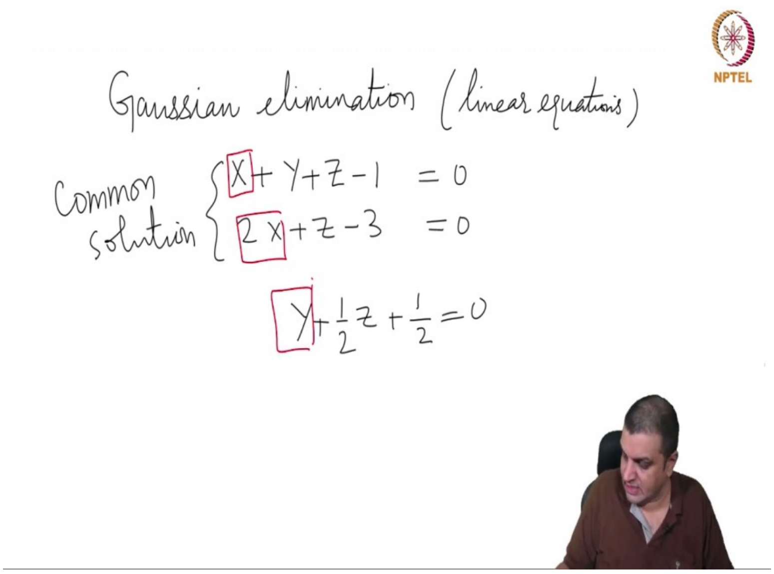
Computational Commutative Algebra
Prof. Manoj Kummini
Department of Mathematics
Chennai Mathematical Institute

Lecture – 14
Elimination

Today's lecture is about Elimination. This is a topic that I mentioned in the previous lecture in the context of finding solving equations in many variables polynomial equations in many variables. So, what is elimination ok? So, this is the more general fancier version of what we do in Gaussian elimination.

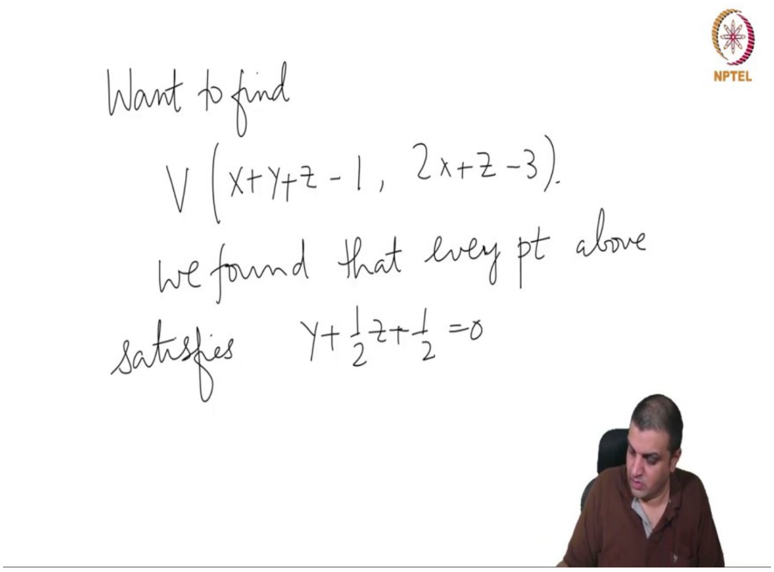
(Refer Slide Time: 00:46)



So, let us go back to the example that we discussed earlier about Gaussian elimination. This is for linear equations. Suppose this was the example that we had considered earlier, suppose we have two equations $X+Y+Z-1=0$ and $2X+Z-3=0$. So, we want to solve these things common solutions and by cancelling out the leading term which is X in this case and also 2 X in this case appropriately, we can get a third equation and this is we saw this last time in an earlier lecture.

$Y+\frac{1}{2}Z+\frac{1}{2}=0$. Now, this is the leading term.

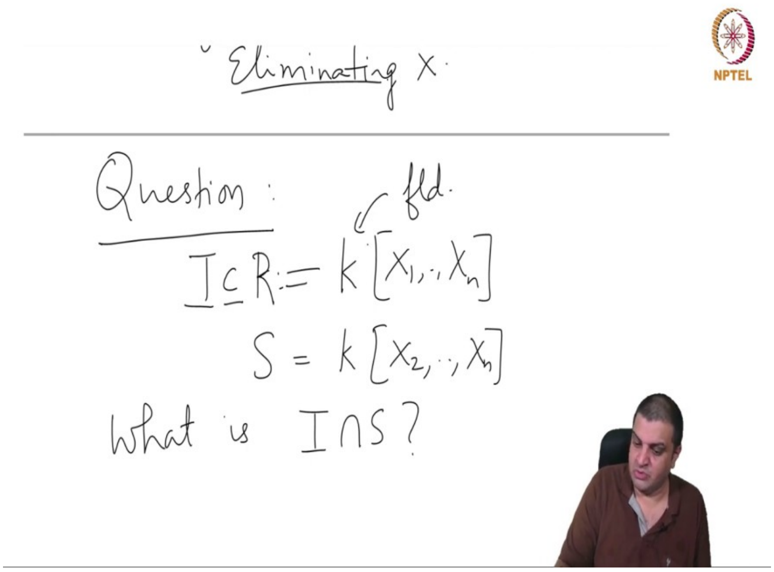
(Refer Slide Time: 02:10)



In other words, so, ideal theoretically what are we saying we want to find. So, we want to find $V(X+Y+Z-1, 2X+Z-3)$. So, when we do this we can find polynomials or in this case linear polynomials which do not involve X.

So, for that is what we just said that we want to find V of this and on the way we found that any solution that every point above satisfies this new equation $Y+\frac{1}{2}Z+\frac{1}{2}=0$. So, how do we find this? So, this is the question.

(Refer Slide Time: 03:29)



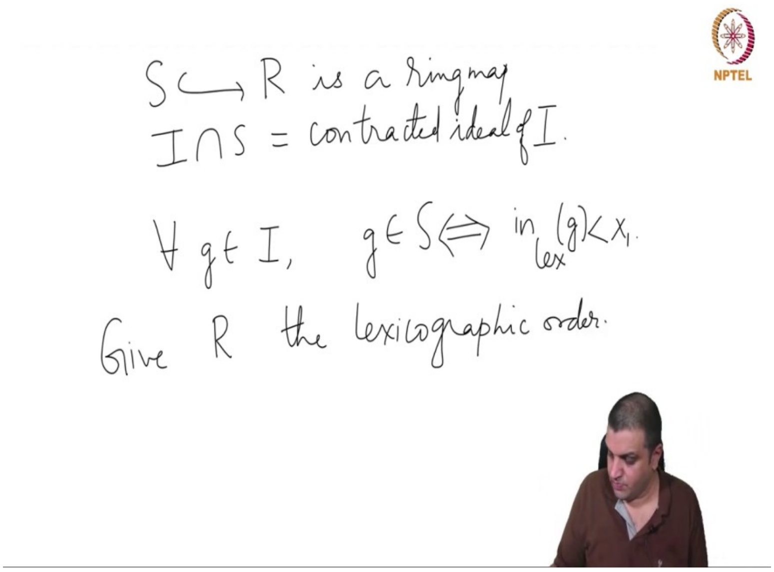
So how did we get this? So, this we got by eliminating, this is what Gaussian elimination did eliminating X.

So, now how we do in the general situation for arbitrary polynomials?

So, now we ask question. So, how do we find such equations? In the linear case we know we just do it by Gaussian elimination which is clearing of the X terms. So, how do we do it properly in the higher degree case? So, I is an ideal of R which is a polynomial ring in some finitely many variables X_1 through X_n. That is $I \subseteq R = k[X_1, \ldots, X_n]$

So, this is a field as usual and again no assumption that it is closed and S is the polynomial ring in one fewer variable. So, in the earlier case the linear form the linear equation case it was X,Y,Z and we leave out the first one and just ask for Y,Z that is what we are doing here. And now we ask what is the ideal; just one observation this is really the contracted ideal.

(Refer Slide Time: 05:17)



So, there is a S sitting inside R is a ring map and I intersect S both in a set theoretic.

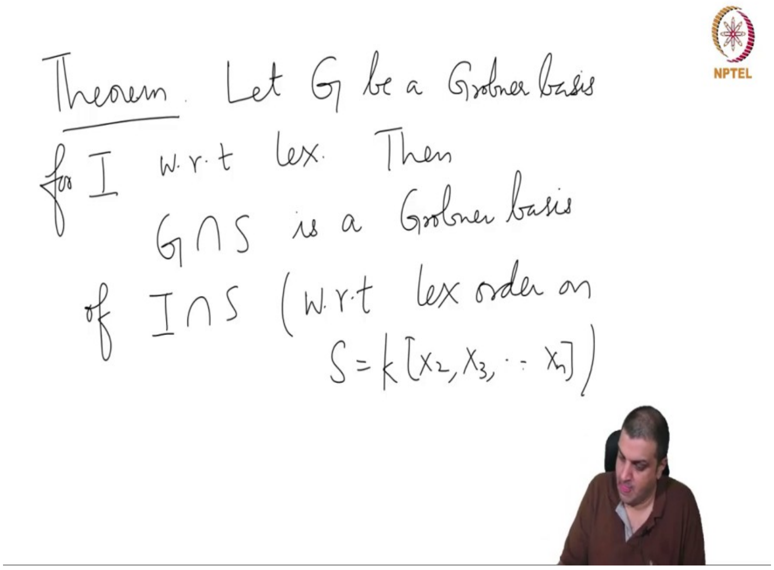
So, when you say S its inside R is a ring map. So, $S \subseteq R$ and $I \subseteq R$ and this would mean the intersection of 2 subsets of R, this is also the contracted ideal of I. So, what is this ideal? So, that is the question, how do we determine this?

So, let us think about what sort of elements belong to I contracted to S. $\forall g \in I$, $g \in S$ if and only if $in_{lex}(g) < X_1$. So, this is an observation that we would like to make that if g belongs to

S then its leading initial term will not involve an X_1 and that is precisely this condition that in the lexicographic order the initial term of g is less than X_1.

So, we can use this. So, what we do is. So, we are going to describe a way to compute this. So, in other words, we will have to use some Grobner basis arguments etc. and we will have to give this thing some monomial order. So, give R the lexicographic order.

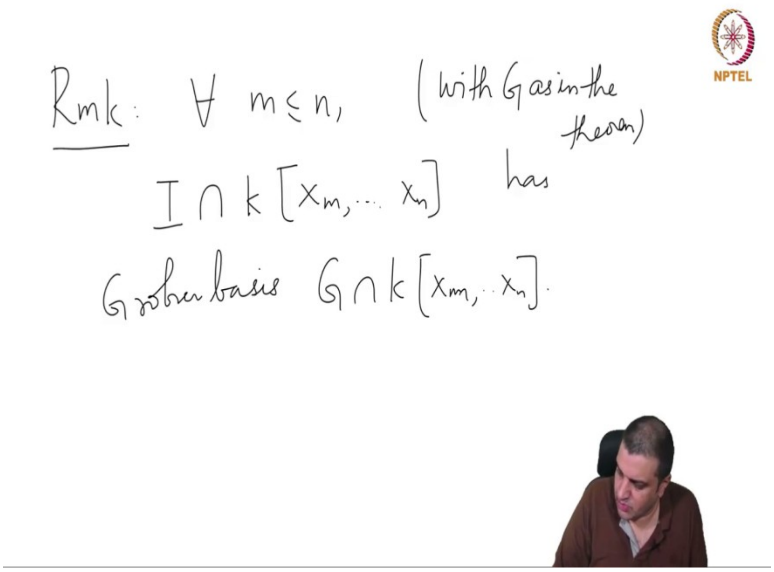
(Refer Slide Time: 07:54)



So, theorem. Let G be a Grobner basis for I with respect to the lexicographic order then G intersect S. So, now, this is just an intersectional vary both are subsets of R and we just take an intersection is a Grobner basis of I contract it to S which is again in this case it is an intersection. So, when we say Grobner basis of this thing with respect to what? With respect to the lex order on S which is the first variable as X_2 now, then is X_3 and so on up to X_n.

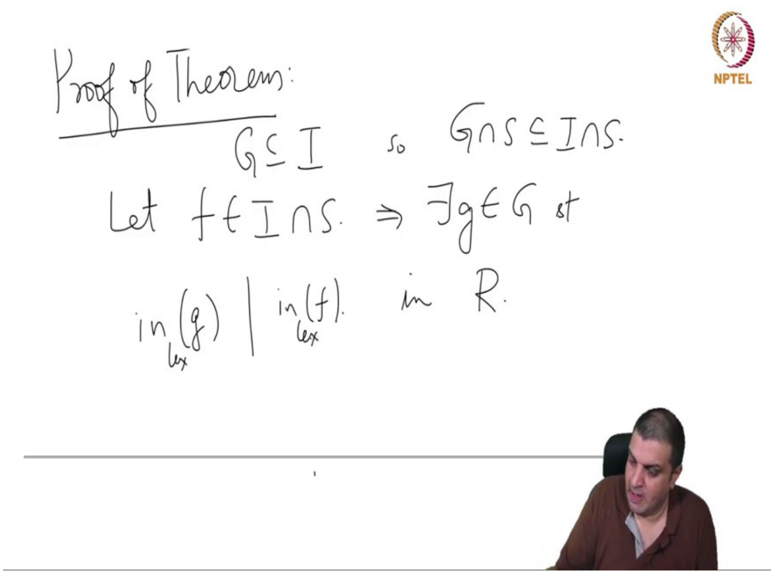
So, we will prove this in a minute it is not a very difficult proof. So, one observation that if you compute the lexicographic order, the Grobner basis of I with respect to the lexicographic order on R then we can compute this step by step eliminate X_1, then eliminate X_1 and X_2 eliminate X_1, X_2, X_3 and so, on.

(Refer Slide Time: 09:31)



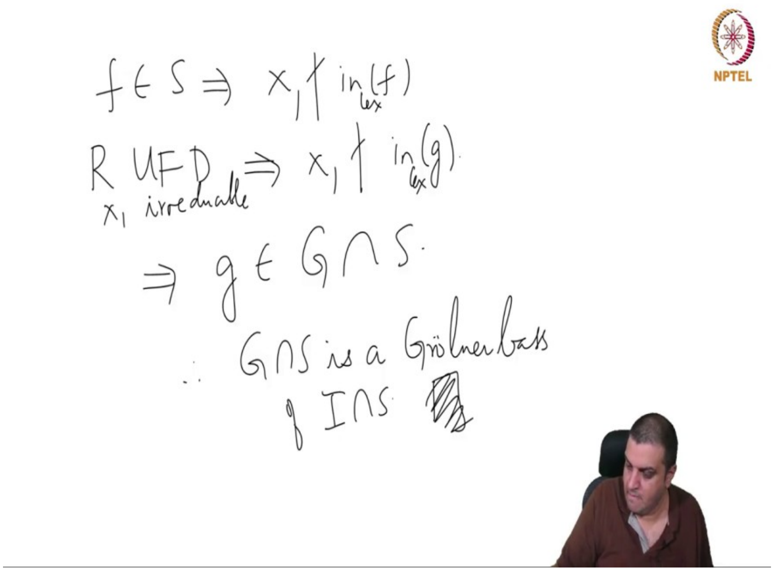
So, just a remark, $\forall m \leq n$, $I \cap k[X_m, \dots, X_n]$ has Grobner basis $G \cap k[X_m, \dots, X_n]$ with G as in the theorem. So, this is one can recursively eliminate more and more variables from the beginning this using lex. Now that observation we can prove the theorem.

(Refer Slide Time: 10:31)



So, note that $G \subseteq I$. So, $G \cap S \subseteq I \cap S$. So, we want to show this is a generating set whose initial terms give the initial terms of the elements of that ideal. So, let $f \in I \cap S$. So, it is inside I there exists a $g \in G$ such that the initial term of g divides the initial term of f in R, but f is inside S.

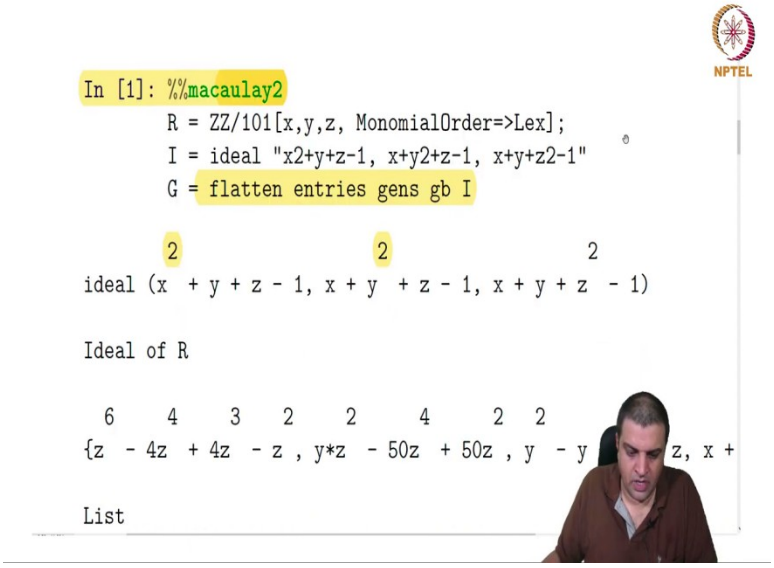
(Refer Slide Time: 11:41)



Notice that f is inside S. So, X_1 does not divide the initial term of f. R is UFD which means that X_1 is reducible X_1 does not divide the initial term of g. So, g is an element of S this now we implies that $g \in G$. So, we started off with an element inside G here and now because of this condition it is inside S. So, in other words this is a Grobner basis. So, around all these are considered with respect to lex.

The only observation that if you compute the initial term of f, $f \in S$, if you compute the initial term of f whether you think of it is an element of R or whether you think of it is an element of S the initial term is the same. So, similarly for g. So, these are with respect to lex and so, hence we see that this is the proof. So, $G \cap S$ is a Grobner basis of $I \cap S$ that is the another proof.

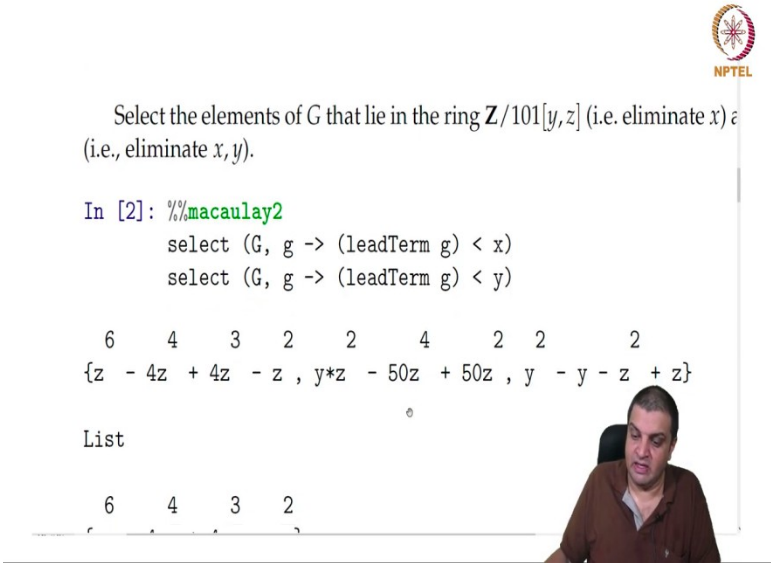
(Refer Slide Time: 13:27)



So, now let us look at one example in Macaulay. So, ignore that the first line, the Macaulay code that we have input is this lines that are offset R equals this and we are defining it in monomial order, then we are giving some ideal $\left(x^2+y+z-1, x+y^2+z-1, x+y+z^2-1\right)$ and then we ask for its Grobner basis then we ask for its generating set and remember in the previous examples we have seen this as a matrix, but in order to make to pick out the things that belong to the subring, we would like to just get it as a list and this is the you take entries it will give a list of lists and out of which you want to flatten it to one list and so, this is what we would get.

So, please look at the help pages of these commands flatten entries to make sure that you understand what this is. So, now, here is the output. If you ask for flatten entries gens. So, we ask for the ideal, ideal is this x square whatever we just put in and this is just some long list which cannot print in one line. So, it just goes on. So, that is the first line.

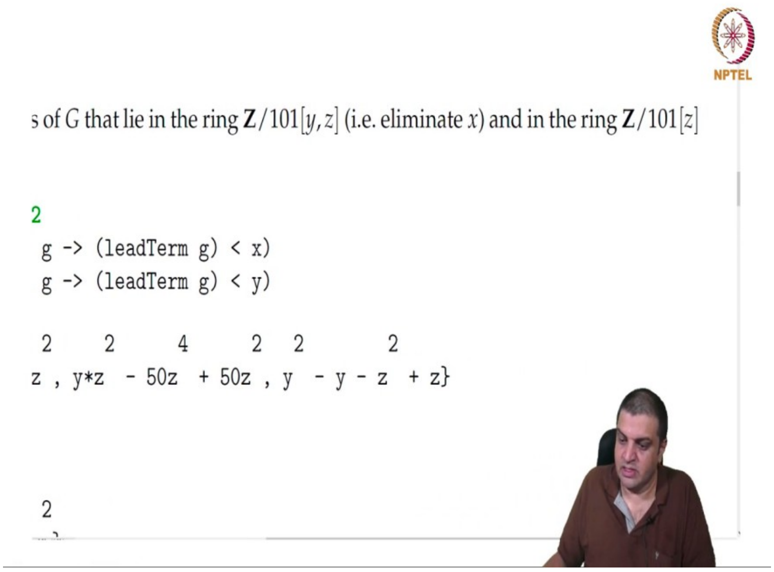
(Refer Slide Time: 14:44)



So, now, we would like to select the elements of G that lie in the ring in the ring where X is not there. So, the last the tail of the variable set y and z that is eliminate x and also in the ring

$\frac{Z}{101Z}$.

(Refer Slide Time: 15:01)



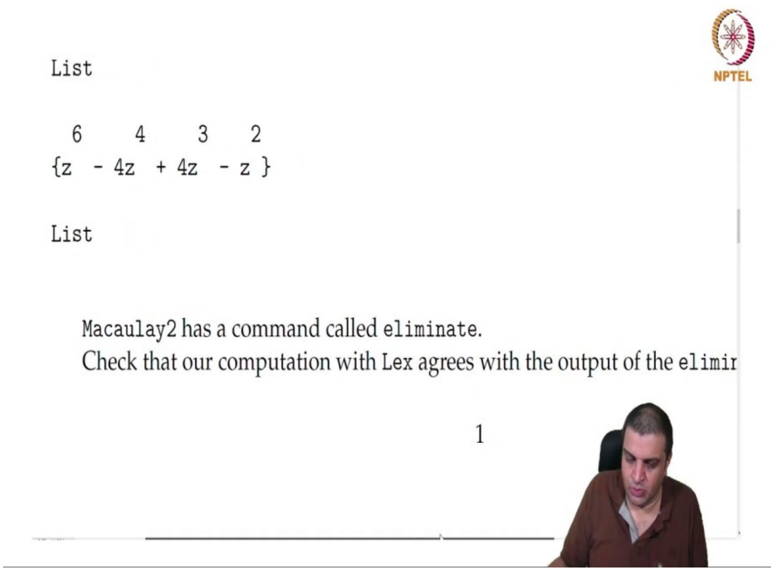
So, 101 is a prime number and $\frac{Z}{101Z}$ is a field and we would like to work with finite field at least to illustrate the examples because the computations are significantly faster and that is the only reason.

So, we would like to eliminate x first here and then x and y here. So, again just ignore this line which says in 2. So, this is just a header. So, just you can what you have to type into Macaulay is this line. So, let us select is a command and what it does is. So, this is a function g, so, this dash greater than denotes the maps to symbol in maths. So, it is a function which we define on without labelling the function. So, it is just. So, this is what we would write as a function. So, g gets mapped to this thing.

So, we are defining a function on g on this on the set on the list G and an element g of that set gets mapped to. So, this is the function lead term of g is less than x. So, this is a Boolean thing this either true or false and what select command does is it applies this function to every element of this list and picks out the one for which the answer here is true. So, here it means that pick out all the ones in which the lead term is lead term involves only y and z and so, it write something out here it is just again very long.

So, here is one with pure power of z here is one with y^2 and so, on. So, it gives us some list. So, this is the elimination in eliminating x. If you ask for the second command the same thing we ask for lead term less than y which means that the lead term the initial term can involve only z.

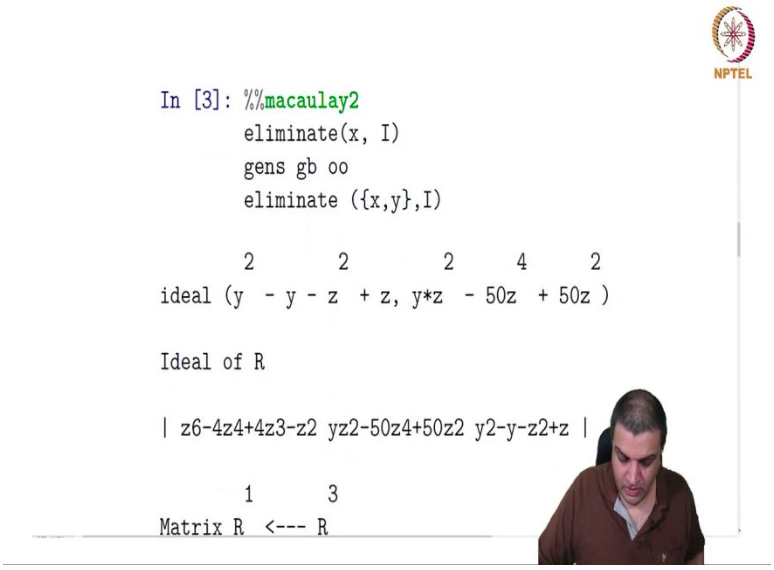
(Refer Slide Time: 17:04)



So, it eliminates everything other than z and here is what we get. So, in fact, there is a simpler there is another command in.

So, this is just to illustrate how lex works. One does not always need to use lex one does not always need to use this approach, there is a command called eliminate in Macaulay directly and the advantage of that command is that depending on the ideal, it can try to make some optimizations which on computing the Grobner basis or maybe skipping some steps etcetera. So, there is a separate function and it is probably better to use that. So, let us just anyway compare it compare that our computation with lex agrees with the output of the eliminate command ok.

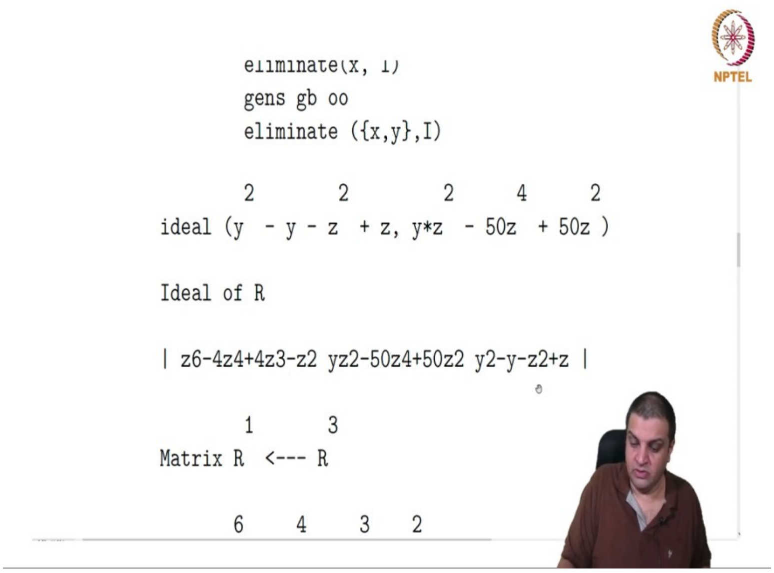
(Refer Slide Time: 18:52)



So, here we are just using this the same I the one generated by those three polynomials. We ask eliminate(x, I) and then we asked show us the generators. So, if you just ask eliminate x,y, it only showed us two generators, but actually if you write out this code here, you will say there are three things here 1, 2 and 3 at least. And when you actually run it, you can count how many there are.

So, here we eliminate we only get two, but the reason is that it has shown as a minimal generating set and not the Grobner basis.

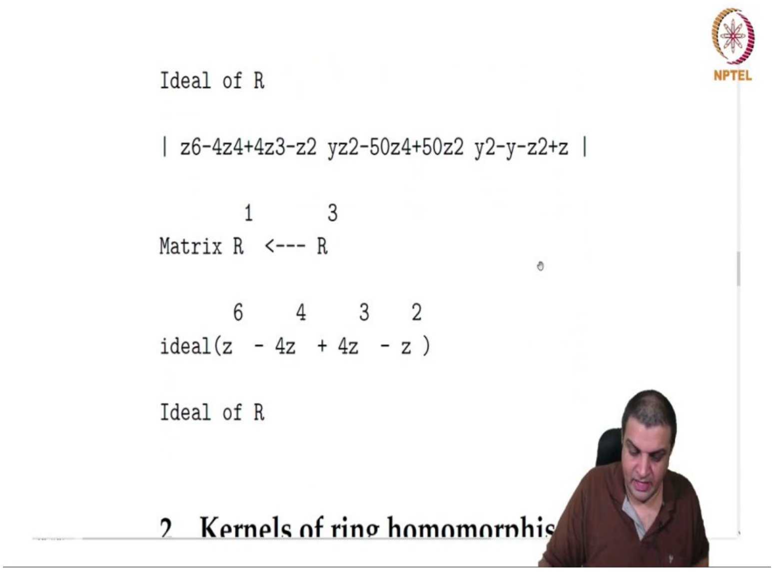
(Refer Slide Time: 18:44)



So, we can ask for its Grobner basis gens gb and it shows us those three polynomials. However this is there in the lex order when we selected everything less than x this is what we would have got and when you ask for eliminate.

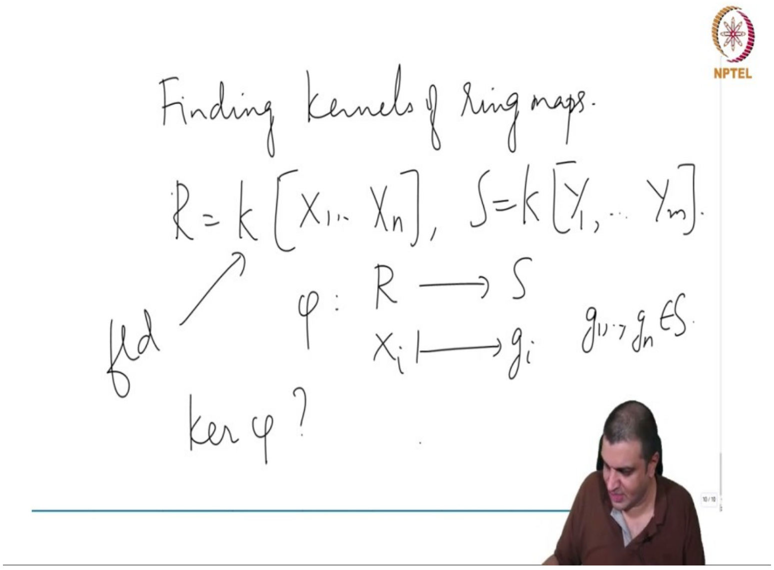
So, now if you want to eliminate multiple variables you have to give them as a list and you can look at the help pages of these commands to see how they have to be invoked.

(Refer Slide Time: 19:12)



So, eliminate x, y the list comma I it eliminates x and y and gives us this output. So, that is the example about a elimination and as an application of this elimination, we want to discuss one problem that we have become familiar I mean one that we saw from the second lectures itself, if finding kernels of ring maps.

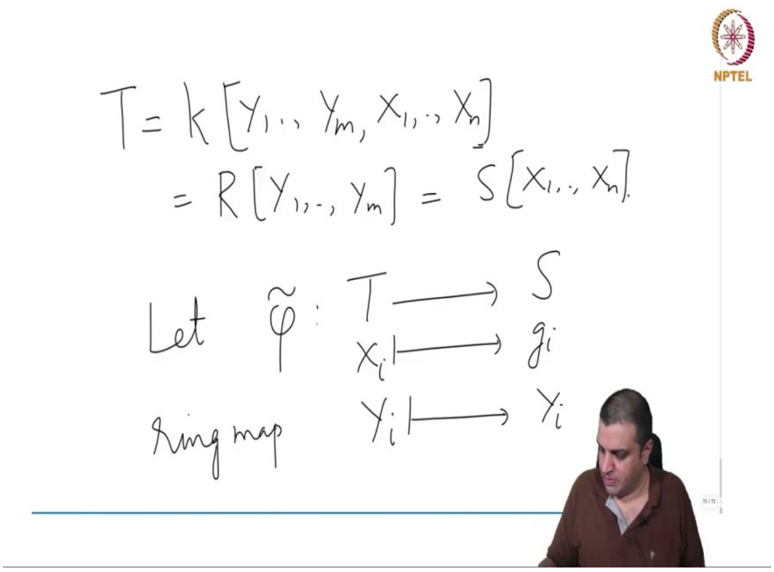
(Refer Slide Time: 19:35)



So, we will be able to do only a special case involving polynomial rings, but nonetheless it should give as an idea on how we can actually compute it ok. So, what we want is, suppose let us say R is a polynomial ring again over a field $R=k[X_1,\ldots,X_n]$, this is a field no assumption on algebraic closure, S is a polynomial ring in some different set of m variables $S=k[Y_1,\ldots,Y_m]$ and ϕ is a map from R to S sending X_i to g_i keeping the elements of k fixed.

So, $g_1,\ldots,g_n$ are elements of S. We would like to know what is kernel of ϕ how would we compute kernel of ϕ. If you ask Macaulay it would compute, but let us try to understand one way of computing it using elimination.

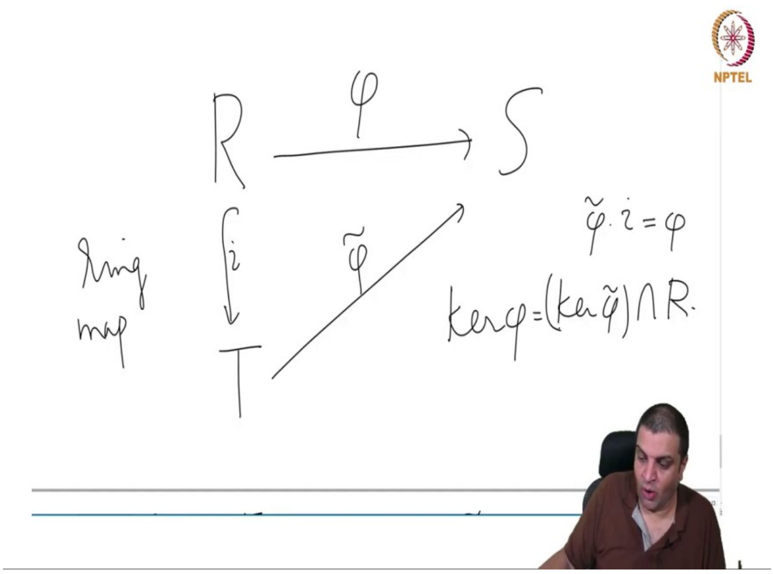
(Refer Slide Time: 21:02)



So, let us define a bigger ring T which is what the Ys and the Xs and we would like to think of this as in two different ways, we can think of it as R adjoin the Ys and also as S adjoin the Xs.

So, now let us define a ring homomorphism, let $\tilde{\phi}$ be the ring homomorphism from T to S in which the X_i variables go to g_i's as it would have happened in R and the Y_i variables are themselves are not changed. So, this is a ring map. What is the kernel of this ring map? So, before we go ask the kernel let us understand why we are interested in this.

(Refer Slide Time: 22:12)

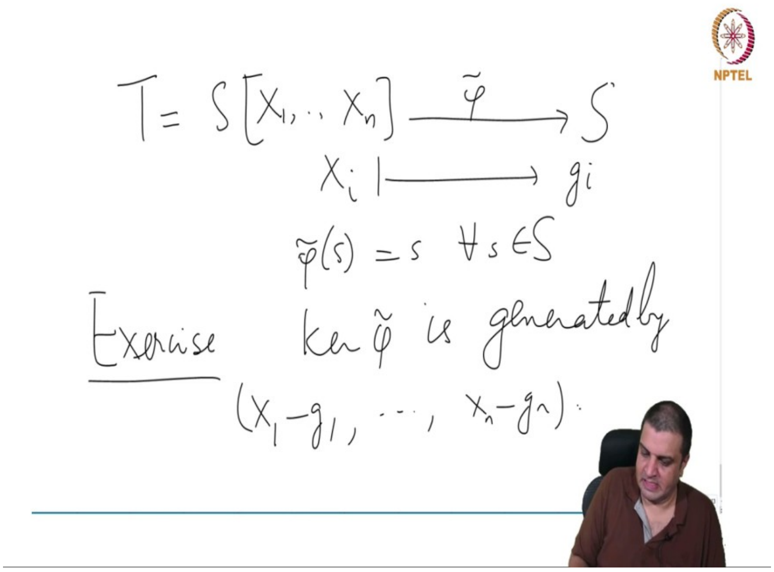


So, we have R here S this is again map ϕ then we have T here and a map $\widetilde{\phi}$.

Now, there is an inclusion map as a ring map. So, let us call this map i for inclusion. So, notice that if you take i and then apply $\widetilde{\phi}$ this is same as ϕ and kernel of ϕ is kernel of $\widetilde{\phi}$ contracted to R. So, that is the reason why we would like to study this map instead of that. So, now, this gives us an idea that maybe there is some elimination involved inside here. So, if you find the kernel of $\widetilde{\phi}$, then we can eliminate the Y variables and then we will just get some ideal inside R.

So, let us try to understand what the kernel of $\widetilde{\phi}$.

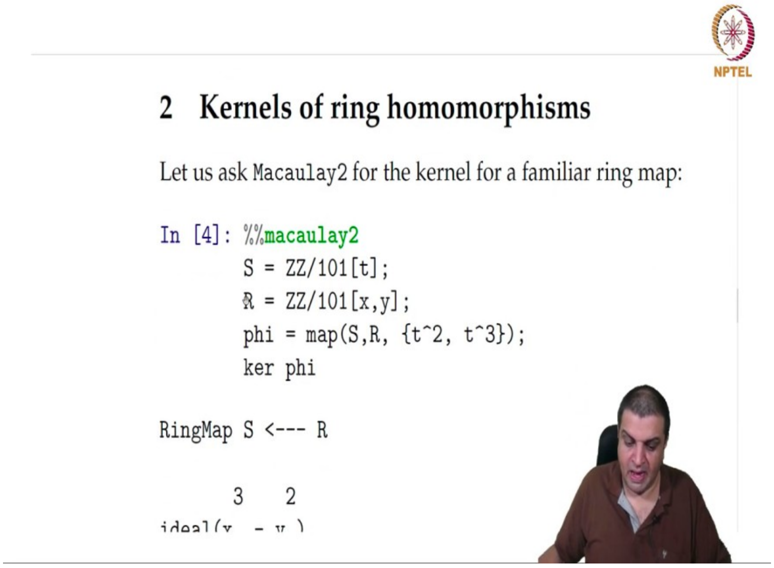
(Refer Slide Time: 23:26)



So, T is S adjoined the Xs and we have a map to S $\widetilde{\phi}$ in which X_i goes to g_i and elements of S are unchanged. So, it would be an exercise and this is something similar to that we did for in the exercise, it is something that we did in the proof of a remark for Nullstellensatz that kernel of $\widetilde{\phi}$ is generated by the set $X_1 - g_1, \ldots, X_n - g_n$.

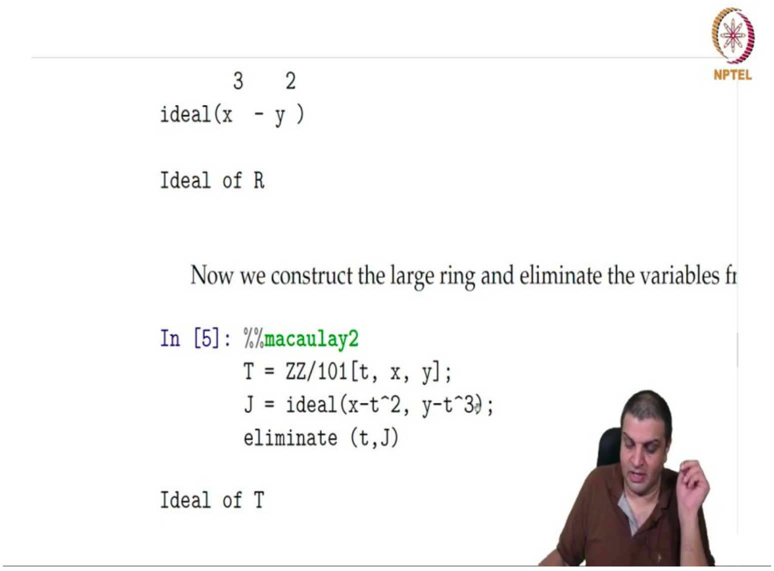
So, this one can prove it without much difficulty and so there is an easy description of this kernel and then going and then we do an elimination remember in the X variables first we will not eliminate the Ys. So, when we order, it should be ordered with the Ys to the beginning and then the Xs in the lexicographic order and then we just apply this algorithm.

(Refer Slide Time: 25:07)



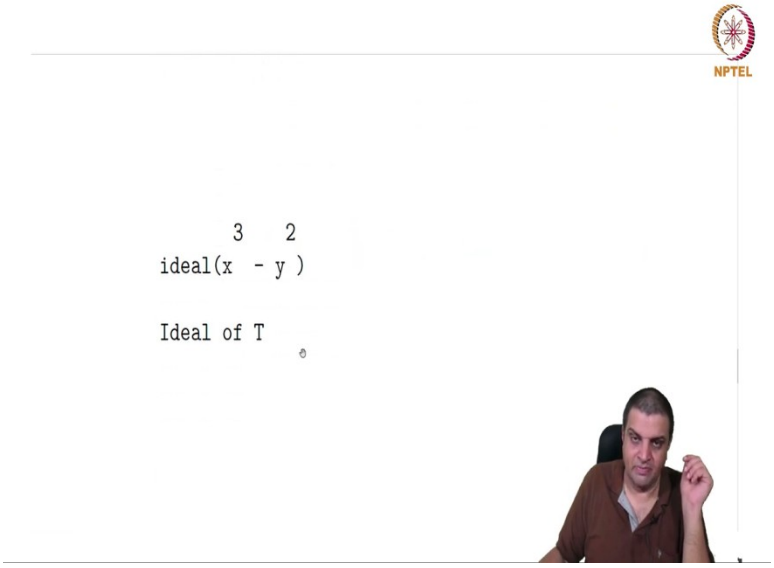
So, now, let us try to do this. So, here we have a map from R to S, R is the polynomial ring in two variable and S is the polynomial ring in one variable and we define a map x goes to t^2 and y goes to t^3 and this we have worked out earlier.

(Refer Slide Time: 25:20)



Now, let us do it the way we had just described earlier, we put the y variables I mean the variables of S first which is the these things and then the variables of the ring R, x and y and then we just generate this ideal we just write down formally write down $x-t^2$ and $y-t^3$ no thought has to be applied depending on and then we just say eliminate t.

(Refer Slide Time: 25:56)



So, if you use this command then you do not have to specify its lex order then Grobner basis etc just use this command directly and it now says ideal $(x^3 - y^2)$ square here it says ideal of R here it says ideal of T. I mean there is still some minor issue like this because elimination in this situation elimination is done in T itself, but one can safely ignore this part and think of it as an ideal of R.

So, that is the end of this lecture on elimination. From now we will discuss a little bit more abstract things and develop more things related to. So, we will start off with modules and then proceed from there.