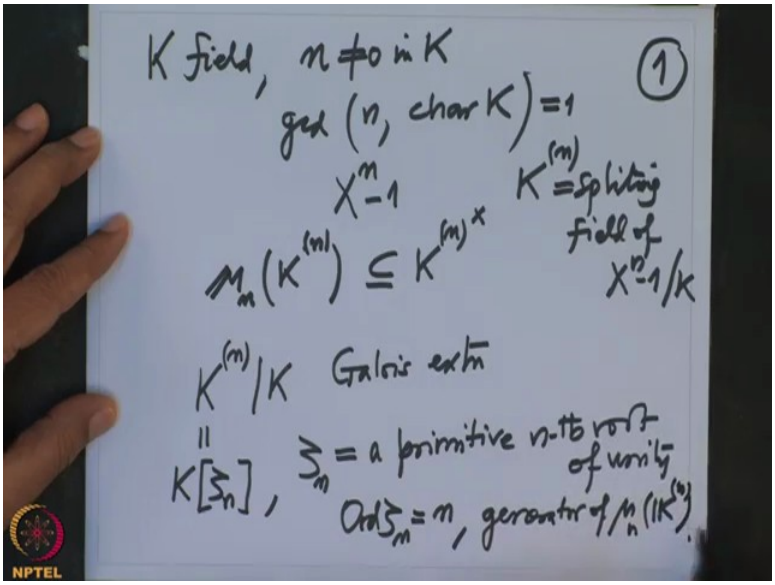
Galois' Theory.
Professor Dilip P. Patil.
Department of Mathematics.
Indian Institute of Science, Bangalore.
Lecture-36.
Irreducibility of Cyclotomic polynomials over Q.

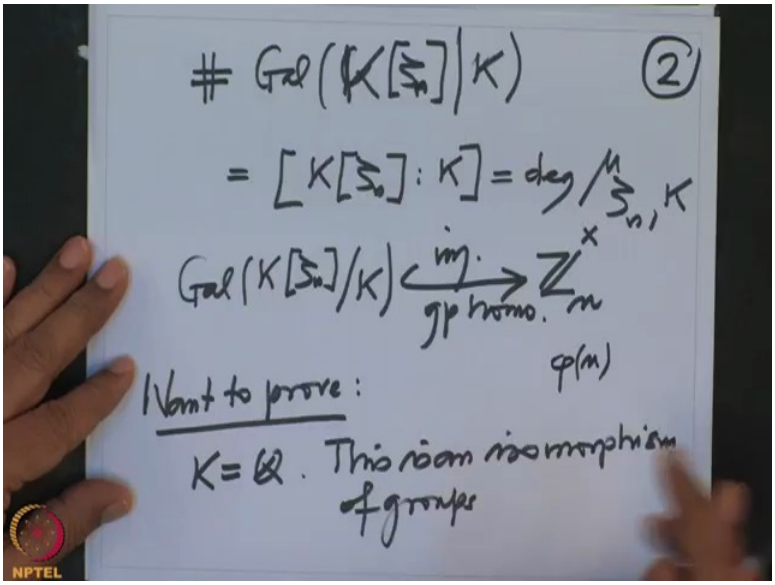
(Refer Slide Time: 0:47)



Recall that in the last couple of lectures, we have been studying special polynomial, namely $X^n - 1$, this is and therefore we are studying Cyclotomic field extensions. So the assumptions are K, if any field, and n was, remember that n is nonzero in K, that means characteristic of K and n, they are co-prime and then we have got an extension, will extension out of this, which is a splitting field of these polynomials.

And remember that $\mu_n\left(K^{(n)}\right)$, we found this $K^{(n)}$ is a splitting field of, splitting field of this polynomial, $X^n - 1$ over K and this is therefore a subgroup of this, which is a cyclic, which are cyclic because we know multiplicative subgroup of a field is cyclic. And we want to now prove, and what we want to compute now is the, we have noted that the field extension is a Galois extension and we have also noted that this field is, as K algebra, it is generated by ζ_n, where ζ_n is a primitive nth root of unity.

(Refer Slide Time: 3:29)

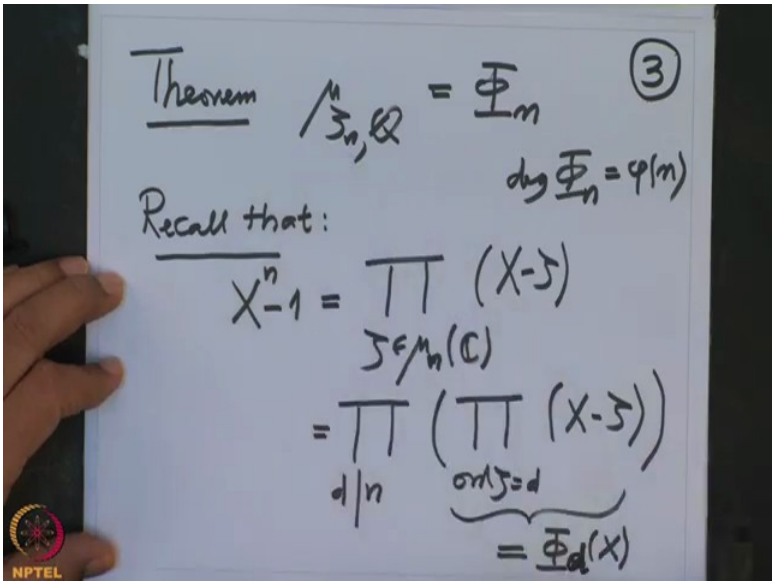


That simply means this is an element of order ζ_n equal to n, this group has order n and this ζ_n is a generator of this, of $\mu_{n,K^{(n)}}$. And what we have noted so far is that the Galois group of this field extension. So, we know the order of this Galois group. It is simple, so it is K adjoint with ζ_n over K, this is same thing as the degree of the field extension because we have checked it is a Galois extension. And what is more important is that n is nonzero in K and this is by degree of minimal polynomial of ζ_n over K.

We do not know what the minimal polynomial is but we approve that this Galois extension, Galois group, there is a canonical injection from this group to the group of units in the ring Z mod m. And this is true for arbitrary field K and this is injective group homeomorphism. And now we want to prove this is what we want to prove, we want to prove, in characteristic 0 case, that is K equal to K equal to $\mathbb{Q}$ case, this is an isomorphism, this is an isomorphism of groups. That is what we want to prove today.

And once you prove that, then we know the Galois group of this is precisely $\mathbb{Z}_n^x$. And we know the order of this group, so that will be $\phi(n)$ and therefore Galois group will have order $\phi(n)$. This is of order $\phi(n)$, ϕ is order Euler's totient function, so this is what we want to prove today. So, we want to find what is the minimal polynomial of ζ_n over $\mathbb{Q}$. So, we are in a characteristic zero case and we want to find minimal polynomial. So the theorem we are going to prove is the following.

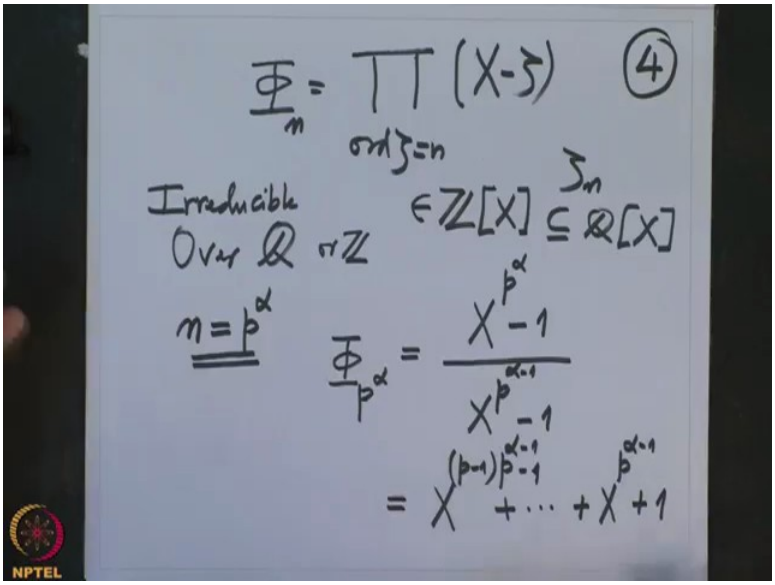
(Refer Slide Time: 5:39)



So theorem, recall that, I will recall, μ_{ζ_n} over $\mathbb{Q}$, this is nothing but $\phi(n)$. So recall that what is $\phi(n)$, and this is enough because we have noted that this, so recall, first let us recall. So from this polynomial $X^n - 1$, we have, this is the product $\zeta \in \mu_n$, if I write in $\mathbb{C}$ is also enough because all the roots are in $\mathbb{Q}^{(n)}$. So this is $X - \zeta$ and because this is cyclic of order n, this I have grouped together and I have written it like this, $d \vee n$ and then product order ζ equal to d $X - \zeta$.

In this we have called it $\phi(n)$. So this clear that the degree of $\phi(n)$ is the number of elements of order d in this perfectly group of order n. So therefore this is nothing but $\phi(n)$. So this is $\phi(n)$ and we are going to prove that this polynomial is precisely the minimal polynomial of ζ_n over K, remember that beta n is the primitive nth root and therefore the order of ζ_n is n. Therefore this is $\phi(n)$, so the number of elements of order n are precisely $\phi(n)$, ζ_n is one of them.

(Refer Slide Time: 7:48)



I notice $\Phi(n)$? $\Phi(n)$ is $\Phi(n)$ it is product order of ζ equal to n $X-\zeta$And ζ is one of the, one of the main ζ_n. ζ_n is one of the linear linear factors which will appear there. And we are interested in these polynomials and we want to prove that this is irreducible over $\mathbb{Q}$, that is what the association is. Alright, so to get a feeling, I am going to do first a particular case. So, first of all know that when I say irreducible over $\mathbb{Q}$, because this is a monic polynomial.

So we have also noted, remember last time we had noted that all these polynomials have coefficients in $\mathbb{Z}$. So there are indeed polynomials in $\mathbb{Z}[X]$ and this is containing $\mathbb{Q}[X]$. And because they are monic, irreducibility over $\mathbb{Q}$ or $\mathbb{Z}$, they are same of $\mathbb{Z}$, they are equivalent because of the Gauss' lemma, that because $\mathbb{Z}$ is a UFD and $\mathbb{Q}$ is a quotient field of $\mathbb{Z}$, so monic polynomial over $\mathbb{Z}$ is irreducible over $\mathbb{Q}$ if and only if it is irreducible over $\mathbb{Z}$. So we will prove that it is irreducible, okay, so, over $\mathbb{Z}$ and that will prove that it is irreducible over $\mathbb{Q}$ also.

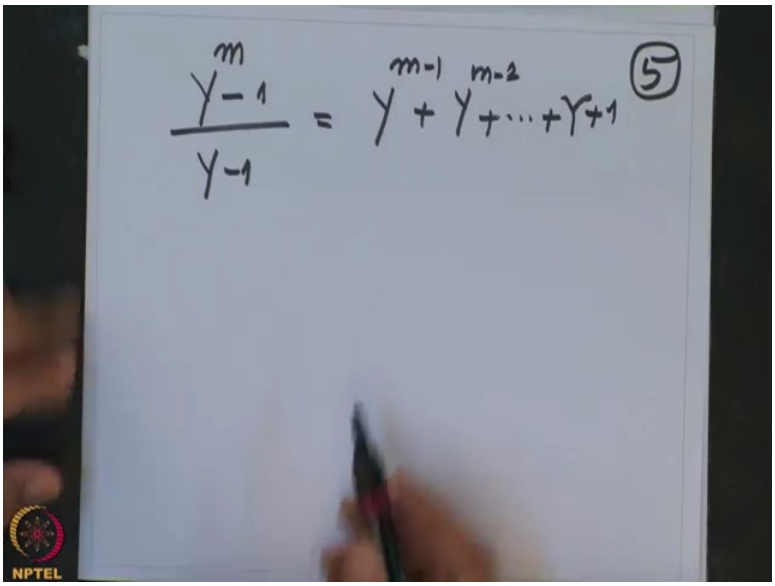
So okay, so for example I will prove this for when n is a power of prime. Suppose n is p^α. I want to do is for feeling and also to get understand what is going on. And that is how it was proved in the history also, first it was proved for n equal to power of a prime and then for arbitrary n. So we are also doing the same thing. So what is $\phi(p^\alpha)$? This polynomial is nothing but, we have to look at the polynomial $X^{p^\alpha}-1$ and divide by $X^{p^{\alpha-1}}-1$, this is this.

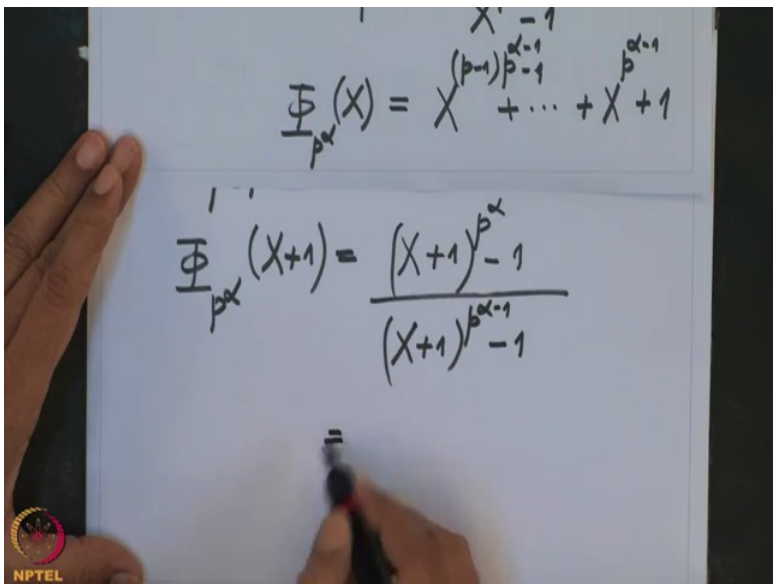
That is very easy to calculate because you see these are the, only one prime is involved, so the orders are either p^α or lesser power. And the lesser power when you group it together,

they will form these polynomials. So this is, this is clear. And now that means what, that means I want to cancel this factor here. So that means, this is nothing but $X^{(p-1)p^{\alpha-1}-1}$+...+ so on and so on + $X^{(p-1)p^{\alpha-1}-1}$+….

This follows from the fact that, you see, you call this $X^{p^{\alpha-1}}$ to be Y. So this is Y -1 and this is $Y^p - 1$. So we are in this, to write this we have used the following formula, which is well-known.

(Refer Slide Time: 11:41)



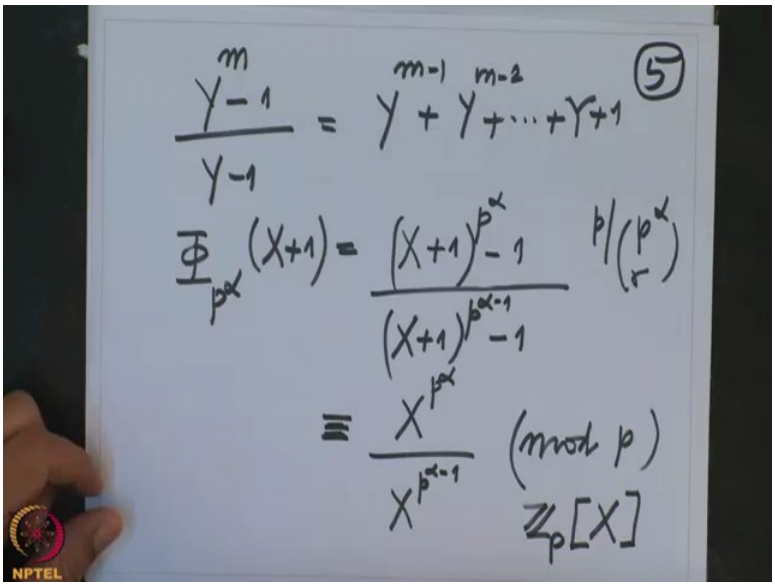


We have used that, if I have Y^m, $Y^m - 1$ divided by Y -1, this is nothing but $Y^{m-1} + Y^{m-2} + \ldots + Y + 1$. So that is why we have used. So that is the reason, so this is Y, so this is Y, this is Y and this is p -1 because this is Y^p and so on. So you have this, but then further,

now this one, this equation. So I want to write, this is $\Phi_{p^\alpha}(X)$, now in this equation, in this polynomial equation, Amway to put X equal to X +1, instead of X I am going to put X equal to X +1.

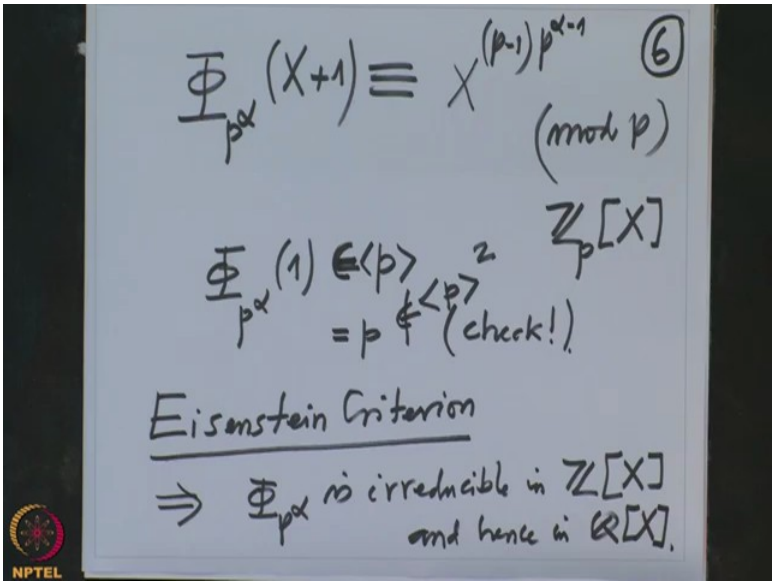
So what will I get, I will get $\Phi_{p^\alpha}(X+1)$ equal to, now instead of X I have to write X +1, so that will be or I could have done directly here. So that is nothing but $\frac{(X+1)^{p^\alpha}-1}{(X+1)^{p^{\alpha-1}}-1}$. But this is same thing as, I want to read, now when I expand these polynomials by binomial theorem and so the top degree term here will be X^{p^α}. And the constant will be 1, 1^{p^α} is one and this 1 will get cancelled.

(Refer Slide Time: 13:59)



In the middle terms will have coefficients divisible by p because they are binomial coefficients of this p^α. So the middle coefficients are p^α Choose r but all these guys are divisible by p. So when I read mod p, all the coefficients will vanish. So I am going to read mod p. And similarly the down polynomial, that will be $X^{p^\alpha}-1$, this is the only term will remain and instead of writing equality, I will then write congruent to mod p. That means, that means I am reading this in the ring $\mathbb{Z}_p[X]$. So, that is what will happen.

(Refer Slide Time: 14:47)



So we have this equation, I will read it once more. The equation we have is $\Phi_{p^\alpha}(X+1)$, this is congruent to, this is X, so this is X is power p^α , $X^{p^{\alpha-1}}$, which is, so cancelling the power we will get X power, so this will, p^α I will take it out, $p^{\alpha-1}$ I will take it out, so it is $(p-1)p^{\alpha-1}$ and this is mod p, mod p. So, now we are working in this ring that means, $\mathbb{Z}_p[X]$. So these 2 polynomials are equal in $\mathbb{Z}_p[X]$.

Therefore even after putting X equal to 0 they will be equal. So, what will be $\phi(1)$? So $\Phi_{p^\alpha}(1)$, this is equal to, this is equal to, X equal to 0, so this is equal to, this is equal to p, multiple of p. This is multiple of p, so because when I put X equal to 0, this side is 0, that means it is a multiple of p. But actually it is finding only that thing, it is a multiple of p, it belongs to ideal generated by p. Actually it is exactly equal to b, that I would just ask you to check, exactly equal to b.

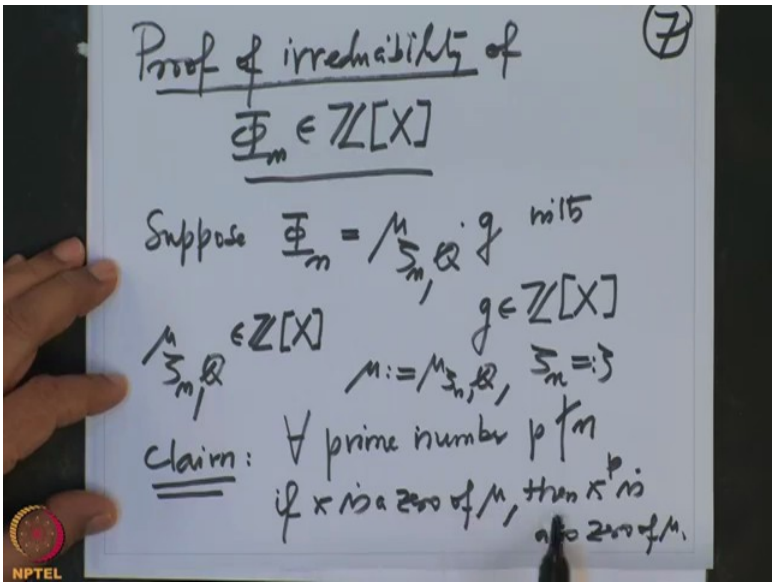
Now, why am I doing this, I want to use Eisenstein's criterion. So, remember here, so to prove $\Phi(X)$ is irreducible, phi p power Alpha is irreducible, we will prove that that the translated polynomial is irreducible. I will prove that $\Phi_{p^\alpha}(X+1)$ is irreducible, for that I need to use Eisenstein's criterion, for irreducibility of the polynomials in $\mathbb{Z}[X]$. So what we need to check, we need to check that that it is a morning polynomial, which it is. Also we need to check that the middle coefficients, they belong to the ideal generated by p.

And we need also to check that the constant term is not in p^2 . So this is a constant term, which is X is, at X equal to 0 it is p. So it is down the ideal generated by p^2 , so this is not

in ideal generated by p^2 , it is not a multiple of p. So I can apply the Eisenstein's criterion and conclude that, so implies Φ_{p^α} is irreducible in $\mathbb{Z}[X]$ and therefore $\mathbb{Q}[X]$ and hence in $\mathbb{Q}[X]$.

So, that proves it is irreducible for p^α. In fact I just want to make a historical comment here that in fact because of this Eisenstein's proof is the Eisenstein's criterion. Because to prove this p^α Cyclotomic polynomial is irreducible, Eisenstein's had discovered this Eisenstein's criterion. Now we will go to the general case. So, general case, we have this polynomial $\phi(n)$.

(Refer Slide Time: 19:13)

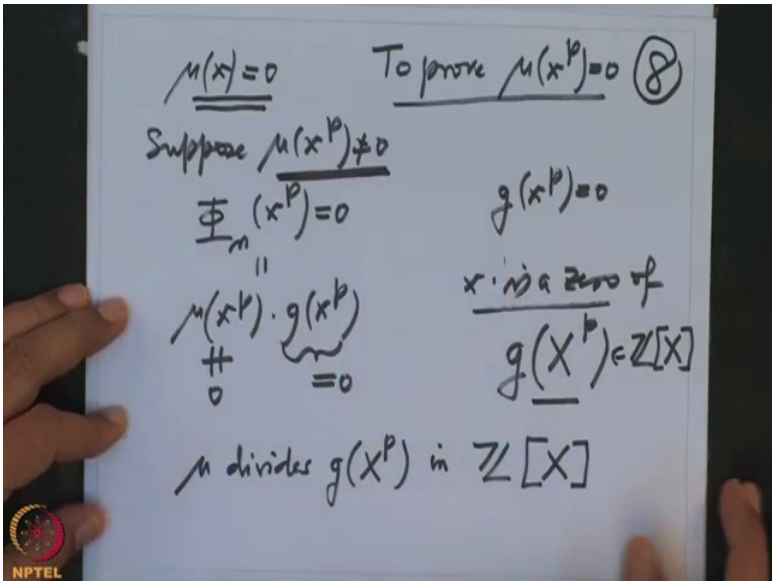


So proof of irreducibility of Φ_n in $\mathbb{Z}[X]$ in a general case. So suppose it is not, suppose Φ_n is not irreducible, that means Φ_n factors. But I know one of the, one of the root is ζ_n. One of the root is ζ_n, so one of the factors, irreducible factors of Φ_n will be μ_{ζ_n} over $\mathbb{Q}$. And the other factor I am calling it g, with g in $\mathbb{Z}[X]$ and μ_n , we know no $\mu_{n,\mathbb{Q}}$, this is actually a polynomial in $\mathbb{Z}[X]$, same thing. Because μ_n is a polynomial which is actually a priory over $\mathbb{Q}$, but μ_n is a divisor of this. And the division algorithm tells you this is actually in $\mathbb{Z}[X]$.

In any case it is like this and we want to get a contradiction, or we want to prove g equal to1, that is what we want to prove, all right. So I will claim, we claim that this is a claim I will prove 1st, that if I have any prime number p, for every prime p which is a divisor of n or not a divisor of n. And I will call, to satisfy the notation, I will simply call μ equal to μ_{ζ_n} over $\mathbb{Q}$

. And instead of keep writing ζ_n, I will write ζ_n equal to ξ . For every prime number p, I know that this, what am I claiming, for every prime number p which does not divide n, if x is a zero of μ , then x^p is also a zero of μ .

(Refer Slide Time: 22:22)



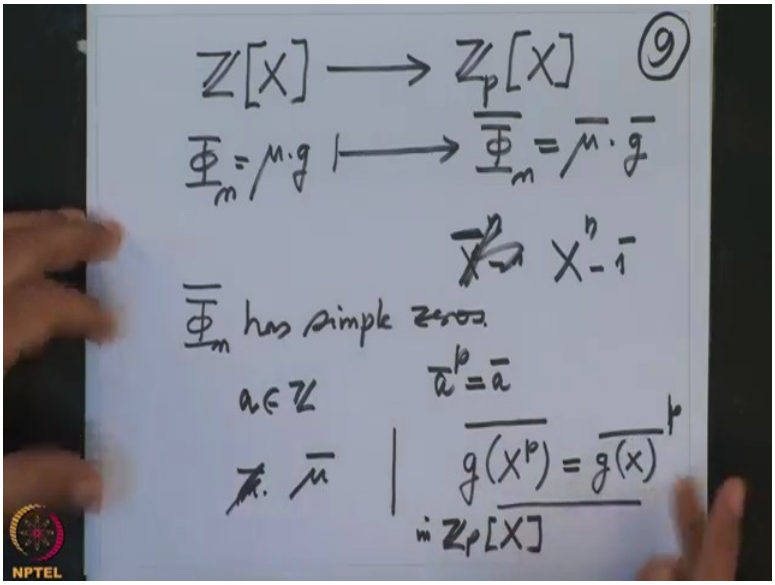
If x is a zero of μ , then x^p is also a zero of μ , this is what I want to prove. So, let us finish of this proof and then we will complete the prove, how does this imply that g equal to1. So x is a zero of μ and I want to prove, so this is to prove $\mu(x^p)$ is also zero. So suppose this is false, suppose this is false, suppose $\mu(x^p)$ is not zero. But then, but then x^p must be a zero of, we know, if x is a zero of μ , then it is a zero of Φ_n, then x power p is also a zero of Φ_n because $(x^p)^n$ is also one because x^n is one.

So therefore, in any case, we know that $\Phi_m(x^p)$ is zero. But this $\Phi_m(x^p)$, we have written it as a product of μ and g, so this is same thing as this, but this is not zero we are assuming, therefore this has to be zero. So, we know than $g(x^p)$ is zero. But that means this x is a zero of the polynomial g substituted instead of x, X^p . Because when I put capital X equal to small x, it is X^p , so X^p is a zero of this.

So that means, that means what? Here is a polynomial g, g is also in $\mathbb{Z}[X]$, so this polynomial is also in $\mathbb{Z}[X]$ and this polynomial when I put capital X equal to x, it becomes zero and μ is minimal polynomial. Therefore μ has to divide, μ divides $g(X^p)$ in $\mathbb{Z}[X]$, this is what we got, by assuming that x^p is not a zero of μ , all right. But now I am going to

read mod p. Remember we are proving the solution for prime numbers p which is not equal to, which is not, which does not divide n.

(Refer Slide Time: 24:53)



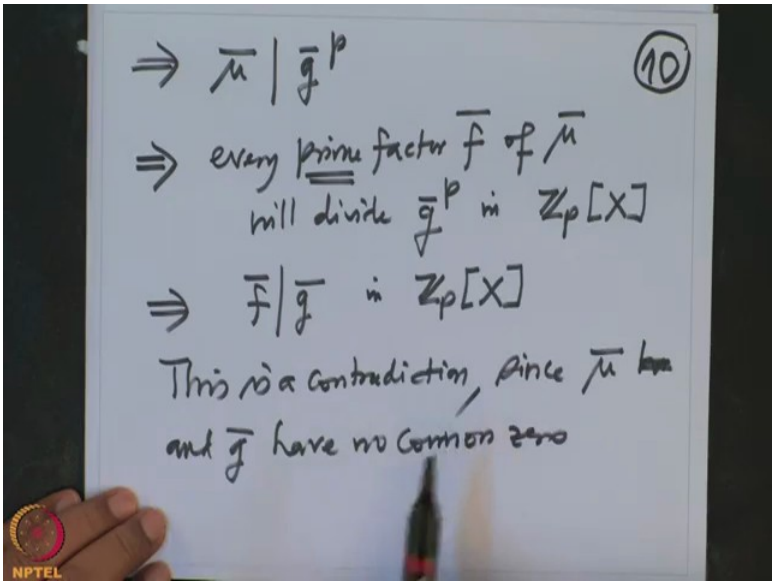
So we have, what we are doing is here, we have $\mathbb{Z}[X]$ here, then $\mathbb{Z}_p[X]$ is here, this is a natural map, when we are reading coefficients model p and there was Φ_n here, and that Φ_n we have written it as μg and that we go here Φ_n, which is $\overline{mu}\,\overline{g}$, where bar means reading coefficients mod p. Okay, first note that we know that the roots of Φ_n are distinct, that we noted because n is co-prime to the, because Φ_n is a factor of $X^n - 1$.

And $X^n - 1$ has distinct roots, so therefore Φ_n has distinct root and the same assertion carries over there because this p is co-prime to n, therefore this $\overline{\Phi_n}$ which is a divisor of $\overline{X^n}$, $X^n - 1$ bar, this polynomial also has a distinct root, because n, it is co-prime to the p also. So therefore Φ_n has distinct roots, therefore there is no root common between $\overline{\mu}$ and $\overline{g}$. And our contradiction, okay, so know that $\overline{\Phi_n}$ has simple zeros, simple zeros.

Okay, now what do you know what about $\mathbb{Z}_p$. Remember that if I have any integer a, then we know that $\overline{a}\,\overline{p}$ is mod p, $\overline{a}\,p$ equal to $\overline{a}$, because it is a group, it is a cyclic group of order p -1 and therefore it raised to p -1, a bar raised to p -1 will be zero, it will not be zero, it will be 1 identity. Therefore a bar power p equal to a. So that we got, therefore, when I now put in this equation, this is an equation in $\mathbb{Z}_p[X]$, so I am going to put in that equation, X, look at $g(X^p)$ and take the bar of this.

Now this power p, I claim this is same thing as $g(\overline{X^p})$, that p will, because characteristic is p. So when I write the equation and all the coefficients are, I can write as p powers and therefore I will take the bracket out, therefore it is this equation. Therefore when I read mod p, I have this equation, so therefore, look here, that because we noted that μ divides g of X p but, therefore $\bar{\mu}$ will divide this in $\mathbb{Z}_p[X]$ but that means this $\bar{\mu}$ will divide $\overline{g^p}$.

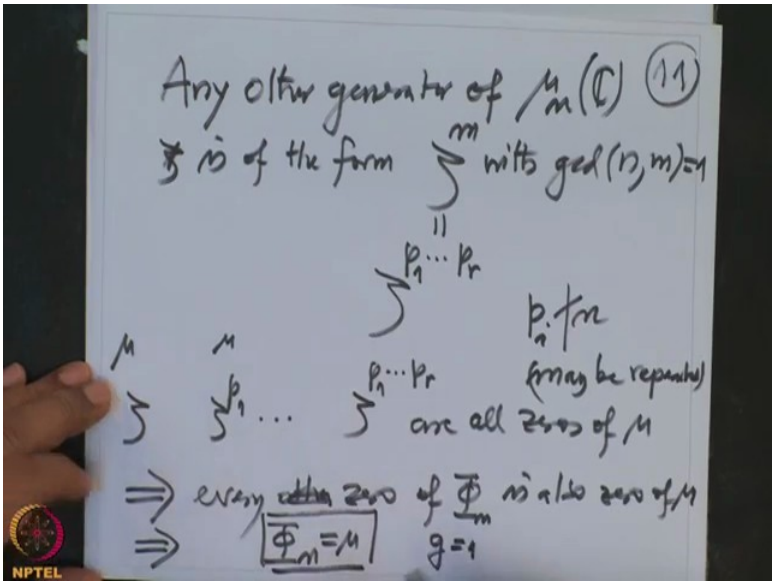
(Refer Slide Time: 28:24)



So that is $\bar{\mu}$ will divide $\overline{g^p}$. That will mean that, I do not know whether you bar is irreducible now because we have gone mod p, irreducibility might be disturbed. But then, but in any case, every prime factor f, $\overline{f(\bar{\mu})}$ has to divide, will divide $\overline{g^p}$ in $\mathbb{Z}_p[X]$. And because it is prime, therefore f bar will also divide $\bar{g}$ in the $\mathbb{Z}_p[X]$. But then, that contradicts because we know, we have proved that μ and g do not have any common root, so this is a contradiction.

This is a contradiction, since $\bar{\mu}$ and $\bar{g}$ have no common zero. Because this $\bar{f}$ is a factor of μ , therefore you take the zero of $\bar{f}$, that is the zero of μ and we have proved that this $\bar{f}$ but divides $\bar{g}$, so $\bar{g}$ will also be the zero of, the zero of $\bar{f}$ will also be a zero of $\bar{g}$. So that is not possible, therefore we get a contradiction, therefore what we proved is, if X is a zero of, we have proved our claim, I will just show you the claim. If X is a zero of μ , then next power p is also a zero of μ , all right.

(Refer Slide Time: 30:46)



Now therefore and remember now, only the last part, that is, so I want to apply this to the following. Now, we know any primitive roots, any other generator, any other generator of $\mu_{n,\mathbb{C}}$, ζ is one of them we have written. So if you take any other, it will be power of ζ and which power, that should be co-prime to n. Any other generator of this is of the form ζ^m with GCD of n and m 1. And they are all roots, they are precisely all roots of Φ_n.

So therefore this ζ^m looks like a $\zeta^{p_1,\ldots,p_r}$ where p_1 to p_r maybe repeated, where p_i 's are prime factors of m and m is co-prime to n, so therefore this pi's do not divide n. And maybe repeated it may be repeated, but that does not matter. So what did we prove, if ζ , we know ζ is a root of μ , then ζ^{p_1} will also be root of μ , this is what we proved, this is also zero of μ . Then successively doing this, ζ^{p_1} ,..., ζ^{p_r} , they are all zeros of, are all zeros of μ .

So, that means every other element of, every other generator of this group is also zero of that. But that means every other root, every other, every zero of Φ_n is also zero of μ . So that means, but there was a factor of Φ_n, so there is no other way because the degree argument will tell you that Φ_n has to be μ and that means g is 1. This is what I wanted to prove, we wanted to prove this. So that completes the proof that Φ_n is irreducible over Z and therefore irreducible over $\mathbb{Q}$ and therefore the Galois group of $\mathbb{Q}^{(n)}$ over $\mathbb{Q}$ is nothing but $\mathbb{Z}_n^x$.

After the break I will make some more comments about this Galois group where the characteristic is not zero now. And this case will be different from the characteristic zero case

because essentially because the finite field, the Frobenius map is a generator for the Galois group and therefore Galois group is cyclic and this will make a difference in the argument. So we will continue after the break.