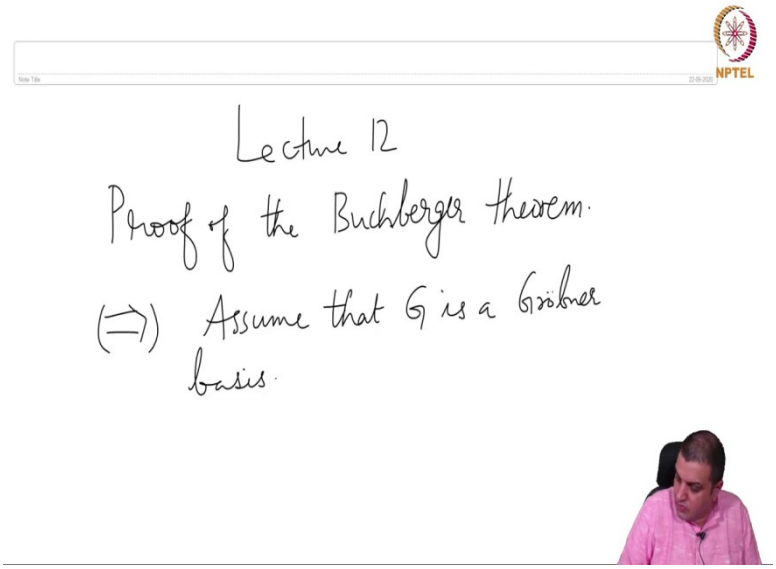
Computational Commutative Algebra
Prof. Manoj Kummini
Department of Mathematics
Chennai Mathematical Institute

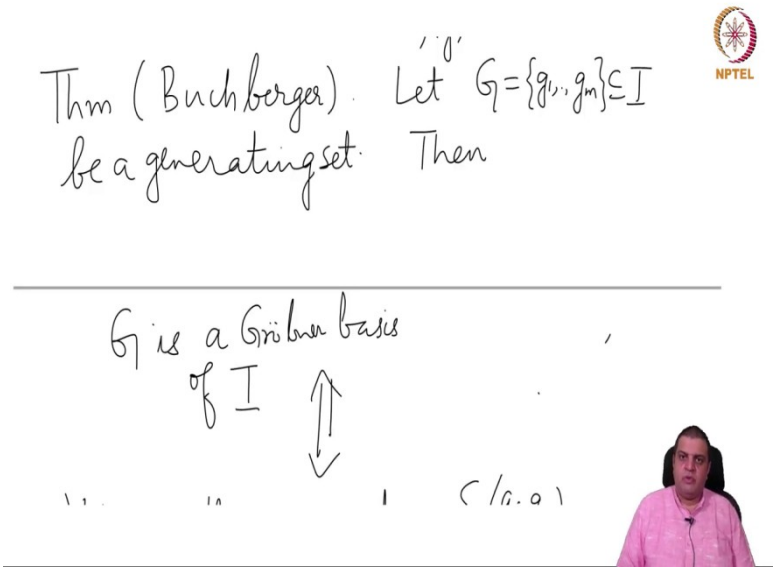
Lecture - 12
Buchberger criterion

(Refer Slide Time: 00:16)



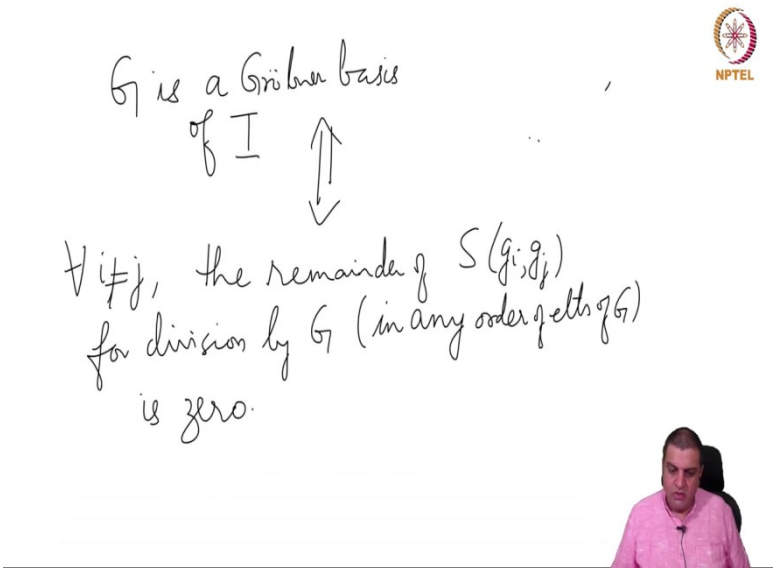
This is the 12th lecture in the series and in this lecture we will prove Buchberger theorem.

(Refer Slide Time: 00:24)



So, this was a theorem that we mentioned in the last lecture. So, I is an ideal in the polynomial ring in n variables over a field k, no assumption on k other than that it is a field and G is a generating set, $G=\{g_1, g_2, \ldots, g_m\}$.

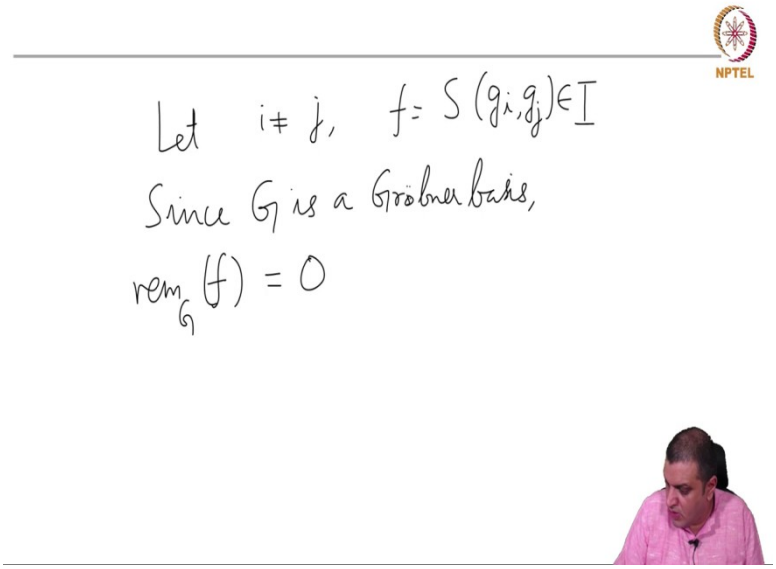
(Refer Slide Time: 00:52)



Then G is a Grobner basis precisely when for every pair i and j the remainder of $S(g_i, g_j)$ when we divide this by elements of G in any order of elements of G the remainder is 0. So, this is a characterization of something being a Grobner basis for I.

So, now let us prove this statement. So, one direction is more straightforward than the other, I mean in fact, quite straightforward so this is the direction. So, assume that G is a Grobner basis.

(Refer Slide Time: 02:04)



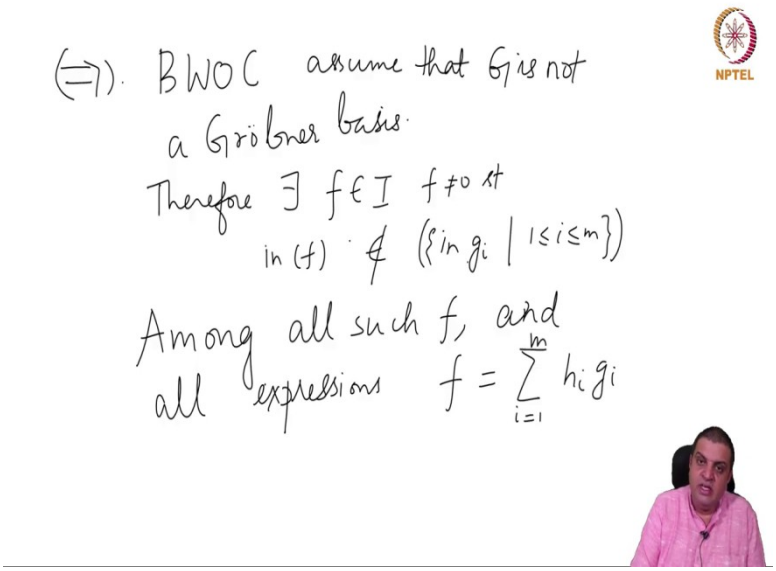
Let i be different from j, and let $f = S(g_i, g_j)$. Recall from the definition of $S(g_i, g_j)$ first you multiply g_i by some monomial, then you multiply g_j by some monomial, and then you take the difference to remove the leading term. So this is inside I. But if f is inside I, we divide f by elements of G, because G is a Grobner basis.

We know that the remainder of G will not depend on the order and which we divide or it is completely independent of what the coefficients of the g's are, the remainder is independent. And f is inside I means that the remainder of this is the characterization of f being inside I. So, this is the proof from one direction.

It is just an old result about which we proved many lectures ago that if something is a Grobner basis, then the remainder is a well-defined quantity irrespective of the order etc and an element is inside I precisely when the remainder is zero. So, this is the easy direction of that theorem.

Now, in the other direction, one needs to prove that it is a Grobner basis. So, we have to prove that for any f, ¿f is divisible by ¿g_j for some j that is what it makes a Grobner basis.

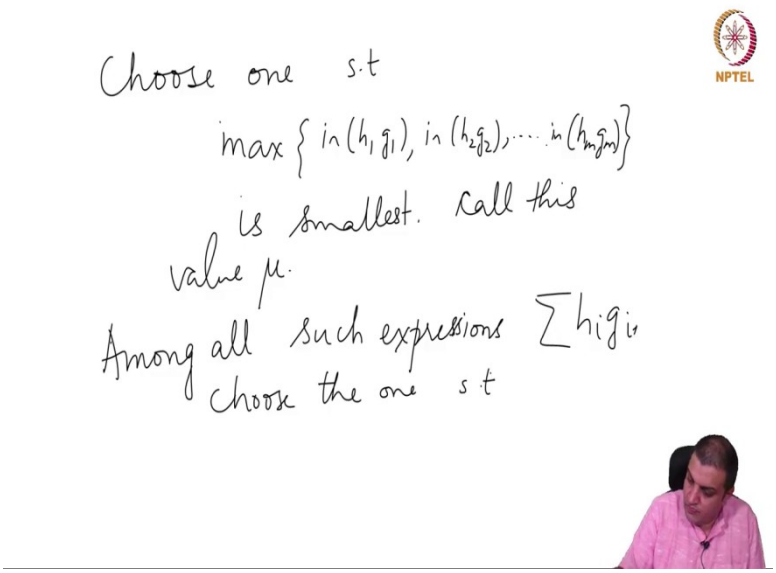
(Refer Slide Time: 04:15)



So, now by way of contradiction, assume that G is not a Grobner basis. Therefore, there exists some $f \in I$ nonzero such that ¿(f) is not in the ideal generated by ¿$(g¿¿i)$¿ for $1 \leq i \leq m$. So the initial terms of g_i do not generate the initial ideal that is what we are assuming. So, there is an f with this property. Now, we are going to make some choice about f, and we will prove that with some property there is a contradiction.

Among all such f, and all such expressions $f = \sum_{i=1}^{m} h_i g_i$. Remember f is in I and the set g_i generates the ideal that is the hypothesis, but it is not a Grobner basis. So, f can be written in terms of the g_i's, but ¿(f) cannot be written in terms of the ¿(g_i)'s that is this hypothesis.

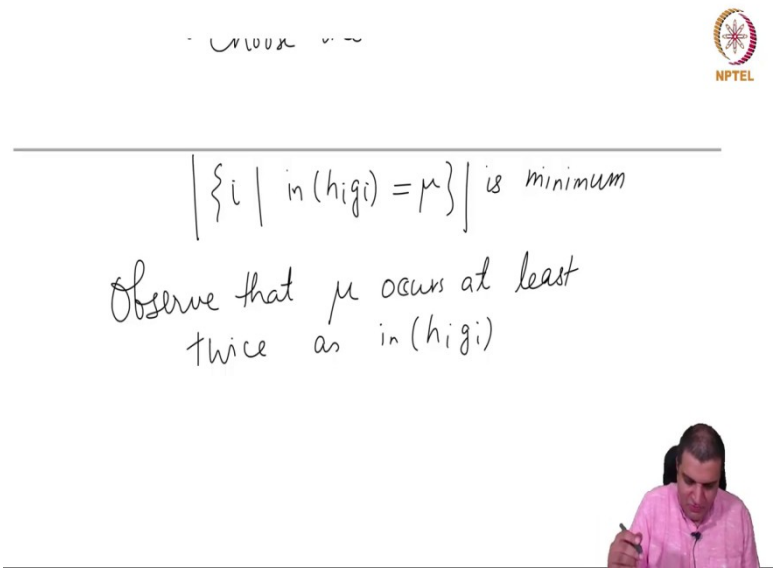
(Refer Slide Time: 06:43)



So, among all such f and all such thing choose one such that $max\{\in h_1 g_1, \in h_2 g_2, \ldots, \in h_m g_m\}$ is smallest, call this value μ. Let us go back and say what this means, what is being said.

So, there is some f with this property. f itself is can be written like this. So, for any such expression compute this maximum of the initial terms of the individual terms in the sum $h_i g_i$, choose one that is smallest, and call that smallest value μ, so that is one thing. Now, it is possible that many of the i such that ¿$h_i g_i = \mu$.

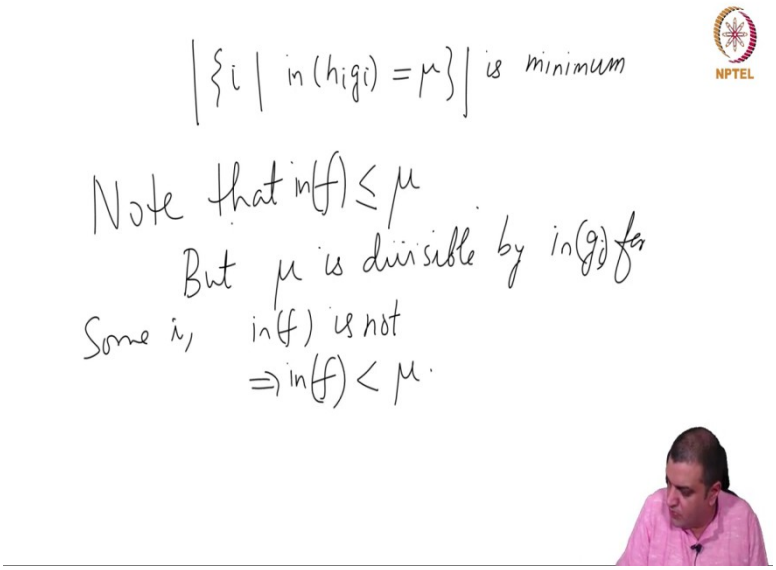
(Refer Slide Time: 09:43)



So, among all such expressions as above choose the one in which the cardinality the set $\{i \mid \in h_i g_i = \mu\}$ is minimum. So, the idea of the proof would be given such an f and such an expression which also determines μ and this number, either this set becomes smaller or m becomes smaller. Either way we have contradict to the choices and that would be the end of the proof.

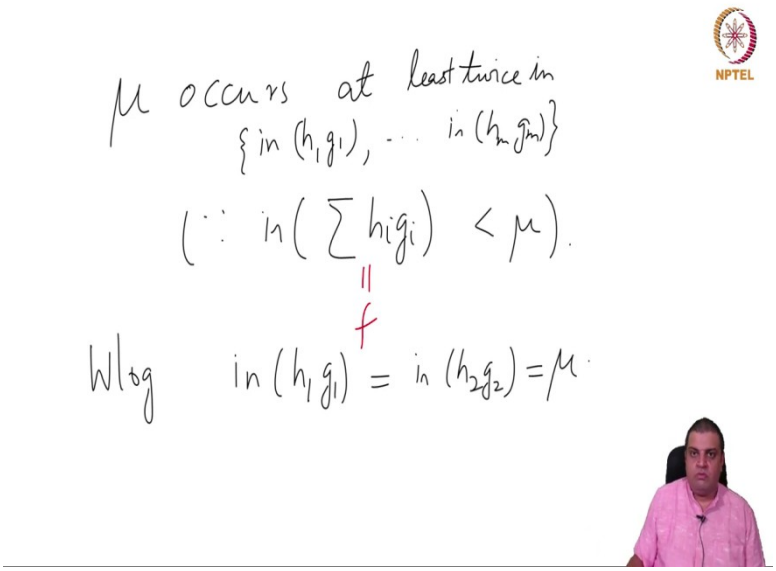
So, what is the relation between the maximum of ¿ $h_i g_i$ and f? So, the sum of $h_i g_i$ gives f. So, the maximum here is less than or equal to the maximum of the initial term here is less than or equal to the maximum of the initial terms of the sum. There may be cancellations, but the initial term of this cannot be greater than the initial term of every one of these things. So, that maximum is μ. So, ¿ f is less than or equal to μ that is sort of by definition. But we can say more ¿ f is less than or equal to μ that initial term here is μ.

(Refer Slide Time: 12:12)



So ¿ f is less than or equal to that, but we can say more because μ is divisible by ¿ g_i for some i, but ¿ f is not. The assumption was ¿ f is not in the initial ideal. So, it is not divisible by the initial terms of the elements of the generator of those g_i. So, this now implies that ¿ f is strictly smaller than μ.

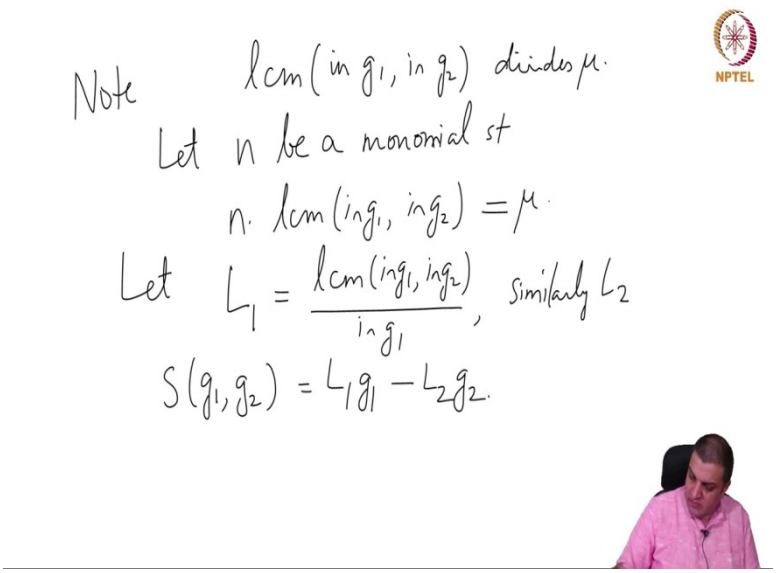
(Refer Slide Time: 13:17)



So, now, let us observe that μ occurs at least twice in the collection $\{\in h_1 g_1, \in h_2 g_2, \ldots, \in h_m g_m\}$. Because if it appear only once, let us say it appear only for ¿$h_1 g_1$. So, ¿$h_1 g_1 = \mu$ everything else here is smaller which means the sum will have initial term ¿$h_1 g_1$ which is μ, but that is the initial term of f also, but that we know is not true since initial term of the $\sum h_i g_i$ which is f, remember that ¿$f < \mu$.

So, the initial terms of at least two of these things should get cancelled before we get f. So, let us make this observation. So, without loss of generality, we can rearrange these terms and assume that $h_1 g_1$ and $h_1 g_1$ have the same initial term μ.

(Refer Slide Time: 14:56)

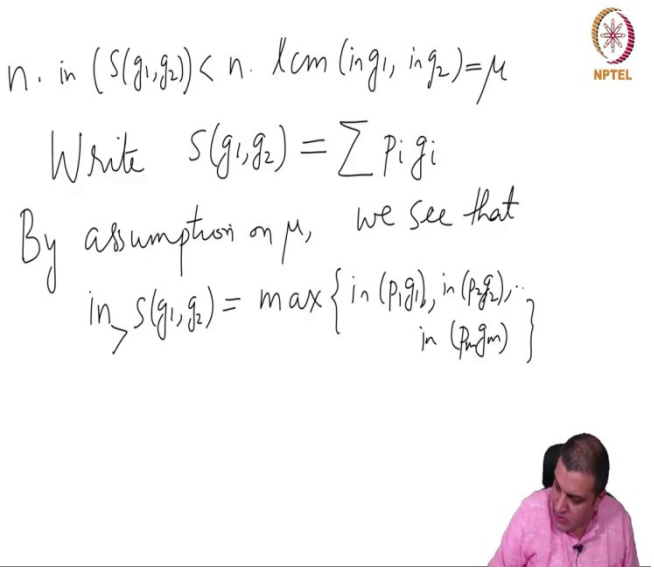


So, note that the initial term of g_1 divides μ, the initial term of the product of two polynomials is the product of their initial terms. So, the initial term of g_1 divides μ, similarly initial term of g_2 divides μ, hence lcm of the initial terms divides μ.

So, we can write this, so let n be a monomial, such that $n \cdot lcm(¿\, g_1 ¿, \in g_2) = \mu ¿$. Now we need to study the S pair. We just need to introduce some notation because you are keep using this thing.

So, let $L_1 = lcm \frac{(¿\, g_1 ¿, \in g_2)}{¿\, g_1} ¿$; similarly $L_2 = lcm \frac{(¿\, g_1 ¿, \in g_2)}{¿\, g_2} ¿$. So, then notice that $S(g_1, g_2) = L_1 g_1 - L_2 g_2$.

(Refer Slide Time: 16:55)



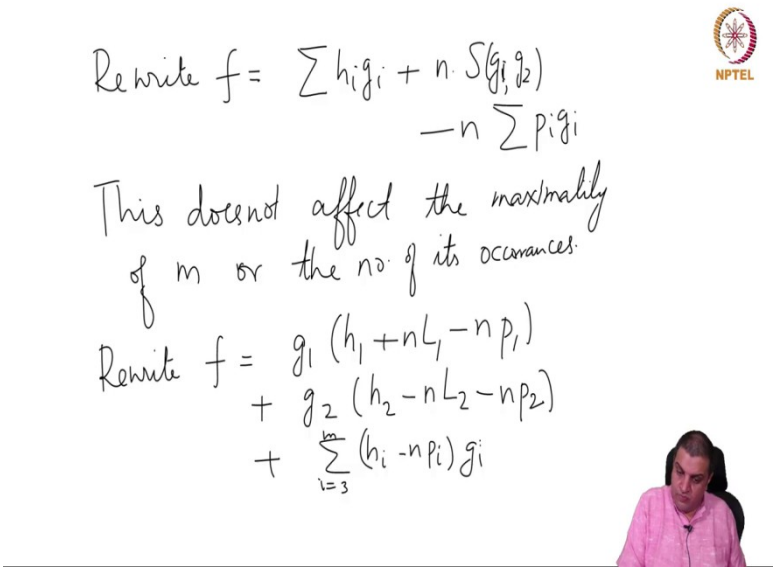
Now, let us look at various of initial terms now. Then $n \cdot \in(S(g_1¿,g_2)) < n \cdot lcm(¿g_1¿,\in g_2) = \mu ¿¿$.

So that is just this expression was constructed precisely to cancel their respective leading terms both of which are have this value and this was μ. So, we would need to use this later. So, notice that the S pair is an element in the ideal. So, it can be written as $S(g_1,g_2) = \sum p_i g_i$.

Its initial term is strictly less than μ. Now μ was the among all such elements whose initial term is not inside the ideal generated by the initial terms of the g_i, choose an expression of this form such that this is smallest and its value is μ, but now we have an expression like this whose initial term is strictly less than μ.

By assumption on μ, we see that the $¿S(g_1¿,g_2) = max ¿\in(p_1¿g_1),\in(p_2¿g_2),\ldots,\in(p_m¿g_m)\}¿¿¿¿¿$. If this were not the max, then this expression would also satisfy the condition which was used to pick out μ, but then the initial term of this is strictly less than μ that would have contradict to the choice of μ. So, one can choose with this property.

(Refer Slide Time: 20:55)



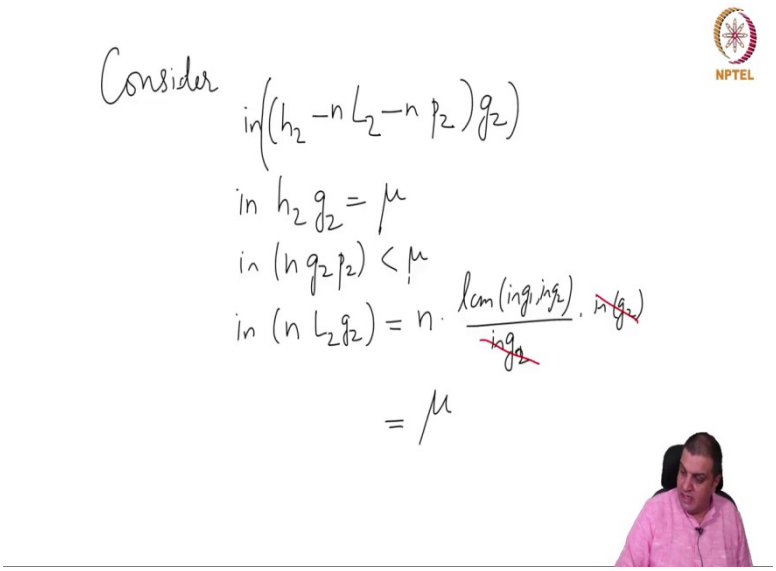
So, now with this, we can rewrite f as $f = \sum h_i g_i + n \cdot S(g_1, g_2) - n \sum p_i g_i$, that is just saying we have just added something and subtracted the same thing. So, it is not changing the value of n.

Now, in this expression, notice that the maximum of the initial term, so we can rewrite like this. So, in this expression, there is a g_1 and g_2 appearing in the definition of S then there is something here. So, in this expression, it does not change the number of times μ occurs as the initial term of these terms inside here nor does it affect. The fact that μ is the maximum of the initial terms on the right side.

So, therefore, let me just summarize that thing. So, this does not affect the maximality of μ or number of its occurrences in this collection. So, we have not removed any of the leading terms for which it is μ. So, now, using this we can rewrite f now as

$$f = g_1(h_1 + nL_1 - nP_1) + g_2(h_2 - nL_2 - nP_2) + \sum_{i=3}^{m} (h_i - nP_i) g_i.$$

(Refer Slide Time: 24:24)

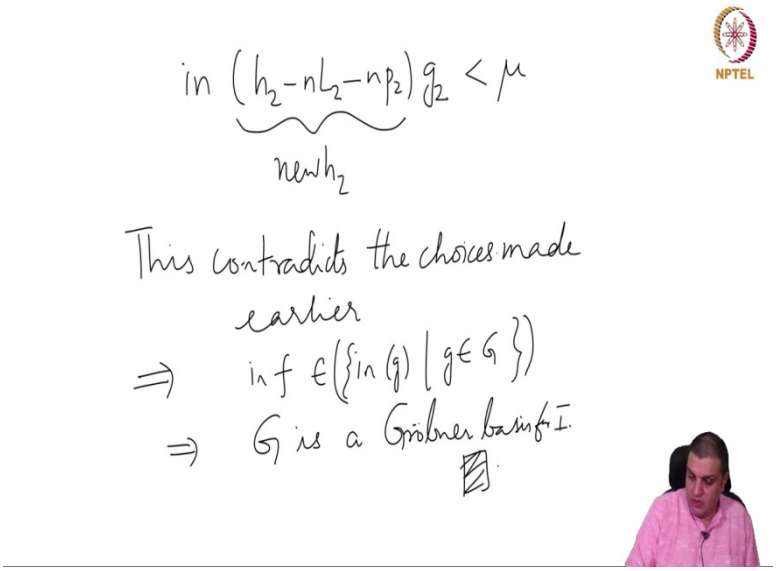


Now, consider $¿((h_2 - nL_2 - nP_2)g_2)$, this is the coefficient of g_2 in this new expression.

So, $¿h_2 g_2 = \mu$ and $¿(n g_2 P_2) < \mu$. And the important point is $¿(nL_2 g_2) = n\frac{lcm(¿g_1, \in g_2)}{¿g_2} \in g_2 = \mu$

.

(Refer Slide Time: 26:48)

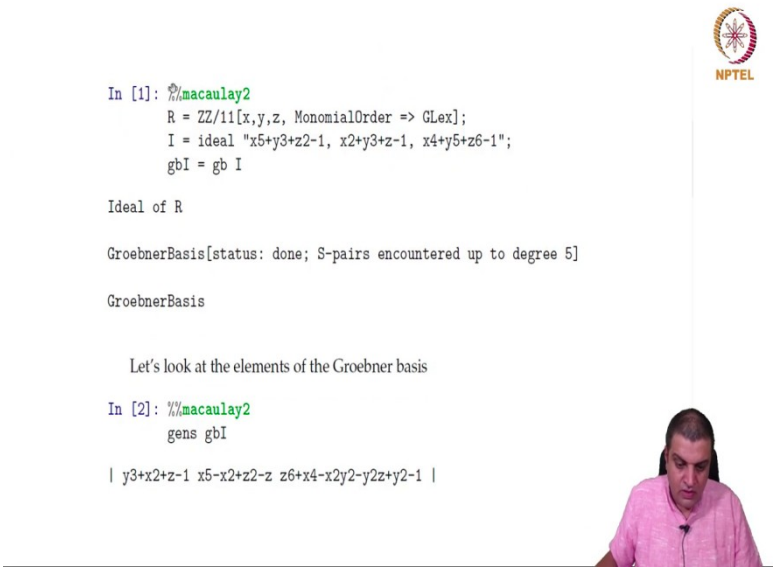


So, in other words the conclusion for us is that ¿$(h_2 - nL_2 - nP_2)g_2 < \mu$. Remember μ was chosen with certain properties, and this contradicts one of those law. Among such expressions the number of times in which this occurs is minimum.

So, previously we had assumed that $h_1 g_1, h_2 g_2$ and possibly other things all had the same initial term μ out of which if we have removed one term which is we have changed the coefficient of g_2, so that the with the new h_2, ¿¿new h_2¿ times g_2 is strictly less than μ. So, this contradicts the choices made earlier.

And hence therefore, the conclusion is there, and all of this came by assuming that there is an f. So, conclusion is that ¿$(f) \in (\{¿(g) | g \in G\})$ in other words G is a Grobner basis for I. So, that is the end of proof.

(Refer Slide Time: 28:39)

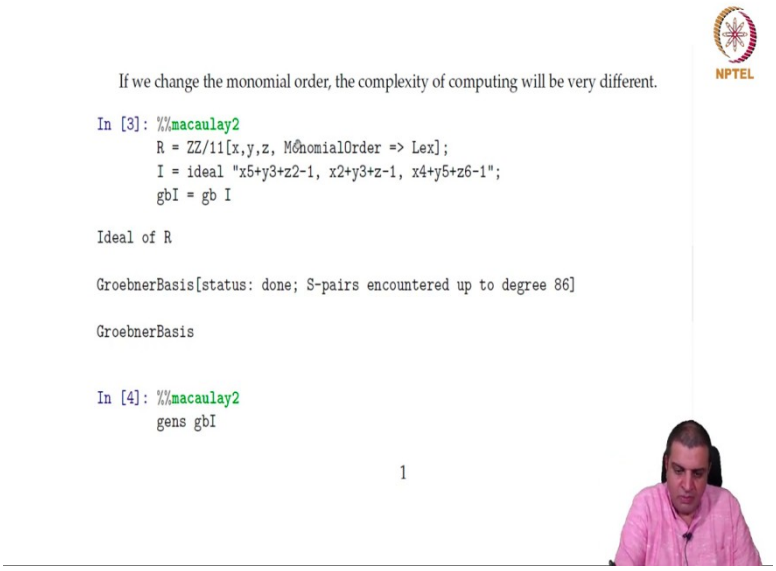


So, now I just want to show one example. So, these lines which follow a two percentage sign macaulay 2 an offset from the left like this like this, this is the macaulay code that we enter and this is the output of various lines that are just sequentially given.

So, in the first line, we just defined a ring and then next line we defined an ideal. And notice the new way in which we have defined the ideals. So, we have just written like a string, we have written $x5+y3+z2-1$. It will understand is as $x^5+y^3+z^2-1$. It is a convenient way of entering polynomials into macaulay2 if the variables do not have subscripts.

The variables have subscripts, we cannot do it. We have to do it the way we were doing it till now like x so caret 5 etc. So, this is a convenient way of doing that. So, these three lines are corresponding out. So, we ask to compute the Grobner basis of I. So, this is defined in the GLex order. And we just call that thing gbI, this is just a name. This is the thing and it says it is a Grobner basis, the status of it is done and S-pairs encountered up to degree 5. So, it kept computing, and it went up to some large degree.

(Refer Slide Time: 30:23)

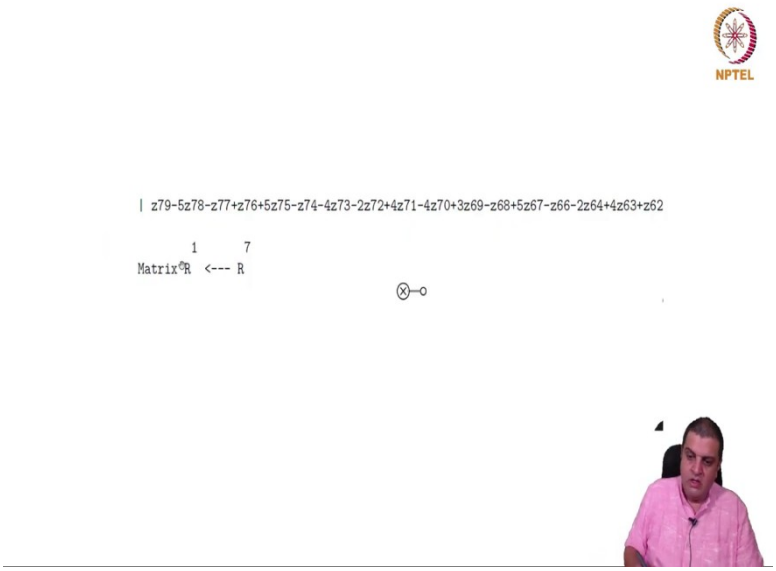


And let us look at the elements of the Grobner basis. So, we continue the calculation. So, this is asking for the generators of the Grobner basis meaning the actual elements of the Grobner basis. So, it output something y^3+x^2+z-1, which is one of the generators. Remember this is GLex so that is the leading term.

So, the complexity of computing a Grobner basis depends heavily on the on the monomial order that we choose. So, we just repeat the same thing. So, here we just did we got something. So, now, we ask same thing we just redo all the calculations, but now the ring is defined with monomial order Lex and the same ideal, and we asked to compute Grobner basis.

Suddenly we notice that S-pairs encountered up to degree 86, there previously it was just 5 ok. So, a substantial difference in the complexity between Lex and GLex.

(Refer Slide Time: 31:42)



So now we ask to show the output and it is so big. So, here this is degree 79 it starts with; z^{79}, z^{78}, z^{77} so on. So, with some very long there are seven generators first of all in that thing, and it is just a very long.

So, this is the end of this lecture. In the next lecture, we will look at quotient rings and how Grobner basis comes in handy to study them. And we will also using the same idea we will also come up with the criterion to decide if some system of polynomial equations has finitely many solutions.