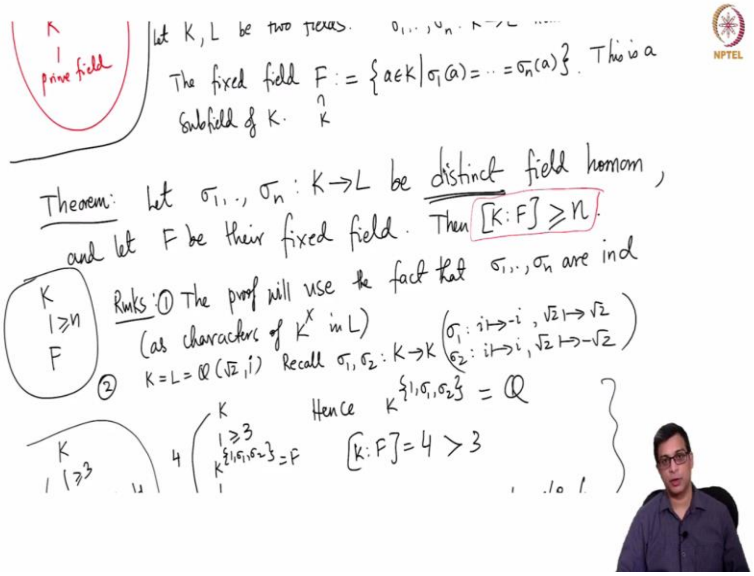
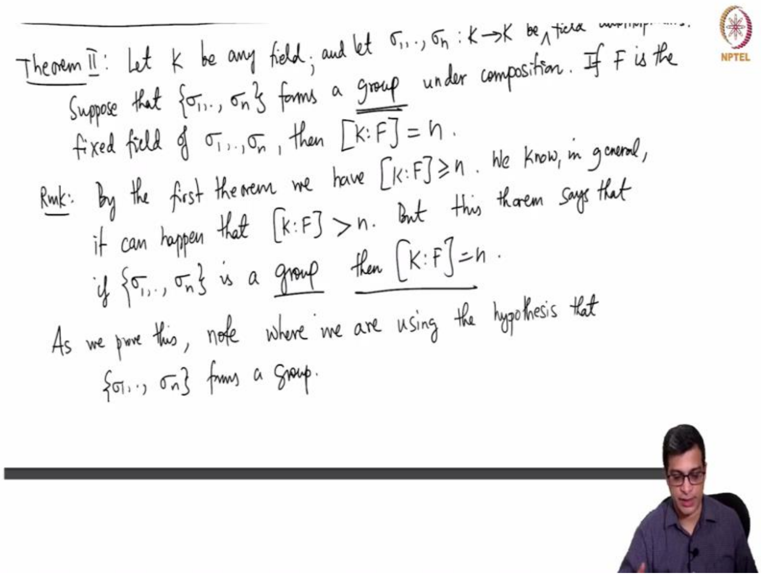
Introduction to Galois Theory
Professor. Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute
Lecture No. 13
Theorem II on Fixed Field

(Refer Slide Time: 00:14)



Welcome back in the last video, we proved an important theorem about fixed fields for a bunch of homeomorphisms from one field to another field. So, if sigma 1 to sigma n are homomorphisms, distinct homeomorphisms from K to L and F is the fixed field, then the degree of K or F is at least n. So, we are now going to prove the second important theorem about fixed fields that I mentioned last time. So, let me write the theorem here and we will prove it in the next slide.

(Refer Slide Time: 00:40)



So, let now K be any field and let sigma 1 through sigma n be field automorphisms remember, I use the word automorphism last time. Automorphism is simply an isomorphism from K to K. So, let these be distinct field automorphisms. So, let me put that here because that is important I need to take only different ones distinct field automorphisms. If F is their fixed field that means F is the So, I am not omitting the main hypothesis.

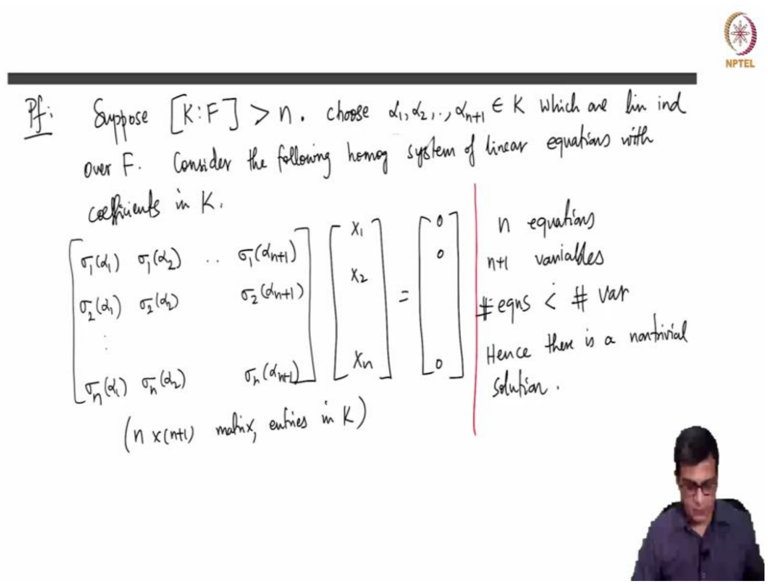
Suppose that sigma 1 through sigma n forms a group so, this is a crucial additional hypothesis forms a group under composition. So, in the language of Galois groups here, of course, I am not starting with a field extension, so, I cannot talk about Galois group, but suppose you did, and the all the sigma is are automorphisms over that base field, then, the hypothesis that the forming group is simply the hypothesis that this is a subgroup of that Galois group.

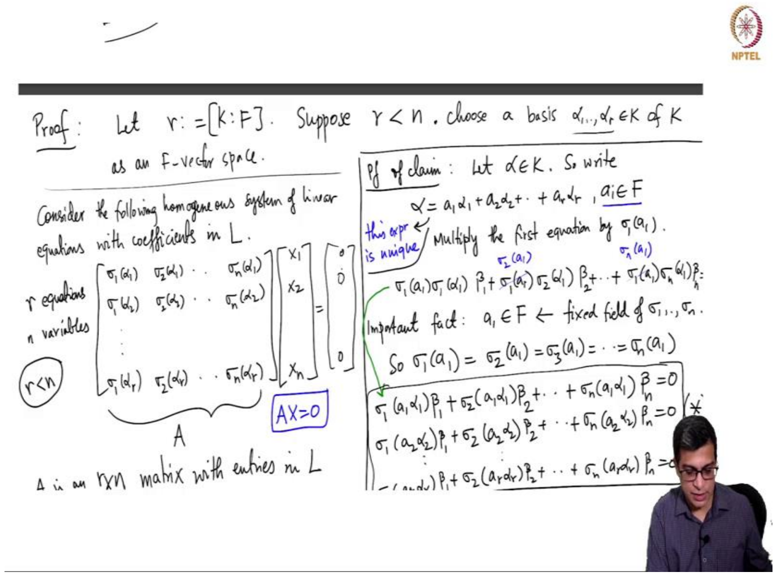
I am not fixing a base field, so I do not want to talk about Galois group here. Suppose that these set forms a group under composition. Now, if F is a fixed field of these n automorphisms, then K colon F, this is the equality so K colon F is equal to n. So, we remarked that by the first theorem, so, think of this as theorem 2, theorem 2 about Fixed Fields. By the first theorem we have a K colon F is at least n. So, we have now to show that it cannot be strictly more than n and we also know in general it can happen that K colon F is strictly bigger than n, but, this theorem says if is a group so, this is a new hypothesis, then equality must hold.

So, K colon F is always at least n and it can be strict as I told you last time, if you take the field Q adjoint root 2 comma i and take 3 automorphisms, 3 homomorphisms or automorphisms actually, in that case, identity sigma 1 sigma 2, the fixed field has degree 4, whereas there are only 3 automorphisms but there they do not form a group because sigma 1 sigma 2 is not in that sector. So, if they form a group, then K colon F is and.

So, as we prove this we will note where we are using the hypothesis about group that this forms a group I mean we have let us not just for fun where we are explicitly using the hypothesis hypothesis because without that hypothesis, the statement is false as that example shows. So, let me start the proof.

(Refer Slide Time: 04:53)





Let me also remark a priori that the proof is actually just linear algebra. It is exactly like theorem 1 except it is a slightly more involved, but it is still elementary linear algebra. So, I will try to go slowly and try to cover all the facts. But you might want to carefully do this, follow this on your own. And if you need it, go over the video again, or ask questions in the forum. The best way to understand these kind of things is to work it out yourself. So, read what I mean, listen to what I am saying, but pause if needed and work it out on your own. So, let r be the index as we actually I am not going to give it a name, because I do not need to.

So, suppose for a contradiction, that K colon F is strictly more than n ecause we know it is at least n and we are trying to show that it is equal to n. We are we were required to do anything only if K colon F is strictly more than n. Then let or choose n1 independent elements. So, alpha 1 to alpha n plus 1 over elements in K, which are linearly independent, over F. This basic linear algebra, you have K is a vector space over F, its dimension is strictly more than n, which is to say that there are n plus 1, at least n plus 1 linearly independent elements, maybe the dimension is n plus 3, I do not care. It is at least n plus 1.

So, I can take n plus 1 linearly independent elements. Now, just like in the previous theorem, we want to cleverly consider homogeneous system of equations, consider the following homogeneous system of equations of linear equations with coefficients again in, in this case, the L is also K so coefficients in K. And what is this equation? So here, it is a homogeneous system of equations. So, as I remarked earlier, these are these 2 are brilliant proofs. So, this is part of the beauty of the whole subject. So, please make sure that you understand this and enjoy the proofs as much as I do, because this is really wonderful.

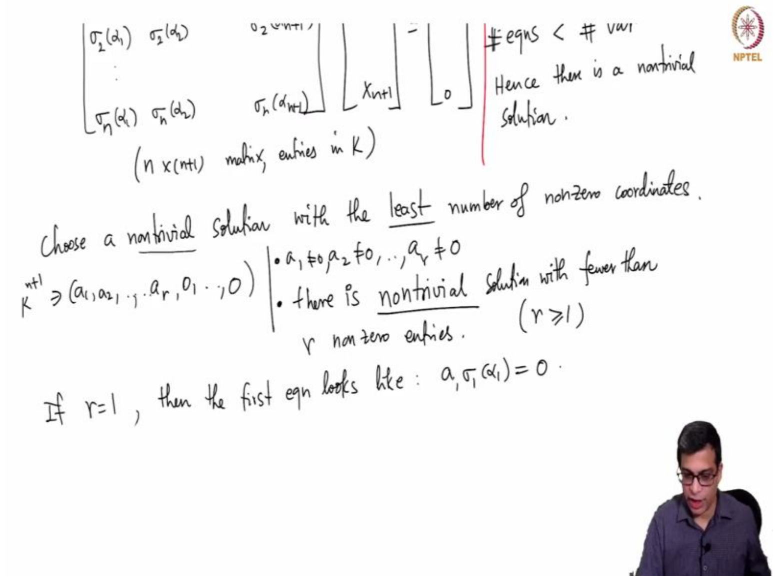
So, what is the little system that I want to consider? See earlier, if you just go back to the proof, I looked at this system where I fixed alpha 1 in the first row alpha 2 in the second row, alpha r in the rth row, and I fixed sigma 1 in the first column, sigma 2 in the second column, sigma n in the last column. Here, I am going to fix sigma 1 in the first row. So, the equation the system is sigma 1 alpha 1, sigma 1 alpha 2, sigma 1 alpha n plus 1 and second row, we will deal with sigma 2 alpha 1, sigma 2 alpha 2, sigma 2 alpha n plus 1.

So, I am fixing sigma's is in the rows now, as opposed to columns in the previous theorem, the last row will be sigma n alpha 1, sigma n alpha 2, sigma n alpha n plus 1. So, alpha i's are fixed in the column. So, alpha 1 takes care of the first column alpha 2 takes care of the second column alpha n plus 1 takes care of the last column. Sigma 1 is the first sigma 2 is first row sigma 2 is the second row and so on. So, the system is this.

So, now, what is the size of this matrix, this is there are n rows and n plus 1 columns there is an n by n plus 1 matrix with entries in K of course. So, in terms of equations and variables, there are n equations n plus 1 variables. So, again, number of equations, just like in the previous case, is strictly less than number of variables. Remember, here, our supposition is the opposite of what we suppose in the previous theorem, there, we assume that a K colon F is strictly less than n. And by arranging the matrix in a clever way, we got number of equations less than number of variables there.

Here we are assuming the opposite K colon F is strictly more than n. That means there are more alpha's than sigma's. But then by, I mean the transposing the matrix, we still have this hypothesis that the number of equations is strictly less than the number of variables. So hence I am just separating these. So hence, there is a non trivial solution. So, there are non trivial solutions, there is at least 1 non trivial solution. Now, here is where we are to be. This is, as I said this proof is a little more tricky than the previous one. So, I am not going to pick any arbitrary non trivial solution, but I am going to choose a non trivial solution of the following type.

(Refer Slide Time: 10:34)



Choose a non trivial solution beta 1, so non trivial solution with the least number of nonzero coordinates. What do I mean by this? So, I am going to choose a non trivial solution. And I am going to say I am completely with rearranging the variables. That means I am completely with a the order of alpha i’s is irrelevant here. So, I am going to rearrange so, take any nonzero solution and arrange rearrange the variables in such a way that the last few the tail of this solution is 0s. So, least number of nonzero coordinates. So here, beta 1 through beta r are all nonzero.

And there is so that is a first statement and there is no nonzero or non trivial solution with fewer than r nonzero entries. So, remember that there is a nonzero solution means 1 of the coordinates is nonzero. So of course, r is greater than equal to 1. So, I am only interested in non trivial solutions, that means at least 1 entry is nonzero. So, I take maybe there is an entry with if, if n is 5, each solution will have 6 entries.

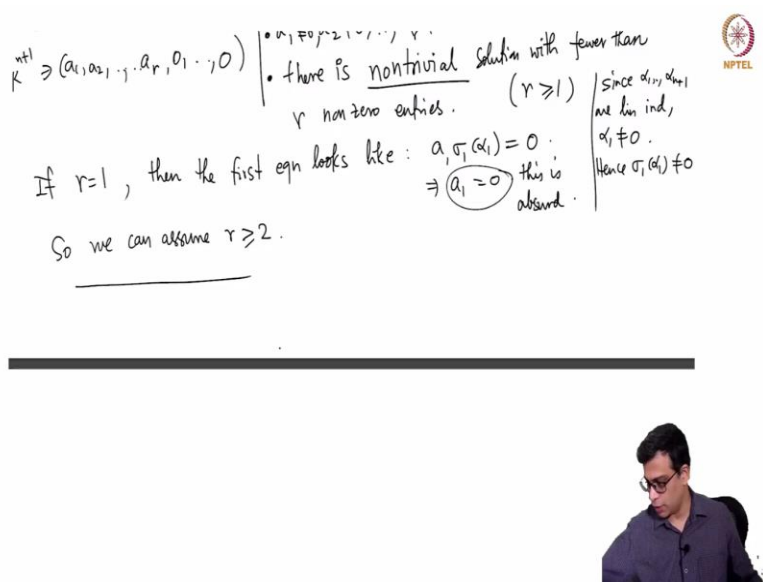
Because these are n here I have n plus 1. So, which I should, so there are n plus 1 increase in the solutions. Maybe there is 1 with 5 non 0s, 0s non nonzero coordinates, there is another solution with 6 nonzero coordinates, there is 1 with 3 nonzero coordinates. So, I pick the least number of nonzero coordinates. So, if there is 3, if it is 3, then there will be beta 1, beta 2, beta 3 followed by 0s, and there is no solution with 1 or 2 nonzero entries. So, that is what I mean.

So, this is the first conceptual point that you have to understand. So, I pick among all non trivial solutions, the one with the least number of nonzero coordinates, remember, the number of nonzero coordinates is a number between 1 it can be 1 to up to n plus 1, maybe there is no nonzero solution. Maybe every nonzero solution is all the entries nonzero, in which r is n plus 1. But maybe there is a solution with 1 nonzero entry, 1 0 entry all others non 0s, in which case I take r to be n and so on, so I do not care what it is. But I take r this, r is a number between 1 and n plus 1. And I am choosing a particular solution which has the exact number of nonzero entries.

So, we will first quickly dispose of the case that are equal to 1, if r equal to 1, then that means you have beta 1 equal to 0 nonzero, beta 2 and beta 3 up to be n plus 1 are all 0s. So this of course, is an element of K power n plus 1, there are n plus 1 entries. So, what are the equations the first equation looks like so, sigma 1 alpha 1 times beta 1, sigma 1 alpha 2 times beta 2, sigma 1 alpha 3 times beta 3 sigma 1 alpha 1 times beta n plus 1, but beta 2 onwards, everything is 0. So, we just have beta 1 times sigma 1 alpha 1 equal to 0.

But then, so actually, I, I do not want to call them beat i's. I do not want to change my the notation in my notes. I will call them a. So, a1, a2, a up to ar and a1 is nonzero, a2 is nonzero, ar is nonzero. So, the first equation will be a1 times. So, this you can put a 1 here, here to here, n plus 1 here. So, a1 times sigma alpha 1 a2 times sigma 1 alpha 2, but a2 onwards everything is 0.

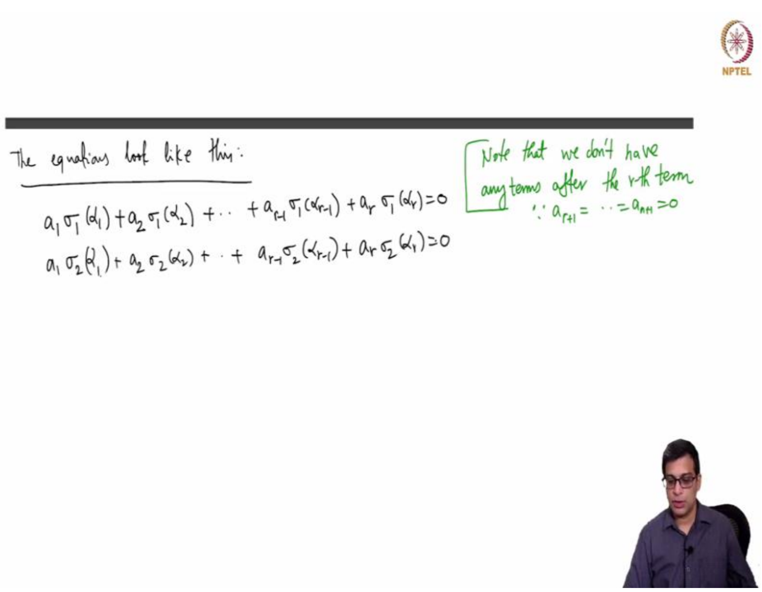
(Refer Slide Time: 15:37)

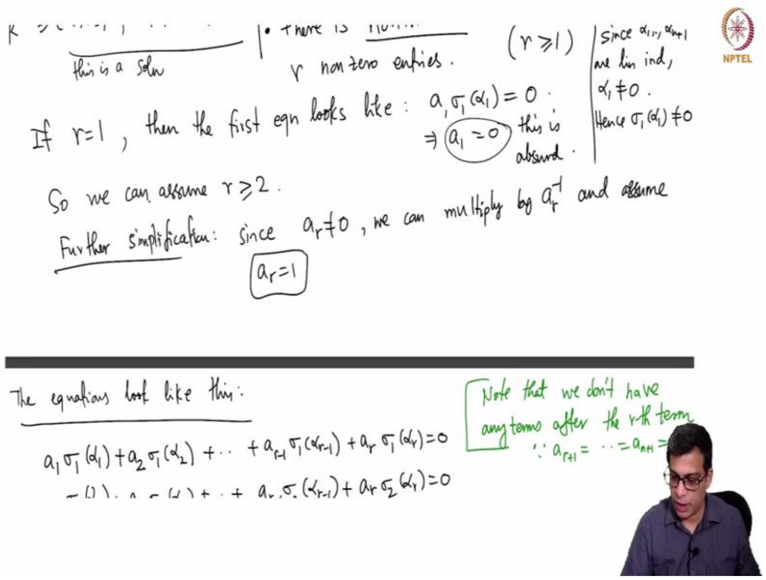


So, this is what we have. But note that, since, alpha 1 through alpha n plus 1 are linearly independent alpha 1 must be nonzero in particular, any linear independent set cannot contain a 0 vector. So, alpha 1 is nonzero and hence, signal 1 alpha 1 is non 0, sigma 1 being a field homomorphism, it must send nonzero elements nonzero elements. So, that means a1 is 0. But that is a contradiction, because we are taking a non trivial solution and if a2 onwards everything is 0, a1 better be nonzero, so, this is absurd. So, we can assume r is at least 2.

So, again to recall the setup is we consider a homogeneous system of equations, where the number of equations is strictly less than the number of variables. And hence, we are guaranteed that there is a non trivial solution. And among all the solutions, we are picking one, which has the least number of non 0 entries. And that r, which is the number of nonzero entries is at least 2 is what I just if r is 1 we are done. So, we are now going to assume r is at least 2. So, now, let us get into the proof really the heart of the proof.

(Refer Slide Time: 17:05)



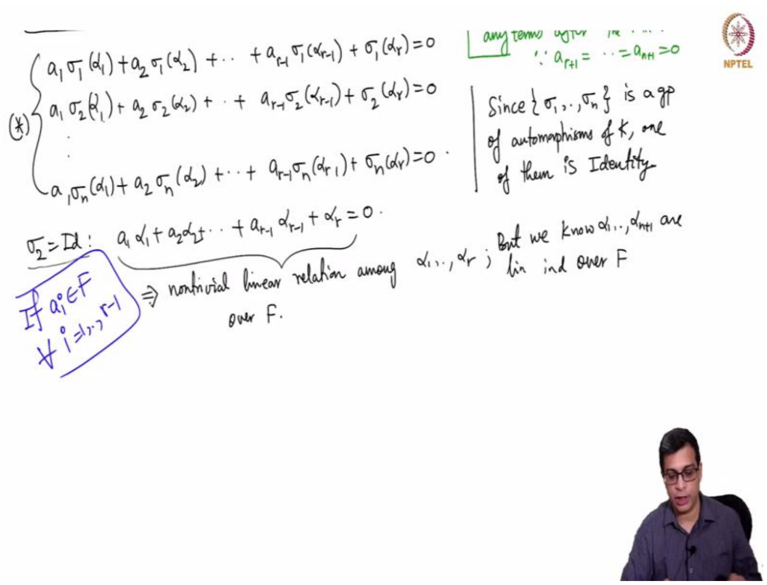


So, I am going to rewrite the equations just for clarity look like this. Equations look like this. So, the previous slide contains the matrix, but I want to write it directly as equations. So, the equations look like this. a1 sigma 1 alpha 1, plus a2. So, I am just going to replace the variables by ai's because that is the solution. This is a solution, so that means a1 times sigma 1 alpha 1, a2 times sigma 1, remember sigma 1 is fixed sigma 1 alpha 2 plus an so here is where I am going to use the fact that everything after ar is 0. So I am going to start with ar, so ar minus 1 sigma 1 alpha r minus 1 plus ar sigma 1 alpha r is 0. So the point is note that we do not have any terms after the rth term. Because this is because ar plus 1 and up to an plus 1 are all 0. So, if this is r, everything below that is 0, so I do not need to try this later part of this.

So, beyond the rth column, so if this rth column, anything beyond that, is not going to contribute to the equations. So, I will stop with this. So, the second equation, just so that, I mean, I am going to write this just for your clarity, so I have sigma 2 is fixed in this row. So, sigma 2 alpha 1, a2 sigma 2 alpha 2 plus, I am going to write these terms because it will become clear what we do later sigma alpha r minus 1 ar sigma 2 alpha. So now, actually, I should have said this here.

I want to make a further simplification since here or is nonzero, so the last entry in the last nonzero entry in the solution, we can multiply by ar inverse and assume here ar equal to 1. So we can multiply by ar inverse and assume that you ar equal to 1 that is because every time you have a solution, if you multiply by a nonzero if you have a solution to homogeneous linear system of equations, multiply the solution by an nonzero scalar what you get is still a solution. So, multiplying by ar inverse, we can assume that ar equal to 1, so I am going to skip that.

(Refer Slide Time: 20:09)



So, that is what that is a simplification. So, I have simply sigma 1 alpha r, sigma 2 alpha r equal to 0. The last equation, so I have written first second, the last equation will be a1 sigma n alpha 1, a2 sigma n alpha 2 ar minus 1, sigma n alpha r minus 1, and ar is 1, so sigma n alpha r equals 0. So, let us call this star. So, star is the original set of equations applied, I mean, a very, very written in terms of this solution that we have chosen a1 through ar, which is the least number of nonzero entries.

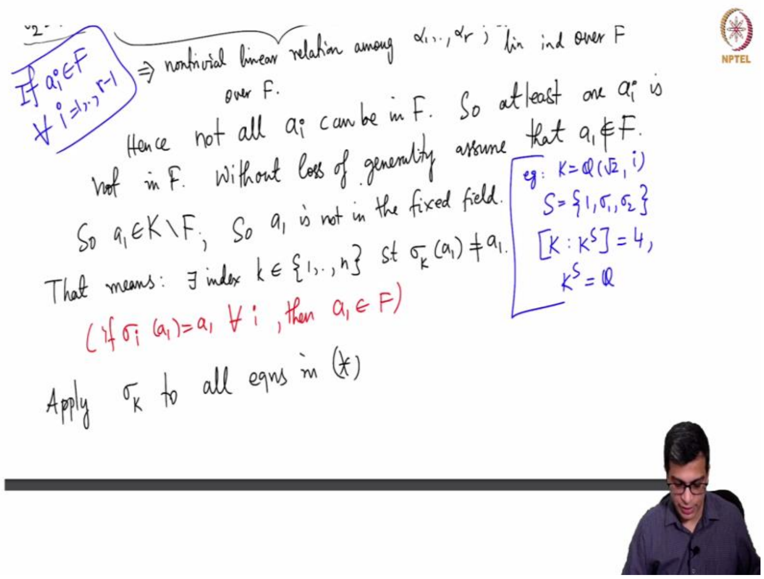
So, just to give you an update about what we will do later, we are going to construct a solution with fewer nonzero entries, and thereby getting a contradiction. So, this is the equations after you plug in the very solution for the variables. Now, I am going to observe a few things here. So, if and just also recall that we have so far not use the fact that sigma i’s for my group, and this is the first place now we are going to use that.

So, the point is so I am going to write it here. Since sigma 1 through sigma n is a group of automorphisms of K one of them is Identity map, one of them is identity. Let us say sigma 2 is identity just for simplicity, and sigma 2 is identity. What is the second equation going to look like a1 alpha 1, a2 alpha 2, sigma 2 is identity. So, a sigma 2 alpha r minus 1 is alpha r minus 1 ar minus 1 alpha minus 1 plus alpha r equal to 0. So, second equation will look like this.

But now remember, here alpha 1 through alpha r are independent. Alpha 1 through alpha n plus 1 are independent, but this is a linear relation, that is non trivial linear relation among, because alpha r has appears with coefficient 1, in fact, all of them are nonzero a1 through ar. So, these are non trivial relation on this, but we know alpha 1 through alpha n plus 1 r linearly independent. So, that means what?

I should have said that this is a non trivial relation. So, I should write if you ai is in F for all i. Otherwise, that is not a relation, non trivial relation among this over F. They are linearly independent over F. So, if they are not enough, there is no problem. But because they are linearly independent over F. They cannot have a linear relation, non trivial integration with coefficients in F. So, if all the F's are in ai is in F, we do get a non trivial relation among all of them.

(Refer Slide Time: 24:00)



So hence, not all your ai's can be in F. So, at least one ai is not in F. So, I am going to simply assume without loss of generality, assume that a1 is not in F. So, a1 is in K, of course, but not in F. So, just a word about why I can choose it to be a1. We know that a1 a2 r minus 1, 1 of them is not in F, because they are all in F, we get a contradiction to the linear independence of alpha i's over F capital F. So, one of them is not F if a2 is not in F, I am just going to interchange and call that a1 I will call a1 a2. So, there is no problem.

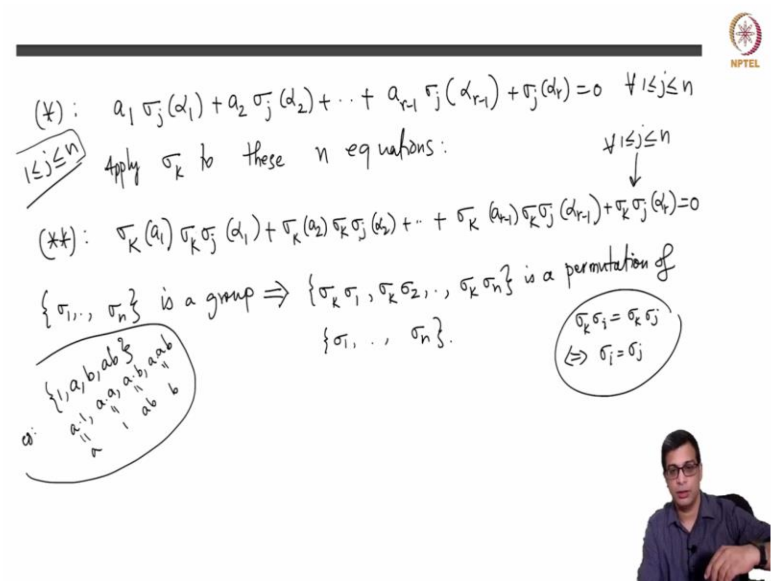
So, just for simplicity, I am going to assume that a1 is not in F. Now, this is the first point where we use the form a group. In fact, we have not used the full force of the group axioms, we have just assumed, we have just used that there is identity. But remember, this is not enough because in the example of K equal to Q adjoint root 2 comma i and s equal to 1, sigma 1 sigma 2 that I mentioned in the previous video, K power s is actually K colon K power s is 4, because K power s is Q.

So, here also there is identity, but still, the equality does not count. So, we have to use more group axioms later on. Nevertheless, let us just assume that for now that a1 is not in F. But if so, a1 is not in the fixed field, a1 is not in the fixed field. So, that means sigma i's of a1 is not equal, they are not all the same elements. So, in particular, one of the elements is identity. So, there exists an index K among the n linear I mean, n homomorphisms such that sigma K of a1 is not equal to a1, because if this is true, I mean, this must be the case because otherwise, they it must be in the fixed field.

So, if a1 sigma a1 is equal to 1 for every K, that means a1 is fixed by all the group elements, sigma 1 to sigma n so there is at least 1 K so that sigma K a1 is not equal to a1. This, you think about this, if sigma K K1 equal to a1 for all K, or let me write it like this sigma 1, sigma i equals a1 equals a1 for all i, then Kr 1 is in the fixed fields. So, that is really what I am saying. So, if that is the case, then a1 will be in the fixed field, which we know is not the case, that means sigma K a1 is not equal to 1 for some K, I am going to fix that K.

And now, the clever thing that we will do is apply sigma K to all equations in star. So, star is this. So, I play sigma K to this. So, unfortunately, I have to go down and write this, but you can pause the video and go back. And I suggest that you take a paper and pen and write all this down and apply sigma K to this. So, I am going to maybe instead of writing all the equations separately, just combine them like this. What is the equations?

(Refer Slide Time: 28:10)



Star can be captured by this star is actually sigma j alpha 1. So, I am going to write j varies over 1 to n. So, j varies over 1 to n. So, I get sigma j a1 rather I get aj see, remember a1 alpha 1 a1 alpha 1, alpha 2 alpha 2, a2 alpha. So, ai? So I, I should write this as a1 sigma j, alpha 1 plus a2 sigma j. So, let me just get this correct, so that I do not make a mistake. So, I get, a1 sigma j alpha 1 plus a2 sigma j alpha 2 r minus 1 to be ar minus 1, sigma j, I skipped something here, sigma j alpha 2 plus ar minus 1, sigma j, alpha r minus 1 plus sigma j, alpha r equal to 0, for all.

So, I am just trying to write all the equations in a single line. So, you vary j equal to 1 to n, you get all the equations, and you put j equal to 1, you get the first equation, you get a1, sigma 1, alpha 1 a2 sigma 1 alpha 2, a r minus 1, sigma 1 alpha r minus 1, which is this and finally, sigma 1 alpha r. If you take j equal to 2, you get the second equation, a1, sigma 2, alpha 1, a2 sigma 2 alpha 2 ar minus 1, sigma 2 alpha r minus 1, sigma r sigma 2 alpha r, which is the last term, if you take j equal to n, you get the last equation.

So, this is just a convenient way of writing all the equations. Now, you apply sigma K to these equations, these n equations. So, I am going to go over 30 minutes for this video, but I want to finish this so, that this will become a self contained video to prove this theorem. So, if we apply sigma K to this, now, I am going to call that star star this looks like this sigma K, sigma K is that fixed K remember that that fixed K which has this property sigma K a1 sigma K is a blue field automorphism. So, sigma K of this will be sigma K of a1 times sigma K sigma j of alpha 1.

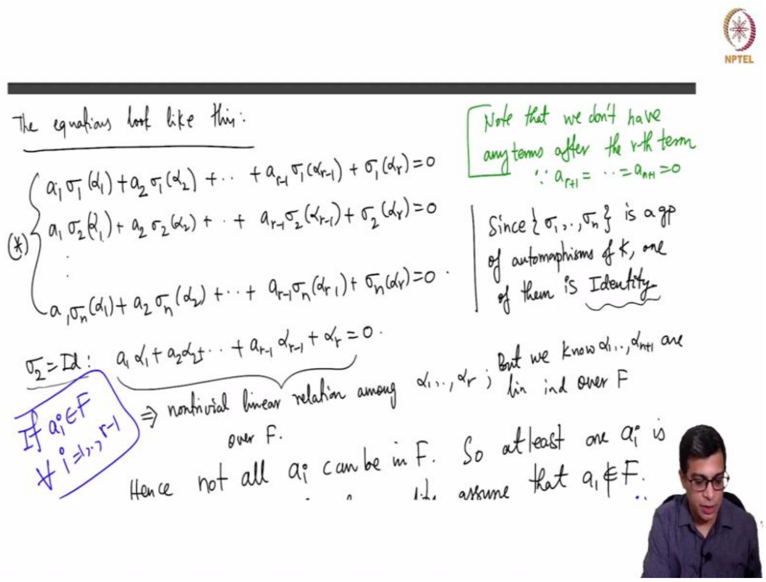
So, that is just composition this is composition, second term will be sigma K a2 sigma K sigma j alpha 2 r minus rth term will be sigma K ar minus 1 sigma K sigma j alpha r minus 1 and finally, sigma K sigma j alpha r equal to 0 again this holds for, for all i for all j between 1 to n. So, j equal to 1 you get all if you apply sigma K to the first equation; j equal to 2, you apply sigma K to the second equation and so on.

So, this is again a compact way of writing really n different and distinct equations. So, I hope this is not becoming too complex or too messy for you, but, if needed, please stop and think about what we are doing here. So, we have now, these equations. Now, this is where we want to use the fact that there is a group earlier we use that there is identity, but now we are going to use more axioms of group.

So, when you take a group, this is some standard things that you have learned in group theory, take a group and multiply all the elements by a single group element. Namely, sigma 1 in our case is a permutation of this. So, if you take a group and you multiply all group elements by a fixed element, you just get the same group, I mean, they are all group elements, but in a different order perhaps.

So, for example, if you take the client for group, so, this is an example, multiply everything by a so, you get a times 1, a times a, a times b, a times ab, but this is a, this is 1, this is ab, and this is b. So, this is just a permutation of the group. So, in general, sigma K sigma i equals sigma K sigma j implies this if and only if sigma equals sigma j, this is the feature of the group because if that has happened, then cancel by sigma multiply by sigma K inverse on the left you get this and if this happens, multiply by sigma K on the left to get this. So, this is just a permutation of sigma i’s. In other words, if you look at star star, sigma k, sigma j is some other sigma j. As you vary K, you get all the group elements.

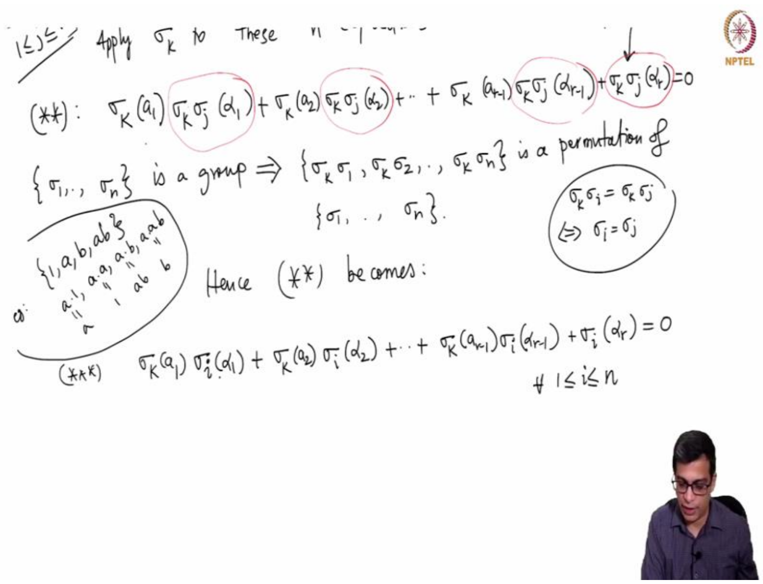
(Refer Slide Time: 33:54)



So, this explaining here, you have let us say 10 elements sigma 1, sigma 2 sigma 10. And K is 5. So multiply sigma 1 the first equation by sigma 5, sigma 5 sigma 1 second equation will be sigma 5 sigma 2, 10th equation will be sigma 5 sigma 10, but sigma 5 sigma 1 will be sigma 6, let us say. So, it will be sigma 6 and sigma 6 will never appear again in the 10 equations, sigma 5 sigma 2 will be sigma something else not sigma 6, it might be sigma 8.

So, sigma 8 will be there, it will not appear again third will be sigma 2 maybe, and the last 1 will be the missing sigma i. So, when really what we have done by multiplying by sigma is sort of interchange the equations. But the first entry will be different, because you are taking sigma K a1.

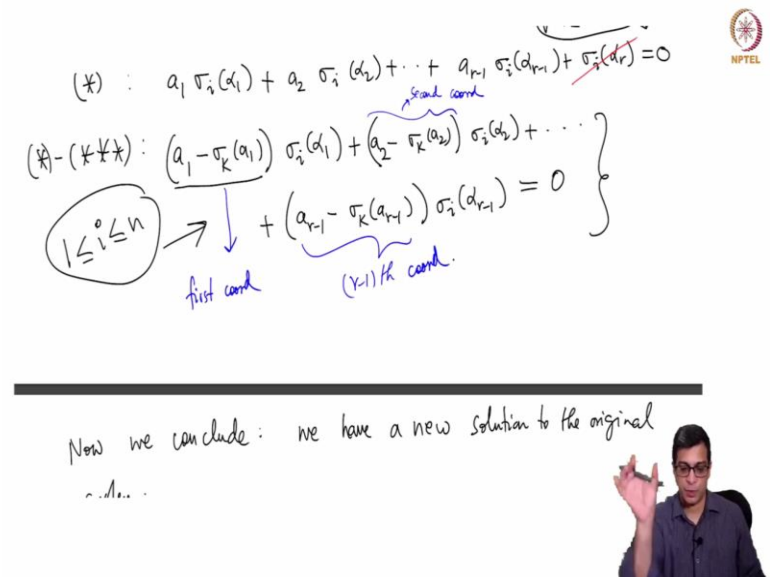
(Refer Slide Time: 34:48)



So, so this star, star becomes. So, basically the upshot is that I do not need to really talk about sigma K sigma j. So, star star becomes triple star which looks like this. So, star, star, star it will be sigma K a1, but sigma K sigma j i replaced by i. So, original order is replaced by a different order, if you just look at these terms. If you look at this term, I am not touching the sigma K a1 those terms this will be sigma i alpha 1 plus sigma K a2 sigma i alpha 2 r minus 1 term will be sigma K ar minus 1 times sigma i alpha r minus 1.

And the last term will be sigma i alpha r equal to 0 where i goes from so, i's are again going from 1 to n, like j's, j's are going from 1 to n, but it is possible a different order. So, I hope this is the really somewhat tricky part, but I hope this is clear. So, we are taking sigma K sigma j, but sigma K sigma j is just another ordering of the group elements. So, I am just using a different letter for the index. So, we have this.

(Refer Slide Time: 36:45)



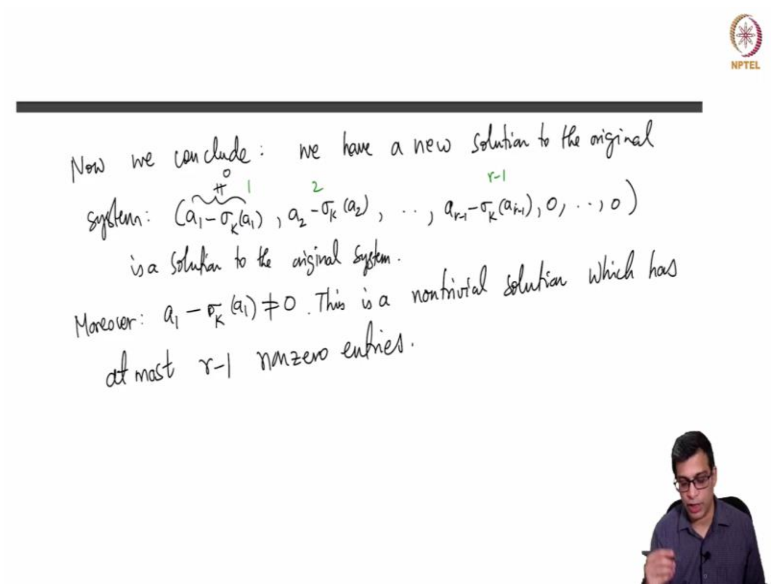
And now I am going to I am going to subtract star minus star, star, star single star minus triple star if I do that, what do I get? So, star was all the way here. So, star maybe I will write star just for in this compact fashion. So, that it becomes clear star is really a1 sigma i alpha 1, a2 sigma i alpha 2 ar minus 1 sigma i alpha r minus 1 plus sigma i alpha r minus alpha r. So, this is star, a1 sigma i a2 sigma i index subscript of a and alpha are same.

a1 alpha 1, a2 alpha 2 ar minus 1 alpha r minus 1, ar alpha r but ar is 1. So, subscript of a and alpha are same the first equation as sigma 1, second equation has sigma 2, third equation has sigma 3, nth equation has sigma n so sigma i. So, again it goes i from 1 to n for both of these. So, now you do star minus triple star so, if you do star minus triple star, we are almost done. So, we are getting there. So, if you do that, again I am going to write the compact form.

So, the first column will have sigma the first equation will have sigma 1 sigma K a1 sigma 1 here it will be a1 sigma 1 alpha 1. So, it will be a1 minus sigma K a1 times sigma i alpha 1. So, sigma i alpha 1 is common. So, you remove that and write sigma K a1 or a1 minus sigma K 1 because you are doing star minus star star star. The second term will be a2 minus sigma K a2 sigma i alpha 2 plus dot, dot, dot r minus 1th term will be ar minus 1 minus sigma K ar minus 1, sigma i alpha r minus 1 and this is the way that we have arranged this the last rounds will go away. Because sigma i alpha r, sigma i alpha r plus there is nothing basically so, that is equal to 0.

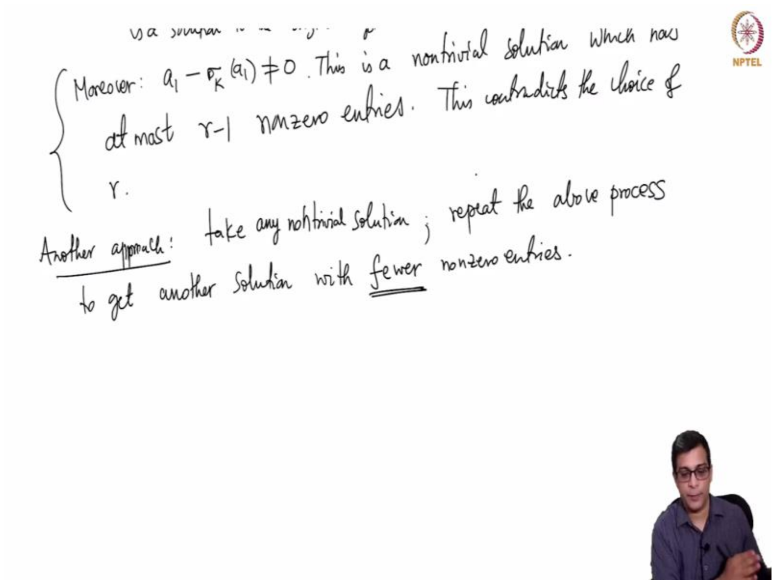
Now, again this is for all i from 1 to n. So, again I invite you to just write down all of them if needed. There any questions? Now, stare at this carefully. Now, what we get is we conclude a new equation new solution to the, a new solution to the original system. What is the new solution? New solution has only r minus 1 terms now, this is the first coordinate of the new solution, this is the second coordinate of the solution, this is r minus first coordinate, because if you plug this in the column vector corresponding to the variables, you get exactly the solution because sigma i alpha 1 sigma i alpha 2 sigma i alpha n plus 1 is the row in any particular row. So, when you multiply that with this entry this vector you get the solution.

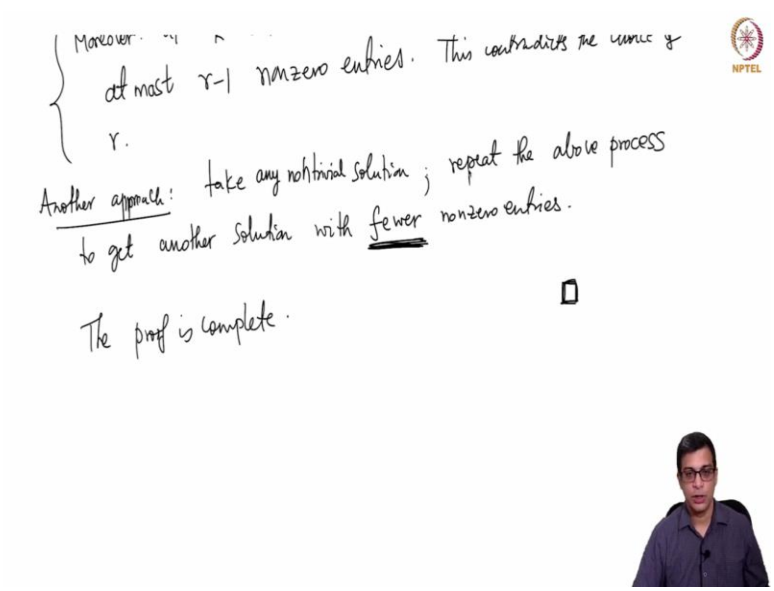
(Refer Slide Time: 40:54)



So, that means solution is a 1 minus sigma K a1, a2 minus sigma K a2 all the way up to ar minus 1 minus sigma K ar minus 1 comma 0, 0, 0. So, this is a solution to the original system. Moreover, a1 minus sigma K a1 is nonzero that we assumed that is how we chose K. So, the first entry is nonzero. So, that means, this is a non trivial solution which has at most r minus 1 nonzero entries, because this is 1 first 1, second 1, r minus first 1.So, there are at most r minus 1 maybe even this is 0 I do not, I do not care but it cannot have more than r minus 1 nonzero entries.

(Refer Slide Time: 42:13)





This contradicts because remember and r was chosen so that you have the least number of 0 nonzero entries in any solution is r. So if you do not like this contradiction method, what you can really interpret what we have done is you take any solution non trivial solution, take any non trivial solution. So, another approach take any nonzero solution repeat the above process to get another solution, take any non trivial solution and repeat the process to get us another solution with fewer nonzero entries.

Another interpretation of this is we originally started with a solution with r entries, r nonzero entries, these are all 0 and 2. So, these n plus 1 minus r 0 entries, we started with a solution with r positive nonzero entries, and ended up with r minus 1 nonzero entries or less, in fact. So, we can always start with maybe there are 100 nonzero entries, repeat this process to get it down to 99. Repeat it again to get it down to 98. And keep all the way to get it to 1. And once it is 1, we get a contradiction directly. So, that is another way to read this proof.

So, take any solution which is non trivial. Repeat the above process of rearranging equations, applying sigma K, and so on to get a solution with fewer nonzero entries. And repeat it, because it is a finite vector, eventually, you will get 1 nonzero entry which will give you the contradiction. So, the proof is complete. Theorem 1 talks about some lower bound on the degree of the field over the Fixed Field. Theorem 2, if you assume that they form a group, then it gives you an exact equality. So these 2 statements are critical for us.

We will repeatedly use them throughout the course, and the proofs are beautiful. So, please make sure that you understand the proof. And if you have any questions, please feel free to ask doubts, but really, there is nothing more than elementary linear algebra here. So, I hope you carefully follow this and work it out yourself if needed to understand the proof. So, let me stop this video here and in the next video, we are going to now make use of these very important theorems and study Galois theory. Thank you.