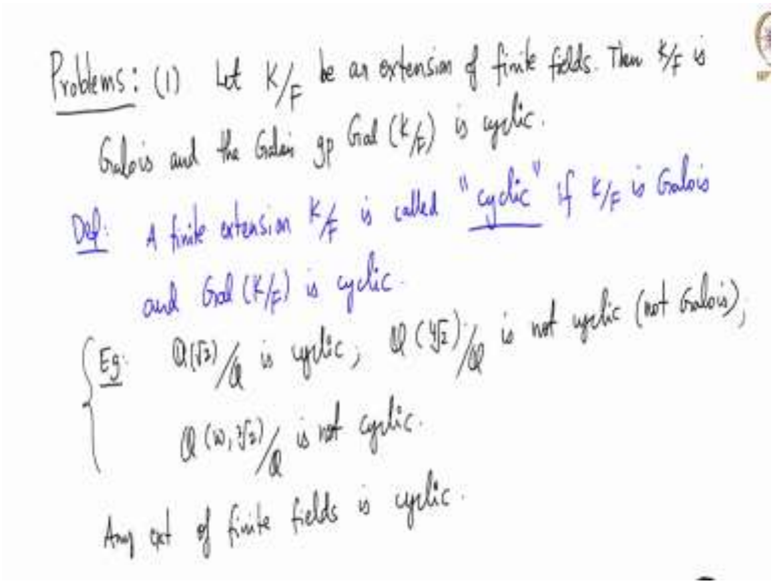
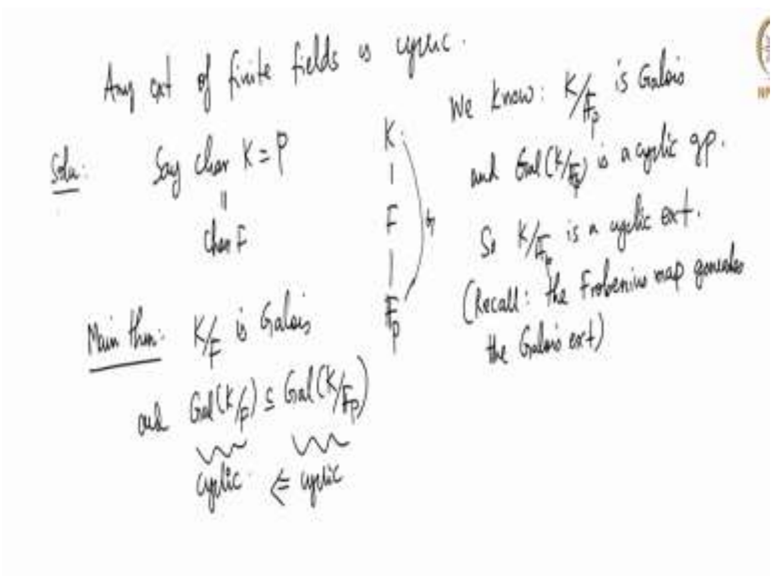
Introduction to Galois Theory
Professor Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute
Lecture 27
Problem Session Part 5

Welcome back. In the last few video we proved the main theory of Galois Theory and we learned, for example, how to prove fundamental theorem of algebra using the main theorem of Galois Theory. So, in this video and one or two videos after this, we are going to do some problems.

(Refer Slide Time: 00:32)





So, before we proceed further and see more applications of main theorem, it is good to learn how to apply so far, whatever we learned so far and solve some exercise. So, let me start with some observations that I made in the past but I want to record them concretely so that you have a record of them and we discuss all the missing details. So, first problem is, let K over F be an extension of finite fields.

So, then K over F is Galois that is the first statement and moreover the Galois group K over F is cyclic, so let me give you a definition here before we proceed with the solution. A finite extension, just a word about the terminology, finite extension always refers to an extension of fields that is a finite extension. Here I am not going to say finite extension, I am not asserting anything whether K and F are finite fields, that is a general statement.

Here I am saying K over F is an extension of finite fields that means K and F are finite fields. So, there is a big difference between this. So, a finite extension of K over F is called cyclic, if K over F is Galois so it has to be Galois first and the Galois group is cyclic. So, cyclic extension is a short form for a Galois extension, whose Galois group is cyclic. So, examples of such things are, Q root 2 over Q is cyclic. Because it is Galois, its Galois group is Z not 2Z. One the other hand, Q adjoin fourth root over Q is not cyclic.

This is because it is not a Galois. It is not a Galois extension so it cannot be cyclic, only after you determine it is a Galois extension, you ask for its Galois group. On the other hand, if you take Q adjoin omega comma cube root of 2 over Q, this is Galois but the Galois group is S3, so it is not cyclic. So, the assertion of this problem is, any extension of finite fields is cyclic. So, that is what the problem is asking you to show.

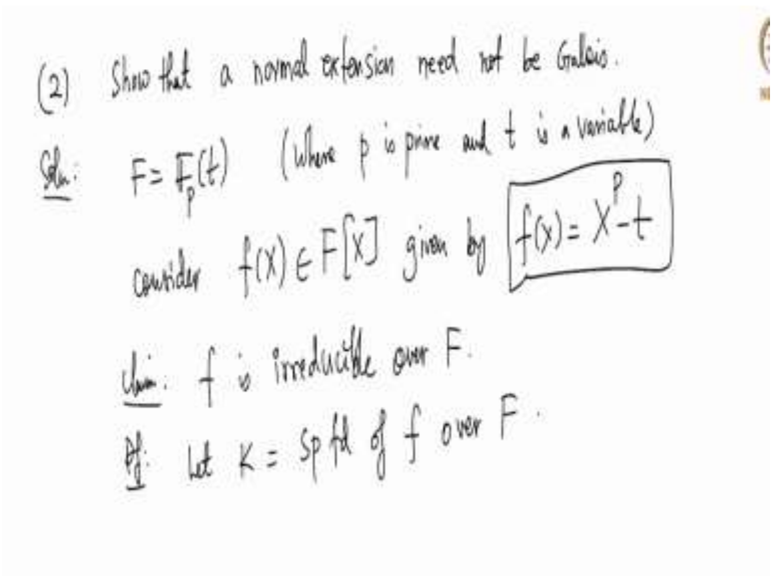
So, if you have 2 finite fields, one containing the other, it is a Galois extension and its Galois group is cyclic. In other words, it is a cyclic extension. Let me prove this, something which we have done before. Let us say characteristic of K is P, so this is of course will be the characteristic of F also, if you feel the extension, both will be of same characteristic. So, you have K or F, but this both live over the prime field.

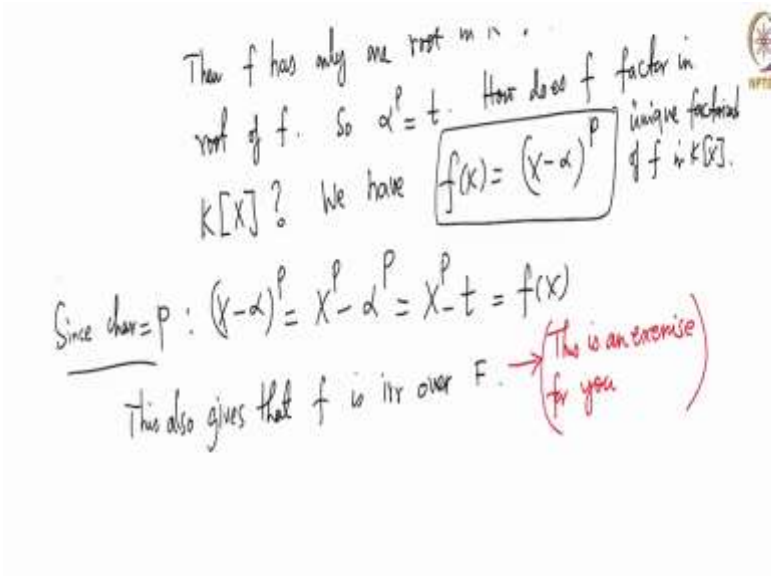
So, we know, so this I will assert without proof, K over FP is Galois and Galois group of K over FP is isomorphic to Z over R… sorry, it is cyclic group, let me simply say that is a cyclic group. So, K over FP is a cyclic extension. So, this is Galois and that is because, recall that, the Frobenius Map generates the Galois group.

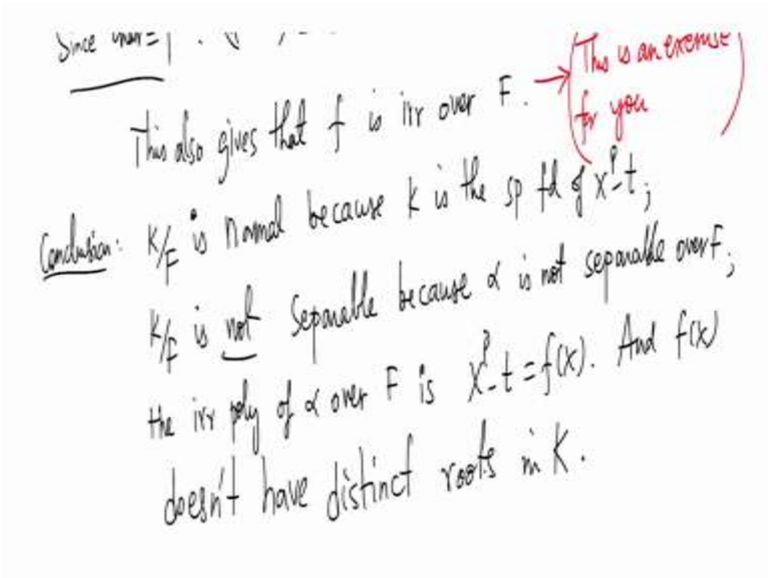
In proving this, in fact, we also proved that it is Galois extension because the Frobenius Map will have the right order so that order is the degree of the field extension. Now by the main theorem, this is not main theorem, I mean K over F Galois is actually not the main theorem. That is just the standard fact about Galois extension because they are supposed to be normal supper able. So, this is Galois, what the main theorem says, is that Galois K over F…

This is even not the main statement of the main theorem but I am putting every statement of the Galois groups and sub groups under the heading of the main theorem. So, it implies that, this is sub group, but this is cyclic so this implies this is cyclic. The sub group of a cyclic group is cyclic, so we are done. So, this K over FP is a cyclic extension so K over F is a cyclic extension. So, that is the solution for the first problem.

(Refer Slide Time: 5:54)







So, this one is the first problem and now the second problem is not new to you, I will sort of mention them before but I wanted to explicitly talk about them once more. So, show that a normal extension need not be Galois, so remember Galois equals normal plus separable, always finite. All extensions are finite for me, so finite extension is Galois if and all if it is normal and separable. But the point is, it is not enough that it is nearly normal. In characteristic zero, of course it is enough but not in general.

So, the argument here is, you take Fp t where p is the prime number of course, and t is the variable. So, this is the field of rational functions in one variable over Fp. And let us consider the polynomial, F of X in FX given by… I think, I have did P equal to 2 case but more generally one can do this. Take X up p minus t. So, first claim is that, f is irreducible over F. So, for P equal to 2, all you need to argue is that, it has no roots.

But for higher values of P, it is not enough to argue that it has not roots. But one can argue that, it is not separable and it has only one root. So, actually what we will show is that, so let us take the fixed field, the splitting field. Let me remind you Fp t, let us take the splitting field of f over t. Then, f has only one root in K so the reason is, so let alpha be root of f in K. Because K is the splitting field, it will… f will have a root so we will pick one of them called alpha. So, we have alpha per p equals t.

So, now I claim that, there cannot be any other root. So, let us take the polynomial x minus alpha, so how does f factor in k, x? So, that is what I am saying, that is what I wanted to understand. So, I claim that, we have f of x, x minus alpha power p, so this is because x minus alpha power p, since characteristics is p, x minus alpha power p will be x minus p minus alpha power p. All the mixed terms will go away.

So, this will be x power p minus t, alpha power p is t, right? So, this is true and in a polynomial ring over a field, factorisation is unique so this also affects. So, this must be the unique factorisation of f in kx, factorisation is not available in capital FX, so this is only available in capital KX. So, this proves you in one short that f is not separable and also it is irreducible. So, note that, this also gives that f is irreducible over F.

So, this is because if it is not.. it will have a factor and those factors must involve x minus alpha. So, actually, this requires a little bit approve, so I am going to leave this as an exercise for you. And I want to get back to the main part of the problem which of course, is to show that K over F is not Galois. For that I do not need F to be splitting field. So, F to be irreducible. This claim is in fact, an exercise. I want to do other problems, so I will skip this.

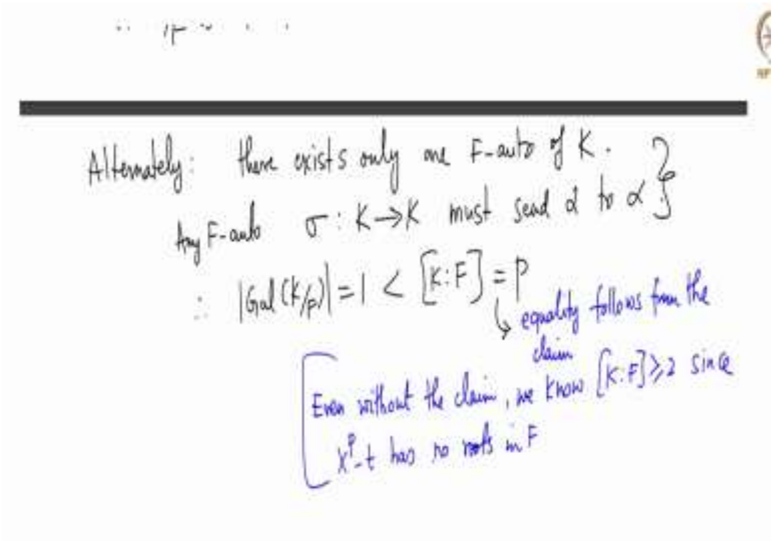
So, I want to say that F is irreducible and it is an exercise for you that is irrelevant to the problem that I am trying to consider. So, now because of this, what is the conclusion of everything that we have done so far? K over F is normal because K is a splitting field of x power p minus t. And K over F is not separable because alpha is not separable over F.

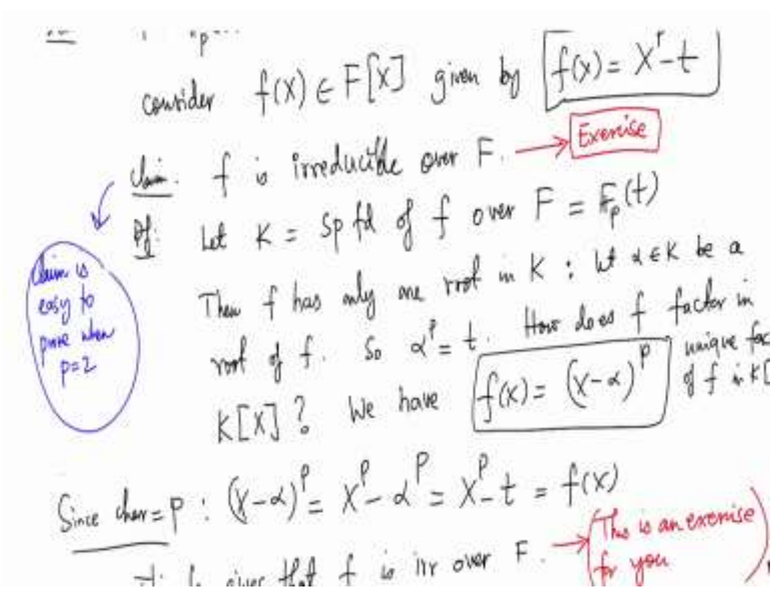
So, this is because irreducible polynomial of alpha over F x or F rather by reclaim is, X power p minus t. At this, technically without proving the claim, all you can say is that, irreducible polynomial is the device of this. But once you prove the claim, you can show that, this is the irreducible polynomial and this of course I call f of x and f of x does not have distinct roots in K. So, it is not separable because it does not have distinct roots.

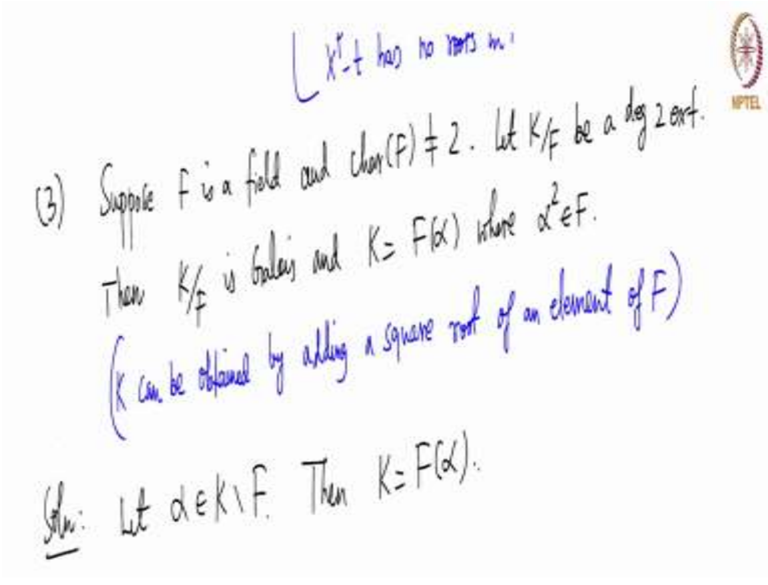
And you can actually make do without this claim because all you need to know if that, the polynomial has no roots in K and no roots in F which of course is true statement because there cannot be rational function whose Pth power is at t. So, that we have viewed before when we talked about this in the previous video.

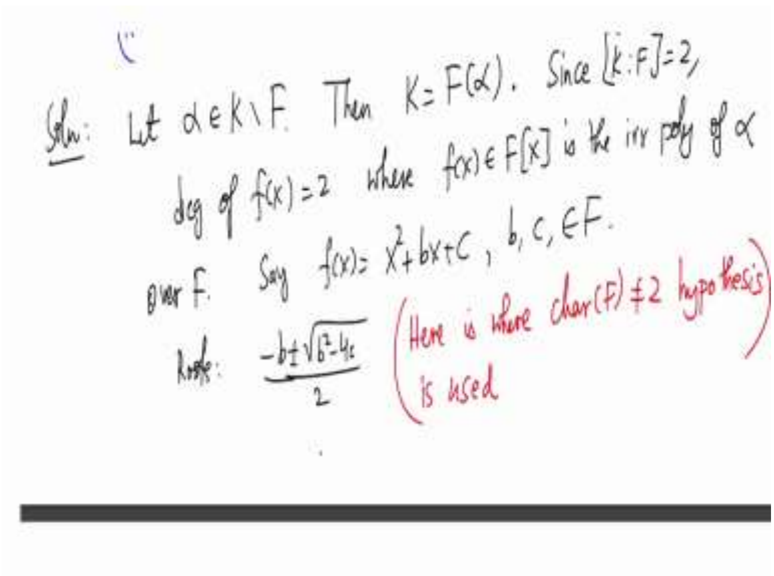
So, this has no roots so the irreducible polynomial will be at least degree 2 and only root of this is alpha so it does not have distinct roots. The number of roots is strictly less than the degree so it does not have distinct roots, irreducible polynomial does not have distinct roots even if irreducible polynomial is not this, and it is a factor is this with degree at least 2. So, it does not have roots and hence it is not separable so K over F is not Galois.

(Refer slide Time: 14:12)









So, you can also see this by… alternatively you can show non-Galois by there exists only 1 F automorphism of K. because any automorphism that fixes F… any F automorphism must send alpha to alpha because alpha is the only root of the irreducible polynomial of alpha. So, any automorphism must send alpha to alpha so that the order of the Galois group is 1 which is strictly less than the degree is p.

So, again the equality here follows from the claim which I have not proved but even if you do not agree that x power p minus t is irreducible, what you can definitely say is that, K colon F is at least 2 even without the claim. We know, K colon F is at least 2. So, suddenly we get a contradiction because we get non-Galois because 1 is strictly less than 2. Since x power p minus t has no roots in F. So, this has no roots in F so this is at least 2 so the cardinality of the Galois group is strictly less than the degree and hence it is not Galois.

And finally before I move on to the next problem, let me remark finally that, the claim is easy to prove when p equals 2. This is the degree to polynomial and degree to polynomial is irreducible if and only it has no roots. So, it has no roots is an easy statement. And that is enough to conclude irreducibility in p equal to 2.

So, you do have a normal extension that is not Galois by taking characteristic to… but in general you can also do this and without proving the claim also we have shown that it is a normal extension and it is not a Galois extension. But it is still nice to prove the claim and complete the picture and conclude that this is an equality, the degree is actually p. That I will leave for you to do.

So, now let me continue and do some more examples, so your next problem… let us see what I want to do next. Yeah, so let us see the following problem, this also is something which came up before but I am trying to tie loose hands here and settle this. This is a nice statement and this is something we will see more generally later. Suppose F is a field and characteristic of F is not 2.

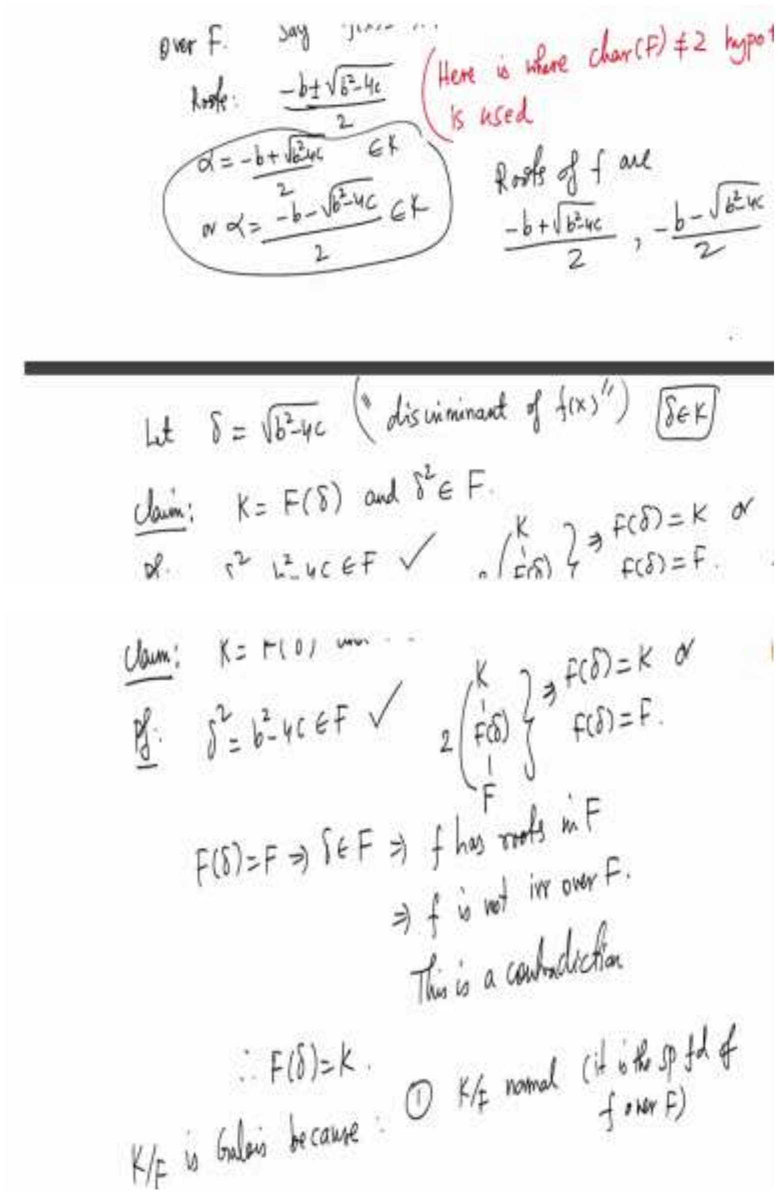
So, F is any field, all we are assuming is that, its characteristics is different from 2. Let K over F be degree 2 extension, then K over F is Galois and K is in fact, equal to F alpha where alpha square is an F. So, in words what we basically say is that, K can be obtained by adding a square root. So, you take alpha square that is an F so you add a square root of that to get alpha so K equal to F alpha so this is a nice structured result for degree 2 extensions of fields which are not characteristic to.

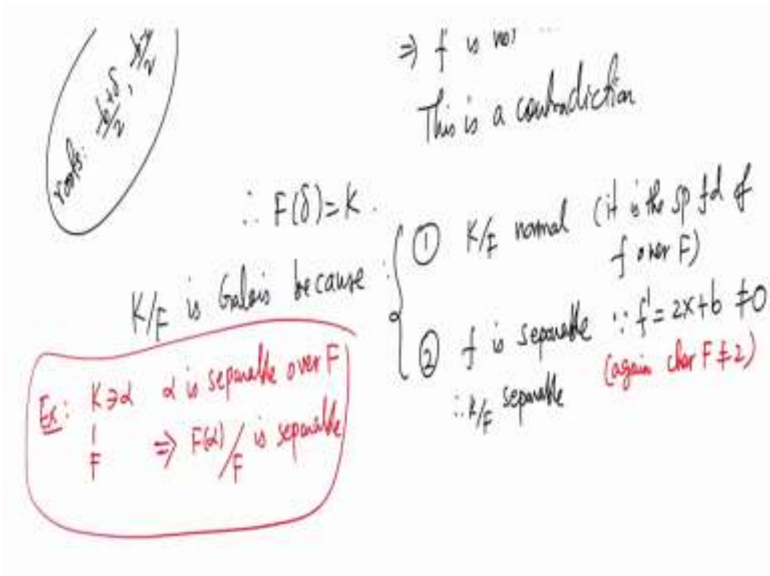
So, the proof is very simple here, so what we know is that degree is 2, so we can assume that, the recent element… not assume, we do know that there is an element that we can take whose… Let us say, beta.. no, let us say alpha is in K minus F so that we know it exists because K is different from F so then, we do not quite know that alpha will do the job for us because alpha square may not be in F so we do not know yet that this particular alpha will do.

So, what we do now is, to exhibit some other element which does the job. So, since K colon F is 2, there exists…. The degree of fx is 2 where capital FX is the irreducible polynomial of alpha over capital F. Remember, K equal to F alpha, so this implies degree of alpha over F is 2. That means its irreducible polynomial is 2 so let us write down what it is. Say, fx equals x square plus bx plus c where b and c are elements of the best field.

So, x square plus bx plus c, now what are the roots, roots of this because of the quadratic formula which we have recalled earlier? These are the roots and here is where the characteristic different from 2 hypothesis is used because you cannot divide by 2 if the characteristic is 2, so roots are given by this is a statement that only holds in characteristic different from 2 so the roots are this.

(Refer Slide Time: 21:00)





Now let us take delta to be square root b square minus 4c so this is called the discriminant, if you are familiar with this terminology, but that is irrelevant. So, let us take this, delta to be this. So, I claim that, K is F delta and delta square is F. So, this proves the part about K being generated by x square root of an element in F. So, clearly delta square is b square minus 4c is F, this is okay. But why is K equal to F delta?

This is also clear because K is here, F delta is of course here because delta is in K because the roots are in K. So, alpha is minus b plus b square minus 4ac by 2 or alpha is minus b minus b square minus 4c by 2. So, alpha is a root, if once alpha is in K, you can clearly rearrange terms to conclude that square root b square minus 4ac is in K. So, F delta is sub field of K and this is a degree to extension.

So, this implies F delta is either K or F delta is equal to F. So, if F delta is K, is the statement, if F delta is equal to F this implies delta is in F. But that means, F has roots in F because if this delta is in F, minus b is of course an F. So, this whole term is an F after dividing by 2 is still in F, similarly this is an F. So, this means, F is not irreducible in F. So, this is a contradiction.

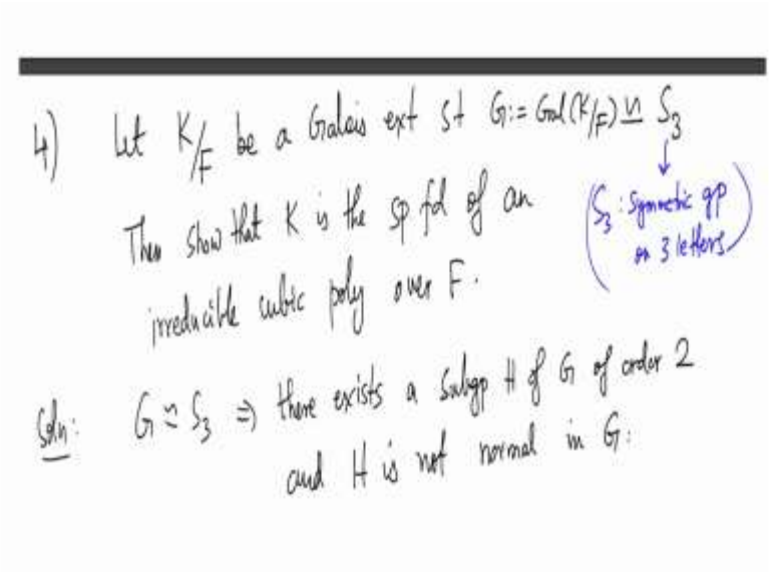
Because F is irreducible polynomial of alpha so that means F delta must be in K. So, that was this, and finally the Galois F is also clear because K over F is Galois because of 2 things, K over F is normal, normal because it is a splitting field, right? Because the roots of F are this, minus b plus square root b square minus 4c by 2, minus b, minus b square minus 4ac by 2. So, the point is if this is alpha and alpha is in K, this means this is also in K.

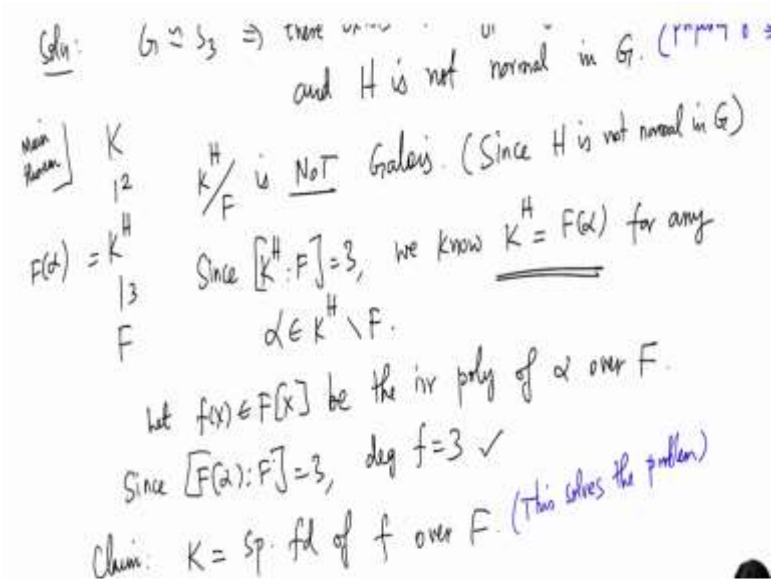
So, this is a simple observation because b square minus 4ac is in K so basically the roots are minus b plus delta by 2, minus b minus delta by 2. If delta is there, then both are there. So, this is the splitting field, and F is separable because its derivative is… so, this is non-zero so we know that non-separable irreducible polynomial must have derivative zero. So, here again characteristic F not equal to 2 is used.

So, it is separable one can argue that, if delta is separable, if alpha is separable then F alpha is separable. So, that is the general statement. So, F is normal and separable so there is a small little statement here. So, this is an exercise which is really an exercise about, if alpha is separable over F, implies F alpha is separable so all polynomials in alpha will continue to be separable. So, this is an exercise about separable extension which I will not do for now because that is not the point of this course.

So, using that, we know that it is Galois. Any degree to extension of a non-characteristic to field is Galois, of course that is false, if you take characteristic 2 as this example, shows. So, this tells me that the third problem is solved so any degree to extension is Galois and it is obtained by adding this square root.

(Refer Slide Time: 26:58)





So, let me do one of the problem before we stop and then we will continue, in the next video I will do some more problems. So, the next problem is very nice also. So, the fourth problem says, let K over F be an orbitory Galois extension with such that the Galois group, let us call that G of that extension is isomorphic to S3. So, S3 is always symmetric group on 3 letters. So, order 6 group and G is isomorphic to that.

Then, show that K is the splitting field of an irreducible cubic polynomial capital F. So, this is a nice statement, in general every Galois extension, whose Galois group is S3, must be the splitting field of an irreducible cubic polynomial. This is a nice statement, so let us see why this is the case. So, because G is isomorphic to S3, the first point is, there exists a sub-group H of G of order 2 and H is not normal.

This is the feature of S3, of course any group of order 6 will have a sub-group of order 2, for that we do not need S3. But you need S3 to conclude that, it is not normal in G because S3 will have degree to elements. For that you take any degree to element and you take the group generated by the other. That will be a group of order 2 and it is not normal. So, this is the property of S3, this is where S3 will be read.

So, let us call that H, so now you have K, the fixed field of this, let us call that KH and living underneath of all that is F. So, now the main theorem of Galois Theory says, here we do need the main theorem or the full force of main theorem in this problem. What does the main theorem says, first of all it says that, degree of this extension is 2 because order of H is 2 and degree of this extension is 3 because index of H is 3, and this whole thing is degree 6.

But more importantly the main theorem says that, it is not Galois. It is not Galois because it is not normal. Since, H is not normal, so it is not Galois so now… but we do know that since it is degree 3, we know K power H is F alpha for any alpha in KH not in F. So, take any alpha because it is not equal as fields. There is an alpha in KH that is not equal to… that is not in F so then F alpha is an intermediate field, it cannot be equal to F but this is a prime degree extension so it must be equal to F alpha. F alpha must be equal to KH.

So, now this means, we have not yet used the non-Galois of KH over F. We are only using the fact that 3 is prime. So, let capital FX be the irreducible polynomial of alpha over F. Now since F alpha colon F is 3, degree of F is 3 because degree of F alpha over F is simply the degree of the irreducible polynomial of alpha which is F. So, this is going to be my cubic irreducible polynomial.

So, the claim is K is equal to the splitting field of F over capital F. So, this proves the problem so this solves the problem. Why does it solves the problem? This solves the problem because, I am asked to show that K is the splitting field of irreducible cubic polynomial. It is a cubic polynomial, cubic means degree 3 of course. It is irreducible by choice because it is the irreducible polynomial of an element so if I show that K is the splitting field, I am done.

(Refer Slide Time: 32:16)

Pf of claim: (i) f splits completely in $K[X]$:

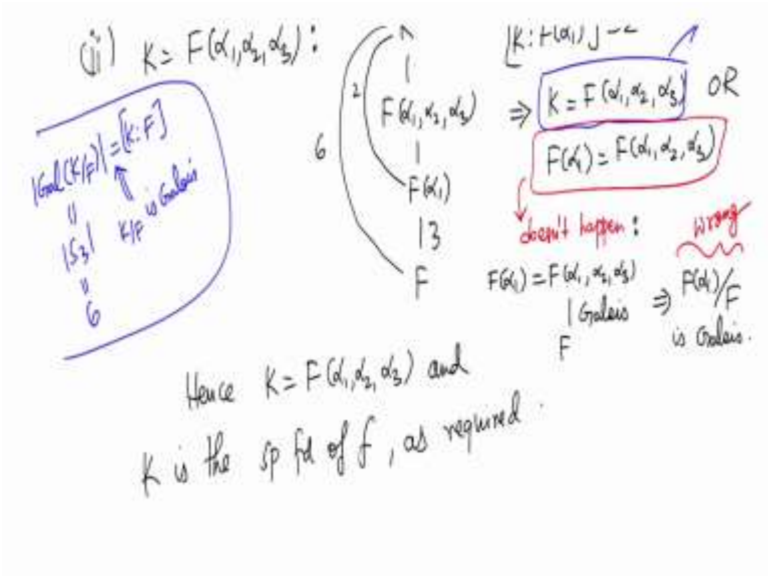
Reason: K/F is normal and $f \in F[X]$ has a root $\alpha \in K$ (and f is irr)

So f splits completely in $K[X]$.

Let $\alpha_1 = \alpha, \alpha_2, \alpha_3 \in K$ be the roots of f in K

(Note: $\alpha \in K$ is separable over $F \Rightarrow f$ has distinct roots in K)

(ii) $K = F(\alpha_1, \alpha_2, \alpha_3)$



So, why is this? So, the proof of this claim, it is very easy to prove this claim and it is where, in this proof we are not using that, KH is not Galois over F. So, first point to note is, K splits completely… sorry f splits completely in KX. Why is this? Reason for this statement, why? Note that K over F is normal because it is given to be Galois, it is important that I take a Galois extension so it is a normal extension and F is a polynomial over the base field has a root alpha in K. So, alpha is in F alpha, of course F alpha is contained in K.

So, it has a root in K so one of the equivalent characterization of normal extensions is that, any polynomial, irreducible polynomial, F is irreducible also. Any irreducible polynomial which has 1 root splits completely. So, that proves the first statement. So, let alpha 1 which is of course alpha, alpha 2, alpha 3 be the roots of F in K because it splits completely, remember there are 3 distinct roots also because it is a normal Galois extension, it is separable so there are 3 distinct roots. So, call them alpha 1, alpha 2 and alpha 3.

So, know that F is separable, rather I will say alpha in K is separable over F so F has distinct roots. Being the irreducible polynomial of a separable elements. So, the second statement to solve the problem is, K equals F alpha 1, alpha 2, alpha 3. Remember splitting field is not just a field where the polynomial splits completely.

In addition, it must be generated by the roots because you can take a bigger field, it will not be a splitting field. So, here I claim that, it is a splitting field, I am not merely claiming that, a cubic irreducible polynomials splits in it. I am trying to show that, it is in fact, generated by the roots. So, let us look at where this can fit in our picture.

So, this is our picture, what we know is that, this is degree 3, this is degree 6 because its Galois group is S3 hence the degree is 6. So, remember of course we do know that, the order of the Galois group is the degree of the field extension because… and this is 6, this is S3 and this is 6 and this equality is because K over F is Galois. So, it is a degree 6 extension, I should have mentioned that before.

So, this is degree 6, this is degree 2, so that means K colon F alpha 1 is 2. May be let me write it here, this is 6, this is 2. So, now F alpha 1, alpha 2, alpha 3 is a intermediate field of degree 2 extension. So, this implies K equals F alpha 1, alpha 2, alpha 3 or F alpha 1 equals, F alpha 1, alpha 2, alpha 3 because this is a degree 2 extension. These 2 numbers multiply to 2, that means you can either have, this is 2, this is 1 in which case this happens or this is 2 and this is 1, in which case this happens.

So, we are trying to show that, this happens and that this does not happens. And we are done now, right? Think why does not it happen? Because if F alpha 1 equals F alpha 1, alpha 2, alpha 3 then this of course is Galois, being a splitting field of a separable polynomial. So, this implies F alpha 1 over F is Galois. This is exactly what I said, is not the case.

So, this is not Galois, this of course is F alpha so if F alpha over F is Galois, the corresponding sub-group will be normal but we know that, in order to sub-group of S3 is not normal so this is not Galois, so this is wrong. So, if this happens, we get a contradiction hence K equals and K is the splitting field of f as required.

So, we did produce that irreducible cubic polynomial, F is irreducible cubic polynomial whose splitting field is exactly K which is what I am trying to show. K is the splitting field of an irreducible cubic polynomial and we showed that here. So, let me stop this video here, with this problem. And we have few more problems that I want to do which apply the main theorem of Galois Theory. Thank you.