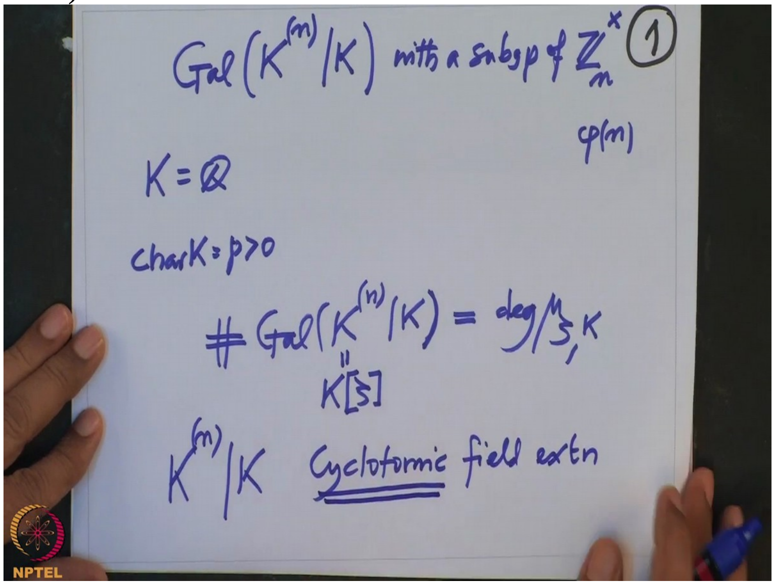
Galois' Theory
Professor Dilip Patil
Department of Mathematics
Indian Institute of Science Bangalore
Week 07

Lecture 35: Cyclotomic Polynomials

So we are studying the field extensions by adjoining the roots of unity.

(Refer Slide Time: 0:44)



$\mathrm{Gal}(K^{(n)}|K)$ with a subgp of $\mathbb{Z}_n^\times$ (1)

$\varphi(n)$

$K = \mathbb{Q}$

$\mathrm{char}\,K = p > 0$

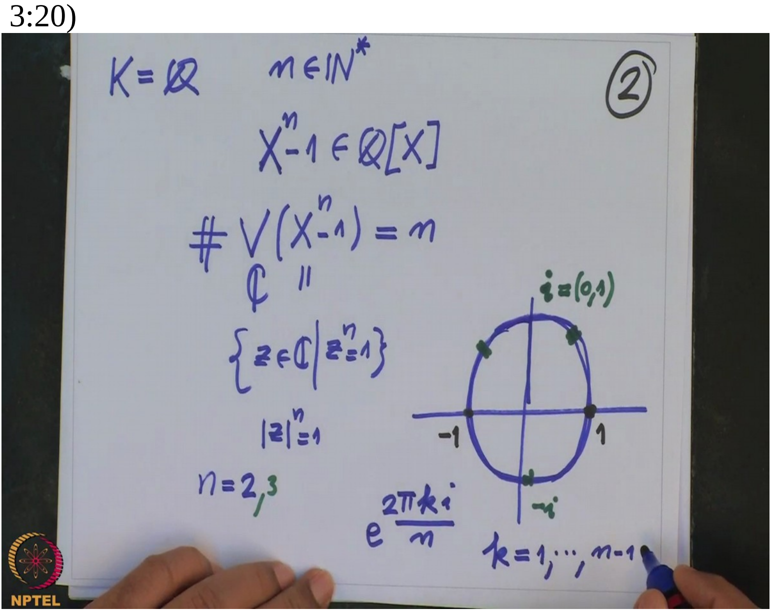
$\#\,\mathrm{Gal}(\underset{K[\zeta]}{\underset{\|}{K^{(n)}}}|K) = \deg \mu_{\zeta,K}$

$K^{(n)}|K$ Cyclotomic field extn

So we have just now checked that the Galois group of the splitting field of $X^n - 1$ over a field K where this n and characteristics of K are co-prime, this Galois group can be identified with a subgroup of $\mathbb{Z}_n$, units in $\mathbb{Z}_n$. And we want, we will know that the this order we know phi of n. So therefore order of this group divides phi of n but we want to find exactly what is the order of this group and that we will do it into steps. First I will assume the characteristic of K is zero. The That means I will assume that K is $\mathbb{Q}$ and the next I will assume characteristic of K is positive. These are the 2 things I will assume.

So as you have seen, minimum I want to exactly find the order of this group. So to find order of this group, this is what our aim is, to find this order. But because this extension is Galois, this order is nothing but and this extension is simple which is generated over K by a preventive root of unity, then this this one, this order is exactly equal to the degree, the minimal polynomial of ζ over K. And we want to find this degree. Moreover actually we want to find what is the minimal polynomial in case of $\mathbb{Q}$ and in case of characteristic positive. This is what our aim is. Before I go on, this extension remember this extension, this is called cyclotomic field extension. I will want to justify this name cyclotomic. So that is done as follows.

(Refer Slide Time: 3:20)



$K = \mathbb{Q} \quad n \in \mathbb{N}^*$

$X^n - 1 \in \mathbb{Q}[X]$

$\# V_{\mathbb{C}}(X^n - 1) = n$

$\quad \quad \parallel$

$\{z \in \mathbb{C} \mid z^n = 1\}$

$|z|^n = 1$

$n = 2, 3$

$e^{\frac{2\pi k i}{n}} \quad k = 1, \dots, n-1$

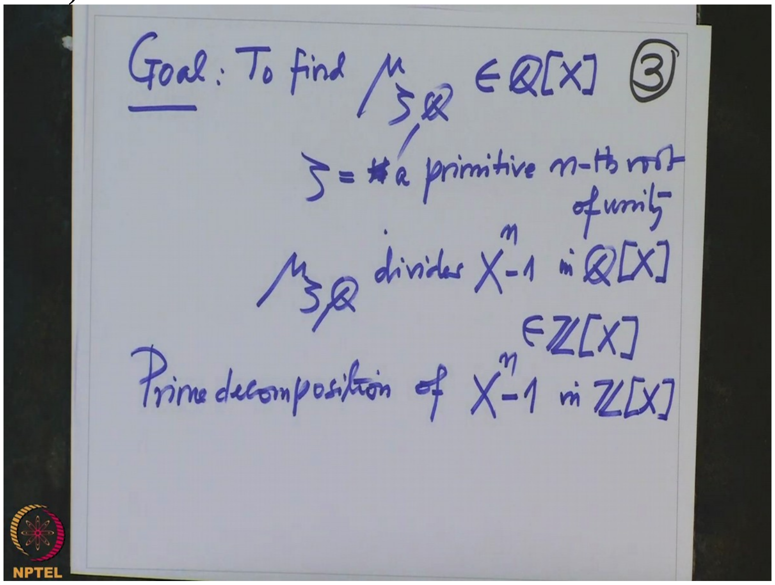
Let us for the understanding, let us take K equal to $\mathbb{Q}$. Then what do we do? We have n any natural number nonzero and no condition because the characteristic is zero. And what did we do? We are looking at the roots of this polynomial. This is the polynomial, this is the polynomial over $\mathbb{Q}$ and we are looking at the roots, zeros. Zeros, all zeros of the polynomial. So this one is over $\mathbb{C}$. These are all zeros. And we know this, they are all simple zeros because this polynomial has no repeated roots again because the derivative and this polynomial do not have any common zero.

So these are all distinct and therefore cardinality of the zero set is nothing but the degree of the polynomial which is n. There are precisely n zeros. And what is that location? So this one is all z in complex numbers such that z^{rn} is equal to 1. So therefore you have this circle, unit circle, all of them lie in this, z is z^n is 1. Therefore mod of z^n is also equal to 1. Therefore mod z will be 1. So it will be on the circle. So for example if I want to locate n equal to 2, so n equal to let us say 2, there are exactly 2 zeros and what is the location?

So one zero is one, this is one. Remember, this is one. Actually, strictly speaking, we should write zero. But this is one. Strictly speaking, we should write one zero, not zero. One zero and this is minus 1. So these are the 2 zeros. So this is n equal to 2 case. If I want n equal to 3 case, then there is only one one zero is real zero, that is somewhere here and then another here and another here. So this circle gets divided into 3 equal parts and then these are the things. 4, for 4 it is 1, minus 1 obviously and this is now I should write it I because that is the identification of these points on the real plane with the complex number.

This is, I is actually zero and then the other one is this, this is minus I and so on. So all these zeros are lying over the boundary of this unit circle and they are equidistant. So in general, the zeros are precisely $e^{2\pi ki/n}$ where this n, k is on whatever 1,2, n - 1. Actually, yes. n actually. Okay. So they are the zeros. So this cyclo word comes from the circle. They are all on the circle.

(Refer Slide Time: 7:29)



Goal: To find $\mu_{\zeta,\mathbb{Q}} \in \mathbb{Q}[X]$ 3

$\zeta =$ a primitive n-th root of unity

$\mu_{\zeta,\mathbb{Q}}$ divides X^n-1 in $\mathbb{Q}[X]$

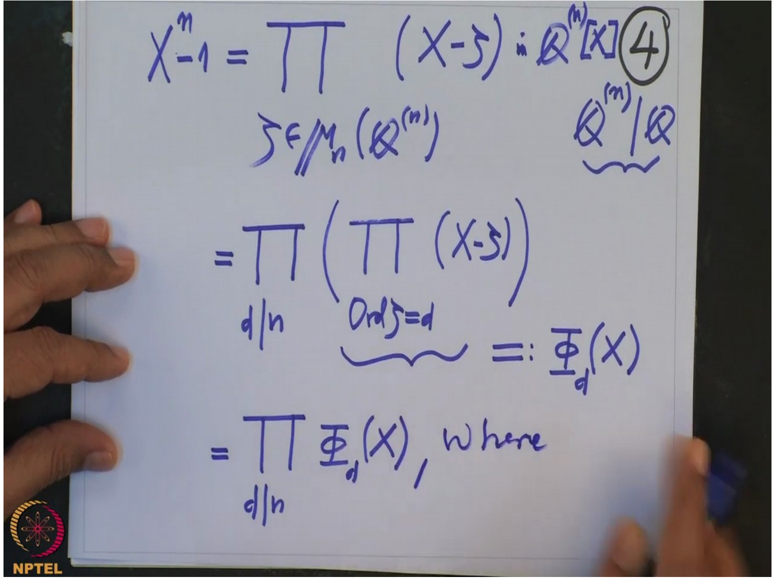
$\in \mathbb{Z}[X]$

Prime decomposition of X^n-1 in $\mathbb{Z}[X]$

Main problem is to find, so our goal is to find minimal polynomial of ζ over $\mathbb{Q}$. I am taking the case K equal to $\mathbb{Q}$. So this is the minimal polynomial ζ over $\mathbb{Q}$ where ζ is the primitive a primitive n-th root of unity. This is what we want to find. And this is this is a polynomial in $\mathbb{Q}[X]$. Monic and ζ is a zero of this polynomial, that is what information we know. More Moreover, more information we have is this $\mu_{\zeta,\mathbb{Q}}$ this divides X^n-1 in $\mathbb{Q}[X]$. This is another information. So therefore we want to find the prime decomposition of $X^n - q$. This is actually also a polynomial in $\mathbb{Z}[X]$.

And this is a irreducible polynomial over $\mathbb{Q}$. Therefore it is irreducible over $\mathbb{Z}$ and also because it is a monic polynomial. So monic polynomials are whether irreducible over $\mathbb{Q}$ and irreducible over $\mathbb{Z}$, they are same. That was also Gauss's theorem. So therefore, we want to find prime composition of this polynomial and the one which is only one of them buying pol only one prime divisor of this. First of all, all the prime divisors will have a multiplicity 1 only because this polynomial is has distinct roots. So now prime divisors will also repeat. So the prime decomposition of of prime decomposition of this polynomial we are interested $X^n - 1$ in $\mathbb{Z}[X]$. And one of the fact one of the prime factors must be this. All right? So how do we find that?

(Refer Slide Time: 10:01)



4

$$X^n - 1 = \prod_{\zeta \in \mu_n(\mathbb{Q}^{(n)})} (X - \zeta) \text{ in } \mathbb{Q}^{(n)}[X] \qquad \underbrace{\mathbb{Q}^{(n)} | \mathbb{Q}}$$

$$= \prod_{d|n} \Big(\underbrace{\prod_{\mathrm{Ord}\,\zeta = d} (X - \zeta)} \Big) \quad =: \Phi_d(X)$$

$$= \prod_{d|n} \Phi_d(X), \text{ where}$$

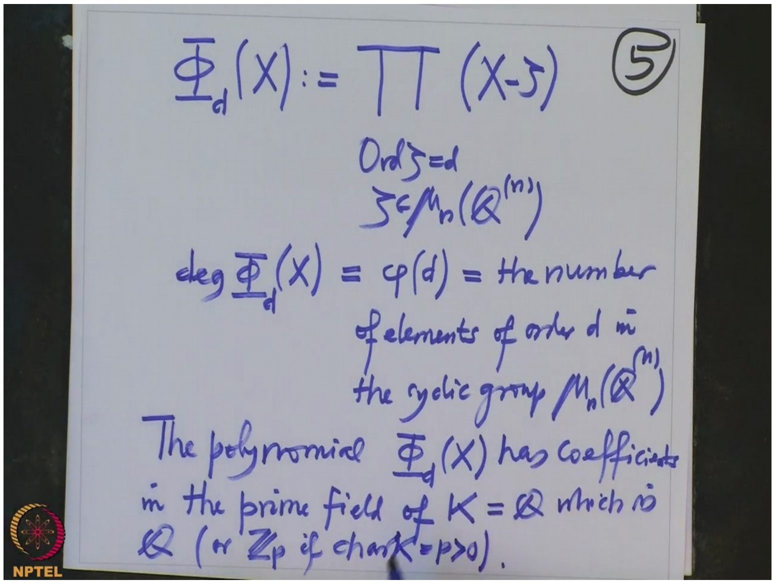
Alright. So what we do is the following. So we have this polynomial $X^n - 1$ and we know all the zeros of this polynomial are precisely the roots of unity n-th roots of unity and all of them lie in our field extension $\mathbb{Q}$ power round bracket n over $\mathbb{Q}$. This is the field extension we are studying. And all the zeros of this polynomial are in this field. Okay. So this one is therefore a product product is running over ζ. ζ is an element in $\mu_n(Q^{(n)})$. These are this is by definition. This is all those elements in $\mathbb{Q}^{(n)}$ where that power n is 1 but they are all of them are here.

That is how we have noted that this is this this is the splitting field of this point normal. So all the roots lie here and all the roots are elements of this. So this $X-\zeta$. This is, this decomposition is where? This decomposition is in $\mathbb{Q}^{(n)}[X]$ but that is not what we want. We want actually in $\mathbb{Q}[X]$ or in $\mathbb{Z}[X]$. All right. So this, I am going to rearrange this product. So this product is same thing as, this product is running over elements in some group, cyclic group. So therefore and the order of that group is n. This is the group, order of this group is n.

So therefore, every element of this group will have order. The order will be positive order and orders are precisely the divisors of n. So this product first of all I want to divide into the according to the order. So this is product d divides n. And then, product where orders of these elements equal to d. We take their corresponding linear factors. So I have just rearranged. d divides n and order of this element d, so that exhausts all elements of this group because this is a group and therefore elements have order d which are divisors of n and then this. Now this this inside thing, I am going to define that as $\Phi_d(X)$.

So therefore in this, this is a product d divides n $\Phi_d(X)$. so this polynomial has is written as a product of these elements where…

(Refer Slide Time: 13:20)



$\Phi_d(X) := \prod (X-\zeta)$ 5

$\text{Ord}\,\zeta = d$

$\zeta \in \mu_n(\mathbb{Q}^{(n)})$

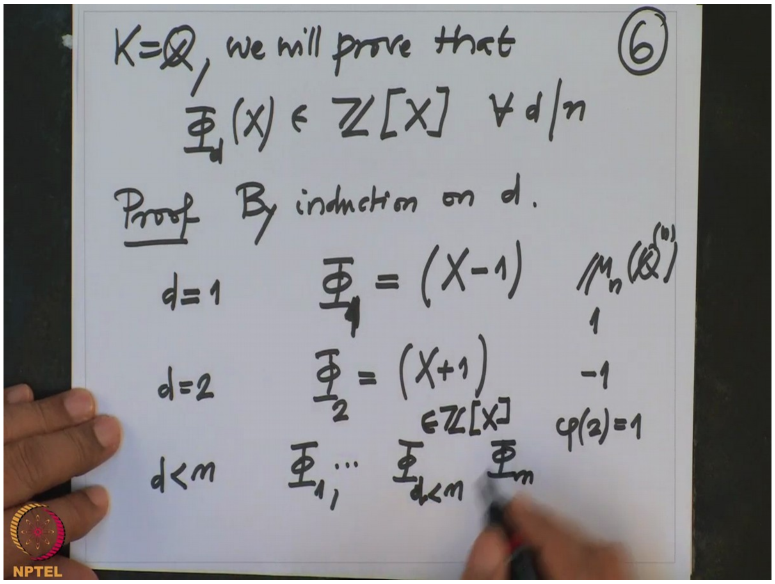
$\deg \Phi_d(X) = \varphi(d) =$ the number of elements of order d in the cyclic group $\mu_n(\mathbb{Q}^{(n)})$

The polynomial $\Phi_d(X)$ has coefficients in the prime field of $K = \mathbb{Q}$ which is $\mathbb{Q}$ (or $\mathbb{Z}_p$ if char $K = p > 0$).

… $\Phi_d(X)$ is by definition product , a product is running over order d elements and ζ is an element in $\mu_n(\mathbb{Q}^{(n)})$ $X-\zeta$. This is what the polynomial is. And therefore we know what is the degree? Degree of Φ_d , this is clearly the number of elements of order D in this cyclic group of order n. So that is Φ_d . This is the number of elements of order D in the cyclic group $\mu_n(Q^{(n)})$ and therefore it is the Euler's free function Φ_d . All right. Now I want to check that the coefficients the coefficients I want to know where apriory this is a polynomial where this is apriory this is a polynomial over this field.

But I want to check that this polynomial actually has integer coefficients. So the polynomial $\Phi_d(X)$ has coefficients in in the prime field of K. Now I do not I do not even have to assume Q. This will work for arbitrary field till here. So prime field of $\mathbb{Q}$ and where K is $\mathbb{Q}$, what is the prime field? That is precisely $\mathbb{Q}$ which is $\mathbb{Q}$ or $\mathbb{Z}_p$ if the characteristic of K was p positive. Anyway, we fix we do it for first the characteristic 0 case which is p. So I know, how am I going to prove this? So this, the coefficient I want to prove that they are in $\mathbb{Q}$. Actually, I want to prove that the coefficients are in $\mathbb{Z}$ actually. In in case of $\mathbb{Q}$, coefficients so let me write.

(Refer Slide Time: 16:42)



K=$\mathbb{Q}$, we will prove that 6

$\Phi_d(X) \in \mathbb{Z}[X]$ $\forall$ d/n

Proof By induction on d.

d=1 $\Phi_1 = (X-1)$ $\mu_n(\mathbb{Q}^{(n)})$ 1

d=2 $\Phi_2 = (X+1)$ -1

$\in \mathbb{Z}[X]$ $\varphi(2)=1$

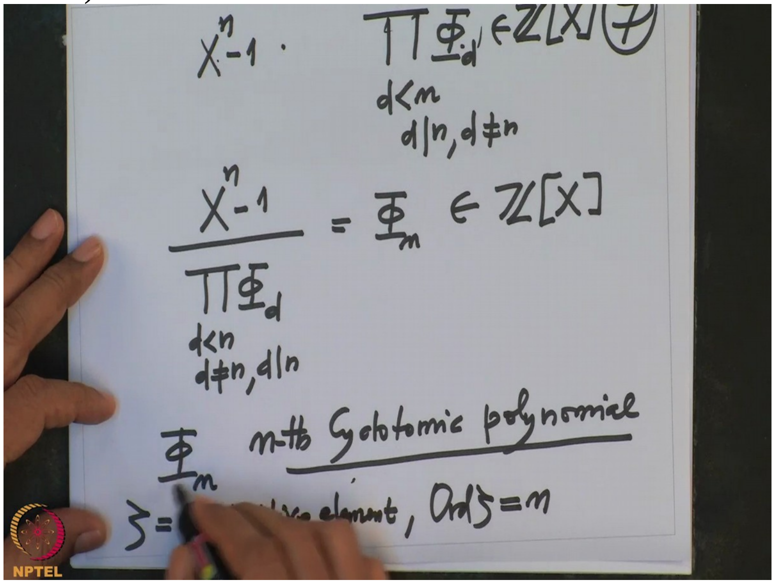
d<m $\Phi_1, \dots \Phi_{d<m}$ Φ_m

They will, so when K equal to $\mathbb{Q}$, we will prove that $\Phi_d(X)$ actually the polynomial over Z for every d divisor of n. This is what I want to prove and this I am going to prove it by induction on d. Proof by induction on d. So let us see what is, when d equal to 1, what is $\phi(1)$? $\phi(1)$ is the product. Product is running over all elements of order 1 but there is exactly one element of order 1 in any group, namely the identity element. So that will be 1, so that is this. phi of 1 is $X-1$ because 1 is the only element in that group of order 1 , yes 1. $\mu_n(Q^{(n)})$ this group has only one, so identity element is 1. So, and this is only one element of order 1. So it is C1 is 1. So d equal to 2. d equal to 2, how many elements are there of order 2?

There are exactly one element of order 2, namely minus 1 because in any cyclic group, order of elements the number of elements of order d are precisely $\phi(d)$ and $\phi(2)$ is one. Therefore there is only one element of order 2 which is minus 1. Therefore $\phi(2)$ is what? $\phi(2)$ is $X+1$. $X-(-1)$, that is + 1. So phi 2 is this. So induction starts. Now for any, I have to, I assume that upto, I only have to prove that the last one because if n, if d were strictly smaller than n, then we know we have proved by induction that all this phi 1, etc, all this phi the last one, I do know what it is, the divisors, this one where this this d, this d is strictly smaller than n, all this and there is nobody, the next one is only $\phi(n)$, all these elements are coefficients in $\mathbb{Z}$ and now I want to prove that this one has coefficients in $\mathbb{Z}$.

But look, we know that when you divide a polynomial over increases by a monic polynomial, the divisors, quotient and the remainder, they are unique elements. In the division algorithm, quotient and the remainders are uniquely determined.

(Refer Slide Time: 20:20)



$$X^n - 1 \cdot \prod_{\substack{d<n \\ d|n,\, d \neq n}} \Phi_d \in \mathbb{Z}[X] \; \textcircled{7}$$

$$\frac{X^n - 1}{\prod_{\substack{d<n \\ d\neq n,\, d|n}} \Phi_d} = \Phi_n \in \mathbb{Z}[X]$$

Φ_n n-th Cyclotomic polynomial

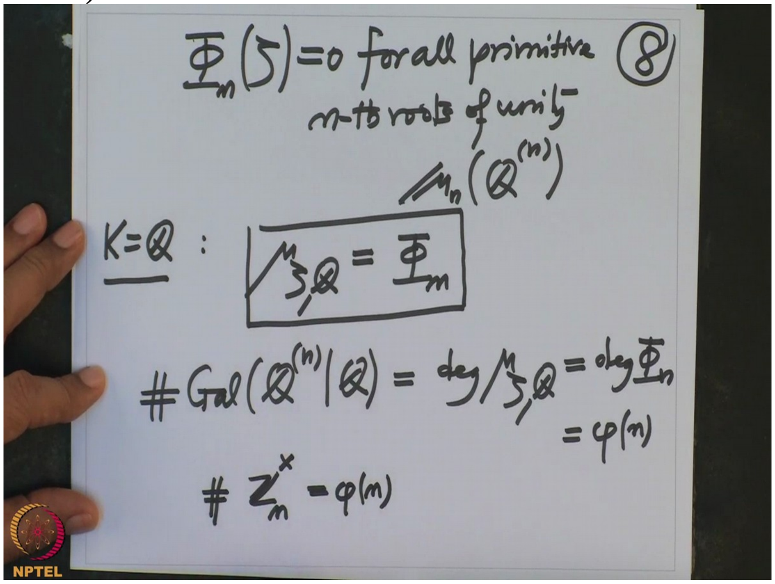
$\zeta =$ [illegible] element, $\mathrm{Ord}\,\zeta = n$

So therefore if I want to divide this polynomial $X^n - 1$ by the product $\phi(d)$ where d is strictly smaller than n and all of them, nobody after that and d is strictly smaller than n, d divides n and d not equal to n, these are already we have checked that all these polynomials are by induction are in $\mathbb{Z}[X]$. So the product is in $\mathbb{Z}[X]$, this is a monic polynomial. So when I divide this polynomial by this product, what do I get? I get this $X^n - 1$ divided by this product, that is d is smaller than n, d not equal to n and d divides n, this is nothing but $\phi(n)$.

Because we know $X^n - 1$ is a product of all $\phi(d)$ s and only one is left. So therefore, this when I divide, when I perform the division algorithm by this polynomial, divide this polynomial by this one, then I get a quotient and the remainder. There is no remainder because this divides this and the quotient is precisely this and this is unique. And this happens in $\mathbb{Z}$. So therefore you have no choice, this has to be in $\mathbb{Z}[X]$. So therefore, we know that all these polynomials phi n are have integer coefficients. So this polynomial $\phi(n)$, this $\phi(n)$ is called n-th cyclotomic polynomial n-th cyclotomic polynomial. Okay.

Now what was our problem? Our problem was to find if I have if I have ζ which is not arbitrary element but the primitive element. If these are if this ζ is a primitive element primitive element, that means a generator of μ_n, so the order of the ζ equal to n, therefore that $X-\zeta$ is comes in a is a factor of this $\phi(n)$. So therefore I definitely know.

(Refer Slide Time: 23:14)



$\Phi_n(\zeta)=0$ for all primitive n-th roots of unity ⑧

$\mu_n(\mathbb{Q}^{(n)})$

$\underline{K=\mathbb{Q}}$: $\boxed{\mu_{\zeta,\mathbb{Q}} = \Phi_n}$

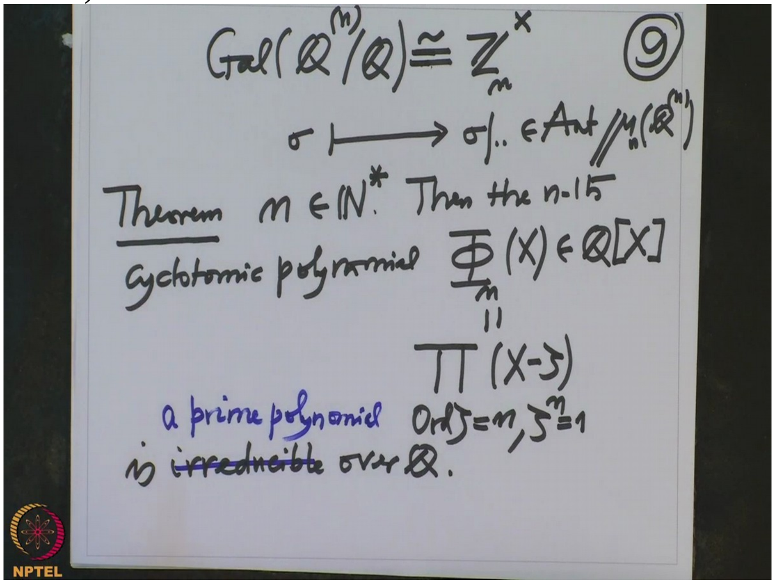
$\# Gal(\mathbb{Q}^{(n)}|\mathbb{Q}) = \deg \mu_{\zeta,\mathbb{Q}} = \deg \Phi_n = \varphi(n)$

$\# \mathbb{Z}_n^{\times} = \varphi(n)$

So this shows that $\Phi_n(\zeta)$, this is zero not only for one primitive, this is true for all primitive Nth roots of unity because they are precisely the generators of this group $\mu_n(Q^{(n)})$. So therefore, we must prove that if K equal to $\mathbb{Q}$, we must prove that myu minimal polynomial of ζ over $\mathbb{Q}$ is nothing but phi n. If we prove this, then we will know. What will you know? So suppose we prove this, then we will know that the order of the Galois group which is equal to the degree of $\mu_{\zeta,\mathbb{Q}}$ which is degree of the polynomial Φ_n I know degree.

This degree is $\phi(n)$ because Φ_n is precisely product of all linear factors which are number of elements of order n in this group and they are precisely $\phi(n)$. So this is precisely the degree Φ_n. On the other hand, this was a divisor of this group was a subgroup of the unit group of $\mathbb{Z}_n^x$ and therefore this order was a divisor of this. But this odd the group of this order is also equal actually.

(Refer Slide Time: 25:19)



$\mathrm{Gal}(\mathbb{Q}^{(n)}/\mathbb{Q}) \cong \mathbb{Z}_n^{\times}$ 9

$\sigma \longmapsto \sigma|_{..} \in \mathrm{Aut}(\mu_n(\mathbb{Q}^{(n)}))$

Theorem $n \in \mathbb{N}^*$. Then the n-th cyclotomic polynomial $\Phi_n(X) \in \mathbb{Q}[X]$

$\Phi_n = \prod (X-\zeta)$ $\mathrm{Ord}\,\zeta = n, \zeta^n = 1$

a prime polynomial
is ~~irreducible~~ over $\mathbb{Q}$.

So therefore, we have no, we get that the Galois group is, so from this we already infer that the Galois group of $\mathbb{Q}^{(n)}$ over $\mathbb{Q}$ is actually $\mathbb{Z}_n^x$. Because it is a subgroup and the orders are same, therefore it has to be equal. This is isomorphic and this is a canonical isomorphism. This can a this isomorphism means any automorphism of $\mathbb{Q}^{(n)}$ over Q, this is mapped to the restriction of that automorphism and that is thought as an automorphism of this group, this cyclic group, $\mu_n(\mathbb{Q}^{(n)})$ which is a cyclic group of order n and therefore automorphism group has order phi n and which is actually this group.

So that gree that gives a complete description of the Galois group of $\mathbb{Q}^{(n)}$ over $\mathbb{Q}$ provided, we prove that this polynomial is the minimal polynomial of this one. So that needs a proof and that is the only nontrivial proof so far. So I will state it as a theorem. So theorem so theorem is what now? n is any nonzero natural number. Then the n-th cyclotomic polynomial Φ_n which is a polynomial in $\mathbb{Q}[X]$, this is defined by a product $X-\zeta$ where order of ζ equal to n and $\zeta^n=1$. So it is n-th root of, primitive n-th roots of unity all the product, this is irreducible over Q. Actually I should write better. I should write, is a prime polynomial. It is a monic polynomial and it is prime, means it is a monic irreducible polynomial and this is, we will prove this next time. We will need a little time to prove this and I will postpone the proof to the next one. So to summarize, what did we did today?

What we did was, the main 2 examples. One is, the finite field, finite extension of the finite field, this Galois group is actually we proved it is a Galois extension, means the Galois group cyclic generated by the Frobenius automorphism and in the 2nd case, we proved that if you take the roots of unity, the splitting field of the polynomial $X^n - 1$ over $\mathbb{Q}$, this is splitting field is a Galois extension of $\mathbb{Q}$ degree $\phi(n)$ and the Galois group is Abelian. In fact, the Galois group is the unit group of the ring $\mathbb{Z}_n$. And then next time we will prove this theorem, irreducibility of the cyclotomic polynomial over $\mathbb{Q}$ and we will further now analyze what happens if I take that characteristic p fields? In particular, finite fields. What happens to the Galois group of the splitting field of the polynomial $X^n - 1$ over a finite field characteristic p. Thank you.