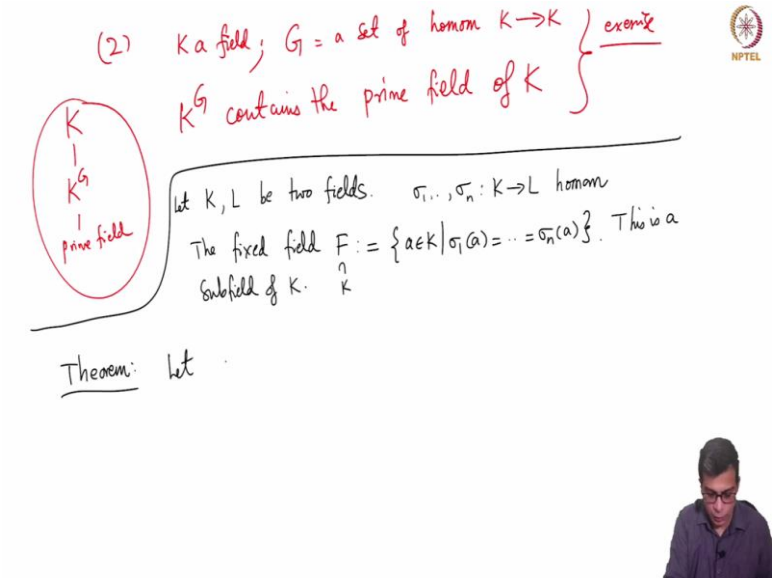
Introduction to Galois Theory
Professor. Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute
Lecture No. 12
Theorem I on Fixed Field

(Refer Slide Time: 00:14)



Welcome back in the last video, we define the notion of fixed fields for a collection of homomorphisms from one field to another field and we looked at various examples of these fixed fields. And I also said that the main case in which we are going to be interested in is when the target and source fields are same. So, you look at homomorphisms from K to K. Today we are going to prove one very important theorem and the next video will prove another theorem.

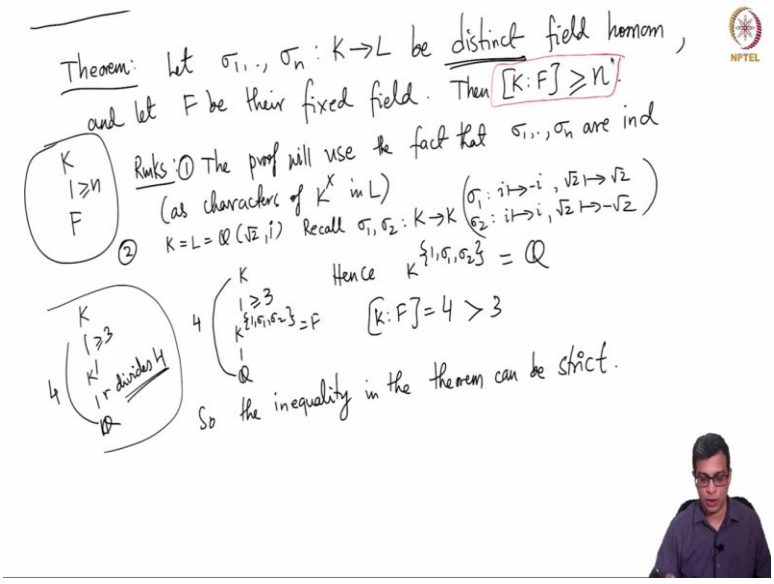
So, the next two videos are two very important theorems about fixed fields. And the entire theory that we will do after will depend on these 2 theorems, these are 2 important theorems. So, please pay close attention to these and the proofs are actually just nothing more than linear algebra. So, it will be very elementary though a little computationally, it will be tricky, but it is very elementary nothing more than algebra linear algebra is used.

So, just quickly recall K and L are 2 fields and you have a collection of homomorphism's the fixed field KF is defined to be all a in K, such that images of a under all these homomorphism's is the same, so this is a subfield of K. So clearly, of course, F is contained in K. So now, the 2

theorems I am going to, I am going to prove which I said already that they are very important. In the first theorem, we are going to be in this general setup where you have two fields and homomorphisms between them.

In the second theorem, we will actually do the main case that we are interested in, where K and L are same. So, the theorem that I want to do now, the first theorem in this video, and it says the following,

(Refer Slide Time: 02:21)



So let, I am going to basically rewrite this, like sigma 1 to sigma n from K to L be distinct. So, the important assumption is that there are distinct field homomorphisms. And let, F be their fixed field. So, let F be their fixed field. So now, the conclusion of the theorem is then the index of K over F is at least n very simple statement, we have n distinct homomorphisms, the degree of K over F is greater than or equal to n. Here's the conclusion. So in general, this is what we can say.

So, what I want to know before I start the proof, just a few remarks, the proof will use very importantly, the fact that women are independent. So, remember, their characters from K cross to L cross, so the characters of the multiplication K cross in the field L. So, I should use the terminology. So, the characters of K cross in L, and they are distinct. So, they are independent. These are foundational theorem that we proved a couple of videos ago. So, this is what we will use.

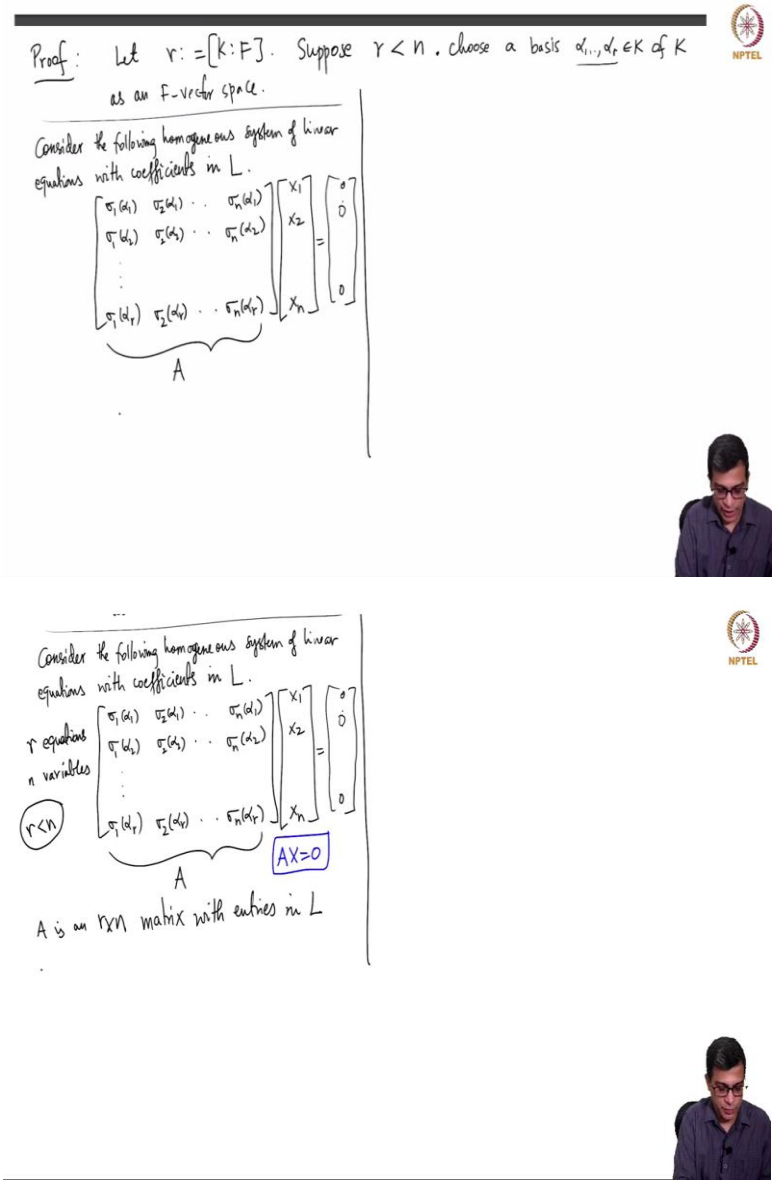
And then, I will also this is the crucial ingredient in this theorem, as well as in the next theorem. And the second remark is really an example. So, I did this. In the last video, we discuss this in more detail. So, I am only going to quickly tell you what happens in this with respect to this theorem. So, sigma 1 to sigma 2 from K to K, they send sigma 1 I think fixes i. So, just to be consistent with the earlier notation, sigma 1 changes i to minus i root 2 to root 2 sigma 2 sends i to i root 2 to minus root 2.

So, let me so sigma 1 sends and sigma 2 sends i to i root 2 to minus root 2. Then, if you think about this, the fixed field of the set 1 sigma 1 sigma 2, I claim this is a sub field and of course, it contains Q. So, now by the theorem that we are now going to prove this is at least 3, because there are 3 distinct homomorphism's 1, sigma 1, sigma 2, so there is at least 3, whereas this is 4, the entire degree of K over Q is 4 and hence the fixed field of must be Q, because any sub index if you have K to Q, and you have some K prime, this is 4.

So, this number whatever this is, let us say this is r divides 4. So, r divides 4, and this is at least 3 that means this better be 1. So, that is explanation. So, that means the, if this is the F in the notation of the theorem, K colon F in this case is 4, which is strictly greater than 3. So, the theorem is true, but the inequality can be strict. So, the inequality in the theorem can be strict. So, the second theorem, which we will prove in the next video deals with this, in a special case, you assume something's about sigma i is namely the deforming group, then the inequality is actually inequality. So, that will do later.

But for now, we are only saying that column F is at least n that is all. So, let me now start the proof. As I said, the proof is really nothing but an exercise in linear algebra. And please pay slowly follow this, this is not difficult. And it is very nice. It is actually a very, very clever proof and it uses pretty much nothing more than linear algebra.

(Refer Slide Time: 07:15)



So, and if needed, you can watch this slowly and follow the proof. So, suppose the proof was by contradiction. So, let r be the index of K or F. Suppose r is strictly less than n. So, we are trying to show that r is at least n. So, these r and r is at least n. So, suppose it is strictly less than. So, what is this index mean? It is the dimension of the vector space K or the field F. So, we want to choose that. So, I am going to try to squeeze everything into this screen so that you can we have all the data in front of us. So, I am going to write smaller letters.

So, let choose a basis alpha 1 through alpha r of K as an F vector space. This is the meaning of the index dimension, the F vector space K is r that means there is a basis consisting of r

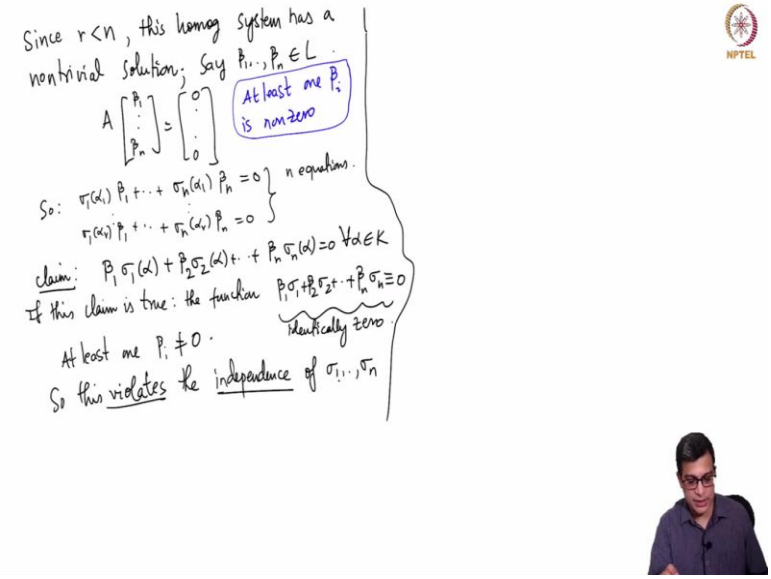
elements. Now, I am going to consider the following. So, I am going to split this into 2 parts. So, consider, consider the following system of it is a homogeneous system, in fact, system of linear equations with coefficients in L. What is the system?

So, I am going to take I am going to represent the system as a matrix. So, I have sigma 1. So, in the first row, I am going to fix alpha 1. So, sigma 1, alpha 1, sigma 2 alpha 1, sigma n alpha 1, alpha 1. In the second row, I am going to fix alpha 2, and sigma is go through from 1 to n, sigma 1, alpha 2, sigma 2 alpha 2, sigma n alpha 2. And in the last row, I am going to fix alpha r, sigma 1 alpha r, sigma 2 alpha r, sigma n alpha r.

So, this times a column of variables. So, this is n variables. I want this to be the 0 vector. So, this is a lean homogeneous system of equations. So, if you think, think of this as an matrix A, A is of course, what is the size of A? A is, so, there are r columns, r rows 123 corresponding to alpha 1 alpha 2 alpha r. So, A is an r by n columns, alpha 1 alpha 2 alpha n so r by r by n matrix with increase in L of course, because sigma is remember the hypothesis, sigma is a functions from K to L, all i is are in K, So, sigma of alpha is, is an L. So, A is an r by n matrix with entries in L in the system is nothing but so the system is AX equal to 0. So, this is a system of the form AX equal to 0.

So, how many equations are there, there are r equations here, r equations and variables, variables are x1 to xn equations are first row here times the vector, second row times the vector, last row times the vector. So, there are r equations. So, now, you know from your linear algebra that you learned a long time ago, that every time you have fewer equations than variables, there is always a non trivial solution for this homogeneous system of equations.

(Refer Slide Time: 11:40)



Since r is less than n, namely, since the number of equations is less than the number of variables, this homogeneous system has a non trivial solution. Say beta 1 through beta n these are system solutions in L. So, what we have is A times beta 1 beta n equal to c. So, I am not going to write all these equations, but you can read this equation, I mean, maybe the first equation. So, the first equation will be sigma 1, alpha 1 times beta 1, sigma n alpha 1 times beta n equal to 0. That is that, so just replace x1 by beta 1 x2 by 2 x2 by beta 2 xn by beta n. So, I am only going to write the first and the last equation, last equation will be sigma 1 alpha r beta 1 all the way up to sigma n alpha r beta n equals 0. So, there are n equations like this.

So, this is just a collection of elements of L and r and this is 0 and at least 1 bit is nonzero. So, at least that is exactly the meaning of it being a non trivial solution. So, this will be useful for us later. So, now, let me try to explain the goal now is to play with this linear system and conclude a contradiction. So, what we are going to claim?

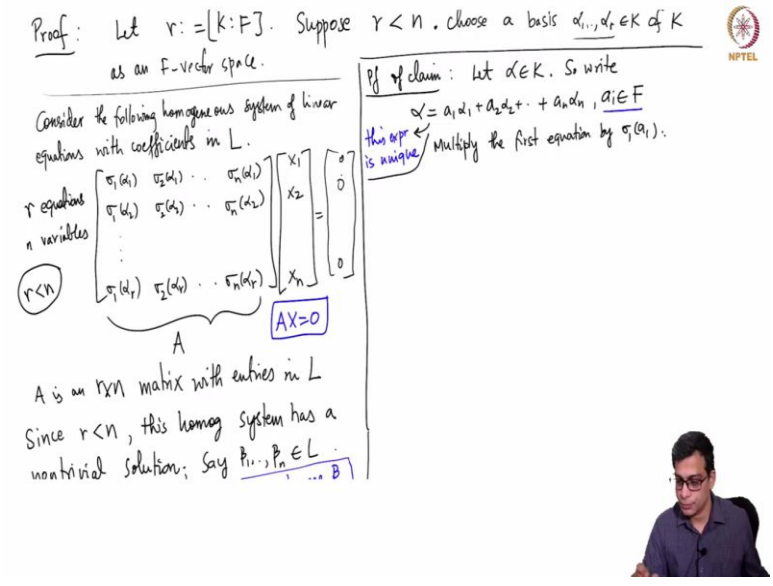
So, maybe I will squeeze the claim here, claim is not to claim that beta 1, sigma 1 alpha plus beta n sigma. So, maybe I will write one more time here, beta 2 sigma 2 alpha plus beta n sigma n alpha is 0 for all alpha in K. That is my claim, if this claim is true, so, I hope you are following this, this is nothing more than just playing with linear equations. So if this claim is true, so I am going to show that beta 1 alpha 1 alpha, beta 1 sigma 1 alpha plus beta 2 sigma 2 alpha plus dot

dot dot plus beta n sigma and alpha 0 for all alpha in K, then the function beta 1 sigma 1 plus beta 2 sigma 2 beta n sigma n is identically 0.

But this violates the and remember one of the beta i is nonzero. So, at least one beta i is nonzero. So, this violates the independence as I told you, this is a crucial hype property that we are going to use of sigma 1 to sigma n. So, this violates the independence of sigma 1 to sigma n and hence r cannot be less than m. So, that is the approach we want to take. So, I hope you can follow so, far the approach is if r is strictly less than n, we have constructed a clever linear system of equations using the fact that r is less than and we are guaranteed and non trivial solution so, that beta i one of the beta i is nonzero and then we are going to prove this claim.

So, that all sigma 1 to sigma n are in fact dependent, they are not independent, but they cannot be dependent because they are distinct characters of a group. So, they must be independent and hence the claim is that there is a contradiction. So, the goal is to prove this now, so, the goal is to prove the claim.

(Refer Slide Time: 16:09)

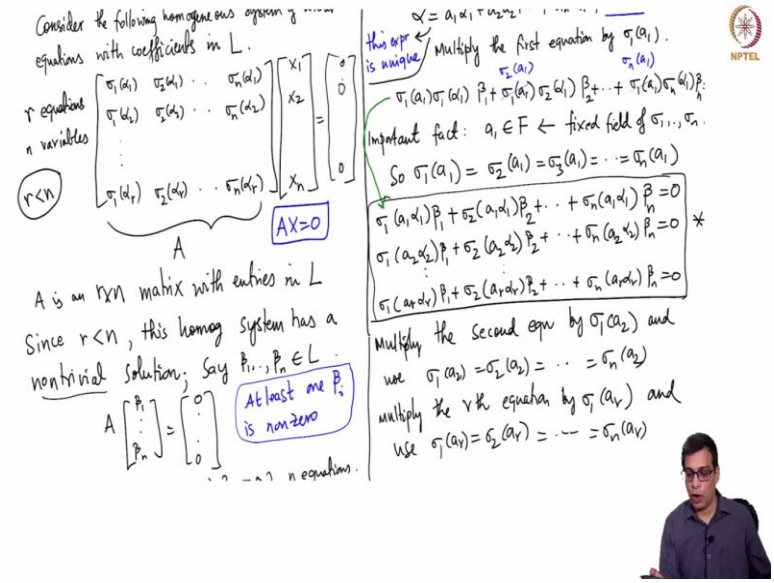


And the claim is proved by essentially using just clever linear algebra, manipulation of linear equations. So, let us take an arbitrary alpha in K, so, we want to show this for any alpha in K. So, the claim is that this is true for all alpha and K. So, I am going to start with an arbitrary alpha and K, alpha 1 through alpha r are a basis for K over a, so write alpha as uniquely right. So, a1 alpha 1, a2 alpha 2 plus an alpha n, where ai is are now in F this is the important fact.

Because K is a vector space over F it has dimension R over F and alpha 1 through alpha r form a basis of K over F. So, any element in K any element alpha and K can be written uniquely this expression is unique. And ai's are in F, that is important statement how important property for us. So, we are going to write this. So now, so I hope you can see this. So, so, this, this is the system that I am interested in.

So, this is the first equation, this is the second equation is not written, but rth equation nth equation. So, you have all these things. So, r equations, so we want to multiply. So, now let me start the proof of the claim. So, multiply the first equation by sigma 1 a1, so I claim that sigma 1 a1 is a scalar. So, if I multiply this equation here, by any scalar, the equation will remain true. So, what we have is, so I am going to write it here.

(Refer Slide Time: 18:11)



So, what we get is sigma 1. So, I am going to write this like this a1, sigma 1, alpha 1 beta 1. So, you can see that here, sigma 1, a1 sigma 1 alpha 1 beta 1, let me write the second term, just so that you understand what is happening. So, second term will be sigma 2, it is here, a sigma 2. So, I am multiplying by sigma 1 a1. So, sigma 1 a1 times sigma 2 alpha 1 times beta 2 plus, last term will be sigma 1 a1, sigma n, alpha 1, beta n is 0. So, that is what the after multiplying by sigma 1 a1 we get this.

Now we are going to use the important fact that a1 is in F, and F is the fixed field of sigma 1 to sigma 1. So, what we have is sigma 1 a1 equals sigma 2 a1 equals sigma 3 a1, all the way up to

sigma n a1. Now, if you look at this equation here, I am going to rewrite that so what we get first term involves sigma 1 a1 time sigma 1 alpha 1. So, I can rewrite that as sigma 1 a1 alpha 1 times beta 1, no problem. But the second one involves sigma 1 a1 times sigma 2 alpha 1, but sigma 1 a1 is same as sigma 2 a1.

So, you can replace this here by sigma 2 a1, sigma 2 a1. So, once you have it sigma 2, a1 it will be sigma 2 a1 times sigma 2 alpha 1, but that means, I can write this as sigma 2 a1 alpha 1. So, and then beta 2 and the last term sigma 1 a1 is equal to sigma n a1. So, that is your sigma n a1. So, sigma n a1 is equal to sigma 1 a1, So, sigma and a1 times sigma and alpha 1 will be sigma n a1 alpha 1 and beta m equal to 0.

So, that means the first equation, so, this becomes this, so, there is using the fact that a1 is in the fixed field that is very crucial, otherwise, you cannot replace the sigma 1 a1 by sigma 2 a1 and then you cannot combine a1 an alpha 1 like this. So, it is important to know that a1 is in the fixed field. Now you multiply the second equation by multiplying. So, I want to write the second equation here.

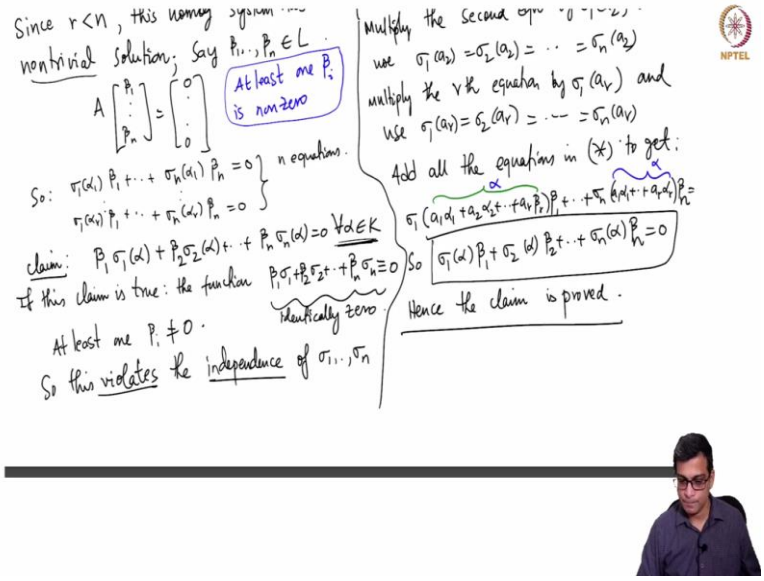
So, multiply the second equation by sigma 1 a2 so, multiply, so I want to have all of them together. So, we I will write it here and write what I get here. So, multiply the second equation by sigma 1 a2. So, I end use the fact that and use sigma 1 a2 equals sigma 2 a2 equals all the way up to sigma n a2. So, I get a priori sigma 1.

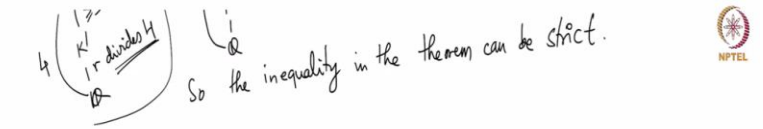
So, the second equation is this, I have not written the second equation, but it is sigma 1, alpha 2 times beta 1, sigma 2 alpha 2 times beta 2 plus sigma n alpha 2 times beta r n is 0, if I multiply by sigma 1 a2, I get sigma 1, the first one will be sigma 1, a2 alpha 2 beta 1, the second equation using this equality will be sigma 2 a2 alpha 2 beta 2. And the last inequality, last term we will be using this it will be sigma n alpha n alpha 2 times sigma n a2 sigma n a2 alpha 2 beta n is 0.

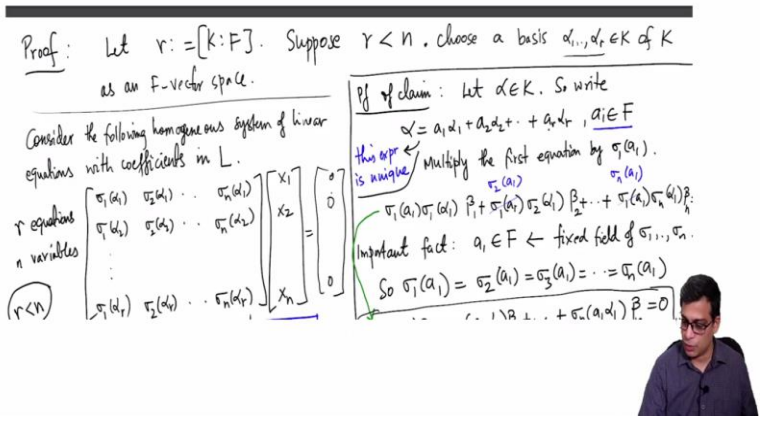
So, now, dot, dot, dot and the last point is you multiply the rth equation, I have been writing very slowly, very small letters. And this might become messy, but I wanted you to see everything on one screen as I am doing this proof. So, I hope this is better. So, multiplying rth equation by sigma 1 ar which and use sigma 1 ar equals sigma 2 ar which is sigma n ar, what I get is sigma 1 ar times alpha r beta 1 sigma 2 ar times alpha r.

So, originally it will be sigma 1 ar times sigma 2 alpha r, but using sigma 1 ar equals sigma 2 ar, I get this. So, it is the same kind of manipulation as this times beta 2 and all the way up to sigma n ar alpha r beta n is 0. So, now, this is the system that we are going to use. So, this system is what is going to do the job for us. Now, if you just stare at this, if you just stare the, the first term in each equation, you get sigma 1 a1 alpha 1 beta 1 a2 alpha 2 ar alpha r. So, if you add all of them, what do you get?

(Refer Slide Time: 24:19)







So, now, add all the equations in star to get. So, this is the last step now, we are done now almost. So, if you add all the terms all the equations in star which is this what is the coefficient of

beta 1, So, beta 1 will be sigma 1 of sigma 1 is a homomorphism. So, sigma 1 of a1 alpha 1 plus sigma 1 of a2 alpha 2 plus sigma 1 of ar alpha will be sigma 1 of a1 alpha 1 plus a2 alpha 2 plus ar beta r times beta 1 and similarly, sigma n of a1 alpha 1 plus ar alpha r times beta r is 0. So, that is what we get, but this, this term inside the bracket, what is this? This is exactly alpha.

So, alpha is a1 alpha 1 plus alpha 2 alpha 2 plus an alpha n. So, I made a mistake here. So, of course, this is not an alpha n. So, this is ar alpha r because alpha 1 through alpha r are the basis elements, so, it only goes up to ar alpha. So, this term is just alpha. So, that is alpha and this is alpha. So, that means, what we get is sigma 1 alpha beta 1, sigma 2 alpha beta 2 sigma and alpha beta r. So, beta n, so again I messing up the indices, so, it will be beta n and at the end, because I have all the way up beta n's.

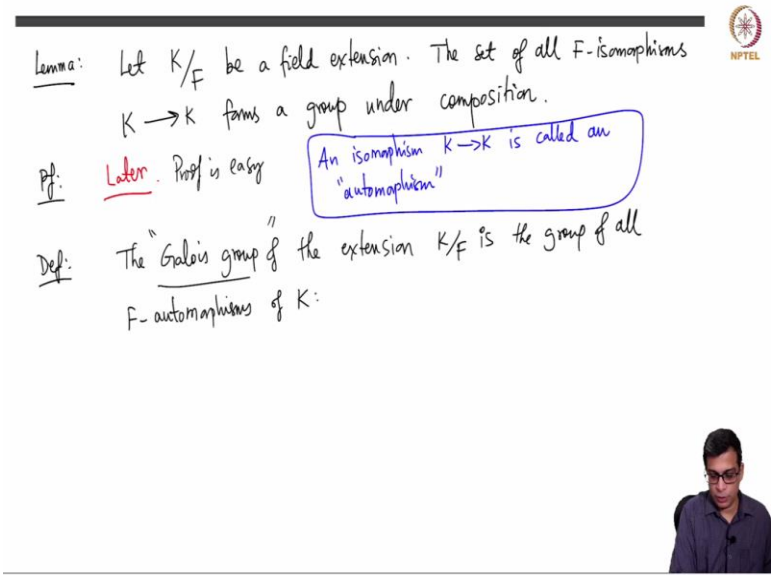
So, I hope I made no further mistakes of indices, but this is the top shot. And this is exactly what you see in the claim. So, you get beta up on of course, I interchange beta 1 and sigma 1 alpha, but that is. These are field elements in L. So, this is true and hence the claim is true. So, this completes the proof, and essentially what we have done is show that the fixed field index.

So, if you start with a bunch of homomorphism's, and you take n distinct homomorphism's, and you take their fixed field, the index of the ambient field or the fixed field is at least n we have seen that the inequality can be strict, but it is always created n equal to n. And the proof is basically a linear algebra proof. I hope you understand the proof, the proof is extremely clever, and uses as you can see nothing more than linear algebra.

So, I really want you to understand the proof carefully, because this is part of the beauty of the subject. So, this is all what you should learn carefully. Statement is still the most important thing that we will use later. But the proof is nice. So, I hope I did not go too fast or did not make it messy for you. But the proof is clear. So, this is where I will stop this video. And this completes the first theorem that I wanted to prove about Fixed Fields.

And in the next video, we will do the second theorem, which restricts to the case K equal to L, and shows that there is an equality in some cases. So, before I stop, let me just end the theorem by defining.

(Refer Slide Time: 28:08)

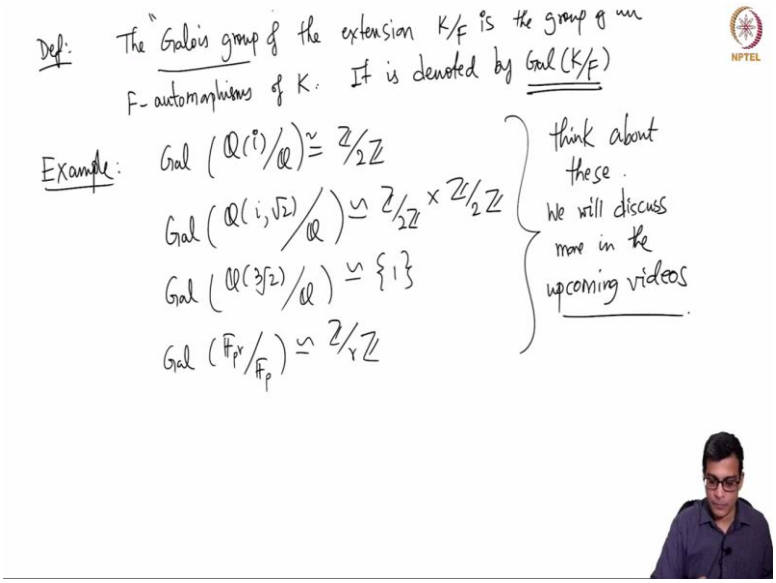


So, maybe I want to use all of the next video for the proof. So, let me just give you quickly the definition here. Let K or F be a field extension. This is not really a definition. Actually, this is a lemma. So, I am going to stick to so a field extension, then the set of all F Isomorphisms from K to K forms a group under composition. So, this forms a group under composition. So the proof, I will do as an as later, because I want to wrap up this video, and we will come back to this later.

So, the set of all F Isomorphism from K to K I should write. And these are called Automorphisms. If you have the same target and source, we call this an Automorphism. So, an Isomorphism K to K is called an Automorphism. That is because auto refers to the fact that it is from K to K. So, the set of all F Automorphisms of K forms a group under composition. And this is a very easy proof by the way, I will do this later.

Proof is very easy because if you compose two automorphisms you get an automorphism identities and auto morphisms. So, that is all really there is nothing more. So, the point is this. So, now, this is the most important definition for us, the Galois Group of the extension K or F is the group of all F automorphisms. So, the lemma says that they form a group and that group is called the Galois group of the extension. It is denoted by. So, this is really the, we are getting to the beginning of Galois theory really, so, this is an important object that Galois theory studies so, it is a called of the Galois group.

(Refer Slide Time: 31:01)



So, let me end the video by giving you a bunch of examples, I will not prove many of these, we will I will not prove them now. They are either easy or we will come back to proof later. So, Galois group of if you take Q adjoint i or Q is Z naught 2Z. So, Galois group of Q adjoint let us say I comma root 2 over Q over Q is isomorphic to Z naught 2Z cross Z naught 2Z and I will write two more Galois group of cube root of 2 over Q is just the trivial element. So, trivial group.

And finally, the Galois group of Fpr over Fp is isomorphic to Z naught rZ. So, these are some things for you to think about this. Think about this. We will discuss more in the upcoming videos. So, I wanted to define this because I want to frame the next theorem in terms of Galois group. So, I defined this, but the main content of this video is this theorem that if you take a bunch of homomorphism's, from K to L, the fixed field is a subfield of K, the index of the K or the fixed field is at least the number of those homomorphism's. It is of course important to take distinct homomorphism's.

Let me stop the video here. And in the next video, we will prove the second important theorem about Fixed Fields. Thank you.