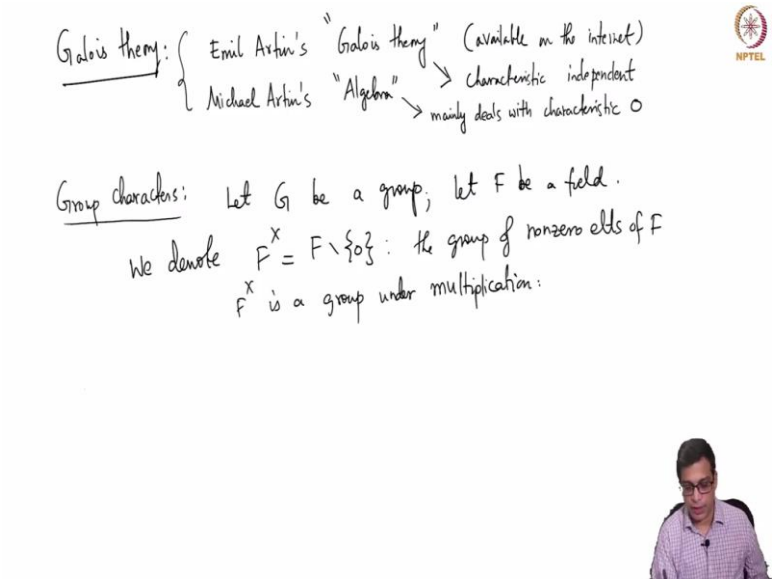
Introduction to Galois Theory
Professor. Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute
Lecture No. 10
Beginning of Galois Theory

Welcome back, in the last few videos, we did some problems which illustrated the notions that we recalled from Groups Links Fields.

(Refer Slide Time: 00:24)



So, now we are ready to start the main component of this course on Galois theory. So, the rest of the course is going to be focused on proving the main theorem of Galois theory and its and learning about its applications that we mentioned at the beginning of the course. So, before I start, let me just give you a couple of remarks on the references. So, the main reference for me, in the beginning of this, of this Galois theory part is a book by Emil Artin's called Galois theory.

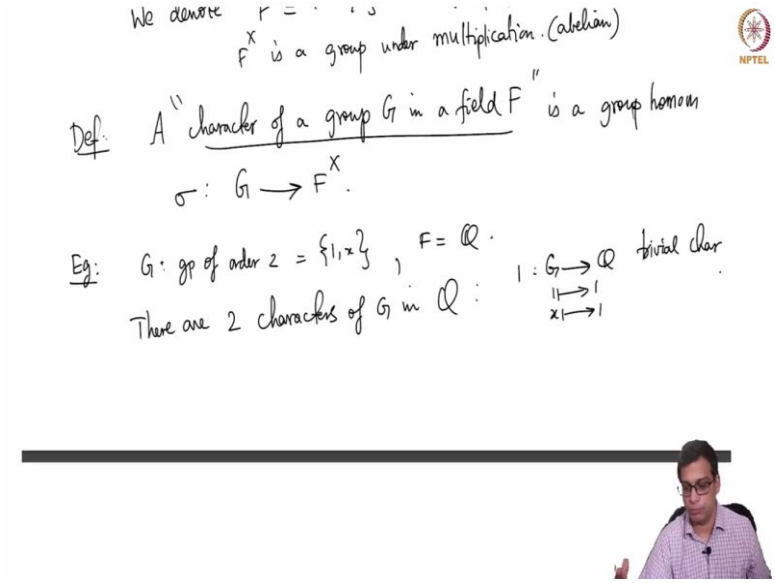
And we are also going to refer regularly to Michael Artin's book Algebra. So, this is available, I mean, this is available on the internet. It is a very small book, less than 100 pages, it only deals with Galois theory and it is actually a very nice reference for Galois theory. And Michael Artin's Algebra is a much more comprehensive introduction to algebra and covers all the topics in basic abstract algebra. And we will deal with the chapters on in this book that deal with Galois theory.

But the reason I want to develop the main theorem of Galois theory using a Emil Artin's book, Emil Artin's is by the way, the father of Michael Artin. And the reason I want to use the Father Artin's book is his treatment is characteristic independent. Meaning, it works for any field of any characteristic, whereas Michael mainly focuses on characteristic 0. So, I will come back to Michael Artin's in his book later and take some components from some theorems from there. But to set up the main theory, I want to use a Emil Artin's book because it is much more general and I think it is done in a more conceptually clear manner.

So, in order to do this in the way of Emil Artin, so I want to introduce an important notion for in Group Theory, called Group Characters, I want to emphasize before I define these, that I am not going to study group characters, I will define them prove exactly one result about them. And then we will not refer to Group characters again. And that result is going to be useful for us, it is essential. In fact, it is extremely critical for everything that we do later. So, if you are not familiar with Group characters, it is absolutely fine. All I need is a definition I am going to give now and the result that I will proof after the definition.

So, let G be any group and we use multiplicative notation for an arbitrary group, because we do not know that it is Abelian and let F be a field. We denote the, the nonzero elements of F by F cross or F star, the set of nonzero elements or the group of nonzero elements. Remember that this is a (multi) group under multiplication, that is the definition that is part of the definition of a field. There is an identity element and every element has an inverse.

(Refer Slide Time: 03:59)

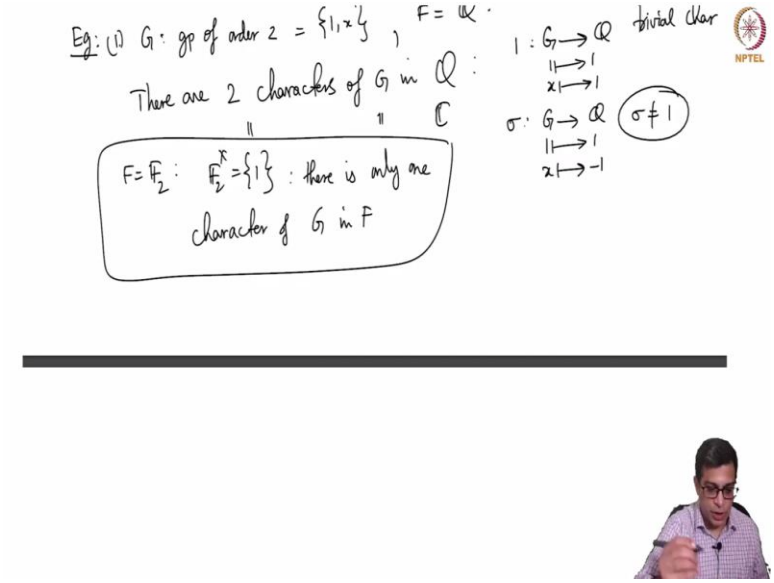


It is in fact, Abelian group. That is also part of the definition of a group of a field. So, now the definition of a group character. So, a character of a group G in a field F. The definition is very simple. It is character of a group in a field F, both G and F are important is simply a group homomorphism. Let me denoted by sigma. That is all. So, character is simply a homomorphism from the given group G to the multiplicative group of nonzero elements in a in a given field.

So, that is all examples. So, I as I said, I am not going to discuss the general theory of characters of a group. I am only interested in it for a very, very special case. So, once I define this give a couple of examples and prove the only theorem that I will prove about characters, I will stick to fields. So, if you are unfamiliar with this, there is no problem. So, let us just I mean, we will develop this from first principles.

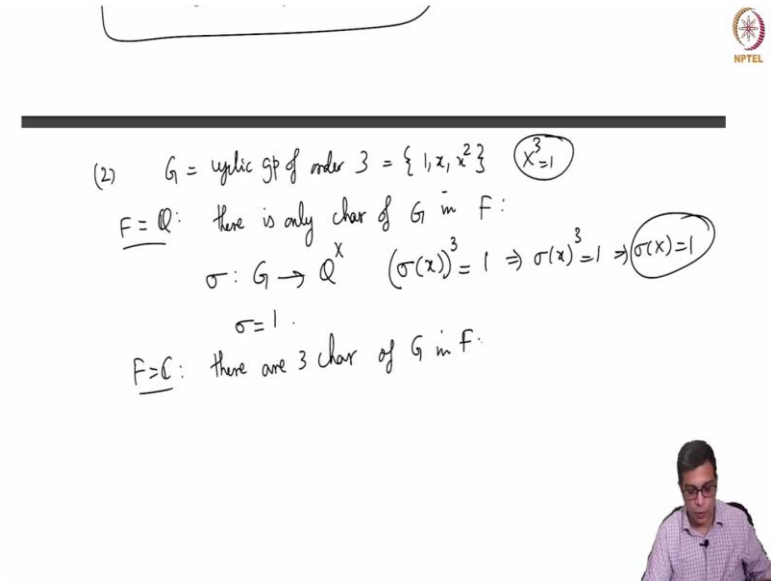
So, this is a character. So, if you take for example, cyclic group of order 2 group of order 2 in fact, I can say. So, we can use 1 comma x for it, so, it is a cyclic group, right x square is 1 and F to be that is a Q, I claim there are 2 characters of G in Q. Namely, 1 is 1 itself, so, I take G to Q send 1 to 1. X1 that is the identity I mean the trivial character. First, everything goes to 1 that is a valid group of homomorphism

(Refer Slide Time: 06:00)



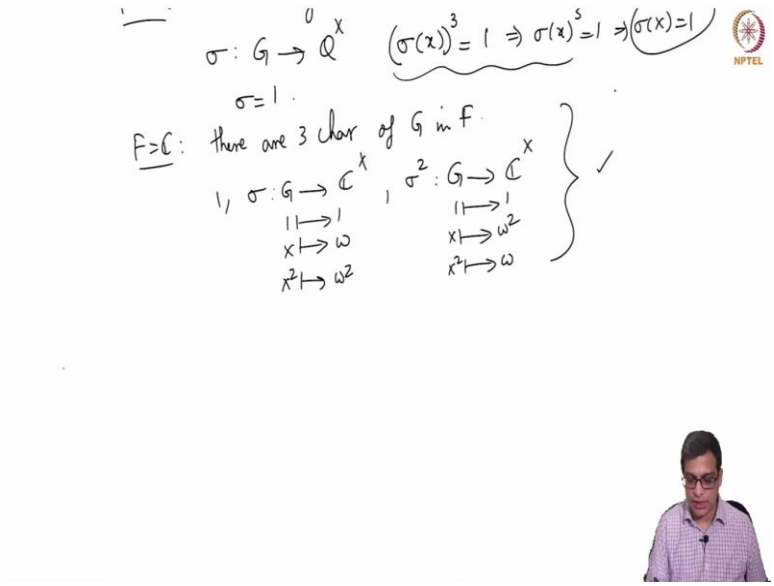
The other 1 sends 1 to 1 of course, because identity has 1 identity, but x to minus 1. So, sigma is of course, not equal to 1 has functions that are distinct. And if you change Q to C, there will still be 2 characters. So, so far there is nothing else so, in Q or C or in fact, if you take another and final field, so, let us say F is F2, then F2 cross is actually just 1. So, there is only one character. So, that is a special case. So, if any character must be the trivial constant map, so, that is the first example.

(Refer Slide Time: 06:54)



So, let us look at now cyclic group of order 2 of order 4 or order 3 rather does not matter what I order 3. So, here I denoted by 1 x, x square. So, if I take F to be Q, there is only 1 character G and F this is because, if you take G to Q cross so sigma is any character what can be sigma x? Sigma x power 3 must be 1 because x cube is 1 that is because x is a generator of this group order 3. So, sigma x cube is 1 that means, sigma x cube is 1, but what are the rational numbers which have this property only 1, so, sigma x has to be 1. So, sigma is the trivial character. On the other hand, if you take F to be C there are 3 characters.

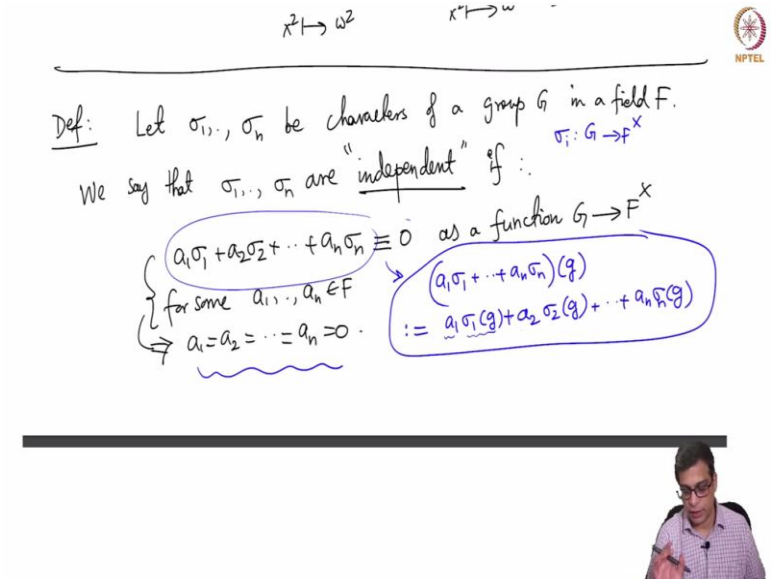
(Refer Slide Time: 08:06)



So, here of course, you can take 1, you can take to be so, 1 goes to 1 x goes to so, this, this relation really says that it must go to a root of unity third root of unity. So, I can send it to omega and x square will go to omega square and I also get another one by taking sigma square and you will understand why I call it sigma square. So, x can go to omega square then x square go to omega.

So, in fact the character characters form a group and if you take characters in C star that gives you if G is inside the cyclic group the characters from another cyclic group which is isomorphic to the group you started with, started with the cyclic group of the same order. So, all that is irrelevant for us for now. So, this is just to give you an idea of characters as I said, we are not interested in the study of characters of a group.

(Refer Slide Time: 09:02)

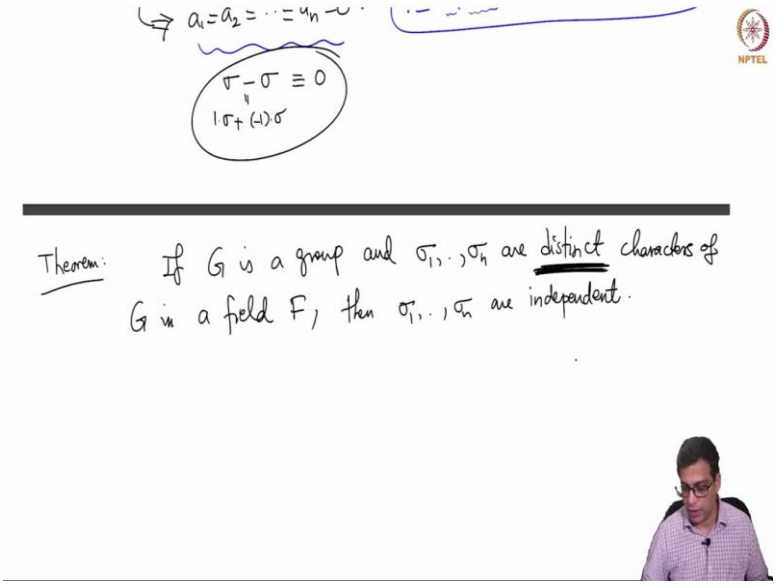


So, let me now give the important definition that I want to make use of so, we will say that lead sigma 2 sigma n can be characters of a group G in a field F. We say that sigma 1 to sigma n are independent. So, we are defining what is the meaning of independent characters if the following holds. a1 sigma 1 plus a2 sigma 2 plus an sigma n is identically 0 as a function of from G 2 F cross for some elements from the field implies, this implies a1 equal to a2 equal to an equal to 0.

Remember that so, let me just briefly explain this what is the meaning of this? Sigma 1 to sigma n are all functions from C to F cross. So, if you think of this as a function it is clear what I mean. So, a1 sigma 1 plus an sigma n or some group element is nothing but a1 sigma 1 of g times so, I take here 2 sigma 2 so, these are functions so, so, I add in the field F is a field so, a1 sigma g plus a2 times sigma 2 g plus an times sigma ng.

So, this remember is a field element. a1 is a field element so, I can multiply them they are all field elements and we can add them so, that is the meaning of this being identical I mean this is a function it means identically 0 means is equal to 0 for all g. So, then the only possibility is that all the coefficients are 0. If the coefficients even 1 coefficient is nonzero then the this linear combination cannot be 0 function that is a meaning of an independent set of characters. Now, this is the definition of characters and their independence.

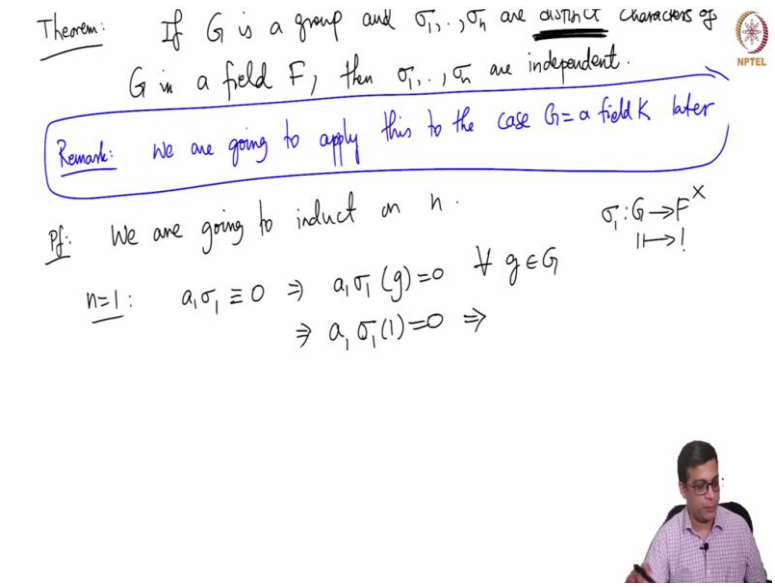
(Refer Slide Time: 11:57)



Now, as I said the only theorem that I am interested in about group characters is this, which is going to be the main theorem for us and this is something that we constantly use not only the statement, but the proof is very important. So, please pay close attention to this and it is very simple standard manipulations involving functions. So, it says that if G is a group and sigma 1 to sigma n are distinct characters of G in a field F, then sigma 1 to sigma n are independent.

So, any set of distinct characters are independent always. Remember I have to take distinct because if I take sigma is a character, sigma minus sigma, so, that means 1 time sigma plus minus 1 times sigma is identically 0. So, sigma x sigma are clearly not independent, sigma is not independent with itself. So, you need in distinct, obviously, that is a necessary condition. But that is also sufficient. If you take distinct characters of a field of a group in a field, then they are independent.

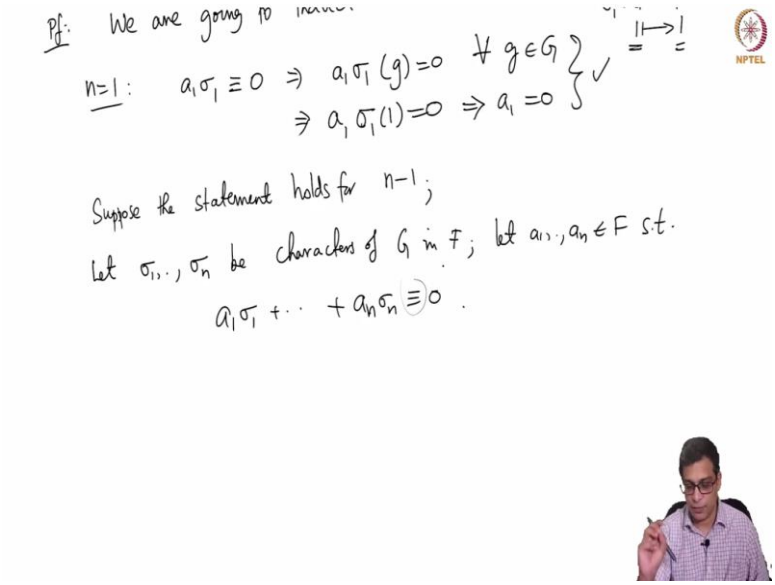
(Refer Slide Time: 13:20)



So, let me remark this here because it might look like this has nothing to do with fields. So we would apply this later. So, as I said, I am not interested in the more general theory of characters of a group, but I am only interested in the case that we have G is also a field, G is also a field and we are going to look at characters of that in another field. So, that is the reason we are doing this. So, I wanted to explain that before we start the proof, so, we are going to do induction on so, we are going to induct on, so, as I said, this is a very simple proof which you would have seen in various courses including some linear algebra courses.

So, first of all n equal to 1. So, that means you have a single character and suppose a1 sigma 1 is identically 0. That means a1 sigma 1 of g is 0 for all G. But that means a1 sigma 1, 1 is 0 g contains the identity element. But sigma 1 of sigma 1 of sigma 1 is a function from group homomorphism from F, G to F cross 1 goes to 1.

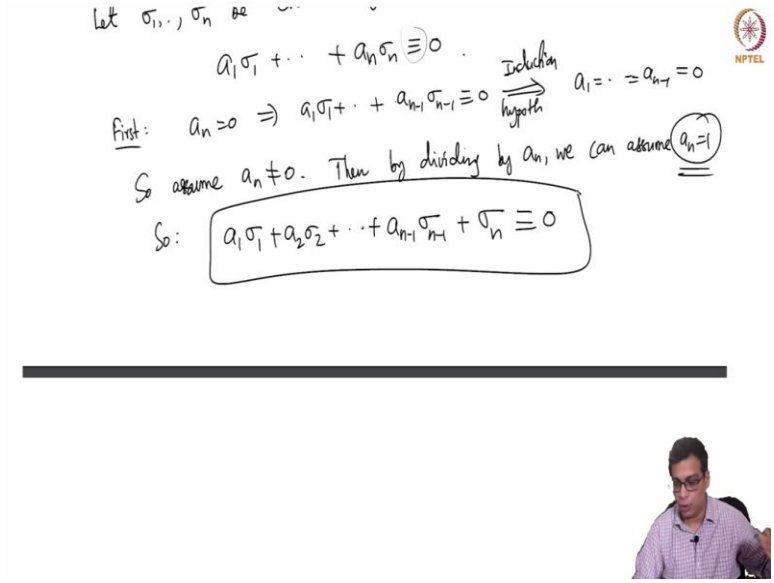
(Refer Slide Time: 15:04)



I am being sloppy here, I am using the letter symbol 1 to denote the multiplicative identity of G and also the multiplicative identity of the field F. But a1 sigma 1 of 1 is 0 means a 1 itself is 0. So trivial to prove for n equal to 1. So, suppose the statement holds for n minus 1. So, and we are going to prove it for n. So, let us take now, n characters, so let the characters, G in F, let a1, a and b field elements, such that a1 sigma 1 an.

Remember I am putting 3 bars here, here, I am putting 3 bars. Here, I am putting 3 bars to indicate the fact that this is not an equality of elements of a field. This is an equality of functions. So, this is the 0 function as a function of G to F cross.

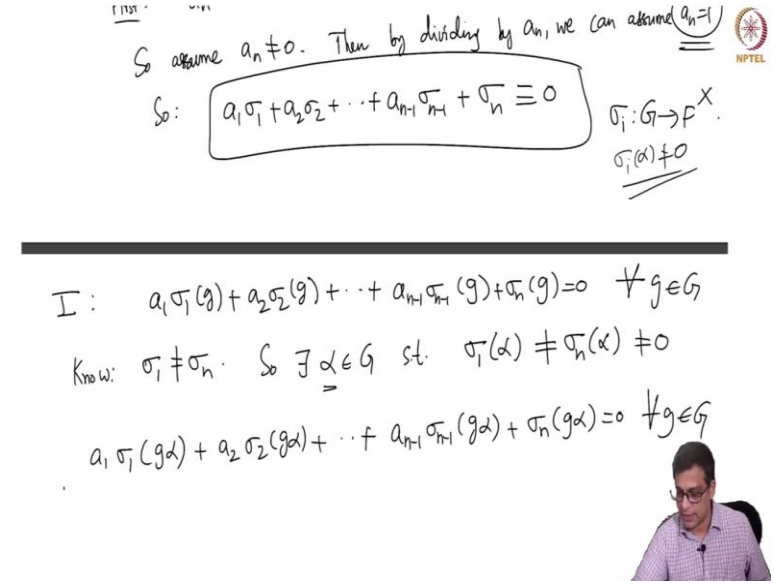
(Refer Slide Time: 16:14)



So, first I know that if n is 0, then we have a1, sigma 1 plus an minus 1, sigma n minus 1 is 0, then by induction hypothesis, a1 to an minus 1 are 0, because any n minus 1 characters are independent, they are all distinct, then they are all independent. So, so, assume an is nonzero, then by dividing we can assume, so, we have a relation by multiplying by a scalar the equality of functions holds. So, we divide by an strictly speaking, I should call them by an prime or something, but to keep the notation simple, I just call the new coefficients by ai's and then I assume an equal to 1.

So, we have a1 sigma 1, a2 sigma 2, an minus 1 sigma n minus 1, plus sigma n is identically 0, that means, if applied to any group element, you get the 0 as an answer.

(Refer Slide Time: 17:38)

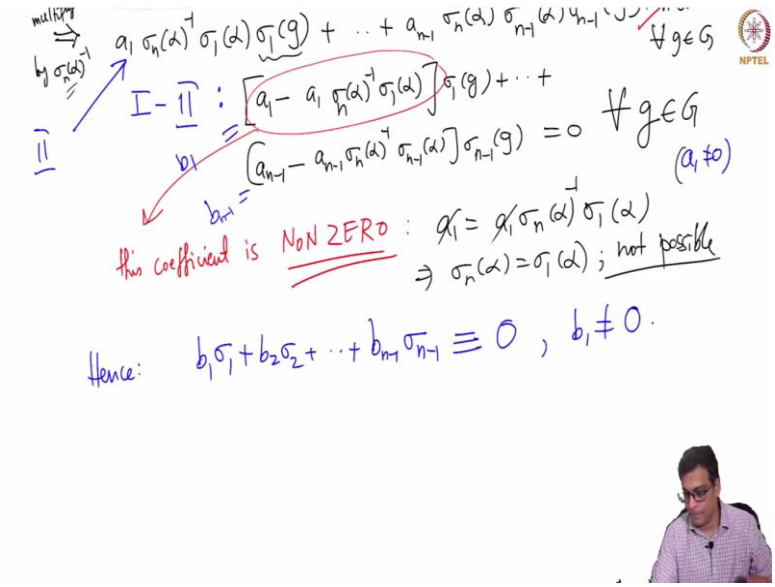


So, that means, so I am going to spell this out. So, first equation is a1 sigma 1 g plus a2 sigma 2 g an minus 1 sigma n minus 1 g plus sigma n of g is 0 for all g in the group G. So, this is the first statement, we now know, we know from the beginning that sigma 1 is not equal to sigma n, so, there exists a group element. So, let us call that alpha such that sigma 1 of alpha is not equal to sigma n of alpha. Remember I am taking distinct characters that means are distinct functions.

So, sigma 1 sigma n are distinct so, when I say distinct I mean any pair of them is distinct, they are mutually distinct. So, sigma 1 sigma n are distinct that means, they differ at least one group element. So, sigma n alpha is not equal to sigma 1 alpha. So, I am going to fix such an alpha and then I have this statement sigma 1, a1 sigma 1 alpha g alpha plus a2 sigma 2 g alpha an minus 1 sigma n minus 1 g alpha plus sigma ng alpha is 0 for all g in G. So, this is of course, true also.

So, as you can see, I am just going towards cancelling some term by subtracting 2 equations like this. So, this gives me so, by just multiplying by sigma n alpha inverse, so, sigma n alpha is nonzero of course, because alpha is a group element sigma is are all functions from G to F cross. So, sigma i of alpha is nonzero.

(Refer Slide Time: 19:45)



Because it lands in nonzero elements of f. So, I can multiply by sigma n alpha inverse. So, I get a1 sigma 1 alpha inverse sigma 1 alpha sigma 1 g. So, this is what I get second term is whatever it is I will write the n minus 1 term. So, I get an minus 1, sigma n alpha inverse sigma n minus 1, alpha, sigma n minus 1 g. So, that is the second last term, what happens to the last term? Last 1 is sigma n g times sigma alpha and multiplying by sigma n alpha inverse, so, I get sigma n g I will write that out here, sigma n g is 0 for all g in G. So, I am going to call this 1, I am going to call this 2.

So, what I have done is I have looked at this equation here, multiplied by sigma n alpha inverse, that has the effect of making the last term, just sigma n g. And other terms become more complicated. Now, what I do is, I am doing 1 minus 2, I believe, because I have sigma n g, sigma n g. So now do 1 minus 2. So, 1 minus 2. So, now the last term goes away, so the last term is this. So, this becomes maybe messy, but once you pause the video and just look at this screen carefully, you will see what I am doing.

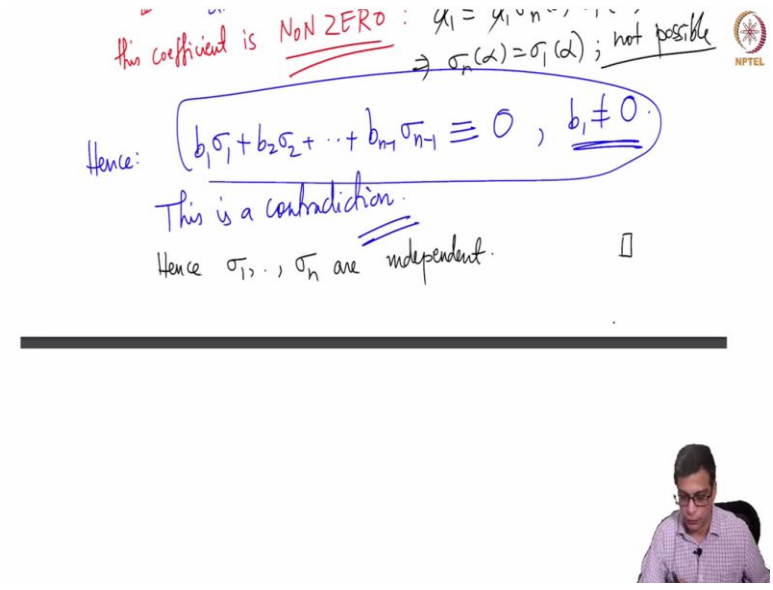
So, if I subtract, I do not care, I mean, the remaining terms will become quite complicated, but let us write down what they are. So, what we have is the first time will have sigma 1 g, sigma 1 g, but coefficients are different. So, it will be a1 minus a1 sigma 1 alpha inverse sigma 1 alpha, I made a mistake here. So, this should be sigma n alpha inverse. Because that is the element I am multiplying with. sigma n alpha inverse this whole thing multiplied by sigma 1 g. So, that is a

first term, second term and so on the n minus 1 term, last term will go away n minus firth term will be an minus 1 minus here an minus 1 sigma n alpha inverse sigma n minus 1 alpha times sigma n minus 1 g is 0, the last term is 0. So, that last term goes away.

Now, we have this is true for all g, that is a point and the point now is this coefficient, this coefficient is nonzero by the choice of alpha. Why is that? Because if this coefficient is 0, then a1 equals a1 sigma n alpha sigma, sigma alpha inverse sigma 1 alpha, but a1 is nonzero, we are going to assume that all the coefficients are nonzero of course, because even if 1 coefficient is nonzero, then we have a coefficient of n minus 1 thinks and we are done by induction, this implies of course, this implies sigma n alpha is equal to sigma 1 alpha.

Because we can cancel this and pull this, this is not possible. This is not possible and hence, this is nonzero. So, you have now whatever this is, I am going to call this b1. So, call this b1 call this b n minus 1. So, you have all the things so hence, we get b1 sigma 1 plus b2 sigma 2 plus b n minus 1 sigma n minus 1 is identical is 0 and n1 is nonzero. This is a contradiction.

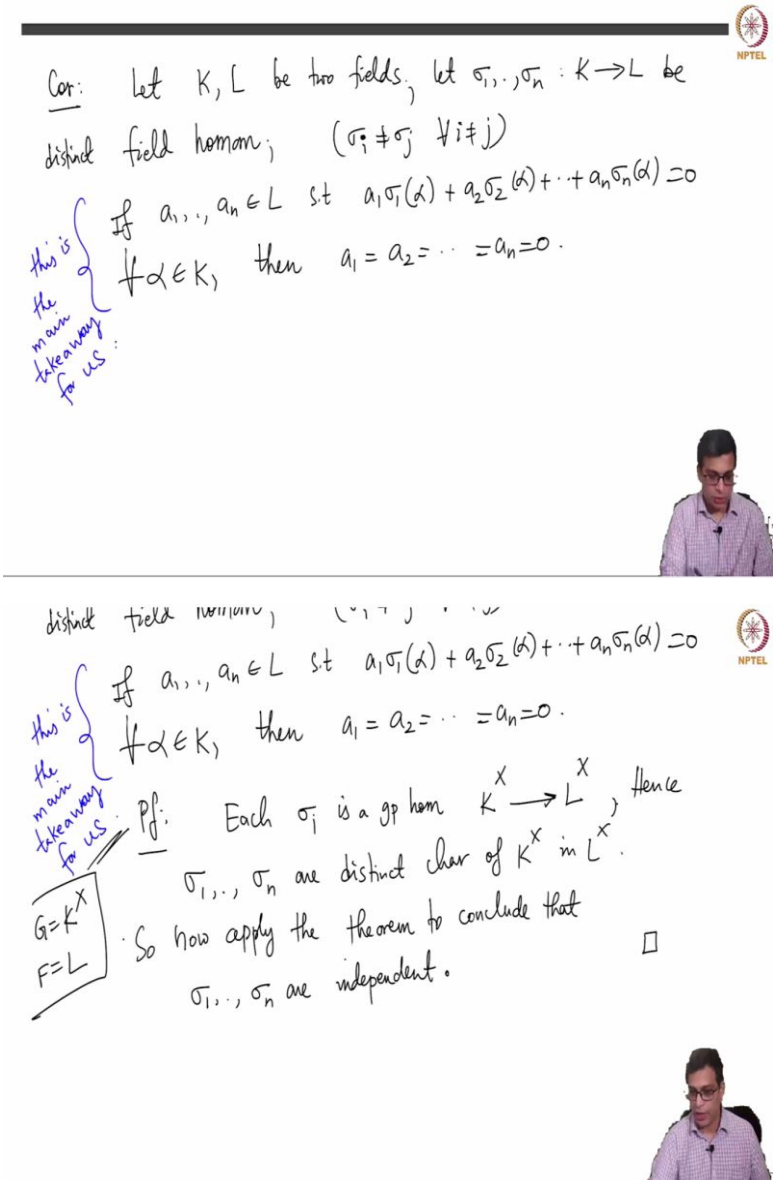
(Refer Slide Time: 24:10)



Because we have already assumed as part of the induction hypothesis that any n minus 1 group characters which are mutually distinct or independent, but here we have a relation with one of them nonzero and the relation is identical is 0. So, this is the contradiction. So, somewhere we have assumed that something somewhere we have assumed something wrong, and that wrong thing is that an is nonzero.

So, if n is nonzero, logically proceeding with the given data, we get a contradiction. So, hence sigma 1 to sigma n are independent. So, that completes the proof. So, the proof of this is also important as I said the statement is important and the proof is also important.

(Refer Slide Time: 25:07)



So, let me end the video by stating the corollary that we are going to mainly use. So, let this corollary is what you should take away from this video. Let K and L be two fields, let sigma 1 so, I am going to strip the language of character from this let sigma 1 to sigma n be field homeomorphisms are distinct field homeomorphisms. So, no two are distinct, same sigma i is not equal to sigma j for all i not equal to j that is what I mean by distinct.

Then so, basically what I mean is if a1 through an are elements of L such that a1 sigma 1 of alpha plus a2 sigma 2 of alpha plus an sigma n of alpha is 0 for all, all alpha in K, then a1 equal to 0, a2 equal to 0 and more generally an equal to 0. So, remember I am stripping this from the stripping from this the language of characters. So, this is the, the main takeaway for us. So, as I said I will never not talk about characters, characters are only needed to prove this very important theorem.

And it this is an important theorem which has lots of applications in Group Theory, but I am only interested in this as I said four characters of a group or other field homomorphism's like this. So, what is the proof of this? Each sigma i see, remember sigma i's are field homomorphism's that means, they are they are thought of as they are a group homomorphism's they respect the addition and multiplication. So, each sigma i is a function is a group homomorphism K cross L cross because sigma i sends to, sigma i sends 0 to 0. So, if you remove 0 K cross any nonzero element must go to nonzero element.

Hence, sigma 1 through sigma n are distinct characters of K cross in L cross. So, now, apply the theorem to conclude that see K cross is a group. So, basically we are applying with K cross equal to G or G equal to K cross F equal to L. So, they are distinct characters of G in L cross in L. So, apply the data to conclude that sigma 1 to sigma n are independent. So, now that means that if this relation holds that means a1 sigma 1 plus a2 sigma 2 plus an sigma is identically 0, then the coefficients are 0. So, that is all. So, the corollary is a special case of the theorem. And that special case is the main takeaway for us and that is what we are going to use.

Let me stop this video here. In this video, we started our study of Galois theory by looking at group characters and proving a very important theorem about group characters. And the end of this video I mentioned this corollary, which is the corollary that we are going to use crucially, and the proof of the theorem is also important. You are going to see similar arguments repeatedly in the course. So, let me stop the video here. And in the next video, we are going to continue with this study of Galois theory. Thank you.