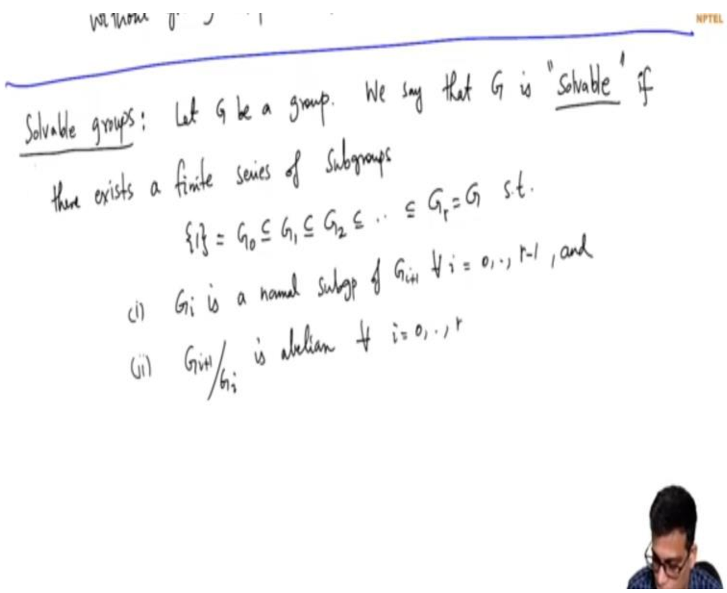
Introduction to Galois Theory
Professor Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute
Lecture 42
Solvable Groups – Part 1

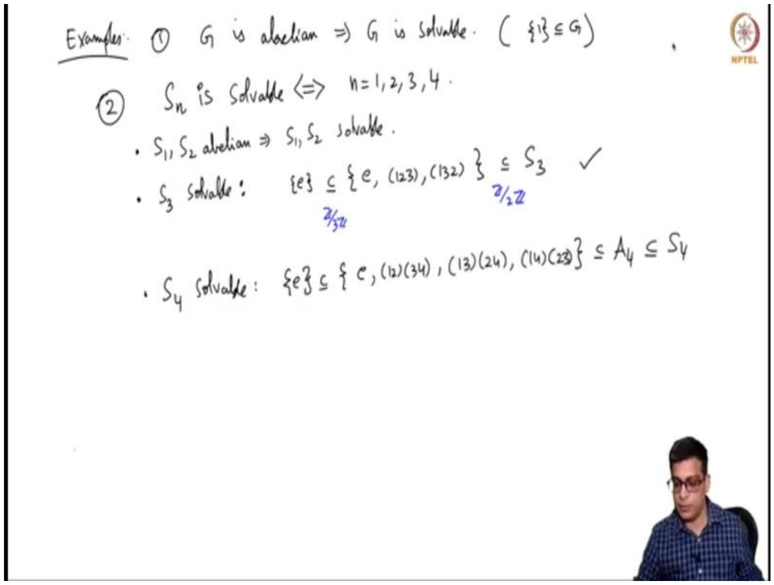
(Refer Slide Time: 00:35)

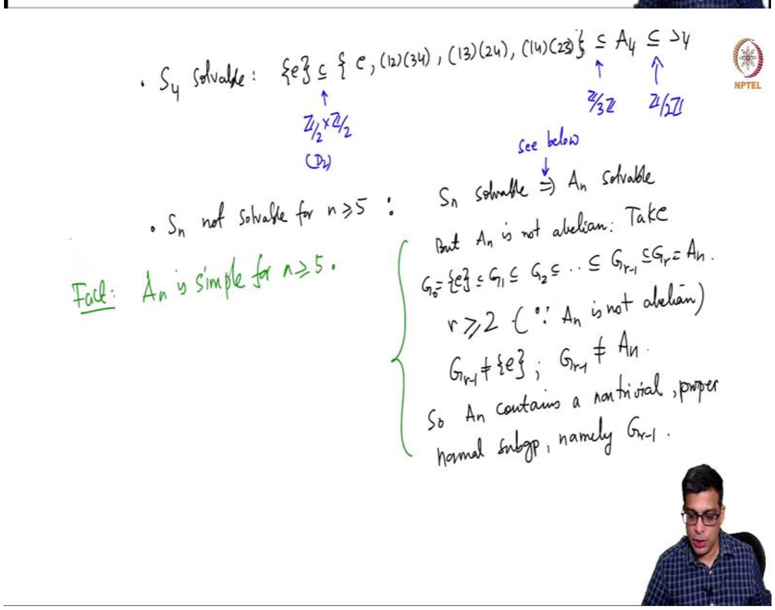


Welcome back. We have so far established that if you start with a subfield of complex numbers and you take a polynomial over that field of degree 1, 2, 3 or 4, the roots of solvable namely enhance the polynomial itself is solvable. So, today what I want to do is introduce another way of looking at this and this is through the notion of solvable groups. I am going to quickly give you the definition. I would not prove many facts about this, because this is going to be an alternate proof of all the things that we are proving directly. So, we have already proved directly that any degree 4, 3, 2, 1 polynomials are solvable, but this is another proof.

So, let G be any group. So, we say that G is solvable. So, you will see that the terminology is the same for a very good reason. If there exists a finite series of subgroups, so let us say, starting with the trivial group, which I will call G0, G1, G2 and ending with Gr which is G such that two things happen. Gi is a normal subgroup of Gi plus 1 for all i from 0 to r minus 1 and Gi mod, rather Gi plus 1 mod Gi is abelian for all i from 0 to r minus 1. So, Gr by Gr minus 1 is abelian, Gr minus 2 by Gr minus 2 is abelian and so on. G1 by G0 is abelian. So, in particular, G1 itself is abelian.

(Refer Slide Time: 02:28)





So, some easy examples I will write here before proceeding. G is abelian implies G is solvable. So, solvable groups are like close to abelian groups. That is the way you should think about them. So, there is a series, finite series where quotients are abelian groups. So, they are close to abelians. So, obviously, if G is abelian, you do get abelian solvability. You can just take e contained in G or 1 contained in G. So, that will do the job. So that is a trivial example, but there are also non-abelian groups which are solvable.

So, I want to write a general statement here. Sn is solvable if and only if n is 1, 2, 3 or 4. So, the reason is S1, S2 are abelian implies S1, S2 solvable. S3 is solvable. It is not abelian, but it is solvable, but it is solvable because you can consider the series given by, so if you take this series, let me use e for the identity element, because indices are already denoted by this.

So, here quotients, I mean, these are all normal subgroups, the quotient here is z mod 3z and the quotient here is z mod 2z. So, this is normal subgroup of index 2 in S3 so quotient is this. So, this solvable. So, this is your example of a non-abelian solvable group. S4 is another such example. So, here I can take e and I take e, 12, 13, 1, 2, 3, 4. This is our group D2 in the previous class and then I take A4, then I take S4. So, the quotients in this case will be z mod 2 cross z mod 2 or D2 in the notation of earlier class. Here, the quotient is, this is a degree 4 group, order 4 group. This is an order 12 group. So, the quotient is the z mod 3z.

So, the normality is something to check. So, that I will leave for you. So, you take any even permutation in S4 and you take conjugate of any element here by that element you will again land here. So, that is something to check. I do not want to do that now. And here the quotient is z mod 2z. So, this is of course normal because of degree 2, index 2. So, this is quotient is normal, quotient is abelian, z mod 2z. So, S3, S4 are solvable.

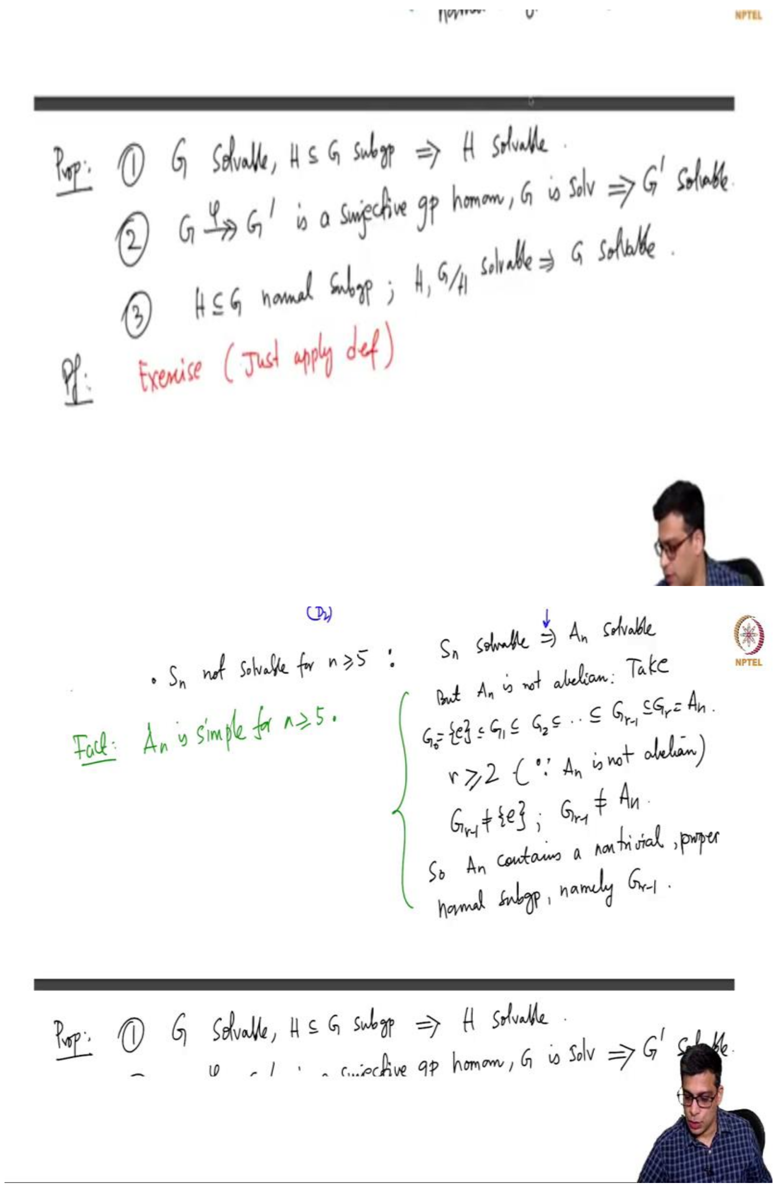
Now, in general, the higher essence are not solvable. So, if we use the following facts, so here Sn is, suppose Sn is solvable, implies An is solvable. So, I am going to see right here, see below. So, I am going to write a proposition at the end after this or really exercise after this, which will tell you this.

So, if Sn is solvable, An is solvable, but An is not abelian so there must be a non-trivial series. So, let us say it is e G1, G2, Gr minus 1, Gr which is An. So, we have r is at least 2 because G is not abelian. If An is not abelian, r is at least 2, because if r is 1, G1 is always abelian, because G1 coefficient by G0 is G1. So, r is at least 2. So, hence, An contains a non-trivial, so basically what I really mean is that Gr minus 1 is not trivial and of course, Gr minus 1 is not An.

So, An contains a non-trivial proper normal subgroup mainly Gr minus 1, but this violates this important fact, An is simple for n greater than equal to 5. So, this is a standard result in group theory. I will not prove it now. If we have time at the end of the course, I will give you some results that I have used in the course and I will in that process prove this, try to prove this at least or give you an idea, but basically the easiest solution in some sense is, you show that 3 cycles generate at least for A5. Maybe I will, so maybe I will just start at this.

So, you say the 3 cycles generate A5 and we show that any conjugate of a 3 cycle is again in A5. So, this will show that A5 is, so I think I sort of confused with this. So, let me not, before I say anything in precise. So, I will try to do this in a separate video that An is simple for every n at least 5. But here if there is a series which makes An solvable, you will conclude that An has a non-trivial proper normal subgroup which is not possible. So, this shows that Sn cannot be solvable. So, Sn is, for n at least 5. So, we have S1, S2, S3, S4 are soluble, but S5, S6 so on are not true, not solvable.

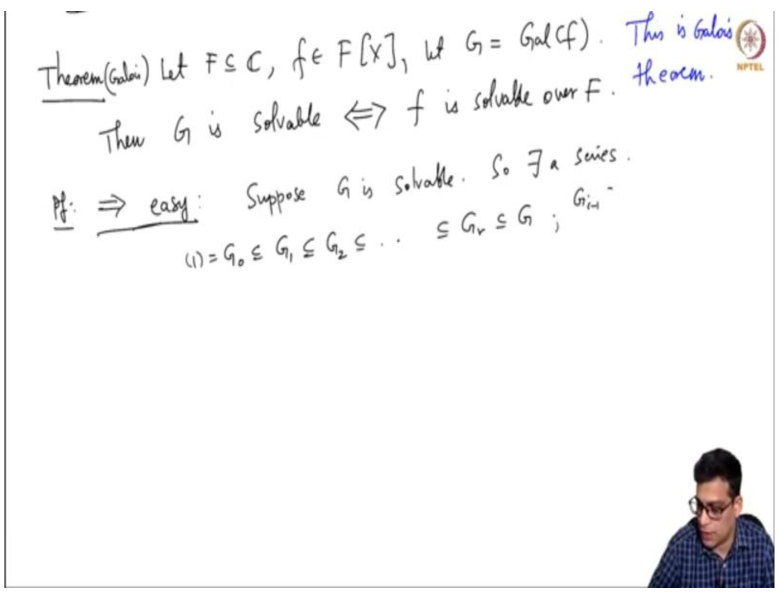
(Refer Slide Time: 09:15)



So, proposition that I want to write, and these are simple facts I will use them later. So, if G is solvable and H is a subgroup, this implies H is solvable. Second statement is, if G to G prime is a surjective group homomorphism so that means, I can put this, group homomorphism and G is solvable implies G prime is solvable. So, the image of a soluble group is solvable. And finally, if H is a normal subgroup of G, H and G mod H are solvable, implies G is solvable. So, I want to leave this as a proof to you, exercise to you. These are not just follow, just apply definitions.

In the first case, for example, if there is a series for G in the, as in the definition, you intersect with H and you take, you show that that works for H. If there is a series for G, you take their images and you show that that works for G prime. And for this you have to do a little bit more work, but this is a standard group theoretic statement. Nothing serious here. So, these are standard statements. So, this first part we have used here. If Sn is solvable, An is a subgroup. So An is solvable so that concludes the general introduction by want to give for solvable groups.

(Refer Slide Time: 11:04)



Pf: $\Rightarrow$ easy: Suppose G is solvable. So $\exists$ $G_{i-1} \le G_i$ normal

$G = Gal(K/F)$. $(1) = G_0 \le G_1 \le G_2 \le \dots \le G_r = G$; G_i/G_{i-1} abelian.

Apply Main theorem to G_i:

$$F = F_0 = K^{G_r} \subseteq K^{G_{r-1}} \subseteq K^{G_{r-2}} \le K^{G_{r-3}} \subseteq \dots \le K^{G_2} \le K^{G_1} \le K^{G_0} = K$$

abelian abelian abelian abelian

G_{r-1} is normal in G_r

$\Rightarrow K^{G_{r-1}}/K^{G_r}$ is Galois with Galois gp G_r/G_{r-1} abelian

K — G_{r-1}

$K^{G_{r-2}}$

$K^{G_{r-1}}$

| Galois G/G_{r-1}

F

Now apply our theorem about equivalent characterization of solvable elements. (Page 74)

K contains all the roots of f

apply Main thm to $K/K^{G_{r-1}}$

Galois gp G_{r-1}

Apply Main theorem to G_i:

$$F = F_0 = K^{G_r} \subseteq K^{G_{r-1}} \subseteq K^{G_{r-2}} \le K^{G_{r-3}} \subseteq \dots \le K^{G_2} \le K^{G_1} \le K^{G_0} = K$$

F_1 F_2 F_r

G_{r-1} is normal in G_r

$\Rightarrow K^{G_{r-1}}/K^{G_r}$ is Galois with Galois gp G_r/G_{r-1} abelian

Now apply our theorem about equivalent characterization of solvable elements. (Page 74)

K contains all the roots of f

apply Main thm to $K/K^{G_{r-1}}$

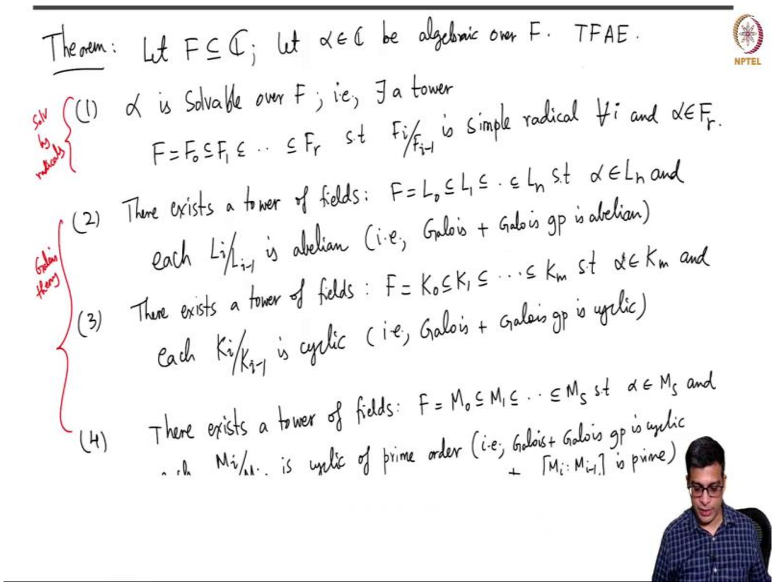
Galois gp G_{r-1}

$G_{r-2} \le G_{r-1}$ normal

So $K^{G_{r-2}}/K^{G_{r-1}}$ is Galois with Galois gp G_{r-1}/G_{r-2} abelian

& F_i/F_{i-1} abelian $\forall i$.

$\Rightarrow f$ is solvable.



So, now, the main theorem that I want to prove connecting solvability of groups, so solvability of the polynomials is the following. Let F be a subfield of C, as always. Let us take a polynomial capital F, in capital F. Then, and let us take the Galois group of f, namely the Galois group of the splitting field of f. Then G is solvable if and only if F is solvable. So, this is the theorem of Galois. So, this is crowning achievement. So, I should really put Galois here. So, while Abel and other people have proved that quintics in general cannot be solved by radicals, Galois was the first person who gave a method to check if a given polynomial is solvable or not and his method is, this is what one wants to know.

He created Galois group theory and attached a group to this polynomial and defined the notion of solvability of groups and he said that F is soluble if and only if G soluble. So, the proof of this I want to give. One direction is easy. So, I will do that first. That another direction is a bit more involved. So, I will do that in the next class, but I want to emphasize here that Galois' main achievement is this theorem. He proved that you can characterize solubility of a polynomial purely in group theoretic terms by looking at the group and see if that group is solvable or not.

Actually, this is not the direction that I want to do. This is the direction that I want to do. So, suppose G is solvable. So, there exists a series. So, 1, which is G0, G1, G2, Gr, each Gi, so let me just record the properties here and Gi, mod Gi minus 1 is abelian. And what is G, remember is K power, G is the Galois group of. So, now you can see is staring in front of you apply main theorem, basically. If you apply main theorem to Gi, what do you get? So, you take K power G which of course is F. So, let us call that F0. Then you take K power G1. Sorry, K power G is K power Gr. Gr is equal to G. Then you take K power Gr minus 1.

So, now I will write the proof here. This, what kind of an extension is this? Gr minus 1 is normal in Gr. So, K Gr, K Gr minus 1 is Galois with Galois group. So, this is the, because we have done all the hard work, this is very beautiful and simple now, with Galois group, Gr over Gr minus 1. This is exactly the main theorem of Galois theory. You take the Galois group of the entire extension. So, here maybe I will write it here also. K and F and I am taking the fixed field of a normal subgroup K Gr minus 1. So, this is Galois with Galois group G mod Gr minus 1, which is abelian by hypothesis. So, this extension is an abelian extension. Now you take K power Gr minus 2. So, I will take K power.

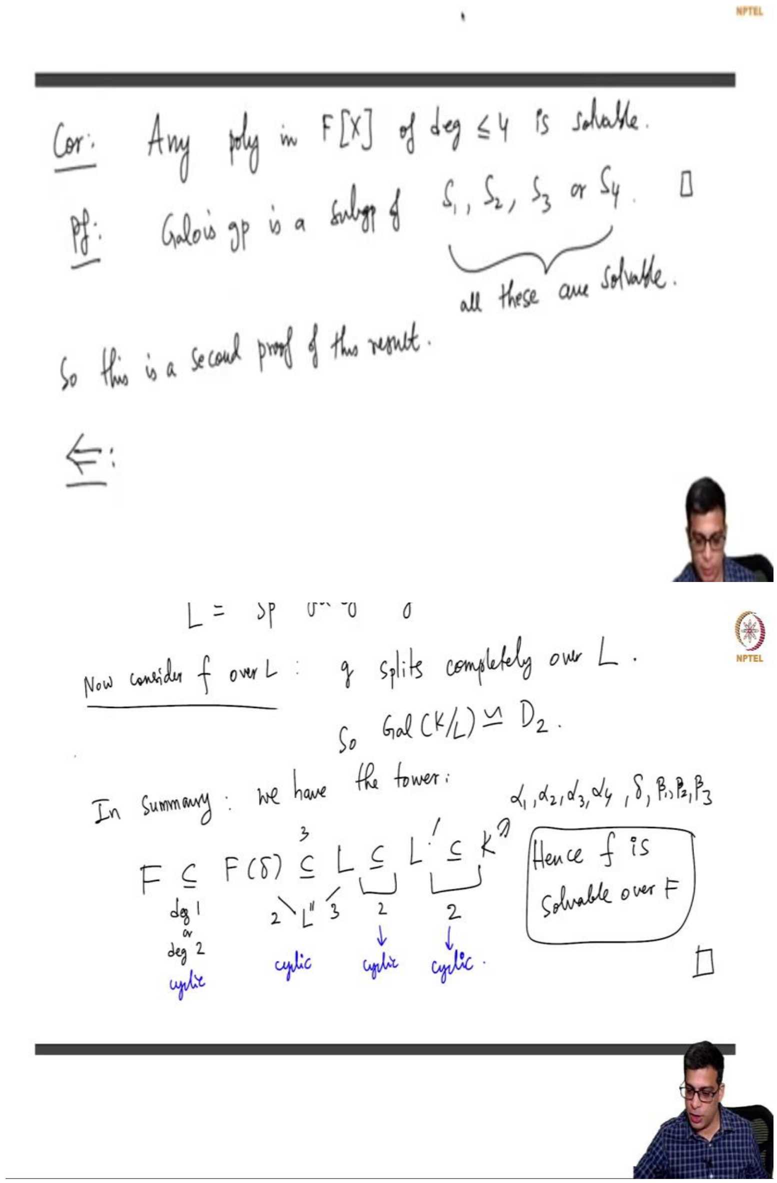
So, basically, what I will now do is look at this extension. What is this extension? This extension, so I will write the reason for that here. Reason for that is or maybe I will squeeze that here. So, apply main theorem to K over K power Gr minus 1 which is Galois. So, I am applying with this. I will analyse this later, but I am applying to this. This is Galois with Galois group Gr minus 1 by the main theorem. This over K is Galois with Galois group Gr minus 1, because if you fix a subgroup and take the fixed wheel, the top is the Galois extension with that subgroup as a Galois group. Bottom is the Galois extension. If the subgroup is normal, the Galois group has a quotient. But here I am taking the top. That is Galois group Gr minus 1. And Gr minus 2 is a normal subgroup of Gr minus 1.

So, this is Galois. So K Gr minus 2 over K Gr minus 1 is Galois with Galois group Gr minus 2 modulo Gr minus 1 or rather Gr minus 1. So this, I will take this quotient, Gr minus 1 modulo Gr minus 2 which is of course abelian. So, and we continue like this K power Gr minus 3, K power G2, K power G1, K power G0 which of course is K. G0 is a trivial group. So, the fixed field of the trivial group is all of K. And the point of all of this is, this is abelian, this is abelian, this is abelian, this is abelian. So, all of them are abelian.

Now, you look at the result on the equivalence of radical extensions. So, now apply, so maybe I will try to finish it here. So, now apply about equivalences, equivalent characterisation of solvable elements. So maybe I will quickly go back and show that on which page we have this. So, equivalent characterizations are here. Sorry, so I think I went way past this. So, these are the equivalent characterizations. What I have now is the second statement. So, I have a tower containing all the roots, the end the field contains all the roots and each intermediate extension is an abelian extension. So, everything in the last field is solvable. So, I wanted to write down the page number so that you have reference to this. So this is page 74. So see page 74.

So, if you apply that theorem, you have an abelian and extension. You have a tower of abelian extensions and the last field contains all the roots. K contains all the roots of f. K is the last field implies and each if you want, this is F1, F2, Fr and each and Fi minus Fi minus 1 is abelian for all i. So, hence, f is solvable. So, this proves the easy direction. If you have this a solvable Galois group, then the polynomial is solvable.

(Refer Slide Time: 20:35)



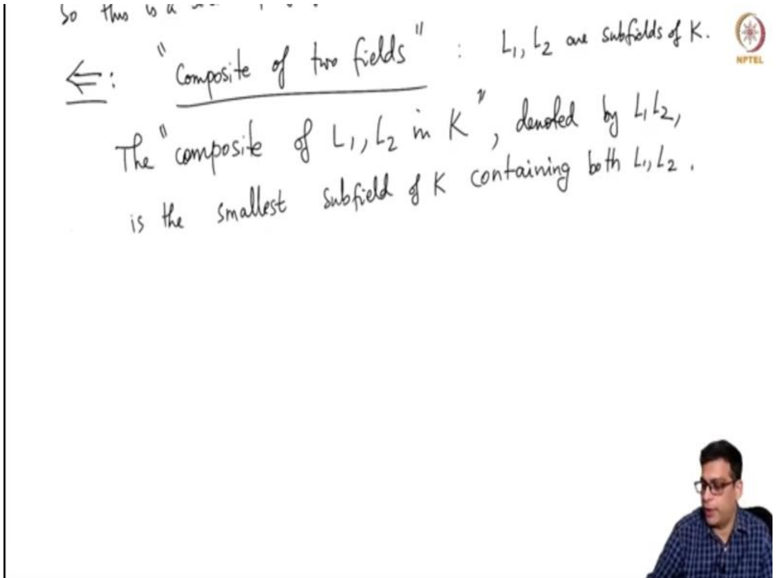
So, now, as a corollary, before I prove the next, other direction, we get a different proof. I said, remember, I will prove every statement about polynomials in two ways. Any polynomial in the polynomial ring FX of degree less than equal to 4 is solvable. Proof, the Galois group is a subgroup of whatever S1 or S2 or S3 or S4 in all of these cases and all of these are solvable by the previous example. So, Galois groups are solvable and hence the polynomial is solvable. So, that is the proof. So, this is a second proof of this result. We have directly exhibited a tower which does the job in each 1, 2, 3, 4 degrees but here is a more conceptual idea and using the actual theorem that Galois proved.

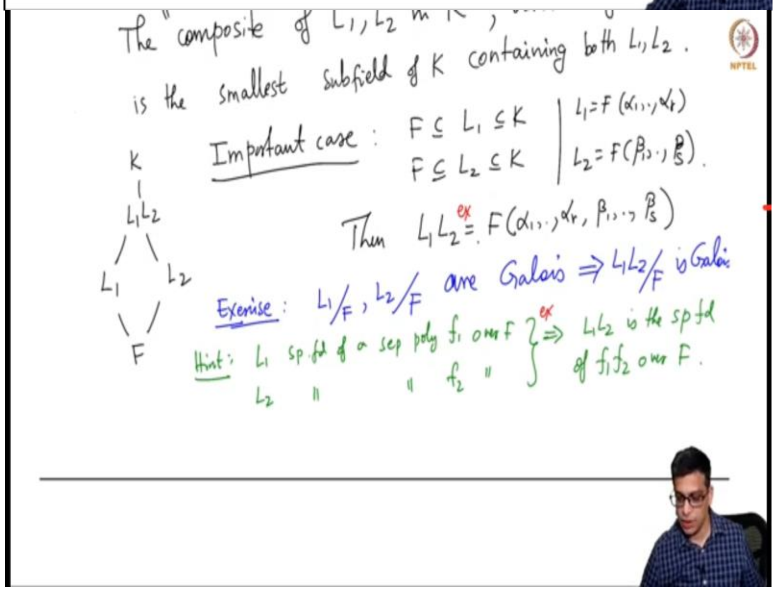
So, for degree 4 or less, you have all of these are solvable so their subgroups are solvable by our general proposition about solvable groups. So, Galois groups are solvable, and by this theorem, the polynomial is solvable. And now the next direction is this. If the polynomial solvable, then the group is solvable and because we know that S5 is not solvable or A5 is not solvable, if you produce a polynomial of degree 5 whose Galois group is S5 or A5, this theorem will show that it cannot be solvable by radicals or rather it is not solvable.

So, now we do that in 2 ways. First, we will prove this theorem in the next class and after that we will work exclusively with a degree 5 polynomials and prove it again, and then we will actually give an example of a polynomial of degree 5 who is Galois group is S5 and thereby exhibiting a polynomial which is not solvable.

So, now let me postpone the proof of this direction, because it is not difficult at all. It is just a little involved because it uses two, three different facts. So, let me stop this class here and then postpone the proof to next class. But before I end the class, because I have a couple of minutes, so let me define an important notion, which I am never mentioned before. I really should have talked about this earlier.

(Refer Slide Time: 23:15)





So, let us say L1, L2 are subfields of K. They are all fields. So, the composite of L1, L2 in K denoted by the symbol just L1, L2 is the smallest subfield of K containing both L1 and L2. So, this is the composite. So, you have K. It contains two fields L1 and L2. The composite is a subfield of the bigger field which contains both of them and often we are interested in the case when you have a base field F. So, one specific example, in fact, this is the only case we will consider. Suppose f is contained in L1. L1 is contained in L2. L1, L2 are contained in K.

So, you have L1, L 2 are both extensions of F and they are both subfields of K. And suppose L1 is F of alpha 1 through alpha r and L2 is F of beta 1 through beta s. Then L1, L 2 is nothing but, it is supposed to contain both L1 and L2. So, it is supposed to contain all of the alpha i's and all of the beta js. So, and the field generated by them over F is a smallest field because it contains alpha i's, it contains beta i's and it is the smallest field containing them. So, any field that contains both L1 and L2 must contain all of f as well as all of the alpha i's, all of the beta i's, so you have this.

So, let me write one exercise here and then we will stop the video. If L1 over F and L2 over F are Galois, then the composite is Galois. So, the exercise has easy solution. L1 is the splitting field of a separable polynomial f1 over F, L2 is the splitting field of separable polynomial f2 over F. Then you show this. This is the exercise for you. L1, L2 is the splitting field of f1, f2 over F.

So, using this idea basically. So, then I will also call this an exercise. So, if you have two Galois extensions, their composite is also Galois extension. So, I want to work with composites in the next class in order to prove the reverse direction of this. So, let me stop this class here. In the next class, we will prove the converse of this theorem, which shows that if F is a solvable polynomial, its Galois group is a solvable group. Thank you.