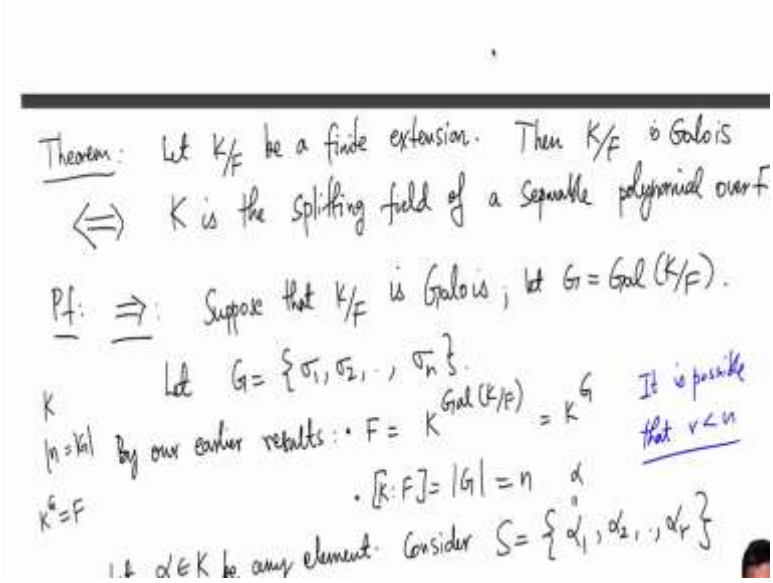
Introduction to Galois Theory
Professor Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute
Lecture – 22
Examples of Galois Extension

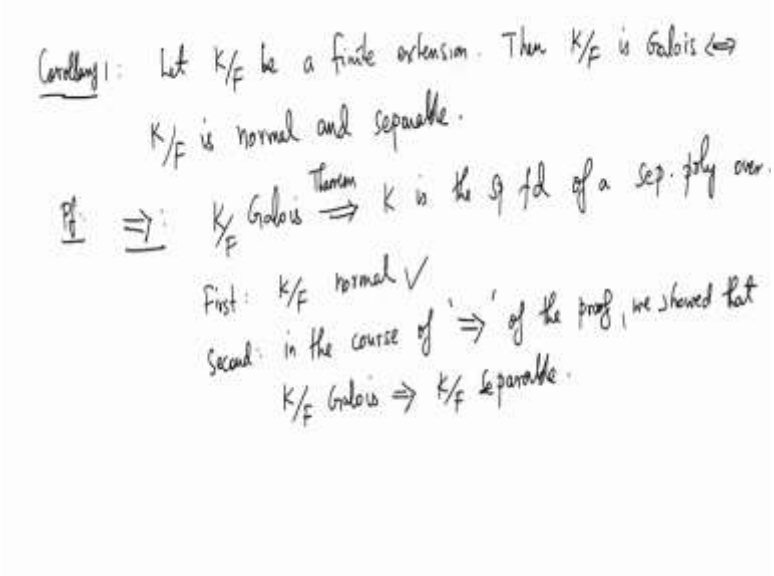
Welcome back, in the last 2 videos we proved an extremely important theorem which characterised Galois extensions. So, let me quickly show that theorem to you.

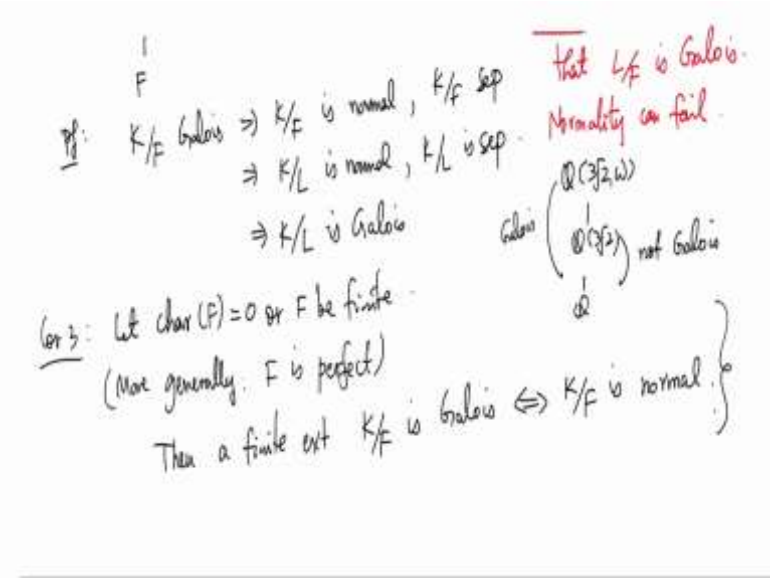
(Refer Slide Time: 0:29)



So, it showed that if you have a finite extension, it is Galois, if and only if it is a splitting field of a separable polynomial.

(Refer Slide Time: 0:40)





So, let me now talk about a couple of important corollaries of this and they are very easy corollaries. And this is in fact, is the most important corollaries for which we prove that theorem. So, 1 is essentially contained in the theorem itself. So, let K over F be a finite extensions so fields then K over F is Galois, this is a different kind of characterisation. Earlier we said, it is Galois, if and only if it is a splitting field of a separable polynomial.

Now we are saying that, K over F is Galois if and only if K over F is normal and separable. So, this is the most common way of stating the pervious preposition, theorem. And in fact, you will see this in any books on Galois Theory. So, let us suppose that K is the splitting field, K Galois, K over F is Galois implies K is the splitting field of a separable polynomial over capital F. So, this is the theorem. So, let me us capital H..

This is the theorem, now this means that first K over F is normal, this is trivial because it is a splitting field of.. Separable or not, it is a splitting field of a polynomial so it is normal. Second, in the course of the proof, in the course of in fact, this forward direction of the proof, and I noted this in fact, at the end of the fact, we showed that K over F Galois implies K over F separable.

So, let me now point out where I did this, but in the beginning of the proof of the previous theorem, we started with alpha in capital K and we in fact, constructed its splitting field… sorry constructed its irreducible polynomial and we showed that it has distant roots. So, it is separable. If it is Galois, then it is normal and separable, the other direction is also clear, so if K over F is normal implies by definition, K is the splitting field of a polynomial, no adjective is added to that polynomial.

Normality simply says, it is a splitting field of a polynomial F over F. Now K over F is normal, separable implies F is separable. Because F is… every irreducible factor is F is a irreducible polynomial of some element of capital K, so F is separable. So, it is splitting field of a separable polynomial, hence is it is normal.. sorry hence it is Galois. So, that proves that a normal separable extension is automatically Galois.

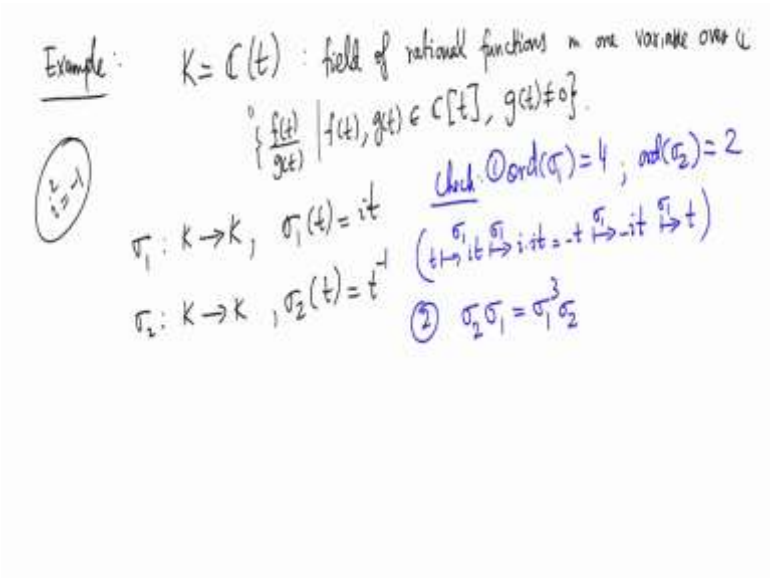
So several corollaries of this, maybe I will call it corollary 1, so corollary 2 is K over L over F are field extensions. K over F is Galois implies K over L is Galois. This is trivial, right? Because K over F is Galois, implies K over F is normal and K over F is separable. But normality and separability is carried to K over L. In fact, separability also follows L over F but normality does not follow L over F, so K over L is normal and K over L is separable so K over L is Galois.

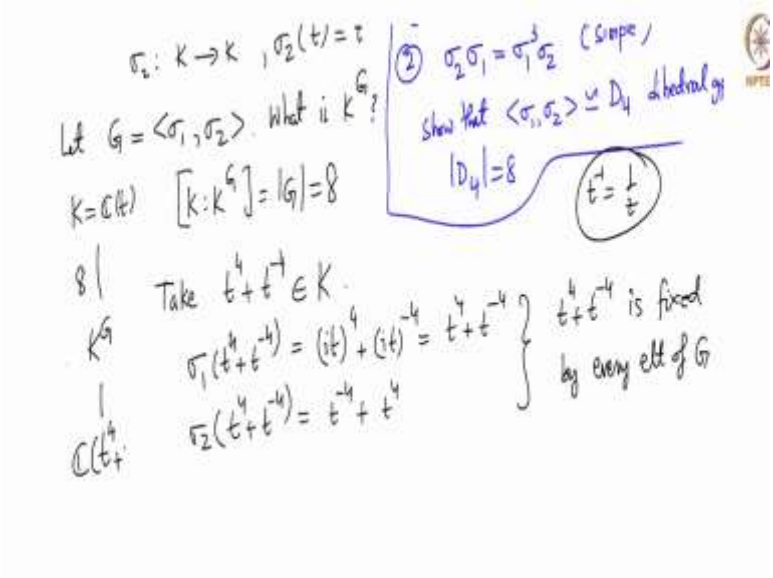
Let me just warn you that, it is not true that L over F is Galois, normality fails not separability. In fact, we saw an example of this, right? You have a degree 4 extension or degree 6 extension which we will discuss later, has intermediate field which is degree 3, Q adjoined cube root of 2 and omega, Q adjoin cube root of 2 Q. So, this is Galois, not Galois. And finally, this is the example where we are going to let characteristic of F be 0 or F is finite, more generally F is perfect.

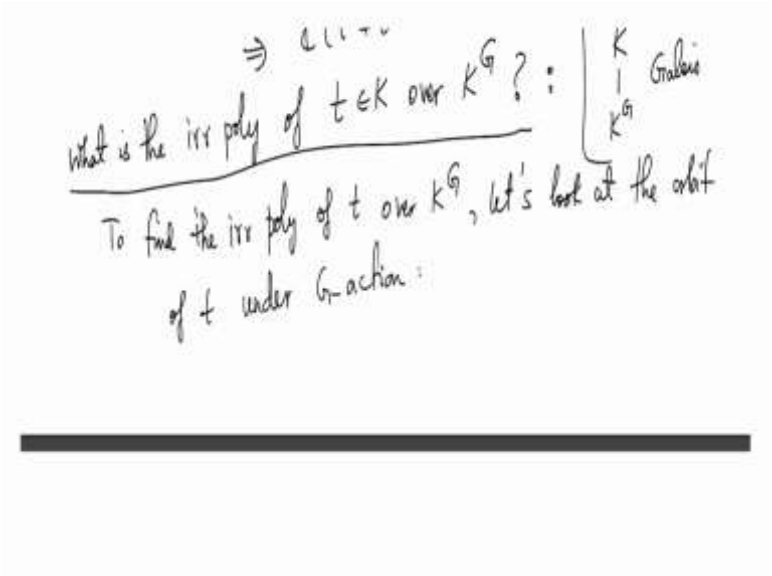
Remember this means that, its characteristic is 0 or every element of F is a Pth power. In characteristic is P and every element is a Pth power. Then the finite extension K over F is Galois if and only if K over F is normal, trivial corollary because we know that Galois if and

only if normal and separable, if the base field is perfect it is automatically separable of Galois is if and only if normal. So, this is…. For example, dealing with only characteristics 0 of its Galois is nothing more than normal. So, that is useful so keep in mind.

(Refer Slide Time: 6:56)







So, let me just quickly do an example that illustrates some of the features of the proof of the previous video. So, let me… these kind of things, we do not typically study in this course but I wanted to do this for your understanding of the process in which we proved the previous theorem. Let us take this to be, K to be CT, so this is the field of rational functions in one variable… remember this means the elements are ratios of rational polynomials.

They are square bracket t and G of course is non-zero. So, we want to look at 2 automorphisms of K, sigma 1 and sigma 2. Sigma 1 sense.. because I want to think of C automorphisms, everything in C is fixed but P goes to i,t, i of course is an imaginary square root of minus 1 so sigma sends C to i, t. Sigma 2 sends t to t inverse. So, t goes to i, t under sigma 1, sigma 2 sends t to t inverse.

So, it is easy to check for you and these are easy exercises that I made it for you. Order of sigma 1 is 4 that means sigma 1 square, sigma 2 square are all different identity. And sigma 1 power 4 is identity. Order of sigma 2 is 2 that is even more easier because t goes t inverse under sigma 2 and t inverse goes to t. Here t goes to i, t under sigma 1 but then i, t goes to, i is constant so i times i, t which is minus t. That is 2 times.

Third time, it will go to minus i, t because minus 1 is constant, t inverse i, t. And finally it goes to minus i times i, t which is t. So, sigma 1 power 4 is identity and none of the smaller powers is identity. So, in fact, the other... I mean this is easy but the main exercise is the group and we need to check that sigma 2, sigma 1 is equal to sigma 1 cube sigma 2. This is a simple calculation. You just see where t goes under both direction, both maps and show that the group generated by sigma 1 and sigma 2 is the dihedral group, in fact, it is.. order is 8.

So, I am going to use this, I am not going to do this in this video, you can check this, this is a simple calculation. This is exactly the defining feature of a dihedral, you have 2 generators, d4 has 2 generators, one is order 2, one is order 4 and 2 generators are this property. So, now use this and prove this on your own. Now I want to understand, let us call this G, let G be the group of automorphisms generated by sigma 1 and sigma 2, we know that it is a diagonal group and we know that it is order 8, so what is the fixed field of this group.

So, the claim first is, K is of course ct, K power G has degree 8 because K colon K power G is the order of G which is 8 so that is part of this exercise. In fact, that is what you want to see and is the fact that it is in fact, before it is irrelevant for us, it is order 8. So, now I want to understand this more carefully, so first note that, take this particular element, P power 4 plus t power minus 4 in K.

This of course is in K, remember t inverse is our usual way of denoting 1 by t. So, t power 4 plus 1 by t power 4. So, then what is sigma 1 of t power 4 plus t power minus 4. So, t goes to i, t so this is i, t power 4 plus i, t power minus 4 which is of course t power 4 t power minus 4. Similarly, sigma 2 of this is t power minus 4 plus t power 4. So, that means t power 4plus t power minus 4 is fixed by every element of G. It is fixed by the generators of G so it is fixed by every element of G.

So, that means, entire… is containing the fixed field because everything is certainly containing the fixed field. So, we have c power P power 4, c adjoin P power 4 plus t power minus 4 is in K, is in KG. Now we want to understand this, so what I am saying is that, this particular element is fixed by G, complex number are all fixed by G, so any rational function in this with complex coefficient is fixed by G so that is in K power G.

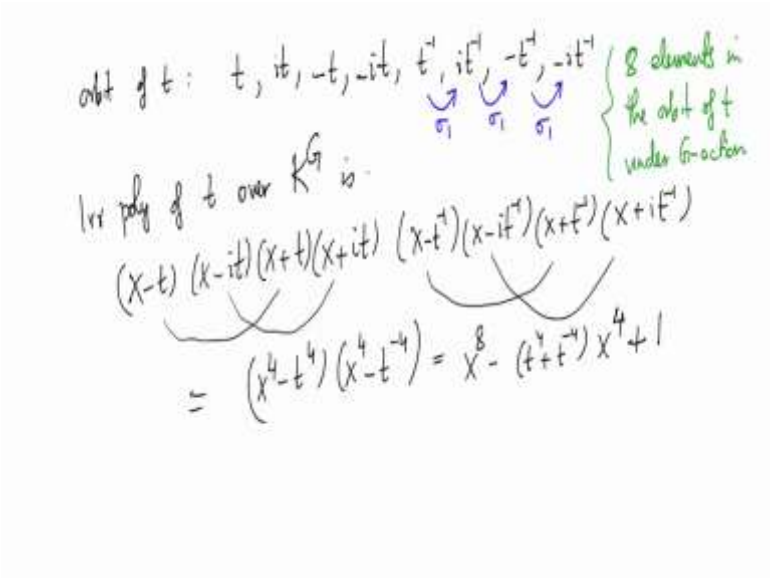
Now, in order to understand the relation between these 2 and in fact, to show that these are equal, I want to understand what is the irreducible polynomial of t which is in K over K power G. And this is the point I wanted to emphasise that is the reason I am doing this example, if you go back to the previous theorem that we proved in the last 2 or 3 videos, this theorem and started with argumentory element.

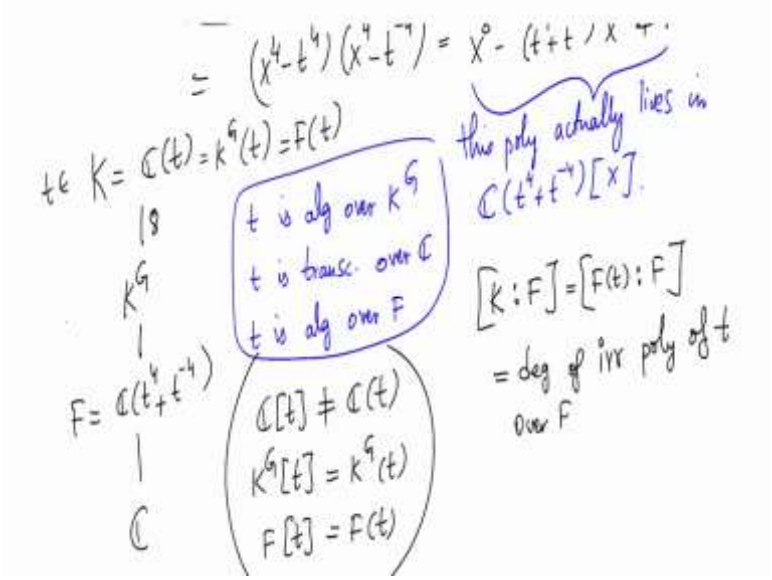
We computed its irreducible polynomial like this, and we remarked at that time, that these are very useful way to find the irreducible polynomial of an element in a Galois extension. So, here all we need to do is, look at the imagine of that element and all the Galois group

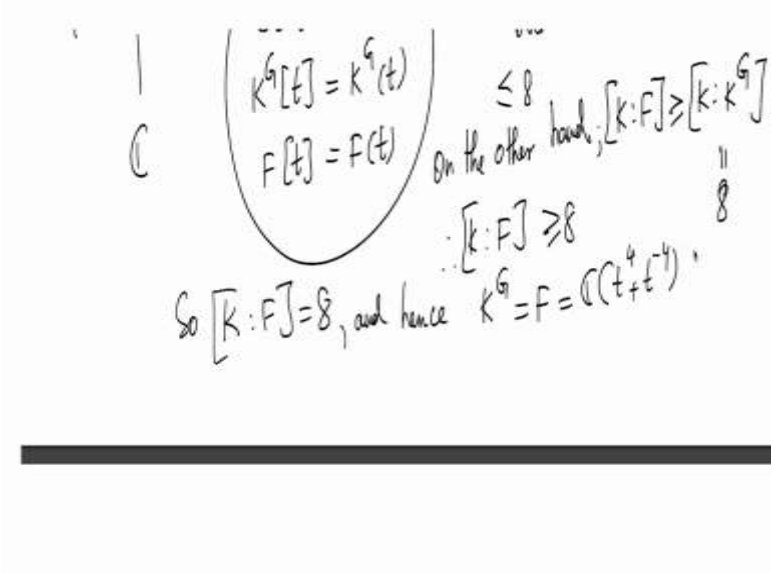
elements and take the distinct set of those and take x minus alpha 1, x minus alpha 2, x minus alpha r. Here of course K over KG is Galois.

In our case, K over KG is Galois, I mean this is trivial, right? Because KG is the Galois group of the… KG is the fixed field of G. So, anything from k over KG is Galois, that is the definition of Galois extensions. So, to find the irreducible polynomial, of t over KG, let us look at the orbit of t, this is the group theory language, orbit of t under G action. So, this is the orbit, meaning where t goes in all the group elements is what we looked at.

(Refer Slide Time: 14:48)







So, what is orbit of? This is easy now, sigma 1, of course t is there, sigma 1 sends it to i, t. That is sigma 1 goes to i,t. Sigma 1 square, I think I wrote these things, will send it to minus t and sigma 1 cube will send it to minus i, t and then you have t which you do not need to write it again, t is already there. Sigma 2 sends t to t inverse. Sigma 1 and sigma 2 will send it to i, t inverse. And then you will get sigma 1 of this.

So, here to here is sigma 1 and again sigma 1,what you get? I times i, t inverse, so minus t inverse. And finally again sigma 1 so minus t inverse times i which is i minus i to inverse, so this is again sigma 1. So, I have this clear so these are the 8 elements in the orbit, in fact, it just happens that, they all are distinct, in general remember some of them can equal each other because t generates the extension here, it must have all the 8 distinct, 1, 2, 3, 4, 5, 6, 7, 8 distinct elements of orbit.

So, the irreducible polynomial of P over KG is x minus P, x minus i, t, x plus t, x plus i, t, so this correspondence to the first 4, now x minus t inverse, x minus i, t inverse, x plus t inverse, x plus i, t inverse. Now it is clear that, you can combine these 2 for example, you will get x square minus t square, you can combine this to get x square plus t square and you combine all of them to get x power 4 minus t power 4 and similarly you combine this 2 to get x square minus t minus 2, x square plus t power minus 2, so you will get x power 4 minus t power minus 4. But this is equal to x power 4 minus t power 4 plus t power minus 4, this is x power 8, t power 4 plus t power mins 4, x power 4 plus t power 8.. sorry this is 1.

So, this is the irreducible polynomial of this over KG. So, this is correct, minus t power 4, minus t power. So this is fine but note that this polynomial actually lives in C, P power 4 plus

t power minus 4 bracket x because the coefficients are 1 which is here of course, P power 4 minus t power 4 plus t power minus 4 which is here and 1 is here. So, that means… now let us draw the picture again, we are almost done and we have K which is CP and K power G which is a degree 8 extension and then we have C t power 4 plus t power minus 4.

Now the irreducible polynomial of t over this has degree 8 because for example, this is generated by, this is also KG, another way of this, this is KG bracket t, t is of course, t is algebraic over, so this is where things get wired here, t is algebraic over KG, t is not algebraic over C, it is transcendental over.. so t is algebraic over this, so this is generated by t. So, that is the degree 8 extension but this on the other hand, this is also, basically this is also, if you call this f, this is also f bracket t.

So, t is also algebraic over F, if you remember this, all the way down, so all these are transcendental extensions. These are all close to each other but there is along gap between these and C. This is also transcendental over C clearly. These are all finite extensions of each other, 3 of them. But they are all transcendental extensions of C. So, I am emphasising this because this round bracket t, in fact, the same square bracket t, because t is algebraic over this, t is algebraic over this.

In fact, the same polynomial is…t satisfies this polynomial over F so it is algebraic where this round bracket is not to be confused with square bracket, those will be very different. Whereas KG…. I mean this is something we discussed a long time ago. So, this is just to make the same point, so what we had is that, irreducible polynomial of t over KG is this, and the same polynomial lives over this, so the degree of the extension, so these are just parenthetical remark, so the degree of K over F is remember same as F t over F because Ft is equal to K, this is just like an algebraic element, t is an algebraic element over F.

This Ft is equal to K, so this is equal to the degree of irreducible polynomial of p over f, by definition, this is the degree of irreducible polynomial P over F. But this is less than equal to 8 because P satisfies a particular degree in polynomial. So, the irreducible polynomial maybe of smaller degree so it sends at most 8, so this polynomial leaves in FX, because F is equal to this. So the irreducible polynomial of t over this could be… maybe smaller degree so it is at least at most 8, so this is already 8 and this we just concluded, is less than or equal to 8.

But this is… Some number is positive number so this is greater than equal to 8. On the other hand… so let me just wrap it up, on the other hand, K colon F is greater than and equal to K

colon KG which is 8. So, K colon F is greater than equal to 8. So, K colon F is equal to 8 that means, this is also equal to 8 and that means this is an equality. And hence, k power G is equal to F which is C adjoin… this is the statement I wanted to make because the question was find the, I do not know where I wrote that, what is K power G?

K power G is concretely described by this analysis. So, it is C adjoined t power 4 plus t power minus 4. So, this is not that important for what we do next, but I wanted to do this because this illustrates the various points raised in the previous theorem which is an extremely important theorem, so please go over the proof of the theorem, the 2 videos then the corollaries and the examples which we just did because these are all important features of Galois Theory.

And in the next video we will start adding towards the main theorem of Galois theory, so I will first give you a couple of motivating examples and then we will state and prove the main theorem of Galois theory. Thank you.