Galois' Theory
Professor Dilip P. Patil
Department of Mathematics
Indian Institute of Science Bangalore
Lecture No 39
Extension over a fixed field of a finite subgroup is Galois Extension

(Refer Slide Time 00:25)

Last few lectures we have been discussing this cyclotomic field

(Refer Slide Time 00:29)

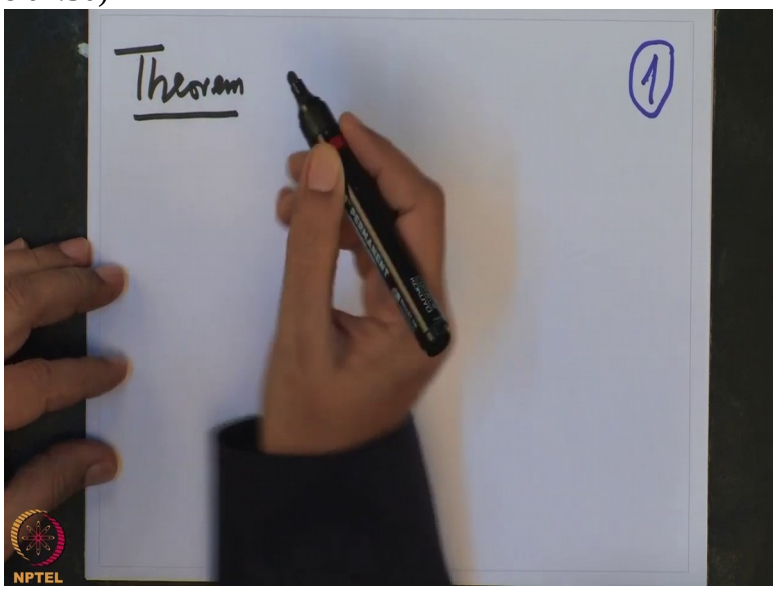
extensions of $\mathbb{Q}$ and cyclotomic field extensions of finite fields. And we have, we now know what exactly their Galois groups are and what are their orders etc, etc.

I still want to further apply these results to particular field extensions of characteristic p to gather some more information about general problems but before that, as we saw in the last lecture at the end we need to decide when the fixed field of the subgroup of Galois extension again be Galois over the ground field.

And for this I want to now prove a general result which will also give us many examples of Galois extensions. So for example I want to prove the following theorem. Now we are, we are in a general case. We are not in characteristic 0 or characteristic positive or any such case but I will now state this theorem in the most generality.

So the theorem one wants to prove is,

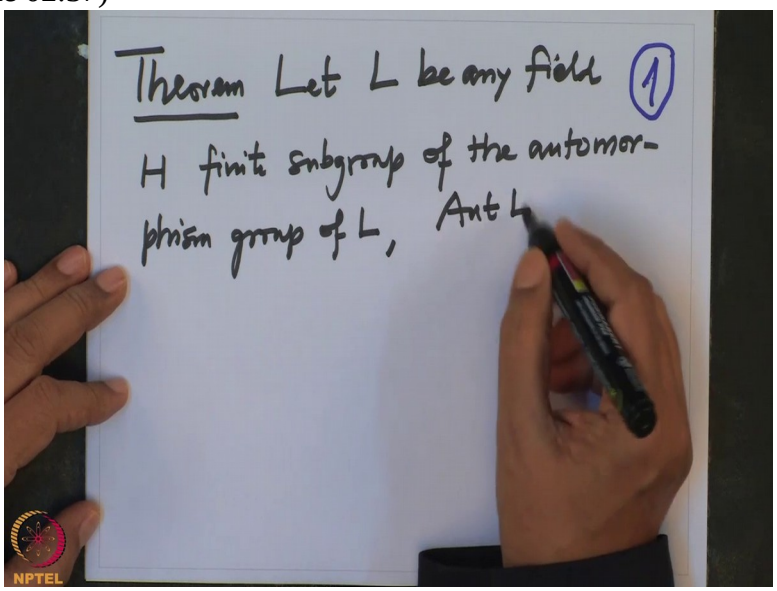
(Refer Slide Time 01:50)



let L be any field. And G and H, H be a finite subgroup of the automorphism group, group of L. So that means what, that means H is a subgroup of Aut L. And I do not write fields. So when I say Aut L of a field that means automorphisms as a field.

So this is

(Refer Slide Time 02:37)

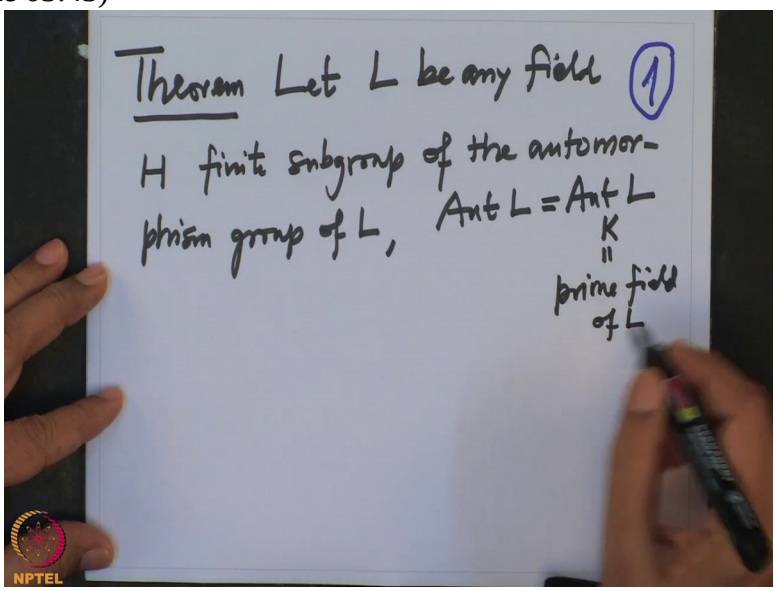


a group composition of 2 automorphisms is again automorphism of field inverse etc. They are all automorphisms. And H is a finite subgroup of that. Let me remind you this automorphism group of a field need not be finite.

In fact it can be very large group even for a field like L equal to $\mathbb{C}$. We only know automorphism group of $\mathbb{Q}$ is trivial, automorphism group of $\mathbb{R}$ is trivial. Also automorphism group of $\mathbb{Z}_p$ is trivial. Automorphism group of a finite prime fields are always trivial because the identity, the only automorphism of the prime field.

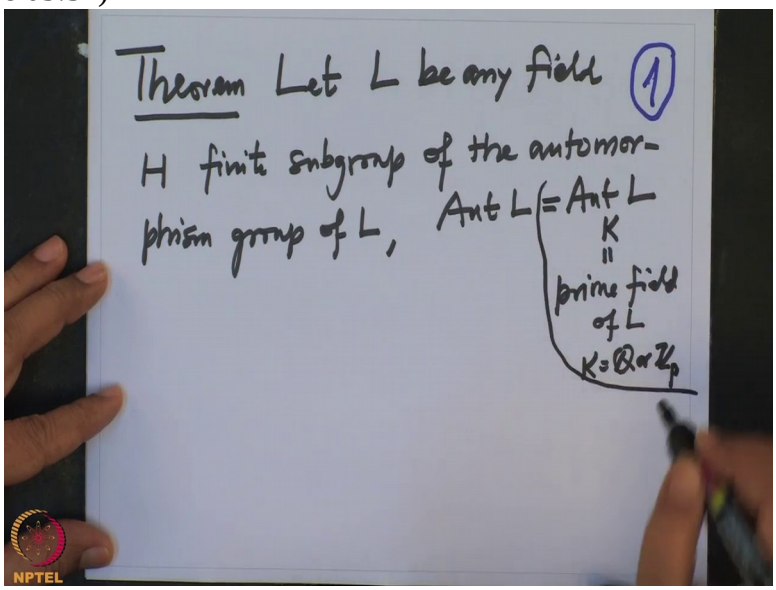
And in general, automorphism of a, automorphism group of a field L is always be over its prime field. So this one is also, it is same as Aut L and K here where K is a prime field of, prime field of L and prime fields are either $\mathbb{Q}$ or $\mathbb{Z}_p$.

(Refer Slide Time 03:43)



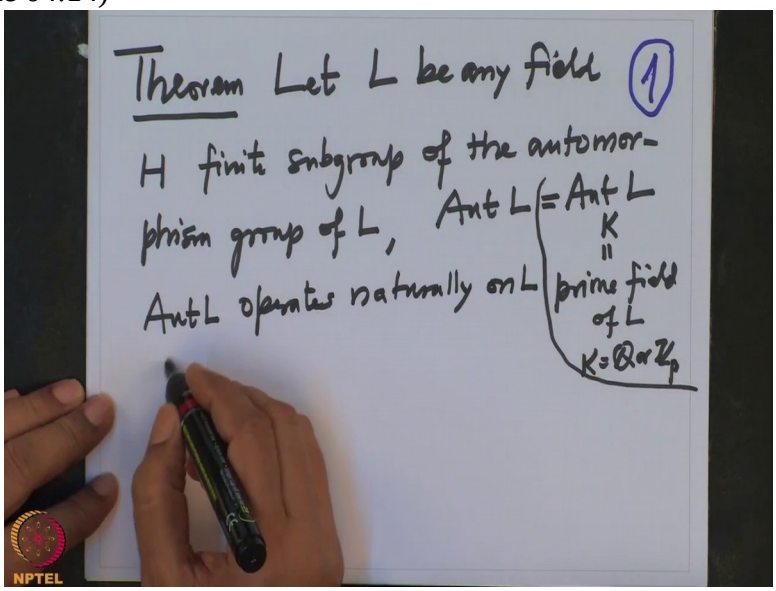
So K is either $\mathbb{Q}$ or $\mathbb{Z}_p$. So this is the side.

(Refer Slide Time 03:52)



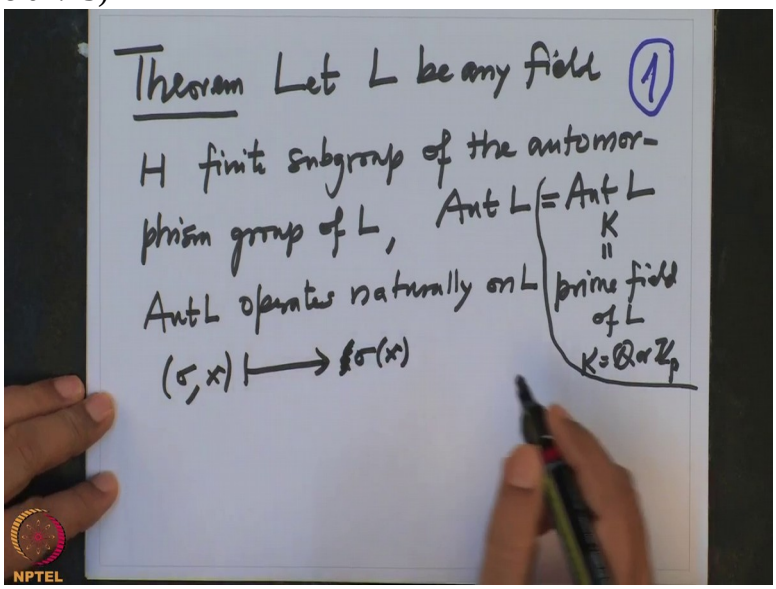
So we have taken any finite subgroup of the automorphism group of a field L. And therefore this Aut L operates naturally on L. Once again I will write

(Refer Slide Time 04:14)



the operation that is (σ, x) this goes to $\sigma(x)$. So its evaluation

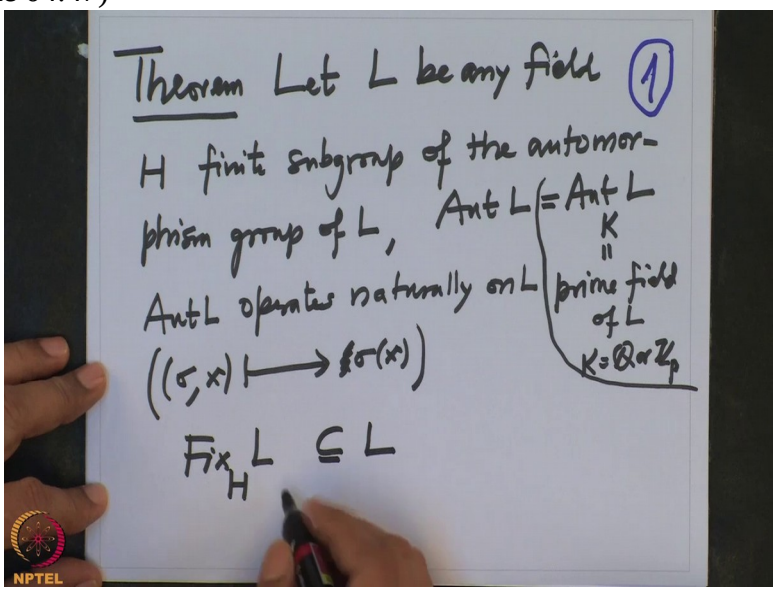
(Refer Slide Time 04:23)



at this x and this is clearly an operation map that we have, one it is very obvious so therefore fixed field of H makes sense.

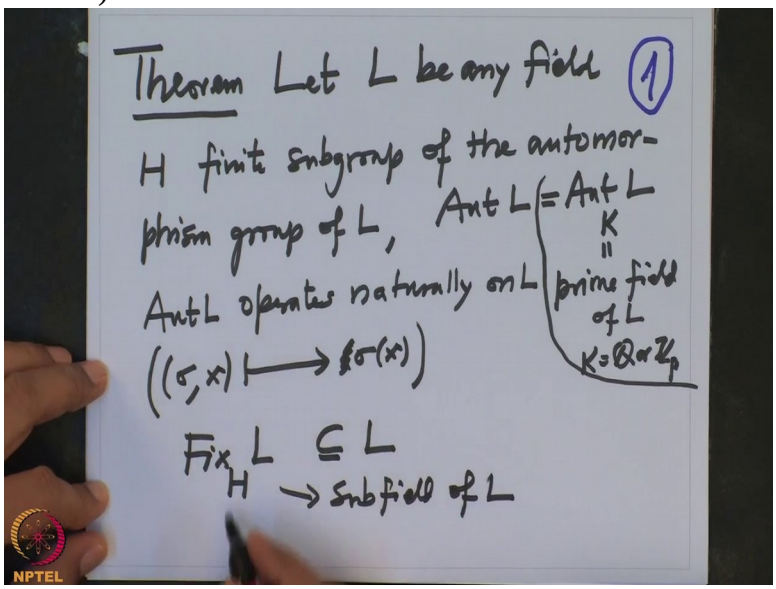
So $Fix_H L$, this is, this will contain a prime field and this is a subfield of L,

(Refer Slide Time 04:47)



this is a subfield of L

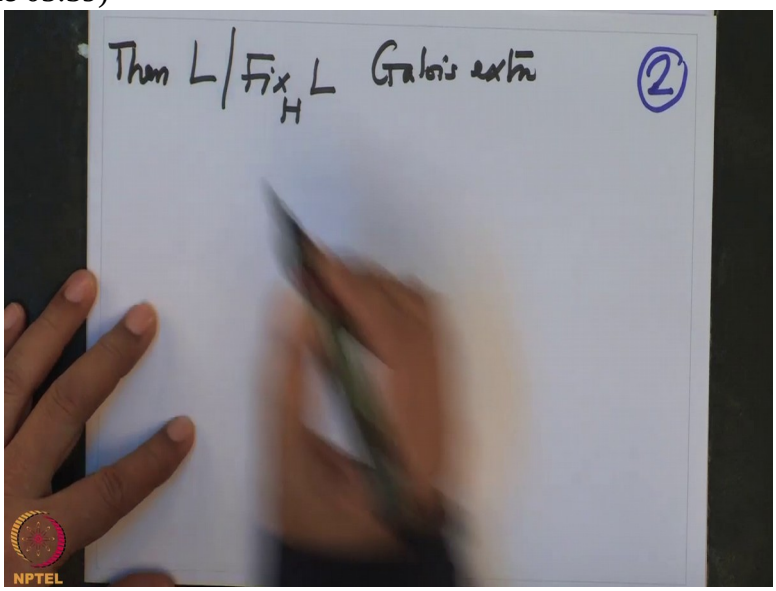
(Refer Slide Time 04:53)



because if x is fixed, x^{-1} is also fixed. $x+y$ is also fixed. $x-y$ is also fixed. And xy is also fixed. And 1 is fixed obviously because 1 is an element in the prime field. So therefore we get a subfield.

Now the question is, the question I want to answer is whether this extension L over fix field of H, whether if this extension Galois or not? And the answer is yes, this is a Galois extension. Then this

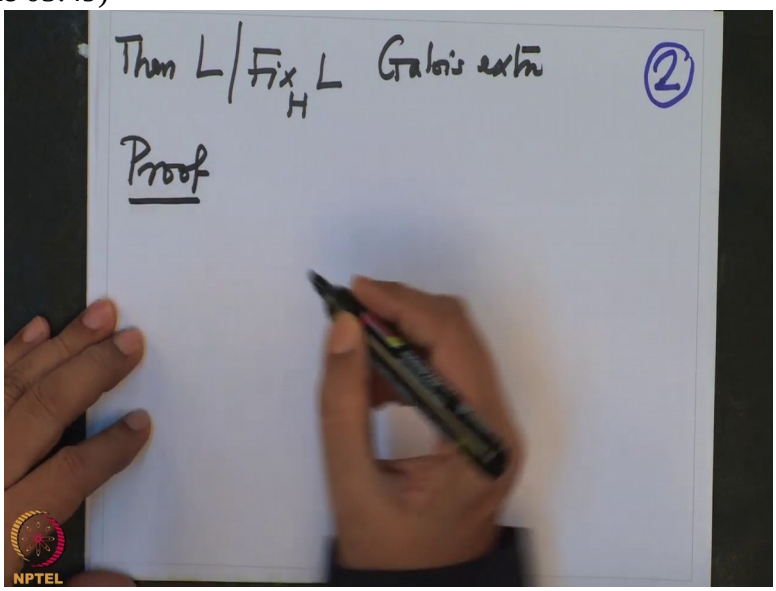
(Refer Slide Time 05:39)



is a Galois extension.

Alright and how am I going to prove this? So proof,

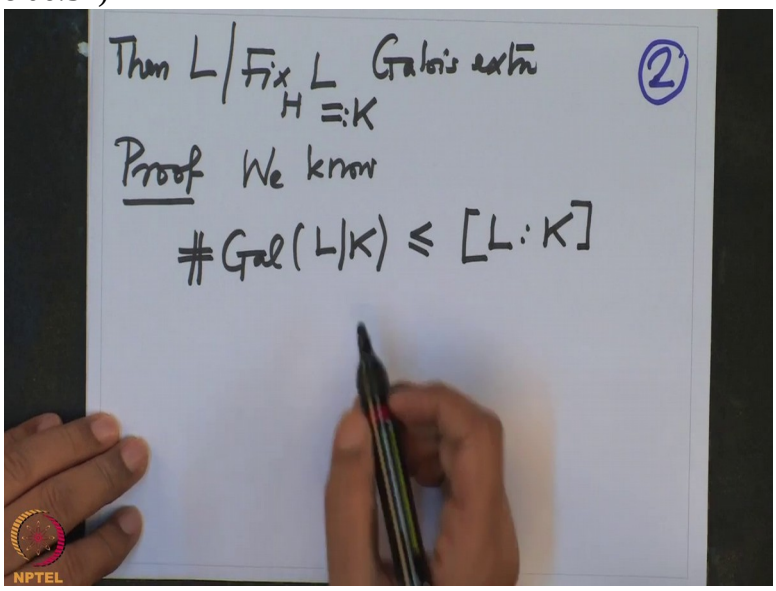
(Refer Slide Time 05:49)



remember, first of all how does one check the field extension is a Galois field extension? One checks that the order of the Galois group equal to the degree of the field extension.

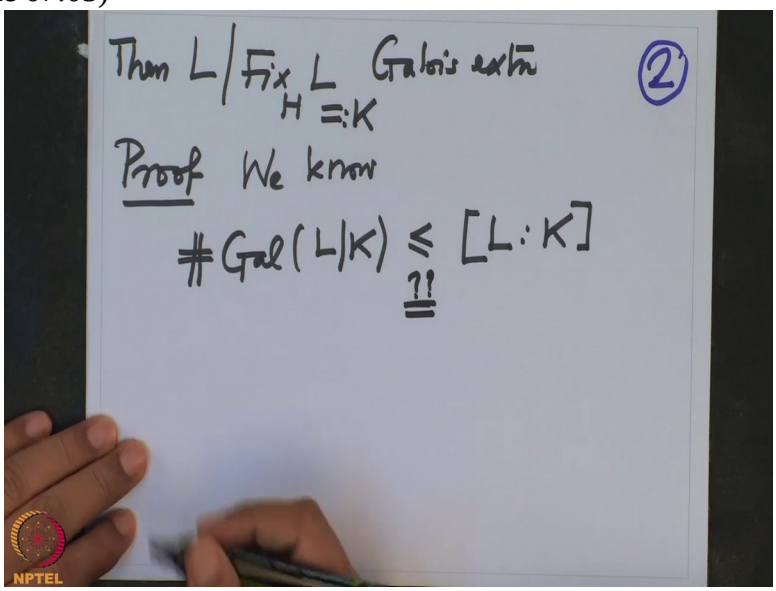
So we have to see what is the order and what is the degree of the field extension. In any case we know that the, the Galois group of this, so we know by Dedekind and Artin, that the Galois group of this, Gal L over, let me call this field as K, L over K this order is bounded by the degree of L over K. This we know.

(Refer Slide Time 06:54)



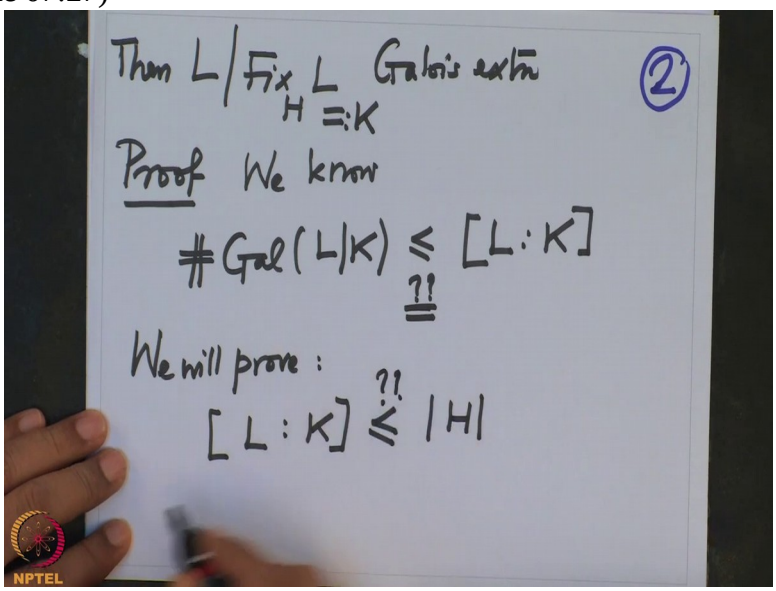
And we are interested in proving the equality. So we want to prove equality here. This is what we want to prove.

(Refer Slide Time 07:05)



So we will prove first that the degree of L over K is bounded by the order of H. This is one. This is what we will prove.

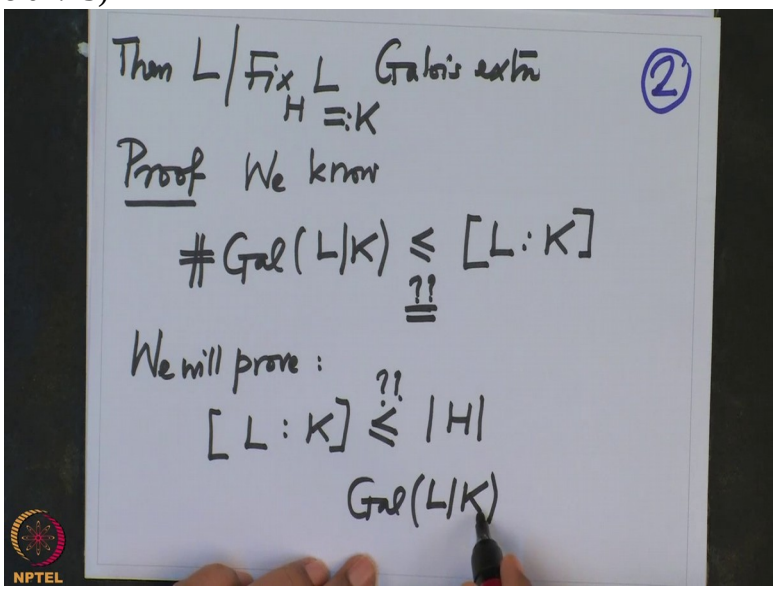
(Refer Slide Time 07:27)



And what is obvious is the following.

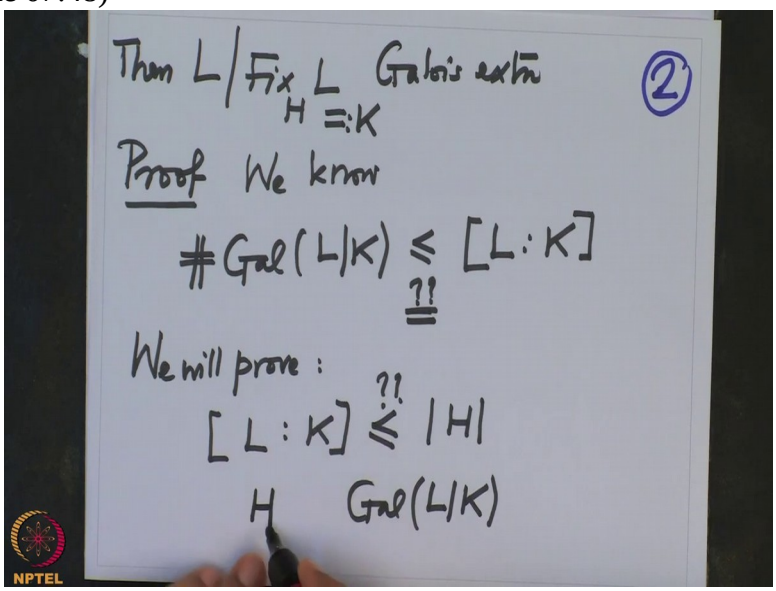
The Galois group of L over K, what are the elements? They are all automorphisms of L which fixes elements

(Refer Slide Time 07:43)



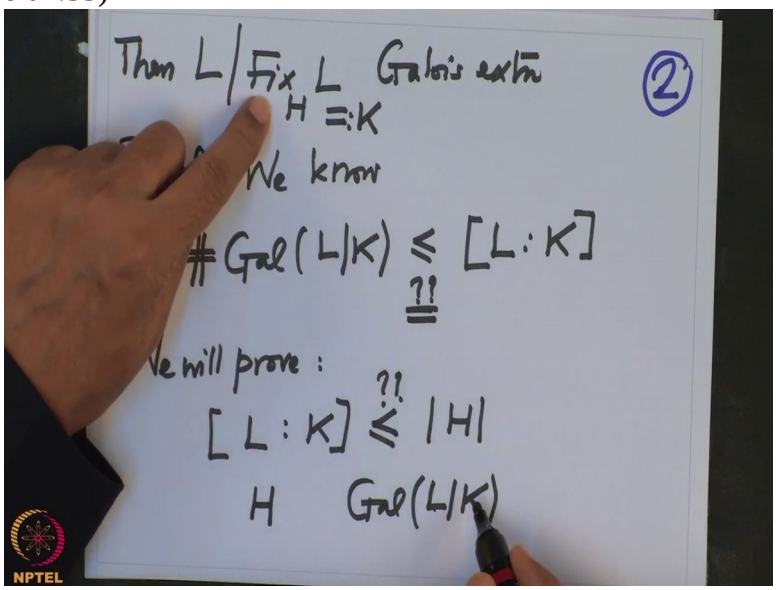
of K, but elements of, so already elements of H,

(Refer Slide Time 07:48)



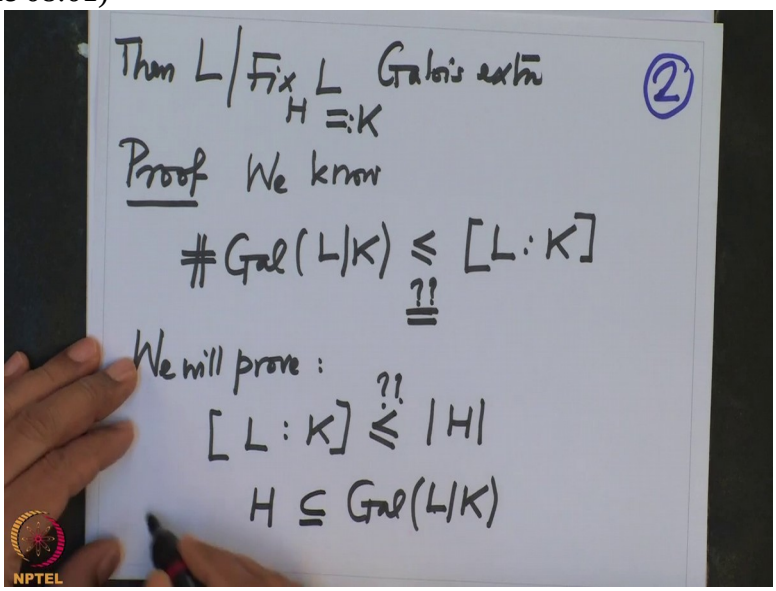
they have this property. Elements of H are automorphisms of L and they fix K because K is by definition, fix field

(Refer Slide Time 07:55)



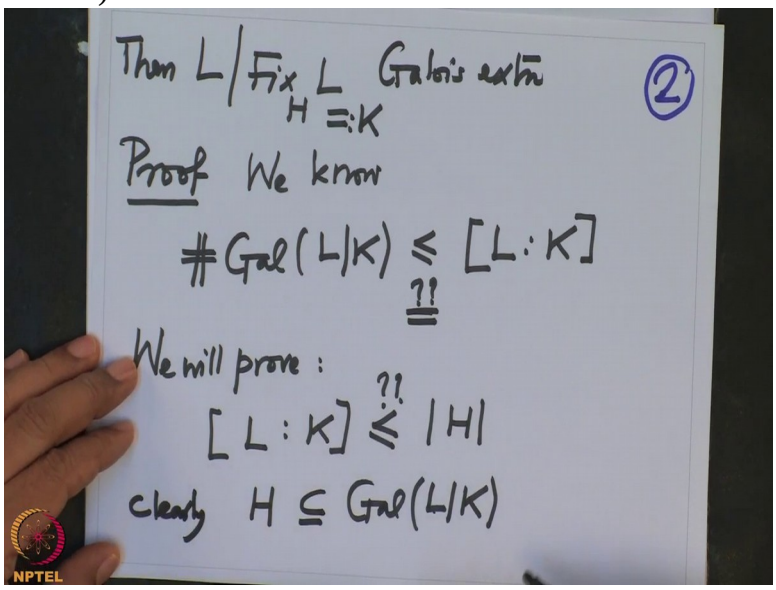
of H so all elements of K are fixed by H. So this inclusion is obvious,

(Refer Slide Time 08:01)



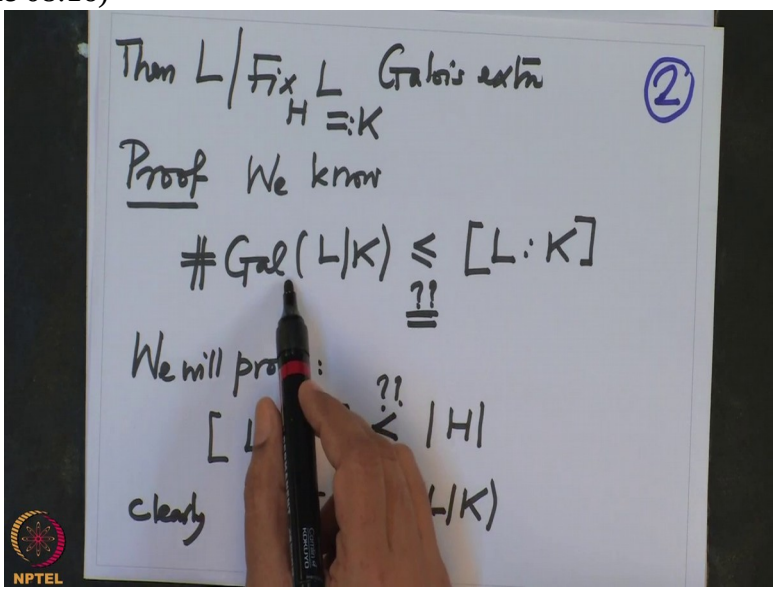
clearly this.

(Refer Slide Time 08:05)



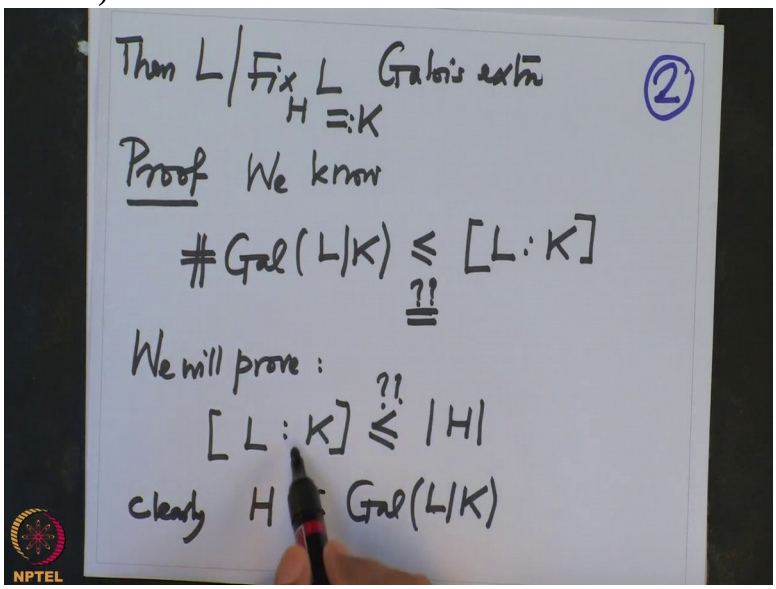
Once I have this and this, then what will I get? I will get order of H is small or equal to the cardinality of L over K

(Refer Slide Time 08:16)



which is small or equal to the degree of L over K. And by

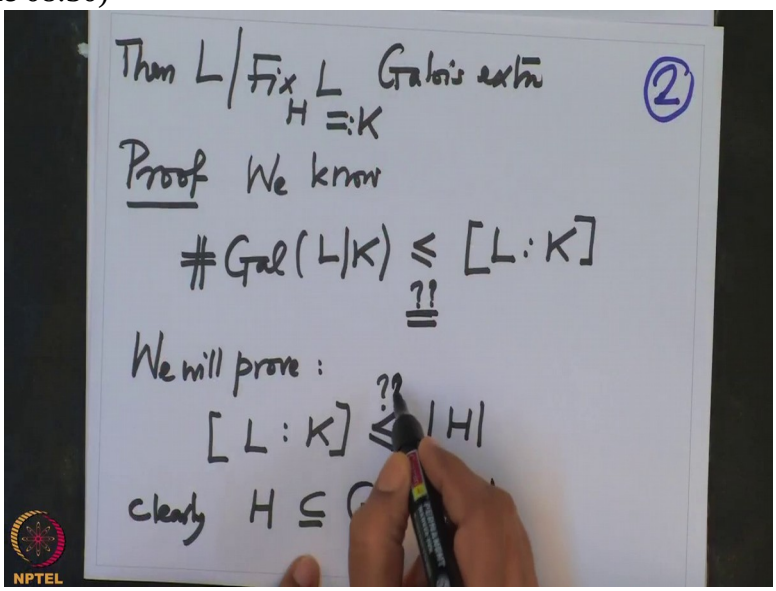
(Refer Slide Time 08:20)



what we would prove that degree of L over K is small or equal to H and therefore the equality is everywhere. And so that will finish our proof.

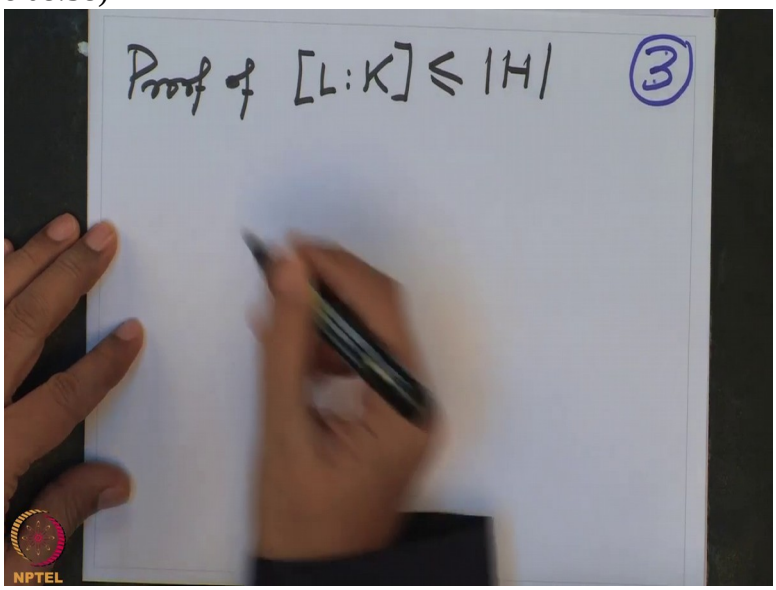
So we only have to prove this double question mark

(Refer Slide Time 08:30)



this. The order of, the dimension of L over K is bounded by cardinality of H. Ok, so this is what we will prove. Ok, alright so proof of L over K, small or equal to cardinality H.

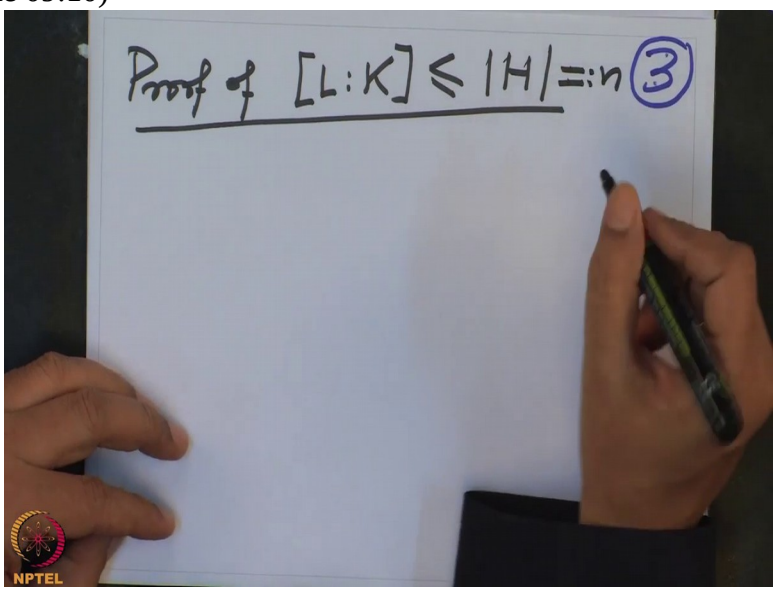
(Refer Slide Time 08:58)



This is what we need to prove.

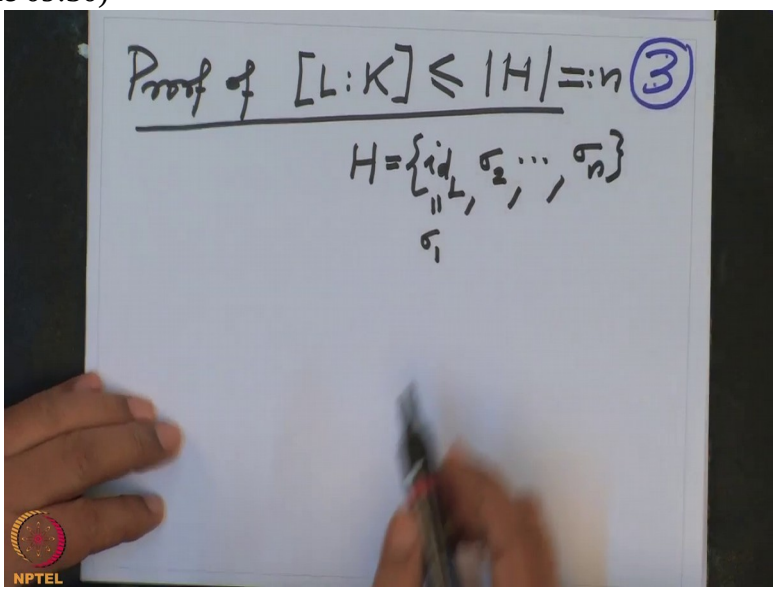
That means, and let us call this cardinality of H to be n.

(Refer Slide Time 09:10)



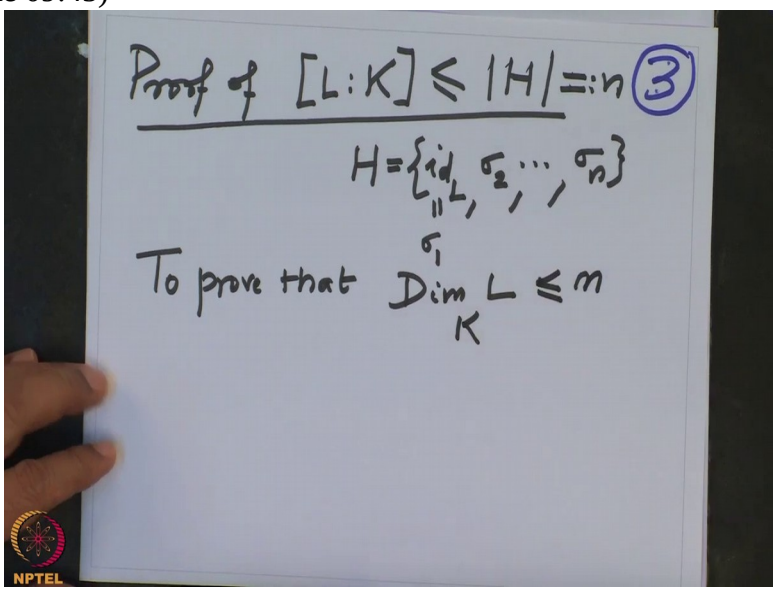
means what, that means H is, H is a subgroup and it has exactly n elements. And one of them is identity, id_L and then σ ; this is $\sigma_1, \sigma_2, \ldots, \sigma_n$. These are all elements of H. And

(Refer Slide Time 09:30)



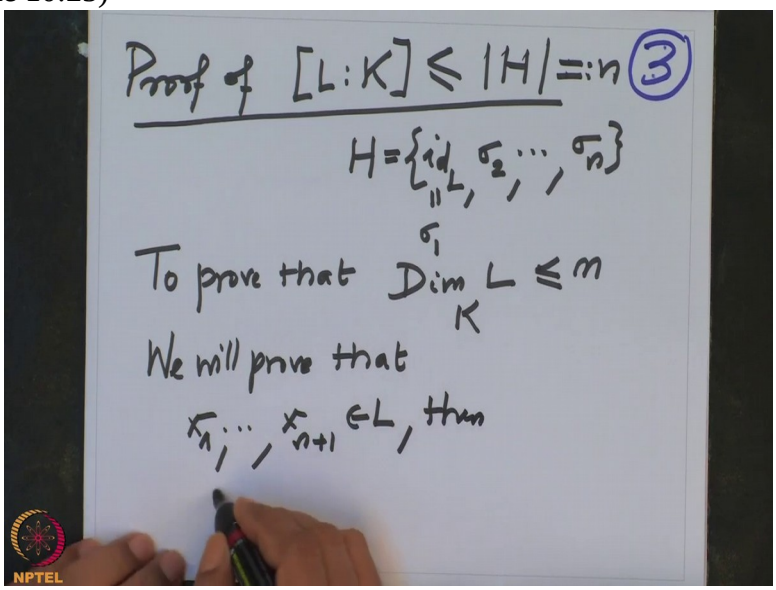
we want to prove that, to prove that dimension of L over K is less equal to n.

(Refer Slide Time 09:45)



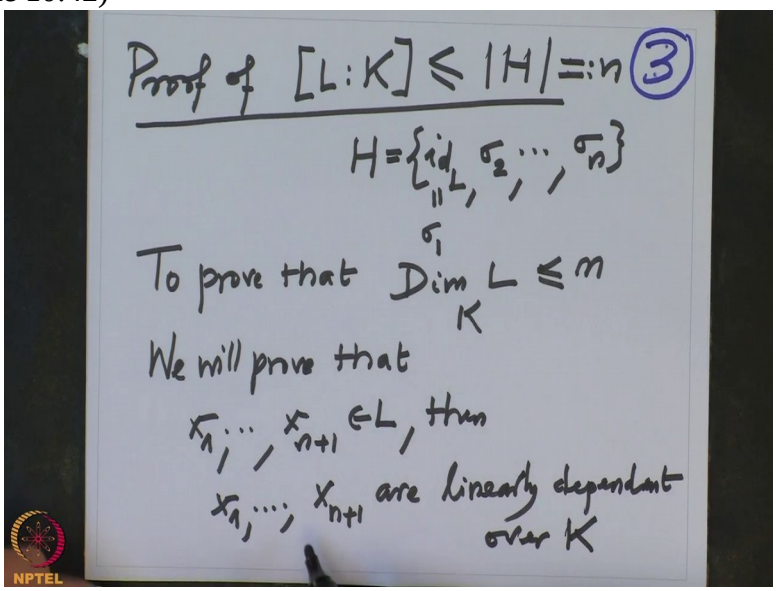
And how does one prove that dimension of L over K is less equal to n? That means I will prove that every $n+1$ elements of L are linearly dependent over K. So we will prove, prove that, if I have $n+1$ elements $x_1, \ldots, x_{n+1}$ are elements in L then

(Refer Slide Time 10:25)



$x_1, \ldots, x_{n+1}$ are linearly dependent over K.

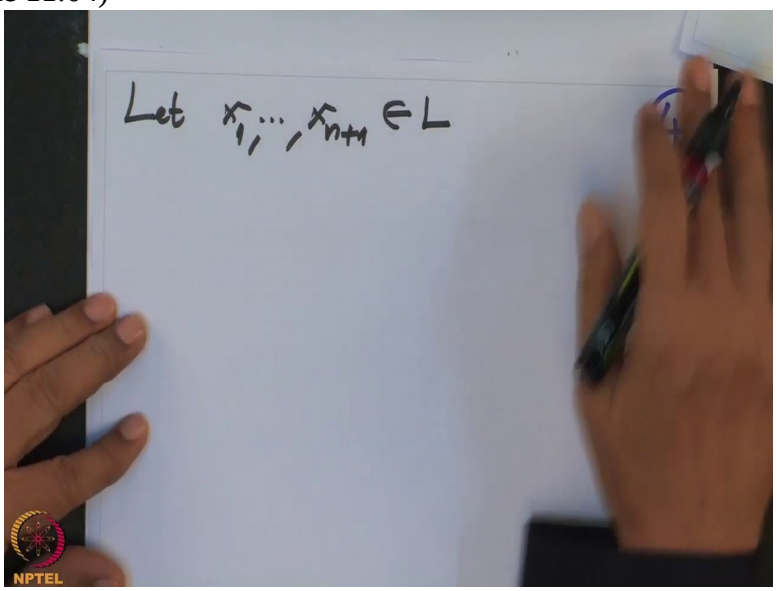
(Refer Slide Time 10:42)



Therefore then the dimension of L over K will not be more than n. That is what we wanted to prove.

So take any $n+1$ element. So let $x_1,\ldots,x_{n+1}$ be elements of L and I want to prove that they are

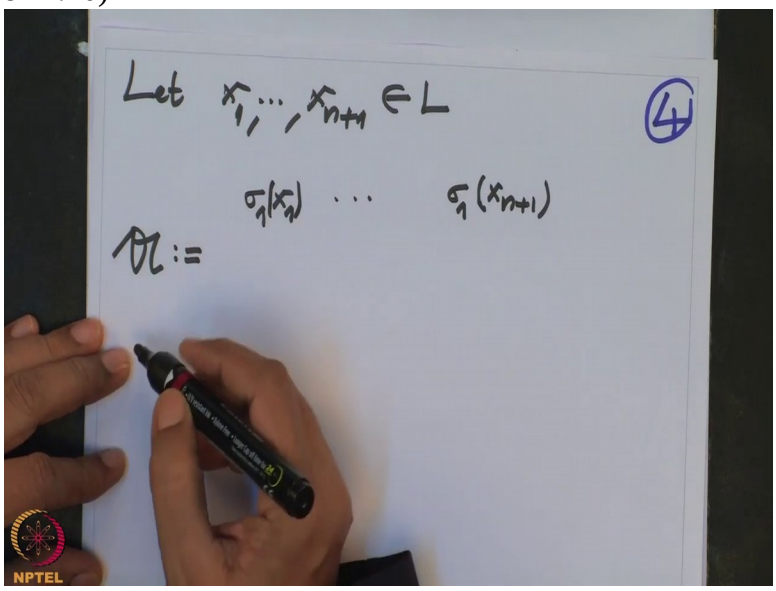
(Refer Slide Time 11:04)



linearly dependent. That means I have to produce a linear dependence relation, alright. So I form a matrix, matrix A. This is the first row. I apply σ_1 to this.

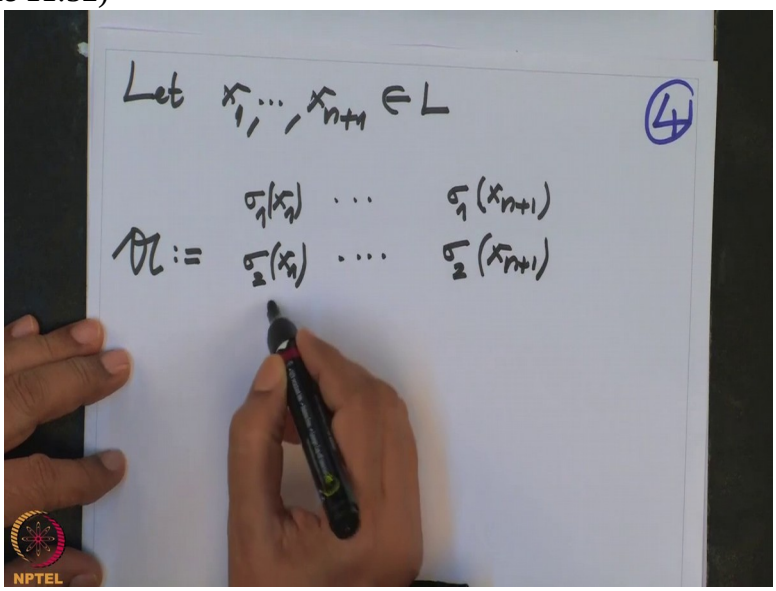
So $\sigma_1(x_1)$, I want to drop that bracket here. It is understood that $\sigma_1(x)$, $\sigma_1(x_{n+1})$. Ok let me write it.

(Refer Slide Time 11:40)



This is the first row. Second row is $\sigma_2(x_1), \ldots, \sigma_2(x_{n+1})$

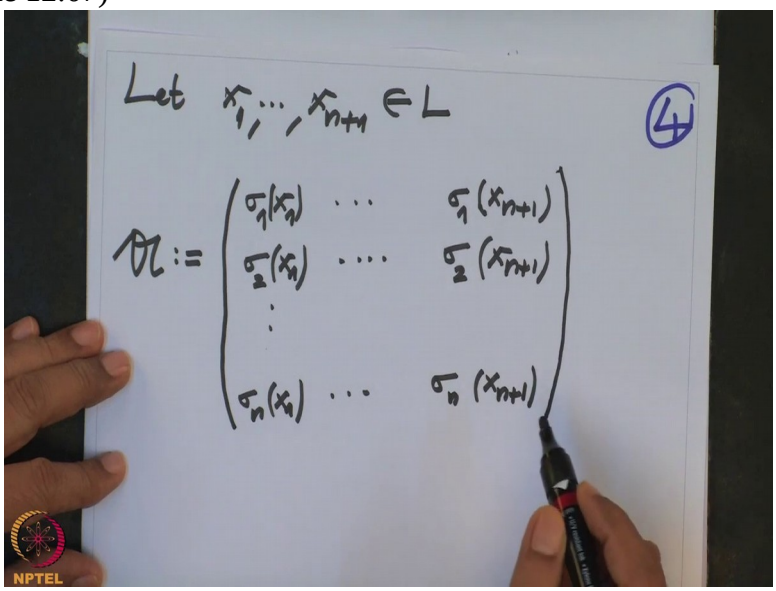
(Refer Slide Time 11:52)



and so on.

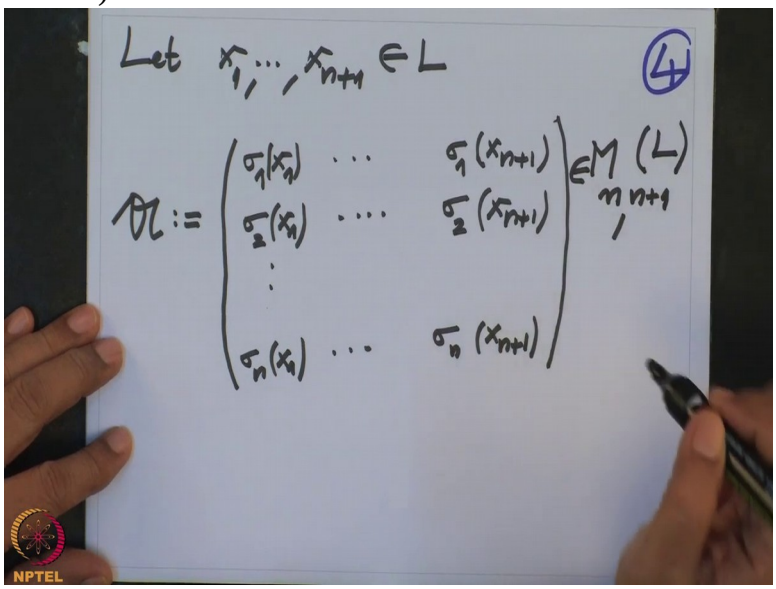
And there are n elements in H so last row is $\sigma_n(x_1), \ldots, \sigma_n(x_{n+1})$. So this is the matrix. The rows are

(Refer Slide Time 12:07)



numbered by the elements of H and the columns are numbered by the elements, the element we started with. So this is a matrix $M_{n\times(n+1)}$ and the entries are in the field L.

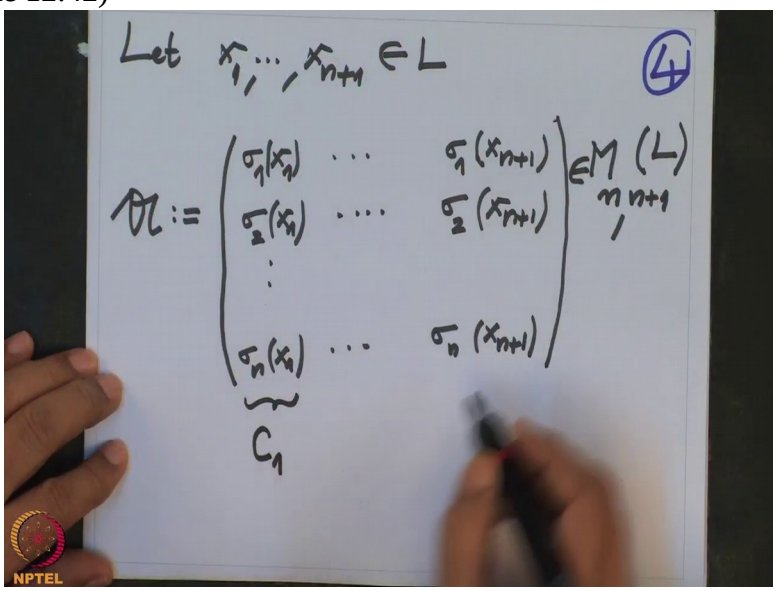
(Refer Slide Time 12:25)



Everything is happening in the field L.

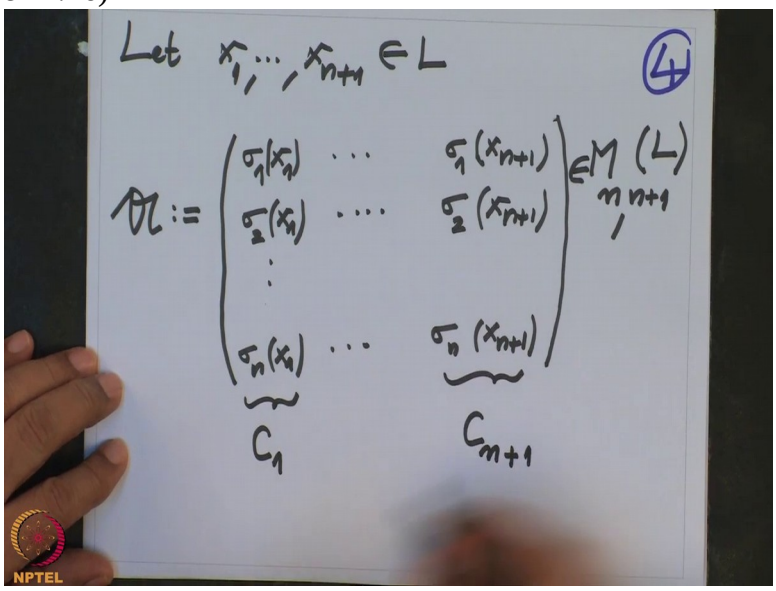
So this is a matrix, n rows, $n+1$ columns. So therefore, and let us call these columns the first column is C_1 ,

(Refer Slide Time 12:42)



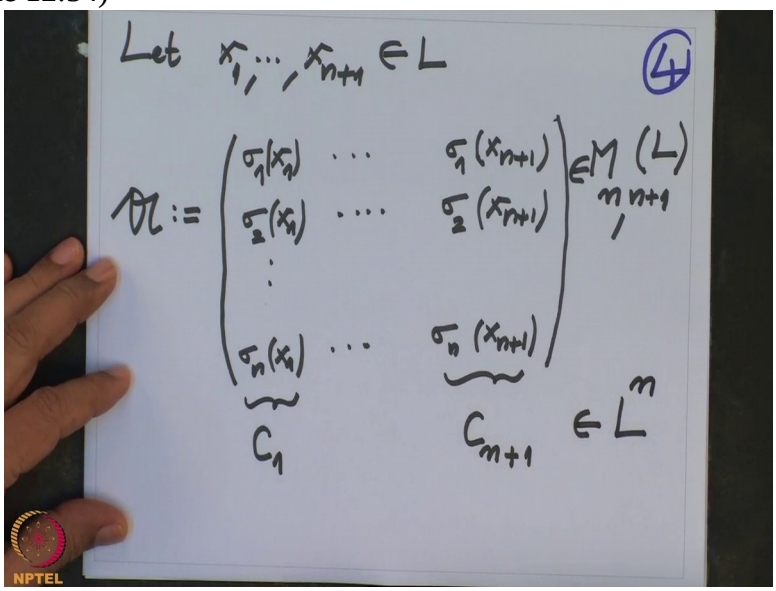
this column is C_{n+1} .

(Refer Slide Time 12:46)



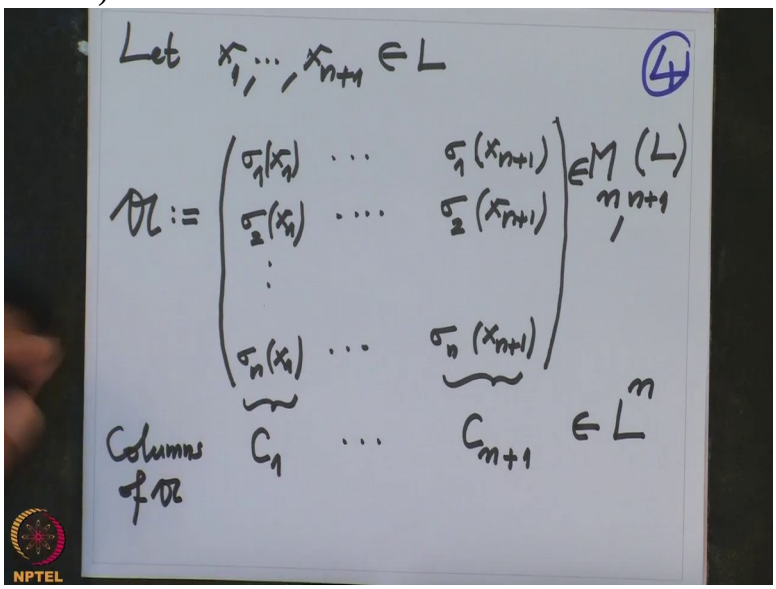
They are elements where? They are elements in, think of column. So they are elements in L^n .

(Refer Slide Time 12:54)



This is the columns; columns of A are denoted

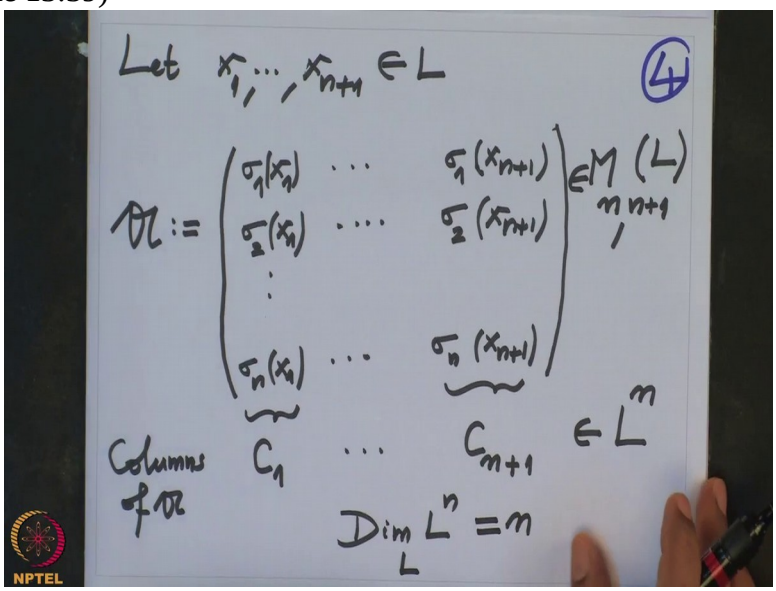
(Refer Slide Time 13:05)



by this. So C_1 is this column and so on. They are $n+1$ elements and this is a vector space of dimension n. Therefore they are linearly dependent over L. I am thinking L^n as a L vector space.

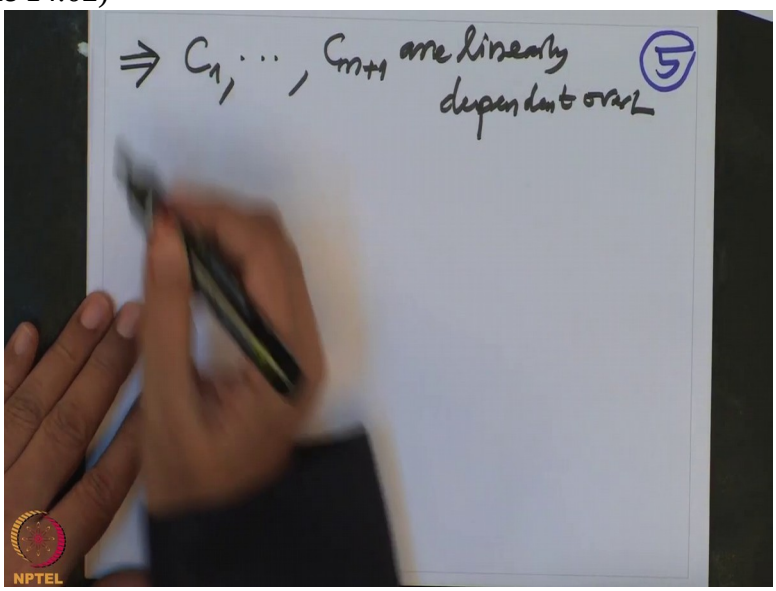
And they are $n+1$ elements there. $n+1$ elements in the vector space of dimension L. Therefore they are linearly dependent. So I will use this. So dimension of L^n over L, this we know it is n and therefore

(Refer Slide Time 13:39)



C_1 to C_{n+1} are linearly dependent. So C_1 to C_{n+1} are linearly dependent over L. So therefore

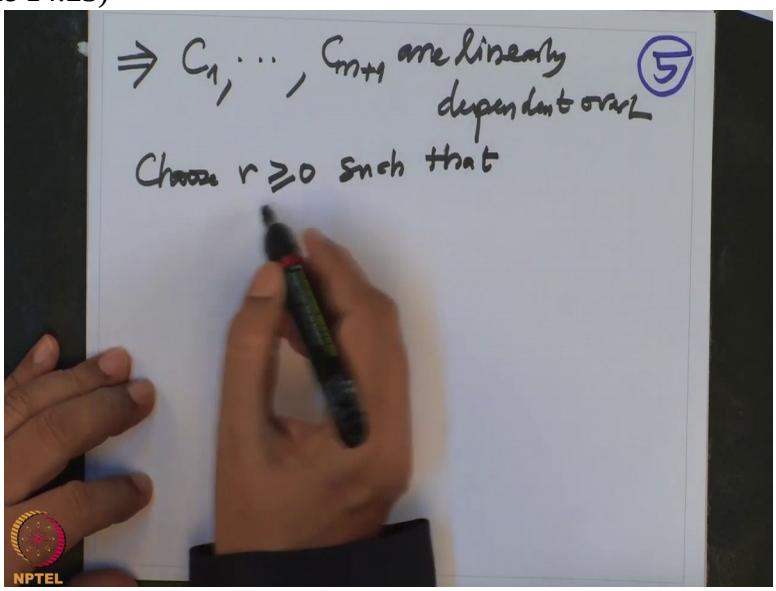
(Refer Slide Time 14:02)



there is a linear dependent relation.

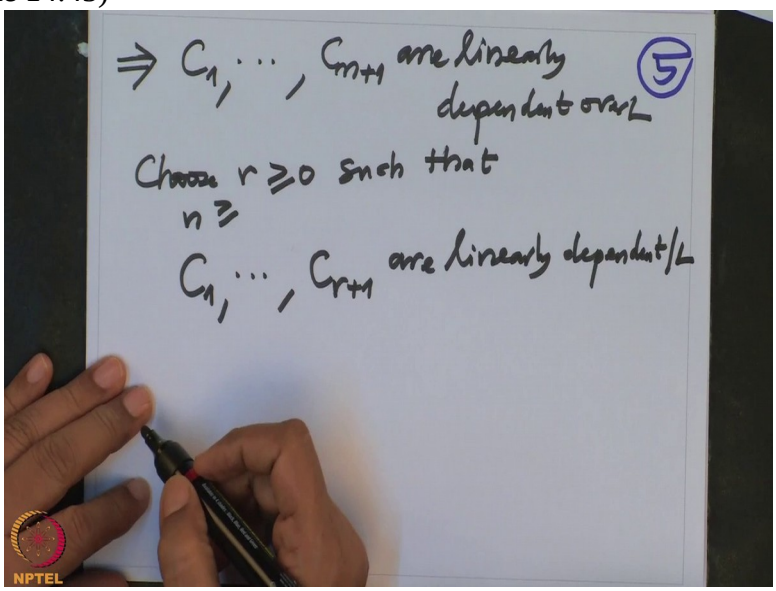
And I am going to choose a minimal linear dependence relation. So that means I am going to choose r, so choose r bigger equal to 0, such that,

(Refer Slide Time 14:23)



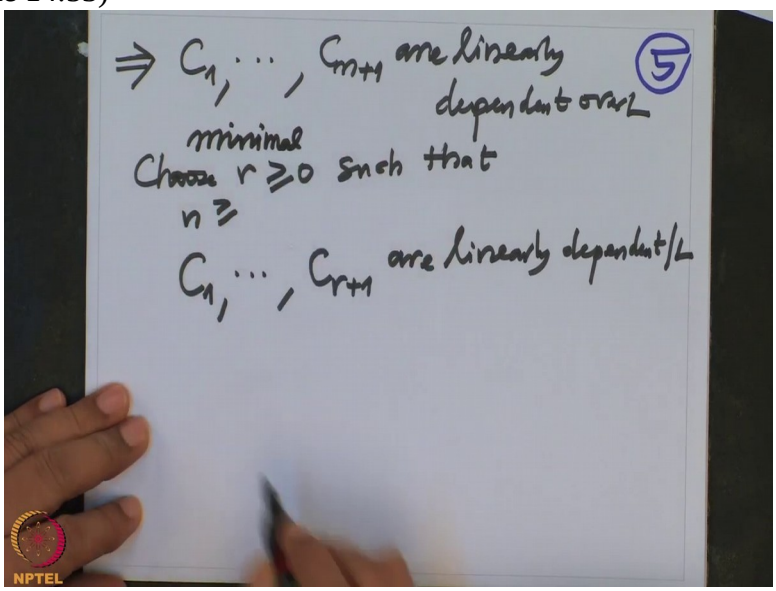
and r of course is smaller equal to n such that, I have a relation like this, such that C_1 to C_{r+1} are linearly dependent over L.

(Refer Slide Time 14:45)



I have taken $r+1$ right, so choose minimal

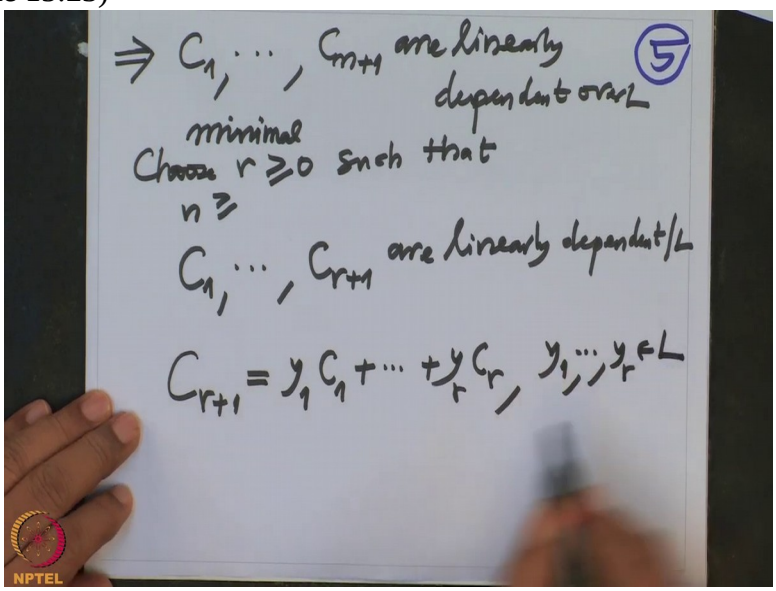
(Refer Slide Time 14:53)



so that this.

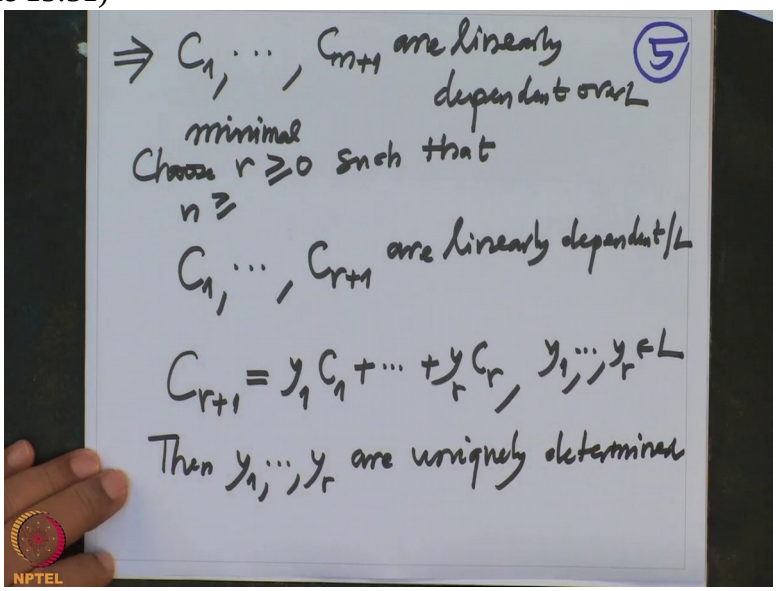
So this means, this means what? This means one of the column is the combination of the other columns. So C_{r+1} equal to $y_1C_1+...+y_rC_r$ where y_1 to y_r are elements in L.

(Refer Slide Time 15:23)



And because I have chosen r minimal, these y_1 to y_r are uniquely determined. Actually I should say that then y_1 to y_r are uniquely determined.

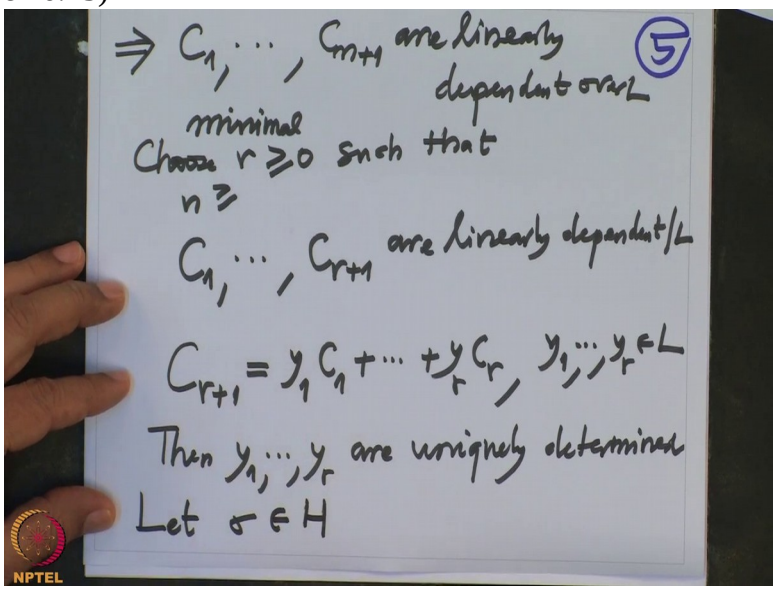
(Refer Slide Time 15:51)



Because otherwise I will subtract and then I will get a smaller relation. So y_1 to y_r are uniquely determined, fine.

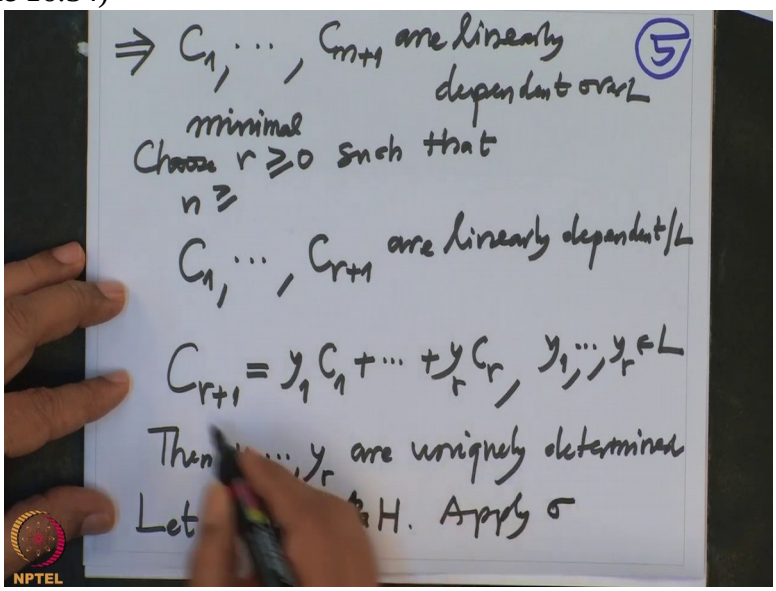
Now to this equation I am going to apply, take any, let σ be any element in H

(Refer Slide Time 16:13)



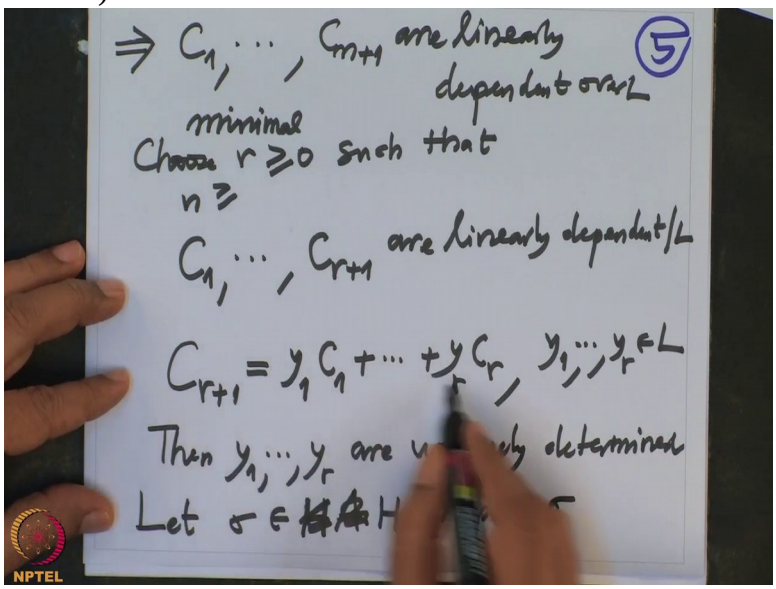
and I am going to apply $y \in H$, σ be any element in G Aut L, no H and apply, apply σ

(Refer Slide Time 16:34)



to the, this equation. This is what

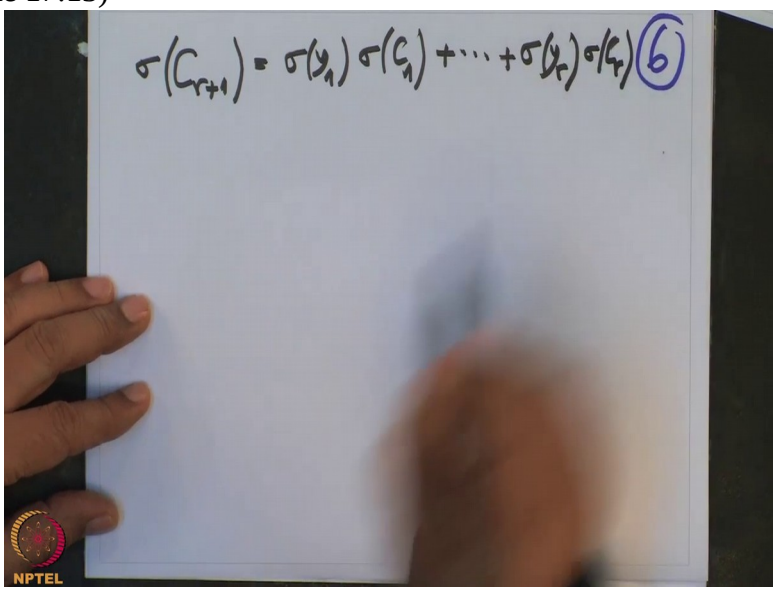
(Refer Slide Time 16:37)



I am going to apply. So what will I get? σ of this so I will get σ of the column C_{r+1} equal to, and σ is, σ respects multiplication.

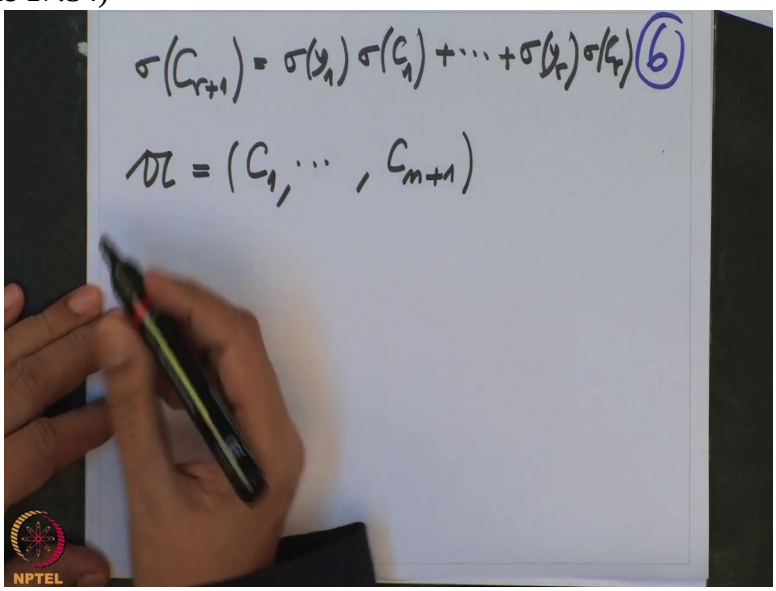
So that means I can take it out individually. So this is σ of y_1 , σ of C_1 etc plus, plus σ respects plus and multiplication therefore I can individually take like this, σ of y_r times σ of C_r .

(Refer Slide Time 17:13)



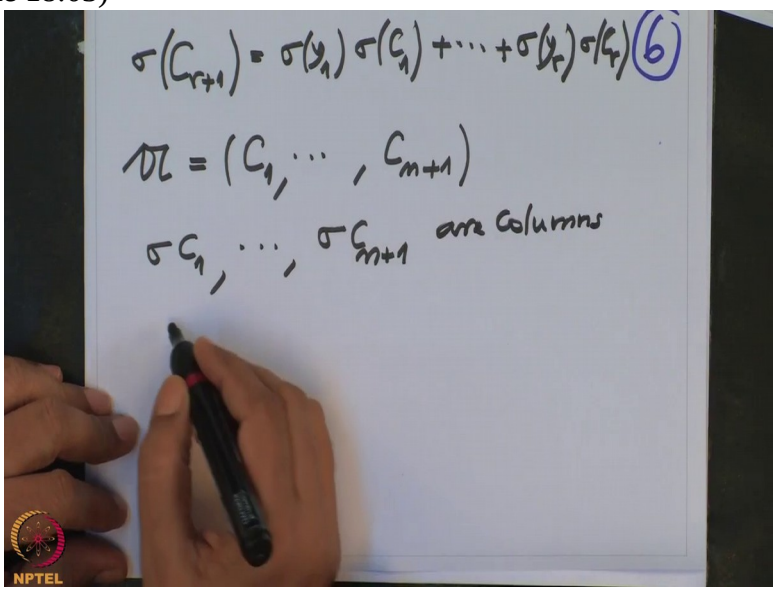
And so now what happened? The matrix, now I had originally the matrix A and the columns were C_1 to C_{n+1} . This was the matrix.

(Refer Slide Time 17:34)



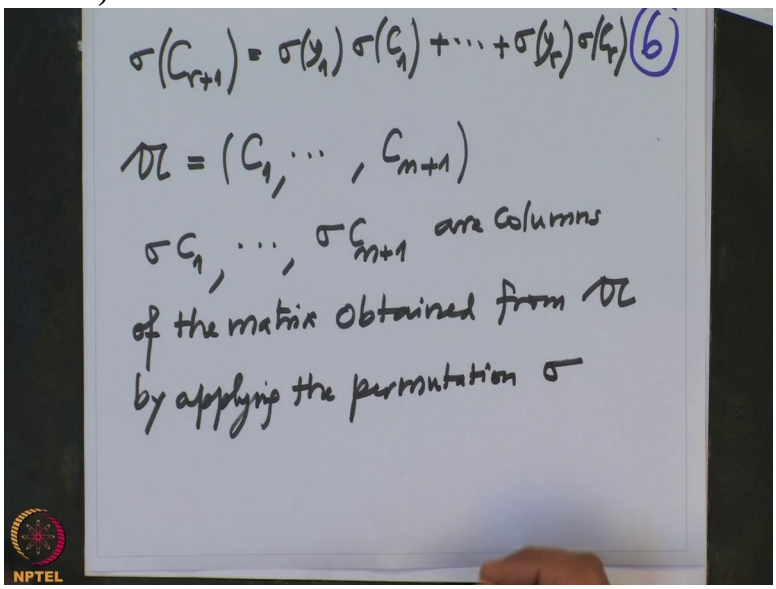
Alright, now if I apply σ to the matrix I will get, so σ of C_1 etc, σ of C_{n+1} are the columns, are columns

(Refer Slide Time 18:03)



of a matrix, of the matrix obtained from A, the matrix A by applying the permutation σ .

(Refer Slide Time 18:30)

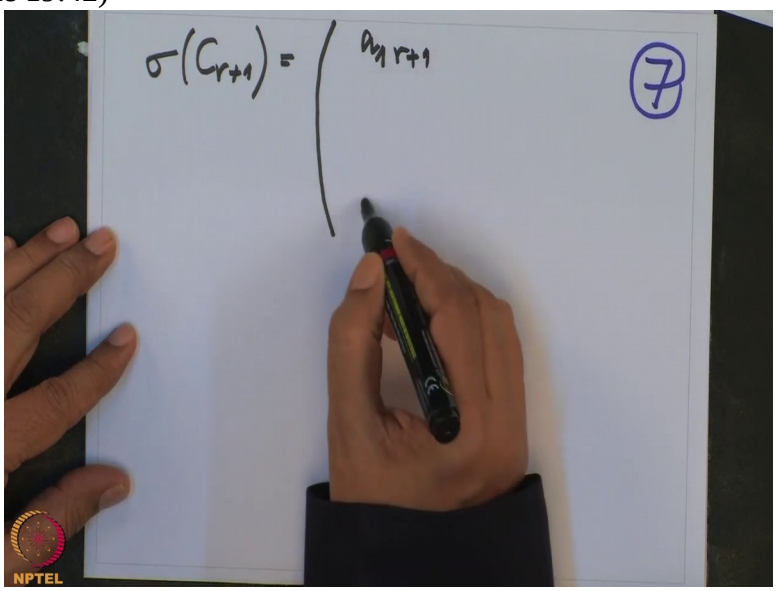


So I have σ , I have the matrix and I have the automorphism of σ , so I apply to the columns. And then the new columns will be $\sigma(C_1),\ldots,\sigma(C_{n+1})$; that will be the new column.

And the above equation shows that the $r+1$ th column is this one. So the r, so the columns are not changing. The columns are only getting shuffled. So in particular the σ_{r+1} is a column somewhere, right.

But then I want to rewrite this column so that, so from here I want to conclude. Now to demonstrate what will be the $\sigma(C_{r+1})$? This is, typically will look like this. This is the, originally it was the $r+1$ th column. So the entries are a_1 ,…, a_{r+1} is fixed. So that the next entry is fixed;

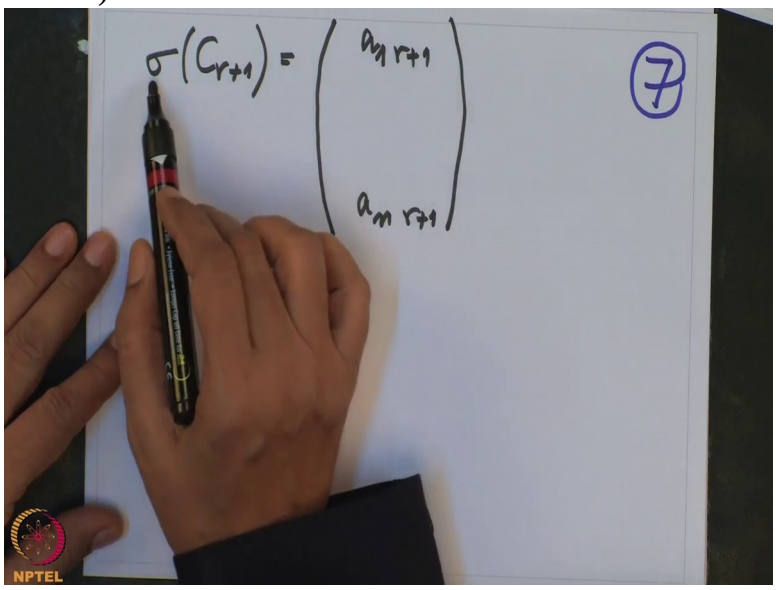
(Refer Slide Time 19:42)



a_{nr+1} . This is the column $r+1$.

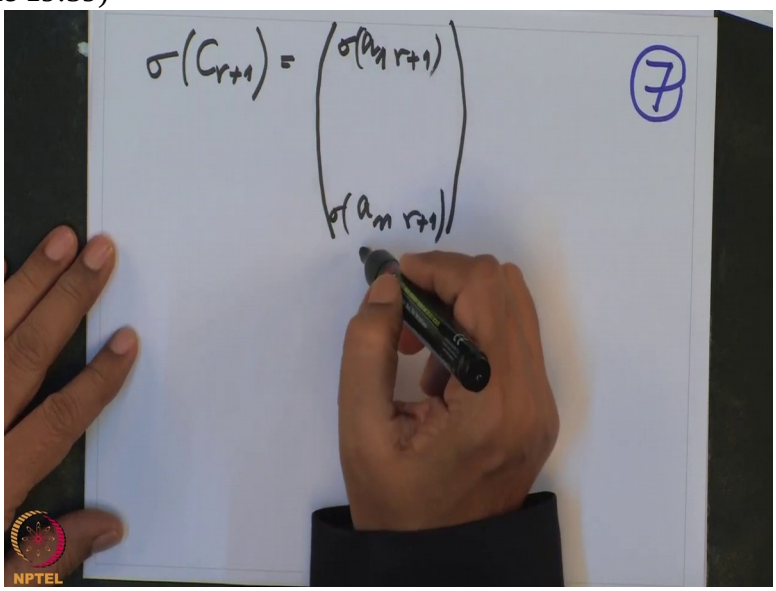
And these I have, this column and I have

(Refer Slide Time 19:53)



applied σ to this, σ to this. But this column

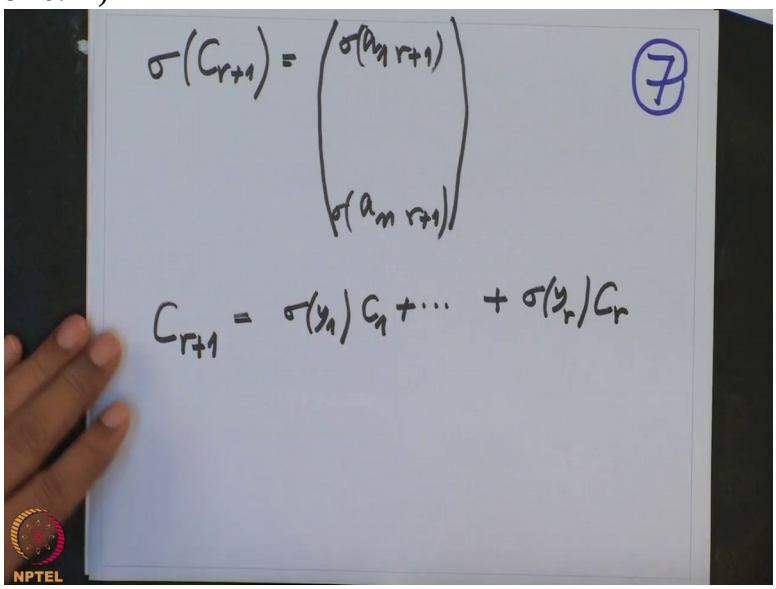
(Refer Slide Time 19:59)



is again a column somewhere, again the same column. So when I rearrange, when I rearrange the rows now, so the equations are same.

Only they are numbered different. So if I use that, that means σ , if a original column $\sigma(C_{r+1})$, this column is also same as $\sigma(y_1 C_1)+...+\sigma(y_r C_r)$.

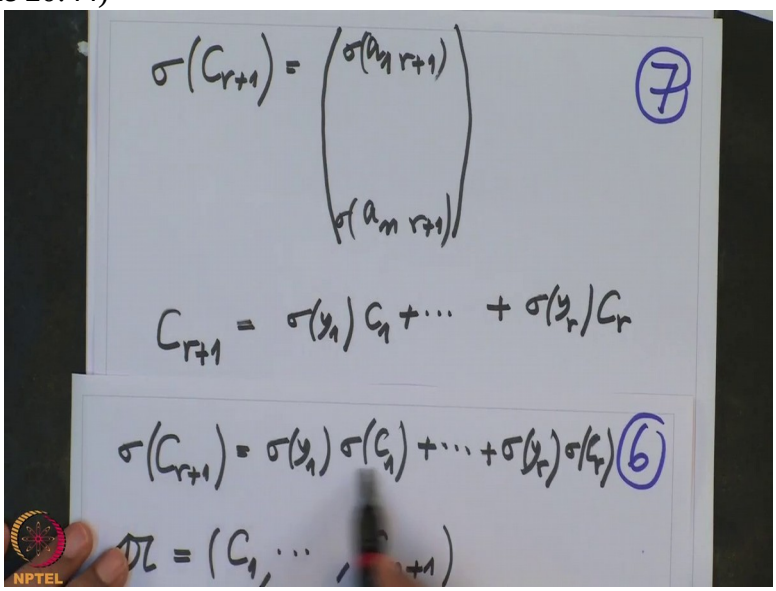
(Refer Slide Time 20:41)



You see what I am saying.

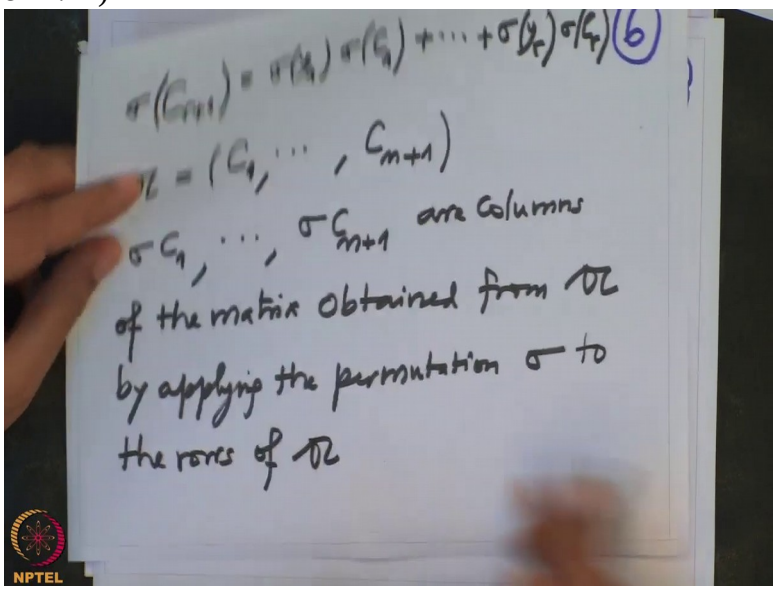
I am saying the following. We had this equation.

(Refer Slide Time 20:44)



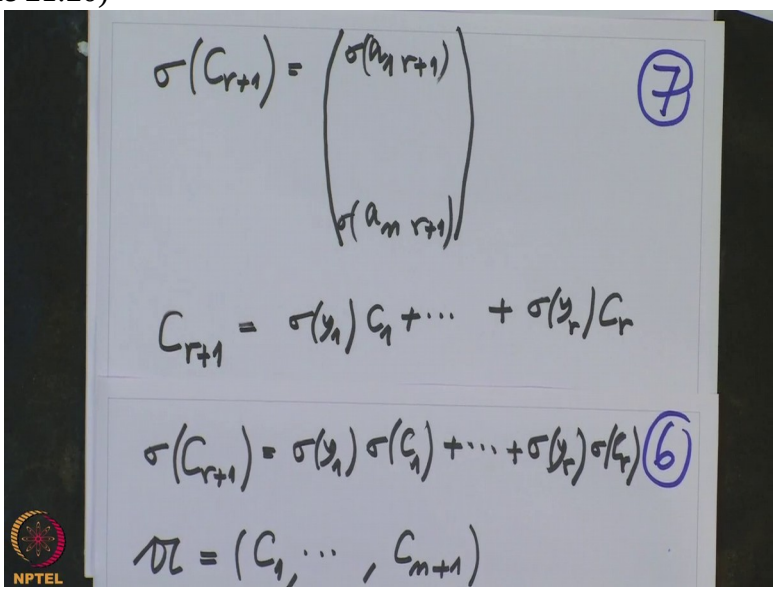
And in this I want to rewrite the rows. When I rewrite the rows I will get this column C_{r+1}, the, the rows, maybe I said one wrong word that this, this matrix is obtained from A by applying a permutation σ to the rows, rows of A.

(Refer Slide Time 21:14)



So therefore when I rewrite this equation, so if

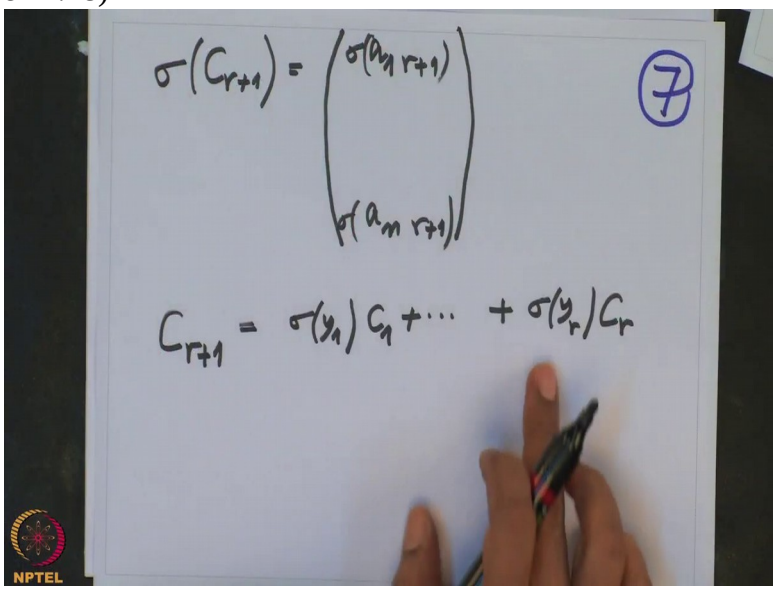
(Refer Slide Time 21:20)



the first row has gone to r th, some s th row then I will write that, write down that equation first.

And then these coefficients

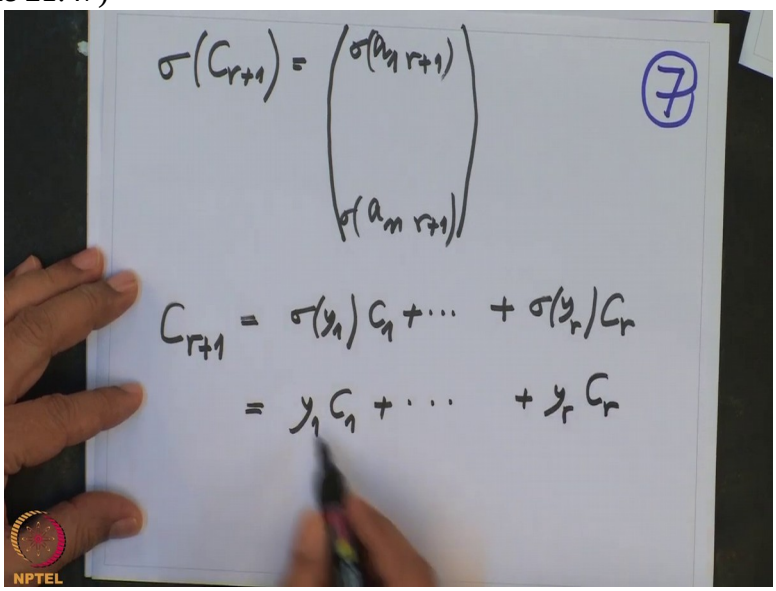
(Refer Slide Time 21:28)



are not changing. They are fixed, coefficients are same. This is an element in L. So therefore by rewriting the rows I get this equation. But this equation, so original equation we had was this.

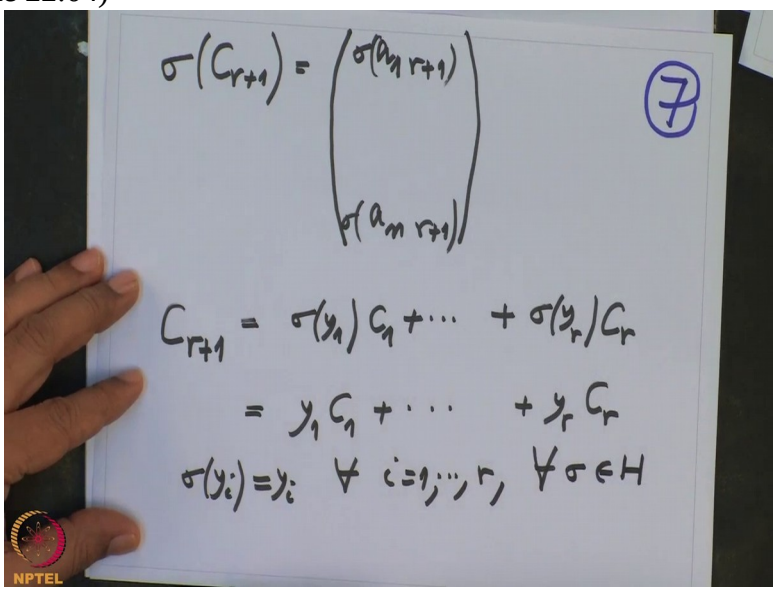
This and therefore

(Refer Slide Time 21:47)



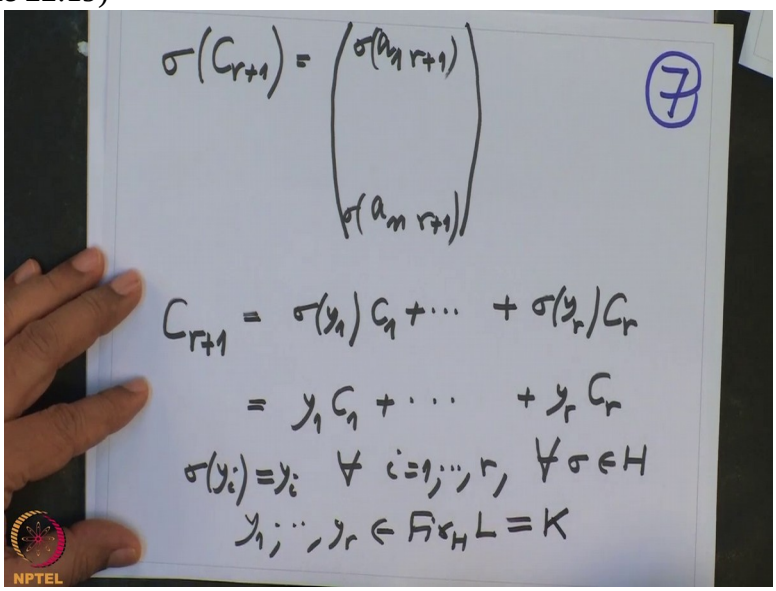
these y is are uniquely determined. Therefore we have no choice but $\sigma(y_i) = y_i$ for all i= 1 to r and this is true for every σ in H.

(Refer Slide Time 22:04)



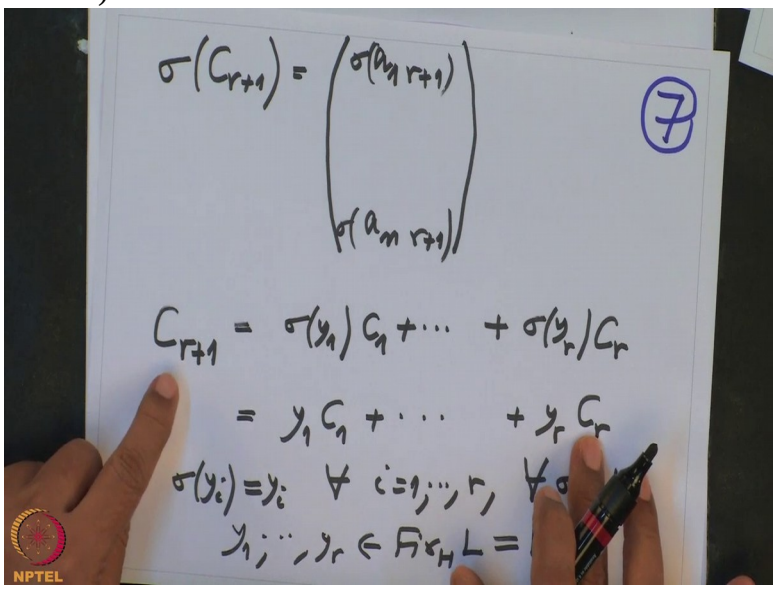
That simply means, so this means y_i is y_1 to y_r , all are elements of the fixed field which is K, which is denoting K.

(Refer Slide Time 22:19)



So therefore we have proved that, what did we prove? Now this C_{r+1} th column is y_1 to y_r, linear combination of this C_1 to C_r. Therefore $(r+1)$ th

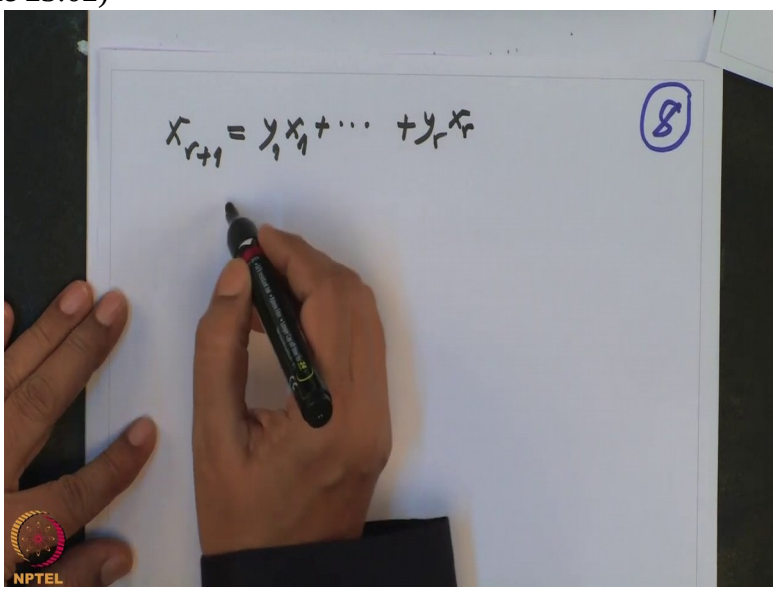
(Refer Slide Time 22:38)



element here, $(r+1)$ th row, that will be x r. So that will check that, so.

So, but you get x_{r+1} which is equal to $y_1 x_1 + \ldots + y_r x_r$.

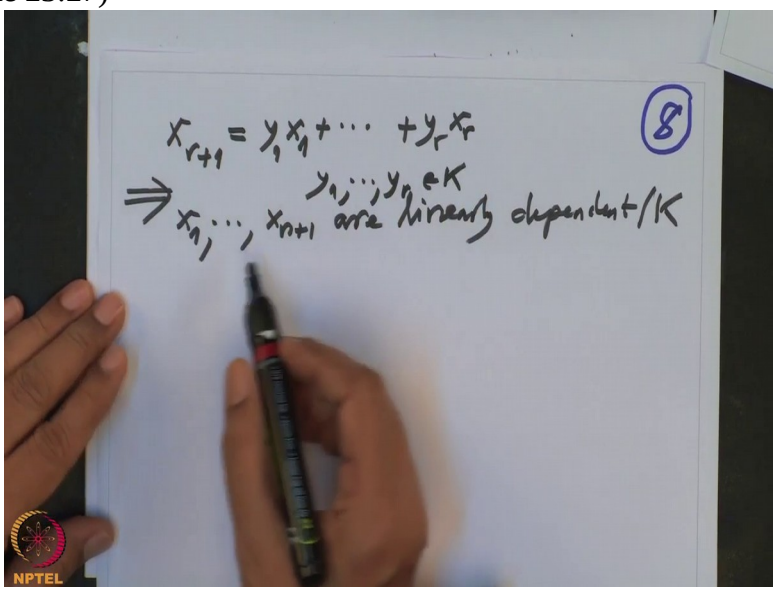
(Refer Slide Time 23:02)



This is, but this means $x_1, \ldots, x_{n+1}$ are linearly dependent over n because the coefficients are in K now, y_1 to y_r in K. That is what we have proved it.

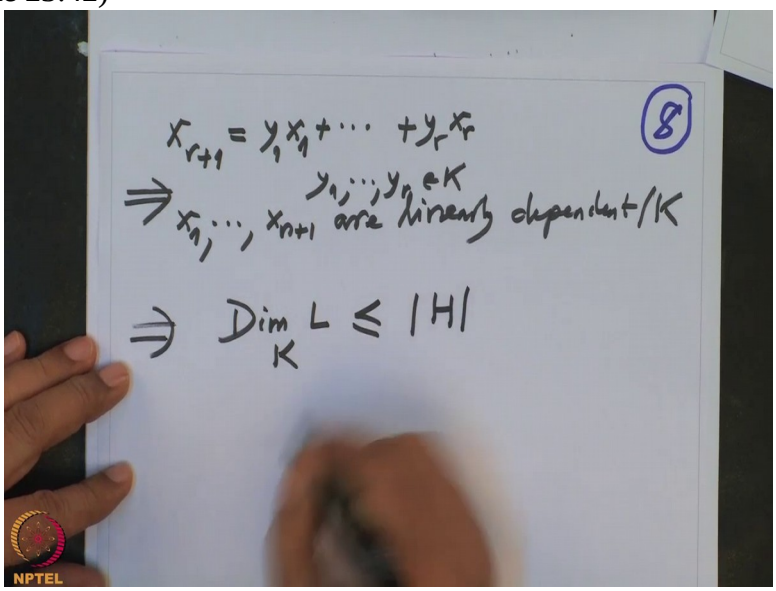
So we

(Refer Slide Time 23:27)



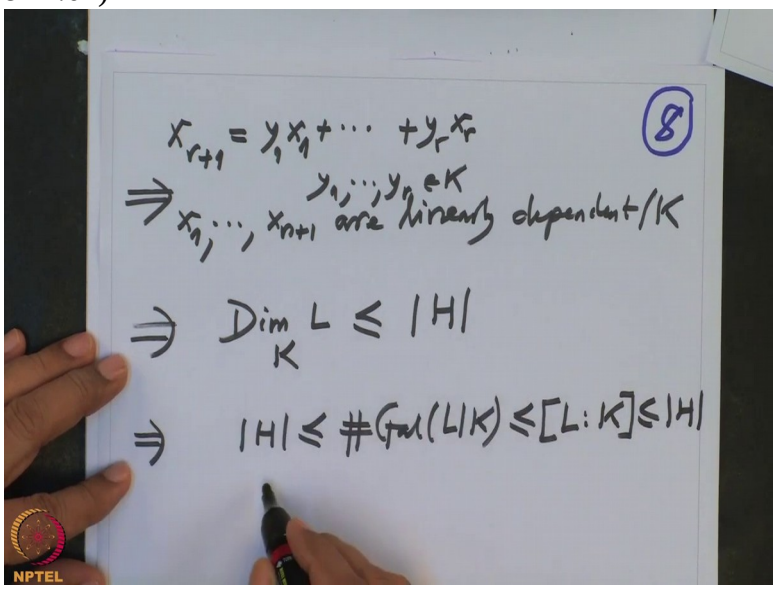
proved that they are linearly dependent. That is what we wanted to prove. And therefore the dimension of L over K will not be more than the cardinality of H.

(Refer Slide Time 23:42)



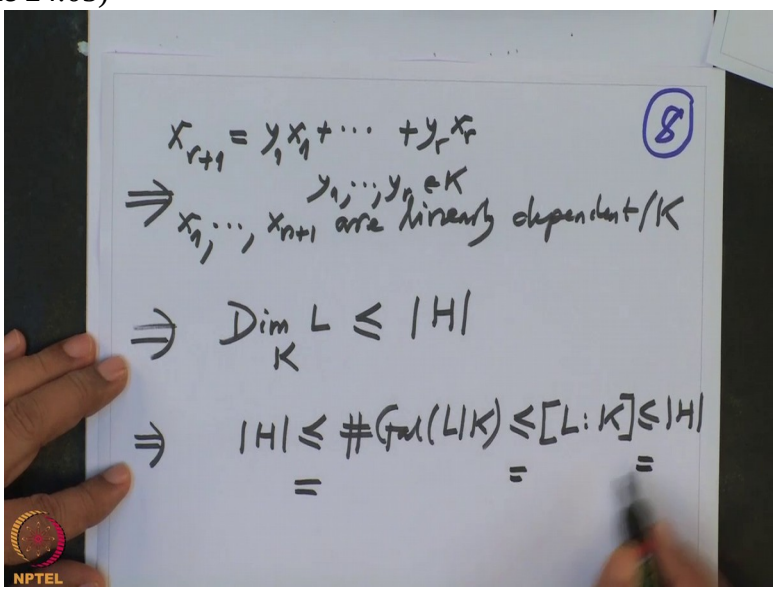
And once we have this, therefore and H is the subgroup of the Galois group so this cardinality will be smaller than cardinality of L over K which is smaller equal to L over K by Dedekind Artin and this is smaller equal to H. We have just now proved.

(Refer Slide Time 24:01)



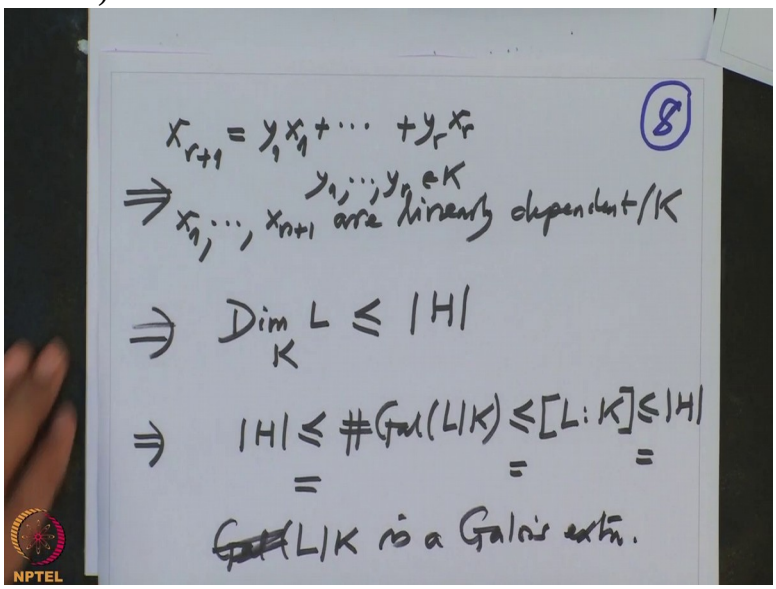
Therefore all are equalities, therefore

(Refer Slide Time 24:05)



Gal L over K, oh therefore L over K is a Galois extension.

(Refer Slide Time 24:18)



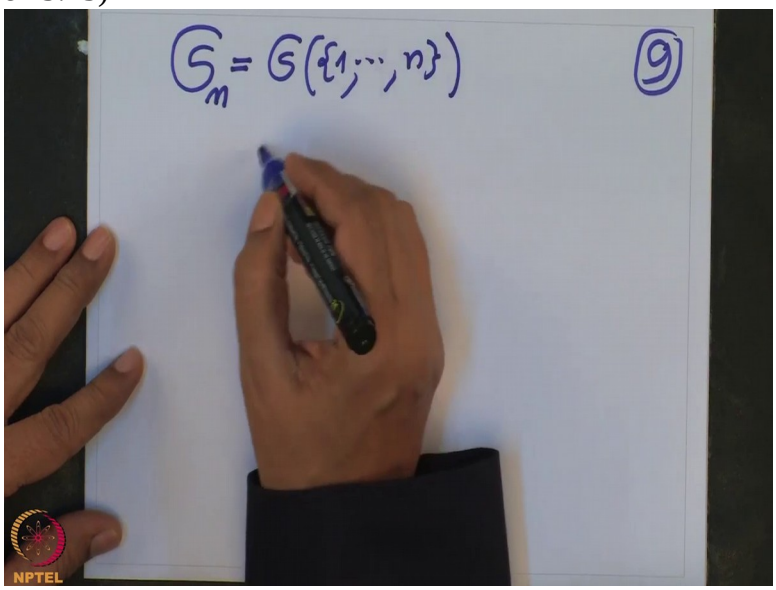
So this is what we have proved it. So it is very simple. You just have to note the following. You have, you form a matrix and apply σ to the matrix. So that means your rows are permuted according to the permutation.

So the first row might go to other row and so on and then you compare the new columns of this matrix. And from there you conclude that their, the coefficients are fixed and therefore they are in the base field K, the fixed field K and therefore they are linearly dependent and therefore dimension is less equal n and so on.

So I want to remind you why did I prove this. So first of all we have many extension, many examples of Galois extensions now, namely what you do is take a field, take a finite subgroup of automorphisms of the field and take the fixed field. And this, the original field will be Galois over the fixed field.

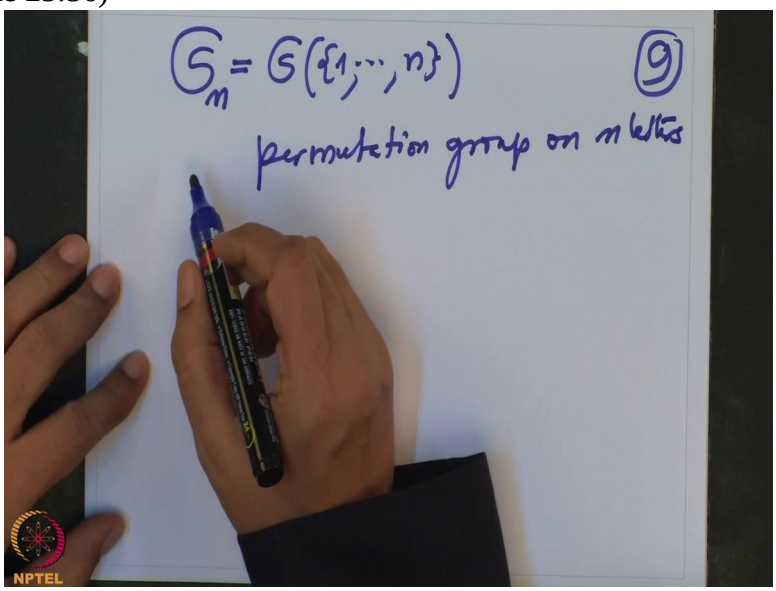
So for example I could simply do the following. So I could take, take the group S_n . Let us take the group S_n . This is my group. This is the permutation group. So these are the bijective maps from 1 to n to 1 to n.

(Refer Slide Time 25:43)



This is permutation group, group on n letters, on n letters. And everybody know this was the first group

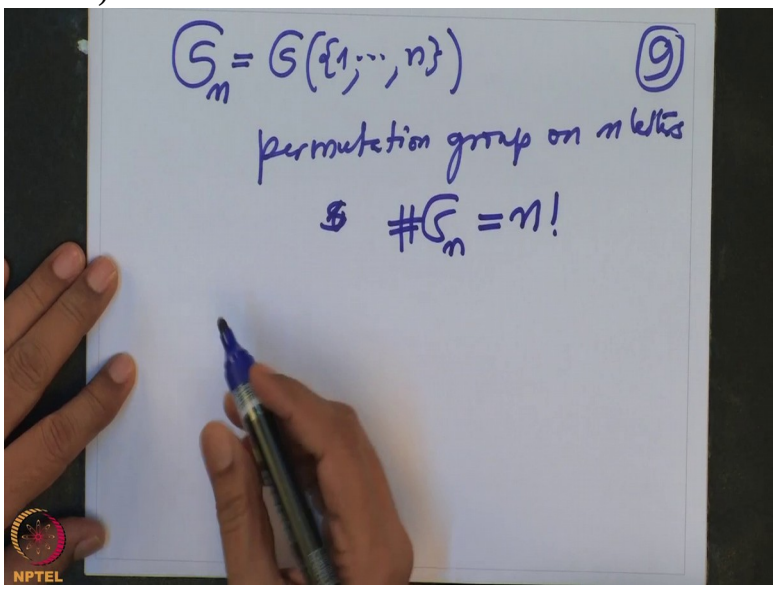
(Refer Slide Time 25:56)



that ever came to study and the study was mostly initiated by Lagrange.

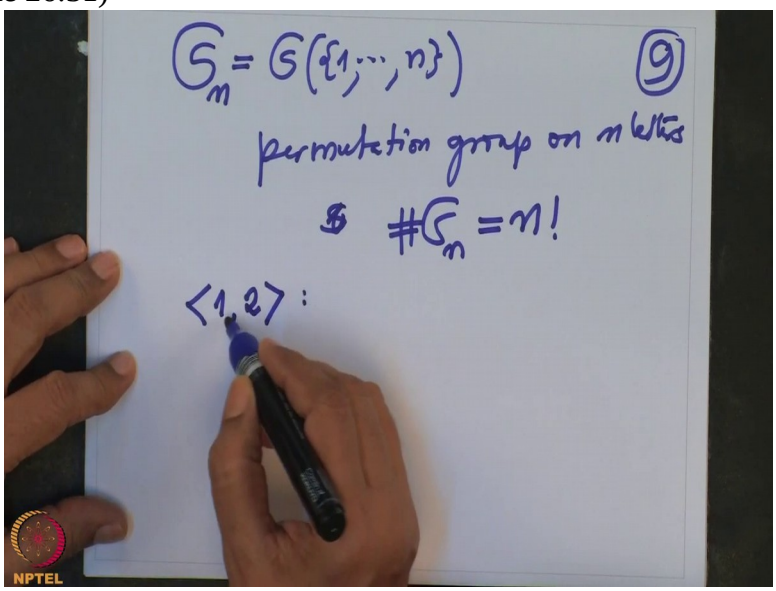
This group has order n factorial; order of S_n is $n!$. This is a big

(Refer Slide Time 26:16)



group and now I take very simple elements here 1, 2. This is a transposition. So this is a map, you should think, so the notation is, it is written

(Refer Slide Time 26:31)

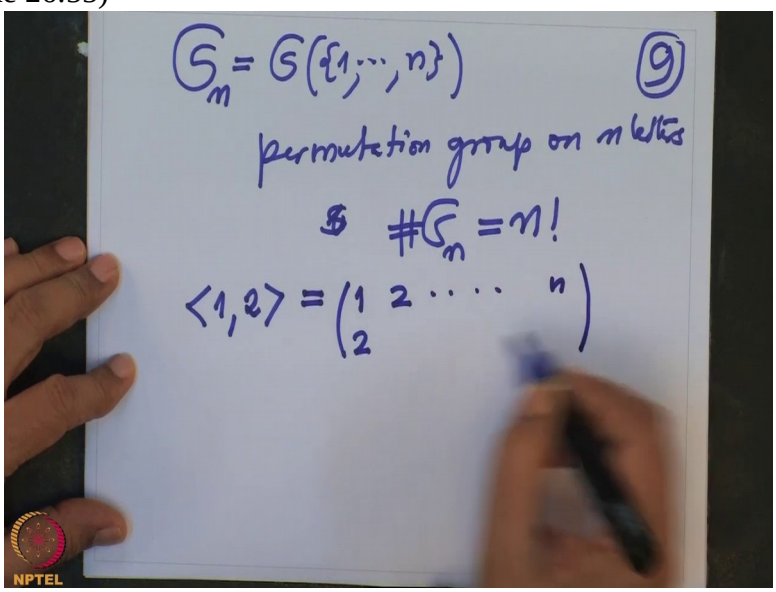


like this that means 1 goes to 2, 2 goes to 1 and the remaining elements are fixed.

So the notation used, the various people use various notation. When there is a more room for confusion, actually we should write it more explicitly and this is usually written as, see 1 goes to 2.

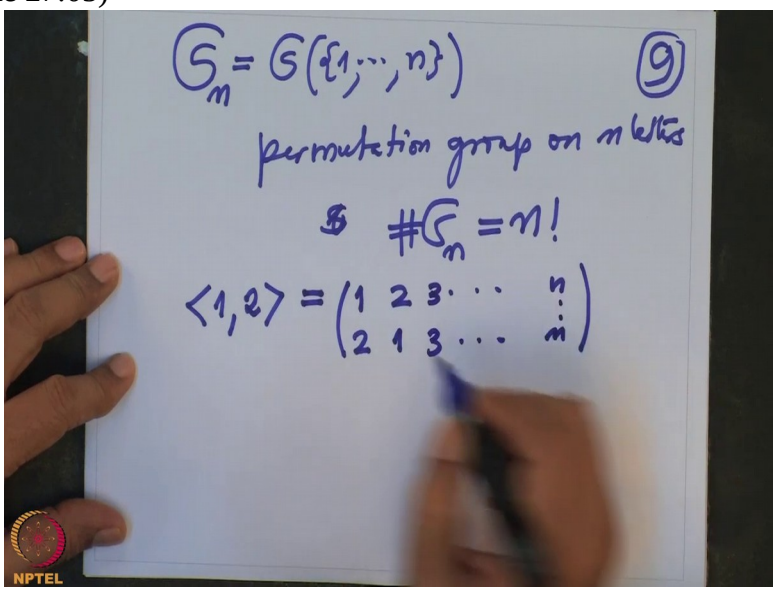
So upper row is the symbols 1 to n.

(Refer Slide Time 26:55)



And the down one is the images, 1 goes to 2, 2 goes to 1 and all other elements are fixed. So 3 goes to 3 and n goes to n

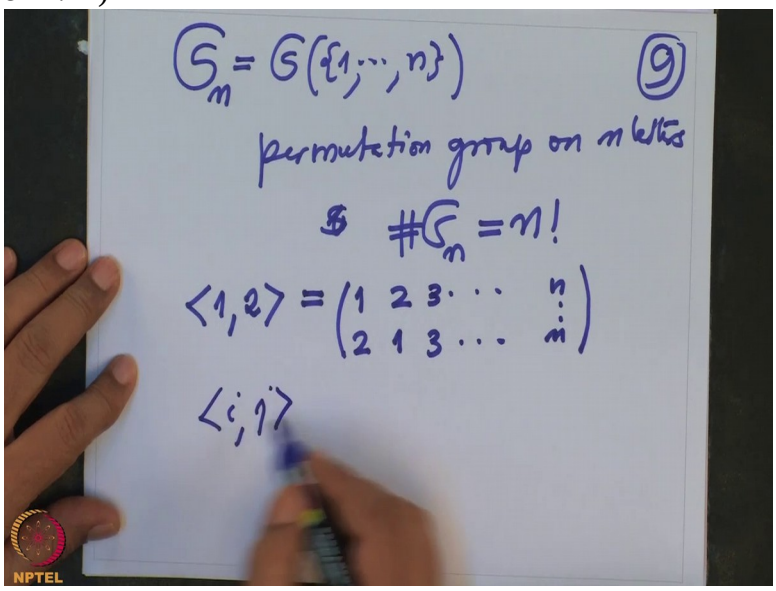
(Refer Slide Time 27:05)



when there is a confusion with the, how many letters etc. like that. These are called transpositions.

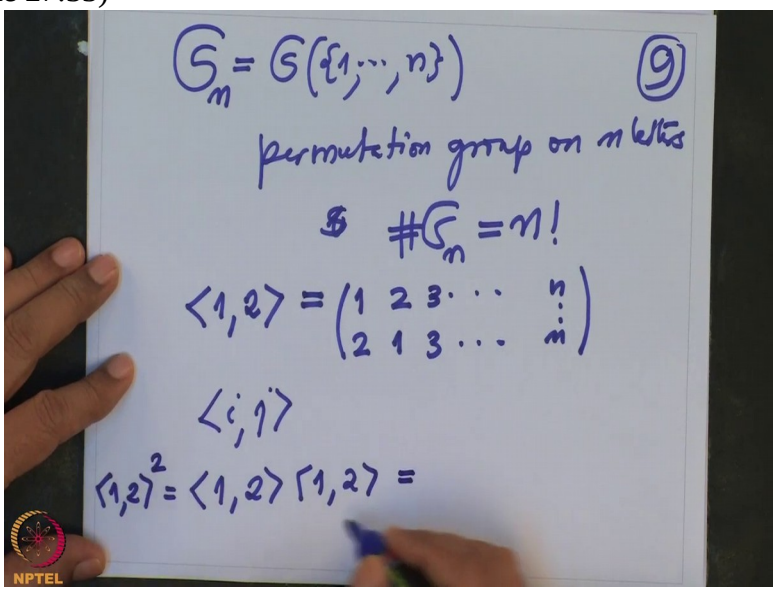
More generally i comma j,

(Refer Slide Time 27:14)



i j are interchanged. And these are elements of order; these are elements of order 2. Because when I compose 1 2 with 1 2, this is 1 2 square and what is the composition?

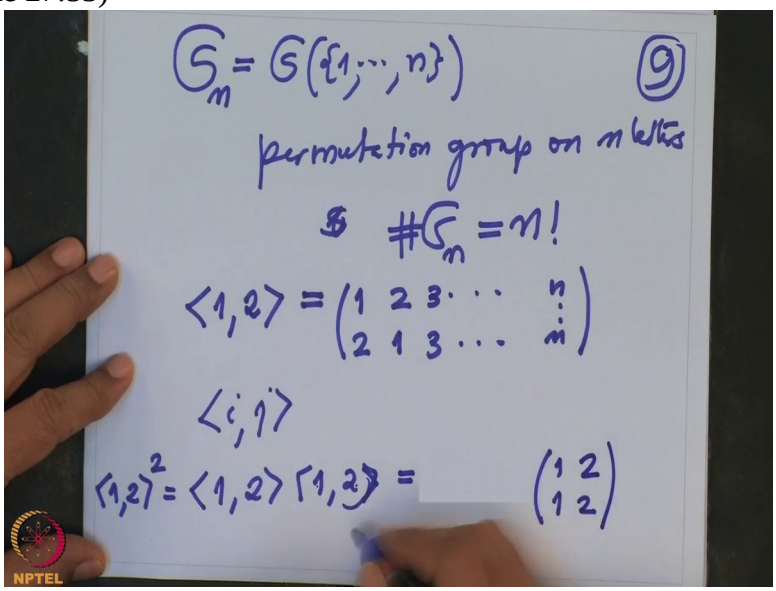
(Refer Slide Time 27:33)



Composition is usually read from this side, from right to left, not left to right. So 2 goes to 1 and 1 goes to 2.

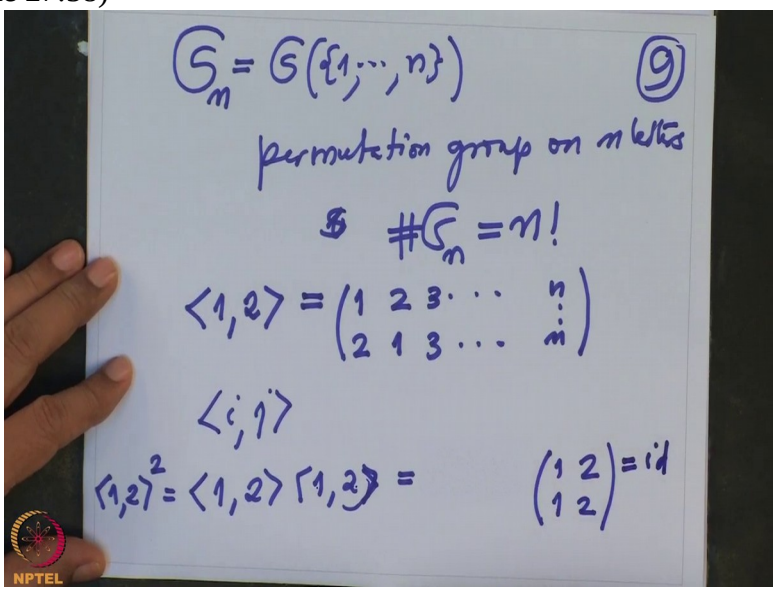
1 goes to 2, 2 goes to 1, so 1 goes to 1. Where do 2 go? 2 goes to 1 and 1 goes to 2. So 2 goes to 2 and

(Refer Slide Time 27:53)



everybody (()) 0:27:53.7. So this is identity.

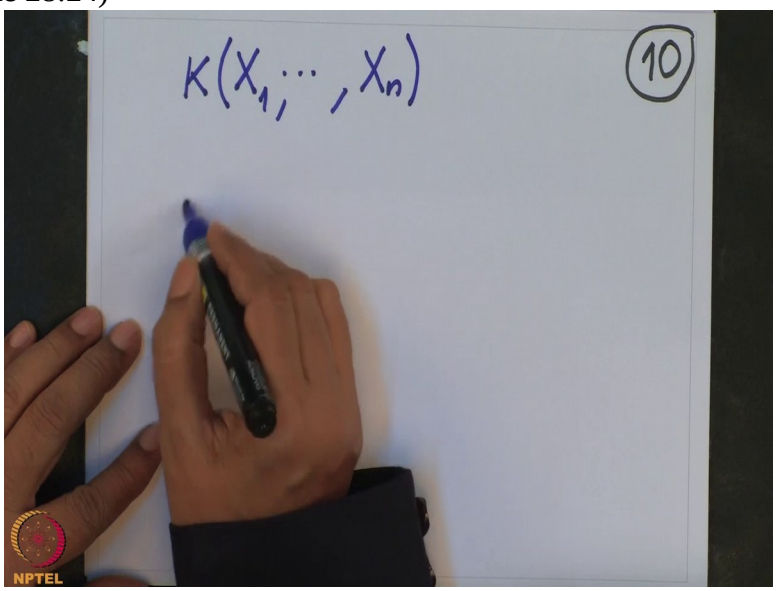
(Refer Slide Time 27:58)



So this is an element of order 2, transpositions are of elements of order 2 in the permutation group, not all elements of order 2 are transpositions. So what do I do?

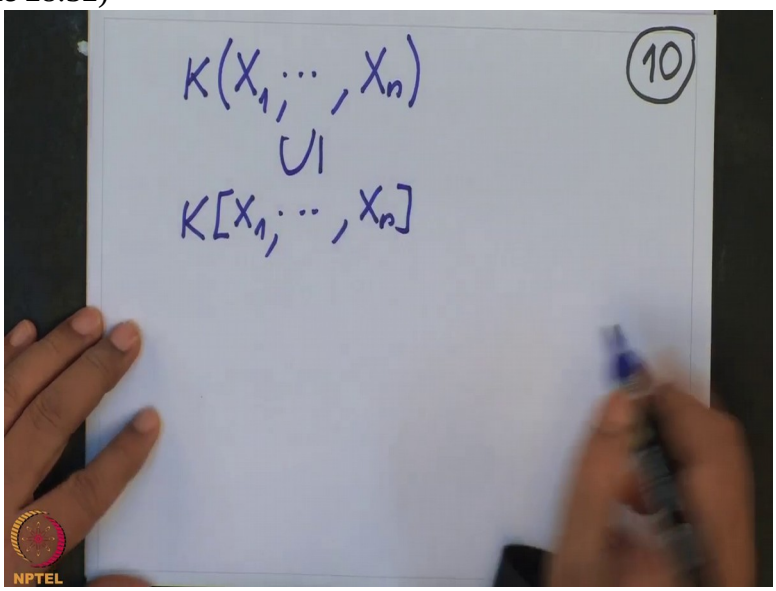
Now I take, take the big field, take any field K and take polynomials in many variables x 1 to x n. And this is the quotient

(Refer Slide Time 28:24)



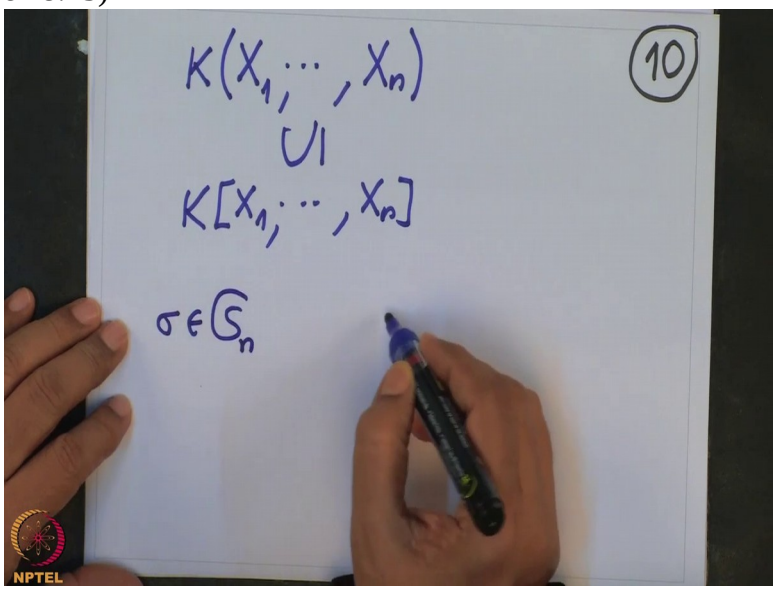
field of the polynomial array. Because we want a field, so this is a quotient field of the polynomial array.

(Refer Slide Time 28:32)



And now the permutations, every σ in S_n ; that gives an

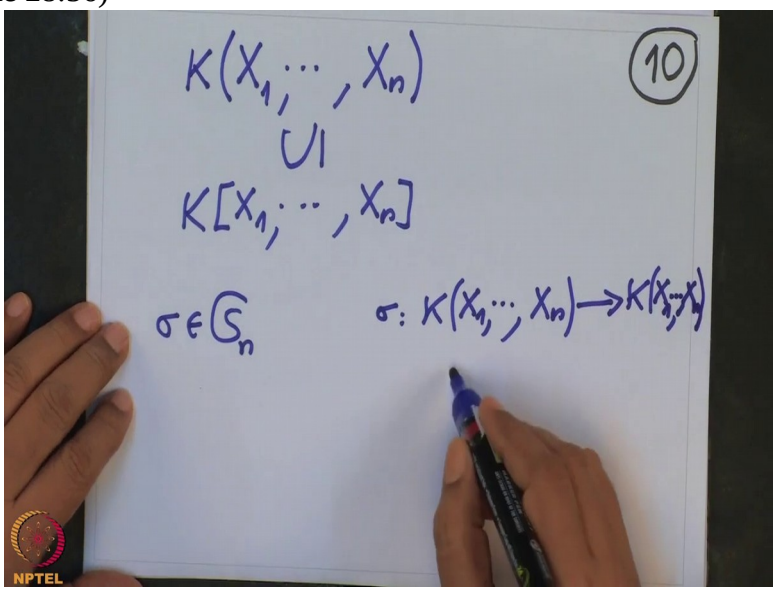
(Refer Slide Time 28:43)



automorphism of this field x 1 to x n.

To give the automorphism of the field I only have to give where

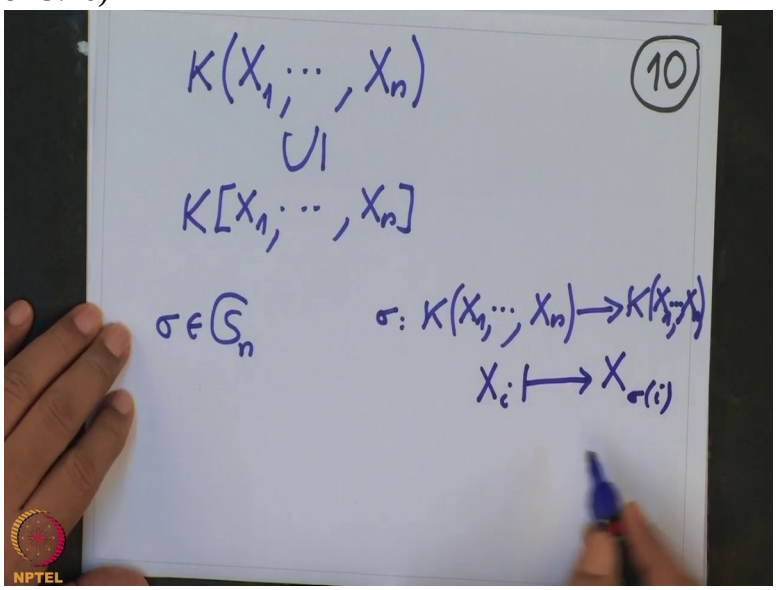
(Refer Slide Time 28:56)



the variables go. Because once I know where variables go and if I want an automorphism of the field which respects addition, multiplication etc so I only have to give where variables go. Then I know where polynomials go. And then I will know where rational functions go.

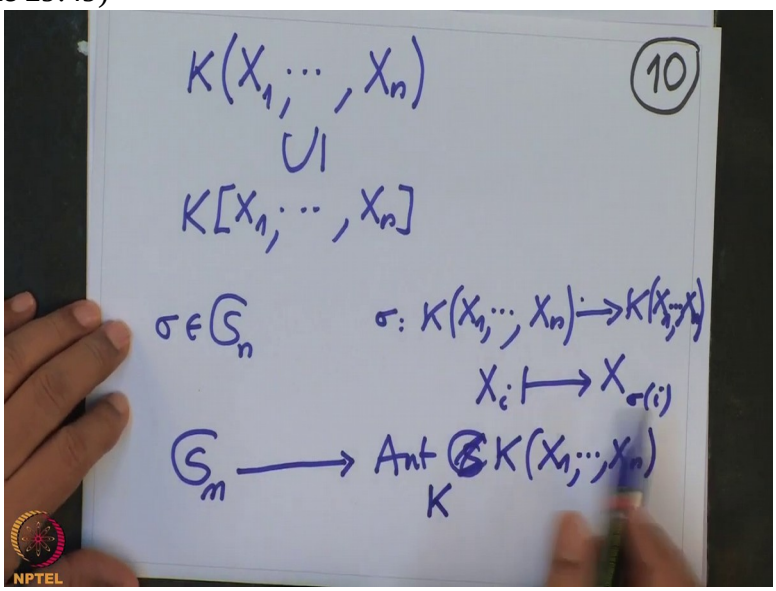
Therefore this automorphism will be uniquely determined where I will send the X is. But I send X is to some X of σ_i .

(Refer Slide Time 29:26)



σ_i is some other number. So this means an automorphism so therefore S_n , there is a natural map from S_n to the automorphism group of, automorphism group of the rational function field in n variables over K, because K linear,

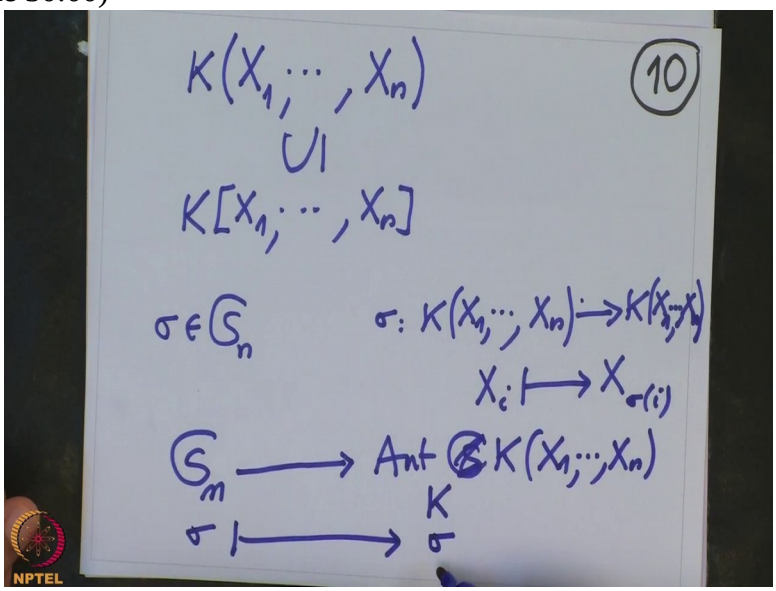
(Refer Slide Time 29:49)



K is fixed and X is are going to X σ is.

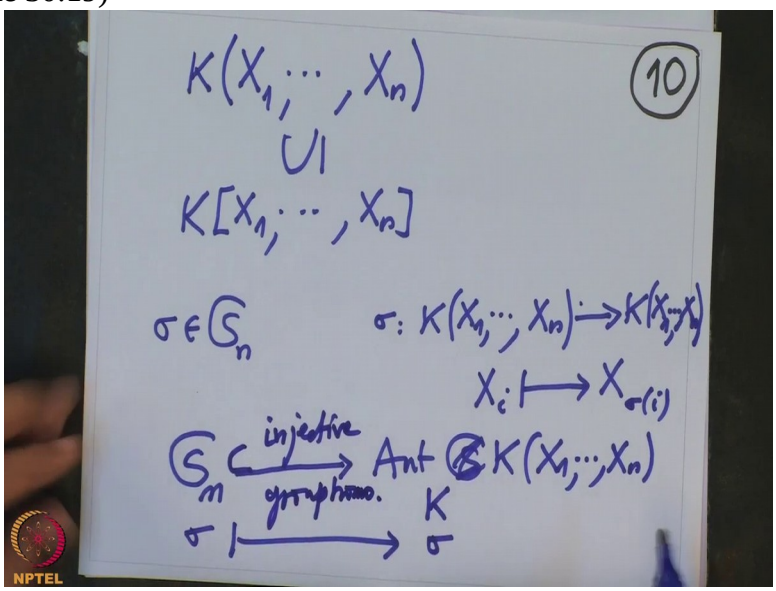
And what is this map? This σ going to this σ , this is the same, same letter.

(Refer Slide Time 30:00)



So σ defines an automorphism and it is clear that this σ is uniquely determined by the permutations, where it goes. So therefore this is actually an injective group homomorphism, injective group homomorphism.

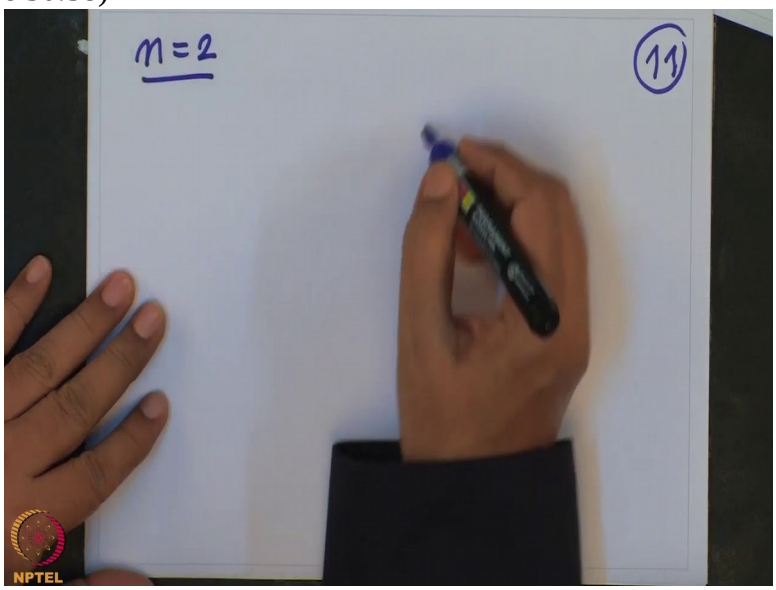
(Refer Slide Time 30:19)



There are many more automorphisms of the rational function field than this one.

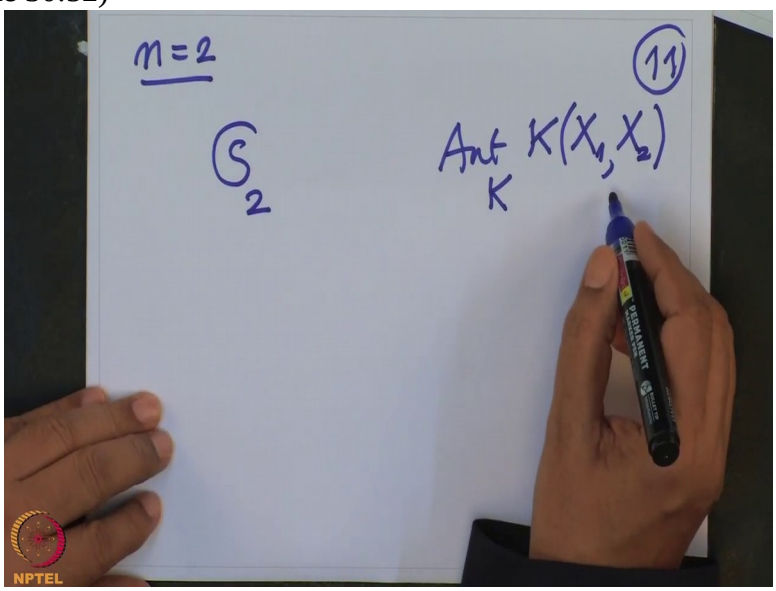
For example I only say this is injective. This will not be surjective in general. In fact it will almost never be surjective. For example just to tell you, take n equal to 2

(Refer Slide Time 30:38)



and then we have automorphisms of K rational function field in 2 variables, X_1 , X_2 and then this was S_2 . S_2 has cardinality 2 and this one

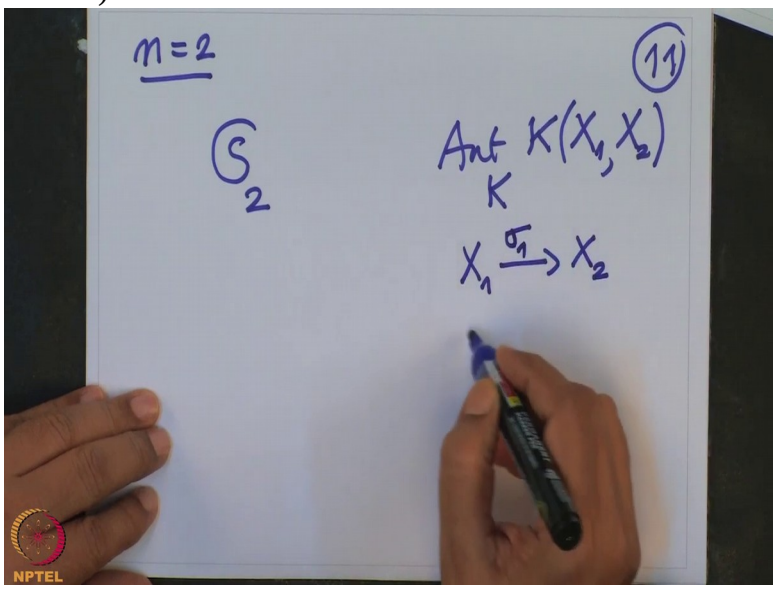
(Refer Slide Time 30:52)



I show you they are many more automorphisms.

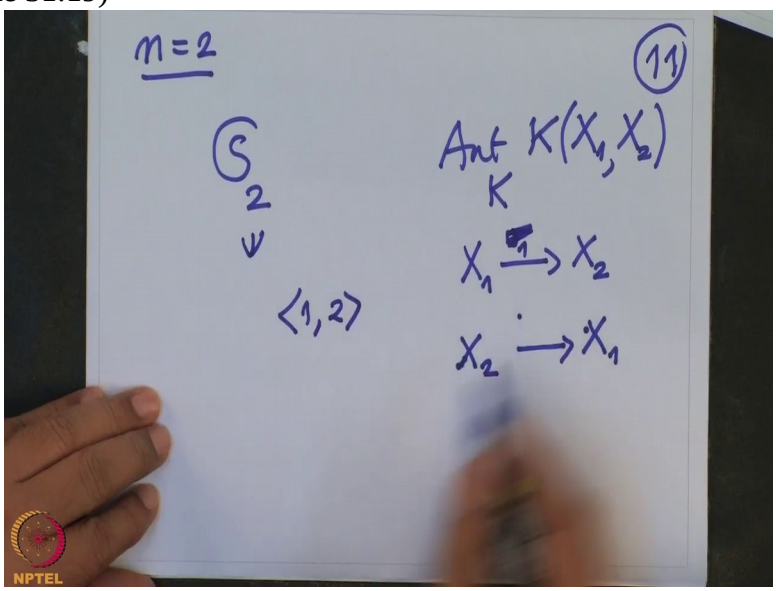
First of all, one automorphism is X_1 goes to X_2. This is σ_1, let us say.

(Refer Slide Time 31:02)



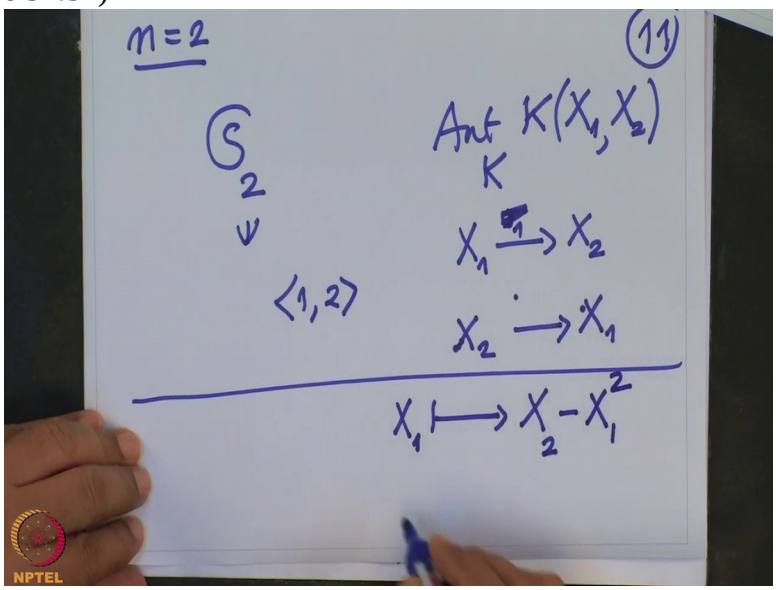
And other one, and X 2 is fixed. No X 2 cannot be fixed. X 2 goes to X 1. This is, this together is the transposition 1, 2. This σ is in 1, 2 and of course identity (()).

(Refer Slide Time 31:19)



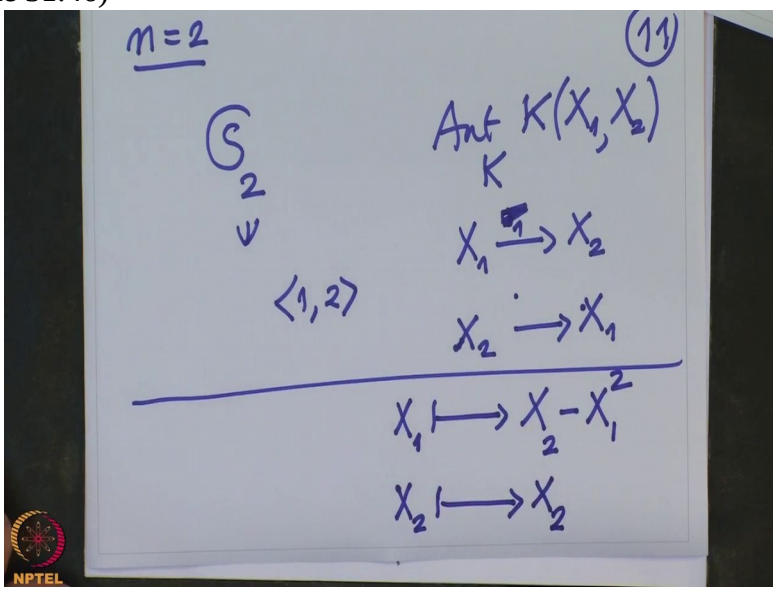
And I want to produce one more automorphism of the, this field over K. So look at that. X 1 I want to map it not to X 2 or not to variable but I will map it to X 2 plus or minus X 1 square.

(Refer Slide Time 31:37)



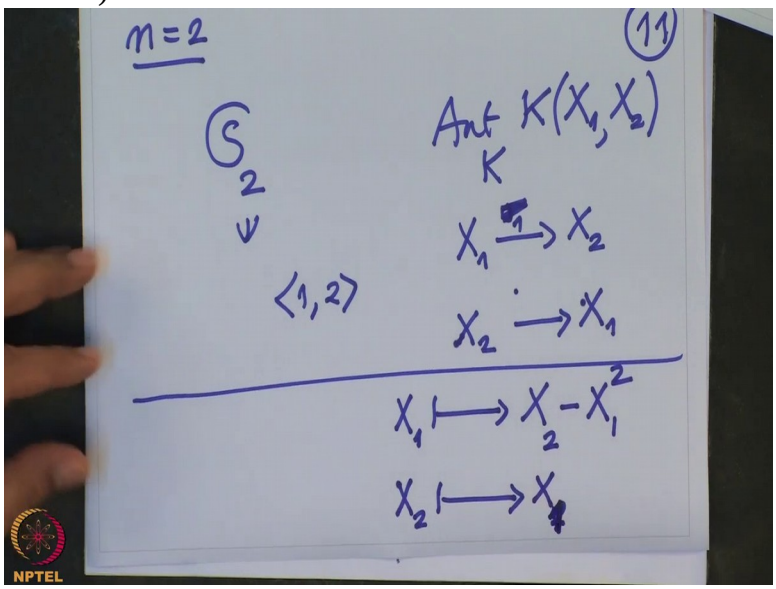
And X 2 is fixed.

(Refer Slide Time 31:46)



I claim this is an automorphism. I should say X 1.

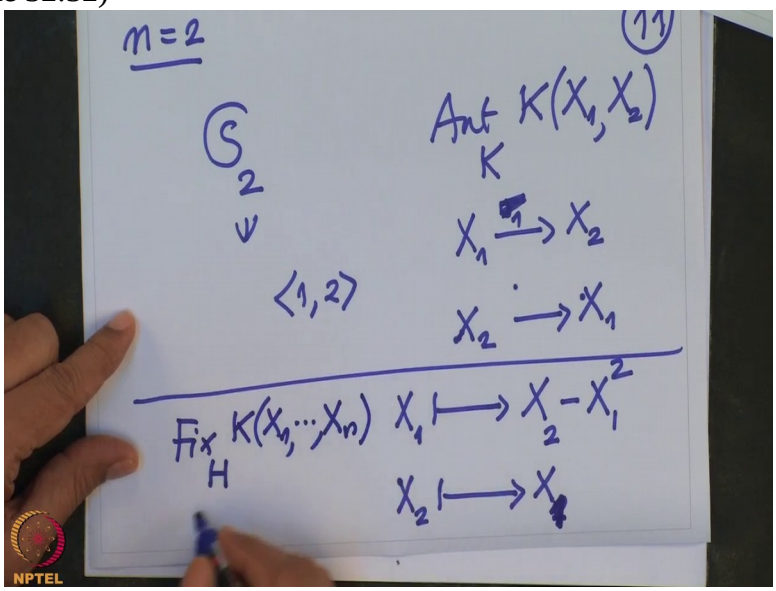
(Refer Slide Time 31:55)



So X 1, X 2 are in the images but this is not of the form this. Because this degree I want to, I am bringing the degree.

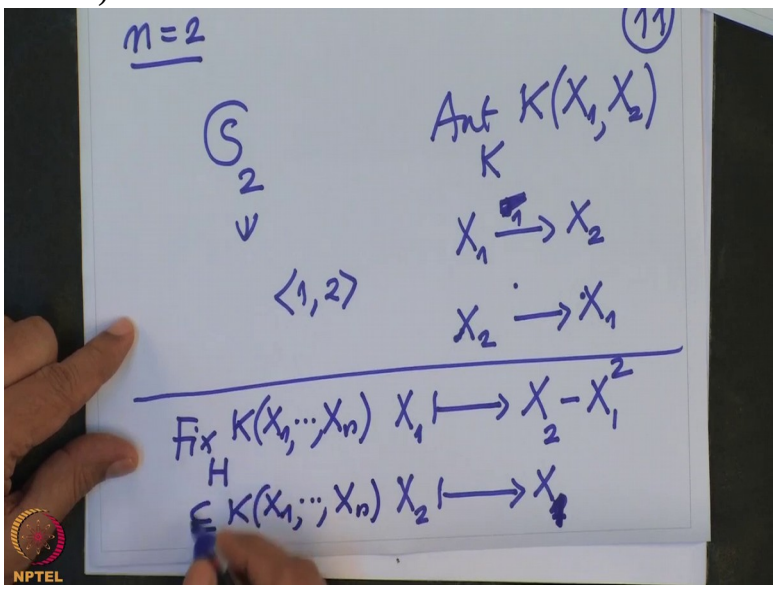
So there are many more automorphisms of the rational function field in n variable over K. They are not only the automorphism but automorphism group is definitely a subgroup there. And I can always take a subgroup of S_n and take fix field of that. So fix field of any subgroup H of this, this is a

(Refer Slide Time 32:32)



subfield of K x 1 to x n. And what we checked that? This is the Galois group

(Refer Slide Time 32:41)



and the Galois group; this is nothing but the given H. This is what we have checked in the above theorem.

And this, I will come back to this more precisely about the automorphism groups of the rational function field and use it also more precisely to prove, produce more examples. And so on.

(Refer Slide Time 33:06)

And then apply to the, the finite field extensions of Q to decide some more facts about the Galois group and so on. Thank you very much, we will continue next time.