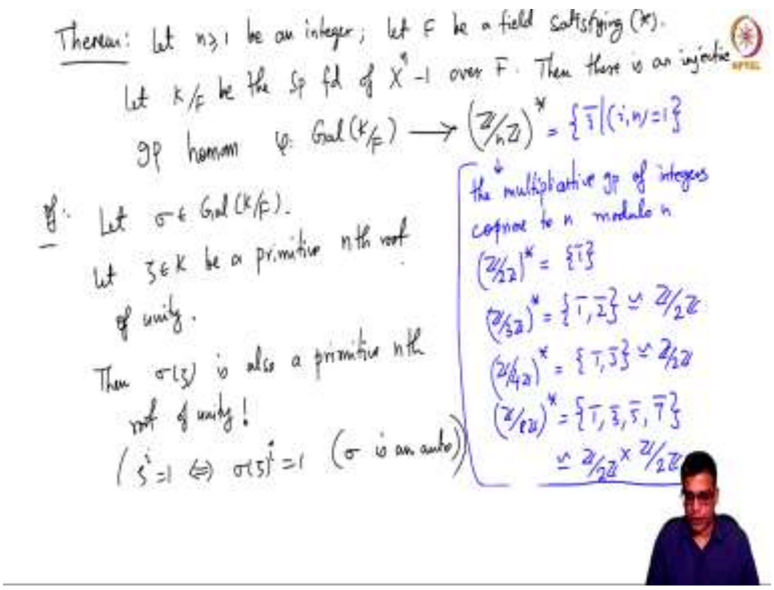
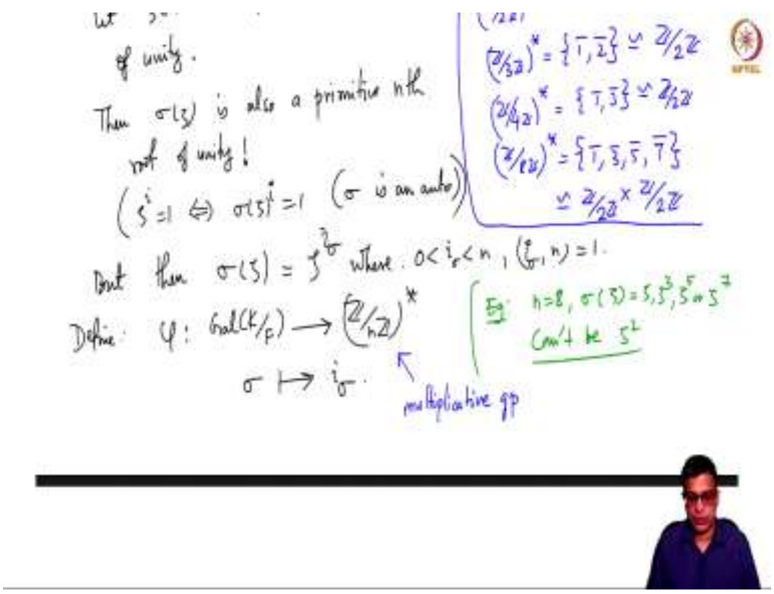
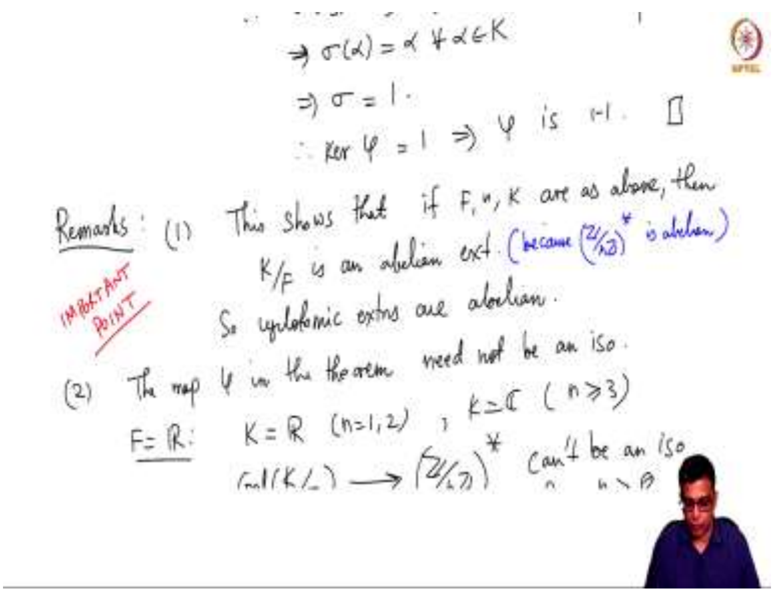
Introduction to Galoiss Theory
Professor Krishna Hanumanthu
Department Of Mathematics
Chennai Mathematical Institute
Lecture - 36
Cyclotomic Extensions – Part 2

Welcome back, in the last video we discussed cyclotomic extensions, which are extensions obtained by adding roots of unity, or roots of 1. In the main theorem, we proved in the last class is the following.

(Refer Slide Time: 00:27)







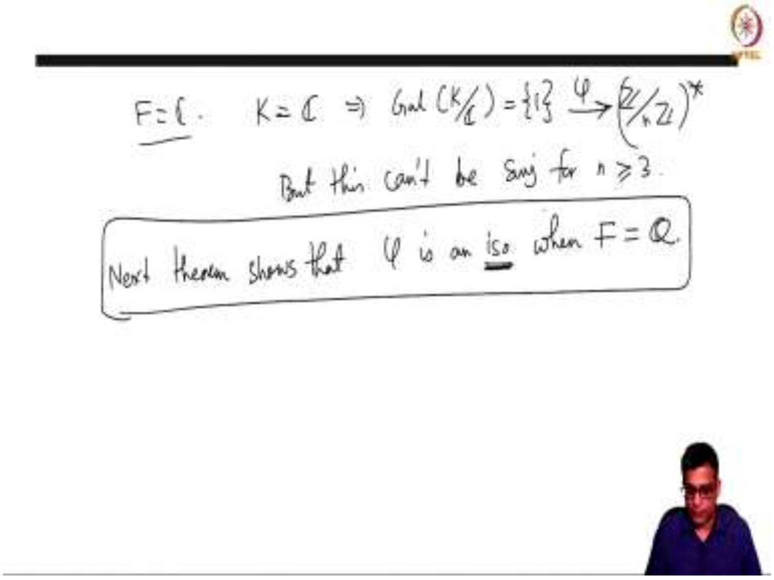
If you have an positive integer n and F is a field, satisfying star. Remember star is the condition that characteristic of F does not divide n, if the characteristic is positive or that characteristic is 0. So, that is a standard assumption for Homan and cyclotomic extensions. And then you take the splitting field of the polynomial X power n minus 1, that is to say that you have added the roots of unity, nth roots of unity to F.

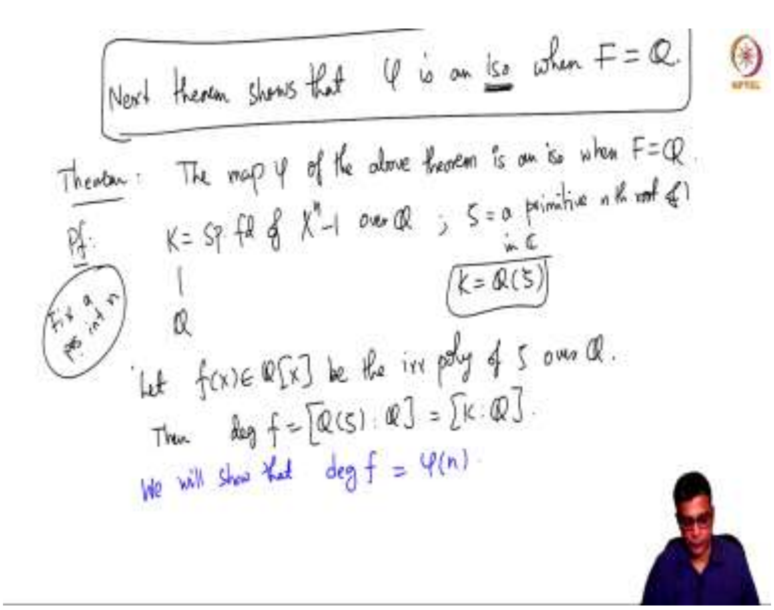
Then there is an injective group of homomorphism from the Galois group to the multiplicative group of integers modulo n. And as part of this, we constructed a specific homomorphism by observing that, if you take the Galois group, an element of the Galois group and you take a primitive nth root of unity; when you apply sigma to zeta you get zeta power a number that is co-prime to n.

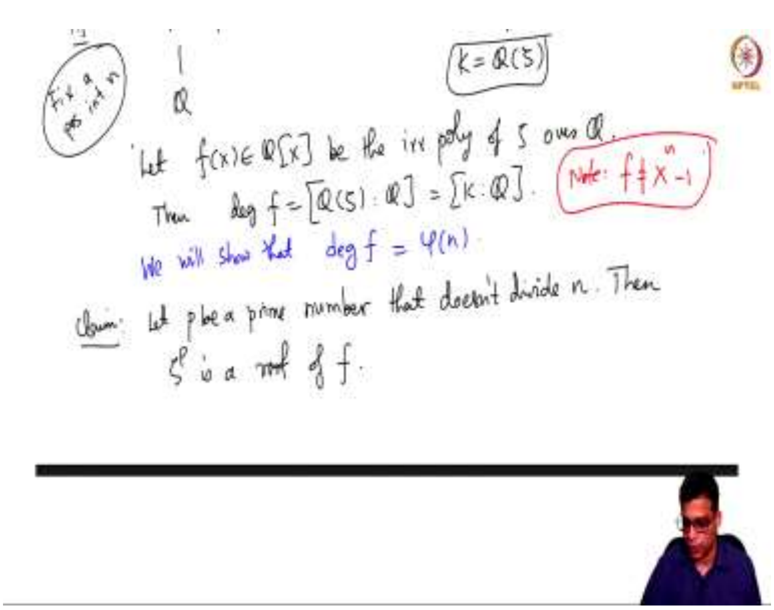
And then, it is easy to see that, that is a group homomorphism, and it is 1 1. And we ended the last class by saying that, in general this map is not surjective, it is only injective. In other it is not necessarily an isomorphism. As the example with F equal to R, or F equal to C, shows and we also commented this is important for us; that you cyclotomic extensions are abelian. So, this is an important point for us, that will come up later.

So it is abelian; because it is a Galois extension. That is obvious, because it is a splitting field of a separable polynomial. And, it is abelian, because it is Galois group, is isomorphic to a sub group of Z mod n Z star; which is to say it is abelian group.

(Refer Slide Time: 02:15)







So now, today we will prove that, the map phi is in fact isomorphism, when the base field is Q. The map phi of the above theorem is an isomorphism, when F is Q. Remember of course, Q satisfies the star hypothesis; because its characteristic is 0. So you have K equals splitting field of X power N minus 1, living over Q and what we do know is zeta is the primitive nth root of 1, let us have in C; so it is a complex number.

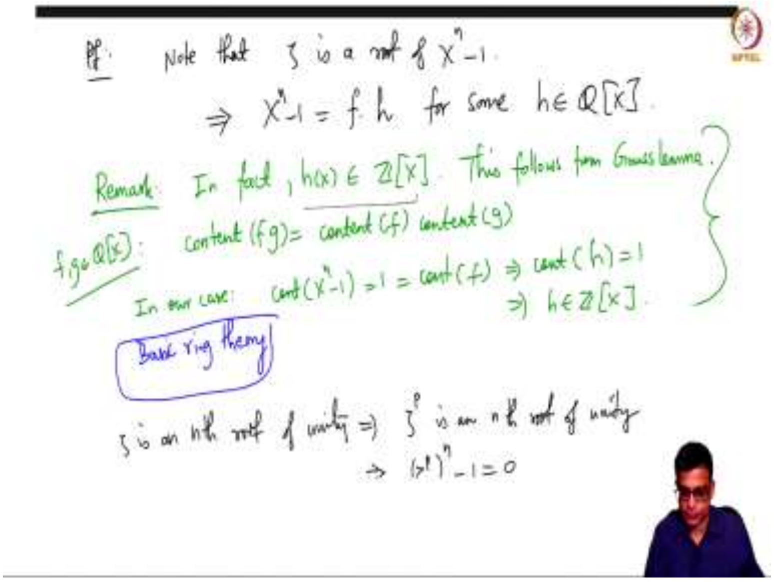
Then K is actually nothing but. Because I already showed that; in the previous video, we already showed that the roots of unity form a fixed nth roots of unity, form a cyclic sub group of C star in our situation. So, once you have a primitive 1, which is a generator of the cycle group, you have all of them. So, this is something to keep in mind. So, what are we going to do? We are going to do following.

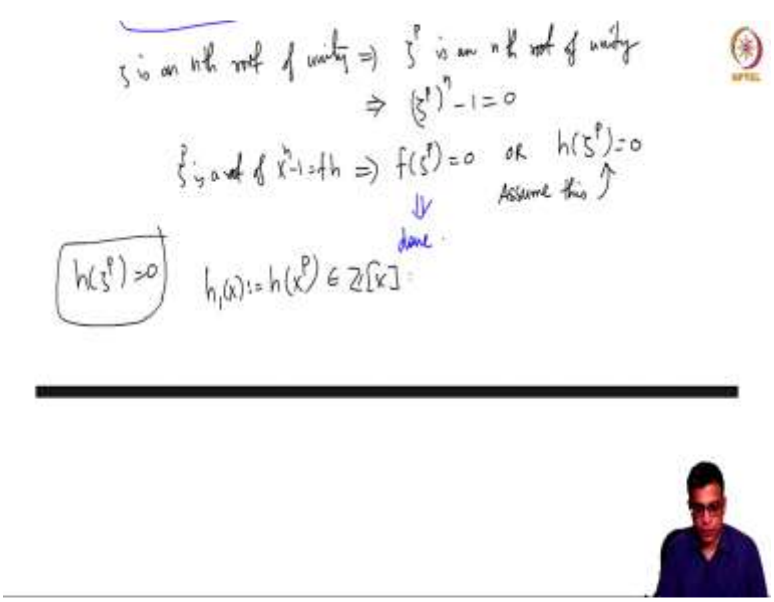
So, let us the irreducible polynomial of the primitive nth root of unity be F. Let, F be the irreducible polynomial of zeta over Q. So, this is a, so then, we know the degree of F is the degree of the extension by definition of the degree. But this is of course K colon Q; because K colon Q is F. So, basically what we will show is, we will show degree of F is phi n.

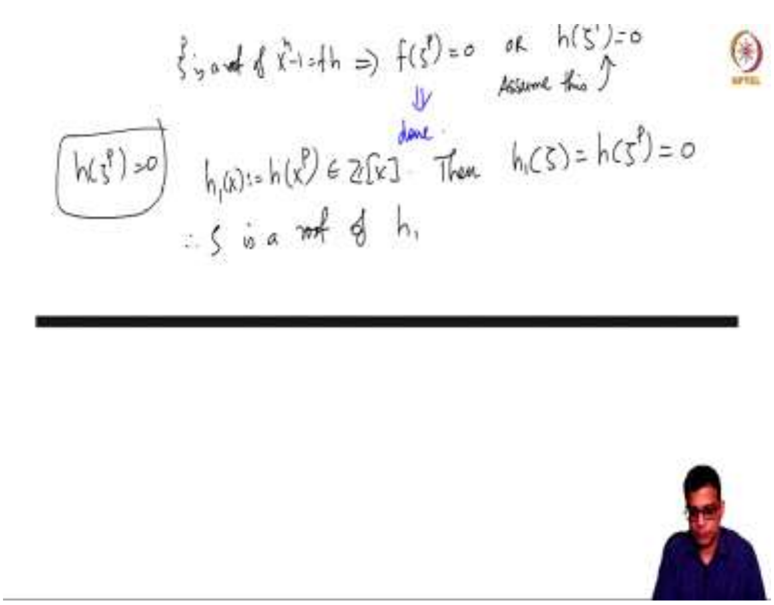
So by the way, I should remember here, that we are going to fix n. So fix an integer n. All this is after you fix a positive integer. If the degree is equal to the Euler Totient function, that is the degree of this extension. But this degree is the cardinality of the Galois group, which is less, which is a sub group of Z mod n Z star. But, hence if they are equal, then it is an isomorphism. So, I will explain this, when we come to it.

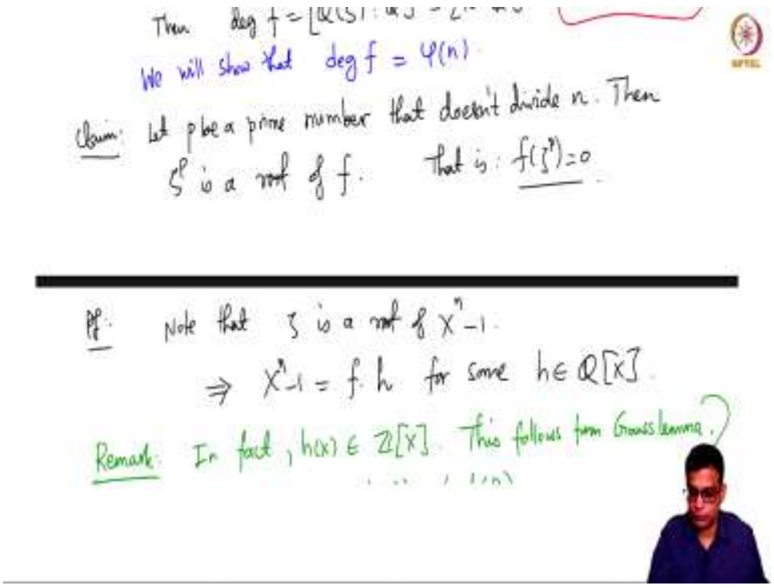
So, the claim, that I want to prove, which proves this statement for me, is the following. Let, p be a prime number. So it is a prime integer that does not divide n. Then I claim zeta power p is a root of f. Not that f is not X power n minus 1. I mean, that sometimes we use the notation f equal to X power n minus 1 maybe in the previous videos. But here, we want f. In fact, we do know that f cannot be equal to X power n minus 1. Because f is irreducible polynomial of zeta, X power n minus 1 is not an irreducible polynomial of over Q. So, it cannot be that.

(Refer Slide Time: 06:05)









So, what I want to show is that zeta power p is a root of f. So, why is this? Note that, first we note that, zeta is a root of X power n minus 1 of course, because it is a primitive nth root of unity. So, this means X power n minus 1 equals f times h for some h in Q X. Because, f is the irreducible polynomial of zeta, X power n minus 1 is some polynomial, which has zeta as a root, so f divides that in Q X.

But now, I want to make the following remark that in fact h of X is in Z X. So, because X power n minus 1 are integer polynomials, if f divides X power n minus 1 in Q X, it divides X power n minus 1 in Z X itself. So, this is a consequences of Gauss Lemma. So, there are several versions of Gauss Lemma. But one, that I will quote here, is content of; if f and g are 2 rational polynomials, content of f times g, is content of f times content of g.

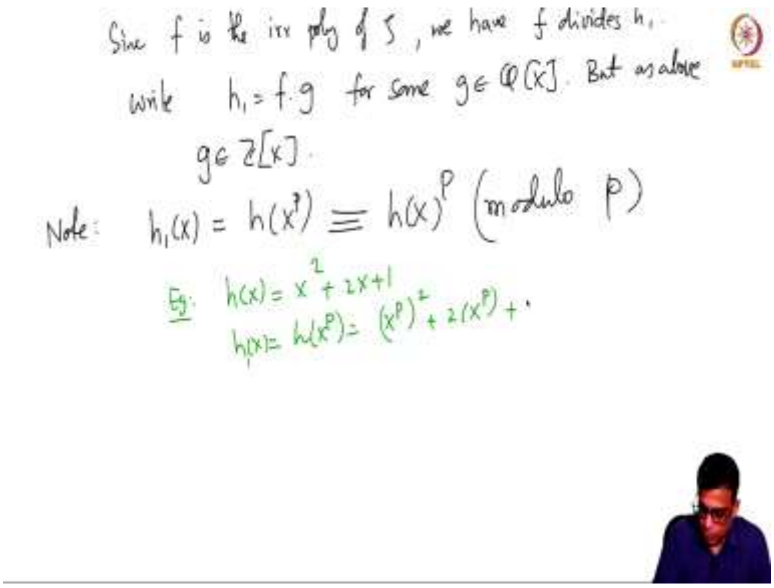
So, content is defined as, if it is an integer polynomial; it is the least, greatest common divisor of all the coefficients. If it is a rational polynomial, you first clear the denominators by multiplying an integer, you take the content of that, and then divide by that common denominator. And then, Gauss Lemma can be stated like this.

In our case, so content of, let us say, this is 1, but that is also content of f. Because f is a reducible polynomial, so it is in fact a monic polynomial. So this forces content of h to be 1, which forces in turn that h is in Z X. So, rational polynomial is defined our integers, if and only if its content is 1. So, this is a subtle point, so this is a basic ring theory here. When you learn about UFD's in ring theory, you learn this. So I am going to use that fact.

So, you have now, let us come back to this. So, you have X power n minus 1 equal to f times h. So, if zeta is an nth root of unity, implies zeta power n is an nth root of unity. So zeta power p, I want to write. Because the power of an nth root of unity is an nth root of unity. So that means. So, zeta is a root of, zeta power p is a root of X power n, which is f times h, but this means f of zeta p is 0, or h of zeta p is 0. In the claim, we are claiming that f of zeta p is 0. Suppose, this happens, we are done.

So suppose, this is not the case, so I assume that. So, we now assume h of, and we want to do some calculations and arrive at a contradiction. So, now if h is an integer polynomial, I can define a new integer polynomial like this. So, this of course is also an integer polynomial. h is some given polynomial integers, with integer coefficients, and I define a new polynomial, where I raise X to the p th power. So then, h 1 of zeta, which is by definition h of zeta power p is 0. So, that means zeta is a root of h1.

(Refer Slide Time: 10:54)



Since f ...

write $h_1 = f \cdot g$ for some $g \in \mathbb{Q}[x]$. But as above $g \in \mathbb{Z}[x]$.

Note: $h_1(x) = h(x^p) \equiv h(x)^p$ (modulo p)

$h_1(x) \neq h(x)^p$

Eg: $h(x) = x^2 + 2x + 1$

$h_1(x) = h(x^p) = (x^p)^2 + 2(x^p) + 1 = x^{2p} + 2x^p + 1$

$\mathbb{Z}[x] \to \mathbb{Z}/p\mathbb{Z}[x]$ $\quad h(x)^p = (x^2+2x+1)^p \equiv (x^2)^p + (2x)^p + 1 \pmod p$

$= (x^2)^p + 2x^p + 1 \pmod p$

$= h_1(x) \pmod p$

$\mathbb{Z}[x] \to \mathbb{Z}/p\mathbb{Z}[x]$ $\quad h(x)^p = (x^2+2x+1)^p \equiv (x^2)^p + (2x)^p + 1 \pmod p$

$= (x^2)^p + 2x^p + 1 \pmod p$

$= h_1(x) \pmod p$

this holds in $\mathbb{Z}/p\mathbb{Z}[x]$ $\leftarrow$ $\therefore$ $h(x)^p \equiv h_1(x) \equiv f(x)\, g(x)$ (modulo p)

Hence $f(x)$ and $h(x)$ have a common factor in $\mathbb{Z}/p\mathbb{Z}[X]$

this holds in $\mathbb{Z}/p\mathbb{Z}[x]$ $\leftarrow$ $\therefore$ $h(x)^p \equiv h_1(x) \equiv f(x)\, g(x)$ (modulo p)

Hence $f(x)$ and $h(x)$ have a common factor in $\mathbb{Z}/p\mathbb{Z}[X]$

UFD

$r(x)$: irr factor of $f(x) \Rightarrow r(x) \mid f(x)g(x)$

$\Rightarrow r(x) \mid h(x)^p$

$\Rightarrow r(x) \mid h(x)$ ✓

But f is a irreducible polynomial of zeta, since f is a irreducible polynomial, we have f divides h1. So, we can write h1 equals f times g for some g in Q X a priori. But as above, because f and h1 are integer polynomials, which are monic, because h1 is monic because h is, but as above g is in fact Z X. So now, let us see where we are.

So we have h1 X, which is by definition h of X power p. Now, this is a crucial statement I want to make here. So, this is the note. See, this of course is by definition, and this is because, if you go modulo Z mod p Z, and you take h power p. So, this is like an example here. If h X, let us say X square plus 2X plus 1, then h1 of X, which is h of X power p, which will be X power p square plus 2 times x power p plus 1. So, h1 is nothing but X power 2p plus 2X p plus 1. But, when you go modulo, these are all integer polynomials.

So, you can go modulo p, which is to say that, you look at the images of this under this. What is h X power p? This is X square plus 2X plus 1 whole p. But this modulo, because all the mixed terms will have coefficients divisible by p, they will vanish in z mod p Z. This is the kind of argument, that we have seen multiple times. I really should write 2X power p plus 1. But, this modulo p of course.

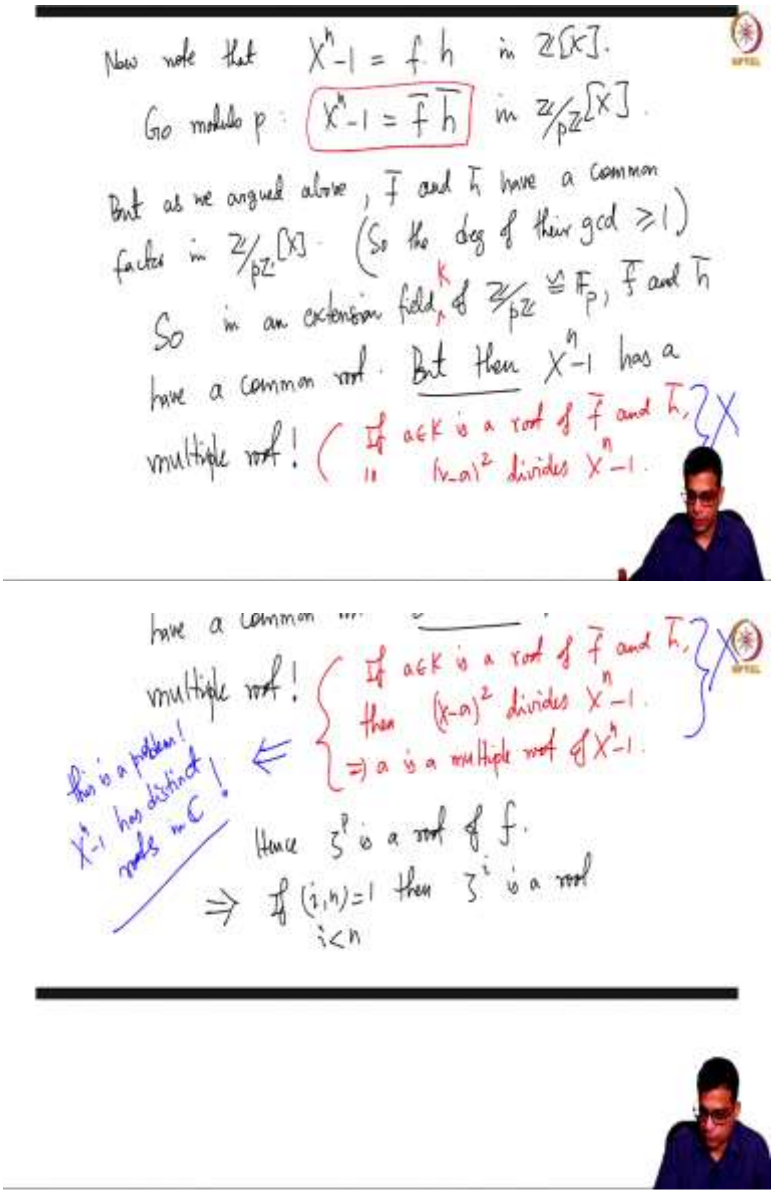
But this is X power 2p plus 2 power p is 2 again. Because in Z mod p Z anything power p is itself. This is of course, h1 of X. So, this is mod p mod p. Only mod p, otherwise of course, h power p is not equal to h1. So generally, is not equal to h X power p. On the note, it is not only modulo p it is, because this is a crucial argument here. So that means, now what do we have? So let us say, h X power p is equal to h1 X.

So, h X power p is congruent to h1 X, which is congruent to f X times g X modulo p. So, strictly speaking, we are taking the images of these things, all these equations, all these polynomials are living in Z X. We can take its image, their images in Z mod p Z X, and then this is what happens. This is to say, that hence f X and h X have a common factor in Z mod p Z X.

So basically, what I am saying is that, this equation here, if you replace with 3 horizontal bars with 2 horizontal bars and make it inequality, this holds in Z mod p Z X. That is the meaning of mod p. Now, this holds in Z mod p Z X. Now f Z mod p Z X is a UFD. So take any irreducible factor of f; let us say r X is an irreducible factor of f X.

Then r X divides f X times g x, and hence r X divides h X power p. Because, r X is an irreducible polynomial, and it divides the product, it divides h X. Remember, this vertical bar is division symbol for me. So this is all I am saying. So, r X is a common factor of f and h.

(Refer Slide Time: 15:58)



Now, what we have is, now note that X power n minus 1 is equal to f times h in Z X. This is something that, we had originally written, that X power n minus 1 is f times h in Z X. Now, go modulo p. In other words, take its images of this 3 polynomials in Z mod p Z X, because the modulo p map is a homomorphism.

What you have is, the image of this, which is of course this; which I do not want to write X bar, I will just write X n minus 1 is f bar h bar in Z mod p Z X. But now, we have a problem.

This, but as we argue about, f bar and h bar have a common factor. So, that is exactly the statement, f and h have a common factor in Z mod p Z X; that means their images have a common factor. But then, that means their gcd is, so the degree of their gcd is strictly greater than 0. So, that means the gcd is non constant polynomial.

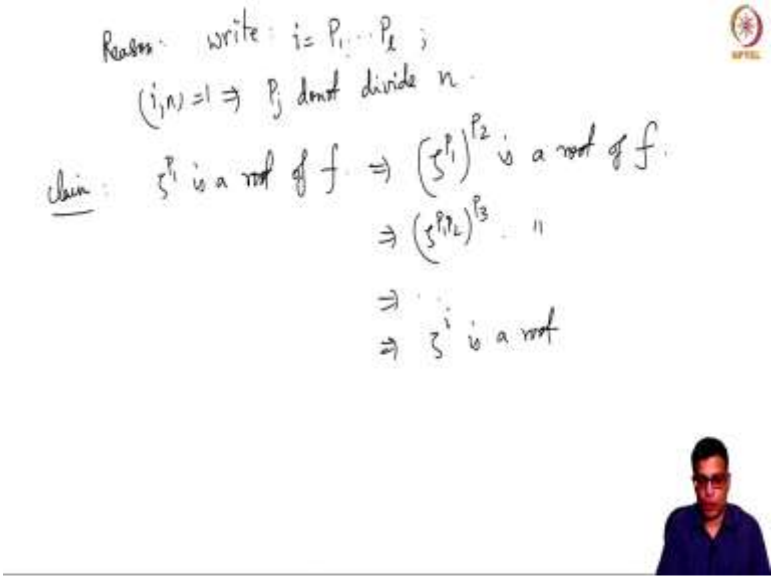
And when I discuss separability and we talked about multiple roots; we argued that if 2 polynomials have their gcd of positive degrees in their base field, and extension field they have a common root. So, in an extension field of Z mod p Z X, which of course is F p, f and h have a common root. But this is a crucial point. But then, X power n minus 1 has a multiple root. Because X power n minus 1 is f bar times h bar.

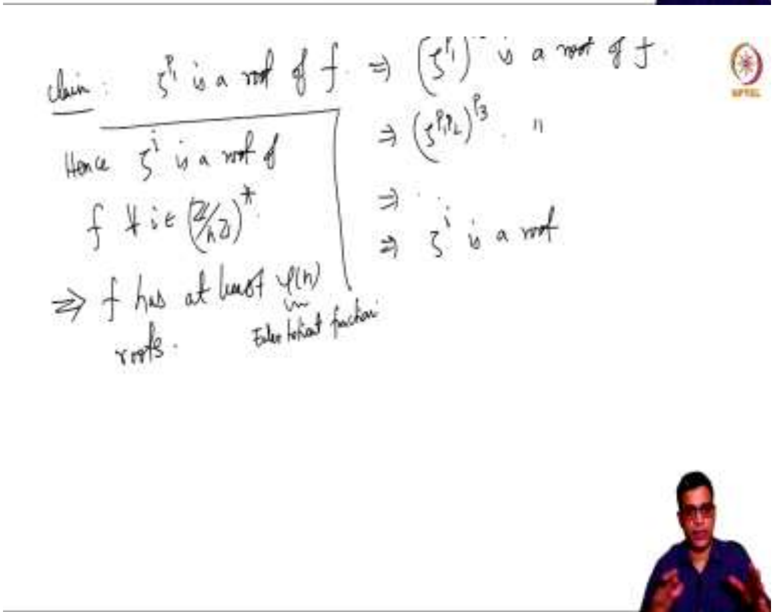
So if, let us say small a is of root f bar, as well as root of h bar; that means X minus a. So, if a; in some extension field K let us say. If a in K is a common root of f bar and h bar, then X minus a square divides X power n minus 1. Because X minus a divides f bar and it also divides h bar, so it appears twice in the factorisations. So, that means a is a multiple root, but that is a problem. Because why is this a problem?

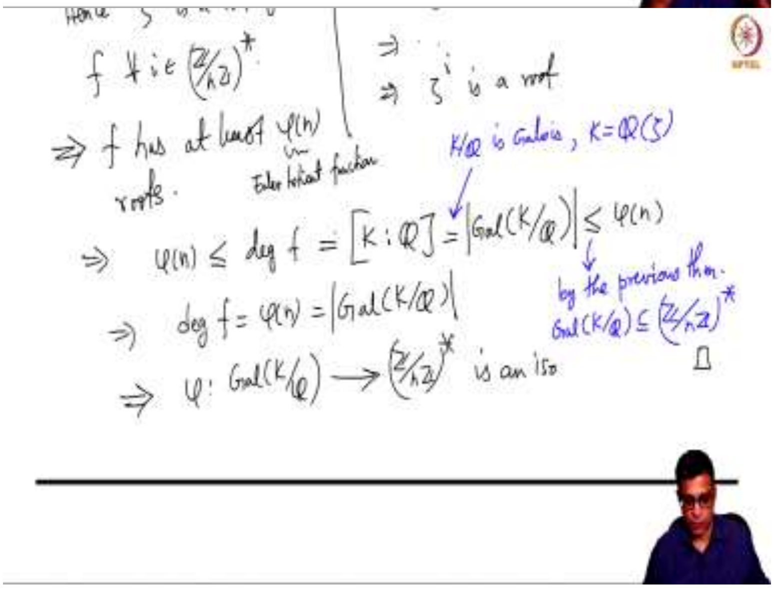
X power n minus 1 has distinct roots. We are in characteristic 0 now, so I will just say just C. It has distinct roots, it has n distinct roots, because there are n distinct, nth roots of unity. So that, this is not possible, that is to say that. So that is all we are done. With this claim, we proved this claim, because we assume that, zeta power p is not a root of f, and then h of zeta power p is 0, and that is where we went wrong.

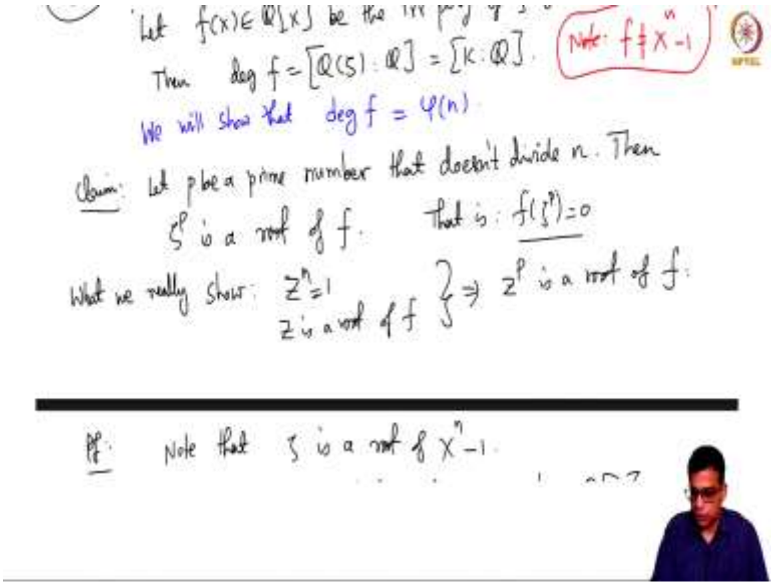
So, after that our analysis shows that we get a contradiction. Hence, is a root of f. Now, this is an immediate implication. Now we can show that, if i and n are co-prime and i is less than n; then zeta power i is a root of f. Why is this?

(Refer Slide Time: 20:34)









The, reason for this is, we write the prime factorization of i. Let us say, i equal to P1 through P l. So, since i and n are co-prime, this is their gcd is 1, implies P1 and P l do not divide n. But then, this implies zeta power P1 is a root of f. If zeta power P is a root of f, by the claim, this implies zeta power P1 P2 is root of f. Because if you go back to the proof, what we critically used, is that zeta is a primitive nth root of unity.

So, if zeta is a primitive nth root of unity, zeta power P1 is a primitive nth root of unity. So, its power, so, zeta is a root of unity, which is a root of f. Then the claim shows that zeta power P is a root of f. So, what we really show is that, I mean if any Z is a root of f, Z power n equal to 1, and Z is a root of f, implies Z power P is a root of f. That is exactly, what we have shown.

Because zeta is a root of X power n minus 1; because Z power n is 1. And then, it is a root of f; so then, the proof will go through. So if, zeta power P1 is a root, zeta power P1 power P2 is a root, which in turn implies zeta power P1 P2 is a root, so P3 is a root and like this. And finally, zeta power i is a root. Because i is a product through P1 to P l, we go one by one and conclude that zeta power i is a root.

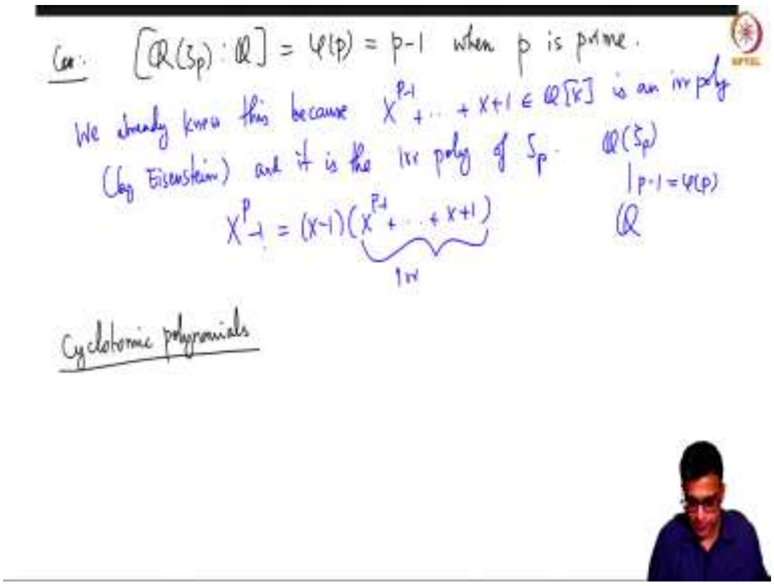
And hence, zeta i is a root of f, for all i in Z mod n Z star. Zeta power i is a root of f , for every i less than n co- prime to n, which is means that every in Z mod n Z star; which is to say f has at least phi n roots because Z mod n Z star has phi n elements. So, this is the Euler function. Everything in Z mod n Z star is an integer less than n. It comes from an integer less than n, which is co-prime to n. And for every such i. f zeta power i is a root, and they are all distinct of course.

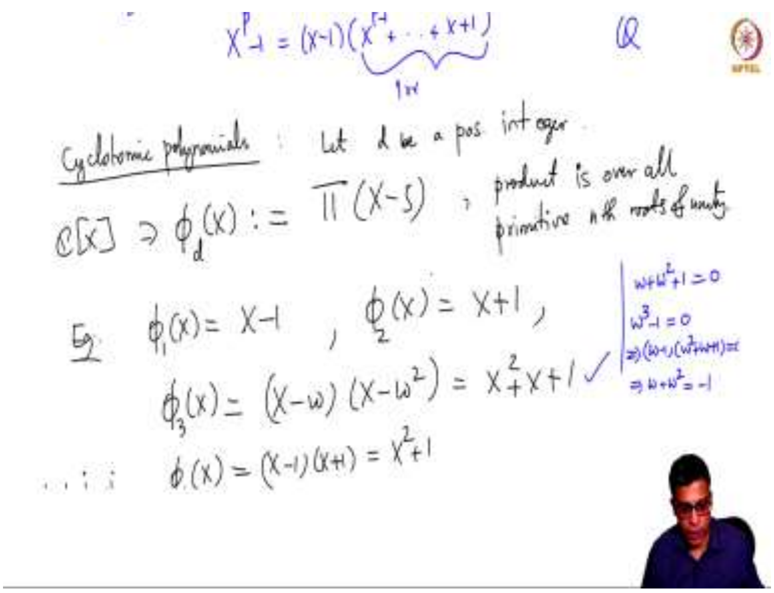
So, f n at least phi n root. This means phi n is less than equal to degree f, which is equal to K colon Q; which is equal to Galois K over Q , and this is because K over Q is Galois, and K is Q zeta. But now, this is less than phi n and this is because by the previous theorem, which I recalled at the beginning of today's video. We exhibited an injective map last time between Galois K over Q into Z mod n Z star.

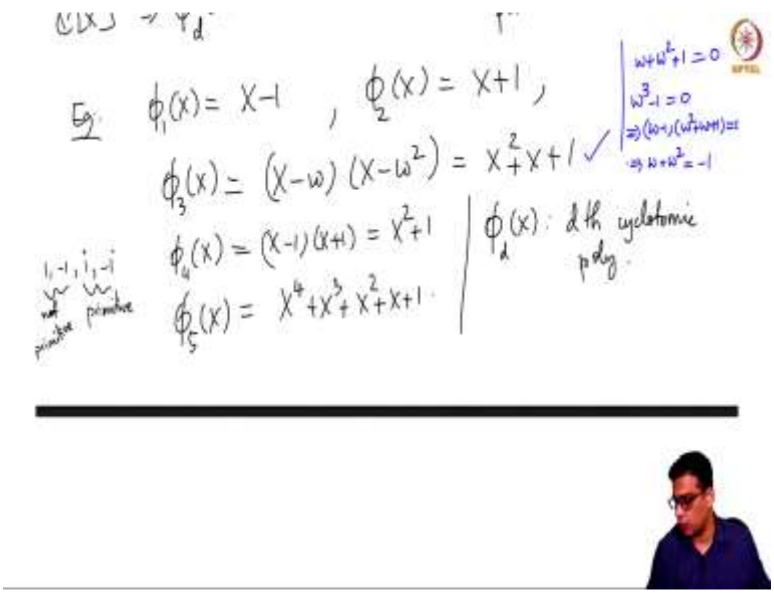
So, the order of this group is less than equal to order of this group, which is phi n. So now, we are done. So this means, all these numbers are equal. So degree f is phi n. So, this is to say that, which is also the order of the Galois groups, so I should put the bar here; order of the Galois group, but that means this is a sub group, but their orders are equal. So, phi from Galois K over Q to Z mod n Z star.

This particular map is an isomorphism. Because, this is an injective map between 2 groups, whose orders are two finite groups, whose orders are equal, so this must be isomorphism. So, that is all. This is, this shows that the Galois group of K over Q is Z mod n Z star. And as I remarked at the beginning, this is only true for space field Q. In general, this is not an isomorphism, for example, if you K to be R or C.

(Refer Slide Time: 25:44)







So as a corollary, what we know is that , when p is prime, the cyclotomic extension over Q, adjoin zeta pth root of unity, has to have degree p minus 1, but let me remark that, we already knew this because, X power p minus 1, X power p minus 2 plus X plus 1, is an irreducible polynomial, by Eisenstein criteria. And it is the irreducible polynomial if zeta p. Because zeta p satisfies this polynomial, which factors like this, and this is irreducible.

So in other words, when you take Q zeta p or Q this is p minus 1, which of course agrees with phi of p. However, for non-primes, it require more work to prove this, because the corresponding polynomial is clearly not irreducible and because n minus 1 is in general not the degree of the cyclotomic extension.

So, let me end this class, by quickly discussing how to go about finding the irreducible polynomials of nth roots of unity, where n is not prime, for n prime this is that. For n not prime we have to do the following work. So, I am going to define the following. So, let d be a positive integer, then define phi d of X.

So, these are all going to be rational polynomials, defined as follows. Phi d, it will be rational, we will show, phi d X is defined to be X minus zeta, product is over all primitive nth roots of unity. So apriori, this is a polynomial with complex coefficients. Before we proceed further, let me quickly give you an example. What is phi1?

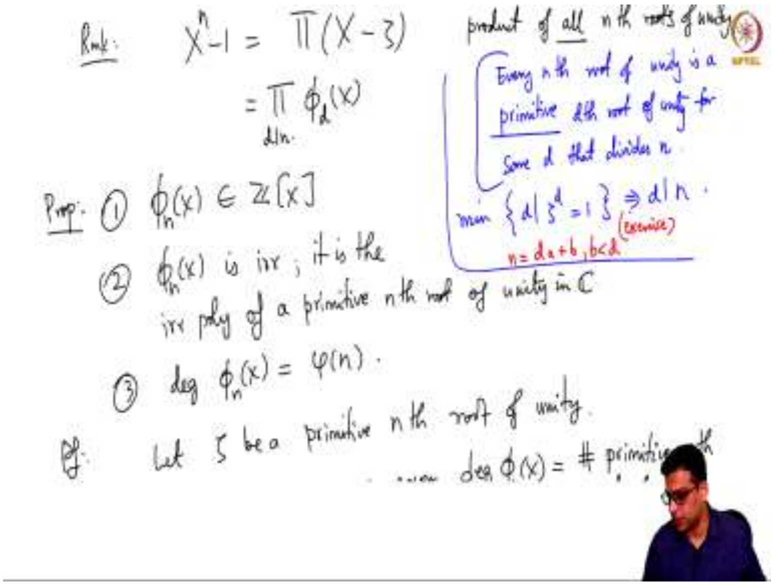
So, you take all primitive first roots of unity. So, that is just X minus 1. What is phi2? You take all primitive second roots of unity. There are 2 second roots of unity; 1 and minus 1; of which, only minus 1 is the primitive second root of unity. So, phi2 is X plus 1. What is phi3? Phi3 is product of primitive third roots of unity. So, there are 2 of them, omega and omega square. Remember, 1 is a third root of unity, but it is not primitive.

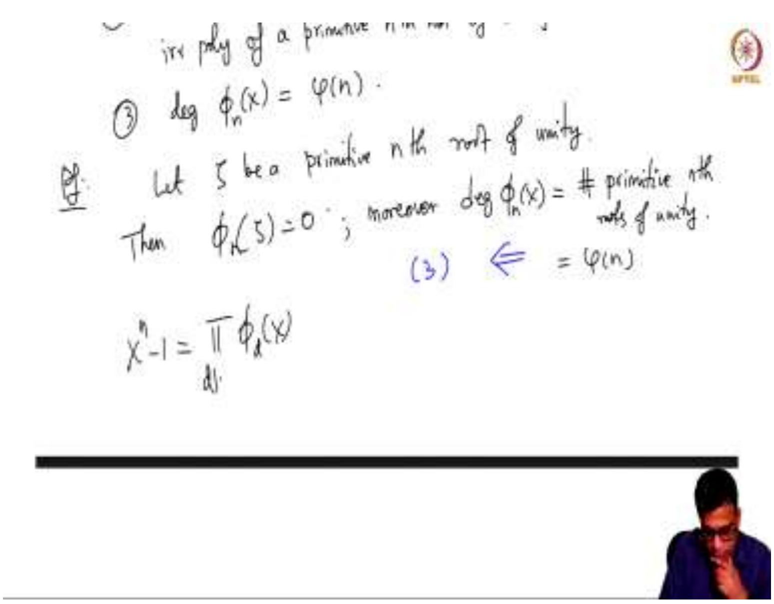
So, you have X times X minus omega times X minus omega square, and if you expand this out, you get 1, because omega plus omega square is 1. So, because roots of this is something that, I will write here, but you you know this because, in omega cubed minus 1 is zero; that means omega minus 1 times omega square plus omega plus 1 is 0.

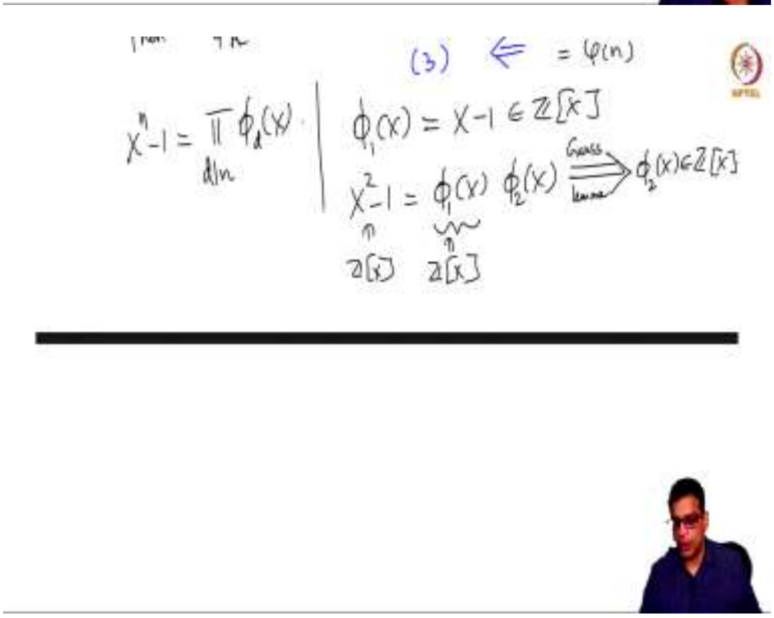
But omega is not 1, so this is 0. So this is exactly, this gives omega plus omega square is minus 1; that means that the roots, sum of the root is minus 1. So, the coefficient of X is minus of minus 1, and omega times omega square is 1. So, this is okay. So, this is the third cyclotomic polynomial. What is phi4? You have to look at fourth roots of unity, they are 1 minus 1 i minus i. But only, these are primitive, these are not primitive.

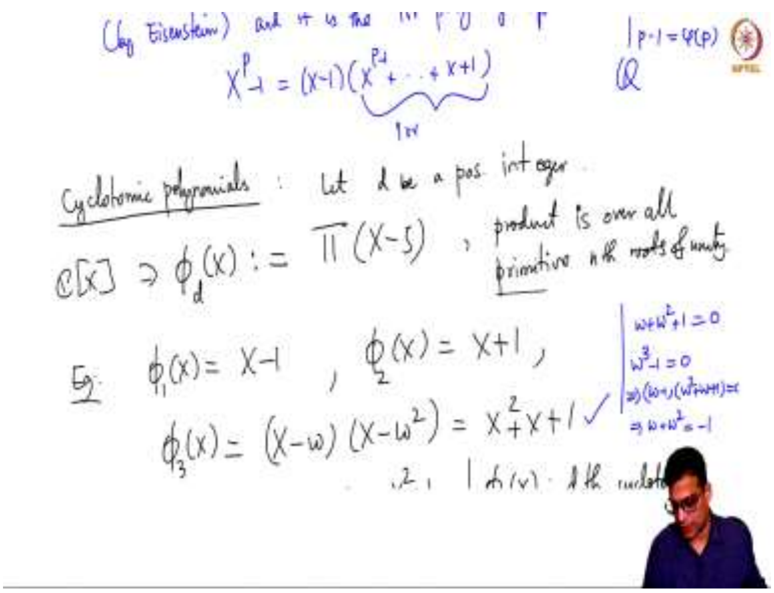
So, you get X minus 1 times X plus 1. So, the fourth cyclotomic polynomial is X square plus 1. And let me write one more example before we proceed, this actually happens to be just. So, these are called, this cyclotomic polynomial; phi d X is dth cyclotomic. And as you see in these examples, that are rational numbers. In fact, they are always, they are rational polynomials, and in fact, they are always rational polynomials.

(Refer Slide Time: 31:10)









First, I will remark that, this is an easy remark. If you take X power n minus 1, this product is X minus zeta; product over all nth roots of unity. You cannot simply take primitive nth roots of unity here, roots of this polynomial are all nth roots of unity. So, you take all nth roots of unity, but every nth root of unity is a primitive dth root of unity, for some d dividing n.

So, the point is every nth root of unity is a primitive dth root of unity for some d, that divides n because, you simply look at the least d. That d is something between 1 and n, for zeta equal to 1, you get 1. For a primitive nth root of unity, you get d equal to n. And then you, zeta will be by definition, a primitive dth root of unity. But because, the order of the group, consisting of all the, zeta is. So, this is a fact. So then, d divides n.

So, I will leave this as an exercise for you. Because if, it is not a divisor, you can write n equals to d a plus b, and then you play around with these equations; zeta power n is 1, zeta power d is 1. But then, zeta power b will be 1, which will violate this statement. So, the upshot of all this is that, these can be written simply as by grouping all nth roots of unity into primitive first roots of unity, primitive; all divisors of n, you group it into those primitive roots, you get simply the product phi d X.

Phi d, remember, is only contribution to phi d is primitive roots. So, you take, you group every nth root of unity in the appropriate primitive d th root, and then you take the product and you get this. So now this is easy. So simple proposition let me quickly do this proposition, and we will stop. So, then we are making some statements here, phi n X is a rational polynomial, phi n X is irreducible, it is the irreducible polynomial of a primitive nth root of unity. I am working exclusively over Q now.

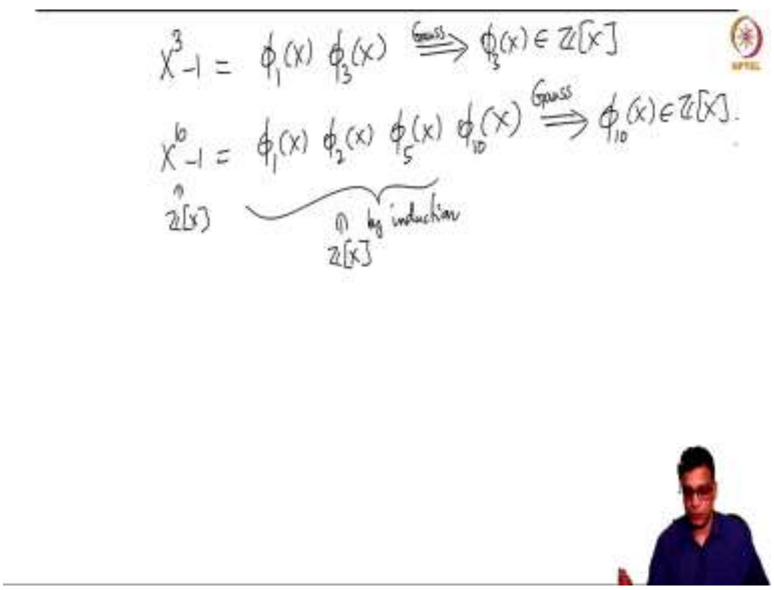
So, you take a primitive nth root of unity in complex numbers, and you take its irreducible polynomial that happens to be phi n and of course the third statement is that degree of phi n is the Euler Totient function, which is exactly the straight consequence of 2. So, let us prove this. So, we know that, so we know that, let zeta be a primitive nth root of unity. So, then certainly we know that phi n, alright because phi n is a product of X minus zeta for all primitive nth roots of unity. So, X minus zeta will be one of the factors. This is 0.

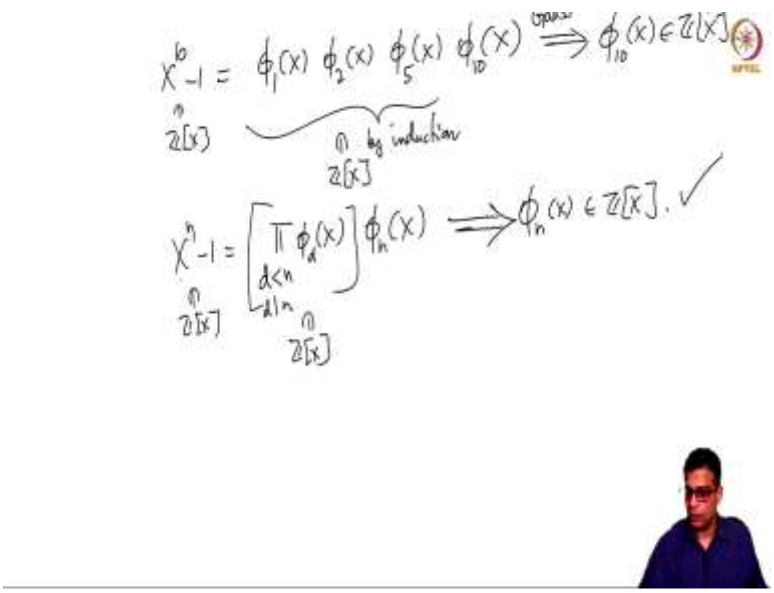
So, this implies, moreover what is the degree of phi n. This is the number of primitive nth roots. Again just look at the definition of phi n. It is product over all primitive nth roots. So, there will be as many factors as there are in primitive nth roots. So, that is the degree, and that of course is phi n. So, this gives, in fact this gives 3 first. So, this the degree is phi n.

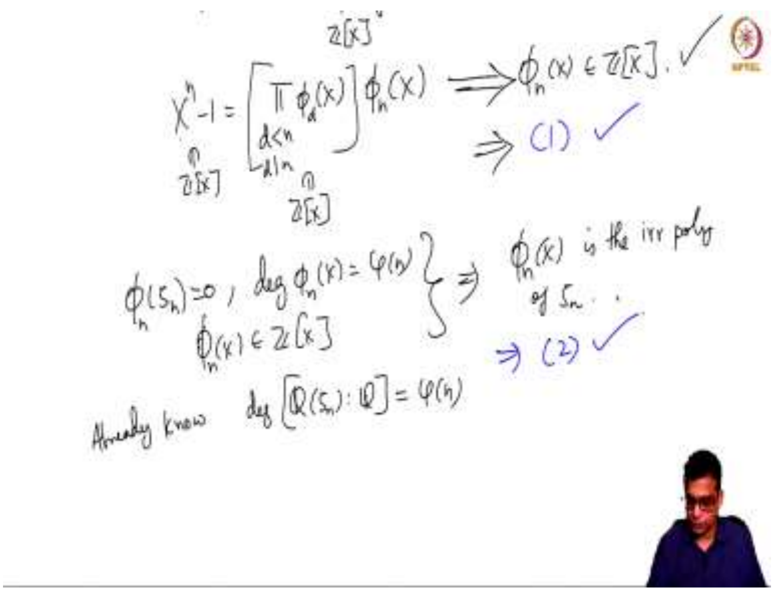
Now, I claim that, it is in Z X in fact. So, let me correct this, it is in fact an integer polynomial. So, why is that? So, note that X minus X power n minus 1 is product phi d, d dividing n. So, let us play around with this. We know phi1 is an integer polynomial, because this is X minus 1. But what is X square minus 1, this is phi 1 times phi 2.

This is in integer polynomial, monic integer polynomial. This is of course a monic integer polynomial. So, my Gauss Lemma phi2 X is an integer polynomial. Say of course I already know that phi2 X is an integer polynomial, but I am trying to set up an inductive argument here. So, phi2 is an integer polynomial.

(Refer Slide Time: 37:23)





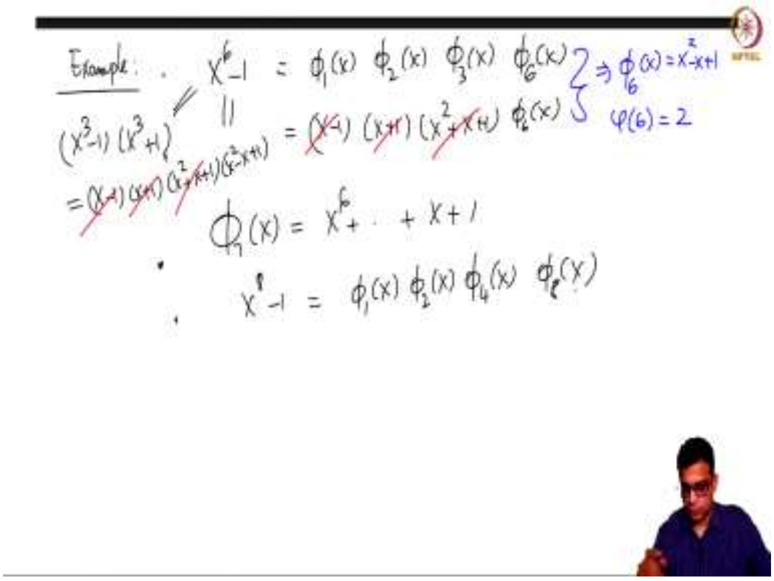


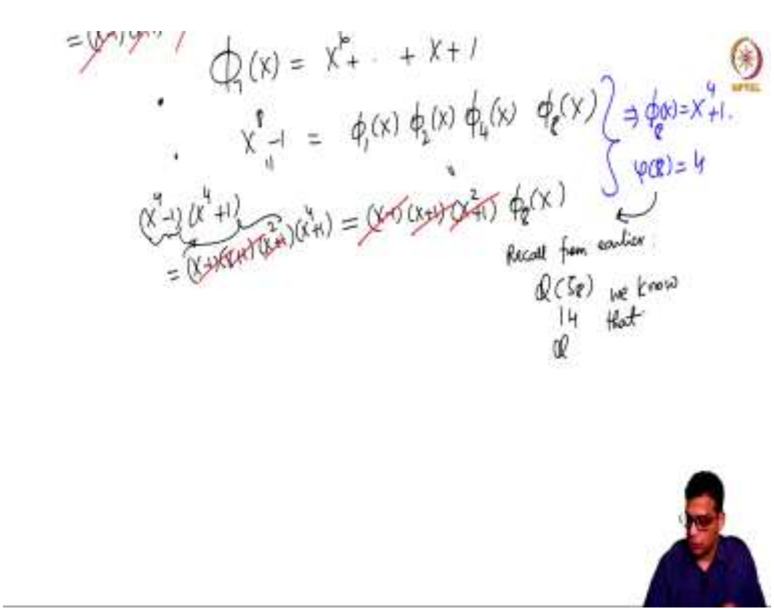
Now let us do X cube minus 1. So, this is phi1 X phi3 X, and as before Gauss Lemma, says that phi3 X is in integer polynomial. So, in general if you have x 10 minus 1, this is phi1 X, phi2 X, phi5 X, phi10 X. By induction, these are all in Z X, and hence this is in Z X of course, and by Gauss Lemma phi10 is in Z X. So, you understand the general argument. So, you write this. So, you write this is as product of phi d, d dividing n, but d strictly less than n, and then you have phi n separately.

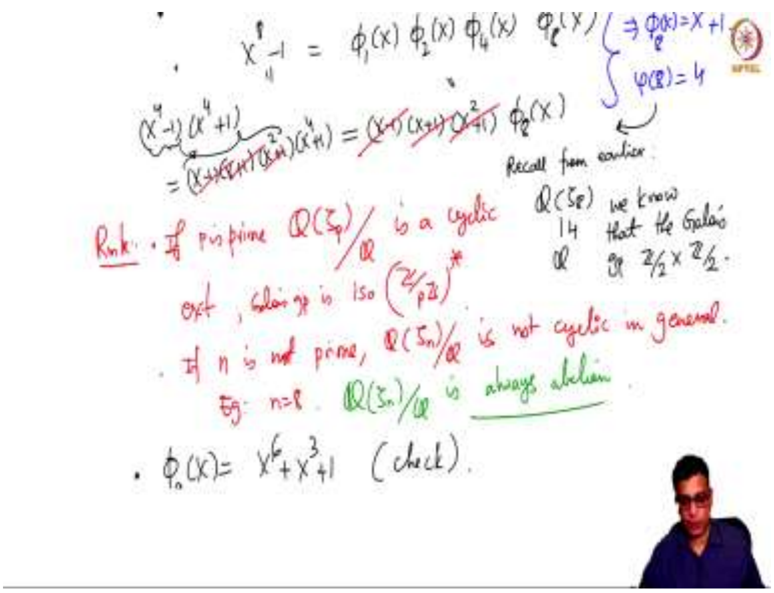
So, this is in Z X by induction hypothesis, and this is of course in Z X on the face of it. So, this means phi n X is in Z X. So, that is the statement 1. But now 1 and 3 imply 2 right? So, since phi n of zeta n is 0, degree phi n X is phi n, and phi n is in Z X better imply that phi n is the irreducible polynomial of zeta n. Zeta n is an irreducible, may be I should have called that a, zeta n is a primitive nth root of unity. It is degree is already phi n, we know.

We already know, degree of Q zeta n colon Q is phi n. So its reducible polynomial will have degree phi n. But here is an irreducible polynomial, here is a polynomial whose degree is the right number, because that is important, whose degree is right and it has zeta n as a root and it is a integer polynomial, all three together implies this. So this implies. So, this proves the proposition. So, this is a recursive method of constructing the irreducible polynomials of primitive nth roots of unity.

(Refer Slide Time: 40:09)







So, let me quickly do this example, and then we will dissolve this class. So, what is this example. So, let me just go ahead and compute some other cyclotomic. So, this is phi1 X, phi2 X, phi3 X, phi6 X. This sorry, this is not that. This is X power 6 minus 1. But this is X minus 1, this is X plus 1 this is X square plus X plus 1. So, now you can go ahead, and you can see that this phi6.

So, basically you can also separately write this as X cube minus 1 times X cube plus 1. This can be further written as X minus 1 X plus one. So, I have this here times X square plus X plus 1 times X square minus X plus 1. So, on the one hand this is equal to this, cause via this you can get this and that's also equal to this. So, now you can easily see, that you cancel this, you cancel this, you cancel this. So, the conclusion is phi 6 X is X squared minus X plus 1.

This confirms also the fact that the Euler Totient number for 6 is 2. So, you can factor this by familiar algebra rules, and then use the recursive definition to cancel out relevant things. Or you can directly divide, but its more direct this way. So, let me do two more examples. So X 7 minus, phi7 of course, there is not much to do, because for a prime number the cyclotomic polynomial is this. What about phi8? For that, let us factor X power 8 minus 1. It is phi1 X, phi2 X, phi4 X, phi8 X.

So, this is equal to X minus 1 X plus 1 X square plus 1 phi8 X. So, now of course you can multiply all this, and then divide X power 8 minus 1 by that product to get this. Another way is, you can factor this to X power 4 minus 1, X power 4 plus 1, which is X minus 1 X plus 1 X square plus 1 times X 4 plus one. So, this is equal to this. Now you can see that, you can cancel these 3 factors. So, the conclusion is phi8 of X is X power 4 plus 1, and this of course confirms that phi8 is 4.

But also, this you should recall from earlier, we worked out the the Galois theory of this extension before. The Galois group here, is in fact Z mod 2 cross Z mod 2. So, this is a good point to remark. If p is prime, is a cyclic extension, because this is, the Galois group is isomorphic to Z mod p Z star, which is a cyclic group of order p minus 1. But if n is not prime, Q zeta n over Q is not cyclic in general.

As this example shows, example n equal to 8. Here the order is 4, and the group is Z mod 2 cross Z mod 2. So, it is not a cyclic group. However, it is always abelian. This I already argued, any cyclotomic extension is abelian. So, the last thing I will write is, you do a similar kind of calculation to conclude that phi9 is x power 6 plus X cube plus 1. So, check this as an exercise.

So, the last point is not quite required for us when we do solution by radicals, but I thought it is a nice way to learn how to compute the cyclotomic polynomials which are the reducible polynomials of primitive nth roots of unity. So, in the last 1 or 2 videos what we did was, we learned about general cyclotomic extensions. For any field F, whose characteristic is 0 or it is, it does not divide n, we learned how to compute the cyclotomic extensions.

We showed that it is an abelian extension, it is Galois, and the Galois group is abelian by exhibiting an injection into Z mod n Z star. In general that injection is not an isomorphism. However, for base field equal to Q it is an isomorphism, and we proved that. And then we learned how to compute the cyclotomic extensions, how to compute the cyclotomic polynomials. Let me stop today here, in the next class we will start learning about solving polynomials by radicals. Thank you.