

Introduction to Galois Theory
Professor Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute
Lecture 16
Problem Session 3

Welcome back, in the last video we define what normal extensions are, in fact I proved a theorem given 3 equivalent conditions for an extension to be normal. And we also looked at another criteria for an extension to be Galois. So, it is a purely numerical statement which says that the degree of the extension should be equal to the order of the Galois group.

(Refer Slide Time: 00:41)


any of the equivalent

Remark { A Galois extension is normal, but the converse is not true, in general
 In char 0, Galois \Leftrightarrow normal (for finite extensions)

Problems Find the Galois groups and determine if the extensions are Galois or normal.

(1) $K = \mathbb{Q}(\sqrt[3]{2})$
 $[K:\mathbb{Q}] = 3$
 $F = \mathbb{Q}$

Galois group $= \{1\}$; not Galois ✓ not normal
 $[K:\mathbb{Q}] = 3$, but $|\text{Gal}(K/\mathbb{Q})| = 1$
 $x^3 - 2 \in \mathbb{Q}[x]$ is irr, has a root in K , but doesn't split completely



$$\begin{aligned}
 & (2) \quad K = \mathbb{Q}(\sqrt{2}, i) \quad \text{Galois group} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \quad K, \text{ but doesn't split completely} \\
 & \quad \quad \quad 14 \quad \quad \quad 4 \text{ elements in } \text{Gal}(K/\mathbb{Q}) \quad \Rightarrow \quad \text{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \\
 & \quad \quad \quad F = \mathbb{Q} \quad \quad \quad \begin{array}{c} 1, \sigma_1, \sigma_2, \sigma_3 \\ \downarrow \quad \downarrow \quad \downarrow \\ i \mapsto -i \quad i \mapsto i \quad i \mapsto -i \\ \text{fixes } \sqrt{2} \end{array} \quad \left| \begin{array}{l} \sigma_1^2 = \sigma_2^2 = \sigma_3^2 = 1 \\ |G| = 4 = [K:\mathbb{Q}] \end{array} \right. \checkmark \\
 & \quad \quad \quad \text{Galois } \checkmark \\
 & \quad \quad \quad \text{normal } \checkmark \\
 & \quad \quad \quad \hookrightarrow \text{sp. fld of } (x^2-2)(x^2+1)
 \end{aligned}$$



So, we have done quite a bit of material in the last few lectures. So, let us take stock and do a few exercises to make sure that we understand all the various features of what we have learned in the last few videos. So, today in this problem session, we are going to essentially look at several examples and show that, determine the Galois groups, determine if it is a Galois extension, if it is a normal extension and so on. So, in each of the below extensions, find the Galois group and determine if the extensions are Galois, normal or normal.

So, we will do a few examples just so that we are familiar with this. So, some of these we have discussed before, let us take this and \mathbb{Q} . So here, the Galois group I will quickly go over this because, we discussed this already, Galois group here is trivial because, cube root of 2 has only one possible image in K . In general, in complex numbers, cube root of 2 can go to cube root of 2, cube root of 2 omega, cube root of 2 times omega square, but the second and third ones are not in K .

So, the only possibilities for cube, images of cube root of image of cube root of 2 is just cube root of itself. So, this is a Galois group and the fixed field is K itself. So, this is not Galois because the fixed field is not \mathbb{Q} or equivalently the degree of the fixed field is one whereas the extension of the, degree of the extension is 3. So, $K:\mathbb{Q}$ is 3, $K:\mathbb{Q}$ is 1, $K:\mathbb{Q}$ is, so what I mean is K over \mathbb{Q} has degree 3. But the Galois group has ordered 1, so this is not Galois.

It is also not normal, I claim. Because, for example, remember the second condition of the previous theorem, it says that if a polynomial, irreducible polynomial has one root, it splits completely, that is not the case here. $X^3 - 2$ is irreducible has a root in K , but does not split completely.

Because it only splits as a linear polynomial, terms a quadratic polynomial because that other 2 roots are not in K , so it is not Galois not normal. And by the remark I ended the last video with because this is characteristic 0, Galois and normal are in fact equivalent. So, if it is not Galois, it cannot be normal. But we have not proved that. So, let us separately check that in each example. The second example is also something that we have seen before, K is \mathbb{Q} adjoin $\sqrt{2}$ comma i and F is \mathbb{Q} again.

So, here are the degree is 4 and the Galois group, again I will go this fast because, we have discussed this in detail in earlier videos, $\sqrt{2}$ can go to either $\sqrt{2}$ or minus $\sqrt{2}$, i can go to either i or minus i , and those $2 \times 2 = 4$ choices will give you a group which is isomorphic to this. So, maybe I have not quite proved this, that it is isomorphic to this, let us do that. So, there are 4 elements in Galois group of K over F .

What are they, 1, σ_1 , σ_2 , and σ_3 , this is something that I have used earlier notation, so I will not write them again. But σ_1 sends i^2 minus i , and $\sqrt{2}$ to $\sqrt{2}$. Maybe I am interchanging these but it does not matter, σ_2 send i to i $\sqrt{2}$ to minus $\sqrt{2}$. And σ_3 sends i^2 minus i $\sqrt{2}$ to minus $\sqrt{2}$. So, here you see that σ_1 , σ_2 is σ_3 , in fact more directly, you see that σ_1^2 equals σ_2^2 equals σ_3^2 square is identity, each of them is an order 2 element.

So, there are only 4 groups of isomorphism, there are only 2 groups up to isomorphism of order 4. One is a cyclic group $\mathbb{Z}/4\mathbb{Z}$, which admits a degree 4 element, the other is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ which is not cyclic, in other words, it does not have a degree 4, order 4 element. So, every element is ordered 2. So, this must be $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

So, that is the Galois group and it is Galois because, for example, the cardinality of the Galois group is 4, which is the degree of the extension it is also normal, because it is a splitting field of, so I am going to write this somewhat messily, but I hope this is okay. It is a splitting field of this,

because you take $x^2 - 2$ it splits completely to take $x^2 + 1$ it splits completely however, it and further it is generated by the roots. So, it is normal and Galois.

(Refer Slide Time: 06:27)

$K = \mathbb{Q}(\alpha)$
 Let $\alpha \in K \setminus \mathbb{Q}$, so $K = \mathbb{Q}(\alpha)$ $\left\{ \begin{array}{l} K/\mathbb{Q} \text{ normal, Galois} \end{array} \right.$
 Let $f = x^2 + bx + c \in \mathbb{Q}[x]$ be the irr poly of α/\mathbb{Q} .
 Suppose α, β are roots of f in \mathbb{C} . $b, c \in \mathbb{Q} \subseteq K$.
 Then $\alpha + \beta = -b \Rightarrow \beta = -b - \alpha \in K$.
 $K = \text{Sp. fld of } f \text{ over } \mathbb{Q} \Rightarrow K \text{ is normal over } \mathbb{Q}$.
 Note that $\alpha \neq \beta$: because f is irr.
 $f = (x - \alpha)(x - \beta)$
 Consider $\sigma: K \rightarrow K$ $\sigma(\alpha) = \beta \neq \alpha$.
 σ is a \mathbb{Q} -auto of K and $\sigma \neq 1$.
 $|\text{Gal}(K/\mathbb{Q})| = 2 = [K:\mathbb{Q}] \Rightarrow K/\mathbb{Q} \text{ Galois}$.
 Remark: Any deg 2 ext of field is normal but need not be Galois.
 Important: An irr poly in $\mathbb{Q}[x]$ has distinct roots in any extension field.

Note that $\alpha \neq \beta$: because f is irr.
 $f = (x - \alpha)(x - \beta)$
 Consider $\sigma: K \rightarrow K$ $\sigma(\alpha) = \beta \neq \alpha$.
 σ is a \mathbb{Q} -auto of K and $\sigma \neq 1$.
 $\text{Gal}(K/\mathbb{Q}) = \{1, \sigma\} \Rightarrow |\text{Gal}(K/\mathbb{Q})| = 2 = [K:\mathbb{Q}] \Rightarrow K/\mathbb{Q} \text{ Galois}$.
 Remark: Any deg 2 ext K/\mathbb{Q} of char 0 fields is Galois.

to be found later

Problems: Find the Galois groups and determine if the extensions are Galois or normal.

(1) $K = \mathbb{Q}(\sqrt[3]{2})$
 $|K:\mathbb{Q}| = 3$
 $F = \mathbb{Q}$
 Galois group = $\{1\}$; not Galois ✓ not normal
 $[K:\mathbb{Q}] = 3$, but $|\text{Gal}(K/\mathbb{Q})| = 1$
 $x^3 - 2 \in \mathbb{Q}[x]$ is irr, has a root in K , but doesn't split completely

(2) $K = \mathbb{Q}(\sqrt{2}, i)$
 $|K:\mathbb{Q}| = 4$
 $F = \mathbb{Q}$
 Galois ✓
 4 elements in $\text{Gal}(K/F)$
 $1, \sigma_1, \sigma_2, \sigma_3 \rightarrow \begin{matrix} \text{irr} \rightarrow i \\ \text{irr} \rightarrow -i \\ \text{irr} \rightarrow -i \end{matrix}$
 $\sigma_1^2 = \sigma_2^2 = \sigma_3^2 = 1 \Rightarrow \text{Gal}(K/F) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$
 $|G| = 4 = [K:\mathbb{Q}]$ ✓

(4) $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$
 $|K:\mathbb{Q}| = 6$
 $F = \mathbb{Q}$
 ω : primitive 3rd root of unity
 $\sqrt[3]{2} \in \mathbb{R}$ cube root of 2
 $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$
 Know: K is the sp. fld of $x^3 - 2$ over \mathbb{Q}
 So K/\mathbb{Q} is normal
 Possible images of $\sqrt[3]{2}$ are: $\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$ (3 choices)
 ω are: ω, ω^2 (2 choices)
 There exists a homomorphism $K \rightarrow K$ for every choice of images of $\omega, \sqrt[3]{2}$.

And the third example is more general example. So, let K be any extension of \mathbb{Q} of degree 2. So, what we have is K over \mathbb{Q} degree 2. So, I claim that here no matter what case, I claim Galois is mod 2 \mathbb{Z} and K over \mathbb{Q} is normal and Galois. So, this is true, in general actually this is true even if you replace \mathbb{Q} by any other field of characteristic 0. So, I will do this example here just to stick to a simple case and we will discuss more generally what this means later.

So, let α be in K which is not in \mathbb{Q} . So, first observation is that K is $\mathbb{Q}(\alpha)$ because it is a degree 2 extension. So, if $\mathbb{Q}(\alpha)$ is an intermediate field, it is either equal to K or equal to \mathbb{Q} because this product of these 2 numbers is 2. So, you can not have, you must have one of them equal to 1. So, either $\mathbb{Q}(\alpha)$ is equal to \mathbb{Q} in which case α is in \mathbb{Q} , but α is not in \mathbb{Q} . So,

$\mathbb{Q}(\alpha)$ must be in K because K is degree 2 extension of \mathbb{Q} it is not equal to \mathbb{Q} , so you can choose α . So, that I should have said first.

So, there is an α in K mod in \mathbb{Q} , so K is equal to $\mathbb{Q}(\alpha)$. Now, let f be the irreducible polynomial of α over \mathbb{Q} . Remember it must be a degree 2 polynomial because it is a degree 2 extension. So, α has degree 2, so this is the irreducible polynomial. So, suppose α and β are roots of f a priori in \mathbb{C} or in some large field. So, we know then $\alpha + \beta$ is equal to $-b$, this implies β is $-\alpha - b$. So, $\alpha + \beta$ is $-b$ I think, because that is the negative.

So, $-\alpha - b$. So, this I claim is in K because b is in \mathbb{C} , remember b, c are in \mathbb{Q} , I should say $\mathbb{Q}(\alpha)$ is K . So, b, c are in K , α is in K , so this is in K . That means, K must be the splitting field of f over \mathbb{Q} . So, this implies K is normal over \mathbb{Q} . So that much is clear, because it is a splitting field so it is normal. So, why is a Galois group $\mathbb{Z}/2\mathbb{Z}$ because here the point is α and β . So, you have α and β distinct that is because, this is because f is irreducible.

So, f is irreducible so if α and β are and f is equal to $X^2 - (\alpha + \beta)X + \alpha\beta$. So, also, so $X^2 - (\alpha + \beta)X + \alpha\beta$ is f and this is here, if α is equal to β that means that, so one has to think about this a little bit, but if you have it is characteristic 0 is important here. So, let me just, so here an irreducible polynomial cannot have distinct, repeated roots, so that, so this is something that maybe you have looked in ring theory courses in the past and we will anyway come back to this when we talk about separable polynomials.

So, the point here is, a irreducible polynomial in $K[X]$ has distinct roots in any extension field where it has roots it roots must be distinct. So, that means, that means, so if it is not irreducible, of course, it need not be because you can have $X^2 - 1$ whole square, it has repeated roots, but it would not happen for irreducible polynomials. So, this is a fact which I will omit, I mean any explanation of this will omit for now, but we will come back to this later.

So, that means σ , so consider σ from K to K sending α to β . So, σ is a K/\mathbb{Q} automorphism of K because it is a splitting field. So, any map like this is an automorphism and

σ is different from identity because β and α are different, α goes to α under identity. So, Galois group is in fact, so, the cardinality of the Galois group is 2 which is the degree of the extension. So, K over F is Galois.

So, any degree to extension is Galois. So, remark exactly the same proof there will be no difference, we will work to show that if K over F is a degree to extension. So, any degree 2 extension of characteristic 0 field is Galois. So, the same proof, the only place where degree characteristic 0 is used is here. So, provided its characteristic 0 in fact, more generally you can say this even in characteristic p and we will do that later, but for now, let me just end this problem with this remark.

So, any degree to extension is normal which is nice. Whereas, you see that degree 3 extensions need not be Galois in general, even in characteristic 0. So, this is not Galois, degree 3 non Galois. So, next let us look at the following examples of 4. Let us look at, this is also something that we have repeatedly seen. So, this is ω is primitive third root of unity and cube root of 2, let us say is a cube root of 2, real cube root of 2.

And this is degree 6, this is something that you can easily conclude by the tower. So, this is 3 because $X^3 - 2$ is irreducible by Eisenstein, and one can argue that this must be 2 because ω satisfies a degree 2 polynomial over \mathbb{Q} . And it cannot be so, it is at least at most 2, it cannot be one because this is real field. So, this is 2. So, this is 6. So, now the question that we want to answer is, what is the Galois group whether it is Galois and whether it is normal.

So, immediately we can conclude that we know in fact that K is the splitting field of $X^3 - 2$ over \mathbb{Q} , so K over \mathbb{Q} is normal, that is all right not. It is a splitting field because it splits $X^3 - 2$ splits completely over this and it is generated by the root, so it is normal. Remember roots of this polynomial are, so all the, all of them are in K and if remove any of them you do not get K you get something smaller. So, K is the splitting field.

So, now, let me address the question of what is the Galois group and what is the, the Galois extension or whether it is a Galois extension. So, actually I forgot to make a remark here. So, remark here is, this degree to extension, any degree to extension of fields is normal. See up to

normality, we have not invoked anything about characteristics 0 or not. So, any degree to extension of fields is normal, but need not, need not be Galois.

So, this will give us an opportunity to construct an example of a normal but not Galois extension. So, by suitably taking a degree to extension, which is not Galois. So that was the remark about this. Let us continue now. So, I want to now understand what the Galois group is. So, now, let me invoke our standard mantra about how to construct field homomorphisms. So, possible images of cube root of 2 are cube root of 2, cube root of 2 mega.

So, there are 3 choices. Remember, all of them are in K . That is part of the fact that it is normal. So, and possible images of ω are, ω and ω square because those are the only roots of its irreducible polynomial, which is $X^2 + X + 1$, this is the irreducible polynomial of ω over \mathbb{Q} . So, ω and ω squared are the possibilities.

Now, one more fact I will repeat now, which maybe I have not emphasized enough is, it is well, and good to say that images of an element are its conjugates only possible images of elements, algebraic elements are its conjugate, so you have to take its irreducible polynomial. And look at the other roots of the irreducible polynomial, but more is true actually, you can construct a homomorphism by sending an element to its conjugate.

So not only is looking at conjugates limits your constraints, but every possibility of an element, its conjugate will give you a homomorphism. So, you can construct a homomorphism from K to K . So in other words, what I am saying is that there exist a homomorphism from K to K , for every choice of images for ω and cube root of 2. This is a stronger statement, I am saying that first step is to limit the possibilities of images for ω , which are only 2 and images of cube root of 2 which are 3.

So, there are 3 choices for cube root of 2 at most 3, at most 2 choices for ω . But now, I am saying an additional statement, which is a stronger statement, you take any choice for example, take ω to ω cube root of 2 to cube root of 2 ω , you can construct a homomorphism that way, you can take ω to any of these 2 and cube root of 2 to any of these 3 and you can construct a homomorphism that way. This is a consequence of extension theorems, that we did in an earlier video.

Very briefly, the point is, you can take cube root of 2 and any other image any other possibility, any other conjugate, you can construct a map because these are both isomorphic to cube root of $Q[X]$ modulo $x^3 - 2$, this is where the conjugates, conjugate is important, because they have the same irreducible polynomial. So, you can construct this and then extension theorem can be invoked to extend it. So, you can put in this place, can put any conjugate here.

So, this later part is extension theorems. So, first step is to construct Q cube root of 2 to $Q(\beta)$, where β is any of these 3 elements or more generally, for any α , you can take any β conjugate and then you extend by extension theorems, so all this song and dance says that there are 6 choices. In fact, let me say automorphisms because ω can go to one of the 2 possibilities and there are independent possibilities cube root of 2 can go to one of the 3 and you can choose them independently.


So, the 3 times 2 6 things and there are only 6 because you take any automorphism of K to K and look at where cube root of 2 goes, it goes to one of these 3, and when you look at where ω goes, it goes to one of these 2, so it must be one of the 6 that we have listed here. And remember once you determine the image of cube root of 2 and ω , the entire automorphism is fixed because K is spanned by these 2 as polynomials with coefficients in Q .

(Refer Slide Time: 20:55)

Hence $|\text{Gal}(K/Q)| = 6 = [K:Q] \Rightarrow K/Q$ is Galois.

Finally what is $\text{Gal}(K/Q)$? There are only 2 groups of order 6, upto isomorphism: $(\mathbb{Z}/6\mathbb{Z})_x$, $(S_3) \checkmark$

$\sigma, \tau \in \text{Gal}(K/Q) : \sigma : \sqrt[3]{2} \mapsto \sqrt[3]{2} \quad \omega \mapsto \omega$ $\tau : \sqrt[3]{2} \mapsto \sqrt[3]{2} \quad \omega \mapsto \omega^2$




(4) $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$ ω : primitive 3rd root of unity
 $\sqrt[3]{2} \in \mathbb{R}$ cube root of 2

Know: K is the s.f.d of $X^3 - 2$ over \mathbb{Q}
 So K/\mathbb{Q} is normal $\Rightarrow \sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$

Possible images of $\sqrt[3]{2}$ are: $\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$ (3 choices)
 ω are: ω, ω^2 (2 choices)

There exists a homom $K \rightarrow K$ for every choice of images of $\omega, \sqrt[3]{2}$.
 This is a consequence of extension theorems:
 Hence there are $6 = 3 \times 2$ automorphisms $K \rightarrow K$, there are only six

$\mathbb{Q}(\sqrt[3]{2}) \xrightarrow{\sigma, \tau} \mathbb{Q}(\sqrt[3]{2})$
 $\mathbb{Q}(\sqrt[3]{2}) \xrightarrow{\sigma, \tau} \mathbb{Q}(\sqrt[3]{2}\omega)$
 $\mathbb{Q}(\sqrt[3]{2}) \xrightarrow{\sigma, \tau} \mathbb{Q}(\sqrt[3]{2}\omega^2)$
 can get any complete set



order 6, upto isomorphism $(\mathbb{Z}/6\mathbb{Z}) \cong S_3$

$$\sigma, \tau \in \text{Gal}(K/\mathbb{Q}) : \sigma : \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega, \omega \mapsto \omega \quad \tau : \sqrt[3]{2} \mapsto \sqrt[3]{2}, \omega \mapsto \omega^2$$

$$\sigma\tau : \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega \mapsto \sqrt[3]{2}\omega^2, \omega \mapsto \omega^2 \mapsto \omega$$

$$\tau\sigma : \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega \mapsto \sqrt[3]{2}\omega^2, \omega \mapsto \omega \mapsto \omega^2$$

ord(σ) = 3, ord(τ) = 2

exercises

So $\sigma\tau \neq \tau\sigma \Rightarrow \text{Gal}(K/\mathbb{Q})$ is Not abelian

Let $\alpha \in \mathbb{C}$

$$f = (X - \alpha)(X - \bar{\alpha})$$

One

has distinct roots in any extension field

Consider $\sigma: K \rightarrow K$ $\sigma(\alpha) = \bar{\alpha} \neq \alpha$

σ is a \mathbb{Q} -auto of K and $\sigma \neq 1$

$$\text{Gal}(K/\mathbb{Q}) = \{1, \sigma\} \Rightarrow |\text{Gal}(K/\mathbb{Q})| = 2 = [K:\mathbb{Q}] \Rightarrow K/\mathbb{Q} \text{ Galois}$$

Remark: Any degree 2 ext K/\mathbb{Q} of char 0 fields is Galois.

$$(4) K = \mathbb{Q}(\sqrt[3]{2}, \omega)$$

ω : primitive 3rd root of unity
 $\sqrt[3]{2} \in \mathbb{R}$ cube root of 2

$$\begin{array}{l} \mathbb{Q}(\sqrt[3]{2}, \omega) \\ |2 \\ \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R} \\ |3 \\ \mathbb{Q} \end{array}$$

Know: K is the sp. fld of $X^3 - 2$ over \mathbb{Q}

So K/\mathbb{Q} is normal roots $\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$

What are the images of $\sqrt[3]{2}$ in K/\mathbb{Q}

Possible images of $\sqrt[3]{2}$ are: $\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$ (3 choices)



$$\begin{array}{l} \sigma: \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega \\ \omega \mapsto \omega^2 \mapsto \omega \\ \tau: \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega^2 \\ \omega \mapsto \omega \mapsto \omega^2 \end{array}$$

} So $\sigma\tau \neq \tau\sigma \Rightarrow \text{Gal}(K/\mathbb{Q})$ is Not abelian

exercises

$$\Rightarrow \text{Gal}(K/\mathbb{Q}) \cong S_3$$

$$(5) \mathbb{Q}(\sqrt[4]{2}) = K \quad \text{Not normal: } f = X^4 - 2 \text{ has a root, but not all roots.}$$

$$\begin{array}{l} |4 \\ \mathbb{Q} = F \end{array}$$

$$\text{roots: } (\pm \sqrt[4]{2}, \pm \sqrt[4]{2}i)$$

$$\text{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}: \text{possible images of } \sqrt[4]{2}$$



$$\begin{aligned}
 & \tau: \sqrt[4]{2} \mapsto \sqrt[4]{2} \quad \omega: \sqrt[4]{2} \mapsto \sqrt[4]{2} \omega \\
 & \omega: \sqrt[4]{2} \mapsto \sqrt[4]{2} \omega \mapsto \sqrt[4]{2} \omega^2 \\
 & \Rightarrow \text{Gal}(K/\mathbb{Q}) \cong \frac{\mathbb{Z}}{6\mathbb{Z}} \quad \text{alternation} \\
 & 5) \quad \mathbb{Q}(\sqrt[4]{2}) = K \quad \text{Not normal: } f = x^4 - 2, \text{ has a root, but not all roots.} \\
 & \quad \quad \quad \mathbb{Q} = F \quad \text{roots: } (\pm \sqrt[4]{2}, \pm \sqrt[4]{2}i) \\
 & \quad \quad \quad \sigma: K \rightarrow K \quad \text{Gal}(K/\mathbb{Q}) \cong \frac{\mathbb{Z}}{2\mathbb{Z}}: \text{possible images of } \sqrt[4]{2} \text{ in } K \\
 & \quad \quad \quad \quad \quad \quad \quad \quad \quad \text{are } \sqrt[4]{2}, -\sqrt[4]{2} \\
 & \quad \quad \quad \quad \quad \quad \quad \quad \quad 1: \sqrt[4]{2} \mapsto \sqrt[4]{2} \\
 & \quad \quad \quad \quad \quad \quad \quad \quad \quad \sigma: \sqrt[4]{2} \mapsto -\sqrt[4]{2}
 \end{aligned}$$



$$\begin{aligned}
 & 5) \quad \mathbb{Q}(\sqrt[4]{2}) = K \quad \text{Not normal: } f = x^4 - 2, \text{ has a root, but not all roots.} \\
 & \quad \quad \quad \mathbb{Q} = F \quad \text{roots: } (\pm \sqrt[4]{2}, \pm \sqrt[4]{2}i) \\
 & \quad \quad \quad \sigma: K \rightarrow K \quad \text{Gal}(K/\mathbb{Q}) \cong \frac{\mathbb{Z}}{2\mathbb{Z}}: \text{possible images of } \sqrt[4]{2} \text{ in } K \\
 & \quad \quad \quad \quad \quad \quad \quad \quad \quad \text{are } \sqrt[4]{2}, -\sqrt[4]{2} \\
 & \quad \quad \quad \quad \quad \quad \quad \quad \quad 1: \sqrt[4]{2} \mapsto \sqrt[4]{2} \\
 & \quad \quad \quad \quad \quad \quad \quad \quad \quad \sigma: \sqrt[4]{2} \mapsto -\sqrt[4]{2} \\
 & \quad \quad \quad [K:F] = 4 > |\text{Gal}(K/\mathbb{Q})| = 2 \quad \Rightarrow K/F \text{ is not Galois.}
 \end{aligned}$$



So, that much says that there are 6 homomorphisms that means, the Galois group has ordered six which is, which is also the degree of the extension this implies K over \mathbb{Q} is Galois. So, this implies that K over \mathbb{Q} is Galois, very good. So, this shows that this is a Galois extension. So, it is a normal extension by the general theorem to be proved later, that in characteristic 0 normal and Galois same, because it is normal that we already know. We already know it is Galois but we are trying to prove this directly.

So finally, what is the Galois group, so often this is the last thing because you can determine Galois extension or not before this. So, now let us use some group theory there are only 2 groups of order 6. When I say a statement like this, or I always mean up to isomorphism. What are they,

they are $\mathbb{Z} \bmod 6$ the cyclic group of order 6 and S_3 the symmetric group of order 6. So now which of them is this Galois group, I claim that it is this and not this.

So why is that, so for this, I am going to exhibit 2 particular elements of the Galois group and show that they do not commute in which case it cannot be a cyclic group, so it cannot be that. So, σ is this choice that I take, cube root of 2 goes to cube root of 2 ω and ω goes to ω^2 . And τ , remember, to determine automorphism of K , all you need to specify is the image of cube root of 2 and ω . So, σ has this property τ sends cube root of 2 to cube root of 2, it fixes cube root of 2 and it sends ω to ω^2 .

So now what is, so you can check later that this is order 3 element, this is order 2 element because if you do σ^2 it will not be identity. However, if you do σ^3 , it will get identity. Similarly, τ^2 is identity, τ is not identity. So, these are both exercises for you. So, I would not do that. What I will now want to show that is $\sigma\tau$ is not equal to $\tau\sigma$. What does $\sigma\tau$ do to cube root of 2, $\sigma\tau$ sends cube root of 2, first see where τ sends cube root of 2 to, it sends cube root of 2 to cube root of 2.

Then what does σ do, σ sends it to cube root of 2 times ω . Now what does τ do to ω , it sends it to ω^2 , σ sends ω to ω^2 , so ω^2 goes to ω . Whereas $\tau\sigma$ goes to, first you apply σ . So that means you go to cube root of 2 times ω . And now τ , sends cube root of 2 to cube root of 2, but ω goes to ω^2 , so that will go to ω^2 times cube root of 2.

Already, you see that they are distinct. Just to finish it, let us see where ω goes under σ , under σ ω goes to ω^2 , but under τ ω goes to ω^2 . So, ω is the same image, but these are not equal. So, $\sigma\tau$ is not equal to $\tau\sigma$. And this implies Galois group of K over \mathbb{Q} is not abelian. So, it cannot be the abelian group of order 6. So that means Galois group is $\mathbb{Z} \bmod 6$. So that completes the analysis of this particular extension.

That is the fourth one, let me do one more. Let us do \mathbb{Q} adjoint fourth root of 2 over \mathbb{Q} . So, this is K , this is F . So, this is the degree 4 extension. So now, immediately, you can see that it is not normal. So you can take f to be $X^4 - 2$. $X^4 - 2$ has a root, but not all


roots because what are the roots of this, these are fourth root of 2 plus minus and plus minus fourth root of 2 times i, these are the roots. So not normal.

What about Galois, so it is also not Galois as we show, because Galois group of K over Q, let me sort of run through this quickly, I claim is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ because what are the possible images of fourth root of 2. So, a priori in the complex numbers, it can be fourth root of 2 minus fourth root of 2, fourth root of 2 i or minus fourth root of 2. But in K, because we are only interested in maps from K to K which fix Q.

Are fourth root of 2 and minus fourth root of 2, so there are 2 of them. So, that means there are only 2 homomorphisms; one is identity, which sends fourth root of 2 to fourth root of 2, the other is non identity, which sends fourth root of 2 to minus fourth root of 2. So, here there are 2 possibilities. So, there is only one group of order 2, namely the cyclic group of order 2.

So that means, the field Extension has degree 4, but this is strictly more than the, the degree of the, the order of the Galois group which is 2. So, this implies K over F is not Galois, so this is not Galois and we have also discussed the Galois group.

(Refer Slide Time: 26:50)



$[K:F] = 4 > |\text{Gal}(K/\mathbb{Q})| = 2$

What is $K^{\text{Gal}(K/\mathbb{Q})}$? We know $[K:K^{\text{Gal}(K/\mathbb{Q})}] = |\text{Gal}(K/\mathbb{Q})| = 2$

$\sqrt[4]{2} \in K = \mathbb{Q}(\sqrt[4]{2})$

$\mathbb{Q}(\sqrt[4]{2}) \subseteq K^{\text{Gal}(K/\mathbb{Q})}$


$\mathbb{Q}(\sqrt[4]{2}) \subseteq K$

$\mathbb{Q}(\sqrt[4]{2}) = K^{\text{Gal}(K/\mathbb{Q})}$

$\sigma(\sqrt[4]{2}) = \sqrt[4]{2} \Rightarrow \sqrt[4]{2}$ is fixed by $1, \sigma$.

$(\sqrt[4]{2})^2 = (\sqrt[4]{2})^2 \Rightarrow \sigma(\sqrt[4]{2}) = \sigma(\sqrt[4]{2})^2 = (-\sqrt[4]{2})^2 = \sqrt[4]{2}$

$\mathbb{Q}(\sqrt[4]{2}) \subseteq K^{\text{Gal}(K/\mathbb{Q})} \Rightarrow \mathbb{Q}(\sqrt[4]{2}) = K^{\text{Gal}(K/\mathbb{Q})}$ \square



$$\begin{array}{l}
 \mathbb{Q} = \mathbb{F} \\
 \sigma: K \rightarrow K \\
 \downarrow \\
 \mathbb{Q}
 \end{array}
 \quad
 \begin{array}{l}
 \text{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} : \text{possible images } \sqrt{2} \mapsto \pm \sqrt{2} \\
 1: \sqrt{2} \mapsto \sqrt{2} \\
 \sigma: \sqrt{2} \mapsto -\sqrt{2} \\
 [K:\mathbb{F}] = 4 > |\text{Gal}(K/\mathbb{Q})| = 2 \Rightarrow K/\mathbb{F} \text{ is not Galois}
 \end{array}$$



$$\begin{array}{l}
 \text{What is } \text{Gal}(K/\mathbb{Q})? \text{ We know } [K:K^{\text{Gal}(K/\mathbb{Q})}] = |\text{Gal}(K/\mathbb{Q})| = 2 \\
 K = \mathbb{Q}(\sqrt[4]{2}) \\
 \downarrow \\
 \mathbb{Q}
 \end{array}
 \quad
 \begin{array}{l}
 \sigma(\sqrt{2}) = \sqrt{2} \Rightarrow \sqrt{2} \text{ is fixed by } 1, \sigma
 \end{array}$$



But just let us for fun, what is determined what is the fixed field of the Galois group. See, we know that $[K:K^{\text{Gal}(K/\mathbb{Q})}] = |\text{Gal}(K/\mathbb{Q})|$, which is 2. So, these are all things that I have recalled, I have done in the past. So, this is true, because this is not $\mathbb{Z}/2\mathbb{Z}$. So, this is going to be a degree 2 extension of here. And that will in turn be a degree 2 extension of \mathbb{Q} , because this is degree 4.

But what is this, if you think about this, what are fixed by both this and this in fact, what is fixed by σ is $\sqrt{2}$. So $\sqrt{2}$, so $\sqrt{2}$ is fixed by 1 and σ . See because $\sqrt{2}$ must go to under σ $\sqrt{2}$ is fourth root of 2 whole square. So, $\sigma(\sqrt{2})$ is $\sigma(\sqrt[4]{2}^2)$ which is $\sigma(\sqrt[4]{2})^2$ which is $-\sqrt[4]{2}^2$ which is $\sqrt{2}$. So, that is the proof. So, $\sqrt{2}$ is fixed. So, that means, $\mathbb{Q}(\sqrt{2})$

So, of course, $\sqrt{2}$ belongs to this now, I should have said first. $\mathbb{Q}(\sqrt{2})$ is contained in the fixed field, but $\mathbb{Q}(\sqrt{2})$ is a degree 2 extension. So, that means $\mathbb{Q}(\sqrt{2})$ is equal to $K^{\text{Gal}(K/\mathbb{Q})}$. So, I went out this fast but I hope you understood the argument here. So, this shows that you have, in there is a first example where the extension fails to be Galois and the fixed field is in fact strictly in intermediate between the 2 fields we started with.

So, it is actually not 1 here, not 1 here. So, I have one more example that I want to do, but let me stop the video here. We have already spent a lot of time on this. And then in the next video, I will do some more problems. Thank you.