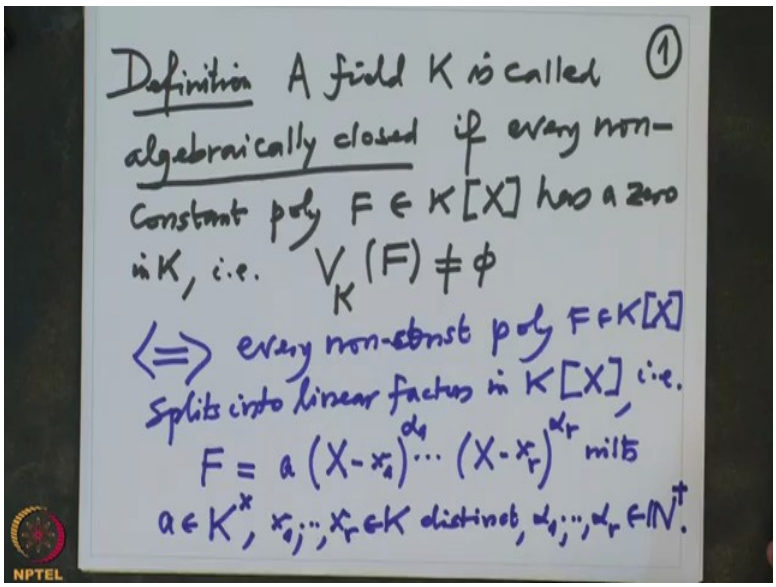
Galois Theory
Professor Dilip P Patil
Department of Mathematics
Indian Institute of Science, Bangalore
Lecture 9
Algebraically closed fields and statement of FTA

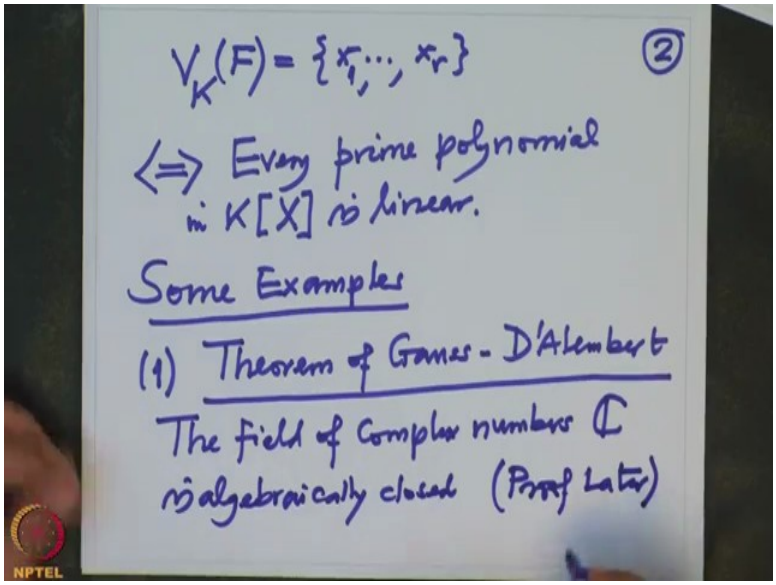
In the last lecture we have studied we have been studying polynomials over a field and in the last I have stated very important theorem which says that the field of complex numbers is algebraically closed.

(Refer Slide Time: 0:54)



So let us recall quickly what we did from the last time and continue from there. So we have defined the definition, a field K is called algebraically closed if every non-constant polynomial F with coefficients in K has a zero in K, then we say the field is algebraically closed. In the notation that is our notation $V_K(F)$ this is the set of zeros of F in K this is non-empty, so that means there is atleast one zero of F in K or equivalently equivalently every non-constant polynomial F in K splits into linear factors in K[X], so again in the notation that is F will look like some constant $a(X-x_1)^{\alpha_1}...(X-x_r)^{\alpha_r}$ with this a is constant non-zero constant and x_1 to x_r are elements of K they are distinct and (with) their multiplicities are α_1 to α_r these are non-zero natural numbers. So in this case we actually know therefore what is $V(F)$.

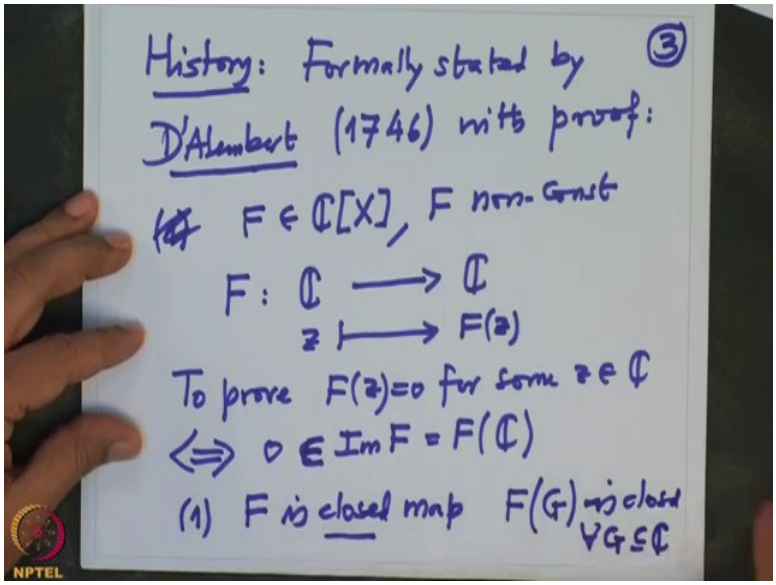
(Refer Slide Time: 3:52)



So therefore $V_K(F)$ actually we know it is a set x_1 to x_r, when you write in the set notation we do not write the multiplicities so this x_1 is occurring α_1 times in F, x_2 is occurring α_2 times in F and so on, x_r is appearing α_r times in the linear factor the multiplicity of x_r also this finding out the multiplicities is also a task but that is not so difficult like a factorization, so that when time comes I will indicate some methods to do so.

Another way of thinking is equivalently every prime polynomial in K[X] is linear that all these conditions are equivalent is very easy to see and after this we should see some examples of algebraically closed fields as well as algebraically non-closed fields. So therefore it is very important after every definition to give examples of that kind and not of that kind. So some examples, so the first one of course is what I stated it as a theorem this is a theorem of which we will proof theorem of Gauss D'Alembert, Gauss was German and D'Alembert was French and the theorem says that the field of complex numbers numbers which we denote by this setC with the double line is algebraically closed I will just mention here, proof later little bit history about the theorem.

(Refer Slide Time: 7:00)



So we have field which is algebraically closed $\mathbb{C}$, I want to give little history and not more it is very interesting. So first of all formally stated stated by D'Alembert 1746 before that the mathematicians were they did not find a need to proof this, they somehow calculating and they were convinced that the zeros of a polynomial equation with real coefficients have complex zeros.

But how did the D'Alembert formulate it because he was actually he formulated this because he wanted to solve differential equations and to solve the differential equations if you know that specially for the partial fractions partial fractions occur there and to do that you need a denominator polynomial should split into linear factors and then you there are standard techniques to integrate the partial fractions and that is what he wanted to do and in that connection he stated this formally and also offered a proof with proof and what was his proof I will just state it he had two steps in the proof.

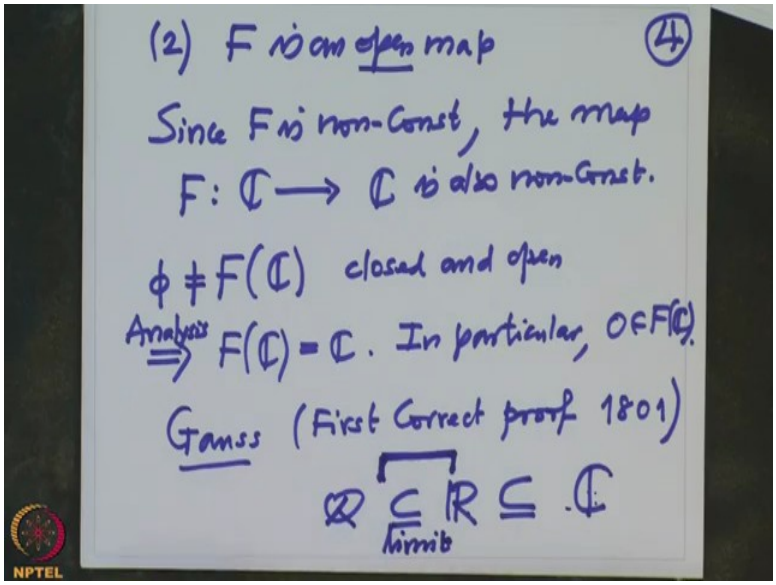
Number 1 the first step in the proof was as I said in the last lecture also you think of polynomials as polynomial functions. So we want to proof that if F is a non-constant polynomial in $\mathbb{C}[X]$, F non-constant then we want to proof that F has a complex 0. So think of F as a function from $\mathbb{C}$ to $\mathbb{C}$, any z going to $F(z)$ and we want to proof that (it has a complex) F has a complex 0 means.

So to prove for some z $F(z)$ become 0, $F(z)$ is 0 for some z in complex number, but this is equivalent to proving 0 in the image of this function F, image of F is by definition take Cos z and take their images in this is F of $\mathbb{C}$, so this is what we want to prove, 0 belong to

the image, then there will be some z which will go to 0 that means what we prove it. So for this he claims two things number 1 he claims (this is not 1) number 1 he claims that F is closed map, here I will use little bit terminology what one learns in a very first course on analysis, so close map means this $\mathbb{C}$ has metric space, $\mathbb{C}$ has a metric on that and we talk about open subsets, closed subsets, etc with respect to that metric.

So closed map means F maps closed set to the closed sets, F maps F of any closed set G is closed is closed for every closed subset G of $\mathbb{C}$ that means F is a closed map.

(Refer Slide Time: 11:24)



And the second claim he makes that second claim he makes that it is F is an open map that means F map closed sets to the closed sets and because of our assumption F is a non-constant polynomial. Since F is non-constant the map F from $\mathbb{C}$ to $\mathbb{C}$ is also non-constant. So we have a map from $\mathbb{C}$ to $\mathbb{C}$ which is open map and which is also closed map and we learn again in the first course of analysis that if you have a map like this so that means F of $\mathbb{C}$ this is because $\mathbb{C}$ is closed in setC this is closed and $\mathbb{C}$ is also open in $\mathbb{C}$, so this is open and because it is non-constant map this is non-empty.

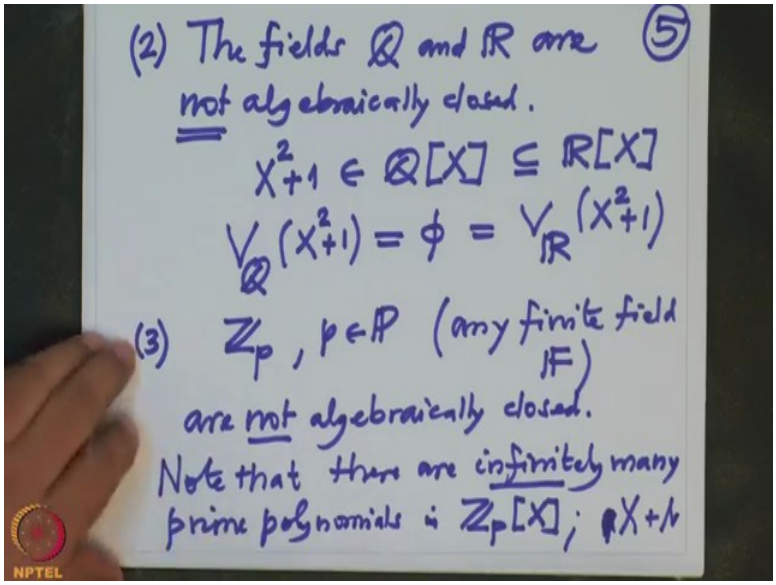
So we have a non-empty subset which is both closed and open and then one learns in a game in first course in analysis that then F of $\mathbb{C}$ must be $\mathbb{C}$, this is I would just say analysis. In particular 0 belongs to F of $\mathbb{C}$ which is what we wanted to proof. Now you see this proof is very good, the first part closed map also can be proved very easily for doing that one needs to use what is known as Heine–Borel theorem which I am not going to elaborate on this because we are going to prove it in a different way.

And this prove was not accepted by mathematicians at that time because that F is open map D'Alembert in state in this format I am stating this format in the modern language but that time this theorem which says that if you have analytic function then it is an open map this was non-constant analytic maps are open maps this was not yet proved, this was finally proved by Gauss later, so this proof was not accepted that time and this proof was considered gaps.

So later on the first person to give correct proof was Gauss first correct proof that was I think 1801 and there that happened because only after that only after he proved open mapping theorem, maximum modulus theorem and all those things Liouville's theorem and only then it became more and more clear till then this was not very clear. Also little word about this any proof will involve some analysis that is unavoidable but one can try to minimize the use of analysis, so this is what I will do it in when I give a formal proof of this theorem that is because if you see definition of (complex numbers is) complex numbers are constructed from real numbers, real numbers are constructed from the rational numbers and this here this gap is big here this construction of real numbers from rational numbers is only by limit which is a concept in analysis, here it is not too bad, here it is an algebra construction, before that also an algebra construction.

But definition itself of $\mathbb{C}$ or $\mathbb{R}$ involve some kind of analysis, so that one cannot avoid to give any proof of fundamental theorem of algebra and I will give a proof which is due to Lagrange after may be 2 lectures, but before that now I want to still discuss examples of continue discussing examples of algebraically closed or non-algebraically closed.

(Refer Slide Time: 16:22)



So far we have one example of algebraically closed field, the fields $\mathbb{Q}$ and $\mathbb{R}$ are not algebraically closed, simply because you look at the polynomial X^2+1, this is a polynomial with rational coefficients and therefore we can think also polynomials in real coefficients and there is no 0, $\mathbb{Q}$ of this polynomial is empty set, also real zeros of this polynomial there is nobody therefore it is an empty set, therefore this polynomial is non-constant in fact degree 2 and has no real or rational zeros, so these fields are not algebraically closed.

So another set of examples $\mathbb{Z}_p$, where p is a prime number or for that matter any finite field F I have not shown you that such fields exist but we will also show in due course later that how to construct more finite fields by using $\mathbb{Z}_p$, $\mathbb{Z}_p$ is very easy to construct just from the congruence modulo p. So these fields are not algebraically closed. So simply because now I have to produce you a polynomial which is a prime polynomial and which is not linear, if I do that then it will not be algebraically closed field, but this also I will postpone it little bit because anyway I am going to discuss some properties of the polynomials and from there it will become more and more clearer that these fields are not algebraically closed.

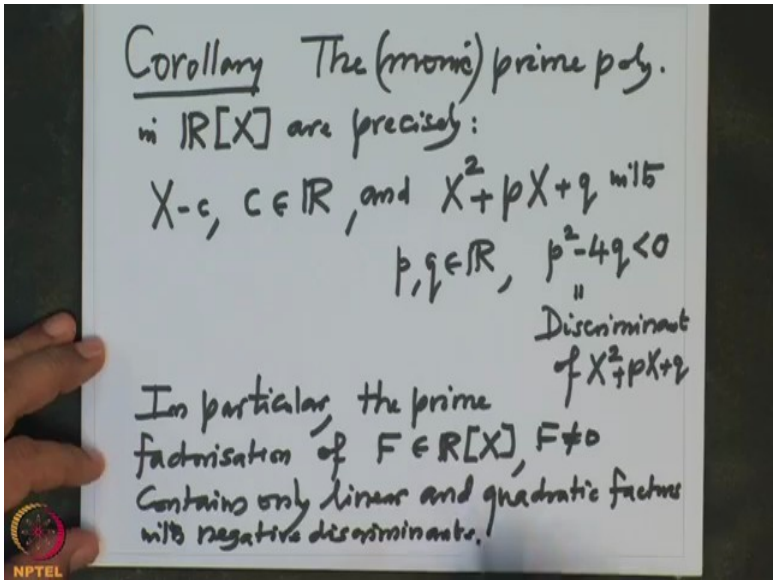
Only I have mentioned last time that the number of prime polynomials with coefficients in $\mathbb{Z}_p$ are infinitely many, but we did not say anything about the degree. Actually that also shows that because if you have noted note that we have proved earlier there are infinitely many prime polynomials in $\mathbb{Z}_p[X]$ we have noted this infinitely many that is same proof

as Euclid's theorem on infiniteness of the prime numbers, but then how many linear polynomials are there? They are only finitely many linear polynomials because linear polynomials looks like $aX+b$ and prime therefore I could have even said monic.

So the linear polynomials are this, so how many polynomials are there? As many as the coefficients b but b can vary only in a finite field, so therefore they are finitely many, so there must be a prime polynomial which is of degree more than 1 and therefore finite fields are not algebraically closed.

So now in formal days like Galois and even his predecessors they were more concerned about the rational polynomials and they were not concerned about over finite fields, finite fields in fact was not clear that time. So I want to draw some consequences of fundamental theorem of algebra that is $\mathbb{C}$ is algebraically closed from this I want to draw some consequences about rational polynomials and real polynomials.

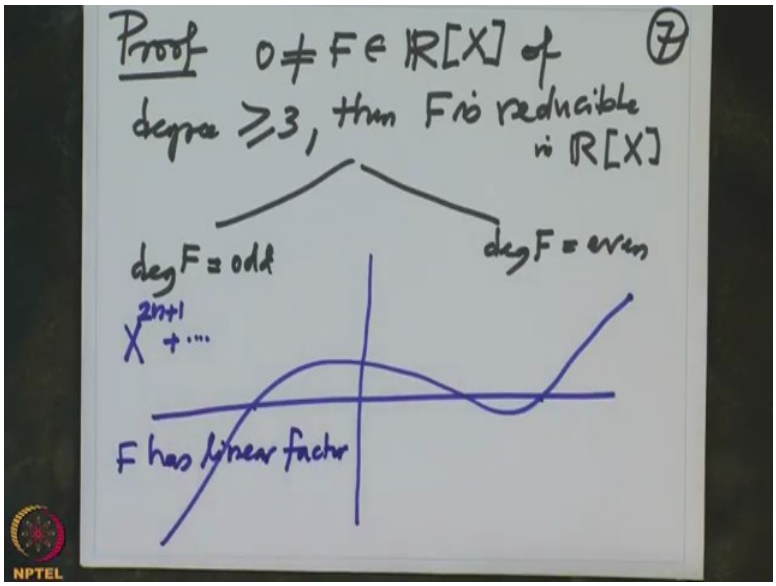
(Refer Slide Time: 20:20)



So the first I want to write that as a corollary, this corollary to the fundamental theorem of algebra. So the monic I want to describe all the monic polynomials in $\mathbb{R}[X]$, the monic prime polynomials, I do not have to say because we have made that can mention monic prime polynomials in $\mathbb{R}[X]$ are precisely they are linear ones so they are like this $X-c$, as setC varies in $\mathbb{R}$ they are infinitely many or and X^2+pX+q with p, q real numbers and p^2-4q is negative.

Note that in the school days you might have realized that this number becomes very important that is called the discriminant of this polynomial, so I will just say discriminant of X^2+pX+q . In particular if I prove this then what would have noted in particular the prime factorization of arbitrary polynomial F in $\mathbb{R}[X]$, where F is non-zero contains only linear and quadratic polynomials with this condition, contains only linear and quadratic factors with negative discriminants. So that is already good information about real polynomials.

(Refer Slide Time: 23:24)



Okay, so now let us spent few sentences for the proof of this corollary. So proof, so we are given a non-zero real polynomial and we want to factorize we want to find a prime factorization and last time (I) for arbitrary field we have noted that if I have a non-zero polynomial then you take out the real zeros and they will corresponds to the linear polynomials and the remaining part is the prime polynomials of higher degree and there I want to show now that higher degree parts are irreducible.

So that means I only have to show that if F is a polynomial non-zero polynomial of degree bigger equal to 3, then F is reducible, so it cannot be prime then so till the degree drops down to less equal to 2 and then we will worry about the discriminant condition. So I have to show this if I have polynomial of degree bigger equal to 3, then it is reducible that means it factorizes into $\mathbb{R}[X]$.

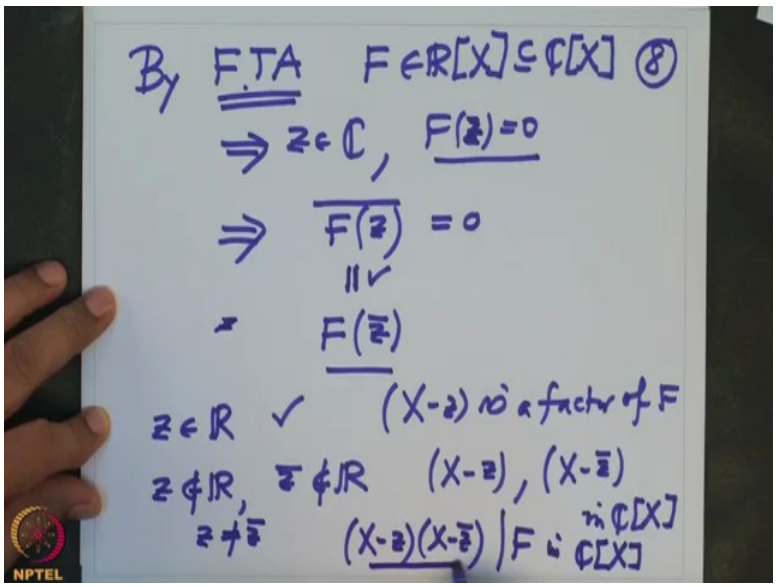
So I will divide the proof in two parts one the degree is odd and the degree is even, odd degree polynomial if you try to draw graph of that (function) polynomial function then the

odd degree polynomial we know that the degree is odd therefore it will look like X^{2n+1} + *lower degree terms* , I could have also assumed it is monic because we only want to, so I could also assume monic.

So (the) when the X becomes very large this is positive and when it becomes very negative large then it will go down to the so it will the graph will look (like) something like this. So that means on the large side large positive side the values of this polynomial is positive and large negative side value is negative because the sign of the value is determined by that top degree term and when X is negative this is odd, therefore it is negative, this is positive.

So that means an F is a continuous function polynomial functions are continuous, therefore it has to cross the real axis somewhere and atleast once, therefore wherever it crosses those are the real zeros but it is atleast 1. So that shows that in fact odd degree polynomial has a linear factor. So F has linear factor, in particular it is not irreducible, in particular that is reducible.

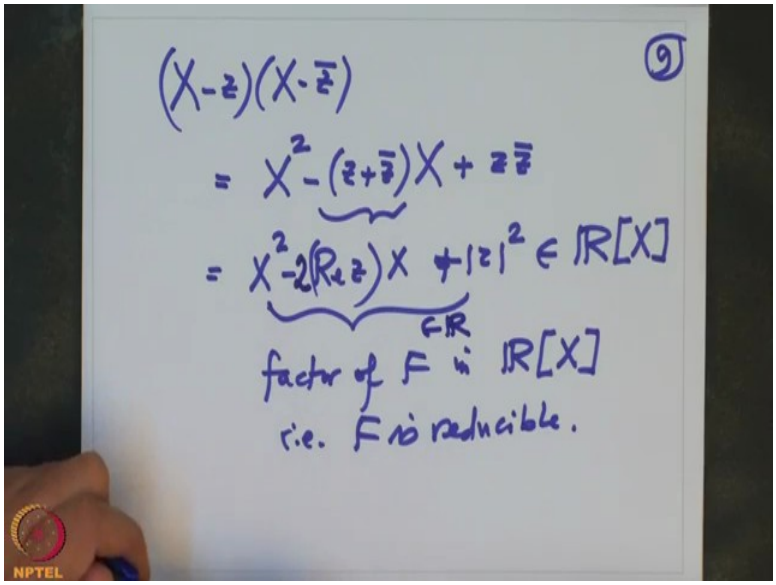
(Refer Slide Time: 26:56)



Now the even degree term if it is even degree then note that because it has real coefficients, coefficients of F are real. So if and we know by fundamental theorem of by FTA fundamental theorem of algebra this polynomial F is in $\mathbb{R}[X]$, therefore it is contained in $\mathbb{C}[X]$ and therefore by fundamental theorem of algebra there exist z in complex numbers, such that $F(z)$ is 0, but if $F(z)$ is 0 then $\overline{F(z)}$ is also 0, but then what is $F(\bar{z})$ that is because F has a real coefficients, this is nothing but $F(\bar{z})$ because when you take the bar of the polynomial that will go down to the bars of the coefficients and bars of the powers of z, that powers of $\bar{z}$ will be powers of bar of the powers of z will be powers of . $\bar{z}$

So then this equality is clear, so that means if $F(z)$ is 0, then $F(\bar{z})$ is also 0. So that means they appear in pair so and if z were a real number we are happy because then $X-z$ is a factor and we know we get what we want, if z is not real then $\bar{z}$ is also not real and therefore these two linear factors of $X-z$ and $X-\bar{z}$ bar they are linear factors in $\mathbb{C}[X]$ and they are different because z and $\bar{z}$ are different. So therefore the product will also divide F, so then $(X-z)(X-\bar{z})$ this divides F in $\mathbb{C}[X]$, but actually this is real polynomial, we just have to write down the formula for that.

(Refer Slide Time: 29:20)



So note that $X-z$ and $X-\bar{z}$ bar when you expand it, it is $X^2-(z+\bar{z})X+z\bar{z}$, but this is same as this is the real part. So this is same as $X^2-2\Re(z)+|z|^2$, so this actually has real coefficients. So therefore this is a factor of F in $\mathbb{R}[X]$, so that means F is not that is F is therefore reducible. So that is slightly one error which I would like to correct it, so for example when I said look at the product $(X-z)(X-\bar{z})$ this product is (this line is okay) here it is 2 times real part of z and 2 times real part is also real number and this is also real number, both these are real numbers.

So therefore this is a factor of F in $\mathbb{R}[X]$, so that means the polynomial F is reducible and that is what we wanted to conclude in the last part. So that proves that our claim that if you have a degree more than 3, then the real polynomial cannot be prime polynomial, okay we will continue after so what we are doing is we are assuming that the assertion that the field of complex numbers is algebraically closed and we want to draw some consequences about the

polynomials and their zeros of in a field of rational or real numbers, I will continue this after the break also, thank you.