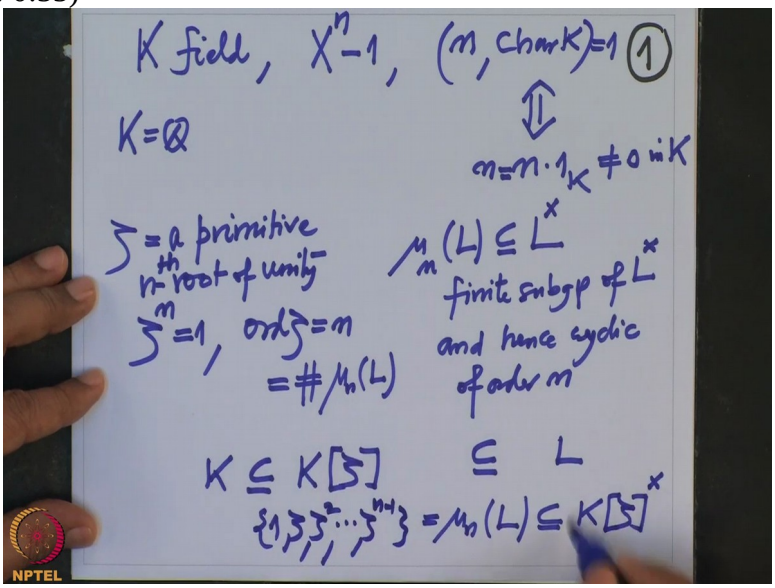
Galois' Theory
Professor Dilip Patil
Department of Mathematics
Indian Institute of Science Bangalore
Week 07
Lecture 34: Cyclotomic Extensions

In the last lecture, we saw roots of unity over an arbitrary feel. And we are trying to study the Galois group of the field extension which we got by adjoining a primitive Nth root of unity to a given ground field. So let me recall the notation.

(Refer Slide Time: 0:55)



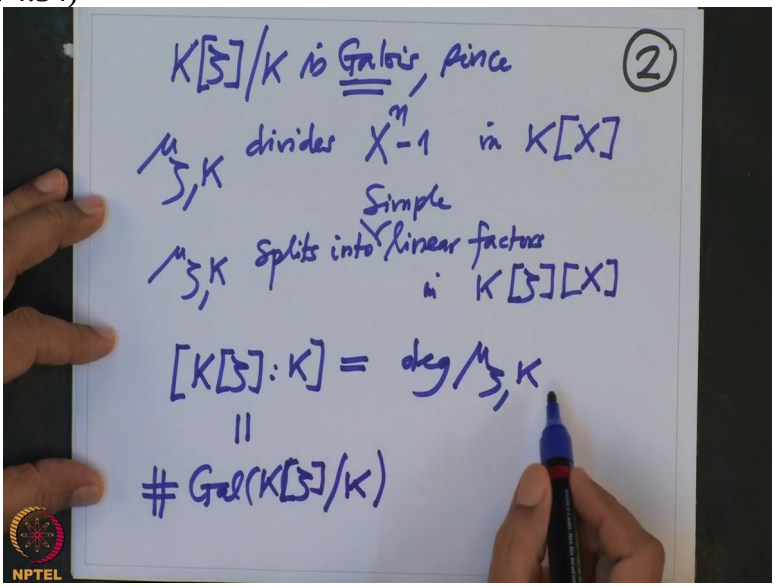
So first of all K field and we are studying this polynomial, X^n-1 and the zeros of this polynomial and we decided that it is enough that we can assume that this n and the characteristic of K, these are co-prime. So in characteristic of zero, this is always true. So if K were Q, there is no condition. And this condition is equivalent to saying that n dot 1 is not zero in K. This is n in K not zero. This is automatic in characteristic zero field. No integer can be zero in the characteristic zero field.

And then we have, what we did was we first enlarged this field L so that it contains all the roots of n-th roots of unity. So $\mu_n(L)$ is contained here and this is actually a finite subgroup of, this is actually contained in L^x, this is a finite subgroup of L^x and therefore cyclic and hence cyclic of order n and it has a generator. Generator, any generator of this group is called a

primitive root of unity. So ζ is a primitive n-th root of unity. That is ζ^n is 1 and not only that, the order of ζ equal to n which is also order of this group $\mu_n(L)$.

And once you have chosen such a root, then we know that if I take a subfield of L generated by this ζ is K, this is contained here, this is contained here. Now we are interested in this relationship because also note that this whole $\mu_n(L)$ group, this is actually a subgroup of $K[\zeta]^x$. That is because one ζ is there. All elements of this which are powers of, this group is nothing but 1, ζ , ζ^2 ,…, ζ^{n-1} , this is that group. So this is visibly contained in this.

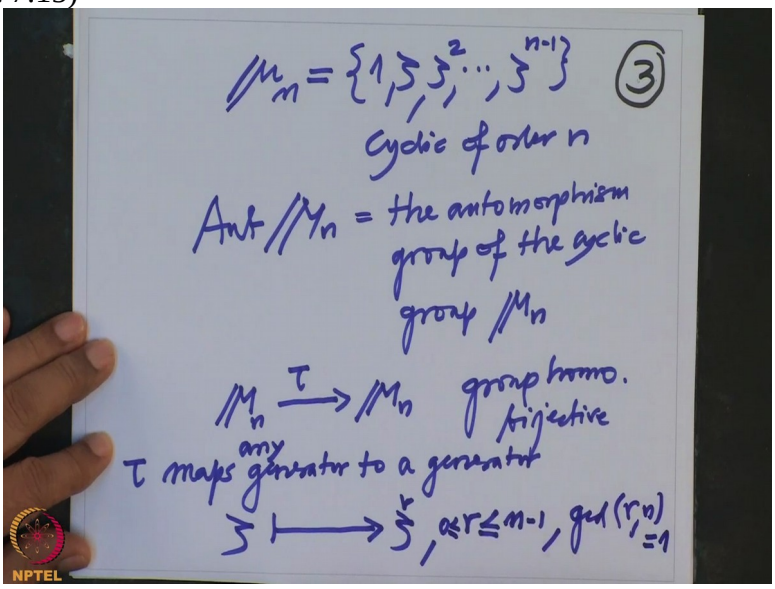
(Refer Slide Time: 4:34)



And we, what we noted was this field extension , this over K is Galois because we know how to test a simple extension is Galois, that is since the minimal polynomial of ζ over K divides X^n-1 in KX. And this polynomial has different routes, distinct roots and all are simple and therefore $\mu_{\zeta,K}$, so $\mu_{\zeta,K}$ splits into linear factors simple linear factors in $\mu_\zeta[X]$ and therefore this extension is Galois. And we also know what is the degree of this field extension. So the degree of the field extension $K[\zeta]$ over K, this I know because it is a simple extension, it is degree $\mu_{\zeta,K}$.

But because it is Galois, this degree is also equal to the order of the Galois group of $K[\zeta]$ over K but we do not know exactly what the order is, we do not know exactly what my is, my ζ is. Therefore we do not know what is the degree is. But still we want to conclude about the structure of this group. In particular I want to note that this group is Abelian and for $\mathbb{Q}$, when K equal to $\mathbb{Q}$, I want to conclude, I want to give a structure for this group, what is the group exactly? This is what we want to do it now. Okay. So one problem is to find a minimal polynomial exactly and therefore we can find the degree and then that we will give a order of the Galois group but that will still not prove it is Abelian for example.

(Refer Slide Time: 7:15)

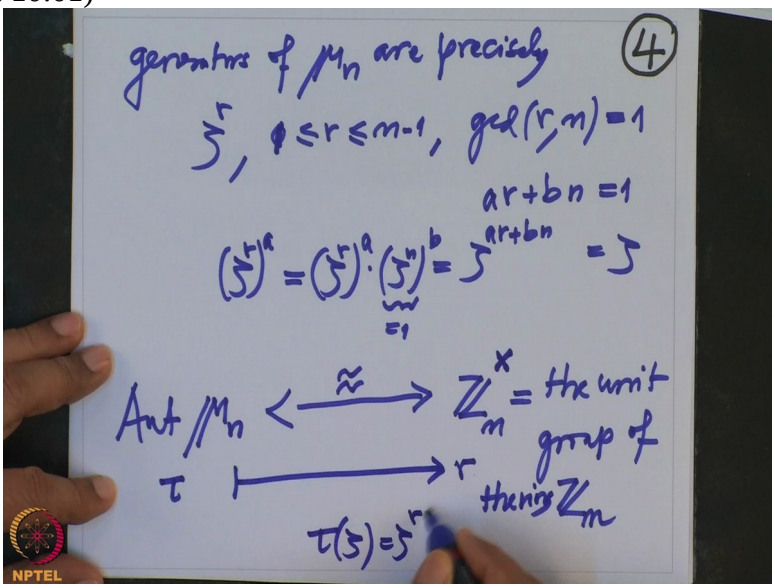


But what information now I want to extract from this group μ_n is this group. μ_n is the the group generated by ζ. This is ζ, ζ^2 ,…, ζ^{n-1}. This is a cyclic group. So this μ_n, I separate that $K[\zeta]$ over K from or L from the notation. This is that group. This is cyclic of order n. And we know what are for example what are the automorphisms as a group? What is the Aut μ_n of this group? Automorphisms as a group, I do not have to write here. This is the automorphism group of the cyclic group μ_n. And we know automorphism group, so that means they are automorphisms of the group.

So that means the elements here are precisely the group homomorphisms from this to this. So let me call it τ. They are group homomorphisms and bijective. Inverse is also group

homomorphisms. So therefore, it is clear that it should map a generator to generator. So τ should map, τ maps generator, any generator to a generator. So one generator, we know it is ζ. This should map it to another generator but we know all the generators of this group. What are the generators of this group? Let me write it on the next page. So the, I will write here the answer first. So it is going to ζ^r where r is small or equal to $n-1$ zero this and also GCD of r and n should be 1. Only those are the generators.

(Refer Slide Time: 10:01)



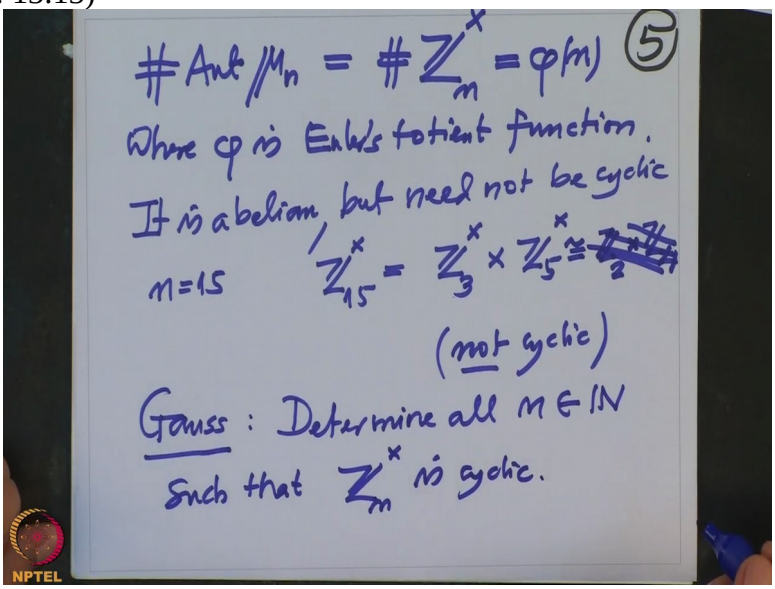
So now this observation, I have deduced it from the fact that generators of this group are precisely, we can describe them in terms of a given generator and the given generators I use is the ζ. They are ζ^r where zero less equal to r less equal to n-1 and actually 1. And GCD of r and n is 1. So it is clear that ζ^r is also generator because the GCD is 1. That means the combination $ar+bn=1$ and this will mean that when I raise it to ζ power 1, so that is ζ will be equal to ζ^{ar+bn}. But this is equal to $(\zeta^r)^a$ and that will be $(\zeta^n)^b$.

But this is 1 and therefore this is nothing but $(\zeta^r)^a$. So once ζ is generate that so this is this power of this is also ζ, that means this also generates and precisely those generates. Because if the GCD is more than 1 then it will generate a subgroup of smaller order and therefore it cannot be the whole group. Therefore it cannot be the generators. So we know the generators. And therefore, this group aut this group μ_n you can identify with the $\mathbb{Z}_n^\times$.

Remember what are the $\mathbb{Z}_n^x$ elements. They are precisely the elements, this is a unit group of the ring $\mathbb{Z}_n$.

That means, they are units in that ring and we know they are precisely the integers which are co-prime to n. And what is the identification? This identification is, any automorphism τ , this τ is uniquely determined by the fact that where τ goes, where the ζ goes. So look at τ of ζ and that is a power of ζ and that power, I am Abelian to that power where this r is defined by this equation, τ of ζ equal to ζ^r . This is the identification. Given any r which is co-prime, you look at this definition, that will give you automorphism of this and this. So this group is the unit group of $\mathbb{Z}_n$ and we know what is the order of this group.

(Refer Slide Time: 13:13)

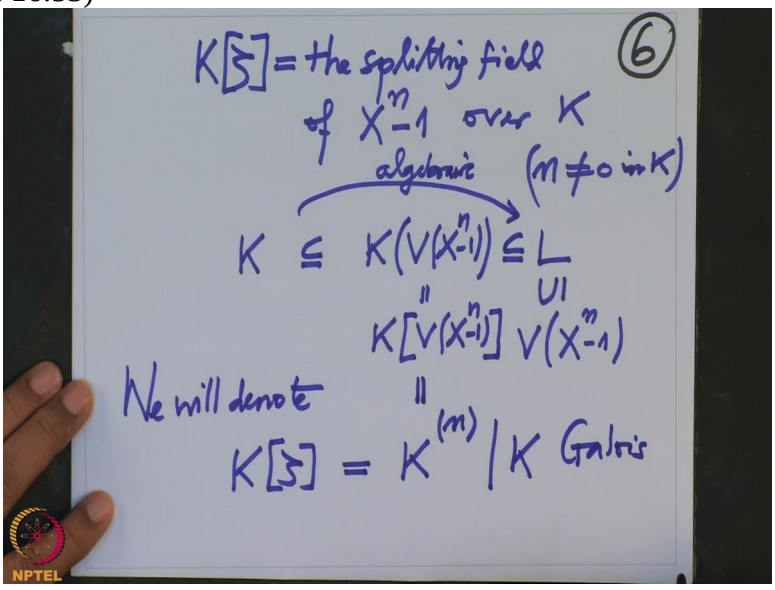


The order of this group is so we know the order of cardinality of Aut μ_n which is the cardinality of the unit group of $\mathbb{Z}_n^x$ which we know it is $\phi(n)$ this where ϕ is Euler's quotient function. Now it is clearly Abelian group. It is Abelian but may not be cyclic but need not be cyclic. For example, when you take n equal to 15, that is $\mathbb{Z}_{15}^x$, this is $\mathbb{Z}_3^x \times \mathbb{Z}_5^x$ and here, you see there are elements here there are the elements of order 2 are more than 1. See in a cyclic group, the elements of order n the elements of order d are precisely few of d.

So I would simply say check that this group is not cyclic. Because this is even order, this is also even order and this is what, what is this group? Actually you can write down, this is $\mathbb{Z}_2 \times \mathbb{Z}_4$. As a group, this is cyclic. So let me not write this. This is cyclic of order 2, this is also cyclic of order 4. These are fields. Therefore the groups are cyclic. This is order 2, this is order 4 and they are, 2 and 4 are not co-prime. So there is an element of order 2 here, that element, identity and element of order 2 here and identity here, there will be at least 2 elements of order 2.

So therefore this group cannot be cyclic. But Gauss has answered this is a theorem of Gauss exactly for which n determine all n such that this group is cyclic and there is a nice answer to this. So you take this as an exercise. So this group is not, so this has something to do with the prime decomposition of n. So I will just say, look at the prime decomposition of n. See, I want to conclude the Galois group, so I want to state the theorem.

(Refer Slide Time: 16:53)



So before I state, I want to create a notation for this $K[\zeta]$. $K[\zeta]$, we know this is the splitting field, I start using this term now, splitting field of $X^n - 1$ over the given field K and remember that n is not zero in K. That is important assumption we have made. So and what is the splitting field? You look at this polynomial and enlarge K so that all the roots lie in that field and take the subfield of that field generated by the roots. So in symbols, first of all you take L so that

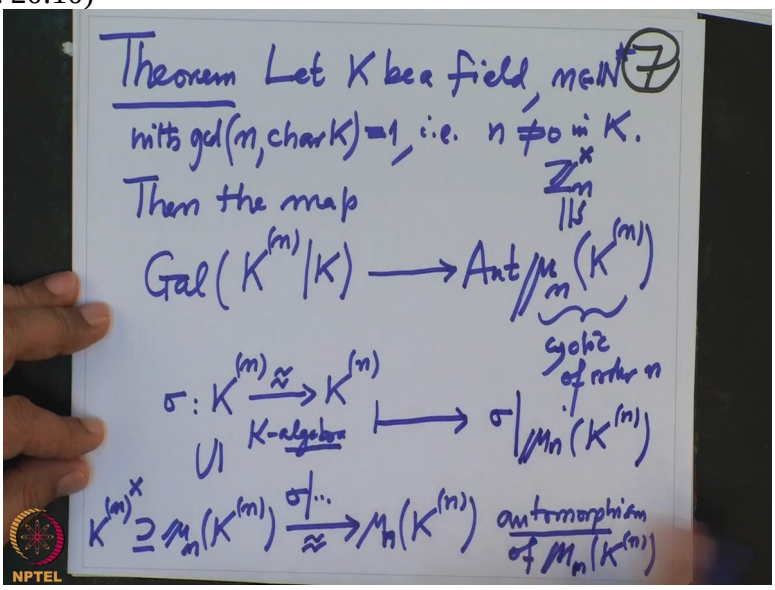
all roots of this polynomial, $V(X^n-1)$ all the roots, they lie here. They are completely contained here.

So I do not have to see here what? So they are all roots and and among…that so take these roots and take the field over K adjoined to all this case and exactly those. This is contained here, this is contained here and this is clearly a subfield because whether they are round bracket or square bracket, it is same because we are in an algebraic case. We are an algebraic feel extension case. Therefore subfield, this is same. Because this extension is algebraic and this is an intermediary field which is generated as a K algebra over K by the roots of this polynomial, that is precisely the splitting field.

So this splitting and this ζ is 1 generator but I want to get independent of that ζ . So I will denote the splitting we will denote this $K[\zeta]$ because this depends only on this N and K. Right? So this I want to denote by $K^{(n)}$. Actually strictly speaking, I should say I denote this by this and we have noted that this equals to this. So this is and we have checked that this extension over K, this is Galois. We know it is a primitive root, primitive element is this but we do not know what is the Galois group.

We do not know what is its degree exactly but obviously now one might have guessed that this degree of this extension has something to do with $\phi(n)$ because this came out of that group which has order, the automorphism group of that μ_n has order $\phi(n)$. Okay, so precisely we will prove the following theorem.

(Refer Slide Time: 20:10)



So theorem. So let K be a field, n a natural number, nonzero with condition that GCD of n and characteristic K is 1. That is n is not equal to 0 in K. This is what the assumption we had. Then the map. I am giving the map between the 2 groups. One group is the group we are interested, that is Galois group of $K^{(n)}$ over K. This is the group we are interested in. We are interested in this Galois extension, we do not know degree, we want to find the degree.

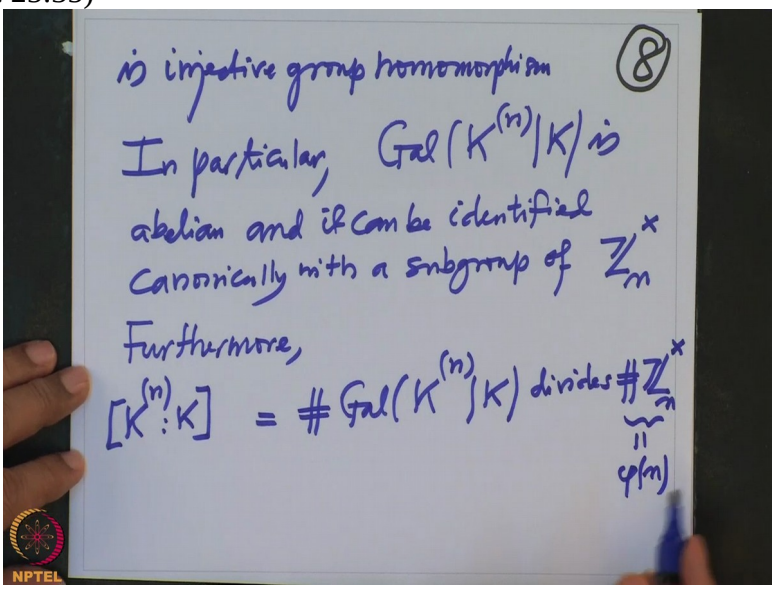
On the other hand, from this n, we got hold of the group μ_n which is a cyclic, which is a finite subgroup of this field cross. Therefore it is fine, therefore it is cyclic and therefore I will talk about, we can talk about automorphism group of that field. μ_n in this field $K^{(n)}$. There are the roots of unity in this field and they are all of them are there. So this group has order n and this is cyclic of order m. But I am not saying the automorphism group is cyclic. But this group I know, this group is isomorphic to $\mathbb{Z}_n$ and then units in that, $\mathbb{Z}_n^x$. This I know.

And I want to give a map here. Then the map, what is the map? That means I have to map any automorphism τ , σ , σ is an automorphism of K^n to K power and, this is a K algebra automorphism. This I want to map it to an automorphism here. Well, but where is this group? This group $\mu_n(K^{(n)})$, this is a subgroup here of the multiplicative group. $\mu_n(K^{(n)})$, this is , this one is a sub of this. Actually it is a subgroup of $K^{(n)x}$ and this σ is a K algebra homomorphism. So σ restricts, σ restricts the multiplication.

So when I, this is contained here, so when I restrict σ to this, σ restricted to this, so I will not write what? σ restriction, so these are the elements and I can restrict σ to that and where does it go? So σ first of all will be uniquely determined by its value on ζ. And once $\sigma(\zeta)$ is that so this the because it is a multiplication also preserved, so it will give you that the group homomorphism here. Actually group automorphism. So this section will give you automorphism of this group. So this is an automorphism of this group, $\mu_n(K^{(n)})$.

Remember, I just said that it is a group homomorphism and because this, this map is automorphism, this σ is an automorphism so it is in particular injective and this is a restriction of injective map, so it is definitely injectable. And this is now a finite set, this is the same set. So in interactive map, from a finite set to finite set is a bijective map. So this is also bijective and it is a group homomorphism because this σ is a multiplication preserving map. So note that this σ is indeed an automorphism of this. So we have given a map, then take any σ and map that σ to this restriction. So σ is mapped to the restriction to this $\mu_n(K^{(n)})$. So we have a map and what is the statement?

(Refer Slide Time: 25:35)



The statement says that the map this map is injective group homomorphism. In particular, this Galois group $K^{(n)}$ over K is abelian because the automorphism group is abelian. Because this group is Abelian because it is $\mathbb{Z}_n^x$, it is a multiplicative group of a ring $\mathbb{Z}_n$, therefore it is

Abelian. Therefore this group is a subgroup of this. You can identify this as a subgroup of this and therefore it is Abelian. And it can be identified canonically with a subgroup of $\mathbb{Z}_n^x$. Again I say canonically because I did not choose any ζ . Furthermore, the order of this group Gal $Gal(K^{(n)}|K)$ the which is equal to the degree the field extension because it is Galois extension, this divides the order of $\mathbb{Z}_n^x$.

This is by Lagrange's theorem. This is a subgroup of this, therefore order divide this. But this order I know, this order is $\phi(n)$. Therefore the order of the Galois group divides $\phi(n)$, that is the information we get it. And okay then I will continue after the break.