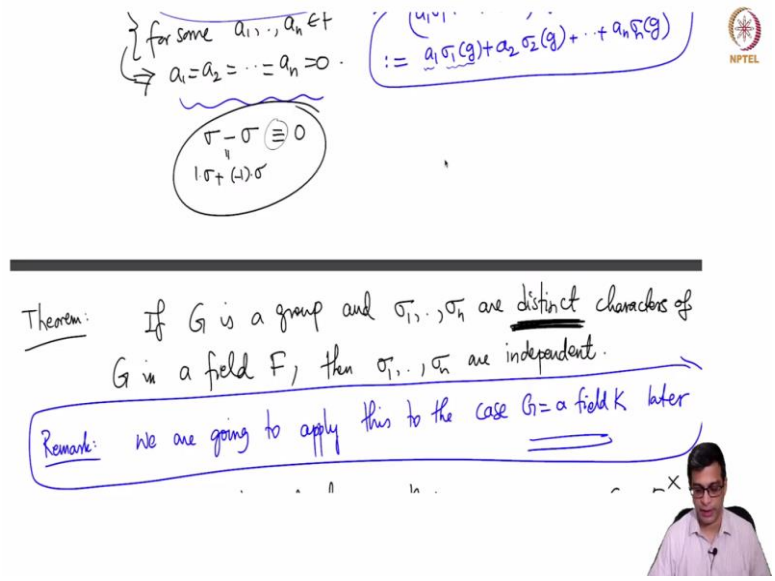
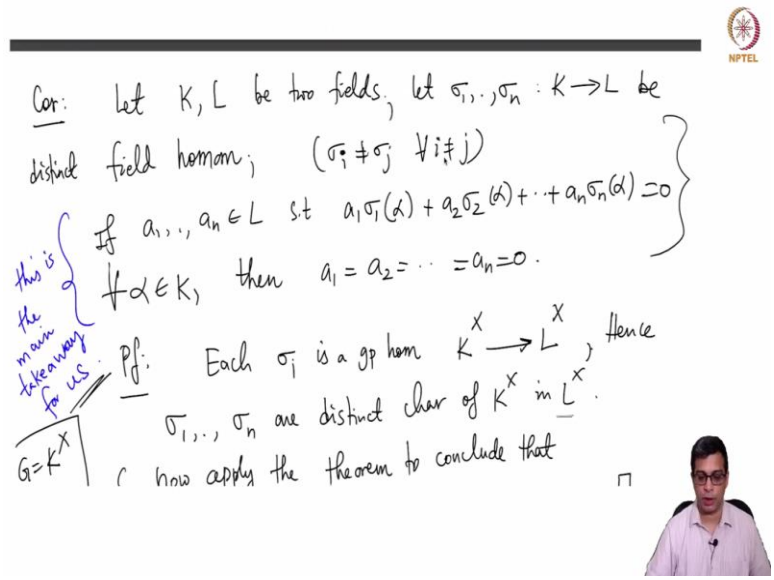
Introduction to Galois Theory
Professor. Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute
Lecture No. 11
Fixed Fields

Welcome back, in the last video, we started Galois theory after revising earlier parts of Group theory, Ring theory and Field theory. And in the last video, I talked about Group Characters and I told you that those are not important in their own right for us, but mainly when we are interested in field homomorphism's.

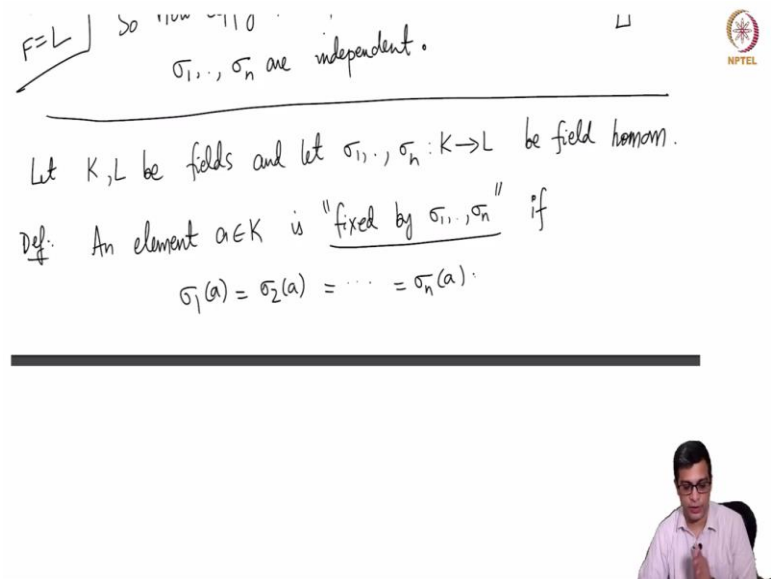
(Refer Slide Time: 00:40)





So, in particular, I wanted you to understand this theorem I proved that if you have a group and a collection of distinct characters in a field F then they are independent. And I also remarked that the main application of this is going to be when we talk about homomorphism's between 2 fields. So, I want to continue this and tell you why we are going to study these characters this way, and when we are going to apply this theorem, so, the theorem is very important for us you will see in the next few videos where the theorem will come in handy for us.

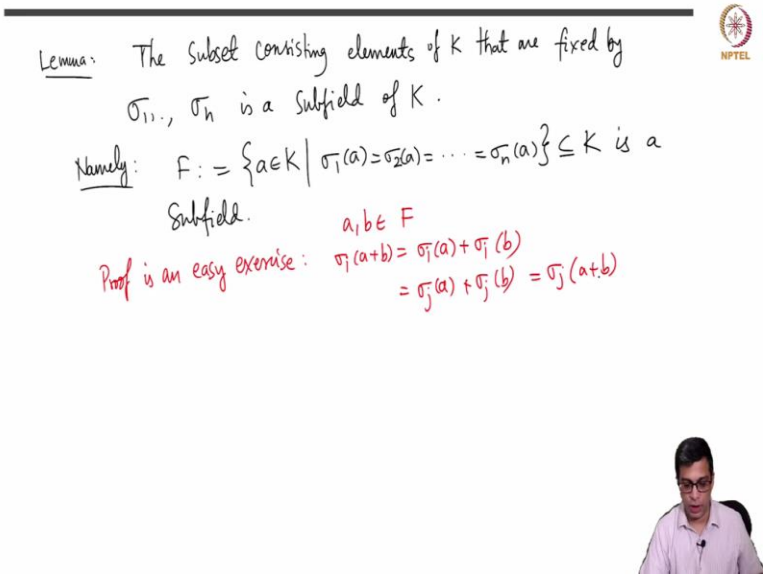
(Refer Slide Time: 01:11)



So, let me set up like that as follows let K and L be 2 fields and let us take a collection of some finitely many field homomorphism's. So, let sigma 1 to sigma n be field homomorphism's. So,

we are going to say that an element so, these are definition an important definition for us an element a and K remember it sigma is a function from K to L. So, an element a and K is fixed by these given, given collection of homomorphism's we say that it is fixed by them, if sigma 1 of a equals sigma 2 of a equals sigma 3 of a and all the way up to sigma n of a. That means, the image of under all of these is equal is the same.

(Refer Slide Time: 02:16)



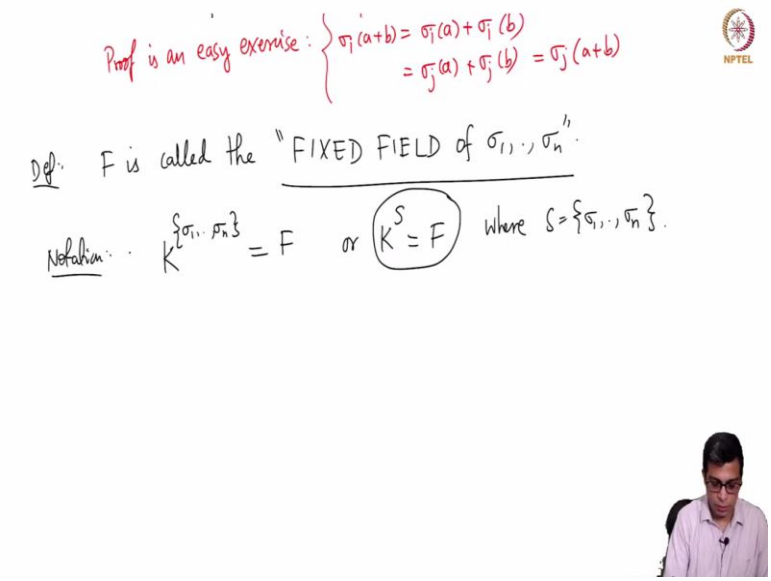
So, this and moreover in this simple lemma, so, you take the collection of all elements fixed by them, that forms a subfield of the subset consisting of a subfield of K, the subset consisting of elements, elements of K that are fixed by sigma 1 to sigma n is field, is a subfield of, of K, namely more precisely. So, let us take F to be the set of all elements in K which are the property that sigma 1 of a equals sigma 2 of a equals sigma 3 of a, and so on all the way up to sigma n of a is a subfield and the proof is an easy exercise for you.

I would not say much more than the following. So, if you have 2 elements in the set F, how do you verify that F is a field, if you give if you are given 2 elements, you want to show that product is there, there some is there, if something is there, its inverse is their identity element is there for both addition and multiplication. So all those are easy. So basically, you take 2 elements, I will just do one of them and you can do the others.

What is sigma 1 of a plus b? That is because sigma 1 is a homomorphism that is same as sigma 1 of a plus sigma 1 of b, but this is true for any i in fact, sigma i of a plus b is equal to sigma of a

plus sigma of b, but then because a and b are in the fixed set sigma i have a is same as sigma j of a sigma of i of b and sigma j of b, which is same as sigma j of a plus b.

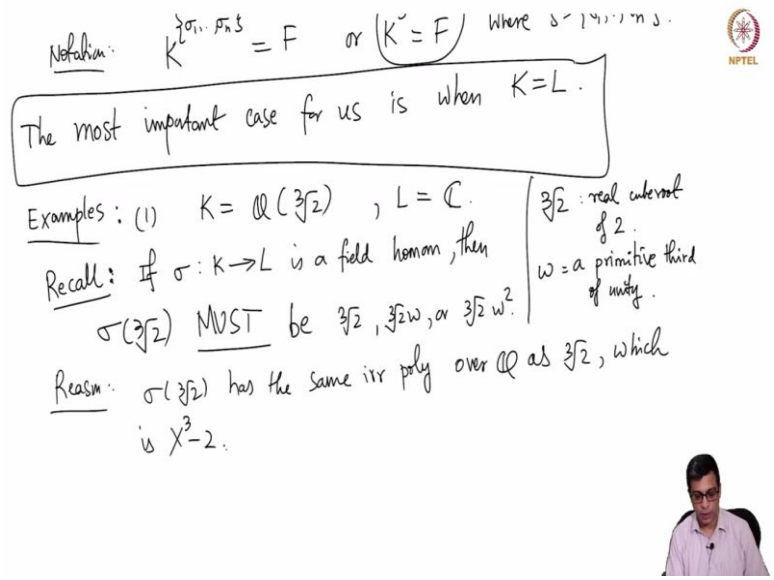
(Refer Slide Time: 04:24)



So, this you use this idea to show that F is a subfield. And the important definition for us is F is called the Fixed Field of sigma 1 to sigma n. So, if you are given any collection of any collection of homomorphism's from the Fixed Field is the collection of elements which have the same image under all of the given homomorphism's and notation instead writing fixed field of this we write K power this. So, fixed field is K power that set or K power S which is more convenient, where S is the set.

So, these are the notations we follow. So now, this really makes sense if you have at least 2 elements, because if you have only 1 element, there is no condition, so, sigma 1 of a, so if you have a single homomorphism if n equal to 1 the fixed field is K itself. So, this is called a fixed field. And the most important so, I am going to do a few examples now. And before that I let me just say that the most important case in which we will study this is when K equal to L.

(Refer Slide Time: 05:54)



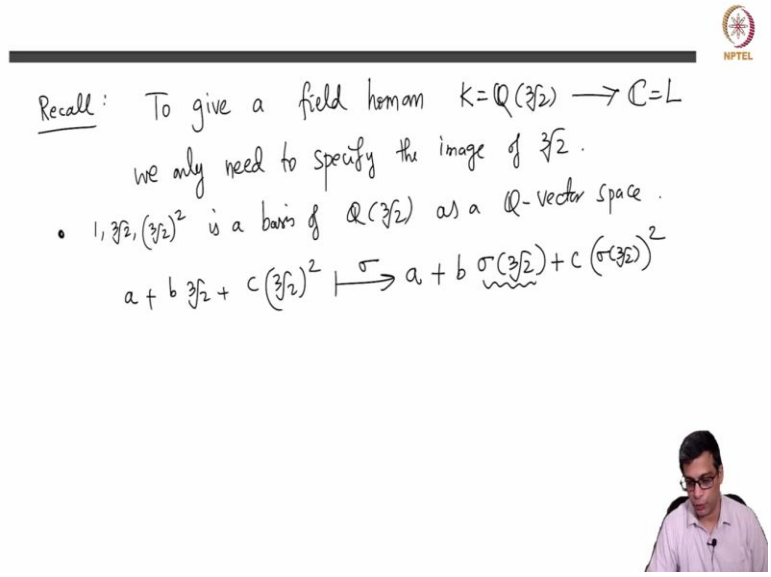
So, the most important case for us and I will do one example, where it is not in this case, but after that everything we do will be in this case, most important case for us is when case K equal to L. And in other words, we are looking at almost homomorphism's from K to K. So, that is the most important case for us. So, let me just highlight this. And when we come to examples, and when we look at this special case, you will also see why we use the word fixed.

So, let me start with a few examples. I am going to, I am going to introduce these examples to you. And then we will come back to these examples repeatedly in the upcoming videos. So, let me first take this field Q adjoint cube root of 2 and L to be the complex numbers. So, here what we have is, cube root of 2 is of course, always when I write like this, I mean, for real cube root of 2 rather to our complex, and other 2 are given by omega times cube root of 2 and omega square times cube root of 2 omega for us represent a primitive third root of unity.

So, now what are homomorphism's from K to L. So, the most important thing that I did in an earlier video, most important feature of Field homomorphism's that I will recall now, is that if sigma is a Field homomorphism's from K to L, then sigma of cube root of 2 must be either cube root of 2 hard cube root of 2 omega or cube root of 2 omega square. And the reason for this is sigma cube root of 2 has the same irreducible polynomial over Q has cube root of 2 which is remember the Q cube root of 2 has irreducible polynomial x cube minus 2.

So, image of cube root of 2 under any field homomorphism's because any field homomorphism's a must fix Q that is the underlying property that we are using. So, image of cube root of 2 must be another root of cube x cube minus 2 and we know that there are only 3 roots, cube root of 2, cube root of time 2 times omega, cube root of 2 times omega square. So, choosing each one we get 3 homomorphism's.

(Refer Slide Time: 08:57)

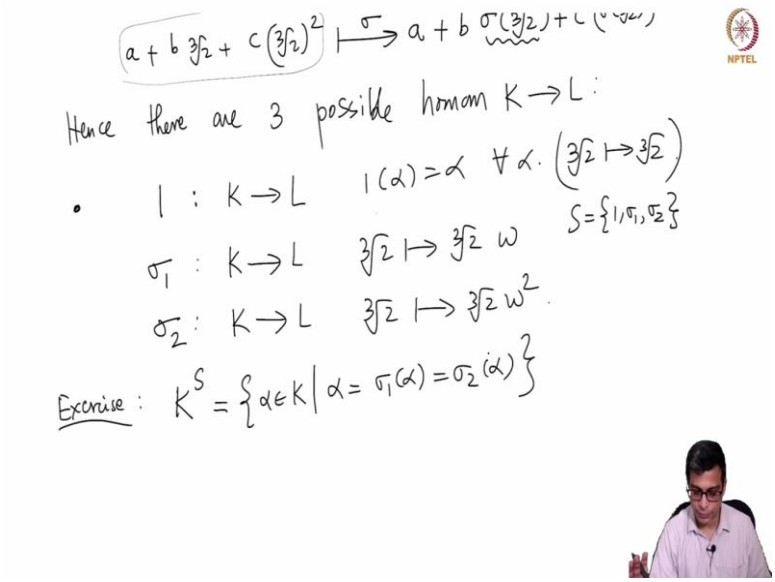


Another important feature which I want to recall in this example, but, we are going to use all these things repeatedly in all the future examples and future videos. But in the first example, I wanted to spell it out in more detail. So, to give a field homomorphism from K which is cube root of Q or adjoint cube root of 2 to see which is L we only need to specify the image of see once you specify the cube root image of cube root of 2, then the fact that it is a field a homomorphism's determines every other image.

This is because 1 comma cube root of 2 comma cube root of 2 square is a basis of Q adjoint cube root of 2 has a Q vector space. So, I am giving you the reasons. So, any element of Q adjoint cube root of 2 can be written as a rational number plus another rational number times cube root of 2, plus another number times cube root of 2 whole square. Now the rational number must vote itself. So, if you have a plus b cube root of 2, plus c cube root of 2 whole square, where can it go under sigma?

a has to go to a because any field homomorphism's of an extension of Q must fix Q, b cube root of 2 must go to b times cube root of 2, because sigma of b times 2 root of 2 sigma b times sigma cube root of 2, but sigma b is b. So, this is the case. And finally, the last time we will go to sigma of cube root of 2 whole square because of field homomorphism property. So, that means only choice is to is to determine the image of cube root of 2. And as I recall earlier, can only possibilities for the image of root of 2 or these 3.

(Refer Slide Time: 11:13)

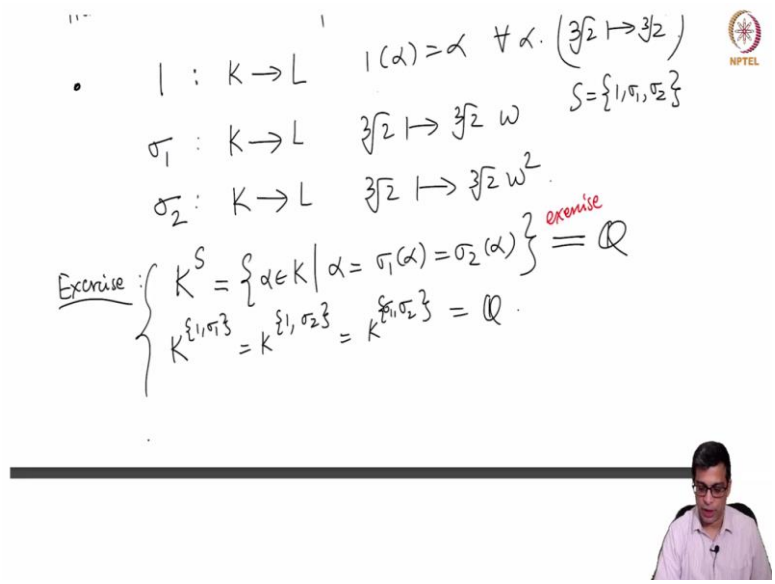


So we have only 3, 3 possible homomorphism's, from K to L. And they are 1 I will denote it by 1, though it is a bit confusing, but 1 of any element is itself. So basically, I send cube root of 2 to cube root of 2. So remember, the image of cube root of 2 determines the homomorphism. And in this first one, I send it to itself. I call it 1. Second one, I will call it sigma 1 and here I sent cube root of 2 to cube root of 2 omega, that is another possibility and sigma 2 will be cube root of 2 going to the third possibility.

So, now, I will leave this mainly I mean mostly as an exercise for you. If you take so, let us denote S by these 3 elements. S is the 3 elements at 1 sigma, sigma 1, sigma 2, Ks is actually Q, if you take an element of K that is fixed by all of them, that is fixed by s meaning it must so maybe I will just spell it out once it is all fine K such that alpha equals sigma 1 of alpha equals sigma 2 of alpha. Because alpha is the image of 1 so I will not write it as 1 of alpha just write it as alpha.

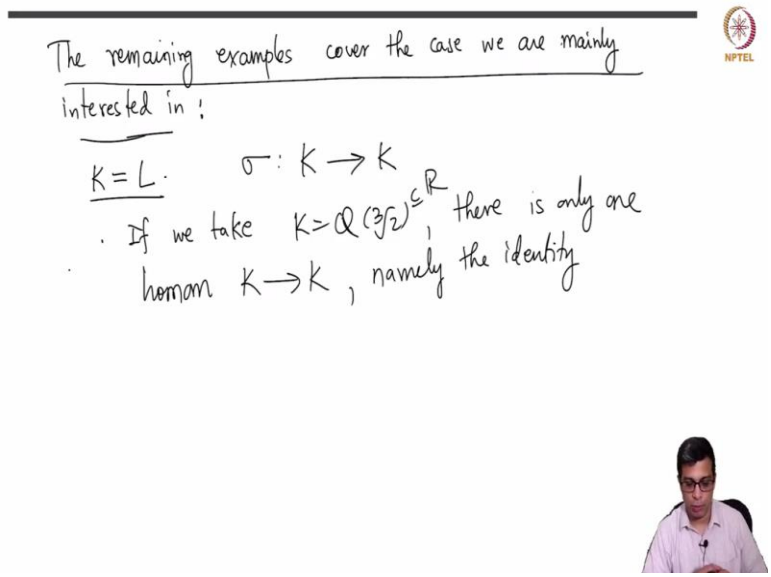
So, if you take an arbitrary element alpha which is of this kind, it goes to a plus b cube root of 2 omega plus c under sigma 1 it goes to b cube root of 2 omega plus c times cube root of 2 omega whole square. Under sigma 2 it will go to some something else you can write it down and if those are equal, you conclude that it must be it must be that b and c are 0. So, that means it is a rational number.

(Refer Slide Time: 13:33)



So, this is the exercise, so, I would not write it down because this is a good exercise for you to familiarize yourself with the, the notion So, in fact, the same is true if you take at least 2 elements of this. So, if you take this or this or so. So, sigma 1, sigma 2, they are all Q. So, this is the exercise for you. So, if you take any 2 elements of s, the fixed field is Q. Of course, if you take 1 element for trivial reasons, the fixed will, will be K, but otherwise it will be Q.

(Refer Slide Time: 14:21)

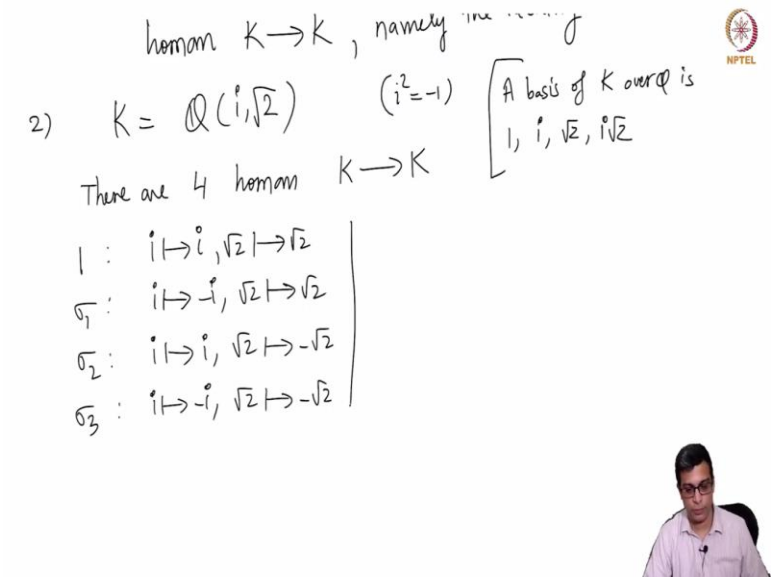


So now, the remaining examples will be, will be the cover the case? We are mostly we are mainly interested in, so what are these remaining examples? So, I hope this is clear this first example the last part I am leaving that as an easy exercise if needed, we can discuss this in a problem session later on, or you can ask questions in problem session about it. But this is a trivial exercise. So, the main case that we are interested in is when K equal to L, and all homomorphism's are from K to K.

So, I am going to just use, I will not use the letter L, I will just call it K. So, this is the main case that we are interested in. So, here we are, if you look at in the previous example, when K is cube root of Q or ad joint cube root of 2, if you are to the target space to be also K, then these are not going to be available for us. So, if we take K to be Q ad joint cube root of 2 there is only 1 homomorphism from K to K, namely the identity map.

That is because again, just to repeat what I said earlier, to determine a map from K, you need to determine the image of cube root of 2 that is all everything else is determined automatically, once you determine the cube root image of cube root of 2 everything else is determined automatically and what are the possible images of cube root of 2 they are cube root of 2 comma cube root of omega comma cube root of 2 omega square, but K contains only cube root of 2 because K is in Q, K is in R whereas cube root of 2 omega is not in R. So, there is only 1 map so that that restricts the possible homomorphism's.

(Refer Slide Time: 16:44)



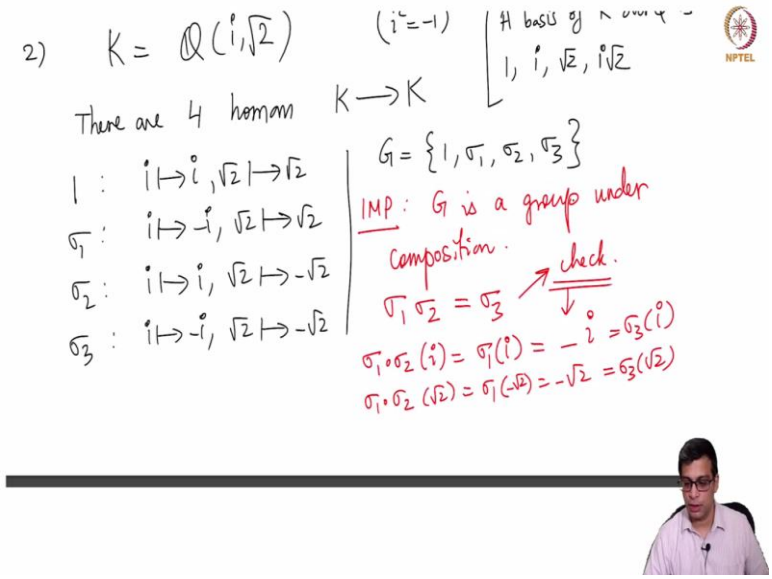
So, now, the second example that I want to study where there is actually interesting homomorphism's from K to K is this field Q ad joint i comma root 2 i is of course, complex square root of minus 1 always. So, what are the homomorphism's? Here I claim there are 4 homomorphism's there are 4 homomorphism's what are they? Remember again, because I recalled this earlier, I would not say this again, I would not write it again. Image of i has to be either i or minus i because those are only roots of the irreducible phenomena i, which is x square plus 1.

Similarly, image of root 2 has to be either root 2 or minus root 2, because those are the those are the only roots of x square minus 2. So, there are 4 homomorphism's basically by taking all the possible images. And one more fact is to determine homomorphism from K to K, all you need to do is determine the image of and root 2 and the basis of K or Q is given by 1 comma i comma root 2 comma i times root 2.

So, every element of cake can be written uniquely as a rational linear combination of 1 i root 2, i root 2. So, if you take that, if you determine the image of i comma root 2, image of i comma root 2 i times root 2 is automatically determined. So, every image will be determined. So, the 4 homomorphism's will be 1, which sends i to i root 2 to root 2, which is 1 will always be used to denote the identity map.

Sigma will be i going to sigma 1 will be i going to minus i root 2 to root 2, sigma 2 will be i going to i root 2 will be minus root, root 2 goes to minus root 2. Sigma 3 will be i goes to minus i root 2 goes to minus root 2. So, the i has 2 possibilities, root 2 has 2 possibilities, so, you have 2 times 2 possibilities for all of them together. So, there are 4 functions like this.

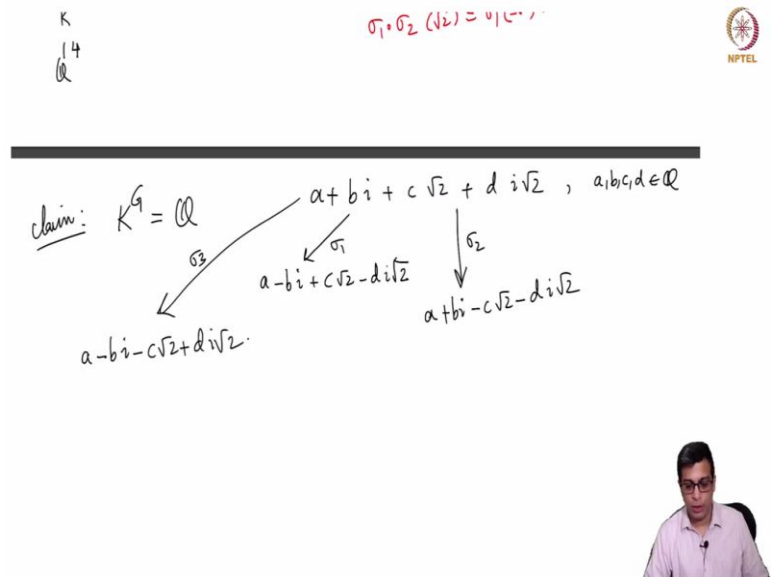
(Refer Slide Time: 19:01)



And I am going to use G for all of them and it is no accident that I use the letter G as opposed to the letter S, because G is a group This is an important point G is a group, so, the case in which we are going to be mainly interested in the case K is equal to L in that case, the homomorphism's form a group under composition. So, here 1 is identity element, sigma 1 sigma 2 and the point is sigma 1 sigma 2 is equal to sigma 3. So, this is something you should check.

So, the composition of sigma 1 sigma 2 for example, what is sigma 1 (compo) sigma 2 of i, this is sigma 1 of sigma 2 i which I and what is sigma 1 of i which is minus i, which is exactly sigma 3 of i. Similarly, sigma 1 composed sigma 2 of root 2 will be sigma 1 of root 2, which is root 2 and sigma 1, sigma 2 of root 2, which is minus 2 minus root 2 and sigma 1 minus root 2 will be minus root 2 because sigma 1 of root 2 is root 2 and this is sigma 3 of root 2. So, I have actually checked this. So, this is a group so, we this is getting to the crux of Galois theory. So, we will analyze this more later. And I will formally state this as a lemma in a future video. But now, let us come back to the Fixed Fields.

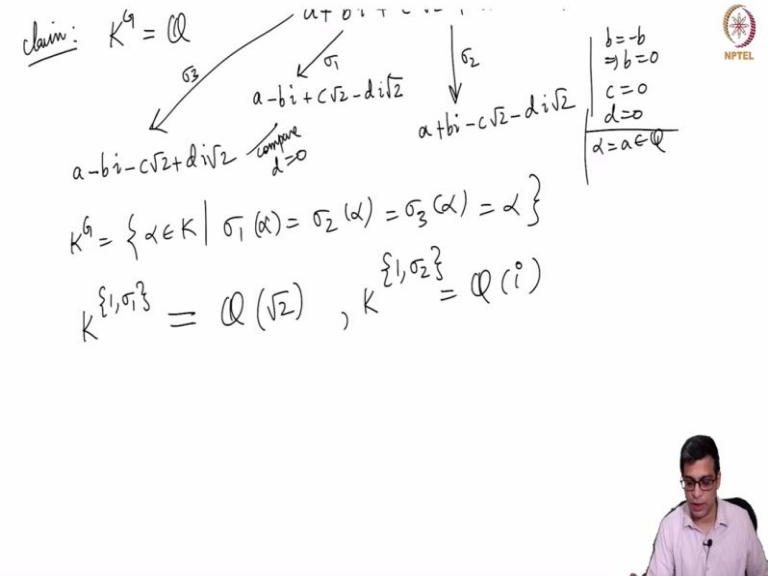
(Refer Slide Time: 20:47)



What is the fixed field? I claim that Fixed Field is Q. So this is something I will allow you to do on your own. But just maybe I will start the process. So, here we can use more analysis here. So, for example, it is a subfield between K and Q. So, remember K to Q is a degree for extension, so, it sits inside between these 2. So, take an arbitrary element of K, it is going to be of this form. Where does it go under sigma 1? Where does it go under sigma 1, it goes so, that is right here. Under sigma 1, it will go to a, a and b and c are rational numbers of course, c d are rational number.

So, under sigma 1 this will go to a plus or because i goes to minus i go to a minus bi plus c root 2 and i times root 2 will go to minus i times root 2. So, this is minus d i root 2. Similarly, what where does it go under sigma 2 it will go to a plus bi minus c root 2 and i root 2 again we will go to minus i root 2 so, this is minus d root 2. And finally, where does it go and a sigma 3 sigma 3 sends i to minus i root 2 to minus root 2, i times root 2 to i times root 2 because that is sigma 3 of i times sigma 3 of root 2 which is minus i times minus root 2. So, this will go to a minus bi minus c root 2 plus di root 2.

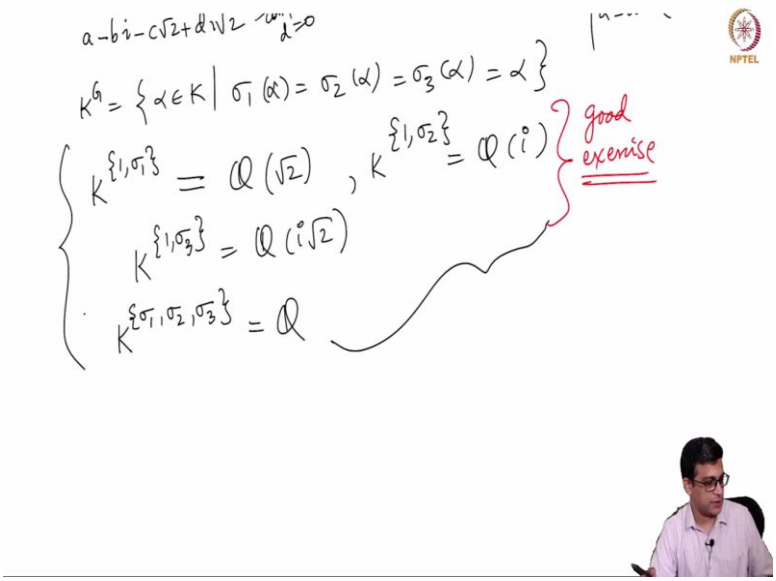
(Refer Slide Time: 22:56)



And KG is all elements all fine K such that sigma 1 of alpha equals sigma 2 of alpha equals sigma 3 of alpha equals alpha. So, all of these are equal to alpha which is this. So, now, using the fact that this is a basis 1i root 2 i root 2 you can immediately see that for example, comparing these 2 these 2 you conclude that b equals minus b that means, b equal to 0 and comparing these 2 again we get c equal to 0 whereas, you compare these 2 you get b equal to 0.

So, that means a b, b c d are 0 that means, that means alpha equals to a which is in, so, simple statement. So, the Fixed Field is K power G. Another what is a fixed field of 1 comma sigma 1 and I will let you do this, this is actually equal to what does sigma 1 fix sigma 1 fixes root 2 and it does not fix minus I so this root 2. K power 1 comma sigma 2 will be Q adjoint i because sigma 2 fixes i it does not fix root 2 so, this requires proof.

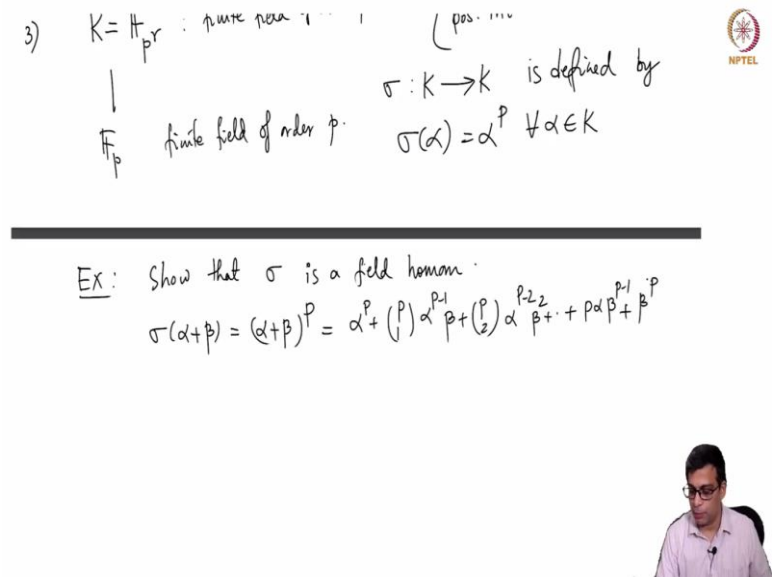
(Refer Slide Time: 24:20)



And finally, if you take K power 1 comma sigma 3 what you get is actually higher ad joint Q ad joint i times root 2. So, exactly the same kind of analysis you take an arbitrary element explicit in terms of basis and use these conditions. So, these are good exercises for you to familiarize yourself with the notion of fixed fields. So, this is the fixed these are the various fixed fields.

On the other hand and you can also look at things like this. This again I claim you get K Q. Similarly, if you take, so, let me just stop here. So, this is another exercise for you. These are all exercises and these are very hands on easy to verify just using the basis description like this.

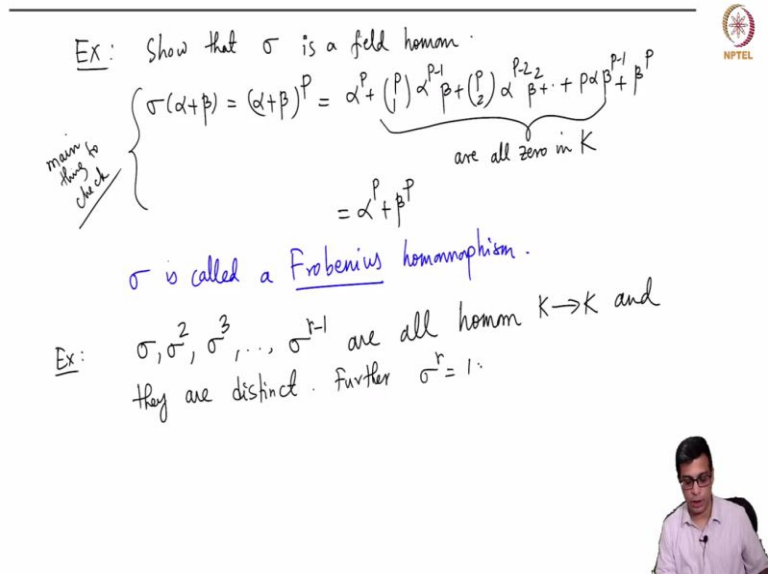
(Refer Slide Time: 25:25)



So, let me quickly do a third example, which is going to be a very important example again for us later on, let us take K to be F power fpr, so, fix a prime p and a positive integer r, positive integer r and this is the finite field, there is only 1 finite field of order p power r up to isomorphism. So, this is denoted by this and of course, this is about its prime field which is finite field of order p. Now, I am going to consider this particular field homomorphism from K to K. So, sigma of alpha is equal to alpha power p for every alpha.

So, now, this in general, this taking powers is not a homomorphism, but for characteristic p field, it is a homomorphism show that sigma is a field homomorphism, you basically you have to show for addition, So, sigma of alpha plus beta will be alpha plus beta power, because sigma sends everything to its pth power. So, this is alpha p plus p choose 1 alpha p minus 1 beta plus p choose to alpha p minus 2 beta square and p alpha beta p minus 1 plus beta power p.

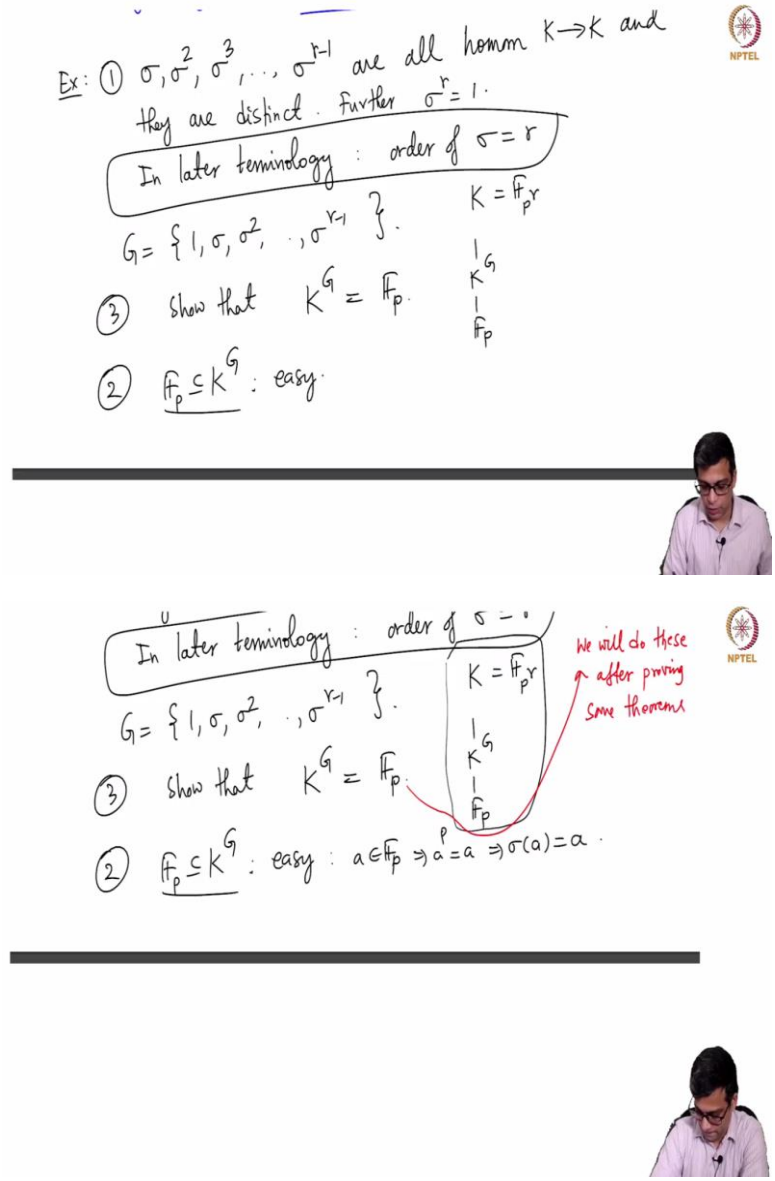
(Refer Slide Time: 27:15)



But because these are all going to be divisible by p these coefficients these are all 0 in K. So, this is just alpha power p plus beta power. So, these are standard statement and other things are trivial. So, this is the main thing to check for homomorphism. So, this is a very important Field homomorphism's for the fields of characteristic p sigma is called a Frobenius, Frobenius homomorphism. So, this is called Frobenius homomorphism and it is a homomorphism is the exercise for you.

Now, sigma square so so, this exercise I want to give now is the following. So, now an exercise for you I will do this in a problem session later on. So, sigma, sigma square sigma cubed up to sigma r minus 1 are all homomorphism's from K to K and they are distinct for the sigma power r is 1. So, basically when we talk about the Galois group of extensions in the next video or a later video sigma belongs to it and sigma has order r.

(Refer Slide Time: 28:59)



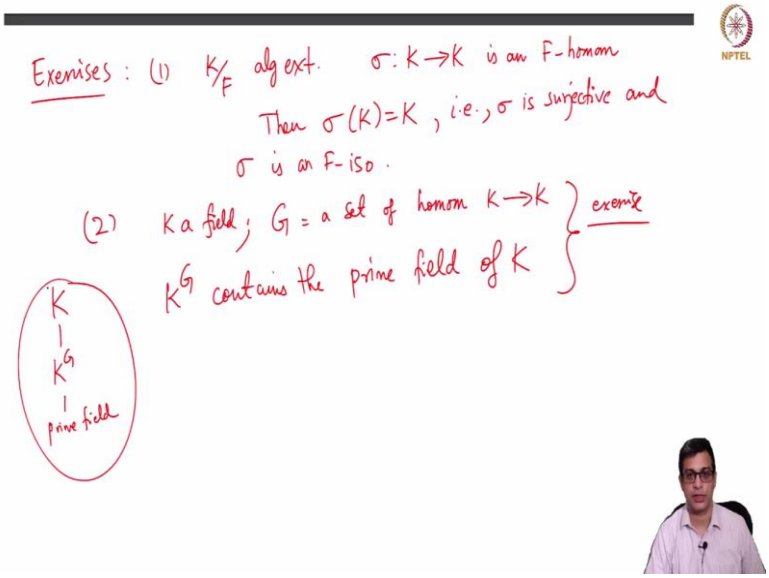
So, in later terminology. So, the exercise amounts to saying that order of sigma is r. So, basically I am taking G to be 1 sigma, sigma square of 2 sigma r minus 1. So, now, the statement this is also an exercise which so, I wanted to record this in this video so that we understand the various types of examples we studied, but these are all going to take time to prove this. So exercise this is 1 show that second exercise is F power p.

So, this is one inclusion is clear. So, you have K which is fp power r KG and Fp. So, this part is clear. So, easy exercise. Maybe I should call it this is 3, 2 is Fp is contained in KG, this is easy. This is because if a belongs to Fp, we know that a power p is a, this is a feature of a finite field of

order p. So, that means sigma of a is a. So, Fp certainly in KG so, the exercise is to show that KG is equal to Fp this we will do after we prove a few theorems. So, let me emphasize that here. So, you can try to do this by elementary methods, but we will do this I wanted to do mention all these things to motivate the kind of theorems I will prove later. We will do this after proving some theorems.

So, let me stop this video here. In this video we have defined what a Fixed Field is for an arbitrary collection of Field homomorphism's. And I gave one simple example in general, but then I essentially said that the only or the most important case in which we are interested in is when the field is same on both sides K and we are interested in maps from K to K. And I gave you a couple of examples.

(Refer Slide Time: 31:25)



So, let me end this video with 2 exercises, which actually you can do without my help, these are exercises to so, the first exercise is, if you have a K or F is an algebraic extension actually one of the exercises is already done. So, it is only one exercise but I will recall it for you. So, K or F is an algebraic extension sigma from K to K is, is an F homomorphism then sigma of K is equal to K so, that is sigma is surjective and sigma is an isomorphism in fact. This was covered in the previous, previous problems.

So, another and the other important example is if you have K to L any so, S is a set of homomorphism's let me just go make it K to K and G is or S is a set of so G is a set of

homomorphism's from K to K. So, K is a field, then K power G contains no fixed field, contains the prime field. Remember prime field is the, the smallest field that contains let us say the Q in characteristic 0 or Fp in characteristic p.

So, I claim that KG contains the prime field. This is fairly easy to check. And this is a good exercise. So, I would not say anything more. So, prime field is always contained in the fixed field. So, you have K KG and whatever its prime field, so KG is always in between the primary key. So, let me stop this video here and in the next video we are going to continue the study of Fixed Fields. Thank you.