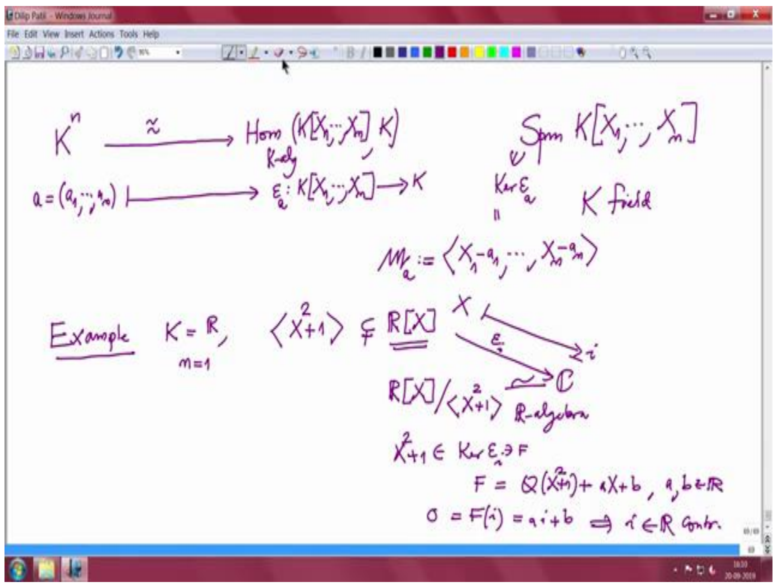
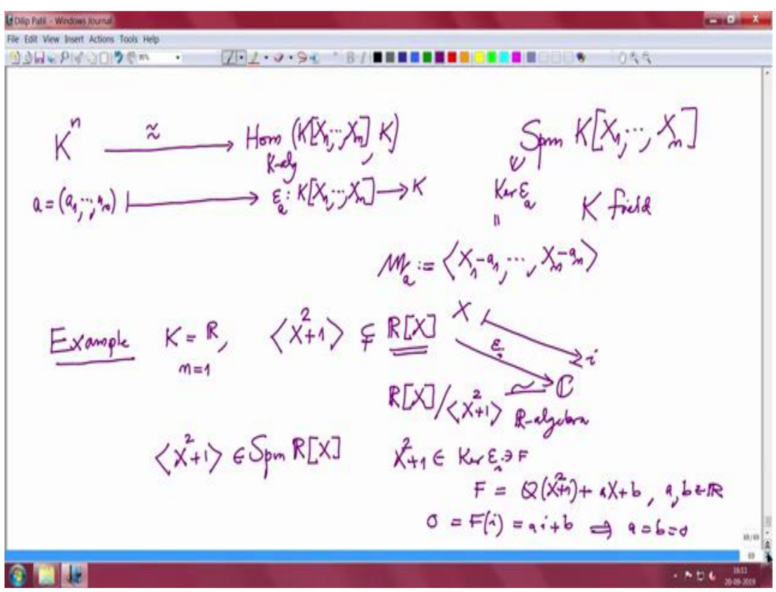
Introduction to Algebraic Geometry and Commutative Algebra
Professor Dr. Dilip P. Patil
Department of Mathematics
Indian Institute of Science, Bengaluru
Lecture 10
Finite and Finite Type Algebras

So, welcome back to this later half of today's lecture. So, we have seen how to produce concrete maximal ideals in the polynomials algebra. We will use this to construct also, maximal ideals which are not of this type.

(Refer Slide Time: 00:59)





So, this so let me write again what we have proved, what we were looking for this set of maximal ideals Spm K X1 to Xn and remember that K is a field and we have Kn here and we have Hom K algebras polynomial ring K X1 to Xn values are in K. This we have checked that, this is an isomorphism, not isomorphism this is a bijective map.

So, a a1 to an this is going to that epsilon a. This is algebra homomorphism from the polynomial ring, K X1 to Xn into A and then we have, what we have checked is the kernel of this homomorphism that is a kernel, kernel of epsilon a this is a maximal ideal that is what we have checked.

And also we have proved that this kernel is generated by these polynomials X1 minus a1, Xn minus an. So, this is also see, this is also I want to denote by m suffix a. Now, one might think that all maximal ideals are like this. So, first of all let us see some examples, so that there are other maximal ideals which are not like this. So, one example let us see, let us take K equal to R and let us look at the ideal generated by X square plus 1. I am taking only n equal to 1.

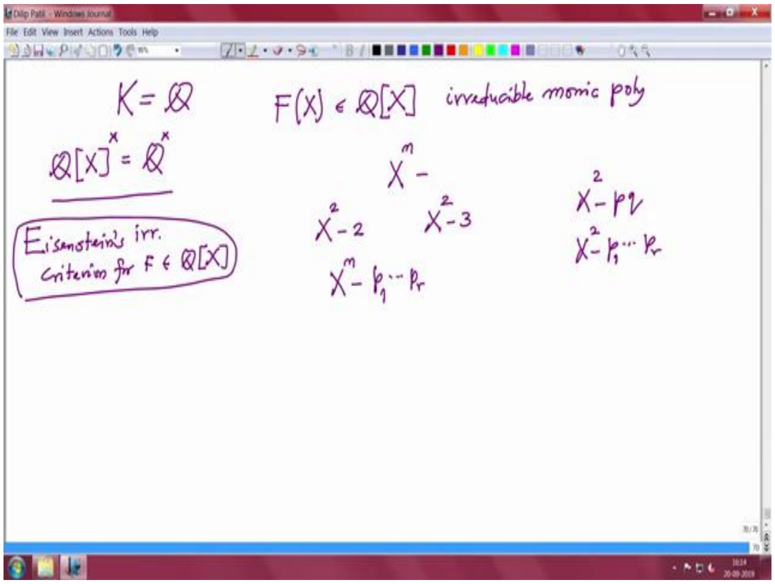
Well, we have checked that this is a proper ideal in R X and then whether it is maximal or not, we have to check whether the question residue class ring is a field or not. So, what is a residue class ring in this case R X mod X square plus 1. This is isomorphic to c as R algebras. In fact, we can give the isomorphism, in fact you can define a map from R X to c by our universal property of the polynomial ring. That I will say in capital X to i, imaginary unit. Once it goes to i, this polynomials is in the kernel. So, this polynomial X square plus 1. This is epsilon suffix i, belongs to kernel of epsilon suffix i.

But now use division algorithm to check that this polynomial generates it. This is a monic polynomial and if you take anybody else in the kernel F, what do you do? This is a real polynomial and divide by this monic polynomial, you can always divide. So, and write it Q times X square plus 1 plus a linear term will come and that will not, so linear term will look like a X plus b and this will never become a and b are real numbers, because we are applying division algorithm on this ring.

So, a b are real numbers and then when you plug it in X equal to i it becomes 0, F of i is 0. Because F is in the kernel here, we have started with this is 0, this is already 0. So, F of i is equal to ai plus b, but then i will you can then, that will imply i is a real number which is no true, contradiction. Either contradiction or say that so, because i is, let me rub this, so that should imply a equal to b equal to 0. Because 1 and i is linearly independent, I would like to use linear algebra as much as possible rather than giving complicated arguments.

So, therefore, we have proved that the kernel is generated by this polynomial X square plus 1, therefore c is isomorphic to this. Therefore, this actually is a maximal ideal. So, this proves that this ideal generated by X square plus 1, is belongs to Spm RX and this is not of that type. So, therefore, this in general this set properly contain. These are not all maximal ideals in general. For example, I can give many more if you can give me, if I take field K equal to K equal to Q.

(Refer Slide Time: 07:07)



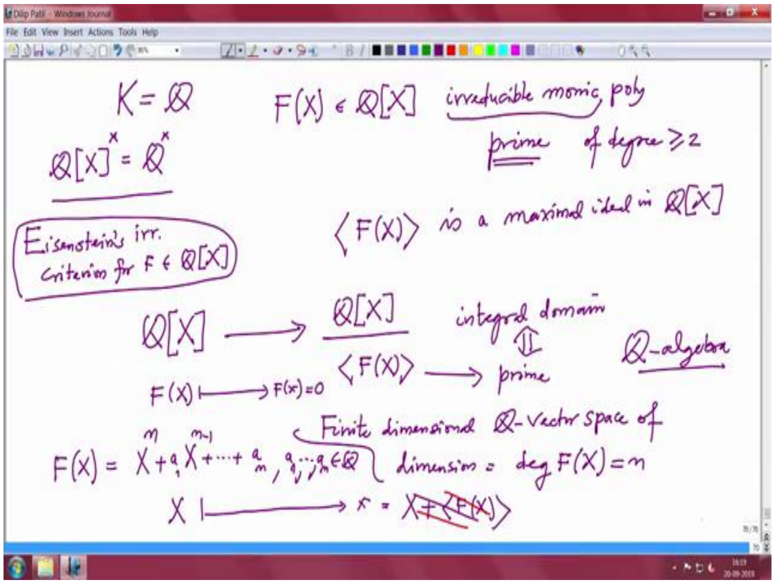
If I take K is equal to Q, what do I do? You see now the problem will shift to somewhere else and suppose I have F X belong to Q X, suppose I have irreducible polynomial and let us also monic polynomial. Irreducible means it does not factor into two proper factors, two non-constant factors because constants in this case are the units. We have checked, let me remind you we have checked or at least I have mentioned that units in this polynomial ring over a field Q is Q cross.

So, the only unit polynomials are the non-zero constant rational numbers. So, if I take any irreducible monic polynomial that will not be constant and there are many as such, you would have seen, you would have seen. So, can you list some of the irreducible polynomials over Q, you can list many. For example, if I take X power n minus let me write for smaller n.

X square minus 2, this is irreducible or X square minus 3 or X square minus pq or why, why two prime numbers, X square minus p1 to pr this is square free. All these polynomial are irreducible and they are monic or and if I want degree n, well degree n also we can write, X power n minus p1 to pr, these are all irreducible polynomial.

So, I will, this immediately follows from what is known as, I will write in this set Eisenstein criterion, Eisenstein's irreducibility criterion for polynomial F inside Q X let us say. I hope you remember this if you do not remember you can learn or I will write in exercises. So, let me rub all this.

(Refer Slide Time: 10:07)



So, you start with any irreducible monic polynomial and this irreducible plus monic, I keep calling prime polynomials. So, and of degree, bigger equal to 2 and we have seen there are many many. In fact given any integer n, given any natural number n there are lots of prime polynomials of degree n. So, now I claim that ideal generated by F X is a maximal ideal in Q X. So, what do I have to prove?

So, first of all what does our residue class ring is Q X mod F X, this is your residue class ring and we definitely know this is an integral domain, this is integral domain. Because that is a prime polynomial and so prime polynomial mean that, if a product is divisible by this F then at least one of them is divisible by F. But this when you translate, that will become a prime ideal. So, this is degree 2, bigger equal to 2 therefore it cannot be unit and therefore this ideal is prime but then that is equivalent to saying the residue class ring is a integral domain.

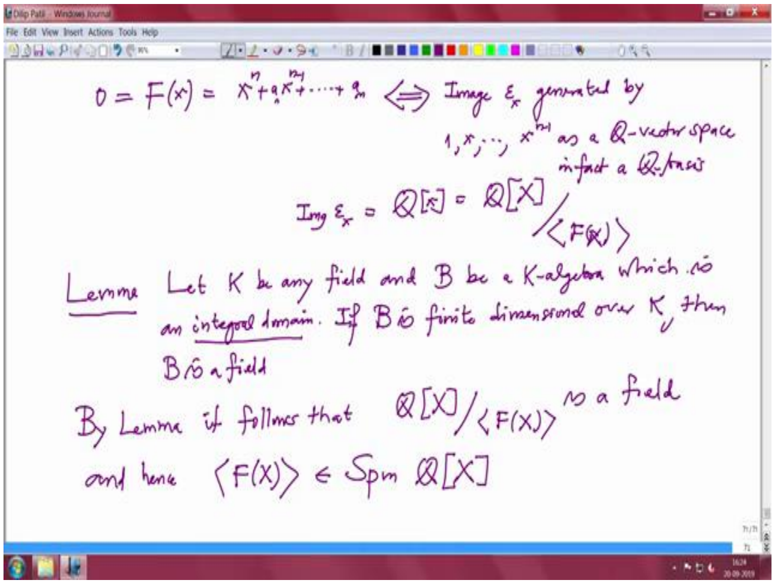
It is a integral domain and it is a monic polynomial. So, I claim that this is also finite dimensional, finite dimensional Q vector space, it is a vector space also, this is a Q algebra, this is residue class of A Q algebra polynomial algebra. So, this is residue class algebra, so this is also Q algebra and it is finite dimensional Q vector space in fact not only Q vector space but it is finite dimension actually and what is how do you check that in fact finite dimensional Q vector space of dimension equal to degree of this polynomial F X.

How do you prove this? So, you see you have a map here, this is residue class map Q X to this and F we have written like this F of X is a monic polynomial. So, let me write F of X as X power let call this degree to be n. X power n plus a1 X power n minus 1 plus, plus, plus, plus an, where a1 to an they are elements in Q.

When you go mod and let us write where do this X go, this I want to write image of X capital X the image is small x, this is surjective map image X capital X go to, so, this is if you are in a lower Kg or upper Kg, then this capital X is in fact capital X, small x is in fact co set of capital X this, this is how we will write the co sets, this is abelian group.

So, you write co sets like that but you see how complicated it is. So, we will, we assume that we have gone to bigger class and we do not write like this. So, small x and once I know, where capital X goes I know were all polynomials go. So, therefore, where will the polynomial F will go, where will this polynomial F x will go, I have to evaluate that F had this small x. But then it is in 0 it is, so this is 0. So, that means what?

(Refer Slide Time: 15:01)



So, that means, so 0 equal to F of small x that means small x power n plus a1 small x power n minus 1 plus, plus, plus, plus, plus, plus an this is 0. That means the, this is equivalent to saying x power n belongs to the sub algebra generated by x. So this belong to Q x, so let me write more explicitly, this means image of this epsilon evaluated x map is generated by 1 x, x power n minus 1 as a Q vector space. Because any element will be a polynomial and you divide that polynomial by this F and then you get a lower degree polynomial.

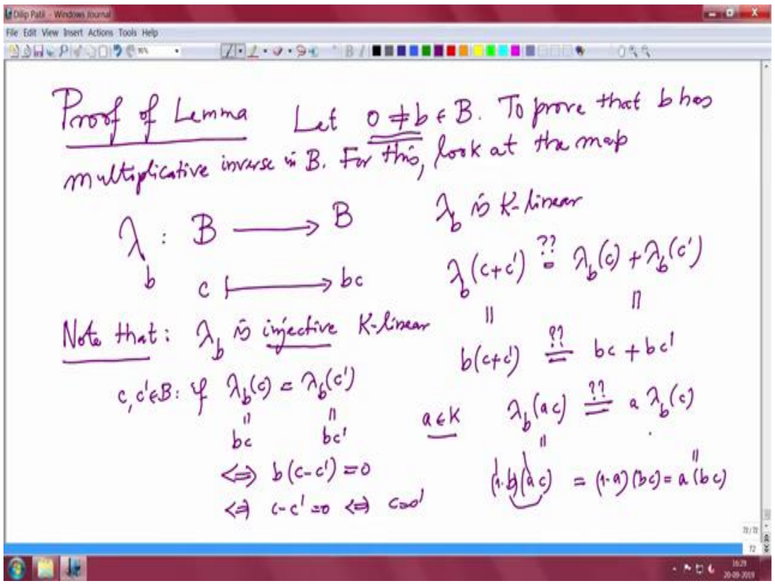
So, image is generated by this. So, that means we have proved that and what is image of epsilon x, image of epsilon x is nothing but Q x, Q small x which is Q X mod ideal generated by F X capital X and this is a generating set for this vector space and also it is linearly independent, because of the you can always, if some combination of this guy is there is a linear dependence relation equal to 0. Then that polynomial will be divisible by that F, but F has a bigger degree than n minus 1 therefore it is 0. So, in fact this is a Q basis, in fact a Q basis.

So, we have proved that this is a finite dimensional Q vector space, this finite dimensional Q algebra. So, then what do you wanted to prove? Now, I want to give you lemma, because this I want to use multiple times. So, K any field, let K be any field and let B be a K algebra which is an integral domain. If B is finite dimensional over K, then B is a field.

We will prove this, but that will finish our problem because what we wanted to prove? We wanted to prove this residue class ring is a field because we wanted to prove this is a maximal ideal but to prove it and we already know it is an integral domain that we already know we have just checked and we also know it is finite dimensional.

Therefore, so by lemma, it follows that Q X module of F X is a field and hence ideal generated by F X is a maximal ideal in the polynomial ring or Q in this. And how many such as many as prime polynomial is definitely and there are so many we saw. So, therefore, whatever we listed those maximal ideals corresponding to the points they are many more outside that also. So, let us prove this lemma.

(Refer Slide Time: 20:13)



So, proof of lemma very simple. What do you want to prove we want to that, b is a field we want to proof. So, let 0 not equal to b in B. To prove B is a field I have to check that every non zero has inverse in b. So, to prove that b has multiplicative inverse, inverse in B that is what we want to prove. So, let us look at the map for this look at the map lambda times a, lambda suffix b, which is a map from B to B, any c goes to b times C.

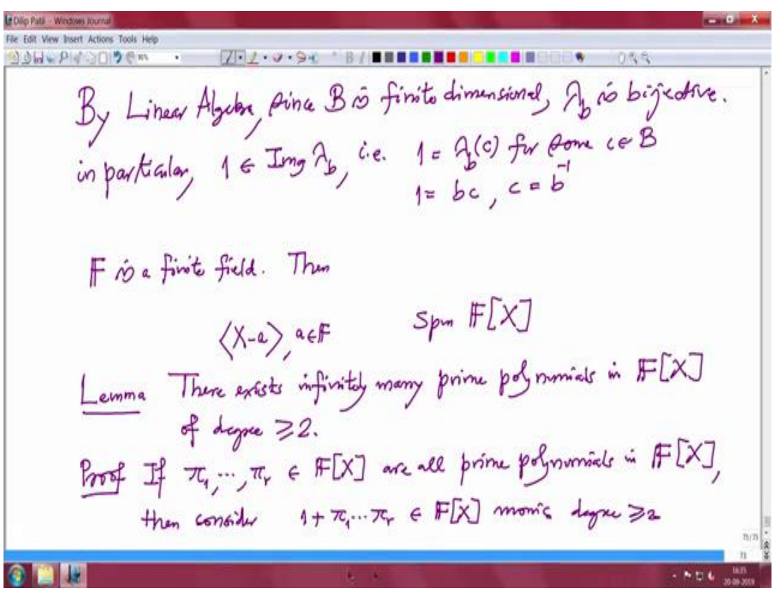
Left multiplication by b this is a map and B was what B was a K algebra. So, this map is I say this map, it is clear that this lambda map is k linear. So, what do I have to check, those precisely will be what will be useful is precisely for the axioms of K algebra. So, for example, I have to check this lambda b of c plus c prime equal to lambda b c plus lambda b c prime. This is what we want to check. Let us see convert it, this is by definition what this is b times c plus c prime and this is by definition this is b c, this is by definition plus bc prime and we want to check this.

But that is the axiom that the plus is compatible with the scalar multiplication. So, this is additivity and now K linearity if I have some a in K what is lambda b of a c and we would like this be equal to what a times lambda b of c, well what is this by definition? This is b times a c, but b is, I will think b as one times b. So, this is a scalar in K, this is scalar in K and these are two elements in b and compatibility of the multiplication and scalar multiplication says that this is same as I can take this a with 1. So, 1 times a times b times c, which is this, which is 1 times a because one is the multiplicative identity in the field K. So, this is a times b c, but this is same thing is this.

So, therefore the algebra b is a K algebra the axioms of K algebra checks that this lambda map is a K linear map and by our assumption given this b is a finite dimensional K vector space. Now, further note that lambda b is injective and of course we have noted that it is K linear. Why is it injective? Because it is an integral domain.

If c and c prime both in B, if lambda b of c equal to lambda b of c prime, what does this mean? This is b c and this is b c prime which is equivalent to saying b times c minus c prime is 0. But b is not 0, therefore c minus c prime is 0 which is equivalent to using c equal to c prime. So, therefore, this is an injective K linear map of the same vector space, finite dimensional, therefore, it is an auto morphism. So, because for a finite dimensional injective, surjective and automorphism they are all equivalent.

(Refer Slide Time: 25:16)



So, by linear algebra, since B is finite dimensional, lambda a is bijective. But, that means everybody is in the image of lambda a, lambda b, I called it b. In particular, 1 belongs to the image of lambda b that is 1 equal to lambda b of c for some c in b but that is, this is same thing as saying 1 equal to b c.

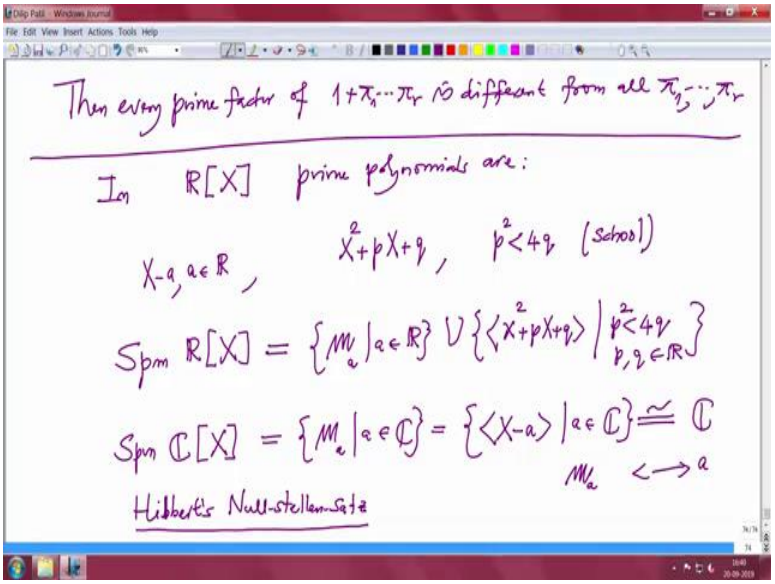
So, I produce actually the inverse of b. So, c is equal to b inverse exist. So, that proves the lemma and that proves we produce many, many maximal ideals in polynomial ring over Q X. Now, same thing you can do it for finite field, F is a finite field with finitely many elements. Then Spm F one variable X this of course contains all these X minus a where a is in F. All these are maximal ideals here.

But we had many more and here also there will be many, many because over a finite field you can find many polynomials which are prime, over a finite field there are many polynomial which are prime. So, let me write a statement, so let us write it as a lemma, there exist in fact infinitely many, there exist infinitely many, prime polynomials in F X of degree bigger equal to 2.

Degree equal to 1 they are only finitely many, they are all these linear monic polynomials and how do you prove this. Proof, suppose they are finitely many. Let me call them, Pi 1 to Pi r in F X., if are all prime polynomials in F X. This is a very famous proof, this is called Euclid’s proof, Euclid’s proof is for numbers but the same trick works for the polynomials over a field, then consider the new polynomial 1 plus Pi 1 to Pi r. This is a polynomial in F X also monic, and also degree bigger equal to 2.

Because you have taken if there are finitely many then few are these linear ones and other may be but any case there are at least two linear factors. So, this polynomial degree bigger equal to 2 and now look at the factorization of that polynomial. We know that polynomials over a field can be factorized into irreducible factors. So, there will be at least one irreducible factor this is not a unit element. So, there is at least an irreducible factor and that will corresponds to a prime polynomial and that prime polynomial have to be different from this Pi 1 to Pi r because that prime factor Pi.

(Refer Slide Time: 30:42)



So, let, I would say just then every prime factor of Pi 1 to this not of 1 plus Pi to Pi r is different from all Pi 1 to Pi r because it is a factor of this, it cannot be equal to this then if it is equal to 1 of them then it will also divide 1 which is not possible. So, therefore, what we have proved is, in polynomial ring or a finite field there infinitely many polynomials which are prime and each one of them will give you the maximal ideal and all these maximal ideals only finitely many, as many as the cardinality of the field they are those linear, the given by the points and the remaining ones are non-points.

So, therefore, now this also suggests that, the field will play very important role in algebraic geometry. So, r Q and finite field will be the worst cases r is little bit better because the only irreducible polynomial is out degree 2 over in note that. So, I just want to note this for future use. In R X what are the prime polynomials? Prime polynomials are obviously the linear ones X minus a, a is in R. They are also unaccountably many and now the quadratic ones.

So, X square plus p X plus q, where B squared minus 4 q should be negative, p square less than 4 q. These are obviously irreducible because if at all it is factors then the zeroes of this polynomial will be real numbers but then the discriminant, know this is school what you studied. So, these are all because if you have a cubic polynomial it has a real 0 and therefore it will not be prime it will be factor.

So, these are maximal ideals and these are maximal ideals because I know, all ideals are principle in R X. So, therefore, Spm R X is precisely equal to these our notation was ma a in R, union if you can identify this may be you can identify this with or keep it the same X square plus p X plus q where p square less into 4 q, pq are real numbers, these are all maximal ideals.

So, we have described the maximal spectrum for the polynomial ring or R in one variable and over Q it is much more complicated you see it is not just these two any degree you will be several for finite field also similar thing. But for C Spm C X, I will prove that this is equal to in fact only this m a, a varies in C that means these are precisely the ideal generated by this linear X minus a, a in C.

So, in other words we can identify this with C a to ma this is the identification and this is not only true for one variable, but we will prove this for many variable finely many variable and that is precisely, one form of Hilbert’s Null-stellensatz. So, this is a very particular case of Hilbert’s Null-stellensatz, this is what, this is the corner stone, this is the bridge between algebra and geometry this I will show you in the coming few lectures many.

So, with this I would stop this lecture and we will continue this. So, you might have realized that we have to study polynomials over fields finitely many variables and ideals in that maximal ideals in that prime ideals in that and so on. So, this is what we will specialize for that I will need some algebraic statement and now and then I will switch to algebra. So, I will stop her,e thank you.