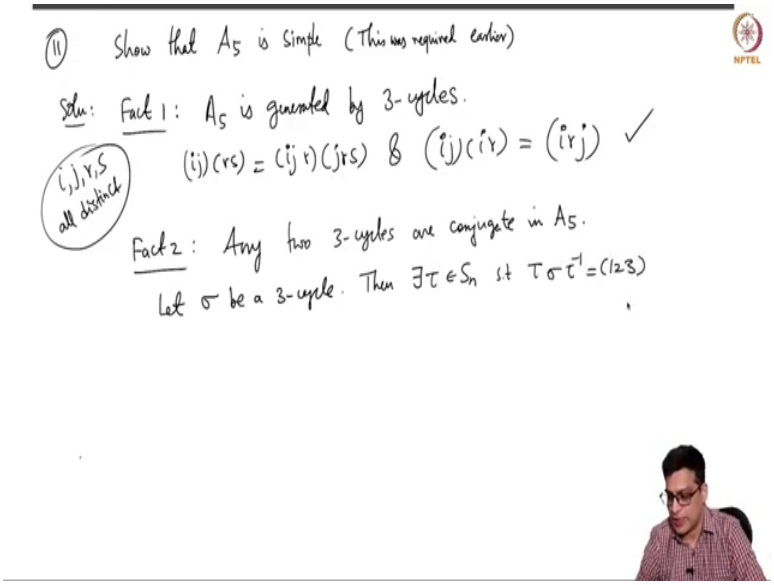
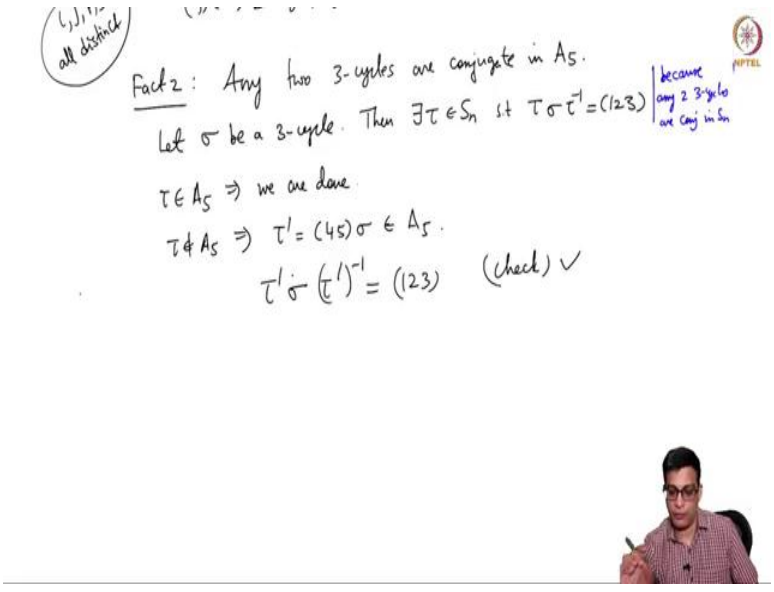
**Introduction to Galois Theory**
**Professor Krishna Hanumanthu**
**Department of Mathematics**
**Chennai Mathematical Institute**
**Indian Institute of Science, Bangalore**
**Lecture 49**
**Problem Session - Part 13**

Welcome back, this is the final video of the course. So, we are now doing some problems before that we finish the main content of the course. And the problem sessions are to illustrate the various features of the theorems that we have proved.

(Refer Slide Time: 0:42)



And now, in fact the last class here is not really a problem session though I continue to call them problems, these are more like theorems, which I wanted to record here because these are useful to keep in mind and I will not give you a complete rigorous proof of this, I will give a rigorous proof of the next theorem, but for now, this one I will just quickly illustrate I mean there are several proofs of this fact. And this one I am going to give is a fairly computational statement, which I will let you work out for yourself the details of which I will leave for you.

So, show that A5 is simple. So, this is required for us, this was required earlier when we discussed the insolvability of quantix. So, I wanted to just give you a hint of how to do this, many of you would have seen this in a previous course in group theory. So, first fact is A5 is generated by 3 cycles.

So, the basic idea is that if you have A5 consists of even permutation. So, for example, it could be a 3 cycle in which case it is already there, but the only real case you have to consider is ij times rs, this is of the form ij times, ij r time times jrs. So i, j, r, s are all distinct. So, if you have 2 distinct permutations transpositions, their product is like this.

On the other end, if you have ij times ir, this is irj. So, any 2 transpositions like this will give you irj. So, and then for you can check that for permutations, or you can pull them up by any even permutation is a product of an even number of transpositions, you take 2 of them at a time and show that they are all products of 3 cycles like this.

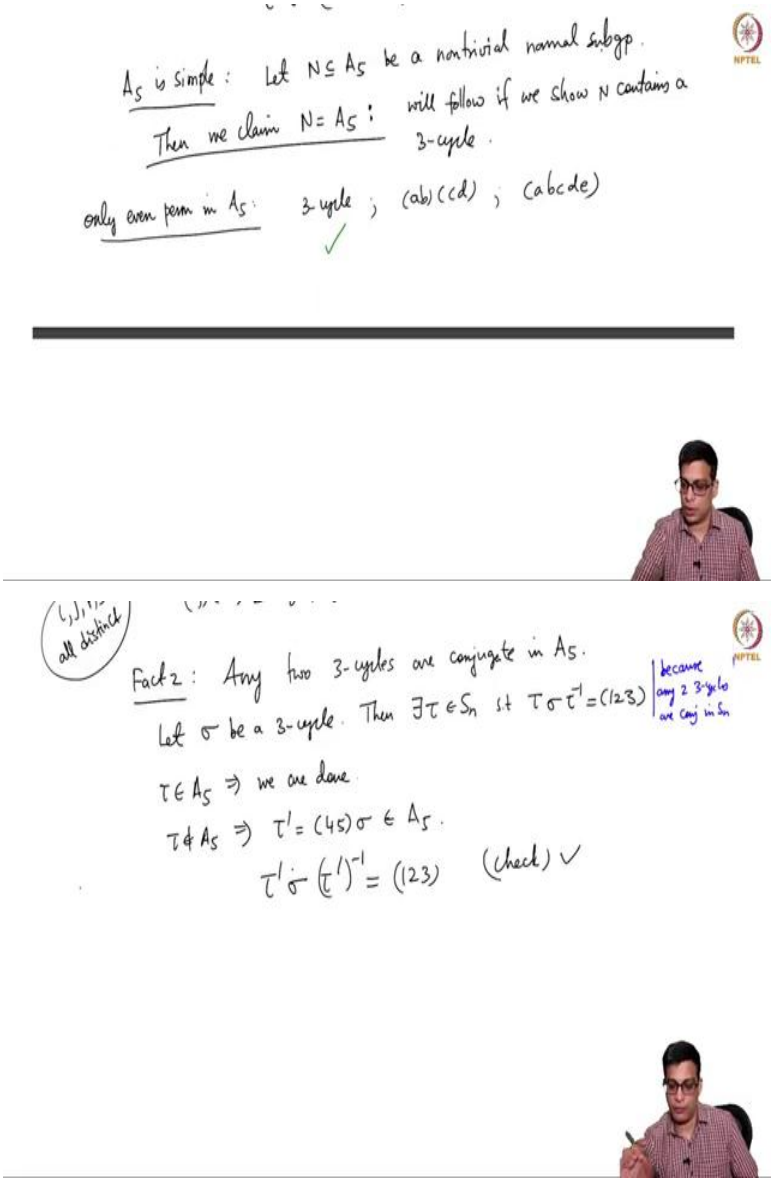
Fact 2, any 3, any 2 3 cycles are conjugate in A5, that means there is an A5 element which conjugates the 2 elements. Of course, they are conjugate in S5, but it requires a little bit work to show that they are conjugating A5. So, let sigma be a 3 cycle, we know that there exists a tau in Sn such that tau circle, there is a tau in Sn such that tau sigma tau inverse is 123.

So, we will show that every 3 cycle is conjugate to the specifics 3 cycle 123. So, this is because any 2 3 cycles are conjugate in Sn. So, in fact, any 2 permutations which have the same cycle decomposition are conjugate in Sn, so, conjugacy classes in Sn are determined by the cycle decomposition. So, this is a general fact.

If tau is in A5 we are done. If tau is not in A5, what we do is that means tau is odd, that means tau is a product of odd number of transpositions. So, let us take tau prime to be 4 5 times tau. So,

then tau prime is in A5. So, now, you can quickly check the tau prime sigma tau prime inverse is 123. So, check this. So, sigma is conjugate 123 via an even permutation.

(Refer Slide Time: 4:58)



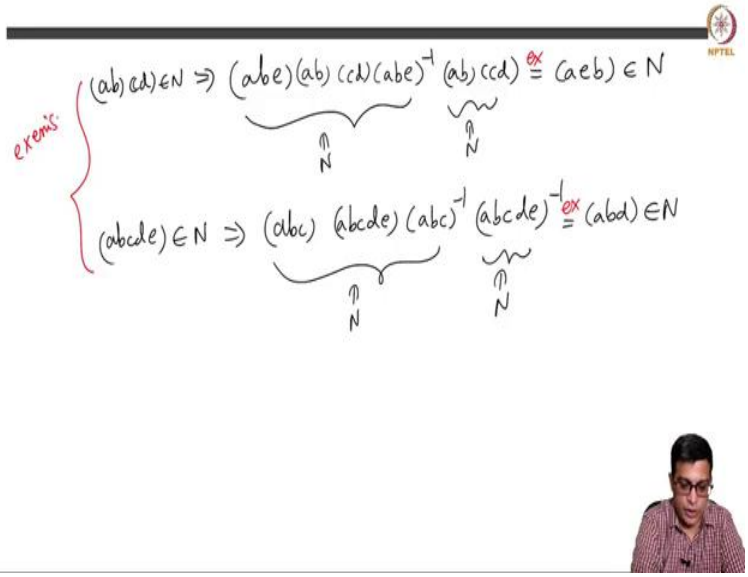

And now fact 3, final fact, that yeah so this is not really a fact but proof of the simplicity A5 is simple. What is simple by the way I should have recalled for you. Let N be a non trivial normal subgroup. So, simple means the only normal subgroups are the group itself and the trivial group.

Suppose, N is non-trivial, then we claim that N is A5, the proof will follow, this will follow if we show N contains a 3 cycle. If it contains a 3 cycle by fact 2, it contains all 3 cycles because N is

even, sorry N is normal. So, every 3 cycle is a conjugate of a 3 cycle by an A5 element that means, that conjugate must land again in N.

So, N contains every 3 cycle and by fact 1 A5 is generated by 3 cycles. So, N will be A5. So, now, N consists of even permutations because N is in A5, only even permutations in A5 are of 3 kinds, 3 cycle, products of 2 cycles like this disjoint 2 cycles or A5 cycle. In this case of course, we are already done. If N must N is non-trivial, so it must contain either this, this or this non-trivial element if it contains that that is already the claim.

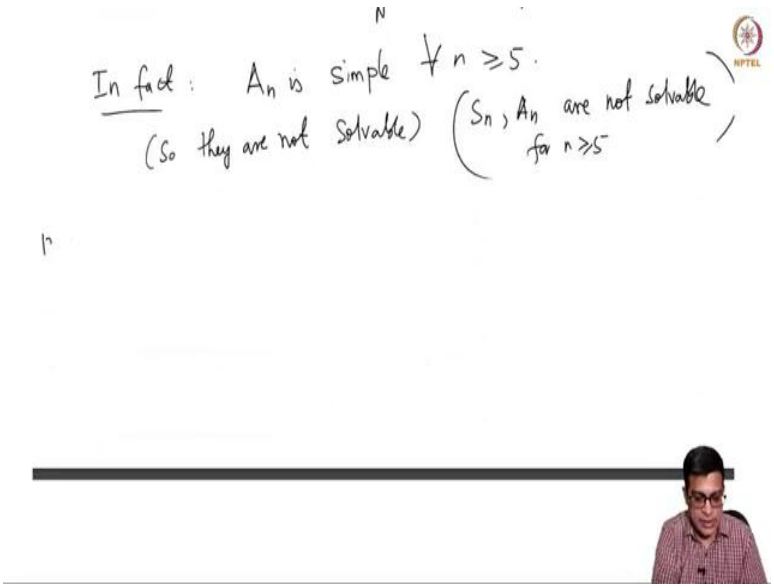
(Refer Slide Time: 6:49)




If ab cd is an N. So, I will not write this full detail, but you take abe is the, there are, there is a fifth index, so, abe times ab times cd times abe inverse times ab times cd, I mean this is just a mess, but you can quickly check. So, this is in N. So, this is in N because N is normal, this is in N, so the product is in N.

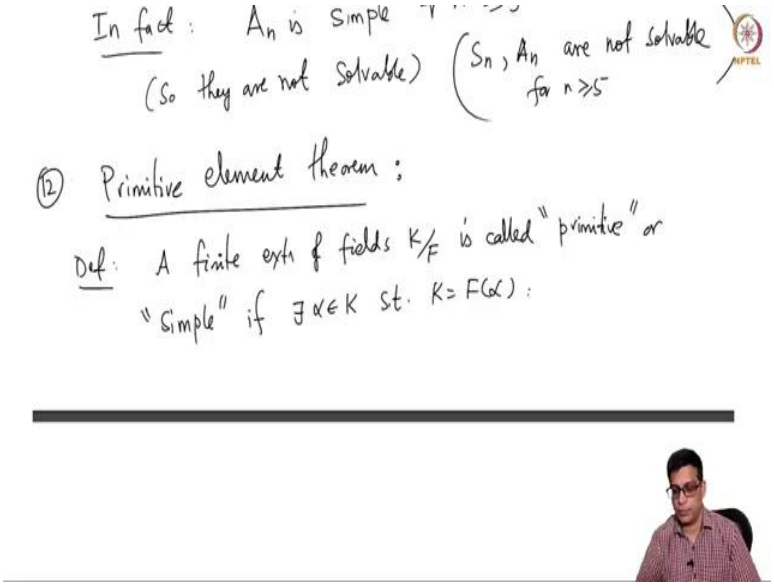
On the other hand, if abcde is an N that means, I will write it down here you can check this abc times abcde times abc inverse times abcde inverse. So, I checked this you can check that, this is an N because N is normal, this is in N because N is in subgroup. So, this is actually abd which is in N, this is also an exercise. So, these are just straightforward exercises to check that N must contain a 3 recycle. So, because N is normal, it contains all 3 cycles. And because A5 is generated by 3 cycles, N itself is equal to A5. So, A5 is simple.

(Refer Slide Time: 8:17)



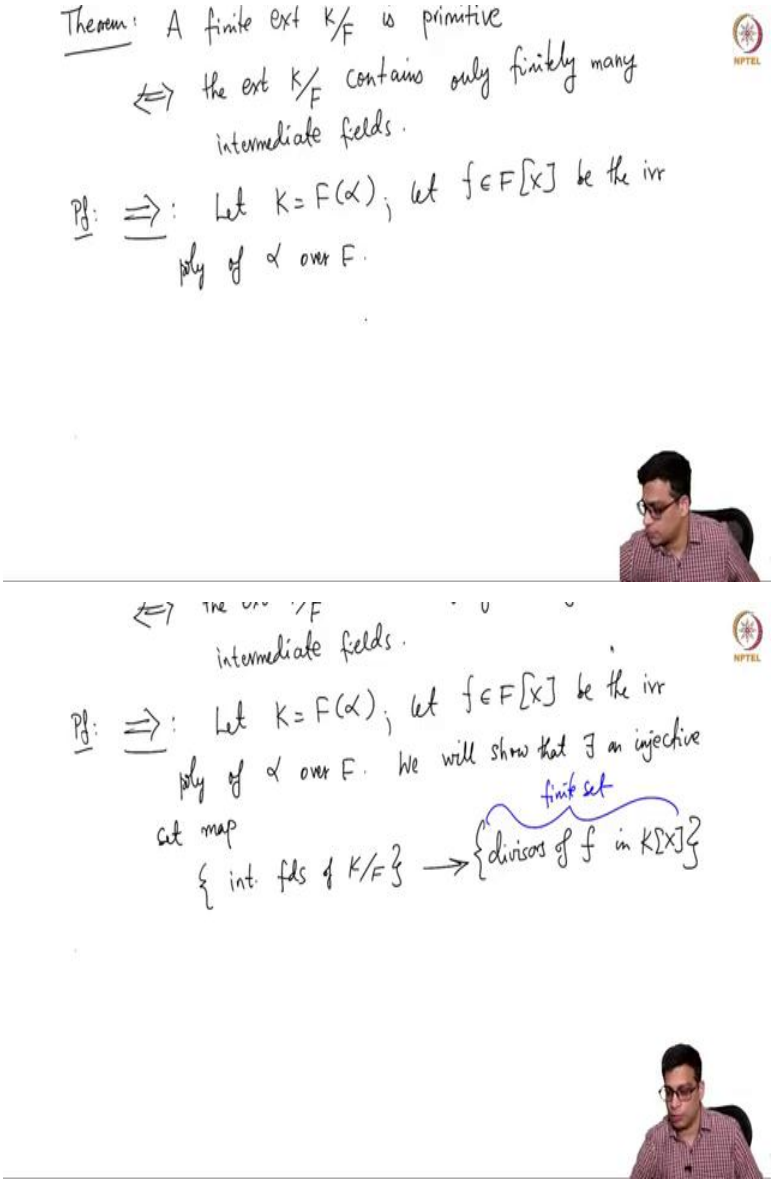

So, in fact, this requires more work An is simple for all n greater than equal to 5. This is a theorem in group theory, but this requires more work, so one can show that all Ns are simple. So, in particular, we know that they are also non abelian they are not abelian. So, they are not solvable. So, that means any polynomial with N as a symmetry, as a Galois group is not solvable. So, hence any monomial with Sn as Galois group are also not solvable. So, An for n at least 5. And Sn cannot be solvable because if it were solvable, its subgroup n would be solvable but it is not.

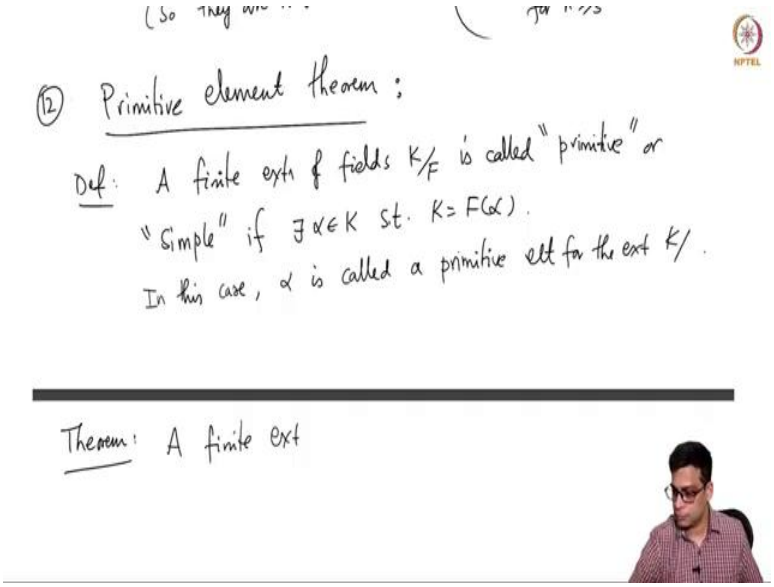
(Refer Slide Time: 9:13)



So, the final thing that I want to do, I will write this as a theorem mass problem, but it is a famous theorem in field theory called primitive element theorem. So, in order to prove this, let me just state the definition of a primitive extension first. So, definition, a finite extension of fields K over F is called primitive or simple or another word for it is simple; if there exists alpha in K such that K is generated over F by a single element. So, now these are very useful extension because it is often easy to work with such things. Now, the theorem that I want to give you at the end of this course is the following.

(Refer Slide Time: 10:08)



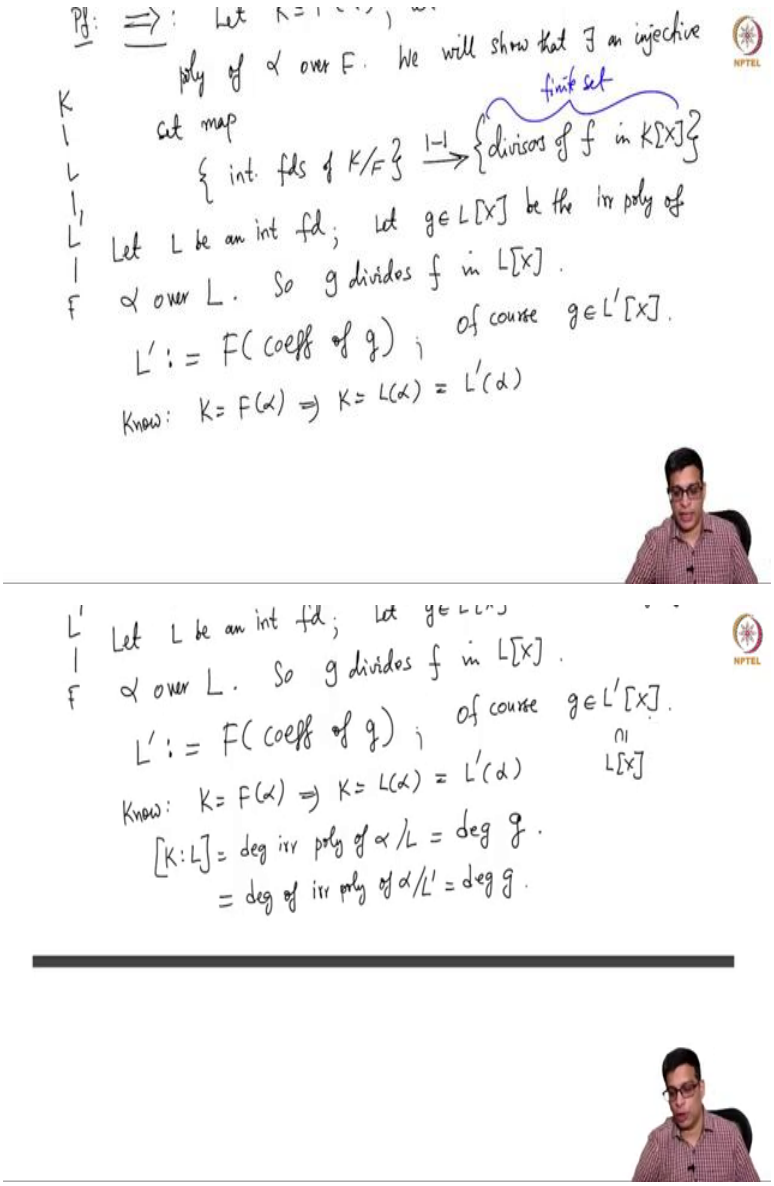



A finite extension. So, and the element alpha is called a primitive element, in this case alpha is called a primitive element for the extension. Now, the theorem is that a finite extension is primitive if and only if the extension K over F contains only finitely many intermediate extensions, intermediate fields.

So, primitiveness is completely determined by the number of intermediate, fields if there is only finitely many it is primitive and if it is primitive conversely there are only finitely many. So, let us prove both directions, the forward direction. So, let K be equal to F alpha and let F be the irreducible polynomial of alpha over F.

We will produce, will show that there exists an injective set map, injective set map from intermediate fields of K or Q, sorry K or F to divisors of F in K X. Of course, this is a finite set because F is a polynomial it can have at most finitely, I mean it can have only finitely many divisors, you look at its irreducible factorization and you write down all the products among them that will give you the divisors.

(Refer Slide Time: 12:34)



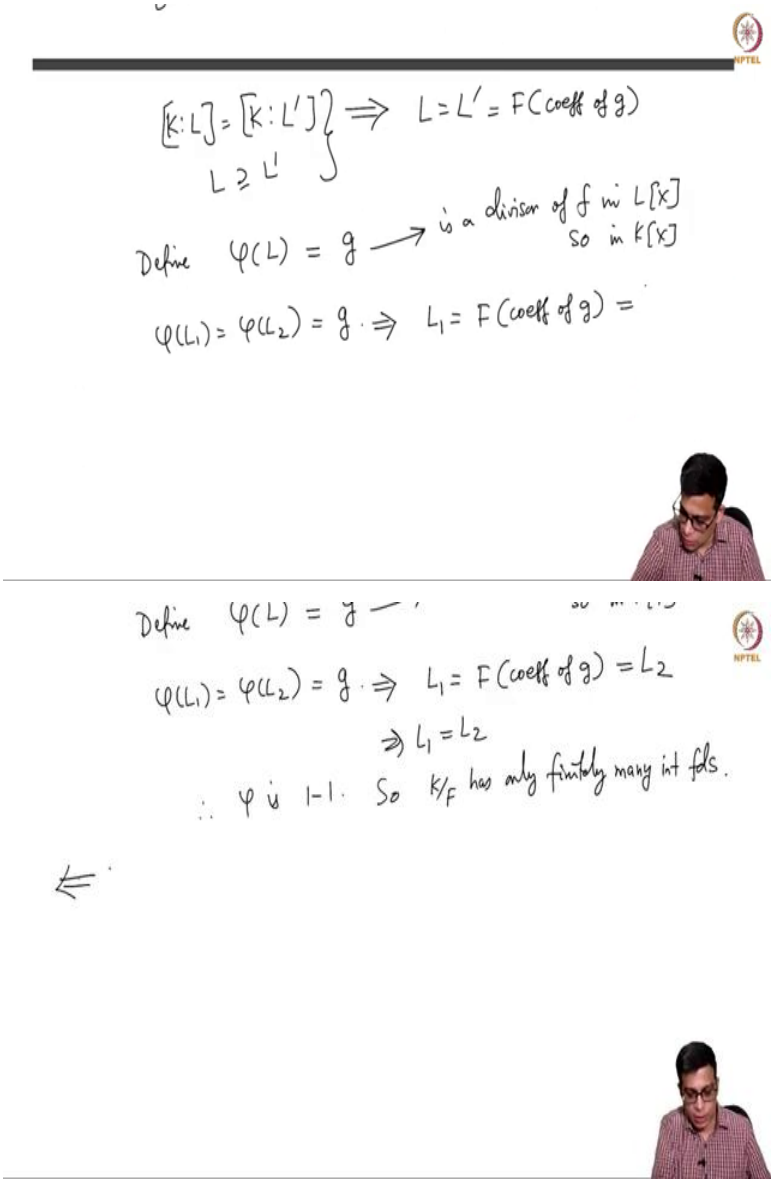

So, if there is an injective map from here to here, this is a finite set though this will be a finite set. So, towards this end, let L be an intermediate field, let L be an intermediate field, then let g be a polynomial in L be the irreducible polynomial of alpha over L. So, you have K L F, F is irreducible polynomial over capital F, g is the irreducible polynomial over capital L.

So, of course, g divides F in L X because F is already in F X, so, it is in L X. So, g is the irreducible polynomial, so g divides F. Now, define a new field L prime which is F adjoint coefficients of L of g. So, g is a specific polynomial I only take its coefficients and define the field generated by them.

So, of course, g is in L prime X by definition and now, we know that K is F L, F alpha, so this implies K is L alpha as well as L prime alpha. So, of course, it is generated by alpha over a small field means it is generated over L and L prime also by alpha. So, K colon L is the degree of irreducible polynomial of alpha over L which is degree g.

But at the same time K colon L is equal to the degree of irreducible polynomial alpha our L prime which is also degree g because g lives in both L prime as well as L. So, it is the irreducible polynomial of alpha over both L and L prime.

(Refer Slide Time: 14:44)



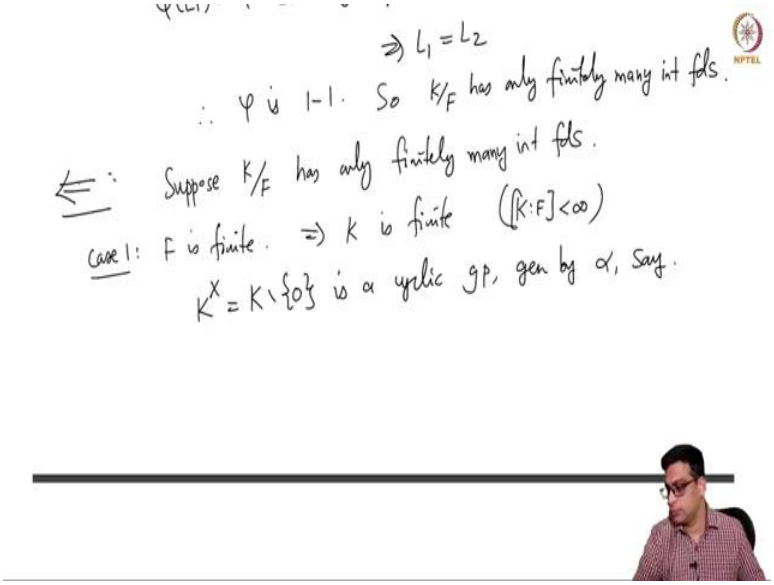
But that means, K colon L, sorry K colon L prime is this, is equal to K colon L prime. This implies L equal to L prime, since L contains L prime. So, L certainly will contain L prime, they have the same degree, K has the same degree over both of them. So, that means L equal to L prime.

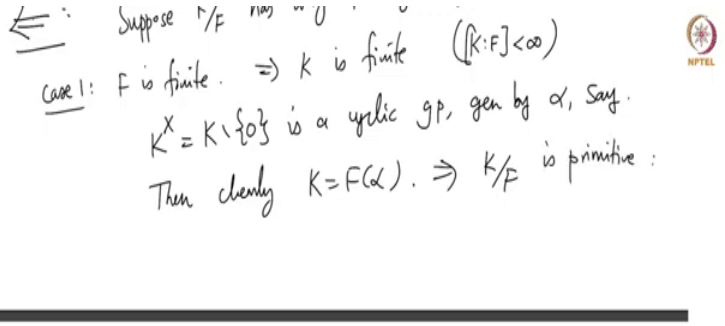
So, now that means, L is determined by the coefficients of g. So, basically now the map is clear phi, so, define phi of L to be g. So, take an intermediate field take its irreducible polynomial of alpha over that intermediate field and take that as the image. So, of course, g is a divisor of F in L X and hence in K X.

So, g does belong to this set, but now, suppose phi L equals, phi L 1 equals phi L 2 if phi L 1 equals phi L 2 that let us say g. That means, g is the irreducible polynomial of alpha over L 1, G is also the irreducible polynomial of alpha over L 2. So, L 1 is equal to by what I just showed L is equal to F adjoint coefficients of g.

So, L 1 is F adjoint coefficients of g which is also L 2. So, L is determined by the coefficients of g. So, that means L 1 equals L 2. So, phi is 1 1. And so, K over F has only many intermediate fields, very good. So, that proves this one direction. Now, let us suppose this.

(Refer Slide Time: 16:50)

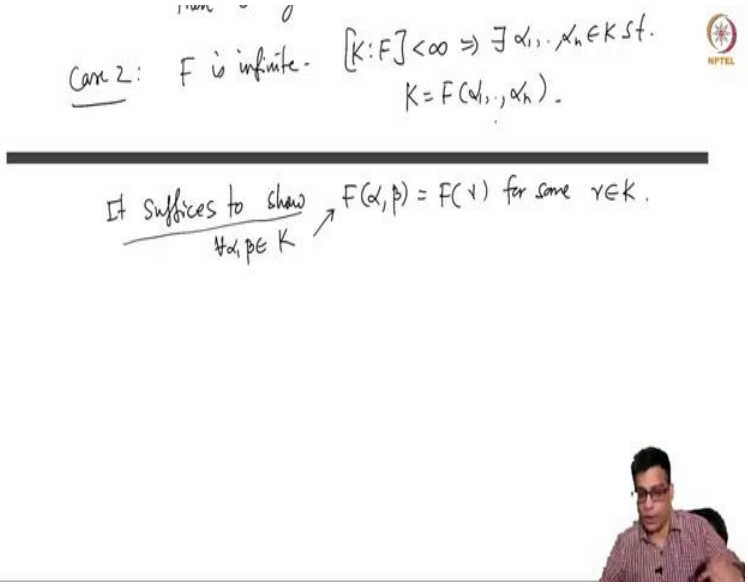





So, suppose K over F has only finitely many intermediate fields, our goal is to show that K over F is primitive. So, what we do is first consider the case that F is finite. This implies K is finite, because K colon F is a finite number we are working with a finite extension. So, K colon F is finite, if the base field is finite the bigger field is also finite.

But then K star is a cyclic group generated by alpha say. Then every element of K nonzero element is a power of alpha. So, in particular, so clearly K is F alpha, in fact, you do not need any polynomials, any complicated polynomials just the polynomial alpha power I will do, every element of K is a power of alpha or it is 0. So, K over F is primitive.

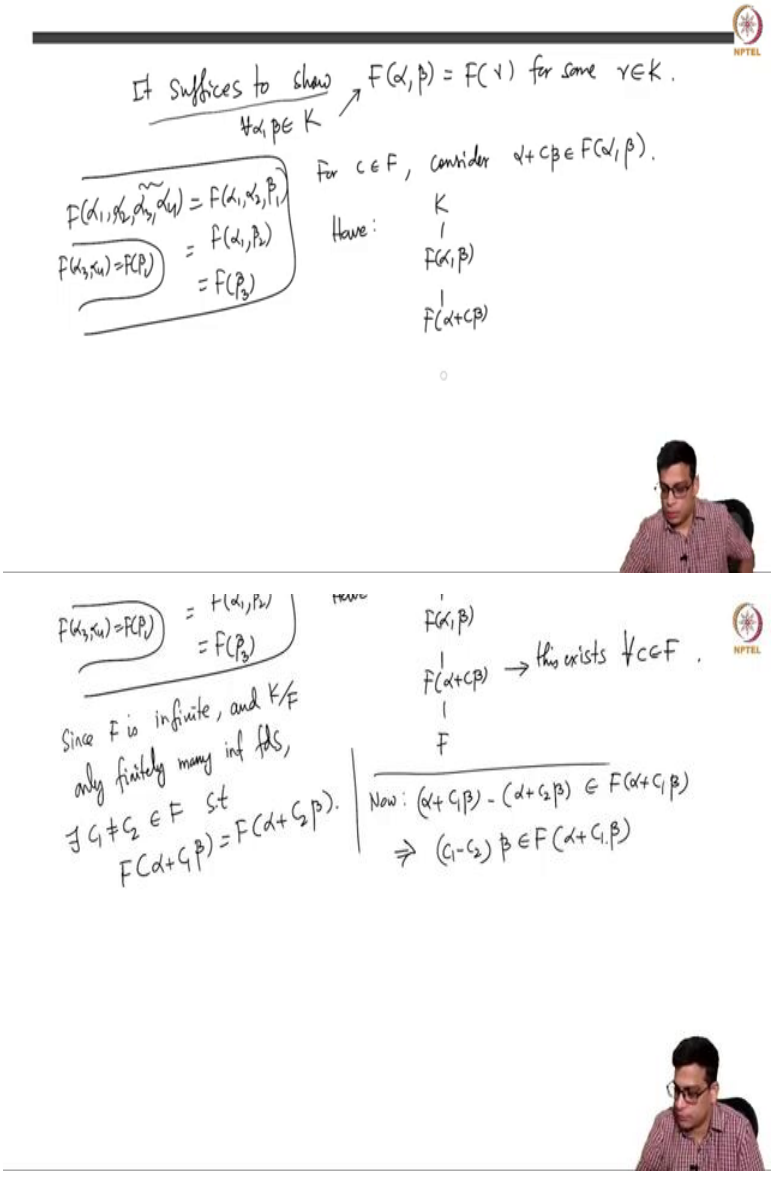
(Refer Slide Time: 18:08)




So, we assume now, assume F is infinite. So, this case is what we want to now consider. So, clearly it suffices to show, since K colon F is finite there exists alpha 1 through alpha n in K such that K is. See, there is no problem with finite generation, primitiveness means, single element will generate, we do have this.

So, it suffices to show F alpha comma beta is equal to F gamma for all alpha beta in K, F alpha beta equals F gamma for some gamma in K. So, if you can go from 2 to 1 then you can by induction go from 3 to 2 and first you can go from n minus 1 to n to n minus 1.

(Refer Slide Time: 19:27)



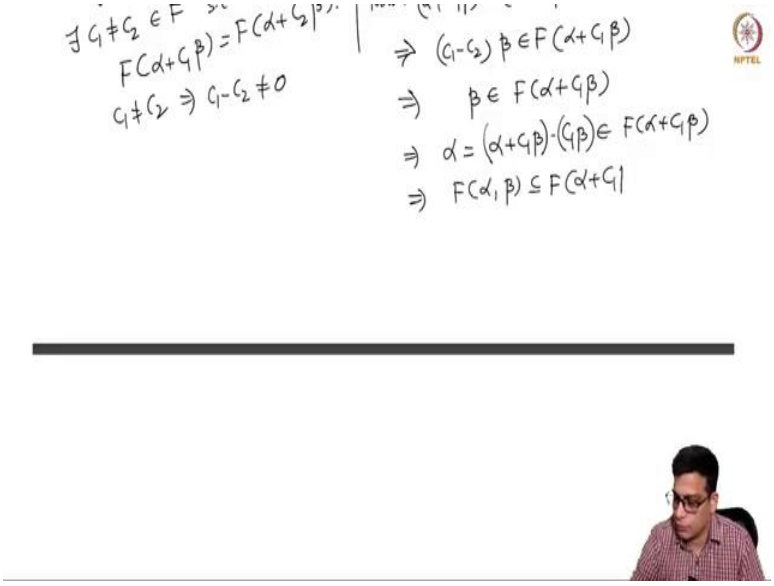

So, if you have, so then, this can be collapsed into 1, because if alpha 3 alpha 4 is F beta 1 by this statement, you can do this then you can do one more time alpha 2 alpha, alpha 2 and beta 1 and finally you get beta 3. So, just a simple trick. So, it is all that matters is if you take 2 elements, then you can reduce it to 1 element.

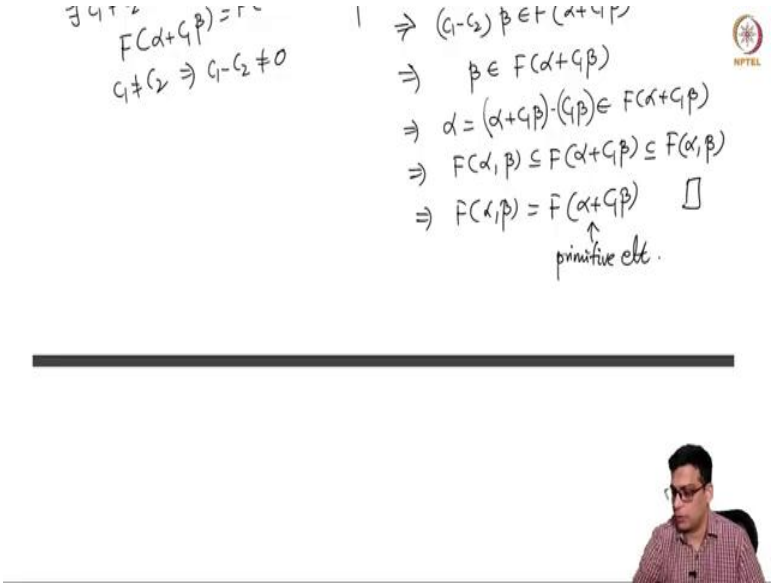
Now, for C in F, for any element in the base field, consider alpha plus C beta in F alpha beta. So, I am taking an arbitrary pair alpha, comma beta in K and taking the field F alpha beta, and I am taking this. So, we have F alpha beta, so K, F alpha beta, F alpha plus C beta over F. So, this exists for all C in F.

But, so, this is an intermediate field and there are infinitely many F, C's. So, since F is in finite and K over F has only finitely many intermediate fields, F alpha plus C beta is an intermediate field. So, you apply this to every C in capital F, which you can do because infinitely many times you can do because F is infinite, but they are only finitely many intermediate fields.

So, there exists C 1, C 2 in F not equal such that, so we are almost done. So, we do have 2 distinct elements in capital F such that F alpha plus C 1 beta is equal to F alpha plus C 2 beta. Now, we will just run with it what can we do? So, now, what we know is that alpha plus C 1 beta minus alpha plus C 2 beta is in F alpha plus C 1 beta because both of them are equal. So, alpha plus C 2 beta is in this, alpha plus C 1 beta is also in this. But this is C 1 minus C 2 beta is in F of alpha plus C 1 beta.

(Refer Slide Time: 22:17)

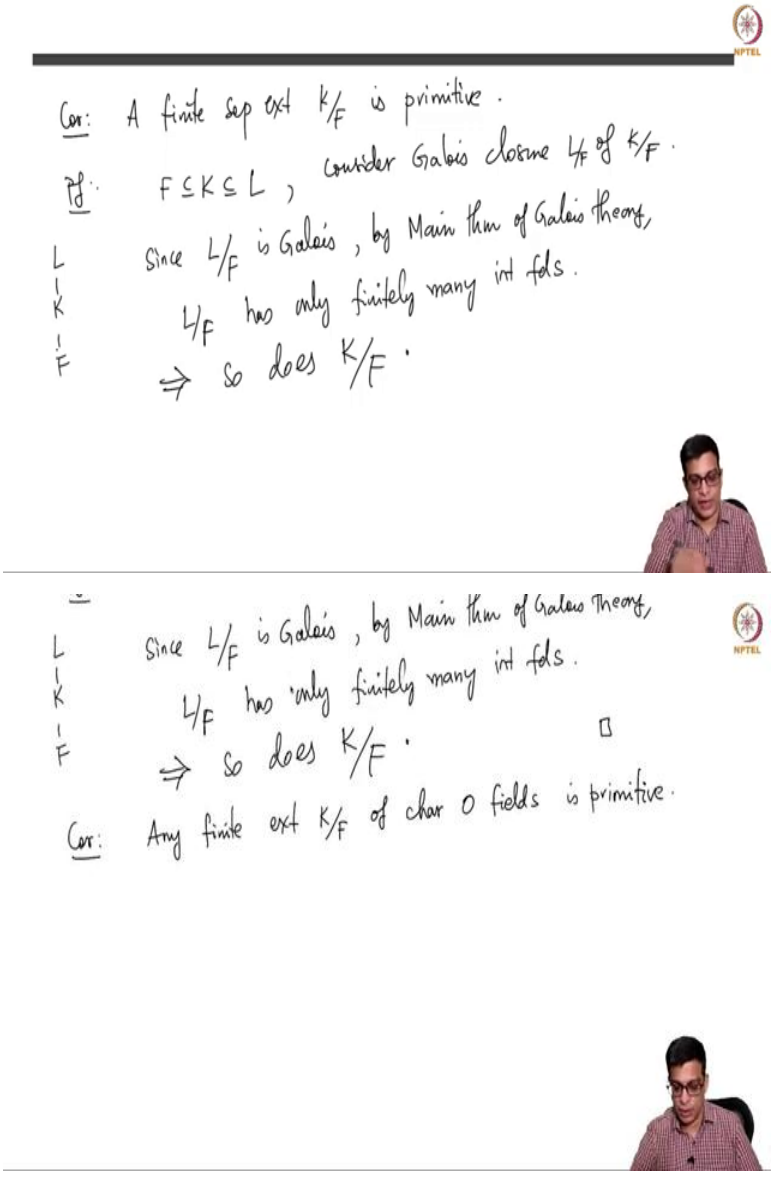





But C 1 is not equal to C 2 implies C 1 minus C 2 is nonzero. So, you can clear that, you can do to multiply by its inverse. So, beta is there, but then alpha which is alpha plus C 1 beta minus C 1 beta is also there because alpha plus C 1 beta is certainly there, once beta is there C 1 beta is there.

So, their difference which is alpha is there, that means, both alpha and beta are there that means, F alpha beta is contained in this, but this is of course, contained in F alpha beta. So, we are done. So, F alpha beta is equal to a single element thing. So, this is a primitive element as required. So, that means, any extension generated by 2 elements can be generated by a single element. So, applying that repeatedly we say that any extension that can be generated by N elements can be generated by one element.

(Refer Slide Time: 23:30)




And a corollary of this which connects it to Galois theory is the following. A finite separable extension K over F is primitive, the proof is very simple. So, given K containing F we take L, consider L Galois closure, which I defined earlier meaning you take the generators of K over F add all the conjugates to F of those elements you get a Galois extension.

Since, L over F is Galois now. So, basically any separable extension can be extended to Galois extension, by main theorem Galois theory L has only finitely many intermediate fields because any intermediate field there is a bisection between intermediate fields of this Galois extension and the subgroups of the Galois group which is a finite group.

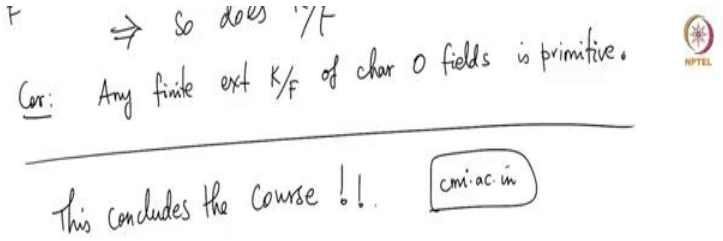
So, if L over has, L over F has finitely many intermediate fields, definitely K over F will also have finitely many intermediate fields, because any intermediate field of K or F is in fact an intermediate field of L over F obviously, so K over F has only finitely many intermediate fields.

And finally, the last corollary, any finite extension K over F of characteristic 0 fields is primitive because separability can be dropped, the word separability can be dropped from the previous corollary because we have characteristic 0 fields, any finite extension of characteristic 0 field is primitive.

So, this is something that has come up in some of the exercises that we have done in the past. So, often it is tricky to find the primitive element, but we know now that they exist for any finite separable extension in general, and in characteristic 0 case for any finite extension, because it is definitely primitive.

So, that completes the course. I hope in the last 3, 4 classes, you understood more about what came before it, because we have done a number of problems in detail. And I am sorry, I skipped details of some of the problems, but those are details corresponding to rings and fields or groups, I hope those are not too difficult and you can provide those details and understand the full proofs of all the problems that we have done. So, let me stop now.

(Refer Slide Time: 26:25)




And in this course, what we have done, this concludes the course. So, I hope you enjoyed the course, in this course, we started with several lectures on revision of rings, fields and groups,

because those are essential for field theory, Galois theory. And then we started the proper study of Galois theory. So, we started discussing group characters, and then started talking about automorphisms of field, fixed group of those automorphisms, fixed fields of those automorphisms, we proved some foundational results for about fixed fields.

And using this, we defined Galois extensions. We proved Galois's main theorem, or main theorem of Galois theory, which establishes bijection between intermediate fields of a Galois extension and subgroups of the corresponding Galois group. And that was sort of the first deep theorem. Of course, the proof was not difficult there. But the first really essential theorem in this subject.

And then we applied that theorem to understand (())(27:29) extensions, cyclotomic extensions, and finally, in understanding radical extensions, and then we ended the course by proving that any polynomial with coefficients in a subfield of complex numbers, but if the polynomial has degree 1 2 3 or 4, then the polynomial is solvable, meaning all the roots can be expressed using radicals and using elements of the base field.

But the same is not true for degree 5 and higher, we produced polynomials of degree 5, and in general for any higher degree, which cannot be solved by radicals. So, they are not solvable in other words, and then in the last few videos, we solved several exercises, which illustrate many of the theorems that we have done. And we ended with the primitive element theorem, which actually is a very useful thing to keep in mind, namely, that any extension which has only finitely many intermediate fields is primitive.

And the most common application of this is in this case, any finite separable extension is primitive. So, I hope you enjoyed the course. This course completes a sequence of algebra courses starting with group theory, ring theory, field theory and Galois theory. And I really hope you enjoyed listening to this course, as I enjoyed lecturing.

Any questions you have, please feel free to ask in the forum and also feel free to contact me by email. If you have any questions. You can find my email on Chennai Mathematical Institute website. You can go to this website and find my email address. I really hope that you enjoyed the course and learn something beautiful and deep in Galois Theory. Thank you.