

**Introduction to Galois Theory**  
**Professor. Krishna Hanumanthu**  
**Department of Mathematics**  
**Chennai Mathematical Institute**  
**Lecture No. 09**  
**Problem Session 2**

Welcome back. In the last video I did a few problems. So, today we will continue this problem session and I want to do a couple of very important exercises in field theory that will be constantly used in the later part of this course on Galva Theory.

(Refer Slide Time: 00:30)

4) Let  $F$  be a field; let  $K, L$  be two extension fields of  $F$ .  
 Suppose  $\alpha \in K$  is alg/ $F$ . Let  $\sigma: K \rightarrow L$  be an  $F$ -homom of fields.

$$\begin{array}{ccc} \alpha \in K & \xrightarrow{\sigma} & L \\ & \searrow & \\ & & F \end{array}$$

Then show that

- $\sigma(\alpha) \in L$  is alg/ $F$ , and
- the irr poly of  $\sigma(\alpha)$  over  $F$  is the same as the irr poly  $\alpha$  over  $F$ .

Solu.



So, the first one is a fairly simple statement that you may have seen in you, you would have seen in any field theory course. So, let me just recall this. Let  $F$  be a field and let  $K$  and  $L$  be two extensions of, extension fields of  $L$  of  $F$ . So, suppose  $\alpha$  in  $K$  is algebraic over  $F$ . Let  $\sigma$  from  $K$  to  $L$  be a, be an  $F$  homomorphism of fields. So, the situation is this. So, you have  $K$  and  $L$  are two extensions of  $F$ ,  $\alpha$  is in  $K$ . It is algebraic over  $F$ . I am not saying  $K$  is algebraic over  $F$  because that is not required for this. I am only going to use the fact that this particular element  $\alpha$  is algebraic over  $F$  and  $\sigma$  is a  $F$  homomorphism.

Every time I draw a picture like this, it is understood that  $\sigma$  is an  $F$  homomorphism. So, then show that 2 things;  $\sigma(\alpha)$  which is in  $L$  is algebraic over  $F$  and the irreducibility it is algebraic, so we can talk about irreducible polynomial of  $\sigma(\alpha)$  over  $F$  over  $\sigma(\alpha)$  over  $F$  is the same as irreducible polynomial  $\alpha$  over  $F$ . So, as I said, this is a very, very

standard result and it is very easy to prove this. But I thought I will mention this because it comes up in the next problem which will be of much more importance for us. So, this is clear. In fact, we will do second part first and then everything will follow.

(Refer Slide Time: 02:25)

The slide contains handwritten mathematical text and equations. At the top, it says "The ... root irr poly  $\alpha$  over  $F$ ." Below that, it says "Soln: Let  $f \in F[x]$  be the irr poly of  $\alpha$  over  $F$ ; let  $\sigma(\alpha) = \beta \in L$ . We will show  $f(\beta) = 0$ . Then the problem is solved." The polynomial is given as  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ , where  $a_i \in F$ . The evaluation at  $\beta$  is shown as  $f(\beta) = a_n \beta^n + a_{n-1} \beta^{n-1} + \dots + a_1 \beta + a_0 = a_n \sigma(\alpha)^n + a_{n-1} \sigma(\alpha)^{n-1} + \dots + a_1 \sigma(\alpha) + a_0 = \sigma(a_n \alpha^n + a_{n-1} \alpha^{n-1} + \dots + a_1 \alpha + a_0) = \sigma(0) = 0$ . A box highlights the "IMP POINT:  $\sigma(a_i) = a_i \forall i$ , Since  $\sigma$  is an  $F$ -homomorphism". A note on the left says  $\sigma(\alpha) = \beta$  and  $\sigma(\alpha^2) = \beta^2$ . The lecturer's video feed is visible at the bottom right.

So, let us say  $F$  is the irreducible polynomial of  $\alpha$  over  $F$  so this is the situation. So, I claim that and let  $\sigma$  of  $\alpha$  be  $\beta$ . So, for simplicity I want to call that  $\beta$ . So, we, we will show then the problem is solved because it will obviously prove that this is algebraic because  $\beta$  is the root of a polynomial over capital  $F$  and  $F$  is irreducible, so it must be irreducible polynomial. So, this is the that is all there is to it.

So, let us say  $f(x)$  equals  $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ . So, here remember,  $a_i$  is in capital  $F$  because this is a polynomial over capital  $F$ . Now what is  $f(\beta)$ ?  $f(\beta)$  is  $a_n \beta^n + a_{n-1} \beta^{n-1} + \dots + a_1 \beta + a_0$ . But this by using the fact that  $\beta = \sigma(\alpha)$ . Remember if  $\sigma(\alpha) = \beta$ ,  $\sigma(\alpha^2) = \sigma(\alpha)^2$ . So, that is  $\beta^2$ . So, that is  $\sigma(\alpha^2)$ . So, that is what I am going to use but this is actually because so now the other important thing. So, this is the important point. Important point is  $\sigma(a_i) = a_i$  for all  $i$  since  $\sigma$  is an  $F$  homomorphism. So, this whole thing will not be true if  $\sigma$  is not an  $F$  homomorphism. So, I am going to crucially use that fact.

So, that allows me to write this as  $\sigma(a_n \alpha^n + a_{n-1} \alpha^{n-1} + \dots + a_1 \alpha + a_0)$ . So, I will skip some of these things. I am not changing anything here because  $\sigma(a_n) = a_n$ , so that I am allowed to do. So, now

using the fact that sigma is an homomorphism, I can pull sigma out all the way. So, that means sigma of an alpha n plus dot, dot, dot, a1 alpha plus a0. But that is 0. So, this part is because right, so that is just F alpha. So, F alpha is 0 because F is irreducible polynomial of alpha over F. So, that means F beta is 0 and we are done. So, that is the proof that if you have a field homomorphism an element can go to a field homomorphism over a Bases field. An element can go to other roots of its irreducible polynomial.

(Refer Slide Time: 05:50)

$\sigma(a_i) = a_i + t_i$ , since  $\sigma$  is an  $F$ -homomorphism  
 $f(\alpha) = 0 \implies \sigma(0) = 0$   
 This is a very easy, but very important, restriction on the images of an alg element under an  $F$ -iso.



So, this is an extremely important. This is a very easy but very important restriction on the images of, of an algebraic element under a  $F$  isomorphism. So, just illustrate this.

(Refer Slide Time: 06:23)

$$\begin{array}{c}
 K = \mathbb{Q}(\sqrt{2}) \rightarrow L = \mathbb{C} \\
 \downarrow \\
 F = \mathbb{Q}
 \end{array}
 \quad
 \begin{array}{c}
 X^2 - 2 \\
 \swarrow \quad \searrow \\
 \sqrt{2} \quad -\sqrt{2}
 \end{array}
 \quad
 \left| \quad \begin{array}{l}
 \sigma(\sqrt{2}) \text{ MUST be either} \\
 \underline{\underline{\sqrt{2}}} \text{ or } \underline{\underline{-\sqrt{2}}}.
 \end{array}
 \right.$$

$f = X^3 + 2X^2 + 1$      $\alpha \in \mathbb{C}$  is a root of  $f$



$$\begin{array}{c}
 F = \mathbb{Q} \\
 \downarrow \\
 X^2 - 2 \\
 \swarrow \quad \searrow \\
 \sqrt{2} \quad -\sqrt{2}
 \end{array}
 \quad
 \left| \quad \underline{\underline{\sqrt{2}}} \text{ or } \underline{\underline{-\sqrt{2}}}.
 \right.$$

$f = X^3 + 2X^2 + 1$      $\alpha \in \mathbb{C}$  is a root of  $f$   
 $\sigma: K \rightarrow \mathbb{C}$      $\sigma(\alpha)$  must be one of the 3 roots of  $f$ .




So, if you have very quickly I will do this,  $\mathbb{Q}(\sqrt{2})$  over  $\mathbb{Q}$  and you, you consider this. So, in our situation I will take this to be  $K$ . I will take this to be  $L$  and I will take this to be  $F$ . So, this is the situation.  $K, L$  are any extensions and I am thinking of this as a  $\mathbb{Q}$  homomorphism. So, this so we, we know that  $\sigma(\sqrt{2})$  must be either  $\sqrt{2}$  or  $-\sqrt{2}$ . So, because irreducible polynomial of  $\sqrt{2}$  is  $X^2 - 2$ , which has only 2 roots. So, this is the simplest example where you can see that  $\sqrt{2}$  cannot go to anything else.

This you can directly prove of course but this general statement here allows you to conceptually visualize this. So, this tells me that  $\sqrt{2}$  can go to other roots of its irreducible polynomial

which of which there are only 2, so root 2 or minus root 2. And now you can apply this problem to any situation. You can take, so if alpha is the root of this, I am just randomly writing an example. So, and sigma alpha where sigma is some K to C, alpha is here, must be 1 of the 3 roots. This is a very powerful restriction, as I said for algebraic elements.

(Refer Slide Time: 08:07)

5) Let  $K/F$  be an algebraic ext; let  $\sigma: K \rightarrow K$  be an  $F$ -homon. 

Then  $\sigma$  is an isomorphism.  $\sigma: K \rightarrow K$   
 $\downarrow$   
 $\alpha$

Soln: Already we have:

- $\sigma$  is an  $F$ -homon ✓
- $\sigma$  is injective ✓

only remains to check:  $\sigma$  is surjective.

---

Let  $\alpha \in K$ .



And one immediate application of this I will do and this is going to be very important statement for us is the following. Let  $K$  over  $F$  and I wanted to also I mean, after this I will write one more exercise and that is we will stop the video after that. So, let  $K$  over  $F$  be an algebraic extension. Now I am taking an algebraic extension. Let sigma from  $K$  to  $K$  itself, it is very important that I have  $K$  to  $K$  here be an  $F$  homomorphism, then sigma is in fact an isomorphism. I want to prove this, solution. So, remember it is an  $F$  homomorphism. It takes  $K$  to  $K$  already we have sigma is an  $F$  homomorphism.

So, of course sigma is an  $F$  isomorphism is a statement that is an  $F$  homomorphism is given. It is injective is given. So, only remains to check sigma is surjective because it, it takes  $K$  to  $K$ . It is homomorphism, it is injective. Only missing point for a homo isomorphism of fields is surjectivity. So, let us take an arbitrary element and show that it is in the image. So, let alpha be in  $K$ . So, you have alpha here.

(Refer Slide Time: 09:55)



Let  $\alpha \in K$ . Let  $f \in F[X]$  be the irr poly of  $\alpha/F$ .  
Let  $\{\alpha = \alpha_1, \alpha_2, \dots, \alpha_n\}$  be the set of all roots of  $f$   
in  $K$ .  
 $\underbrace{\hspace{10em}}_A$   
claim:  $f(\alpha_i) = \alpha_j \quad \forall i=1, \dots, n$ . ✓  
Follow from the previous problem.



So, let us now consider the irreducible polynomial of  $\alpha$  over  $F$ . Recall that  $K$  over  $F$  is an algebraic extension, so every element of  $K$  is algebraic over  $F$ . So, I can ask for its irreducible polynomial. Let  $f$  be the irreducible polynomial of  $\alpha$  over  $F$ . Let  $\alpha = \alpha_1, \alpha_2, \dots, \alpha_n$  be the set of all roots of  $f$  in  $K$ . Note that  $f$  may not split in  $K$  we are not given any such assumption. All we know is that  $K$  over  $F$  is an algebraic extension. So, it will have some roots, may not be all root of  $f$  in an arbitrary splitting field. But I do not care about that. I will take all the roots.


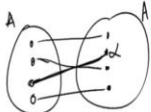
We know there is 1 root at least because  $\alpha$  is there. Let us take all the roots, it is a finite set that much we know because  $f$  is a specific polynomial. Its roots will be finitely many. So, let us call this set  $A$ . So,  $A$  is the set of roots of  $f$  in  $K$ . Now I claim that  $f(\alpha_i) = \alpha_j$  for all  $i$ . This is by the previous exercise. That is the point. So, image of  $\alpha_i$  must be another root of the irreducible polynomial namely  $f$ . But the only roots of the irreducible polynomial are these. So, this is immediate consequence of the previous exercise.

(Refer Slide Time: 11:43)

So we can restrict  $f$  to  $A$ :  $f|_A: A \rightarrow A$

Now look at  $f|_A: A \rightarrow A$ . It is injective because  $f$  is. But  $f|_A$  is an injective map from a finite set to itself. So  $f|_A$  must be surjective.

That means:  $\exists \alpha_i \in A$  s.t.  $f(\alpha_i) = \alpha_i = \alpha$ .  
So  $\alpha \in f(K) \Rightarrow f$  is onto (=surjective)  $\square$



So, now that means so we can restrict  $f$  to  $A$ . So,  $f|_A$  remember is a function from  $K$  to  $K$ .  $A$  is a small subset here,  $K$  is an infinite field potentially so,  $A$  is a finite set. In general  $f$  of  $A$  could be some other set in  $K$ , but we just showed that this implies basically that  $f$  of  $A$  is contained in  $A$  because you take an element of  $A$ , apply  $f$  to it, you land again in  $A$ . So,  $f$  can be restricted to  $A$  to  $A$ , a map from  $A$  to  $A$ . Now look at  $f|_A$  I will call the restriction also  $f$  or  $f|_A$ . So, it is a restriction of  $f$  to only  $A$ . It is injective because  $f$  is. So,  $f|_A$  is a security injection. So, 2 distinct elements in capital  $K$  go to 2 distinct elements in capital  $K$ , so 2 distinct elements in capital  $A$  obviously go to 2 distinct elements in capital  $A$ .

But  $f|_A$  is an injective map from a finite set to itself. So,  $f|_A$  must be surjective. So, this is a trivial statement, so you have finite set with 4 elements and you are considering maps on that element that set to itself but you also know that it is injective so this goes to this, maybe this goes to this, this goes to this, this goes to this. So, there is no way that it fails to be surjective. So, it has to be surjective. That is, there exists  $\alpha_i \in A$  such that  $f(\alpha_i) = \alpha_i = \alpha$  because  $\alpha$  is 1 of them? So, maybe  $\alpha$  is this. So, this must map to  $\alpha$ . So,  $\alpha$  is in the image of  $K$  itself. So, that means  $f$  is onto.

So, onto remember equal surjective, surjective is a synonym for onto. So, that means  $f$  is an onto function which is exactly what we needed to prove. So, this completes the solution. So, this is going to be a very, very important statement for us, namely that if you have an algebraic

extension and you are looking at maps from  $K$  to  $K$  this is very important for us. Then it is an isomorphism. So, if  $K$ , this  $K$  is different from this  $K$ , then we cannot say any statement like this.

(Refer Slide Time: 14:50)

The diagram shows a field extension  $\mathbb{Q}(\sqrt[3]{2}, \omega) = K$  over  $\mathbb{Q}$ , where  $\omega$  is a primitive 3rd root of unity. A map  $\sigma: K \rightarrow L$  is defined, where  $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$ . The map  $\sigma$  sends  $\sqrt[3]{2}$  to  $\sqrt[3]{2}\omega$ . A note indicates that  $\sigma$  is not surjective. The diagram also shows  $K = \mathbb{Q}(\sqrt[3]{2})$  and  $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$ .



So, that is the statement I want to show that if you know that you have an algebraic extension and a homomorphism from it to itself then it must be an isomorphism. So, for example if you take  $\mathbb{Q}$ , cube root of 2, zeta 3 or omega as it is called. So, this is the splitting field of over  $\mathbb{Q}$ . So, this is  $K$ . So, any map you take it must be an isomorphism. But if you take to  $\mathbb{C}$ , so let me not get into this. So, this is all I am saying. So, on the other hand if you take  $\mathbb{Q}$  adjoined cube root of 2, you can take cube root of 2 times omega. So, omega is the primitive third root of unity, that must be an isomorphism. So, cube root of 2 times omega that is another root of the irreducible polynomial of cube root of 2.

So, this is a valid map. So, here  $K$  is this and  $L$  is this. So, it is an isomorphism but it is from  $K$  to  $L$ . So, I may have confused you a little bit but I just want to emphasize that you can have different fields. So, for example yeah, so maybe I could have just taken  $\mathbb{C}$  here. So, then I will send cube root of 2 to cube root of 2 omega. So, it is an algebraic extension but it is so or I can take some big fields so  $K$  adjoined cube root of  $K$  adjoined om cube root of 2 omega comma omega,  $\mathbb{Q}$  adjoined cube root of 2 comma omega. So, here  $L$  is algebraic over  $\mathbb{Q}$ ,  $K$  is algebraic over  $\mathbb{Q}$  but this is not an isomorphism, is not surjective rather so  $L$  is not  $K$ . So, that is why it fails.




So, here it is very important that I have same field, so same field. Then you have a surjective map otherwise you have an isomorphism but onto something smaller than L potentially. So, that is all I am emphasizing here. So, now let me just give some terminology and stop this video.


(Refer Slide Time: 17:39)

$\alpha \in K$   
 $|$   
 $F$

$\alpha$  is alg/F;  $f = \text{irr poly of } \alpha \text{ over } F$   
 Roots of  $f$  are called "conjugates of  $\alpha$ "  
 There are only finitely many conjugates for an alg elt.


6) Let  $F$  be a field. The "prime field" of  $F$  is defined as:  
 $\mathbb{Z} \xrightarrow{\varphi} F$  unique ring homom; let  $I = \ker \varphi$ .  
 We know:  $I = (0) \Rightarrow \mathbb{Q} \subseteq F$   
 $I = p\mathbb{Z} \Rightarrow \mathbb{Z}/p\mathbb{Z} \subseteq F$   
 $p$  prime






There are only finitely many conjugates...

6) Let  $F$  be a field. The "prime field" of  $F$  is defined as:  
 $\mathbb{Z} \xrightarrow{\varphi} F$  unique ring homom; let  $I = \ker \varphi$ .  
 We know:  $I = (0) \Rightarrow \mathbb{Q} \subseteq F$  : prime field of  $F = \mathbb{Q}$   
 $I = p\mathbb{Z} \Rightarrow \mathbb{Z}/p\mathbb{Z} \subseteq F$  : prime field of  $F = \mathbb{Z}/p\mathbb{Z}$   
 $p$  prime






So, if you have an element so  $K$  over  $F$  is an algebraic extension rather field extension,  $\alpha$  is algebraic over  $F$ . And let us say  $f$  is the irreducible polynomial of  $\alpha$  over  $F$ , roots of  $f$  are called conjugates of  $\alpha$ . So, this is the terminology, conjugates of  $\alpha$  are the roots of its irreducible polynomial. So,  $\alpha$  is a conjugate of itself and other roots are called conjugate other conjugates of  $\alpha$ . So, the problem here, fourth problem here says that image of an

algebraic element must be a conjugate of that element. So, conjugates are they are only finitely many conjugates and they are the only possible images under a field of  $F$  homomorphism, finitely many conjugates for an algebraic element.

So, let me just write one more exercise because I meant to do this or I would I would not give you the details now because I am running out of time. So, I just want to give you a quick stare argue I mean, very sketchy argument and ask you to finish it. So, let  $F$  be a field. The prime field of  $F$  is defined as follows. So, you consider the unique ring homomorphism from  $\mathbb{Z}$  to  $F$ . There is always a unique ring homomorphism from  $\mathbb{Z}$  to any field or any ring in fact commutative ring with over unity so, take that.

Let  $i$  be the kernel of fine so we know  $i \neq 0$  in which case  $\mathbb{Q}$  is contained in  $F$  because  $\mathbb{Z}$  is then a sub ring of  $F$ .  $F$  is a field so  $\mathbb{Z}$  will con and  $\mathbb{Z}$  is contained in it so all ratios of integers will be contained in it, so  $\mathbb{Q}$  is in  $F$ . Otherwise  $i$  is  $p\mathbb{Z}$ ,  $p$  prime in which case  $\mathbb{Z}/p\mathbb{Z}$  is contained in  $F$ . So, any field will continue the  $\mathbb{Q}$  for  $\mathbb{Z}/p\mathbb{Z}$  for a prime  $p$ . So, the prime field of  $F$  here is  $\mathbb{Q}$  in this case and prime field of  $F$  is  $\mathbb{Z}/p\mathbb{Z}$ . So, as you can easily see this is all easy or not yet writing the exercise.

(Refer Slide Time: 20:42)



So:  $\text{char } F = 0 \Rightarrow$  prime field of  $F = \mathbb{Q}$   
 $\text{char } F = p \Rightarrow$  "  $F = \mathbb{Z}/p\mathbb{Z}$

Let  $K$  and  $L$  be two fields of same char and let  $F$  be their prime field. Let  $\sigma: K \rightarrow L$  be a field homom.

Then  $\sigma$  is an  $F$ -homom.

ALL FIELDS of CHAR 0

$\mathbb{Q}$

FIELDS of CHAR 2

$\mathbb{Z}/2\mathbb{Z}$

ALL FIELDS of CHAR p


$\mathbb{Z}/p\mathbb{Z}$

$K \xrightarrow{\sigma} L$

$\sigma(a) = a$

$\forall a \in F$

**exercise** use  $\sigma(1) = 1$



So, basically what I am saying is that characteristic of  $F$  is 0 implies prime field of  $F$  is  $\mathbb{Q}$  if characteristic of  $F$  is  $P$  prime field of  $F$  is  $\mathbb{Z}/p\mathbb{Z}$ . So, now let  $K$  and  $L$  be 2 fields of same characteristic and let  $F$  be their prime field. So, remember prime field is think of it as the base for

any field. So, every field of characteristic 0 sits above  $\mathbb{Q}$ . So,  $\mathbb{Q}$  is all the way down, all fields of characteristic 0 are above  $\mathbb{Q}$ . Similarly if  $F$  is a field of characteristic 2, it lives above  $\mathbb{Z}/2\mathbb{Z}$  and all fields of characteristic 2 live above  $\mathbb{Z}/2\mathbb{Z}$ . So, basically what we have is that, all fields lie above this. Similarly, all fields, similarly  $\mathbb{Z}/p\mathbb{Z}$  for all primes.

So, now you if take 2 fields in any box here that is what I am taking,  $K$  and  $L$  are here or here or here. So, and then take  $\sigma$  be a field homomorphism, then  $\sigma$  is in fact an  $F$  homomorphism. So, any field homomorphisms, so if  $F$  and  $L$   $K$  and  $L$  are 2 fields which have the same characteristics characteristic and  $F$  is a prime field so if  $F$  is in the  $\mathbb{Q}$  or  $\mathbb{Z}/p\mathbb{Z}$ . Any  $\sigma$  fixes every element in  $F$ . So, this is a very easy exercise. We briefly mentioned this 1 characteristic is 0 but the same idea carries over in general. So, this is an exercise for you. I would not do this but the point is 1 must go to 1. So, use once 1 goes to 1,  $\sigma(2)$  is 2,  $\sigma(-1)$  is  $-\sigma(1)$  is  $-1$  and so on. And generalize that to show that it fixes the prime field.

So, this is the, these are a few exercises that I wanted to do in detail for you so that you are more comfortable with the concepts that I recalled. So far in the course we have really done nothing more than recalling and next video we are going to start our study of Galva Theory. Thank you.