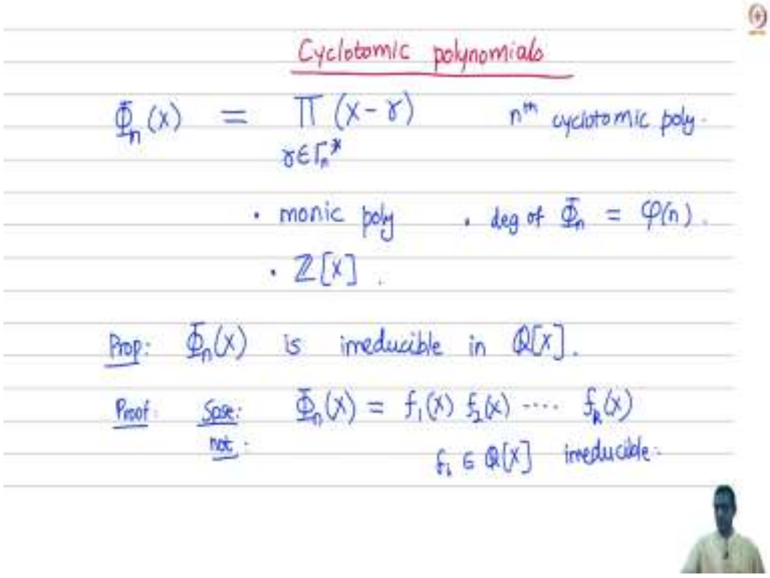
Algebra - II
Professor S Viswanath
Department of Mathematics
The Institute of Mathematical Science
Lecture 40
Irreducibility of the Cyclotomic Polynomials

(Refer Slide Time: 00:14)



Cyclotomic polynomials

$\Phi_n(x) = \prod_{\gamma \in \Gamma_n^*} (x-\gamma)$ n^{th} cyclotomic poly.

• monic poly • deg of $\Phi_n = \varphi(n)$.

• $\mathbb{Z}[x]$.

Prop: $\Phi_n(x)$ is irreducible in $\mathbb{Q}[x]$.

Proof Spse: not. $\Phi_n(x) = f_1(x) f_2(x) \cdots f_k(x)$

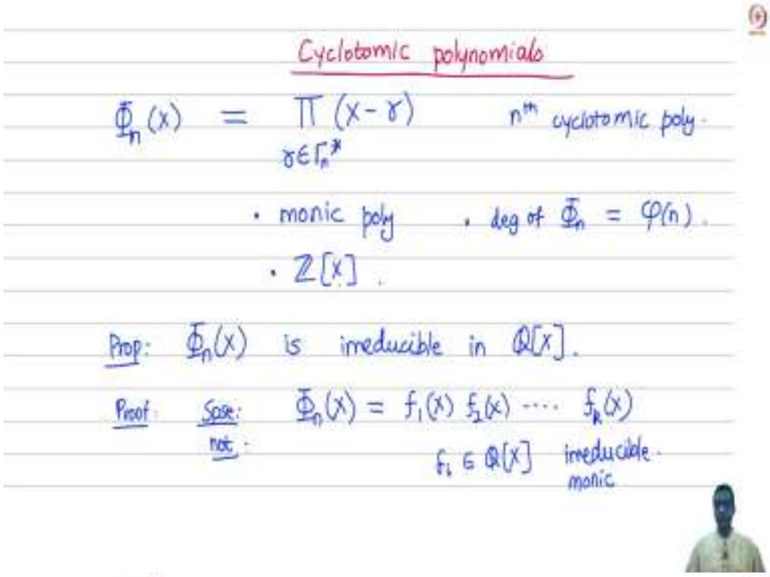
$f_i \in \mathbb{Q}[x]$ irreducible.

Last time we were talking about cyclotomic extensions. So let me continue proving a few more facts about these cyclotomic polynomials. So, recall we have shown the following; if I take phi n of x, capital phi n of x to be the product of the primitive nth roots of unity. So, look back on the last lecture for the notation. So, these are the primitive gamma n star as primitive nth roots of unity. He called this the nth cyclotomic polynomial and what we have shown so far is that this is a monic polynomial with coefficients in Z.

Now, this time we will establish the following important statement that in fact this is an irreducible polynomial in Q x. So, observe the other thing we know is that the degree of this polynomial is just the value of Euler’s totient function, the number of numbers which are between 1 and n which are relatively prime to n. So, we need to show the irreducibility of this polynomial. That is our next claim.

So, the proof is, it involves a few arguments which are reminiscent of what was used to prove Gauss’s lemma, just mostly reduction module of p. So, let us go ahead and write out the proof. So, suppose this is you know, so if it is not irreducible; suppose, we can write it as a product of irreducible factors. So, write it like this. So, suppose not, suppose it is not irreducible then I can write it like this, some product of irreducible factors. The phis are all elements of Q x irreducible.

(Refer Slide Time: 02:38)



Cyclotomic polynomials

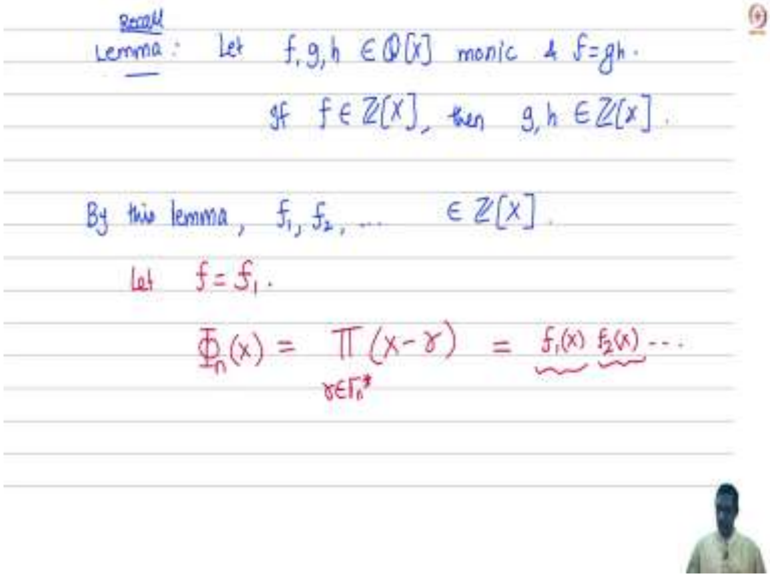
$\Phi_n(x) = \prod_{\gamma \in \Gamma_n^*} (x-\gamma)$ n^{th} cyclotomic poly.

- monic poly
- deg of $\Phi_n = \varphi(n)$.
- $\mathbb{Z}[x]$.

Prop: $\Phi_n(x)$ is irreducible in $\mathbb{Q}[x]$.

Proof Spse not: $\Phi_n(x) = f_1(x) f_2(x) \cdots f_k(x)$

$f_i \in \mathbb{Q}[x]$ irreducible. monic



Recall Lemma: Let $f, g, h \in \mathbb{Q}[x]$ monic & $f = gh$.

If $f \in \mathbb{Z}[x]$, then $g, h \in \mathbb{Z}[x]$.

By this lemma, $f_1, f_2, \ldots \in \mathbb{Z}[x]$.

Let $f = f_1$.

$$\Phi_n(x) = \prod_{\gamma \in \Gamma_n^*} (x-\gamma) = \underset{\sim}{f_1(x)}\, \underset{\sim}{f_2(x)} \cdots$$

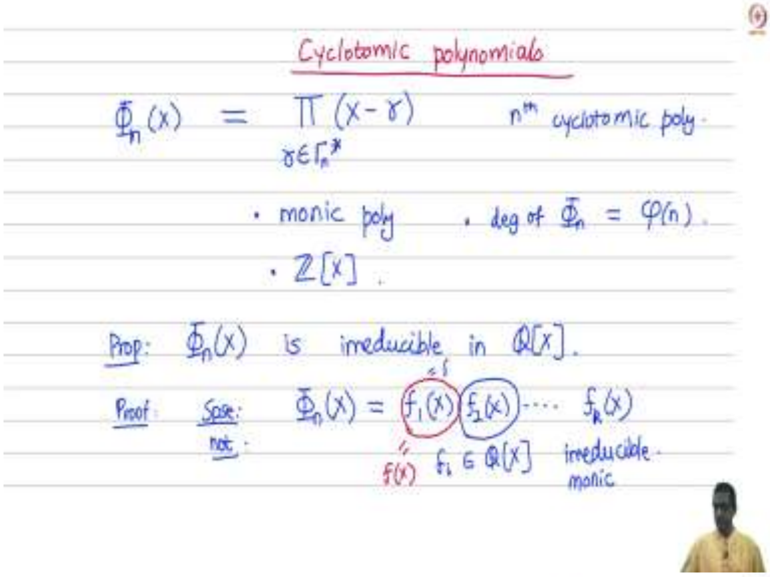
Now, recall the little lemma from last time, which was a consequence of Gauss's lemma, which says that, if I have three monic polynomials f, g, h in Q x are all monic and f equals gh, then, so if f, let if f as integer coefficients, then g and h must also have integer coefficients. So this was a corollary to Gauss's lemma. So, we will use this repeatedly.

So, by this lemma what can we conclude? So, observe we have written phi n of x as a product of f ks, the f ks are all irreducible, I can always assume they are all monic. So, now this lemma applies because phi n of x we have already shown to be a monic polynomial with coefficients in Z of x. So, by the lemma we can conclude the following that the irreducible factors f 1, f 2, f 3 et cetera, are all coefficients, are all polynomials with coefficients in Z.

So now, let me do the following, let me call this first term, so I have many of these terms. So, let me call the first term as something so, I will call this as f of x, so let us call this f of x. Now, what does this imply? So, let f equals the very first irreducible factor and let us pick well we sort of know what the, let beta be root of f. So, remember I know what my entire product looks like phi n minus x is the product of all the primitive nth roots of unity and this I am writing as f 1 of x f 2 of x and so on.

So, of course the roots of f 1 of x will be some subset of the primitive roots. f 2 of x will have roots which are you know some other subset of the of gamma n star and so on. So, when you go to the complex numbers, for example, think of them as polynomials of the complex numbers, the roots of f 1, f 2 and so on are all going to be some subsets of gamma n star.

(Refer Slide Time: 05:32)



Cyclotomic polynomials

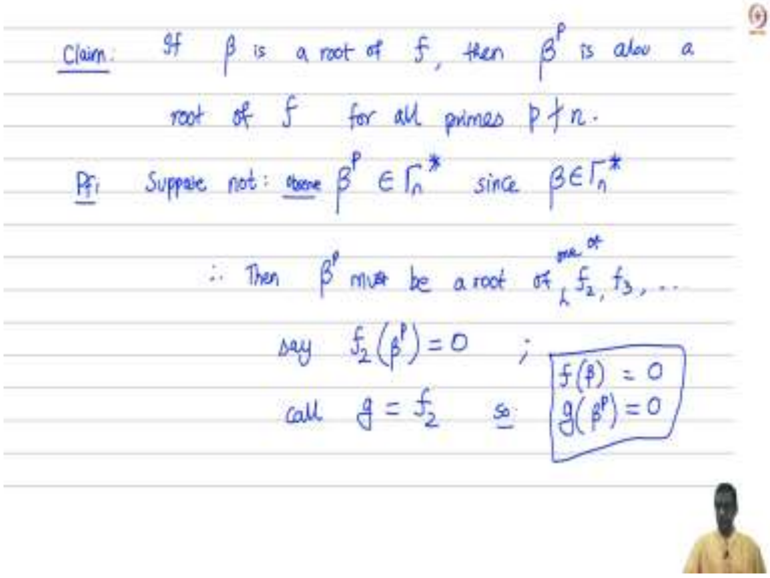
$\Phi_n(x) = \prod_{\gamma \in \Gamma_n^*} (x-\gamma)$ $\quad$ n^{th} cyclotomic poly.

- monic poly $\quad$ • deg of $\Phi_n = \varphi(n)$.
- $\mathbb{Z}[x]$.

Prop: $\Phi_n(x)$ is irreducible in $\mathbb{Q}[x]$.

Proof Spse not. $\Phi_n(x) = \overset{= f}{\boxed{f_1(x)}}\,\boxed{f_2(x)} \cdots f_k(x)$

$f(x)$ $\quad$ $f_i \in \mathbb{Q}[x]$ irreducible. monic



Claim: If β is a root of f, then β^p is also a root of f for all primes $p \nmid n$.

Pf: Suppose not: observe $\beta^p \in \Gamma_n^*$ since $\beta \in \Gamma_n^*$

$\therefore$ Then β^p must be a root of one of $f_2, f_3, \ldots$

say $f_2(\beta^p) = 0$;

call $g = f_2$ $\quad$ so $\boxed{\begin{array}{l} f(\beta) = 0 \\ g(\beta^p) = 0 \end{array}}$

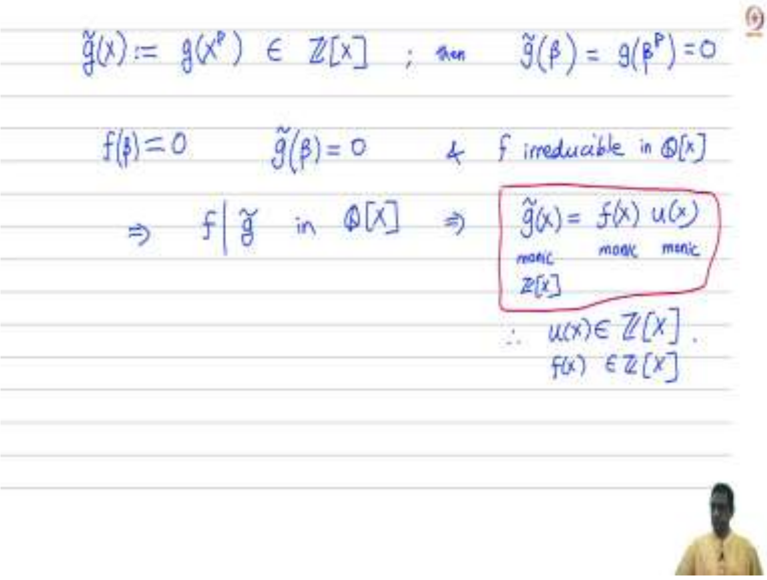
Now, so I picked one root, so let beta be a root of f, maybe I should let me not call this single beta here. So, let me just make a more precise claim; claim proposition: if beta is the root of, is a root of f then beta power P is also root of f and what is P, for all primes P which do not divide n. So, that is our claim.

So, let us prove this, suppose not, so observe beta power P is also primitive nth roots of you know, if beta is primitive nth roots of, nth root of unity and P is relatively prime to n. So, then beta power P is also a primitive nth root of unity because the order. So, recall what was the nth root of unity definitions those elements of gamma n whose order is n.

So, beta has order n then I raise beta to a power P which is relatively prime to n, then this also has order n. So then so suppose not, so first observe that beta power P is also a primitive nth root of unity. Therefore, if beta power P is not a root of f, then beta power P must be a root of one of the other factors, then beta power P must be a root of one of these other factors f 2, f 3 etc, of one of these, one of.

So let me say that that polynomial is f 2, so let us say suppose f 2 of beta power P is zero. So let us again call this something, we will keep needing to use it again. So let us just give it a simpler name. Let us call f 2 as g. So I know the following that g on beta power P is 0. What else do we know? I know that beta is the root of f and f and g are just the names I gave to the first two factors f 1 and f 2.

(Refer Slide Time: 08:13)



$\tilde{g}(x) := g(x^P) \in \mathbb{Z}[x]$; then $\tilde{g}(\beta) = g(\beta^P) = 0$

$f(\beta) = 0$ $\tilde{g}(\beta) = 0$ & f irreducible in $\mathbb{Q}[x]$

$\Rightarrow f \mid \tilde{g}$ in $\mathbb{Q}[x]$ $\Rightarrow$ $\boxed{\underset{\substack{\text{monic}\\ \mathbb{Z}[x]}}{\tilde{g}(x)} = \underset{\text{monic}}{f(x)}\ \underset{\text{monic}}{u(x)}}$

$\therefore$ $u(x) \in \mathbb{Z}[x]$.

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

So these are, no one guy is called f the next one is called g. So let us remember all these pieces of notation. Now, what does this mean? So, you look at this f beta 0, g of beta power P is 0. So therefore, it says that if I form the new polynomial g tilde of x, what is g tilde of x, is the same as g evaluated at x power p.

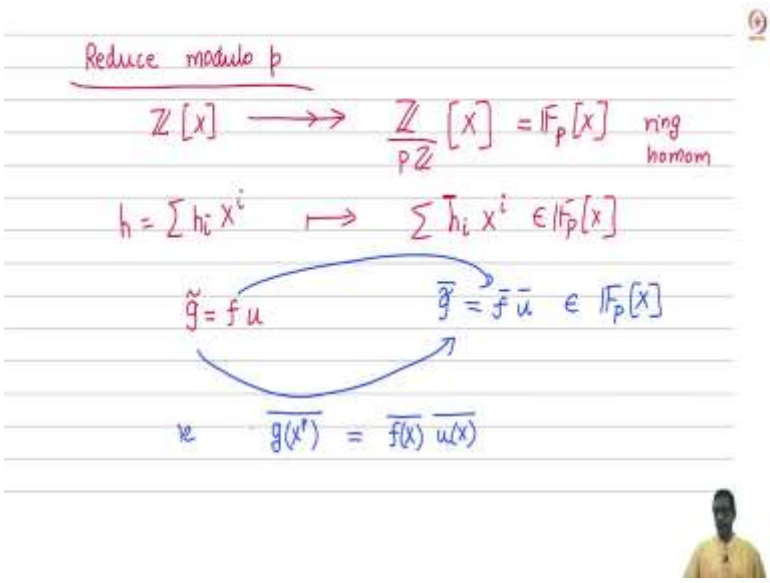
This is again some polynomial in fact; it is polynomial coefficients in Z. Observe f 1 and f 2 have coefficients in Z. So, of course so does g tilde. If I define g tilde in this manner, then observe that g tilde evaluated on beta just as g evaluated on beta power P is 0. So, now I have the following; I know that beta is the root of this irreducible polynomial f and beta is also the root of another polynomial g tilde and f remember is irreducible.

So, what does this mean? It tells me that f must divide g tilde in Q of x, in fact by using our lemma, so what does this mean? f divides g tilde in Q of x means that, so everything here is over the field Q x. This means, I can write g tilde of x as f times some quotient u of x but again I can use that lemma once again.

See, I know that g tilde is again a monic polynomial, f is monic. So, of course u is automatically monic. further I know that this is in Z of x because of course, g tilde is just in the same as you know I take the polynomial f 2 and I put x power P instead of x. So, this is in Z x and therefore, by that lemma both f and u are automatically in Z x.

So, therefore I mean f, I already know is Z x. So, the only new information is that u of x is in Z x. Good. So, now this is the equation that I that I want. I also know that f x is in Z x. So, I am going to use this equation. So, let us do the following.

(Refer Slide Time: 10:41)



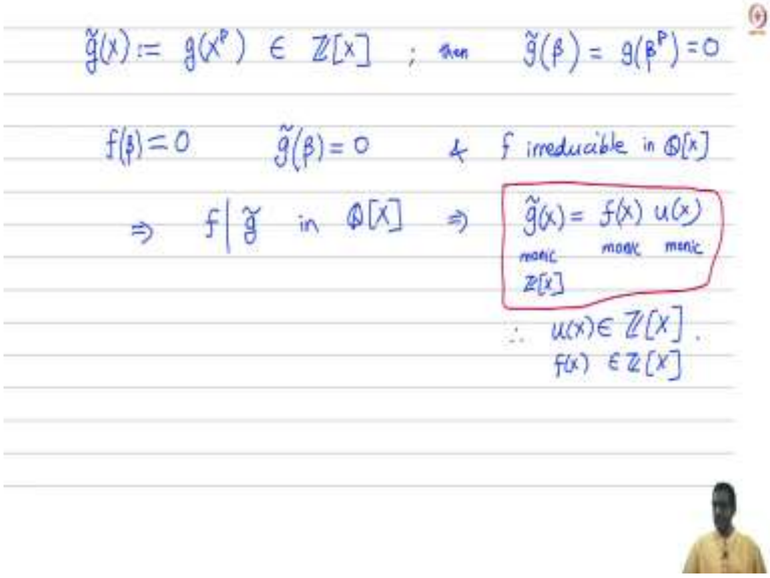
Reduce modulo p

$$\mathbb{Z}[x] \twoheadrightarrow \frac{\mathbb{Z}}{p\mathbb{Z}}[x] = \mathbb{F}_p[x] \quad \text{ring homom}$$

$$h = \sum h_i x^i \longmapsto \sum \bar{h}_i x^i \in \mathbb{F}_p[x]$$

$$\begin{tikzcd} \tilde{g} = fu \arrow[r, bend left] \arrow[r, bend right] & \bar{\tilde{g}} = \bar{f}\,\bar{u} \in \mathbb{F}_p[x] \end{tikzcd}$$

ie $\overline{g(x^p)} = \overline{f(x)}\;\overline{u(x)}$



$\tilde{g}(x) := g(x^p) \in \mathbb{Z}[x]$; then $\tilde{g}(\beta) = g(\beta^p) = 0$

$f(\beta) = 0$ $\quad \tilde{g}(\beta) = 0$ & f irreducible in $\mathbb{Q}[x]$

$$\Rightarrow f \mid \tilde{g} \text{ in } \mathbb{Q}[x] \Rightarrow \boxed{\underset{\substack{\text{monic}\\ \mathbb{Z}[x]}}{\tilde{g}(x)} = \underset{\text{monic}}{f(x)}\;\underset{\text{monic}}{u(x)}}$$

$\therefore$ $u(x) \in \mathbb{Z}[x]$.
$f(x) \in \mathbb{Z}[x]$

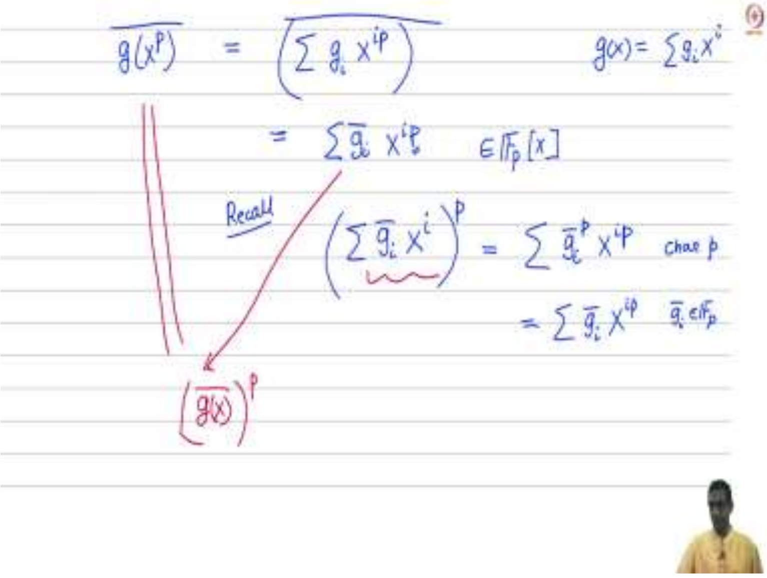
So, this is the key step here. So, this is what you also used in the proof of Gauss's lemma. This is reduce modulo p. What does this mean? This means: consider the following ring homomorphism. If I have a polynomial with integer coefficients, I can just reduce each coefficient modulo p, this is F p of x. So, what does it mean?

If I have summation, say h is a polynomial, h i x power I, h i is an integer, I just read it modulo p it becomes h i bar that is my new coefficient. So, that is my map. That is called the reduction modulo p map and this map is in fact, this a surjective map, this is a ring homomorphism as you have seen before. So I can take integer polynomials and convert them into polynomials over the finite field F p.

So now, the fact that it is ring homomorphism means the following: recall, I have this equation here that g tilde is f into u and all three things are in Z x. So I will just apply my homomorphism to this to this equation. So I have g tilde equals f into u, that is identity that is true in Z x. If I apply my homomorphism, my reduction modulo p to each of these terms, g tilde will go to some polynomial g tilde bar and f will map to some polynomial f bar, u goes to u bar.

And because it is a homomorphism the same identity holds, that g tilde bar is f bar u bar and this is now an identity in the ring f p of x. So, what does that mean? So let us analyse this reduced equation. This just means, if I take the polynomial g tilde, was just the polynomial g of x power p and I reduce it modulo p, then that is just going to give me f of x bar u of x bar

(Refer Slide Time: 13:03)



$\overline{g(x^p)} = \overline{\left(\sum g_i x^{ip}\right)}$ $\qquad g(x) = \sum g_i x^i$

$= \sum \overline{g_i}\, x^{ip} \in \mathbb{F}_p[x]$

Recall

$\left(\sum \underbrace{\overline{g_i}\, x^i}\right)^p = \sum \overline{g_i}^{\,p} x^{ip}$ Char p

$= \sum \overline{g_i}\, x^{ip}$ $\quad \overline{g_i} \in \mathbb{F}_p$

$\left(\overline{g(x)}\right)^p$

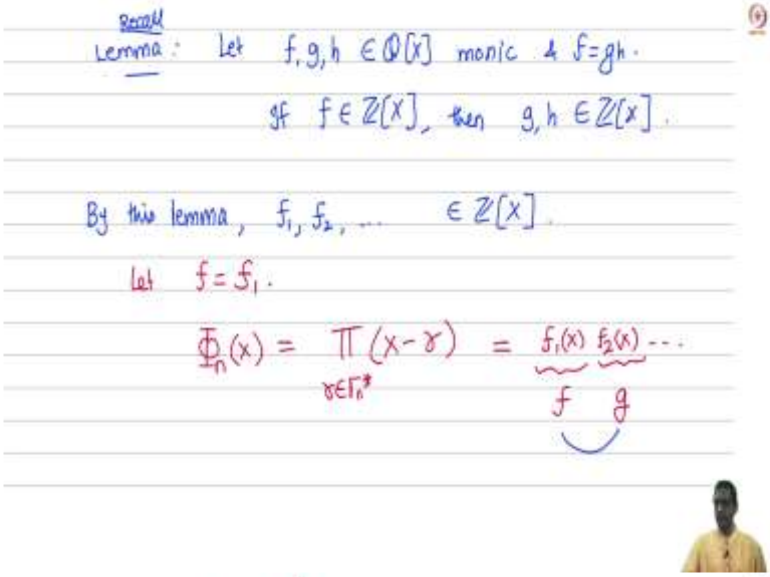
But what is this g of x power p bar? That is the thing we want to understand. Observe, what is g of x power p the whole bar means? Means I, so let us say g looks like some g i x power i, then first I have to replace x by x power p. So I am saying, suppose g x is the polynomial g i x power i then I first plug in x power p and then I do bar of this. Which means I just take summation g i bar x i p and this is a polynomial f p of x.

But recall the, I mean there is a reason for reducing modulo that same prime p and that p and this p are the same. This is a calculation which we have done many times; if you have a field of characteristic p, then when you want to raise this, this to the power p, then what you get? Well, you just get the same coefficient. So it is it is this power p. So recall that if I computed this quantity, then that would just be g i bar power p, x to the i p.

But g i bar is in the, so this is because the characteristic is p, field has characteristic p but further, g i is g i bar, come from my finite field f p and in my finite field f p. This is because g i bar come from f p. If I raise an element to the pth power, I just get back itself. So that is the important observation here.

So finally, we conclude that this quantity here is nothing but you take g of x bar, that is the thing that is inside here and you raise it to the p. So g of x power p bar is the same as g bar x whole power p. That is a strange identity but that comes about because the (character) I mean you are going modulo the same prime p here somehow.

(Refer Slide Time: 15:18)



Recall

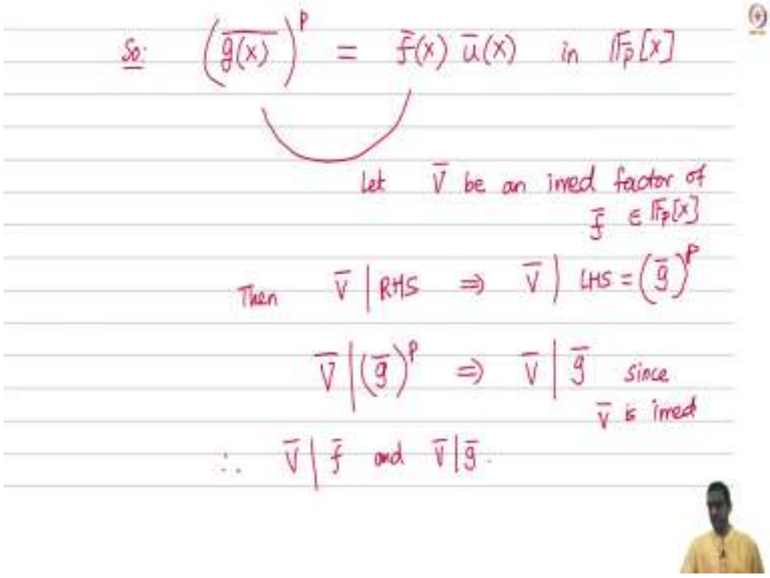
Lemma: Let $f, g, h \in \mathbb{Q}[x]$ monic & $f = gh$.

If $f \in \mathbb{Z}[x]$, then $g, h \in \mathbb{Z}[x]$.

By this lemma, $f_1, f_2, \ldots \in \mathbb{Z}[x]$.

Let $f = f_1$.

$$\Phi_n(x) = \prod_{\gamma \in \Gamma_n^*} (x-\gamma) = \underbrace{f_1(x)}_{f}\ \underbrace{f_2(x)}_{g} \cdots$$



So: $\left(\overline{g(x)}\right)^p = \bar{f}(x)\,\bar{u}(x)$ in $\mathbb{F}_p[x]$

Let $\bar{v}$ be an irred factor of $\bar{f} \in \mathbb{F}_p[x]$

Then $\bar{v} \mid RHS \Rightarrow \bar{v} \mid LHS = (\bar{g})^p$

$\bar{v} \mid (\bar{g})^p \Rightarrow \bar{v} \mid \bar{g}$ since $\bar{v}$ is irred

$\therefore\ \bar{v} \mid \bar{f}$ and $\bar{v} \mid \bar{g}$.

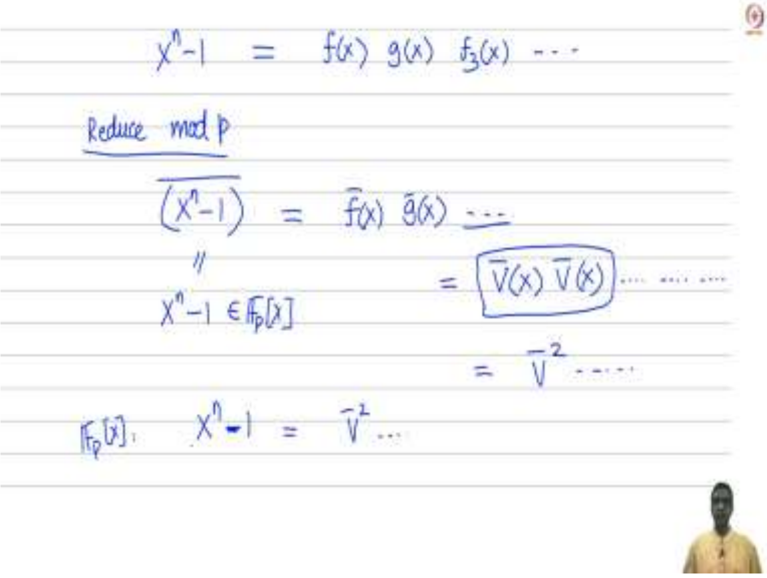
So now we are ready to complete the proof. So what do we get? So we have g of x, I take g x bar whole power p is the same as f bar of x, u bar of x. It is an identity which holds an f p of x. But what does that mean? It means that you know, f bar and g bar must have a common factor. This means well, let us let us establish that properly the following.

So let us do the following. Let us just take an irreducible factor of f bar. So let some polynomial v bar be an irreducible factor of f bar. Then what do we know? Therefore, v bar divides the hand side. Therefore, v bar divides the left hand side of this equation, this is just g bar whole power p. But if an irreducible factor, so v bar is irreducible or it is prime in that ring, you know it is in f p of x over the field f p.

If v bar divides some power of a polynomial, then since v bar is reducible, v bar has to divide that polynomial itself. Since v bar is irreducible, so what does that mean? Therefore, v bar is common to both f bar and g bar. So therefore, v bar divides f bar. That was our assumption and v bar must also divide g bar. So that is really what we were after. Now, let us go back and see what f and g were? We have managed to get a common factor.

So this was this was our original phi n of x. So I called this as f, this was my second factor was g. Now what I sort of concluded is that f and g, they have a common factor. So it seems like f and g have a common factor. That was my v bar but this common factor is after reduction modulo p. It is not as they are but only after reduction modulo p. But that is still good enough.

(Refer Slide Time: 17:52)



$$x^n - 1 = f(x)\, g(x)\, f_3(x) \cdots$$

Reduce mod p

$$\overline{(x^n-1)} = \bar{f}(x)\, \bar{g}(x) \cdots$$

$$\parallel$$

$$x^n - 1 \in \mathbb{F}_p[x]$$

$$= \boxed{\bar{V}(x)\, \bar{V}(x)} \cdots \cdots \cdots$$

$$= \bar{V}^2 \cdots$$

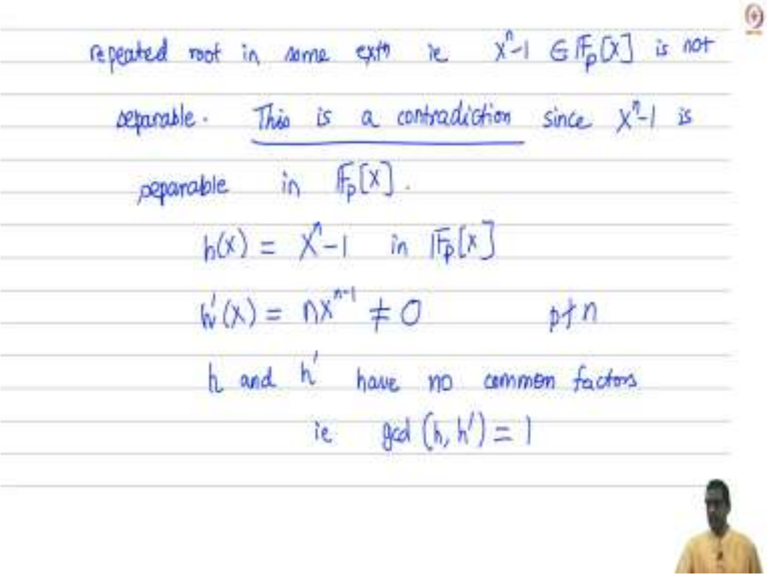
$$\mathbb{F}_p[x]: \quad x^n - 1 = \bar{V}^2 \cdots$$

So let us reduce everything modulo p and show that this is a contradiction. So now, let us go back and recall. Where are we, this is f, g and then maybe there are other factors. But now let us reduce both sides modulo p. So I will take this x n minus 1, think of it as reduced modulo p, the coefficients which means it is really again x to the n minus 1 but in the, so this is just , you know when I reduce the coefficients, modulo p I just get back one again.

But I have to think of these as now being ones in f p, this is f bar of x into g bar of x into some other terms but f bar and g bar have one common factor, which is v bar. So there is definitely v bar inside f bar, there is another v bar inside g bar, then there will be some additional factors in f and some additional factors in g and then there were these other additional factors.

So I do not care about all those. So I have many more factors maybe, but what I care about is that the right hand side has v bar squared, followed by some other polynomials. Now, why is that a contradiction? Well observe that the left hand side is the polynomial x to the n minus 1 in f p of x. So there is now one identity in f p. This is v bar squared into other terms. This means that the left hand side has a repeated root.

(Refer Slide Time: 19:34)



repeated root in some extn ie $x^n-1 \in \mathbb{F}_p[x]$ is not separable. This is a contradiction since x^n-1 is separable in $\mathbb{F}_p[x]$.

$h(x) = x^n-1$ in $\mathbb{F}_p[x]$

$h'(x) = nx^{n-1} \neq 0$ $\quad p \nmid n$

h and h' have no common factors

ie $\gcd(h, h') = 1$

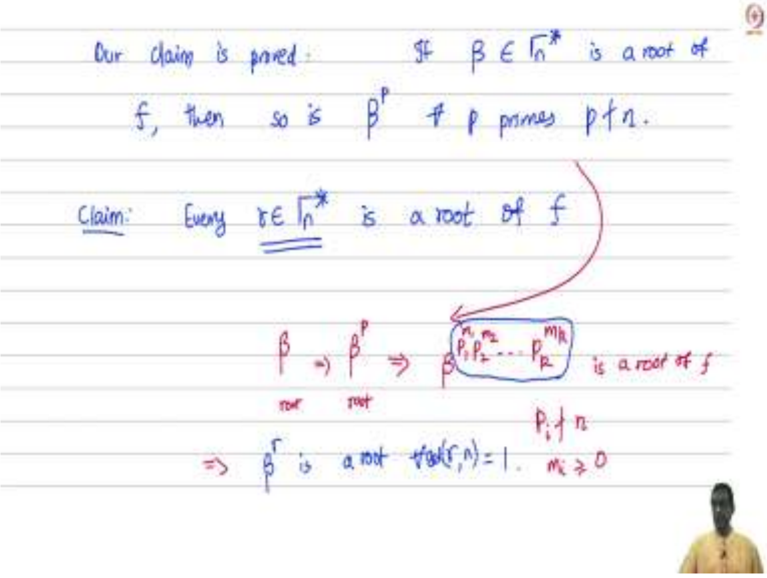
Because this is p bar squared. So this means that x to the n minus 1 has a repeated root in some extension. So it is not a separable polynomial. i e x to the n minus 1 thought of as an element of f p x is not separable. Why is that? Because there is a v bar square on the right hand side, so if you go to some extension in which v bar has a root, then that root will occur twice on the right hand side.

But this is a contradiction. Why? Because we can easily check that x to the n minus 1 is separable. This is a contradiction, since x to the n minus 1 is separable in f p x and how do we check it? Remember, we have the derivative criterion, let us check. So I just take this polynomial, it is called h of x to the n minus 1.

What is its the derivative? h prime or d h? Well, it is just n x to the n minus 1 and observe that p was chosen to be not dividing and so n x to the n minus 1 is not 0 here. Because p does not divide n. Therefore, n times something is not 0 in the field f p and observe that h and h prime do not have any common factor have no common factors.

In other words, the g c d is 1. Why is that? Because the only factors of h prime are powers of x themselves, I mean, it is just x power something. So the only thing that can possibly divide h prime is some power of x but powers of x do not divide h. So this has only 0 as a root and that definitely does not have 0. So, that that is the contradiction.

(Refer Slide Time: 21:54)



Our claim is proved: If $\beta \in \Gamma_n^*$ is a root of f, then so is β^p $\forall$ p primes $p \nmid n$.

Claim: Every $r \in \Gamma_n^*$ is a root of f

$$\underset{\text{root}}{\beta} \Rightarrow \underset{\text{root}}{\beta^p} \Rightarrow \beta^{\boxed{p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}}} \text{ is a root of } f$$

$p_i \nmid n$

$m_i \geq 0$

$\Rightarrow \beta^r$ is a root $\forall$ $\gcd(r, n) = 1$.

So that contradiction establishes the following claim. So, therefore our claim is establish; our claim is proved. What was our claim? Well, our claim was the following; that if beta is, so if some primitive root of unity nth root is, if this is the root of f, then so is any power, then so is beta power p for all p, primes not dividing n. Now, so that was our claim really. Now, it proves this claim.

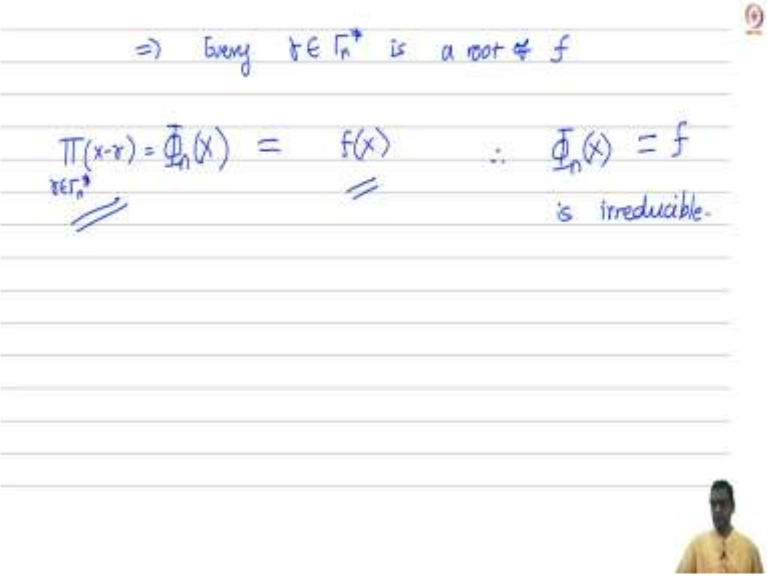
Now, from here one can conclude that in fact, every primitive root of unity must be a root of f. So, from this, we make a further claim. This means that every gamma, every gamma in gamma n star is a root of f and well, that is rather straightforward, because all you have to do is observe that from this, this claim that we have just shown, this says that you know, if beta is root, then beta power p for any prime p not dividing n is root.

But beta power p is a root so that power another prime is a root and so on. So, this is a root implies this is a root. Now, you keep iterating this, this tells you that anything of this form beta power p 1, p, p k is a root provided the p's do not divide and take primes which do not divide n and of course, you can repeat the prime so I can say p 1 to the m 1, p 2 to the m 2.

So, each of these is a root of f and this is for all in m i’s greater than or equal to 0. So I am just iterating my earlier claim. So what does that mean? In particular, it means, see look at these numbers on top, what are these? These are exactly how you construct. This is exactly how you construct numbers which are relatively, prime to n.

So those are just going to be powers products of, you know prime powers where the primes do not divide n. So this means that beta power r is a root for all integers r, which are relatively prime to n. so for all r such that the g c d of r and n is 1 but then recall that is exactly how you get every element of gamma n star.

(Refer Slide Time: 24:48)



$\Rightarrow$ Every $\gamma \in \Gamma_n^*$ is a root of f

$$\underline{\underline{\prod_{\gamma \in \Gamma_n^*} (x-\gamma)}} = \Phi_n(x) = \underline{\underline{f(x)}} \qquad \therefore \ \Phi_n(x) = f$$

is irreducible.

So, this means that every element gamma in gamma n star is a root of f. So what does that mean? It means that our original equation x to the, sorry this was phi n of x, we had this was the full product of x minus gammas, gamma and gamma n star. This was f of x into g of x into you know other terms and so on.

But what we just proved is that all these guys all these roots are all roots of f of x itself, which means that none of these other factors could have existed and everything is already a root of f of x. Therefore, it means that and remember f was irreducible. It was the first irreducible factor. Therefore, we have shown what we claim that phi n x is f and therefore is irreducible.