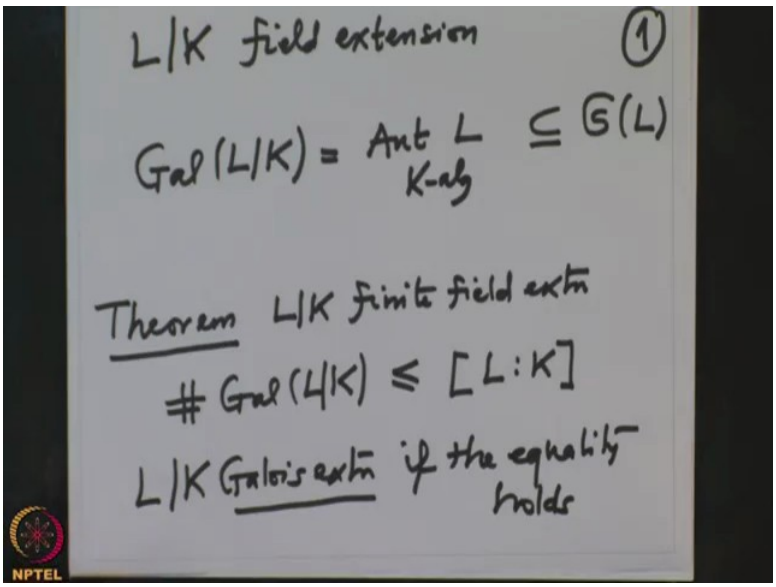
Galois' Theory
Professor Dilip P. Patil
Department of Mathematics
Indian Institute of Science Bangalore
Lecture No 28
Examples of Automorphism Groups

(Refer Slide Time: 0:51)

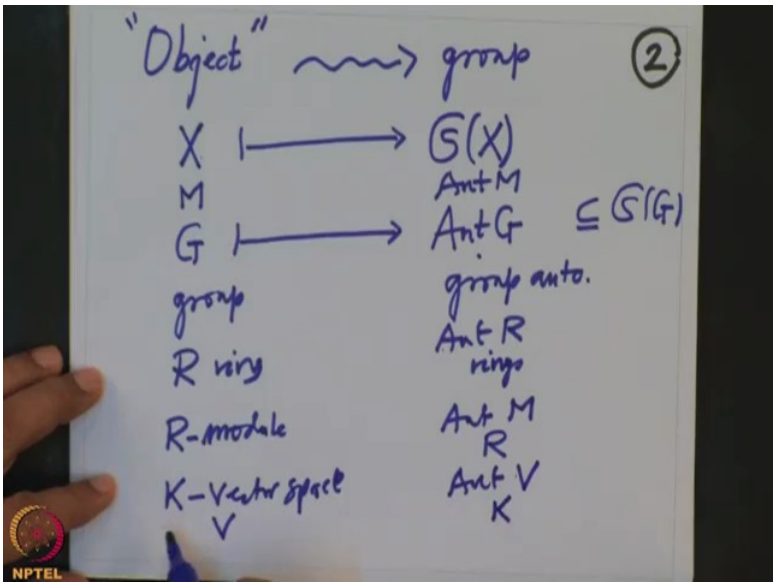


So in the last lecture we have seen the connection between the degree of the field extension and the order of the Galois group, so let me recall briefly that in this course we are studying field extensions with the help of groups and for arbitrary field extension L over K this is field extension. The group we are talking about is the Galois group $Gal(L|K)$ this group was precisely the automorphism of the field L as K algebra, L is a field over K therefore L is thought as a K algebra over K and we are looking at the automorphism of that algebra and that is clearly a group because composition of automorphism is again automorphism.

So it is a group under composition. In fact this is a subgroup of this is a subgroup of $S(L)$ the permutation, this permutations of L is a very big group. They are only bijective from L to L and automorphism are particular bijections namely they are the ones which preserve the addition and multiplication and also 1 goes to 1, so these group was first considered by Galois and in the whole course we are going to study field extensions by using this group and this intimate connection is precisely called Galois theory and what did we proof so far is this was the theorem we proved. This was the order of the Galois group is bounded by the degree of the field extension and this theorem is proved under the assumption that L over K is the finite extension, finite field extension.

I think because this side should make sense, degree of L over K should make sense, so therefore we need finite field extension. Alright, so and we define extension to be Galois extension, L over K Galois extension if the equality holds and after that we have seen some examples which also shows that and we analyse the simple extension will be Galois extension that was what we have analysed and that is if and only if the minimal polynomial splits into distinct simple linear factors in L, so that means all roots of the minimal polynomial of this generating element should lie in L and they are different they are no repeated roots, so that was what we have checked that, that is how simple extensions are Galois.

(Refer Slide Time: 4:33)



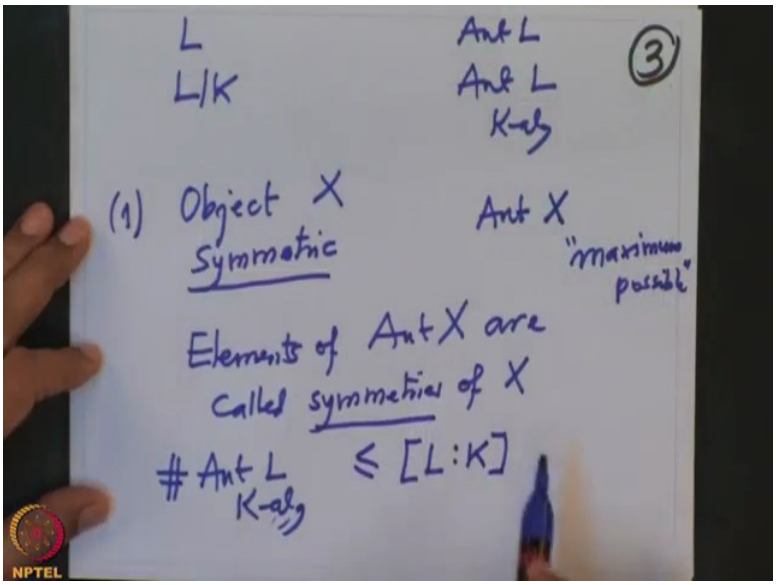
Now today I want to also little bit tells a more general comments about this philosophy that for example to each object this is to each object we attach a group. For example to a set, set is an object. See this object concept can be made more careful with the definition of categories but we do not need in that generally, so I will just explain you buy examples. For example sets are objects, so when one set, when one studies set theory we compare 2 sets. Also we study the maps between them, we study different kinds of special maps between them namely injective maps, surjective maps, bijective maps and so on, so to each set we have attached a group called a symmetric group of $S(X)$.

They are precisely bijective maps from H to X. Now instead of set if I had a group G I would attach not only all bijective maps but special kind of bijective maps namely the bijective maps which preserve the group structure that means bijective maps which respect the group structure, so those are precisely called automorphism of G and then a group, so I will not

write that suffix here it is understood that when I write Aut G mean G is the object this is a group, these are precisely group automorphism and that is clearly a group, it is a subgroup of $S(G)$.

Similarly if I had more, if I had say monoid, before that I should have said if M is monoid then Aut M, it is automorphism of monoid here little bit we have to be careful that we need to assume that monoid morphism map identity to identity that is not a consequence in general unlike groups. Similarly if you have a ring, R ring then we have Aut R, to be very clear one usually writes here rings similarly we will write groups and so on. So more generally if you have a module over ring R, R-module then we have automorphism is of that module M as a R, so R linear maps which are bijective, so this is also a group. So if you have a vector space K, this is a particular case of the above examples if K is the vector space then we have Aut… vector space V then Aut V over K this automorphism, so each object we have, we have a automorphism group of that object.

(Refer Slide Time: 7:55)

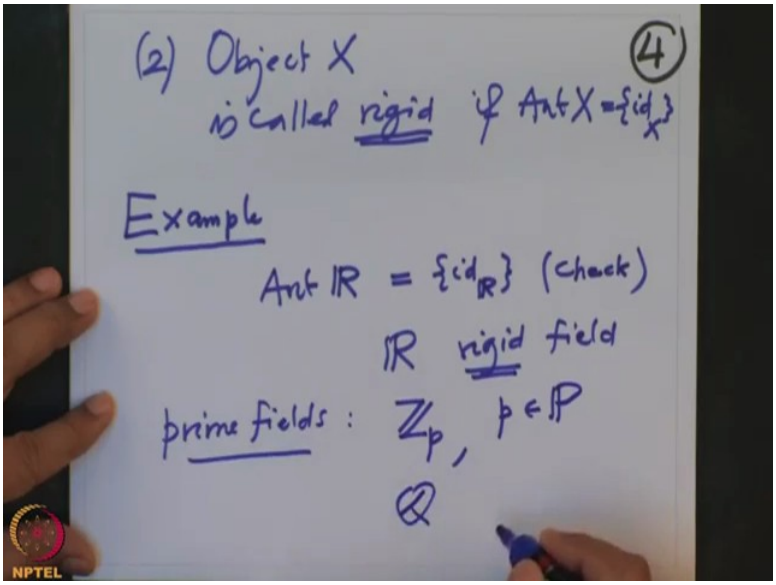


For example the one we are interested in the field extension L over K field extension then we have this automorphism as a K algebra this is precisely the group we want to study more carefully. We could have also done if we have a field L then Aut L just automorphism of the field and philosophy is from the knowledge of the automorphism groups you get the knowledge of the object and conversely, so this interplay is very important in mathematics and it does not stop here you can go on, you topological space homeomorphism, differential

manifolds, differentiable maps and so on I will not go much into that what I want to say that, the 2 definition I want to make, when do you call an object symmetric?

Object is called symmetric if the automorphism group of that object, let us call that object to be X automorphism group of this object X, this should be maximum possible, maximum possible this is little bit vague but I will make with examples more clear and element of these automorphism group are called symmetry of that objects. Elements of Aut X are called symmetries of X For example what we proved that the cardinality of this automorphism group of the field extension can at most be the degree of the field extension. So these are the Symmetric of the field extension and when will it be maximum, when the equality holds here and that is precisely what are called Galois extension, so Galois extensions are the most symmetric field extensions with this definition. So similarly other objects, so these are the symmetric objects and opposite of that is what are called rigid objects.

(Refer Slide Time: 10:32)

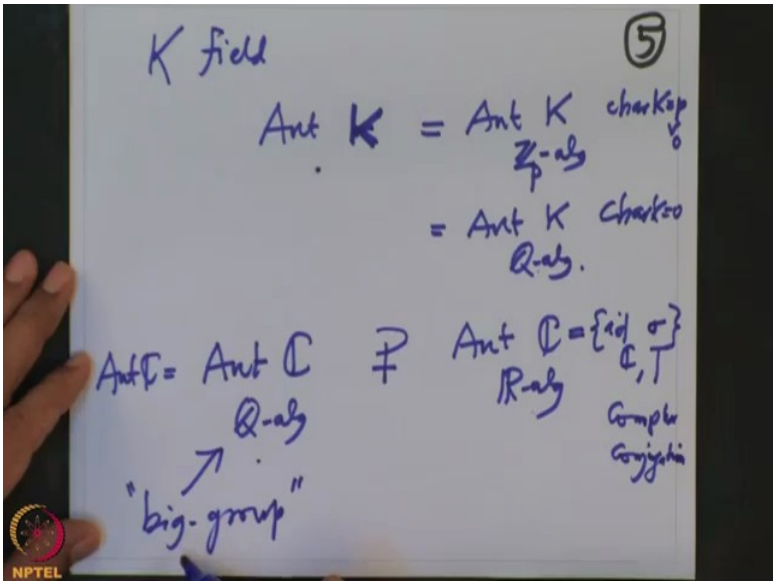


So objects are called object X is called rigid if the automorphism group is a trivial group just identity of X, identity of X is clearly an automorphism, so automorphism group is a trivial one that is then the object is called rigid that means there are no symmetries of X other than the identities. Now one can ask various questions, can one characterise rigid sets, rigid groups, rigid rings, rigid automorphism rigid field extension and so on or rigid fields or you can also keep asking ordered sets, ordered sets are also objects and Symmetric of the order sets are precisely the order preserving maps which are bijective.

So all these questions will come up how do you say that the objects are symmetric, characterisation of orders objects which are symmetric and which are rigid. These are of very prime importance in studying in any subject and in this course we are only studying field extension which are symmetric and they are Galois extension and how do we characterise them and so on, so we are studying Galois extension and that is why this is called Galois theory.

So for example I want to remind, example last time we have said is automorphism of $\mathbb{R}$ as a field Aut $\mathbb{R}$ this is a trivial group this needs a proof, so I will just here check. This is… Therefore $\mathbb{R}$ is a rigid field, $\mathbb{R}$ is a rigid field because the only automorphism is identity. More examples of rigid fields are for example if you take the prime fields, prime fields are precisely $\mathbb{Z}_p$ where p varies in prime numbers and $\mathbb{Q}$ these are rigid fields, these are for each characteristics there is exactly one prime field that means if K is a field of characteristics P then it contains $\mathbb{Z}_p$ and if K is a characteristics of 0 then it contains definitely field $\mathbb{Q}$.

(Refer Slide Time: 13:33)



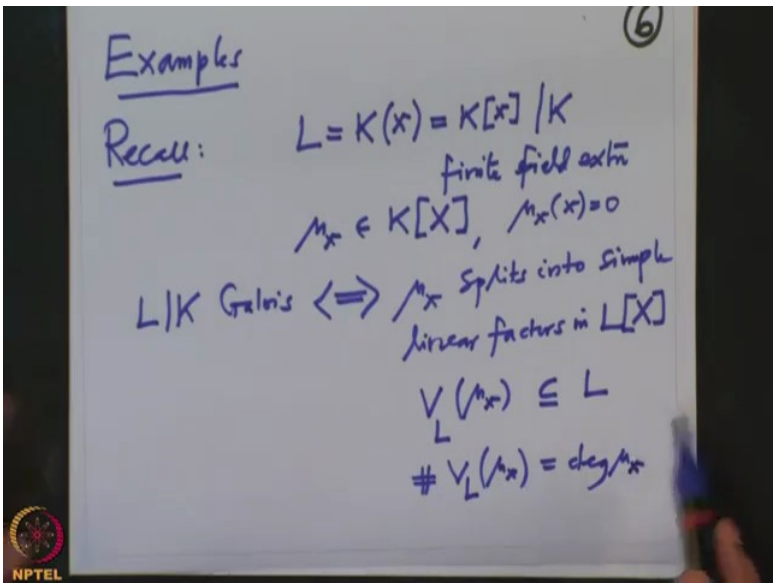
And therefore with this also we know because we are considering if K is any field and if I just take Aut K automorphism of the field K that is same thing automorphism of the field K or the prime field, so let us call so if K has characteristics p then it is a $\mathbb{Z}_p$, if characteristics K is p positive, if it is 0 this is Aut K $\mathbb{Q}$ algebra I should say $\mathbb{Q}$ algebra because they are automatically… If characteristics is p every automorphism will automatically be $\mathbb{Z}_p$ linear because $\mathbb{Z}_p$ is generated, identity group generated by one,

so once you know one goes to one then you know where the sum goes and so on and everybody know all the elements are going to themselves so they have $\mathbb{Z}_p$ linear similarly for $\mathbb{Q}$.

So automorphism of a field if I just take Aut K is field that is same thing as Aut_K $\mathbb{Z}_p$ algebra or Aut K $\mathbb{Z}_q$ algebra depending on K is characteristic 0 or p. Alright, so also remember I will raise this question now but the answer we will answer later, so for example if I want to know what is Aut $\mathbb{C}$? Aut $\mathbb{C}$ is therefore Aut $\mathbb{C}$ as $\mathbb{Q}$ algebra, this is same as Aut $\mathbb{C}$ by the above remark and I have explained you what is the Aut $\mathbb{C}$ as $\mathbb{R}$ algebra homomorphism, so that means the $\mathbb{R}$ linear so and these is precisely 2 elements one is identity map of $\mathbb{C}$ and the other is σ which is a complex conjugation.

This is complex conjugation, this is what we proved last time and this is clearly contained here because $\mathbb{R}$ linear will imply $\mathbb{Q}$ linear but I want to stress here that this is not equal, in fact this has cardinality to this group is very big group and this is even uncountable cardinality this is a big group and to write the elements explicitly will not be possible unless you have 2 take methods from transfinite site et cetera et cetera which with the help of what is called a transcendent basis of a field extension with that helped we can describe this group but right now we do not have those machinery to describe this group.

(Refer Slide Time: 16:43)

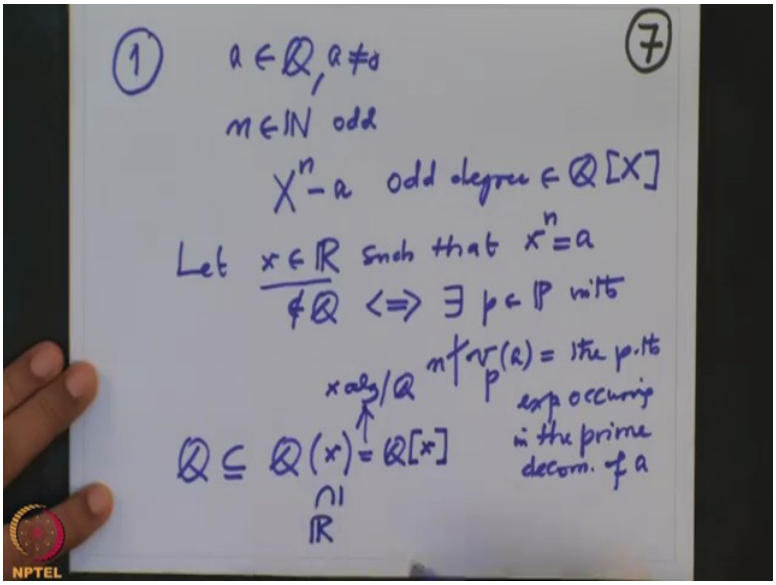


Alright, so we continue our examples, a few more examples of non-Galois extension, so examples, so far remember we have $\mathbb{C}$ over $\mathbb{R}$ is a Galois extension. Also we have checked that finite field, finite extension of a finite field is always Galois extension and in

this case the Galois group is cyclic and it is generated by the Frobenius map. I just want to recall we have proved that if I have us simple extension L simple means in generated by one element an algebraic extension, so whether I write round bracket or square bracket it is same over K finite extension, finite field extension and then we have analysed then for this generator of L as K algebra this X we have the minimal polynomial, this minimal polynomial is a monic polynomial with coefficients in K and $\mu_x(x)$ is 0, it is irreducible polynomial because mod ideal generated by that is precisely this with L therefore it is a non-zero prime ideal and therefore irreducible.

So we have proved that L over K is Galois if and only if μ_x splits into simple linear factors in $L[X]$, so that in other words in the notation if I take 0 set of μ_x in L this is 0 set of μ_x in L this as cardinality equal to degree of… That means all this has 2 conditions that means all roots are in L and all are simple, right. So I want to give examples so that if you if any condition fails there are 2 conditions here namely the roots are simple and all roots lie in L. If anyone of these 2 conditions fails then the field extension is not Galois. I want to see these examples exquisitely.

(Refer Slide Time: 19:36)



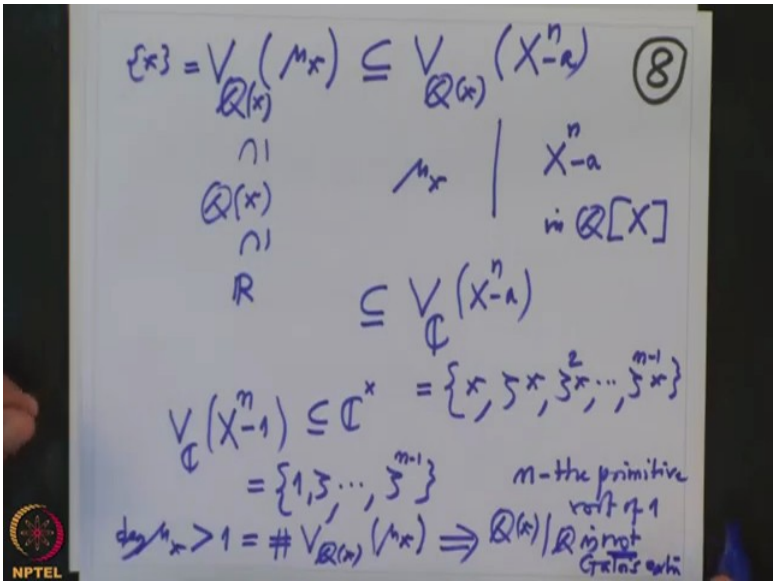
So 1st example let us take now rational number a, a is a rational number, nonzero and also take any natural number n odd and now I look at the polynomial $X^n - a$, so this is a polynomial of odd degree, so odd degree polynomial and which has a rational coefficients therefore it has real coefficients and therefore we know from our college study that this polynomial definitely has one real root, so let small x be $\mathbb{R}$ such that, it is a 0 of this

polynomial means small X^n equal to a and I want to choose now a carefully so that this x is not in $\mathbb{Q}$ and how do I make sure that that will mean that this rational number.

So this is equivalent to saying the rational number, the prime decomposition of its rational number a does not have all the p exponents for the primes occurring in the prime decomposition of a they cannot be all divisible by n, so simply in the notation is equivalent to saying there exist prime number p with v_p of a is n does not divide this and what is v_p of a this is a p-th exponent occurring in the prime decomposition of a, this the p-th exponent occurring in the prime decomposition of a. It can be negative integer.

So you will see that why I put this condition but now the situation is I am considering a field extension now, $\mathbb{Q}$ is containing $\mathbb{Q}[x]$ remember whether it is round bracket or square bracket it is the same because it is finite field extension x is algebraic, this is x is algebraic over $\mathbb{Q}$, so I will not repeat again and again few times it is good to repeat, so I have a field extension and note that because I have chosen X as a real number this $\mathbb{Q}[X]$ is already containing the field R, alright now I want check that whether this $\mathbb{Q}[X]$ over $\mathbb{Q}$ this is a simple extension I want to check this is Galois or not and our observation shows that if I want to check this I should check that all zeros of the minimal polynomial should lie completely inside this field that is 1st condition and not only that it should lie here but they should be all distinct they should not be any repeated 0.

(Refer Slide Time: 23:26)



Okay, so but let us see how many 0 lie in therefore we are interested in the number of 0 in $\mathbb{Q}[X]$ of this polynomial μ_x and what is the minimal polynomial of μ_x whatever it

is μ_x is the minimal polynomial and because μ_x is the smallest degree polynomial that x satisfies over $\mathbb{Q}$ and 1 polynomial definitely I know this, so this polynomial x is a root of this polynomial so therefore this should divide this where in the polynomial being $\mathbb{Q}[X]$, so therefore whatever the 0 of μ is that will also be 0 of X^n-a , so that shows that this 0 set is contained in therefore $V_{\mathbb{Q}(X)}(X^n-a)$.

So I should know what are the zeros of X^n-a but well this 0 set is also contained in $V_{\mathbb{C}}(X^n-a)$ and this 0 set are precisely… I am going to write down this 0 set this is precisely x is obviously one of them and then $\zeta x, \zeta^2 x, ..., \zeta^{n-1} x$, what is ζ ? So let me remind you we have also discussed that if I take the polynomial X^n-1 the roots of this polynomial in complex numbers, this is precisely the roots of unity and we have checked that this is finite subgroup of $\mathbb{C}^x$ and therefore it is cyclic and therefore it has a generator and that generator is called primitive n-th root, n-th primitive root, root of unity and that is therefore this group is…this 0 set is nothing but ζ and so on to ζ^{n-1} , precisely n because this polynomial X^n-a has simple roots because when you differentiate it the roots are not so.

Therefore this 0 set is precisely containing this set and on the other hand we know these are all real and they are all containing $\mathbb{Q}[X]$ and $\mathbb{Q}[X]$ is containing real numbers therefore we are interested only in the real zeros but only real 0 among them is X, so therefore that proves that this set is only singleton x, so therefore minimal polynomial not split into the linear factors in $\mathbb{Q}[X]$ unless μ_x is x only but that cannot happen because x is a real number this does not have the condition why did I put that n does not divide v_p of a because I wanted a non-rational real root.

So therefore our degree μ_x is definitely more than one and this one is cardinality of the 0 set of this minimal polynomial of μ_x in $K[X]$ therefore the condition, one of the condition is not satisfied therefore as a conclusion we conclude at $\mathbb{Q}[X]$ over $\mathbb{Q}$ is not Galois is not Galois extension and in the later half I will give another example where actually the minimal polynomial has all the roots lie in the field but there some of them could be repeated root therefore the extension cannot be Galois, so this example we will give it in the later half. Thank you.