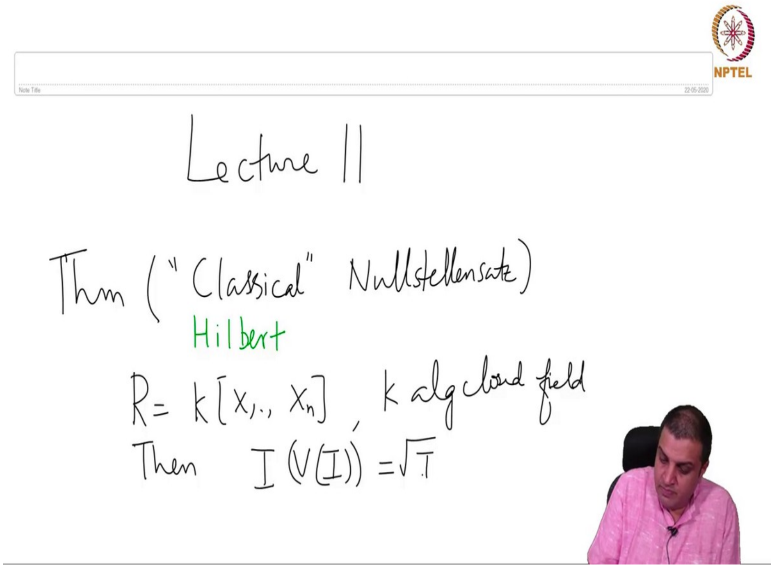
Computational Commutative Algebra

Prof. Manoj Kummini
Department of Mathematics
Chennai Mathematical Institute

Lecture - 11
Nullstellensatz – Part 2

(Refer Slide Time: 00:14)



Note Title 22-05-2020

Lecture 11

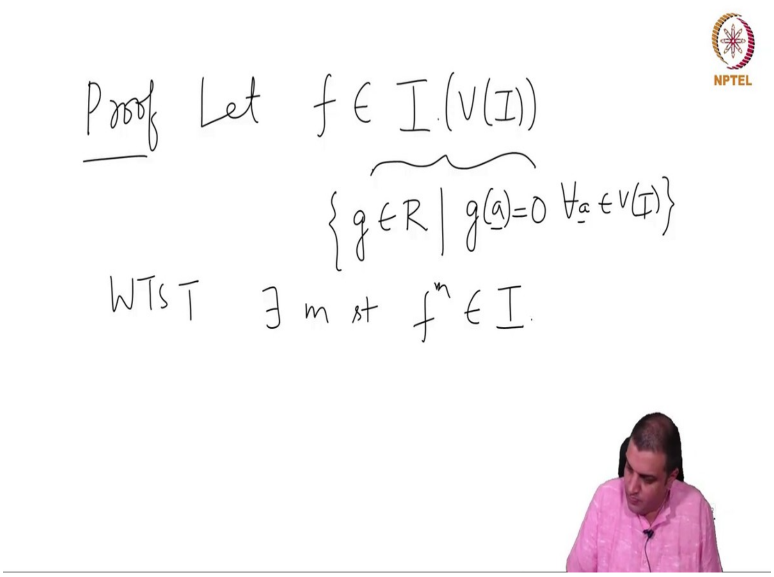
Thm ("Classical" Nullstellensatz)
Hilbert

$R = k[x_1,., x_n]$, k alg closed field
Then $I(V(I)) = \sqrt{I}$

So, this is lecture 11 and here we look at another version of Nullstellensatz, this is the more classical version. So, this is; so, this is a classical version of Nullstellensatz and proved by Hilbert. So,so again the notation is $R=k[x_{1,\dots},x_n]$, k algebraically closed. Then, $I(V(I))=\sqrt{I}$.

So, let us prove this. Again, we will prove it assuming the versions the equivalent versions that we proved in the last lecture I mean, assuming the 2 versions that we saw in the last lecture which we proved were equivalent to each other, but we did not prove either that either of them were true. So, assuming that statement we will prove this and as I mentioned we will prove the version 2, the description of maximal ideals after we develop some more algebra.

(Refer Slide Time: 01:56)



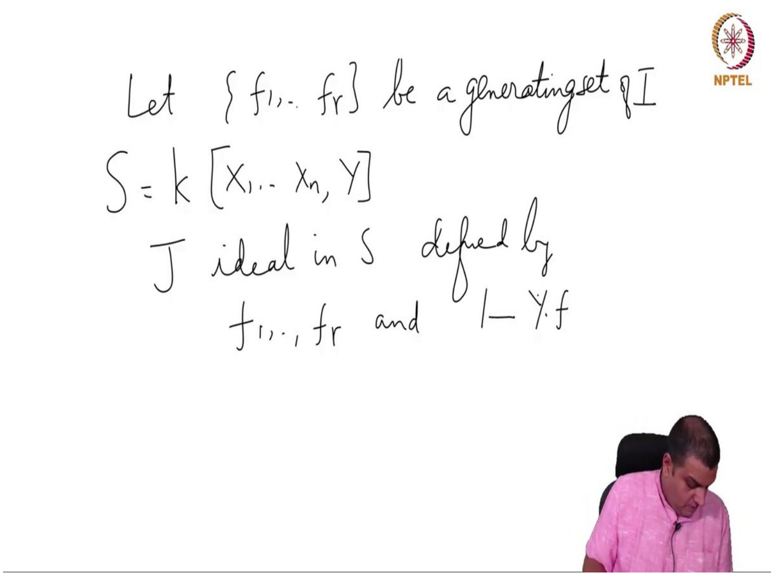
Proof Let $f \in \underbrace{I(V(I))}_{\{g \in R \mid g(\underline{a})=0 \ \forall \underline{a} \in V(I)\}}$

WTST $\exists\ m$ st $f^m \in I$.

So, let proof let $f \in I(V(I))$, so let me just remind you what this is given any variety we can look at so, given any given any I we can look at its variety and then we can ask what are all the polynomials which vanish on that V of I, so, maybe I should just to remind ourselves we should say what this is.

So, this is $\{g \in R s: g(a)=0\, for\, all\, a \in V(I)\}$ and we want to show that, so we want to show that there exist an m such that $f^m \in I$. So, the proof of the statement is clever trick done as follows.

(Refer Slide Time: 03:16)



Let $\{f_1,.. f_r\}$ be a generatingset of I

$S = k[X_1 .. X_n, Y]$

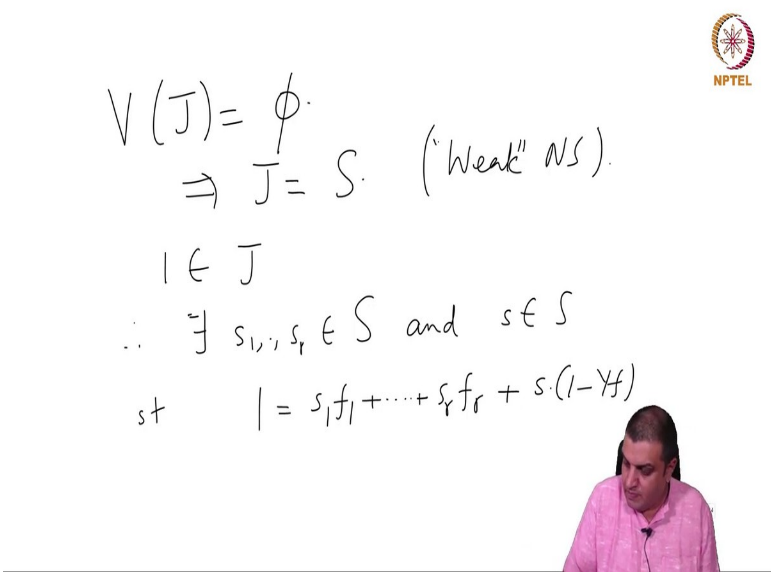
J ideal in S defined by

$f_1,.., f_r$ and $1 - Y.f$

So, let $\{f_{1,\dots},f_r\}$ be a generating set of I. yes what we want to show is that $f^m \in \{f_{1,\dots},f_r\}$ is in this ideal, the ideal generated by these elements.

So, we define a new ring $S=[X_{1,\dots},X_n,Y]$ in that we define a new ideal in S defined by $f_{1,\dots},f_r$ the generators of I and a new element which is $1-Yf$. So, f is a polynomial just in the X’s. So, we are generate writing a polynomial like this ok.

(Refer Slide Time: 04:38)



$V(J) = \phi.$

$\Rightarrow J = S.$ ("Weak" NS).

$1 \in J$

$\therefore \exists\ s_1,.., s_r \in S$ and $s \in S$

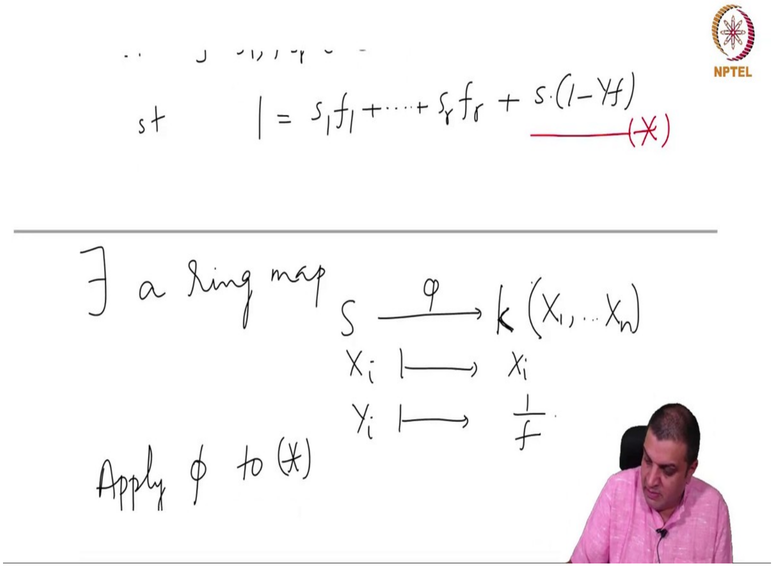
st $1 = s_1 f_1 + \dots + s_r f_r + s \cdot (1 - Yf)$

So, now the observation that we want to make is that V (J) is empty. So, let us look at why that is the case? So, you this you will you should write out the details it is not very difficult. So, i if b is an n + 1 tuple which is in V(J), then these polynomials vanish by definition of f vanishes, but then 1- Yf cannot vanish so, that is . So, check please check this detail.

So, V (J) is empty which means that J = S. So, this is the what we call the "Weak" Nullstellensatz. So, in other words $1 \in J$. So, we can write 1 in terms of these elements ok. Therefore, there exist $s_{1,\ldots,}s_r \in S$ and some $s \in S$ such that, $1 = s_1 f_1 + \ldots + s_r f_r + s(1 - Yf)$ let us just say 1 is an ideal generated by $\{f_{1,\ldots,}f_r\}$ and 1 + Yf.

The coefficients have to come from s. So, now let us we do so this is all part of the trick.

(Refer Slide Time: 06:24)



st $| = s_1 f_1 + \cdots + s_r f_r + s\cdot(1-Yf)$ $\underline{\qquad}(*)$

∃ a ring map $S \xrightarrow{\varphi} k(X_1, \ldots X_n)$

$X_i \longmapsto X_i$

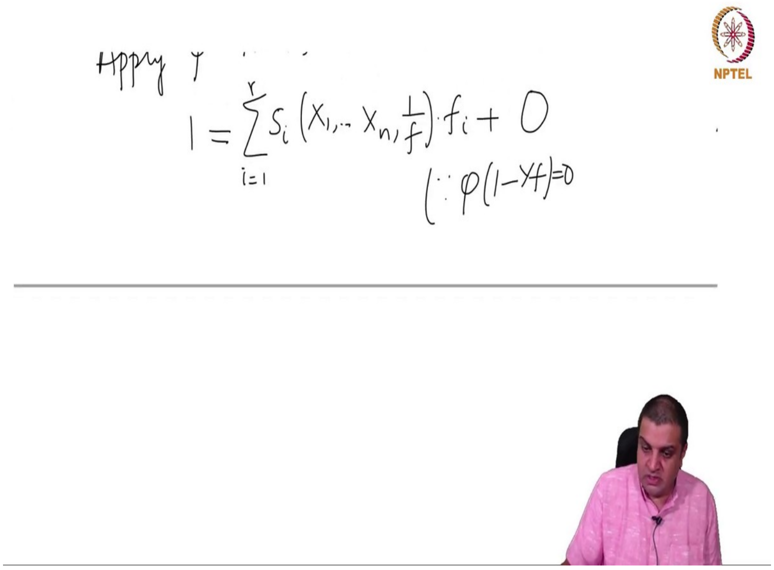
$Y_i \longmapsto \frac{1}{f}$

Apply ϕ to $(*)$

So, the next is we consider a ring map. So, there exist a ring map which goes from S to some large ring we can make it more precise after we develop some things, but it is not relevant for the proof. The ring that we will consider is the rational function field $k(x_{1,\ldots,}x_n)$

So, there exist a ring map, in which k elements of k go to the same elements here X_i also go to goes to x_i and Y_i goes to $\frac{1}{f}$ ok. So, now let us apply so, let us call this thing star apply and let us call this map φ . Let us apply phi to star this equation here.

(Refer Slide Time: 07:38)



Apply φ

$$1 = \sum_{i=1}^{r} S_i\left(X_1,\ldots X_n, \frac{1}{f}\right)\cdot f_i + 0$$

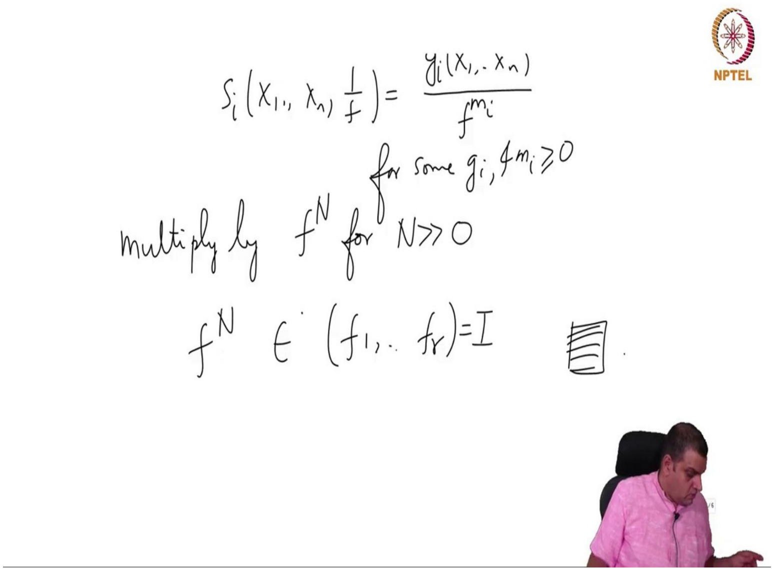
$$\left(\because \varphi(1-Yf)=0\right.$$

So, φ is a ring homeomorphism $\varphi(1)=1$ f_i involve only the X’s and X_i is map to X_i ’s. So, that is just f_i . But, on the other hand what is S_i goes? S_i is a polynomial in n +1 variables; the X’s and Y, Y becomes 1 / f , f_i is unchanged and so this is the first term the first part.

So, these terms this is what it becomes and S goes to whatever it is 1 – Yf becomes 0, that is exactly why this is written like this plus 0. So, this is because $\varphi(1-Yf)=0$. That is the.

So, now, we got an expression about 1 not involving polynomials, but one also needs to allow for rational functions which have an f in the denominator. this is not exactly an expression in the ring R, but it is an expression in the rational function field in the same variables, the only observation you are to make is the denominator will only involve powers of f it will not involve other polynomials .

(Refer Slide Time: 09:32)



$s_i(X_1,.., X_n, \frac{1}{f}) = \frac{g_i(X_1,.. X_n)}{f^{m_i}}$

for some g_i, & $m_i \geq 0$

multiply by f^N for $N \gg 0$

$f^N \in (f_1,.. f_r) = I$ ▤.

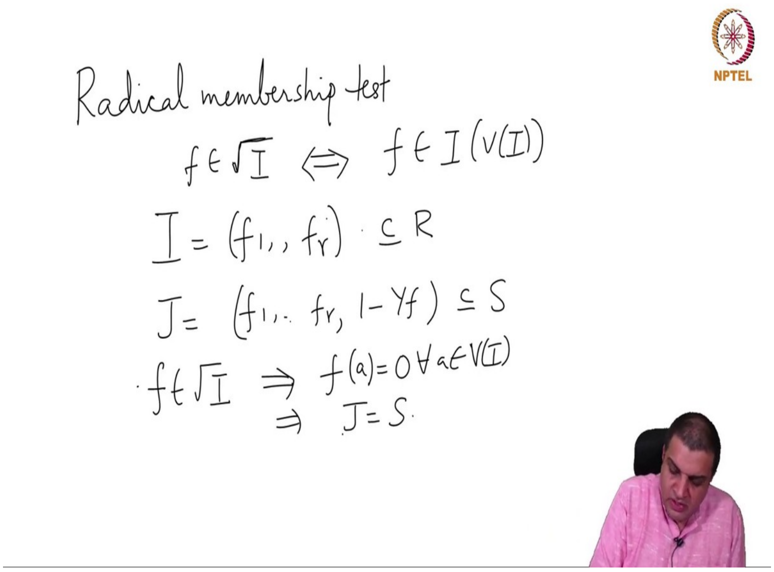
So, because of this we can clear denominators. So, what does $S_i(X_{1,...}, X_n, \frac{1}{f})$ will look like some polynomial some $\frac{g_i(X_{1,...}, X_n,)}{f^{m_i}}$, so, when we write this out and then in the expression of the polynomial clear denominators and then you will get some f^{m_i} .

So, that gives us for some g_i ; g_i and $m_i \geq 0$, g_i is just a polynomial. So, we can write it like this. So, now, multiply by a large n power of a multiply by f^N for some for sufficiently large N that would clear all the denominators of which have f's the powers of f in the denominator .

So, this is in the ideal generated by $f_{1,...}, f_r$ which is I , so this is the proof. So, this is just its just a clever trick so, what it does is, it passes to a larger ring and where after a substitution we can introduce f's in the denominator and then clear the denominators one would get an expression like this. So, this is what we wanted to prove.

So, based on this. So, the so from what we have seen so far, it is now sort of clear that, the radical of an ideal is an important part important object associated to an ideal. So, we can ask so we saw in the last lecture, how to test for memberships in ideals? So, now, we can ask whether we can testified membership in ideals and so, this is called radical membership test.

(Refer Slide Time: 12:05)



Radical membership test

$f \in \sqrt{I} \iff f \in I(V(I))$

$I = (f_1, , f_r) \subseteq R$

$J = (f_1, .. f_r, 1-Yf) \subseteq S$

$f \in \sqrt{I} \Rightarrow f(a)=0 \; \forall a \in V(I)$

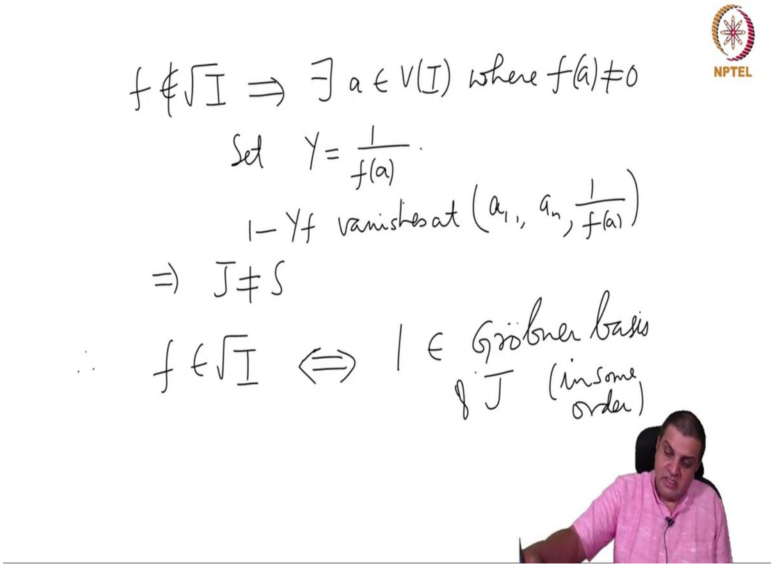
$\Rightarrow J = S$

Notice that, $f \in \sqrt{I}$, if and only if $f \in I(V(I))$ this is what we just proved that radical of I is equal to this . So, if f is in radical of I then, there is a point if f is in radical I then, now let us consider so, $I=(f_1,\dots,f_r)$. $J=(f_1,\dots,f_r,1-Yf)\subset S$ same notation as in the theorem. Now, if f belongs to this equivalently if f belongs to this, this ideal would be the unit ideal.

If f does not vanish at some point where, the f_i is vanish then this has a solution ok. So, let us check this let me write down what I just said. So, if f vanishes everywhere where the f_i is vanish then f is in the radical. So, we can write from the previous theorem that f is in the radical implies that $f(a)=0 forall a \in (V(I))$. So, if you substitute a point where the f_i is vanish, then f will also vanish and hence it does this does not have any solution.

So, this means that J is the unit ideal. Let us think about the converse, if J is the unit ideal then, let us do it the other way around.

(Refer Slide Time: 14:37)



$f \notin \sqrt{I} \Rightarrow \exists\, a \in V(I)$ where $f(a) \neq 0$

Set $Y = \frac{1}{f(a)}$.

$1 - Yf$ vanishes at $\left(a_1, a_n, \frac{1}{f(a)}\right)$

$\Rightarrow J \neq S$

$\therefore\ f \in \sqrt{I} \iff 1 \in$ Gröbner basis of J (in some order)

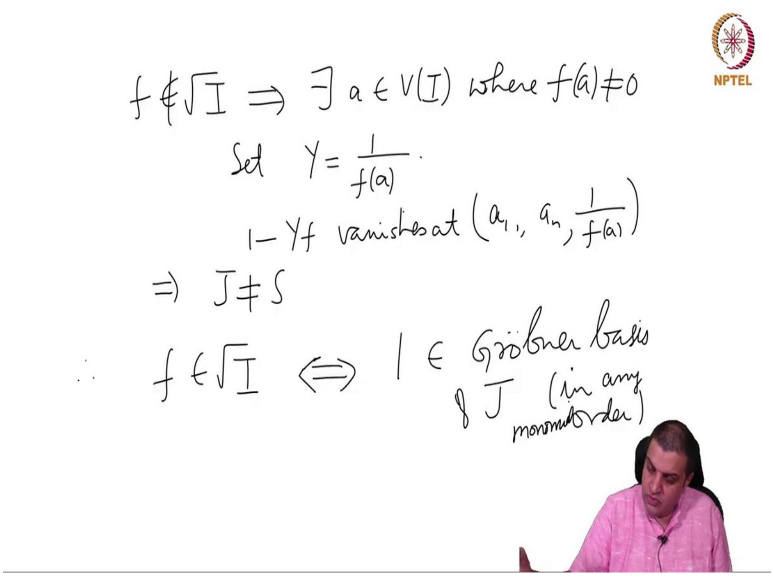
let us suppose f is not in the radical, this implies that there exists some $a \in (V(I))$ where, $f(a) \neq 0$; this is where the other direction of the every f is not in the radical means $f \notin I(V(I))$. So, there is such a point , so we get this.

And, from this what can we conclude? If you substitute a to these polynomials these things vanish so that is . And, f does not vanish, then appropriately you can choose a Y such that, 1 - f Y vanishes. So, then set $Y = \frac{1}{f}(a)$ then 1 - Yf vanishes, I mean this value of Y vanishes at $\left(a_{1,} \dots, a_n, \frac{1}{f(a)}\right)$.

And, this is well defined because it is nonzero. So, in other words $J \neq S$. So, the question whether the question whether f is inside the radical of I is precisely determined by whether J is S or not and then we know that the test therefore, the test is f is in the radical of I, if and only if 1 is in the Grobner basis of J in some order.

Notice that, in these discussions we do not need to decide if the discussion does not have an underlying one need not worry about an underlying order, but to use this theorem we once we have to set an order compute the Grobner basis in any order not some, in any order in any order in any monomial order.

(Refer Slide Time: 16:52)



$f \notin \sqrt{I} \Rightarrow \exists\, a \in V(I)$ where $f(a) \neq 0$

Set $Y = \frac{1}{f(a)}$.

$1 - Yf$ vanishes at $\left(a_1, \ldots, a_n, \frac{1}{f(a)}\right)$

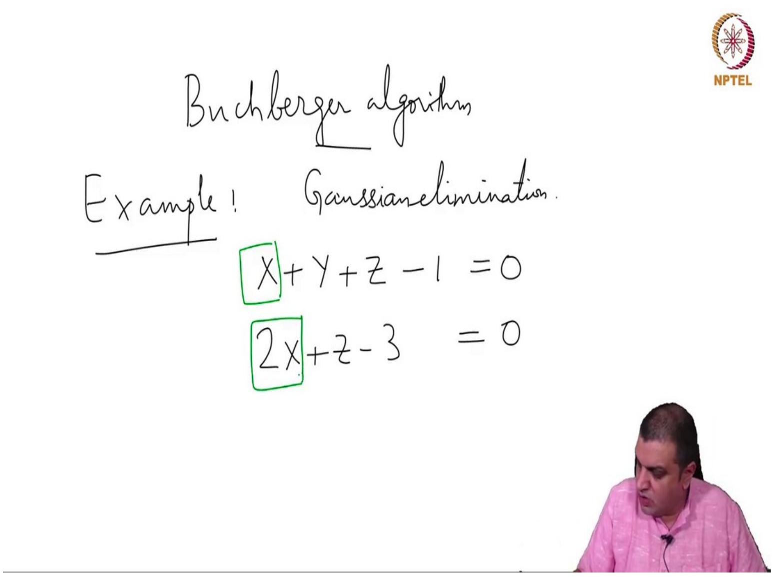
$\Rightarrow J \neq S$

$\therefore\ f \in \sqrt{I} \iff 1 \in$ Gröbner basis of J (in any monomial order)

So, this is the radical membership test , f is inside radical of I is same thing as J being equal to S which is same thing as one being inside J and one can immediately write this in terms of a Grobner basis .

So, now we want to sort of study some more about Grobner basis. And, in fact how do we compute a Grobner basis given a generating set. So, typically when we write a program it would be you one would write down the generating set and then one would need to know the Grobner basis and so this is; so this is called Buchberger algorithm.

(Refer Slide Time: 17:48)



Buchberger algorithm

Example! Gaussian elimination.

$\boxed{X} + Y + Z - 1 = 0$

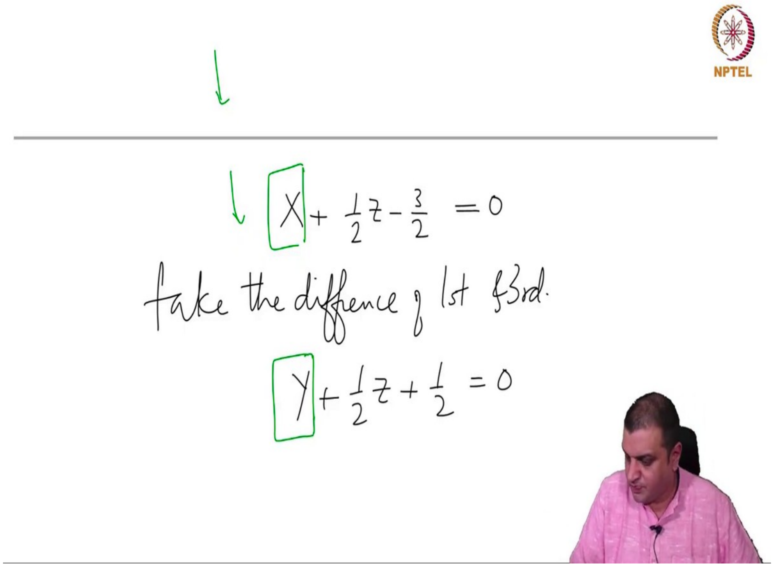
$\boxed{2X} + Z - 3 = 0$

So, I will quickly discuss 2 examples of this. Although, we never learned it as examples of this and the Buchberger algorithm cleverly puts these things together and proceeds. So, the first example is Gaussian elimination of solving linear equations. So, let us say we have 2 polynomials X +Y + Z = 1; so I will write it as X+ Y + Z- 1= 0.

And, let us mark the leading terms well, we do not know what leading times when you do Gaussian elimination, but we knew we get rid of the X and then and so on. We write it in a matrix and do row reduction, but I am just writing it writing the same thing in polynomials just to see that this is what we were doing. Let us say the other polynomial is 2X+ Z- 3 =0, whose leading term is this.

So, we would like to simplify these leading terms just for convenience we would like to make them all 1.

(Refer Slide Time: 19:26)



$\boxed{X} + \frac{1}{2}Z - \frac{3}{2} = 0$

take the diffence of 1st & 3rd.

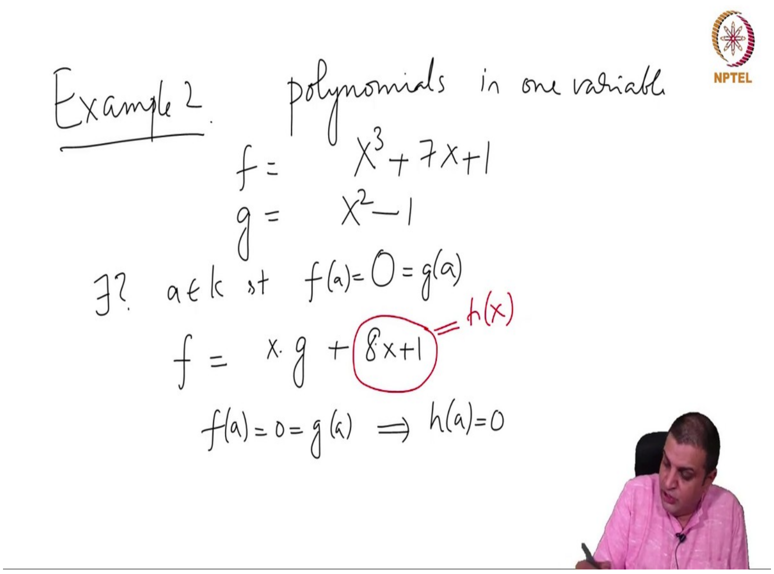
$\boxed{Y} + \frac{1}{2}Z + \frac{1}{2} = 0$

So, let us rewrite this as as $X+\frac{1}{2}Z-\frac{3}{2}=0$, and the leading term does not change. So, now these 2 the first and the third equation have the same leading term take the difference. So, that when you take the difference of 1st and 3rd.

So, that would give us $Y+\frac{1}{2}Z+\frac{1}{2}=0$, for which this is the leading term ok. So, now if you go back how this was done in matrices we would say there are 2 pivot variables X and Y different ones and this is all that Gaussian elimination can do. So, we will now solve for Y, we will set arbitrary values to Z and solve for Y then together in this equation and then we will go back to this equation and solve for X.

So, that is how Gaussian elimination or we could use these 2 equations, give arbitrary values to Z and then solve for Y from here and solve for X from there. So, this is what we did in Gaussian elimination.

(Refer Slide Time: 21:10)



Example 2. polynomials in one variable

$f = X^3 + 7X + 1$

$g = X^2 - 1$

$\exists ?\ a \in k$ st $f(a) = 0 = g(a)$

$f = X \cdot g + \boxed{8x+1} = h(x)$

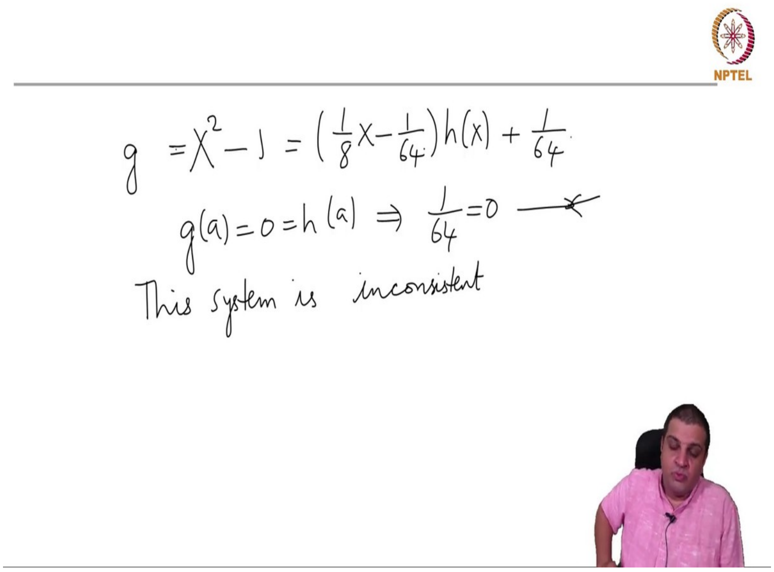
$f(a) = 0 = g(a) \Rightarrow h(a) = 0$

Now, example 2 is polynomials in one variable. So, earlier we looked I mean the linear things many variables, but linear equations now polynomials, but in one variable.

So, let us take one some example let us say that, $f = X^3 + 7X + 1$ and $g = X^2 - 1$, we want to know if they have a common 0. Does there exist a point a in k such that, f (a)= 0 g (a). That is the that is what we would like to answer and so, we would do division algorithm here. So, we would write division algorithm as $f = X g + 8X + 1$.

So, the first round of; first round of division algorithm gives this remainder. So, then if f (a)= 0 and g (a)=0, then for this also it would be 0. So, let us call this thing h(x). So, f (a)= 0 and g (a)=0 of a would imply that, h (a)=0. Now, we will do between h and g.

(Refer Slide Time: 23:10)



$g = X^2 - 1 = \left(\frac{1}{8}X - \frac{1}{64}\right)h(x) + \frac{1}{64}$

$g(a) = 0 = h(a) \Rightarrow \frac{1}{64} = 0 \longrightarrow\!\!\!\times$

This system is inconsistent

And, this is a little complicated expressions, let me just copy what I have already worked $x^2 - 1 = (\frac{1}{8}X - \frac{1}{64})h(x) + \frac{1}{64}$. So, this is what we have.

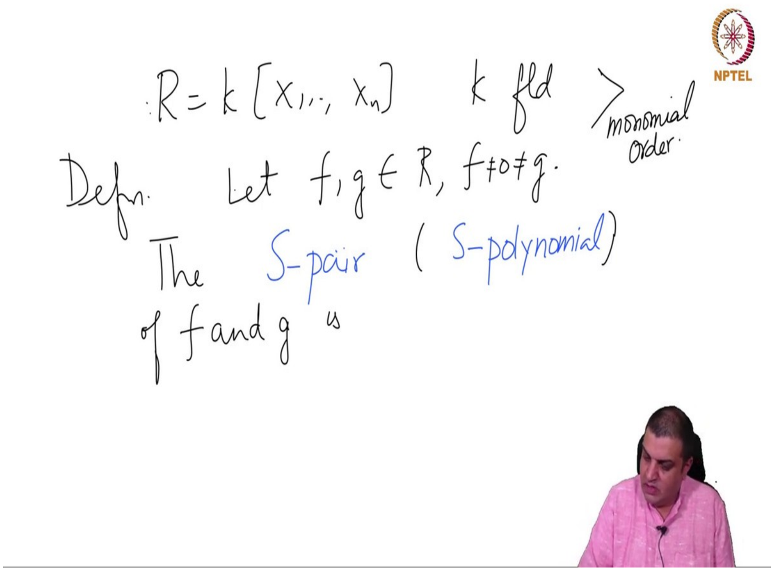
So, now so this is g. So, if g(a)= 0 and h (a)=0, then $\frac{1}{64}$ is 0. This is a contradiction. So, what does that say it says that the system is inconsistent. We would like so what Buchberger algorithm does is to put these ideas together and do for multivariate polynomials in of arbitrary degree not linear polynomials.

So, we need an important notion and how these things are canceled so, it has to do with so let us look over here how were the leading terms canceled the coefficients were adjusted and then subtract. Here, how was it done? Well, the the leading terms were adjusted by multiplying by monomials.

So, here it was some x time's g and then we cancel the leading term. And here so I suppress 2 steps it was really $\frac{1}{8}xh(x)$ and then some leftover was there which was adjusted through this. So, I suppress 2 steps inside here, but even here this can be broken into two steps in which monomials were multiplying the devisor and then canceling with the polynomial from which we were dividing.

So, we would like to form I mean capture this thing properly. So, this is an important definition in this study of Grobner basis.

(Refer Slide Time: 25:25)



$R = k[x_1, .., x_n]$ k fld $>$ monomial order.

Defn. Let $f, g \in R$, $f \neq 0 \neq g$.

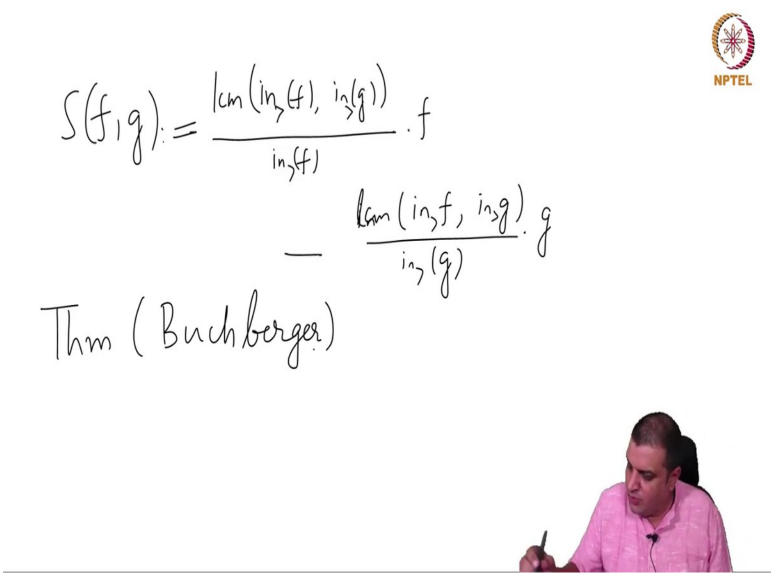
The S-pair (S-polynomial)

of f and g is

So hereafter $R=k[x_1,\ldots,x_n]$ no assumption on k it is a field, but no assumption that it is algebraically closed or any field is fine. Definition let f and g be 2 polynomials in R non-zero. The S-pair so I must apologize I do not know why it is called a pair? It is a single sorry let me finish that, S-pair or sometimes called I mean I think also called polynomial of f and g is.

There is some monomial order, we are discussing Grobner basis so, there is some order that is be used that is be a yes.

(Refer Slide Time: 27:01)



$$S(f,g) := \frac{\mathrm{lcm}(\mathrm{in}_>(f), \mathrm{in}_>(g))}{\mathrm{in}_>(f)} \cdot f - \frac{\mathrm{lcm}(\mathrm{in}_> f, \mathrm{in}_> g)}{\mathrm{in}_>(g)} \cdot g$$

Thm (Buchberger)

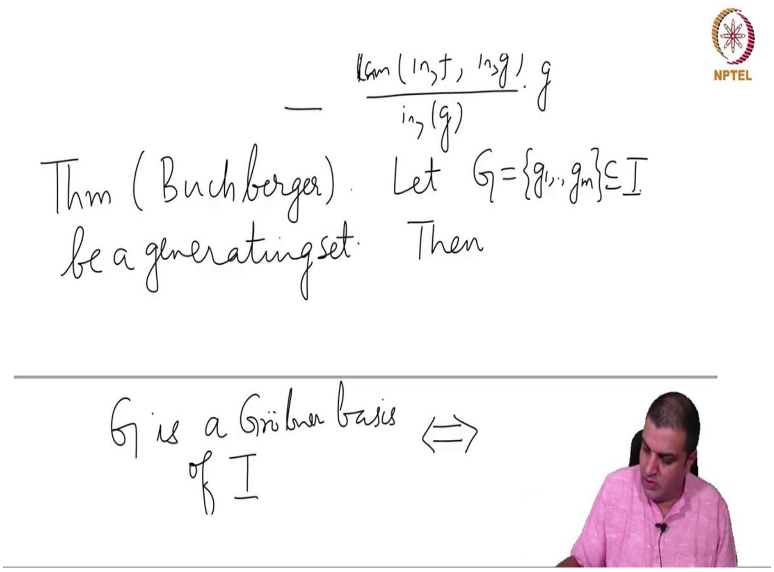
So, let me write it here the we take the $S(f,g) = \frac{lcm(in(f), in(g))}{in(f)} f - \frac{lcm(in(f), in(g))}{in(g)} g$.

Now, if we notice both of these things have the same initial term which is the lcm ok, which is why precisely we took the lcm divided by initial term multiplied by f would just make first of all this is a monomial and you multiply that monomial to f the initial term will get multiplied by this monomial. So, they both have the same leading term and the difference is what is called the it is called written S(f, g) .

So, this is sometimes called S-pair, although it is not clear why it is called a pair, but many books and Macaulay also uses S-pair and sometimes some books refer to it as S-polynomial. So, we will interchangeably use both (Refer Time: 28:23) yeah sorry this is this is what so, this is what S-pair is.

So, this is the key idea behind canceling leading terms multiply appropriately and then subtract we did this in many of the examples yesterday not yesterday in one of the previous lectures sorry not in the previous lecture. So, now so this is the key result of Buchberger which we will prove in the next lecture. So, for now we will just state it and use it as you describe an algorithm.

(Refer Slide Time: 29:21)



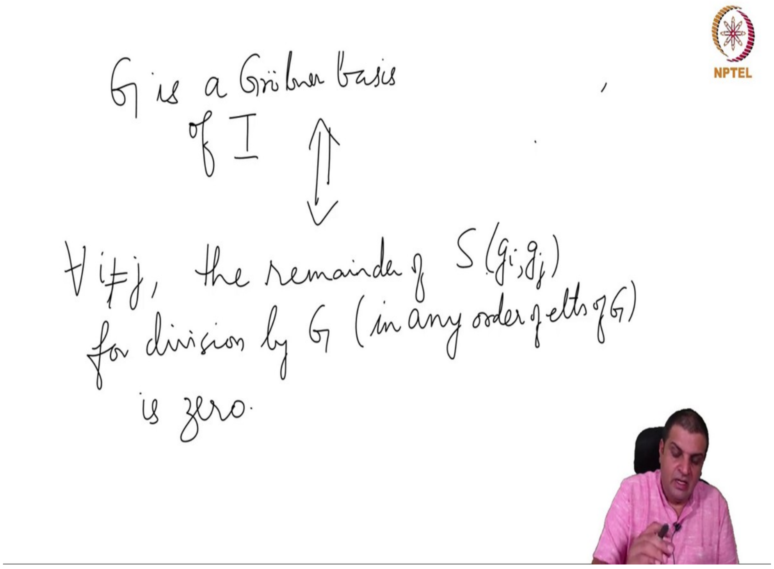
$$-\frac{\text{lcm}(\text{in}_> f,\ \text{in}_> g)}{\text{in}_>(g)}\cdot g$$

Thm (Buchberger). Let $G=\{g_1,\ldots,g_m\}\subseteq I$ be a generating set. Then

G is a Gröbner basis of I $\Longleftrightarrow$

Let *G inside I* be a generating set. Then G is a Grobner basis of I, if and only if the following condition holds.

(Refer Slide Time: 29:40)



G is a Gröbner basis of I

$$\Updownarrow$$

$\forall\, i\neq j$, the remainder of $S(g_i, g_j)$ for division by G (in any order of elts of G) is zero.

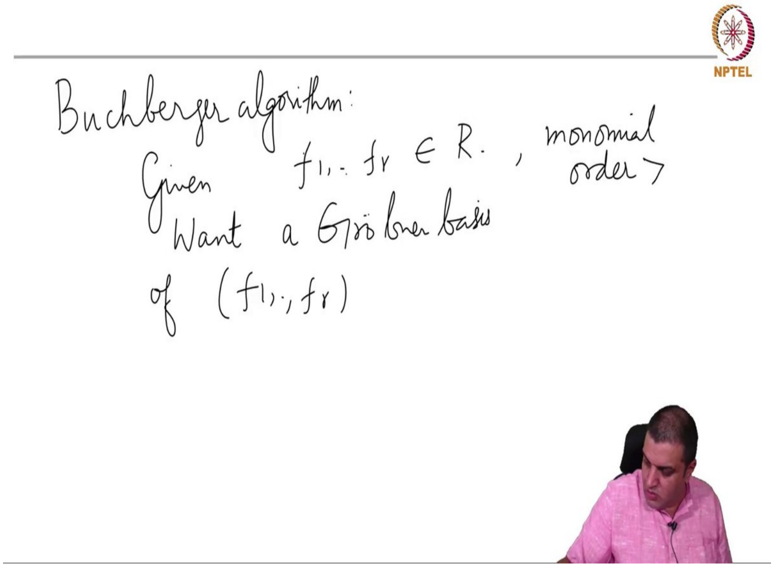
So, this is a sorry I should have said it is a finite I let me just sorry let me just fix this thing a little bit let me actually label it is a finite set and let me write them as $G=\{g_1,\ldots,g_n\}$ for all if and only if for all pairs i different from j. So, now we can apply the division algorithm on the S we can first compute $S(g_i,g_j)$ we can apply the division algorithm by elements of G it in any order we want.

So, the remainder of sorry let me just it is badly positioned we are here write it here for all i different from j and the remainder of $S(g_i,g_j)$ the we take the we appropriately multiply $g_i g_j$ and take the difference to cancel the leading term so, we take this. $S(g_i,g_j)$ the remainder of this for division by G in any order in any order of elements of G is 0.

So, we can apply the division algorithm and run the division algorithm on this remainder by elements of g in some order and it does not matter which order you choose, if the remainder is 0, then this is true for every pairs i and j then G is a Grobner basis.

So, this is what sorry this is slightly more, longer to write than actually to say what it is. We take S for S-pairs for arbitrary i j; i different from j and then we just run the division algorithm by the elements of G in some order independent of the order the remainder should be 0.

(Refer Slide Time: 32:50)



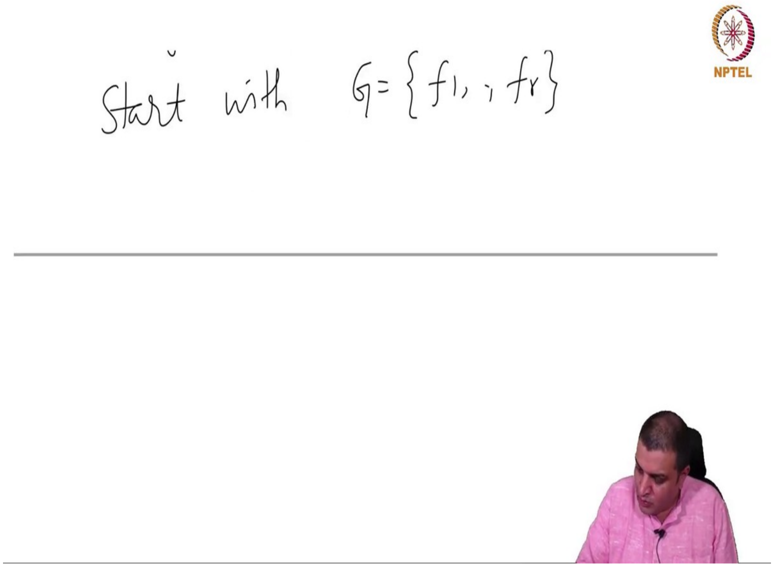
Buchberger algorithm:

Given $f_1,..f_r \in R.$, monomial order $>$

Want a Grobner basis of $(f_1,.,f_r)$

So, we will quickly describe the Buchberger algorithm to compute Grobner basis which is based on that theorem. So, what is given some $\{f_1,\ldots,f_r\} \subset R$ and what we want is given a monomial order > symbol. Want a Grobner basis of the ideal of generated by a $\{f_1, \ldots, f_r\}$.

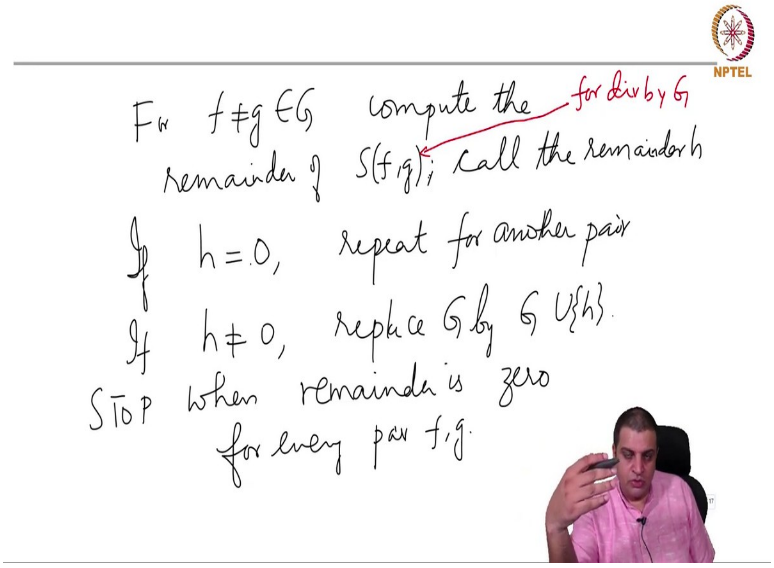
(Refer Slide Time: 33:55)



Start with $G = \{f_1, , f_r\}$

So, start with G as the set .

(Refer Slide Time: 34:10)



For $f \neq g \in G$ compute the remainder of $S(f,g)$ for div by G; call the remainder h

If $h = 0$, repeat for another pair

If $h \neq 0$, replace G by $G \cup \{h\}$.

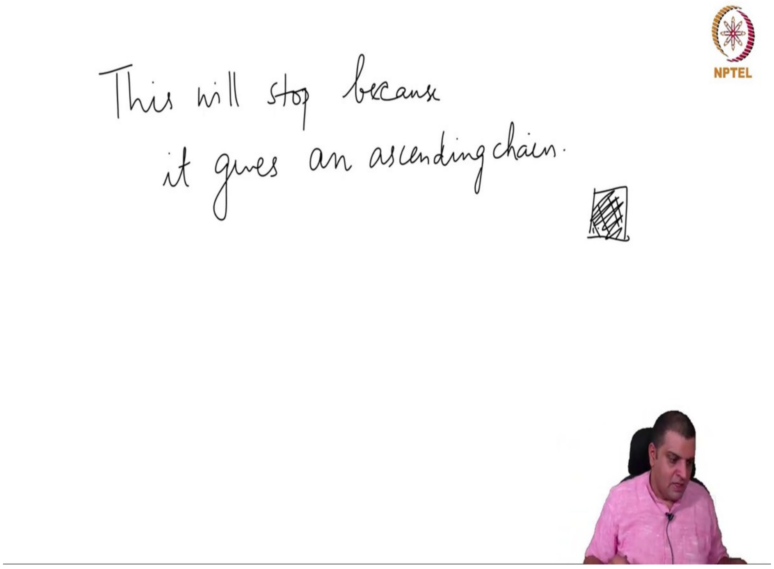
STOP when remainder is zero for every pair f, g.

And, we repeatedly asked the following do the following computation. For f different from g inside G both of them inside G compute the remainder of S(f, g) call the remainder h. If h is 0, nothing could be done this step just do for another pair . So, repeat for another pair.

And, if h is non-zero replace G by we throw in h also into the collection. And, now again do this and stop when the remainder is 0 for every pair remainder division by a compute the remainder of S(f, g) sorry I should have said this here for division by G. So, compute the remainder for 1 and then we just check.

So, the remainder will have terms none of which was divisible by in G in of an element inside the group inside the set G. So, then throw that if it is non-zero then throw that also and this enlarge is G, if it is 0 there is nothing to do repeat this at some stage this will stop.

(Refer Slide Time: 36:30)



This will stop because
it gives an ascending chain. ▨

So, why this will stop, because it gives an ascending chain. As you add more and more elements to G, the ideal generated by G goes up a little bit; but eventually it has to stop.

So, this is the algorithm and this is the most basic elementary algorithm to compute Grobner basis many of the programs have various improvements over these things; we will not discuss those things we just want to have one conceptual understanding of how Grobner basis is computed ok. So, we will prove the theorem this theorem in the next lecture.

Which is that this is the crucial property of Grobner basis that a generating set as a Grobner basis precisely, when the S polynomial between pairs reduced to 0, when you divide by elements of G.