

Algebra - II
Professor S Viswanath
Department of Mathematics
The Institute of Mathematical Science
Lecture 38
Solved Problems (Week 5)

(Refer Slide Time: 00:14)

Problems

Compute the Galois group of the following Galois extensions:

(i) $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$: (a) Galois $\begin{cases} \rightarrow \text{normal: SF of } (x^2-5) \in \mathbb{Q}[x] \\ \rightarrow \text{separable } \checkmark \text{ char } \mathbb{Q} = 0. \end{cases}$

(b) $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = |\text{Aut}(\mathbb{Q}(\sqrt{5})/\mathbb{Q})| = 2$

(c) The elts $\pm\sqrt{5}$ are the roots of $f(x) = x^2 - 5$, which is irreducible in $\mathbb{Q}[x]$.



Let us do some problems on computing Galois groups. Compute the Galois group of the following Galois extensions. So the first problem; so let us look at the Galois extension $\mathbb{Q}(\sqrt{5})$ over \mathbb{Q} . So first we should ensure that this is indeed a Galois extension. In this case observe it is Galois. Well, that means two things; normal and separable.

To check that it is a normal extension, we just have to realize that this field $\mathbb{Q}(\sqrt{5})$ is actually nothing but the splitting field of an obvious polynomial. Look at the polynomial $x^2 - 5$ with coefficients in \mathbb{Q} . The splitting field of this, so what are the roots of this? Plus and minus root 5 and this field is generated by the roots of that polynomial.

So, by the usual definition of splitting fields, this is exactly the splitting field. So it is normal and separable comes for free because the characteristic of \mathbb{Q} is 0. So recall that if the base field is either characteristic 0 or perfect field, then any algebraic extension is automatically separable. So what is a Galois group?

So, let us see, observe that we know the cardinality of a group that is exactly the cardinality of its Galois group and in this case, $\mathbb{Q}(\sqrt{5})$ over \mathbb{Q} is of course, a degree 2 extension as we have seen before. Now, therefore, the Galois group must have two elements. So, well what

So you can also say it is a splitting field with a collection of polynomials and so that means it is normal and as before, separable is just because of characteristic 0. So let us see what the degree of this extension is, that will tell us the cardinality of the Galois group. So we can think of this extension as being obtained in two steps.

So let us say we first adjoin root 5 and then we adjoin square root of 7 to this field. So maybe we will call this field as K_1 which is \mathbb{Q} of root 5. Now the, what we already know is that \mathbb{Q} root 5 over \mathbb{Q} is of degree 2 and to that field K_1 , we are adjoining an additional element square root of 7. Now we need to figure out what the degree of this extension is.

So now I claim that this is also a degree 2 extension. Why is that? Observe that, what is the polynomial that square root of 7 satisfies? That we have to find out the minimal polynomial of square root 7 over the field K_1 ; now, what polynomial does it satisfy? Well, let us say is the root of well, the obvious polynomial $x^2 - 7$, which I can think of as having either rational coefficients or coefficients in K_1 .

So definitely this square root of 7 satisfies this degree 2 polynomial, but maybe it also satisfies a degree 1 polynomial. We do not know that. In other words, could it happen that square root of 7 already lies inside K_1 ? If that happened, then of course, K over \mathbb{Q} would only be a degree 2 extension. So therefore, so this implies that K over K_1 is, at most the degree of G , it is at most a degree 2 extension.

(Refer Slide Time: 07:05)

But claim: $\sqrt{7} \notin \mathbb{Q}(\sqrt{5})$ ✓ ; if not $\sqrt{7} = a + b\sqrt{5}$ $a, b \in \mathbb{Q}$
 $7 = a^2 + 5b^2 + 2ab\sqrt{5}$
 $\Rightarrow ab = 0 \Rightarrow a \text{ or } b = 0$
 But: if $b = 0$, $a^2 = 7 \Rightarrow a \notin \mathbb{Q}$
 if $a = 0$, $b^2 = \frac{7}{5} \Rightarrow b \notin \mathbb{Q}$
 $\therefore [K : \mathbb{Q}] = 4$

But claim: it cannot be a degree 1 extension. In other words this element that we adjoin, cannot already be inside this field $\mathbb{Q}(\sqrt{5})$. Why is this? Well, this is sort of one of those nice little proofs like $\sqrt{2}$ is irrational and so on.

Suppose not, you would try and write if not, then you should be able to write square root of 7 in terms of, that of the form $a + b\sqrt{5}$ where a and b are both rational numbers, because that is what elements of $\mathbb{Q}(\sqrt{5})$ look like and then you sort of square both sides of this equation and conclude that, this is $7 = a^2 + 5b^2 + 2ab\sqrt{5}$.

Now, the only way this equation can hold true is if, well observe that $\sqrt{5}$ is irrational. So, you know, all the other terms are rational, this implies that that term $2ab\sqrt{5}$ cannot occur. Since all the other terms are rational, this would be the only irrational term otherwise. Which means a or b is 0.

But in that case, observe that this, this equation cannot hold. So I have already said this is 0. Now, if you look at what is left, $7 = a^2 + 5b^2$, if I put a equal to 0 or b equal to 0, then I cannot find a rational solution for the other guy. But observe, if b equal to 0, then I conclude $a^2 = 7$. Which means that, you know, a is not as we know square root of 7 is not rational.

So I am using some facts, that square root of 7 is not rational here. Similarly, if $a = 0$, this will imply that $5b^2 = 7$, $7/5 = b^2$ and therefore b is, again b cannot be rational because b is the square root of $7/5$. So we have used a couple of facts that square root of 7 and square root of $7/5$ are not rational numbers.

But that proof is the usual kind of proof, like proving square root of 2 is irrational. So that is basically what this claim involves. So we have shown this therefore, we conclude the following that K over K_1 is a degree 2 extension, K_1 over \mathbb{Q} is the degree 2 extension. Therefore, K over \mathbb{Q} is a degree 4 extension.

(Refer Slide Time: 09:48)

$\Rightarrow |\text{Aut}(K/\mathbb{Q})| = 4$

observe any $\sigma \in \text{Aut}(K/\mathbb{Q})$ is uniquely determined by $\sigma(\sqrt{5})$ and $\sigma(\sqrt{7})$

\therefore List the possibilities for $\sigma(\sqrt{5})$ and $\sigma(\sqrt{7}) \in K$

$\alpha = \sqrt{5}$ and $\beta = \sqrt{7}$ $\mathbb{Q}(\sqrt{5}, \sqrt{7})$

$\sigma(\alpha)$ must be a root of the minimal polynomial $m_\alpha(x) \in \mathbb{Q}[x]$

$m_\alpha(x) = x^2 - 5$

Now, what does that mean? That means that the Galois group K over \mathbb{Q} should have 4 elements. So of course the next question is what group of order 4 is it? What is the structure of this group? So let us try and find some elements in this group just like what we did in the earlier case. So recall you know, how do I find elements of this Galois group?

Observe the following fact; any element in this automorphism group, Galois group is uniquely determined once I know what it does to the two generators square root 5 and square root 7. So observe sigma, any sigma in any element of the Galois group is uniquely determined by its actions on the generators.

Why? Because any other element of the field just can be expressed as a polynomial in these generators and so sigma acting on that element can be uniquely computed. So let us see what are all the possibilities so therefore, we will try to list the possibilities for these two elements; sigma root 5, and sigma acting on root 7. So what are these?

They are both elements of K . So, both sigma root 5 and sigma root 7 are elements of this field $\mathbb{Q}(\sqrt{5}, \sqrt{7})$. Now, recall you know as we have seen before, the same fact that we used earlier that you know, the minimal polynomial of square root 5, so observe that sigma root 5 must be root of, so maybe we will just call these numbers something like, let alpha root 5 and beta denote root 7, then sigma of alpha must be the root of the minimal polynomial of alpha over \mathbb{Q} .

This is a minimal polynomial of alpha over Q. So, what does this mean? This means that and what is this minimal polynomial? It is the smallest degree irreducible polynomial that root 5 satisfies and this case, it is easy to see, this minimal polynomial is just x square minus 5.

(Refer Slide Time: 12:52)

$\Rightarrow \sigma(\alpha) = \sqrt{5} \text{ or } -\sqrt{5}$ | similarly: $m_{\beta}(x) = x^2 - 7$
 $\sigma(\sqrt{5}) = \pm\sqrt{5}$ | $\therefore \sigma(\sqrt{7}) = \pm\sqrt{7}$

\therefore The Galois group $\text{Aut}(K/\mathbb{Q})$ has the foll 4 elts

σ	τ	$\sigma\tau$	id
$\sqrt{5} \rightarrow -\sqrt{5}$	$\sqrt{5} \rightarrow \sqrt{5}$	$\sqrt{5} \rightarrow -\sqrt{5}$	
$\sqrt{7} \rightarrow \sqrt{7}$	$\sqrt{7} \rightarrow -\sqrt{7}$	$\sqrt{7} \rightarrow -\sqrt{7}$	

$\sigma^2 = \tau^2 = \text{id}$ $\sigma\tau = \tau\sigma$ Klein 4-group $\cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$



$\Rightarrow |\text{Aut}(K/\mathbb{Q})| = 4$

observe any $\sigma \in \text{Aut}(K/\mathbb{Q})$ is uniquely determined by $\sigma(\sqrt{5})$ and $\sigma(\sqrt{7})$

\therefore List the possibilities for $\sigma(\sqrt{5})$ and $\sigma(\sqrt{7}) \in K$

$\alpha = \sqrt{5}$ and $\beta = \sqrt{7}$ $\mathbb{Q}(\sqrt{5}, \sqrt{7})$

$\sigma(x)$ must be a root of the minimal polynomial $m_{\alpha}(x) \in \mathbb{Q}[x]$

$m_{\alpha}(x) = x^2 - 5$

So, therefore we conclude that when I act sigma on this element alpha, it has to be a root of the polynomial x square minus 5. Therefore, this can only be one of two possibilities. So, this can either be root 5 or minus root 5. Now, similarly I also look at the other guy beta, observe that it is minimal polynomial over Q is just x square minus 7.

I mean, we have to show this is irreducible, but we have done examples like this before. Now, the roots of this polynomial are plus or plus or minus square root 7. Therefore,

analogously when it takes sigma, I acted on root 7, I can only get plus or minus roots 7. Those are the only possibilities just like here sigma of root 5 can only be one of these two numbers.

So, how many possibilities are there in all? Well, there are two possibilities for sigma of root 5, there are two possibilities for sigma root 7, between them you get only four possible you know, choices of sigma. So, what this means, in particular is that all these four must actually be elements of the Galois group because the Galois group we have already deduced has four elements.

So, all these four possibilities must in fact be realized. So therefore the Galois group, the group is the Galois group of automorphisms of K or Q has the following four elements, which are determined by what it does to each of them. So one of them is root 5 it says, root 5 goes to minus root 5, root 7 goes to plus root 7.

So we will call this something sigma, root 5 goes to plus root 5, root 7 goes to minus root 7, call this tau and then there is the composition of sigma tau which takes both of them to the negatives and then there is the identity map of course. So these are the four elements, which belong to the Galois group and this should be familiar.

I mean, observe that each of them sigma square, tau square are both identity, if you apply them twice sigma tau and tau sigma the same, does not matter which order you do it and this is exactly the set of relations for the Klein four group or if you wish, it is the direct sum of two copies of said $Z \text{ mod } 2$.

(Refer Slide Time: 15:43)

(3) $f(x) = x^3 - 5$ $K =$ Splitting field of $f(x)$ over \mathbb{Q}

$K = \mathbb{Q}(\sqrt[3]{5}, \sqrt[3]{5}\omega, \sqrt[3]{5}\omega^2)$ $\omega = e^{2\pi i/3}$
 $= \mathbb{Q}(\alpha, \omega)$ $\alpha = \sqrt[3]{5} \in \mathbb{R}$

$K = \mathbb{Q}(\alpha, \omega)$

$\mathbb{Q}(\omega) = K_1$

\mathbb{Q}

α is a root of $x^3 - 5$
irreducible over \mathbb{Q}
(by Eisenstein criterion, with $p=5$)

Good. So let us do another one, slightly slightly more complicated which is, let us take the base field again to be \mathbb{Q} and let us take the polynomial x cubed minus 5 and let K denote its splitting field, splitting field of this polynomial over the base field \mathbb{Q} . What does that mean? Well, I have to just take the roots of this polynomial; I know what the roots are in the complex numbers.

So cube root of 5 and cube root of 5 ω , cube root of 5 ω^2 , where ω is primitive cube root of unity. Maybe I will give cube this this real cube root of 5. So this is something, this as a real cube root of 5, I call it α . Observe, this is also the same as you first had adjoin α then you adjoin ω to it separately because if I have α and I have $\alpha \omega$, I can get ω from it.

Good. So what do we know about this this field? Again, it is Galois because it is the splitting field already. It is separable, because again it is characteristic 0. Now, let us try and figure out what the degree of this extension is. So, I start with \mathbb{Q} and I need to go all the way up to K , which is $\mathbb{Q}(\alpha, \omega)$.

Again, I will think of it as being realized as successive tower of extensions. So I first adjoin α ; now what polynomial does α satisfy over \mathbb{Q} ? What is the minimal polynomial? So observe, α satisfies α is the root of the polynomial x cubed minus 5 and in fact, we know that this polynomial is an irreducible polynomial, it is irreducible over \mathbb{Q} .

For example, by using the Eisenstein criterion so, recall the Eisenstein criterion requires a certain prime number P that you use to prove the irreducibility. Here you can take the prime to be 5. So, this prime divides the well it does not divide the leading term, it divides the constant term and the square of this prime does not divide the constant term. Those were the conditions you needed for the Eisenstein criterion for irreducibility.

So, alpha is the root of this cubic polynomial which is known to be irreducible over \mathbb{Q} , which implies that this extension here must be a degree 3 extension because the degree is the same as the degree of the irreducible polynomial that alpha satisfies. Now, what about the other one up here, we need to look for what is the polynomial that omega satisfies over this field \mathbb{Q} alpha. So, this field we are adjoining omega to the field \mathbb{Q} now.

(Refer Slide Time: 19:01)

ω is a root of $x^2 + x + 1 \in K_1[x]$.
 irreducible in $K_1[x]$, because if not,
 then $\omega \in K_1 = \mathbb{Q}(\alpha) \subseteq \mathbb{R}$
 \uparrow
 not real. contradiction!

$\therefore [K:\mathbb{Q}] = 6 = |\text{Aut}(K/\mathbb{Q})|$


$\sigma \in \text{Aut}(K/\mathbb{Q})$ is determined by $\sigma(\alpha), \sigma(\omega)$

(3) $f(x) = x^3 - 5$ $K = \text{Splitting field of } f(x) \text{ over } \mathbb{Q}$

$K = \mathbb{Q}(\sqrt[3]{5}, \sqrt[3]{5}\omega, \sqrt[3]{5}\omega^2)$ $\omega = e^{2\pi i/3}$
 $\alpha = \sqrt[3]{5} \in \mathbb{R}$
 $= \mathbb{Q}(\alpha, \omega)$

$K = \mathbb{Q}(\alpha, \omega)$
 $\mathbb{Q}(\omega) = K_1$
 \mathbb{Q}

α is a root of $x^3 - 5$
 irreducible over \mathbb{Q}
 (by Eisenstein criterion, with $p=5$)




(3) $f(x) = x^3 - 5$ $K = \text{Splitting field of } f(x) \text{ over } \mathbb{Q}$

$K = \mathbb{Q}(\sqrt[3]{5}, \sqrt[3]{5}\omega, \sqrt[3]{5}\omega^2)$ $\omega = e^{2\pi i/3}$
 $\alpha = \sqrt[3]{5} \in \mathbb{R}$
 $= \mathbb{Q}(\alpha, \omega)$

$K = \mathbb{Q}(\alpha, \omega)$
 $\mathbb{Q}(\omega) = K_1$
 \mathbb{Q}

α is a root of $x^3 - 5$
 irreducible over \mathbb{Q}
 (by Eisenstein criterion, with $p=5$)



Now observe omega satisfies, well is the root of certain quadratic polynomial. So recall the cube root of unity satisfies this polynomial and this is, well it has rational coefficients but I can also think of the coefficients as coming from this larger field K_1 . So omega satisfies a quadratic polynomial with coefficients in K_1 which implies that this, this extension here, so that I do not know at this moment whether this is an irreducible polynomial or not but whatever it may be, I know that this extension is utmost degree 2.

Now, the claim is this is in fact irreducible. This polynomial is irreducible. So this is irreducible. In even over this larger field K_1 x, why? Because if not, if it is not irreducible it has to factor into a product of two linear factors. This is after all quadratic; if not then it would imply that, then both roots belong to K_1 .

So, then it will imply in particular that ω comes from K . Now, which is not true because remember K is just \mathbb{Q} adjoin a certain real number, which is α in this case, so I adjoin α ; the answer is definitely real, so subfield of the real numbers but ω is definitely not a real number. We know what ω is, it is got a certain non-zero complex part. So, this is not real. So this is a contradiction.

So, this establishes that ω does not belong to the field K therefore, this polynomial is irreducible. Therefore, score back we can remove this less than or equal to symbol. This is exactly a degree 2 extension. So, all told therefore it is a degree 6 extension. Therefore, K over \mathbb{Q} is degree 6 and so, this must also be the cardinality of the Galois group. So, there should be 6 automorphisms of K which fix \mathbb{Q} pointwise.

So, let us look for those 6. Let us try and figure out just like we did earlier what those 6 must look like and as before we will try to analyse; so, observe as before that if I give you a σ in the Galois group, is determined uniquely by its action on the 2 generators. In this case the 2 generators were; cube root of 5 which is α and the cube root of 1 the complex cube root of unity which is ω .

(Refer Slide Time: 22:09)

(1) $\sigma(\alpha) =$ one of the 3 roots of the min poly of α over \mathbb{Q}
 \parallel
 x^3-5
 $\alpha, \alpha\omega, \alpha\omega^2$

(2) $\sigma(\omega) =$ one of the roots of $m_\omega(x) \in \mathbb{Q}[x]$ $\omega \in K$
 \parallel
 x^2+x+1 \mathbb{Q}
 ω, ω^2



So, let us see what these things have to be. So, observe for a start that what can $\sigma(\alpha)$ be? What are the possibilities? $\sigma(\alpha)$ can only be one of the three possible roots of the minimal polynomial of α . So possibilities; $\sigma(\alpha)$ has to be one of the three roots of the minimal polynomial of α over the base field. Again, what was that

minimal polynomial? We already said this it was $x^3 - 5$ and so what are the three possible roots of that equation?

They were just cube root of 5, cube root of 5 ω and cube root of 5 ω^2 . So, there are three possibilities for α can map. There are three possibilities for σ of α . It can either go to α , $\alpha \omega$ or $\alpha \omega^2$. Now analogously we ask what about the other generator? What can σ of ω map to?

By the same token now, we need to ask, what is the minimal polynomial that ω satisfies over \mathbb{Q} ? So, I have this element ω in K , ω satisfies some irreducible polynomial over \mathbb{Q} , σ must map ω to one of the roots of that irreducible polynomial. So it is one of the roots again similarly, it is one of the roots of the minimal polynomial, let us call it $m_\omega(x)$. This is the minimal polynomial of this over \mathbb{Q} .

Now, what is that? Well, it is actually the same polynomial $x^2 + x + 1$. We already know what polynomial ω satisfies over \mathbb{Q} even. This is just $x^2 + x + 1$ and this is of course, irreducible for the same sort of reason that we gave earlier. It is irreducible over \mathbb{K} over \mathbb{Q} as well as over \mathbb{K}^1 for the same sort of reason. If not, then ω would have to be an element of \mathbb{Q} , which we know for sure is not the case.

So therefore σ of ω can either be ω or the other root of this polynomial which is ω^2 . Now again, there are how many possibilities for σ ? It can map α to one of these three choices, it can map ω to one of these two choices, put together there are six possible choices maximum.

(Refer Slide Time: 24:43)

∴ All 6 possibilities do arise!

$\alpha \xrightarrow{\sigma} \alpha$	$\alpha \xrightarrow{\tau} \alpha\omega$	$\sigma \circ \sigma = \sigma^2: \alpha \rightarrow \alpha \rightarrow \alpha$ $\omega \rightarrow \omega^2 \rightarrow \omega$
$\omega \rightarrow \omega^2$	$\omega \rightarrow \omega$	

∴ $\sigma^2 = \text{id}$

$\tau^3 = \text{id}$, $\sigma \tau \sigma^{-1} = \tau^2$ (ex)

∴ σ and τ do not commute.

⇒ $\text{Aut}(K/\mathbb{Q}) \cong S_3$

Diagram: $\begin{matrix} \text{id} & \tau & \tau^2 \\ \sigma & \sigma\tau & \sigma\tau^2 \end{matrix}$

All choices need not always be consistent but these are the maximum possible choices. There are only six of them. But we already know that the Galois group has exactly six elements, which means that all six of these possibilities must actually be, you know, really possible. They must arise. Therefore, what we conclude is that all six possibilities do arise when you look at the possible elements of the Galois group.

So let us, let us write out, you know, these six elements. So let me like we did earlier, let me say, alpha goes to alpha, let us say omega goes to omega square. So let me give this map a name. It is called the sigma. Now, let us look at another one; alpha can go to alpha omega, let us call this tau and omega goes to omega.

Then, let us look at what are the other possibilities. So the remaining elements can more or less be obtained by looking at various compositions of sigmas and taus. Now, just with this sigma and tau observe many things that if I, for example, compose sigma with itself, what is sigma composition sigma? Well, this map which we will call sigma square, takes alpha to alpha to alpha.

I am composing it twice. Omega goes to omega square and when I compose it once more, what should it do? Well, omega squared so it goes to omega squared, squared when I apply sigma again but that is omega to the four which is omega. Therefore, what do I conclude? Sigma square is therefore just identity map because it maps both alpha and omega to themselves.

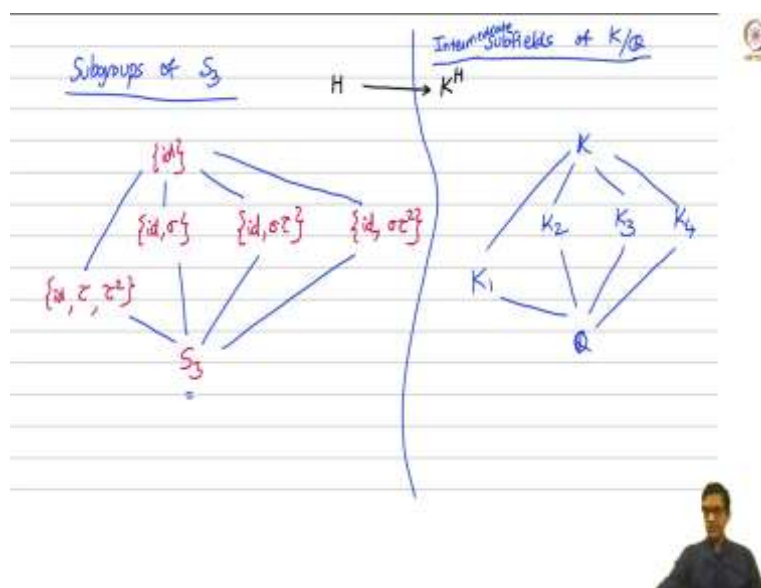
Of course, it maps Q , Q to Q as pointwise identity. Now, similarly, if you compute tau cubed, you will notice that, it is again the identity map and if you compute sigma tau sigma inverse, you will notice that this is tau square. So I am sort of leaving these two here as exercises for you to compute. So, what we have generated are well 5 elements I suppose.

Sigma tau, well not quite, we have only looked at sigma and tau as elements and then we are looking at the various relations that they satisfy. So, observe that this this final equation here tells you that this group is non-abelian because sigma tau is not the same as I mean, sigma tau sigma inverse would have given you tau, if sigma and tau commuted with each other.

So, this implies that sigma and tau do not commute and of course, all this fuss is more or less to say that, you know, this is a non-abelian group of order 6 and you know, the relations are probably familiar already. This is the group S_3 or if you wish, it is the dihedral group with 6 elements. It is another way of saying the same thing.

So, observe that the 6 elements are exactly the automorphism group of K over Q in this case is just a symmetric group S_3 . You could write out all the 6 elements if you wish. Its identity tau, tau square, then that is sigma, sigma tau and sigma tau square. They will realize these six elements will give you all the six possibilities, alpha mapping to one of the three alpha, alpha omega, alpha omega square omega mapping to one of the two possibilities omega or omega square.

(Refer Slide Time: 28:55)



∴ All 6 possibilities do arise!

σ	τ	$\sigma \circ \sigma = \sigma^2: \alpha \rightarrow \alpha \rightarrow \alpha^2$ $\omega \rightarrow \omega^2 \rightarrow \omega$ ω
$\alpha \rightarrow \alpha$ $\omega \rightarrow \omega^2$	$\alpha \rightarrow \alpha\omega$ $\omega \rightarrow \omega$	

∴ $\sigma^2 = \text{id}$

$\tau^3 = \text{id}$, $\sigma\tau\sigma^{-1} = \tau^2$ (Ex.)
 ↳ σ and τ do not commute.

⇒ $\text{Aut}(K/\mathbb{Q}) \cong S_3$

Now, recall that you know, what are the subgroups, look of this one of the subgroups look like? So, let us try to bring in the fundamental theorem of Galois Theory here. So, what are the subgroups of S_3 look like? So, let us, well I just wrote out all 6 elements and it is easy to see that this for example, is a subgroup of order 3. It is the only subgroup of order 3, the alternating group and there are a few subgroups of order 2, identity sigma, identity with sigma tau, identity with sigma tau square.

These are 3 subgroups of order 2 and that is it. So let us write out all the possibilities. There is the identity and just call it E in this case, then there is maybe we should just write it as id , says the identity subgroup. Then there is identity sigma, sigma tau, identity with sigma square. These are the order 2 subgroups and then there was an order 3 subgroup identity tau, tau square and then finally, the full group itself just the group S_3 in this case.

Now, let us draw the inclusion relations among them. So, this contained this, this is contained in this. So, when you draw a line, it just means that the subgroup on top is contained in the subgroup on the bottom. So this is the partial partially ordered set, whose elements are the subgroups and the partial order is just one of containment.

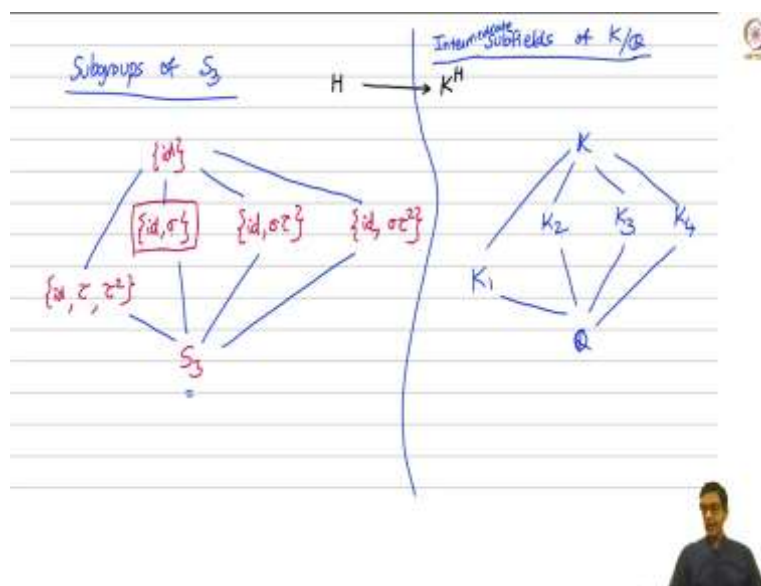
So, I have drawn them here. Now, what is the fundamental theorem of Galois Theory say that this is in one to one correspondence with the subfields of K . Well, I should actually say the intermediate subfields of this extension; meaning subfields which lie between K and \mathbb{Q} . So let us see what are the various possibilities? We already know what this map is.

So given a subgroup recall what the fundamental theorem of Galois Theory says? If I give you a subgroup H , you are supposed to send it to the fixed field of H , the elements of K , which are pointwise fixed by every element of H . So, now I know that some things are obvious. If I take the identity then the identity fixes every element of K that goes to K .

If I take S_3 , then the only elements of K fixed by all elements of the Galois group that is going to be the base field, so that was the definition of Galois extension, if you wish. Now, I have K and Q at the two ends and then I have, there should be some subfields corresponding to these four subgroups. So, let me call it K_1 , K_2 , K_3 and K_4 .

So, again I should have now inclusion relations in the same way. I should be able to find subfields like this, which are all, which have the same inclusion relations. So, recall this is an inclusion reversing bijection between these two sets. So, the question is what are these K_1 , K_2 , K_3 and K_4 ? Let us try and figure them out. They are the fixed fields.

(Refer Slide Time: 32:43)



Now, what is K_1 ? K_1 is by definition, the fixed field of the subgroup whose elements are identity τ and τ square. Now, what do we know? Well, what is τ ? I sort of said what τ does; it maps α to $\alpha\omega$, ω goes to ω^2 . So, definitely ω is fixed by τ because ω maps to itself, ω^2 also maps to itself, I mean any multiple of ω will map to itself, any power of ω sorry, ω is also fixed by τ square.

So, observe τ and τ^2 both fix ω . So, one thing we know for sure is that Q and ω are both inside this field K_1 . Now, what is $Q(\omega)$? Well, what is the degree of $Q(\omega)$ over Q ? So, recall we have already said this ω satisfies a degree 2 polynomial over Q . So, this is just a degree 2 extension.

Now, we will soon see that it is actually equality there. So let us move on to the other one. So, what is K_2 ? K_2 is the fixed field of identity with σ . Now, identity with σ is what are the possibilities σ maps α now to α maps ω to ω^2 . So by the same reasoning as before, definitely this fixed field contains Q and it contains α . So it contains the field $Q(\alpha)$ and how big is that $Q(\alpha)$ over Q is as we saw earlier.

α satisfies a degree 3 irreducible polynomial. So this is a degree 3 extension. So now let us go back and use another part of the fundamental theorem of Galois Theory. So recall again, fundamental theorem says the following. If I have the subgroup H , then the cardinality of H is actually the same as the degree of the extension K over K^H . So this was one of the parts of the fundamental theory.

So let us use this now because it gives us some valuable information. So, what does it say? Let us look at the subgroups. So, these are the three subgroups here whose cardinality is 2. So identity σ has cardinality 2. So, it says that K over K_2 , this extension must have degree 2. This is a subgroup of cardinality 2. So, this extension must have degree 2 and similarly, this extension must have degree 2.

Similarly now, this is a subgroup of cardinality 3, therefore this extension must have degree 3. So that is what we conclude. Now, observe that the total extension, which is K over Q , that we already know what its degree was, that was the original Galois extension whose degree was 6. So that allows us to sort of conclude that in order to calculate the degrees of these other extensions by using the tower property.

So for example, I go from Q to K_1 to K , the total degree must be 6. So, therefore this must be 2. Now, total must be 6, so these 3 must all be threes. So, I can work out all the degrees of the extensions by using this other part of the fundamental theorem. Now, let us go back and revisit what we know about K_1 , K_2 and so on. So K_1 over Q , I know is degree 2. Now, what do I know about K_1 ? I know that K_1 contains $Q(\omega)$ certainly.

K 1 is at least as big as Q omega but Q omega over Q is already degree 2. So by degree considerations by degrees, I (compute) I conclude that K 1 cannot be any bigger than Q omega. That is about it because already I have gotten a degree 2. By the same token, I take K 2 which is, it contains Q alpha for sure. But the degree of K 2 over Q is 3.

So, I have already gotten 3. I cannot get anything larger. So this can only be Q alpha and similarly, if you look at the other two fields K 3, similarly will be Q of alpha omega and K 4 turned out to be Q of alpha omega square. So these are all the degree 3 extensions. So what we have really is, you know, we have sort of looked at the entire Fundamental Theorem of Galois theory in this case.

(Refer Slide Time: 38:04)

(4) F_{p^n}/F_p Galois: \checkmark Normal: $F_{p^n} = \text{SF of } X^{p^n} - X$

\checkmark separable: F_p is perfect.
(any alg. extⁿ of F_p is separable)

$[F_{p^n} : F_p] = n = |\text{Aut}(F_{p^n}/F_p)|$

recall: Frobenius automorphism of F_{p^n}

$F_{p^n} \xrightarrow{\varphi} F_{p^n}$; $\varphi(a) = a^p \quad \forall a \in F_p$
 $a \rightarrow a^p \quad \Rightarrow \varphi \in \text{Aut}(F_{p^n}/F_p)$



Good. Now, let us do one last computation and this time not over the field Q but rather over a finite field. So compute the Galois group of the extension F_{p^n} over F_p . First, let us check that this is Galois again. So, we need what? Normal and separable; normal is easy because recall F_{p^n} more or less is the splitting field. This is how it was constructed if you wish; you just take this polynomial, x raised to the p to the n minus x and in fact, all the solutions, the roots themselves form a field.

So for sure, it is the splitting field of this polynomial. This polynomial splits completely over this field. So therefore, it is normal and separable recall again comes for free in this case, because we had shown that F_p being a finite field is perfect. Therefore, any algebraic extension of a perfect field is automatically any algebraic extension of F_p is automatically separable. So it is Galois for sure. So the question is what is the Galois group?

Well, we know the cardinality F_p^n over F_p recall is just an extension of degree n . Therefore, the Galois group the automorphisms which fix F_p , this must have cardinality n . So again, we could try and find some elements of this Galois group. Now, you know, since we did not quite construct F_p^n as F_p adjoin with some elements. Rather, we did something more indirect; you know wrote it as a splitting field of some polynomial and so on.

So we do not quite know given an element of F_p^n . What is, what exactly is its irreducible polynomial and so on. So the sort of analysis we did for the first three problems will not work here. But fortunately, we actually have some readymade elements of the Galois group. So recall, when we talked about perfectness, and so on we introduced what we call the Frobenius map.

So what was the Frobenius? Well, because F_p is perfect, it is automorphism for F_p^3 n , in fact. So recall the Frobenius automorphism of F_p^n is just a map. Let us call it ϕ , which takes any element to its p th power. We had shown that this is a field automorphism because F_p^n is finite. This is, I mean, it is always injective because F_p^n is finite; this is surjective as well.

So it was an automorphism. So here is at least one element ϕ . It is an automorphism of F_p to the n . Observe that if I take an element a which comes from the base field, F_p then ϕ of a is actually equal to a because remember, elements of F_p , they satisfy $a^p = a$. So every element of F_p certainly satisfies this equation. Now, so why did I say this, this therefore means that ϕ is an element of the Galois group. It not only is an automorphism of F_p^n , it also fixes every element of the base field F_p .

(Refer Slide Time: 41:56)


(4) $\mathbb{F}_{p^n}/\mathbb{F}_p$ Galois: \checkmark Normal: $\mathbb{F}_{p^n} = \text{SF of } X^{p^n} - X$

\checkmark separable: \mathbb{F}_p is perfect.
(any alg. extⁿ of \mathbb{F}_p is separable)

$[\mathbb{F}_{p^n} : \mathbb{F}_p] = n = |\text{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p)|$

recall: Frobenius automorphism of \mathbb{F}_{p^n}


$\mathbb{F}_{p^n} \xrightarrow{\varphi} \mathbb{F}_{p^n}$; $\varphi(a) = a^p \quad \forall a \in \mathbb{F}_{p^n}$
 $a \mapsto a^p \Rightarrow \varphi \in \text{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p)$



claim: $\underbrace{\varphi \circ \varphi \circ \dots \circ \varphi}_{k \text{ times}} \neq \text{id}$ if $1 \leq k < n$.

Pf: If $\varphi^k = \text{id} \Rightarrow \varphi^k(a) = a^{p^k} = \text{id}(a) = a$
 $\forall a \in \mathbb{F}_{p^n} \Rightarrow a^{p^k} - a = 0 \quad \forall a \in \mathbb{F}_{p^n}$

$f(x) = X^{p^k} - X \in \mathbb{F}_p[X]$ degree p^k
 has p^k roots in \mathbb{F}_{p^n} ; impossible if $n > k$.



Now, the claim is that this element phi that we have constructed let us try and compute its order in this group. It is an element of the Galois group. What is its order? The total order is n. So the order of this element in the Galois group can, has to be some divisor of n but the claim is that the order is exactly n. In other words, the Galois group is cyclic.

So what does that mean? I have, here is what I am going to prove that if I compose phi with itself, k times. Suppose I compose phi with itself k times to get identity, then this means that you know, this cannot happen if k is smaller than n. So let us just say this. This cannot be the identity. If k is any number, that is smaller than n k times.

Why is this? Well, let us try to see what this would mean. So if phi to the k is identity, so phi to the k is just this composition. What does this mean? This means that, how do I apply phi? I

keep you know, so I acted on an element phi to the k acting on an element a is just a to the p, the whole to the p to the whole to the p and so on.

So it is a to the p square, a to the p cubed etc. So this is just a to the p to the k. So if this is equal to a, so this is on the one hand, the identity map is just a. So these are both equal to each other implies that so this is for every element a of my field F_{p^n} . Therefore, what I am claiming is a to the p to the k is equal to a for all elements of F_{p^n} .

But observe that, if you looked at this polynomial x to the p to the k minus x , consider this polynomial. What is the degree of this polynomial? It is just p to the k and what we are claiming is that this polynomial has p to the n roots because every element of F_{p^n} is root a root of this polynomial and now, what we are concluding is that this polynomial has p to the n roots in this extension field F_{p^n} .

This is clearly impossible if n is bigger than k. you can only have p to the k possible roots maximum. You cannot get p to the n, where n is bigger than it. So that is the contradiction. So that tells you that phi to the k cannot possibly be the identity if k is strictly smaller than n.

(Refer Slide Time: 45:03)

Note: $\varphi^n = \text{id}$ since $a^{p^n} - a = 0 \quad \forall a \in F_{p^n}$

$\Rightarrow \text{Aut}(F_{p^n}/F_p) = \{ \text{id}, \varphi, \varphi^2, \dots, \varphi^{n-1} \}$

FTGT

Subgroups: $\{ \text{id}, \varphi^d, \varphi^{2d}, \dots, \varphi^n \}$ where $d|n$

$= H_d$

$\left(F_{p^n}\right)^{H_d} = \left\{ a \in F_{p^n} \mid \varphi^d(a) = a \right\} = \left\{ a \in F_{p^n} \mid a^{p^d} - a = 0 \right\}$



So what this means is and of course phi to the n is identity is clear. Also, observe more or less by the definition of the finite field, phi to the n is surely identity. Since a to the p to the n minus a is 0 for all a in the finite field. So the conclusion is that the Galois group, the automorphism group of F_{p^n} over F_p is exactly the cyclic group generated by phi.

What are the elements; identity, ϕ , ϕ^2 and so on ϕ^{n-1} . So, these are the elements of the Galois group and again sort of by similar token, one can work out the fundamental theorem of Galois Theory. So, will tell you that the subgroups of this group are in one to one correspondence with the intermediate subfields and if you sort of see, what are the sub groups of a cyclic group?

They can only look like; they are also cyclic generated by some element ϕ^d , ϕ^{2d} , ϕ^{3d} , ..., $\phi^{(n/d)d} = \phi^n = 1$, where d is some divisor of n . so you can look at these groups and so if you take this, maybe we should call this something H_d . So, what are the possible sub groups? They all look like this. H_d , where d divides n and you can ask what is the fixed field of this group?

So, this is my F_{p^n} and I need to ask, what is the fixed field of this sub group? By definition, it is all those elements which are fixed. It is enough if it is fixed by ϕ^d then it would be automatically fixed by all the others. So this is almost like the calculation we just did. So what is this? This is just all those elements a such that $a^{p^d} - a = 0$. So, it is all those elements of F_{p^n} which satisfies this property.

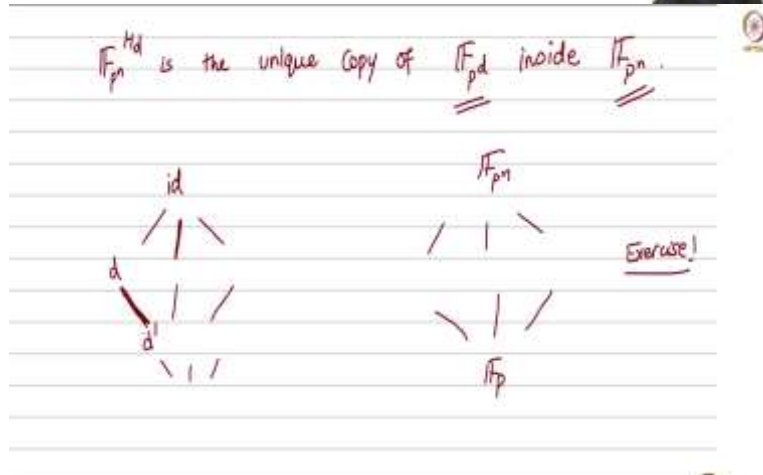
(Refer Slide Time: 47:34)

$$\text{Note: } \varphi^n = \text{id} \text{ since } a^n - a = 0 \quad \forall a \in \mathbb{F}_{p^n}$$

$$\Rightarrow \text{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \{\text{id}, \varphi, \varphi^2, \dots, \varphi^{n-1}\}$$

FTGT
 Subgroups: $\{\text{id}, \varphi^d, \varphi^{2d}, \dots, \varphi^n\}$ where $d|n$
 $= H_d$

$$\left(\mathbb{F}_{p^n}\right)^{H_d} = \left\{ a \in \mathbb{F}_{p^n} \mid \varphi^d(a) = a \right\} = \left\{ a \in \mathbb{F}_{p^n} \mid a^{p^d} - a = 0 \right\}$$



And recall, that from the earlier discussion of subfields of finite fields and so on, this collection here is actually is, so this H_d , the fixed field is, it is the copy of, it is the unique copy of the finite field \mathbb{F}_{p^d} that lives inside \mathbb{F}_{p^n} . So recall, go back and look at that earlier lecture, for every divisor d of n you can find a unique copy of \mathbb{F}_{p^d} inside \mathbb{F}_{p^n} and how do you get that copy?

You just take those elements of \mathbb{F}_{p^n} which satisfy, which satisfy this exact equation, $a^{p^d} - a = 0$. Good. So that sort of ties it up nicely with what we have seen earlier and you know you can also draw for example, the same sort of diagram which we did. You can see, what are the device a relation and so on and similarly you can get something on the other side, which tells you how the various sub groups live inside \mathbb{F}_{p^n} .

So I am going to leave that as an exercise for you to figure out. So these lines here are just going to go between two numbers d and d' whenever d divides d' . That is going to be the, those lines there.