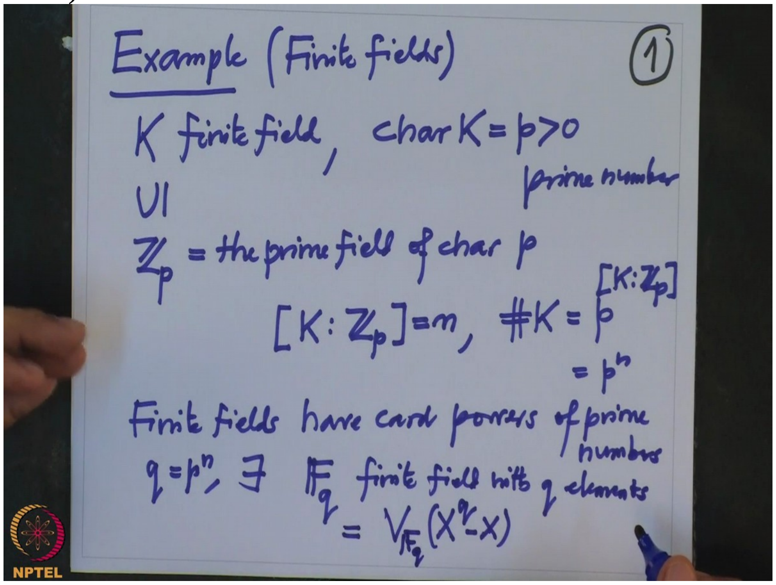
Galois' Theory
Professor Dilip Patil
Department of Mathematics
Indian Institute of Science Bangalore
Week 07
Lecture 33: Fundamental Theorem of Galois Theory [Contd]

So we have seen the fundamental theorem of Galois theory and its proof. Now I want to illustrate this fundamental theorem by some examples. Actually some part of these examples also we have discussed before.

(Refer Slide Time: 0:57)



Example (Finite fields) 1

K finite field, $\operatorname{char} K = p > 0$ prime number

$\cup|$

$\mathbb{Z}_p$ = the prime field of char p

$[K:\mathbb{Z}_p] = n$, $\#K = p^{[K:\mathbb{Z}_p]} = p^n$

Finite fields have card powers of prime numbers

$q = p^n$, $\exists$ $\mathbb{F}_q$ finite field with q elements $= V_{\mathbb{F}_q}(X^q - X)$

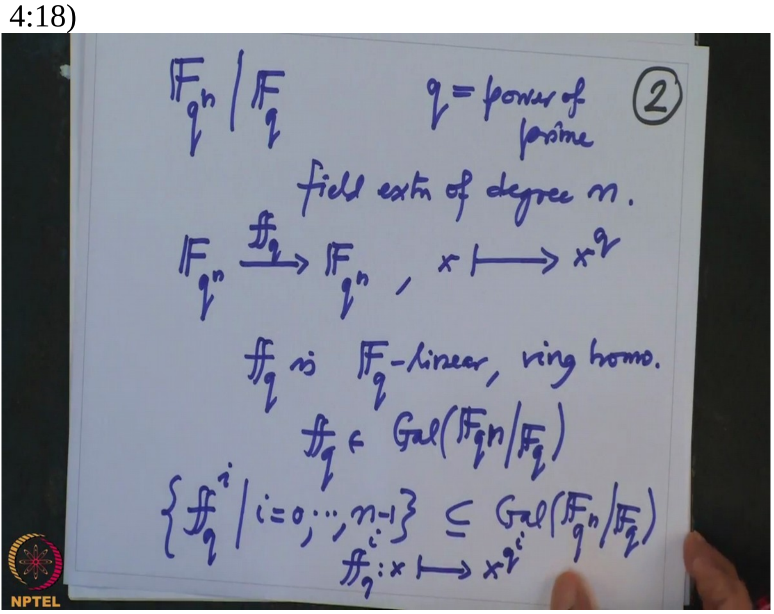
So the first example is about finite fields. So let us recall that supposed K is a finite field, then we now that the characteristic of the finite field cannot be positive cannot be zero. So characteristic of K has to be p positive. p prime number. Because K is a field, therefore the characteristic has to be prime number and because it is finite, it has to be positive. That simply means that K contains the field that $\mathbb{Z}_p$, this is the prime field of K. This is the prime field of characteristic p. And then the degree of the field extension has to be finite K over $\mathbb{Z}_p$'s capital and. Then the cardinality of K has to be p^n. p power this which is p^n.

That is clear because this dimension is n, therefore K as a vector space of $\mathbb{Z}_p$ has dimension N, therefore K is isomorphic to Z Power N as a vector space, in particular the cardinalities are same.

So in particular this. Conversely, we have proved that given any power of a prime number, these are series with exactly p^n elements. All right. And that so the power finite fields have cardinality power of prime powers of prime numbers and conversely, given any prime power $q=p^n$, there exists a field F_q, they are denoted by, this is the field, finite field with q elements.

And you know, this finite field is nothing but the zero set of the polynomial $X^q - X$. And this polynomial have all the zero inside this field F_q. And also we have checked that any 2 fields of the same cardinality are isomorphic as big. In fact, they are isomorphic over the prime field. So this is a big discussion about the finite fields.

(Refer Slide Time: 4:18)



$\mathbb{F}_{q^n} / \mathbb{F}_q$ $\quad q =$ power of prime $\quad$ 2

field extn of degree n.

$\mathbb{F}_{q^n} \xrightarrow{\mathfrak{f}_q} \mathbb{F}_{q^n}$, $x \longmapsto x^q$

$\mathfrak{f}_q$ is $\mathbb{F}_q$-linear, ring homo.

$\mathfrak{f}_q \in Gal(\mathbb{F}_{q^n}/\mathbb{F}_q)$

$\{\mathfrak{f}_q^i \mid i=0,\dots,n-1\} \subseteq Gal(\mathbb{F}_{q^n}/\mathbb{F}_q)$

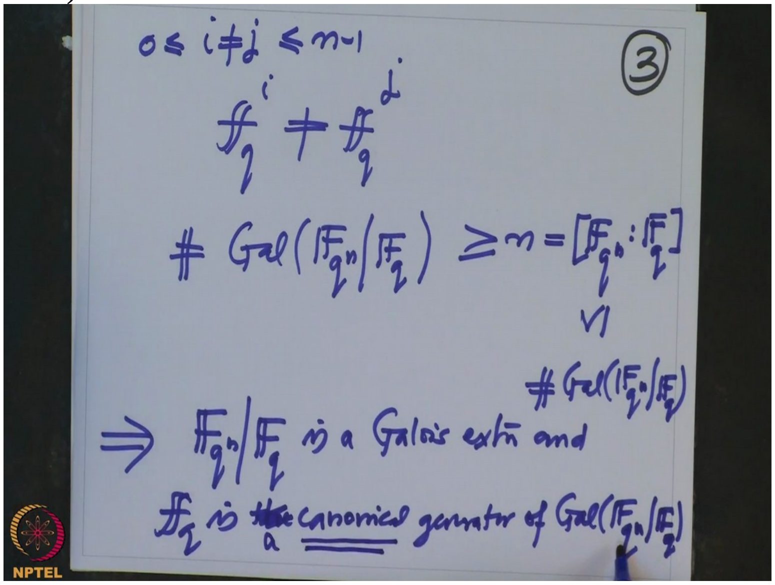
$\mathfrak{f}_q^i : x \longmapsto x^{q^i}$

And then now if I take a field extension, F_{q^n} over F_q. Now q is a power of prime, that q is a power of prime. So any field, any finite field extension of F_q has to be this because we know that any two fields with cardinality q^n, they are isomorphic. So anyway this is a finite this is a field extension of degree n. And first of all, note that I want to show that this extension is Galois extension first. So that is because look at this map from F_{q^n} to F_{q^n}, this automorphism is very important, it is denoted by f_q.

What is the map? This is x going to x^q . This is the map. So obviously this map f_q is F_q linear. It fixes elements of F_q because when you raise it to the power q , it becomes X. So it is F_q . So this is and it is clearly ring homomorpohism. In other words, I am saying that this F_q is indeed an element of the Galois group of F_{q^n} over F_q . And note that if I take the powers of F, the powers of this f_q , f_{q^i} and i is varying from 0 to $n-1$. These are the composites of the automorphisms of F_{q^n} over F_q .

So they are contained in obviously in this Galois group and they are clearly different. Different because what do the x? f_q where do x go under this? This go to x^{q^i} .

(Refer Slide Time: 7:27)



$0 \leq i \neq j \leq n-1$

3

$f_q^i \neq f_q^j$

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

$\mathbin{\rotatebox{90}{$\geq$}}$

$\# Gal(\mathbb{F}_{q^n}|\mathbb{F}_q)$

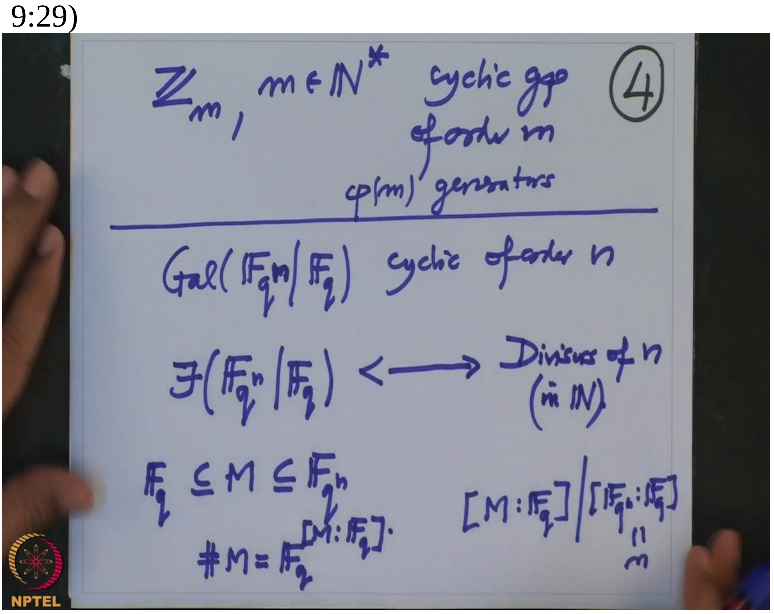
$\Rightarrow$ $\mathbb{F}_{q^n}|\mathbb{F}_q$ is a Galois extn and

f_q is ~~the~~ a $\underline{\underline{\text{canonical}}}$ generator of $Gal(\mathbb{F}_{q^n}|\mathbb{F}_q)$

So therefore, if I and they are different, not all elements, so therefore this shows that if i is different from j and in between 0 and $n-1$, then $f_q^i \neq f_q^j$. Just if they are equal, then for all x they will be equal. But then the polynomials of degree i and degree j, you work out that argument that shows the same. So that means this, the $Gal(F_{q^n}|F_q)$, this has at least, cardinality of this is at least n. But on the other hand, this n is nothing but the degree of F_{q^n} over F_q , the degree is precisely n.

But this is bounded by this, this bounds the cardinality of the Galois group. So that means equality happens. So that shows that this extension F_{q^n} over F_q , this is a Galois extension and this F_q is the canonical generator of this Galois group. I am not saying it is the only generator. It is a canonical of this. And what I just want to explain this word, why do I say canonical? So in particular, this group is cyclic. So therefore finite field extension, the Galois group is cycling. It is a Galois group extension with Galois group is cyclic. So before I go on, I want to explain this word about canonical.

(Refer Slide Time: 9:29)



4

$\mathbb{Z}_m$, $m \in \mathbb{N}^*$ cyclic grp of order m

$\varphi(m)$ generators

$\mathrm{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q)$ cyclic of order n

$\mathfrak{F}(\mathbb{F}_{q^n}|\mathbb{F}_q) \longleftrightarrow$ Divisors of n (in $\mathbb{N}$)

$\mathbb{F}_q \subseteq M \subseteq \mathbb{F}_{q^n}$

$\# M = \mathbb{F}_q^{[M:\mathbb{F}_q]}$.

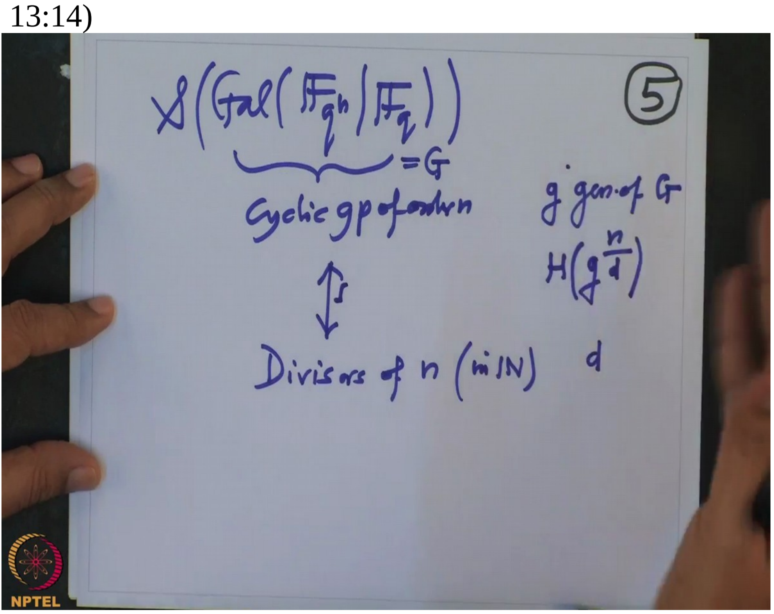
$[M:\mathbb{F}_q] \,|\, \underset{n}{\underset{\shortparallel}{[\mathbb{F}_{q^n}:\mathbb{F}_q]}}$

So look at the cyclic group. So $\mathbb{Z}_n$ where n is some nonzero natural number. We know this is a cyclic group. Cyclic group under addition of order n. This group has many generators and when we say that this cyclic group, these elements generate the cyclic group, that means we have a choice and the choice involves how many elements? We know, this group has cm generators. And we make the choice. But in that case of the Galois extension of the finite field, the choice is clear, the choice is canonical, that means the power map does not depend on the choice. So that is why it is called a canonical generator.

So this Galois group is cyclic of order mn. Now fundamental theorem says the subgroups of this group and intermediary field extension, so what are the intermediary field extensions? F_{q^n} over F_q . Their field sign here is F_{q^n} and this. So we know, this M is also finite field and therefore, M will have cardinality power of this q because cardinality of n will precisely be equal to Fq Power what? The dimension, the degree of M over F_q .

And this one is this one M over F_q divides F_{q^n} over F_q . This is n I know. So these are precisely the divisors of n. So if we have intermediary field then there is a divisor of, this corresponds to a divisor of n. Conversely, given any divisor of n, there is a unique field, unique finite field of the cardinality q^d . So therefore the intermediary fields, they correspond to precisely the divisors of n. When I say divisor, that means divisors of n (in $\mathbb{N}$). They precisely one-to-one correspondence, given any divisor, there is a finite field of that p^d element. And because they are unique it is a intermediary field. Conversely, given any intermediary field, there is a the degree of that field extension over the base field F_q , we will have divisor of M. So these are one-to-one correspondence with the divisors of F. Now what are the subgroups?

(Refer Slide Time: 13:14)



5

$$\mathcal{S}(\underbrace{\mathrm{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q)}_{=G})$$

Cyclic gp of order n

$\updownarrow$

Divisors of n (in $\mathbb{N}$)

g gen. of G

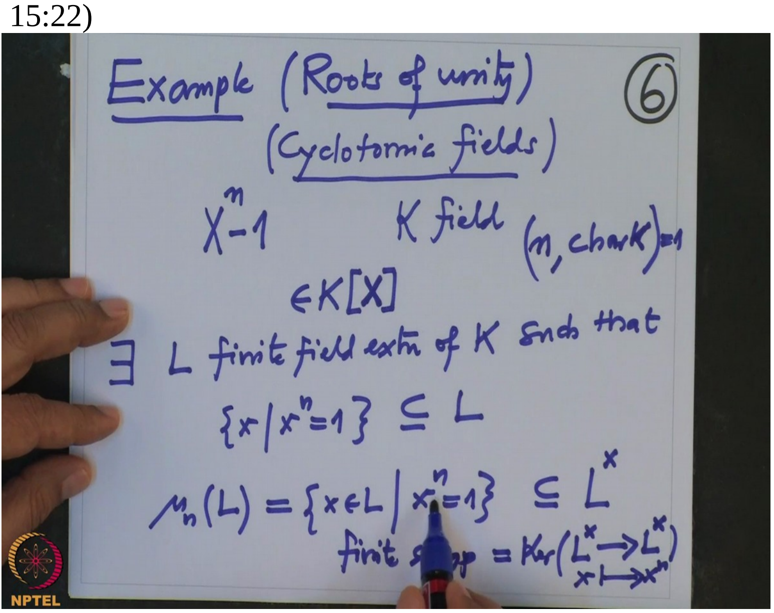
$H(g^{\frac{n}{d}})$

d

The subgroups of Galois group of F_{q^n} over F_q , so this is now subgroup. This is a cyclic group of order n and we know, given a cyclic group of order n order all the subgroups, given a divisor d, so they also corresponds to divisors of n. So when I say divisors of n, they are always in natural numbers. So how? Given any divisor d, I want a subgroup of order d. So what do we do? We take a generator x, generator G, G generator of the group. Let us call this group as G. Generator of G. Then you raise this $g^{\frac{n}{d}}$ and take the subgroup generated by that.

So this subgroup will have order d. So given a divisor, we have a subgroup of order d. Conversely, given a subgroup H of G, Lagrange theorem will tell you the order of H will divide the order of G. So that gives this by bijective correspondence. So therefore the Galois correspondence which gives the bijective map from the intermediary fields and the subgroups of the Galois group, this is so natural. They are only the divisors of the extension. So there is not much to study in this case but what is more important I will show you later in the later lectures. How to choose primitive elements? How to choose primitive elements for the intermediary fields? That was precisely done by the Gauss and that was known as Gauss periods. So how to compute them, that we will learn later.

(Refer Slide Time: 15:22)



Example (Roots of unity) ⑥

(Cyclotomic fields)

X^n-1 $\in K[X]$ K field $(n, \text{char} K)=1$

$\exists$ L finite field extn of K such that

$\{x \mid x^n=1\} \subseteq L$

$\mu_n(L) = \{x \in L \mid x^n=1\} \subseteq L^\times$

finite group $= \text{Ker}(L^\times \longrightarrow L^\times, x \longmapsto x^n)$

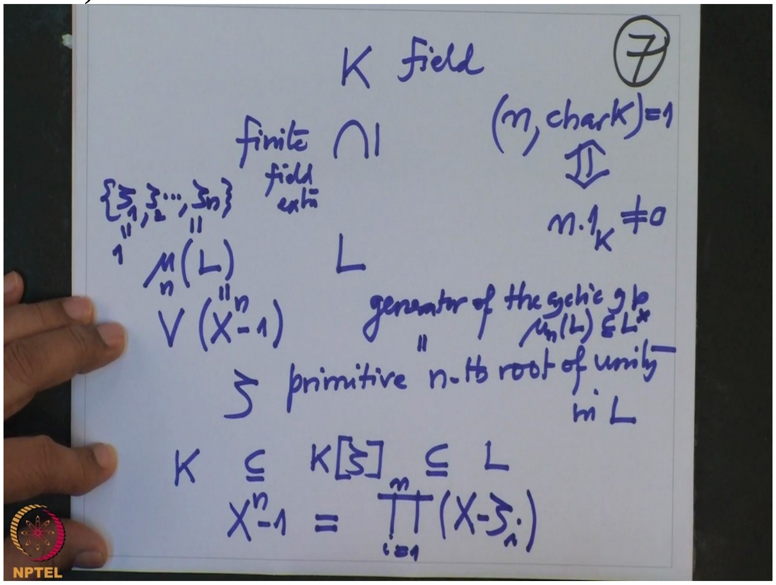
Now the 2nd example, very important again is about the roots of unity. Roots of unity. Now first of all, note that this also we have remarked earlier that these are also, this will lead to what is called cyclotormic fields. Okay what are these? So roots of unity means we are concerned with the polynomial X^n-1 . So if we have a field, so K is a field. And this polynomial we are considering as a polynomial in $K[X]$. And the zeroes of this polynomial, so I have used

Chronica's theorem to say that there exists a field L, finite field extension of K such that all the roots of this polynomial lie in L.

So that means all the elements X such that $X^n = 1$, these are contained in L. Note that because we are concerned with the roots of this polynomial, they are called the roots of unity because the power that is 1. And also I have noted earlier that to study these roots, we might have assumed that n and the characteristic of the field are co-prime. Because remember, roots of this polynomial are precisely what are called roots of unity and then that I have denoted by $\mu_n(L)$, this is all the roots $x \in L$ such that $x^n = 1$.

And this is clearly a subgroup of L^x. This is a finite subgroup of L^x. In fact, it is a kernel of L^x to L^x, this is a group homomorphism, x go to x^n. This is clearly a group homomorphism and it is a kernel of this. And therefore, it is a cyclic group. So the order of this group is not more than n. When it is exactly n, it is cyclic and the generators of this group are called primitive elements primitive roots of unity.

(Refer Slide Time: 19:17)

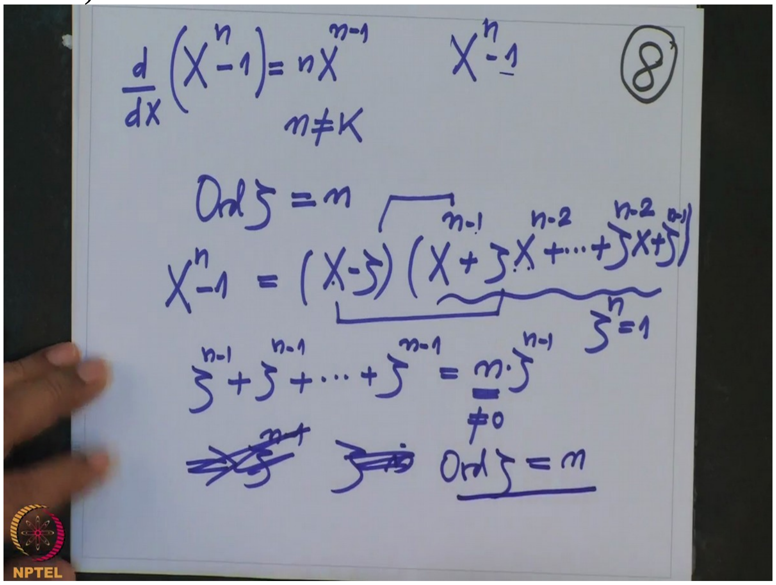

7
K field
finite ∩| field extn
L
$(n, \text{char} K) = 1$
⇕
$n \cdot 1_K \neq 0$
$\{\zeta_1, \zeta_2, \dots, \zeta_n\}$
$\zeta_1 = 1$
$\mu_n(L)$
$V(X^n - 1)$
generator of the cyclic gp $\mu_n(L) \subseteq L^x$
ζ primitive n-th root of unity in L
$K \subseteq K[\zeta] \subseteq L$
$X^n - 1 = \prod_{i=1}^{n} (X - \zeta_i)$
NPTEL

And now what we want to study? So we are assuming the characteristic of the base field. So this is upper base field L K the base field and we are assuming n and the characteristic of the base field is 1. That simply means, the GCD means n times 1_K is nonzero. So n is not a zero element of the field. That is what it means. And this field, we have enlarged to L. So that all, all my, all the roots, so $V(X^n-1)$, they are all, all are there. So this is $\mu_n(L)$ is precisely this. And we know that this is a finite extension.

So therefore, there is a root, I want to say that there is a ζ primitive n-th root of unity in L. okay. So that means K and L is here and in between, there is a subfield called generated by K and ζ , this is in between. So this ζ is a preventive root means, it is a generator of, this is a generator of the cyclic group $\mu_n(L)$ which is a subgroup of L cross. Now I want to show, once we know it is a generator, then all other elements are the powers of this ζ . So that means, this X^n-1 , this polynomial is a product of all the elements here. If μ this group if it is, this group has N elements, so these are $\zeta_1, \zeta_2, \ldots, \zeta_n$, these are all elements.

And this one is 1, one of them is 1 and the others are root. So they and they are all and I want to say they are distinct. So this is 1 to n, this. This is this product because this polynomial splits and why are they distinct?

(Refer Slide Time: 22:27)



$\frac{d}{dX}(X^n-1) = nX^{n-1}$ $\quad X^n-1$ $\quad \boxed{8}$

$n \neq K$

$\operatorname{Ord}\zeta = n$

$X^n-1 = (X-\zeta)(X^{n-1}+\zeta X^{n-2}+\cdots+\zeta^{n-2}X+\zeta^{n-1})$ $\quad \zeta^n = 1$

$\zeta^{n-1}+\zeta^{n-1}+\cdots+\zeta^{n-1} = n\cdot\zeta^{n-1}$

$\neq 0$

$\Rightarrow \zeta \ \operatorname{Ord}\zeta = n$

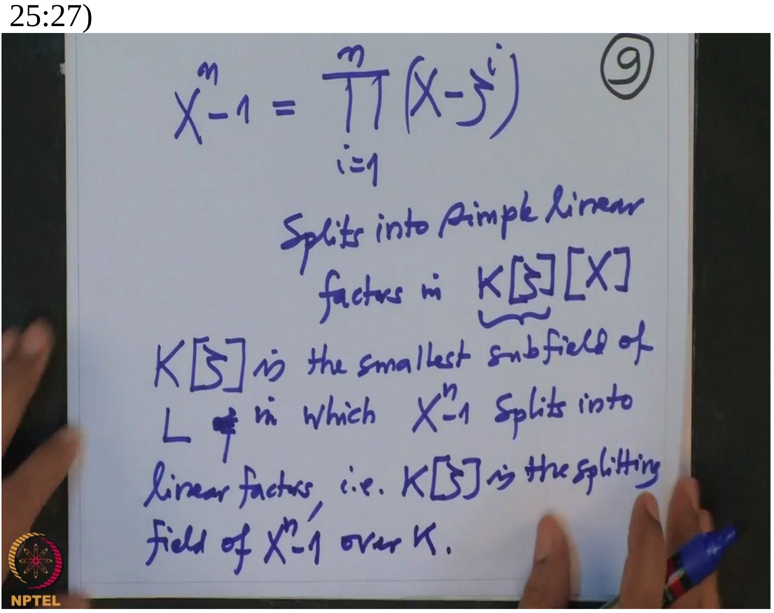
So to show that they are distinct, the derivative of this polynomial, the $\frac{d}{dX}$ of this polynomial has no common zero with X^n-1 . But what is $\frac{d}{dX}$ of all…In other words this polynomial and this polynomial, they are co-prime. So this is what? This is nX^{n-1} and n is nonzero in K.

And the roots only are 0. And they are not roots of this. So therefore none of the roots are common. So they are distinct. And not only that, directly from here also, we will see that the order of the element ζ equal to n. That is because you see it is you look at this $X^n - 1$, this will this is $X - \zeta$ is one of the roots, so it will come out as a factor and what is the remaining factor?

$X^{n-1} + \zeta X^{n-2} + \ldots + \zeta^{n-1}$. This is clearly, this product is clearly equal to this because X times this is X^n, this one $-\zeta$ times power $n-1$, this is going to get canceled with this term. This term will get cancelled with this term and so on. Successive terms will get canceled and only the last one will remain, ζ times this ζ^{n-1} which is ζ^n which is 1 because it is a root of $X^n - 1$. So we have this. So when I look at when I put X equal to ζ in this, what do I get? I have to show that this is nonzero because this is a simple route. That means when I have to put X equal to ζ in this expression, it should become nonzero.

But what is that? That is $\zeta^{n-1} + \zeta \zeta^{n-2}$, that is ζ^{n-1} etc etc ζ^{n-1} , this is nothing but n times ζ^{n-1} . n is nonzero in the field K. Therefore this is, if this, after putting X equal to ζ , if it were zero, then ζ^{n-1} will be nonzero. So this implies ζ^{n-1} . So that implies ζ is a simple root. So order of ζ equal to n. This is a simple root. All right.

(Refer Slide Time: 25:27)



9

$$X^n - 1 = \prod_{i=1}^{n} (X - \zeta^i)$$

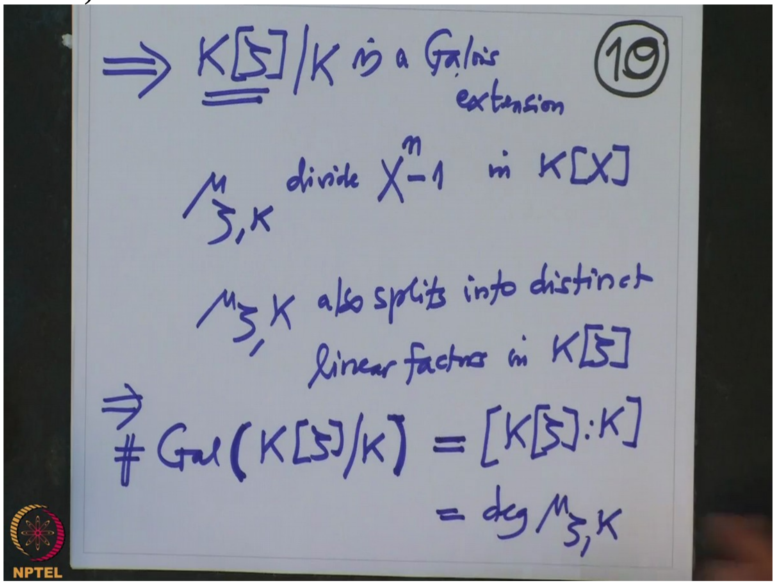
Splits into simple linear factors in $K\underbrace{[\zeta]}[X]$

$K[\zeta]$ is the smallest subfield of L in which $X^n - 1$ splits into linear factors, i.e. $K[\zeta]$ is the splitting field of $X^n - 1$ over K.

Actually, therefore this polynomial $X^n - 1$, this is product $X - \zeta^i$, i is from 1 to n. So this is a degree n polynomial. I know all these are the roots because each root of unity is a power of ζ . So therefore, this polynomial actually splits into simple linear factors in the field in the polynomial range over this field. All of them are here and all of them are different from therefore, over this field this polynomial splits into linear factors. So therefore, this $K[\zeta]$ is the smallest subfield of that L of which is which is an extension of K which in which $X^n - 1$ splits into linear factors.

So this is also called, that means, let me use the word, that means $K[\zeta]$ is the splitting field of $X^n - 1$ over K. And now what do want to prove?

(Refer Slide Time: 27:36)



$\Rightarrow \underline{\underline{K[\zeta]/K}}$ is a Galois extension

10

$\mu_{\zeta,K}$ divide $X^n - 1$ in $K[X]$

$\mu_{\zeta,K}$ also splits into distinct linear factors in $K[\zeta]$

$\Rightarrow \# \mathrm{Gal}(K[\zeta]/K) = [K[\zeta]:K]$

$= \deg \mu_{\zeta,K}$

So therefore $K[\zeta]$ over K is a Galois extension. Okay. So to check somebody the Galois extension, what do we want to do? This is already a simple extension. And if we want to check it is a Galois extension, I only have to check that the minimal polynomial of ζ splits into linear factors over K. So what is the minimal polynomial of ζ ? In any case, minimal polynomial of ζ is the smallest degree polynomial where ζ is the root but one polynomial I know definitely this polynomial, this is also polynomial in $K[X]$ and this polynomial also has ζ as a root.

So therefore this minimal polynomial has to divide this in $K[X]$. So it divides in $K[X]$. But we have noted that these polynomial factors into simple linear factors over this field. Therefore, all the roots of this pronominal lie here and they are simple and this one therefore, therefore so is true for minimal polynomial also. so minimal for nominal of ζ over K also splits into distinct linear factors in $K[\zeta]$. Therefore this extension is Galois because one of the immediately when we defined our Galois extension, we checked that how can a simple extension be Galois.

That is when you only have to look at the minimal for nominal and the minimal polynomial should split into distinct linear factors over that field. So which is 2 in this case. Therefore it is a Galois extension. So the next question therefore is what is the Galois group? So what is $Gal(K[\zeta]|K)$? And we don't know yet, what is exactly the degree? We only know, this is the Galois extension. We don't know this is, this should be…we know that this order of this Galois group equal to the degree of $K[\zeta]$ over K, this we know because the field extension is Galois and this degree of this simple linear extension is nothing but the degree of the minimal polynomial of ζ over K.

But we don't know what is the minimal polynomial. So we want to know what is the minimal polynomial and that we will do it next time and that will also illustrate what is the Galois correspondence in this case. Now what is the Galois group precisely? What is this group? Like in the case of finite field extension, we proved that Galois group is actually cyclic. In this case, what is exactly the Galois group? It may not be cyclic in this case but we will prove it is an Abelian group and we will also calculate its order. Okay. . we will continue in the next lecture about the analysis of the Galois group, its order and the structure. Thank you.