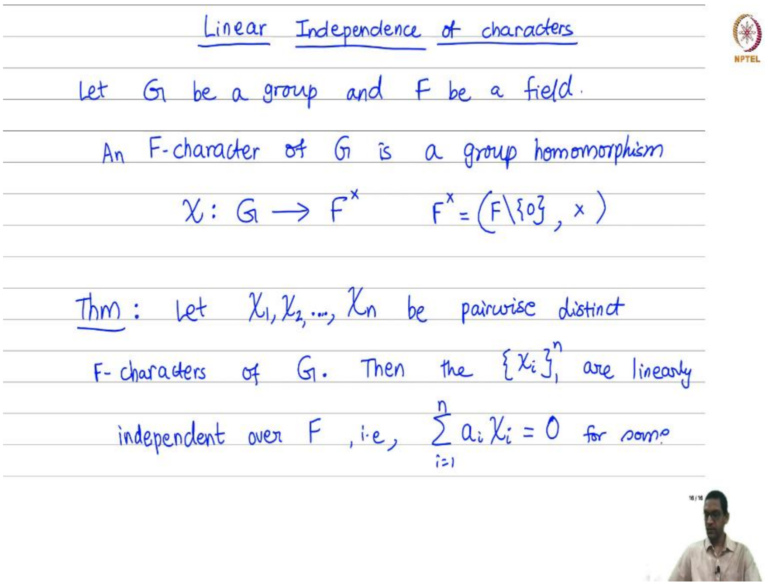
Algebra II
Professor S Viswanath
The Institute of Mathematical Sciences
Lecture 31
Linear Independence of Characters

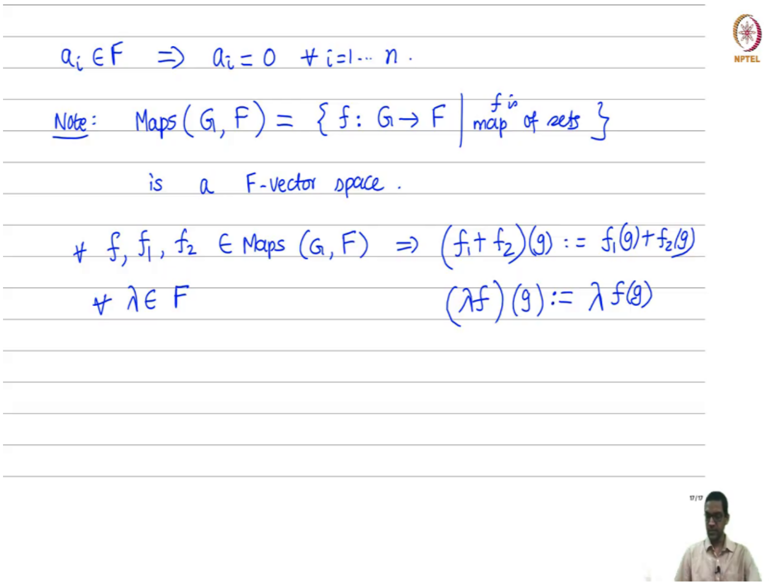
(Refer Slide Time: 00:16)

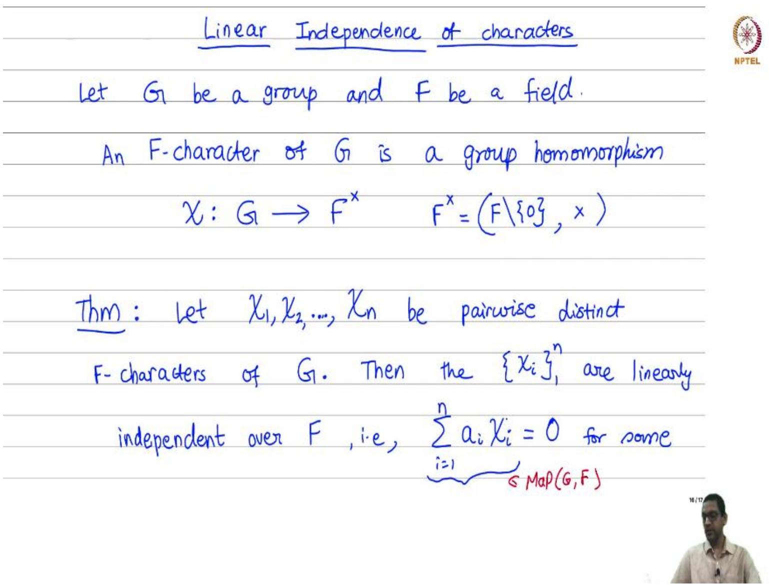


Today we will take a short detour and talk about Linear Independence of Characters. So here is the, here are the definitions; so, let G be a group not necessarily finite and F a field. So, by a character will mean the following or maybe just to emphasize the field an F character of G is a group homomorphism let us call it chi from the group G to the group F cross, which is the multiplicative group of the field. So, this is the field, delete the origin. Think of it as a group under the multiplication.

So, this is a definition of an F character, just a group homomorphism from G to the multiplicative group of the field. And here is the theorem says that, if I have a collection of characters chi 1, chi 2, chi n. Let us say chi 1, chi 2, chi n be pairwise distinct characters, F characters of a group G, then the chi i are linearly independent, 1 to n are linearly independent over F. So, what does that mean? In other words, if I take a linear combination, so other words if I take summation ai chi i equal to 0. So, what are these now? Chi i's are all interpreted as functions from the group G to the field F. And when I say summation, I just mean point wise summation for some ai.

(Refer Slide Time: 03:05)





So, this is 0 for some elements ai of F, then this implies that all the ai's must be 0. So, this is the usual definition of linear independence. The only little thing that requires explanation here is what we mean by this this summation. I know what do you mean by a linear combination of characters? So, note, what we are probably thinking of is the following vector space. So, let me just call it maps from G to F. What is this?

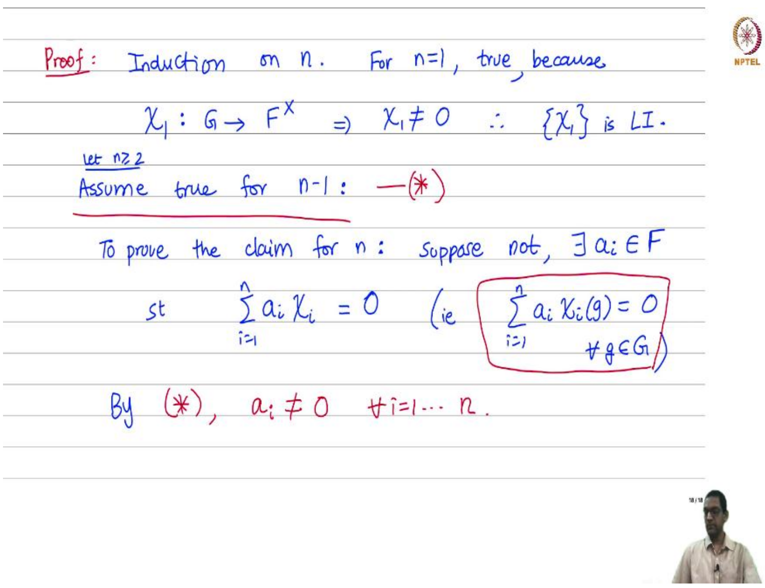
This is just all functions, set maps, do not put any further structure on anything, look at all set maps from G to F, just a map of sets, such that F is a map of sets. So, this collection of all maps is in fact, is a vector space in the F, is a F vector space. What I mean is I have a notion of addition and scalar multiplication which satisfies the axioms. How do you add two maps?

Well, you just add them point twice. So, how do you add to have f1 and f2, which are both maps.

In fact, I do not even need G to be a group for all this, any set will do. Then I define f1 plus f2 pointwise to be just this and how do you scalar multiply f, f1, let us here also use f. So, if I multiply f by a scalar lambda from the field f, this is just I apply f to g, it is now an element of the field f and I multiply it by lambda. So, this is now for all lambda in F. So, these are the definitions, this is how addition and scalar multiplication of maps are defined and under these, I mean it is easy to check that with these definitions, it forms a F vector space.

And so, when we say linear independence here, what we mean is, this linear combination is thought of as an element of this vector space of maps. So, think of this as a now map from G to F, which is basically pointwise linear combination on every element of the group G, you just have to compute summation ai chi i of G. So, in this vector space, this is a set of linearly independent elements. That is the content of the (()) (5:36).

(Refer Slide Time: 05:45)



So, let us prove this now. So, the proof is by induction on n. So, I am just going to do this by induction. So, for n equals 1, this is trivially true. Why? Because a single character, so if I only have one character chi 1, then that character is not 0. A character is definitely a nonzero map. Why? Because its range is actually inside F minus 0, because chi 1 is such a map, therefore chi 1 cannot be the 0 map.

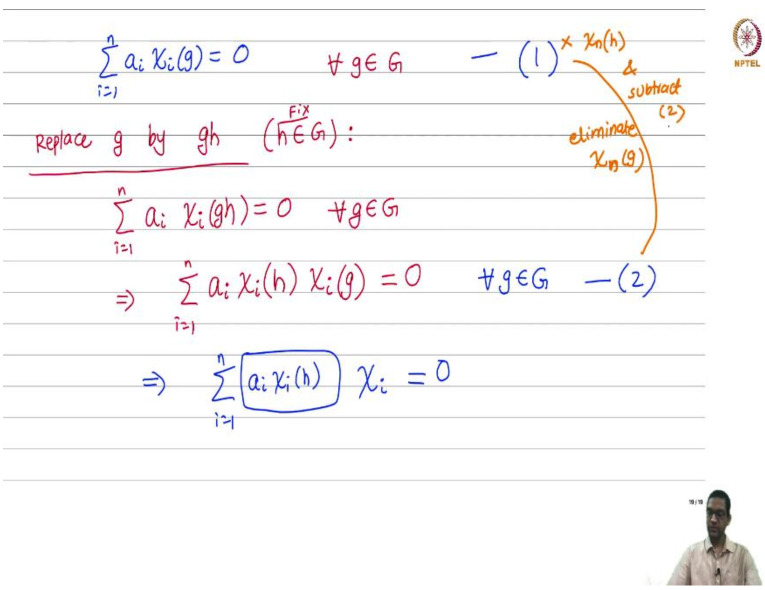
The 0 map is the one which takes all the elements of the group to the element 0 of the field. So therefore, chi 1 itself is linearly independent. Let us put LI for linear independence. So now let us assume that this is, this holds for n minus 1, assume induction hypothesis that assumes this is true for n minus 1. So, let us take n to be at least 2 for this. So, when I say assume true for n minus 1, I mean for any collection of n minus 1 characters, any collection of n minus 1 characters is assumed to be linearly independent.

And now we need to show that any collection of n characters is also linearly independent. So, suppose not, so, to prove the claim for n, let us proceed by contradiction. Suppose not what does that mean? It says that there exists some linear combination which is 0. So, there exists scalars, that are elements ai in F such that this linear combination ai is 0. And we call what that just means is the pointwise sum ai chi i of g, it gives me 0, for all group elements G.

Now, observe that because of the induction hypothesis that every n minus 1 among these n are linearly independent. So, by the induction hypothesis, maybe we will give it a name. So, we will say since this, so I will call this star the hypothesis by the induction hypothesis, what we conclude is that none of the ai's can be 0. Because even if one of them is 0, what you would obtain is a linear dependence relation among n minus 1 or fewer of these chi i's, but we know that no n minus 1 are linearly dependent.

So that is the, that is the conclusion. All the ai's are nonzero. That is what we have. Now, let us see. So, this little relation here is what we need. We know that this linear combination is 0. And what we are going to do is to substitute in place of g, we will substitute gh. So let us keep this in that, just copy.

(Refer Slide Time: 09:17)



So here is what I know to be true. So let us, this is true for all g in G. So, in particular, it is true if I replace g by the element gh. So, I am going to replace g by gh, h is some element of the group, I do not care. Pick any element, replace g by the element gh. So, what do we get? Well, I get the new relation, ai chi i of gh is also 0. And I think of g as sort of varying here. I will fix h, fix h and let think of g as varying across the elements of the group.

So here is my my relationship. And what does this imply? This says that, well, I have to use somewhere that chi i is a character, that it is a group homomorphism. And now is the time to use it. So, I am going to rewrite this as chi i of h, chi i of g is 0. Now, what does this mean? Well, I will reinterpret this equation as follows. This just says that this is true for all g in G.

So, it is almost like the original equation that I had. So, this was my original equation 1 and from that, I have obtained a second equation 2, in fact, I have obtained one such equation for every element h that I can fix. So, from one dependence relation that I had, I have generated many more dependence relations. So, observe, this just means that ai chi i of h, so I will rewrite this as a ai chi i of h, think of that as a new constant times the function chi i is 0.

So, now I have removed g from this picture. So, what does this imply? I have many different dependence relations among the chi i's. And therefore, it allows me to eliminate, so I can now do the following. I can, from these I can eliminate, so let us take these two. And let us eliminate chi n from this equation. So, let us eliminate last fellow chi n of g.

Now, what does that mean? Well, I have to multiply 1 by chi n of h. So, how do I eliminate chi n of g from these two equations? I multiply the first equation by chi n of h, and I subtract it from the second equation. So, I, to do this, I have to multiply this by chi n of h and subtract the second equation from it. So, let us do that and see what we get.

(Refer Slide Time: 12:20)

$$\sum_{i=1}^{n} a_i \chi_n(h) \chi_i(g) - \sum_{i=1}^{n} a_i \chi_i(h) \chi_i(g) = 0$$

$$\Rightarrow \sum_{i=1}^{n-1} a_i \left(\chi_n(h) - \chi_i(h) \right) \chi_i(g) = 0 \quad \forall g \in G$$

$$\Rightarrow \sum_{i=1}^{n-1} a_i \left(\chi_n(h) - \chi_i(h) \right) \chi_i = 0 \quad \text{in Maps}(G, F)$$

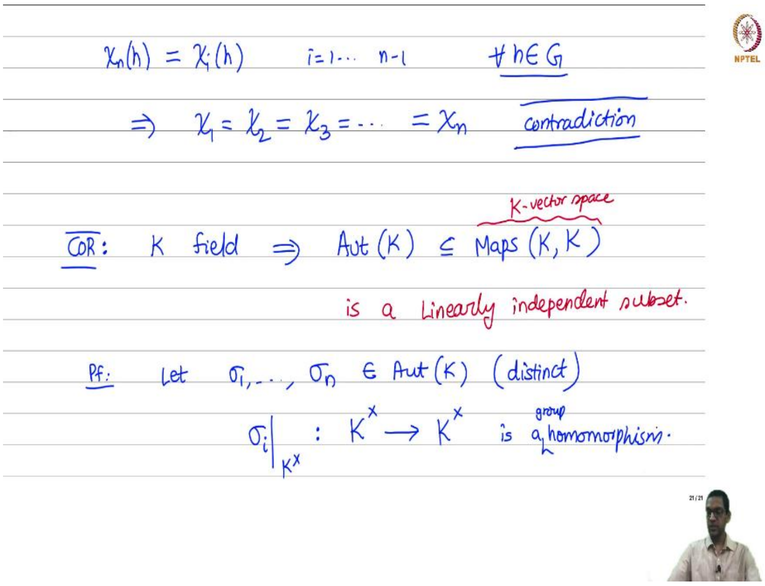
$$\Rightarrow \overset{\neq 0}{a_i} \left(\chi_n(h) - \chi_i(h) \right) = 0 \quad \forall i = 1 \ldots n-1$$

So here is what we will get, summation i goes now only from 1 to n minus 1, because the last terms were to get cancelled ai and so, let us write everything out for a moment ai chi n of h chi i of g, this is my first equation with chi n of h multiplied minus the summation ai chi i of h chi i of g, goes from 1 to n. So, this is what I get. So, this difference is of course also 0. But now observe that the nth term in these two summations cancel each other This means that I can rewrite this as 1 to n minus 1 ai and I get chi n of h minus chi i of h times chi i of g is 0. And this is true for all g in G.

Now, what does it imply? This is exactly a linear dependence relation between the first n minus 1 chi i so this I can think of as, I will just remove the g now from this, think of it as a linear dependence relation, which connects the first n minus 1 chi i's. So, this is now an equation if you think of it in the vector space all maps from G to F.

Now, what does that mean? We remember had assumed by induction that the any n minus 1 chi i's are linearly independent, but here is a linear dependence relation amongst them and all the, so therefore, all the coefficients have to be 0. So ai into chi n of h minus chi i of h have to be 0, for all i equals 1 to n minus 1, but we recall had said that the ai is themselves were all nonzero by the induction hypothesis, that means that the inside has to be 0.

(Refer Slide Time: 14:33)



So, we conclude then that chi n of h therefore, equals chi i of h, and this is for i equals 1 to n minus 1. But remember this is the important observation h itself was arbitrary, we fixed h to be any element of the group g. So, this arbitrary choice tells you that well as characters, chi 1, chi 2, chi 3 are all equal to chi n. But that is a contradiction. In fact, it is our original assumption was that, the chi's are all pairwise distinct elements, so chi n cannot equal any one of the previous ones. Here we therefore get a contradiction.

So that completes the proof, shows that the by induction, we have shown that any set of pairwise distinct characters is necessarily linearly independent. And so here is a little corollary. And it is in this form that this will find application. So, if K is a field, then look at the set Aut K. Recall, Aut K is just a set of all field homomorphisms of K, this is, well, this is linearly independent. So, you can think of Aut K as follows. You know, these are just, this is a subset of all maps from K to K, all set maps from K to K.

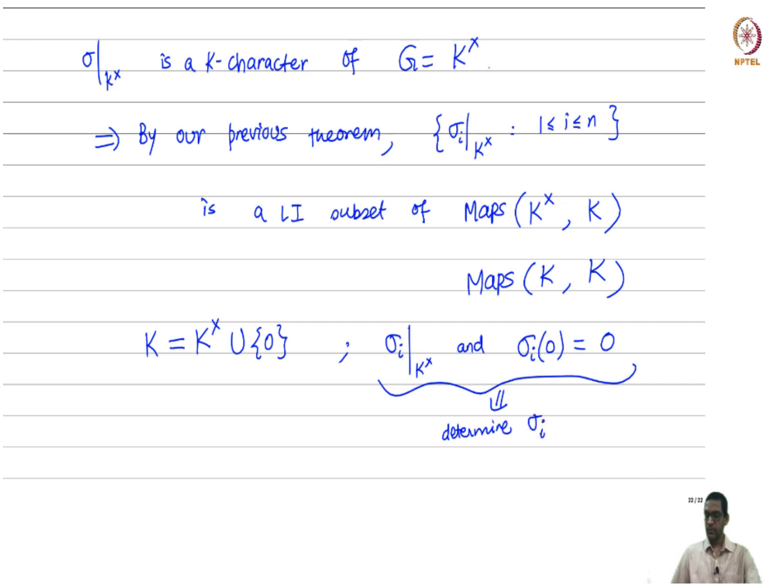
And as we just said, the set, the set maps from K to K is a K vector space. So, this is a K vector space. So, the set of automorphisms is well, it is it is not a subspace, it is a subset of the K vector space. And the claim is that this is a linearly independent subset of this K vector space. So, it is linearly independent over K. So, K is the only field here really.

So, we claim that any collection of automorphisms is, well, the set of all automorphisms is a linearly independent set. And, well the proof is, is rather easy, it just follows from the previous theorem that we have already shown. So, observe that to show that a set is linearly independent, just means you pick any finitely many out of them, you pick any finite number of elements from Aut K and you must show they are linearly independent.

So, it is only a checking, only involves checking finitely, many at a time. So, let us pick finitely many automorphisms and show that they are linearly independent. So, let sigma 1, sigma 2, sigma n be distinct, let us assume they are all pairwise distinct automorphisms. And you need to claim they are linearly independent somehow by using the previous theorem.

Now, how do we think of them as characters? Well, they are maps from K to K. So, observe that each sigma i, I can think of as follows, I will restrict sigma i to K minus 0. I will think of it as a homomorphism from the multiplicative group K cross to itself. So, this is a group homomorphism. It is a group homomorphism.

(Refer Slide Time: 18:04)

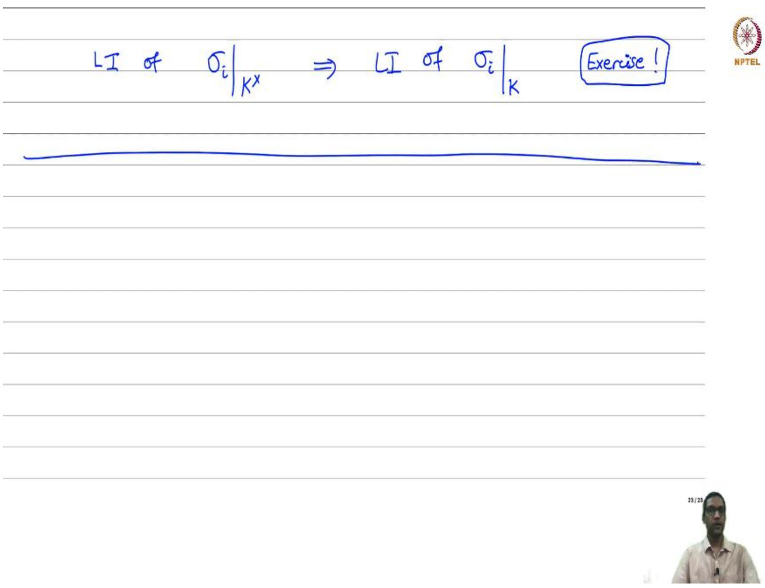


So, if instead of sigma, I look at sigma restricted to K cross, then this is therefore, this is a character, this is a K valued character. So, this is a K character if you wish, of what is the group involved group? Well a group is just K cross. So, by the previous theorem, therefore, you can apply our previous theorem, by our previous theorem conclude that and what do we conclude?

That the collection of all sigma i restricted to K cross from 1 to n is linearly independent subset of the set of all maps from G to K and G here is K cross to K. But that is more or less all that we need, because observe that maps from you know, K minus the origin to K. And maps from K to K are, well, they are almost the same thing. So, if instead of, so, I mean, what do the sigma i's, what is the difference? Sigma i restricted to K cross.

And what is the extra point? K only has one additional point; K is just K cross union 0. And therefore, if I know sigma i on K cross, then I know sigma i completely. Because observe sigma i on 0 is 0. So, sigma i on K cross, if you know that and if you know sigma, well, if sigma i is 0 is certainly 0, because it is a homomorphism. So, these two determine sigma i. This tells me what sigma i is.

(Refer Slide Time: 20:09)



So, in other words and of course, one has to check this, but the linear independence of, so observe that the linear independence of sigma i restricted to K cross implies the linear independence of the sigma's that sigma i's on all of K, sigma i on K. Why is this? Because, well, how can it possibly fail, only if it fails at the origin.

So, if there is some linear dependence relation at the, which somehow fails at the origin alone, but that is not going to happen. So, this is an easy verification. So, I should just say exercise maybe, so this is one additional point does not cause any problem. So, this is an important result which will be used to prove Artin's theorem.