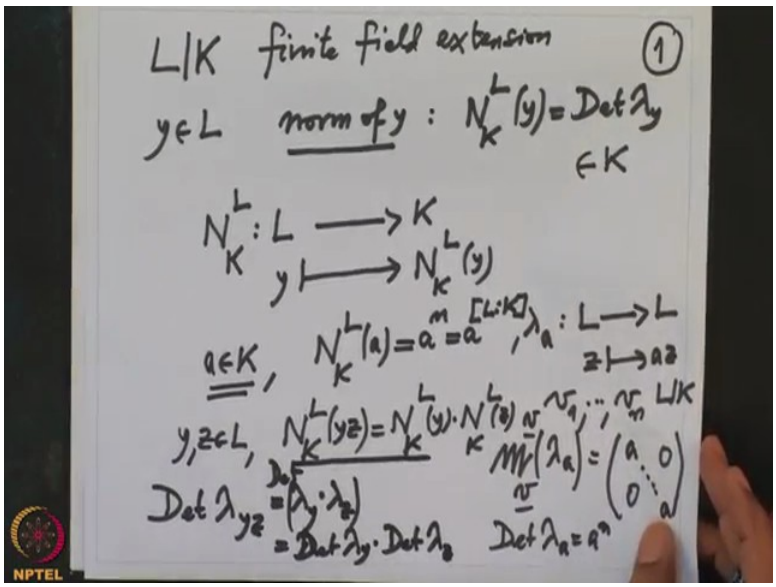
Galois' Theory
Professor Dilip P. Patil
Department of Mathematics
Indian Institute of Science Bangalore
Lecture No 31
Primitive Element Theorem for Galois Extension

(Refer Slide Time: 0:44)



In the last lecture we have defined norm and trace of an element of a field extension, so let me write down the definition once again, so we started with the finite field extension L over K finite field extension and for an element y in L we have defined 2 elements one is called a norm of y this is by definition $N_K^L(y)$ this is nothing but the determinant of the K linear map λ_y and this is an element of K, so therefore norm of L over K you can think it is a map from L to $K[y]$ going to norm of y.

So what are the properties? First of all it is obvious that if a is in K then what is the norm of a? So for that I will have to compute the metrics of λ_a map, λ_a is a map from L to L multiplication by a, so z going to az, so remember a is in K therefore if I take any basis any v_1 to v_n any basis of L over K then where will λ_{v_1} will go? λ_{v_1} will go to av_1, so

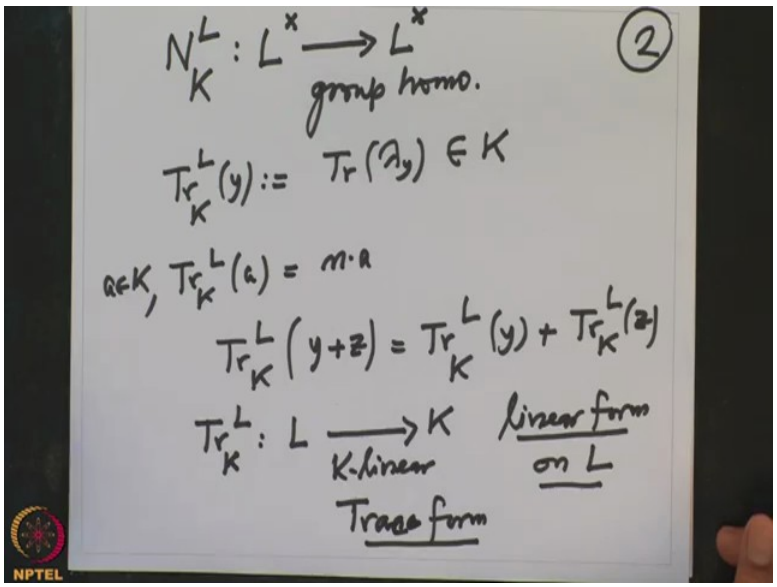
therefore the matrix of λ_a with respect to the basis v this is nothing but the diagonal

$$\begin{bmatrix} a & 0 & \cdots & 0 \\ 0 & & & 0 \\ \vdots & & & \vdots \\ 0 & 0 & \cdots & a \end{bmatrix}$$

, so therefore the determinant of λ_a is a^n therefore λ_a is a^n .

Remember this n is the degree of the field extension, so for base elements this a power that, moreover it is multiplicative, so λ if y and z are 2 elements in L then L norm of yz is same thing as norm of y times norm of z. This is clear from the fact that determinant is multiplicative, determinant of λ_{yz} is same thing as λ_y composition λ_z this is clear. So if I take determinant of this it is determinant of λ_y times determinants of lambda z and that precisely mean this formula, so it is a multiplicative map from L to L it preserve multiplication. In other words the norm of 0 is… what is norm of 0? It is 0 because it is a determinant of a 0 matrix, so actually one should say 1.

(Refer Slide Time: 4:10)

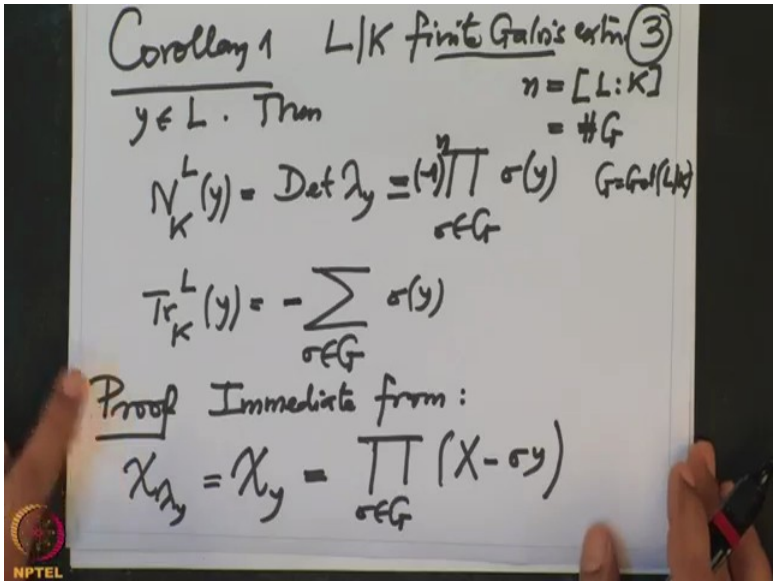


So therefore you can think norm is a map from L^x to L^x and this is a group homomorphism. Alright now about the trace, so what was trace of y that is also same notation this is by definition the trace of this matrix λ_y , so first of all note that what will be the trace of an element in K if a is in K then the trace is nothing but n times a because the matrix is a diagonal matrix in this case with respect to any basis a diagonal matrix with entries a, so

therefore trace is n times a. Moreover it is K linear so that means $trace_K^L(y+z)$ is same thing as $trace_K^L(y)+trace_K^L(z)$, so therefore trace is a linear map from L to K.

This trace is an element in K, so therefore it is a K linear map from L to K therefore it is also called a linear form therefore it is a linear form on the vector space L, so therefore it is also called a trace form this is the reason it is called a trace form and this is very important to study separability but I do not need it right now it is more important for us to prove now what other formulas if you assume the extension is Galois then can we say something what about computation of norm and trace in terms of the Galois group. So all our methods should not address always something about field extension in terms of the groups and conversely that is always our motto in this course.

(Refer Slide Time: 6:36)

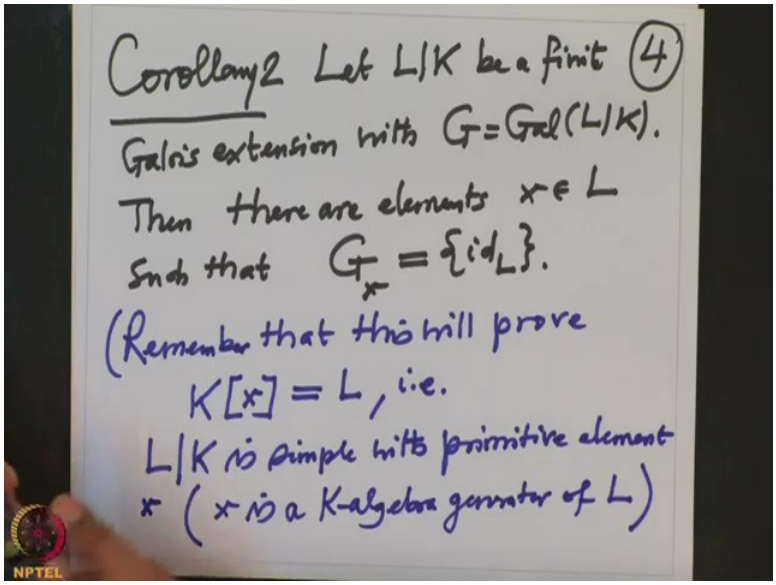


So I will write corollary 1 to our theorem which we proved which describe minimal polynomial, characteristic polynomial and also which said when can L be simple that is if and only if the isotropy is trivial, so L over K corollary 1, let us take L over K to be finite Galois extension and y is an element in L then I want to write down the formulas for the norm and trace. Norm of y is nothing but which is by definition it was the determinant of y which is nothing but product σ in G $\sigma(y)$, so if you know y if you know the Galois group you can computed easily.

Trace of y is sum of the $\sigma(y)$ where σ is in G and how do you prove this? The simply follows so proof immediate from the equation characteristic polynomial of why equal to the

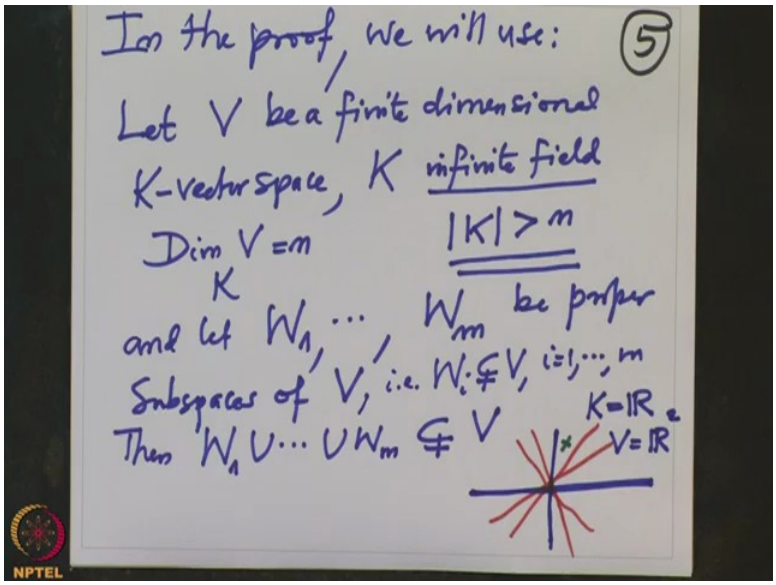
product $\sigma \in G$ $X - \sigma(y)$ because what is the norm? Norm is a determinant up to a sign and trace is the second coefficient but this is as I said to check in the last lecture this is λ_y, so once you know this then what is the constant term? That is you have to put X equal to 0 but that is precisely this. I think I have to right sign here so that sign will be $(-1)^n$ where n is the degree of this field extension which is also equal to the cardinality of G because we are assuming it is a Galois extension and G is the Galois group of L over K. Okay and this one is clear that is the 2nd coefficient, so this is also the minus sign. Alright, so these are the formulas for the trace and norm.

(Refer Slide Time: 9:53)



Now what we have kept pending is the finite Galois extensions as primitive elements, so that I want to deduce now, so I will call it a corollary 2, let L over K be a finite Galois extension with Galois group G with G equal to $Gal(L|K)$ and what do you want to prove? We want to prove that it is a simple extension, so then there are elements $x \in L$ such that isotropy at x is a trivial. Remember if you prove this so I will just note it here, remember that from the last lectures this will prove $K[x]$ equal to L that is L is L over K is simple with primitive element x. Note that I will also keep using the term x is a K algebra generator of L. So this will prove our observation so I want to choose an element x, I want to show that existence of elements so that the isotropy is trivial. This is very simple again let us prove this.

(Refer Slide Time: 12:27)

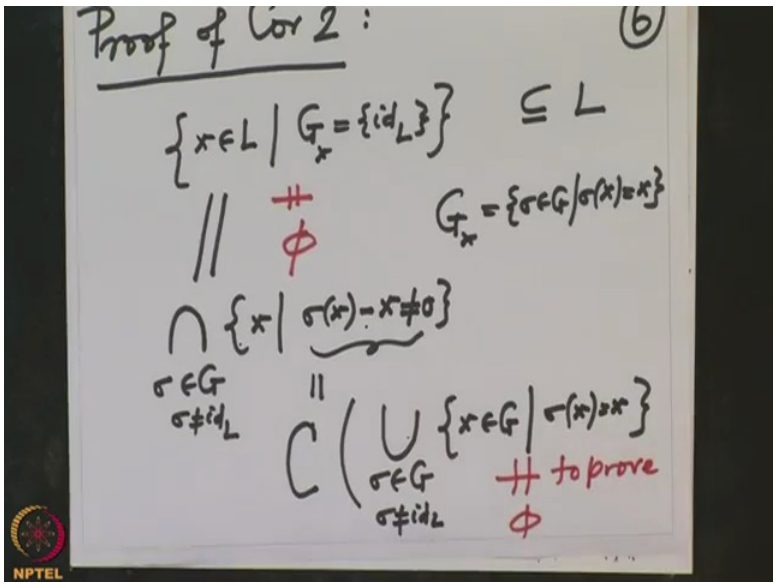


Again I want to remind you what I am going to use in the proof, we will use the following things again from linear algebra, so let V be a finite dimensional K vector space where K is now let us assume infinite field. Actually it is not really fully needed to assume K is infinite, what is needed is? Let me see what is needed is… I am assuming it is a finite dimensional vector space, so let us assume at the dimensions of V over K is n then I will need to assume that this field K has cardinality bigger than n that is enough but assume it is infinite, if one wants to do it little bit more okay then what I want to say.

If you have a finite dimensional vector space over infinite field and let W_1 to W_m be proper subspaces of V that means no W_i is V, so that is W_i is properly contained in V for all i. Then the union $W_1 \cup ... \cup W_m$ this is a proper subset of V. This union may not be a subspace so I can only say it is a proper subset, so that means I can find an element in V which is not in the union and I will simply tell you the proof of this pictorially and I assume that you know this proof from linear algebra but the idea is the following.

If suppose let us take K equal to $\mathbb{R}$ so that I can draw the picture, so I have 2 dimensional vector space that is V is $\mathbb{R}^2$ the real plane this is my vector space and now what other proper subspaces? They are precisely the lines passing through the origin and if I take finitely many lines I still have element outside the union namely this. The finitely many lines will never cover the whole plane that is the proof of this and it is very easy, so I will assume that you know this and resume to the proof of corollary 2, I am looking for x so that the isotropy is trivial.

(Refer Slide Time: 16:01)



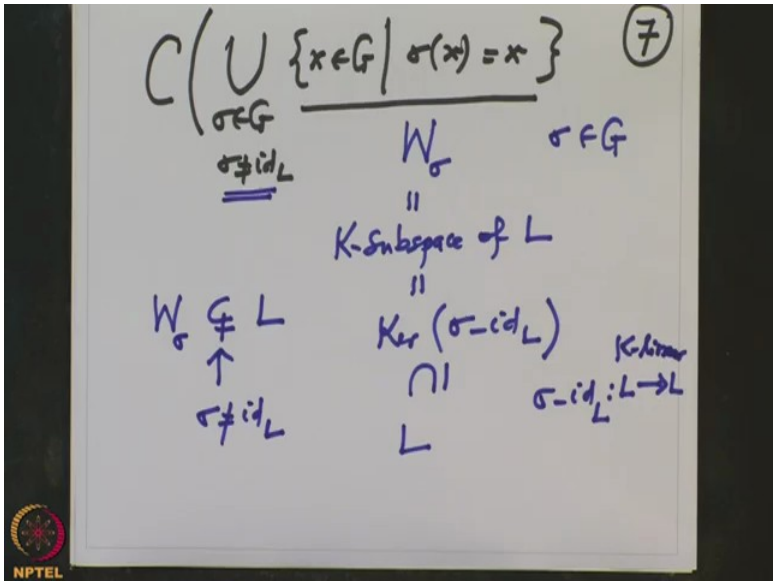
So proof of corollary 2 so what am I looking for? I am looking for element x in L such that the isotropy at x is trivial this is what I want to prove, so I am looking at this subset. This is a subset of L and what do I want to prove? I want to prove that this subset is nonempty, this is what I will prove, this is need to be proved. Once I prove this, what does that mean? There is some element x whose isotropy is trivial and that is what we wanted, so I want to prove this is nonempty set, alright. So what should I prove? Okay so I will prove that the complement… So what is this set first of all let us describe what is this set?

This set is what, that means no σ should fix… There should be σ … Isotropy trivial means what? Let us write down the definition of isotropic. This is all the σ in G such th $\sigma(x)$ at is x. Alright, so I should prove that if I take the intersection, let us look at the intersection of…this intersection is running over $\sigma \in G$ and $\sigma \neq id$. Okay and all those x such that $\sigma(x)$ is $-x$ is not 0. This means what? This precisely means $\sigma(x)$ is not x that means this X is not fixed by σ and if I take intersection that means this x is not fixed by σ , right? That means it is fixed only by identity and that will mean that for this x Gx is identity, so these 2 sets are equal. Is that clear?

Now what is the advantage? The advantage is the following, okay before I go on we want to prove this set is nonempty, if I want to prove this set is nonempty I will prove that the complement of this set is… If I want to prove this set is nonempty what do I have to prove? Complement…so if I want to take the complement of this that will become union and then the complement, so this is complement of whom? Let me write down then it will be clear this is same thing as complement, so c is for complement of the union, its intersection is becoming union, union is over $\sigma \in G$, σ not equal to id_L and this complement of this is what?

All those elements $x \in G$ such that $\sigma(x) = x$, this is a complement and I want to prove this complement is nonempty because I have wrote this equal to this equal to this because if I take complement of the union, the union will become intersection and the complement condition is not equal, so therefore we need to prove that this is nonempty, so I will prove this is nonempty. So this is nonempty, this is what we will prove. Alright, now what is the advantage? Advantage is the following, so that means what I have to check, what is this subset? So now what is the last subset? It is the complement of whom? Complement of this G is the finite union, G is the Galois group of a Galois extension.

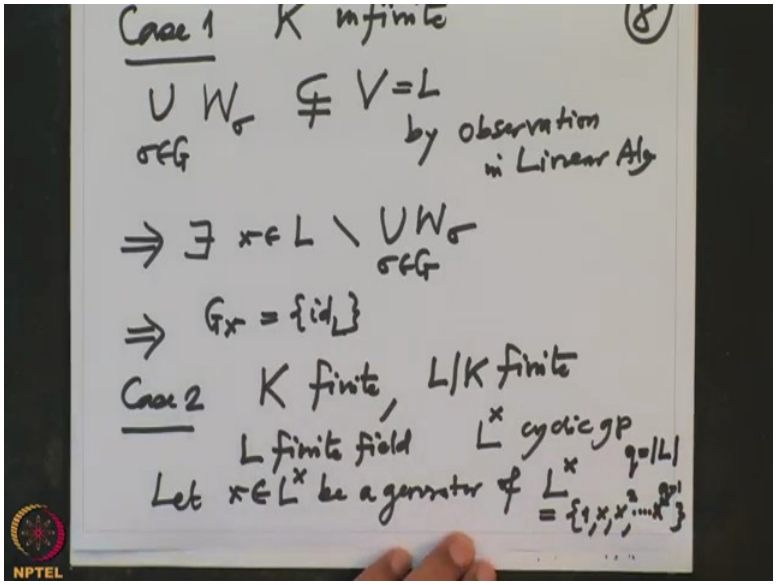
(Refer Slide Time: 21:03)



So let me write the last one I want to prove this once again I will write on this page, so complement of union $\sigma \in G$, σ not equal to id_L and all those $x \in G$ such that $\sigma(x)$ equal to x. Now let us give this guy a name, I want to give the name to be… It depends only on σ , all those relevant which fix a σ let us give name W_σ , so W_σ , σ is in G, G is a finite group and W_σ is clearly subspace, so this is K subspace of L in fact it is a kernel of σ minus id_L .

σ is a linear map, σ is an algebra automorphism there in particular it is a linear map id is a linear map the difference is also linear map, so it makes sense to talk about kernel of this σ minus id_L is a linear map from L to L, K linear map and therefore it makes sense to talk about the kernel and kernel this is a subspace of L, so there are so many subspaces and σ is not identity, we are taking σ not identity, so this W_σ is definitely not whole L this is because σ is not identity because if σ is… When will this be equal? It means $\sigma(x)$ equal to x for all x but that will mean σ is identity but σ is not identity therefore these are finitely many subspaces of this vector space and now I want to divide proof in 2 parts when the base field is infinite or base field is finite.

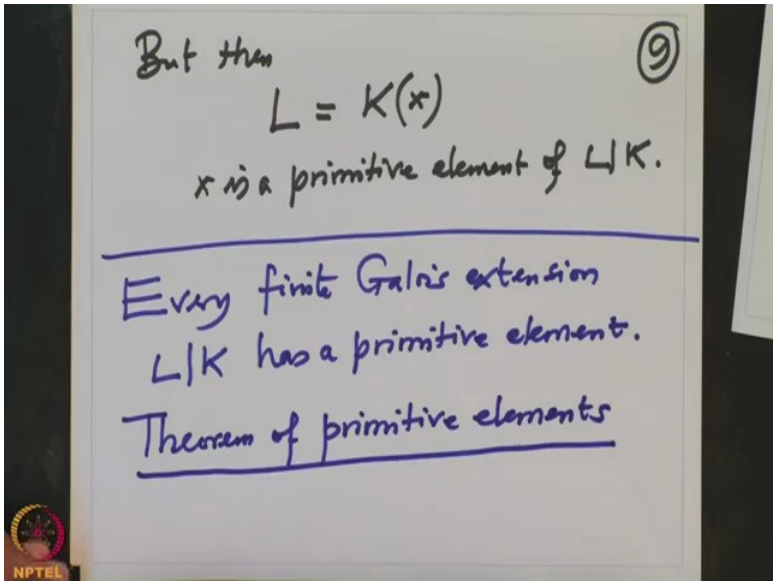
(Refer Slide Time: 23:08)



So case 1 K is infinite then what we know? We know that if I take this union W_σ , σ varies in G this is also proper subset of this. V is L this is by observation in linear algebra but that will mean that I can choose an element x here which is not here so therefore there exist x in L which is not in the union of W_σ but by definition the isotropy at x will be identity only, so that proves case 2, case 2 is even more simpler.

I do not have to use all the above arguments, so K is finite and L over K is also finite therefore L is also finite for you and not only that then I know that this L^x is cycling group because it is a multiplicative group of a finite field and therefore the generator, so let $x \in L^x$ be a generator of L^x . What does that mean? It means every element of L is a power of x, so this means this L^x is precisely identity that is 1, x, x^2 and can go on long because L is a finite field, so it will go onto x^{q-1} where q is the cardinality of L but then this L is a primitive element.

(Refer Slide Time: 25:53)



But then L will be equal to K at join x because this already contain all the powers of x therefore these are equal, so therefore x is a primitive element of L over K, so in both the cases we have proved that every finite extension which is Galois has a primitive element, so therefore I will write once more it is very important observation what we have proved is every finite Galois tension is over K has a primitive element. There may be many primitive elements and may not be one like a cyclic group can have more than one generator. This theorem is called theorem of primitive elements. This was one of the main duration of Galois when he created the Galois Theory.

So because of that so therefore what we have completed our definition of Galois extension that shows that Galois extension has a primitive element and once you know it has a primitive element. Now the problem is how do you find the primitive element because once you find a primitive element then we know how to calculate the Galois group because Galois group will precisely map primitive element to the other root of the minimal polynomial of that primitive element, so it is very important if one wants to do algorithms one wants to write computer algorithms to find primitive element it is very important to know how… What is the recipe?

So it is most of the time not very easy to find a primitive element and how do you find a primitive element that the best way is the proof I gave that means we have a finite dimensional vector space, we have finitely many proper subspaces and from that we have to choose an element outside that, so actually this is very good algorithm because all you have to find is those subspaces and find an element outside their union, so we will continue in the next time. Next time…so far we have only defined Galois extension in the case where the

field extension is finite. Now earlier also I (())(29:03) if your field extension is not finding it then one would like to have alternative definitions.

In other words even for finite extension I want to find equivalent definitions or equivalent conditions so that the field extension is Galois. We have only our definition of Galois extension is only a numerical definition, it only says that Galois group and degree of the field extension these 2 numbers are equal, so now one definition we will have a using the group action and the other definition which is used in most of the text books that is normal separable that will also be another definition.

In addition to this I want to also define Galois extension in case when the field extension is not algebraic also or even algebraic but not finite and eventually I would like to have a definition where the field extension is not even algebraic because remember that we have defined the Galois group even when the field extension is not algebraic because we are only saying that look at the K algebra automorphism is one of the bigger field and this definition does not require algebraic, okay. Thank you.