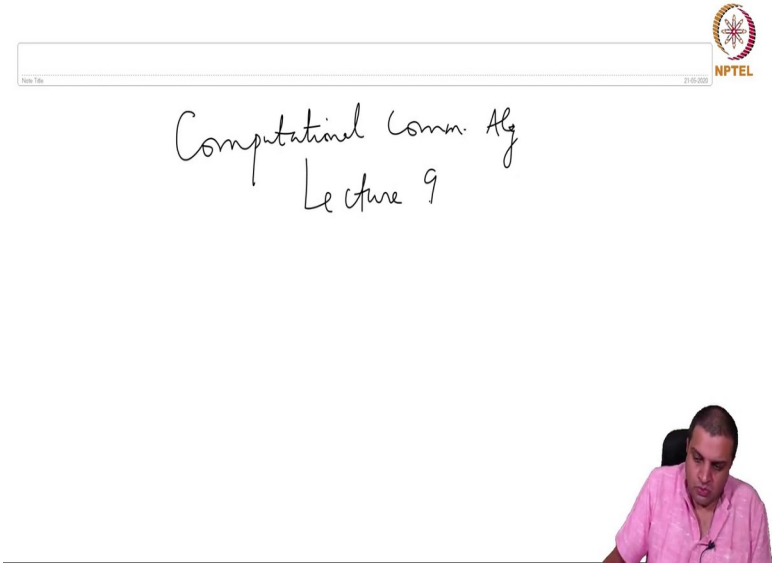
Computational Commutative Algebra
Prof. Manoj Kummini
Department of Mathematics
Chennai Mathematical Institute

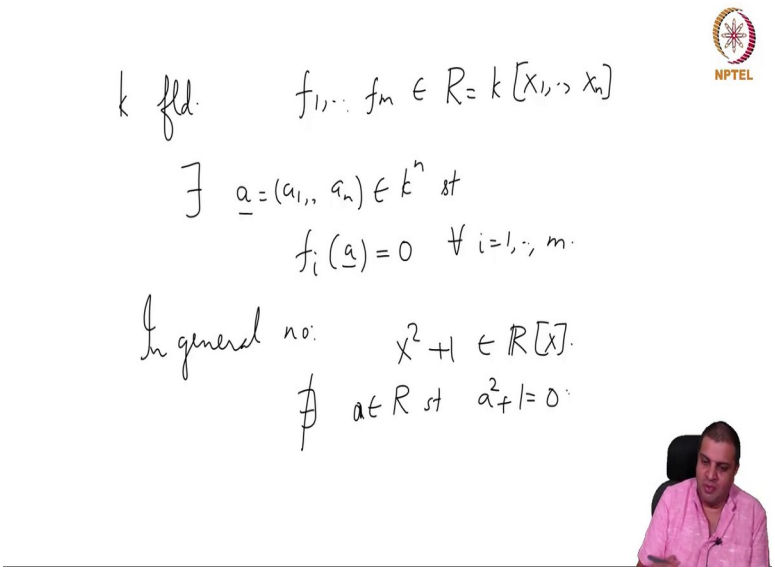
Lecture – 09
Solving Polynomial Equations

(Refer Slide Time: 00:21)



Welcome this is the 9th lecture of Computational Commutative Algebra. And in this lecture we will look at the question about Solving Polynomial Equations and some definitions and notions that we have developed along the way. And we will learn so, in and in the subsequent towards the lectures we will look at this theorem called Nullstellensatz originally proved by Hilbert and we will see some few variations of that same theorem and we will prove them as we need.

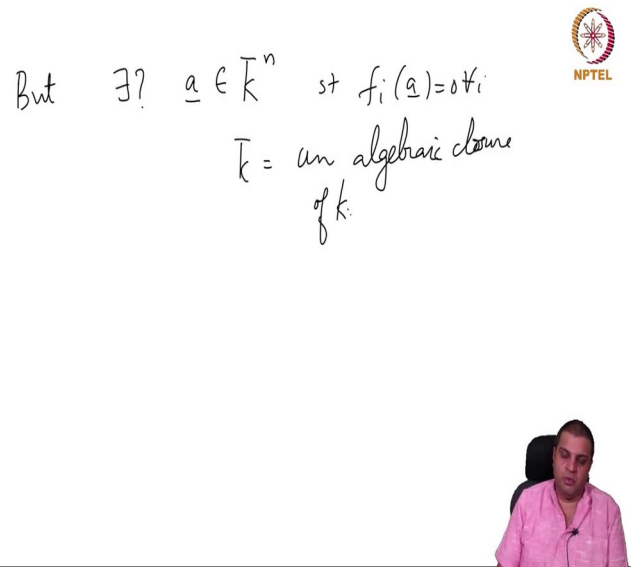
(Refer Slide Time: 01:10)



So, we ask the following question; k it is a field and we take some m polynomials $(f_1, \ldots, f_m)$ in $k[x_1, \ldots, x_n]$. I mean finitely many polynomials in finitely many variables. Then we ask this question does there exist such that $f_i(a) = 0$ for all $i = 1, \ldots, m$.

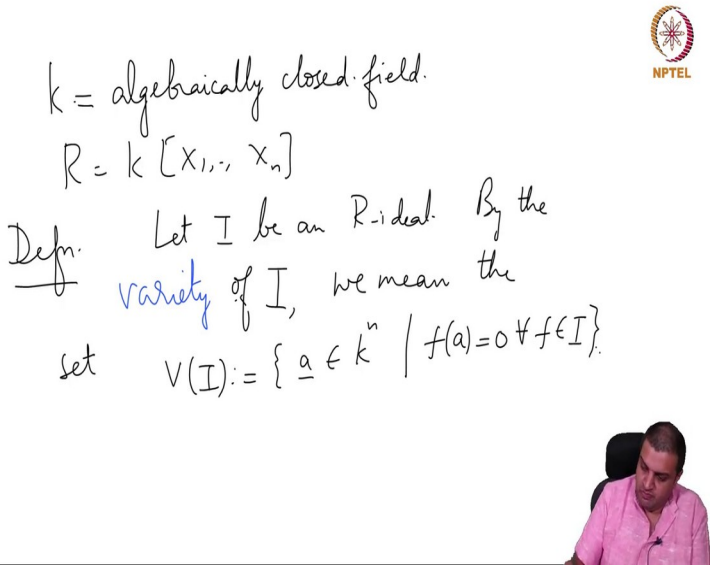
So, we know the answer right away the answer in general is no, if you look at the polynomial $x^2 + 1 \in R[x]$. there does not exist any real number a such that $a^2 + 1$ is 0. So, the answer in general is no but, well that is because R is not algebraically closed. So, we might say that. So, that is what we want to understand.

(Refer Slide Time: 02:39)



But does there exist a point $a \in \bar{k}^n$ such that $f_i(a) = 0$ for all i. So, we may want to ask this question. So, $\bar{k}$ here is an algebraic closure. So, this at least we can try to solve and this is what we want to do now.

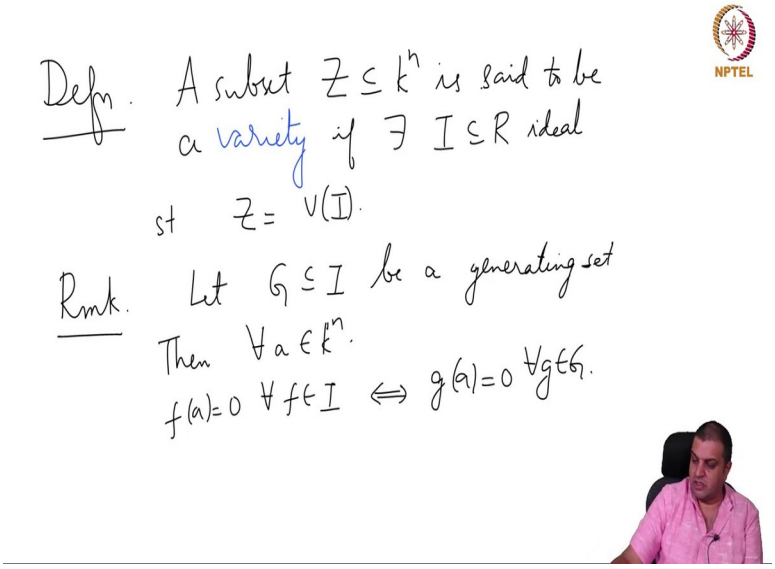
(Refer Slide Time: 03:31)



So, now we take k to be algebraically closed because even single polynomial in one variable might not have a solution if the field is not algebraically closed. So, we would like to construct we would like to work with them. So, $R = k[x_1, \ldots, x_n]$ and definition.

Let I be an R ideal, by the variety of I we mean the set $V(I) := \{a \in \bar{k}^n : f(a) = 0 \ \forall f \in I\}$. In other words this is the set of common zeros of all the elements in I and sometimes it is called an affine variety, but for us this is the only thing that we are going to see for now. So, we just use the word variety.

(Refer Slide Time: 05:20)

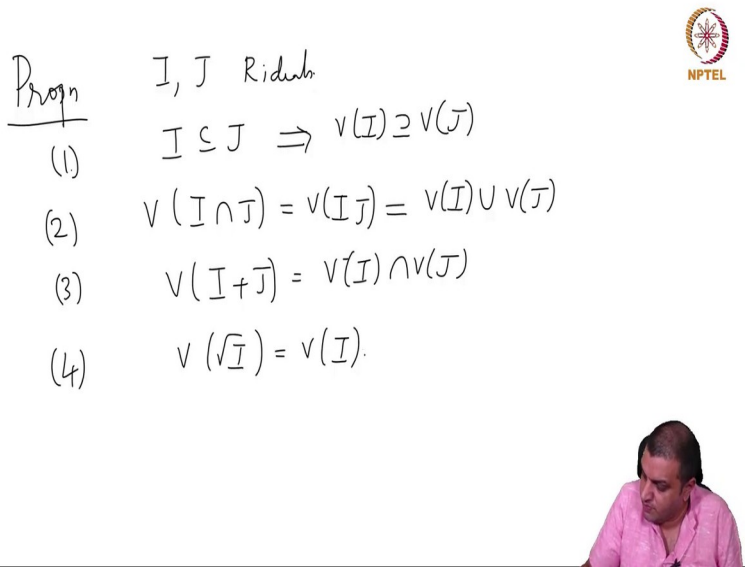


Definition, a subset $Z \subset k^n$ is said to be a variety if there exist an ideal I such that $Z = V(I)$. So, the point is we are interested in studying the set of zeros of a family of polynomials.

So, remark; let $G \subset I$ be a generating set , then for all $a \in k^n$, $f(a) = 0$ for all $f \in I$ is equivalent to saying that $g(a) = 0$ for all elements in the generating set G . So, this is not this is not very difficult to prove and I will leave it as an exercise.

So, if you prove that for a generating set any such f can be written as an R linear combination of these g's and evaluating f at a is same thing as evaluating the combination at a, then you will get R of a times g of a and then. So, you can write this condition . So, here are some basic properties.

(Refer Slide Time: 07:20)



So, throughout I, J are R-ideals in this list of properties,

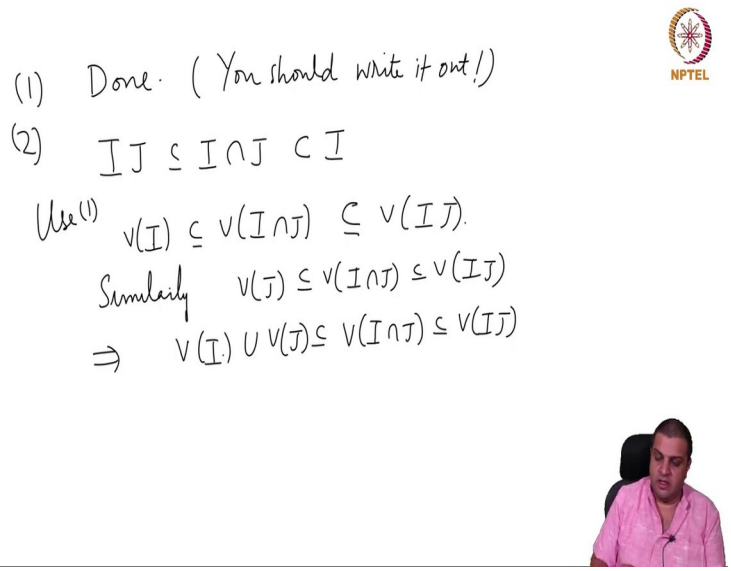
1) if $I \subset J$, then $V(J) \subset V(I)$ so, this is containment order reversing.

2) $V(I \cap J) = V(IJ) = V(I) \cup V(J)$.

3) $V(I+J) = V(I) \cap V(J)$ perhaps we did not discuss what a sum of 2 ideals is. So, when I prove it I will just explain what that is.

4) $V(\sqrt{a}) = V(I)$. 4 is related to Nullstellensatz this is an extremely weak version I mean this is not our goal it is just an easy observation for now. So, let us prove these things.

(Refer Slide Time: 08:58)



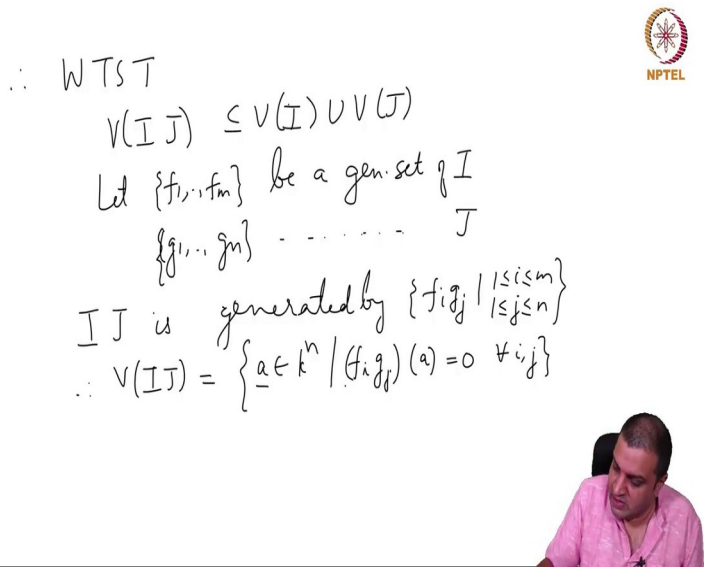
So, let us look at 1. So, 1 is going to be an exercise $I \subset J$. So, we want to prove this statement.

So, if you take a point a inside V(J), every element of J vanishes there hence every element of I vanishes there. So, that gives us proof. So, 1 is done I mean or you should rewrite whatever I just said you should write it out.

2, (Refer Time: 09:44), So, we will use 1) throughout in these arguments. So, let us look at these statements. So, notice that $IJ \subset I \cap J \subset I$ also intersection is inside J. So, this thing applying 1 to this we would get that $V(I) \subset V(I \cap J) \subset V(IJ)$.

So, this is just a use 1) we have this order and V reverses that order. So, this is the smallest, this is the middle one and this is the largest similarly $V(J) \subset V(I \cap J) \subset V(IJ)$ same reason we could put a we could have put a J there . So, hence these are subsets of this set so, $V(I) \cup V(J) \subset V(I \cap J) \subset V(IJ)$. So, what we need to prove is this is contained inside here. therefore, we want to show that $V(IJ) = V(I) \cup V(J)$.

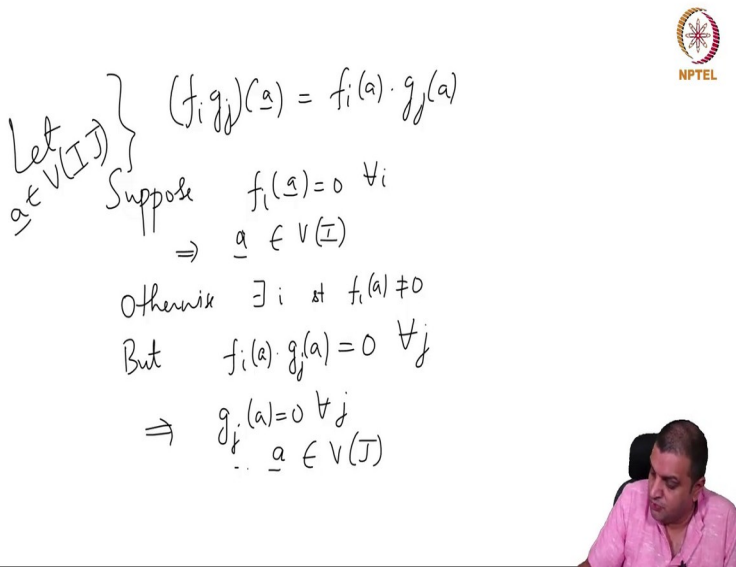
(Refer Slide Time: 11:27)



So, let us take generating sets for these let these. So, we have already proved that these ideals are finally, generated. So, for simplicity let us just take finite generating set $\{f_1,\ldots,f_m\}$ be a generating set of I and respectively $\{g_1,\ldots g_n\}$ generating set for J ok. Then I J is generated by the product $\{f_i g_j : 1\le i\le m, 1\le j\le n\}$.

. So, then we already noticed that therefore, $V(IJ)=\{a\in k^n : f_i g_j(a)=0\ \forall\ i,j\}$ So, now let us this is the remark that we made earlier, but what does this say? Suppose.

(Refer Slide Time: 13:32)

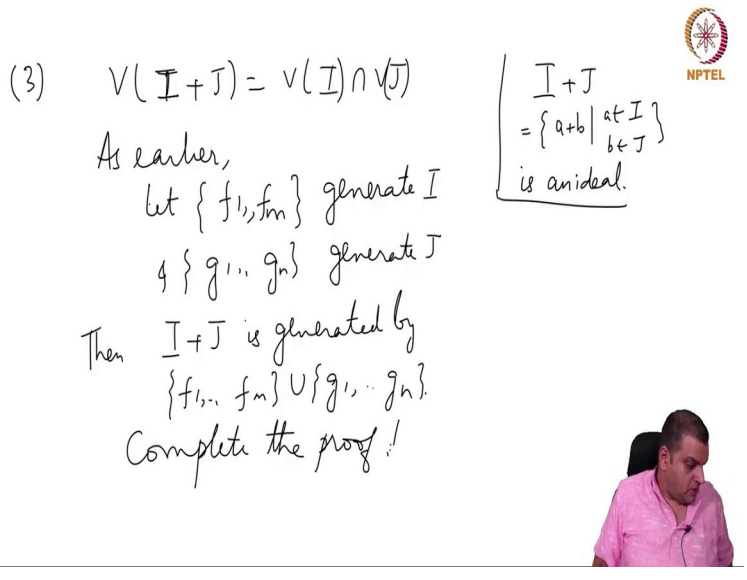


So, let us notice that when we evaluating a product of a polynomial at a point is same as evaluating them individually and then take the product. Now let $a \in V(IJ)$ suppose $f_i(a)=0$ for all i.

We want to show that it $a \in V(I) \cup V(J)$. So, if this is true then $f_i(a)=0$ for all i, then $a \in V(I)$ otherwise there exist an i, such that $f_i(a) \neq 0$, but now we use it as a product, but $f_i g_j(a)=0 \; \forall \; j$. So, in other words this says that $g_j(a)=0$ for all j or in other words $a \in V(J)$ which is what we wanted to prove $a \in V(I)$ or $a \in V(J)$.

So, this proves this claim and then putting that back here we get equality for these three thing that was statement 2.

(Refer Slide Time: 15:29)



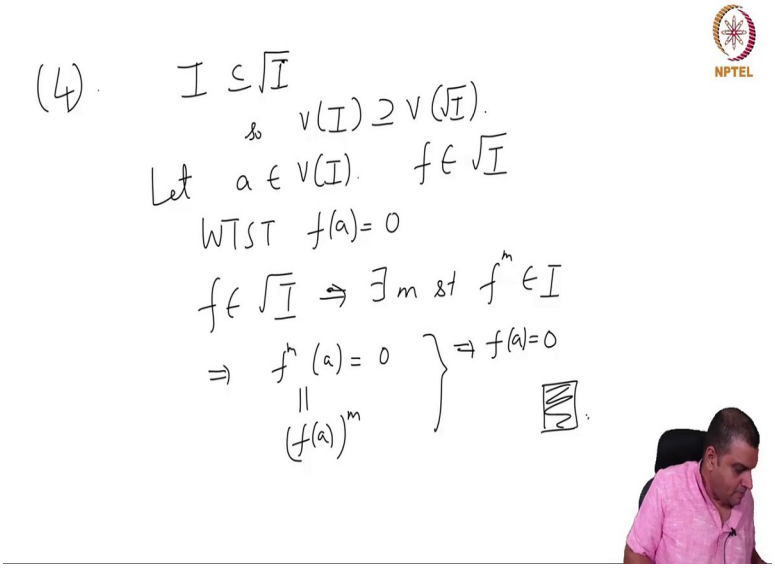
So, now 3 is we want to prove that $V(I+J)=V(I) \cap V(J)$. let me just briefly say what $I+J$ is. So, this is in general for any ring not just polynomial rings etcetera. $I+J=\{a+b : a \in I, b \in J\}$ is an ideal and one can show that this is the smallest ideal that contains I and J or in other words it contains $I \cup J$. So, I plus J it is it is easy to check that if you take sums of elements like this if you take b to be 0 then it is just the same as I.

If you take a to be 0 this is just same as J and if you take elements like this a sum of 2 such elements will also have the same form if you take such an element and multiply by an element of the ring it will still have the same form. So, this is an ideal. So, the remark that we want to make is so, as in the as earlier as earlier.

Let $\{f_1, \ldots, f_m\}$ generate I and $\{g_1, \ldots, g_n\}$ generate J. So, then I plus J is generated by the union $\{f_1, \ldots, f_m\} \cup \{g_1, \ldots, g_n\}$. So, if a point vanish is inside here then it vanishes for these and for these which proves that it is in the intersection.

So, now the rest is let me complete the proof I will say it, but. So, let me just say it you should write out the details. So, what is $V(I+J)$. So, it is a point which it is a at which these functions and these functions vanish since these functions vanish it is in $V(I)$ since these functions vanish it is in $V(J)$. So, the left side is inside the right side. Conversely if you take a point inside $V(I) \cap V(J)$ these functions vanish and these functions vanish hence every linear combination of it R linear combination also vanishes. So, it is inside V (I + J) . So, this is the proof.

(Refer Slide Time: 18:49)



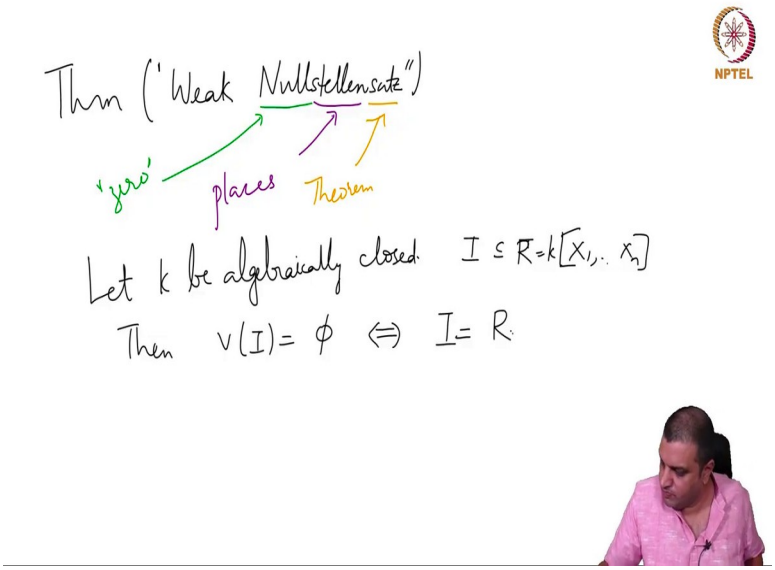
So, next is a precursor to the Nullstellensatz. So, this is the fourth statement that we had. So, we know that $I \subset \sqrt{I}$. So, $V(\sqrt{I}) \subset V(I)$. So, this is on the statement. Now let us prove the other direction.

So, let $a \in V(I)$ and $f \in \sqrt{I}$. So, we want to show that $f(a)=0$ that is what we will prove that $a \in V(\sqrt{I})$, but f is inside the radical means that there exist an m such that $f^m \in I$ which means that $f^m(a)=0$.

But what is this, this is the same as $f(a)^m$. So, now, this implies that `f(a)=0` which is what we wanted to prove. So, an ideal and it is radical have the same variety. In fact, Hilbert's Nullstellensatz will say that the radical of the ideal is the largest ideal with the same variety as the ideal. So, $\sqrt{I}$ is the largest ideal J such that $V(J)=V(I)$ that is Nullstellensatz.

So, it will take us a little while to get there . So, now, let us state Nullstellensatz which talks about solutions to polynomials.

(Refer Slide Time: 21:02)

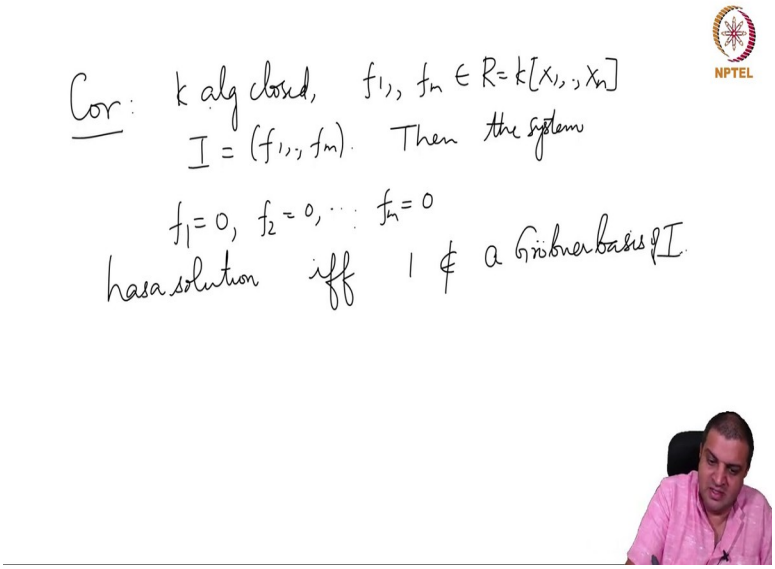


So, this is theorem this we will refer to as the 'Weak Nullstellensatz' following the book by (Refer Time: 21:10) and there are various versions some weaker than the other weak Nullstellensatz. So, what does this mean, what is the word Nullstellensatz mean. So, null here is for 0, then stellen is here for places and satz is theorem. So, I mean not this version, but a different version of this was proved by Hilbert it is called it is been stated probably in the next lecture Hilbert's Nullstellensatz and that was a theorem about when polynomials would have solutions and we will see the way it is stated.

So, let k be algebraically closed. I an ideal of $R=k[x_1,\ldots,x-n]$, then $V(I)=\emptyset$ if and only if I = R. In other words any proper ideal of R every element of it vanishes at some point inside k^n it there cannot be a common solution if and only if I is not a proper ideal.

So, we will not prove this now we will we postpone the proof to the next lecture. So, now, we would like to see it as a way of solving polynomial equations. So, we will still see do this only for algebraically close fields and in the exercises I will tell you how to do this for the same statement for other fields. It requires a little bit of calculation and thinking about how to go from an arbitrary field to an algebraic to an algebraic closure. So, we will not do that right now.

(Refer Slide Time: 23:51)



So, here is a corollary which is what is useful for us to solve how is all the Grobner basis coming to picture to do this. So, let us just assume k is algebraically closed $\{f_1,\ldots,f_m\}$ inside polynomial ring, then let I be the ideal generated by them then the system $f_1=0, f_2=0$.

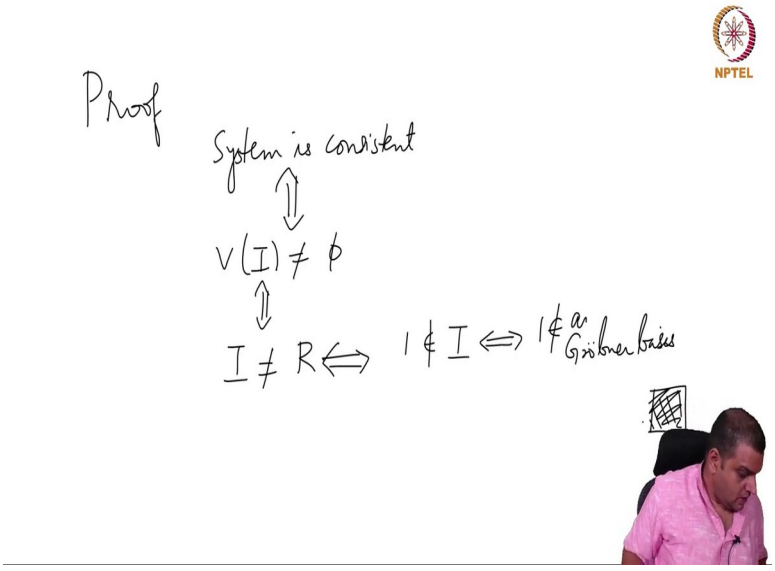
So, this is what we mean by solving polynomial equations of course, we could put constants there also, but we can put the bring the constant back to the side and make it 0 just relabel what f_1 means or what f_2 means. So, we can as well assume that we are

interested in solving polynomials equal to 0. So, zeros of polynomials system has a solution if and only if 1 is not in any 1 is not in a Grobner basis of I. So, here is an immediate application of what we have studied so far and whether 1 is in a Grobner basis. So, this is again I mean you can rephrased as an ideal membership problem, but it is easier to state at least it is easier to visualize this way there are algorithms which we will compute Grobner basis.

So, given $\{f_1, \ldots, f_m\}$, we just put these into the algorithm it will give us some $\{g_1, \ldots, g_n\}$ which is a Grobner basis for 1 and you just check if 1 is there in it or not if 1 or any constant is not is not there then it has a solution. So, this is a very convenient computational way of determining. So, of course, it is not actually giving us the solutions it actually has only tells us if the thing is if the system is consistent.

So, there are other ways to solve the system, but that we will you know we are not ready to discuss it now. So, let us prove the corollary and in the exercises we will we will remove the requirement of algebraically closure close in this part, but; however, we can never determine using these arguments whether there is a solution in that field itself I mean all of these arguments will only give us a if there is a solution in the algebraic closure and we will see some example we will see an example.

(Refer Slide Time: 27:01)

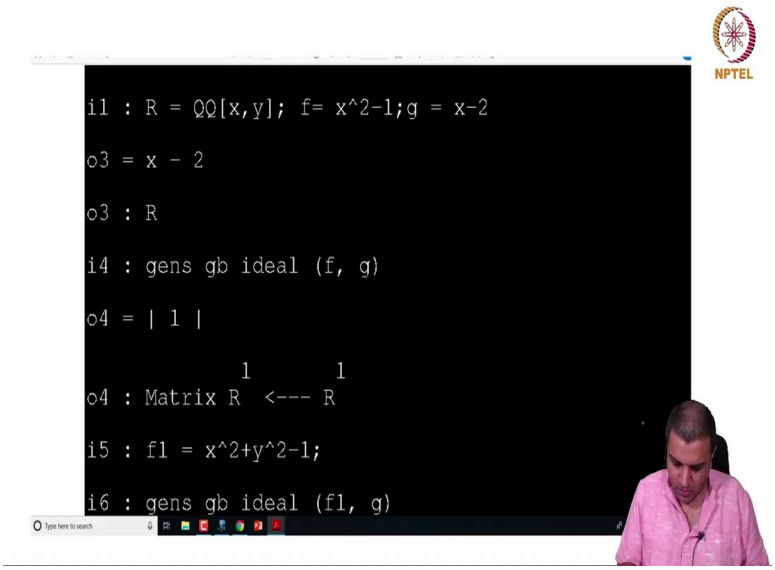


So, the proof is not very difficult at all, system is consistent is same thing as saying that $V(I) \neq \emptyset$, this is the same thing as saying $I \neq R$, well I is not R. So, we want to show that this is the same thing as this is the same as saying 1 is not in the ideal, but what does this say? This is the same as 1 is not inside I.

If 1 is inside I then every ring element is inside I conversely I mean if if I = R then 1 is inside I. So, this is equivalent, but notice that this is the monomial, 1 is a monomial . So, therefore, this must 1 is not in any in a Grobner basis. So, that is the that is it is an easy proof all the new thing that we need to observe is that I is equal to R if and only if 1 is inside I.

If and only if 1 is in a Grobner basis. So, this is all that we need. So, Grobner basis and with the version of Hilbert's Nullstellensatz that we just proved gives us ah. So, a way to determine if a system of polynomial equations is consistent , with this we you shall let us look at a small example in macaulay. So, just one small example mostly yeah.

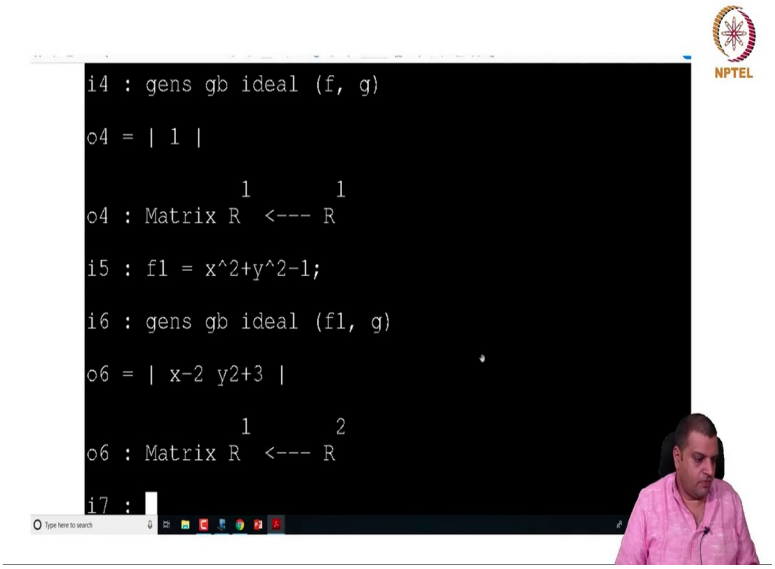
(Refer Slide Time: 28:44)



So, here a polynomial ring in 2 variables over the rationals $f = x^2 - 1$ and $g = x - 2$. So, there are not going to have a solution in the integers, sorry this is not going to have any solution over any field, g = 0 implies that x = 2, but if x = 2 then $x^2 \neq 1$. It is true I mean I apologize it is true in Z mod 3, but it is it is not going to have a solution in Q . So, sorry that is just.

I forgot to put a semicolon here. So, it just gave the output of what g is, it did not it suppress the other outputs let us ignore that. We ask generators, for generators of a Grobner basis of the ideal generated by f and g and it returns 1. So, 1 is there in a Grobner basis and this system is inconsistent $x^2-1=0, x-2=0$ is inconsistent I mean this we can do it by inspection by ourselves.

(Refer Slide Time: 30:06)



But if you had a larger system in many variables this is a convenient way. Let us look at a slightly different example x^2+y^2-1. So, this is the equation of a circle if you are thinking about it in R^2 and then we ask f this equation along with $x-2$ of course, this has no solution in rationals because if x= 2, then you cannot get $x^2+y^2=1$.

Let us compute Grobner basis, but the Grobner basis does not contain 1 and the reason is well let us let us look at this way x = 2 $y=i\sqrt{3}$ that is $y^2+3=0$ is a solution. So, the Grobner basis will only detect if there is a solution or the system is consistent or inconsistent with respect I mean in the algebraic closure and not directly in the field itself ok.

So, this is a part that we have to be aware of and of course, we are not proved this fact that, but here at least it is clear that this system has a solution over Q bar algebraic

closure of Q. So, this is the end of this lecture and in the next lecture we will study we will try to prove Nullstellensatz and then other way other versions of Nullstellensatz and we will use this further to understand some more properties of Grobner basis.