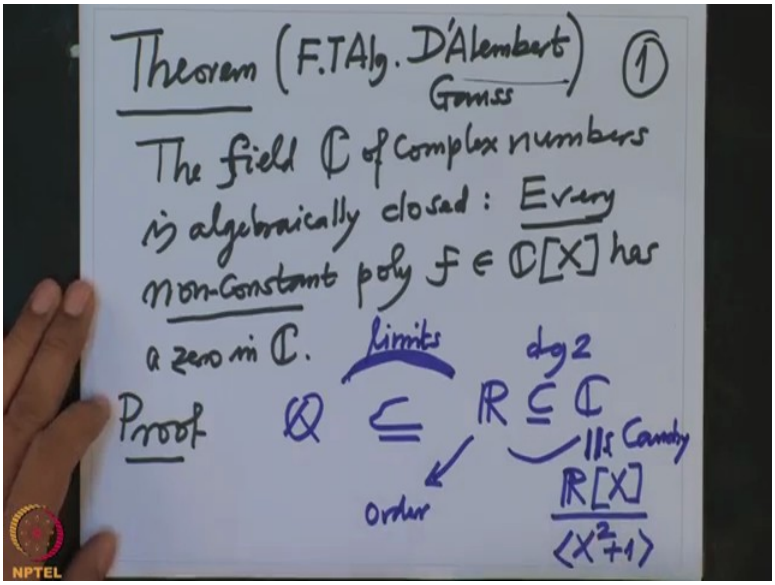
Galois' Theory.
Professor Dilip P. Patil.
Department of Mathematics.
Indian Institute of Science, Bangalore.
Lecture-53.
Proof of The Fundamental Theorem of Algebra.

(Refer Slide Time: 0:46)



Right, last lecture we saw algebraic closure of a field exists and they are unique up to K isomorphism, now we come to the proof of fundamental theorem of algebra. So we are going to prove the theorem. This is also called FTA, fundamental theorem of algebra, also, if you see the books, it is it is stated as D'Alembert Gauss. In French books it is written as theorem of D'Alembert, in German books it is written as theorem of Gauss and in English books it is written as theorem of D'Alembert Gauss.

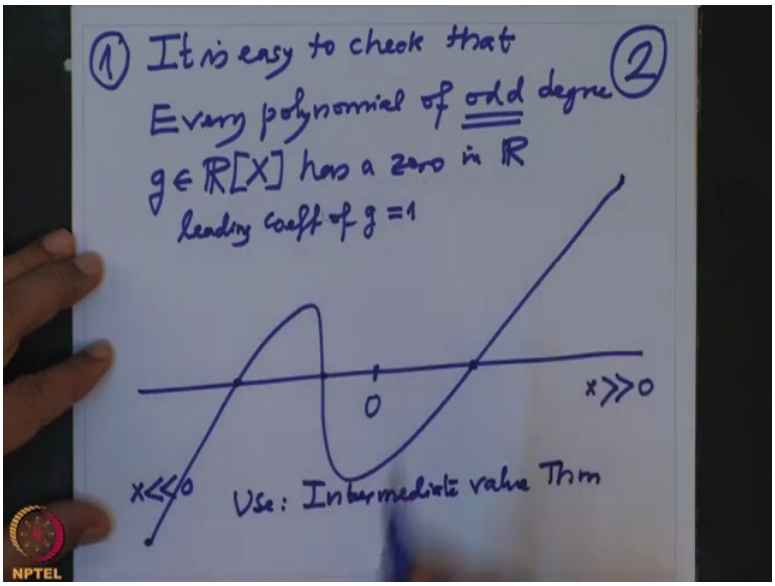
So the field $\mathbb{C}$, this is the field $\mathbb{C}$ of complex numbers is algebraically closed. So we will prove that every nonconstant polynomial f with complex coefficients has a zero in $\mathbb{C}$. This is equivalent to Checking $\mathbb{C}$ is algebraically close, every nonconstant degree is bigger equal to1, it has its complex zero, this is what we need to prove. Proof, what will be used in the proof, that is 1st I will indicate. So 1st of all note that the definition of $\mathbb{C}$ is not completely algebraic.

So we have seen rational numbers, then real numbers and then complex numbers, this is contained here, this is contained here and there is a big gap here, this gap is big and this is small, this is degree 2 extension. This is in fact $\mathbb{C}$ is $\frac{\mathbb{R}[X]}{\langle X^2+1\rangle}$. And this polynomial does not

have real zeros, this is irreducible because $\mathbb{R}$ has order. So no square will be negative. Therefore this polynomial is prime over $\mathbb{R}$, therefore it generates a prime ideal, also this is a feel in that field is precisely $\mathbb{C}$.

This was what Cauchy's and here we need limits. So definitely we will have to use some kind of algebra, some kind of calculus. And the, this proof will contain least of calculus and more of algebra, that is what it is planned here.

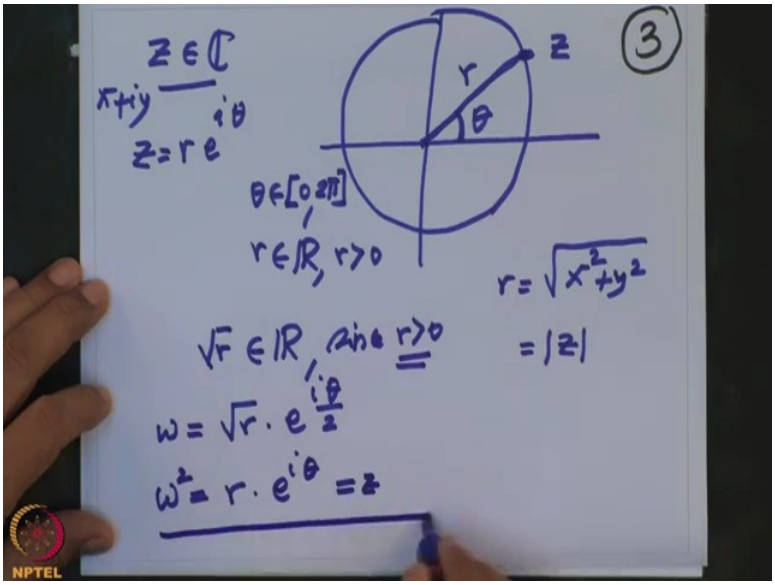
(Refer Slide Time: 4:23)



Okay, this is one remark and 1st observation I want to do that this is easy, it is easy to check that if I have every polynomial of odd degree, odd very important, odd degree g in $\mathbb{R}[X]$ with real coefficients has in zero in $\mathbb{R}$. This is very easy, what do is try to plot the graph of this function g. So observe that when you take X large positive, then obviously the sign of the $g(X)$ will be positive. So assuming that without laws we assume that leading coefficient of g is 1. If necessary we divide by that because we only have to say something about 0.

So because of that the value $g(X)$ will depend, we will be dominated by the leading term of the polynomial, which is X^n. So when X is large positive, this will be positive and similarly when X is large negative, then the polynomial, the value of the polynomial at X will be negative. So therefore the nature of the graph of g will be like this. So therefore it has to cross x-axis at least once, maybe several tough but at least once.

(Refer Slide Time: 7:05)

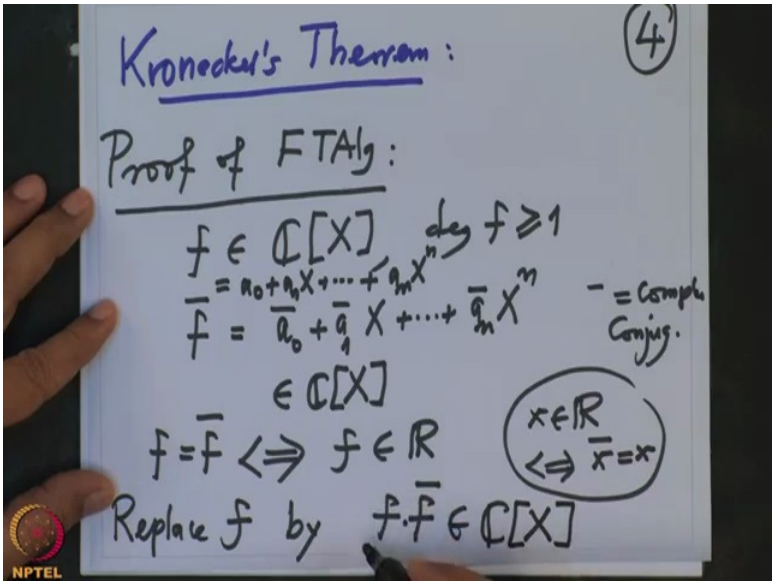


So therefore now use Intermediate Value Theorem, so that it causes the x-axis, that means it has at least one real 0. So, this was observation 1. The another observation, we use is the following. This is observation 2, every complex number $z \in \mathbb{C}$ is a square of some complex number w. So, that is there exists $w \in \mathbb{C}$ such $w^2 = z$. This is what we will also used in the proof later. You are given z, z complex number is given. So look at the polar representation of this f.

That means what, this is z, z is somewhere here and this radius and this angle. So this is z we can write it as, this is $r e^{i\theta}$ where θ is in between 0 and 2π. Actually you can make it more precise but it is okay, 0 is in between these and r is a positive real number. So this is r is in fact, if z, if z we have written it as $x+iy$ then r is nothing but $\sqrt{x^2+y^2}$, this is $|z|$. And Theta is the angle that it makes. So once you have z like this, then you have a positive real number, positive real number has a square root in real numbers.

So therefore I can talk about square root of r which is again a real number, since r is positive, this exists. And so therefore I can take w equal to square root $r e^{i\theta/2}$, take the half angle. So this is clearly when I square its, this will be r and this will be by De Moivre or , so this is e power i Theta, which is z. So every complex number has a square root and complex numbers, that I am going to use, and every odd degree polynomial has a real zero, with real coefficients, all right.

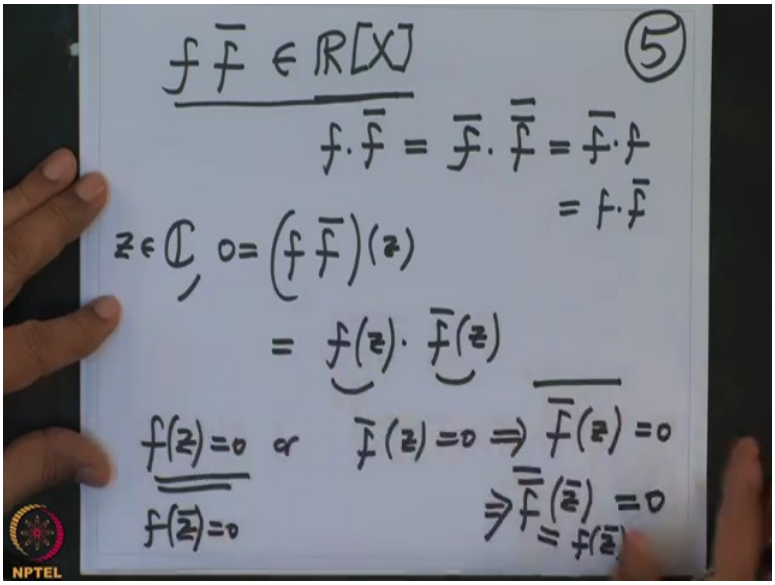
(Refer Slide Time: 10:16)



So, also I will use Kronecker's theorem, which says that if I have a polynomial over arbitrary field, nonconstant, then I can enlarge the field so that all zeros are lying in that field. So this I will not straight again, so this is what I will use here. Now let us start the proof. So, proof of FTA, so let f be a polynomial with complex coefficients, degree f bigger equal to 1, this is given to us. Okay, 1st of all let us denote f bar to be the polynomial which I obtained from f by applying conjugate, there is a complex coefficients, so I will apply conjugate to the coefficients.

So this is $\overline{a_0}+\overline{a_1}X+...+\overline{a_n}X^n$. So, where f is, f was $a_0+a_1X+...+a_nX^n$. So this bar means complex conjugation, okay. So this is another polynomial in $\mathbb{C}[X]$. It is clear that f equal to f bar if and only if this polynomial has real coefficients. That is precisely because we know that a is a, x is a real number if and only if $\overline{x}=x$, all right. So, now we want to show that this f has a complex 0.

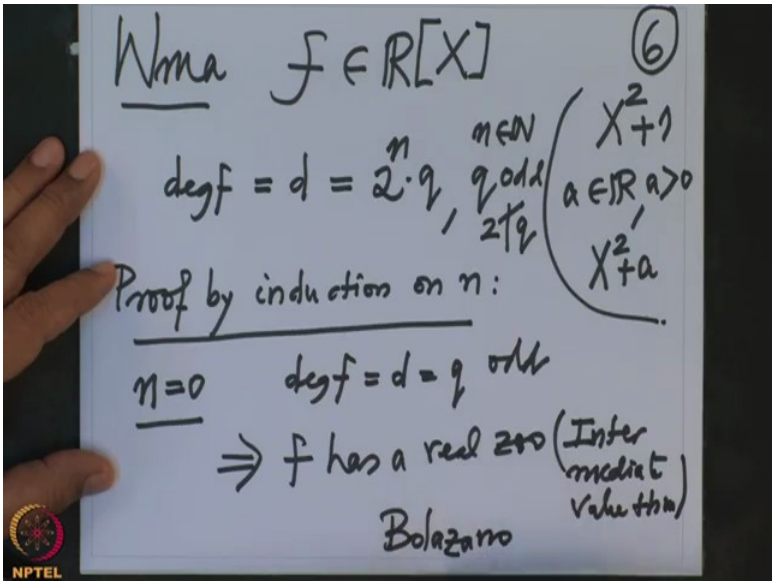
(Refer Slide Time: 13:07)



So replace f by $f.\bar{f}$. Now look here $f.\bar{f}$ is a new polynomial, this is also polynomial in $\mathbb{C}[X]$, but the advantage is this is actually real polynomial because when I take the bar of that, will get, so f by f, we are replacing f by $f.\bar{f}$, the advantage is this polynomial f times f bar has actually real coefficients. Because, how do I take somebody, some polynomial has real coefficient, I take a bar of that, bar of that is ring homeomorphism, so it is $\bar{f}\bar{\bar{f}}$ but this is $\bar{f}f$, which is the same polynomial. It is commutative, so it is $f.\bar{f}$, therefore it has real coefficients.

And if I proved that this polynomial of the complex zero, so if $z \in \mathbb{C}$ is a zero in this product polynomial, but this is same thing as $f(z).\bar{f}(z)$. And if this is zero, then this, one of them is zero at least, $f(z)$ is zero or have $\bar{z}$ is zero. If $f(z)$ is zero, we are happy, that is what we wanted, if this is zero, then you take the bar of that, so $\bar{f}(z)$ and bar that is also zero. But bar of that is same as $\bar{\bar{f}}(\bar{z})$, this is zero. But $\bar{\bar{f}}$ is f, so this is equal to $f(\bar{z})$ which is zero.

(Refer Slide Time: 14:53)



So either this or $f(\bar{z})$ is zero. In either case they found a complex zero. So therefore without loss I will assume the polynomial has a real coefficients. So, we may assume therefore f is actually polynomial in $\mathbb{R}[X]$ and we are looking for f has a zero in complex numbers. And we see it may not have a zero in $\mathbb{R}$ that our typical example is X^2+1 or for that matter any positive number, any positive real number a, we can talk about positive, negative and so on.

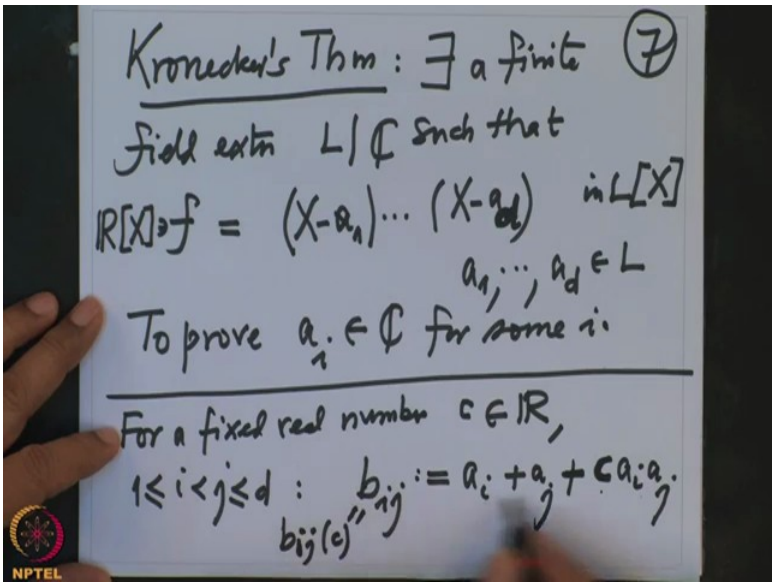
So this for example X^2+a, that cannot have zero in real numbers, because if it has a zero, then if it is b, b^2 will be equal to - a, - a is negative but b^2 is always positive. So, therefore we cannot hope to find a zero always in real numbers, all that. So we may assume f is real number, f has real coefficients. Now look at the degree of f. Degree of f we know it is bigger equal to 1, it is nonconstant. So I can always write in the form this is d, which I can always write in the form $2^n q$, where q is odd. q is odd and n is a natural number, n maybe zero also.

And I am going to prove the assertion, proof that, proof by induction on n. This is what I will do. What will be the assertion? By induction I will prove that this f has complex zero, this n. And q is odd means 2 does not divide q. This is a set. So induction will always started $n=0$, n equal to 0, what is the degree of f? Degree of f, n is zero, so degree of f is q, which is odd. Therefore what I explained in the beginning, therefore f has a, actually in this case f has a real zero.

Again I will say intermediate value Theorem. So, if you see in the history, intermediate value theorem was proved by Bolazano. This was proved by Italian mathematician Bolazano and he did not call intermediate value theorem, he called it zero theorem. So he called, he also stated

in this language that it has a real zero. Alright, so therefore our induction starts. So our strategy will be now to, from a given f which is the real coefficient, construct a new polynomial which has a real coefficient and this exponent of 2 drops and therefore we can apply induction approach.

(Refer Slide Time: 18:29)



This is to assume that the new constructed polynomial has is zero and from that zero we have to go back to the given polynomial, that is the strategy. Alright, so what am I going to do? So, first of all, so that is, we know by Kronecker's theorem tells, Kronecker's theorem says that I can enlarge my field of real numbers, there exists a finite field extension L over K or L over $\mathbb{C}$, such that f, I can write, split in $L[X]$, this I am writing in $L[X]$, I will assume it is monic for simplicity.

So it will be like $(X-a_1)...(X-a_d)$, a_d because the polynomial has Degree d and a_1 to a_d, they are elements in L. Because the same polynomial I will think polynomial with complex coefficients, though it has real coefficient. I enlarge the field L, so that it has all the zeros lying in that field. And I want to now prove that at least one of the zeros is a complex number. So to prove ai belong to see for some i, that is what we need to prove. This is what we need to do.

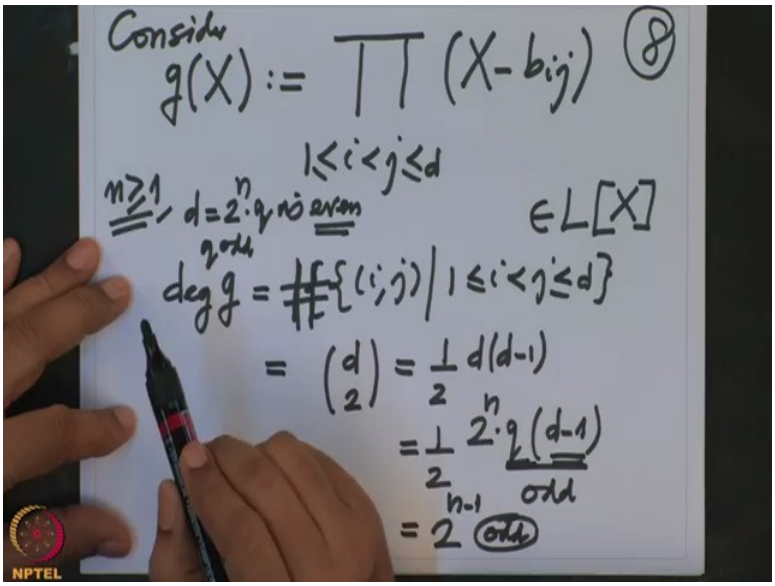
Alright, so all our calculation is done, this, this is done because all our calculation we are doing it in the field L or all the polynomials we are writing in $L[X]$, that is why we have chosen bigger field so that all the equations etc. we will write in L. Alright, now that is our aim, that we want to check that at least one of them will lie in $\mathbb{C}$. And but you will see the

proof, 2 of them will I see, that is because this has a real, where assuming this is actually real coefficient and we know therefore if we have a complex zero, one zero, then conjugate of that is also zero. So you will get into zeros, that is not surprising. So that will also come out in the proof.

Alright, so what am I going to do with this now? I am going to, for a fixed real number $\mathbb{C}$ in R and any pair one less than equal to i strictly less than j less equal to d. For this I am defining b_{ij} 's, these are another numbers, all these are happening in L, this is by definition $a_i + a_j + c\, a_i a_j$, this is b_{ij} . Strictly speaking I should write the notation b_{ij} and this b_{ij} depends on this c and therefore I write $b_{ij}(c)$. But I will, I will use this only when it is necessary, it will come at some stage where I will have to use this, then it depends on c.

But right now c is fixed and I am considering this b_{ij} and with this b_{ij} I am considering new polynomial. Remember our problem is to construct a new polynomial whose degree, in the degree, the power of 2 drops.

(Refer Slide Time: 22:34)

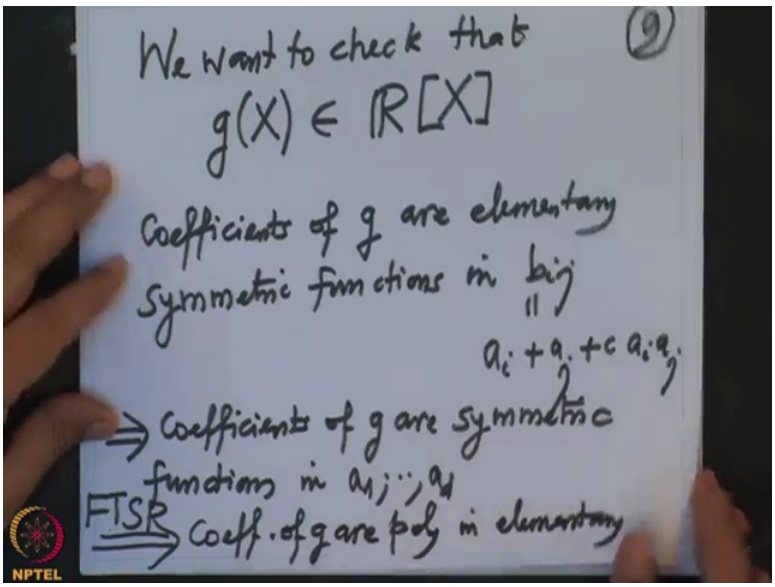


So we are considering now a new polynomial, consider a polynomial new $g(X)$, this is by definition product, product is running over $1 \leqslant i < j \leqslant d$, $X - b_{ij}$, look at this polynomial. So where is this polynomial, this polynomial a priori in $L[X]$ because a_{ij} is in L, and R is in L, therefore c is in L and therefore all these coefficients, all these products is in L. So it actually splits in L and these are the roots. What other degree, so let us find out what is the degree of g. Degree of g is the number of pairs with this property.

So, this is cardinality of the set of all pairs i, j, such that $1 \leqslant i < j \leqslant d$, this cardinality is precisely, this cardinality is precisely, you know it is, d choose 2, which is $d(d-1)/2$, which is half d I know, d we have written as $2^n q$. And remember we are assuming now what, we are assuming n is at least 1. And therefore d is, what is d, d is able to power n q, q is odd. Therefore, d is even because n is at least 1, so d -1 is odd, so this is odd, this is odd, therefore this is odd and this power of 2 is now 2^{n-1} times some odd integer.

So the degree of g has in the power of 2 has dropped there, so therefo re I will be eligible to use the induction hypothesis provided I have to assure that this polynomial has a real coefficient. That is what we have, right now I only know this polynomial has only the coefficients in the field L but now I want to check that this polynomial has coefficients in real numbers.

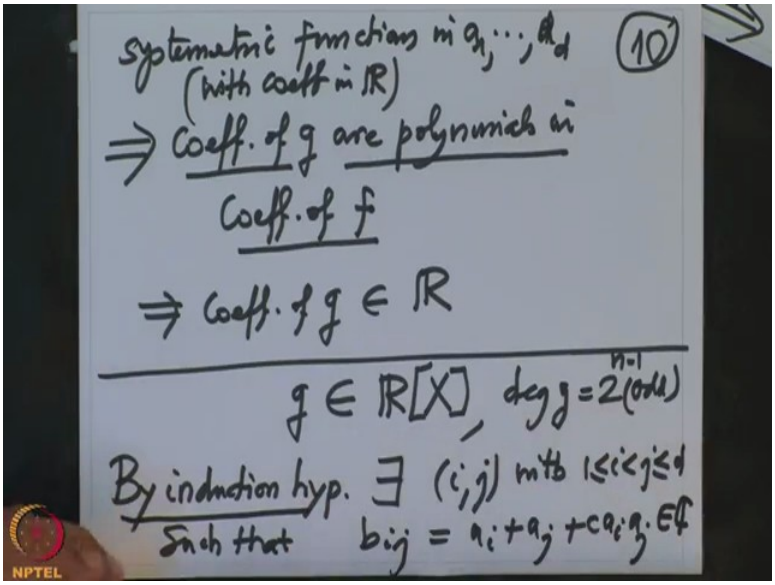
(Refer Slide Time: 25:35)



Alright, so we want to check that $g(X)$ is indeed a polynomial $\mathbb{R}[X]$, so that we can apply induction approaches. So why that, now look at the coefficients of g. Coefficients of g are, so what are the coefficients? So, look here, I have the g and the coefficients, when I multiply it out. They are elementary symmetric functions in bij, are elementary symmetric functions in bij. And what was $b_{ij}, b_{ij} = a_i + a_j + c\, a_i a_j$. And therefore they are, so, so therefore they are, so that implies coefficients of g are symmetric functions, symmetric polynomials I should say, symmetric functions in a_1 to a_d .

That is also clear because when I change, when I permute this a ij, this bij will go to some bkl, so therefore they are symmetric functions in a_1 to a_d . I cannot say they are elementary symmetric functions in a_1 to a_d , but there are elementary symmetric functions because these are elevated symmetric functions and those are, when I permute a_i , they will not change, so they are symmetric functions in a_1 to a_d . So therefore our fundamental theorem on symmetric polynomials says that these symmetric polynomials are polynomials in, so the coefficients of g are polynomials in elementary symmetric elementary symmetric functions in a_1 to a_d .

(Refer Slide Time: 28:25)

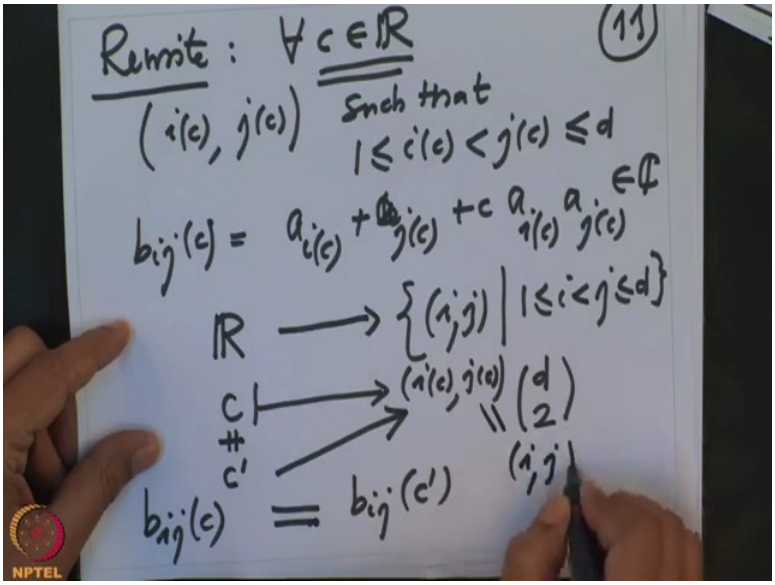


But what are the elementary symmetric functions in a_1 to a_d ? So, therefore coefficients of g and where are the coefficients, with coefficients in R, because our base field is $\mathbb{R}$. So coefficients of g are polynomials in elementary symmetric functions in a_1 to a_d , they are the coefficients of, coefficients of the given polynomial f. So the coefficients of g are polynomials in the coefficient of f with real coefficients. So altogether that proves that coefficients of g belong to $\mathbb{R}$.

So we have proved that this polynomial g is actually polynomial with real coefficient. And we have used your nice theorem which is element, fundamental theorem on symmetric polynomial. Alright, so we have established the fact that coefficients of g are in $\mathbb{R}$. So this g belongs to $\mathbb{R}[X]$, we have already noted that degree of g is 2^{n-1} times some odd number, some order number. So therefore by induction hypothesis, hypothesis, one of the zeros of g should lie in complex numbers.

So, there exists a pair i, j with 1 less equal to i less than j less equal to d, such that this b_{ij} which is $a_i + a_j + c\, a_i a_j$, this should belong to complex number, this is by induction hypothesis because I have polynomial with real coefficients, a power of 2 has dropped, therefore the, so this is, this was happening for every c real numbers. So strictly speaking I should write now c. So, let me write that, that is very important now.

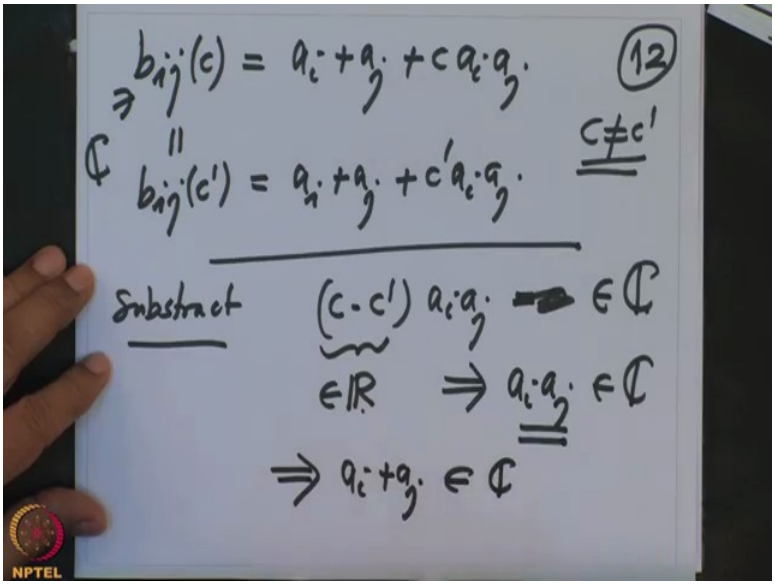
(Refer Slide Time: 30:57)



So, I am rewriting this, rewriting rewrite, what did you get? For every c in numbers, I found everywhere, the pair will also depend on c, i, c, j, c, such that 1 less equal to i, c, j, c less equal to d and b_{ij} e which is a_i , c + b, not b, $a_j c$ + e times $a_i c\, a_j c$, this belongs to complex numbers for every c. But, now note that, that means what, we have defined a map, so that is we have defined a map from R to the best with this property, we have defined a map from $\mathbb{R}$ to i, j such that 1 less than equal to i strictly less than j less equal to d, this pair.

This is a finite set of cardinality d choose 2 and we have map namely c going to (ic, jc) . So we have a map, this, we know real numbers is infinite set and the set is finite, so this map cannot be injective, this map cannot be injective, therefore there are 2 non-equal real number so that they have the same pair. Same pair means what? That means $b_{ij} c$ and $b_{ij} c'$, there equal. But what does this quality means? This equality means what, this equality means what? This equality means, so this pair is, so they are going to same pair, c and c' go to the same pair, that pair I am calling it i, j. So this c goes to this and c' also goes to that.

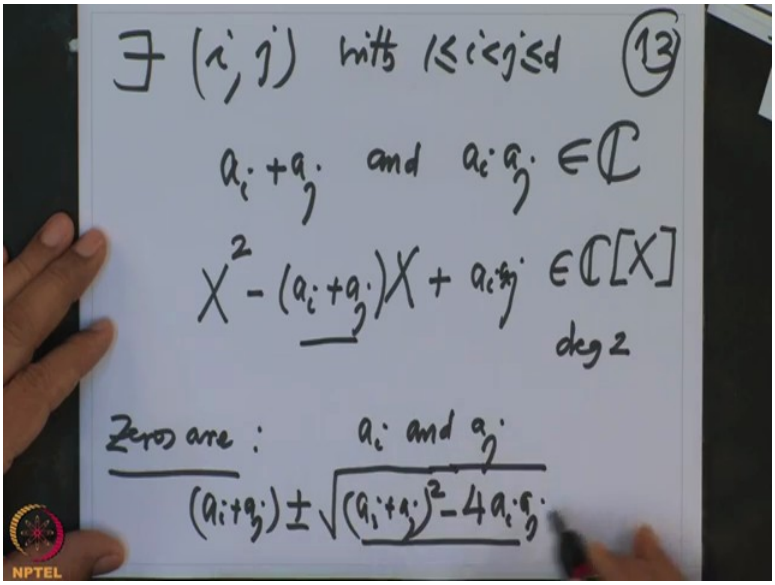
(Refer Slide Time: 33:17)



That means what bij c, this is $a_i + a_j + c\,a_i a_j$ and this is also equal to $b_{ij}c'$, that means this is equal to $a_i + a_j + c'a_i a_j$, and c is not equal to c'. Now subtract these equations, if we subtract it, this will go away, so when subtract we will get this ai will disappear, a_j will disappear and $c - c'$ will be ai aj, so this c and c' is in real numbers. So, this is, this is I know this is a real, this is, these are same, and we know they are complex numbers, so they are subtraction will also be complex numbers.

Because we are assuming this by induction this has a complex zero and that is same thing as this, so this is in complex number, this is real number and this is nonzero, therefore I can conclude the product ai aj belongs to the complete numbers. When this belongs to the complete number, c is real number, therefore I can conclude immediately $a_i + a_j$ is also complex number.

(Refer Slide Time: 34:54)



So, I got, I got a pair, so what did we conclude, the conclusion is there exists a pair i, j with 1 less equal to i less than j less equal to b, such that $a_i + a_j$ and $a_i a_j$, both these are complete numbers. And from here I want to conclude now both individually they are complete numbers. That is because now look at the quadratic equation, $X^2 - (a_i + a_j)X + a_i a_j$, this is a polynomial with complex coefficients. And degree is 2, degree 2 and we know how to solve this.

The roots are, zeros are precisely what? Zeros are precisely, what formula, that is -b, so what are the zeros, they are precisely $a_i a_j$, a_i and a_j and we know how to solve quadratic equations over c. That will just amount to say that if you can solve, so the zeros, our formula is - the coefficient of b, that is $a_i + a_j \pm \sqrt{b^2}$, that is $a_i + a_j$ whole square - 4, this is $a_i a_j$. But I know this is a complex number, this is a complex number, this is a complex number, so inside is a complex number and square root is also complex number because we check that for every complex numbers are the square root is also a complex number.

So this is complex, this is also complex number, so this is a complex number. So, therefore but there actually this, the zeros are, when you simplify this formula, 0 is precisely this, zeros are ai and aj, so this is ai or aj and so therefore they are complex numbers. And therefore we are done, because we have actually checked that 2 of them are complex numbers. Not surprising because we had reduced to the case where the polynomial has real coefficients. So

with this now we have proved that fundamental theorem of algebra, which was very important and as you see this proof has used the analysis least possible.

Obviously you cannot all the way avoid completely analysis but this is, this avoids many other, other, this is much, in my opinion, this proof is much simpler than any other proof and let me say that this proof is actually based on the ideas of Lagrange. So, with this I will stop this and we will continue our study of zeros of the polynomials on one side, on the other side the groups and especially Galoi's groups of the field extinctions. So, given polynomials, we will construct fields and given fields we will talk about groups and then this interplay we will make it more and more intimater, that is the whole goal of this course. Okay, thank you.