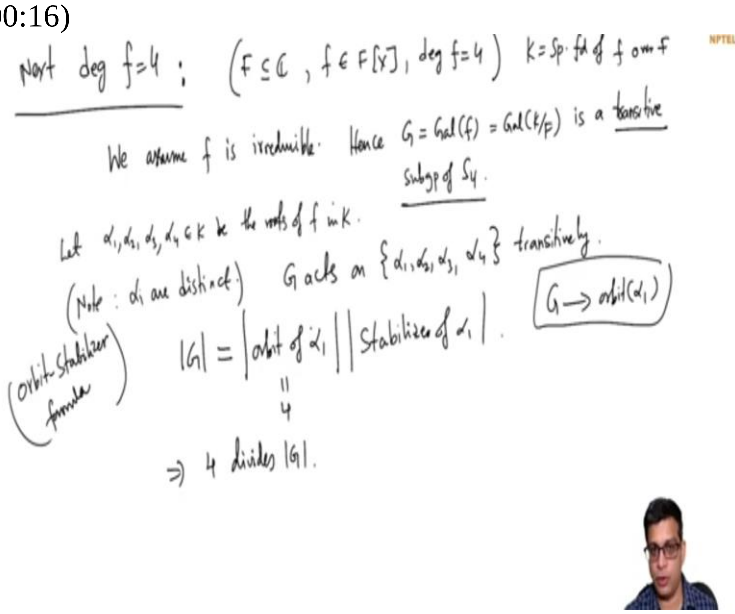
Introduction to Galois Theory
Professor Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute
Lecture 41
Quartics are Solvable

(Refer Slide Time: 00:16)



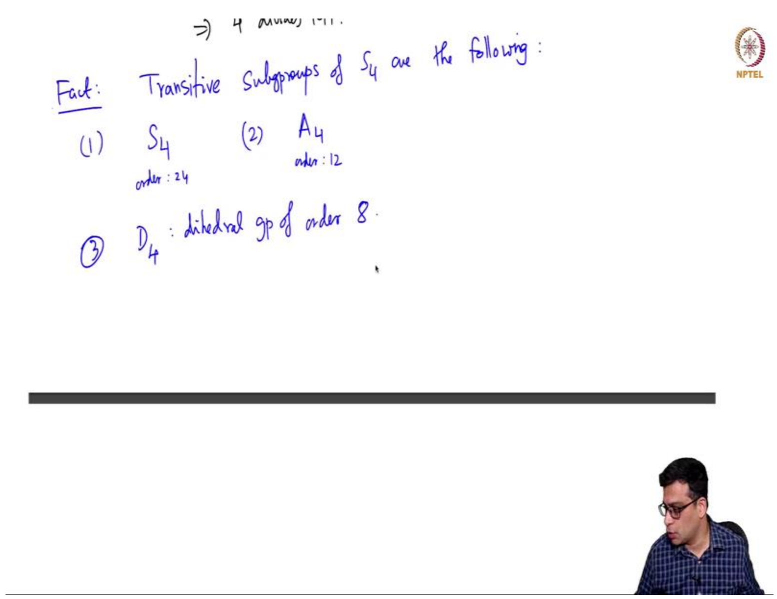
Welcome back. We are in the process of proving this theorem which says that if you have a subfield of complex numbers and the polynomial over that field of degree 1, 2, 3 or 4 that polynomial is solvable. We in the last class took care of the cases 1, 2, 3 degrees. Now, let us take care of the degree 4. So, of course, we assume that f is irreducible. That is because if it is not irreducible, it is a product of two polynomials of smaller degree and those we have already considered. So, any polynomial of degree 3 or less is already solvable. So, if f is gh, this is solvable, this is solvable means f will be solvable, because any root of f is a root of g or root of h. So, the only new case is when f is irreducible. So, we are going to assume this.

So, hence Galois group of f, which I denote G. Of course, K is the splitting filed small f over capital F. So, the Galois group of f is the Galois group of the extension K over F is a transitive subgroup of S4, because here there are 4 indices and because f is irreducible, it is a transitive subgroup of S4. And now if you think about this that really what I am saying is, let alpha 1, alpha 2, alpha 3, alpha 4 be the roots of f in K. So, we of course recall here that they are distinct, alpha i's are distinct, because f is irreducible and you are in a characteristic 0 field.

So, there are in fact four distinct roots and G acts on this set transitively because f is irreducible. So, that means given any pair of roots of f, there is an automorphism which sends 1 to the other. That means we know by the orbit stabilizer formula, I think it is called, or counting formula from group theory it is, for example, orbit of alpha 1, the cardinality of the orbit of alpha 1 times the order of this stabilizer of alpha 1. So, there is a map from G to orbit of alpha 1, which sends sigma to sigma of alpha 1 and the kernel is and this has, only things that map to alpha 1 are in the stabilizer. So, using that, you can prove this formula, but this is 4, because G acts on this transitively, orbit of alpha 1 is the entire set alpha 1, alpha 2, alpha 3, alpha 4. So, this is equal to 4.

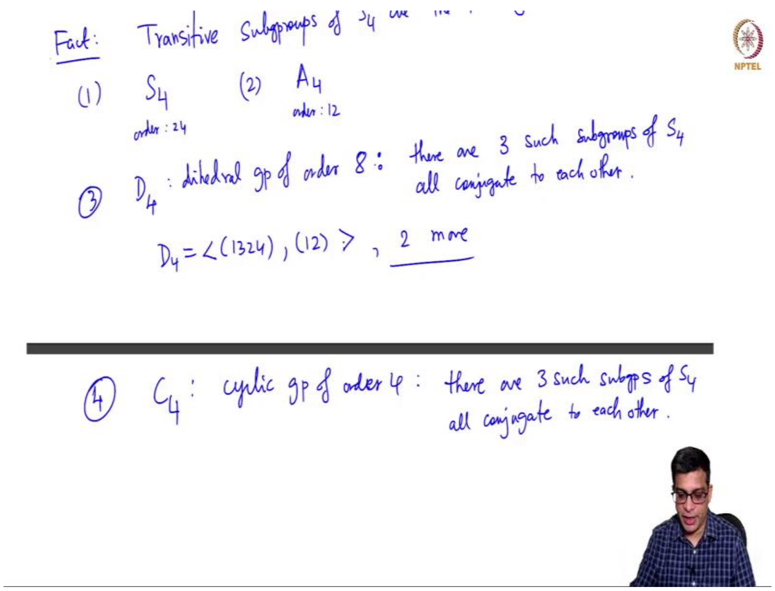
So, we conclude that 4 divides, so this is a major constraint on the possible transitive subgroups of S4, because we are only allowed to have groups of order divisible by 4. That rules out, for example, a group of order 6. It cannot be a transitive subgroup. And in fact, this is a fact, so this alone is not in this, this observation is not enough to conclude the following statement, but I do not want to prove this group theoretic statement, because it will take me far from the main purpose of the course. So, I will simply state this as a fact.

(Refer Slide Time: 03:49)



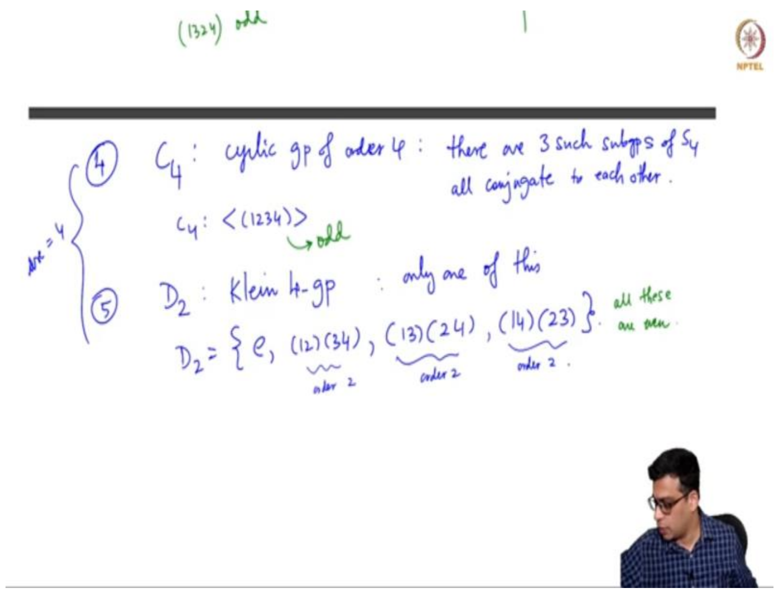
Transitive subgroups of S4 are the following. So, I only made this very easy observation to at least rule out things whose orders are not divisible by 4, but you need to do more work to conclude this. So, first is of course S4, second is A4. So, S4 and A4, here order is 12, order is 24 here, order is 12 here. These are both going to be transitive obviously, because you can find every, given any pair of indices, there is an even permutation which sends 1 to the other. The third one is a collection of groups which are all isomorphic to dihedral group of order 8.

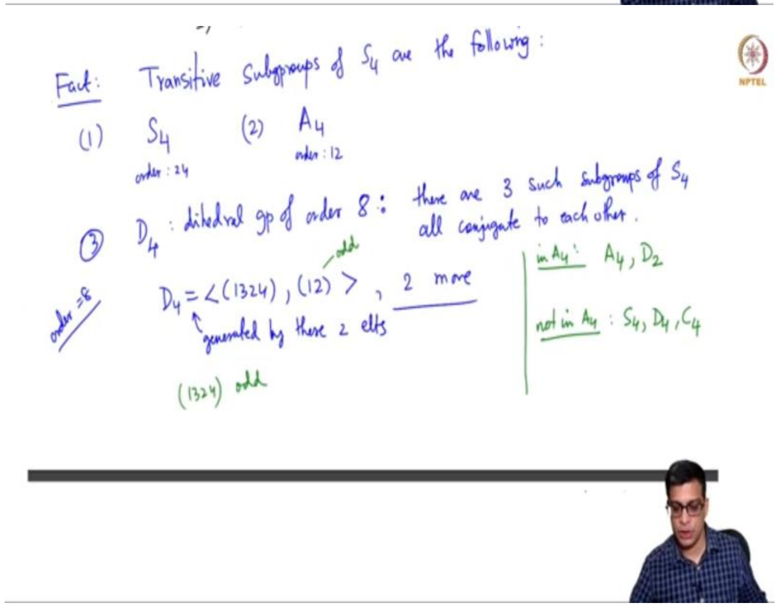
(Refer Slide Time: 5:00)



So, these, there are three of them, three, there are three such subgroups, S4 conjugate to each other. For example, 1 is given by, so they are all going to be generated by, remember a dihedral group has two generators. D4 has two generators. One of order 4, another of order 2 and there is a particular relation between them. So, that is satisfied if you take a degree, order 4 element, that means 4 cycle at a 2 cycle and you can there are two more I guess. So, I do not, for now, want to write those. This is one and there are two more. Each of them is in fact a dihedral group of order 8 and this is a cyclic group of order 4. Again, there are three of these.

(Refer Slide Time: 06:12)





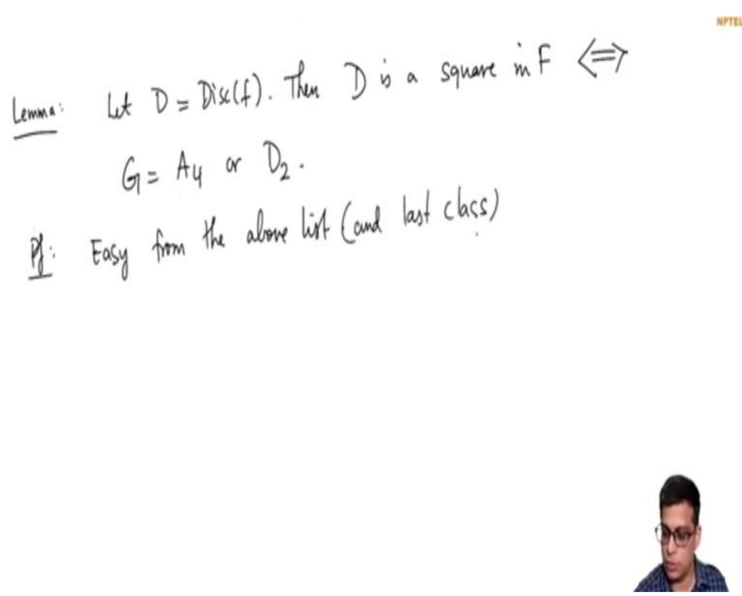
So, there are three subgroups of S4, isomorphic to the cyclic group of order 4 and they are all conjugate to each other. For example, you take one of them to be the group generates of the, sorry, this is not the set. I should not write like this. This is generated by these two elements. So, you take those and here, of course you take any 4 cycle and you take the group generated by that for example this. So, these are some groups generated by the 4 cycles. So here that is 1, I mean there are 3 but they are all isomorphic to C4. And finally you have D2, which is Klien 4 group.

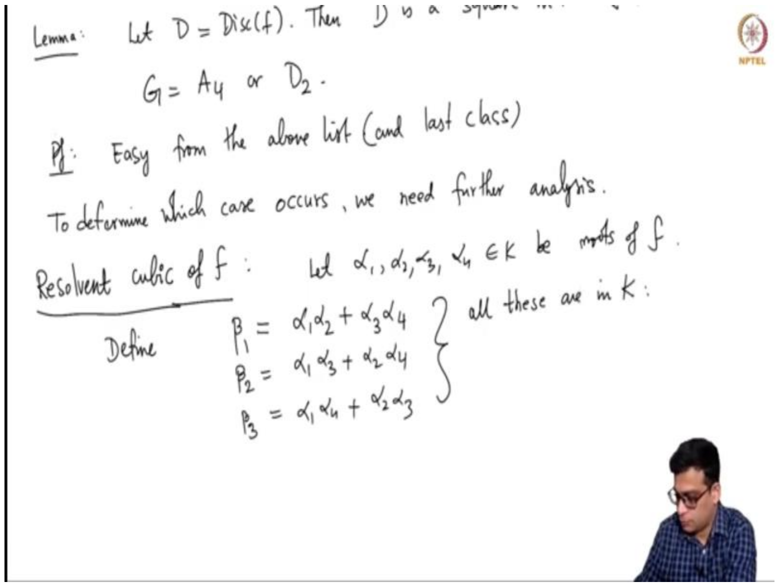
So, formally it is a dihedral group of order 4 and this there is only 1 of this and this is, you take disjoint transpositions. So for example, you take 12, 34, 13, 24, 14, 23, so each has ordered 2. So, this is order 2. This is order 2. This is order 2. So, this is a group of order 4, but it is not cyclic group, it is the Klien 4 group. So, as, this observation tells me that the only possible orders of a transitive subgroup of order of S4 are those whose order divides is divisible by 4. So, 24 is one possibility, 12 is another possibility, 8 is one possibility and order 4 is the final possibility. We have cyclic group order 4 or Klein 4 group.

So, as I said, I am not going to prove this. I am going to assume this. And further, I want to separate out this in terms of which of them are in S4, which of them are in A4 and which of them are not in A4. So, in A4, of course, there will be A4, 1324 is odd. This can be written as, I mean, this is A4 cycle, of course, this is also odd. So, not in A4 will be D4, S4 of course, D4, and this also is not in A4 and the last one is in A4 because this is a product of two transpositions. So, this is even. All these are even.

So, there are 5 possible non-isomorphic groups, possibilities for capital G, 3 of them are in, they are going to contain odd permutations so they are not in A4 and 2 of them consists only of even permutations. So, they are in A4. So, now the question is, in all of these cases we want to show that you have solvability by radicals.

(Refer Slide Time: 09:40)



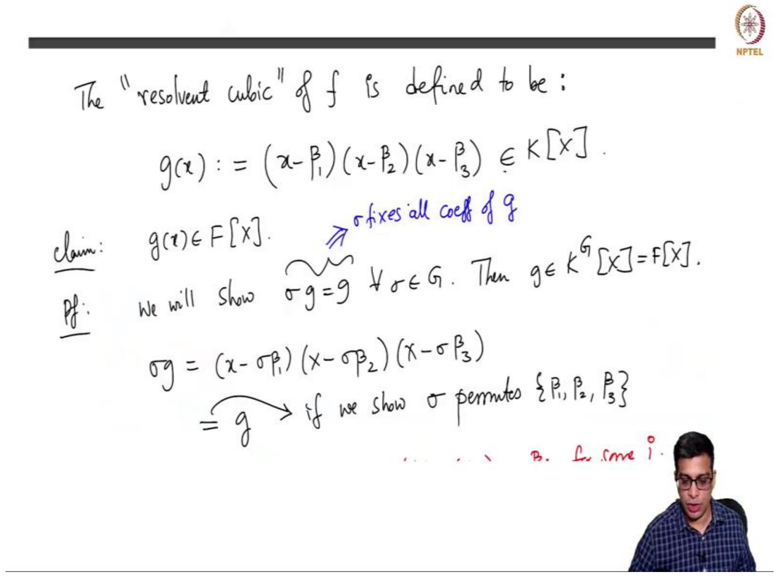


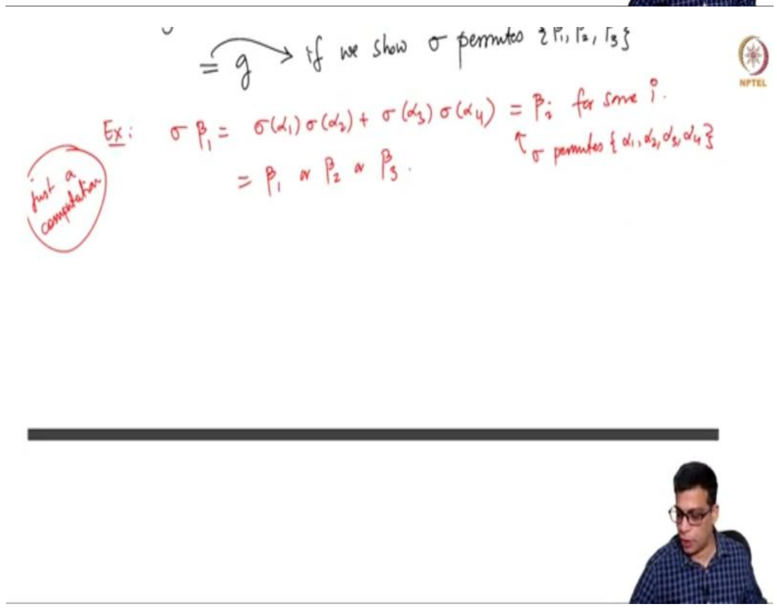
So, the first observation, which I will immediately write this follows from the preposition that I proved last time. Let D be the discriminant of f. Then D is a square in F if and only if G is A4 or D2. So, those are the only two cases in which D is a square in F. So, that in all other cases, D is not a square, because that means in all other cases, so from the above list and last class and the theorem from last class. This is trivial.

Now, to further analyse, so earlier in the cubic case discriminant determined the Galois group. It is a square in, f means it is A3, it is not a square means it is an S3. So, there is no further analysis that is required in degree 3, but to determine which case occurs, we need further analysis. So, we need further analysis and this is what we do now.

So, I am going to define a very important cubic polynomial attached to a quartic polynomial. So, degree 4 polynomial leads to something called resolvent cubic. So, let alpha 1, alpha 2, I mean this I noted, but I am going to recall, be roots of f. So, I am going to define three new elements in K, beta 1 to be, so I will take essentially any two of them, multiply them and then take the other two and multiply them and finally add. So, alpha 1, alpha 3 plus alpha 2, alpha 4, finally, alpha 1, alpha 4 plus alpha 2, alpha 3. So, if you recall the D2 sort of this has close connection to that. I take product of two transpositions. So, all these are in K.

(Refer Slide Time: 12:24)





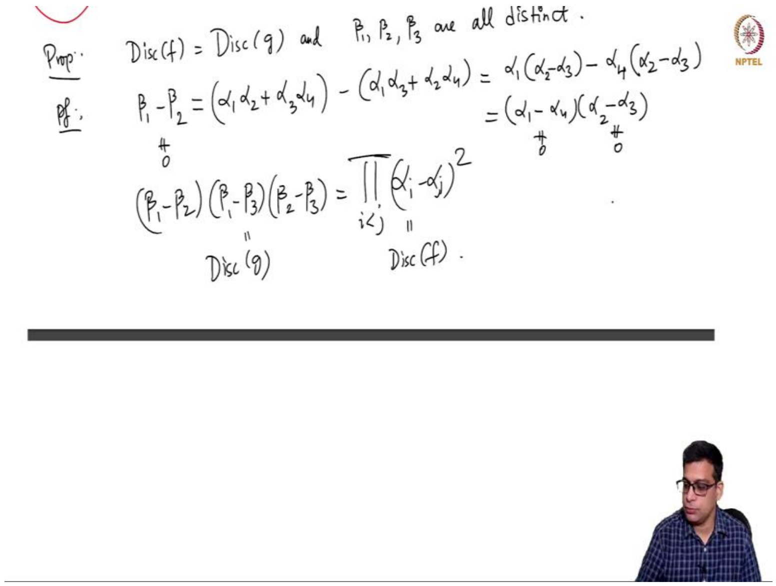
Now, the resolvent cubic of f is defined to be g of x is x minus beta 1, x minus beta 2, x minus beta 3. So, I will do an example where this becomes clear. So, now I claim, I mean, this is of course a priori in KX and beta i are in K so that means this is in KX, but we claim that GX is in fact in the base field. Beta always may not be there, but gx will be in the base field. The coefficients of g will be in the base field. So, the point is, so let us say g. So, we will show sigma g is g for all sigma in g. Then g is in KG X, because sigma g is in g implies sigma fixes all coefficients of f of g. That means all the coefficients of g are in K power G. K power G is F, because K over F is Galois. So, all we need to do is this.

But what is sigma g? Sigma g is x minus sigma beta 1, x minus sigma beta 2, x minus sigma beta 3. Now, we are done if we show that sigma permutes. So, we are done. So, this is g if we show sigma permutes the set beta 1, beta 2, beta 3. That means this may be x minus beta 2. This may be x minus beta 3. Then this will be x minus beta 1. So, if sigma permutes them, then these three factors are just rearranging the original factors. So, this will happen to be again g. But why does sigma permute beta 1, beta 2, beta 3? And that is because if you go back to this.

So, this is an exercise of, this is just a, if you go back to the definition of beta 1, this is sigma alpha 1, sigma alpha 2 plus sigma alpha 3 times sigma alpha 4, but sigma alpha 1, so remember sigma permutes alpha 1 to alpha 4. So, if you take any permutation of four elements and you take sigma beta 1, this will be some alpha i and this will be some alpha j. This then will be the other two elements. So, it will be beta 1 or beta 2 or beta 3. So, this I will leave you to do because this much better if you just do this on your own because instead of explaining this, all I will say now is you take sigma alpha 1.

If it is alpha 2 and sigma alpha 2 is alpha 3, then this will become alpha 1 plus alpha 1 alpha 2 times alpha 3, but then because sigma permutes them, these must be alpha 1 and the remaining things alpha 1 and alpha 4. So, that means that will become beta 3, I think. So, then sigma beta 2 will be something else. So, this is just a computation. So, just a computation. This point is important later on in the proof also, but I do not want to do this because this is just, this is easy. It just a computation. So, that means G is a polynomial in the base field. So, let me stop the prove there and move on. So, that is the first observation.

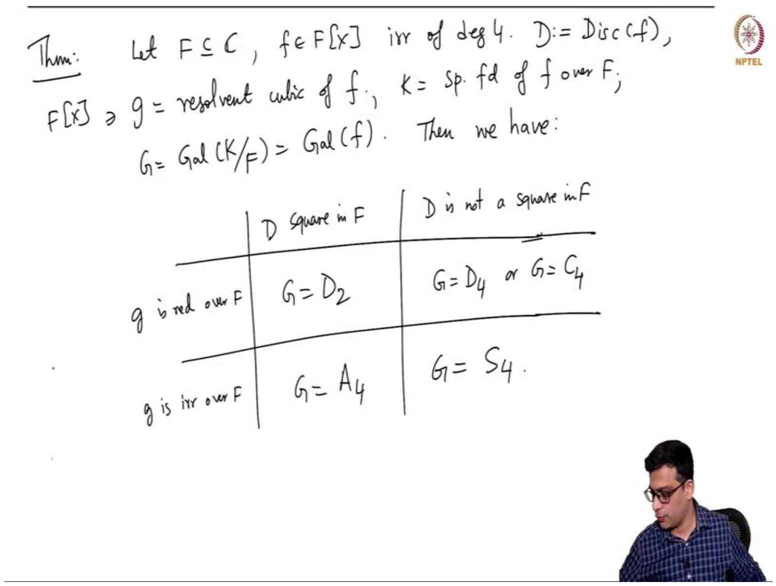
(Refer Slide Time: 17:01)



And the second observation which again I will indicate the proof quickly is that discriminant of f is equal to discriminant of g. The point is you have constructed a cubic polynomial which has the same discriminant and they are all distinct. So, the proof, I will not give the full proof, but only observe for example, the following. So, if you did beta 1 minus beta 2, if you go back and see the definition, beta 1 is alpha 1 plus alpha 1 times alpha 2 plus alpha 3 times alpha 4, beta 2 is alpha 1 alpha 3, so the next term will be alpha 2 alpha 4. And if you simplify this, you will get alpha 1 times alpha 2 minus alpha 3 and you do alpha 3, so actually alpha 1, alpha 2 minus alpha 3, then alpha 4 times, minus alpha 4, so this is alpha 2 minus alpha 3.

So, that means this is non-zero. This is non-zero. So, this is non-zero, because alpha i's are distinct so beta i's must be distinct. Moreover, discriminant of f is the squares of these things. So, beta 1 minus beta 2 takes care of two things. Similarly beta 2 minus beta 3 takes care of two more things. So, beta 1 minus beta 2 times beta 1 minus beta 3 times beta 2 minus beta 3 will be the product of all the pairs cycles. So, this is discriminant of g and this is discriminant of f. So discriminant is the same for these two polynomials. One quartic meaning degree for the other cubic meaning degree 3 and the roots of the resolvent cubic are also distinct.

(Refer Slide Time: 19:18)

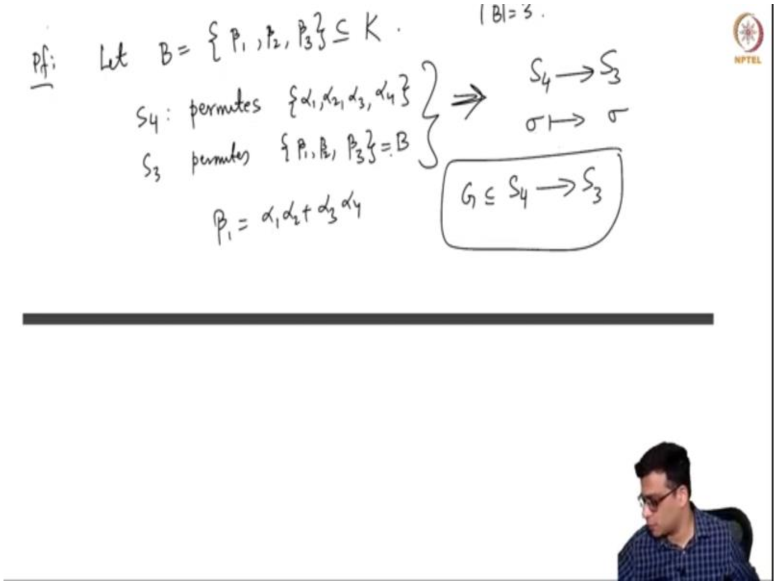


So, now, we are ready to prove the main theorem about quartic polynomials over characteristic 0 fields or subfields of C irreducible of degree 4. Let us say D is the discriminant of f and g is the resolvent cubic of f and then let us take K to be the splitting field of f over capital F. And finally, I am just recording all the notations so which is also called the Galois group of the polynomial f. Then we have the following possibilities. I will draw a diagram, a table really.

There are four situations. So, g is reducible over capital F, g is irreducible over capital F. Remember, g is a polynomial in capital F. So, g is in capital FX. Rather on the, here I will write D is square in F, D is not a square in F. So, in these cases, we have the following cases. So, in this case G must be the Klien 4 group. In this case G must be A4. So, remember when D is a square, I already noted, we have A4 and D2 and those possibilities are going to be determined by the situation of G, whether G is reducible or irreducible. When D is not a square, we have the other possibilities. So, we have D equal to a D4 or G equal to C4 and in this case G is S4.

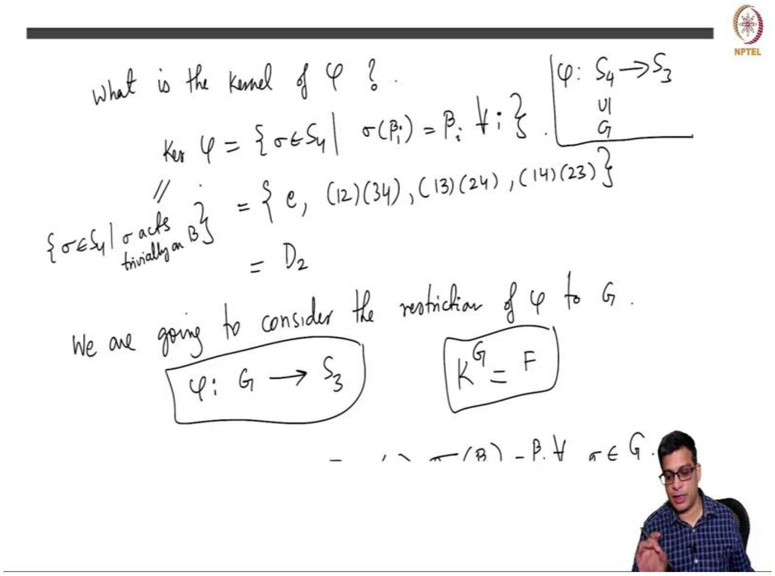
In this case, this case, this completely determined. In this case, you have potentially two possibilities, but the degree of the extension will tell you which one will occur, because in here degree is 8, in this case degree is 4. So, if you know the degree and you know the behaviour of capital D discriminant and the resolvent cubic, you know the Galois group. So these are the four possibilities.

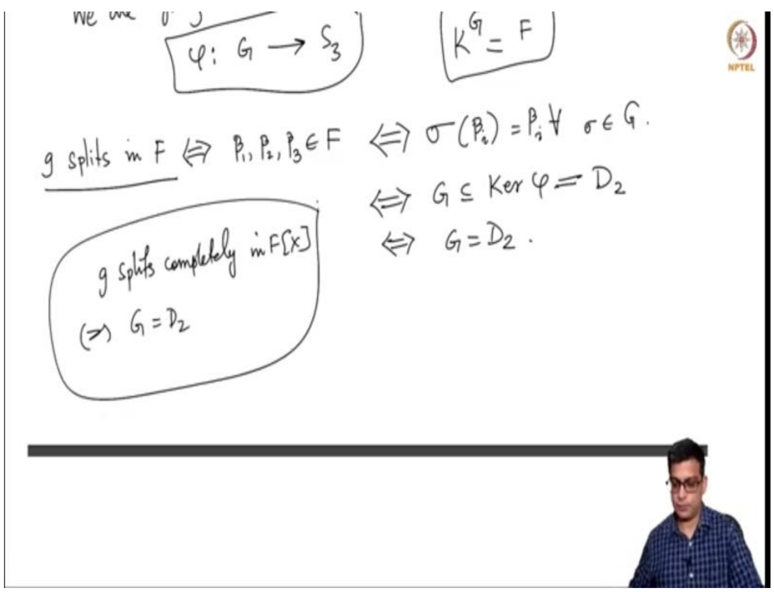
(Refer Slide Time: 21:58)



So, now let me start the proof. So, I do not know if I can finish this, but let me just see how much I can do. So, let me give a name to the set of beta i's. So, this is three elements in capital B, three distinct elements. That I already observed. So, B have three elements. So, now, S4 permutes alpha 1, alpha 2, alpha 3, alpha 4, S3 permutes, so this gives me a map from S4 to S3. So, you take any element of S4 and you apply it to, I mean, you, so I do not want to, you, if I will just write like that, but because beta 1 is alpha 1, alpha 2 plus alpha 3, alpha 4 and we already noted that sigma permutes beta i, so this is that map. So, sigma is a function of from this set to this set and you can think of sigma as a function from this set to this set. And of course, S3 is sitting, G is sitting inside S4. This is the situation we have. G is in fact a transitive subgroup of S4. So let us call this map phi.

(Refer Slide Time: 23:30)





$\text{ord}=4$

④ C_4 : cyclic gp of order 4 : there are 3 such subgps of S_4 all conjugate to each other.

$C_4 : \langle (1234) \rangle \hookrightarrow$ odd

⑤ D_2 : Klein 4-gp : only one of this

$D_2 = \{ e, \underbrace{(12)(34)}_{\text{order } 2}, \underbrace{(13)(24)}_{\text{order } 2}, \underbrace{(14)(23)}_{\text{order } 2} \}$. all these are even.

Lemma: Let $D = \text{Disc}(f)$. Then D is a square in $F \iff G = A_4$ or D_2.

Pf: Easy from the above list (and last class)

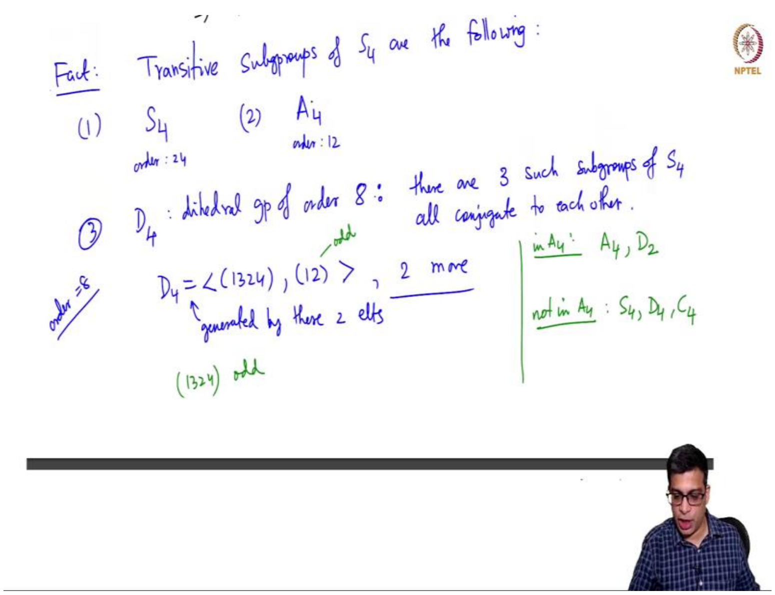
Pf: Easy from the above list (and last class)

To determine which case occurs, we need further analysis.

Resolvent cubic of f: Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in K$ be roots of f.

Define
$$\left.\begin{aligned} \beta_1 &= \alpha_1\alpha_2 + \alpha_3\alpha_4 \\ \beta_2 &= \alpha_1\alpha_3 + \alpha_2\alpha_4 \\ \beta_3 &= \alpha_1\alpha_4 + \alpha_2\alpha_3 \end{aligned}\right\}$$ all these are in K.

The "resolvent cubic" of f is defined to be:



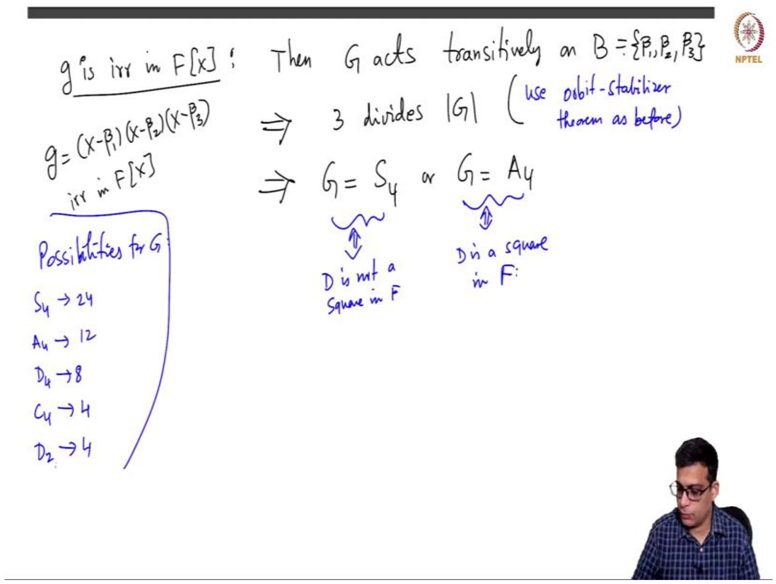
What is the kernel of phi? So, kernel of phi is all the things that fix beta i. That means it consists of elements of S4 that, which have this property. But if you look at this, of course, identity will be there. It will also contain this, because this fixes beta 1, this also fixes beta 2 and this fixes because alpha 1 goes to alpha 3. So, what is the D, this D2, so 13, 24. So, this fixes beta 2 because alpha 1, alpha 3 goes to alpha 1, alpha 3, alpha 2, alpha 4 goes to alpha 2, alpha 4.

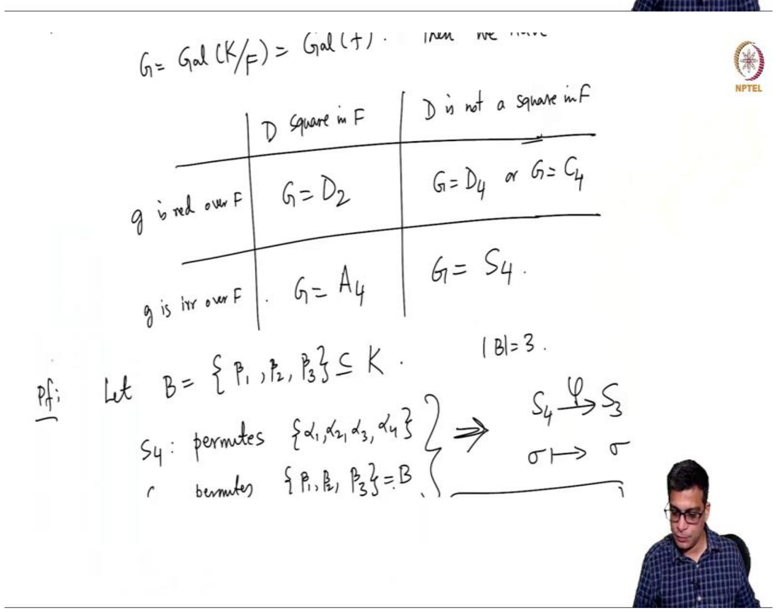
Similarly, 14, 23 fixes this because 1, 4 that means alpha 1, alpha 4 goes to alpha 1, alpha 4. So, this is 13, 24, 14, 23. So, this of course, in my earlier list this is D2. So, kernel is precisely D2. Now, we are going to consider. So, phi is from S4 to S3 and G is 0. So, no doubt, consider the restriction phi to G. So, I am also going to denote that by phi, by abuse of notation, I will use the same phi and you show that, I will analyse this.

So, first I want to assume g splits in F. I will analyse this case. That means this is equivalent to, splitting for me always means it is a product of linear polynomials. G is a product of linear polynomials. It is x minus beta 1 times x minus beta 2 times x minus beta 3. So, that means beta 1, beta 2, beta 3 are in F, but this means sigma of beta i is equal to beta i for all sigma in G, because sigma fixes any element means those elements, if every element of G fixes something that is in the fixed field, which is F.

So, sigma beta is equal to beta i for all sigma in G, but that means G is kernel phi, because what is kernel phi. These are elements in S4 such that sigma x trivially, I mean, this is what in words it means. Those things that map beta is 2 beta themselves. Each beta into that beta i is in the kernel but remember, on the other hand, G from our list, the list of possible Gs. It is contained in D2 now we concluded but it cannot be S4, it cannot be A4, it cannot be D4 for obvious degree order reasons. It cannot be C4 also because C4 cannot be contained in D2. Kernel is D2. That I established already. So, that means G is equal to D2. So, if G splits completely, the Galois group must be D2. So, if G splits completely in FX, the Galois group is D2. So that is what I have proved.

(Refer Slide Time: 27:41)



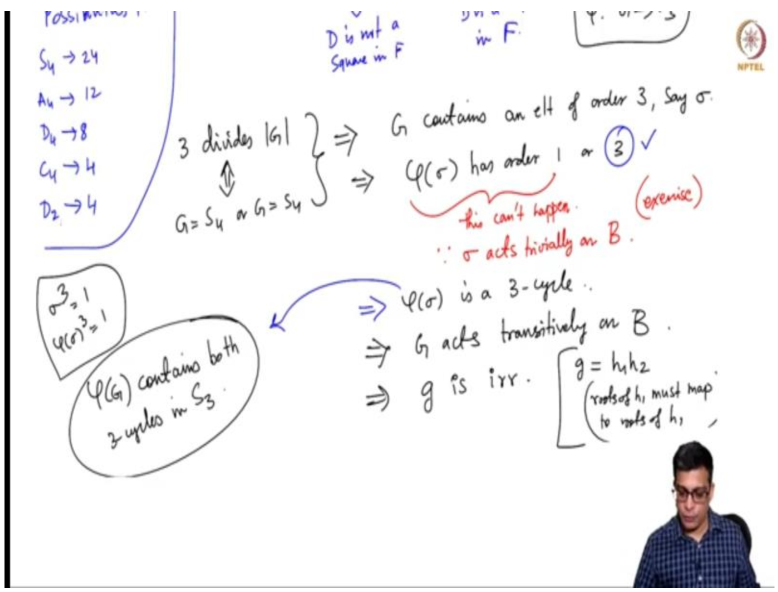


Now, I will consider the case that G is irreducible. Of course, maybe it is not irreducible and maybe it does not split completely, but nevertheless I will consider these two cases first. G is irreducible in FX, but then G acts transitively. See, that is because G is x minus beta 1, x minus beta 2, x minus beta 3 and this is irreducible in FX. That means any two roots can be permuted by a Galois group element. So, G acts transitively on B.

That means G acts transitively on 3 means, 3 divides order of G. So, this is as before. Because you take the orbit of beta 1 times the stabilizer of beta 1 is the cardinality of G. Orbit of beta 1 is 3, so 3 divides G. This implies, there is only one possibility, two possibilities rather, G is A4 or S4. Because, I mean, I will maybe instead of just going back I will write possibilities for G. So, S4 degree 24, A4 degree 12, D4 degree 8, C4 degree 3, D2, sorry, C4 degree 4, D2 also degree 4. So, 3 divides the cardinality of the group means it has to be the first 2.

So, G is S4 or A4. That is good. On the other hand, and of course this happens if and only if D is not a square in F. This happens if and only if D is a square in F. Of course, if D is a square in F, it can also be D2 but I am in the sub case of G irreducible here. So, I am beginning to prove this theorem. G is reducible, I have already showed that it is either A4 or S4. So this case I have done. Of course, I have to show that this does not happen here, that I will show next.

(Refer Slide Time: 30:34)



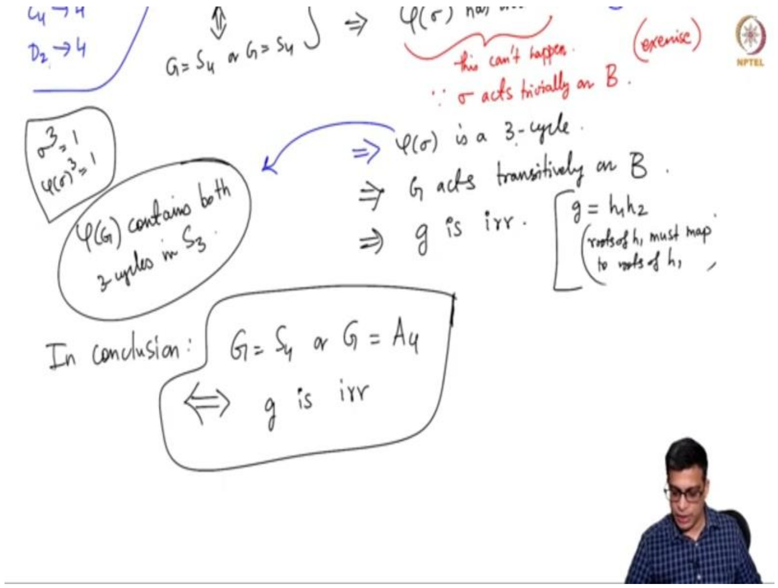
Now, I consider the case, 3 divides the order of, so that means G is A4 or S4. So, 3 divides the order of the group and among the list, the only possibilities are these two, because these numbers are not divisible by 3. So, in this case, G contains an element of order 3, because 3 is a prime and Cauchy's theorem says that, if a prime number divides order of a finite group, there is an element of that order. That means safe sigma. Sigma has order 3. So, phi of sigma, phi is a map from G to S3. Phi of sigma has order 1 or 3 because order of an element, order of the image of an element divides the order of that element.

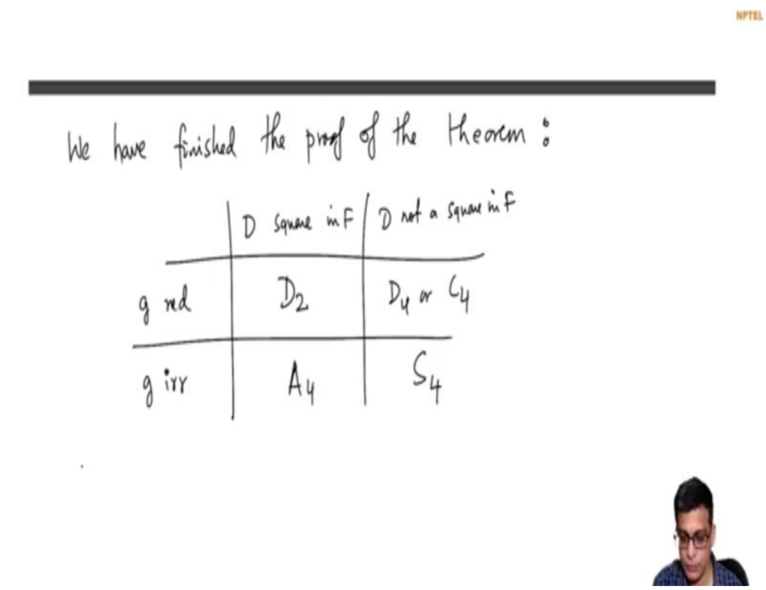
So, phi of, so basically sigma cube is identity, so phi of sigma cube is identity. That means phi of sigma has order 1 or order 3. But phi of sigma has order 1 is not possible, because this cannot happen, because if phi of sigma has order 1, so this means sigma acts trivially on B. So, I, so let me just leave this as an exercise. I do not at this point quickly recall the statement here, but this is to do with this case. So, I will tell you this in the next video, but it cannot be this. So, I claim that it has to be this. Let me move on. We will come back to this.

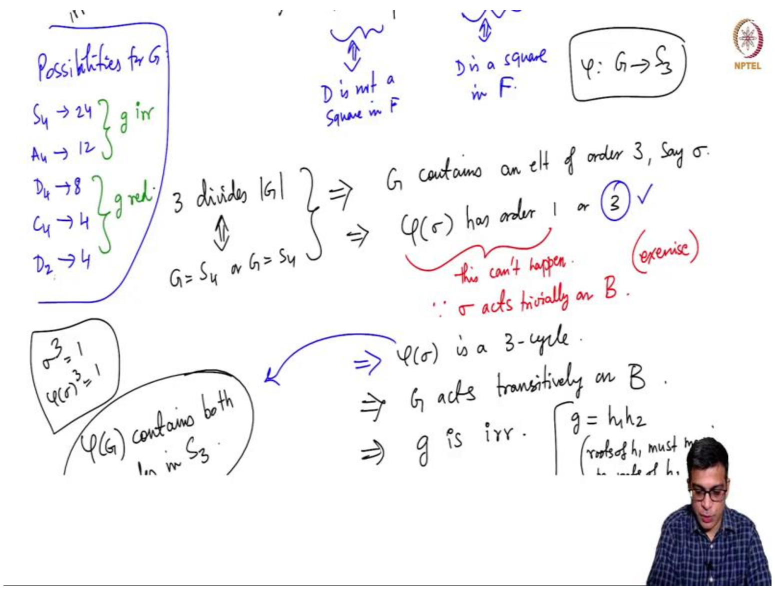
So, phi of sigma has order 3. But if phi of sigma has order 3 in S3, so phi of sigma is an S3 so that means it is a 3 cycle. That means G acts transitively on B, because a 3 cycle already interchanges all, if phi of sigma is 3 cycle, then phi of sigma square is the other 3 cycle and together they are transitive. So, that means image of G contains both 3 cycles in S3, because phi of G contains phi of sigma as well as phi of sigma square. So, that means phi of G is a transitive subgroup of S3. That means G acts transitively on B.

This implies G is irreducible. So, this is because if G is not irreducible, you cannot interchange roots of distinct irreducible factors. So, if G is equal to h1 h2 and both are degree, positive degree so roots of h1 must map to and roots of h2 also. So, you cannot send a root of h1 to another root of h2. So, if it is irreducible, G cannot act transitively. So, the statement is the Galois group acts transitively on the roots of a polynomial if and only if the polynomial is irreducible. So, G is irreducible. So, what we have shown is, if G is irreducible G is equal to S4 or A4. If G is equal to S4 or A4, G is irreducible.

(Refer Slide Time: 35:00)





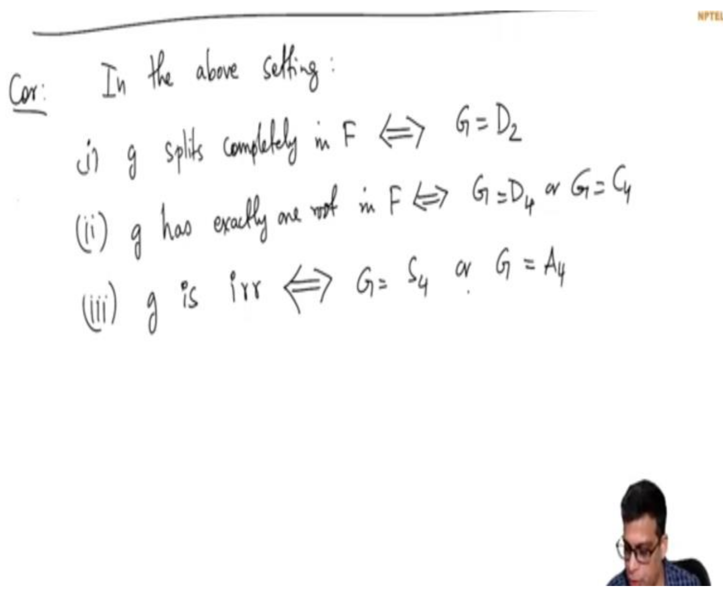


So, in conclusion G is S4 or G is A4 if and only if G is irreducible. So, I am sorry. I am going fast about this and maybe this is just too much material to grasp in a video, but please pause it, watch it multiple times if needed to conclude what I am writing here. So, essentially this slide here contains the proof that this this equivalence. If G is a irreducible, you concluded that capital G is S4 or A4. On the other hand, if capital G is S4 or A4, we have concluded that small g is irreducible.

And now I claim that we have finished the proof. We have finished the proof of the theorem, because, maybe I will write the proof here, statement here. So, D square in F, D not a square in F, g reducible, g irreducible. So, this is A4, this is S4. I hope that is what I wrote. So, this bottom row I have established conclusively. If g is A4, then it is irreducible, g, S4 then it is irreducible. If it is irreducible then it is A4 or S4, and where they fit in depends on the discriminant, whether it is a square or not.

So, the other case is this. In this case, you have only 3 possibilities. So this, these are when G is irreducible. These are when G is reducible and G is reducible and capital D is a square. It has to be D2, because only possibilities are D2, C4, D4, but the cases of C4 and D4 are not in that case, they contain odd permutations. So, D is not a square. So, finally, we have D4 or C4. So, this is done.

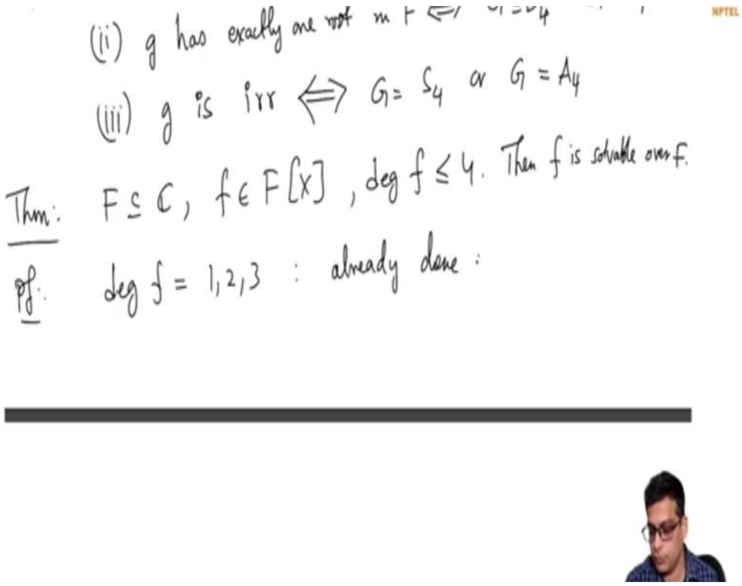
(Refer Slide Time: 37:25)

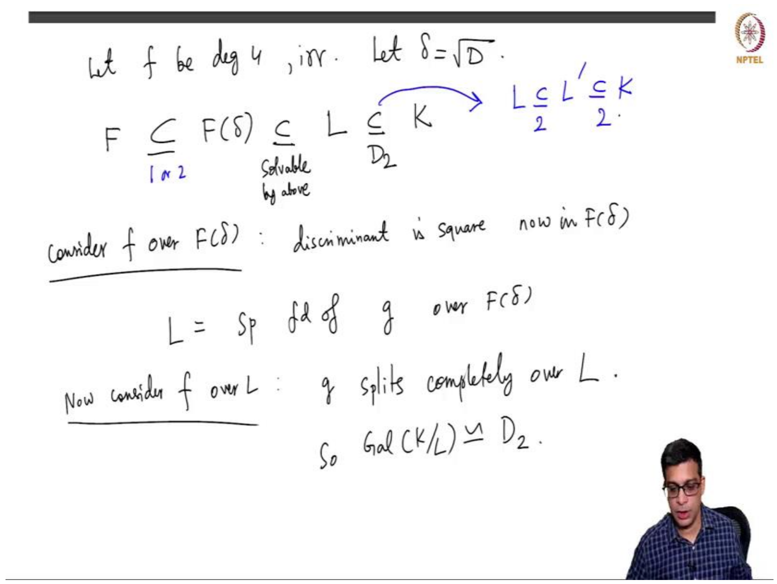


And in fact, I want to write, so this finishes the proof and I want to summarize this in a better way in the following statements, so in the above setting, same as above. G splits completely in capital F. This implies G is D2. In fact, you do not need to worry about whether capital discriminant is a square or not, because if G completes, if G splits completely we have showed that g is, small g spits completely, g is D2. So, I wanted to write this here. If G does not split completely but it is not irreducible that means it has exactly one root because if it has two roots, it will have the third root. So, if it is reducible does not split completely, that means it has exactly one root. So, this is a convenient way of doing this.

This is if and only if, then in this case G is either D4 or C4, if and only if again. The third one is g is irreducible if and only if G is S4 or G is A4. So, by looking only at the behaviour of G, you do get a lot of information. And to separate out these cases, in the second one, you cannot separate out these cases by discriminant because they both occur when D is not a square. You can only separate it out by looking at the degree or the order of G. In the third case, you can separate it out by looking at the discriminant. So, I hope this is clear. The proof essentially gives you this.

(Refer Slide Time: 39:16)





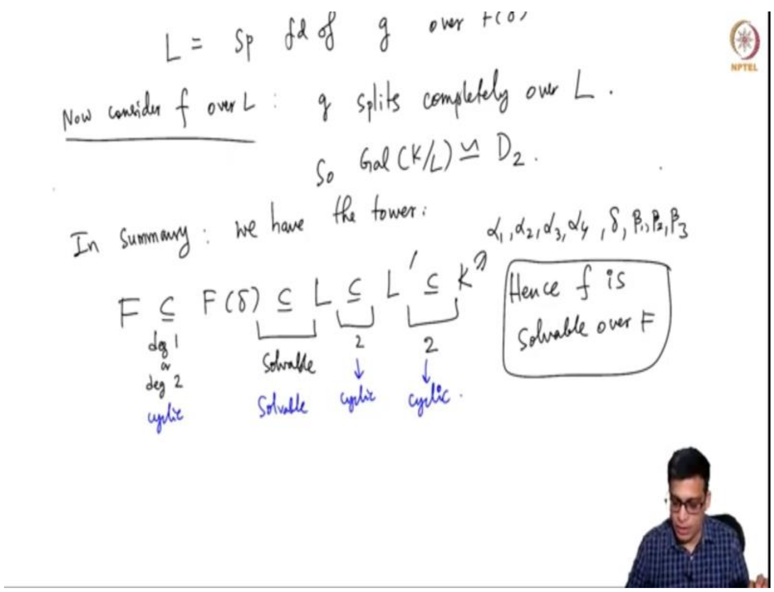
So, now finally the statement. So, capital F is a subfield of C, small f is a polynomial, degree f is less than or equal to 4. Then f is solvable over capital F. The proof, so this is our goal. In these two videos we are trying to prove this. First, we have already taken care of the cases 1, 2, 3. So, now let f be degree 4 irreducible. So, now what I do is, I do the following chain, tower. So, I start with F. Let delta be the square root of D. So, I will take F of delta. This is either degree here. So, this degree here is 1 or 2. Why is that? It is 1 or 2 depending on whether delta is in F or not. In other words, D is square or not. If D is a square, it is 1, if D is not a square it is 2.

But now look at f over this. Consider f over F delta. Here discriminant is a square now, because we have attached the discriminant. The polynomial is the same. The polynomial is still F. It is discriminative still capital D. The square root of the discriminant is still delta. But now in our base field, discriminant is there. So, now take the splitting field of the resolvent cubic over F delta. So you have L here. So, now this is a degree 3 polynomial over a field F delta. So this is solvable by case 3, because we have already taken care of degree 3 polynomials. So, this being the splitting field of a degree 3 polynomial is solvable.

Now, consider the same polynomial f over L. Now, the point is G, resolvent cubic stays the same. Again, F is the same F, resolvent cubic is the same. So, G splits completely over L. So, now you can consider, the splitting field will be the same, capital K, see, because along the way you have to add roots of all the, you have to add delta to get roots and you have to also add beta 1 through beta 2, beta 3 are all in K. So, all of this is happening within underneath K and this is degree 4.

Remember, if G splits completely in F, then G is D2. Capital G is D2. So, this is D2. So, Galois group of K over L is isomorphic to D2. But now D2 is solvable, because you can write L or K. L as K. So, this is degree 2. This is degree 2.

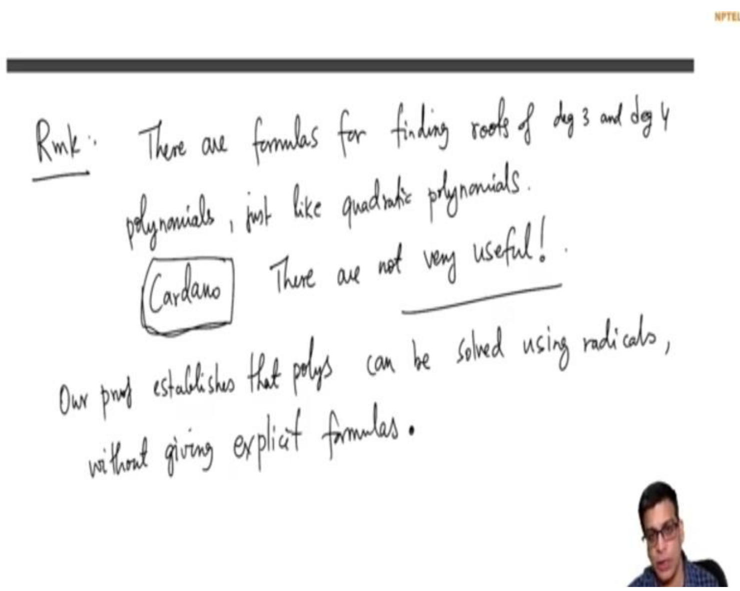
(Refer Slide Time: 43:08)

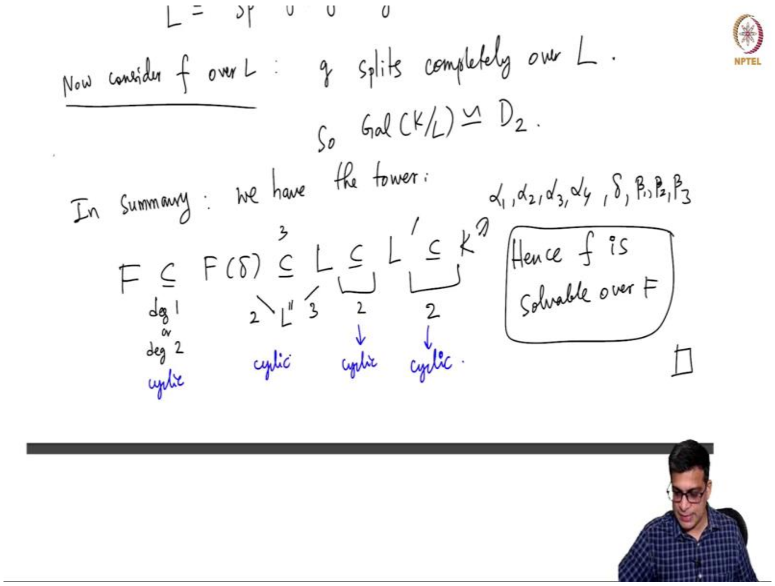


So now in summary what we have is, so this tower I will write in more detail. We have the following tower. So, we have F, F delta and L, L prime K. So, this is degree 1 or 2. This is solvable. This is 2, this is 2 and all the roots are in K. So, the point is delta is in K. Beta 1, beta 2, beta 3 are all in K. So, F delta, L, L prime are all in K. So, this is a tower. So, now this is degree 2. So, this is cyclic. Of course, this is solvable. So, it can be a tower of cyclic extension. This is cyclic. This is cyclic. So, we have a tower of cyclic extensions containing all the roots. So, hence, F is solvable over capital F.

So, this is a beautiful argument. So, you have all the roots living in a field which is a radical extension by our general theorem that we have proved. Remember that theorem allows, so the theorem is crucial here, because we are not talking about radical extensions here at all. I am not saying that each of them is obtained by adding a radical. I have taken care of that in my previous theorem and a now I am only saying that each of them is a cyclic extension. So, small f is solvable over capital F and this finishes the theorem. So, I have taken a lot of your time in this class. I am sorry about that, but let me end this class by the following remark.

(Refer Slide Time: 45:08)





So, there are formulas for finding roots of degree 3 and degree 4 just like quadratic formula, quadratic polynomials. So, the name that you see here is an Italian mathematician called Cardano. So, you find out if you search in various books or in, on the Internet, you will find that Cardano gave formulas for degree 3 degree 4, but these formulas are not very useful, because there is a lot of ambiguity about, when you take roots fifth root, third root, fourth root, it is not clear which roots you have to take. So, there is some ambiguity, and hence, they are not very useful. However, we have conceptually proved that there would be formulas using radicals by using this.

So, our proof establishes that roots can be solved using radicals, so rather polynomials can be solved using radicals without giving explicit formulas. So, we do not necessarily give explicit formulas, because that is not clear. We are conceptually saying that all the roots are in a tower or in a field and there is a tower starting in that field, ending with the base field where each of them is a cyclic extension.

So, now, I do not, so maybe I should really write here. So, this is degree 2, maybe L double prime so this is 2 and 3 or this is 3. So, I do not want to write solvable, but to say that everything is cyclic, so there is a tower of cyclic extensions ending with a field containing all the roots. So it is solvable. So, we do not necessarily have formulas and often we do not use formulas. We do not need to compute the roots explicitly, because the roots, the formulas themselves are often ambiguous and hence not useful.

But conceptually we have established that degree 4 polynomials, degree 3 polynomials, degree 2 and degree 1 polynomials can be solved by radicals and next we will take care of degree 5. And before that I am going to give you alternate proofs of these statements in the next class using solvable groups. So, let me stop this class here and in the next class we will continue studying solving polynomials by radicals. Thank you.