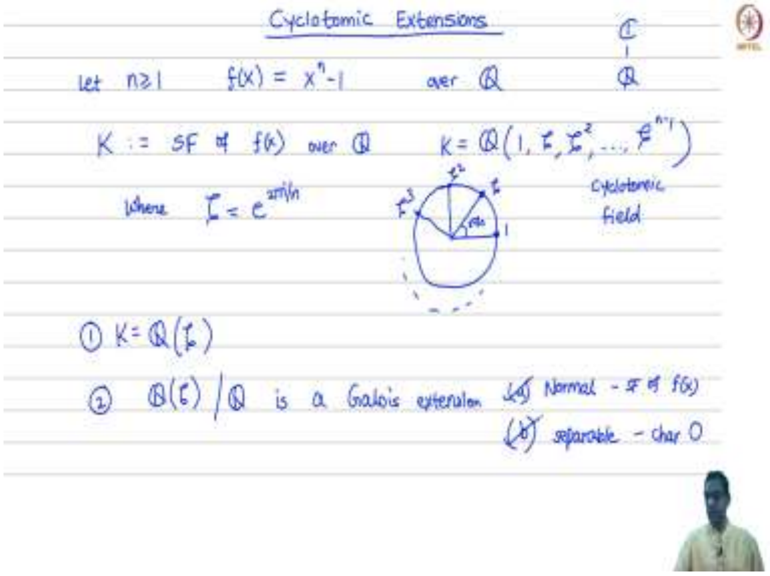
Algebra - II
Professor S Viswanath
Department of Mathematics
The Institute of Mathematical Science
Lecture 39
Cyclotomic Extensions

(Refer Slide Time: 00:14)



Cyclotomic Extensions

$\mathbb{C}$
$|$
$\mathbb{Q}$

let $n \geq 1$ $\quad f(x) = x^n - 1$ over $\mathbb{Q}$

$K :=$ SF of $f(x)$ over $\mathbb{Q}$ $\quad K = \mathbb{Q}(1, \zeta, \zeta^2, \dots, \zeta^{n-1})$

where $\zeta = e^{2\pi i/n}$ $\quad$ cyclotomic field

① $K = \mathbb{Q}(\zeta)$

② $\mathbb{Q}(\zeta)/\mathbb{Q}$ is a Galois extension (a) Normal - SF of $f(x)$
(b) separable - char 0

Today we will talk about cyclotomic extensions. So what are these? Well, they are what we usually call the roots of unity. So let me make this more precise. So let us take a number n greater than or equal to 1 and let us take the polynomial f of x to be x to the n minus 1 and my base field here is the field of rational numbers and what we are going to do is to look at the splitting field of this.

So let K, or maybe I will call it K sub n, in this case. So, let us fix n for now. So let me just call it K; K is the splitting field of this polynomial f x over Q. Recall what does that mean? You just have to adjoin to K, the roots of this polynomial over some algebraic closure. So since the complex numbers is one ready, algebraic closure that we know about.

So all we have to do is adjoin the roots of unity. The roots of this polynomial, which if you remember, are just 1 zeta, zeta square till zeta to the n minus 1, where what zeta, zeta is just e to the 2 pi i by n and recall, we have our usual picture on the unit circle. So one of the rules is 1, the next fellow is zeta, which forms an angle of 2 pi by n and then the next one is zeta square.

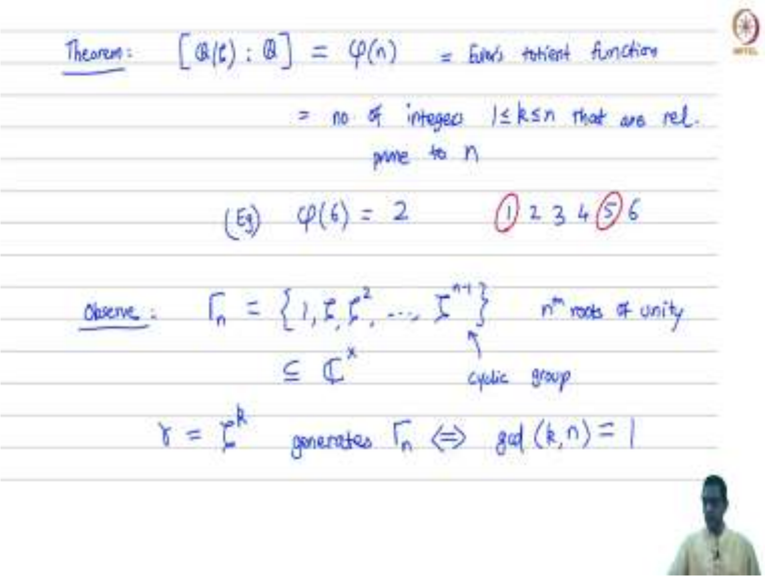
So they form the vertices of a regular n gone on the circle like this. So those are the roots of unity and this field, K is what we call the cyclotomic field or the cyclotomic extension of Q and this is indexed by this number n that we fixed. So here are some basic facts about this. So let us look at this cyclotomic extension K.

So we encountered this once before, one of the examples that, well you do not need to adjoin n minus 1 or n of these roots. It is enough to adjoin just one of them. That is because once you are joined zeta, all the powers of zeta automatically in this field. So that is K is just Q zeta. Now, Fact number 2 is that Q zeta is a Galois extension of Q.

So, this is a Galois extension. Galois is that you need to check two things; that it is normal inseparable. It is normal as an extension because it is the splitting field of a bunch of polynomials. Well, in this case, it is the splitting field.

Since this is given as a splitting field of some polynomial and separable comes for free because observe that we are talking about characteristic 0 fields and there we have seen that all algebraic extensions are automatically separable. So, this is just both are straightforward in this case.

(Refer Slide Time: 03:44)



Theorem: $[\mathbb{Q}(\zeta):\mathbb{Q}] = \varphi(n)$ = Euler's totient function

= no of integers $1 \le k \le n$ that are rel. prime to n

(Eg) $\varphi(6) = 2$ 1 2 3 4 5 6

Observe: $\Gamma_n = \{1, \zeta, \zeta^2, \dots, \zeta^{n-1}\}$ n^{th} roots of unity

$\subseteq \mathbb{C}^{\times}$ ↑ cyclic group

$\gamma = \zeta^k$ generates $\Gamma_n \iff \gcd(k,n) = 1$

So what we are talking about is a certain Galois extension of the field of rational numbers and our goal is really the following theorem; proposition which says that the degree of this Galois extension is for phi of n. So what is phi of n? This is Euler’s totient function which counts. So this is the number of natural numbers, are number of integers k, from 1 to n that are relatively prime to n that are relatively prime to n.

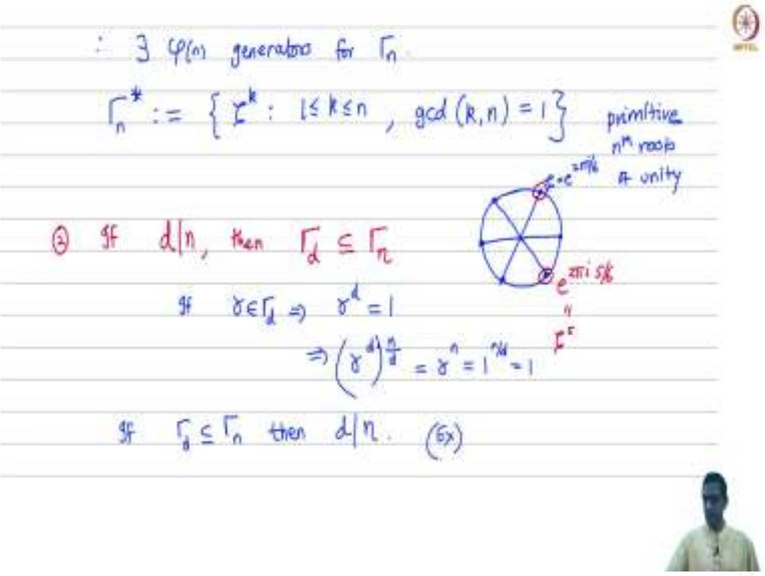
So, you have seen this before. So, for example if I take phi of 6 this is just 2 because among the numbers 1, 2, 3, 4, 5 and 6 only two of them are relatively prime to 6, which is the numbers 1 and 5. Now, let us prove this theorem. That is our goal. So various facts to observe; so here is: observe the following.

So, I am going to prove this over the course of several steps. Let us make some preliminary observations, the roots of unity that I just wrote out 1 zeta, zeta square; so let us call that gamma n. So, these are what we call the nth roots of unity. So, these form, they form a multiplicative group. So, this is a, think of it as a subset of the multiplicative group of nonzero complex numbers.

So, this forms in fact a cyclic group, gamma n is a cyclic group and of course, it has zeta itself is a generator but there are many other generators for this group, gamma n, so which are the generators? How, you know which elements generate this group? So let us say gamma equals zeta power k generates, so let me generates this cyclic group means what?

Well recall you know, when does an element zeta power k generate the cyclic group? While this can only happen if k and n are relatively prime. So, this is just from our usual knowledge about cyclic groups and so on and so, what does that mean? It says that, in fact there is exactly, phi of n generators for this cyclic group.

(Refer Slide Time: 06:38)



$\therefore \ \exists \ \varphi(n)$ generators for Γ_n.

$\Gamma_n^* := \{ \zeta^k : 1 \le k \le n, \ \gcd(k,n) = 1 \}$ primitive n^{th} roots of unity

$\zeta = e^{2\pi i/6}$

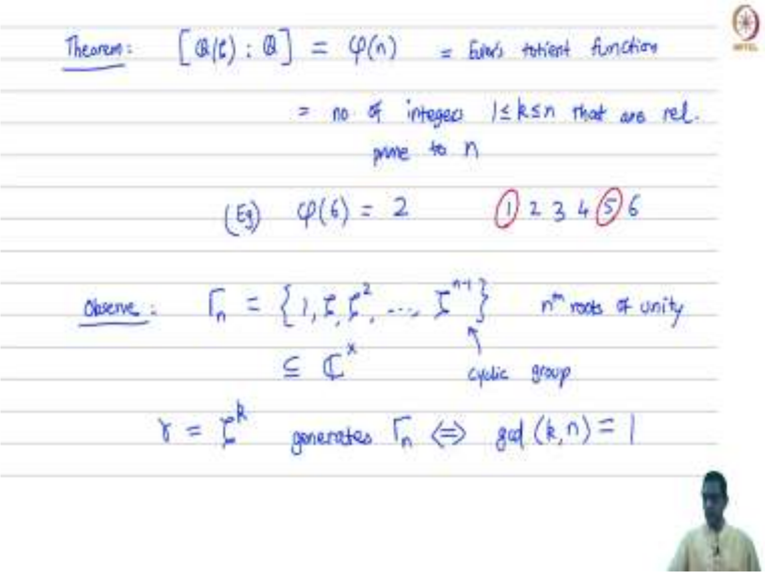
$e^{2\pi i \, 5/6}$ $\parallel$ ζ^5

③ If $d|n$, then $\Gamma_d \subseteq \Gamma_n$

If $\gamma \in \Gamma_d \Rightarrow \gamma^d = 1$

$\Rightarrow (\gamma^d)^{\frac{n}{d}} = \gamma^n = 1^{n/d} = 1$

If $\Gamma_d \subseteq \Gamma_n$ then $d|n$. (Ex)



Theorem: $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$ = Euler's totient function

= no of integers $1 \le k \le n$ that are rel. prime to n

(Eg) $\varphi(6) = 2$ 1 2 3 4 5 6

Observe: $\Gamma_n = \{1, \zeta, \zeta^2, \ldots, \zeta^{n-1}\}$ n^{th} roots of unity

$\subseteq \mathbb{C}^\times$ cyclic group

$\gamma = \zeta^k$ generates $\Gamma_n \iff \gcd(k,n) = 1$

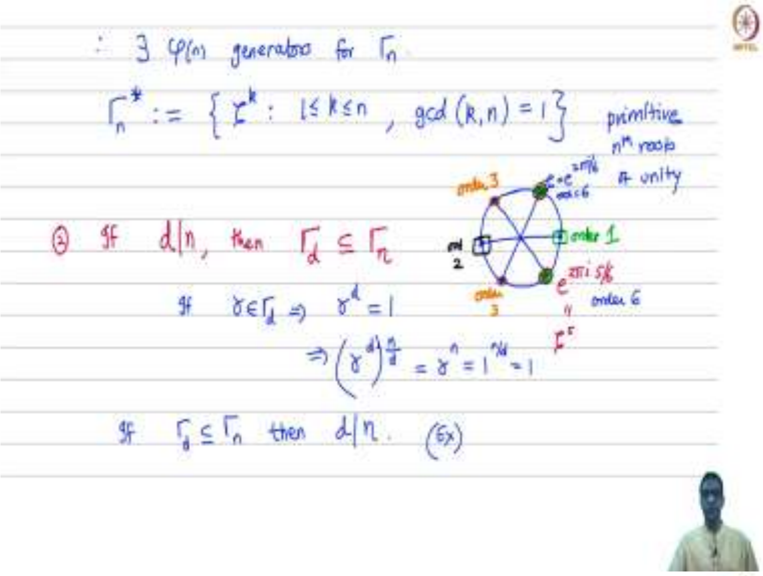
So, therefore there exists phi of n generators for this cyclic group gamma. So those many possibilities and these generators are what are called the primitive. So, let me give this a name, so gamma n star is just a set of these generators or it is the set of all zeta power k, k from 1 to n such that the GCD of k with n is 1. So, this set is called the set of primitive nth roots of unity and in our previous example, so when we talks about n equals 6, for instance so these are the, so you have 6, 6 roots of unity.

So, these are the 6 of them and so this is zeta is e to 2 pi i over 6 and then the various powers of zeta and only 2 of them are primitive. So, which is e to the 2 pi i over 6 and e to the 5 pi i over 6, sorry 2 pi I into 5 by 6. So, these are the two so, this is zeta power 5. So, these are the two primitive 6th roots of unity, the other roots of unity are not primitive.

Now, let us also look at what can we say about the other roots? So, this is observe more facts, maybe we will number these. So, observe fact 1, so observe 2, that if d divides n then what does it mean? It says that the dth roots of unity are necessarily contained inside the nth roots of unity. So why is this? Well, it is sort of more or less obvious, you just have to see take any dth root of unity and just see that it lives inside the set of nth roots of unity.

So let us just check this quick check. So, if gamma is an element of gamma d, that just means gamma power d is 1, of course d divides n. Therefore gamma d power, if a raise this to be n over d, then that is just gamma and 1 power n over d is just 1. So, if something power d is 1, something power n is automatically 1 and in fact, the converse is also easy to see that if n divides, if gamma d subset of gamma n so, another quick statement for you to check. If this is contained, then d must divide n. So I leave this as an exercise.

(Refer Slide Time: 09:45)



$\therefore\ \exists\ \varphi(n)$ generators for Γ_n

$$\Gamma_n^{*} := \{ \zeta^{k} : 1 \le k \le n,\ \gcd(k,n) = 1 \}$$

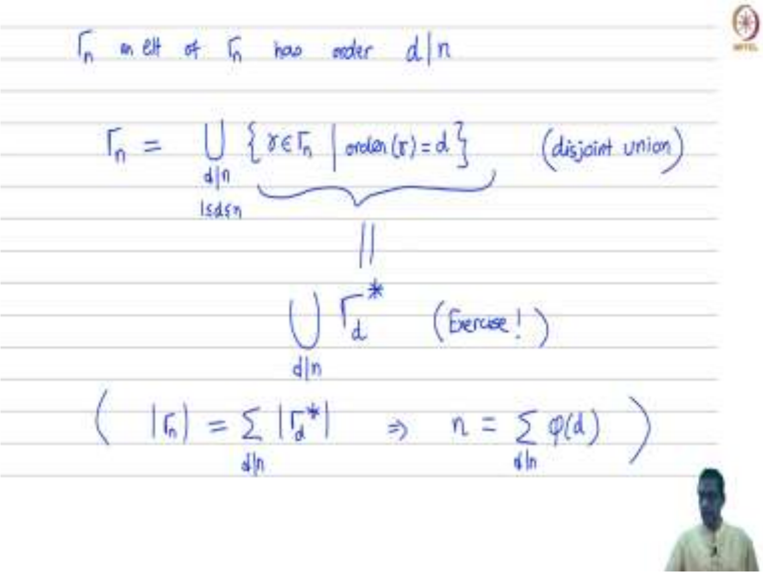
primitive n^{th} roots of unity

(2) If $d|n$, then $\Gamma_d \subseteq \Gamma_n$

If $\gamma \in \Gamma_d \Rightarrow \gamma^{d} = 1$

$$\Rightarrow (\gamma^{d})^{\frac{n}{d}} = \gamma^{n} = 1^{n/d} = 1$$

If $\Gamma_d \subseteq \Gamma_n$ then $d|n$. (Ex)



Γ_n an elt of Γ_n has order $d|n$

$$\Gamma_n = \underbrace{\bigcup_{\substack{d|n \\ 1 \le d \le n}} \{ \gamma \in \Gamma_n \mid \text{order}(\gamma) = d \}}_{\displaystyle \| \atop \displaystyle \bigcup_{d|n} \Gamma_d^{*}} \quad \text{(disjoint union)}$$

(Exercise!)

$$\left(|\Gamma_n| = \sum_{d|n} |\Gamma_d^{*}| \Rightarrow n = \sum_{d|n} \varphi(d) \right)$$

Now, let us look at the various elements of order d dividing n. So we did a talk about d dividing n. So observe if I take gamma n, the elements so what can I say about a typical element of gamma n? An element of gamma n has order and talking about the cyclic group and gamma n, in that cyclic group; this element must have some order and recall that the order of an element necessarily divides the cardinality of the group.

So, I can therefore decompose gamma as follows. I say, let me take I will write it as a union and in this union is disjoint. It is a union over all d, dividing n. So d is now a number between 1 and n of the set of elements gamma in gamma n, such that the order of gamma is d. So I can write gamma n like this as a disjoint union.

So if you go back to this example, notice that the 2 things I circled in red, both have order 6. So these, these are the primitive roots of unity, they are the generators; so these two have order 6. Now, if I take this element here, which is element 1, this has order 1 because it is the identity. Now, if I take the element at the other end that is minus 1, this has order 2 because when you square it, I get identity and the remaining elements have order 3.

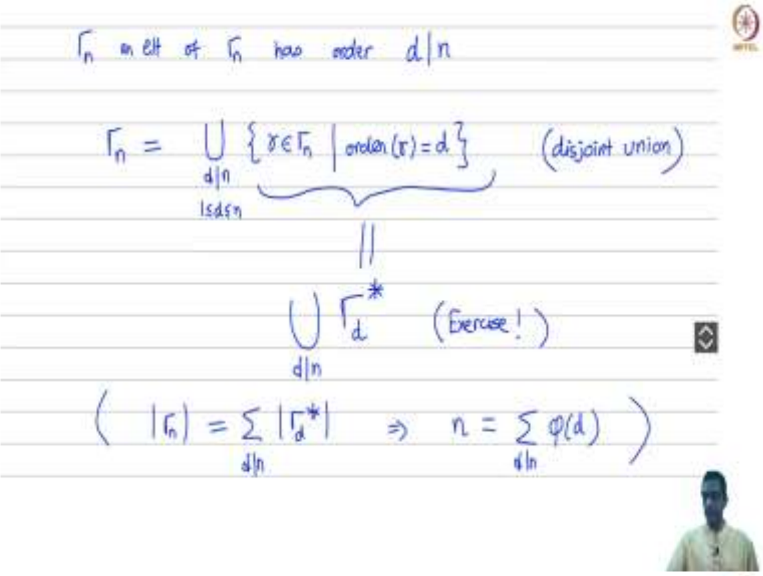
So if we take this element and this element they both have order 3 in the cyclic group and the original elements, like I said, both have order 6 of these orders 6. So this is the decomposition I am talking about, just look at what the orders of the different elements are and split them up into a disjoint, split gamma n up into a disjoint union of subsets of different orders and now here is the, here is the very interesting important fact.

If I look at these elements here, the ones whose order is exactly d, then you will observe that this is actually just the set gamma d star. So in other words, this is the union d dividing n of gamma d star. Now, maybe again I leave this as a little exercise for you to check. It is a easy, easy sort of exercise. So, you know look back on this previous diagram that we drew and sort of see how those came about.

So notice that the elements of order 3 that I drew in this picture are exactly what we would usually call omega and omega square, the cube roots of unity and so on. And the proof is just more or less from the definition; just see what it means for an element who have order d and what it means for an element to belong to gamma d star and you will notice that these two are exactly the same. So in particular, what is this, this proof?

So this is sort of an aside observe that the cardinality is on both sides must be equal. So this in fact implies that n is the cardinality on the left hand side is the sum of phi d d dividing n and this is one of those classic identities for the Euler totient function.

(Refer Slide Time: 13:40)



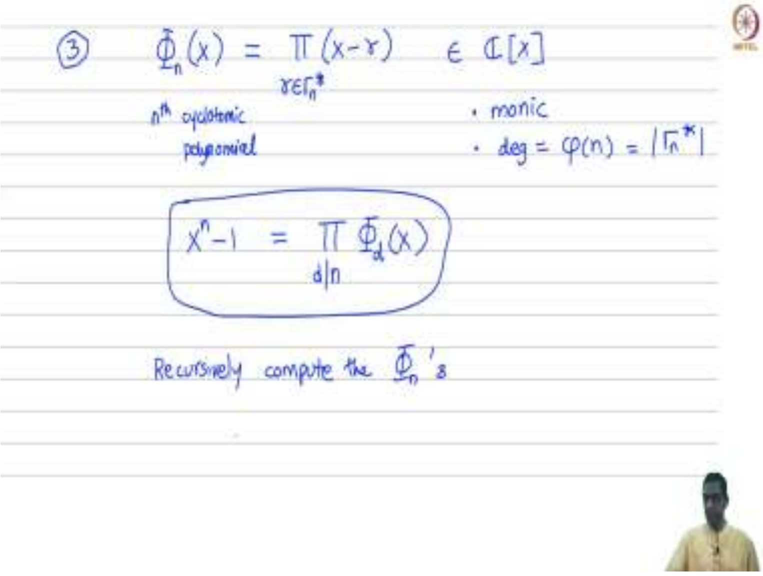
Γ_n an elt of Γ_n has order $d|n$

$$\Gamma_n = \bigcup_{\substack{d|n\\1\le d\le n}} \underbrace{\{\gamma\in\Gamma_n \mid \text{order}(\gamma)=d\}} \quad \text{(disjoint union)}$$

$$\|$$

$$\bigcup_{d|n}\Gamma_d^* \quad (\text{Exercise!})$$

$$\left(|\Gamma_n| = \sum_{d|n}|\Gamma_d^*| \Rightarrow n = \sum_{d|n}\varphi(d) \right)$$



③ $\Phi_n(x) = \prod_{\gamma\in\Gamma_n^*}(x-\gamma) \in \mathbb{C}[x]$

n^{th} cyclotomic polynomial

- monic
- $\deg = \varphi(n) = |\Gamma_n^*|$

$$\boxed{x^n-1 = \prod_{d|n}\Phi_d(x)}$$

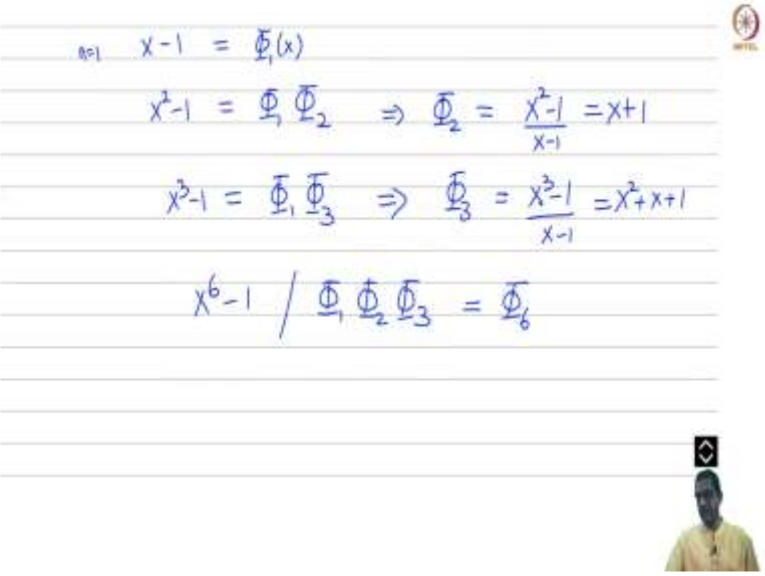
Recursively compute the Φ_n's

But our main interest is in trying to understand this cyclotomic extension. So, let me so we quoted it facts 1 and 2. Let us move on to fact 3; is really a definition. So let us define the polynomial of interest. Phi n of x, this is just the product of x minus gamma where; gamma ranges over the primitive nth roots of unity. And observe that, well at the moment, what can I say? I can say that I am only taking a primitive and at the roots of unity, this is maybe a polynomial with complex coefficients.

That is about it so far. I know something more about it. It is a monic polynomial and the degree of this polynomial is exactly the number of terms which is the cardinality of gamma and star if just phi n. So this capital phi n of x is what is called the nth cyclotomic polynomial. It is got roots. The roots of this polynomial are just the primitive nth roots of unity. So observe that the decomposition I talked about earlier, gamma n being a disjoint union of the gamma d stars, it translates into the following identity d dividing n.

It is the same thing, you are just taking those all n roots on the left side and you are sort of taking roots collected together by their order on the right hand side. So this is an important identity because it actually allows you to calculate what the phi ds are. So observe, this can be used to recursively, compute recursively compute these polynomials capital phi ns by well, for example; so let us just do the first few cases.

(Refer Slide Time: 15:53)



$n=1 \quad x-1 = \Phi_1(x)$

$x^2-1 = \Phi_1\Phi_2 \Rightarrow \Phi_2 = \frac{x^2-1}{x-1} = x+1$

$x^3-1 = \Phi_1\Phi_3 \Rightarrow \Phi_3 = \frac{x^3-1}{x-1} = x^2+x+1$

$x^6-1 \,/\, \Phi_1\Phi_2\Phi_3 = \Phi_6$

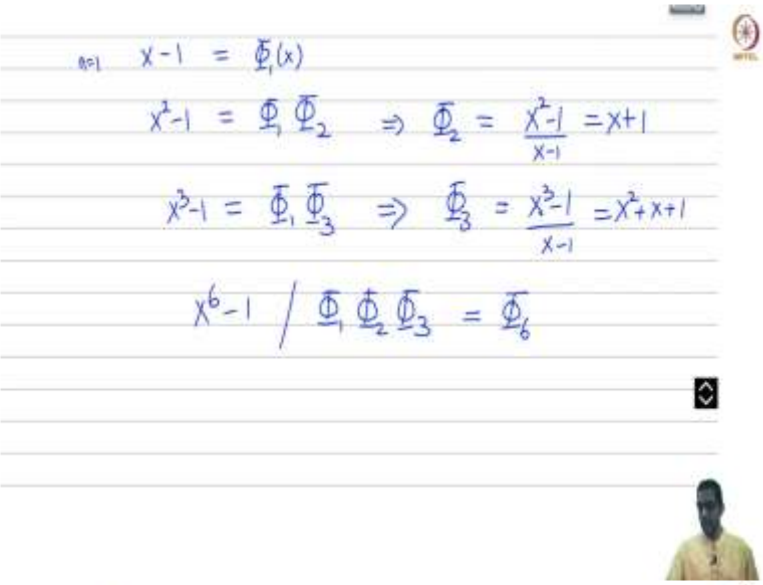
So if I take n equals 1, then it says x minus 1 is just my polynomial phi 1 of x, x square minus 1 is phi 1. So I will just supress on the right side phi 1 into phi 2. So what does this mean? It tells me that my polynomial phi 2 is just x square minus 1 by x minus 1. So similarly, x cubed minus 1 becomes. So observe I should only run over the divisors of n. So it tells me phi 3 is just x cubed minus 1 by x minus 1.

So that is x square plus x plus 1 and so on. So for example, if you did phi 6 will notice this will be sorry, if you wanted to do it for phi 6, this is x to the 6 minus 1 equals phi 1, 2, 3 and 6 and from here, you could just take x to the 6 minus 1 and divide it out by the preceding three fellows. That answer is phi 6, whatever it turns out to be.

Now, one obvious conclusion from here lead this recursive procedure is that even though it seemed to have complex coefficients a priori to start with, in fact it has a rational coefficients.

Why? Well, because we can sort of compute it in this way. We can calculate it by this recursive procedure.

(Refer Slide Time: 17:32)

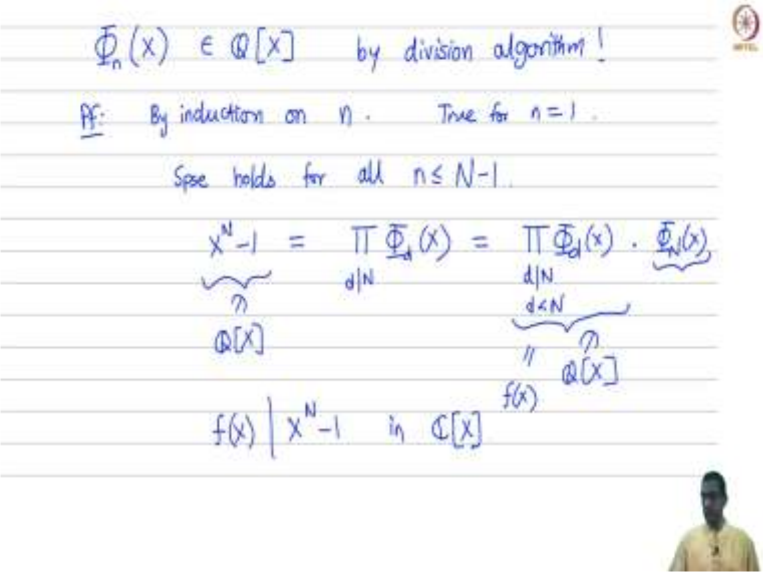


n=1 $x-1 = \Phi_1(x)$

$x^2-1 = \Phi_1\Phi_2 \Rightarrow \Phi_2 = \frac{x^2-1}{x-1} = x+1$

$x^3-1 = \Phi_1\Phi_3 \Rightarrow \Phi_3 = \frac{x^3-1}{x-1} = x^2+x+1$

$x^6-1 \,/\, \Phi_1\Phi_2\Phi_3 = \Phi_6$



$\Phi_n(x) \in \mathbb{Q}[x]$ by division algorithm!

Pf: By induction on n. True for $n=1$.

Spse holds for all $n \le N-1$.

$$\underbrace{x^N-1}_{\underset{\mathbb{Q}[x]}{\cap}} = \prod_{d|N}\Phi_d(x) = \underbrace{\prod_{\substack{d|N\\ d<N}}\Phi_d(x)}_{\underset{f(x)}{\parallel}\ \underset{\mathbb{Q}[x]}{\cap}} \cdot \underbrace{\Phi_N(x)}$$

$f(x) \mid x^N-1$ in $\mathbb{C}[x]$

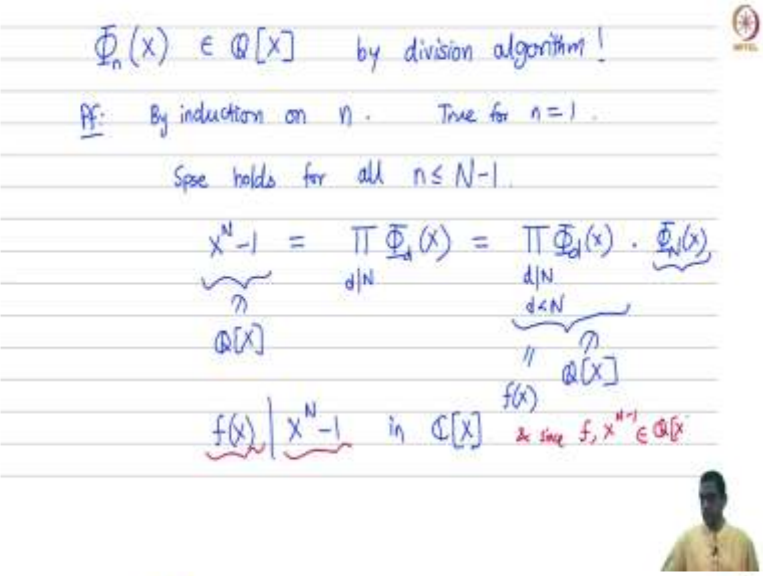
So observe this procedure implies the following that phi n x phi n of x, facts is actually polynomial rational coefficients. Why is that? By if you wish, by the division algorithm. So what do we mean by that? So let us maybe prove this formally. So what I mean is, it is an inductive proof; proof is by induction on n. So these formulas here, sort of prove it for the first few values of n.

So let us just say we know how to prove it for n. So true for n equals 1 and suppose it holds for all n less than or equal to some capital N minus 1, then how do you prove it for capital N? Well, you just use the recursive procedure. You write it as phi 1, whatever I do not know what the divisors are. So maybe I will just write it in general product of phi d of x, d divides N and from this, I will just pull out the last term phi n alone.

So I will take product of the phi ds, d dividing n but d is strictly smaller than n times capital phi n of x. Now, by induction this product, so I have assumed already that all the phi ds for these smaller than n are n Q x. So this is n Q x. So what does that mean? That at least I know the following that this is in Q x; In fact, it is in it is inside of x.

Now when I divide this and I know that phi n of x is just a quotient of these 2 polynomials. So I know that this polynomial here or whatever we should call it something f of x. So I know this f of x definitely divides x to the n minus 1 in C of x. If you view everything as being polynomials with coefficients in complex numbers, then f definitely divides the polynomial x to the n minus one and the quotient is exactly what we are calling phi n of x.

(Refer Slide Time: 20:05)



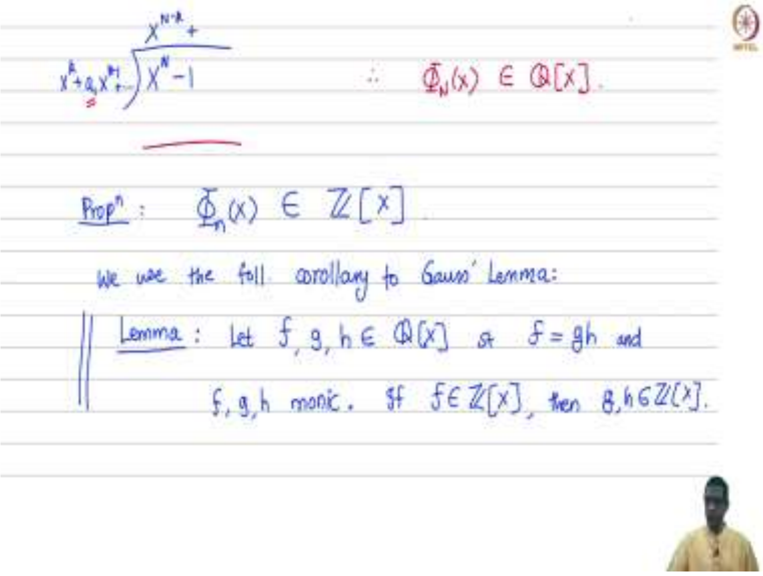
$\Phi_n(x) \in \mathbb{Q}[x]$ by division algorithm!

Pf: By induction on n. True for $n=1$.

Spse holds for all $n \le N-1$.

$$\underbrace{x^N-1}_{\substack{\cap \\ \mathbb{Q}[x]}} = \prod_{d|N} \Phi_d(x) = \underbrace{\prod_{\substack{d|N \\ d<N}} \Phi_d(x)}_{\substack{\shortparallel \quad \cap \\ f(x) \quad \mathbb{Q}[x]}} \cdot \Phi_N(x)$$

$f(x) \mid x^N-1$ in $\mathbb{C}[x]$ & since $f, x^{N-1} \in \mathbb{Q}[x$



$$x^k + a_1 x^{k-1} + \cdots \overset{x^{N-k} +}{\overline{\big) \, x^N - 1}}$$

$\therefore \Phi_N(x) \in \mathbb{Q}[x]$.

Prop^n: $\Phi_n(x) \in \mathbb{Z}[x]$.

We use the foll corollary to Gauss' Lemma:

Lemma: Let $f, g, h \in \mathbb{Q}[x]$ st $f = gh$ and f, g, h monic. If $f \in \mathbb{Z}[x]$, then $g, h \in \mathbb{Z}[x]$.

But how does one compute the quotient? So if you sort of remember what the division algorithm does, you sort of calculate the coefficient or if you wish, we think in terms of long division. How do you how do you perform long division? So you take x to the n minus 1, then I have this polynomial f of x here.

So you sort of divide, I take the coefficients of x in the sum a, k, x power k, so this is monic plus a 1 x to the k minus 1 and so on and I sort of divide out coefficient by coefficient. So, if you just imagine how the long division process is carried out, so you will notice that this will be some x to the n minus k plus some next term but this next term will only involve rational numbers.

Why is that? Because if you remember how those are computed, it only involves these numbers a 1 or the numbers which arise during this process, all of which are rational. So that is sort of one argument; you can make this argument a bit more formal as well. But the broad idea is that if f x divides this in C x and if these two are in Q x and if f I mean and since these are in Q x, one can also conclude that F divides x to the n minus 1 in Q x.

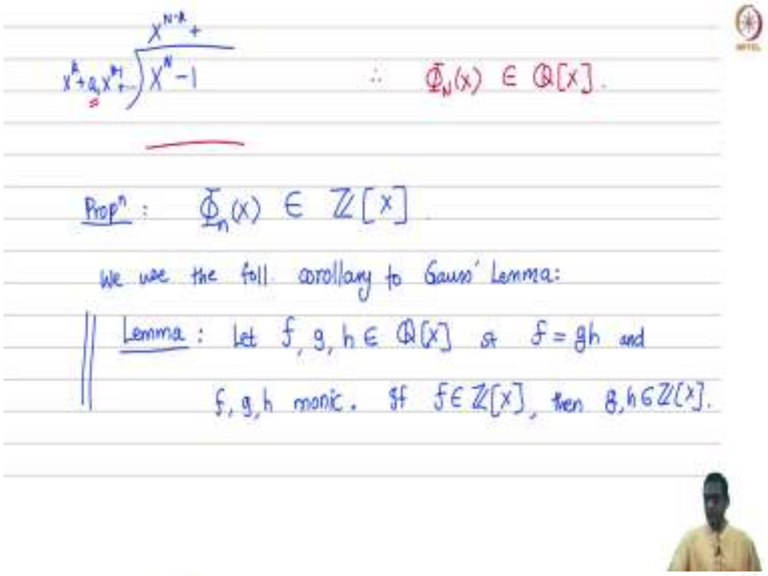
In other words, the quotient is actually in Q x. So what does that mean? Therefore, we have concluded that phi n of x has rational coefficients. So that is an important simplification. But in fact, there is something more and this is rather remarkable. So it is a little proposition here that actually these polynomials have integer coefficients, not just rational in fact, their coefficients are integers.

So, to prove this, so you had seen something along these lines in the earlier lecture on Gauss's lemma and so on. So, to use this I mean to prove this we use a corollary of Gauss's lemma. So, we use let me call, state this as a lemma because it will be used repeatedly in this in this whole analysis of cyclotomic polynomials and so on.

So, this lemma says that, if I have f, g, h polynomials with rational coefficients such that f equals g into h, let this happen. Now, if monic so I should also said Q x such that they are all monic polynomials and f g h monic. Now, if f is in z x, if f has integer coefficients, then both g and h also have integer coefficients.

So, this was one of the corollaries that you had looked at the following corollary to Gauss lemma. So, please look back on the lecture on Gauss's lemma. This just involves observing that the contents are 1 on both sides and then applying Gauss's lemma. So, this is a very very important statement, that if I have two monic polynomials g and h, whose product is f and if f is you know integral, it has integer coefficients, then g and h must also have integer coefficients.

(Refer Slide Time: 24:19)



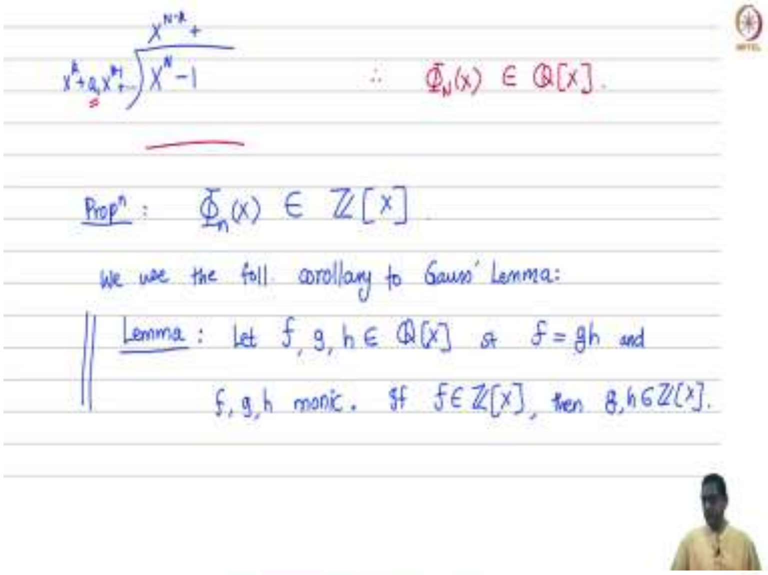
$$x^k + \underset{=}{a_1} x^{k-1} + \cdots \overset{x^{N-k} +}{\overline{\big)\, x^N - 1}}$$

$\therefore \quad \Phi_N(x) \in \mathbb{Q}[x]$.

Propⁿ: $\Phi_n(x) \in \mathbb{Z}[x]$.

We use the foll. corollary to Gauss' Lemma:

Lemma: Let $f, g, h \in \mathbb{Q}[x]$ st $f = gh$ and f, g, h monic. If $f \in \mathbb{Z}[x]$, then $g, h \in \mathbb{Z}[x]$.



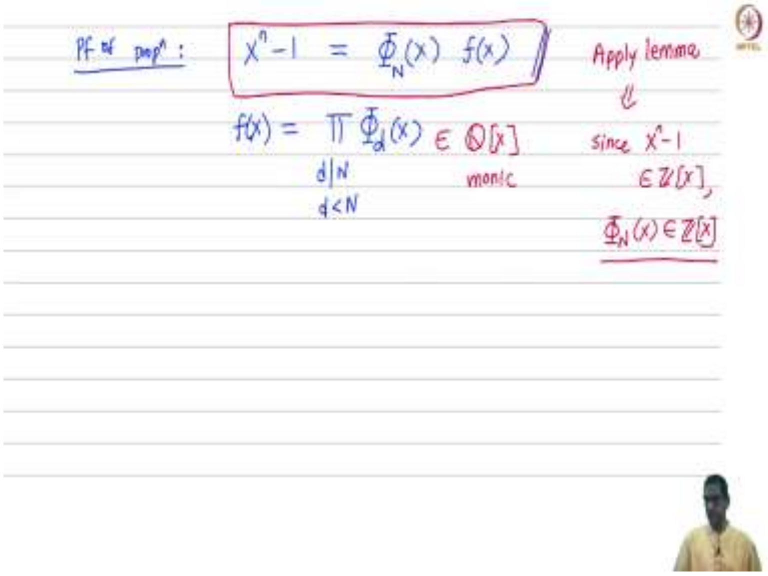
$$x^k + \underset{=}{a_1} x^{k-1} + \cdots \overset{x^{N-k} +}{\overline{\big)\, x^N - 1}}$$

$\therefore \quad \Phi_N(x) \in \mathbb{Q}[x]$.

Propⁿ: $\Phi_n(x) \in \mathbb{Z}[x]$.

We use the foll. corollary to Gauss' Lemma:

Lemma: Let $f, g, h \in \mathbb{Q}[x]$ st $f = gh$ and f, g, h monic. If $f \in \mathbb{Z}[x]$, then $g, h \in \mathbb{Z}[x]$.



Pf of propⁿ: $\boxed{x^n - 1 = \Phi_N(x)\, f(x)}$

$$f(x) = \prod_{\substack{d|N \\ d<N}} \Phi_d(x) \in \mathbb{Q}[x]$$

monic

Apply lemma

$\Downarrow$

since $x^n - 1 \in \mathbb{Z}[x]$,

$\Phi_N(x) \in \mathbb{Z}[x]$

Now, how does that help us in this case of phi n? Well, again this is by induction. So, let us complete the proof of this proposition. Proof of this proposition: mean we do not even really need induction here. So, observe that x to the n minus 1 has been written as the product of phi n or just say, let me go back to my earlier inductive sort of thing for n of x into f of x and what is f of x?

It was the product of the other divides N, d is smaller than N. So now, we will prove this proposition also by induction, if you wish. So it is true for n equals 1. It is true that phi 1 of x has integer coefficients and again, you assume it is to assume for n less than n minus 1, then you try to prove it for capital N itself.

And now, that is this identity here, x to the n minus 1 is phi n of x f x. Now just apply the lemma. So by the induction hypothesis, so since we assumed it for all n, so for all n, so then by the induction hypothesis, we conclude that each phi d of x, so each phi d has integer coefficients and it is all monic.

So we know that the phi ds are all monic. So therefore, the product is also integral and monic. So that we know, but so what else do we know? We know, it is it is all rational. So let us just look at, so in this case, I guess we did not quite need the induction hypothesis, we just (want) need to know that they are all rational.

So we just need to (get) you know, know that they are in Q x. So, sorry we do not need this really. So let us just recall from what we already know, that f x is. So we do not even need an induction here because we are just going to use the lemma straight away. So I already know this that this is in Q x. We have already proved that portion of the statement and now, so apply the lemma that I just talked about.

The lemma says that if I can write f as g h, where all three are monic and that is exactly what I can do here. So I already know this monic. So x to the n minus 1 is monic, phi n monic, f x is monic. The fact that it is monic is just from the definition. All of them are in Q x. That is a bit I just proved by induction.

And so by the lemma, it means that, but it since the left hand side, x to the n minus 1 is integral, it is got integer coefficients. Therefore, phi n of x and f of x both have integer coefficients but I am only interested in phi n. So that completes the proof, just a simple application of Gauss’s lemma.