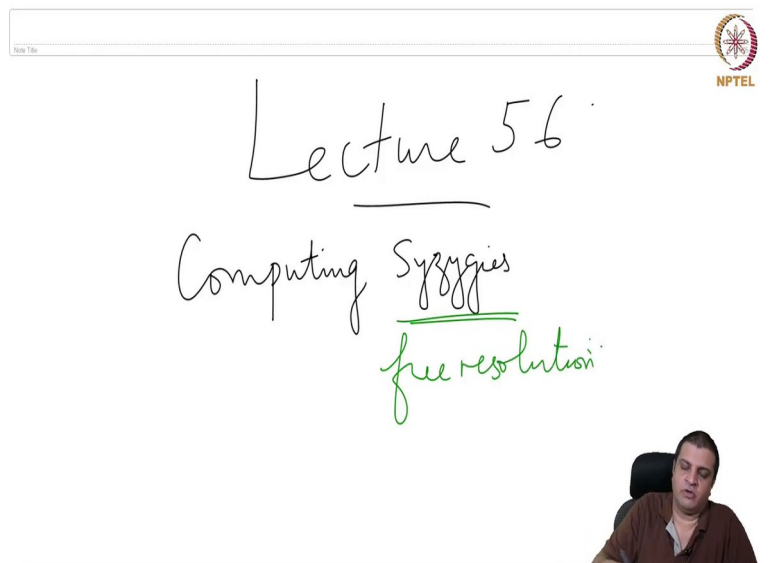


Computational Commutative Algebra
Prof. Manoj Kummini
Department of Mathematics
Chennai Mathematical Institute

Lecture – 56
Computing syzygies

(Refer Slide Time: 00:15)



The slide features a white background with a thin horizontal line at the top. In the top right corner, there is a small circular logo with a star-like pattern and the text 'NPTEL' below it. The main content is handwritten in black and green ink. 'Lecture 56' is written in black, underlined. Below it, 'Computing Syzygies' is written in black, with 'Syzygies' underlined. Underneath that, 'free resolution' is written in green. In the bottom right corner, there is a small video inset showing a man with short dark hair, wearing a brown shirt, sitting in a black chair and looking towards the camera.

Welcome. This is lecture 56 and in this we go back to our Groebner basis things and then we will see we saw how it could be used to compute syzygies for an ideal. So, this is mostly an overview of things that we will not prove, but at least to discuss how one could use this to compute a free resolution not just the; not just the syzygy of an ideal. So, I mean really when I meant here at this point when I meant syzygies I meant I mean we do mean free resolution all of them syzygies then the syzygies of them and so on.

(Refer Slide Time: 01:03)


In an earlier lecture we
saw how Gröbner basis
was used to construct syzygies of an ideal
Generalize to submodules of free modules
(f.g.)



So, in an earlier lecture we saw how a Groebner basis was used to construct syzygies of an ideal and we so, far we only looked at computing Groebner basis for ideals, but it can actually be generalized to not all modules, but sub-modules of free modules, how is that done? So, remember an ideal itself ideal also is a submodule of a free module it is a submodule of a free module of rank 1.


So, that is and again this is this would be finitely generated at least for us we would not worry about arbitrary (Refer Time: 02:27) . So, I will just briefly give an overview of how this can be done . It is essentially just rewriting everything that we did for ideals in terms of modules. So, it is also way for us to recap how I mean one proceeded with ideals.

(Refer Slide Time: 02:46)



Let $F = \bigoplus_{i=1}^r R e_i$ $\{e_1, \dots, e_r\}$ basis


By a **monomial** in F , we mean
 an elt of the form $X_1^{a_1} \dots X_n^{a_n} e_i$
 for some $a_1, \dots, a_n \geq 0, 1 \leq i \leq r$



So, let $F = \bigoplus_{i=1}^r R e_i$ be a free module with a given basis $\{e_1, \dots, e_r\}$ of rank r . By a monomial of F , we mean an element of the form $X_1^{a_1} \dots X_n^{a_n} e_i$ for some $a_1, \dots, a_n \geq 0, 1 \leq i \leq r$. So, this is what we mean by a monomial in F .

So, it is exactly like a monomial ideal it is exactly a monomial in the polynomial ring R , it is just. A monomial submodule of F is a submodule generated by monomials of F .


(Refer Slide Time: 04:19)



A **monomial** submodule of F is
 a submodule generated by
 monomials in F .

Let M be a monomial submodule.

Then $M_i := \{r \cdot e_i \mid r \cdot e_i \in M\}$
 is a submodule of M



Now, if we have a monomial sub module then generators would be of this kind let us collect

all the generators with a fixed e_i . If you multiply them by elements of R we would get all R -linear combinations of these monomials in other words we will get a monomial ideal just the.

If we just look at all elements in the monomial submodule where which involves only one term e_i and arbitrary R -linear combinations. So, we would just get some element in a monomial ideal times e_i that is a first observation. So, I will write them, but let me finish the.

So, let M be a monomial sub-module. Then $M_i = \{r e_i : r e_i \in M, r \in R\}$. of course, it is a sub module sub module of M and is of the form $I_i e_i$ for some monomial ideal I_i inside R .

(Refer Slide Time: 06:30)

And is of the form $I_i e_i$ for some monomial ideal $I_i \subseteq R$.



$$M_i \cap M_j = 0 \quad \forall i \neq j$$

$$M = M_1 + M_2 + \dots + M_r$$

$$\Rightarrow M = \bigoplus_{i=1}^r M_i$$



That is because we take a generating set in which a generating set for M which involves monomials. We fix a monomial generating set for M and in that pick out all the ones that have this e_i and then our linear combinations would just be combinations of that. So, this is the first observation that we want to make.

Secondly, $M_i \cap M_j = 0$ for all $i \neq j$ that is clear because all of these are multiples of e_i , all of these are multiples of e_j and they cannot have an intersection. And thirdly, $M = M_1 + M_2 + \dots + M_r$ and this now says that $M = \bigoplus_{i=1}^r M_i$. So, in other words conversely if M is a direct sum of such things then M is a monomial sub module.

(Refer Slide Time: 08:01)

$M \subseteq F$ is a monomial submodule
 \Updownarrow
 $\exists I_1, \dots, I_r$ monomial ideals in R st
 $M = I_1 e_1 \oplus \dots \oplus I_r e_r$



So, a monomial submodule is. So, $M \subseteq F$ is a monomial submodule if and only if there exist I_1, \dots, I_r monomial ideals in R such that . Each of them is a sub module of the corresponding factor inside here and then the direct sum of that is M . So, this is what we just wanted to observe.

(Refer Slide Time: 08:52)

Can define a monomial order
on F analogous to R
of F total order on the set of
monomials that respects mult
by monomials of R .



So, now, we can define a monomial order. So, a monomial order on F analogous to R how it is done on R . Meaning we have to give a total order on the set of monomials that respects multiplication. So, total order on the set of monomials that respects multiplication. So, these

are monomials of F that respects multiplication by monomials of R and these are monomials of R .

(Refer Slide Time: 10:05)

Eisenbud's comm. alg. book.
Analogue of Buchberger theorem.
Let $g_1, \dots, g_t \in F$ non-zero
For



So, by the way I should have stated this, this description in this generality is there in Eisenbud's book. Eisenbud's one of the references that I had given. Not every book discusses this in that generality, but there discussing it for ideals is not enough to describe how syzygies would be how a free resolution would be computed.

So, then we have an analogue of Buchberger theorem. I mean all those things analogue of Buchberger theorem. So, let us briefly review how that is. So, F as above and let $g_1, \dots, g_t \in F$ non zero elements for $i \neq j$ (Refer Slide Time: 11:16)

1, ..., n-1
 Let $g_1, \dots, g_t \in F^0$ nonzeros



For $i \neq j$, define

$$m_{ij} = \frac{\text{lcm}(\text{in } g_i, \text{in } g_j)}{\text{in } g_i}$$



define $m_{ij} = \frac{\text{lcm}(\text{in } g_i, \text{in } g_j)}{\text{in } g_i}$.

(Refer Slide Time: 11:52)

$$m_{ij} = \frac{\text{lcm}(\text{in } g_i, \text{in } g_j)}{\text{in } g_i}$$



Division algorithm gives:

$$m_{ij}g_i - m_{ji}g_j = \sum_u q_u^{(ij)} g_u + r_{ij}$$

with no term of r_{ij} div by $\text{in}(g_u)$ for any u



So, this is and for each. So, then division algorithm, I mean not division algorithm, but the consequence. So, there is a division algorithm in this context division algorithm gives $m_{ij}g_i - m_{ji}g_j$. So, this is the S polynomial this would be the analogue of the S polynomial in


the ideal case, this is of the form $\sum_u q_u^{ij} g_u + r_{ij}$. So, we are expressing the s polynomial in terms of the other I mean in terms of the generators not necessarily other generators, but the

generators plus some r_{ij} .

And again we have seen this r_{ij} need not be unique, but one can ensure that no term of r_{ij} is divisible by the initial term of any g_u . So, with no term of r_{ij} divisible by $\text{in}(g_u)$ for any u . So, we can all this is just the same thing that we did for modules for ideals. So, we can write it like this and then the Buchberger criterion is. Buchberger criterion, the theorem.

(Refer Slide Time: 13:35)

Buchberger theorem:
 $\{g_1, \dots, g_t\}$ is a Groebner basis
 for the submodule F generated by it i.e.,
 $\{\text{in}(g_i) : 1 \leq i \leq t\}$
 \Downarrow
 $r_{ij} = 0 \quad \forall i \neq j$ generates the submodule




That I mean Buchberger's theorem was for ideals, but it can be generalized like this $\{g_1, \dots, g_t\}$ is a Groebner basis for the submodule of F for the submodule of generated by it if and only if $r_{ij} = 0$, for all $i \neq j$. Same I mean we compute this and it is it becomes a Groebner basis exactly when this remainder is 0 and if the remainder is.

So, the algorithm is we compute this, the remainder is nonzero then add that also to the list of to the set G and then we do redo all the calculation once more and then we check if there is any leftover remainders and then we add and so on.

So, and what does this mean? I mean what does it mean Groebner basis for the sub module? So, it means exactly what it had meant earlier that is $\{\text{in}(g_i) : 1 \leq i \leq t\}$ generates the submodule generated by generates the submodule of F generated by the initial terms of all the elements in M .

(Refer Slide Time: 15:46)

the submodule F generated by
 $\{in(g) \mid g \in M\}$.



Now we have constructed
 a Groebner basis for M .



So, exactly analogous to what we do for ideals one can prove the statement and we will. So, we will not attempt to prove it. So, this is. Now, the key point in this. So, this is just describing how to compute. So, now, we have constructed. So, now, we have constructed a Groebner basis for M and then it means that.

(Refer Slide Time: 16:49)

a Groebner basis for M .
 $G = \{g_1, \dots, g_t\}$



$$\therefore \forall i \neq j, \quad m_{ij}g_i - m_{ji}g_j = \sum_u q_u^{(ij)} g_u$$



So, therefore, for all i, j . So, let us say this Groebner basis is $\{g_1, \dots, g_t\}$, then for $i \neq j$ we have

$$\text{this } m_{ij}g_i - m_{ji}g_j = \sum_u q_u^{ij} g_u$$

that is precisely when it is a Groebner basis.

(Refer Slide Time: 17:33)

$$\begin{aligned} \therefore \forall i \neq j, \\ m_{ij} g_i - m_{ji} g_j = \sum q_n^{(ij)} g_n \\ \leadsto \text{gives a syzygy} \\ \text{Repeat this for the kernel of } \epsilon. \\ F_1 \xrightarrow{\epsilon} M \subseteq F. \end{aligned}$$



So, this gives us a syzygy right this can be rewritten as a relation. So, this gives a syzygy and the theorem is that all syzygies are generated like this. So, this tells us what is the kernel of the surjection and then from that we can construct a presentation matrix and so on and so, we can proceed.

. So, repeat this for the kernel of. So, remember $M \subset F$ some F_1 surjects onto M because we can choose a Groebner basis like this and then we know what the we will get a surjective map and then we repeat this for the kernel of this map.

So, let us just call this thing ϵ repeat this for the kernel of ϵ . So, I mean this thing tells us the kernel of ϵ and then repeat the same thing compute the Groebner basis and so, on and then repeat this and that would give us a free resolution. Now, in theory this will also prove Hilbert's Hilbert syzygy theorem, but we need a technical statement for that.

(Refer Slide Time: 19:05)

In principle, one can prove
Hilbert's syzygy theorem this way:



Key point: For every $f.g.$ R -module M ,
 $\beta_{i,j}(M) \geq \beta_{i,j}(\mathcal{L}(M))$



So, in principle one can prove a Hilbert's syzygy theorem this way. How? Well, we need a key point which we will not be able to prove this is a this requires some development of what is called flatness. For every finitely generated R -module M , the graded Betti numbers $\beta_{ij}(\mathcal{L}(M)) \geq \beta_{ij}(M)$.

So, this needs a way to be able to move from M to $\mathcal{L}(M)$ in some control fashion in which you can compare the free resolutions, the ranks of the free modules in the free resolution. So, this is well beyond our scope now.

(Refer Slide Time: 20:37)

Reduce the proof of Hilbert's syzygy theorem
to monomial submodules.



$$\bigoplus_{i=1}^r I_i e_i \quad \{e_1, \dots, e_r\} \text{ basis of } F$$


Reduce to monomial ideals.



So, but, there is such a result. So, with this we can actually now reduce to monomial sorry reduce meaning reduce a proof of reduce the proof of Hilbert's syzygy theorem to monomial submodules of M but what do they look like?

They look like $\bigoplus I_i e_i$ where you know F has basis $\{e_1, \dots, e_r\}$. So, this is basis of F , but this is this direct sum as direct sum of modules and it is not very difficult to check that if you take minimal resolution of each one of the components, the direct sum of the complexes will give a direct resolution of the free resolution of the direct sum. So, therefore, further we reduce to monomial ideals to each component of this and then this is just something dummy you can just treat just have to prove for I_i .

(Refer Slide Time: 22:17)

WTST for a monomial ideal $I \subseteq R = k[x_1, \dots, x_n]$ 
 I has a minimal free resolution length $\leq n$
 I monomial ideal is a prime ideal
 $\Leftrightarrow I = (x_{i_1}, \dots, x_{i_c}) \quad 1 \leq i_1 < \dots < i_c \leq n$



So, we want to show that for a monomial ideal $I \subseteq R$, I has a minimal free resolution of length n , n is the number of variables. In fact, I mean there are explicit description of what a free resolution would be; it need not be minimal, but at least we can prove this statement from that.

So, this is not I mean there are concrete descriptions of non-minimal free resolutions or more correctly not necessarily minimal free resolutions of length less than n . So, definitely a minimum resolution will have length less than n . So, one can prove this, but I would like to do it in a slightly different way which will motivate us to for the next lecture.

So, if I is not prime let us ask. So, I monomial ideal when will I be a prime? Well if it

involves an if a minimal generating set involves an actual monomial meaning a monomial of degree at least two, then it cannot be prime because that would it would be something of the form some $X_i X_j X_k$, but if that in that case either X_i or X_j or X_k has to be inside here.

So, is a prime ideal if and only if I is generated by something of the form X_{i_1}, \dots, X_{i_n} , $1 \leq i_1 \leq \dots \leq i_n$. It is generated by a bunch of variables the subset of the variables. So, this is only when it is prime.

(Refer Slide Time: 24:28)

If I is not prime, choose a variable $X_i \notin I$. & X_i divides a monomial minimal generator of I

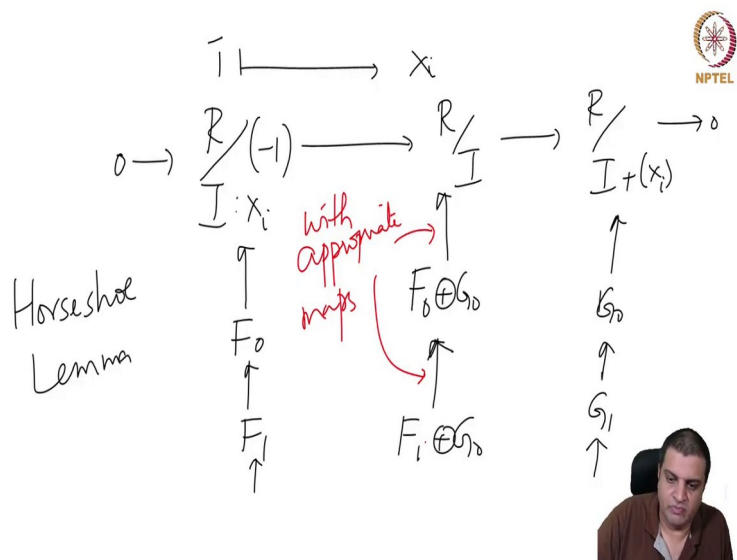


$$\begin{array}{ccc} (I : X_i) & \cap & I + (X_i) = I \\ \cap & & \cap \\ I & & I \end{array}$$



if I is not prime choose a variable $X_i \notin I$ and X_i divides a monomial minimal generator of I such thing will exist then check that $I : X_i$. So, this will be an exercise intersect. So, this will be strictly bigger than I and $I + (X_i)$ this will also be strictly bigger than equal to I . So, this you will do as an exercise.

(Refer Slide Time: 25:31)



So, now, we have a we have an exact sequence $0 \rightarrow \frac{R}{I: X_i} \rightarrow \frac{R}{I} \rightarrow \frac{R}{I+(X_i)} \rightarrow 0$. So, this is great degree preserving an element of homogeneous element here goes to a homogeneous and its residue class of same degree here. So, this degree preserving, in order to make this degree preserving the 1 bar here has to go to X_i . So, in order to make this degree preserving the generator here has to be in degree 1. So, now, this is degree preserving.

So, now, there is a standard construction homological algebra called horseshoe lemma which you will work out as an exercise. If you have a resolution like $\rightarrow F_1 \rightarrow F_0 \rightarrow I$ mean and say $\rightarrow G_1 \rightarrow G_0 \rightarrow$ one can construct a resolution for the middle term by taking $F_1 \oplus G_0 \rightarrow F_0 \oplus G_0$ appropriate maps, maps are not obvious.

I mean one can work it out, but they are not their maps are not just direct sums and so on, so with appropriate maps. So, this will be in the exercises to figure out what the map should be. So, there is more there is actually which we will see later what is called a map of complexes which we will see in the next lecture, but there is such a thing. So, in other words if this has length less than or equal to n and this is length less than or equal to n this also has length less than or equal to n .

(Refer Slide Time: 27:31)

\therefore By noetherian property,
 we may assume the result
 for $I : X_i, I + (X_i)$
 By horseshoe lemma true for I



So, therefore, we can. So, if you choose i to be maximal where it is not less than or equal to n by noetherian we these two things are less than or equal to n . So, by noetherian property we may assume that assume the result for $(I : X_i)$ and $I + (X_i)$ by horseshoe lemma it is also true for I . So, this work I mean this argument work precisely because it is not prime.

(Refer Slide Time: 28:25)

\therefore May assume I is prime
Example $I = (X_1)$
 $0 \rightarrow R(-1) \xrightarrow{\cdot X_1} R \rightarrow 0$
 $I = (X_1, X_2) \rightarrow R(-2) \xrightarrow{\begin{bmatrix} -X_2 \\ X_1 \end{bmatrix}} \bigoplus_{R(-1)} \xrightarrow{\begin{bmatrix} X_1 & X_2 \end{bmatrix}} R \rightarrow 0$



So, then now, therefore, we can assume it is prime. So, now, we have to handle the prime case. So, therefore, may assume I is prime. So let us take a couple of examples and this will be; this will be done using what is called Koszul complex. So, let us say $I = (X_1)$. So, this for

now it is just an example we will do this properly in the next lecture.

So, then here is what we could do. We could take I we could take $0 \rightarrow R(-1) \xrightarrow{x_1} R \rightarrow 0$ it has to be injective I mean it will be injective this is a domain and then 0. This is the resolution for one variable. If you have two variables $I=(X_1, X_2)$ then the resolution is $0 \rightarrow R(-2) \rightarrow R(-1) \oplus R(-1) \rightarrow 0$

So, the kernel of this one can verify again that. So, I will explain the shift here, but the kernel here again the same idea $R_1 e_1 + R_2 e_2 = 0$ means $R_1 X_1 + R_2 X_2 = 0$, X_2 and X_1 are irreducible elements not multiples of each other. So, then X_1 has to divide R_2 and X_2 has to divide R_1 and then we would get this.

It is the same argument that we did in the earlier example in the previous lecture. So, this is a this it is a free resolution in two variables these are examples of what is called Koszul complexes. So, in the next lecture we will look at Koszul complexes try to understand the construction behind them. Again it will require some detour into homological techniques, you could use this as a motivation to study more homological algebra. So, this is the end of this lecture.