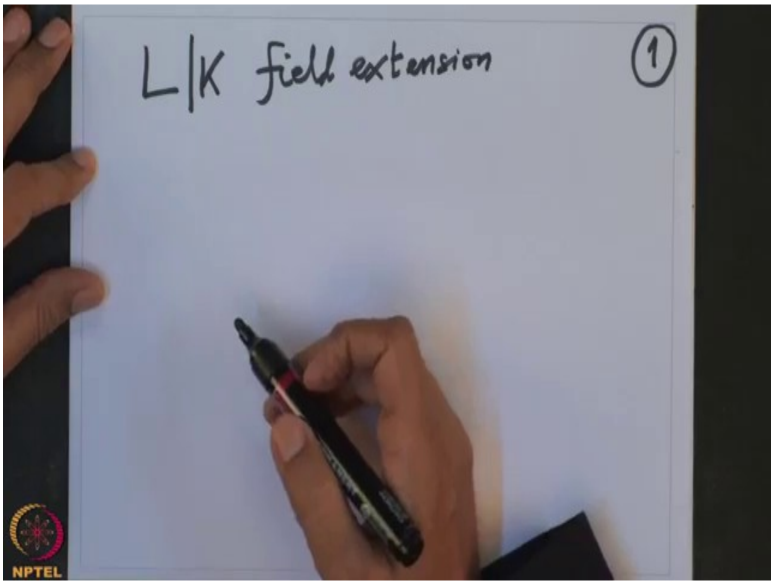
Galois' Theory
Professor Dilip P. Patil
Department of Mathematics,
Indian Institute of Science, Bangalore.
Lecture No. 24

Automorphism groups of a Field Extension

In the last lecture, we have seen a group actions and some easy examples, today I will start with a field extension and then so called the Galois group of that and this will be the central theme in our course, so let us set up some notations.

(Refer Slide Time: 1:02)

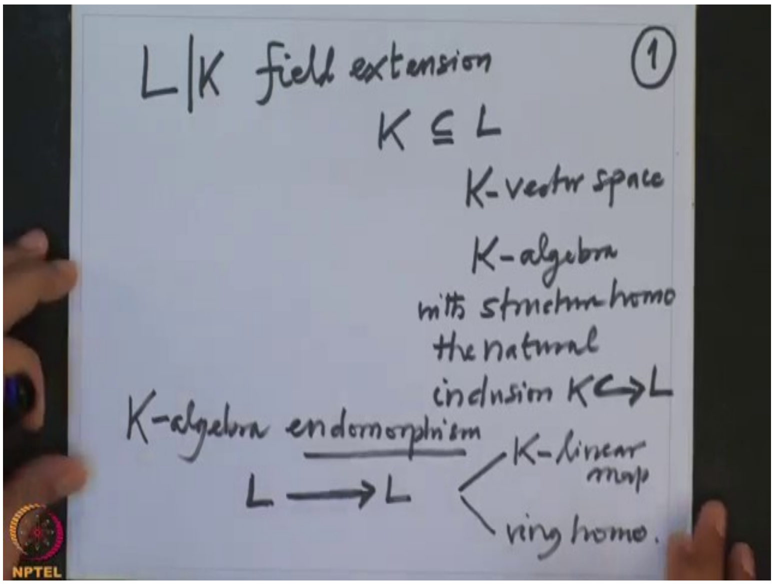


$L|K$ field extension

1

So I will usually denote L over K field extension, to each such field extension I will associate a group, what that group will be called a Galois group.

(Refer Slide Time: 1:27)



$L|K$ field extension 1

$K \subseteq L$

K-vector space

K-algebra

with structure homo

the natural

inclusion $K \hookrightarrow L$

K-algebra endomorphism

$L \longrightarrow L$

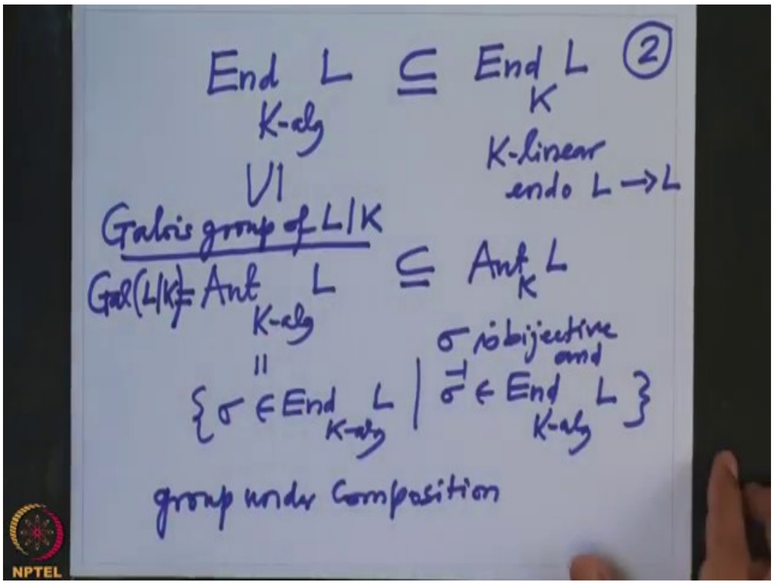
K-linear map

ring homo.

So when you will a field extension that means K is a field of L that means the bigger field L you can think a vector space over K, so this L is a K vector space, not only K vectors space it is because it has it is own multiplication as a ring, so this actually K algebra, these we saw in earlier lectures it has a structure of K algebra and usually when one says algebra then there is a structure homomorphism, in this case the structure of homomorphism in this inclusion in map.

This naturally inclusion with structure of homomorphism the natural inclusion K to L, this gives an algebra structure of K algebra structure of on L, on the field L, so therefore it makes sense should talk about K algebra endomorphism for examples, endomorphism from L to L, that means when one says K algebra endomorphism means let us spell out what it means for sure it is a map from L to L, it is a K linear map and also it is a ring of homomorphism, that means it is preserves the multiplication, that means it respect the multiplication and obviously we have made our convention earlier that under ring of homomorphism, multiplicative identity goes to multiplicative identity, so that is still we are assuming that and the set of all endomorphisms of the field L.

(Refer Slide Time: 4:08)



$$\underset{K\text{-alg}}{\mathrm{End}}\, L \subseteq \underset{K}{\mathrm{End}}\, L$$ ②

K-linear endo $L \to L$

$\cup\!\vert$

Galois group of $L|K$

$$Gal(L|K) = \underset{K\text{-alg}}{\mathrm{Aut}}\, L \subseteq \mathrm{Aut}_K\, L$$

σ is bijective and

$$\| $$

$$\{\sigma \in \underset{K\text{-alg}}{\mathrm{End}}\, L \mid \sigma^{-1} \in \underset{K\text{-alg}}{\mathrm{End}}\, L\}$$

group under Composition

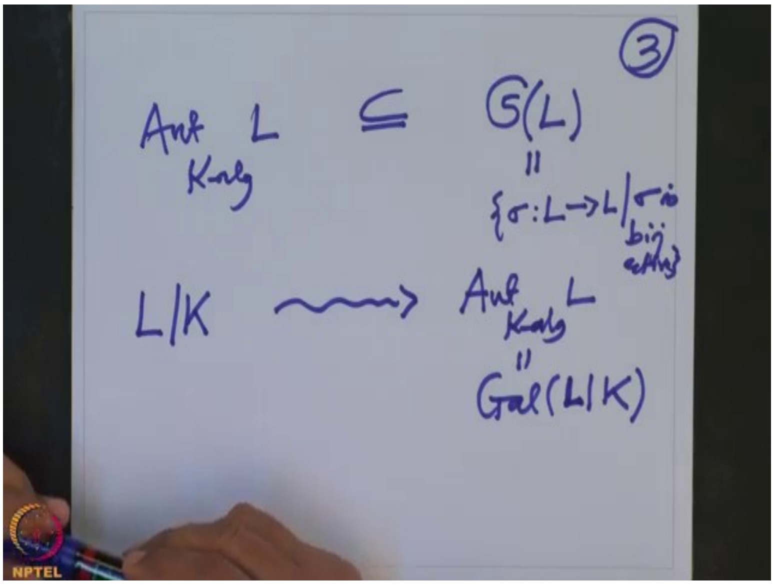
Of the K algebra L that I will denote End K algebra L, so this is just to remember that this is K algebra endomorphisms of L, L to L and K algebra that means it is K linear, that means it is a vector space endomorphism and in addition to that it is a ring of homomorphism, so if I write some from these sum notations will be obvious from $End_K L$, this is just K linear one, these are just a vector space K linear endomorphisms of L to L only the vector space that means it is a K linear and it respects the addition, so therefore this is a subset of these, it may be a proper subset.

And when I say Automorphism, $Aut_{K-algebra} L$, this means they are not only endomorphism, but there bijective and inverses are also K algebra endomorphism, so this is precisely all those σ from endomorphisms such that σ^{-1} is also endomorphism, the σ is bijective and σ^{-1} also is an K algebra endomorphism of L.

So this is a subset of these and more importantly, this is actually a group under composition, it is a group under composition, because we have seen if you have two algebra homomorphisms they are composition is also algebra homomorphism, already inverses algebra homomorphisms, so under composition, it becomes a group and let me also remind you this is, if I write only $Aut_K L$, this should mean only a vectors space automorphisms.

So this is also subset here and it maybe a proper, this also may be proper and etc. So we are concentrating on these group, these group also I will keep denoting $Gal(L|K)$, this is called a $Gal(L|K)$, note that these group I have defined for arbitrary field extinction and the I still use a word Galois group because Galois is the first who started with such studying such a group, of course Galois started studying such a group in a very particular situation, but the name continues to be for arbitrary field extension, so couple of remarks about this group.

(Refer Slide Time: 7:29)



③

$$\mathrm{Aut}_{K\text{-alg}}\, L \subseteq \mathfrak{S}(L) = \{\sigma : L \to L \mid \sigma \text{ is bijective}\}$$

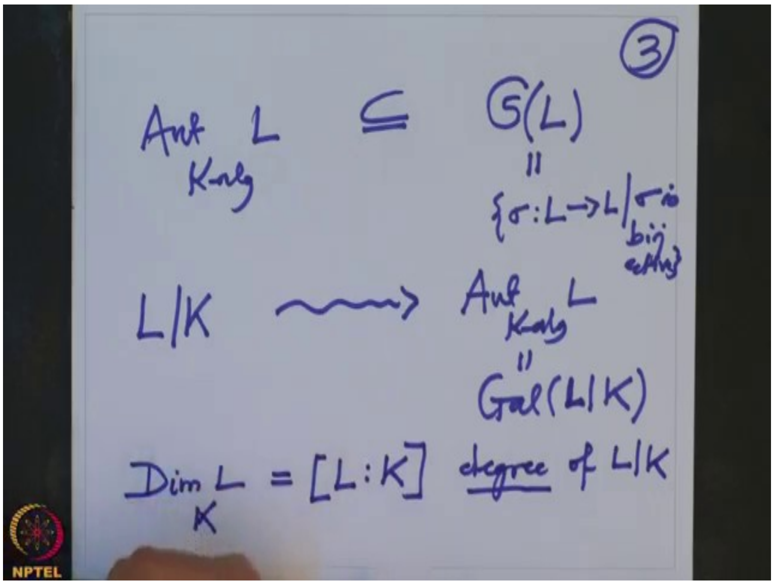
$$L|K \rightsquigarrow \mathrm{Aut}_{K\text{-alg}}\, L = Gal(L|K)$$

So first of all note that this $Aut_{K-algebra}L$ this is, if I take all bijective maps from L to L, $S(L)$, this is the notation I keep using last time also use, this is the set of all bijective maps from L to L, σ from L to L bijective, σ is bijective, this is called a symmetric group on the symbols L the symmetric group of L, so this is actually a subgroup of these, because we know that the multiplication binary operation of these group is a composition, and the same is, this is a group, this is a big symmetric group, this is a very big group but this is some elements among them, this is the Galois group.

And we are going to study, we are going to do the following this field extension and a group that is $Aut_{K-algebra}L$, this is Gal, I should start using the notation $Gal(L|K)$. Because the more you use the more you will get acquainted with, so this association from field, field extensions to groups, we are going to interplay between this, so we are going to extract information about field extension from this group and also conversely from this group information about the field extension and from field extension about this group both ways not just one way traffic both ways, so that is what, therefore we have to understand these association more and more ultimately that is what we will do it.

For example, if this group finite, if L over K is finite, if this group finite, if it is, what is the? What can be the order? And so on such questions, so in the beginning I will try to extract information only from the numeric invariants.

(Refer Slide Time: 9:52)



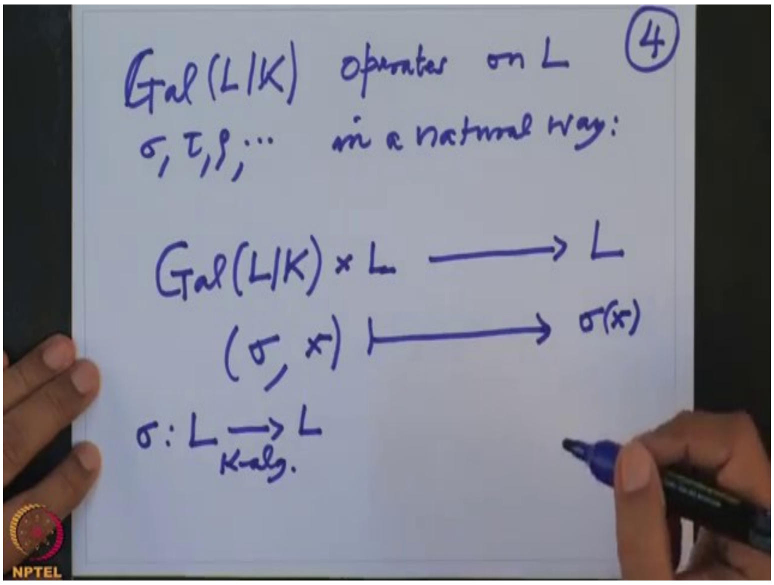
③

$$\operatorname{Aut}_{K\text{-alg}} L \subseteq \mathfrak{S}(L) = \{\sigma : L \to L \mid \sigma \text{ is bijective}\}$$

$$L|K \rightsquigarrow \operatorname{Aut}_{K\text{-alg}} L = \operatorname{Gal}(L|K)$$

$$\operatorname{Dim}_K L = [L:K] \ \underline{\text{degree}} \text{ of } L|K$$

For example, to a field extension we have because L is a K vector space, so we have this number dimension of L over K, this is the cardinality of a basis of L over K, this is also denoted by L over K and this is also called a degree of the field extension, degree of L over K. And also we have group, so we have the order of that group, so the first question is what is relation? And some kind of relations, so this is what first I am going to do that, this is the most important fact in this course will be the following, namely, this automorphism group, (Refer Slide Time: 10:37)



④

$\operatorname{Gal}(L|K)$ operates on L

$\sigma, \tau, \rho, \ldots$ in a natural way:

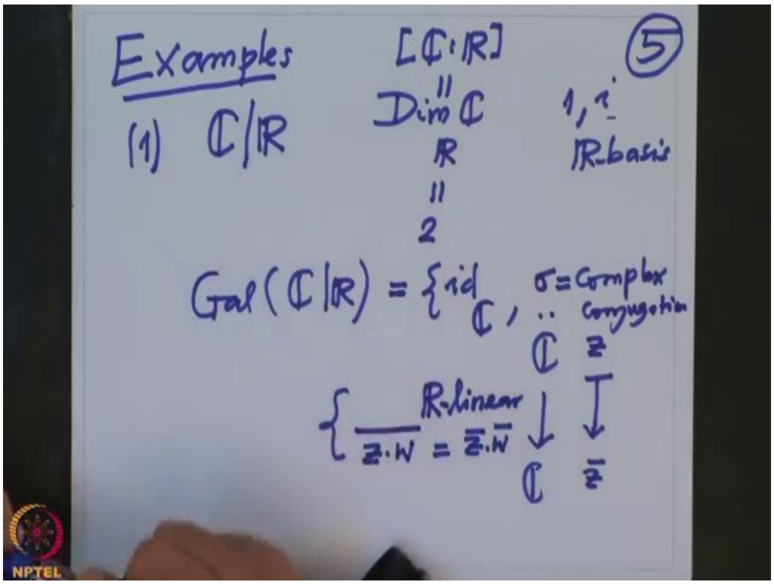
$$\operatorname{Gal}(L|K) \times L \longrightarrow L$$
$$(\sigma, x) \longmapsto \sigma(x)$$

$$\sigma : L \xrightarrow[K\text{-alg.}]{} L$$

So $Gal(L|K)$. The elements I will denote σ, τ etc. elements are denoted by σ, τ, ρ etc. they are automorphism of the field extension L over K, this group operates, last time we saw group operation . This group operates on L in a very natural way, in a natural way, what is a natural way it is? It is so natural that very easy to write, so I want a map from $Gal(L|K)\times L \rightarrow L$, this is my set X, the set X and this is a group and when I, when we know that the group operates means there is a map from $G\times L \rightarrow L$, which satisfy those two properties.

So what is a map? Take any σ and take any x element in L and when can I map it? How do I get another element in L that is σ of X, because σ is what? σ is an automorphism of L, K algebra automorphism, this is a K algebra automorphism, so σ operates on this, now the whole Galois Theory will centre around studying this operation. What does that mean? That means studying the orbits, studying the stabilisers and studying fixed points and so on, so the as we progress in this lectures, I am going to make the vocabulary of group actions more and more intimater and with supplement it by more and more examples.

(Refer Slide Time: 12:43)



Examples

5

(1) $\mathbb{C}|\mathbb{R}$

$[\mathbb{C}:\mathbb{R}] = \mathrm{Dim}_{\mathbb{R}}\,\mathbb{C} = 2$

$1, i$ $\mathbb{R}$-basis

$Gal(\mathbb{C}|\mathbb{R}) = \{id_{\mathbb{C}}, \sigma =$ Complex Conjugation

$\mathbb{C} \rightarrow \mathbb{C}$, $z \mapsto \bar{z}$

$\{$ $\mathbb{R}$-linear

$\overline{z\cdot w} = \bar{z}\cdot\bar{w}$

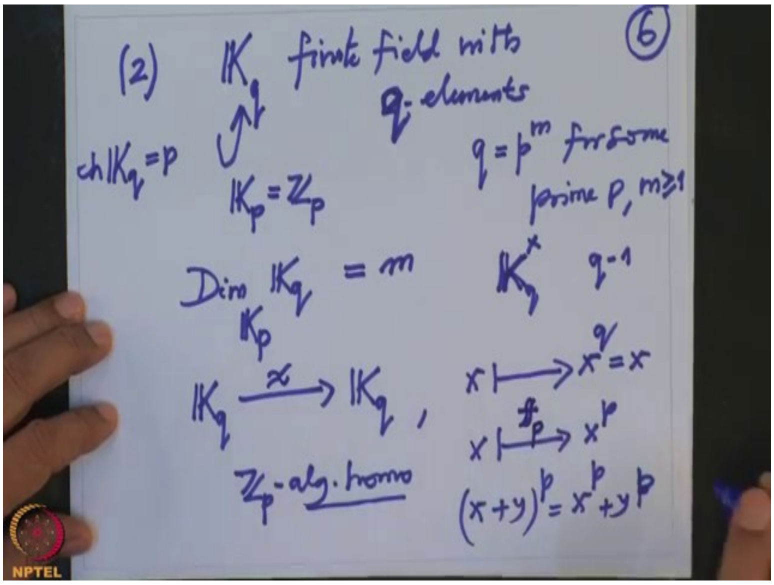
So before I, we go on to the numerical invariants, so some examples. I should write in this view now, so first of all, if I look at the extension, the easy one, $\mathbb{C}$ over $\mathbb{R}$, this will extension also first of all what is the degree? Dimensional of $\mathbb{C}$ over $\mathbb{R}$ is to, in fact 1 and I is a basis, this is $\mathbb{R}$ basis and definitely I know, so therefore the degree, this is the degree, this is $\mathbb{C}$ over $\mathbb{R}$, this degree is 2 cardinality of a basis and was is the Galois group of $\mathbb{C}$

over $\mathbb{R}$, this has definitely two elements I know, one is, definitely identity is always a algebra homomorphism, identity of $\mathbb{C}$ and then other $\mathbb{R}$ algebra homomorphism is, we want the $\mathbb{R}$ linear map of $\mathbb{C}$ which also should preserve the multiplications which also respect the multiplications.

And obviously the σ which is a complex conjugation that is the map from $\mathbb{C}$ to $\mathbb{C}$ which maps z to $\bar{z}$, this is obviously $\mathbb{R}$ linear, $\mathbb{R}$ linear is obvious because z is real number if and only if $\bar{z}$ is z, so $\mathbb{R}$ is linear is obvious and also it respects the multiplication that means all that we need to check is zw then the bar of that is same thing that $\bar{z}\,\overline{w}$, this precisely means this two together means and obviously one goes to one, this means that σ is indeed an $\mathbb{R}$ algebra automorphism of $\mathbb{C}$.

So this, this group definitely has two elements, identity and σ and soon I am going to prove that, this is the, these are the only two elements, so therefore in this case Galois group is of order two and as we know the studying groups of order two is very simple, therefore studying this extension will also be simple that we also know, we have been studying complex numbers or real numbers very neatly, so this is one example.

(Refer Slide Time: 15:31)



(2) $\mathbb{K}_q$ finite field with q-elements ⑥

ch $\mathbb{K}_q = p$

$\mathbb{K}_q \uparrow$, $\mathbb{K}_p = \mathbb{Z}_p$

$q = p^m$ for some prime p, $m \geq 1$

$\mathrm{Dim}_{\mathbb{K}_p} \mathbb{K}_q = m$ $\quad \mathbb{K}_q^{\times}$ $q-1$

$\mathbb{K}_q \xrightarrow{\sim} \mathbb{K}_q$, $\quad x \longmapsto x^q = x$

$\mathbb{Z}_p$-alg. homo $\quad x \overset{f_p}{\longmapsto} x^p$

$(x+y)^p = x^p + y^p$

So another example is, suppose I take a finite field K, field with q elements, K is a field with q elements, so we have seen that q has to be the power of p, p^m , for some p, for some prime number p, p and some non-negative integer m, so therefore this is a vectors space over $\mathbb{Z}_p$, K_p is $\mathbb{Z}_p$ in our notation, this is $\mathbb{Z}_p$, so this extension, this is a field extension and we know what is the dimension? The dimension of K_q over Kp is nothing but m, this power m, that we have done in the last lecture.

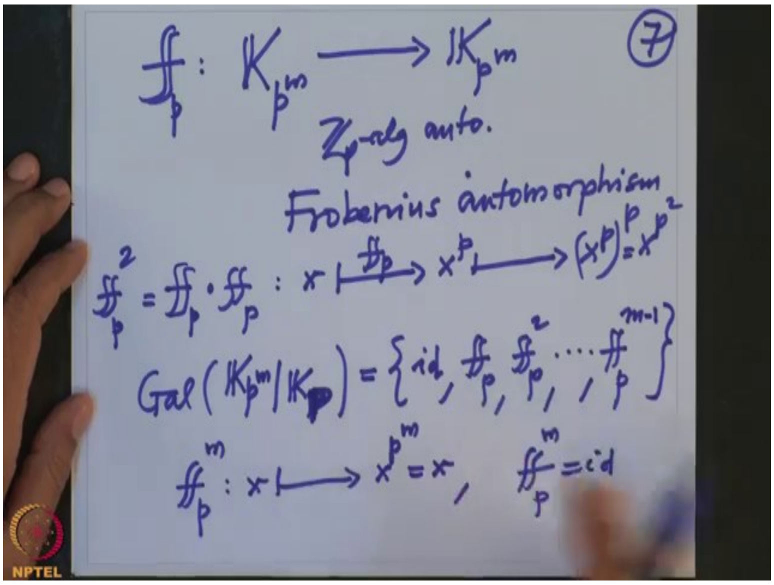
So this is a finite field extension of degree m, now when should give some elements in the Galois group, so I want to give some elements which are automorphisms of K_q as K_p linear right, so I am looking for a maps which are $\mathbb{Z}_p$ algebra homomorphism, which should preserve the multiplication, which should respect multiplication, which should respect addition and also the scalar multiplication.

Okay, but obviously in this case not much to check, so will give you the map directly, so let us take the map x going to x^q , what is this map? We have seen that if I take raise it to the power q, I get back x, because we know this K_q^x , this group is cyclic and order is $q-1$ therefore when I raise arbitrary element to the power q, $q-1$, I get identity, so when I take one more then you will get x, so this is just a identity map, but instead of this, if I would have taken x goes to x^p , let us check whether it is a algebra homomorphism.

So what do we need to check first of all, it is K linear, so this is K algebra homomorphism, that is very clear because of this, $(x+y)^p$ is same thing as x^p+y^p , that is because p is a characteristic of K_q , characteristic of this field is p, therefore when I raise at respect to addition multiplication is no problem and linear it is also no problem. So, it is a actually $\mathbb{Z}$ algebra homomorphism and it is automorphism because it is injected, it is a map from a field to somewhere, but a map from a field is always injective because it is a ring of homomorphism also.

So carnol cannot, carnol has to be either zero or whole, it cannot be whole because one goes to one, therefore any endomorphism, any map from any algebra homomorphism from a field is always injective, so it is a injective and it is also bijective because of the cardinality argument because it is a finite set injective map, Pigeonhole principal will say this map is bijective, so we have this, this map is very very important, this map is called a Frobenius. The Frobenius was the first to consider this map, so I will keep this map as f_p .

(Refer Slide Time: 20:17)



7

$\mathfrak{f}_p : K_{p^m} \longrightarrow K_{p^m}$

$\mathbb{Z}_p$-alg auto.

Frobenius automorphism

$\mathfrak{f}_p^2 = \mathfrak{f}_p \cdot \mathfrak{f}_p : x \overset{\mathfrak{f}_p}{\longmapsto} x^p \longmapsto (x^p)^p = x^{p^2}$

$Gal(K_{p^m}|K_p) = \{id, \mathfrak{f}_p, \mathfrak{f}_p^2, \dots, \mathfrak{f}_p^{m-1}\}$

$\mathfrak{f}_p^m : x \longmapsto x^{p^m} = x,\quad \mathfrak{f}_p^m = id$

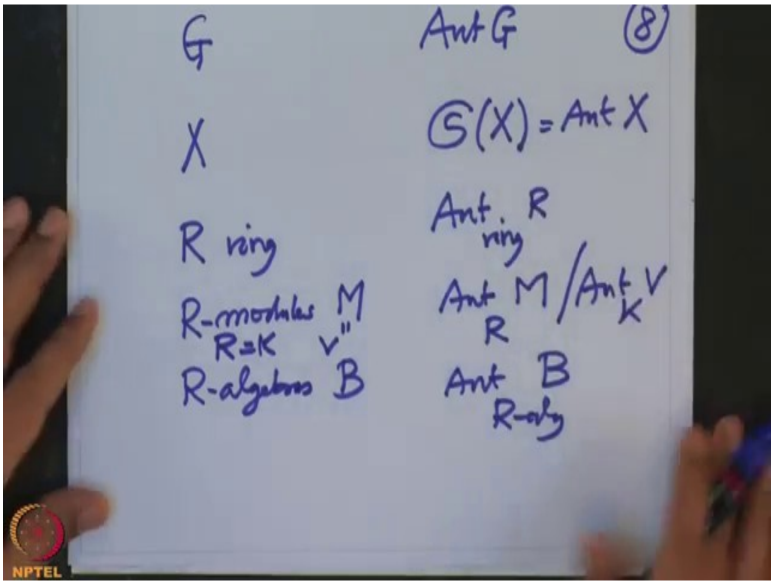
So this is, I will go to the next page, so this map, so fp this is a map from, instead of q I will write p power m, because then it is more visible, so K_{p^m} to K_{p^m} , this is obviously element in the, this is $\mathbb{Z}_p$ algebra homomorphism, algebra automorphism that is what we have check this is called Frobenius automorphism.

Okay, once you have one automorphism, if I compose with itself that also should be automorphism, so f compose f, f_p compose f_p , let us see, what does this map is? This should be denoted f_{p^2} , this is what this map? Where will it send x? The first f we will send it to x^p , this is the first f_p and the next one again it will send to power p power of this, so that is $(x^p)^p$, which is x^{p^2} .

And so we have definitely these Galois group, $Gal(K_{p^m}|K_p)$, this Galois group definitely we found some elements, one is obviously the identity map of K_{p^m} to K_{p^m} , then fp, then f_{p^2} , then I could take cube also, that will become the map x going to x^{p^3} and I can keep doing it to up to p^m , but when I do p^m , I will get back to identity map, so this one I can definitely go on till $f_{p^{m-1}}$.

Because f_{p^m} is the map of x going to x^{p^m} , which is x, so therefore f_{p^m} is nothing but the identity map, so definitely I got m elements there and I will show you that this is, these are the only elements, so we would have completed the Galois group and then we would have compared with its the degree, in this case degree is m and this if I prove this equality, then the cardinality of this set is also obviously m and therefore the degree will be equal to the order of Galois group, alright, so that will be the I will give more and more example as we progress with more and more vocabulary. Alright, so and studying this, see we are studying objects with their automorphisms that means we are studying.

(Refer Slide Time: 23:32)



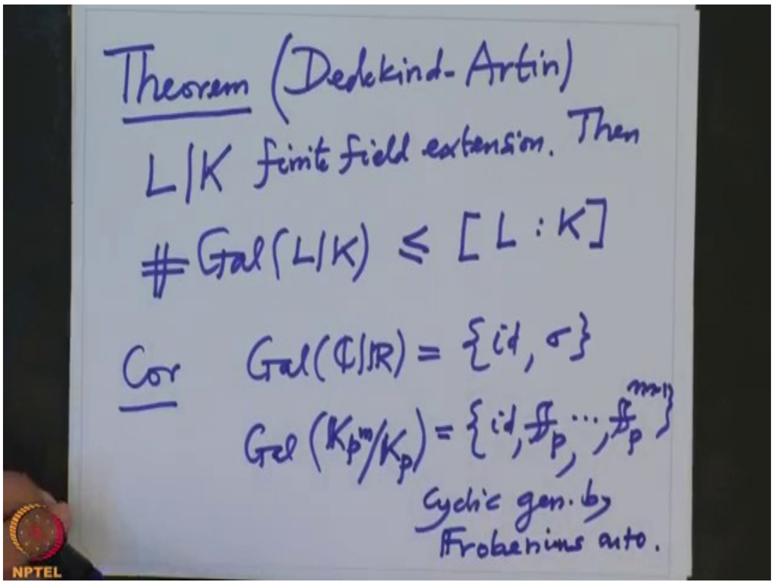
G	$\mathrm{Aut}\, G$	(8)
X	$\mathfrak{S}(X) = \mathrm{Aut}\, X$	
R ring	$\underset{\text{ring}}{\mathrm{Aut}}\, R$	
R-modules M $R = K$ V"	$\underset{R}{\mathrm{Aut}}\, M \,/\, \mathrm{Aut}_K V$	
R-algebras B	$\underset{R\text{-alg}}{\mathrm{Aut}}\, B$	

For example, we could be studying groups G with automorphism group of G that is Aut G, simply the notation will be this they are automorphism of G or before this you could have done sets, a set X with the automorphism of set means the justice simply bijective map, because there is no structure on the set other than the set, so that is all bijective maps of this, so this is Aut X.

So, similarly you could have done it for ring R, then ring automorphism, so I should write now Aut ring, so the notation also becomes clearer that we have to specify, what structure is a ring map? We want to study, so module R modules just say Aut R then module M, $Aut_R M$, that means all automorphisms of the modules means they are R linear maps, there are module homomorphism and bijective module homomorphism, their automorphism, or you can do R algebras. Generally, so that will be Aut R alg and R algebra is B, then it is Aut algebra B.

So vectors space is a special case of this, so this is $Aut_K V$, right, so this is $Aut_K V$, if R is K and then this M is V, then we write this, if this K is K algebra, then this is a field L then that is our Galois group, so in all these are groups and we are studying this objects with these groups, so now it is, how big are these groups? The bigger the groups the structurally more complicated, a smaller the groups the structure will be crocked, because then you have not many possibilities to have automorphism, so that is Aut.

(Refer Slide Time: 26:13)



Theorem (Dedekind-Artin)

$L|K$ finite field extension. Then

$\# \mathrm{Gal}(L|K) \leq [L : K]$

Cor $\mathrm{Gal}(\mathbb{C}|\mathbb{R}) = \{id, \sigma\}$

$\mathrm{Gal}(K_{p^m}/K_p) = \{id, f_p, \ldots, f_p^{m-1}\}$

cyclic gen. by Frobenius auto.

So I will prove the first connection, the numerical connection that this theorem, I will prove it when I in the next half, so theorem we want to prove is the following, theorem, this is called Dedekind Artin, so L over K finite field extension, then the order of the Galois group, cardinality of the Galois group is less equal to the degree of the field extension, so we know that if we have a finite field extension, then the order is, order of these group cannot be more than this, already this, this will tell you for R over $\mathbb{C}$, we have seen this is 2 and this is also 2, so equality should hold here and then the group cannot be more.

Similarly for finite field extension of finite fields, already, we have check that this group contains so many elements, so equality should hold here, so this already proves that Galois group $\mathbb{C}$ over $\mathbb{R}$ is only two elements, Identity and σ , the complex conjunction, similarly Galois group of K_{p^m} over K_p this is already identity f_p and so on and $f_{p^{m-1}}$, because this cannot have more elements and once you check their distinct that is all.

And in particular, this group is cyclic, now wonder because it has only two element, but even this group is cyclic, because it is generated by the Frobenius, so this is cyclic generated by Frobenius map, Frobenius automorphism, so we will come back and prove this theorem and for this theorem, we will use so-called dedicate other chronicus theorem, we will see, I will, my plan is to keep prerequisite as minimal as possible. Okay, so we will continue in the next half.