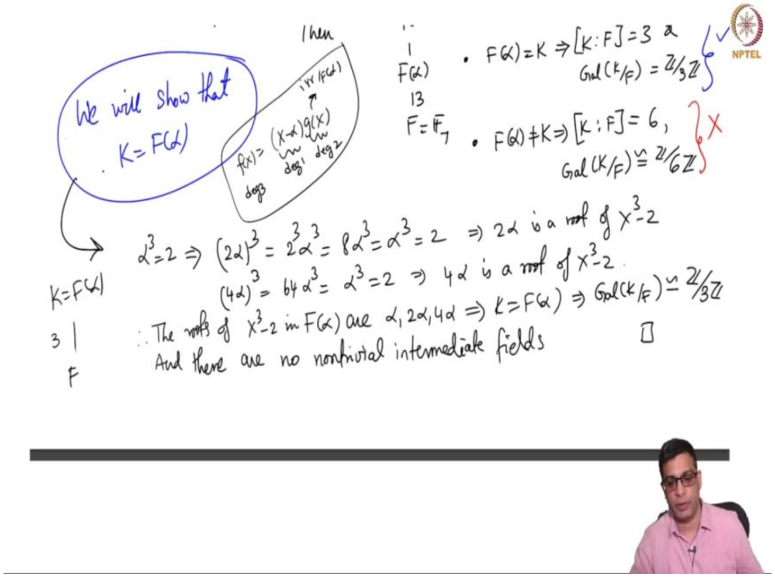
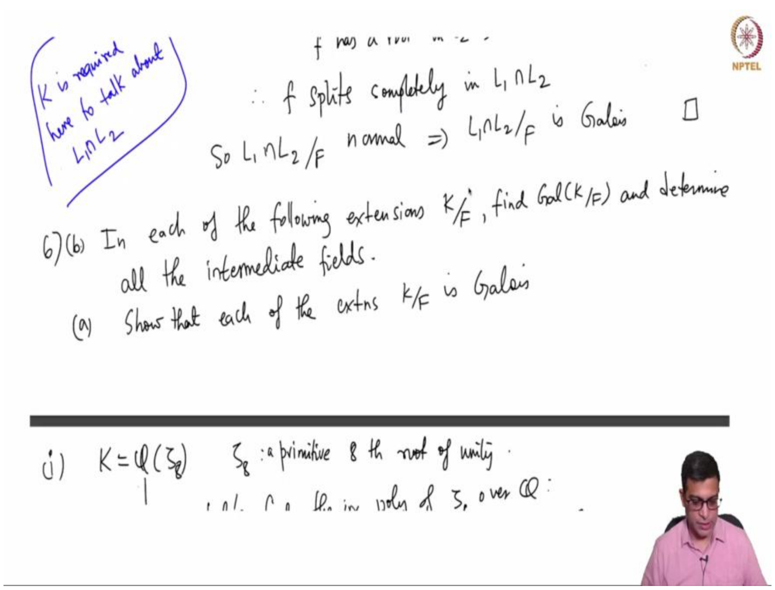
Introduction to Galois Theory
Professor Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute
Lecture No. 29
Problem Session - Part 7

(Refer Slide Time: 00:15)



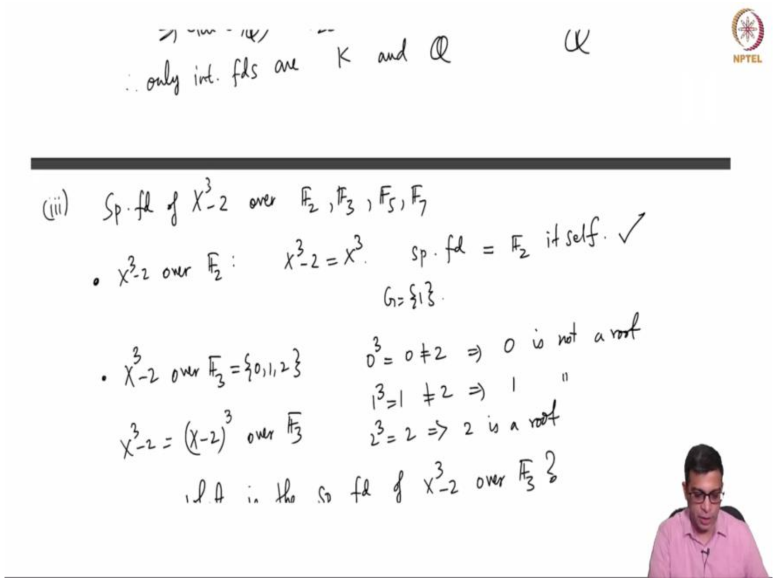
Welcome back, we are doing some problems sessions. And last class I ended with this problem where I left it in the middle of the problem. And I will complete it now. So this is actually easy to finish this problem now.

(Refer Slide Time: 00:30)



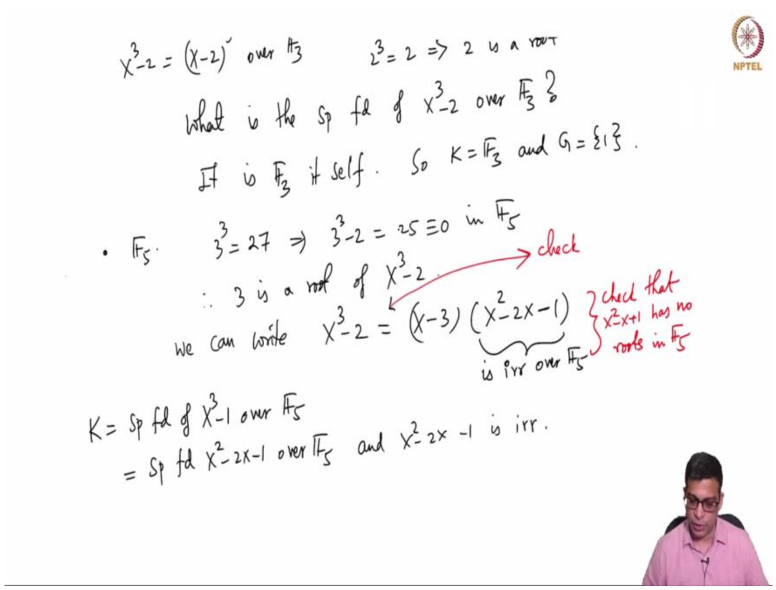
So if you recall, in this problem, we are asked to, so let us see, six, in each of the following extensions first show that it's Galois, and then find the Galois group and find all the intermediate fields. We are looking at various fields in this problem.

(Refer Slide Time: 00:45)



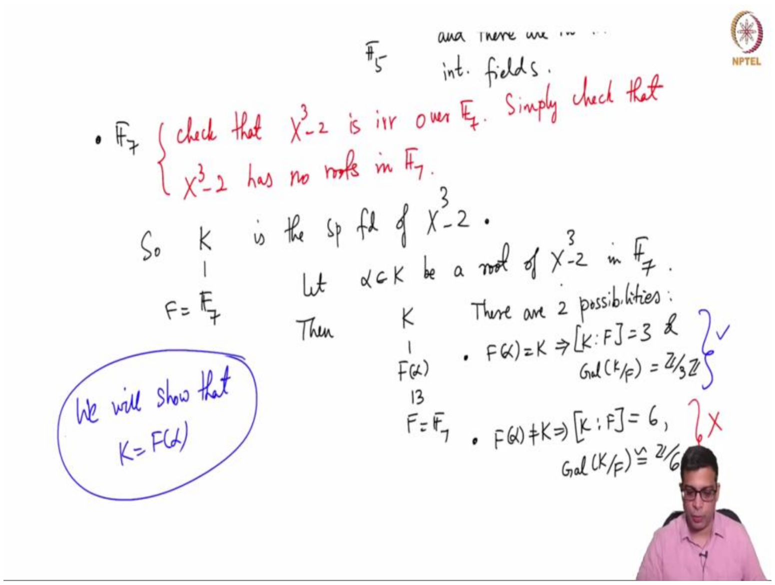
And the last part, we are looking at the splitting field of this particular polynomial over various finite fields. We did F2, then it is just the F2 itself is a splitting field because the polynomial splits completely. The same happens for F3.

(Refer Slide Time: 01:05)



F5 there is one root and after you factor it out you have a quadratic polynomial. So, the splitting field will be a degree to extension and the Galois group is Z naught2Z.

(Refer Slide Time: 01:18)

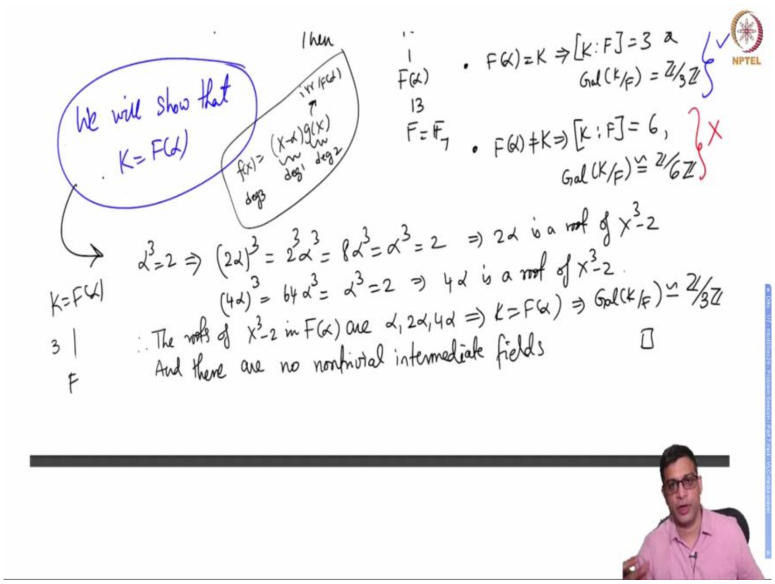


And finally, we are down to F7. And I wanted you to check, which is written in red here, is that this polynomial is irreducible, simply check that it has no roots, because it is a degree three polynomial, it suffices to check that it has no roots, and you can conclude that it is irreducible, and that is a trivial verification.

So, then we took the splitting field and let us say alpha is this single root and we joined F alpha. So, then in general when you add roots of a cubic polynomial, irreducible cubic polynomial over a field, you can always add one root to get a degree 3 extension. Now, the question is, are other roots already in F alpha or other roots need to be added extra?

So, these two possibilities are listed here, either the other roots are already in F alpha in which case K itself is equal to F alpha, the splitting field is F alpha and the degree of the splitting field is 3. And hence, Galois group has to be Z naught 3Z, because it is a degree 3 extension and whose Galois group is going to be of order 3.

(Refer Slide Time: 02:20)



Other, the second possibility is that the roots are not in F alpha, in which case you will have to add them. And then it must be degree 2 exactly, because the after you factor out x minus alpha from the polynomial in question, this is degree 3, this is degree 1, so this will be degree 2. And by the assumption that F alpha has no roots, no other roots, this G will be reducible over F alpha, and that would be the degree,in this case the degree of K over F alpha will be 2. Okay, so this is just a parenthetical remark.

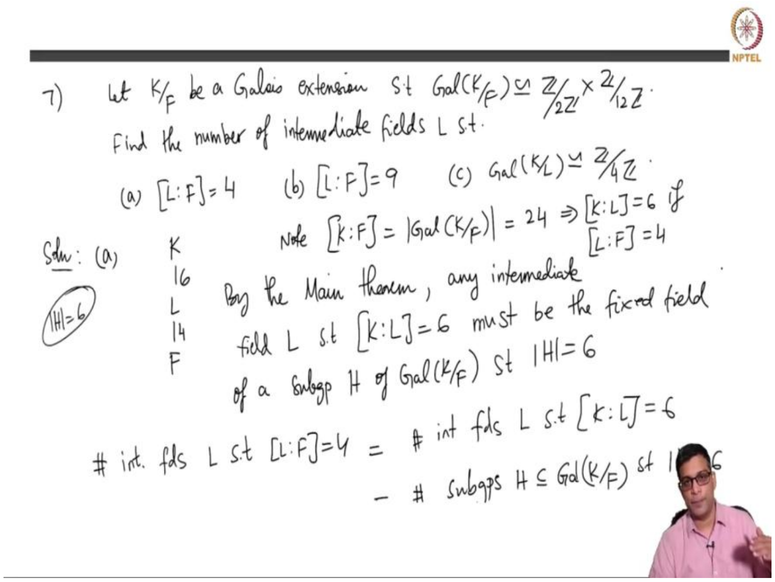
So, in our problem which of these cases happens. So, I claim that K is in fact F alpha. And for this, it's a simple statement, we note simply that once alpha cubed is 2, what is 2 alpha cubed? So, alpha is in k, alpha is an F alpha, alpha is the root of x cube minus 2, so alpha cubed is 2. So, what is 2 alpha cubed?So, this is 2 cubed alpha cubed.So, that means it is 8 alpha cube, but eight is 1 in F7, right. So, this is alpha cubed, which of course is true.So, that means 2 alpha is a root.

Similarly, if you do 4 alpha cubed, you get 64 alpha cubed. So, this is again, 63 is a multiple of 7, so this is alpha cubed. So, 4 alpha is a root. So, once you have a root the other two roots are simply 2 alpha. And so the roots of x cube minus 2 in K in F alpha, in fact, are alpha, 2 alpha and 4 alpha and hence K is F alpha, as I claimed at the end of last class.

So, the point is, there is a cube root of 2 or cube root of 1 in F7, namely 2 and 4. So, once you have a cube root of 2 and a cube root of 1, you can multiply them to get another cube root of 2. So, this implies that Galois group has to be a group of order 3 and there is only one such group at isomorphism and there are no non-trivial in intermediate fields, right, because it is a degree 3 extension.

So, if you take any field, here,the product of this number and this number is 3. So, one of them has to be 1, in which case that L will be equal to F or K alpha. So, in general, if you have a prime degree extension, it won't have any proper or nontrivial intermediate fields. So, that solves this problem, okay. So, this completes this particular problem. So, let us do a few more problems.

(Refer Slide Time: 05:36)



So, the seventh problem I want to do is the following. Let K over F be a Galois extension, such that the Galois group is isomorphic to Z naught 2Z cross Z naught 12Z okay. So, this is a problem which gives you an idea of how to apply group theory to derive information about the fields that we are working with. So, the problem asks you to find the intermediate fields L such that they have three properties.

L colon F is 4, then L colon F is 9. And finally, the Galois group of K over L is isomorphic to Z naught 4Z, okay. There are three parts to this problem. So given a Galois extension, whose Galois group is Z naught 2Z cross 12 naught 12Z, actually the question is find the number of intermediate fields. So, I cannot really find an L, because K or F is an arbitrary extension, we have no information about it, other than it is have Galois group. So really, I can only do the number of intermediate fields with these properties.

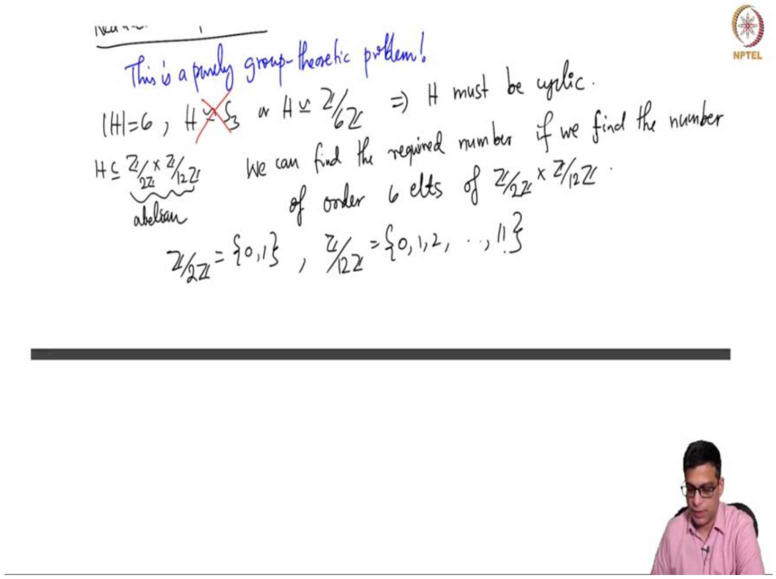
So let us first do A. So, let us draw the picture that we are now comfortable with. So, given extension is K over F, what is K colon F? K colon Financial, because the extension is Galois, this is the order of the group, which is 24, because it's a group isomorphic to Z naught 2 cross Z naught 12. So, that first is a group of 2, order 2, second is a group of order 12 so the product will have order 24. And we want this to be 4, that means this to be 6. So, implies K colon L is 6 and if L colon F is 4, okay.

So, now, what are intermediate fields L with this property? By the main theorem, any intermediate field such that K colon L is 6, must be the fixed field of a subgroup H of Galois group such that order of H is 6. So, now, if you remember the Main theorem, Main theorem gives a by bijection between subgroups of the Galois group and the intermediate fields and the order of the Galois group is the top degree and the index of the order of the subgroup is the top degree, index of the subgroup is the bottom degree. So, this is equal to 6.

So, the number we are looking for, so the number of intermediate fields L such that K colon L or this is the given problem, L colon F equals 4, this is equal to the number of intermediate fields L such that K colon L is, because L colon f is 4 is exactly the same as saying K colon L is 6. And this more interestingly is the number of subgroups H of the Galois group such that order is 6, okay.

So, now, we have reduced the whole problem to find the number of order 6 subgroups of Z naught to 2Z cross Z naught 12 Z. Remember Galois group is isomorphic to Z naught 2 cross Z naught 12. So, the Number of subgroups of order 6 of the group is exactly the number of subgroups of order 6 of this very nice group, concrete group, okay. So, if two groups are isomorphic, the things like number of elements of fixed order, number of subgroups have a fixed order andorder of the group itself, they are all same for both groups right.

(Refer Slide Time: 09:46)

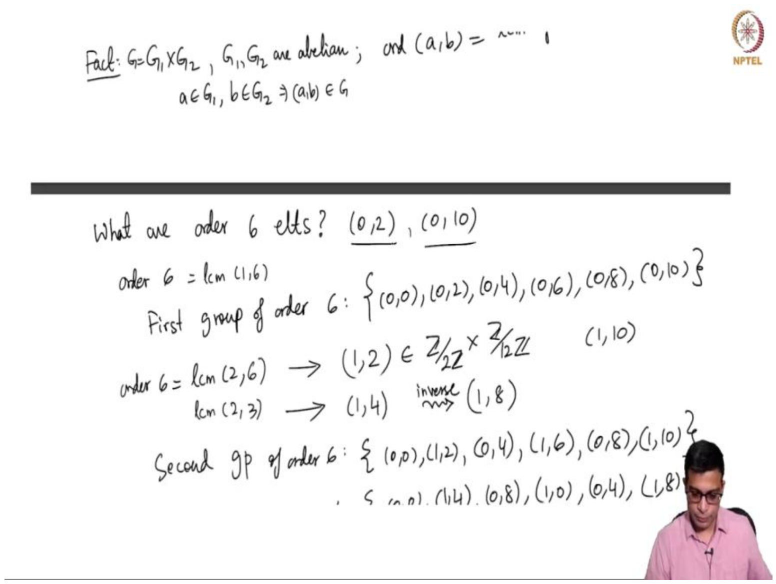


So, now we have reduced the whole problem to a purely group theoretic problem, this is a group theoretic problem okay. So, what was originally a number, a field theory question became really a group theory question, because of the Main theory that is a crucial ingredient in this solution, okay. Now, I will just quickly tell you how to do this, you all know what Z naught 2Z cross Z naught 12Z is.

So, first note that if order of H is 6, in general, H can be either this or the cyclic group of order 6, but H is a subgroup of Z naught 2 cross Z naught 12. But this is abelion, so H is abelion. So basically this cannot happen. So we are looking for cyclic groups of order 6, right. So,H must be cyclic. So, we will know the number of such H, we can find the required number if we find the number of order 6 elements of Z naught 2Z, cross Z naught 6Z, 12Z. Okay, so that is the, this is what we need to find out.

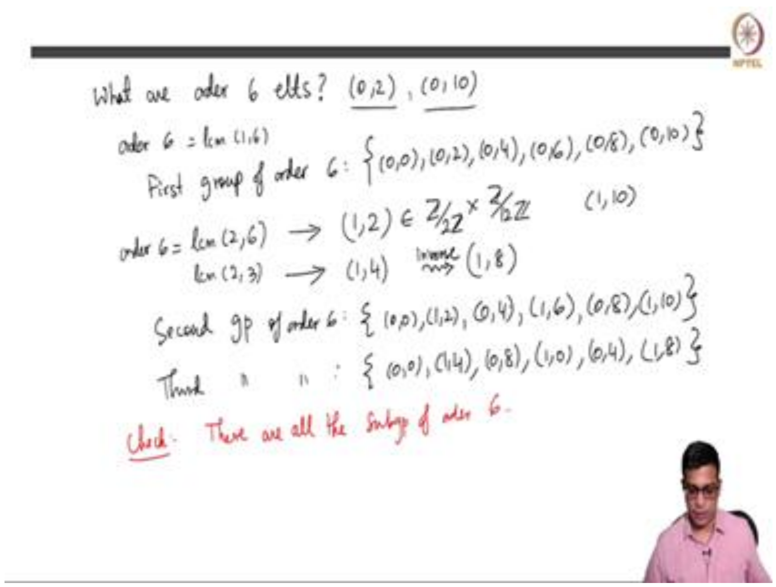
Note that the number of groups of order 6 is naughtequal to the number of order 6 element, because if you take an order 6 element its inverse will also have order 6, so these two will give the same group. So it is really the number of order 6 elementsdivided by 2. But now we are in business, because we have to find order 6 elements. So, now I am going to use additive notation, right. So 01, I mean, I will omit writing bars here, because it is cumbersome to do that, but you all understand that 1 plus 1, for example, is 0 here. And I will by use of notation called is this. Okay.

(Refer Slide Time: 12:59)



For now let us try to write down what are the order 6 elements. So what are order 6 elements? Order 6 elements are, I can take 0 in the first coordinate, then the second coordinate must have so order 6. So, this is a fact that I am going to use, it is a useful fact. If you have an abelion group, so G1 cross G2, let us say G is this, G1 and G2 are abelion; order of Acomma B, where A and B are in G1 and G2 respectively, is LCM of orders of A and order of B.

(Refer Slide Time: 14:01)



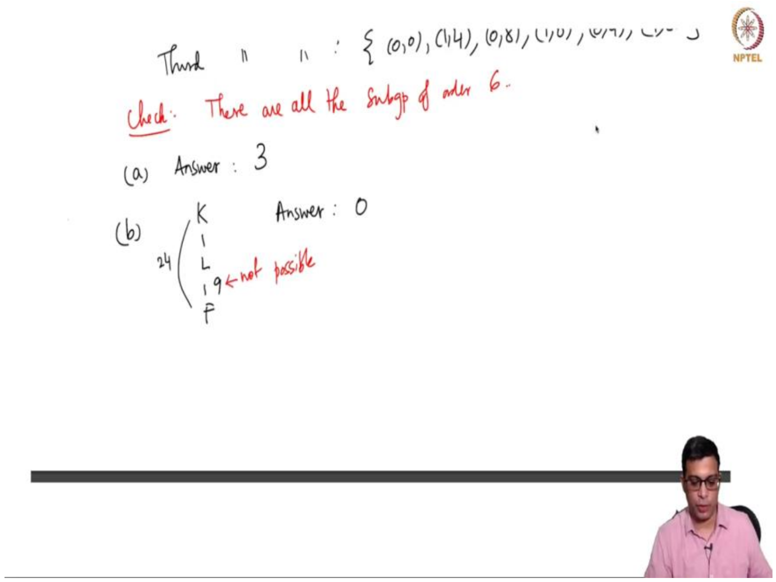
The order of the tupple AB, so that is in G is LCM. So, in order to get order 6 element, one possibility is, so we want order 6. So this could be LCM of 1 and 6, right? So, 0 is an order 1 element in Z naught 2Z. So, to get an order 6 element, I have to take 2 for example. So this is an order six element, and its inverse, of course, will be 0, 10, because the inverse of 2 is, so one group, so first group of order 6 is simply 0,0;0,2; 0,4;0,6; 0,8 and 0,10. So this is 1,2,3,4,5,6 elements. Now, this is the only group which coordinate is 0.

Now, what are other elements?So these are some possibilities. On the other hand, we can also do order 6 equals LCM of let us say, now you put 1 in the first coordinate, so that is 2. So you can put 6 here, or you can also do LCM of 2 and 3. So, this now gives you more possibilities. So, that means you take 1 and order 2 element, order 6 element. So I am going fast about this because this is just, I mean, standard group theory. But pleasecarefully watch this if it is not clear to you, and to get. So this is an element of Z naught 12, Z naught 2 cross Z naught 12, and it has order 6 because you can write down, for example, all its multiples, the sixth multiple will be 00.

And, other element will be, order 3 element will be 4. So these are 2 order 6 elements in Z naught 2 cross Z naught 12. So in fact, this will give its inverse. So, 1,2 and its inverse will be 1,10. And its inverse will be1,8. Okay, so 4, 8, 12; 4 is an order 3 element. Okay, so this, the second group of order 6, so I am just explicitly writing this 0,0 of course will be there, but the generator is 1,2 and then it's twice that is 2,4, add 1,2 to this, you get 0,8; add 1,2 to this which is 1,10 which is the inverse and you stop. So 1,2,3,4,5,6. So, third group of order 6 will be generated by 1,4, so 1,4 it's twice will be 0,8. (0.8) plus 1,4 will be 1. 8 plus 4 is 0, then you add 1,4 to this, you get 0,4. And then you add 1,4 to this, you get 1,8, which is the inverse. So 1,2,3,4,5,6,7,6.

So these are the three groups and you can check that these are all the subgroups of order 3, order 6. There cannot be any more subgroups of order 6. So this is easy to check, because there are only six elements of order 6 constructed this way. So, this is the, these are two of them. These are two more and these two more.

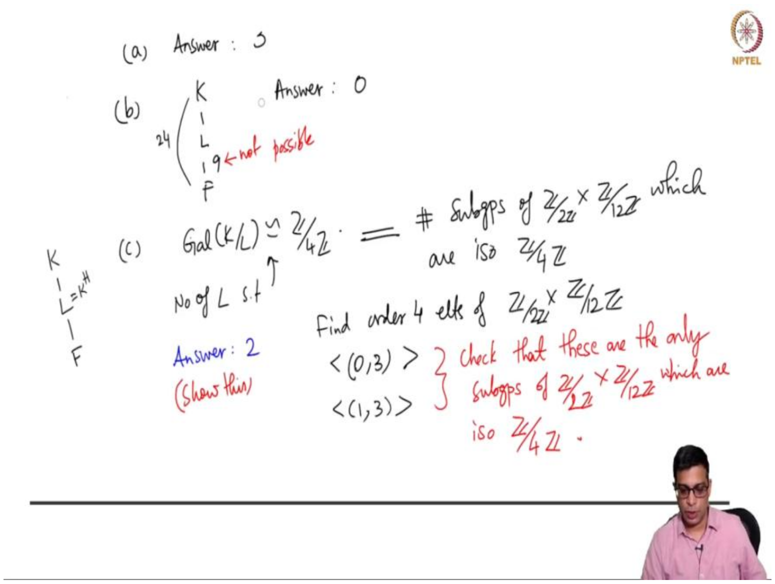
(Refer Slide Time: 17:52)



Okay. So the answer to the part A is 3.There are 3 fields L, such that L colon F is 4. Okay, so I hope this is clear. I mean, I had to go fast with this. But, this is just the main thing, I want you to comfort, to be comfortable with this, the reduction of the problem to group theory, and then treat the group theory problem as a separate isolated problem and just work out, this is a very concrete group to work with and it is 24 elements you can write down and check that these are all the order 6 subgroups.

Now let us go to B. So, we have to find subfields, intermediate fields such that this degree is 9, but this is actually a very simple nontrivial question because this is 24 so this cannot be 9. So the answer in B is 0, right. What is the number of subfields, intermediate fields such that L colon F is 9, it is0, because there can't be, so this is not possible. And so there are no intermediate fields with this property.

(Refer Slide Time: 19:05)



And finally, let us look at L such that Galois group of K over L is isomorphic to Z naught 4Z. So, this is more direct. So the number of L such that Galois group, okay, so let us say number of L such that this happens is equal to number of subgroups of Z naught 2 cross Z naught 12, which are isomorphic to Z naught 4Z, right, because if you have K and L and F, this has to be the number of any intermediate field with this property has to be the fixed field of subgroup Hwhich is isomorphic to 4Z and there is a bijectivecorrespondence between all such L and also such subgroups.

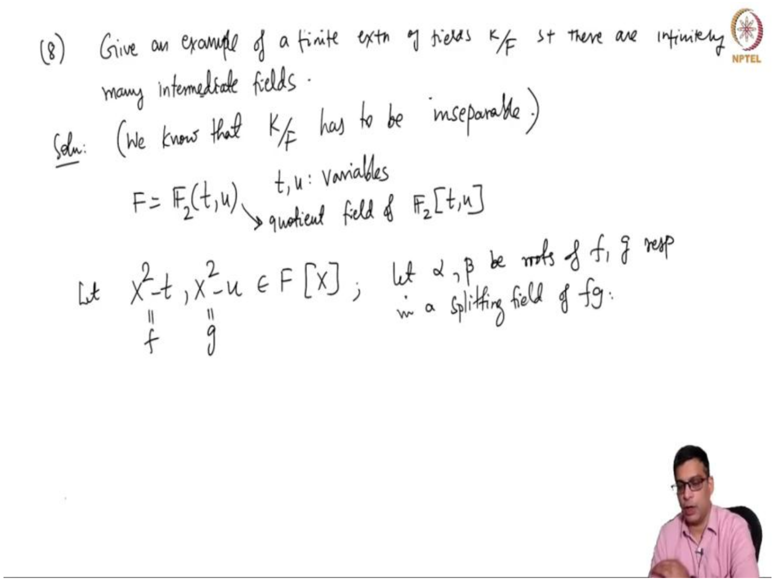
So, how do you find the number of subgroups like this exactly as we did in 6, Part A? So, we, there were a number of subgroups isomorphic to Z naught 6Z and here we have to find number of subgroups which are isomorphic to Z naught 4Z. So, I will give you the answer, answer is 2 and I will let you check the solution. So, show this.

So, because we have done Part A in detail, so I will not give you the details here, but find order 4 elements. So, you can take 0 order 4, so, 1,4 will give the LCM 4 just like before, so 0 has order 1, but what is the degree 4 element, order 4 element? You take 3, so and then you take its subgroup generated by this. So, I am really giving you this and you have to verify that these are the only things.

And other possibility is, you can take 1 which has order 2; and to get order 4, the other thing has to be order 4. So, again, you have to have order 3. So, check that, these are the only subgroups of

Z naught 12 2cross Z naught 12,which are isomorphic to Z naught 4Z, okay so the answer is 2. So, the part C has answered 2. So, the number of intermediate fields which Galois group K or L is isomorphic is Z naught4Z is exactly 2.

(Refer Slide Time: 22:05)



So, let me now continue to the next problem, I want to do two more problems. So, all these problems are hopefully giving you a more comfortable picture of what we have done so far. And they illustrate the theory that we are trying to develop. To study field theory, we are reducing it to some questions on group theory. And then you will see much more substantial applications later, but these are all nice problems to know how to solve because they help you understand the theory well, okay.

So, the next problem that I want to do is a problem that I remarked on earlier. So, this is the problem is asking to show that, give an example of a field extension of a finite extension of fields that is K over F, such that there are infinitely many intermediate fields. So, you want K over F finite, but this will have infinitely many intermediate fields.

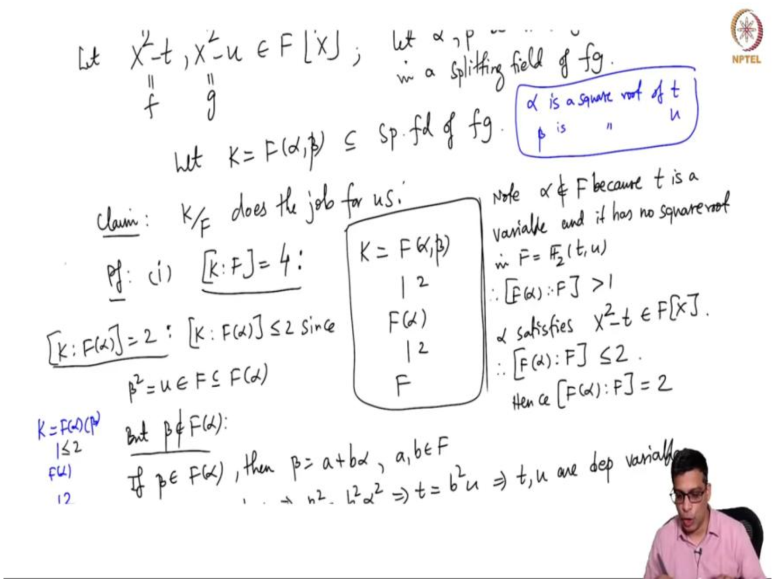
So, I gave, immediately after proving the Main theorem we showed that if you have a separable finite extension, there are only finitely many intermediate fields. So, we know that any example that can have this property has to be inseparable. So, immediately, we have to go to characteristic prime, not only that, we have to go to infinite fields of characteristic prime because finite fields are perfect. So, any extension is separable. So I will give you the example that works.And I will explain to you how we prove the statement.

So, we take F to be, F2 bracket t comma u. So, these are variables. So far, we have looked at rational function filled in one variable to construct some examples of normal non-Galois extensions, here we are taking rational functions and two variables. So let me naught belabor this point, but the elements of this are ratios of polynomials into variables. So this is nothing but a quotient field of F2 square bracket t.

So, you take polynomial in two variables and take its quotient field, that means elements of F, capital F, are simply going to be ratios of polynomials F by G, where F and G are polynomials in two variables. And in this what we do is, consider X square minus t and X square minus u. Remember, in the earlier example of a normal non Galois extension, we took one variable and this particular polynomials. We take now two. So we are taking two polynomials over capital F, t and u remember are constants because they are in capital F.

What do we do is we let alpha, beta be roots of, let us call this, F respectively in a splitting field, let us say of FG. So, I can only construct a bigger field where they both split. So, now within that, so alpha is the root of x square minus 3, beta is root of x squared minus 2, so alpha squared is a t, beta square as u.

(Refer Slide Time: 25:55)



So now, let K be F alpha beta. So, this is inside that splitting field. This is in fact the splitting field if you think about this for a bit, but I do not care. K is this. So, now my claim is K over F does the job for us. K over F is the finite extension which has infinitely many intermediate fields. So, let us prove this. This is a finite extension and it will have infinitely many intermediate fields.

Okay, let us prove first that, first claim, that it is a finite extension in fact, it is a degree 4 extension. So, this is very easy, let me just quickly do this. But in the process, I want to maybe explain carefully what is required. So K colon F is 4 is the claim. So obviously, we know that K is F alpha beta, the trick is to do F alpha and then F.

So, if I show that both of them are 2, then I am done. So, the proof is basically here, I am going to write this here. So, we first note that alpha is naught in F. Because t is a variable and it has no square root in F, which F2 t, u, I mean, this is a broad statement we mentioned before, right? Because you cannot find the ratio of two polynomials, square is t for degree considerations.

So, basically, let me write it here alpha is a square root, loosely speaking, of t, beta is the square root of u. So, they don't exist in capital F. F itself does naught contain square roots of t or u. So, alpha is naught in F. So, that means F alpha colon F, is strictly more than 1. On the other hand, alpha satisfies alphaX square minus t, which is a polynomial in FX. So that means, F alpha colon F is less than or equal to 2 right, because it satisfies the degree 2 polynomial.

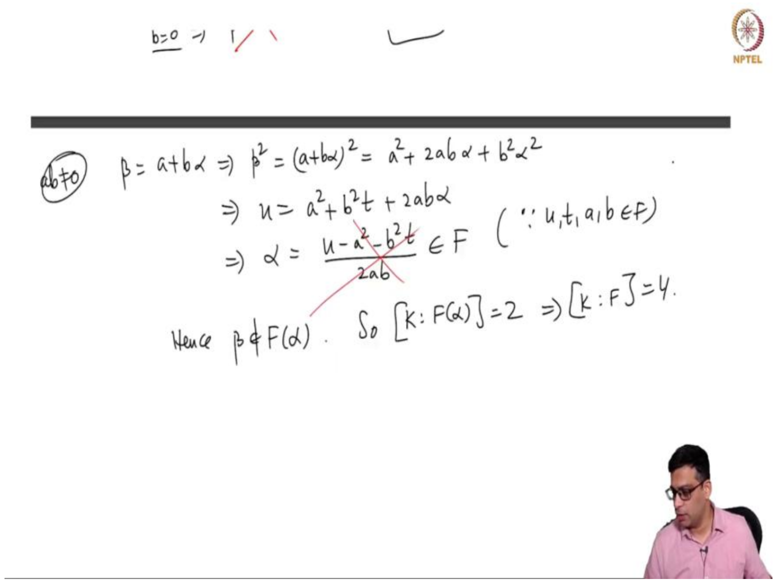
So, its degree of alpha is at most 2, maybe it satisfies a linear polynomial, also in which case degree will be 1, but it does not. So, hence,so this is 2. So, the second part is to argue that K colon F alpha, so I am sorry I am sort of writing it all over the place, but I want to keep everything in front of you. So, first note that, F alpha is a degree 2 extension of F. So, now, first note that, so I want to prove this, but we do know that since beta square is, which is of course u, is an F which is an F alpha. So, note that K is actually F alpha bracket beta. So, we do know that beta generates K over F alpha, it satisfies a degree 2 polynomial, namely x square minus u, which lives in capital F in fact, so it certainly lives in capital F alpha. So, let me draw some lines so, this is the original picture, okay.

So this can be at most 2, right, because it does satisfy our degree 2 polynomial over F alpha. So, now the question is it 2 or 1? So, we now claim beta is not in F alpha, then these are distinct fields, K and F alpha will be distinct fields and hence it will be 2. So, why is beta naught in F alpha? So, this is because suppose beta is in F alpha. If beta is in F alpha, then we can write beta, because F alpha is a degree 2 extension, beta can be written as sum A plus B alpha, where A and B are in F. So, this is a standard argument, but I will work through this because first time I am doing this, or maybe I have naught explicitly done this before. So, we have this, right, because F alpha is a vector space or capital F with basis 1 and alpha, so we have this.

So now, let us square both sides. So, beta is this. And of course, I mean, let me first get rid of trivial cases. If A is zero, this implies beta equals B alpha, this implies beta square equals B square alpha square, this implies beta square is u, alpha square is t, so t equals B square u. But this means, t and u are dependent variables. But that is not the case, t and u are independent variables, I should really write this. They are independent. They are independent variables.

So, there is no polynomial that is 0, if it has nonzero coefficient. So, this cannot happen. So, A cannot be zero. On the other hand, if B is 0, that means beta equals A. But this is in Financial so this is also naught possible, because we already agreed that alpha is naught in capital F similarly, beta is naught capital F. And hence we conclude that a B is nonzero.

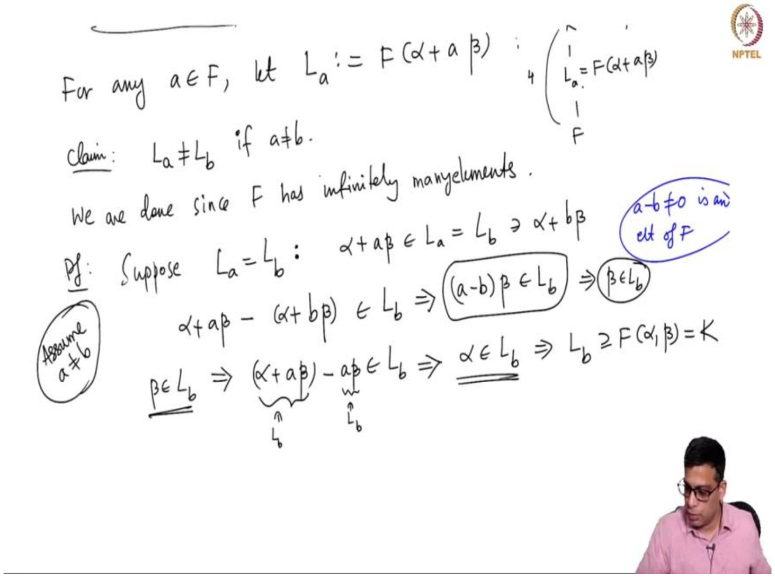
(Refer Slide Time: 32:35)



So we are going to use this later, now, beta equals A plus B alpha. So, let us square both sides. So, we get B square equals A plus B alpha whole square, which is A square plus 2 A B alpha, plus B square alphasquare. This implies u, which is beta square is equal to A square plus B square t, because alpha square is t, plus 2 A B alpha. But that means alpha equals u minus A square minus B squared t divided by 2 A B, because A B is nonzero, that we have established, this is a valid element of the field F, because u, A, B, t are all in F right. So, since u, t, A,B are in F.

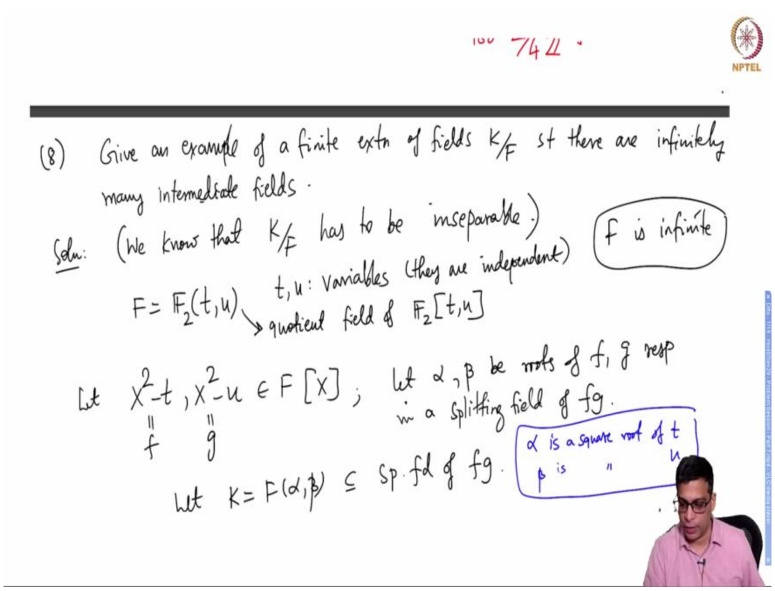
So, this is not possible again this is a contradiction, alpha is naught F. So, this is not possible. Hence, beta is not in F alpha. So K colon F alpha is 2. So I am justified in putting a 2 here. So, that means this is also 2,. So hence, K colon F is 4.So, it is a finite extension. Next step is to show that it has infinitely many intermediate fields. So let us do this.

(Refer Slide Time: 34:22)



So let us do this. So for any A in capital F, let L sub-A be defined as F of alpha plus A beta. F sub-alpha plus A beta. So of course, there is an intermediate field of the extension. So K is here, which is F alpha beta.La is here, which is F alpha plus A beta and F is here, so this is a degree for extension. So, we are going to claim now that these are all distinct fields. So La, is different from Lb, if A, B are different.

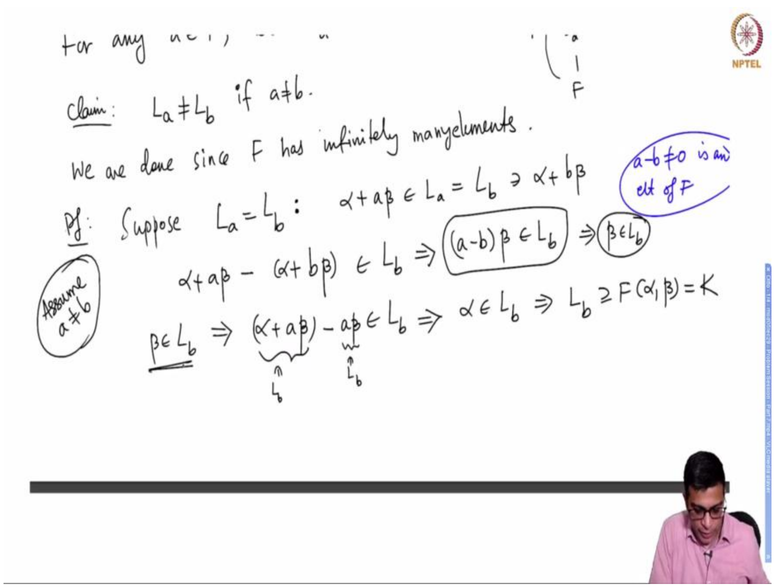
(Refer Slide Time: 31:30)



La is not equal to Lbif A and B are different and hence there will be infinitely many, okay. So, also, yeah, F has infinitely many elements, so we are done since F has infinitely many elements. Note that F2 has finitely many elements, but capital F is F2 round bracket t,u. So, you can take any polynomials of arbitrary degrees, so F is certainly in finite field. Remember in fact, if you take a finite field you cannot hope to get an example with this property, meaning having infinitely many intermediate fields because finite fields are perfect. So, it has to be in finite but that it is, because you can take arbitrary high arbitrary high degree polynomials.

So, you can take A and B to be A and B from infinitely many elements and La and Lb are different if A and B are different. So, La I mean, in fact, La is never equal to K or F, but you don't care because maybe for one L, La is K for another A, La is F, but all the other things are going to be proper intermediate fields.

(Refer Slide Time: 36:19)



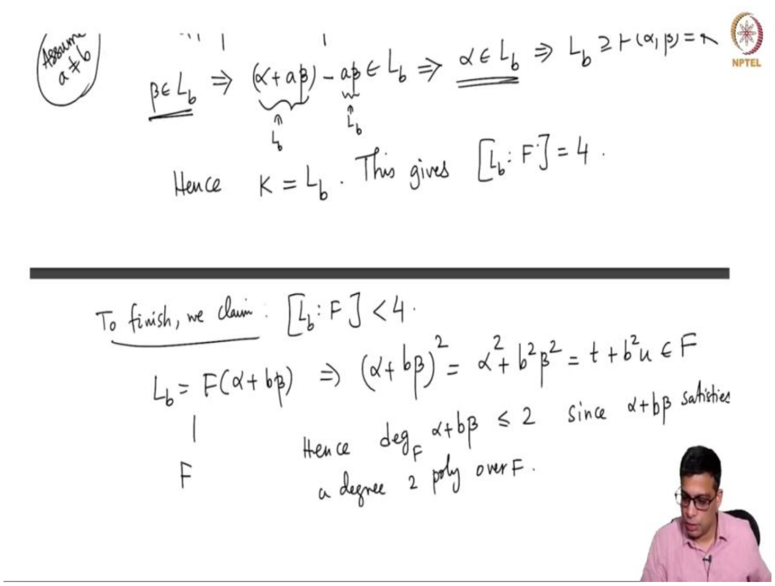
Why is this? So, the proof is, sothis is a simple calculation I will show you now. So, suppose La equals Lb, then what is the problem that will happen? So, then La remember is F of alpha plus A beta. So, this is an La, sothis is an Lb. So, that means alpha plus Aa, A beta is in Lb. But then we do know that alpha plus A beta minus alpha plus B beta is in Lb because, Lb also contains alpha plus B beta. In fact, Lb is generated by alpha plus B beta. So, the difference between these two is in Little bit. But what is the difference between these two?

You get your a times beta minus b times beta, so alpha cancel, so, a beta minus b beta is an Lb, that means, a minus b times beta is in Little bit. But, so assume,of course I should say assume a isnot equal to b. So, a minusb is nonzero, is an element of Financial, of course, because the a and b are elements of F. So, A minus B can be canceled to get beta as in Lb, this is the thing that I am after. So you divided by a minus b or multiply by a minus b inverse, you get beta is equal to Lb. Now, I claim that this is not possible.

So, if beta is in Lb, this means alpha plus a beta, which is anLb of course, minus a beta is an Little bit. Because, this is anLb and this is an Lb. Alpha plus a beta is in Lb by hypothesis and a beta is in Lb so times beta is in because a is also an Lb. So, A is an element of F so, it certainly in Lb. So, this difference is in Lb that means, alpha is in Lb.

That means both alpha and beta are in Lb. So, in fact what I will now show is that Lb, okay, o, actually I need to do a little bit more work, but immediately we conclude that Lb contains both A and B and it of course contains F, so it contains K. So, beta is in Lb, alpha is in Lb. So, F is of course in Lb. So, F alpha B is beta is in Lb but F alpha beta is K. And hence, K equals Little bit, right, because Lb is an intermediate field. So, this gives, by what we have already showed, this gives this, but because K is a degree 4 extension.

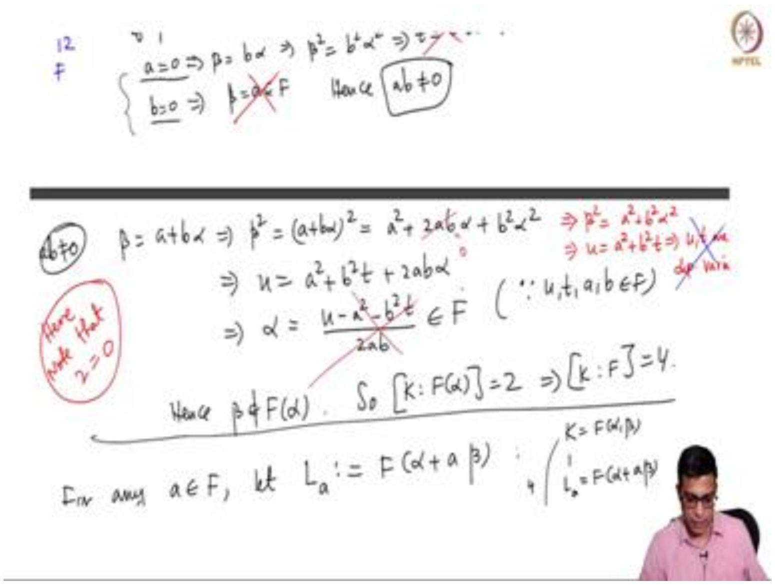
(Refer Slide Time: 39:27)



And so to finish, we claim now, actually yeah, I didn't think we need this but we need this. If Lb colon F is 2,it will not be 4. So, basically what I want to claim is this is less than 4. Why is this?

So Lb recall is F. This is very easy. Alpha plus b beta, right? But what is alpha plus b beta whole square? This is equal to alpha square plus 2 b alpha b.

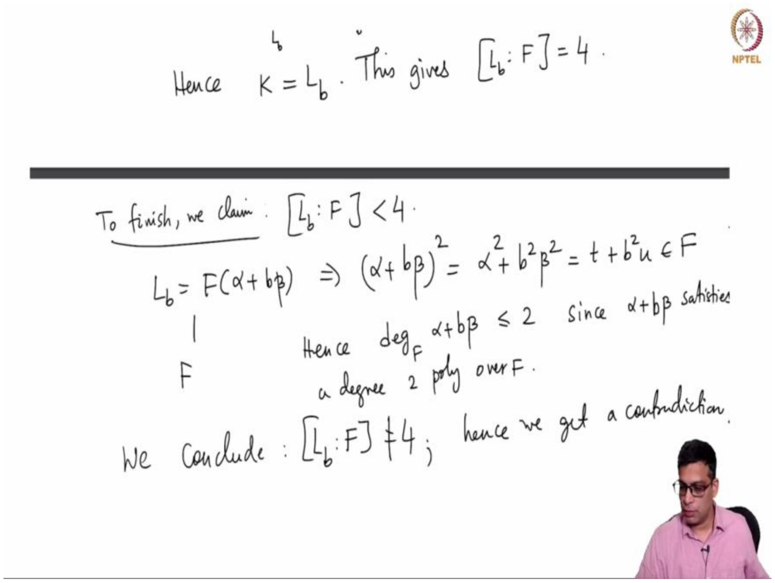
(Refer Slide Time: 40:36)



So, actually now recall that we are in a characteristic 2 field. So, that means this is just, I sort of did some unnecessary work here, because this 2 is 0, so I think there is an error here. So, here note that, so I think that simplifies this calculation. So, you have beta square is equal to a square plus b square, so you don't need to do this. But basically, there is a mistake here. So, this gives me beta square equals a square plus b square alpha square. But that means u equals a square plus b square t. But that is a violation of the fact that u and t our independent variable. So, because this relation makes they are independent, this equation forces them to be dependent variables, but that is not possible because u and t are independent variables.

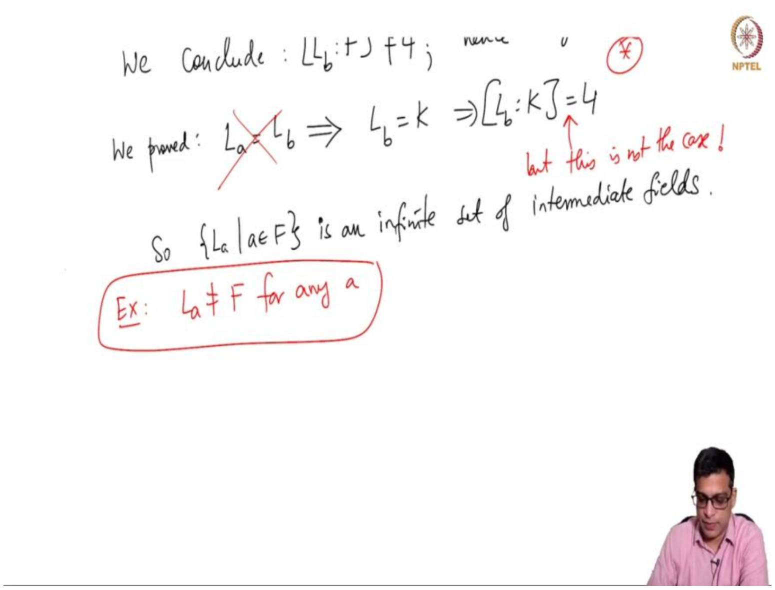
So, in fact I did not need to do all this work, sorry about that. So, there is a small error here, I did more than what is required, I can just use the fact that this must be zero and directly show that I get a dependence relation between u or t, which is not possible. So, I did more work, but I hope that is fixed, that you understand the error and you realize that we nevertheless have the result that we want. So, go back to that if needed.

(Refer Slide Time: 42:05)



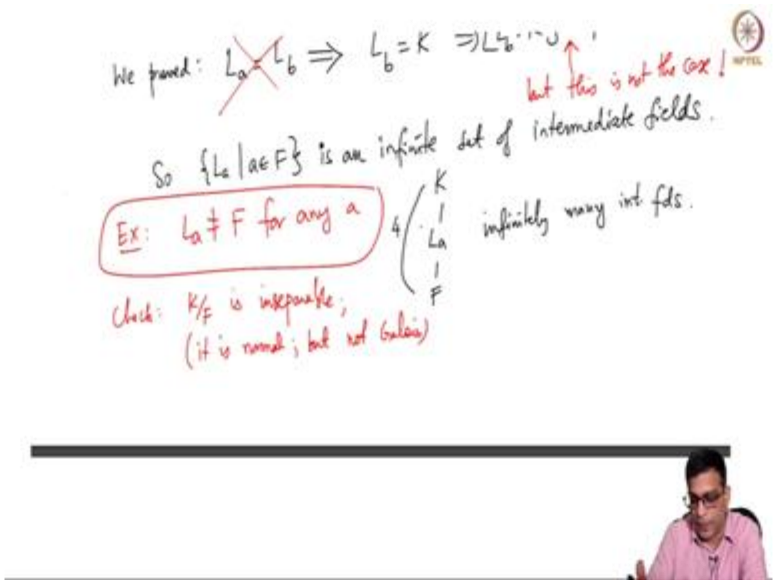
So, now, let us come back here. So, what we have is alpha plus beta b, b beta whole square is this, but alpha square is t, beta square is u. So, you have t plus b square u and this of course is an F. So, hence degree over F of alpha plus bbeta is less than or equal to 2, because alpha plus b beta satisfies a degree 3 degree 2 polynomial over F. So, this concludes the proof that, so, we conclude that Lb cannot be K because, so, yeah this contradict this. So, this we conclude from this argument that Lb colon F is naught 4 and hence, we get a contradiction.

(Refer Slide Time: 43:02)



So, I am sorry, I just sort of messed up at the end here by confusing you with notation, but basically this is the contradiction. The contradiction is that if La and Lb are equal, so what we have essentially proved La equals Lb, implies Lb equals k, this implies Lb colon K is 4, but this is naught the case and hence La cannot be equal to Lb. So, the set of La is an infinite set of intermediate fields.

(Refer Slide Time: 01:05)



Okay. So, this, I mean, you can separately prove has an exercise that La can never be equal to K; sorry F, for any a. You can prove this separately because using the same kind of arguments that we used here in proving that, for example, K is not equal to F alpha. Similar arguments will give you this. But I claim that this is naught relevant. At most you can have one La equal to F, but because they are all distinct, other things must be proper intermediate fields.

So, even though this degree is 4, there are infinitely many intermediate fields. So, this is a weird thing that happens for inseparable extensions. Of course, k over F is inseparable. So, also check K over F is inseparable. Because is this polynomial whose splitting field, it is normal but not galvois because it's not separable, it's not Galois.

It is normal because it is a splitting field of these polynomials, that you can check. And those elements are inseparable. So, theseare inseparable extension, which is finite yet admits. So think of theseLa'sare sitting inthe middle horizontally, right, you cannot compare them because there is not enough room here. There is degree 4 extension, but they are all horizontal, they are all in the same level in some sense.

So, this shows that you can have a finite extension with infinitely many intermediate fields. So, let me stop this class here. In the next class, we will do one more problem which illustrates Galois' Main theorem, and then we go on to applications of Galois theory. Thank you.