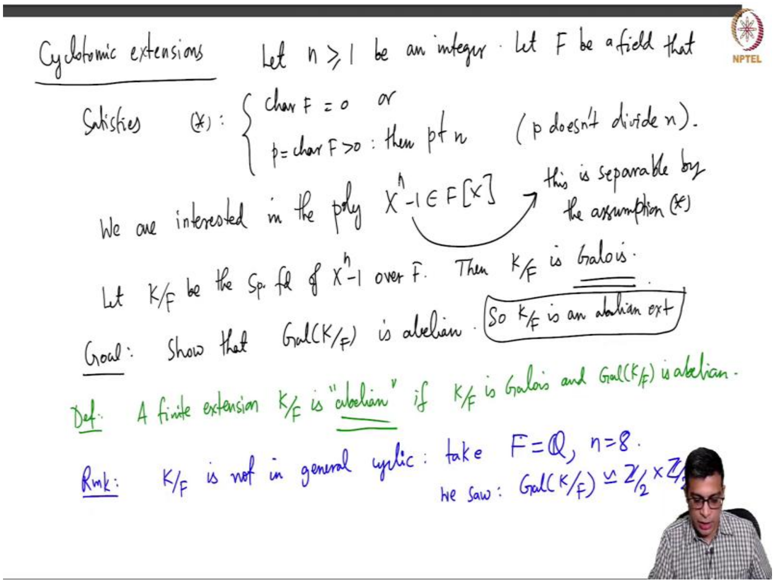
Introduction to Galois Theory
Professor Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute
Lecture 35
Cyclotomic extensions- Part 1

(Refer Slide Time: 00:16)



Cyclotomic extensions Let $n \geq 1$ be an integer. Let F be a field that

Satisfies $(*)$: $\begin{cases} \text{char } F = 0 \text{ or} \\ p = \text{char } F > 0 : \text{then } p \nmid n \end{cases}$ (p doesn't divide n).

We are interested in the poly $X^n - 1 \in F[X]$ → this is separable by the assumption $(*)$

Let K/F be the Sp. fd of $X^n - 1$ over F. Then K/F is Galois.

Goal: Show that $Gal(K/F)$ is abelian. $\boxed{\text{So } K/F \text{ is an abelian ext}}$

Def: A finite extension K/F is "abelian" if K/F is Galois and $Gal(K/F)$ is abelian.

Rmk: K/F is not in general cyclic: take $F = \mathbb{Q}$, $n = 8$.
We saw: $Gal(K/F) \simeq \mathbb{Z}/2 \times \mathbb{Z}/$

Welcome back. In the last few classes we looked at Kummer Extensions and I also in the last class indicated how Kummer Extensions are going to be useful to us, because they are quite close to being radical extensions which is of interest was later on. So, except that there is one assumption that you have to make that the field contains a primitive nth root of unity. So, to resolve that wrinkle, we have to learn about Cyclotomic Extensions. So, this is going to be the topic for next one or two videos now.

Cyclotomic extension, in this part, we are going to formally define what primitive nth roots of unity are and also prove some facts about them. So, as before, we are going to fix a positive integer and we are going to assume that F is a field satisfying our standing assumption. Let F be a field that satisfies this condition star, which is that characteristic of F is 0, or if characteristic of F is positive, then P does not divide n. So, P does not divide n.

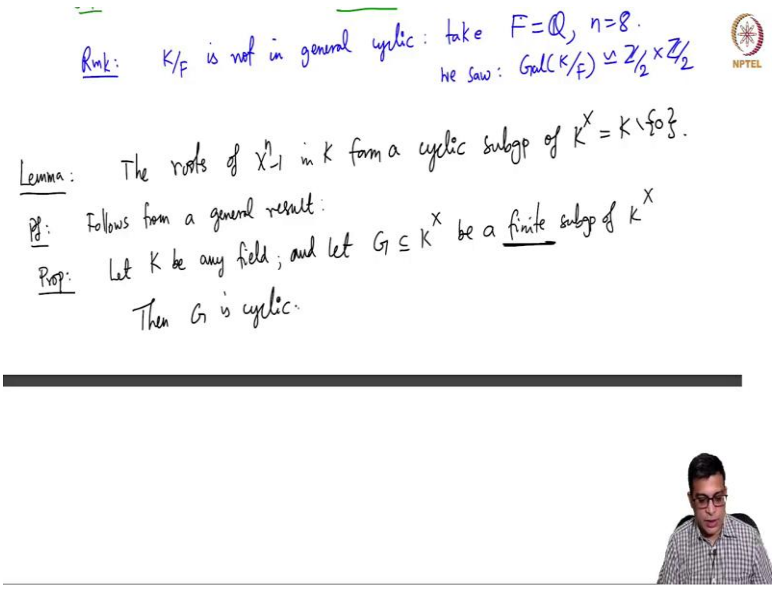
So, this is a standard assumption. So, in this case, we are going to be interested in, we are interested in the polynomial. So, by assumption, this is separable, meaning that this polynomial and its derivative have no common roots. So, this is an assumption ‘star’. So, let K be the splitting field, then K over F is Galois. So, our goal is to understand a little bit about what kind of Galois group it can have, it can very well be non-cyclic, but we will show that it has to be abelian always.

So, first goal, I mean, one goal is that show that it is abelian. So, this is a definition for you, a finite extension K over F is abelian if K over F is Galois and the Galois group is abelian. One of the achievements of Galois Theory is to connect field theory to group theory. So, any adjectives that you have in groups can be now applied to field extensions, because Galois groups of those field extensions are groups.

So, cyclic extension is an extension which is Galois to begin with, because of the association between groups and fields, field extensions works best when you have a Galois extension. So, Galois extension is cyclic, if it is Galois, of course, but the Galois group is cyclic. If the Galois group is abelian besides it is an abelian extension. So, in other words, K over F is an abelian extension with this definition, and we remarked that K over F is not in general cyclic, take K F to be Q and n to be 8.

So, we saw earlier that Galois group of K, which is splitting field of this is Z naught 2 cross Z naught 2. So, in general, it is not a cyclic extension like a Kummer extension, but nevertheless, it is an abelian extension. So, remember that K over F is a radical extension because you are attaching an nth root, in this case, nth root of 1. So, the goal is to prove this.

(Refer Slide Time: 05:10)



Rmk: K/F is not in general cyclic: take $F=\mathbb{Q}$, $n=8$.
We saw: $Gal(K/F) \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$

Lemma: The roots of X^n-1 in K form a cyclic subgp of $K^\times = K \setminus \{0\}$.

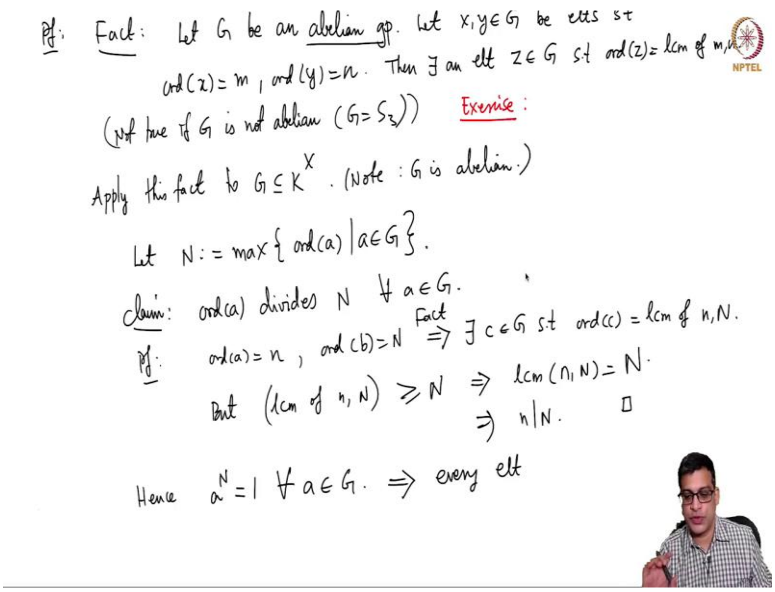
Pf: Follows from a general result:

Prop: Let K be any field; and let $G \subseteq K^\times$ be a finite subgp of $K^\times$
Then G is cyclic.

But before that let me prove a nice result which is sort of important in field theory and which I have implicitly used several times before. So, K and F are as before, so F is a field which has this property ‘star’, K is the splitting field of the polynomial X power n minus 1. The roots of X power n minus 1 in K, form a cyclic subgroup of the multiplicative group.

So, this proof in fact follows from the general result, which I will write now. Let K be any field. So, just for the purpose of this proposition forget the entire picture. So, here K is any field, and let G be a finite subgroup, multiplicative subgroup of course, of K star, the nonzero elements of K. This is under multiplication, finite is important, then G cyclic.

(Refer Slide Time: 06:41)



Pf: Fact: Let G be an abelian gp. Let $x, y \in G$ be elts s.t $\text{ord}(x) = m$, $\text{ord}(y) = n$. Then $\exists$ an elt $z \in G$ s.t $\text{ord}(z) = \text{lcm of } m, n$.

(Not true if G is not abelian $(G = S_3)$) Exercise:

Apply this fact to $G \subseteq K^{\times}$. (Note: G is abelian.)

Let $N := \max\{\text{ord}(a) \mid a \in G\}$.

Claim: $\text{ord}(a)$ divides N $\forall a \in G$.

Pf: $\text{ord}(a) = n$, $\text{ord}(b) = N$ $\overset{\text{Fact}}{\Rightarrow}$ $\exists c \in G$ s.t $\text{ord}(c) = \text{lcm of } n, N$.

But $(\text{lcm of } n, N) \geq N \Rightarrow \text{lcm}(n, N) = N$.

$\Rightarrow n \mid N$. □

Hence $a^N = 1$ $\forall a \in G$. $\Rightarrow$ every elt

So, this is the fundamental result in field theory and it has several proofs, I will give you one proof modular one fact, which maybe I can do in a problem session later. So, let G be an abelian group, let us take two elements in G such that order of x is m, and order of y is n. So, this is a purely group-theoretic statement. So, you have an element of order m, an element of order n. Then there exists an element z in G such that order of z is the LCM of m, n.

So, this is true for an abelian group, not true if G is not abelian. For example, S3, S3 has an order 2 element as well as an order 3 element but LCM of 2 and 3 is 6. But S3 of course cannot contain an order 6 element, because it is not cyclic. So, this is a general fact and I will leave this as an exercise and we will do this later if we have time.

Let us use this theorem. Certainly, so coming back to the proof of our proposition, apply this fact, it is a fairly easy fact to prove, just straightforward, apply this factor to G in K. Note that G is abelian. Because a field of course, multiplication in a field is abelian.

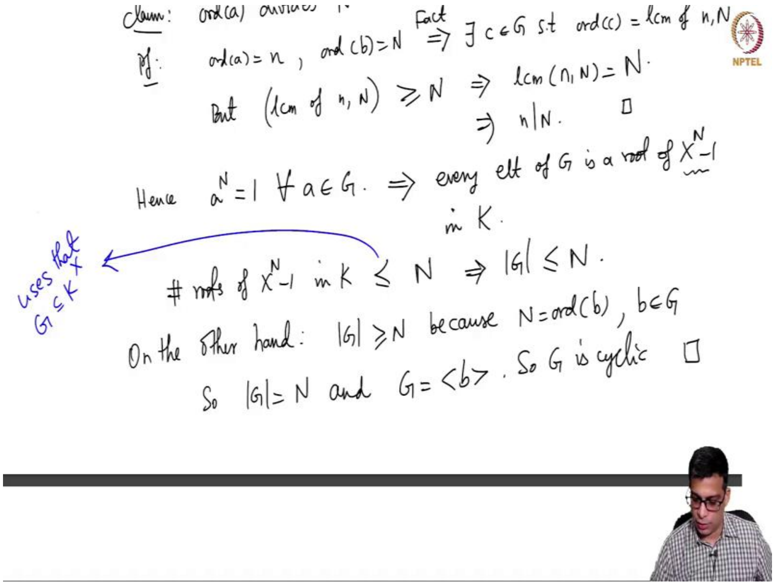
Now, let us take N to be max orders of elements of G. Remember, G is a finite group by hypothesis. So, you list all the elements look at their orders, that is a collection of positive integers you take n. So, claim is that G is in fact of order n. So, we will prove this in the following way.

So, let us take, so claim in fact is order of a divides N for all a in G. So, the proof of this claim is follows. So, let us say order of a is small n, and order of b is capital N, because capital N is order of some element there is a b such that order of b is capital N. So, then by the fact there exists c in G such that order of c is LCM of n, and N. But then LCM of n, and N is greater than or equal to N. Because LCM is the least common multiple, so it a multiple of capital N. So, hence it is greater than or equal to n.

But capital N is the maximum order. So, LCM of n, and N is N. But that is to say that n divides N, because small n divides its LCM which is capital N. So, small n divides capital N. Hence the claim is proved. Hence a power N is 1 for all a in G, because order of a divides n, so a power N is 1 for all a in G. That means, every element now we are going to bring in the field. So far it is a group, of course not every group is cyclic. So, we have to use the fact that this group sits inside a field somehow.

So, every element of G is a root of X power n minus 1. But the number of roots of X power n minus 1 in K is greater than equal to N, or less than or equal to N. So, a polynomial of degree N cannot have more than N roots. So, this implies the order of G is less than or equal to N because every element of G is a root. So, the set of roots has cardinality less than or equal to N means, order of G is less than or equal to N.

(Refer Slide Time: 11:13)



Claim: ord(a) divides N

Pf: ord(a) = n , ord(b) = N $\overset{\text{Fact}}{\Rightarrow}$ $\exists\, c \in G$ s.t ord(c) = lcm of n, N

But (lcm of n, N) $\geq N$ $\Rightarrow$ lcm(n, N) = N.

$\Rightarrow n \mid N$. □

Hence $a^N = 1$ $\forall a \in G$. $\Rightarrow$ every elt of G is a root of $X^N - 1$ in K.

roots of $X^N - 1$ in K $\leq N$ $\Rightarrow |G| \leq N$.

uses that $G \subseteq K^\times$

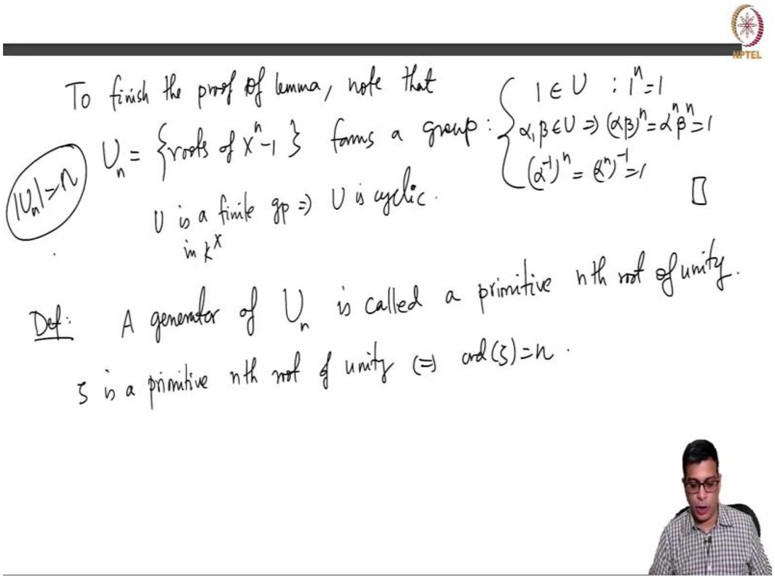
On the other hand: $|G| \geq N$ because $N = \text{ord}(b)$, $b \in G$

So $|G| = N$ and $G = \langle b \rangle$. So G is cyclic □

On the other hand, order of G must be greater than N, because N is an order of an element in G, the order of the group is always at least order of any given element in this. So, order of the group is at least N, so that means order of group is equal to N and G is equal to b. So, G cyclic.

So, we have proved this general fact that a finite subgroup of the multiplicative group of any field is cyclic. So, in particular, the roots of this polynomial form a cyclic group, so I will tell you in a minute why it is a group, to begin with. So as I said, this fact here uses the fact that because the roots in a field are at most the degree not in general.

(Refer Slide Time: 12:23)



To finish the proof of lemma, note that

$U_n = \{\text{roots of } X^n - 1\}$ forms a group: $\begin{cases} 1 \in U : 1^n = 1 \\ \alpha, \beta \in U \Rightarrow (\alpha\beta)^n = \alpha^n \beta^n = 1 \\ (\alpha^{-1})^n = (\alpha^n)^{-1} = 1 \end{cases}$ □

$|U_n| = n$

U is a finite gp in $K^\times$ $\Rightarrow$ U is cyclic.

<u>Def</u>: A generator of U_n is called a primitive nth root of unity.

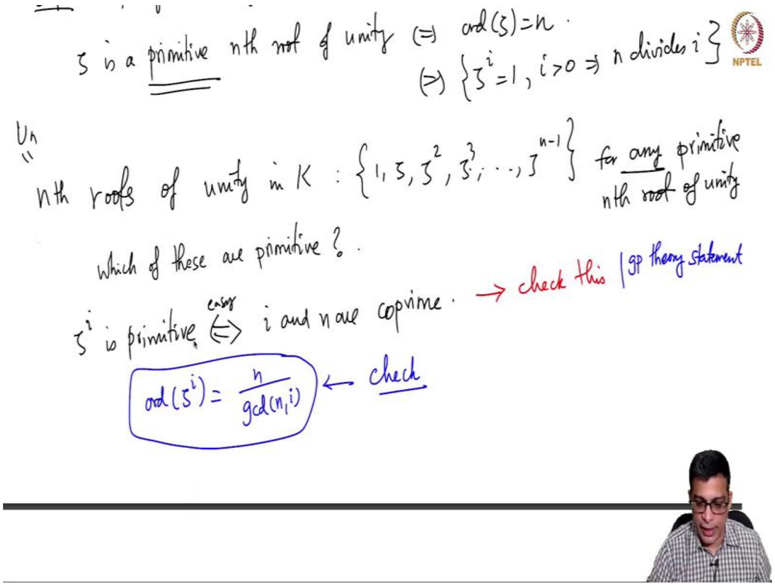
ζ is a primitive nth root of unity $\Leftrightarrow$ $\mathrm{ord}(\zeta) = n$.

So, now to finish the proof of the lemma, note that roots of X power n minus 1 forms a group. This is trivial because 1 is there, so U, 1 is in U because 1 power n is 1. And if alpha and beta are in U, that means alpha in U plus alpha n, so it is a group, it is a finite group implies U in K cross, implies U is cyclic. So, this completes the proof of the lemma which says that the roots of X power n minus 1 in K for the cyclic group of K star.

So, now definition; A generator of U is called, so Un, if you wish, is called a primitive nth root of unity. This is equivalent to, so zeta is a primitive nth root of unity if and only if order of zeta is n because order of Un is n, right, because it is a separable polynomial there are exactly n roots of unity in K, out of which a primitive root will have order n. So, that means zeta i equal to 1 and i positive implies n divides i.

So, this is the condition that we mentioned in the class when we talked about Kummer extensions. So, this is about primitive nth roots. So, I just wanted to do this in detail, so that you are comfortable with the notion of roots of primitive roots of unity.

(Refer Slide Time: 15:04)



ζ is a primitive nth root of unity $\iff \mathrm{ord}(\zeta) = n$.

$\iff \{\zeta^i = 1,\ i > 0 \implies n \text{ divides } i\}$

U_n "

nth roots of unity in K : $\{1, \zeta, \zeta^2, \zeta^3, \ldots, \zeta^{n-1}\}$ for any primitive nth root of unity

Which of these are primitive?

ζ^i is primitive $\overset{\text{easy}}{\iff}$ i and n are coprime. → check this | gp theory statement

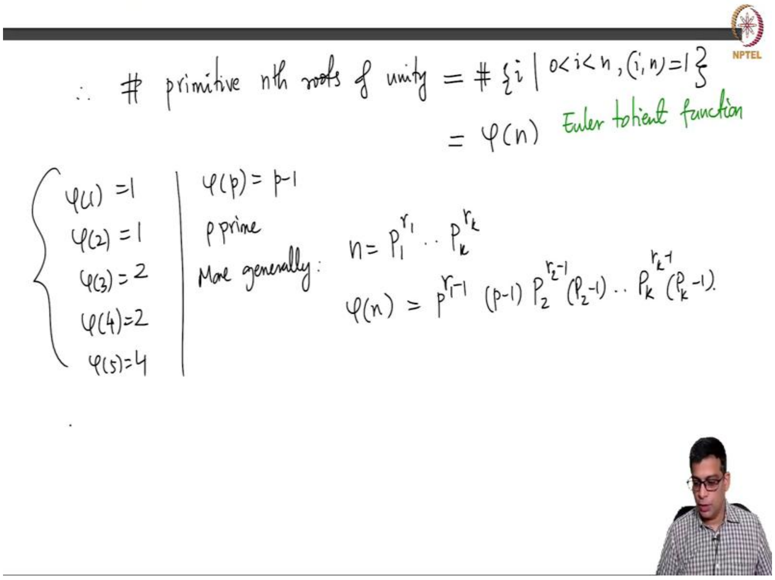
$\boxed{\mathrm{ord}(\zeta^i) = \frac{n}{\gcd(n,i)}}$ ← check

So, now, let us continue. So, nth roots of unity in K, which I called Un if you wish, are 1 zeta, zeta square, zeta cubed, zeta n minus 1 for any primitive nth root. So, once you get hold of a primitive nth root, its powers will give you all the nth roots. But which of these are primitive? So, take a zeta i, when is this primitive? Any nth root of unity is of the form zeta i, when is this primitive? Of course, it is primitive when i is equal to 1, because that is zeta, it is not primitive and i equal to 0. What about zeta square? So, now, this depends on the order n and how i is related to n. This is an easy statement.

So, this is an important fact, check this, this is easy as I said, because this is a group theory statement really, this is a group theory statement because you have a cyclic group generated by zeta. If zeta square generates it, that means zeta square, zeta power 4, zeta power 6, and so on, also generate it. That means 2 and n have to be co-prime. This uses the fact that, order of zeta i is, so maybe I do not remember the exact statement to write here, but order of zeta square will be less than n if and only if 2 and n have a common factor.

So, I think I will attempt to do this, order of zeta i will be n divided by LCM of or GCD of n and i, so I think this is the correct statement. If the GCD is 1 then order is 1, order is n divided by 1 which is n, otherwise it will be strictly less than n. So check this. This is just a simple calculation, because zeta i power this will be 1 because it will be n times something and zeta i power anything less will not be 1.

(Refer Slide Time: 18:12)



$\therefore$ # primitive nth roots of unity $= \# \{ i \mid 0 < i < n, (i,n)=1 \}$

$= \varphi(n)$ Euler totient function

$\varphi(1)=1$

$\varphi(2)=1$

$\varphi(3)=2$

$\varphi(4)=2$

$\varphi(5)=4$

$\varphi(p)=p-1$

p prime

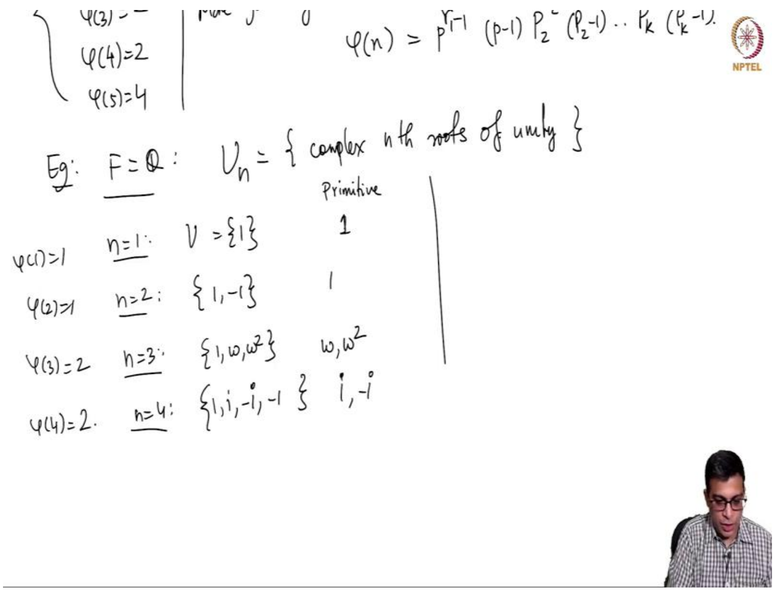
More generally: $n = p_1^{r_1} \cdot\cdot p_k^{r_k}$

$\varphi(n) = p^{r_1-1}(p-1)\, p_2^{r_2-1}(p_2-1) \cdot\cdot p_k^{r_k-1}(p_k-1).$

So, that means, the number of primitive nth roots of unity is equal to a member of i, such that i is positive and less than n and i and n are co-prime. So, these are number of positive integers less than n that are co-prime to n. This is called, usually denoted by phi n, this name is Euler totient function. So, this is easy, so this, for example, phi of 1 is 1, phi of 2 is 1, phi of 3 is 1, 2 or co-prime, so both of them, so phi of 3 is 2, phi of 4 is also 2 because 1 and 3, phi of 5 is 4 and so on.

So, in general, phi of a prime number is p minus 1, because every integer less than p minus 1 will be co-prime to P. So, more generally, so if n is an integer which has this prime decomposition, p power r1. We will not need this; I am just writing this because this is something that you might find useful sometimes. So, I do not need brackets here. So, I am going to use the fact that number of roots of unity is phi n, the formula for phi n is not relevant for us. So, just before I state the main theorem that I want to do in this class, let me just give you some examples.

(Refer Slide Time: 20:14)



$\varphi(3) = $

$\varphi(4)=2$

$\varphi(5)=4$

$\varphi(n) = p^{r_1-1}(p-1)\, p_2^{\,r_2-1}(p_2-1) \cdots p_k^{\,r_k-1}(p_k-1).$

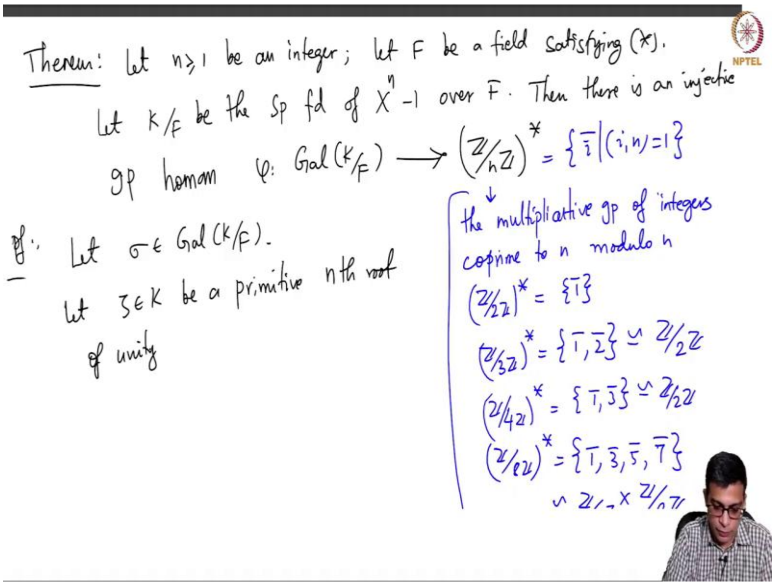
Eg: $\underline{F = \mathbb{Q}}$: $U_n = \{$ complex nth roots of unity $\}$

			Primitive
$\varphi(1)=1$	$\underline{n=1}$:	$U = \{1\}$	1
$\varphi(2)=1$	$\underline{n=2}$:	$\{1,-1\}$	1
$\varphi(3)=2$	$\underline{n=3}$:	$\{1,\omega,\omega^2\}$	ω,ω^2
$\varphi(4)=2$.	$\underline{n=4}$:	$\{1,i,-i,-1\}$	$i,-i$

So, let us take F to be Q for simplicity, what are primitives? So, let us denote Un by a set of roots of unity, complex nth roots of unity. So, for n equal to 1, Un is of course 1 and primitive are 1, primitive I will write here. For n equal to 2, U 2 is 1 minus 1, and primitive is just 1. n equal to 3, you have 1 omega, omega square, and primitive are omega and omega square. For n equal to 4, you have 1, i, minus i, minus 1, primitive are just i and minus i, and so on.

And this, remember, phi of 1 is 1, phi of 2 is 1, phi of 3 is 2 confirmed by two of them, phi of 4 is 2 confirmed by this. And similarly, you have four primitive 5th roots of unity. So, this is just to give you a basic idea of what primitive roots of unity are. And the key observation I want to emphasize again is that primitive nth roots are, you fix a primitive nth root zeta, other primitive nth roots will be zeta power i, where i and n are co-prime. Now, using that I want to prove the standard theorem here.

(Refer Slide Time: 21:58)



Therem: Let $n \geq 1$ be an integer; let F be a field satisfying $(*)$.

Let K/F be the sp fd of $X^n - 1$ over F. Then there is an injectie gp homom $\varphi: Gal(K/F) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^* = \{\bar{i} \mid (i,n) = 1\}$

Pf: Let $\sigma \in Gal(K/F)$.

Let $\zeta \in K$ be a primitive nth root of unity

the multiplicative gp of integers coprime to n modulo n

$(\mathbb{Z}/2\mathbb{Z})^* = \{\bar{1}\}$

$(\mathbb{Z}/3\mathbb{Z})^* = \{\bar{1}, \bar{2}\} \cong \mathbb{Z}/2\mathbb{Z}$

$(\mathbb{Z}/4\mathbb{Z})^* = \{\bar{1}, \bar{3}\} \cong \mathbb{Z}/2\mathbb{Z}$

$(\mathbb{Z}/8\mathbb{Z})^* = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$

$\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

So, remember our setup. F is any field. So, maybe our theorem I will write down because that is a good way to capture all the notation. So, let n be a positive integer, let F be a field satisfying ‘star’, meaning it is either characteristic is 0, or its characteristic is positive, but does not divide n. Let K be the splitting field of X power n minus 1 over F. Then, there is a group homomorphism phi from Galois group of K over F to Z mod n Z star.

So, recall that Z mod n Z star is the multiplicative group of integers co-prime to n modulo n. So, that is not, I mean, it is statement is not compactly written, but you take Z mod n Z and look at all the units in that group in that ring. So, units, multiplicative units in that ring. So, those which admit inverses, so this is i bar where i and n are co-prime. And that is a group under multiplication.

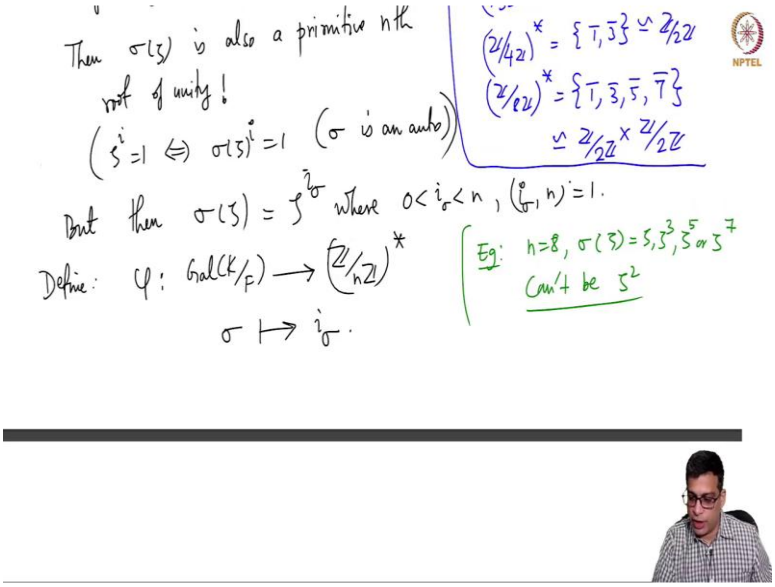
So, because 1 is there, and if you multiply two units you get another unit, inverse of a unit is a unit and so on. So, Z mod 2 Z star is just 1, Z mod 3 Z star is 1 bar 2 bar, that is cyclic and is isomorphic to Z mod 2 Z, Z mod 4 Z star is 1 bar 3 bar, and this is isomorphic to Z mod 2 Z also, but Z mod 8 Z star, so I do not have to spend too much time but you can see that this is 1 bar, 2 is not co-prime to 8, 3 is co-prime to 8, 4 is not 5 is, 6 is not 7 is, and this you can check.

There is a group of order 4, but 3 squared is 1 because 3 squared is 9, which is 1 mod 8, 5 squared is 1 mod 8, 7 squared is 1 mod 8. So, this is Z mod 2 Z. Now, let us come back to the proof statement. So, there is an injective group homomorphism, I forgot a key word here, injective group homomorphism from Galois group to Z mod n Z star. I think that is all. So, let us prove this.

So, let sigma be in the Galois group, the proof is fairly straightforward, it is somewhat like the theorems we proved on Kummer Extensions. So, let zeta be a primitive nth root of unity in K, K is a splitting field of X power n minus 1. We have so far proved in this class that those roots form a cyclic group of all the roots of X power n minus 1. By the way, X power n minus 1 is a special polynomial which has this property.

Almost never again you will see that roots of a polynomial form a group, it is very special to this particular polynomial, X power n minus 1. So, X power n minus 1 roots of that form a group which is a cyclic group any generator is called a primitive nth root of unity, let us take one of them. What happens to zeta under sigma? Then I claim is also a primitive nth root of unity.

(Refer Slide Time: 00:16)



Then $\sigma(\zeta)$ is also a primitive nth root of unity!

$\left(\zeta^i = 1 \Leftrightarrow \sigma(\zeta)^i = 1 \quad (\sigma \text{ is an auto})\right)$

But then $\sigma(\zeta) = \zeta^{i_\sigma}$ where $0 < i_\sigma < n$, $(i_\sigma, n) = 1$.

Define: $\varphi : Gal(K/F) \longrightarrow \left(\mathbb{Z}/n\mathbb{Z}\right)^*$

$\sigma \mapsto i_\sigma$.

$\left(\mathbb{Z}/4\mathbb{Z}\right)^* = \{\bar{1}, \bar{3}\} \simeq \mathbb{Z}/2\mathbb{Z}$

$\left(\mathbb{Z}/8\mathbb{Z}\right)^* = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$

$\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Eg: $n=8$, $\sigma(\zeta) = \zeta, \zeta^3, \zeta^5$ or ζ^7

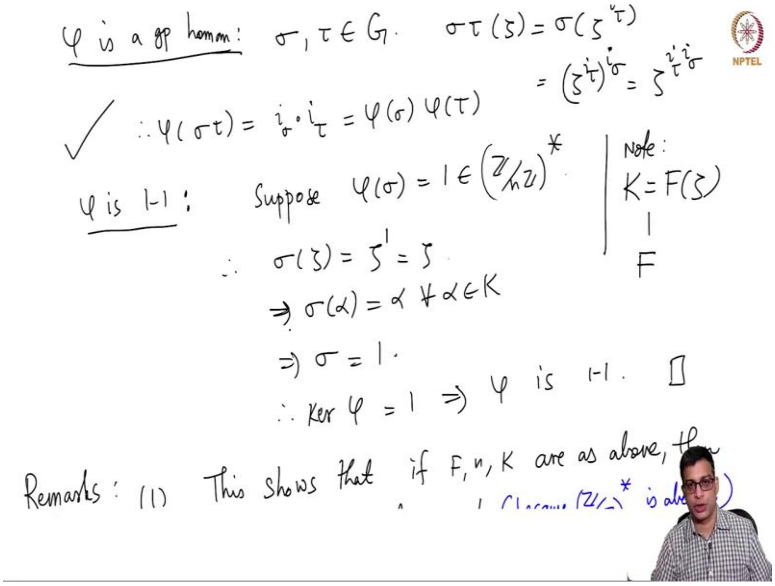
Can't be ζ^2

Why is this? That is because, note that if you have zeta i equal to 1, this implies sigma of zeta power i is also 1. Similarly, sigma of zeta is 1 implies zeta is 1 because sigma is an automorphism. That means it is an isomorphism of K star 2 K star. So, this implies that the least integer such that sigma zeta power that is 1, is the same whatever is the least integer for zeta which is n.

So, sigma zeta is also a primitive nth root of unity. But then by the analysis that we did earlier, sigma zeta must be sigma zeta power i sigma, where i sigma is a positive integer which is co-prime to n. So, sigma zeta must be a primitive nth root of unity, that means it must be a power which is co-prime to n. So, as an example, let us say n equal to 8, then sigma zeta must be either zeta or zeta cube or zeta 4 or zeta 5 or zeta 7, it cannot be zeta square, for example.

Because zeta square is not a primitive nth root of unity because zeta square power 4 is identity. So, sigma zeta cannot be this. So, now we have our map, so define phi from Galois group to Z mod n Z star simply send sigma to phi sigma. Because of what I noted here, i sigma is co-prime to n, so it belongs to this. So, in the case of 8, it would may up to Z mod n Z star.

(Refer Slide Time: 28:41)



φ is a gp homm: $\sigma, \tau \in G$. $\sigma\tau(\zeta) = \sigma(\zeta^{i_\tau}) = (\zeta^{i_\tau})^{i_\sigma} = \zeta^{i_\tau i_\sigma}$

✓ $\therefore \varphi(\sigma\tau) = i_\sigma \cdot i_\tau = \varphi(\sigma)\varphi(\tau)$

φ is 1-1: Suppose $\varphi(\sigma) = 1 \in (\mathbb{Z}/n\mathbb{Z})^*$.

$\therefore \sigma(\zeta) = \zeta^1 = \zeta$.

$\Rightarrow \sigma(\alpha) = \alpha \ \forall \alpha \in K$

$\Rightarrow \sigma = 1$.

$\therefore \operatorname{Ker} \varphi = 1 \Rightarrow \varphi$ is 1-1. □

Note:

$$\begin{tikzcd} K = F(\zeta) \arrow[d, dash] \\ F \end{tikzcd}$$

Remarks: (1) This shows that if F, n, K are as above, th

(because $(\mathbb{Z}/n)^*$ is ab

So, claim is that sigma phi is a phi is an injective group homomorphism but first, why is it a homomorphism? It is a group homomorphism, so why is it a group homomorphism? It is a group homomorphism because if sigma and tau are in G, this is very similar to what we did in the Kummer extensions, there we used additive and here we use multiplicative notation.

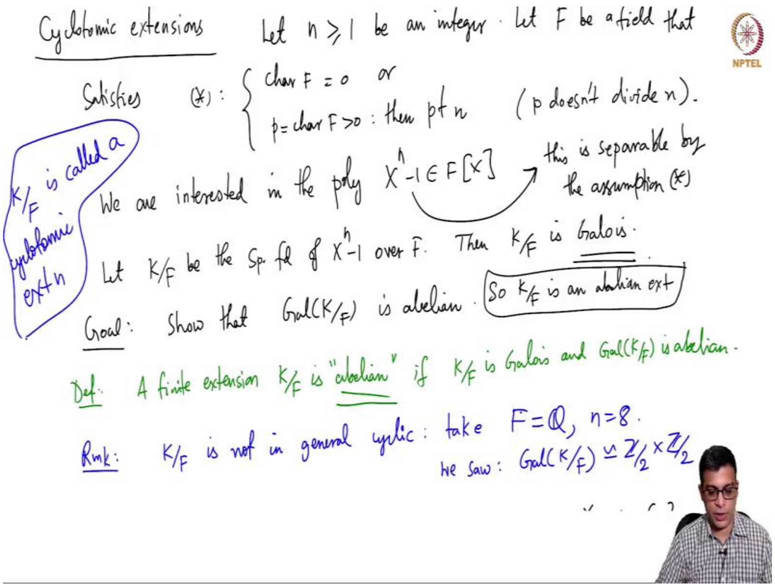
So, sigma tau of zeta is sigma tau of zeta which is zeta power i tau, which is zeta power i tau power i sigma. Because zeta goes to zeta power i sigma under sigma, so zeta power i goes to zeta power i tau power sigma, which is zeta power i tau phi sigma. Earlier, we had i tau plus i sigma there, there the target group was a relative group. So that worked well. So, that means phi of sigma tau is i tau times i sigma or i sigma times i tau which is phi of sigma times phi of tau.

So, that is required property, because here my operation is multiplication. So, it is a group homomorphism. And finally, why is it 1-1? It is 1-1 because suppose phi of sigma is 1, which is the identity in Z mod n Z star, multiplicative identity. So, that means sigma of zeta is zeta power 1. But then remember, I should have mentioned this earlier. Note that K is F zeta, because K is a splitting field of X power n minus 1 and we just argued that or we argued earlier in the video that zeta generates all the rules.

So, if sigma fixes zeta sigma fixes every alpha in ,K because of course it fixes F it fixes it zeta, so it fixes every polynomial in zeta that means, sigma is identity. So, therefore, kernel of phi is identity implies phi is 1-1, so phi is an injective homomorphism from Galois group of K over F to Z mod n Z star. So, that, I will make 1 or 2 remarks and then we will stop. So, the first remark is that; Hence, this shows that if F, n, K are as above then K over F is an abelian extension.

As I remarked, this is what I wanted to do earlier, because Z mod n Z star is abelian. Because multiplication of integers is commutative, hence multiplication of integer is modulo n is committed to so, and G is isomorphic to a subgroup of an abelian group, so it is abelian. So, that is good. So, cyclotomic extensions are abelian.

(Refer Slide Time: 32:40)



Cyclotomic extensions Let $n \geqslant 1$ be an integer. Let F be a field that

Satisfies $(*)$: $\begin{cases} \text{char } F = 0 \text{ or} \\ p = \text{char } F > 0 : \text{then } p \nmid n \end{cases}$ (p doesn't divide n).

K/F is called a cyclotomic extn

We are interested in the poly $X^n - 1 \in F[X]$ → this is separable by the assumption $(*)$

Let K/F be the Sp. fd of $X^n - 1$ over F. Then K/F is Galois.

Goal: Show that $\text{Gal}(K/F)$ is abelian. So K/F is an abelian ext

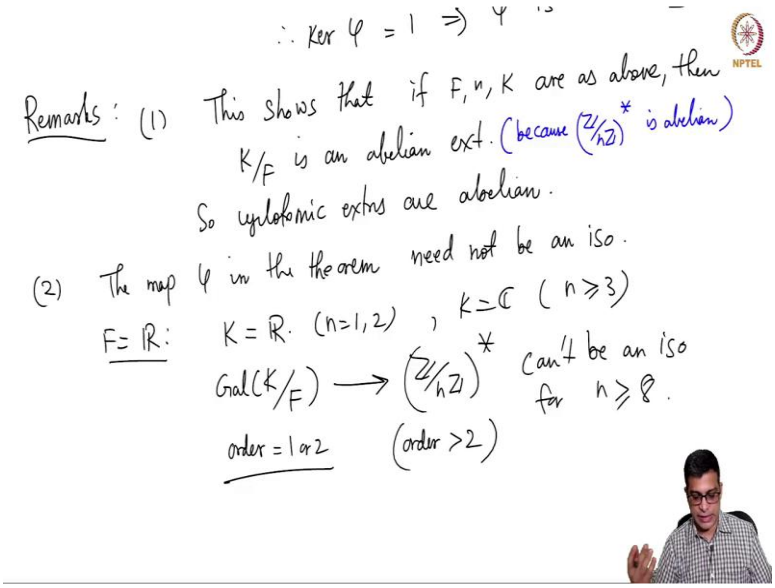
Def: A finite extension K/F is "abelian" if K/F is Galois and $\text{Gal}(K/F)$ is abelian.

Rmk: K/F is not in general cyclic: take $F = \mathbb{Q}$, $n = 8$.

We saw: $\text{Gal}(K/F) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$

So, by the way, I should define this, I will write down at the end but K over F is called cyclotomic extensions, I should have defined this but it is in fact, nth cyclotomic extension of F. So, what this is saying is that, so cyclotomic extensions are abelian.

(Refer Slide Time: 33:18)



$\therefore \text{Ker } \varphi = 1 \Rightarrow \varphi$ is

Remarks: (1) This shows that if F, n, K are as above, then K/F is an abelian ext. (because $(\mathbb{Z}/n\mathbb{Z})^*$ is abelian)

So cyclotomic extns are abelian.

(2) The map φ in the theorem need not be an iso.

$F = \mathbb{R}$: $K = \mathbb{R}$. $(n = 1, 2)$, $K = \mathbb{C}$ $(n \geqslant 3)$

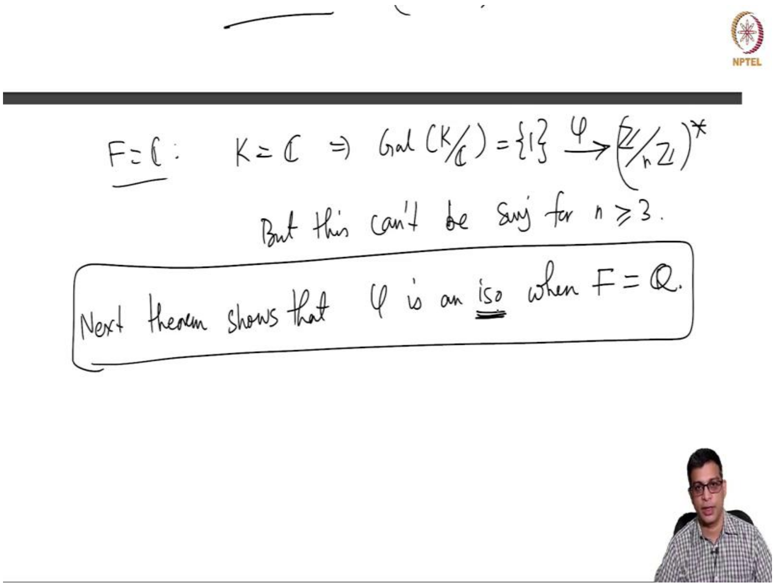
$\mathrm{Gal}(K/F) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*$ can't be an iso for $n \geqslant 8$.

order $= 1$ or 2 (order > 2)

Second remark is the map phi in the theorem which is an injective group homomorphism, need not be an isomorphism. In other words, it need not be a surjective map. Because if you take F equal to R and n equal to, I mean any n. So, then K is either R or I mean most of the time in fact K is C. Because if you take X power n minus 1, this is R if n equal to 1 and 2 and K equal to C, if n is greater than equal to 3.

Because, you have only primitive square root and first root of 1 in R, every other primitive nth root of a 1 is a non-real complex number. So, the map to Z mod n Z star cannot be an isomorphism, for n I think greater than 8 or something. Because this order is 1 or 2. And this order is very soon after some time, it will be at least 3, so order is at least 3.

(Refer Slide Time: 34:51)



$\underline{F = \mathbb{C}}$: $K = \mathbb{C} \Rightarrow \mathrm{Gal}(K/\mathbb{C}) = \{1\} \xrightarrow{\varphi} (\mathbb{Z}/n\mathbb{Z})^*$

But this can't be surj for $n \geq 3$.

$\boxed{\text{Next theorem shows that } \varphi \text{ is an } \underline{\underline{\text{iso}}} \text{ when } F = \mathbb{Q}.}$

Or more clearly if you take F equal to C, K equals C, because C already contains all primitive nth roots of unity, C is algebraically closed. So, Galois K over C is identity. Of course, it sits insides Z mod n Z star, but this cannot be an isomorphism, can be surjective for n greater than 3, I think. So, see Z mod n Z star, the target group does not keep track of how big K is compared to F, so clearly this cannot be in general an isomorphism.

Because this Z mod n Z star keeps going. But K over F can be small, as in these two examples, K equals R and K equal to C. I hope that is clear. So, the groups Galois K over F are very small, trivial when K equal to C, and a group of order 2 when F equal to R, and n equal to, I mean for large n, but Z mod n Z star is a big group.

But next theorem, which I will prove next class, next theorem shows that phi is in fact an isomorphism when F is Q, which is going to be crucial for us, which is a nice structural result for cyclotomic extensions of Q. So, this is something that will prove in the next video. So, let me stop now. And in the next video, we will prove this theorem, learn a little bit more about cyclotomic extensions. And after that we will get to the main focus of this whole course, which is solving polynomials by radicals. Thank you.