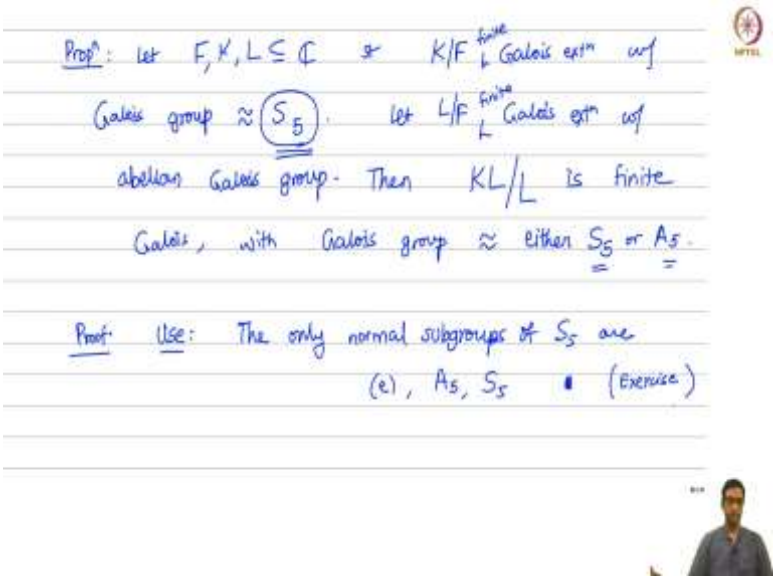
Algebra - II
Professor S Viswanath
Department of Mathematics
The Institute of Mathematical Science
Lecture 44
Insolvability of the General Quintic – Part 3

(Refer Slide Time: 00:14)



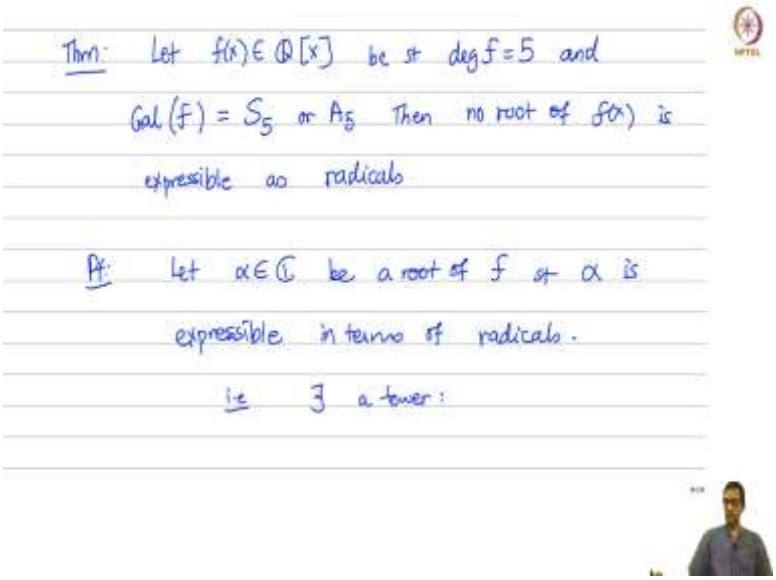
So we have proved the following corollary, recall that if I have K over F non-abelian and simple Galois extension L over F abelian, then you know, what it means is that these two groups cannot have then, so I should just write this down, then K intersection L is just F and the group K L over L has the same Galois group as K over F. Now, the point is we use this simplicity in a very important way. But it is, it is easy. If you just go back and see how the proof worked, we can actually prove the following proposition.

So, I have just written out here that even if it is not simple, but almost simple then we are still in good shape. So specifically, this is relevant to the insolubility of the quintic. So same assumptions as before I have K, F and L like before, except now I am assuming that so L over F is still abelian, K over F I assume is, it has Galois group S 5, then the conclusion K L over L is finite and its Galois group is not necessarily the same as this group S 5.

But it can differ by it by just a little bit, it can either be S 5 or it can be the alternating group A 5 and let me just say the proof is, well the exact same argument, we just have to use the following important property of S 5 that it is almost simple. The only normal subgroups have S 5 are in addition to identity and S 5 there is one additional guy which is A 5.

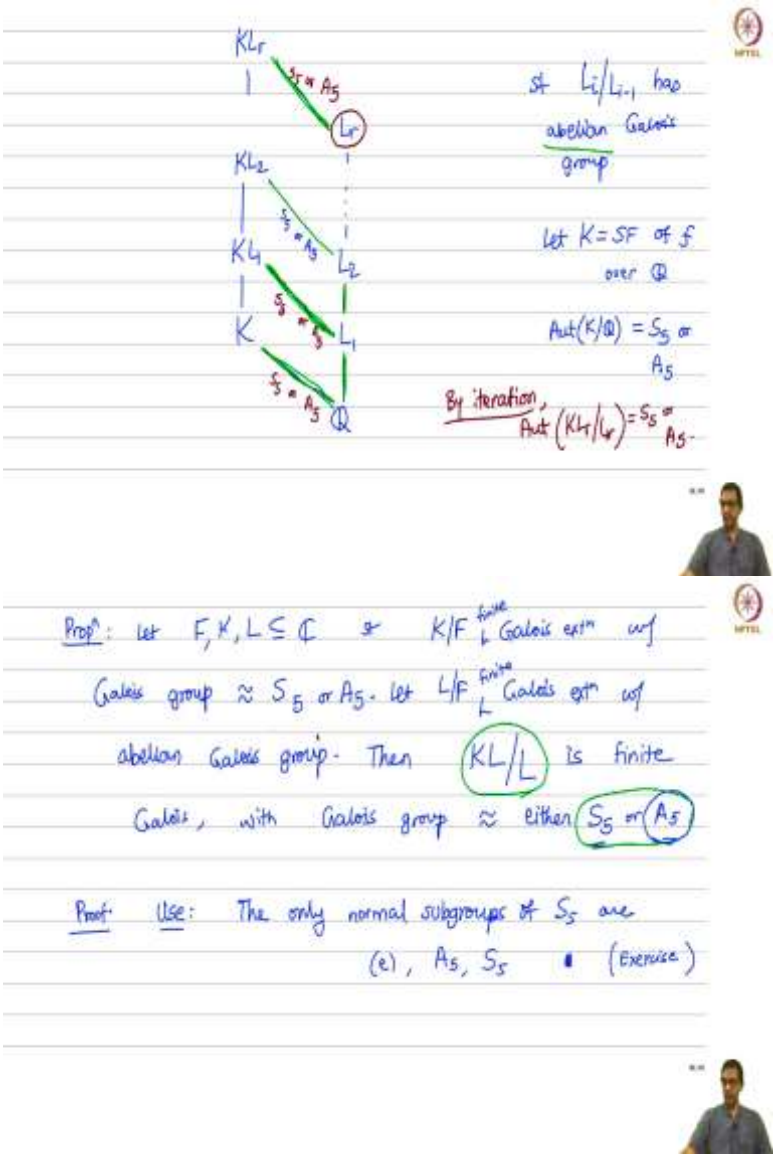
That is all you need to use. So I am just going to leave this proof as an exercise. Just redo all the very same steps and still works for a group like S 5 which is almost simple. Good and this is going to be relevant to the insolubility of the quintic. So Let us prove the main theorem on insolvability.

(Refer Slide Time: 02:38)



Says that, sorry state this earlier, let f of x in Q x be such that the degree is 5 and the Galois group Galois group of F, which means it is the Galois group of its splitting field. Galois group of F is S 5 or A 5 then no root of f x is expressible in terms of radicals.

(Refer Slide Time: 04:01)



Proof: So suppose I have a root, let alpha in C be a root of f such that alpha is expressible in terms of radicals. What does that mean? i e that exists a tower of fields. So what does the tower look like? So I have to take Q, which is my L 0 then there is L 1, L 2 and so on. So to till some L r so, that is my tower fields.

So maybe we will just push it down a little bit. So here is my tower fields; call this L 0. Well, with what property this tower has the following property; that each successive extension, each of these L i's is such that a L i by L i minus 1 has abelian Galois group. This was one of our propositions, has abelian Galois group and recall we did this by first adjoining and appropriate root of unity.

So the first step was the cyclotomic extension, which of course had an abelian Galois group. All the successive steps were just simple, radical extensions which had in fact cyclic Galois group but whatever it is every extension here has abelian Galois group. Now, what else are we assuming? We are assuming that, so let K be the splitting field of the given polynomial f over Q.

So, I have a polynomial a K, so let me do the following let me just push these make space for K. So this is my tower of extensions and K is the splitting field of this polynomial over the base field Q. Now, what does that mean? I mean how can I start using my previous proposition? We are given the following that the Galois group so auto morphism group of K over Q is S 5 or A 5. So, let us say suppose it is S 5. Let, let it be S 5 or A 5. This is given; now observe that you know how are we going to use our previous proposition?

So, let us see what the proposition said. It said if I have extensions in which the Galois group is S 5, then I can the group K L over L that Galois group is either S 5 or A 5. Now, in fact, this is for S 5 which is almost simple, if it is actually A 5, if the Galois group is equal to A 5, then the Galois group of K L over L is equal to A 5 also.

That is by the one corollary before this, if this is simple, then K L over L has the same Galois group. If it is almost simple like S 5, then the Galois group can (define) differ by a little bit, it became either S 5 or A 5. So, I can actually write my proposition like this, if originally my Galois group was S 5 or A 5, then the composite will also have Galois group either S 5 or A 5. So now that that allows us to make this argument a bit more compact.

So what am I assuming? I am assuming that this Galois group here K over Q is either S 5 or A 5; I know that this Galois group L over Q is abelian that was my assumption. Therefore, by our composites theorem, it says if you look at the composite of K and L 1, so let us look at the composite K L 1, then K L 1 over L 1 is also Galois and its Galois group is either S 5 or A 5.

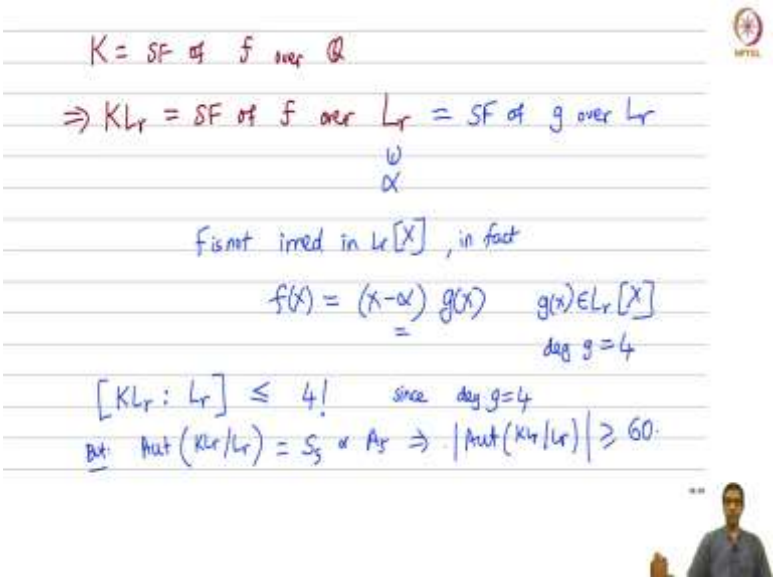
So, let us just mark this here, so this guy here has Galois group S 5 or A 5 and by our previous corollary, this also has Galois group S 5 or A 5. Now it is, it is perfect for an iteration. This guy here L 2 over L 1 is again, abelian. This parallelogram arrow here is it is a Galois group. It is a Galois extension with S 5 or A 5 as Galois group.

So again, we can perform another composite. So let us look at K L 1 with L 2. So it is K L 1 L 2 that is the same as K L 2 because L 2 is bigger than L 1. So, the composite K L 2 again by the same logic, because this fellow is S 5 or A 5 and the other one is abelian this has to be a S 5 or A 5 and so on.

So, you go all the way up till you reach the composite K L r and you conclude that at even the top most step there at this extension K L r over L r has Galois group, which is S 5 or A 5. So, by iteration of this argument, what do we conclude? We conclude that the auto morphism group of K L r over L r is either S 5 or A 5.

Now, what did we assume about this this tower? There exists a tower such that forgot to say this alpha belongs to the topmost, the topmost layer of this tower, the element alpha that we picked which can be expressed in terms of radicals alpha belongs to L r. Now, observe that what is this this K L r that we are talking about here?

(Refer Slide Time: 09:51)



See K was the splitting field of the polynomial f over Q. Therefore, by what we had seen earlier the composite K L r is just a splitting field of the same polynomial, but over a larger field, over the field L r. Now, the interesting thing is this root alpha is actually already in L r and that that is a, that is an important fact. The root f has one root alpha in this field L r. So, how does f split over L r?

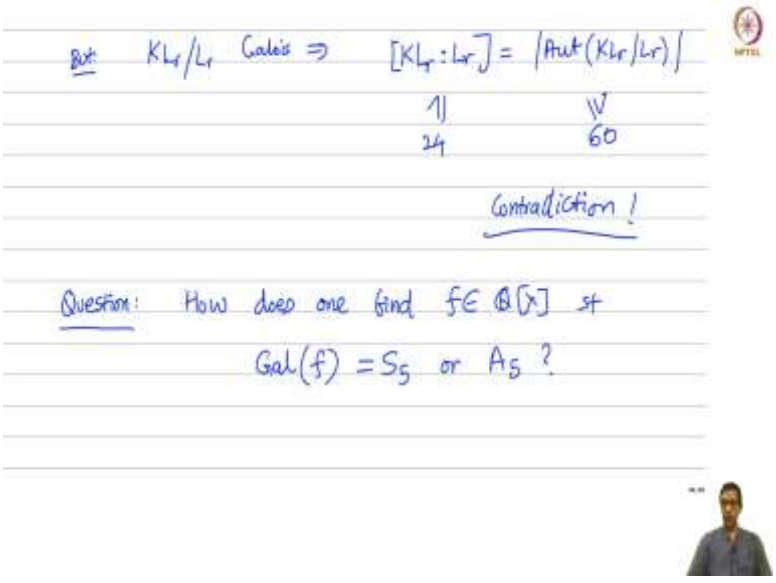
If you wish, so if you, you know the key point is f cannot be irreducible. f is not irreducible, definitely f is reducible. In fact, what do we know f of x can be written as surely x minus

alpha is a factor times some polynomial G x. So what is G x? G x is a polynomial of degree 4. Now, the splitting field of f over L r since alpha is already there in L r, you do not need to look for something which splits that, this is the same as the splitting field of G over a L r because alpha is already taken care of that factors taken care of.

Now, G however is really a degree 4 polynomial the degrees come down by 1 and that is going to be a problem, why? Because recall, we know something; the splitting field of a polynomial, the splitting field of the polynomial G over the base field, the degree I mean, this extension has degree which is at most, the degree of the polynomial factorial.

Since degree of G is 4 the splitting field of G can be at most 4 factorial degree over L r. But what do we know? We also know that the Galois group, we know this is Galois and the Galois group is either S 5 or A 5. But now, here is the contradiction; auto morphism group of K L r over L r by our iteration argument was either S 5 or A 5, which implies its cardinality is at least that of A 5.

(Refer Slide Time: 12:37)



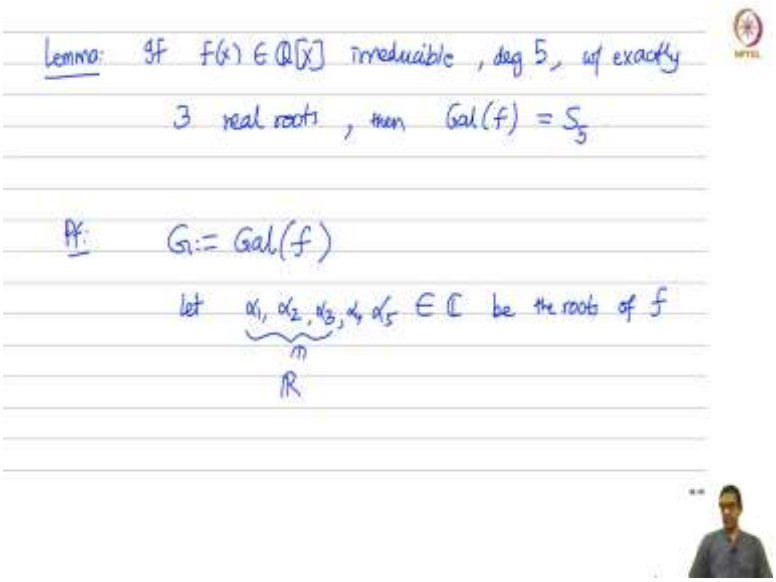
So the cardinality of the auto morphism group is at least 60, which is the cardinality of A 5 but these two numbers must be the same because it is a Galois group. But because it is a Galois extension, so K L r over L r is Galois implies that the degree of the extension is equal to the cardinality of the Galois group.

Now, that is a contradiction because on the one hand, this fellow is at most 24 and on the other hand, this is at least 60. So that is a contradiction. So, we have managed to show that

you cannot hope to express root of such a polynomial by means of radicals but this you know, this still leaves open the following final question which we lack an answer.

Just how does one find a polynomial whose Galois group is either a S 5 or A 5? How does one find a polynomial f in Q x such that its splitting field has Galois group over Q, which is either S 5 or A 5? How do you find it?

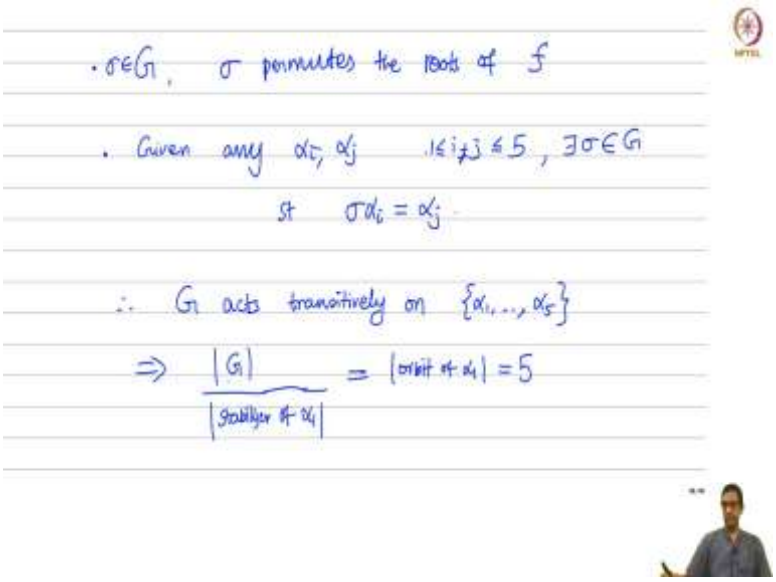
(Refer Slide Time: 13:52)



And now there is a little lemma which tells us when this will hold, lemma is that if I take an irreducible polynomial, irreducible degree 5 with exactly 3 real roots, the other 2 have some they are complex, they have some non-zero imaginary part. If this happens, then the Galois group of this polynomial is in fact S 5.

So this this gives you a way of constructing a polynomial whose Galois group is S 5. So Let us prove this. So suppose I take this, this is such a polynomial, let us give it a name, let me call its Galois group G. Now observe, so let alpha 1 through alpha 5 be the complex roots of this polynomial and C be the roots of the polynomial and we will assume that the first three guys are real and the other 2 are not real.

(Refer Slide Time: 15:13)



So let us say that these three are our real numbers. Now the first observation which is we know, you know to prove that the Galois group is S 5, we will construct you know elements with generator S 5 inside the Galois group. So observe firstly that the Galois group what does it do when it acts. So, if we take an element of the from G, then what does sigma do to any one of the alphas?

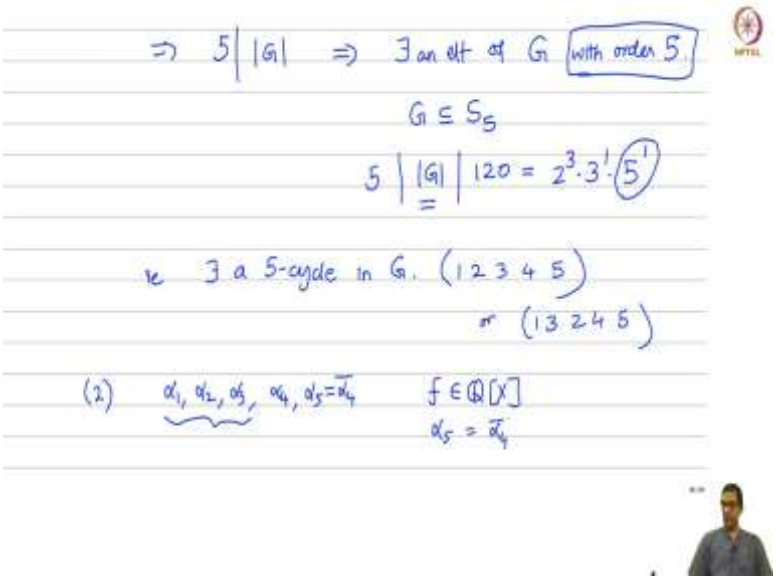
Sigma must map each alpha i to one of the other alpha j's. Sigma permutes the roots of f necessarily. So, there is our usual fact if alpha is the root of f sigma alpha must be root of f. So, sigma must permute the roots of f among themselves and there are 5 roots and we also know that sigma, there are there always exists an element of the Galois group which takes any root of f to any other root of f if f is irreducible.

So, given any alpha i and alpha j here, i and j between 1 and 5 so, any two distinct guys, there always exists an element of the Galois group, which maps alpha i to alpha j. It is the other fact that we have seen before. So, in terms of group actions, what this says is that, if you recall group actions, this says that G acts transitively on the set alpha 1 to alpha 5.

It always acts transitively, meaning there is only a single orbit. Therefore by the orbit stabilizer theorem for transitive actions, this says that the cardinality of G modulo the cardinality of the stabilizer of any one element, let us say the stabilizer of alpha 1, this is just the cardinality of the orbit of alpha 1 and the orbit cardinality is 5 in this case. So, this is the

orbit stabilizer theorem for group actions. So, what this means is that the cardinality the group is of the form 5 times something.

(Refer Slide Time: 17:25)



So, this means that 5 divides the cardinality of the group. So, I still do not know that G is S 5, but at least I know that 5 divides the cardinality of the group and so what can I conclude by that? This means that there exists a 5 cycle so there exists an element of G with order 5. So, observe that G must necessarily be well what else do we know?

G is surely you can think of it as a subgroup of S 5 because G permutes the 5 roots. So, the cardinality of G divides 120, which is the cardinality of S 5 and we also know that 5 divides the cardinality of the group. So, in fact I mean the 5 Sylow subgroup if you wish. So, what is 120? It is 24, which is 8 into 3 into 5.

So, since you know the cardinality of G can only have at most 5 power 1 as a power and 5 definitely occurs therefore, this element of order 5, it generates, in fact the 5 Sylow subgroup if you wish of this group G. So that surely is a 5 Sylow subgroup and so we take, we take that 5 Sylow subgroup or the element of that, that cyclic so we take that element there. So, let us give this a name that exists an element of with order 5.

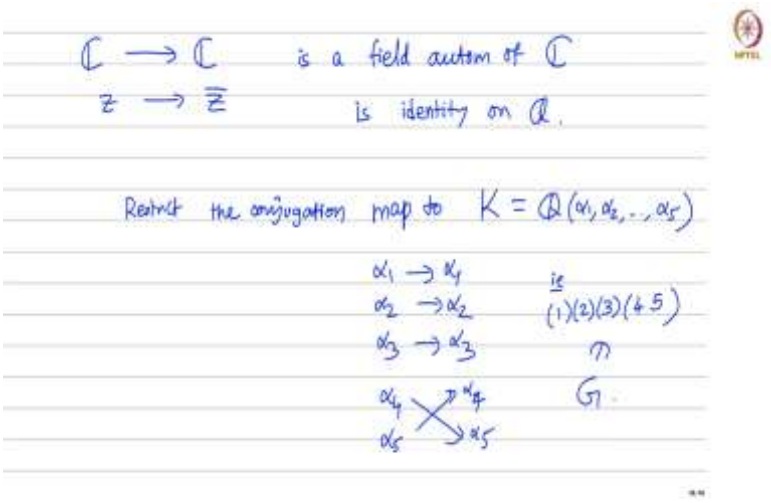
So that is a 5 cycle, i e there exists a 5 cycle. So what are the elements of S 5 whose order is 5? So they all look like this. So it is it they permute the 5 numbers cyclically among themselves. Now or you know, 1 3 to 4 or 5, whatever. So anything which permits the 5

numbers cyclically will have order 5 and those are the only numbers, only permutations which with order 5.

So this is, this is the first observation about G. Now, there is a second observation which comes from the fact that it is got exactly 3 real roots and 2 roots which have non-zero imaginary part. Now, look at these two roots alpha 4 and alpha Phi. So observe that so you know this fact that if I have a polynomial with real coefficients, so in this case, rational coefficients are certainly real coefficients, when its roots occur in conjugate pairs.

So here, these three are of course already real and the other two guys which are not real must be conjugate of each other. So, we also know this alpha 5 must actually be the complex conjugate of the element alpha 4. Alpha 5 is the complex conjugate.

(Refer Slide Time: 20:14)

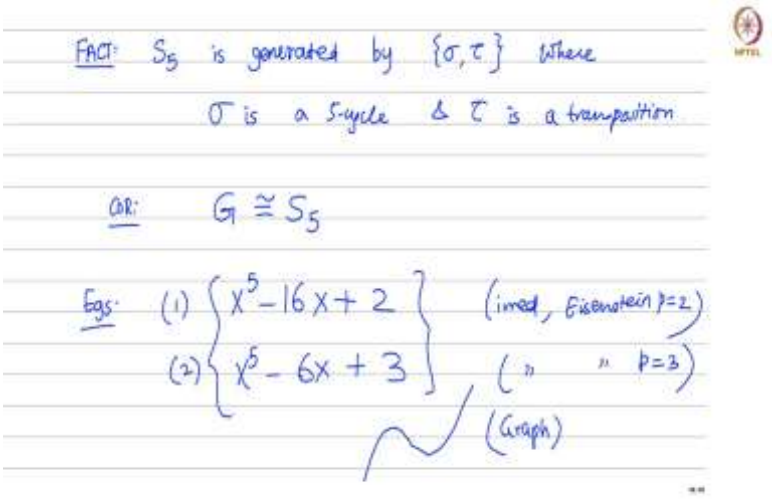


Now, observe that we have an auto morphism of C. So, look at the complex numbers, the conjugation map is actually a field auto morphism if you wish, this is a field auto morphism preserves all the operations the field auto morphism of C and its identity is, this map is of course, identity on r and therefore on C on Q sorry. Now so, what you do is you restrict this this conjugation map to K.

So, you restrict the conjugation map to the splitting field K, K is just Q alpha 5. Now, what is this conjugation map do? Well, it fixes alpha 1, 2 and 3. So this map behaves like this on the roots, it sends these to themselves and it interchanges these two guys alpha 4 and 5 alpha 4, alpha 5.

Now, what sort of element is this, if you think of in terms of the group action on these 5 elements, this is like a transposition? i.e, this acts as follows. It is like it sends the first three elements to themselves and it transposes the fourth and the fifth elements. So such there exists a transposition in your group G.

(Refer Slide Time: 21:44)



So the Group G has two kinds of elements, it is got a 5 cycle and a transposition and this is now a fact about the symmetric group as 5 that you need these two elements generate S 5, S 5 is generated by any pair sigma tau, where sigma is a 5 cycle and tau is a transposition. So with this fact one is, one is more or less done because now corollary; so let us accept this without proof.

It is rather easy to prove this. Now, what this implies is that G contains both a 5 cycle and a transposition. So there is no other way out. It is got to be the entire group S 5 and finally, what are examples of you know, so there is always so we have a nice criterion here, what sort of polynomials will have this property?

You just need to look for something which is irreducible and has three real roots. So to do irreducibility, you could look for things; you can use the Eisenstein's criterion. So let me just give you two examples of polynomials which have this property.

It is got degree 5 and this is irreducible because you can use Eisenstein's criterion with P equals 2, the one below is irreducible by using Eisenstein with P equal to 3 and to check that they have only three real roots, what you could well maybe do is sort of look at the graph of

the polynomials. So just graph the polynomial and you know, of course that is probably not a completely fool proof thing.

But, you know you can check that it is got only three real roots. So such a graph will look like this? So it is got one real root, two real roots and three real. So if it is monic, then it is like this or you can take derivatives and so on. So any which way so, here are examples now of the polynomials which, no matter how hard you try, you cannot write the roots of this polynomial using radicals.