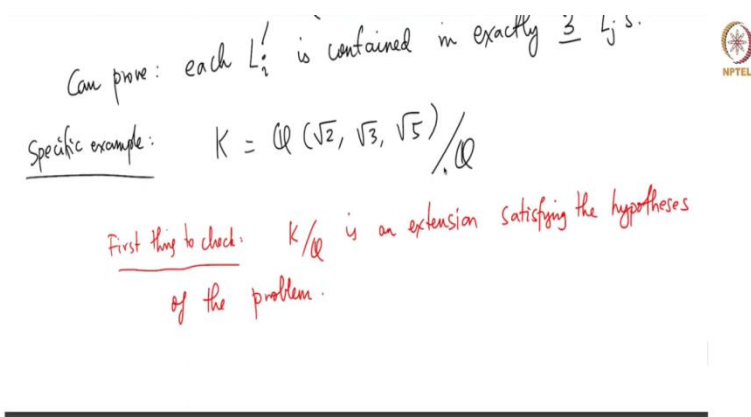


Introduction to Galois Theory
Professor Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute
Lecture No. 31
Problem Session - Part 9

(Refer Slide Time: 00:23)



Can prove: each $L_i^!$ is contained in exactly $\underline{3}$ L_j 's.

Specific example: $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q}$

First thing to check: K/\mathbb{Q} is an extension satisfying the hypotheses of the problem.



Welcome back. We are in the middle of doing one problem. And I wanted to do a separate video for this particular example because it illustrates many of the beautiful things that Galois Theory tells us. Okay, so let me continue just where I left last time, and then work out the Galois Theory of this extension in complete detail. So we have this extension.

(Refer Slide Time: 00:41)

Claim: $[K:Q] = 8$

$Q(\sqrt{2}, \sqrt{3}) = Q(\sqrt{2})(\sqrt{3})$
 $|\leq 2$ (*)
 $Q(\sqrt{2})$

$\sqrt{3}$ satisfies a deg 2
 poly over $Q(\sqrt{2})$, namely $x^2 - 3 \in Q(\sqrt{2})[x]$

To prove $= 2$ in (*), we need to show $\sqrt{3} \notin Q(\sqrt{2})$

$K = Q(\sqrt{2}, \sqrt{3}, \sqrt{5})$
 12
 $Q(\sqrt{2}, \sqrt{3})$
 12
 $Q(\sqrt{2})$
 12
 Q

why is this 2?
 definitely know this has deg 2.

$\sqrt{3} \in Q(\sqrt{2})$
 $\sqrt{3} = a + b\sqrt{2}, a, b \in Q$
 $a=0 \Rightarrow \sqrt{3} = b\sqrt{2} \Rightarrow 3 = 2b^2 \Rightarrow b^2 = \frac{3}{2} \cdot x$
 $b=0 \Rightarrow \sqrt{3} = a \in Q \cdot x$
 $ab \neq 0 \Rightarrow 3 = a^2 + 2b^2 + 2ab\sqrt{2} \Rightarrow \sqrt{2} = \frac{3 - a^2 - 2b^2}{2ab}$

So first claim that I want to make is $K:Q$ is 8. So I want to do this in detail, because once you understand the calculations I do in this example, you can use this in many problems. And these are sort of standard calculations that come up all the time. So K is by definition, root 2, root 3, root 5. So I am going to do this in the following way. So first do root 3 root 2, then do root 2, then do Q . So the way of proving this is, of course, to prove that these are all 2. But we have never really discussed why these are all 2.

We definitely know this has degree 2. That way, definitely not because root 2 is not in Q . And root 2 satisfies a degree 2 polynomial Q , that is irreducible. So this is true. But why is this 2? So, as I said, I am going to do this really from first principles and work out the details. So, Q adjoined root 2 root 3 is of course Q adjoined root 2, then Q adjoined root 2. So, you can think of this as an explanation of Q root 2 generated by root 3, and root 3 satisfies a degree 2 polynomial over Q root 2, namely $x^2 - 3$, which is in $Q[x]$, which is of course in Q root 2 x also. So, this to begin with is at most 2 is all we can say, to prove equality here. To prove equality in star, we need to show root three is not in Q root 2.

So, it could very well be, right, unless you prove it, you cannot be sure about this. So, if root 3 is in root 2, Q root 2, then this will be a degree 1 extension. So Q root 2, 3 Q root 2, root 3 will be same Q root 2. So, why is this true? The proof of this is as follows. So, suppose, root 3 is in Q root 2, we already know that Q root 2 is a Q vector space spanned by 1 and root 2. So, there will

be a, b rational numbers such that $\sqrt{3}$ is equal to $a + b\sqrt{2}$. So, if a is zero, this implies $\sqrt{3}$ is equal to $b\sqrt{2}$, this implies 3 equals to $b^2 \cdot 2$. So that means b^2 is $3/2$, but this is not possible because there is no rational number whose square is $3/2$. So because $3/2$ square root is irrational. Similarly b is zero, this is more easy, $\sqrt{3}$ is in \mathbb{Q} , this is not possible.

This is my symbol for contradiction, okay. So, suppose AB is nonzero, the third case is a zero then we are done b zero, we are done. So both of them are nonzero. Then square this to get $3 + 2ab\sqrt{2}$ equals $a^2 + 2b^2 + 2ab\sqrt{2}$, right. But this means $\sqrt{2}$ equals $(3 - a^2 - 2b^2) / (2ab)$, which is in \mathbb{Q} . So that is again a contradiction, right? So this is a standard calculation that comes in the beginning of field theory. So this is just a way of reminding you this calculation. So hence, this is 2, right. So this is 2, $\sqrt{3}$ is not in $\sqrt{2}$.

And another way of stating this is, $\sqrt{3}$ is not in $\sqrt{2}$ means this is equivalent to saying that $\sqrt{3}$ and $\sqrt{2}$ are linearly independent as elements of vector space over \mathbb{Q} . Because if $\sqrt{2}$ and $\sqrt{3}$ are not linearly independent, you can write $\sqrt{3}$ as a linear combination of 1 and $\sqrt{2}$ okay. So that you can check, I mean, it is, in fact, $\sqrt{2}$ times a . This is equivalent to this, almost equivalent to this. So this way of raising this will also be useful later. Because that is another way of showing that these are, this is a degree 2 extension, okay. This is degree 2, but now the question is, why is this degree 2? Because, if this is degree 2, then the whole thing will be degree 8.

(Refer Slide Time: 06:12)

To prove $[K:Q] = 2$ in (8), we need to show $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$.
 Another way of stating this: $\sqrt{3} \notin \mathbb{Q}(\sqrt{2}) \Leftrightarrow \sqrt{2}, \sqrt{3}$ are lin ind over \mathbb{Q} .
 Why is $[K:Q(\sqrt{2}, \sqrt{3})] = 2$? As before $[K:Q(\sqrt{2}, \sqrt{3})] \leq 2$.
 $[K:Q(\sqrt{2}, \sqrt{3})] = 2 \Leftrightarrow \sqrt{5} \notin \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
 But by main theorem, we know already
 $\sqrt{5} \in \mathbb{Q}(\sqrt{2}, \sqrt{3}) \Rightarrow$
 $\mathbb{Q}(\sqrt{2}, \sqrt{3})$
 \mid
 $\mathbb{Q}(\sqrt{5})$
 \mid
 \mathbb{Q}

$a=0 \Rightarrow \sqrt{3} = b\sqrt{2} \Rightarrow 3 = 2b^2 \Rightarrow b^2 = \frac{3}{2} \cdot X$
 $b=0 \Rightarrow \sqrt{3} = a \in \mathbb{Q} \cdot X$
 $ab \neq 0 \Rightarrow 3 = a^2 + 2b^2 + 2ab\sqrt{2} \Rightarrow \sqrt{2} = \frac{3 - a^2 - 2b^2}{2ab} \in \mathbb{Q} \cdot X$

So, the last step is, why is $[K:Q(\sqrt{2}, \sqrt{3})] = 2$? So as before, $[K:Q(\sqrt{2}, \sqrt{3})] \leq 2$, because K is generated over $Q(\sqrt{2}, \sqrt{3})$ by $\sqrt{5}$, and $\sqrt{5}$ does satisfy a degree 2 polynomial over that field, namely $x^2 - 5$. So the degree is at most 2, and it is equal to 2 if and only if $\sqrt{5}$ is not in $Q(\sqrt{2}, \sqrt{3})$. Because that means if it is not 2, that means it is 1. If it is not 2, that means it is 1, but that means $\sqrt{5}$ is already there. But suppose $\sqrt{5}$ is not there, so this is a cute argument, so please think, look at this carefully.

Suppose, so I am trying to show that $\sqrt{5}$ is not there, but if $\sqrt{5}$ is in there, then we have that $Q(\sqrt{5})$ is an intermediate field. So that means $Q(\sqrt{5})$ is an intermediate field of this extension, but by Main theorem of Galois Theory, we know already that there exists only 2 trivial nontrivial but 4 altogether intermediate fields of $Q(\sqrt{2}, \sqrt{3})$ over Q , right.

So, what I am hiding under the carpet here is the Galois group of $Q(\sqrt{2}, \sqrt{3})$ over Q is $Z_2 \times Z_2$, because $\sqrt{2}$ and $\sqrt{3}$ are independent, you can send $\sqrt{2}$ to any of its conjugates independently of image of $\sqrt{3}$, and there are 4 such automorphisms and they are $Q(\sqrt{2}, \sqrt{3})$, the 4 intermediate fields are $Q(\sqrt{2}, \sqrt{3})$, $Q(\sqrt{2})$, $Q(\sqrt{3})$ and Q . So, clearly $Q(\sqrt{5})$ cannot be equal to this.

So, $Q(\sqrt{5})$ is one of them. Can it be equal to this? Cannot be for degree reasons right because $Q(\sqrt{5})$ is a degree 2 extension this, whereas, this is a degree 4 extension as we just shown. So, it

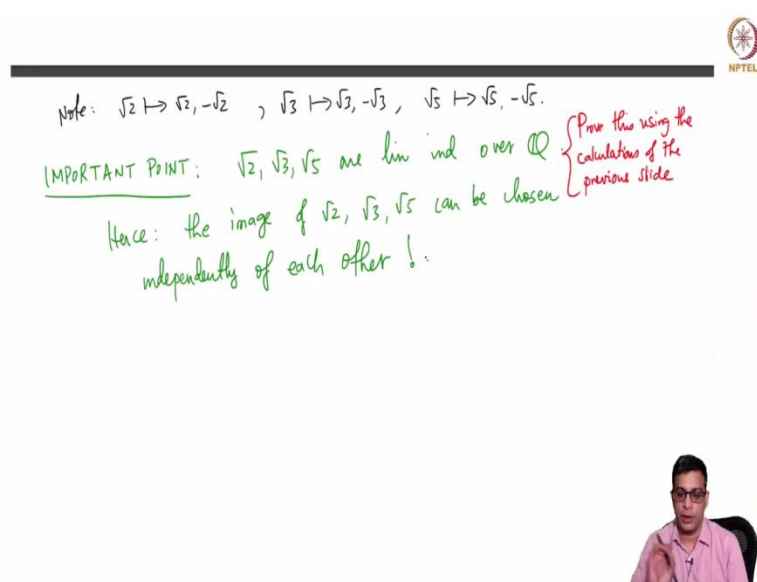
cannot be this. Similarly, it cannot be, so, let me just write all of them and eliminate obviously, whatever is not possible, okay. So, it cannot be this of course, again for degree reasons.

(Refer Slide Time: 09:05)

To prove $=2$ in (x), we need to show $\sqrt{2}, \sqrt{3}$ are lin ind over \mathbb{Q} .
 Another way of stating this: $\sqrt{3} \notin \mathbb{Q}(\sqrt{2}) \Leftrightarrow \sqrt{2}, \sqrt{3}$ are lin ind over \mathbb{Q} .
 Why is $[\mathbb{K} : \mathbb{Q}(\sqrt{2}, \sqrt{3})] = 2$? As before $[\mathbb{K} : \mathbb{Q}(\sqrt{2}, \sqrt{3})] \leq 2$.
 $\sqrt{5} \in \mathbb{Q}(\sqrt{2}, \sqrt{3}) \Rightarrow$
 But by main theorem, we know already that \exists only 4 int. fds of $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$:
 $\mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}$
 (The diagram shows a tree of field extensions starting from \mathbb{Q} , branching into $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$, and then into $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. The branches to $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ are marked with 'x' and 'y' respectively, indicating they are not the correct path for the proof.)
 This proves $[\mathbb{K} : \mathbb{Q}] = 2 \cdot 2 \cdot 2 = 8$.
 (Additional notes on the right side of the slide: $\Rightarrow 3 = 2b^2$, $\Rightarrow b^2 = \frac{3}{2}$, $b=0 \Rightarrow \sqrt{3} = a \in \mathbb{Q}$, $ab \neq 0 \Rightarrow 3 = a^2 + 2b^2 + 2ab\sqrt{2}$, $\Rightarrow \sqrt{2} = \frac{3-a^2-2b^2}{2ab} \in \mathbb{Q}$)

But can it be these? If $\mathbb{Q}(\sqrt{5})$ is in $\mathbb{Q}(\sqrt{2})$, root 5 is in root 2 by exactly the argument that is in blue here. If this equality holds implies root 5 is in $\mathbb{Q}(\sqrt{2})$ and this leads to a contradiction exactly as before, okay. The numbers will slightly change, but it is essentially the same argument. So, this cannot happen. Similarly, if this happens, root 5 is in $\mathbb{Q}(\sqrt{3})$ but that leads to a contradiction exactly as before. So this cannot happen. So $\mathbb{Q}(\sqrt{5})$ is not an intermediate field of this extension. That means root 5 cannot be inside this. That means this must be true. So this is also true. So this proves really concretely this proves $[\mathbb{K} : \mathbb{Q}] = 2 \cdot 2 \cdot 2 = 8$.

(Refer Slide Time: 10:25)



Note: $\sqrt{2} \mapsto \sqrt{2}, -\sqrt{2}$, $\sqrt{3} \mapsto \sqrt{3}, -\sqrt{3}$, $\sqrt{5} \mapsto \sqrt{5}, -\sqrt{5}$.

IMPORTANT POINT: $\sqrt{2}, \sqrt{3}, \sqrt{5}$ are lin ind over \mathbb{Q}

Hence: the image of $\sqrt{2}, \sqrt{3}, \sqrt{5}$ can be chosen independently of each other!

Prove this using the calculations of the previous slide

Okay, now what is the Galois group? Okay, now here is where we can explicitly list all the known automorphisms, possibly major ones of $\sqrt{2}$, $\sqrt{2}$ minus $\sqrt{2}$, for $\sqrt{3}$ it is $\sqrt{3}$ and minus $\sqrt{3}$ and for $\sqrt{5}$, it is $\sqrt{5}$ and minus $\sqrt{5}$. And now, I want to make a remark which I think I sort of glossed over in the earlier part of the course, is that clearly $\sqrt{2}$ can go to any of these two, but if you chose a particular value for image of $\sqrt{2}$, we are not forced to choose any particular value for $\sqrt{3}$, because the $\sqrt{2}, \sqrt{3}, \sqrt{5}$ are independent.

So, the important point here is, which I did not explicitly state before, $\sqrt{2}, \sqrt{3}, \sqrt{5}$ are linearly independent over \mathbb{Q} . So, the proof of this essentially is contained in the previous slide, you can prove this using the calculations on the previous slide. So, because $\sqrt{2}, \sqrt{3}, \sqrt{5}$ are linearly independent. So, essentially we have proved that $\sqrt{2}, \sqrt{3}, \sqrt{5}$, any two of them are linearly independent, you can then prove that the three are linearly independent, because if you can write $\sqrt{5}$ as a linear combination of $\sqrt{2}$ and $\sqrt{3}$, $\sqrt{5}$ is inside this which is a contradiction.

So, now, hence, the image of possible $\sqrt{2}, \sqrt{3}$ and $\sqrt{5}$ can be chosen independently of each other. So, $\sqrt{2}$ can be sent to $\sqrt{2}$ or minus $\sqrt{2}$ no matter what you choose there, $\sqrt{3}$ can be separately chosen to be image can be $\sqrt{3}$ or minus $\sqrt{3}$, and no matter what choice you made for $\sqrt{2}$ and $\sqrt{3}$, $\sqrt{5}$ can go to either $\sqrt{5}$ or minus $\sqrt{5}$, this is possible only if they are linearly independent.



(Refer Slide Time: 12:40)

Note: $\sqrt{2} \mapsto \sqrt{2}, -\sqrt{2}$, $\sqrt{3} \mapsto \sqrt{3}, -\sqrt{3}$, $\sqrt{5} \mapsto \sqrt{5}, -\sqrt{5}$.

IMPORTANT POINT: $\sqrt{2}, \sqrt{3}, \sqrt{5}$ are lin ind over \mathbb{Q} { Prove this using the calculations of the previous slide

Hence: the image of $\sqrt{2}, \sqrt{3}, \sqrt{5}$ can be chosen independently of each other!

$\sqrt{2} \mapsto 0$
 $5\sqrt{2} = \sqrt{3} \mapsto 0$

See, just for argument's sake, let us say root 2 and root 5 root 3 are not linearly independent, then the choice of root 2 will determine the choice of root 3 because if root 3 is 5 times root 2, it is not of course, but that is silly. But to just give you an idea of how the argument works. If you choose alpha here, you have to choose 5 alpha, you cannot choose anything else, they are independent means root 3 can be sent to any of the possible values of course, for other reasons, we know that root 3 has only two possibilities, root 3 and minus root 3. So, that is the reason that we can choose any of them.

(Refer Slide Time: 13:18)



Note: $\sqrt{2} \mapsto \sqrt{2}, -\sqrt{2}$, $\sqrt{3} \mapsto \sqrt{3}, -\sqrt{3}$, $\sqrt{5} \mapsto \sqrt{5}, -\sqrt{5}$.

IMPORTANT POINT: $\sqrt{2}, \sqrt{3}, \sqrt{5}$ are lin ind over \mathbb{Q} { Prove this using the calculations of the previous slide

Hence: the image of $\sqrt{2}, \sqrt{3}, \sqrt{5}$ can be chosen independently of each other!

Similar reasoning is required in the case of $\mathbb{Q}(\omega, \sqrt[3]{2})$ that we did before:

$\omega \mapsto \omega$ or ω^2
 $\sqrt[3]{2} \mapsto \sqrt[3]{2}$ or $\sqrt[3]{2}\omega$ or $\sqrt[3]{2}\omega^2$
 IMP that $\omega, \sqrt[3]{2}$ are ind/ \mathbb{Q} .
 This is trivial to show

So, I want to remind you that similar reasoning is required in the case of \mathbb{Q} adjoined omega and cube root of 2, that we did in an earlier video. Because if omega goes to omega or omega square, cube root of 2 goes to cube root of 2 or cube root of 2 omega or cube root of 2 omega square. So, we wrote six automorphisms, two for omega, two choices, three choices for cube root of 2 and there are two times three equal to six choices and we said that all these six are valid automorphisms. But that is only true because the choice of omega does not determine the choice of cube root of 2. So here it is important that omega and cube root of 2 are independent over \mathbb{Q} .

And this is trivial to show because cube root of 2 is real omega is not real for example. So if a times omega plus b times cube root of 2 is zero, omega can be written as a linear combination of cube root of 2 which it cannot happen. So that is required. So, I wanted to highlight this because I did not highlight this in the corresponding video.

(Refer Slide Time: 14:50)

Handwritten notes on a whiteboard:

$\sqrt{2} \mapsto \sqrt{2}$	$\sqrt{2} \mapsto \sqrt{2}$	$\sqrt{2} \mapsto \sqrt{2}$	$\sqrt{2} \mapsto \sqrt{2}$	$\sqrt{2} \mapsto -\sqrt{2}$	$\sqrt{2} \mapsto -\sqrt{2}$	$\sqrt{2} \mapsto -\sqrt{2}$	$\sqrt{2} \mapsto -\sqrt{2}$
$\sqrt{3} \mapsto \sqrt{3}$	$\sqrt{3} \mapsto \sqrt{3}$	$\sqrt{3} \mapsto -\sqrt{3}$	$\sqrt{3} \mapsto \sqrt{3}$	$\sqrt{3} \mapsto -\sqrt{3}$	$\sqrt{3} \mapsto \sqrt{3}$	$\sqrt{3} \mapsto -\sqrt{3}$	$\sqrt{3} \mapsto -\sqrt{3}$
$\sqrt{5} \mapsto \sqrt{5}$	$\sqrt{5} \mapsto \sqrt{5}$	$\sqrt{5} \mapsto \sqrt{5}$	$\sqrt{5} \mapsto -\sqrt{5}$	$\sqrt{5} \mapsto \sqrt{5}$	$\sqrt{5} \mapsto -\sqrt{5}$	$\sqrt{5} \mapsto \sqrt{5}$	$\sqrt{5} \mapsto -\sqrt{5}$
σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7	σ_8

$G = \text{Gal}(K/\mathbb{Q}) = \{1, \sigma_1, \dots, \sigma_7\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$

Hence this is a special example of the general case we are looking at.

NPTEL

So, now with this understanding, let us write down what are all the possible automorphisms of K . Okay, so I am going to write eight of them, because that is already clear to us, right? Because root 2 has two choices, root 3 has two independent choices, root 5 has two independent choices. There are total of eight choices then, 2 times 2 times 2. And I am going to write all of them here. And I am going to essentially write them in a way that is analogous to the case that I described in this case. I mean, okay, I went too far back, like this.

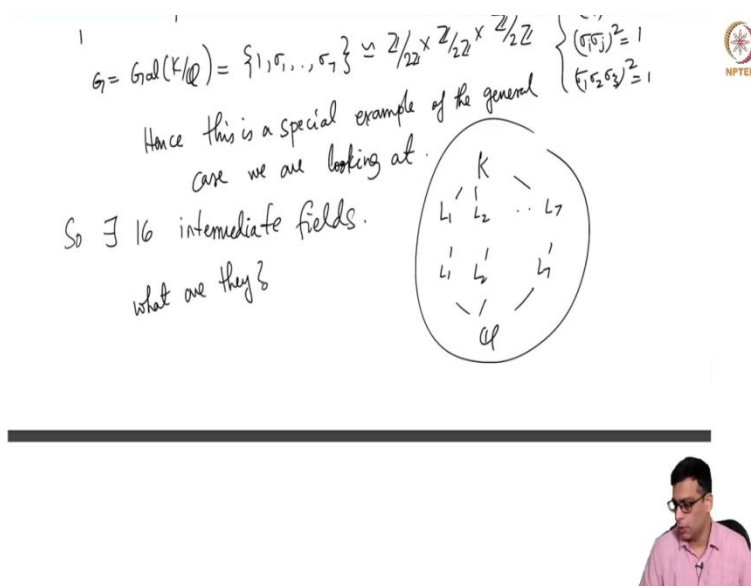
So, the first one is the identity map. So, let me write it like this. Root 2 going to root 2, root 3 going to root 3, and root 5 going to root 5. That is one. So I will try to stick to all five, eight here. So that is one, of course. The other is root 2 go into minus root 2, root 3 going to root 3, root 5 going to root 5, so this is sigma 1. The third one is root 2 going to root 2, root 3 going to minus root 3, root 5 going to root 5. So this is sigma 2. The third generator will be fixing root 3 and root 2 but root 5 is changed. So this is sigma 3. And then you have sigma 1, sigma 2, which you can check is root 2 going to minus root 2, root 3 going to minus root 3, root 5 going to root 3. So this is sigma 1, sigma 2. Sigma 1, sigma 3 will be root 2 going to minus root 2, root 3 on two root 3, root 5 going to minus root 5.

So this is sigma 1, sigma 3. Remember that once you determine the images of root 3, root 2, root 5, everything else in K image of everything else is determined because everything in K is a rational polynomial in root 3, root 5. And root 2, root 3 will be root 2 going to root 2, root 3 going to minus root 3, root 5 going to minus root 5. So, you can check these compositions trivially, right, because root 2 root 3 means first you send root 2 to root 3, root 2 under sigma 3, then root 2 will go to root 2. So that is fixed. Root 3 will go to root 3, and then it will go to minus root 3, root 5 will go to minus root 5 and root 5. So this is that. And finally, everything is interchanged here. This is sigma 1, sigma 2, sigma 3.

So these are the eight elements of the Galois group. So the Galois group. And as you can clearly check, each of them is degree 2 element other than 1, right, because any of them, σ_i^2 is one for all i , right, and $\sigma_i \sigma_j^2$ is 1 and $\sigma_1 \sigma_2 \sigma_3^2$ is 1, So, this is an abelian group where every element as order 2 every non-identity. So this is $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$. And hence, this is a special example of the problem.

General casewe are looking at. In this problem we are looking extensions K over Q where the Galois group is $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$. So, this is a special case of that situation.

(Refer Slide Time: 19:09)



$G = \text{Gal}(K/\mathbb{Q}) = \{1, \sigma_1, \dots, \sigma_7\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \quad \left\{ \begin{array}{l} (\sigma_i \sigma_j)^2 = 1 \\ (\sigma_i \sigma_j \sigma_k)^2 = 1 \end{array} \right.$

Hence this is a special example of the general case we are looking at.

So \exists 16 intermediate fields.
What are they?

Diagram illustrating the field extensions:

```

    graph TD
      K --- L1_prime[L1']
      K --- L2_prime[L2']
      K --- L7_prime[L7']
      L1_prime --- L1[L1]
      L2_prime --- L2[L2]
      L7_prime --- L7[L7]
      L1 --- Q[Q]
      L2 --- Q
      L7 --- Q
  
```

The diagram shows a central field Q at the bottom, with three intermediate fields L_1 , L_2 , and L_7 above it. Each of these is further extended to a prime field L_1' , L_2' , and L_7' respectively, which all contain the top field K .

Now, because of that, there are 16 intermediate fields that we know, all we need to do is what are they? Okay, so there are 16 intermediate fields. So, the fields will be K , and they will be L_1 , L_1 , up to L_7 ; and there will be L_1 prime, L_2 prime to L_7 prime, and then there will be Q . And there, we do not know, the relations between the inclusions between L_1 prime and L_2 prime and we do know, however, that each of these L_1 primes is contained in exactly three of them L_i 's. But the question now is, in the general case, all we can do is determine the number of intermediate phase, but now we can ask what are they.

(Refer Slide Time: 20:00)

$\checkmark L_i$: fixed fields of order 2 subgroups.

$L_1 = K^{\{1, \sigma_1\}} = \mathbb{Q}(\sqrt{3}, \sqrt{5})$

$L_2 = K^{\{1, \sigma_2\}} = \mathbb{Q}(\sqrt{2}, \sqrt{5}) = \mathbb{Q}(\sqrt{10})$

$L_3 = K^{\{1, \sigma_3\}} = \mathbb{Q}(\sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{15})$

$L_4 = K^{\{1, \sigma_4\}} = \mathbb{Q}(\sqrt{5}, \sqrt{6})$

$L_5 = K^{\{1, \sigma_5\}} = \mathbb{Q}(\sqrt{3}, \sqrt{10})$

$L_6 = K^{\{1, \sigma_6\}} = \mathbb{Q}(\sqrt{2}, \sqrt{15})$

$\sigma_2(\sqrt{2}) = -\sqrt{2}$
 $\sigma_2(\sqrt{5}) = \sqrt{5}$
 $\sigma_2(\sqrt{10}) = -\sqrt{10}$

$\text{reason: } [K : K^{\{1, \sigma_1\}}] = 2$
 $\sqrt{3}, \sqrt{5} \in K^{\{1, \sigma_1\}}$

$\mathbb{Q}(\sqrt{3}, \sqrt{5}) \subseteq K^{\{1, \sigma_1\}}$

8

$\sqrt{6} \sqrt{15} = \sqrt{90} = 3\sqrt{10}$
 $\sqrt{6} \sqrt{10} = \sqrt{60} = 2\sqrt{15}$

$\sqrt{10} \sqrt{15} = \sqrt{150} = 5\sqrt{6}$

$\sqrt{10} \sqrt{15} = \sqrt{150} = 5\sqrt{6}$

Okay, so let me just start exploring that. For example, let us look at L_1 's. These are fixed fields of order 2 subgroups, right. These are fixed fields of order 2 subgroups of G , but that for example we can take L to be K power the fixed field of, let us say σ_1 . So, this is simply, if you go back to σ_1 that fixes both root 3 and root 5. So, that is \mathbb{Q} root 3 and root 5.

So there is a small required argument here, so why is this? Why is an equality? So, general theory tells us that $[K : K^{\{1, \sigma_1\}}] = 2$, because that is the order of the group $\{1, \sigma_1\}$. So, on the other hand, root 3 and root 5 both belong to $K^{\{1, \sigma_1\}}$. Because σ_1 fixes root 3 and σ_1 also fixes root 5, so, root 3 and root 5 are in $K^{\{1, \sigma_1\}}$. So, \mathbb{Q} adjoined root 3 root 5 is contained in this. So, the picture that we can draw now is $K, K^{\{1, \sigma_1\}}, \mathbb{Q}$ adjoined root 3 root 5 and \mathbb{Q} .

So, now by the general theory of Galois, this is degree 2, right, this is captured in the Main theorem, for example. But we already know this is 4, that is a calculation that we did earlier. This extension is degree 4. So, this better be 1, right. So that is the equality. This is 2 this is 4, this whole thing is 8 so these two must be equal. So, this is that. And now we can quickly write for example, $K^{\{1, \sigma_2\}}$ will be just go back and see what is σ_2 , it fixes root 2 and root 5, so this is root 2 root 5. And similarly, L_3 will be $K^{\{1, \sigma_3\}}$, I am just choosing some numbering, so this will be \mathbb{Q} root 3 root 5.

Now, more interestingly what is L_4 ? If that is $1, \sigma_1, \sigma_2$, let us say. σ_1, σ_2 fixes, root 5 for sure, but what else does it fix? So, σ_1, σ_2 , so which is here. So let us look at this σ_1, σ_2 . σ_1, σ_2 fixes root 5, does not fix root 2 root 3. By that it fixes root 2 times, root 3. So, σ_1 fixes σ_1, σ_2 , root 2 times root 3 will be minus root 2, minus root 3, so root 2 root 3. So, that means it is root 6 is fixed.

So, that is the thing root 6 is fixed. Again the same argument, Q adjoined root 3 root 6 is degree 4 over Q and so is this, so they are equal. L_5 $K^{\text{power one}}, \sigma_1, \sigma_3$, let us say. σ_1, σ_3 fixes root three as well as root 10 now, root 2 times root 5. So, this is Q adjoined root 3 root 10, and L_6 is K adjoined $K^{\text{power sigma 2, sigma 3}}$. And σ_2, σ_3 fixes root 2 and the product of root 3 and root 5 so this. And finally L_7 , there are only seven in this case, $1, \sigma_1, \sigma_2, \sigma_3$, what does this fix? It fixes all mutual products. So, for example, it fixes root 6 and root 15. But root 10 I claim is already there, so I can else take root or root 10 or root 6 and root 15 and root 10.

Why is this? Because see if you take root 6 times root 15, this is root 90 but that is 3 times root 10. So, root 10 is already here, because that is three time root 10 is there. Similarly, root 6 times root 10 is root 60, which is 15 times 4. So, this is root 10 15. And similarly, root 10 times root 15 is root 150. And so that is in factor of 10, 5 root 6. So, so root 6 is here. Similarly, root 15 is here, similarly root 10 is here. So, these are all equalities. So, these are the seven degree 4 extensions of Q that are intermediate.

(Refer Slide Time: 25:40)

$L_6 = K^{\{1, \sqrt{5}, \sqrt{3}\}} = \mathbb{Q}(\sqrt{6}, \sqrt{5}) = \mathbb{Q}(\sqrt{6}, \sqrt{10}) = \mathbb{Q}(\sqrt{6}, \sqrt{15})$
 What about $\mathbb{Q}(\sqrt{2}+\sqrt{3})$? Can check $[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}] = 4$.
 $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$
 $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2}) \Rightarrow \sqrt{3} \in \mathbb{Q}(\sqrt{2})$
 can't be equal
 $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$
 "primitive" or "simple"
 \mathbb{Q}

But what are the degree 2? So, before I continue to degree 2, let me ask about, what about root 2 plus root 3. One can check actually by brute calculation that can check because root 2 plus root 3 satisfies the degree 4 polynomial, it cannot be decreed 2 because again if it is a degree 2 extension it will be inside $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. And this has only four intermediate fields, clearly this is not \mathbb{Q} and you can argue that this is not $\mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{3})$, because if this is equal to $\mathbb{Q}(\sqrt{3})$, let us say, this implies root 3 is in $\mathbb{Q}(\sqrt{2})$, because once root 2 is there, root 2 plus root 3 is already there, so root 3 will be there. So, this is not equal.

So, I should not change this, so this cannot be equal. So, that is equal to this. So, this is $\mathbb{Q}(\sqrt{2} + \sqrt{3})$. So, this is in fact equal to okay. So, this is what is called a primitive extension. So, this is a primitive or simple extension, meaning it is generated by a single element. Here it is generated by two elements, but you can choose a suitable degree single element which generates it. Similarly, you can check now, this is same as $\mathbb{Q}(\sqrt{3} + \sqrt{5})$ and so on. Okay, so, these are primitive elements for these extensions. At the end of this example, I will also show that K over \mathbb{Q} itself is simple. So, now, this takes care of L_1 .

(Refer Slide Time: 28:14)

L'_i : fixed fields of order 4 subgroups of L/\mathbb{Q}

distinct.

$L'_1 = K^{\{1, \sigma_1, \sigma_2, \sigma_1 \sigma_2\}} = \mathbb{Q}(\sqrt{5})$
 $L'_2 = \mathbb{Q}(\sqrt{2})$
 $L'_3 = \mathbb{Q}(\sqrt{3})$
 $L'_4 = \mathbb{Q}(\sqrt{6}), L'_5 = \mathbb{Q}(\sqrt{6}), L'_6 = \mathbb{Q}(\sqrt{15})$
 $L'_7 = \mathbb{Q}(\sqrt{30})$

reason: $\sqrt{5} \in K^{\{1, \sigma_1, \sigma_2, \sigma_1 \sigma_2\}}$

$\begin{matrix} 11 \\ 12 \\ \mathbb{Q} \end{matrix}$

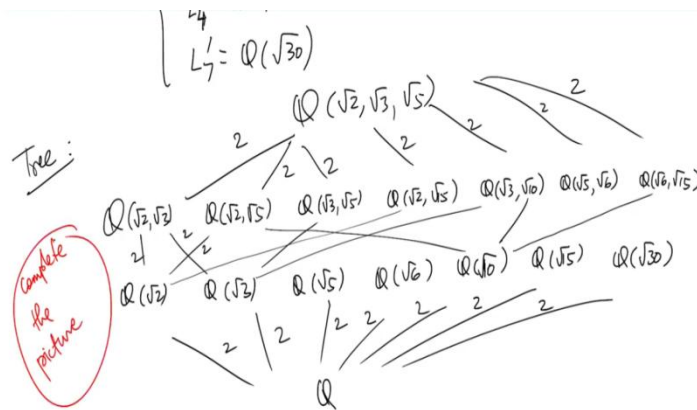
What are L_i primes? Okay, these are degree 2 extensions, right. So, these are fixed fields of, let me write it like this, order 4 subgroups, right. So, we can write for example, L_1 prime is K power, so let me try to write down the way that I have in my notes, so it does not matter but I will just write one of them. So, $1 \sigma_1 1, \sigma_1 2, \sigma_1 1 \sigma_1 2$. See, already in the previous video, we looked at the order 4 subgroups of $Z \text{ not } 2 \text{ cross } Z \text{ not } 2 \text{ cross } Z \text{ not } 2$.

So, here, we want to look at things that are fixed by $\sigma_1 1, \sigma_1 2$ as well as $\sigma_1 1, \sigma_1 2$. So, $\sigma_1 1$ fixes root 3 and root 5, but among this $\sigma_1 1 \sigma_1 2$ fixes root 5, right? $\sigma_1 2$ fixes root 5, so root 5 is the only one. So this, again, the argument is, why is this true? Root 5 is in the fixed field, that is the fastest step. If you go back and look at the slide where I have all these automorphisms written, you can see that $\sigma_1 1$ fixes root 5, $\sigma_1 2$ fixes root 5, $\sigma_1 1 \sigma_1 2$ fixes root 5, so that is there. And the extension of this is degree 2, as well as this is degree 2 because K over this is degree 4, right? So this is degree 2.

So that means these are equal. So this is an equality. So you can now write down all other, okay, so I do not want to list them. This is just boring. You can write down on your own. You will get 2, you will get 3 of course, you will get the products of pairs of them, so you got 10, you get \mathbb{Q} root 10. You get 6, you get \mathbb{Q} . Sorry, I keep writing this. So L_5 prime will be \mathbb{Q} root 6, and L_6 prime will be \mathbb{Q} root 15 and finally L_7 prime will be \mathbb{Q} root the product of all of them, so that is 30. You can argue that they are all distinct. Either using the Galois Theory that we of this

extension or you can directly argue that using the kind of argument we did earlier, to show that root 2 is not in $\mathbb{Q}(\sqrt{3})$, you can argue that they are different.

(Refer Slide Time: 31:18)



So the tree of intermediate fields will be \mathbb{Q} adjoined root 2, root 3, root 5 and then you have $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, maybe I would not have place to write all of them. So what are the other things? Root 5, root 6, root 3, 10; 2, 15. And finally, I will just try to squeeze that here, \mathbb{Q} , so maybe closer I will write. So $\mathbb{Q}(\sqrt{3})$, root 5, $\mathbb{Q}(\sqrt{2})$, root 15, I will take one of them and take the product of the others, so root 10, $\mathbb{Q}(\sqrt{5})$, root 6 and any two of them. So for example, the last one is 6 and 15, right. So I have already written all seven of them. So, this is 2, 2, 2 and of course I have $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, here I can write all of them, so $\mathbb{Q}(\sqrt{6})$, $\mathbb{Q}(\sqrt{10})$, $\mathbb{Q}(\sqrt{15})$, $\mathbb{Q}(\sqrt{30})$.

Okay, now you can actually fill the thing here. So it is contained in this, as well as this. This is contained here, this becomes messy of course and then this is contained here. As we argued here, there will be three arrows coming above each degree 2 extension, then you have \mathbb{Q} , 2, 2, 2, 2, 2 and this is 2, 2, 2 and so on. So for example, root 10 will be contained in this, it will be contained in this. And we argued that it is going to be contained in this. So, there will be three. Okay, so you can fill in the other complete the. So these are all the 14 intermediate fields on this extension. Okay, so I hope this gave you a clarity on what kind of information that you can hope to get from Galois Theory.

(Refer Slide Time: 34:18)


Finally we claim: $K = \mathbb{Q}(\sqrt{2} + \sqrt{3} + \sqrt{5})$. (primitive extn)

Remark: It is possible to prove this by brute force.
But here is a beautiful, simple argument using Galois theory:

Prf: Note that $\sigma_i(\sqrt{2} + \sqrt{3} + \sqrt{5}) \neq \sqrt{2} + \sqrt{3} + \sqrt{5} \quad \forall i=1, \dots, 7$.

$\sigma_1(\sqrt{2} + \sqrt{3} + \sqrt{5}) = -\sqrt{2} + \sqrt{3} + \sqrt{5} \neq \sqrt{2} + \sqrt{3} + \sqrt{5}$

Use the lin ind of $\sqrt{2}, \sqrt{3}, \sqrt{5}$ over \mathbb{Q}



Okay, so finally, one last thing I want to do about this example. Finally, we claim K itself can be generated by root 2 plus root 3 plus root 5. So this is also a primitive extension. So I want to remark that it is possible that to prove this by brute force. Meaning, you can just calculate and show that root 2 plus root 3 plus root 5 has degree 8 over \mathbb{Q} , and then show that the field generated by them, that element must be K , because K is a degree 8 extension.

But here is a beautiful simple argument using Galois Theory. And what is that argument? So, the argument is the following. So, we note that none of the Galois group elements fix this, so note is, σ_i of root 2 plus root 3 plus root 5 is not equal to root 2 plus root 3 plus root 5, for all i from 1 to 7. For example, where will σ_1 send this to? So, this is root 2 is interchanged, so this is not root 2 plus root 3 plus root 5.

So, here, use the linear independence of root 2, root 3, root 5 over \mathbb{Q} . So, this has to be used repeatedly. So this is not equal. And you can see now that you take any of the other σ_i 's, let me take σ_1 , σ_3 , then root 2 plus root 3 plus 5 will go to minus root 2 plus root 3 plus minus root 5. So, clearly not equal. The last one will send it to minus root 2, minus root 3 minus root 5, which cannot be equal to root 2 plus root 3 plus root 5, because they are linearly independent, the only linear combination of them that is equal to this is when you have 1, 1, 1.

(Refer Slide Time: 37:16)

$\sigma_1(\sqrt{2}+\sqrt{3}+\sqrt{5}) = \sqrt{2}+\sqrt{3}+\sqrt{5}$
 Suppose $\mathbb{Q}(\sqrt{2}+\sqrt{3}+\sqrt{5}) \neq K$: then $\mathbb{Q}(\sqrt{2}+\sqrt{3}+\sqrt{5}) =$ one of the other 15 intermediate fields.
 $\therefore \mathbb{Q}(\sqrt{2}+\sqrt{3}+\sqrt{5}) = K^H$ for a subgroup $H \leq G, H \neq G$.
 But then $\sigma_i \in H$ for some i and
 $\sigma_i(\sqrt{2}+\sqrt{3}+\sqrt{5}) = \sqrt{2}+\sqrt{3}+\sqrt{5}$ *Not possible.*
 Hence $K = \mathbb{Q}(\sqrt{2}+\sqrt{3}+\sqrt{5})$

Okay, that means, so now if you want you can look at if root 2. So suppose, so, I am trying to just think of what is the best way to argue. So, suppose this is not equal to K, then $\mathbb{Q}(\sqrt{2} + \sqrt{3} + \sqrt{5})$ is equal to one of the other 15 intermediate fields. Let us call, in each of them there will be a group element which will fix this that is a point. So, $\mathbb{Q}(\sqrt{2} + \sqrt{3} + \sqrt{5})$ is fixed by some non-identity element. In fact, I do not need to know this. This can be done directly. I do not need to know which of these intermediate fields it is.

So, it is equal to K^H for a subgroup H of G , which is different from G or rather which is different from identity. Because there is a bijective correspondence between intermediate fields and subgroups, this is a proper intermediate field, meaning it is not equal to the entire field. So, the corresponding group cannot be trivial group, because only group that corresponds to K is the trivial group. So, if you have an intermediate field that is different from K , so if this is not equal then the corresponding group H cannot be 1. But then σ_i belongs to H for some i , right because GH is not equal to identity. So, that means, H contains σ_i for some i .

So, σ_i is in H which is not a trivial group, so it must contain a non-identity, that means it must contain $\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6$ or σ_7 . So, let us end σ_i of $\sqrt{2} + \sqrt{3} + \sqrt{5}$ is $\sqrt{2} + \sqrt{3} + \sqrt{5}$, because σ_i is in H and $\sqrt{2} + \sqrt{3} + \sqrt{5}$ is in the fixed field, I hope I have written 5 everywhere root 2

plus $\sqrt{3}$ plus $\sqrt{5}$ is in the fixed field of H . So, σ_i fixes this but this we just argued, is not possible. So, $\sqrt{2}$ plus $\sqrt{3}$ plus $\sqrt{5}$ is not fixed by any of the σ_i 's.

So, the group corresponding to \mathbb{Q} adjoined $\sqrt{2}$ plus $\sqrt{3}$ plus $\sqrt{5}$ must be the identity group and hence, K is equal to $\sqrt{2}$ plus $\sqrt{3}$. So, I want to just ponder about this proof for a minute. We have proved a fact which can be proved using brute force by messy and long calculations, very cute argument using standard Galois Theory. So, this is a good illustration of how Galois Theory can give you nice proofs and sometimes only proofs of nice facts.

So, here purely field theoretic statement that $\sqrt{2}$ plus $\sqrt{3}$ plus $\sqrt{5}$ generate K over \mathbb{Q} can be proved using this Main theorem of Galois Theory. So, let me stop this video here. We have done several videos containing lots and lots of problems. So, hopefully all these problems help you understand the subject better. And you are ready now to proceed further in the course. And we will do that in the next video when we start talking about Kummer extensions. Thank you.