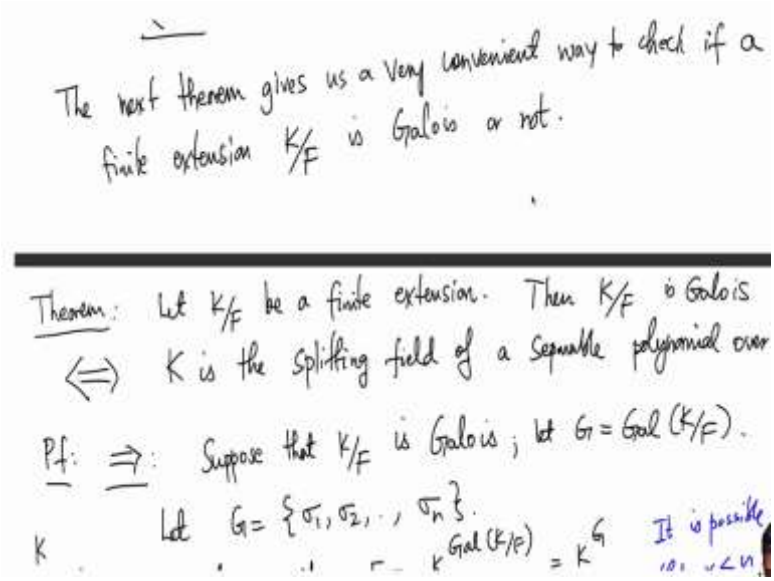
Introduction to Galois Theory
Professor Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute
Lecture – 23
Motivating the main theorem of Galois Theory

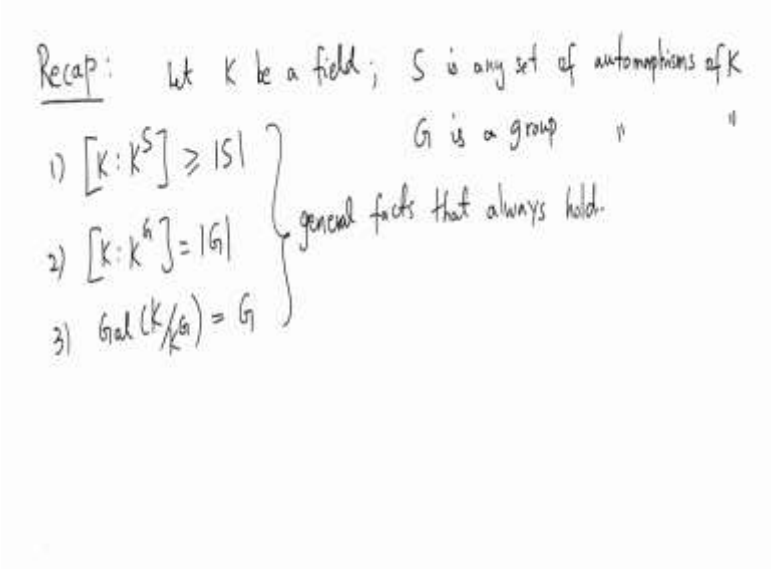
Welcome back, in the last video we proved important characterization of finite extensions to be Galois.

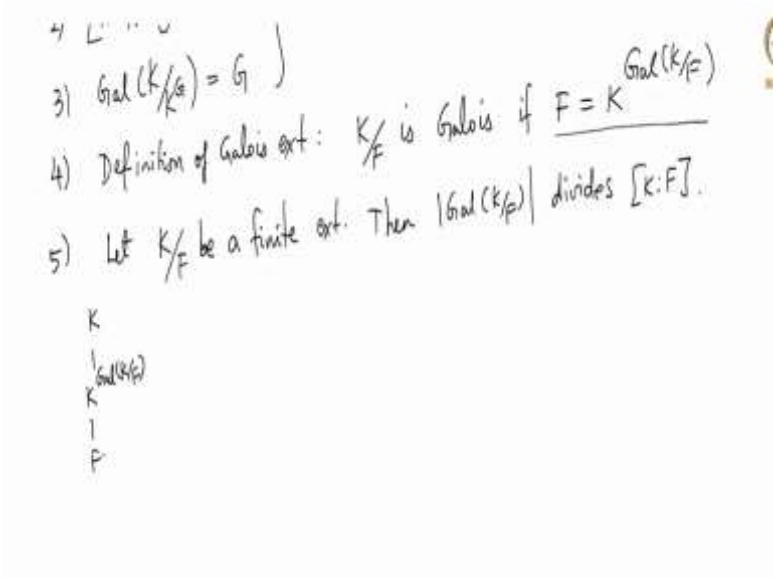
(Refer Slide Time: 0:28)

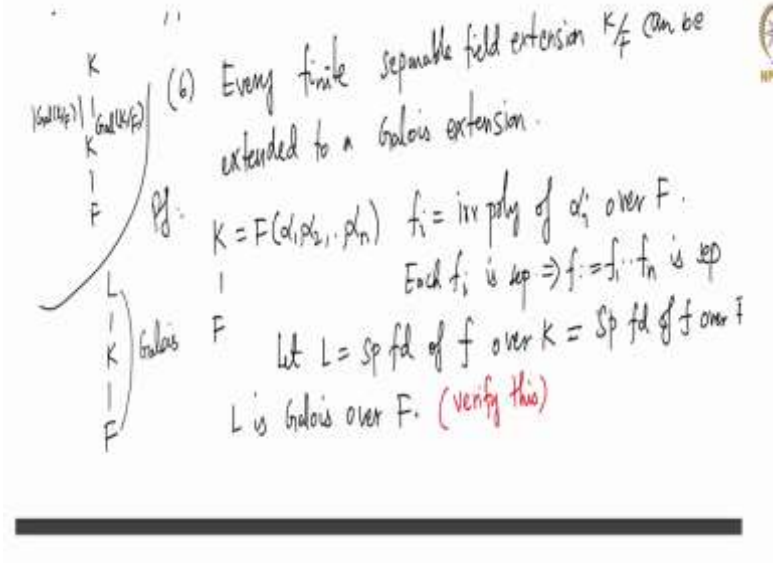


So, let me just recall the statement here, so we showed that a finite extension is Galois if and only if it is the splitting field of separable polynomial over the base field F.

(Refer Slide Time: 0:44)







So, today we are going to start discussing towards the main theorem of Galois theory but I thought it is a good time to quickly recap some important things we have learned in the course, sort of a revision or recap. So, I want to write this down so that it is clear to you and I have done that over the last few videos. So, I want to recall few things, so let K be a field, this is something that I have written in the past.

And S is any set of automorphisms of K and G is a group of automorphisms of K. So, S denotes the set, G denotes the group. Some other things which we have done, so these are all done and you can look at the appropriate videos here, so the degree of the field extension K over K is at least the cardinality of S, but if you take the group, you get exactly the cardinality of the group, the order of the group.

And we also showed the Galois group of K over K, G is precisely G. And these are general facts that always holds. So, there is no further assumption about the field K, the far last statement that I want to recall in this situation is the definition of Galois extensions. So, K over F is Galois, so I want to write further things here today, but let me recall the definition, if F is K power Galois K over F, correct?

So, this is the definition of Galois extensions. An extensions is Galois if this happens. So, in general we know that the fixed field is an intermediate field between K and F. It certainly contains, because these are all F automorphisms of K, but if it is equal to F, we say that it is Galois extension. So, some other things, these are so far, this was done earlier and I recall these as it is. But now I am going to recall some other facts or observations.

These are not exquisitely mentioned before, but I want to list them here because it is a good way to list the important things that we are going to require later on. So, let K over F be a finite extension. Then, the order of the Galois group divides the degree of the field extension. In particular, the order of the Galois group is less than or equal to the degree of a field extension. And this is a triviality because you have K, K power Galois K over F and over F, so this is always an extension and this degree is exactly the order of Galois K over F.

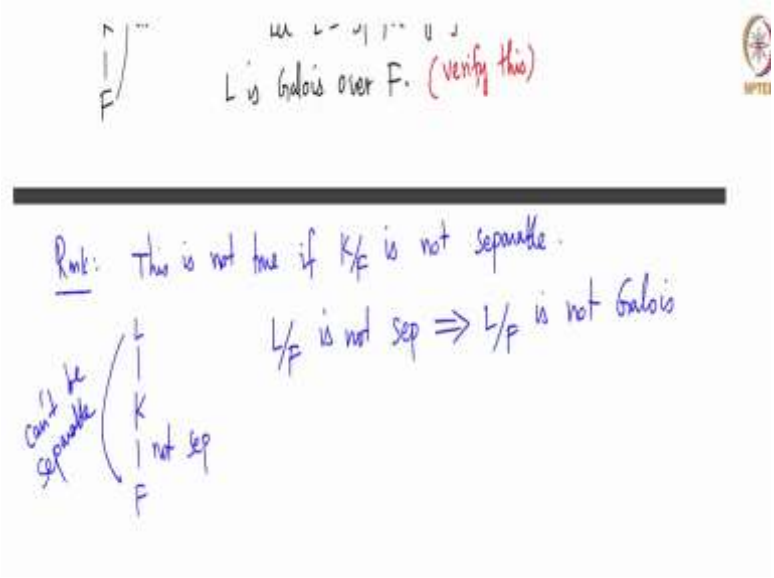
So, this is equal to this, the degree is equal to this so because of the multiplicative property of the field extensions, this divides the degree of K over F, because degree of F is K colon K power Galois K over F times K power Galois K over F colon F. So, this is a triviality. So, the sixth statement that I want to write is that, every finite separable field extension K over F can be extended to a Galois extension.

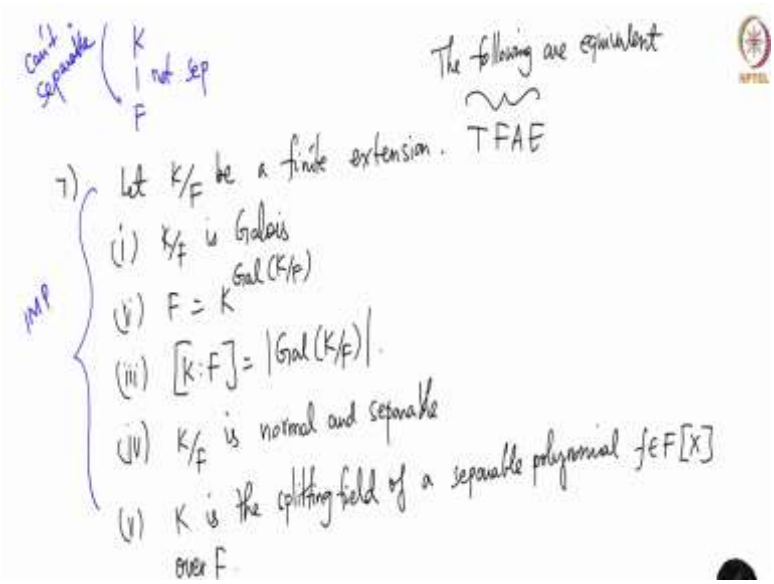
So, I am calling this recap, but technically it is really not a recap. But I just want to explain why this is the case. So, let us say K over F is a given Galois extension, so K can be written as alpha 1, alpha 2… sorry given separable extension. It is a finite separable extension so express like this. So, we can always choose like this, and let us say, Fi is the splitting, irreducible polynomial of alpha i over F.

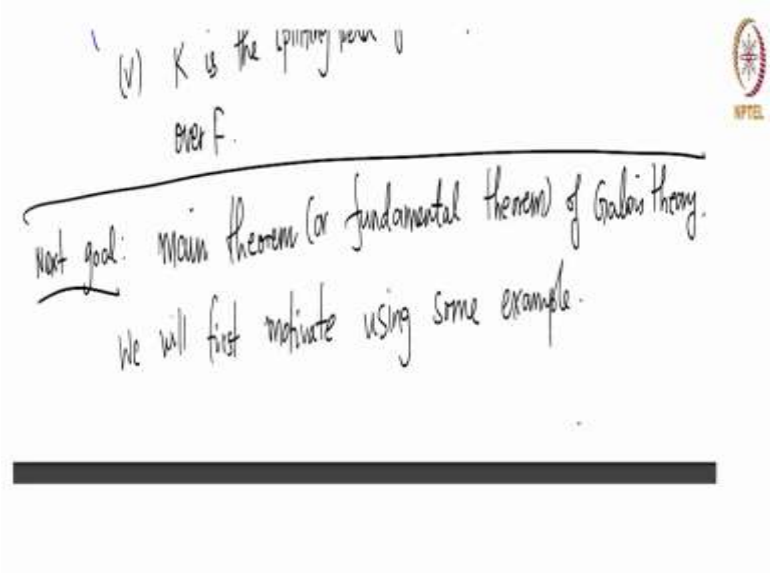
So, each Fi is separable by hypothesis, right? Because K over F is a separable extension, each Fi is separable; this implies F which is defined to be F1 to Fn is also separable because, irreducible factorization of F is this, F1, F2, Fn. And each of them is separable so F is separable. Now let L be the splitting field of F over K. So, what we have is, so L sits above K and you have given extension here. So, I claim that L is Galois over F.

So, this is what I mean by this. You can always extend the given extension to make this Galois; this is because L over K is… so the verification of this, I will leave it for you. You can do this in number of ways but the point is L is the splitting field of F over F also… Splitting field of F over F also because F is a polynomial in Capital FX, it is a separable polynomial and it is generated by the roots, so L is Galois over F. Or you can argue that it is normal and separable. So, this is a useful property for us, every finite extension given finite separable extension can be embedded in Galois extension of the base field.

(Refer Slide Time: 6:59)







I will remark here that, this is not true if K over F is not separable because if K over F is not separable, you put any field here, this cannot be separable. Because we argued already in the videos when we discussed separable extensions that is L over F is separable L over K and K over F are separable. So, if L over F is separable K over F will be separable but K over F is given to be not separable.

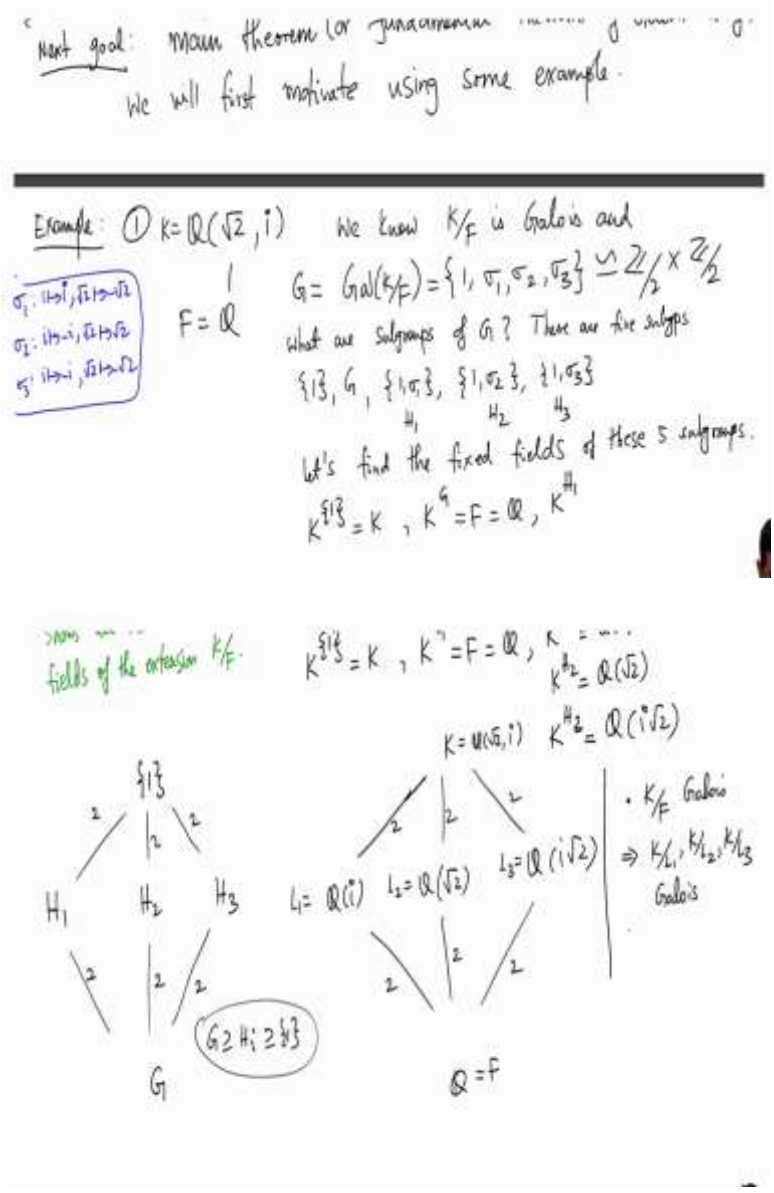
So, L over F cannot be separable and hence of L over F is not separable, implies L over F is not Galois because the Galois extension is separable, so if it is not a separable extension it cannot be Galois. So, if you are given a non-separable extension, you cannot extend it and make it a Galois extension. Finally let me summarize all the equivalent conditions for a Galois extension. So, let K over F be a finite extension, the following are equivalent, t, f, k, e always stands for the following or equivalent.

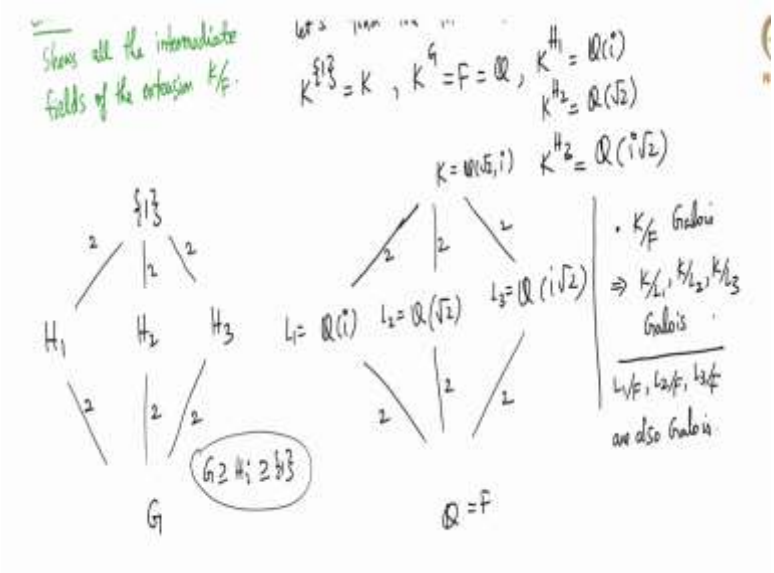
The first statement I want to make is, K over F is Galois, this is our first statement, and second statement is F is K power Galois K over F. Of course, 1 and 2 is just the definition but I wanted to nevertheless write this because it is a good way to keep track of all the equivalent conditions for been Galois. So, 3 is something we have discussed also, 3 colon F is out of the Galois group, this is same as been Galois. 4 K over F is normal and separable.

Again, we have shown that, it is same as been Galois and finally 5, K is the splitting field of a separable polynomial overhead. SO k is a splitting field of a separable polynomial over the base field, so this is just a convenient way of remembering all the equivalent condition of a Galois extensions. So, this is something that I wanted to write so that you have this slide in front of you and you can often refer to this.

So, this 2 slides so far are the 7 facts that I wanted to record, many of them are recaps so essentially trivial extensions of what we have learned. So, only 6 is really new for you. 5 and 6 are explicitly mentioned for the first time, so these are the 7 facts that I wanted to highlight for you before we proceed. So, the next goal, as I said, is to prove the main theorem of Galois Theory, also called the fundamental theorem sometimes. So, before we state and prove, it is fairly a simple proof actually, whoever it is, it is important starting point for the study of Galois Theory. So, the main theory, I should not theorem, not theory, it is a specific theorem.

(Refer Slide Time: 11:22)





So we will first motivate using some examples, so I want to give 2 examples to describe the, 2 or 3 examples to give you a flavour of what the main theorem does. So, the first example something which we have discussed in detail before but I want to quickly discuss this, K over F is Galois so we already know K over F is Galois. So, what is… let us analysis this, what is a Galois group?

We already know that, and the Galois group, K over F is... I have denoted this by this, this of course we know also for abstractly this is the client for group which is equivalent to, which is isomorphic to Z not 2 cross Z not 2. And I wanted to, Galois's main theorem connects the intermediate fields of the Galois extensions in the sub-groups of Galois group. So, what are the sub-groups, so here, let us call this G for convenience so I wanted to do this in the slide so the entire picture is in front of you.

What are the sub-groups of this, so let us start with this, what are the sub-groups of.. so G is the group of order for, it has 5 sub-groups really. So, there are 5, there are 5 sub-groups, what are they? Of course we have 1 and G, the trivial group and the full group and then we also have 1 comma, sigma 1, 1 comma sigma 2, and 1 comma sigma 3. We have h1, h2, h3. So, the 3 fields, the sub-groups will be something like this, so I have G, and 1 here. And all the other 3 are basically… maybe I will write this down after sometime.

So, these are the 5 sub-groups, you have trivial group, full group, h1, h2, h3. I want to find out what are the fixed fields of this groups, so find the fixed fields? So, let us find the, of these 5 sub-groups. So, I have already alluded to this in the previous video, if you have a group containing another, there will be an opposite inclusion of fixed fields. So, what is the

fixed fields of 1. So, these are the things which are fixed by 1, so that is exactly K, what is the fixed field of G, because it is a Galois extension, this is F.

What is the fixed field of h1. Now I wanted to recall what sigma 1 does, maybe I will write it here, sigma 1, it does not really matter whether you change this, but I wanted to be precise, so sigma 1 sends y to i minus root 2 to minus root 2, sigma 2 sends i to minus i, root 2 to root 2, sigma 3 sends i to minus i and root 2 to minus root 2. So, the first 2 things are not interesting, the fixed field of the trivial group is K, the fixed field of the full group is F.

What is the fixed field of H1, if you think about it, i is fixed here, right? So, i is fixed so it must be Qi, this is something that we have discussed at length in the past because it is the degree to extension contains i so it must be i, similarly fixed field of h2 must be Q root 2 and fixed field of H3 must be i root 2. And now I want to draw the tree, groups are one side and fields are another side. So, you have G, and 1 and you have h1, h2, h3.

Let us denote this, so this bar here represents, the fact that the bottom one contains the above one. This is the opposite of, this is the reverse of the field situation, what is the fixed field of G, we agreed that the fixed field of G is Q and the fixed field of 1 is K. And then you have the Q root 2 are Qi, just to be Q root 2, Qi root 2. So, we have these 2 equations. Here the bar represents, the top one contains the bottom one, the group level, the bar represents the bottom one contains the top one, so G contains Hi and Hi are in 1. So, that is the convention.

So, now the question that I want to ask is, the sub-group tree is completely written now because there are no other sub groups, is it just the group out of 4 and it is very clear that, these are all the sub groups there cannot be another sub-group. But what about, the intermediate field tree, it is conceivable that there are other intermediate fields, so now this what I want to address when we do the main theorem, the claim that we want to make is, that the tree below shows all intermediate fields of the extension.

So, that means, there are exactly 5 intermediate fields of K over F, K and F themselves and this 3 proper intermediate fields. And the reason for that, and we formally prove this in the main theorem is that, every time you take an intermediate field, there is a mysterious field outside these, you can take the Galois group of that and that will give you the sub group. So, the first statement of the group is there is a bijection between the sub-group of the Galois group and the intermediate fields of the extension.

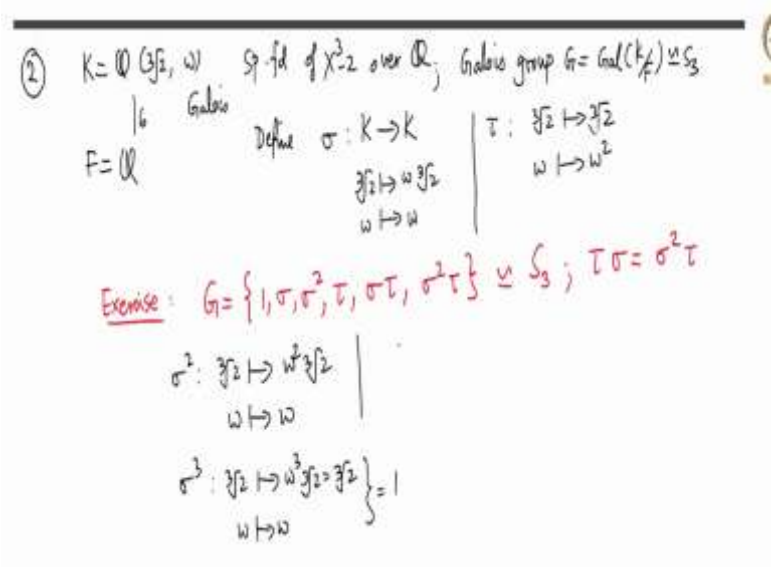
So, I do not want to do this in detail because will prove this anyway. But the point is there are no other intermediate fields and orally I will simply say it again, that if there is any intermediate field, you can take it to the Galois group of K over that intermediate field and that must fit into this. So, it must be one of these but then, if it is one of these, that intermediate field must also be one of these.

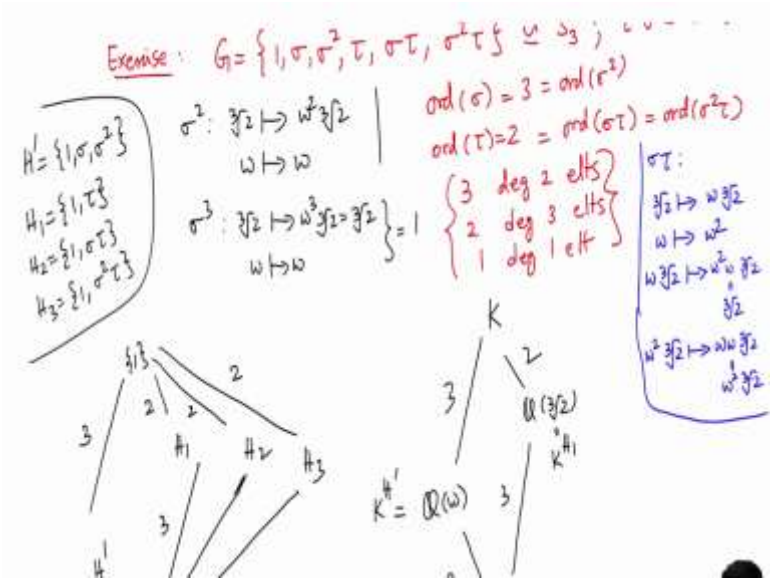
So, this is the reason for, the fact that these are all the intermediate fields. And now I will also emphasis another fact here, K over F is Galois is given so this implies, K over, let is call this F1, not F1, L1, L2, L3. So, K over L1, K over L2, K over L3 are all Galois. This is just a feature of Galois extensions. You have a Galois extension, the top one is Galois over any intermediate field, so these are Galois.

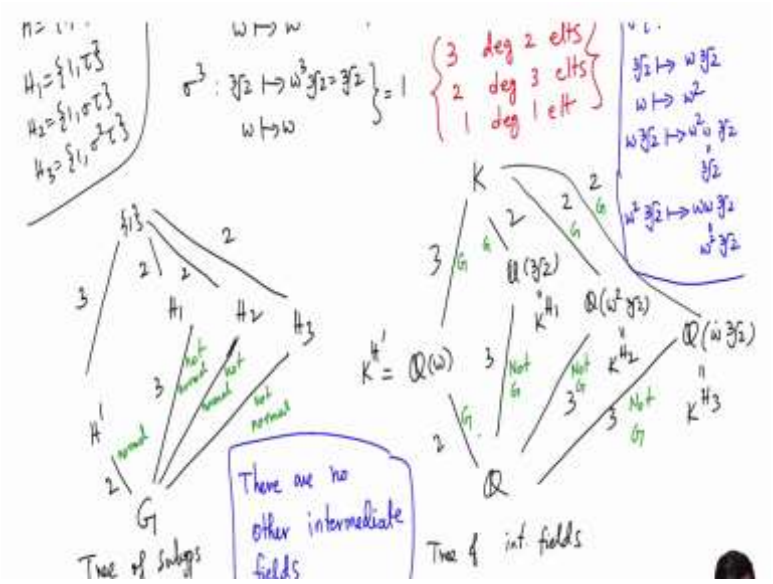
So, let me now write those but let me write the degrees here, this is degree 2, this is degree 2, this is degree 2, this is degree 2, this is degree 2, this is degree 2. And here I am going to write the index of this, what is the index of this? This is 2, this is 2, this is 2. Every number here is 2, we will see in a minute, why these are important. But what about, L1 over F, in fact, L1 over F, L2 over F and L3 over F are also Galois.

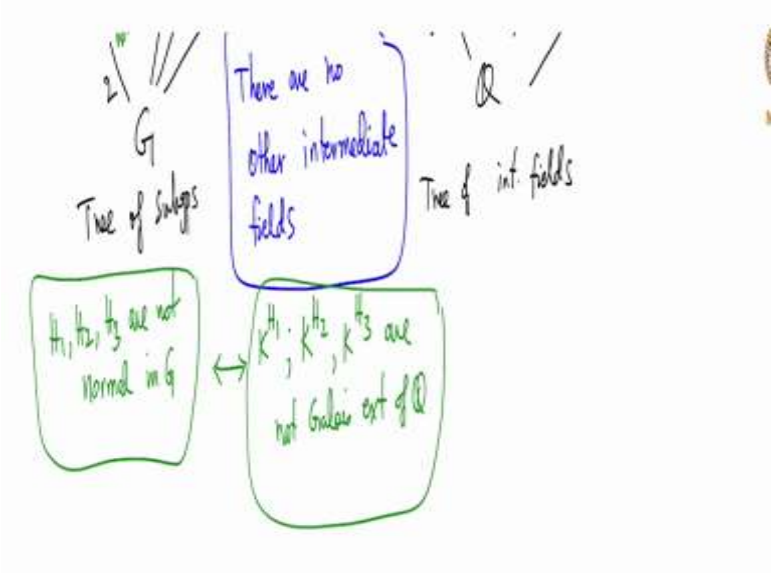
These are not in general true, right? We know that, this bottom part is not in general true, but in this case they are also Galois. So, this is the first example.

(Refer Slide Time: 20:16)




Exercise: $G_1 = \{1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\} \cong S_3$
$H' = \{1, \sigma, \sigma^2\}$
$H_1 = \{1, \tau\}$
$H_2 = \{1, \sigma\tau\}$
$H_3 = \{1, \sigma^2\tau\}$
$\sigma^2 : \sqrt[3]{2} \mapsto \omega^2\sqrt[3]{2}$, $\omega \mapsto \omega$
$\sigma^3 : \sqrt[3]{2} \mapsto \omega^3\sqrt[3]{2} = \sqrt[3]{2}$, $\omega \mapsto \omega$ } $= 1$
$\mathrm{ord}(\sigma) = 3 = \mathrm{ord}(\sigma^2)$
$\mathrm{ord}(\tau) = 2 = \mathrm{ord}(\sigma\tau) = \mathrm{ord}(\sigma^2\tau)$
3 deg 2 elts
2 deg 3 elts
1 deg 1 elt
$\sigma\tau$:
$\sqrt[3]{2} \mapsto \omega\sqrt[3]{2}$
$\omega \mapsto \omega^2$
$\omega\sqrt[3]{2} \mapsto \omega^2\omega\sqrt[3]{2}$
$\sqrt[3]{2}$
$\omega^2\sqrt[3]{2} \mapsto \omega\omega\sqrt[3]{2}$
$\omega^2\sqrt[3]{2}$
K
$\mathbb{Q}(\sqrt[3]{2})$
K^{H_1}
$K^{H'} = \mathbb{Q}(\omega)$
$\mathbb{Q}$
G_1
H'
H_1
H_2
H_3


$H_1 = \{1, \tau\}$
$H_2 = \{1, \sigma\tau\}$
$H_3 = \{1, \sigma^2\tau\}$
$\sigma^3 : \sqrt[3]{2} \mapsto \omega^3\sqrt[3]{2} = \sqrt[3]{2}$, $\omega \mapsto \omega$ } $= 1$
3 deg 2 elts
2 deg 3 elts
1 deg 1 elt
$\sqrt[3]{2} \mapsto \omega\sqrt[3]{2}$
$\omega \mapsto \omega^2$
$\omega\sqrt[3]{2} \mapsto \omega^2\omega\sqrt[3]{2}$
$\sqrt[3]{2}$
$\omega^2\sqrt[3]{2} \mapsto \omega\omega\sqrt[3]{2}$
$\omega^2\sqrt[3]{2}$
K
$\mathbb{Q}(\sqrt[3]{2})$
$\mathbb{Q}(\omega^2\sqrt[3]{2})$
$\mathbb{Q}(\omega\sqrt[3]{2})$
K^{H_1}
K^{H_2}
K^{H_3}
$K^{H'} = \mathbb{Q}(\omega)$
$\mathbb{Q}$
G_1
H'
H_1
H_2
H_3
Not normal
Not G_1
Tree of subgps
There are no other intermediate fields
Tree of int. fields


G_1
Tree of subgps
There are no other intermediate fields
$\mathbb{Q}$
Tree of int. fields
H_1, H_2, H_3 are not normal in G_1
$\leftrightarrow$
$K^{H_1}, K^{H_2}, K^{H_3}$ are not Galois ext of $\mathbb{Q}$

Let me do another example to illustrate again some features of this. So, here I will take Q adjoin, cube root of 2 comma omega over Q. So, this is a degree 6 extension. And this is a Galois extension because this is the splitting field of X cubed minus 2 over Q. So, here and we also know that the Galois group G is isomorphic to S3, and without maybe proving this carefully, I did say it in some point and now I will just give you exactly what the generators are.

So, here define sigma from K to K, remember K is generated over Q by cube root of 2 and omega so to determine an automorphisms of K, all you need to do is tell where the image of cube root of Q and what the image of omega is. Cube root of 2 can go to either cube root of 2, cube root 2 omega or cube root of 2 omega square. Omega has to go to either omega or omega square. So, let us say, cube root of 2 omega cube root of 2 and omega 2, let us define tau, to be cube root of 2 goes to cube root of 2 and omega goes to omega square.

So, then I will let this… leave this as an exercise for you… I may say few things and then I will move on. G is exactly equal to 1 sigma, sigma square tau, sigma tau, sigma square tau. And it is isomorphic to S3. So, the… and the relation is the following, the tau sigma is sigma square tau. So, you verify this, these are just direct calculations.

For example, what would be sigma square, sigma square sends, you can see cube root of 2, first we will go to cube root of 2 times omega, then you send omega to omega cube root of 2, 2 omega cube root of 2 that is omega square cube root of 2, omega will go to omega. So, this is the new element whereas sigma cube will send cube root of 2 so now you will apply sigma again to this.

Omega square will go to omega square but cube root of omega go to cube root of square. So this is omega cubed cube root of 2 which is cube root of 2, omega will be omega. So, this is equal to 1. So, sigma is an order 3 element, tau square is of course is identity because cube root of 2 is anyway effects, omega goes to omega square, omega square will go to omega square square which is omega 4, this is identity and so on. So, I want maybe to check other things but this is left it to you.

So, in fact, what you can show is that, order of sigma is 3, order of tau is 2, in fact, order of sigma square is also 2, 3 and order of sigma tau equals order of sigma square tau. These are degree 3 elements, so there are 3, so there is 3 degree 2 elements and 2 degree 3 elements and 1 degree 1 element. So, this is the nature of the group G, so this is the well-known group to

us, symmetric group. So, now for each of this sub-groups, I want to write the, on the fly I will write down the, the fixed fields.

So, we have G, of course we have… let me just give some names to this, it will be easier. So, I call H prime to be the order 3 sub-group, H1 to be 1 comma tau, there will be 3 order 2 sub-groups corresponding to 3 degree to a limit. H2 will be 1 sigma tau, and H3 will be 1 sigma square tau. So, apart from the trivial group and the full group, these are the 4 proper sub-groups. So, these are the 6 sub-groups are going to be there.

So, G and I am going to write, index 3 here, sorry index 2 thing here. H prime is index 2 and index 2 things will be here, index 3 things will be here. And they are all of course going to contain the trivial group. And here index is 3, because this is order 3, this index is 2. Now what are the… this is the tree of sub-groups. And what is the tree of sub fields, intermediate fields. So, of course we have Q and we have K, so those are the corresponding sub fixed fields. G has fixed field Q because it is a Galois extension, 1 has fixed field K.

Now what is the fixed field of H prime, it must be… because H prime is an order 3 group, it must be field such that degree of K over that is degree 3. So, if you look at the sigma, what is fixed under sigma, sigma is going to fix omega, similarly sigma square will also fix omega. So, if you take Q omega, this is going to be degree 2 extension of Q and it will be degree 3 extension of… so Q omega is containing K power H prime.

And K power H prime is a degree 2 extension of Q so Q omega is also degree 2 extension of Q, so this must be that. So, this is K H prime. What is K H1? What is tau fix? Tau fix is cube root of 2 so cube root of 2 is here that is the degree 2 extension and this is the degree 3 extension. So, this is equal to K power H1, now what is K power H2? What is sigma tau? Now I am going to write down sigma tau because it will be useful to write down the fixed field. So, just write down what is sigma tau.

Sigma tau, where does it send omega.. cube root of 2, 2. First see that tau sends cube root of 2, 2 cube root of 2 and sigma sends cube root of 2, 2 omega cube root of 2. And where does omega go under this? So, omega goes under tau to omega square and sigma will go to omega square. Now it does not look like, it fixes anything, right? But where does omega cube root of 2 go? Omega cube root of 2 will go to, omega will go to omega square and cube root of 2 will go to omega cube root of 2, so that is cube root of 2.

Even that is not fixed, what happened to omega square cube root of 2? Where does that go? So, that goes to omega, square will go to, omega square whole square, that is omega and cube root of 2 will go to omega cube root of 2, so this is omega square cube root of 2. So, that is a fixed element of H2 but now you can argue that, that will have degree 2 over Q, so I will write it here. Q adjoined omega square cube root of 2.

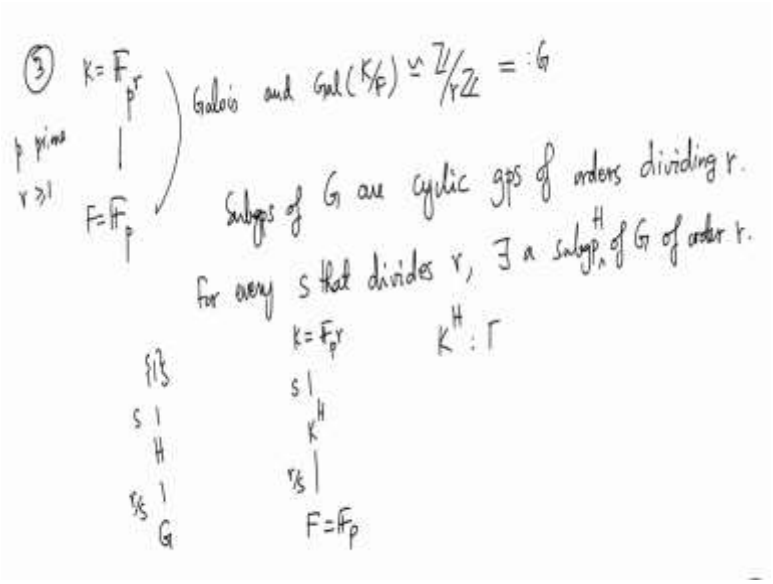
So, that is a degree 2 element, degree 2 extension that is a degree 3 extension.. Sorry this is a degree 3 extension, this is degree 2 and I claim that this is K power H1. So, you can check that because it is fixed, omega square cube root of 3 is fixed by H2. And that is supposed to be degree 3 extension of Q. So, there is a lot of stuff going on here, we are using everything that we have done so far, so finally you have Q adjoined omega cube root of 2 and this is going to be K power H3, this is degree 3.

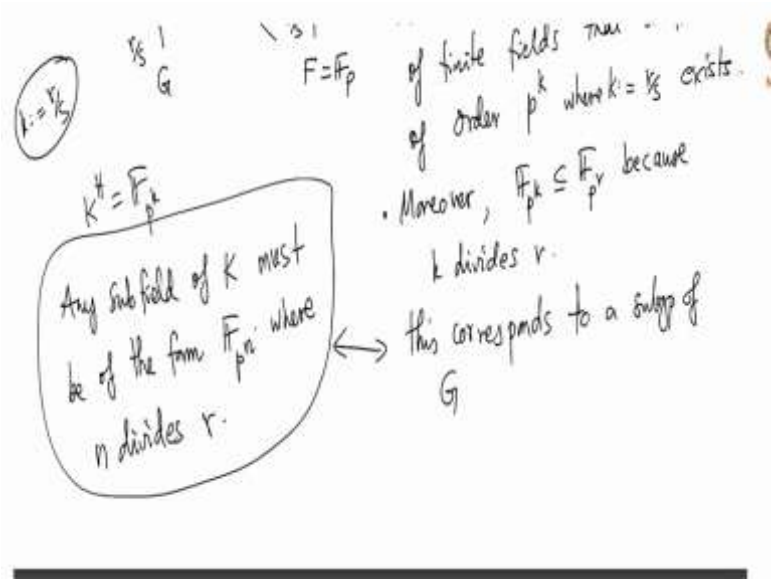
So, this is dual pictures, you have tree of fields and tree of intermediate fields. And again as before, there are no other intermediate fields. This is going to be a consequence of the main theorem. Now, let us notice which of these are Galois, of course this is Galois, so I will write G of that. This is Galois, this is Galois, this is Galois, this is Galois because K over Q is Galois, right? So, K over K is Galois so K over all this intermediates fields is Galois. But the bottom ones in general are not Galois, in this case they happen to Galois.

This is Galois, but what about these? This been a degree 2 extension is Galois, but this is not Galois, that we have seem because the conjugates are not there. Similarly, this is not Galois and this is not Galois. So, I want to now emphasis which property of the group side determines that. So, I claim that, this is a normal sub-group but this is not normal. This is not normal, this is not normal. H1, H2, H3 are not normal in G, so that is equivalent to the fact that K H1, K H2, K H3 are not Galois extensions of K.

So, this is just an observation I am making but we will prove this in the main theorem. So, here of course the Galois group is abelian. So, everything is normal, this is normal, normal, normal. So, these are normal hence these are Galois. Here this is normal so this is Galois, these are not normal so these are not Galois. So, whether the bottom half of the Galois extension, extension is Galois or not is determined by the corresponding sub-groups are normal or not.

(Refer Slide Time: 31:44)





Let me quickly, I want to end this video soon, but I want to give you one more example, but this I will not do in detail, let us take this, P is the prime number as always, r is the positive integer, so this of course is Galois and Galois group is a cyclic group of order 4, order r. So, I want to without drawing the tree, I want to just tell you this, sub-groups of G, let us call this G are cyclic groups of order diving r.

So, basically what I am saying is that, for every S that divides r, are positive integers that exists the sub-group of G of order r. So, let me just… let us call that H, so I want to just highlight what the corresponding picture is going to be. So, G has order r so H is order r that means H has index, 1 has index this in r and this.. Sorry this is not r, this is S and this is r by S. Because index will be r by S.

So, now at the field level, the fixed field of G is F of course because it is a Galois extension. Fixed field of 1 is of course the full field, what is the intermediate field corresponding to this? This extension is going to of degree equal to the cardinality of H so that is exactly H and this is r by S. But what is this field here, so K power H is a field which has index r by S, that means the cardinality of K power H is r by S, p power r by S.

But such a field exists, right? We know that such a field exists and this is the sub-field of, we know already from the structure theorem of finite fields that a field has order that is K which is r by S exists… sorry p power K where K is r by S exists, that of course we know but we also know from the structure theory that K power H, I am claiming is F, p power K. K is again r by S and not only that, moreover F p power K is contained in F p power r because K divides r. So, that is the sub-field.

So, now all sub-fields here will be of the any sub-field of K must be of the form, F p power n where n divides r. So, this is one of the exact statements in the structured theorem of finite fields. So, this exists, let us say this is F p power n, now this corresponds to a sub-group of G. So, I went over very fast, but idea is that because G is the cyclic group of order r, there is a sub-group of every deviser of r.

Similarly, there is a sub-group of every index, any possible index. So, there will be a sub-group of index n whose fixed field will be the field F sub p power n. So, I wanted to introduce another class of fields to illustrate the main theorem, so I did not spend too much time on this, maybe I will come back to this later and talk about this but these 3 examples are supposed to give you an idea of how the group theory of the Galois group, what are the sub-groups, what are the normal sub-groups is supposed to shed light on, what are the intermediates fields of the given extension and which are Galois.

So, let me just end this video with final comment which is that, everything here is Galois, all intermediate fields are Galois extensions of F because any extensions of finite fields is Galois which corresponds to the fact that, G is a abelian. And every sub-group is normal. So, this is akin to the first example where everything is normal. And this is different from the second example, where there are not normal sub-groups corresponding to non-normal, non-Galois extensions.

So, let me stop this video here and now we are ready to state and prove the main theorem of Galois Theory which we will do in the next video, thank you.