

Introduction to Galois Theory
Professor Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute
Lecture No 14
Galois Extensions, Galois Groups

(Refer Slide Time: 00:15)

Another approach: take any rational solution; repeat the above process
 to get another solution with fewer nonzero entries.
 The proof is complete. \square



K
 \vdots
 K^n
 prime field

K^n contains n

let K, L be two fields. $\sigma_1, \dots, \sigma_n: K \rightarrow L$ homom.
 The fixed field $F := \{a \in K \mid \sigma_1(a) = \dots = \sigma_n(a)\}$. This is a
 subfield of K .

Theorem I: let $\sigma_1, \dots, \sigma_n: K \rightarrow L$ be distinct field homom.,
 and let F be their fixed field. Then $[K:F] \geq n$.


Remarks: ① The proof will use the fact that $\sigma_1, \dots, \sigma_n$ are ind.
 (as characters of K^\times in L)
 ② $K = L = \mathbb{Q}(\sqrt{2}, i)$ Recall $\sigma_1, \sigma_2: K \rightarrow K$ $\left(\begin{matrix} \sigma_1: i \mapsto i, \sqrt{2} \mapsto \sqrt{2} \\ \sigma_2: i \mapsto -i, \sqrt{2} \mapsto -\sqrt{2} \end{matrix} \right)$
 Here, $K^{\{\sigma_1, \sigma_2\}} = \mathbb{Q}$



$$\text{Gal}(\mathbb{Q}(i, \sqrt{2})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

$$\text{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) \cong \{1\}$$


$$\text{Gal}(\mathbb{F}_p/\mathbb{F}_p) \cong \mathbb{Z}/p\mathbb{Z}$$



We will discuss
now in the
upcoming videos

Theorem II: Let K be any field, and let $\sigma_1, \dots, \sigma_n : K \rightarrow K$ be ^{distinct} field automorphisms. Suppose that $\{\sigma_1, \dots, \sigma_n\}$ forms a group under composition. If F is the fixed field of $\sigma_1, \dots, \sigma_n$, then $[K:F] = n$.

Proof: By the first theorem we have $[K:F] \geq n$. We know, in general, it can happen that $[K:F] > n$. But this theorem says that $\therefore \leftarrow \therefore \therefore n$ group then $[K:F] = n$.





Welcome back. In the last two videos, we proved two important theorems about fixed fields and now we are ready to start defining Galois extensions and then study them in detail. So, just to quickly recall, we proved the first theorem, which says that if you have two fields and a bunch of distinct fields homomorphisms, then the degree of K over the fixed field of those is at least the number of homomorphisms.

But if the fields are equal, so, namely K equal to L , and the homomorphisms that you are actually considering are actually automorphisms and there are N distinct ones and they form a group, then the degree of K over the fixed fields is exactly equal to N . So, in this video we are going to start defining Galois extensions.

(Refer Slide Time: 01:06)

Recall: Let K/F be a field extension. Then
$$\text{Gal}(K/F) = \{ \text{all } F\text{-automorphisms of } K \}$$

→ Called the GALOIS GROUP
Claim: $\text{Gal}(K/F)$ is a group under composition:
Easy to prove: $\begin{cases} 1: K \rightarrow K \text{ Identity} \in \text{Gal}(K/F) \checkmark \\ \sigma_1, \sigma_2: K \rightarrow K \text{ } F\text{-auto} \Rightarrow \sigma_1 \sigma_2 \text{ is also an } F\text{-auto } K \rightarrow K \checkmark \\ \sigma^{-1}: K \rightarrow K \text{ is an } F\text{-auto.} \end{cases}$



So, first let me quickly recall something I did in a video earlier but I want to repeat it again. Let K over F be a field extension. Then, the symbol here Galois, G-A-L K over F represents all F automorphisms of, okay? This, we claimed earlier and I did not prove this, but this is a trivial exercise, is a group under composition. So, this is easy to prove. So, let me just say a couple of lines about this but not give you a rigorous proof.

I am taking all F automorphisms right? So, identity is certainly an auto F automorphism and if σ_1 and σ_2 are F automorphisms, it is a triviality to check that their composition is also, is an F automorphism, right? That is all. So, you have inverse. By definition, an automorphism has an inverse; σ_1 inverse is an F automorphism. That is all.

So, it is not in general an abelian group. We will see that later because composition is not commutative and Galois groups can be non-commutative. So, this is called the Galois group of the extension. So, in the later part of this video I am going to give you more examples of this or explain the examples that I gave earlier.

(Refer Slide Time: 3:23)

Prop: Let K be any field and let G be a finite group of automorphisms of K .
Suppose F is the fixed field of G . Then $G = \text{Gal}(K/F)$.

Pf: • Know from theorem I: $[K:F] = |G| = n$.
• Clearly $G \subseteq \text{Gal}(K/F)$: this is because any $\sigma \in G$ fixes every element of F (i.e., $\sigma(a) = a \forall a \in F$),
So σ is an F -auto of K .



$$\text{Gal}(\mathbb{F}_p/\mathbb{F}_p) \cong \mathbb{Z}/p\mathbb{Z}$$

Theorem II: Let K be any field, and let $\sigma_1, \dots, \sigma_n: K \rightarrow K$ be ^{distinct} field automorphisms.
Suppose that $\{\sigma_1, \dots, \sigma_n\}$ forms a group under composition. If F is the
fixed field of $\sigma_1, \dots, \sigma_n$, then $[K:F] = n$.

Proof: By the first theorem we have $[K:F] \geq n$. We know, in general,
it can happen that $[K:F] > n$. But this theorem says that
if $\{\sigma_1, \dots, \sigma_n\}$ is a group then $[K:F] = n$.

As we prove this, note where we are using the hypothesis that
 $\{\sigma_1, \dots, \sigma_n\}$ forms a group.



Suppose F is the fixed field of G . Then $G = \text{Gal}(K/F)$.

Pf: • Know from theorem II: $[K:F] = |G| = n$.

• Clearly $G \subseteq \text{Gal}(K/F)$. This is because any $\sigma \in G$ fixes every element of F (i.e., $\sigma(a) = a \forall a \in F$); So σ is an F -auto of K . $\therefore \sigma \in \text{Gal}(K/F)$.

$\left. \begin{array}{l} \sigma \in \text{Gal}(K/F), \text{ so } \\ \sigma(a) = a \forall a \in F \\ \Rightarrow a \in K^S \end{array} \right\} \begin{array}{l} a \text{ is fixed by} \\ \text{every thing in } G \end{array}$

Suppose $\sigma \in \text{Gal}(K/F)$, $\sigma \notin G$. Let $S = G \cup \{\sigma\}$.

$|S| = |G| + 1 \leq [K:K^S]$

↑
by theorem I



Prop. Let K be any field and let G be a finite group of automorphisms of K . Suppose F is the fixed field of G . Then $G = \text{Gal}(K/F)$.

Pf: • Know from theorem II: $[K:F] = |G| = n$.

• Clearly $G \subseteq \text{Gal}(K/F)$. This is because any $\sigma \in G$ fixes every element of F (i.e., $\sigma(a) = a \forall a \in F$); So σ is an F -auto of K . $\therefore \sigma \in \text{Gal}(K/F)$.

$\left. \begin{array}{l} \sigma \in \text{Gal}(K/F), \text{ so } \\ \sigma(a) = a \forall a \in F \\ \Rightarrow a \in K^S \end{array} \right\} \begin{array}{l} a \text{ is fixed by} \\ \text{every thing in } G \end{array}$

Suppose $\sigma \in \text{Gal}(K/F)$, $\sigma \notin G$. Let $S = G \cup \{\sigma\}$.

$|S| = |G| + 1 \leq [K:K^S] \leq [K:F] = n$ This is a contradiction



But now let me prove a corollary to the previous theorem which is actually an important proposition for us. Let K be any field and let G be a finite group of automorphisms of K . So, G is a finite group of automorphisms of K . Let F be the fixed field of, of G . So, these are the elements that are fixed by all the elements of G . Then, G happens to be the Galois group of K over F . So, this is a trivial statement. We will explain this in a minute. So, what we know is that we know from theorem II of the previous video, theorem II about the fixed fields.

Since this has the K colon F is cardinality of G , right? This is exactly say G , say it is denoted by N . If you have a field, theorem II, remember, is exactly this. If you have a field and a distinct set of automorphisms, then the degree of K over the fixed field is exactly N . So, I am denoting by N

the cardinality or order of G and this is equal to that. Now, also, clearly, this is just a straightforward statement, G is contained in the Galois group of K over F .

This is because, what is the Galois group of K over F ? It is all F automorphisms of K . Galois group consists of all F automorphisms of K but any σ in G fixes F , by definition because F is the fixed field, fixes, let me say, every element of F , that is, $\sigma(A) = A$ for all A in F . So, σ is in F automorphism. Simple, right? Galois K over F consists of all F automorphisms of K . G consists of a collection of automorphisms whose fixed field is F .

So, $\sigma(A) = A$ for all A in F which is to say, σ is an F map. This is what I defined way back in the course. You have an extension and F automorphism is something which fixes F pointwise. So, $\sigma(A) = A$ for all A in F means σ is an F automorphism. So, σ is in the Galois group. So, the proof of this inclusion is given here So, G is certainly contained in the Galois group of K over F . We need to show the other inclusions.

So, suppose it is not equal. Suppose σ is in, and let us say σ is not in G . So, suppose this is a strict inclusion. If possible, let it be strict inclusion in which case we can pick a σ which is in the Galois group but not in G . And let S equal G union σ . I have been using the letter S to denote collections of maps which do not form a group. So, G is a group but G union σ is of course not a group because you are just adding one element.

Most of the time it will not be a group, so, let us call it S . Now what we know is that $N + 1$ which is the order of S , cardinality of S , is less than or equal to $[K:F]^{|S|}$. This is by theorem I. If you take any collection of homomorphisms which do not necessarily form a group, then you can apply only theorem 1, which says that degree over fixed field is at least as much as the number of homomorphisms, so in this case $N + 1$.

But $[K:F]^{N+1}$, where is $N+1$? So, maybe I should draw the picture here. So, K is here because σ , so maybe I will squeeze in the argument here, σ is in Galois K over F . So, $\sigma(A) = A$ for all A in F . So, σ that means this implies A is in the fixed field of because A is anyway fixed by everything in G right? So, A is fixed by, by definition because A is in F and F is the fixed field.

But A is also fixed by σ by this statement because σ is in $\text{Gal}(K/F)$. By definition, $\text{Gal}(K/F)$ is all F automorphisms of K , so, σ being in $\text{Gal}(K/F)$; that way. So, that this is a very simple point but this is crucial to the whole theory. σ is in $\text{Gal}(K/F)$. So, σ , and F is the, sorry, σ is in $\text{Gal}(K/F)$, $\text{Gal}(K/F)$ is the collection of F automorphisms of K , so, if A is in F , σ fixes A .

So, A is in F , A is fixed by σ as well as everything in G . So, A is fixed by G everything in G union σ , that means A is in K^G . That means K^G is a sub field of F . So, that means F is contained in K^G . So, this is the tower, K contains K^G , K^G contains F . Once F is contained in K^G , $[K : K^G]$ is greater than or equal to $[K : F]$. So, because this is a product of this times this times this, so, $[K : F]$ is at least as much as $[K : K^G]$.

But, $[K : K^G]$, $[K : F]$ we already know is equal to n . So, this is a contradiction. So, you will see where we will use this theorem later on but this is a contradiction. You have $n + 1$ is strictly or $n + 1$ is greater than or less than equal to n , so that is a contradiction. That means G equals $\text{Gal}(K/F)$, the contradiction is to the fact that there is something in σ that is, there are some σ in $\text{Gal}(K/F)$ that is not in G .

So, that must be the, that must be an equality. The proposition is proved. So, let me write one corollary to this. You may not see why the corollary is important now but as you learn more you will see this is a statement that you will use often. Let K be a field. There cannot be two different groups, let us say, finite groups of automorphisms of K with the same fixed field.

(Refer Slide Time: 11:57)

Definition: Let K/F be a field extension. K/F is called a "Galois extension" if F is the fixed field of $\text{Gal}(K/F)$.

Remark: F is always contained in the fixed field of $\text{Gal}(K/F)$.
Reason: if $\sigma \in \text{Gal}(K/F)$ and $a \in F$, then $\sigma(a) = a$.



Recall: Let K/F be a field extension. Then

$\text{Gal}(K/F) = \{ \text{all } F\text{-automorphisms of } K \}$ → called the GALOIS GROUP of the ext K/F .


Claim: $\text{Gal}(K/F)$ is a group under composition.

Easy to prove: $\begin{cases} 1: K \rightarrow K \text{ identity} \in \text{Gal}(K/F) \checkmark \\ \sigma_1, \sigma_2: K \rightarrow K \text{ } F\text{-auto} \Rightarrow \sigma_1 \sigma_2 \text{ is also an } F\text{-auto } K \rightarrow K \checkmark \\ \sigma^{-1}: K \rightarrow K \text{ is an } F\text{-auto.} \end{cases}$




Prop: Let K be any field and let G be a finite group of automorphisms of K .
Suppose F is the fixed field of G . Then $G = \text{Gal}(K/F)$.



Remark: F is always...
 Reason: if $\sigma \in \text{Gal}(K/F)$ and $a \in F$, then $\sigma(a) = a$
 That means $a \in K$
 Hence $F \subseteq K^{\text{Gal}(K/F)}$ **ALWAYS HOLDS**
 \rightarrow always holds.



Remark: F is always contained in the fixed field of $\text{Gal}(K/F)$.
 Reason: if $\sigma \in \text{Gal}(K/F)$ and $a \in F$, then $\sigma(a) = a$
 That means $a \in K$
 Hence $F \subseteq K^{\text{Gal}(K/F)}$ **ALWAYS HOLDS**
 \rightarrow always holds
 The extension is Galois iff $K^{\text{Gal}(K/F)} = F$.
 This doesn't hold in general!



That is because if you have two different, if you have group G , that group G determines the fixed field in this way. So, they, if you have a group G_1 and G_2 have the same fixed field, G_1 must be equal to the Galois group of K over the fixed field which is G . So, in other words if you have G_1 and G_2 have same fixed field, so, the proof.

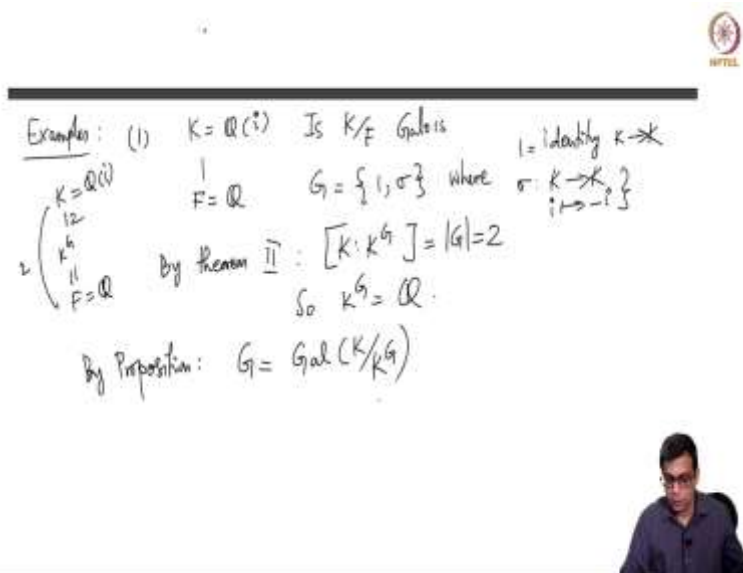
Then G_1 equals Galois group of K over F by the corollary, by the proposition, which is also same as G , G_2 . So, that tells me that there cannot be two different groups which have the same fixed field. So, now let me give you the most important definition of the whole course and then we will do some examples in this video to understand this definition.

So, let K over F be a finite extensions of fields. So, this is the definition of Galois extensions. So, this is the crucial statement for us in the whole course. Let K over B be a finite extension of fields. Then, K over F is called in Galois extension, and Galois extension if F is the fixed field of Galois K over F . This definition will take some and getting use to but let me give a remark and a few examples to, to motivate this definition and give some examples.

So, note that, first note that F is always contained in, this came up in the previous proof, always contained in the fixed field of Galois K over F . Why is this? The reason is if σ belongs to Galois K over F and A belongs to F , then σA is equal to A by definition because σ is an F automorphism of K . Galois K over F consists of things which are automorphisms of K that fix F point-wise. So, σ in Galois K over F and A in F means $\sigma A = A$.

That means A is in the fixed field of this. So, A is fixed by all the Galois group elements. So, A is in the Galois fixed field, so, hence F itself is contained in. So, emphasizing this, this always holds. So, we always have this tower for any given finite extension, so, this always holds. The extension is Galois if the bottom part is inequality. The extension is Galois if the bottom part is an equality. The extension is Galois if K Galois K over F is equal to F .

(Refer Slide Time: 16:10)



Example: (1) $K = \mathbb{Q}(i)$ Is K/F Galois

$F = \mathbb{Q}$ $G = \{1, \sigma\}$ where $\sigma: K \rightarrow K, i \mapsto -i$

$K = \mathbb{Q}(i)$
 \downarrow
 $K^G = \mathbb{Q}$
 \downarrow
 $F = \mathbb{Q}$

By theorem II: $[K:K^G] = |G| = 2$
 So $K^G = \mathbb{Q}$.

By Proposition: $G = \text{Gal}(K/K^G)$



Prop: Let K be any field and let G be a finite group of automorphisms of K .

Suppose F is the fixed field of G . Then $G = \text{Gal}(K/F)$.

Pf: • Know from theorem II: $[K:F] = |G| = n$

Remember the proposition as:
 $G = \text{Gal}(K/F)$

• Clearly $G \subseteq \text{Gal}(K/F)$

∴ this is because any $\sigma \in G$ fixes every element of F (i.e., $\sigma(a) = a \forall a \in F$),
So σ is an F -auto of K .
∴ $\sigma \in \text{Gal}(K/F)$

$\left. \begin{matrix} K \\ | \\ K^G \\ | \\ F \end{matrix} \right\}$

$\sigma \in \text{Gal}(K/F)$, so $\sigma(a) = a \forall a \in F$
∴ a is fixed by any $\sigma \in G$
∴ $a \in K^G$

Suppose $\sigma \in \text{Gal}(K/F)$, $\sigma \notin G$. Let $S = G \cup \{\sigma\}$

$\sigma \notin G$ This is a contradiction



Examples: (1) $K = \mathbb{Q}(i)$ Is K/F Galois

$1 = \text{identity } K \rightarrow K$

$F = \mathbb{Q}$

$G = \{1, \sigma\}$

where $\sigma: K \rightarrow K$
 $i \mapsto -i$

$\left. \begin{matrix} K = \mathbb{Q}(i) \\ | \\ K^G \\ | \\ F = \mathbb{Q} \end{matrix} \right\}$

By theorem II: $[K:K^G] = |G| = 2$

So $K^G = \mathbb{Q}$

By Proposition: $G = \text{Gal}(K/K^G) = \text{Gal}(\mathbb{Q}(i)/\mathbb{Q})$

Hence $\mathbb{Q} = K^G$





This doesn't hold in general.



Examples: (1) $K = \mathbb{Q}(i)$ Is K/F Galois?

$F = \mathbb{Q}$ $G = \{1, \sigma\}$ where $\sigma: K \rightarrow K$ $i \mapsto -i$

By Theorem II: $[K:K^G] = |G| = 2$

So $K^G = \mathbb{Q}$.

By Proposition: $G = \text{Gal}(K/K^G) = \text{Gal}(\mathbb{Q}(i)/\mathbb{Q})$

Hence $\mathbb{Q} = K^G$ Hence $\mathbb{Q}(i)/\mathbb{Q}$ is Galois



$K = \mathbb{Q}(i)$ $F = \mathbb{Q}$ $G = \{1, \sigma\}$ where $\sigma: K \rightarrow K$ $i \mapsto -i$

By Theorem II: $[K:K^G] = |G| = 2$

So $K^G = \mathbb{Q}$.

By Proposition: $G = \text{Gal}(K/K^G) = \text{Gal}(\mathbb{Q}(i)/\mathbb{Q})$

Hence $\mathbb{Q} = K^G$ Hence $\mathbb{Q}(i)/\mathbb{Q}$ is Galois

Can prove this directly also



This may not always happen. This does not always happen. So, Galois extensions are those extensions where there is an equality. Let us say equality holds if K over F is Galois. So, let me quickly do a few examples and then we will stop in this video, So, examples. So, the first example, let us take K equal to \mathbb{Q} adjoined i and F to be \mathbb{Q} is K over F is Galois. So, what is the Galois group? So, in all these cases you have to first find out the Galois group.

So, let us take G to be $1, \sigma$ where 1 is of course the identity map and σ is the map from K to K which sends i to minus i . Remember any automorphisms of K must send i to a conjugate of i meaning another root of $x^2 + 1$ which is the reducible polynomial of i . So, only roots of $x^2 + 1$ are i and minus i . So, σ sends i to $-i$, one sends i to minus i .

Sorry, σ sends I to I , σ sends I to $-I$. Then what is K^G ? So, we have a few statements here. So, using the proposition that I did earlier, K^G , so, without using that let us say what is K^G . K^G is between, K is here, K^G is here, and Q is, F is here. F is Q , this is Q . K^G remember is always going to contain F or actually let me not use that remark. I am just saying that both σ and τ fix every rational number. In fact Q is the prime field.

So, this is something we have. Now, this proposition here, G is a finite group of automorphisms in the, our example, there are two, and F is the fixed field. In this case K^G is the fixed field. So, K , G is equal to Galois group of, okay, so, actually, let me not use that. By theorem II, what is the degree of this? So, this is 2. That means this is inequality, because this whole thing is 2, so, this is already 2.

That means K^G is equal to Q . So, K^G is equal to Q . Now, let us apply the proposition that I proved at the beginning of today's video. So, if you have a field, a finite group of automorphisms, F is a fixed field, then G is the Galois group of, by proposition that I proved today. G is the Galois group of K over K^G . Remember proposition as always proving that, so, remember proposition by this version. Remember this by, as what we have is Galois group.

What do I mean by this? So, G is the Galois group of K over K^G . So, it is a good way to remember this. So, if K is any field G is an arbitrary group of finite (automorph), finite, arbitrary finite group of automorphisms of K and F is the fixed field. So, it is useful to write K^G so that you keep track of that. Then G is Galois group of K over F .

So, that means G is Galois group of K over K^G . In this case, G is Galois group of K over K^G but K^G is Q , so G is the Galois group of K over Q . So, G is the Galois group of Galois group of K over Q and its fixed field is Q . Hence Q is K^G Galois K over Q . This is exactly what Galois extension is. So, again remember this as K over F is Galois if F is equal to the fixed field of Galois group of K over F .

So, remember this as K over F is Galois if F is the fixed field of the Galois group. Remember fixed field is, fixed fields are always represented by K^G that group. So, F is equal to K^G Galois K over F implies K over F is Galois. Here Q is the fixed field of Galois K over Q .

Q. Q equals K power Galois K over Q and hence, you can also directly prove that Galois group of QI or Q is actually just G because there are only two automorphisms, you think about this.

So, you can prove this directly. Directly also by just arguing that any automorphisms must send I to a conjugate of I and there are only two possibilities. But please there is a subtle thing here involved.

(Refer Slide Time: 22:01)

Hence $Q = K$

(2) $K = \mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ Here there is only one automorphism $K \rightarrow K$.
 $\sqrt[3]{2}$ must go to $\sqrt[3]{2}, \omega \sqrt[3]{2}, \omega^2 \sqrt[3]{2}$
 only this is in K
 $\text{So } \text{Gal}(K/F) = \{1\}$. $K^{\text{Gal}(K/F)} = K \neq F$.
 So $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is NOT Galois

That means $a \in K$

Hence $F \subseteq K^{\text{Gal}(K/F)}$ **ALWAYS HOLDS**
 The extension is Galois if $K^{\text{Gal}(K/F)} = F$.
 This doesn't hold in general!

Examples: (1) $K = \mathbb{Q}(i)$ Is K/F Galois
 $F = \mathbb{Q}$ $G = \{1, \sigma\}$ where $\sigma: K \rightarrow K$
 $i \mapsto -i$

So, please carefully think about this and make sure that you understand the every point that I am using. What about $K = \mathbb{Q}$ adjoined cube root of 2? So, here there is only one automorphism.

Because cube root of 2 must go to, cube root of 2, omega cube root of 2 as we discussed this many times, or this, or this, but only this is available in K.

These are not in K. So, the only automorphism is the identity automorphism. So, I am going to go over this fast but this is hopefully clear to you. The Galois group of K over F. So, F is Q. So, K is Q adjoined root 2, Q adjoined cube root of 2, F is Q. Galois group is exactly 1. So, what is the fixed field of the Galois group.

Fixed field of identity element is K and it is not equal to F. So, in this case Q adjoined cube root of 2 or Q is not Galois. So, you see where, this is an example where this is not an equality. In fact, the fixed field happens to be all of K. So, this is not an equality. As we will see more examples later, the fixed field could be something in between these two.

(Refer Slide Time: 23:46)

Handwritten notes on a slide:

- $F = \mathbb{Q}$
- Directly prove: $K^{\text{Gal}(K/F)} = \mathbb{Q} = F$
- Also we can argue like this: by theorem 2
- Theorem 2: $[K:K^G] = |G|$
- $K^{\text{Gal}(K/\mathbb{Q})} = \mathbb{Q}$
- $\Rightarrow K/\mathbb{Q}$ is Galois
- can show
- $\sigma_1 \sigma_2$
- $|\text{Gal}(K/\mathbb{Q})| = 4$



Prop: Let K be any field and let G be a finite group of automorphisms of K .
 Suppose F is the fixed field of G . Then $G = \text{Gal}(K/F)$.
 Pf: • Know from theorem II: $[K:F] = |G| = n$.
 • Clearly $G \subseteq \text{Gal}(K/F)$.
 • This is because any $\sigma \in G$ fixes every element of F (i.e., $\sigma(a) = a \forall a \in F$).
 So σ is an F -auto of K .
 $\therefore \sigma \in \text{Gal}(K/F)$.
 Suppose $\sigma \in \text{Gal}(K/F)$, $\sigma \notin G$. Let $S = G \cup \{\sigma\}$.
 This is a contradiction.

Remember the proposition as:
 $G = \text{Gal}(K/F)$

$\sigma \in \text{Gal}(K/F)$, so $\sigma(a) = a \forall a \in F$.
 $\Rightarrow a \in F$.
 $\Rightarrow a$ is fixed by every $\sigma \in G$.

K
 $|$
 K
 $|$
 F

Another way to prove $\{1, \sigma_1, \sigma_2, \sigma_3\} = \text{Gal}(K/\mathbb{Q})$:
 This $\Rightarrow K^G = \mathbb{Q}$.
 Prop (today) $\Rightarrow G = \text{Gal}(K/K^G) = \text{Gal}(K/\mathbb{Q})$.

K
 $|$
 K^G
 $|$
 \mathbb{Q}

by theorem II

So, one more example I want to give. This is the third example. So, here I take \mathbb{Q} adjoined root 2, I as K and K and F as \mathbb{Q} . So, here one can show, can show this, essentially we have shown this earlier following the notation that I used, so notation that I used in an earlier video where we looked at 4 automorphisms of K .

One is identity automorphism; the other one sends root 2 to root 2 I to minus I. One sends root 2 to minus root 2 I to I; the third one sends root 2 to minus root 2 I to minus I; and the third one is actually equal to the product of sigma 1 and sigma 2. So, here if you think about this, the index of K , I mean you can directly prove.

And we did directly say this, directly prove that K power Galois K over F is actually F . This we have checked by explicitly figuring out which are fixed elements. But also we can argue like this using the theorems that we have proved.

So, we have K . K power Galois K over Q and Q . The cardinality of the Galois group here is 4. So, that is by the theorem II, this is 4, because K colon, so, theorem II can be remembered as K colon K power G is cardinality of G . This is a short way to remember theorem II. K colon K power G is cardinality of G .

So, this is the cardinality of G is 4, so, this is 4 but so, is this. So, this must be 1. So, this implies K power Galois K over Q is Q and hence K over Q is Galois. So, just to complete this circle of ideas, another way to prove G that I defined here, that this is the exactly the Galois group. Again, you can argue this by showing that there is not much choice for I and root 2 but there is another way to prove that this is equality of Galois groups using our results.

So, call this group G . So call this group G , then, and let us look at K power G because Q is the prime field, Q is fixed by G obviously, so, Q is contained in KG . So, we have this tower. By theorem II, this is 4. So, by theorem 2, this is 4 and this is 1. So, theorem II implies KG equals Q but by the proposition that we proved today, K , G equals Galois K over K power G .

Today's proposition implies G equals, G is now this, is Galois K (pow) K over K power G . This means this is Galois K over Q because K power G is Q , so, G is Galois, remember proposition can be remembered like this, G equals Galois K over KG but KG equals Q by (prop) theorem II, so, G is equal to Galois K over Q .

(Refer Slide Time: 28:09)

Theorem 2: $[K:K^G] = |G|$

Another way to prove $\{1, \sigma_1, \sigma_2, \dots, \sigma_{|G|-1}\} = \text{Gal}(K/\mathbb{Q})$:

K
 \downarrow
 \mathbb{Q} $\Rightarrow 1/\mathbb{Q}$

by Theorem 1: $\text{This } \Rightarrow K^G = \mathbb{Q} \checkmark$
 Prop (Today) $\Rightarrow G = \text{Gal}(K/K^G) = \text{Gal}(K/\mathbb{Q})$

4) $K = \mathbb{F}_p$ is a Galois ext. (Will do this later)



$\left[\begin{array}{c} K \\ K^S \\ F \end{array} \right]$ $\sigma(a) = a^4 a^{a^4} \dots$ | any way may $\sigma \in \text{Gal}(K/F)$
 $\Rightarrow a \in K^S$

Suppose $\sigma \in \text{Gal}(K/F)$, $\sigma \notin G$. Let $S = G \cup \{\sigma\}$

$n+1 = |S| \leq [K:K^S] \leq [K:F] = n$ This is a contradiction

\uparrow
 by Theorem 1

Hence $G = \text{Gal}(K/F)$ \square

Cor: Let K be a field. There cannot be two different finite groups of automorphisms of K with the same fixed field.



$$\text{Gal}(\mathbb{F}_p/\mathbb{F}_p) \cong \mathbb{Z}/p\mathbb{Z}$$



Theorem II: Let K be any field, and let $\sigma_1, \dots, \sigma_n: K \rightarrow K$ be ^{distinct} field automorphisms. Suppose that $\{\sigma_1, \dots, \sigma_n\}$ forms a group under composition. If F is the fixed field of $\sigma_1, \dots, \sigma_n$, then $[K:F] = n$. $[K:K^G] = |G|$

Proof: By the first theorem we have $[K:F] \geq n$. We know, in general, it can happen that $[K:F] > n$. But this theorem says that if $\{\sigma_1, \dots, \sigma_n\}$ is a group then $[K:F] = n$.

As we prove this, note where we are using the hypothesis that $\{\sigma_1, \dots, \sigma_n\}$ forms a group.



K
 \uparrow
 K^G
 \uparrow
fixed field

Let K, L be two fields. $\sigma_1, \dots, \sigma_n: K \rightarrow L$ homom.
The fixed field $F := \{a \in K \mid \sigma_1(a) = \dots = \sigma_n(a)\}$. This is a subfield of K . $[K:F] \geq |S|$



Theorem I: Let $\sigma_1, \dots, \sigma_n: K \rightarrow L$ be distinct field homom., and let F be their fixed field. Then $[K:F] \geq n$.

Proof: The proof will use the fact that $\sigma_1, \dots, \sigma_n$ are ind. (as characters of K^\times in L)
 $K = L = \mathbb{Q}(\sqrt{2}, i)$ Recall $\sigma_1, \sigma_2: K \rightarrow K$
 $\sigma_1: i \mapsto i, \sqrt{2} \mapsto \sqrt{2}$
 $\sigma_2: i \mapsto -i, \sqrt{2} \mapsto \sqrt{2}$
Hence $K^{\{\sigma_1, \sigma_2\}} = \mathbb{Q}$
 $\therefore [K:F] = 4 > 3$



$K = \mathbb{Q}(i)$
 $F = \mathbb{Q}$
 $G = \{1, \sigma\}$ where $\sigma: K \rightarrow K, i \mapsto -i$
 By Theorem II: $[K:K^G] = |G| = 2$
 So $K^G = \mathbb{Q}$
 By Proposition: $G = \text{Gal}(K/K^G) = \text{Gal}(\mathbb{Q}(i)/\mathbb{Q})$
 Hence $\mathbb{Q} = K^G$
 Hence $\mathbb{Q}(i)/\mathbb{Q}$ is Galois
 (2) $K = \mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ Here there is only one automorphism $K \rightarrow K$ NOT in K
 $K = \mathbb{Q}(\sqrt[3]{2})$ $\sqrt[3]{2}$ must go to $\sqrt[3]{2}, \omega \sqrt[3]{2}, \omega^2 \sqrt[3]{2}$

So, these are various strands of ideas that we are learning in this course. And now I will not, I will write this one for now but we will discuss this later is the fourth example. If you take the field extension, finite fields \mathbb{F}_P power R over \mathbb{F}_P , so, P is prime of course and R is a positive integer. This is Galois. This is a Galois extension.

So, I want to stop here because we have done enough but we will do this later by, I will, I will start next video with some problems, and in that video we will discuss this in more detail. So, just I wanted to write this however because I want to give examples of Galois extensions and also an example which is something not Galois. So, let me stop this video.

In the last three, four videos, I have thrown a lot of materials at you. So, please carefully follow this and I have sort of indicated how to remember these things in a convenient fashion. So, make sure that you digest all these things carefully. So, theorem II is this. Theorem II remember is the statement that $K \text{ colon } K^G$ is cardinality of G . That is the, how you remember theorem II.

Theorem I is $K \text{ colon } K^S$. So, this is, here S is not a group. So, S is any collection of homomorphisms. So, $K \text{ colon } K^S$ is at least cardinality of S ; $K \text{ colon } K^G$ is cardinality of G . Here, G is a group and then we defined a finite (exten), a finite extension is Galois if F is equal to $K^{\text{Galois } K \text{ over } F}$.

So, using these short forms, we prove various facts here. Please carefully think about all these things because it is important to digest these very well before we proceed to the next concepts.

Let me stop this video, in the next video will do some problems to make sure that we understand all these concepts. Thank you.