Galois' Theory

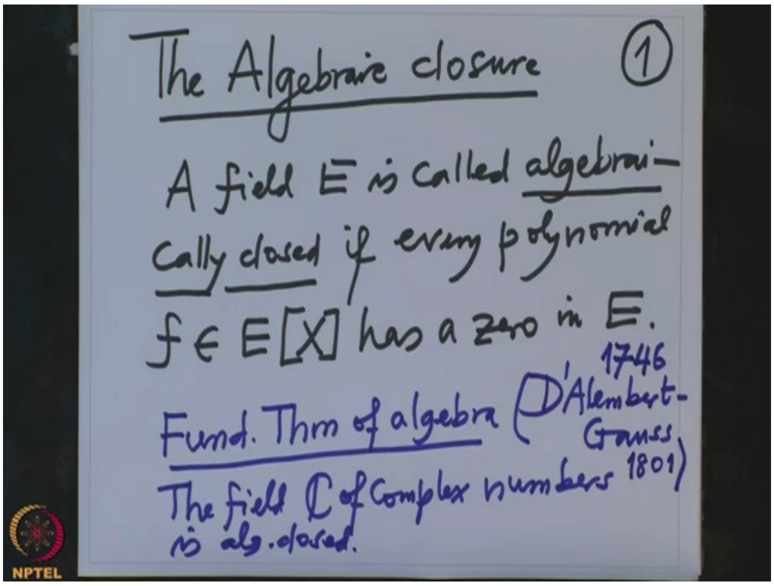
Professor Dilip P. Patil
Department of Mathematics
Indian Institute of Science, Bangalore

Lecture 51

Existence of Algebraic Closure

In the last lectures we have been studying field extensions, algebraically field extensions and sometimes in between also I have used the words like algebraically closed or algebraic closure of a field, etc. etc. now we will prove the existence of algebraic closure for an arbitrary field and also we will prove long pending statement which I have been saying that is the fundamental theorem of algebra which says that the field of complex numbers is algebraically closed alright.

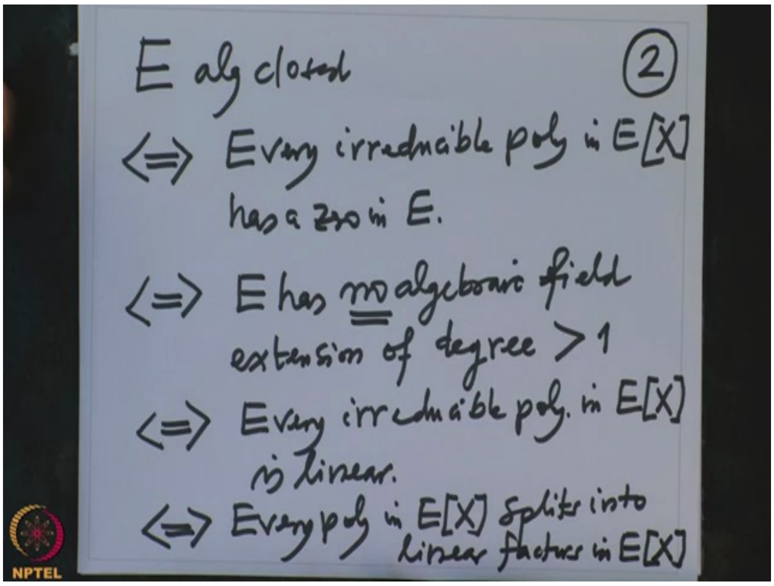
(Refer Slide Time: 01:05)



So first let me prove the existence of the algebraic closure, so this today's lecture is about the algebraic closure alright so recall that field E is called algebraically closed if every polynomial f with co-efficients in E has a zero in E then we call the field to be algebraically closed and we will prove that $\mathbb{C}$, this is what we will prove, this is the fundamental theorem of algebra this is the field of, the field $\mathbb{C}$ of complex numbers is algebraically closed.

This is also known as theorem of D'Alembert-Gauss, D'Alembert stated this in 1746, D'Alembert was a French mathematician and Gauss was German as one knows, this is was proved in 1800 approximately 1801, that is Gauss and Gauss's proof was considered first complete correct proof of this theorem which he did in approximately 1800 but there are other proofs also today and the proof I am going to give is will be based on the ideas of Lagrange which was before Gauss.

(Refer Slide Time: 04:03)

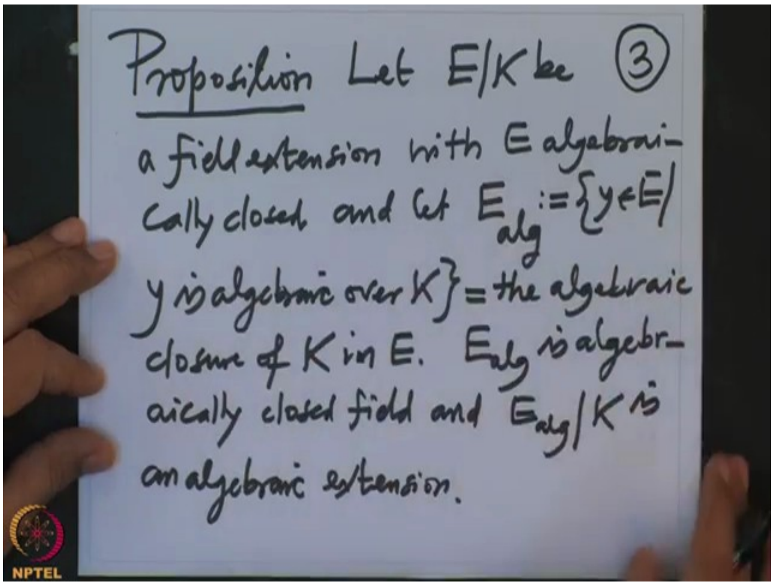


Okay so let us prove, I want to prove that every field has an algebraic closure but before that let us observe some easy facts so let E be a field so E is algebraically closed that means every polynomial with co-efficients in E has zero in E, this is equivalent to saying every irreducible polynomial in $E[X]$ has a zero in E because we know every polynomial is a product of irreducible polynomials so if an irreducible factor is zero then the product will have also zero the same zero.

So I am noting this side because I will use this with reference further so this is also equivalent to E as no algebraic extension, algebraic field extension of degree strictly bigger than 1, no algebraic extension of E as degree more than 1 so that means the only algebraically extension of E is E itself also equivalent to saying that every irreducible polynomial in $E[X]$ is linear, linear polynomials are the only polynomials okay.

Also equivalent to saying that every polynomial in $E[X]$ splits into linear factors in $E[X]$, this is also because every polynomial splits into irreducible one and irreducible polynomials are linear therefore all these equivalences are just nearly a re-statement of the definition, so I will use them whenever there is a possibility and I will not explicitly say why it is so.

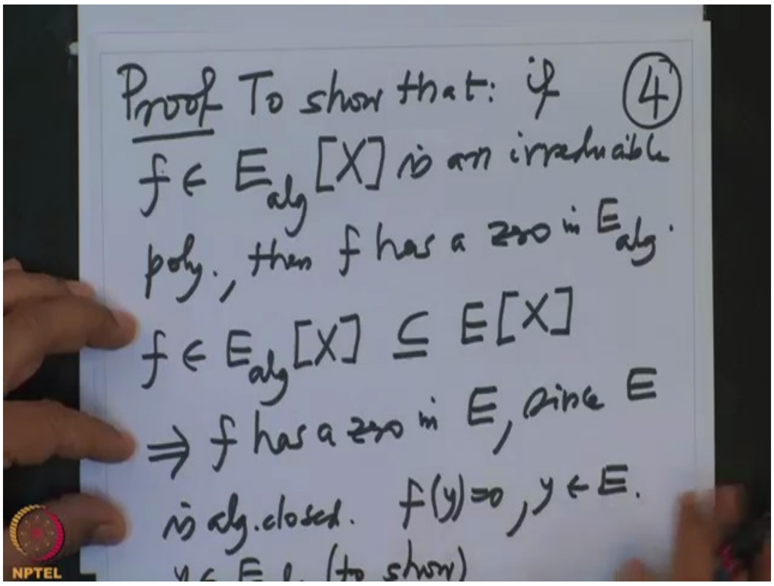
(Refer Slide Time: 06:33)



Now another easy preposition, so let E over K be a field extension with E algebraically closed then and let us denote E alg, this is by definition, all those elements in E, y in E such that y is algebraic over K so this is what we call it the algebraic closure of K in E, we have seen that the algebraic closure is a sub-field and now this says if E was algebraically closed then the assertion says that E algebraic, this alg is algebraically closed field and obviously E alg over K, K is an algebraic extension.

This is clear because these are precisely all algebraic elements over K so this is algebraic extension is clear I want to show that E is algebraically closed field and this is because E is algebraically close okay so let us prove this, so proof, what do we want to show?

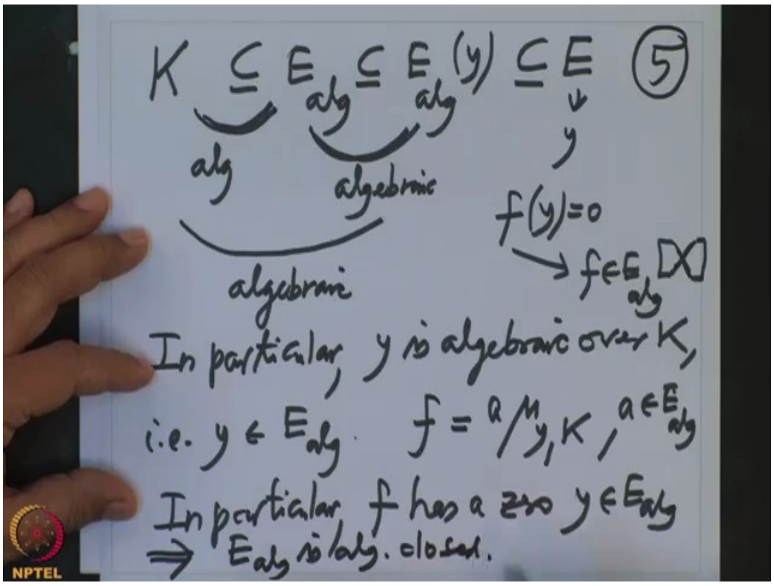
(Refer Slide Time: 08:46)



We want to show that every polynomial so we want to show that, so to show that if f is an polynomial with co-efficients in this E alg, this is an irreducible polynomial then I want to show that has then f has a zero in E alg, this is what I want to show, well but f is an polynomial in E alg, coefficients are in E alg that means the co-efficients of f are algebraic elements over K because this is a sub-field of E is clearly contained in $E[X]$.

So f is a polynomial in $E[X]$, E is algebraically closed, f may or may not be irreducible in $E[X]$ because we are taking over a bigger field but in any case this polynomial will have a zero in E because E is algebraically closed then f has a zero in E since E is algebraically closed and let us call that zero, f has a zero so $f(y)$ is 0 for some $y \in E$, I want to actually check that this y lies in E alg. So to show that we will show that y is in E alg that means I want to show that y is actually algebraic over K, so this is to show.

(Refer Slide Time: 10:59)

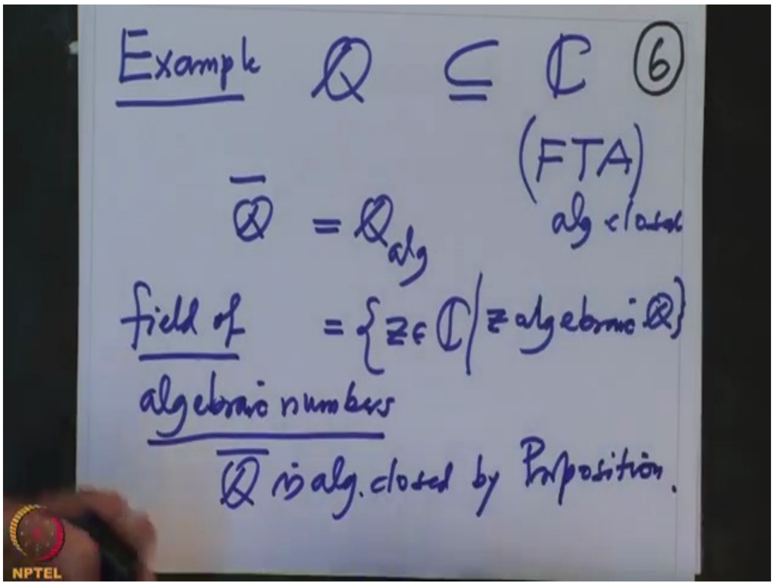


Well but what do we know? We know the following thing, K is here, E alg is here, E is here and then this I want to adjoin that y which is here, now this y is an element in E, y was an element here and y satisfies the polynomial f, so note that this extension is algebraic but definition of this and this extension is also algebraic because this y satisfies the polynomial $f(y)$, this f was polynomial in E has co-efficients in this.

So therefore this extension is algebraic, this extension is algebraic, therefore composite is algebraic, the transitivity of algebraic elements so this extension is algebraic, in particular y is algebraic over K, but this means so that is y belong to E alg by definition of E alg but then if Y belong to E alg and this $f(y)$, so that means there is, so this means this f which was an irreducible polynomial in E alg, this was irreducible in E alg, so this has to be a multiple of, a minimal polynomial of y over K, some constant a, a belonging to some constant, where it is, it does not matter.

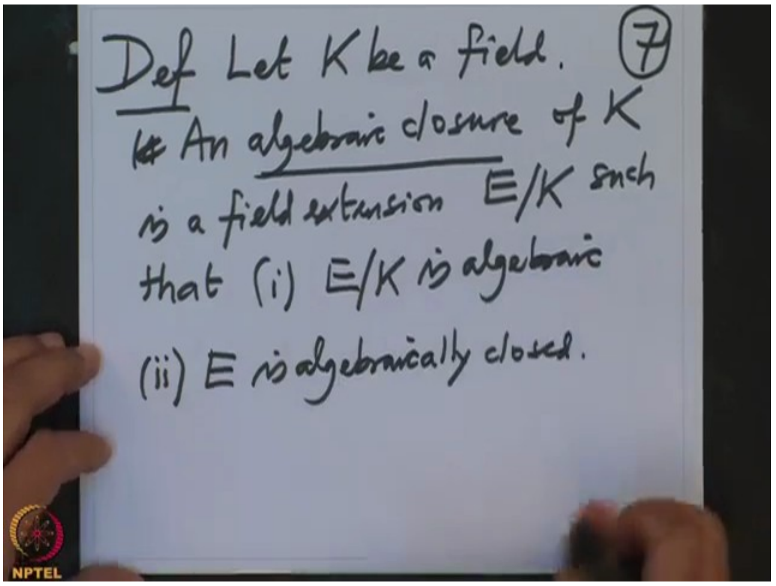
So therefore this f has a zero, so in particular F has a zero y which is also in E alg so that means we have proved that every irreducible polynomial in E alg X has a zero in E alg so that therefore so this shows that so therefore E alg is algebraically closed this is what it proved, so remember what we have proved is, if you have an algebraically closed field which is an extension of a field, then the algebraic closure of this field in that is also algebraically closed, typical situation is the following.

(Refer Slide Time: 14:10)



So example, so we have $\mathbb{Q}$ here and $\mathbb{Q}$ is a sub-field of complex numbers and fundamental theorem of algebra FTA says that this is algebraically closed, we have not yet proved but we will prove, this is algebraically closed and now we take the algebraically closure of $\mathbb{Q} \subseteq \mathbb{C}$ that is also denoted by $\mathbb{Q}$ alg this is also standard notation is $\overline{\mathbb{Q}}$ which is by definition all those complex numbers $z \in \mathbb{C}$ such that z is algebraic over $\mathbb{Q}$, this is a field, it is called field of algebraic numbers and above preposition says that this is $\mathbb{Q}$ bar is algebraically closed by preposition so because $\mathbb{C}$ is algebraically closed alright.

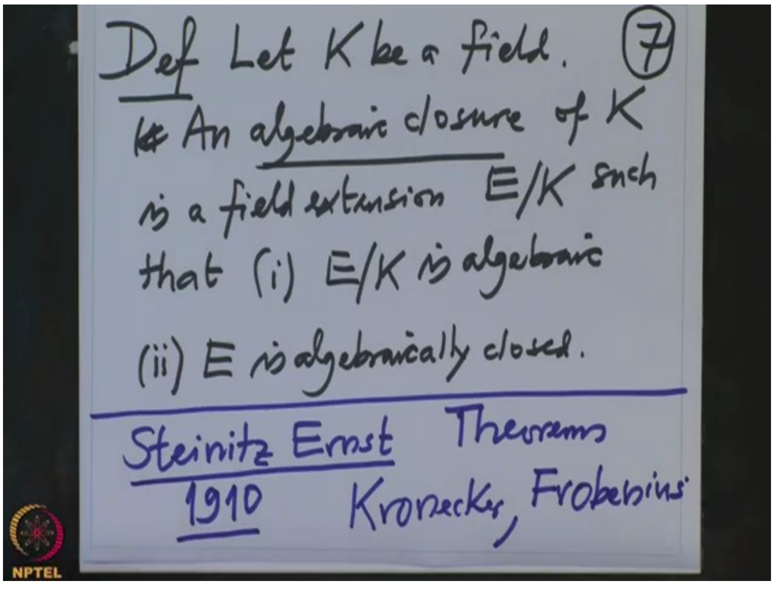
(Refer Slide Time: 15:39)



So let us continue, now I want to prove that every field has an algebraic closure, so first let us define properly, what is an algebraic closure so definition, let K be a field, a field extension an algebraic closure of K is a field extension E over K such that two conditions, 1 is E over K is algebraic that means every element of E is algebraic over K and second e is algebraically closed.

So this means in some sense this is the smallest algebraically closed field which contains K but this is more precise where smallest means what, that is little bit loose but this is proper now we want to show that given any field K there is a field extension such that E is algebraic and E is algebraic over K and E is algebraically closed.

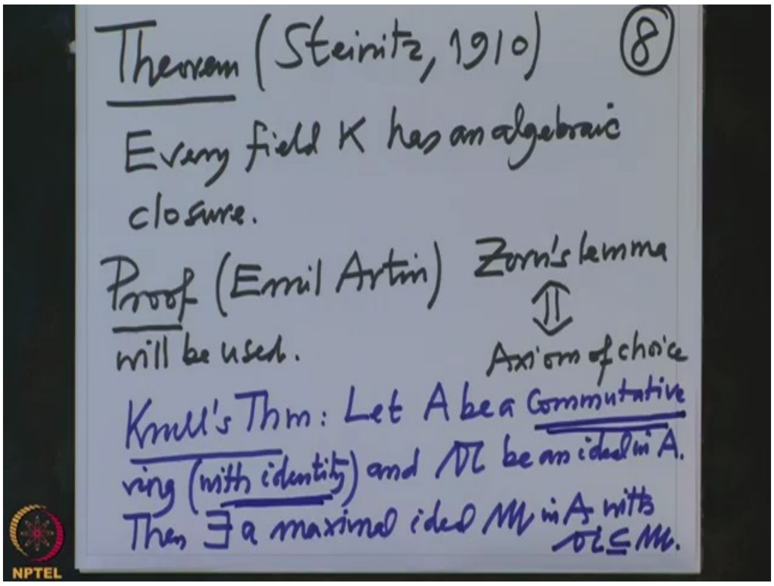
(Refer Slide Time: 17:20)



So these theorems were proved by, so these are called Steinitz Ernst theorems and he proved this theorems in approximately in 1910 where the rigorous algebra started or rigorous theory of fields was first done properly by Steinitz in 1910, Steinitz was a student of Kronecker and also one of his teachers was Frobenius, so we will prove this precise theorems and these was the first time was used the main ingredient in the proof was little bit abstract that is why this theorems were proved only after the set theory became more prominent and transfinite methods of set theory was introduced by Cantor and Steinitz used them.

Steinitz used them in the proofs and also worth noting that Steinitz used Axiom of Choice because but I am going to use Zorn's lemma so they say in proof but instead of Axiom of Choice, I am going to use Zorn's lemma which is more comfortable, Zorn's lemma was proved in 1940s, Zorn was a student of Artin alright so let us state the theorem.

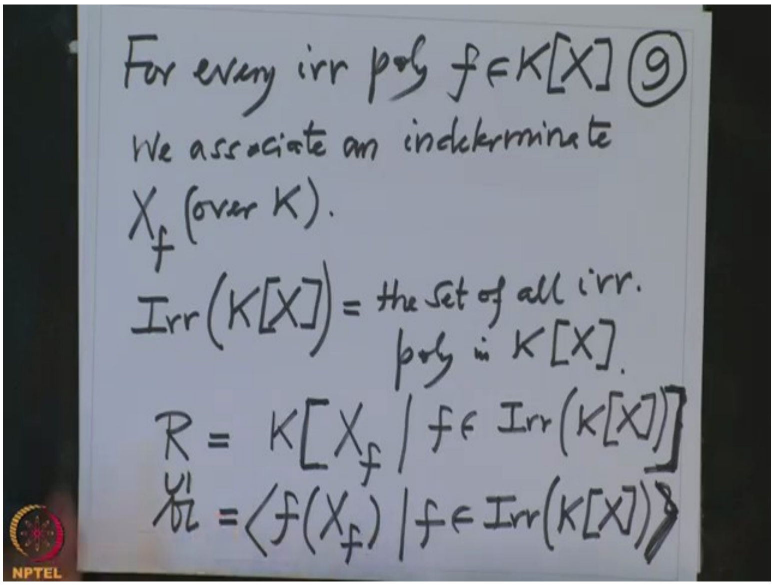
(Refer Slide Time: 19:10)



So this is the theorem we are going to prove, this is Steinitz, 1910, so every field K has an algebraic closure, proof, as I said the same proof but this is arrangement form Emil Artin and what we will use is, we will use so called Zorn's lemma, Zorn's lemma will be used in this proof, so we know Zorn's lemma which is equivalent to Axiom of Choice, I mean I am not going to go to these proofs, this is just for the side comments and how will it be used?

It will be used in the form that, let me recall you that we are going to use this fact, this is known as Krull's theorem which says that let A be a commutative ring and remember that our ring has always identity but I will stress it here with identity and a be an ideal in the ring A then there exists a maximal ideal m in A which contains with a is contained in m, so I will use this Krull's theorem which uses Zorn’s lemma and therefore I said in the proof of this theorem we will use Zorn’s lemma and remember in this Krull's theorem commutative is very important and the ring with identity is also very important alright.

(Refer Slide Time: 22:15)

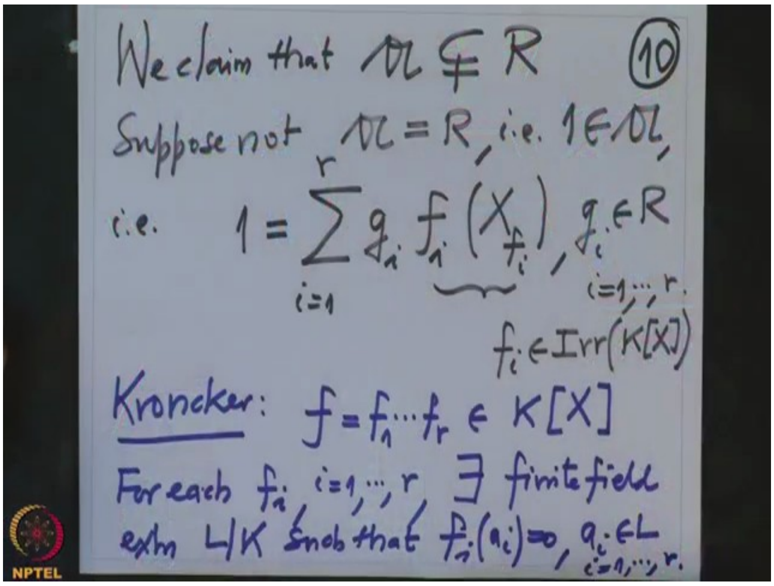


So let us continue the proof, we want to construct am algebraic closure for a given field alright so what do we do, first I will construct a ring, so what we want to prove, so I want to do that for every irreducible polynomial $f \in K[X]$, I want to associate, we associate an indeterminate which I will denote by X_f over K so that means what, so and the set of all irreducible polynomials I am going to to denote by $Irr(K[X])$, this is the set of all irreducible polynomials in $K[X]$.

So they are many, infinitely many, in fact if your field is uncountable this also will be unaccountably many and so on and I am going to consider a ring R which is the polynomial ring over K in all these indeterminates, X_f where f is varying in this set of irreducible polynomials in $K[X]$, so this is a polynomial ring in infinitely many variables, this is a polynomial ring in so many variables, they are many many variables.

So we are going to consider this and also I will consider ideal A in this ring R which is generated by this elements, so this is ideally generated by f and you write instead of $X, X_f, f(X_f)$ where X is varying in irreducible polynomials of $K[X]$, so this is an ideal generated by this polynomials, so that means all R linear combinations of these are contained there right, this is ideal generated by this set is precisely all R linear combinations of this polynomials f evaluated at X_f and first thing is now we claim that this is a proper ideal.

(Refer Slide Time: 25:12)

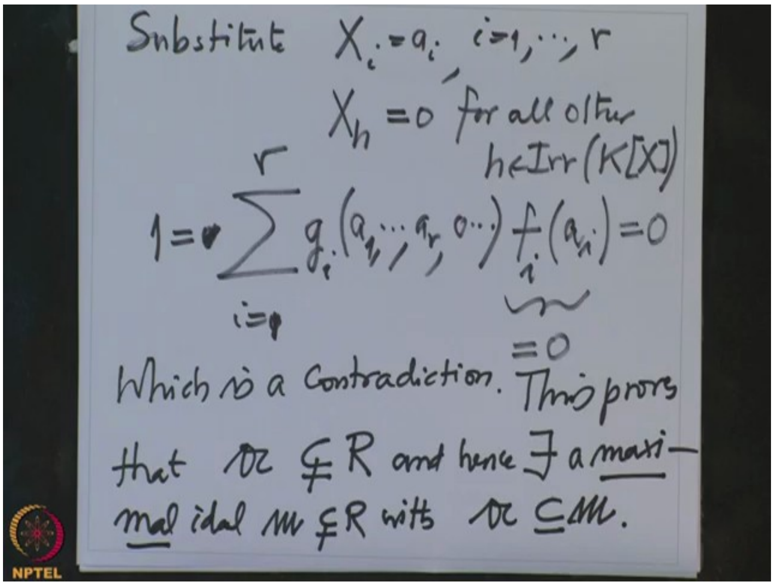


Because I want to choose a maximal ideal in this ring so maximal ideal which contains all this polynomials so I want to claim that this ideal A is, so we claim that this idea a is a proper ideal, so suppose a contrary, suppose not that means what, a is R but that means that is 1 will belong to a but that means that is I will have 1 can be written as a combination of R linear combination of finitely many polynomials so those are $f_i(X_{f_i})$, i is from 1 to r where gi's are arbitrary polynomials in R and these are the generators of this ideal a.

And I am looking for a contradiction, these f_i 's were some irreducible polynomials, now I am looking for a contradiction, so the contradiction will come because now I am going to use Kronecker's theorem, Kronecker's theorem says that if I have a polynomial over arbitrary field then that polynomial splits if I enlarge the field then that polynomial splits completely into that field, enlarged field.

So Kronecker's theorem I am going to apply it to the polynomial f which is the product of these finitely many f_i 's so $f_1,\dots,f_r$, this is the polynomial in $K[X]$ and I will assume for each f_i, i is from 1 to r, there is a field L finite field extension L over K such that $f_i(a_i)=0$ with $a_i \in L$ and this is true for all i, 1 to r, this is by Kronecker's theorem, now once I have that we have this equation, this equation I am going to substitute in that equation.

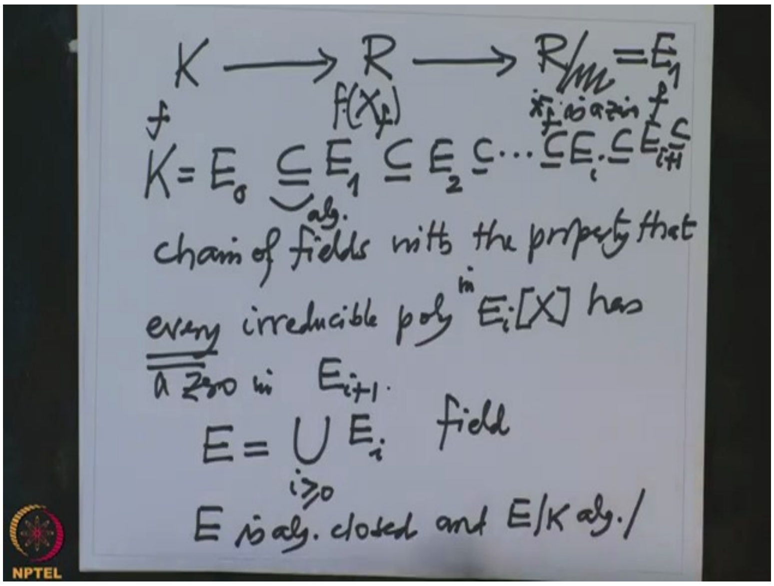
(Refer Slide Time: 27:59)



So substitute X_i equal to these a_i this is for i equal to 1 to r and all other variables, all other X_h put them to 0 for all other $h \in Irr(K[X])$, so what we will get, I get 1 here so we will get 1 equal to summation i equal to 1 to r, g_i evaluated at this $a_1, \ldots, a_r$ and the remaining variables are putting zeroes and f_i all these variables we are putting a_i 's. But this that is 0, therefore all together 1 will be equal to 0 which is a contradiction because which is a contradiction.

So therefore this proves that the ideal a is cannot be unit ideal so it is a proper ideal and hence there exists a maximal ideal m in R with a contained in m and why maximal, because we want to construct a field so therefore we have the situation now is this.

(Refer Slide Time: 30:03)

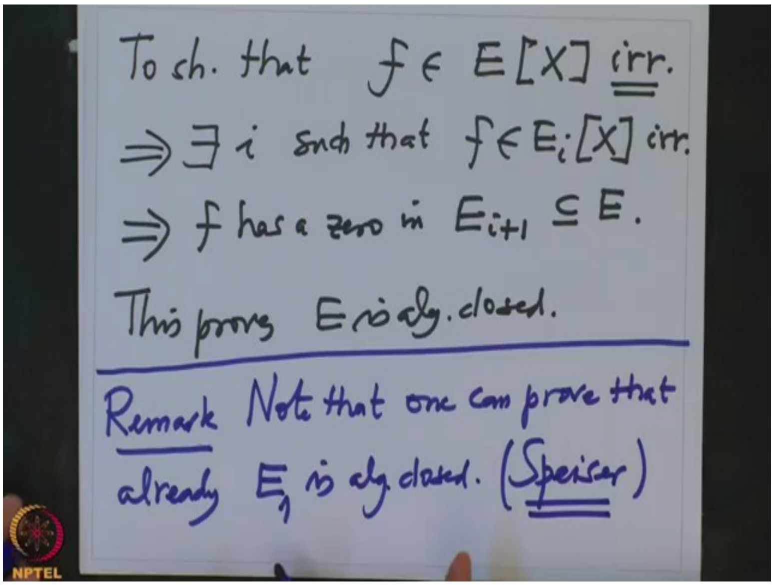


K to R with a natural infusion and R to the residue map, R to $\frac{R}{\langle m \rangle}$, this is a field and this is even and therefore I get even and field extension of K so K is here that we call it E_0 and I have extended this to E_1 and I will repeat this process, what process, I take all irreducible polynomials and adjoin and take the polynomial ring and consider the ideal and so on, so this is embedded in E_2 , etc. and keep doing this, this is embedded in E_i , this is embedded in E_{i+1} , so I have the chain of fields and with what property?

With the property that every irreducible polynomial in $E_i[X]$ has a zero in E_{i+1} , every, so here this is E_1 and if you take an irreducible polynomial f here we have that variable X_f here and this has a zero here namely image of this X_f , small x_f this x_f is a zero of f in E_1 , so that is how we have chosen this maximal ideal which contain all these generators $f(x_f)$ and this goes to zero here therefore this property and this we are doing it for every step.

So and now I want say, we want to claim that I take the union now, E is a union of all these i big or equal to 0 E_i , this is a field and we want to check that this is E is algebraically closed and obviously each this stays is algebraic and therefore E is and E is algebraic over K okay so how do you check? First of all it is a field, why? Because all these E_i 's are field and therefore we can define addition and multiplication and those will be well defined because it is a chain, so it becomes a field and now I have to show that it is obviously algebraic over K because each stage is algebraic over K and algebraic is transitive.

(Refer Slide Time: 33:19)



Now we only have to justify that E is algebraically closed but that means what we want to check that, so to check that, to show that if I have a polynomial f in $E[X]$ irreducible then I should prove that it has a zero in E but I know this f is one polynomial so it will have involve only finitely meaning co-efficients so therefore there exists an index i such that f actually has co-efficients in E_i and if it is irreducible here, it will also be irreducible here and therefore by construction f has a zero in E_{i+1} but E_{i+1} is contained in E, so that is it.

So this proves that E is algebraically closed so we have finished the proof of the Steinitz Theorem which say that every field has an algebraic closure, now I want to remark here which I do not know whether it will be proved in this course but it is very very important, the above process actually should stop at 1 only so note that one can prove that already E_1 is algebraically closed, this was remarked by Speiser, which if I have time I would comment it when we have the appropriate machinery.

Okay with this I will stop and continue in the next uniqueness of the algebraic closure, so we will have to state it precisely and prove that it is unique, unique upto K-isomorphism this is what we will do it after the break, thank you.