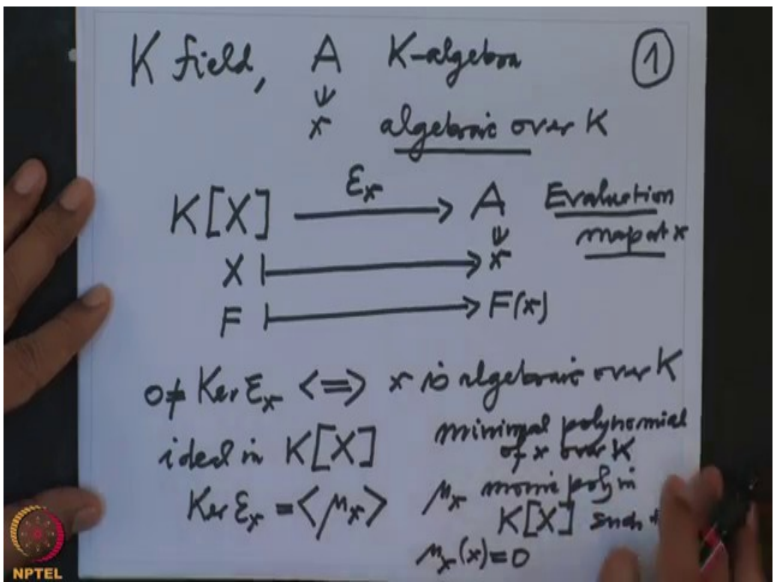
====Galois Theory
Professor Dilip P. Patil
Department of Mathematics
Indian Institute of Science, Bangalore
Lecture 17
Theorem of Kronecker

So in today's lecture we will prove very important theorem so called Kronecker's theorem which says that given a polynomial over arbitrary field I can enlarge this filed to a finite field extension so that the given polynomial has all its roots in a bigger field.

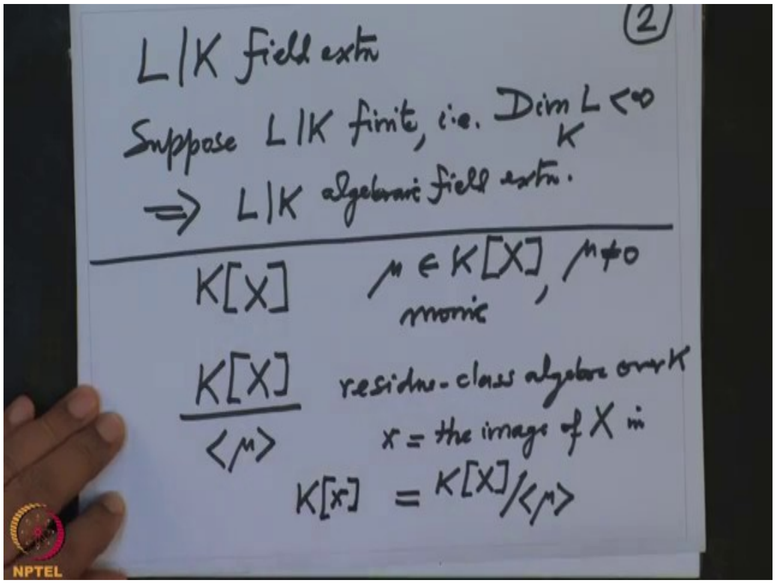
(Refer Slide Time: 00:56)



Let us recall first what we have been doing so K is our base field and A is the K algebra and we have defined elements $x \in K$ which is algebraic over K this means the evaluation map from the polynomial ring to A this is the evaluation map by x that means the variable X is mapped to the element x small $x \in A$ and therefore the polynomial F will be mapped into F evaluated at x.

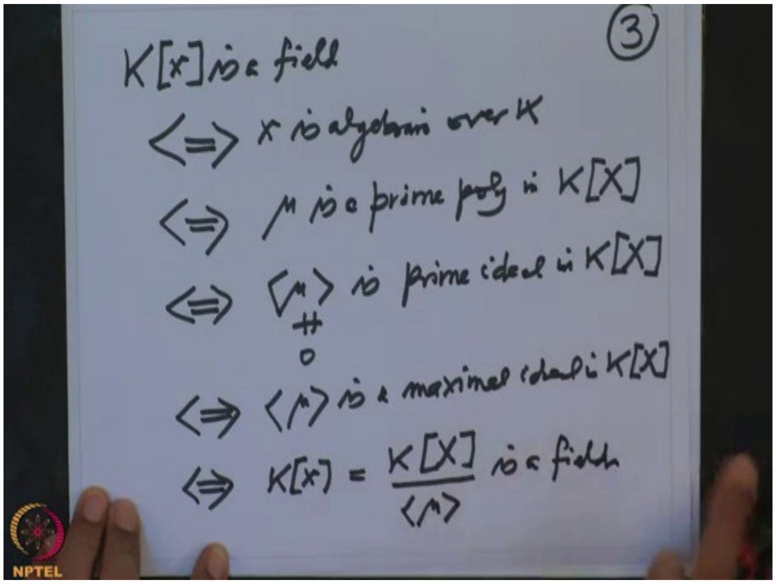
So this is called the evaluation map mapped at x and x is called algebraic if the Kernel of this evaluation map is non-zero that is if and only if x is algebraic over K but this means note that this Kernel is an ideal in the polynomial ring over a field K and for we know that all ideals in this ring are principle therefore this ideal Kernel of epsilon x is generated by a polynomial μ_x is μ_x I can choose monic polynomial in $K[X]$ such that this μ_x belong to the Kernel means μ_x is evaluated at x is zero, that means x is a zero of μ_x this unique it is unique because we have chosen to be monic polynomial, this polynomial is called minimal monic or minimal polynomial of X over K.

(Refer Slide Time: 3:58)



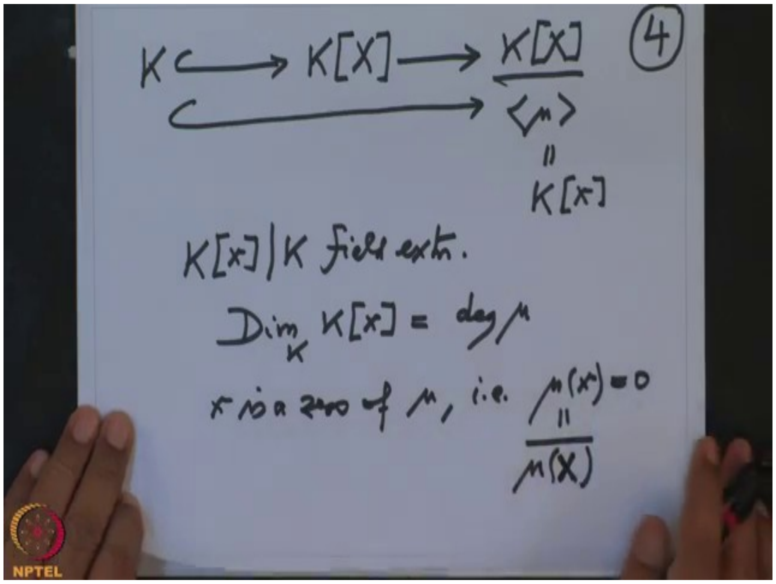
So we have a field extension if L over K is a field extension and suppose L over K is finite that means dimension of L as a vector space over K is finite then we know every element that L over K is algebraic that means the field extension L over K is algebraic field extension that's all. We have $K[X]$ and suppose I have a non-zero polynomial in μ_x in $K[X]$, μ is non-zero as shown it is monic then you look at the residue class algebra $\frac{K[X]}{\langle \mu_x \rangle}$ this is a residue class algebra over A and let us denote x to be the image of capital X in this residue class algebra.

(Refer Slide Time: 5:55)



So that means this residue class algebra is generated as a algebra over K where small x and where it is a field, so $K[x]$ is a field, if and only if x is algebraic over K and which is equivalent to saying μ_x is a prime polynomial in $K[X]$ that is equivalent to saying μ_x this ideal generated by μ_x is a non-zero prime ideal in $K[X]$ but we know non-zero prime ideals in a PID are principle so this is equivalent to saying μ_x is a maximal ideal in $K[X]$, so this means so in other word this means $K[x]$ is a field, $K[X]$ which is the residue class algebra $K[X]$ mod ideally generated by the maximal ideal generated by μ_x this is a field.

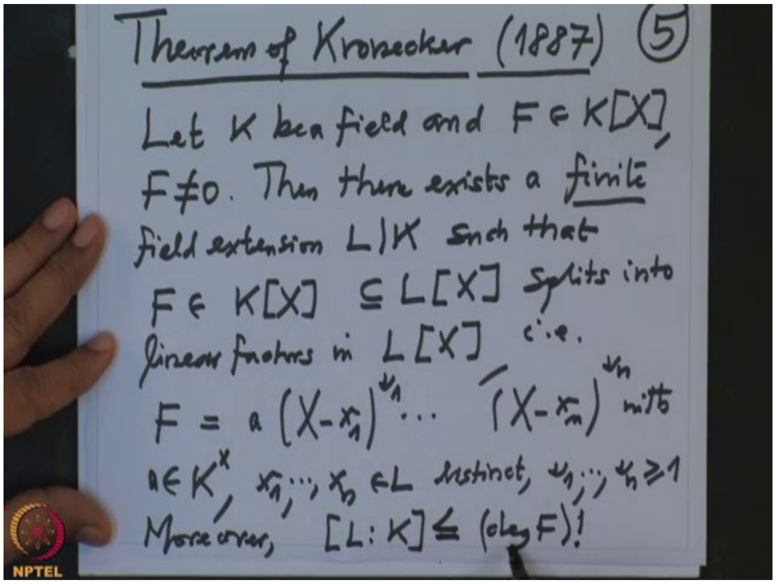
(Refer Slide Time: 7:40)



So we add a map K is here, K is naturally contained in the polynomial $K[X]$ and from $K[X]$ we have $\frac{K[X]}{\langle \mu_x \rangle}$ and this inclusion, this is naturally inclusion because this K is a field and all this, this both these are ring homorphism therefore because there are no ideals other than zero and the whole K and Kernel cannot be the whole K because one goes to one and our ring of morphism so therefore this you can say field extension, this is so therefore $K[x]$ over K is a field extension and infact the degree of this field extension that is dimension of K over $K[x]$, this dimension is nothing but the degree of μ_x and also we know this x is a zero of μ_x that is $\mu_x(x)$ is zero.

This μ_x is precisely the residue class of μ_x, but because it belongs to the ideal generated by μ_x this is zero so x is a zero of μ_x.

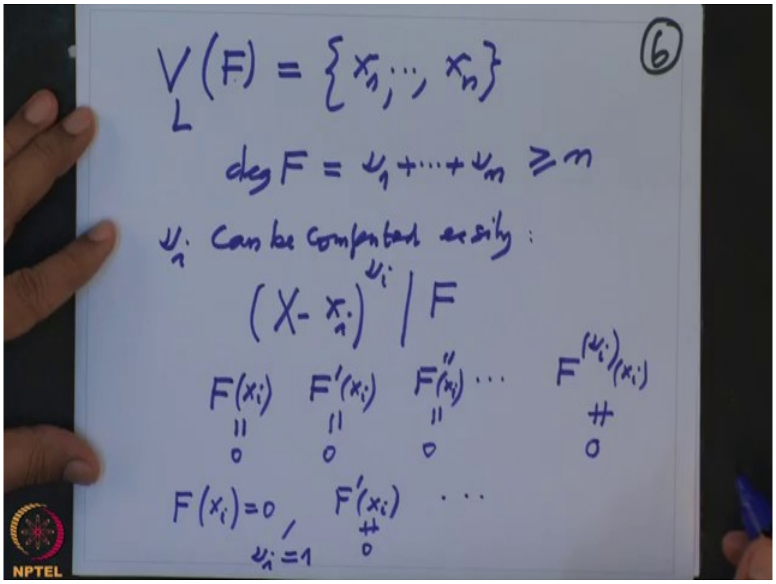
(Refer Slide Time: 9:26)



So now we come to the theorem of Kronecker, which is used very often in this course so this is the theorem, this is theorem of Kronecker, alright so this was proved that Kronecker around 1887 alright so let K be a field and capital F be a polynomial in coefficients in K, F is in $K[X]$ and F is non-zero polynomial then there exists a finite field extension, finite field extension, L over K such that F which is a polynomial in $K[X]$ also you can think of it is a polynomial in $L[X]$ splits into linear factors not in $K[X]$ but in $L[X]$.

That means F is of the form $a(X-x_1)^{v_1}...(X-x_n)^{v_n}$ where with a is some constant in (A) constant in K, x_1 to x_n they are elements in L distinct and this v_1 to v_n there are the multiplicities of x_1 to x_n respectively which are non-zero natural numbers, check that the degree of L over K will not exceed degree factorial less equal to degree factorial if F is of degree d then degree factorial is d factorial but before I prove that let us recall little bit about the multiplicities, so also the notation which we keep using in this course later again and again.

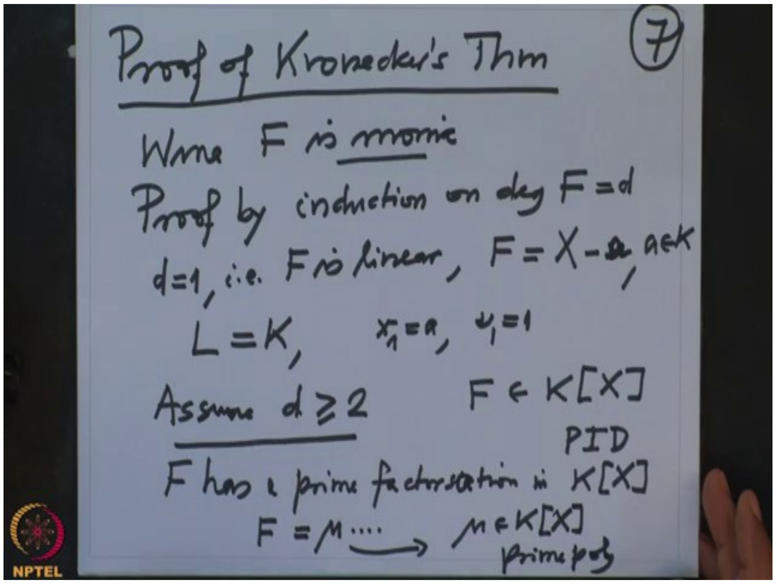
(Refer Slide Time: 12:32)



When I say V of a polynomial F in the field L this are the zeros of F inside L, so these are x 1 to x n so this means they have different elements of L and all of them are zeros of F and the degree of F is $\nu_1 + \dots + \nu_n$ which is obviously big or equal to n because x_1 is a zero of multiplicity ν_1 x_n is zero of multiplicity ν_n and this ν_i s can be computed easily without actually computing the factorization of F as follows because this will mean that X minus x i this factor this is a factor of F and to check that this is the highest factor of F you just have to compute the derivatives of F so F is here, F', F double prime these are the formal derivatives of F and F' and so on and now you have to evaluate them at x_i, so this should be zero, this should be zero and this should be zero and the first time you hit that, that is non-zero, that will be the multiplicity.

So for example if F, $F(x_i)$ is zero but the derivative is non-zero that means the multiplicity ν_i is equal to one it is not more than one and so on. So that is a very effective way of computing the multiplicity of a zero of a polynomial.

(Refer Slide Time: 15:10)



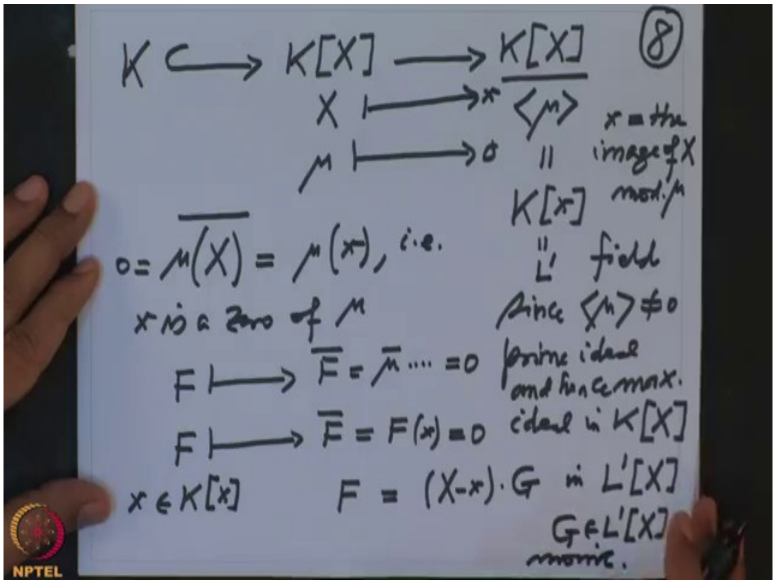
Now let us prove Kronecker theorem, so proof of Kronecker's theorem, proof of Kronecker's theorem, so first of all we may assume F is monic if necessary you divide by that leading quotient of F and we are going to prove the assertion proof by induction on the degree, degree of F let us call this degree to be d.

So it is obvious that if d is 1, that means it is linear that is F is linear and because we are assuming it is monic then F must be of the form some X minus some $x_1 = a$, where a is actually coefficient in coefficient of F which is in K because we are assuming F as coefficient in K and therefore we are done because in this case we can take L equal to K and there is only one zero x_1 is a and ν_1 is also 1 and that's it. So in this case, we know the assertion but only to enlarge the field K at all.

So now assume that degree d is big or equal to 2, alright. So we have this polynomial F in $K[X]$ and we know that this is a PID and therefore every element of this as a factorization into prime factors so F has a prime factorization in $K[X]$ which is essentially unique up to permutation of the prime factors. So therefore definitely this F you have because we are assuming it is monic this will have at least one of the prime factor μ and maybe more. So this μ is a polynomial in

$K[X]$ a prime polynomial, prime means it is monic and it is you cannot factorize anymore inside $K[X]$.

(Refer Slide Time: 18:22)

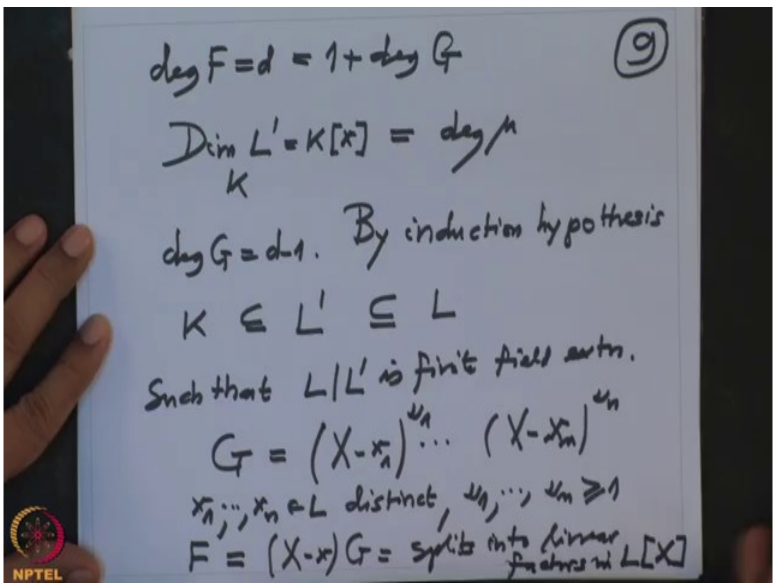


So once you have this then you look at from a residue class algebra, so K is here containing the polynomial algebra, this is a ring homorphism and then you will have gone modulo μ ideal generated by μ that is a residue class algebra and this we know it is denoted by K small x where this small x is the image of (the image of) capital $\frac{X}{\mu}$ and because μ is irreducible we use prime it generates a prime ideal and therefore it generates a non-zero prime ideal and therefore like earlier argument this must be a field, so this $K[x]$ is a field.

Since μ generates a non-zero prime ideal and hence a maximal, maximal ideal in $K[X]$, therefore modulo a maximal ideal you always get a field, therefore this is a field and now also where do capital X goes here? Capital X goes here to a small x but μ, where do μ go? μ goes to zero and this ring homorphism therefore $\mu(\overline{X})$ this is zero but bar is saying this as because this is ring homorphism it commutes to the polynomial so this is $\mu(x)$, so actually x is a zero of μ that is x is zero of μ and where do F go?

F goes to F bar but F bar is $\bar{\mu}$ times or more that is but already $\bar{\mu}$ goes to zero Mod μ, so therefore F bar also goes to zero. So therefore definitely F of X, F is going to F bar but F bar is nothing but a F of x which is also zero, therefore this x is an element in $K[X]$ this field and it is zero of F therefore I can divide F by $X-x$ in the in this L' this is L', so this will be F will be multiple of this in $L'[X]$, this x is zero of F in this field therefore it looks like this and monic therefore G is G belongs to $L'[X]$ this is also monic polynomial, factor of a monic is always monic. So therefore now we are going to apply and (what is) the degree, what is degree of F in terms of degree of G?

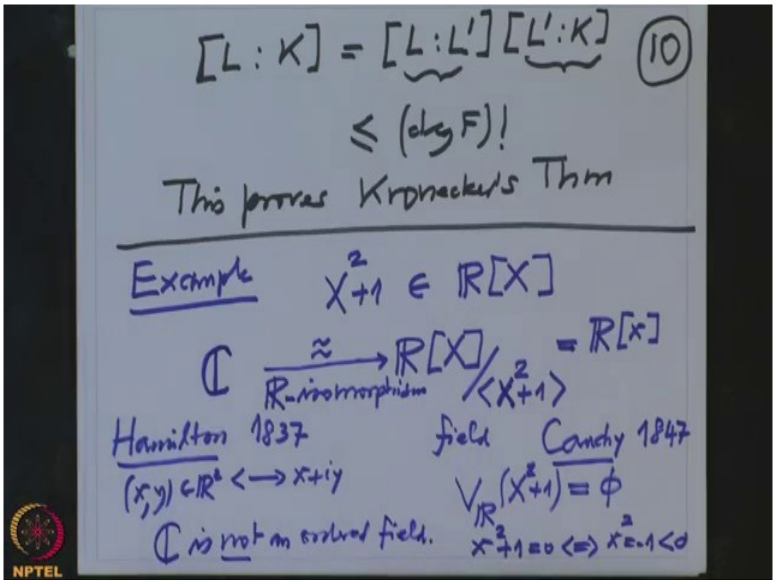
(Refer Slide Time: 22:03)



So we know degree of F which was d which will be equal to 1 plus degree of G and therefore and also we know dimension of L' over K, L' was $K[x]$, this dimension equal to the degree of μ therefore I want to apply now so therefore the degree of G has dropped, degree G is one less than the degree F equal to d minus 1, so by induction hypothesis I can enlarge the field L prime to L such that, so this L prime L in over L prime is finite field extension and G prime, G we split into linear factors in L x, so G will look like $(X-x_1)^{\nu_1}\dots(X-x_n)^{\nu_n}$, where x_1 to x_n they are elements in L and distinct and this ν_1 to ν_n are their multiplicities of this one.

But then F will, F will also splits into L in $L[X]$ because F equal to $(X-x)G$ which is now you can this x maybe one of them or maybe different so therefore this also splits into linear factors in $L[X]$.

(Refer Slide Time: 24:26)



So that proves our assertion also the last assertion which say that the degree of L over K this is a degree of L over L' times degree of L' over K and this degree we know it is so this is less equal to this degree is all together less equal to degree of F factorial, so this proves Kronecker theorem.

So this completes, this proves Kronecker's theorem, alright. We will use this Kronecker's theorem very often. So other example let us discuss one example, for example suppose we have this polynomial X square plus 1 this is a polynomial with real coefficients think of (())(25:42) with real coefficients and what we did to obtain the bigger field? So what we did was, we try to find F factor of this but his already is prime polynomial therefore we go Mod this $\mathbb{R}[X]$ mod this ideally generated by X square plus 1 and one note that this is a field, this field this nothing but a field so in our notation big $\mathbb{R}[x]$ where small x is the image of capital X inside this residue class $\mathbb{R}$ algebra and but this field is isomorphic to $\mathbb{C}$, then isomorphism from these to $\mathbb{C}$ this is an $\mathbb{R}$ isomorphism, $\mathbb{R}$ algebra isomorphism.

So the number complex numbers that was defined by Hanilton around 1837 and Hanilton because he was from physics he thought complex numbers as a pairs of real numbers x, y $\mathbb{R}^2$ and when they correspond to $x+iy$, so he thought as a pairs the complex numbers but this description was due to Couchy which was around 1847, 10 years later than that of Hanilton and it was based on the fact that if you take the real polynomial X^2+1 is doesn't have real zero (()) (27:51) and also note that this description shows also that the which was the order, order of the field of real numbers it is last when you go to complex numbers because X^2+1 is zero in this field that means $X^2=-1$ but this is not possible because on one side it is negative, on the other side positive squares have always positive order.

So therefore one cannot extend the order of real numbers to the order of to the order on complex numbers. So therefore with this $\mathbb{C}$ is not an order field. So this is a last we have extended the field R to the complex numbers by looking at the zeros of the single polynomial and after that we will prove in this course of lecture that, that is enough now $\mathbb{C}$ is algebraically closed that means every polynomial with coefficients in $\mathbb{C}$ has a complex zero, this we will prove in the new course of this lectures but we will stop this lecture here now and try to see more examples in the coming lecture, thank you.