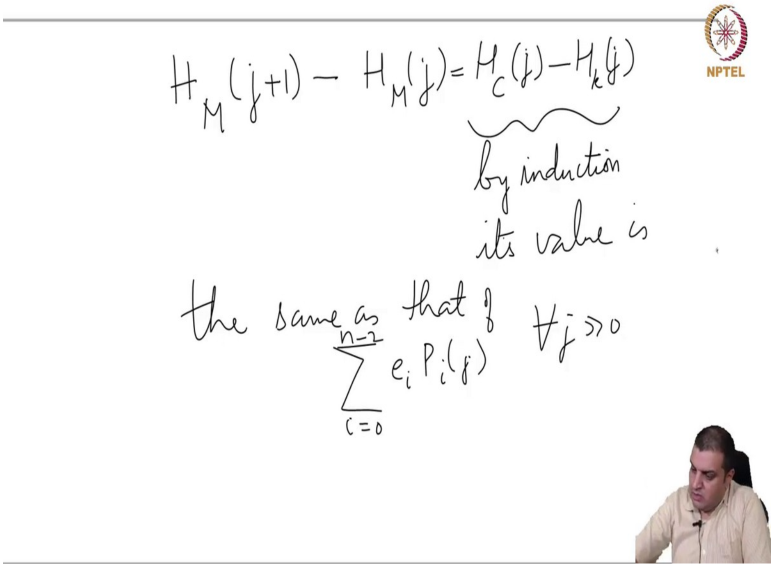
(Refer Slide Time: 00:14)



So, we now continue with the proof of the theorem, we have done the following. So, this is where we had stopped in the last lecture, which is that we had a finitely generated graded module. And we had $0 \to ker(\varphi) \to M \xrightarrow{x_n} M \to coker(\varphi) \to 0$; this shifts degree by 1 degree, j part here goes to degree j +1 1, and then we had $coker(\varphi)$ and $ker(\varphi)$. So, this is the situation we are we were in.

And we wanted to prove that, by induction we wanted to prove that the Hilbert function of M agrees with the polynomial in sufficiently large degrees. And not just that it agrees, it is a Z-linear combination of the polynomial, the binomial polynomials x choose k. If we take degree j part here, it gets multiplied to degree j + 1 ; degree j part of the cokernel and degree j part of the kernel.

(Refer Slide Time: 01:45)



So, let us call $C = coker(\varphi)$ and $K = ker(\varphi)$ and the observation was that C and K are modules over $R[X_1, \ldots, X_{n-1}]$. $H_M(j+1) - H_M(j) = H_C(j) - H_K(j)$, so, depending on how you grade it, it would be either j or j + 1 but we will just call it j. So, we are taking this, subtracting the length from here and then on this side we will have kernel. So, if you have any. So, this is an exact sequence; sorry let us go back a little bit, this is an exact sequence.

If you look at elements of degree j that go to 0, that will; so that is here. Then here we will be look at elements of degree j + 1 and here we get some; depending on how what you cal C degree j or degree j + 1. So, we would get something here. So, the alternating sum of their length should be 0. So, that is any that is a property about an exact sequence of finite length modules, which we will work out in an exercise

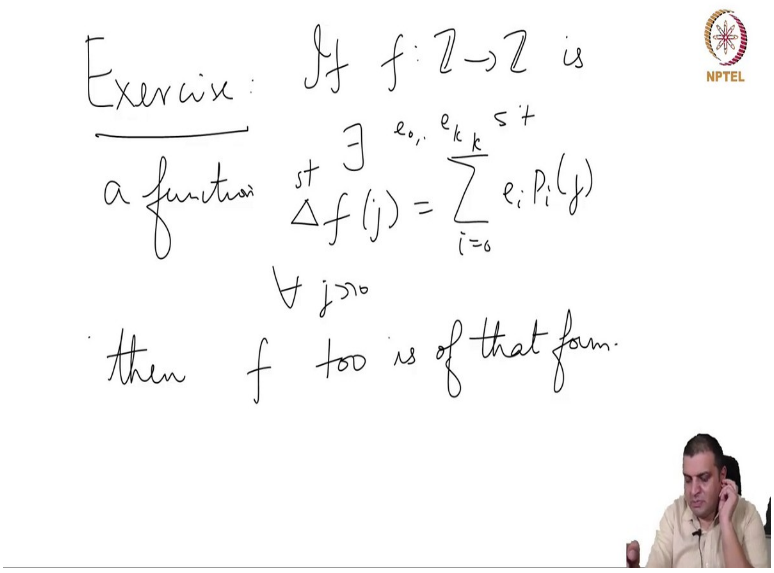
So, here there is a degree j part of this, degree j part of this, degree j+1 part of this and degree j part of this; in that sequence all kernels are equal to all images of the previous map. And hence the sum alternating sum would be 0. And so in that case; so we are taking the length of this, minus this, minus this.

So, alternating sum means, length of this minus this minus this plus this is equal to 0; in other words, length from these two parts this and this will be equal to length from these two parts.

And so, this is and when we rewrite it we would just get $H_K(j)$. So, this is from the fact that, in each degree this would give an exact sequence, but bear in mind that there is a change in degree for this map. So, now, what do we know? So, by induction, this is a function which agrees with a polynomial of that form. So, this agrees with by induction, this is equal to.

So, its value is the same as that of $\sum_{i=0}^{n-2} e_i P_i(j),$ j>>0, remember these are in n minus 1 variable, so this is what we would get for all sufficiently large j. So, this function itself are not polynomials; it is only for all sufficiently large values that on the right side this agrees with the polynomial.

(Refer Slide Time: 05:57)

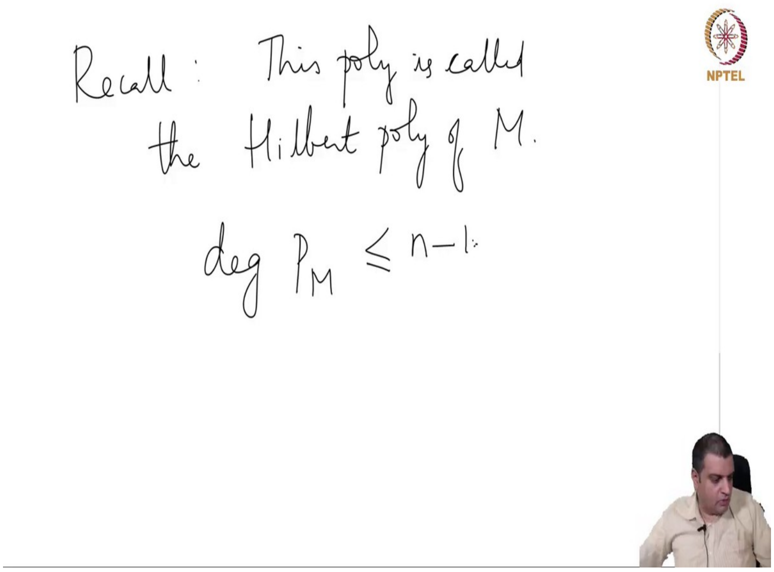


So, now, here is an exercise which I will outline how it should be done with hints. If $f: Z \to Z$ is a function, such that there exists some $e_0, \ldots, e_k$ such that $\Delta f(j) \sum_{i=0}^{k} e_i P_i(j)$ for j>>0. So, this is the delta of the function of the Hilbert function; this is the first difference of the Hilbert function. So, to finish the proof, we will have to prove or one way to prove would be that; if the first difference satisfies this property, then the function also satisfies that property. So, that is what we will.

So, that this would be an exercise; it would be done in a way similar to the lemma was proved and I will outline the steps then f too is of that form. That is for all sufficiently large j, f_j will also be some integer linear combination of $P_i(j)$. So, this you will do the exercises, not very difficult; once we understand what happened in the proof of the lemma and so that is the end of the proof.

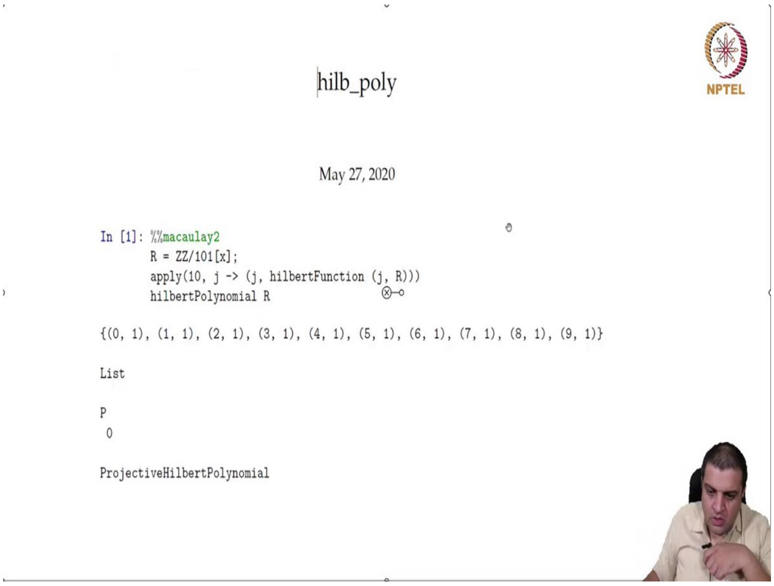
So, the first difference of the Hilbert functions satisfy that by induction and hence Hilbert function also satisfies that property. So, the precise nature of these coefficients we will not worry about; sorry in this course, but they are also of interest in various contexts. So, now, let us look at.

(Refer Slide Time: 08:31)

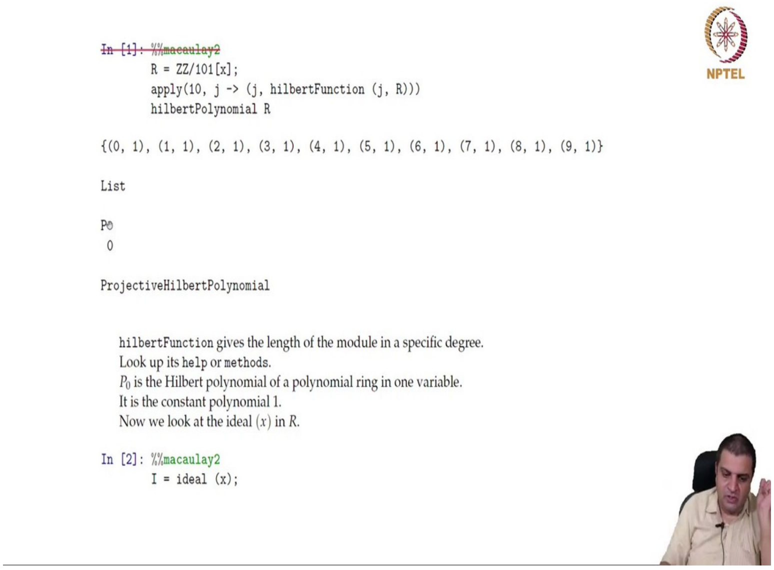


So, recall that this polynomial is called the Hilbert polynomial of M as an S-module. And note also that $deg\, P_M \leq n-1$; that it is at least 1 less than the number of variables , we would need this information literally. So, let us look at a Macaulay example.

(Refer Slide Time: 09:10)



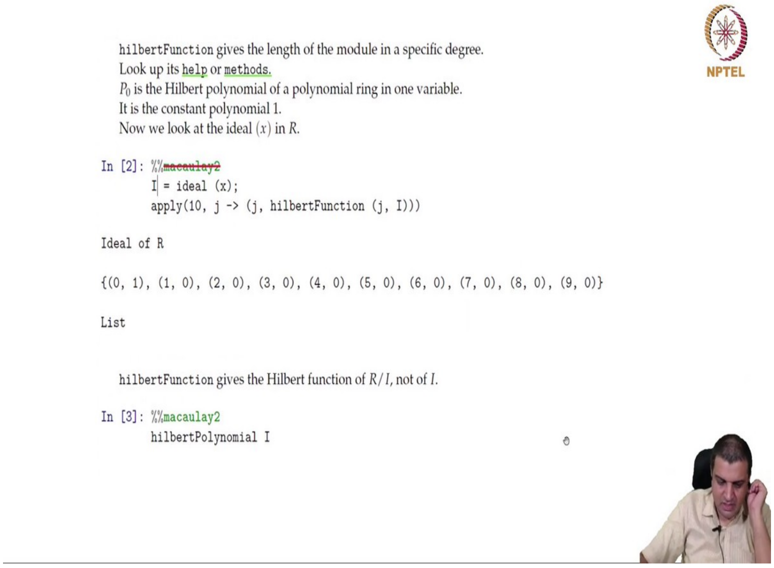
(Refer Slide Time: 09:14)



So, this is a calculation about the Hilbert polynomial. So, we ask calling. So, the function, relevant functions are Hilbert function with a camel case. So, f is a upper case, H is lower case. And so again, so R is a polynomial ring in one variable, apply 10. So, this means integer 0 through 9, the function j goes to. So, if I want to print j and the Hilbert function just for reading it.

So, it says in degree 0 it is 1,in degree 1, it is 1, in degree 2 it is 1 and so on which is what is expected, because this is the basis for that is x^j. So, in each degree it is going to be 1 and we ask for its Hilbert polynomial. And it gives a list, sorry it gives P_0 and it is a projective Hilbert polynomial; let us not worry about it now, it has to do with I mean, the word has to do with some projective geometry and which we will come to later, but right now we just. So, this P_0 is what we defined as P_0 in the lecture.

(Refer Slide Time: 10:25)

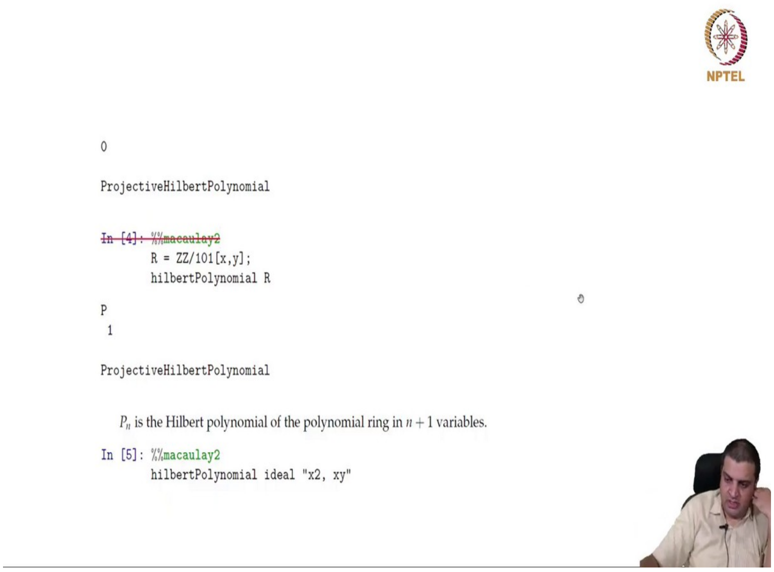


So, Hilbert function gives the length of the module in a specific degree. So, make it a habit if you see a command in macaulay2, that you do not know; make it a habit to look at its help. Look at its help or its methods that will tell you in which ways you can use it. So, P_0 is a Hilbert polynomial of a polynomial ring in one variable.

So, this is what we had; it is the constant polynomial 1. Let us look at the ideal $(x) \in R$; then we ask the same question; apply I, j goes to j , Hilbert function (j, I).

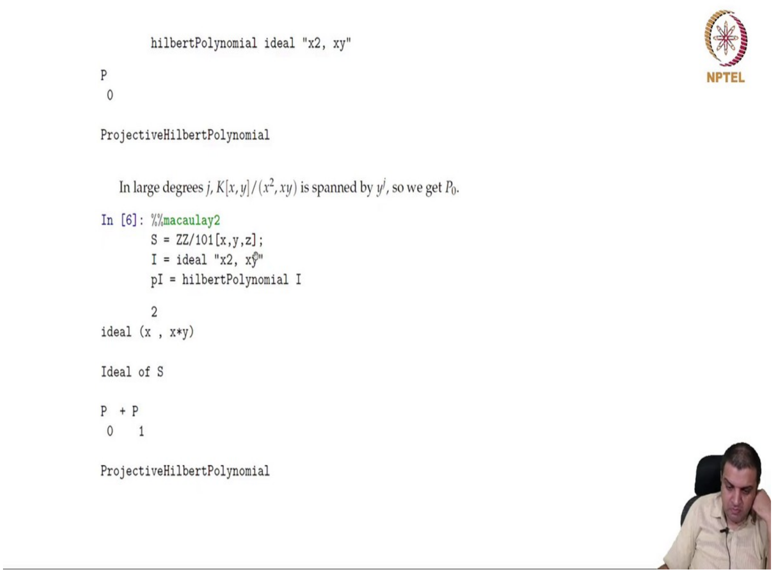
And just notice that for every $j \geq 1$, it is actually printing 0's. The first, in any ordered pair, the first is just j itself; second one is the value of the Hilbert function it print 0's. So, actually it is not the Hilbert function of I, it is a Hilbert function of the quotient then this printing.

(Refer Slide Time: 11:35)



So, please remember this, we ask for its Hilbert polynomial and it prints 0 and it says the projective Hilbert polynomial; it is a constant polynomial 0, again it is of the quotient, a polynomial in two variables. And ask for its Hilbert polynomial and it says P_1. So, this same notation as what we were using in the lecture. P_n is the Hilbert polynomial of the polynomial ring in n plus 1 variables, so it is.

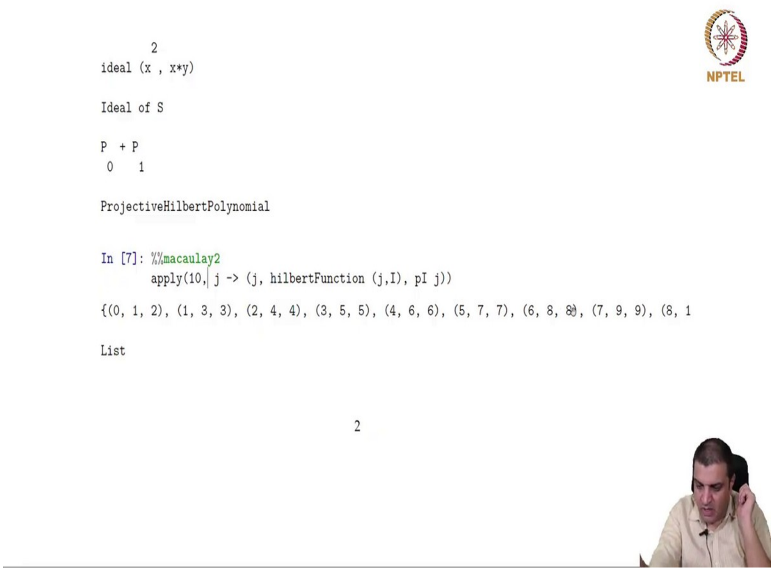
(Refer Slide Time: 11:59)



Now, we ask Hilbert polynomial of the ideal generated by (X^2, XY) and so, we get. So, remember the ring is ring is this in two variables. So, if you kill this ideal in degrees greater than or equal to 2, power of X would not be there and in degrees greater than or equal to 2, mixed terms involving XY will would not be there; then for only thing that would be left is just powers of Y.

So, is spanned by y^j. So, this it is again the constant polynomial 1 and therefore, we get P_0 that is what it said; Hilbert polynomial of, remember this is in the quotient. So, Hilbert polynomial of this is P_0.

(Refer Slide Time: 12:53)



Now, we change the ring just a little bit k[x, y, z] and $I=(x^2, x\,y)$ same polynomial Hilbert polynomial in a polynomial of I. So, then we get P_0+P_1; remember in the quotient now, there are also terms that would involve z. So, there will be powers of y and every multiple of z will be there in the quotient. So, we get a different number of Hilbert polynomial P_0+P_1.

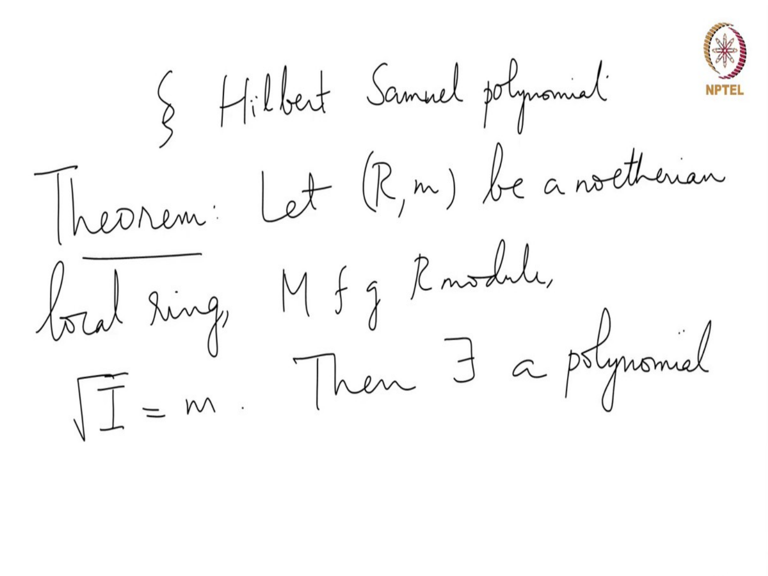
And so, this particular thing I have asked just for that one could refer to it later, I have called it pI. and in this here we ask for integers $0,\ldots,9$ print the I mean give list the values. This is just to keep track of the degree in each of these in the output. First give the Hilbert function of the quotient in degree j, and then give the value of the Hilbert polynomial in degree j.

So, out here we suddenly see that the Hilbert function does not agree with the Hilbert polynomial value; this is the correct one, because it is in degree 0, all that is left is the field. So, it has to be one dimensional and this 2 is some; it is a value of the polynomial, it need not be the Hilbert function.

But in this particular case, here after it agrees with the Hilbert polynomial in degree 1 it is a rank 3 vector space, it is spanned by x, y and z and the polynomial also takes value 3. In degree 2, there are 6 degree two vector space in 3 variable,so it 6 dimensional in which we have killed 2.

So, in the quotient there is 4 and that is what we will show is here and then one can this. So, it grows up linearly and that is why there is a P_1 ; it goes linearly, because we have not done anything to z. So, every multiple of z is there forever. So, that is, so the rank grows linearly and we see that in a P_1 . So, now we use these ideas to study local rings, a noetherian local rings; we use these ideas to study noetherian local rings.

(Refer Slide Time: 15:28)

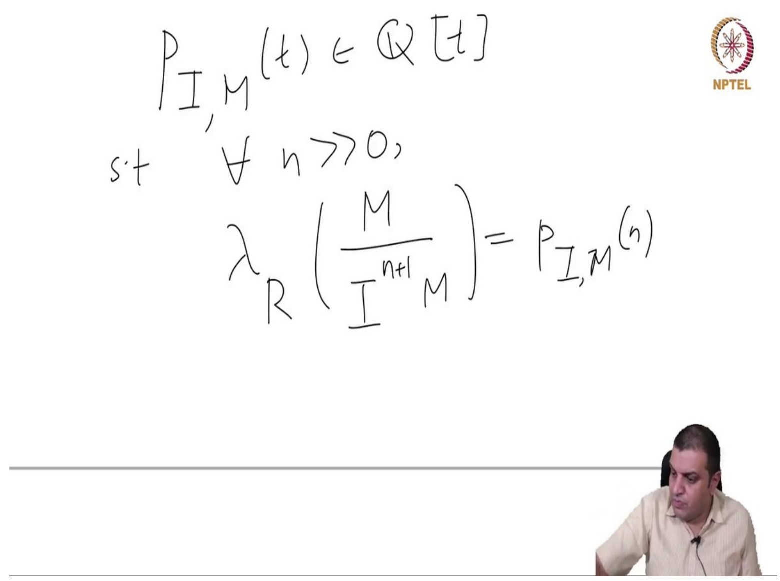


And so, the thing is called Hilbert Samuel polynomial. So, Hilbert polynomial, the study of this Hilbert function etcetera goes back to Hilbert. So, the beginning of the 20th century or around that time, turn of the century from 19th to 20th; but the (Refer Time:

15:45); local ring is there, structure etcetera were all from the middle of the last century Samuel and various other people.

And so, this is called Hilbert Samuel polynomial. So, here is a theorem. So, let me state the theorem and then we will try to set up and then prove it. Let (R, m) be a noetherian local ring; M finitely generated R-module, I an m-primary ideal. Remember saying that the radical of I is a maximal ideal is same thing as saying it is primary to that maximal ideal. So, we often write it and might just say m primary ideal; then there exist a polynomial.

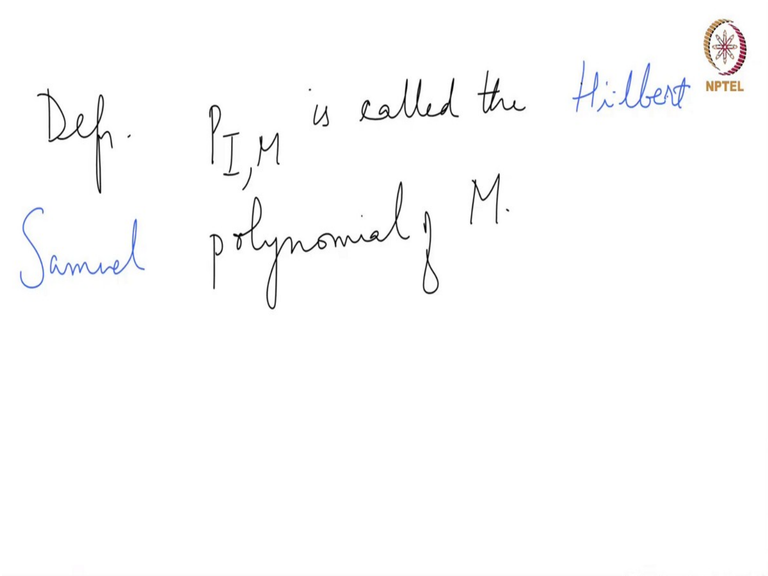
(Refer Slide Time: 17:04)



$P_{I,M}(t) \in Q[t]$ such that for all n>>0, $\lambda_R(\frac{M}{I^{n+1}M}) = P_{I,M}(t)$.

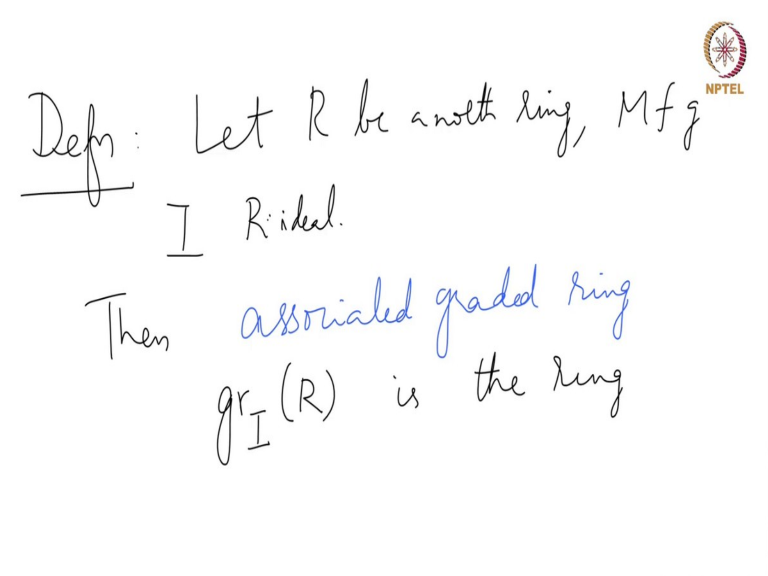
So, this is sort of a similar flavor as the Hilbert polynomial theorem, except there are no graded ring structure at this point; it is just a local ring and modules over it and then quotients. And the model that we will consider is this quotient, $\frac{M}{I^{n+1}M}$.

(Refer Slide Time: 18:09)



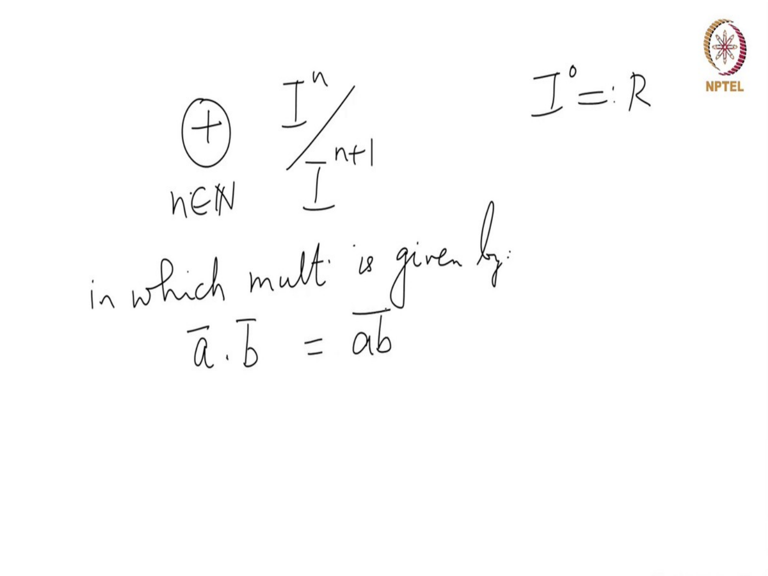
So, this is the thing. So, let us define this $P_{I,M}(t)$ is called the Hilbert Samuel polynomial, polynomial of M. So, when we prove, we will get some idea of what the, what is I mean; how many way degree etcetera . So, in order to prove this statement; we need to introduce a new object.

(Refer Slide Time: 19:04)



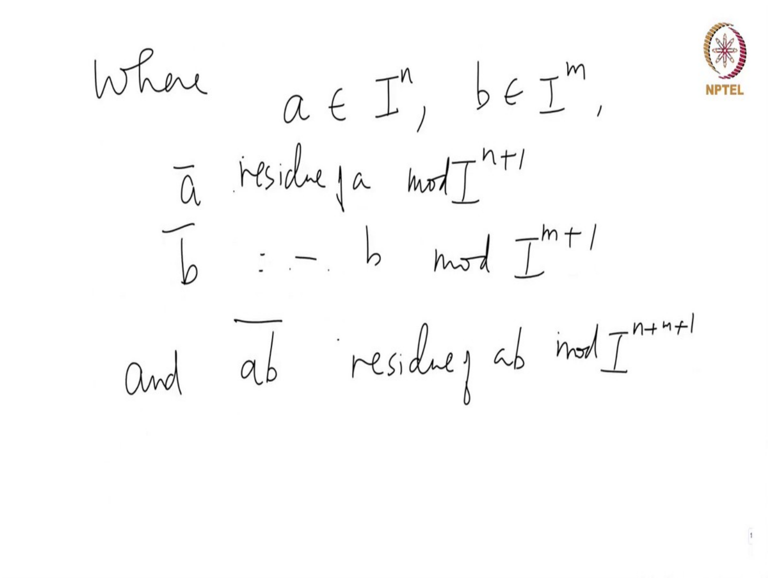
So, let R be a noetherian ring, M finitely generated and I an R ideal. Then the associated graded ring, $gr_I(R)$ is a graded ring.

(Refer Slide Time: 19:53)



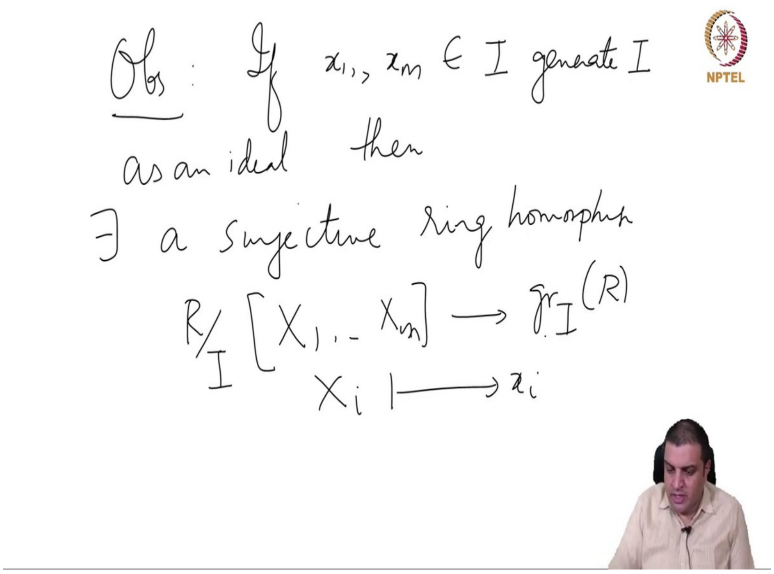
$\bigoplus_{n in N} \frac{I^n}{I^{n+1}}$. So, here I^0 by definition by that we mean R, So, we will define multiplication for homogeneous elements. $\bar{a}\,\bar{b} = \overline{ab}$;

(Refer Slide Time: 20:44)



Where $a \in I^n, b \in I^m$; $\bar{a}$ is residue of mod I^{n+1}, $\bar{b}$ is residue of b mod I^{m+1}, and ab in I^{n+m}, but $\overline{ab}$ is residue of ab in mod I^{n+m+1}. So, this is the definition of the associated graded, addition is just these are all abelian groups are. So, this is what we can. So, what do we need to do we use multiplication.

(Refer Slide Time: 22:08)

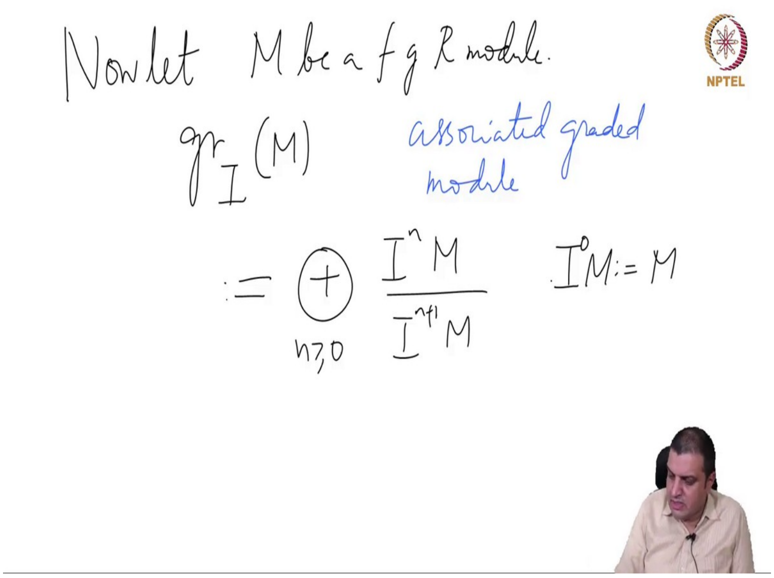


And the observation that we would like to make at this point is ; if $x_{1,} \ldots, x_m \in I$ generate I as an ideal, then there exists surjective ring homomorphism

$\frac{R}{I}[X_{1,} \ldots, X_n] \to gr_I(R)$; put variables enough of m of them to the associated graded ring, $X_i \to x_i$. So, this is the, this is the property; this need not be an isomorphism, there could be a things in the kernel, but there is definitely a surjective homomorphism.

Because in any degree, all that we need to generate is some product of these generators and there R linear combinations. But for the R-linear combination, we may as well assume that there are elements not inside I, so you can take work with the residues. And for getting the powers products of the generators, one can just use this map. So, the, there is a surjective homomorphism is what we use.

(Refer Slide Time: 24:05)

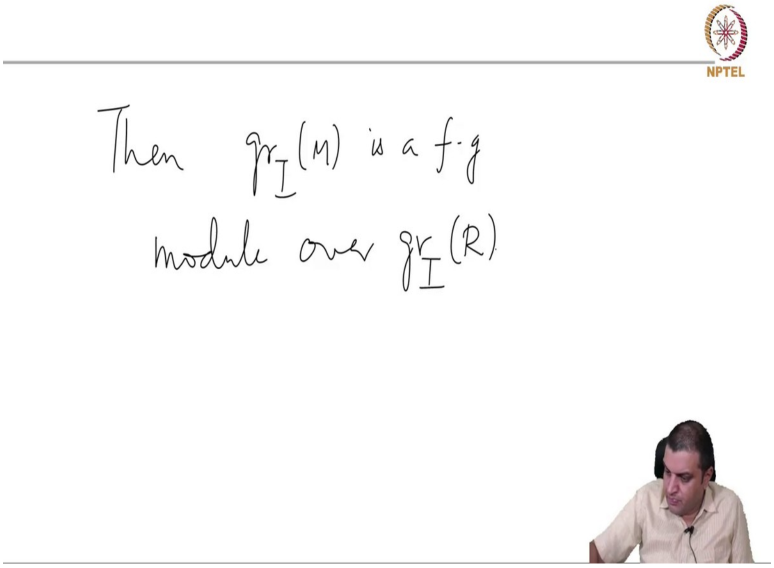


So, now let M be a finitely generated R-module ; then we can construct the corresponding associated graded module , given by $\oplus_{n \in N} \frac{I^n M}{I^{n+1} M}$

and M itself is not a graded module; R is some noetherian ring and M is some modulo over it, from which we can get this graded. when we say $I^0 M$ is by definition M.

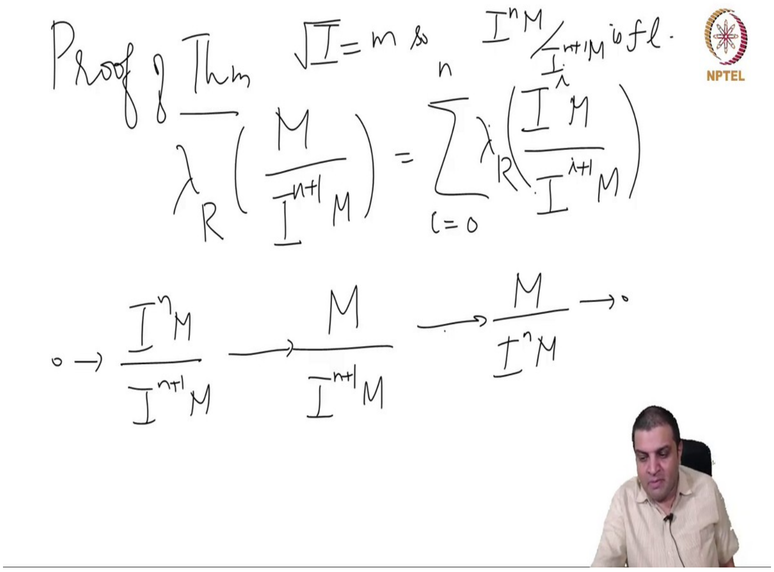
So, this is I get this thing. So, now, putting these, so, the observation is that; so we are assuming that M is finitely generated.

(Refer Slide Time: 25:15)



So, then the associated graded module is finitely generated module over the associated graded ring. So, now, let us prove the theorem. So, recall the theorem was here, we need to look at $\frac{M}{I^{n+1}M}$. So, the length of this. So, proof of the theorem

(Refer Slide Time: 26:08)

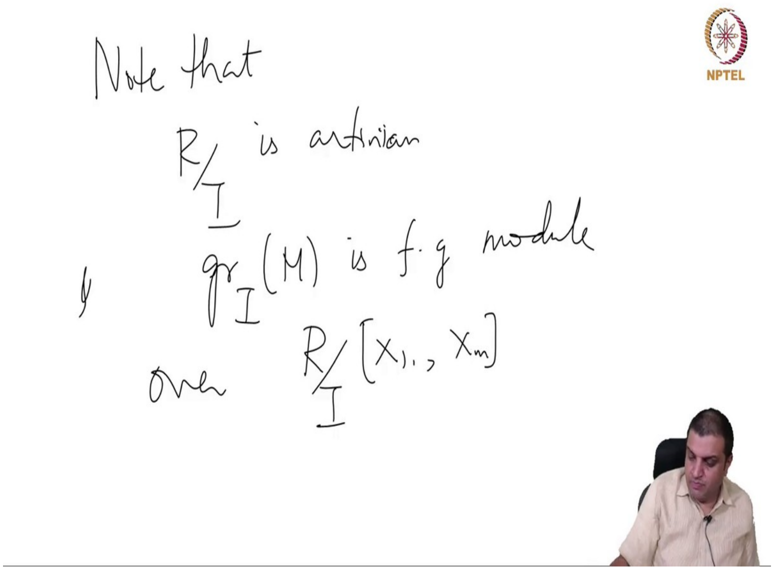


So, $\lambda_R(\frac{M}{I^{n+1}M}) = \sum_{i=0}^{n} \lambda_R(\frac{I^i M}{I^{i+1}M})$. That is because, this is, this can be prove by induction on n. So, let us look at the last step in the induction. So, the last step in the induction would be let us write it as a short exact sequence, $0 \to \frac{I^i M}{I^{i+1} M} \to \frac{M}{I^{n+1} M} \to \frac{M}{I^n M} \to 0$ So, therefore, there is this surjective map and the kernel of this map is $\frac{I^i M}{I^{i+1} M}$. So, recall that, in the theorem I is m-primary. So, $\frac{I^i M}{I^{i+1} M}$ is finite length. So, we can talk about length and then by induction, this is equal to the corresponding sum all the way up to n- 1; and then for n we add this, we get the length of this thing.

All of these are finite length modules, length is additive in an exact, short exact; I mean the middle length of the middle one is the sum of the lengths of the outer two and therefore, the length of this is these two and then by induction one can show this. So, now there is a polynomial.

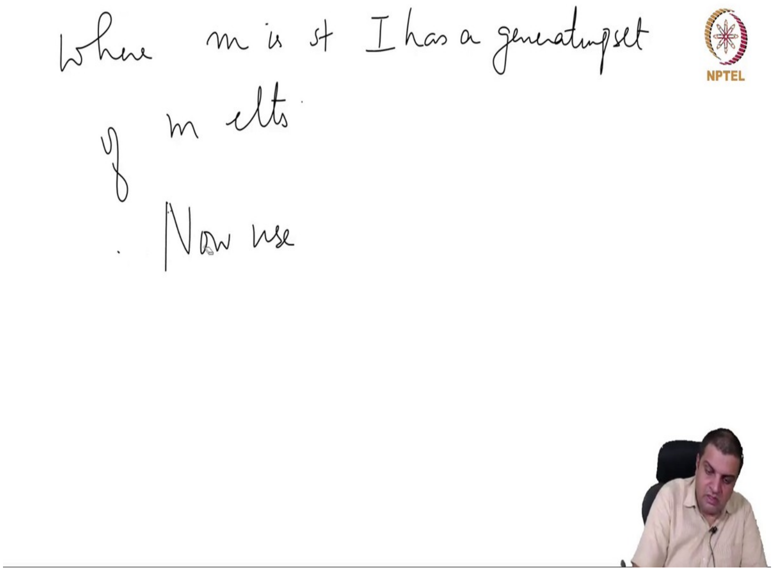
So, notice that this is the graded part of the. So, this $\frac{I^i M}{I^{i+1} M}$ this is the graded, I th graded part of the associated graded module, which is a finitely generated module over a the polynomial ring over $\frac{R}{I}$ which is Artinian. Note that $\frac{R}{I}$ is Artinian.

(Refer Slide Time: 28:37)



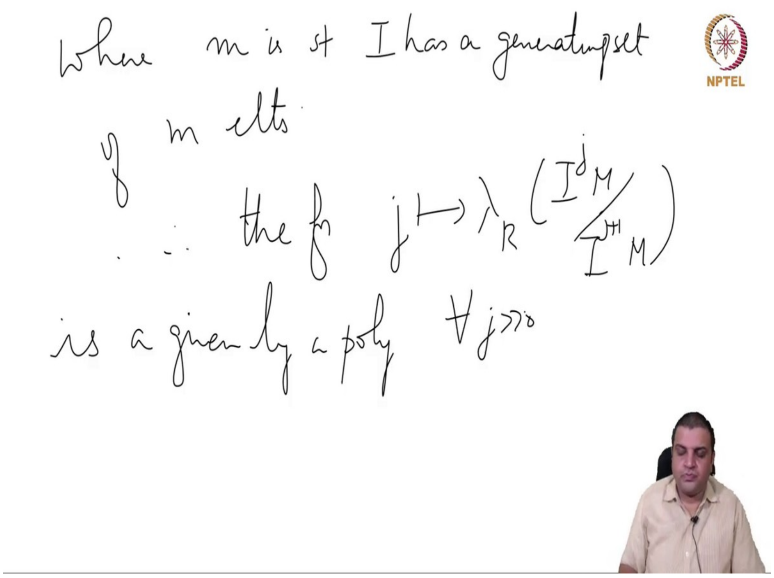
And the $gr_I(M)$ is finitely generated module over $\frac{R}{I}[X_1, \ldots, X_m]$, where m is such that I has a generating set of m elements.

(Refer Slide Time: 29:05)



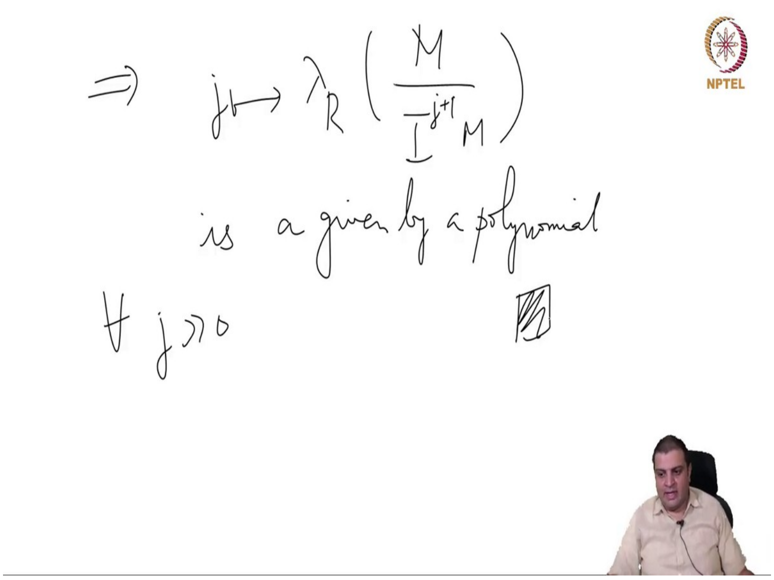
So, this is a finitely generated module over that . So, therefore, by the previous theorem, which is about the existence of Hilbert polynomial for modules over such rings; each degree piece eventually is given by a polynomial. And using the same argument as earlier, this length is also given eventually by a polynomial; there will be an initial part where the polynomial would not agree, but afterwards it will agree with the polynomial.

(Refer Slide Time: 30:10)



So, now therefore, now use the previous result. So, maybe I should just write; therefore the function $j \to \lambda_R(\frac{I^j M}{I^{j+1} M})$ is given by a polynomial for all sufficiently large j which now implies that, the function $j \to \lambda_R(\frac{M}{I^{j+1} M})$

(Refer Slide Time: 30:36)



is given by a polynomial, for all sufficiently large j. So, this is the end of this proof. So, in the next lecture, we will prove that the degree of the polynomial does not depend on the ideal. And that is therefore, an invariant of the module itself. And then we will relate these two dimension. So, that is the, that would be the in the next few lectures.