

Introduction to Galois Theory
Professor Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute

Lecture No. 30

Problem Session - Part 8

Welcome back. In the last class we did a couple of more problems. So I wanted to do one more problem which is a very nice problem because it gives you a flavor of what Main theorem does and what really Galois theory does in terms of explaining how a given field extension behaves. So we do this one problem and then we move on to the next topic in Galois Theory.

(Refer Slide Time: 00:45)

9) Let K/\mathbb{Q} be a normal extension st $|\text{Gal}(K/\mathbb{Q})| = 8$ and $\sigma^2 = 1 \ \forall \sigma \in \text{Gal}(K/\mathbb{Q})$. Find all the intermediate fields of the extension K/\mathbb{Q} .


Sol. Note that K/\mathbb{Q} is Galois (since $\text{char } \mathbb{Q} = 0$)


$\therefore [K:\mathbb{Q}] = |\text{Gal}(K/\mathbb{Q})| = 8$

Let $G = \text{Gal}(K/\mathbb{Q})$. Then $\sigma^2 = 1 \ \forall \sigma \in G$. So for $\sigma \in G$

$$\text{ord}(\sigma) = \begin{cases} 2 & \sigma \neq 1 \\ 1 & \sigma = 1 \end{cases}$$

Also: G is abelian: $\sigma, \tau \in G \Rightarrow (\sigma\tau)^{-1} = \tau^{-1}\sigma^{-1} = \tau\sigma$





So, this is the problem number, let me see, nine. Okay. So I want to do this problem in detail to understand what is going on. So, let K over, let us say F , be a normal extension, such that, let us take characteristic 0. Let K over \mathbb{Q} be a normal extension such that the order of the Galois group is 8. And the Galois group has the property that $\sigma^2 = 1$ for all σ in the Galois group.

So the question is, find all the intermediate fields of the extension. In fact, you can take \mathbb{Q} to F but make it characteristic 0 field, then this works. Okay, so the solution to this is the following. So first note that this is the Galois extension, since characteristic \mathbb{Q} is 0. So that means it is automatically separable. It is given to be normal so it is Galois. So therefore, K colon \mathbb{Q} , which is

the cardinality of the Galois group, because it is a Galois extension and that is given to be 8. So you have degree 8 extension.

Now let us use this very strong property of the Galois group. So let G be the Galois group, I am going to write Galois group as G because it is convenient. Then $\sigma^2 = 1$ for all σ in G , this is the hypothesis given, right. This means, so basically order of elements of G , this σ in G are given like this. Order of σ , so for σ in G order of σ is 2, if it is not identity, 1 of course if it is identity. Because identity also is its property but it is also equal to identity, so it has order 1. But for every non-identity element, σ is not equal to 1, $\sigma^2 = 1$. So that is the order 2 element. That is an order 2 element.

(Refer Slide Time: 03:50)

Let $G = \text{Aut}(K/\mathbb{Q})$

$$\text{ord}(\sigma) = \begin{cases} 2 & \sigma \neq 1 \\ 1 & \sigma = 1 \end{cases}$$

Also: G is abelian: $\sigma, \tau \in G \Rightarrow (\sigma\tau)^{-1} = \tau^{-1}\sigma^{-1} = \tau\sigma$

Hence $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ *This is a group theory fact.*



Note that also, also note G is abelian. This is because if σ and τ are in G , let us say, then $\sigma\tau$ inverse is τ inverse, of course, $\sigma\tau$ inverse is $\sigma\tau$, because square is identity means an element is its own inverse. $\sigma\tau$ is equal to $\sigma\tau$ inverse, but $\sigma\tau$ inverse in general in any group you take the product and you take inverse, you interchange the elements.

So $\sigma\tau$ inverse is τ inverse σ inverse, but τ inverse is τ , σ inverse is σ . So, $\sigma\tau$ is equal to $\tau\sigma$. So G is abelian. So G is an abelian group order 8, every element has order 2, every non-identity has order 2. So hence, so this group theory fact,

any abelian group which has this property must be isomorphic to $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ or $\mathbb{Z} \times \mathbb{Z}$.

So this is a fact from group theory. Okay so this you can for example prove using the fundamental theorem for finite abelian groups, you can write them as products of certain groups, in this case 8 so the only possibilities are $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ or $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ or $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$, but in all of those cases there will be elements whose order is not equal to 2, non-identity elements whose order is not equal to 2. So this is the only possibility.

(Refer Slide Time: 05:36)

Also: G is abelian: $\sigma, \tau \in G \Rightarrow (\sigma\tau)' = \tau^{-1}\sigma^{-1} = \tau\sigma$

Hence $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Let L be a nontrivial intermediate field.
 $L \neq K, L \neq \mathbb{Q}$

This is a group theory fact

K
 L
 \mathbb{Q}



So with this data, now let us go about finding intermediate fields. So, let L be a nontrivial intermediate field. So of course there are two obvious intermediate fields, K and \mathbb{Q} , but we are interested in, right, so this is not \mathbb{Q} and this is not K . So L is not K , L is not \mathbb{Q} . Those are there, those are already there but what about others?

(Refer Slide Time: 06:06)

$$\begin{array}{l|l}
 \text{Case 1: } [K:L] = 4 & \text{Case 2: } [K:L] = 2 \\
 L = K^H \text{ where } H \leq G \text{ has order 4} & L = K^H \text{ where } H \leq G \text{ has order 2} \\
 \# \text{ of such } L = \# \text{ of subgrps of order 4 in } G & \# \text{ such } L = \# \text{ subgrps of order 2 in } G \\
 & = \# \text{ elts of order 2 in } G \\
 & = 7
 \end{array}$$

$$G = \{ (0,0,0), (1,0,0), (0,1,0), (0,0,1), (1,1,0), (1,0,1), (0,1,1), (1,1,1) \}$$

$\begin{array}{cccccccc}
 & \parallel & \parallel & \parallel & \parallel & \parallel & \parallel & \parallel \\
 0 & x_1 & x_2 & x_3 & x_1+x_2 & x_1+x_3 & x_2+x_3 & x_1+x_2+x_3
 \end{array}$



So now there are two possibilities. Case 1, L colon, so we have two numbers who product is 8 and they are both different from 1 because K is different from L and Q is different from L. So, the possibilities are K colon L is 4 and the other possibility is case 2, K colon L is 2. So we have either 2, 4 or 2 here, similarly 2 or 4 here, because only divisors of 8 are 1,2,4,8 we don't want 1 and 8 appear here. So, 4 and 2. If this is 4, this is 2. If this is 2, this is 4. So now let us analyses these.

(Refer Slide Time: 07:02)

$$\begin{array}{l}
 \text{Let } L \text{ be a rational intermediate field.} \\
 L \neq K, L \neq Q. \\
 \text{If } L = K^H, \text{ then } [K:L] = [K:K^H] = |H|.
 \end{array}$$

$\begin{array}{l} K \\ 14 \text{ or } 2 \\ L \\ 12 \text{ or } 4 \\ Q \end{array}$

$$\begin{array}{l|l}
 \text{Case 1: } [K:L] = 4 & \text{Case 2: } [K:L] = 2 \\
 L = K^H \text{ where } H \leq G \text{ has order 4} & L = K^H \text{ where } H \leq G \text{ has order 2}
 \end{array}$$



In this case, L is equal K power H , where H is a subgroup of G of order 4. And in this case, L is K power H where H has order 2. This is all from the main theorem. So K colon L , this I will write one more time, maybe I will start here. If equals K power H , then K colon L , which is of course K power H , is cardinality. This is not in main theorem, this is our preparatory theorems that we proved before the main theorem. So K colon L is 4, means order of L/H is 4.

So again, see the question really should ask, find the number of such intermediate fields, because this is an arbitrary extension. So the question of find all the intermediate field does not really makes sense. After doing this, we will do a specific example of such thing where we can ask to find intermediate fields. So really the question is, find the number of intermediate fields. So the number we did for here is so then number of such L is number of subgroups of order 4.

So number of such L here is number of subgroups of order 2. So let us do the second case first because it is more in some sense easy. So here subgroups of order 2 will be generated by order 2 element. So this is really elements of order 2. So number of elements of order 2, each element will give a unique subgroup, right. Because if you have order 2 subgroup generated by x and order 2 generated by y , these are different means x equal to y . So, the only way they can differ is by that element. What is the number of element of order 2 in our group? That is exactly 7, because you have every non-identity is order 2. So there are 7, so this is easy. There are 7 such subgroups.

But for order 4 you have to be a bit more work. So let me do some more notation, so G can be thought of as, so G is $\mathbb{Z}/2 \times \mathbb{Z}/2$. So I am going to, I mean, I don't want to spend too much time here but let us start the process and I will let you work it out in detail for you, sir. So let me write the elements like this, 0,0,0; 1,0,0; 0,1,0; 0,0,1; 1,1,0; 1,0,1; 0,1,1; and finally 1,1,1. So I am going to call this 0, call this x_1 , call this x_2 , call this x_3 , in some sense they are generators. Then this will become x_1 plus x_2 . This will become x_1 plus x_3 .

This will become x_2 plus x_3 , this becomes x_1 plus x_2 plus x_3 . So it is an abelian group we are going to use additive notations. We are going to use this. So here Hx_i and their sums has order 2, so the seven subgroups of order 2 are going be 0×1 is one, 0×2 is another, 0×3 is third one and so on. But what are the subgroups of order 4?

(Refer Slide Time: 11:17)

$$L_1, L_2, \dots, L_7 \quad L'_1, L'_2, \dots, L'_7$$

$$G = \{ (0,0,0), (1,0,0), (0,1,0), (0,0,1), (1,1,0), (1,0,1), (0,1,1), (1,1,1) \}$$

$$\begin{array}{cccccccc} \parallel & \parallel & \parallel & \parallel & \parallel & \parallel & \parallel & \parallel \\ 0 & x_1 & x_2 & x_3 & x_1+x_2 & x_1+x_3 & x_2+x_3 & x_1+x_2+x_3 \end{array}$$

Subgroups of order 4:
(each of them is iso to $\mathbb{Z}_2 \times \mathbb{Z}_2$)

$$\begin{array}{l} \{0, x_1, x_2, x_1+x_2\} \\ \{0, x_1, x_3, x_1+x_3\} \\ \{0, x_2, x_3, x_2+x_3\} \\ \{0, x_1, x_2+x_3, x_1+x_2+x_3\} \end{array} \quad \left\{ \begin{array}{l} \{0, x_2, x_1+x_3, x_1+x_2+x_3\} \\ \{0, x_3, x_1+x_2, x_1+x_2+x_3\} \\ \{0, x_1+x_2, x_2+x_3, x_1+x_2+x_3\} \end{array} \right.$$

Again 7 of them.

Hence there are exactly $2+7+7=16$ intermediate fields.



$$\text{Case 1: } [K:L] = 4$$

$$L = K^H \text{ where } H \leq G \text{ has order 4}$$

$$\# \text{ of such } L = \# \text{ of subgroups of order 4 in } G$$

$$= 7$$

$$L_1, L_2, \dots, L_7$$

$$\text{Case 2: } [K:L] = 2$$

$$L = K^H \text{ where } H \leq G \text{ has order 2}$$

$$\# \text{ such } L = \# \text{ subgroups of order 2 in } G$$

$$= \# \text{ elts of order 2 in } G$$

$$= 7$$

$$L'_1, L'_2, \dots, L'_7$$

$$G = \{ (0,0,0), (1,0,0), (0,1,0), (0,0,1), (1,1,0), (1,0,1), (0,1,1), (1,1,1) \}$$

$$\begin{array}{cccccccc} \parallel & \parallel & \parallel & \parallel & \parallel & \parallel & \parallel & \parallel \\ 0 & x_1 & x_2 & x_3 & x_1+x_2 & x_1+x_3 & x_2+x_3 & x_1+x_2+x_3 \end{array}$$



So order 2 are clear, there are seven of them. But for order 4, see remember order 4, each of them has to be isomorphic to \mathbb{Z} naught 2 cross \mathbb{Z} naught 2, because there is no \mathbb{Z} naught 4Z here, so they are all degree 2 elements. So they are all climb 4 groups. But you have to be careful in writing these down. So I am going to clearly list them. First you can take 0, x_1 , x_2 , x_1 plus x_2 .

So basically you take any two and their sum will be a valid group. Similarly you take x_1 and x_3 , you get x_1 plus x_3 . So for some reason I have sort of messed up the notation in my notes, but anyway let us do that here. I am not going to do full details here anyway. So these are all distinct groups of order 4, right. But what else we do? We can 0, x_1 and then we take some other

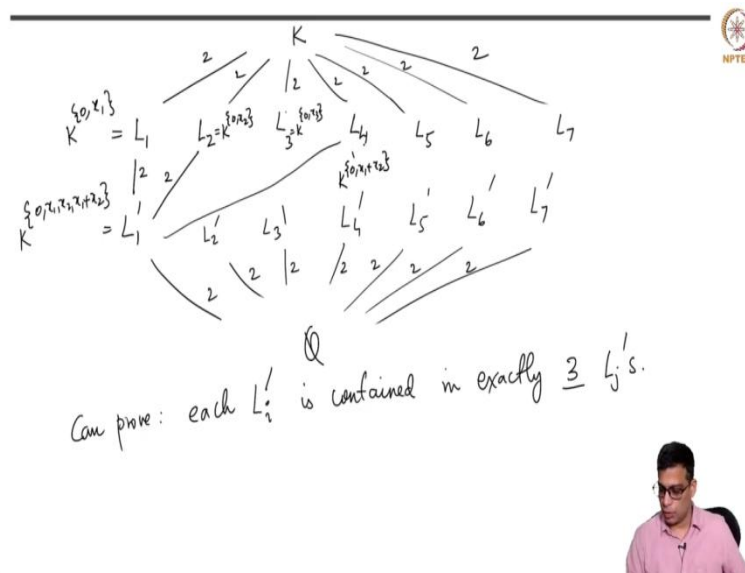
element. For example, x_1 plus x_2 . And then if you take their sum, you get x_2 . So this is same as the first one, so I do not want this. So I will take x_1 plus x_3 , then I get x_3 again. So I don't want to take either of these elements.

So maybe I will take x_1 , let us see, I get x_1 and x_2 plus x_3 . That appears here but that x_1 is not here, so I get x_1 plus x_2 plus x_3 . There are four so far and let me write it here. Then I will take 0, I think if I take x_1 I have already 1,2,3 and the remaining two elements will cover all the six remaining elements. x_2 , x_1 plus x_2 , x_3 , x_1 plus x_3 , x_2 plus x_3 and x_1 plus x_2 plus x_3 . So then I will take x_2 , let us say. I have written x_2 with x_1 and x_3 , and I have x_1 plus x_2 , x_2 plus x_3 . So I can take x_1 plus x_3 . So I do x_1 plus x_3 , then I get x_1 plus x_2 plus x_3 . As you can see, this is different from any of the things that we have written, okay.

Now I have three with x_2 , so that is already done. So I have one 2 with x_3 , so I will take third one with x_3 . With x_3 I have covered x_1 and x_2 , x_1 plus x_3 , x_2 plus x_3 . So let us take x_1 plus x_2 . x_1 plus x_2 is not there, so I will do x_1 plus x_2 plus x_3 . So I have six of them. So is there anything left? So I now can take one without x_1 or x_2 or x_3 . So then I can take x_1 plus x_2 , x_2 plus x_3 . Then if I add them I will get x_1 plus x_3 . So there are again seven of them.

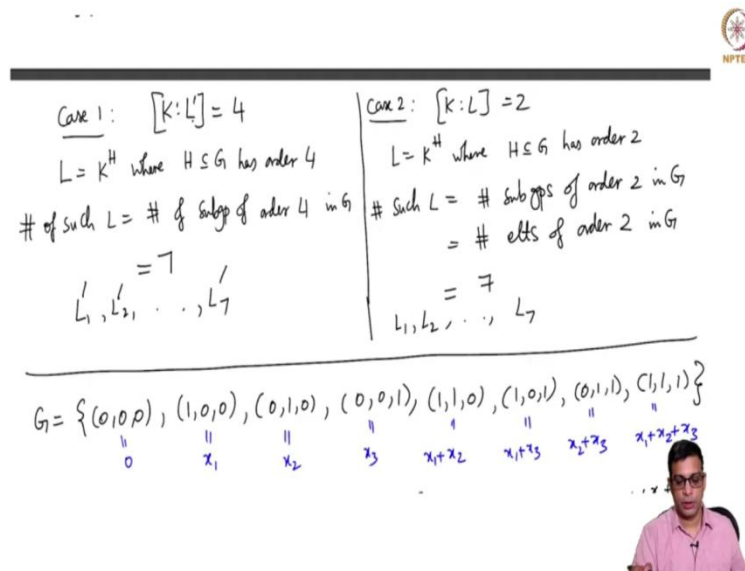
So there are seven such groups. So there are seven such intermediate fields. So let me give some names to this. Let us call this L_1 , L_2 , I mean, I will use prime to denote the second case. L_1 , L_2 to L_7 . I have L_1 prime, L_2 prime up to L_7 prime. Okay, so these are all the intermediate fields so let us agree now that there are exactly, so 2 trivial ones, K and Q , 7 in the first case and 7 in the second case. So there are 16 intermediate fields.

(Refer Slide Time: 15:48)



Okay, so let me also try to make an attempt, I will make an attempt to draw the tower of fields. So you have K and you have Q here.

(Refer Slide Time: 15:52)



But the L ones will appear, L1 primes will appear. So let me just use my notation here, so actually I call this prime and this not prime. Okay. So without prime or degree 2 under Q, so these will appear with degree 2.

(Refer Slide Time: 16:21)

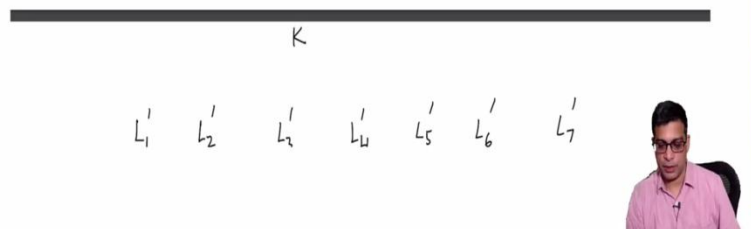
subgroups of order 4 :
 (each of them is iso to $\mathbb{Z}_2 \times \mathbb{Z}_2$)

$$\begin{array}{l} \{0, x_1, x_2, x_1+x_2\} \\ \{0, x_1, x_3, x_1+x_3\} \\ \{0, x_2, x_3, x_2+x_3\} \\ \{0, x_1, x_2+x_3, x_1+x_2+x_3\} \end{array} \quad \left| \begin{array}{l} \{0, x_3, x_1+x_2, x_1+x_2+x_3\} \\ \{0, x_1+x_2, x_2+x_3, x_1+x_3\} \end{array} \right.$$

Again 7 of them.

Hence there are exactly $2+7+7=16$ intermediate fields.

check: There are no more.



So, L_1 prime, L_2 prime, L_3 prime, L_4 prime, L_5 prime, L_6 prime, L_7 prime. So before I write this, it is clear that there are no more and these are all different, 16 different. First of all these are all different because their degrees are different and the corresponding.

(Refer Slide Time: 16:35)

$$G = \{ (0,0,0), (1,0,0), (0,1,0), (0,0,1), (1,1,0), (1,0,1), (0,1,1), \dots \}$$

Subgroups of order 4:

(Each of them is $\cong \mathbb{Z}_2 \times \mathbb{Z}_2$)

$$\begin{aligned} & \{0, x_1, x_2, x_1+x_2\} \\ & \{0, x_1, x_3, x_1+x_3\} \\ & \{0, x_2, x_3, x_2+x_3\} \\ & \{0, x_1, x_2+x_3, x_1+x_2+x_3\} \end{aligned}$$

Again 7 of them.

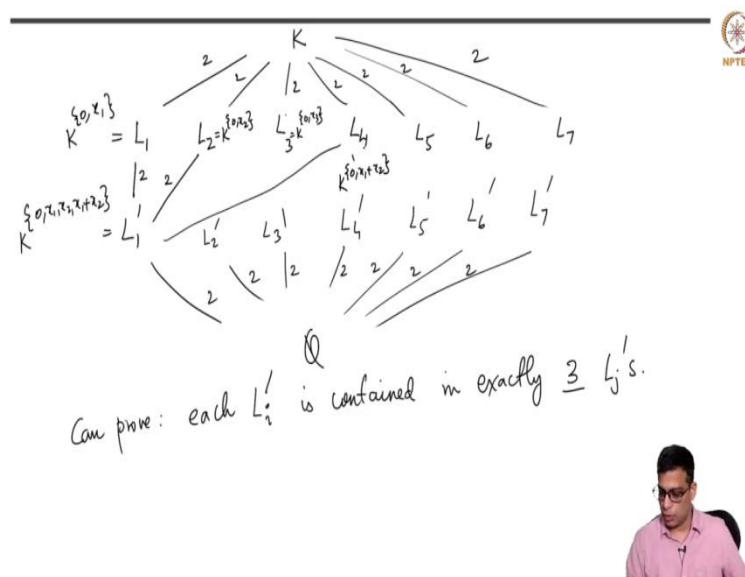
Hence there are exactly $2+7+7=16$ intermediate fields.

check: There are no more and these 16 are all distinct.

So K is of course not equal to any of the L_i primes or L_i 's and similarly Q is not equal to any of these. And any L_i prime is not equal to any L_j , for degree reasons. Now among L_i 's they are all distinct because the corresponding groups are distinct. Similarly among L_i primes there are no common ones. So there are no more and these 16 are all distinct.

All distinct is because of what I just said and there are no more because if you put any in between K and Q , it is either Q we are done in that case. K we are done in that case. Otherwise K colon L will be 4, or 2. If it is 4, it appears in case 1, if it is 2 it appears in case 2. So, that means it must be one of the 16s, so there are exactly 16 intermediate fields. So to speak we really solved this problem, right, find the number of intermediate fields. But I wanted to give an idea of how the inclusions among these works.

(Refer Slide Time: 18:08)



So, these are all 2. 2,2,2,2,2. So L_1 prime let us say is the fixed field of the first two order group we take, let us say 0, x1. So, this is L_1 prime. So I do not know what I am doing, but this is not prime, right, this is without prime. These are degree 2. So just depends on the notations that we are using, but let us say this is the fixed field of this. Then L_1 prime and let us say L_1 prime is the fixed field of this. So this is H_1 prime and this will be K , the fixed field of x_1, x_2, x_1 plus x_2 .

So this will be contained in L_1 and now depends on what L_2 and L_3 are. But let us say L_2 is fixed field, so I am going to squeeze this here, 0, x2. And this is the fixed field of 0, x3. So there will be an inclusion here and it will be a degree 2. But there is nothing here, right. This cannot exist. There is no line here because 0, x3 is not contained in this. This is the application of the main theorem. Only where you will have an inclusion is that there is a reverse inclusion of the Galois, of the groups.

So 0, x1 is contained in this, so L_1 prime is contained in this. 0, x2 is contained in this, so this will be contained in this. So there is nothing here, but what will this be. There will be one more that contains this and that would 0, x1 maybe this K power 0x1 plus x_2 , whatever that is, there will be an inclusion here. Okay and L_1 prime will not be contained in any other things, so basically and of course underlying all of these is Q . So these are all two of course.

So now the missing thing in this picture is what lines to put between primes and L_i 's and L_i primes, which I will, I mean, this depends on how we are calling these things. And you can prove

that, each can prove, each L_i is contained in exactly one or each L_i prime is contained in exactly three L_j 's. Okay so each L_i prime for example L_1 prime is contained in L_1, L_2, L_4 in my notation here. So I cannot erase this, but it should be L_4 . So, L_j 's, so L_1 prime is contained in L_1, L_2, L_4 and maybe L_2 prime is contained in something else. So it depends on the notation but that is the picture of this.

(Refer Slide Time: 21:51)

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

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



Now, let me end this class with a specific example of such a thing. So let us take K to be \mathbb{Q} adjoined square root 2, square root 3, square root 5. Okay. So the first thing to check is K over \mathbb{Q} is an extension satisfying the hypothesis of the problem. So this is because, first you note that, this I would like to do in detail because this kind of thing is important, so let me carefully check some of these things.

Okay, so it has been already quite a bit of time I spent, so maybe I will just stop this class now so that you can start fresh with this specific example again. So let me stop this class now. In the next video we will work out this specific example in detail. Thank you.