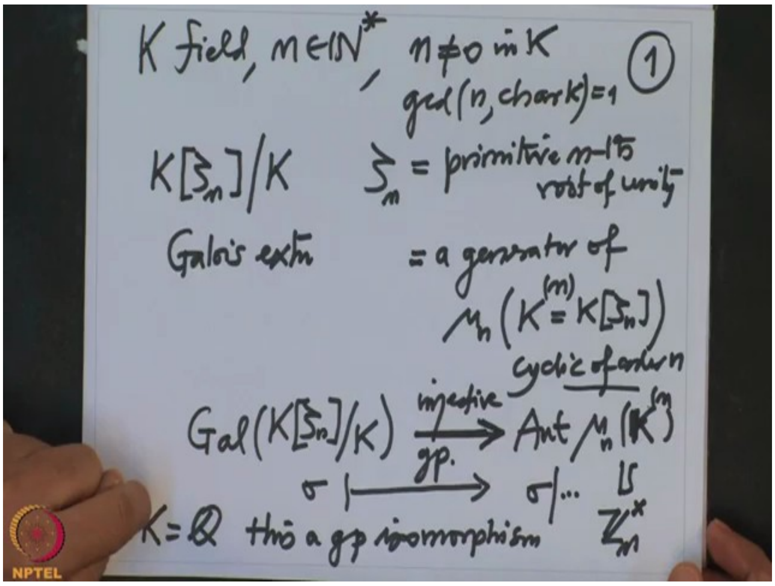
Galois' Theory.
Professor Dilip P. Patil.
Department of Mathematics.
Indian Institute of Science, Bangalore.
Lecture-37.
Reducibility of Cyclotomic polynomials over finite fields.

(Refer Slide Time: 0:37)



K field, $n \in \mathbb{N}^*$, $n \neq 0$ in K 1
$\gcd(n, \operatorname{char} K) = 1$

$K[\zeta_n]/K$ ζ_n = primitive n-th root of unity
Galois extn = a generator of
$\mu_n(K^{(n)} = K[\zeta_n])$
cyclic of order n

$$\mathrm{Gal}(K[\zeta_n]/K) \xrightarrow[\text{gp.}]{\text{injective}} \mathrm{Aut}\,\mu_n(K^{(n)})$$
$$\sigma \longmapsto \sigma|\ldots \quad \cong$$
K = ℚ this a gp isomorphism $\mathbb{Z}_n^\times$

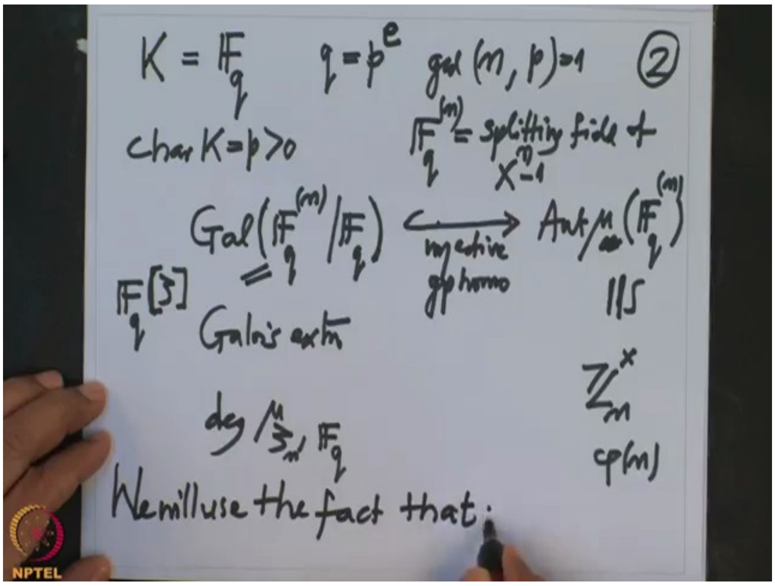
Okay, so let us summarize what we have done in the last lecture and a couple of lectures before that. What we did was K, any field, n, nonzero natural number and the function n not equal to 0 in K so that is GCD of n and characteristic of K, these are co-prime. Then we are studying the field extension K, ζ_n over K, where this ζ_n is a primitive nth root of unity, which is a generator, a generator of this group μ_n , $K^{(n)}$, remember our notation for $K^{(n)}$ is $K[\zeta_n]$. This is a multiplicative subgroup of $K^{(n)}$ it is cyclic of order n and we want to, we are proved that this extension is Galoi's, Galoi's extension and we are wanted to find the Galoi's group of this extension.

And what we proved is, the first what we proved in the last 2 lectures, the Galoi's group of $K[\zeta_n]$ over K from this group to the Automorphism group of this cyclic group $\mu_{n,K(n)\text{¿}}$, this is cyclic group of order n, so there is a canonical homomorphism here. Namely σ goes to the σ restricted to that because this is a subgroup of this. So I can restrict and because it is a restriction, this group homomorphism is injective, injective group homomorphism.

And in the last lecture we approved actually that this group homomorphism is bijective, when K equal to $\mathbb{Q}$. K equal to $\mathbb{Q}$, this is a group isomorphism. Therefore the Galoi's group of this is the Automorphism group of the cyclic group and the Automorphism group of cyclic group of order n is, we can identify this cyclic group, this Automorphism group with the group $\mathbb{Z}_n^x$. And how is the identification gone? That is if you have an Automorphism, it will map generator to a power of generator and that power should be co-prime to the order of the generator and therefore it is mapping to that, this is the identification.

So for $\mathbb{Q}$, we have the complete answer, namely the order of this Galoi's group is precisely the order of this Automorphism group, which is precisely the order of this is $\mathbb{Z}_n^x$ group which is precisely Euler's torsion function $\phi(n)$, value of the Euler's torsion function at n. Now we want to do this for finite field case. So characteristic p case, where K is a prime field of characteristic p, this was a prime field of characteristic zero.

(Refer Slide Time: 4:29)



$K = \mathbb{F}_q \quad q = p^e \quad \gcd(n, p) = 1$ ②

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

$\mathbb{F}_q^{(n)} =$ splitting field of $X^n - 1$

$$\mathrm{Gal}(\mathbb{F}_q^{(n)}/\mathbb{F}_q) \xrightarrow[\text{gp homo}]{\text{injective}} \mathrm{Aut}\,\mu_n(\mathbb{F}_q^{(n)})$$

$\mathbb{F}_q[\zeta]$ $=$ Galois extn $\cong$ $\mathbb{Z}_n^\times$

$\deg \mu_{\zeta_n, \mathbb{F}_q}$ $\varphi(n)$

We will use the fact that:

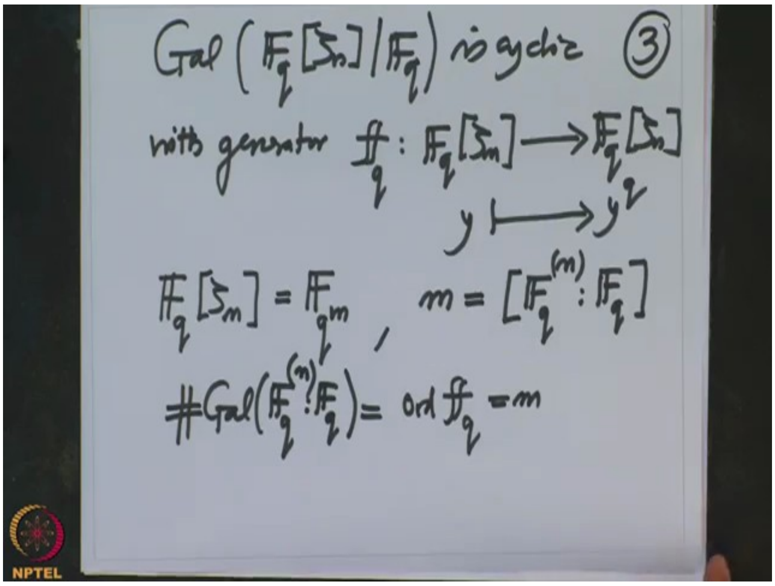
Now we are assuming that K is actually, actually I will do little bit more general, actually I will assume that K is a finite field of order q, where q is, characteristic has to be prime, characteristic K is p Positive, therefore this q, the number of elements has to be power of the characteristic. So I will denote q equal to p^e . And we do the same, what do we do, we have now n, which is now co-prime to p and we are interested in finding out what happens to this map, this F_{q^n} over F_q , this Galoi's group and this Automorphism, $Aut\,\mu_n$, do not write μ_n here $\mu_{F_q}^{(n)}$.

So this is F_q , this is nothing but the splitting field of, field of the polynomial, and $X^n - 1$. That means you are attaching all the roots of this polynomial to this field and we are considering the field extension. Now what we know, we do not know what is the order, we only know that this is a subgroup, this map is injective, this restriction map, this is injective. That is the only information we have, group homomorphism. And these are, this we know, this is identified with $\mathbb{Z}_n^x$. So this order we know, this is $\phi(n)$ and in case of characteristic zero, we actually proved this map is bijective.

So then the order of the Galoi's group in the characteristic zero case, it is same as $\phi(n)$. We actually found the minimal polynomial, now here also we know that this is the Galoi's extension, therefore order of this group I know. Order of this group is precisely degree of the minimal polynomial of ζ_n over F_q , minimal polynomial of this because this is a, because this extension is generated over F_q by the root, primitive root. That we know, we have, we know that information because this is a splitting field and ζ is a generator of this group, μ_n , $\mu_{F_q,n}$, this is cyclic.

So if I know one element, where all the elements, their powers of σ and therefore this extension is cyclic, therefore we know this is Galoi's extension and the order of the Galoi's group equal to the degree of the field extension which is in this case because it is simple, it is degree of the minimal parliament. This is all we know, now we want to check, it is not bijective in general, so we want to check therefore what is the image and the extra information we have in a finite field case that this group is cyclic.

(Refer Slide Time: 8:36)



$\mathrm{Gal}\left(\mathbb{F}_q[\zeta_n] / \mathbb{F}_q\right)$ is cyclic ③

with generator $\mathrm{F}_q : \mathbb{F}_q[\zeta_n] \longrightarrow \mathbb{F}_q[\zeta_n]$

$y \longmapsto y^q$

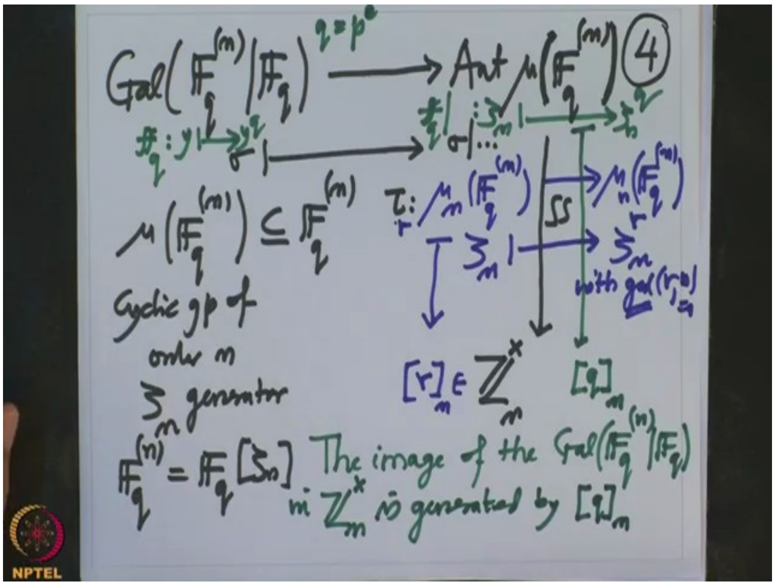
$\mathbb{F}_q[\zeta_n] = \mathbb{F}_{q^m}$, $m = [\mathbb{F}_q^{(m)} : \mathbb{F}_q]$

$\#\mathrm{Gal}(\mathbb{F}_q^{(m)} : \mathbb{F}_q) = \mathrm{ord}\, \mathrm{F}_q = m$

We know, now we will use information, the fact that, I will write on the next page. This group $Gal(F_q[\zeta_n] | F_q)$ is cyclic with generator, I know also generator, I know also its generator. What is a generator, it is the Frobenius f_q , that is, this is a map from $F_q[\zeta_n]$ to $F_q[\zeta_n]$, it maps an element y to y^q . So , remember that this $F_q[\zeta]$, F_q in this time, these are also finite fields. And it will have certain number of elements, common elements, let us write that also, $F_q^{(n)}$ this is a finite field with n elements and what is n, n should be the degree of the dimension of $F_q^{(n)}$ Over F_q , the dimension, this is the degree, that is n.

And we know this Galoi's group, therefore has cyclic of order n. So this has $F_q^{(n)}$ order, order of F_q is n, which is also the order of the Galoi's group. Right, and now I want to see, I want to write down now the identification more precisely because we want to see what is image. And because a map is injective, the image of a cyclic group will also be cyclic. The image will be generated by the image of a generator, therefore I know, therefore we have to understand the identification.

(Refer Slide Time: 11:21)



$Gal(\mathbb{F}_q^{(n)}|\mathbb{F}_q) \longrightarrow Aut\,\mu(\mathbb{F}_q^{(n)})$ ④
$q = p^a$
$\#_q : y \mapsto y^q$
$\sigma \longmapsto \sigma|\ldots$
$\#_q|$: $\zeta_n \longmapsto \zeta_n^q$
$\mu(\mathbb{F}_q^{(n)}) \subseteq \mathbb{F}_q^{(n)}$
$\tau_r : \mu_n(\mathbb{F}_q^{(n)}) \to \mu_n(\mathbb{F}_q^{(n)})$
$\zeta_n \longmapsto \zeta_n^r$
with $gcd(r,n)=1$
Cyclic gp of order n
ζ_n generator
$[r]_n \in \mathbb{Z}_n^{\times}$
$[q]_n$
$\mathbb{F}_q^{(n)} = \mathbb{F}_q[\zeta_n]$
The image of the $Gal(\mathbb{F}_q^{(n)}|\mathbb{F}_q)$ in $\mathbb{Z}_n^{\times}$ is generated by $[q]_n$
NPTEL

So I will let it once more, so this is $Gal(F_q^{(n)}|F_q)$, this means the injective map as given to the Automorphism group of $\mu(F_q^{(n)})$. These are roots of unity in $F_q^{(n)}$ and this map is σ going to, σ restricted to that. Because this is $\mu(F_q^{(n)})$, these are the roots of unity inside $F_q^{(n)}$, they are all of them there. This is a group of order, cyclic group of order n and ζ_n is a generator. This is what all we know and then we know $F_q^{(n)}$, this is nothing but $F_q[\zeta_n]$, this is all we know. And then we have identified this, this identification with $\mathbb{Z}_n^x$.

And what is the identification, if we have an Automorphism τ of the cyclic group, so let me just write down the elements of this Automorphism group down here or I will write it here. τ , if it is an Automorphism of this group $\mu_n(F_q^{(n)})$ to $\mu_n(F_q^{(n)})$. So the Automorphism of a cyclic group will map a generator ζ_n to a generator. But I know all the generators of the cyclic group, I know one of them, I know the order of the group, then I know all the generators. All the generators will be of the form ζ_n^r , where r is co-prime to n.

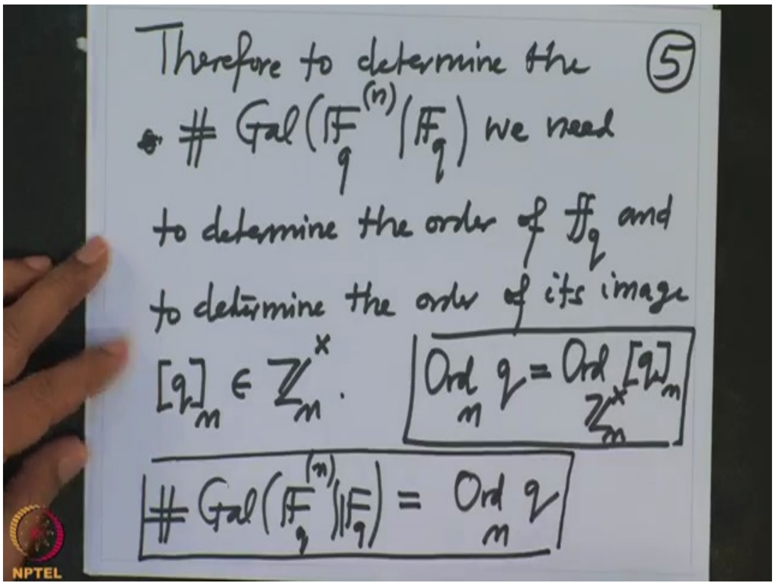
GCD of r and n is equal to 1. And then we are identifying this τ , this τ is uniquely determined by the r. So I could have simply written this τ as τ_r . So each co-prime integer r to n will give you τ_r and each τ will give you r. So the identification of this, this is r, this is r, that is the identification. And this r, we are reading mod n, strictly speaking it is r, I should write rn. When you are reading r modulo n. And that is clearly an element Because r and n are co-prime, so they are precisely the units in this ring.

So therefore, our problem is where we will Frobenius, which is a generator of this group, where will it go under this identification, that is what we want to understand. So where we will Frobenius go? So, I will, I still have the space here, so I will use now the green colour. So we are interested in where we will Frobenius go. What is the Frobenius? Frobenius is, it is denoted by Fq and Fq, what is the Fq map, that maps any element y of the field to y power q. So and where will it go here, that is Frobenius restricted to this group, that means it is restricted to the unity, roots of unity.

But where will that map ζ_n , ζ_n will get mapped to ζ_n^q . And q, what was q? q was p, the power of p, the q was characteristic, q was the power of the characteristic. So q was p^e . And that, that one, I want, that q goes to, you are reading that q, where will this Frobenius go then, this q reading mod n and then that is reading mod n is this notation, so q goes to the. So therefore the image of this Galoi's group in this generated by that q.

So I will write here, the image of the Galoi's group, $Gal(F_{q^n}|F_q)$ is in $\mathbb{Z}_n^x$ is generated by $[q]_n$. That integer q which is the power of p will generate the image of the Galoi's group. So in particular it is cyclic. So therefore we have to find, you have to find the order of the Galoi's group, I have to find the order of the generator.

(Refer Slide Time: 17:25)



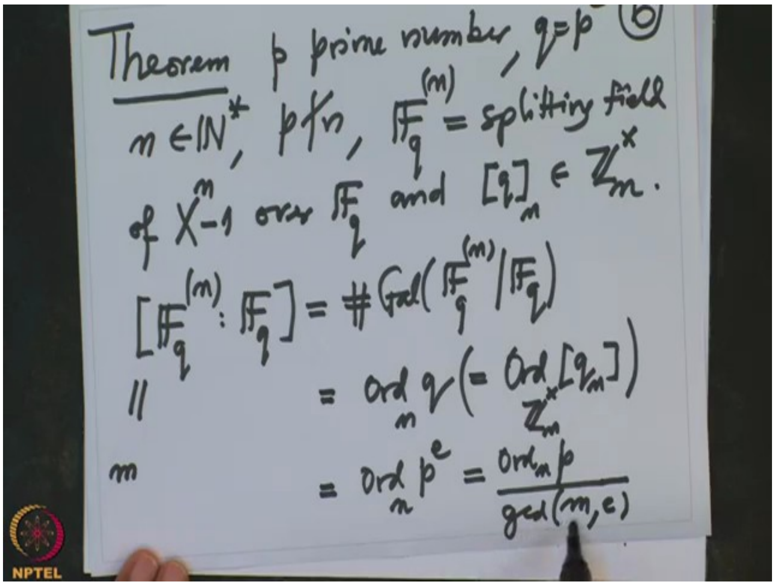
Therefore to determine the ⑤

$\# \mathrm{Gal}(\mathbb{F}_q^{(n)}|\mathbb{F}_q)$ we need to determine the order of $\mathbb{F}_q$ and to determine the order of its image $[q]_n \in \mathbb{Z}_n^\times$. $\boxed{\mathrm{Ord}_n\, q = \mathrm{Ord}_{\mathbb{Z}_n^\times} [q]_n}$

$$\boxed{\# \mathrm{Gal}(\mathbb{F}_q^{(n)}|\mathbb{F}_q) = \mathrm{Ord}_n\, q}$$

So, therefore to determine the order, the cardinality of the Galoi's group, we need to determine the order of F_q . And hence to determine the order of its image, which is a residue class of q in the group $\mathbb{Z}_n^x$. And this order I am going to denote by order of $[q]_n$, this is precisely the order of the residue class of q mod n in the group $\mathbb{Z}_n^x$, this is what we need to compute. In other words, what we have proved is Galoi's group, the order of the Galoi's group, this order equal to order of q n. This is by definition the order of the residue class q in $\mathbb{Z}_n^x$. So this is what we proved.

(Refer Slide Time: 19:45)



Theorem p prime number, $q = p^e$ ⑥

$n \in \mathbb{N}^*$, $p \nmid n$, $\mathbb{F}_q^{(n)}$ = splitting field of $X^n - 1$ over $\mathbb{F}_q$ and $[q]_n \in \mathbb{Z}_n^\times$.

$$[\mathbb{F}_q^{(n)} : \mathbb{F}_q] = \# \mathrm{Gal}(\mathbb{F}_q^{(n)}|\mathbb{F}_q)$$

$\parallel \qquad = \mathrm{Ord}_n\, q \; (= \mathrm{Ord}_{\mathbb{Z}_n^\times} [q_n])$

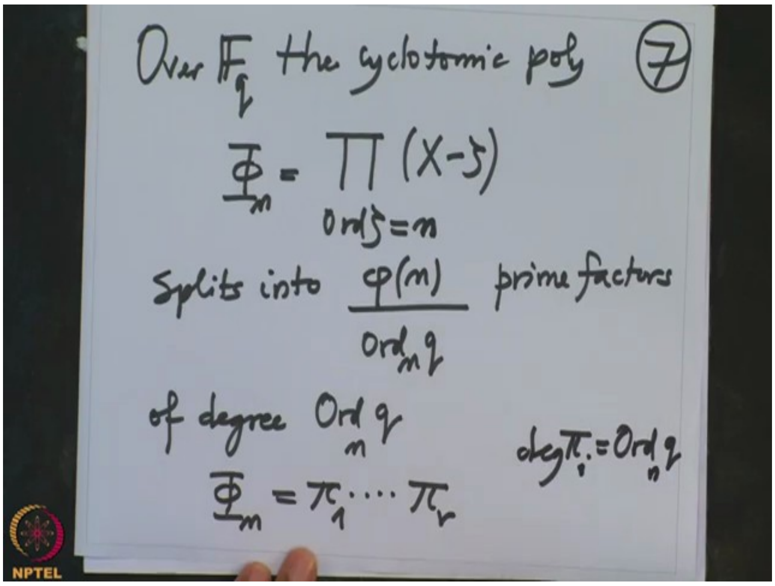
$m \qquad = \mathrm{Ord}_n\, p^e = \dfrac{\mathrm{Ord}_n\, p}{\gcd(m, e)}$

So let me write this as theorem, I will summarise in the theorem and, so the theorem what we proved is the following. So, we are taking p prime number and q is the power of p, exponent and we are considering the polynomial an n, integer n nonzero natural number, n is co-prime to p and we are taking the $F_q^{(n)}$, this is the splitting field of the polynomial $X^n - 1$ over F_q . And we are denoting qn, this is a residue class of q in $\mathbb{Z}_n$. And note that this q and n are co-prime because q is a power of p and p does not divide n, so this an element here.

Okay, with this notation, then we know that the degree of the field extension, this is equal to the order of the Galoi's group and we know it is a Galoi's extension, therefore this equality, in fact we also know that this group is cyclic. So we have used that information to check that this order is nothing but the order of q n, this is precisely by definition order of q n in this group. And what is your do then? But q is a power of p and I know what is the power of, what is, this is precisely the order of order $n p^e$. And I know how do you compute order of element, order of an, power of an element in terms of the elements.

So this order is same thing as order of p divided by GCD of n and e. And what is n is, where n is, n is equal to this order, whatever it is. So we have become so these I wrote, the last 2 equalities I wrote precisely for the calculation purpose. So, the order of p power e, you only have to calculate the order of that prime number p in $\mathbb{Z}_n$ and we have to go mod, divide it by the GCD of n and e, so where n is the order of that group, where we are working. So order of n is also the order of, this is the order of n, this group. So this n is the degree of this field extension.

(Refer Slide Time: 23:49)



Over $\mathbb{F}_q$ the cyclotomic poly 7

$$\Phi_n = \prod_{\text{Ord}\,\zeta = n} (X - \zeta)$$

Splits into $\dfrac{\varphi(n)}{\text{Ord}_n q}$ prime factors

of degree $\text{Ord}_n q$ $\deg \pi_i = \text{Ord}_n q$

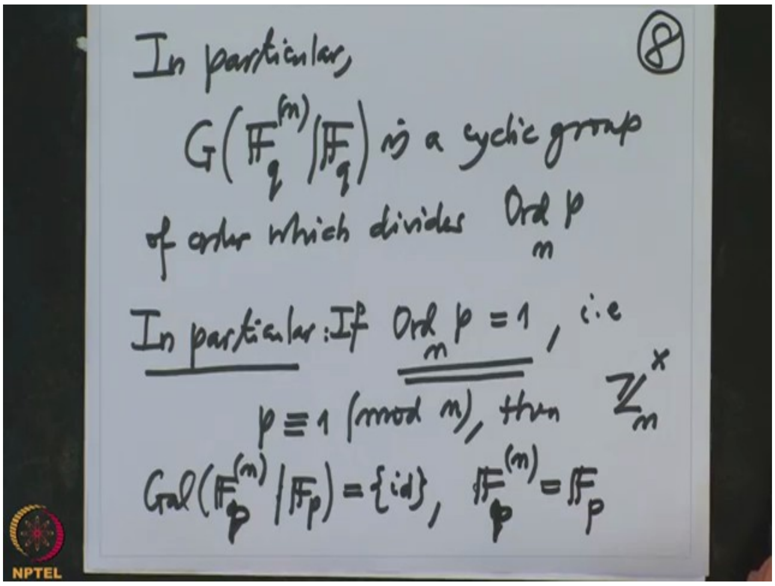
$$\Phi_n = \pi_1 \cdots \pi_r$$

So that is a complete answer to this. Now, therefore what will be the, it is therefore, question remains, what is the minimal polynomial? Whatever it is, so I know therefore phil n, so I will just write a statement over Fq, the cyclotomic polynomial. What is a cyclotomic polynomial? You take Φ_n , that is you take all elements of order n, $X-\zeta$ and order of ζ is n. This is, this is a cyclotomic polynomial. This order, this polynomial now split into how many factors? I know, this group has order, this group has order so much and this is a sub group of this group $\mathbb{Z}_n^x$.

So therefore the cyclotomic polynomial splits into how many irreducible factors? The total was , Φ_n the degree of this polynomial is $\phi(n)$ and among them I have to calculate, I have to take order n q divide by order n q because that is the order of this subgroup, that is the order of that subgroup. So cyclotomic polynomial is split into so many prime factors of degree order q n. Because each irreducible factor will give you finite field extension of the same degree, therefore this polynomial you spread into so many linear factors. So many, not linear, so many prime factors and it will be of this order.

So, so Φ_n will be equal to $\pi_1 \ldots \pi_r$, there are no multiplicity because they are all, there is no repeated zeros here because of our assumption locus and is not equal to, n is not divisible by p. And so each one of them Φ_i have degree this. So with a degree of π_i equal to order q n. So that is a complete information about the Galoi's group of a finite field. What we have proved is the following.

(Refer Slide Time: 26:45)



8

In particular,

$G(\mathbb{F}_q^{(m)}/\mathbb{F}_q)$ is a cyclic group of order which divides $\mathrm{Ord}_m\, p$

In particular: If $\mathrm{Ord}_m\, p = 1$, i.e $p \equiv 1 \pmod{m}$, then $\mathbb{Z}_m^{\times}$

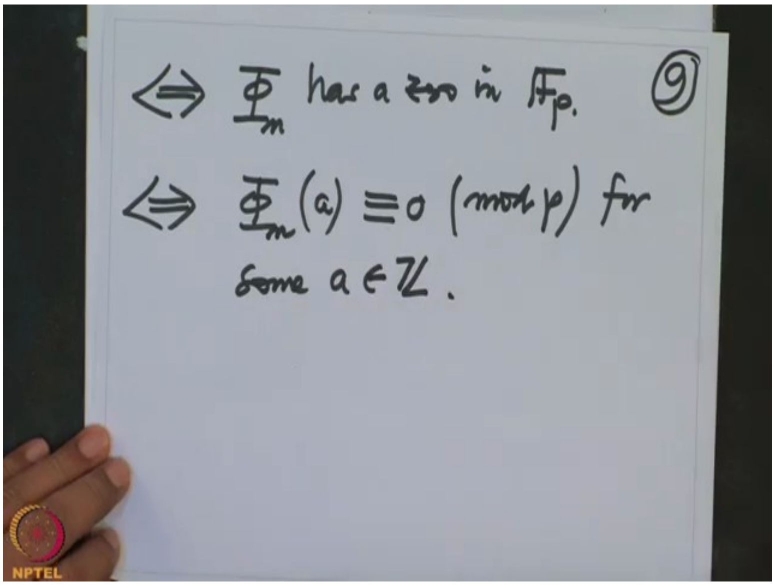
$\mathrm{Gal}(\mathbb{F}_p^{(m)}/\mathbb{F}_p) = \{id\}$, $\mathbb{F}_p^{(m)} = \mathbb{F}_p$

In particular, $Gal(F_q^{(n)}|F_q)$, this is a cyclic group of order which divides order of p mod n. See, because of answer should be in terms of the given data and given data is we have an integer and we have p. Because once we have p, we have q. So these answers depend only on p and n, okay. So the divisor of this, okay, so the particular case is what? So, in particular, further in particular, let us look at the case, when order of p is 1, what does that mean? This means what? If the order of p is 1, that means what?

That is p mod n is order 1, that means p has to be congruent to 1 mod n. Order 1 in which group, we are looking at this group $\mathbb{Z}_n^x$ and order 1 element here is precisely the identity element and identity element is precisely 1. So that means 1 and p coincides in this group, that means p is common to 1 mod n. So in this case, therefore the order of the Galoi's group which is the divisor of this order but this order itself is 1. So then the Galoi's group has order 1, that means these fields are equal.

So then $Gal(F_p^{(n)}|F_p)$, this has to be trivial, in particular therefore $F_p^{(n)}$ equal to F_p . And when can this occur, when will this occur? That means, that will mean that the phi, the cyclotomic polynomial should have zero in p only.

(Refer Slide Time: 29:44)



$\Longleftrightarrow$ Φ_n has a zero in $\mathbb{F}_p$. (9)

$\Longleftrightarrow$ $\Phi_n(a) \equiv 0 \pmod{p}$ for some $a \in \mathbb{Z}$.

That is if and only if, so, which is if and only if Φ_n has zero in the F_p . So that is if and only if $\phi(n)$ at a is congruent to 0 modulo p for some a in integer, it is clear. So here you see this equality means, this was a splitting field of $X^n - 1$ and this is generated by the roots of, the order 1, order n elements of that multiplicative group, consisting of roots of unity, that is all containing F_p. In particular this $\Phi(n)$ has a zero. But $\Phi(n)$ has a zero means, in F_p that means at some a it is zero but mod p everything, so that means this.

So, with this I will deduce further more corollaries from this in the next lecture. And then I will switch onto more examples of field extension which are Galoi's and debating how do you realise any finite abelian group as a Galoi's group over q. Okay, thank you.