Galois' Theory
Professor Dilip P. Patil
Department of Mathematics
Indian Institute of Science Bangalore
Lecture No 38
Minimal Polynomials

(Refer Slide Time 00:25)

Recall that last time we have proved that the Galois' groups

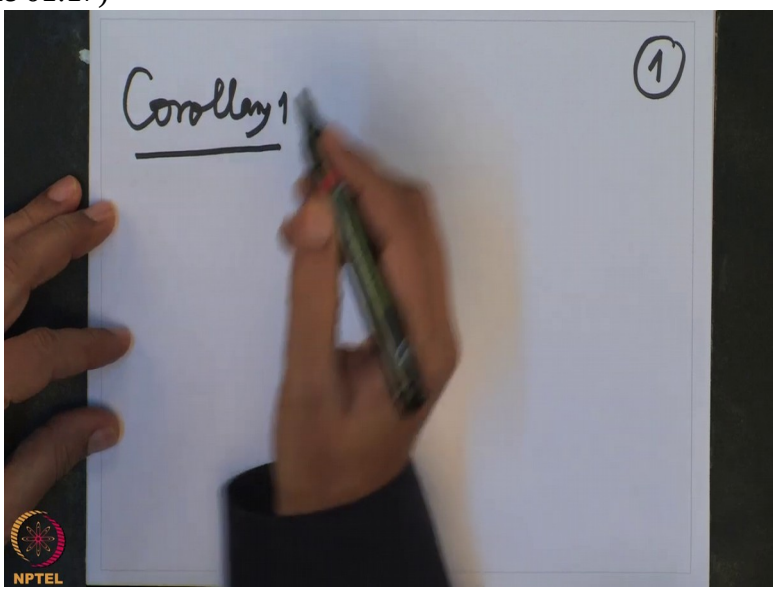
(Refer Slide Time 00:32)

of cyclotomic fields in characteristic 0 as well as characteristic p, in both the cases they are abelian groups. And these groups are connected to the, the unit groups of the ring $\mathbb{Z}_n$. So let me, and I want to give few applications of this.

And first of all, I want to write down the last statement I proved that if you have, so that I want to write it as a corollary.

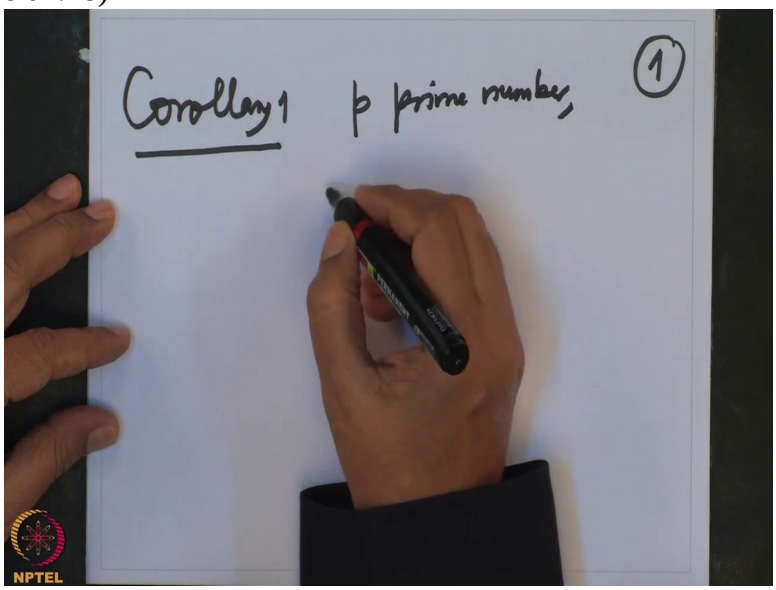
So corollary 1,

(Refer Slide Time 01:17)



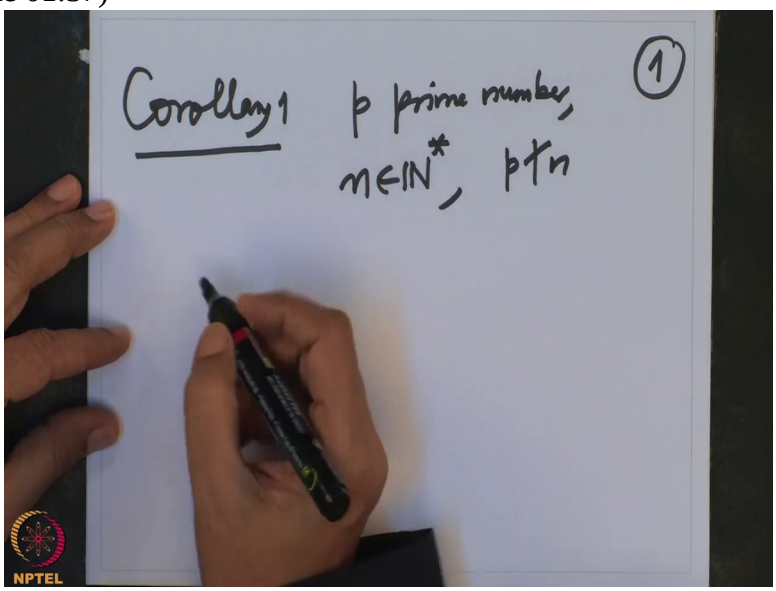
so if I have a prime number p, p is a prime number and suppose

(Refer Slide Time 01:28)



n is a non-zero natural number such that p does not divide n then

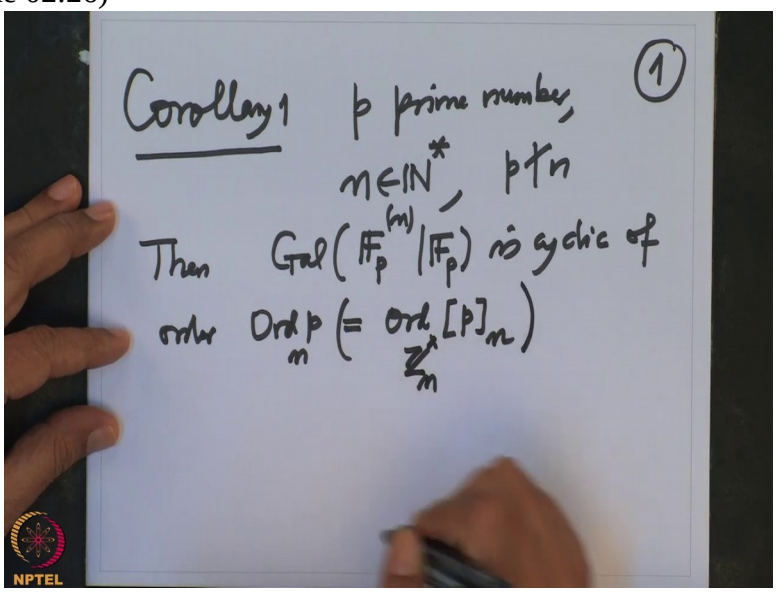
(Refer Slide Time 01:37)



the Galois' group of the cyclotomic extension $F_p^{(n)}$ over F_p, this Galois group is cyclic, cyclic we knew it before, generated by the Frobenius of order, order p modulo n.

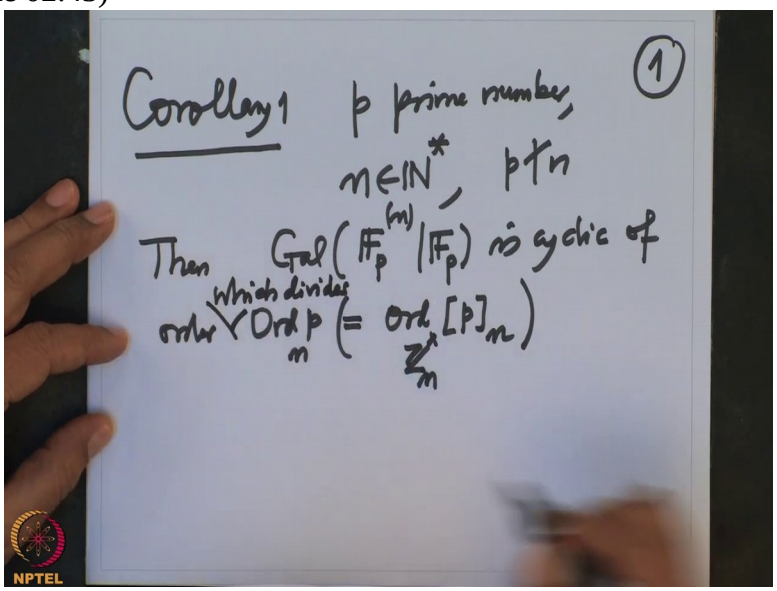
This is the definition of order of the residue class of p in the ring n, in $\mathbb{Z}_n$ and in the, this order is in the group $\mathbb{Z}_n^x$.

(Refer Slide Time 02:26)



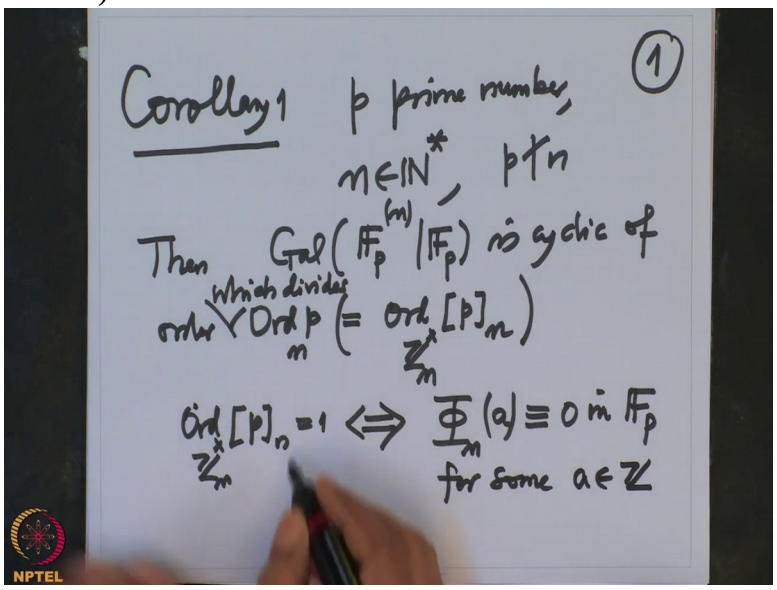
This is the cyclic group of order n which, not order this, order which, of order which divides this.

(Refer Slide Time 02:43)



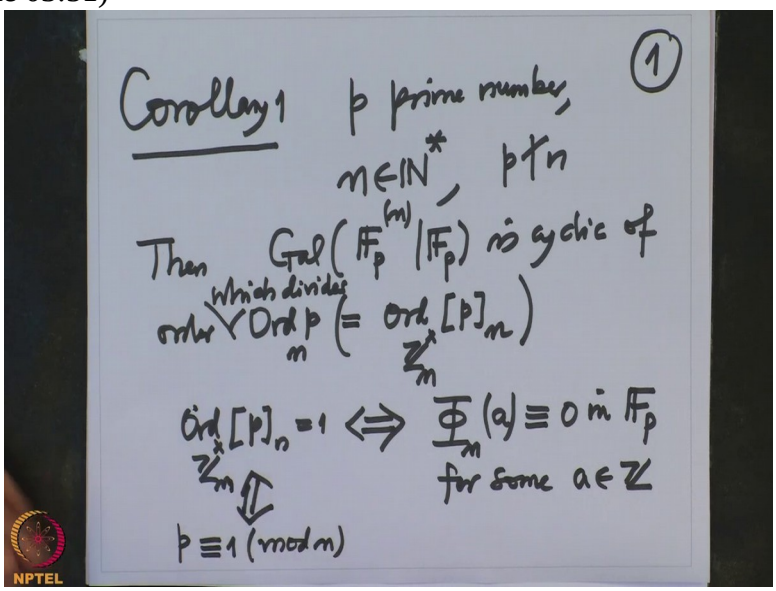
When is the, when is then, it is of order, when will be the, this order will be 1? Then the, this group will also be trivial. So order, so and when will this occur? This occurs if and only if, so order of p n in $\mathbb{Z}_n^x$, this order is 1 if and only if the cyclotomic polynomial Φ_n has a 0 mod p equal to 0 in F_p for some integer, for some $a \in \mathbb{Z}$.

(Refer Slide Time 03:36)



And when is the order 1? That is if and only if that p should be congruent to 1 mod n because we are reading everything mod n.

(Refer Slide Time 03:51)

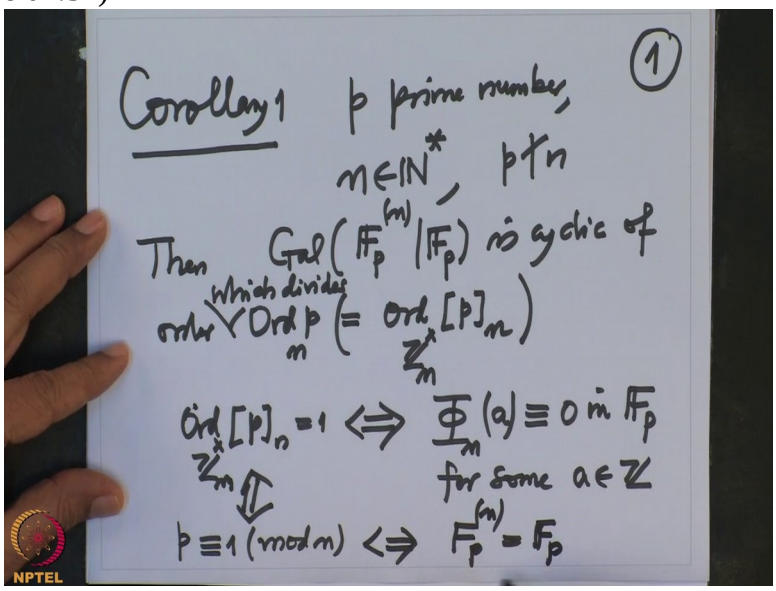


So cyclotomic, if the cyclotomic polynomial, this is the polynomial with integer coefficients actually. When I read mod that p and if it has a 0 for some, 0 is in therefore F_p , if it has a 0 in F_p , which is equivalent to p congruent to 1 mod n.

And that is then, will imply the Galois group of the cyclic extension is cyclic, this cyclic Galois group is trivial. That will mean that, so this is equivalent to saying $F_p^{(n)}$ equal to F_p .

That means

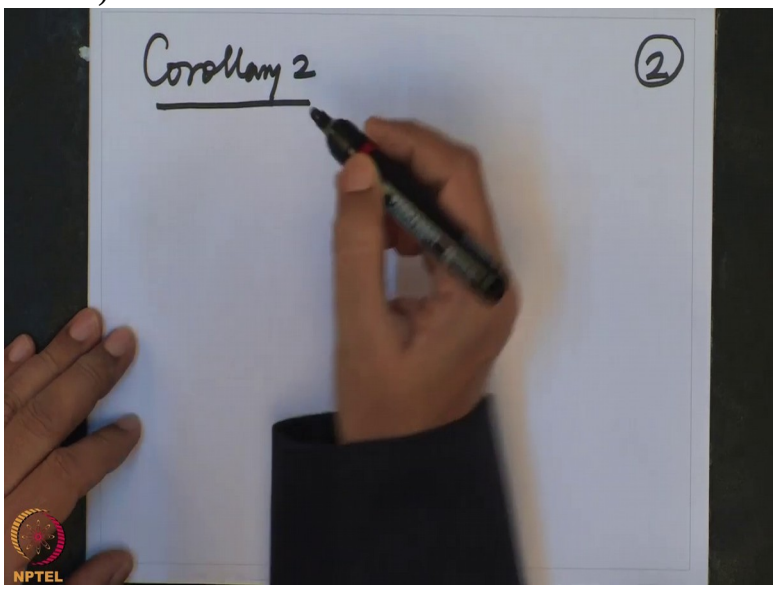
(Refer Slide Time 04:34)



all group, all the nth roots will lie actually in F_p . So that is the meaning of this corollary. And I want to use this corollary to prove some more results on Galois groups, Ok. So question is for which p this will happen? So that I want to state it as a corollary.

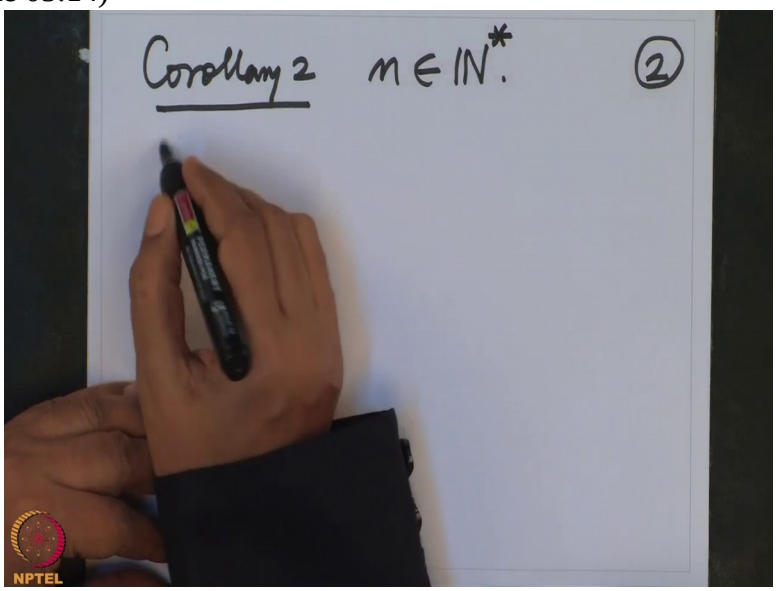
Corollary 2, corollary 2 as

(Refer Slide Time 05:08)



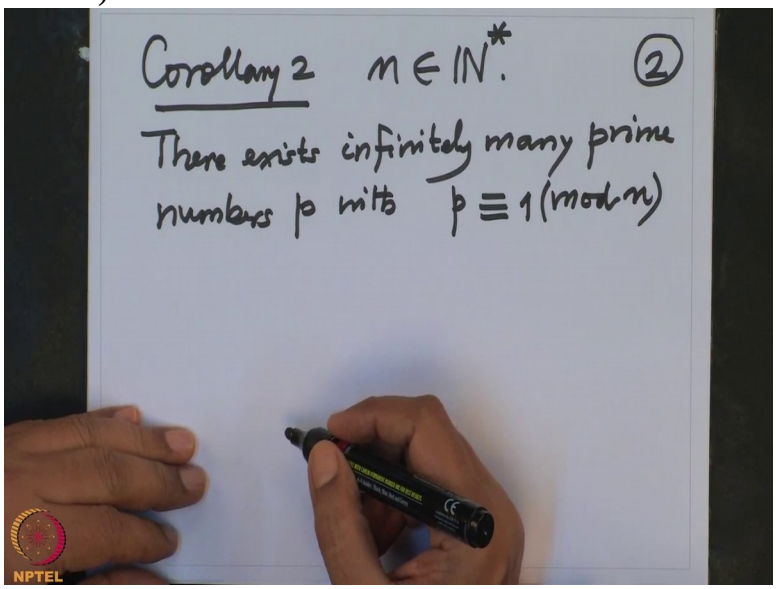
n is, given any non-zero natural number

(Refer Slide Time 05:14)



there exists infinitely many prime numbers p with p congruent to 1 mod n.

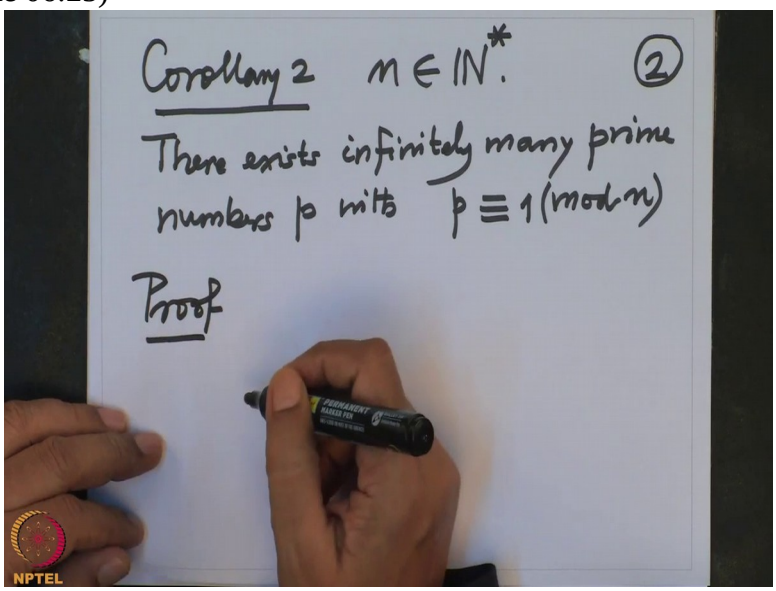
(Refer Slide Time 05:47)



So that means what, that means if I take, if I given n and if I am looking for nth roots of unity, for many, many ps that F_p will contain those nth roots of unity. So the, Φ_n will have 0 there, not all of them but phi n will have 0 in F_p, alright.

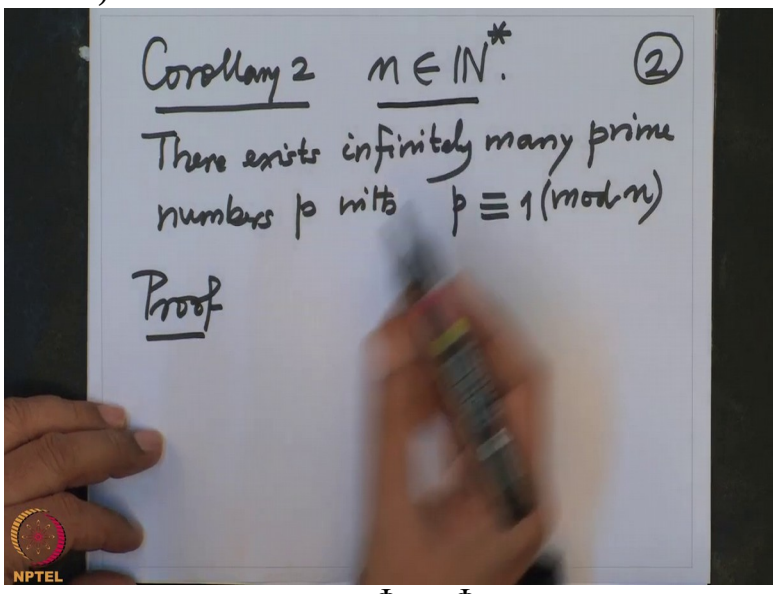
So actually this is, this will follow from the following. And so proof.

(Refer Slide Time 06:25)



So I am going to, we have given n.

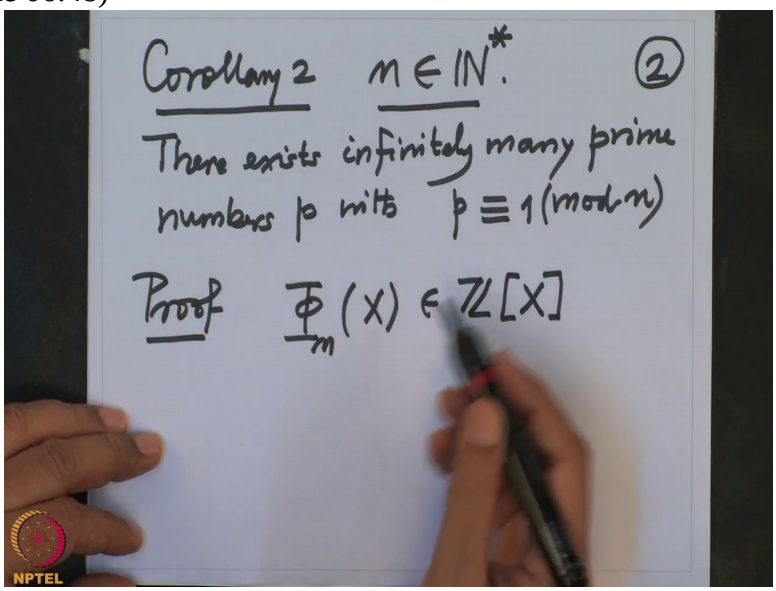
(Refer Slide Time 06:30)



So I am going, we have given therefore Φ_n. Φ_n is a polynomial in X with integer coefficients. And what do we want to prove?

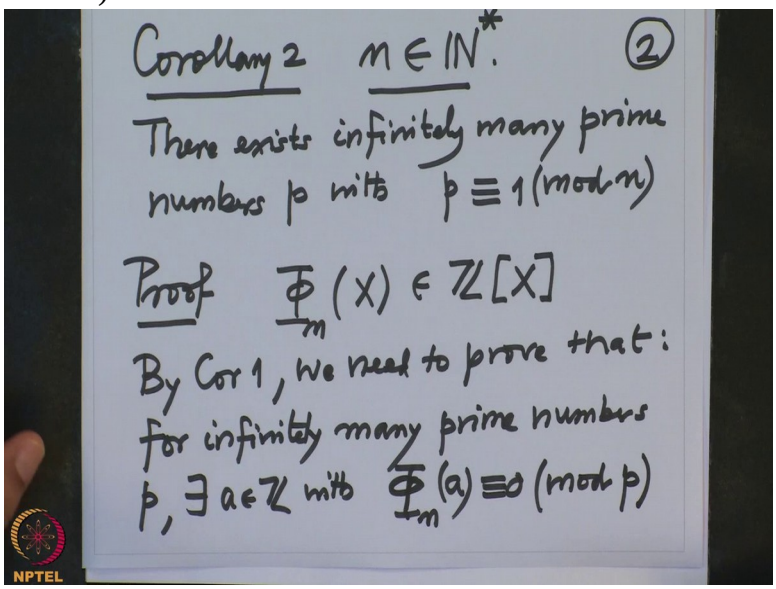
We want to prove there are finite; infinitely many prime numbers p such that p is congruent to 1 mod n.

(Refer Slide Time 06:48)



That means we want to prove by corollary 1, we need to prove that, for infinitely many primes, many prime numbers p, there exists an integer a with Φ_n, $\Phi_n(a)$ is congruent to 0 modulo p.

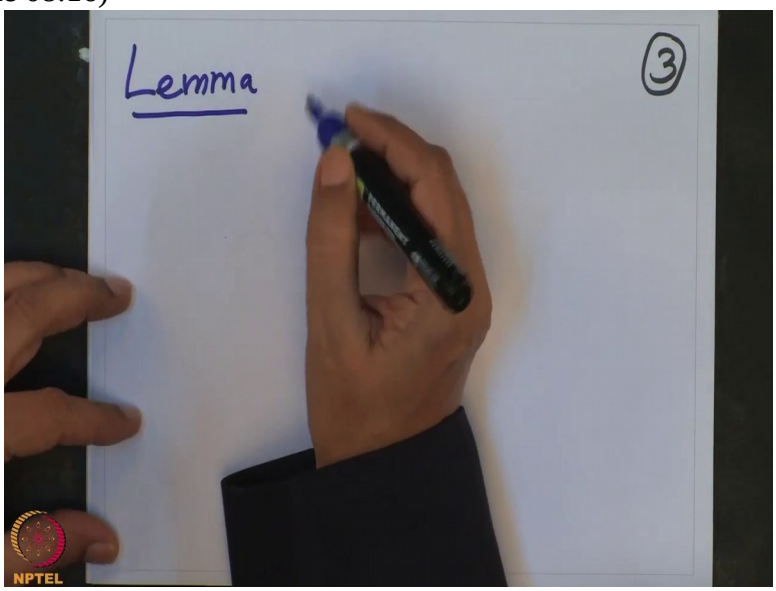
(Refer Slide Time 07:40)



Because this condition, phi n has a 0 mod p is equivalent to, p is congruent to 1 mod n. So I want to find infinitely many primes so that this polynomial has 0 in mod p. But this is very easy, so this will; I will state a general interesting observation. So therefore the question becomes the following lemma. This will follow from the following lemma.

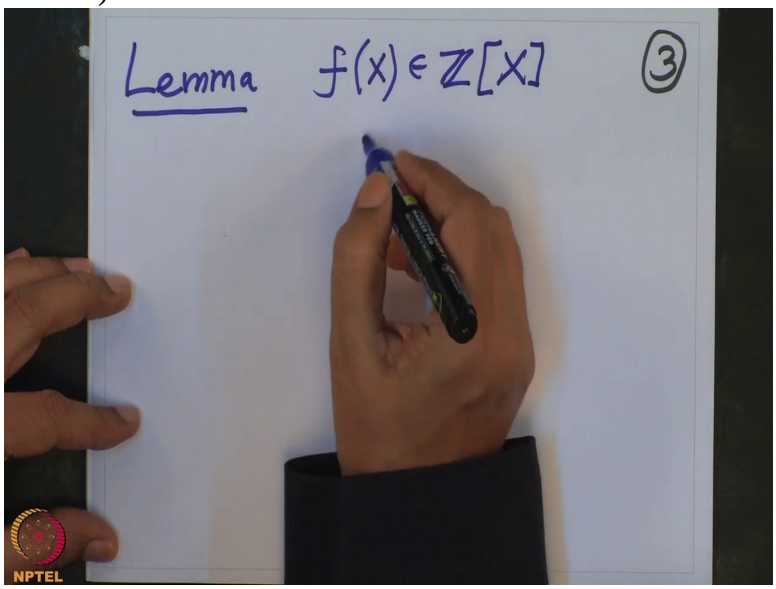
So I have a polynomial f,

(Refer Slide Time 08:16)



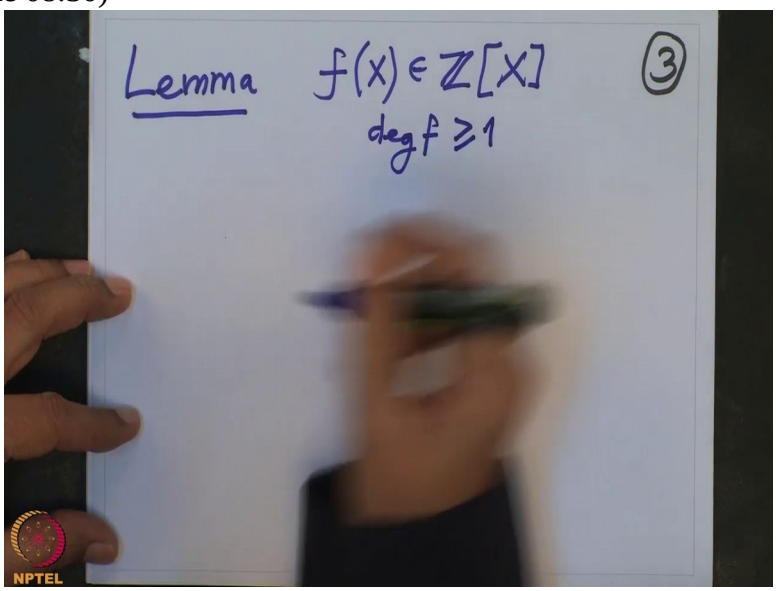
f is a polynomial with integer coefficients and the degree

(Refer Slide Time 08:25)



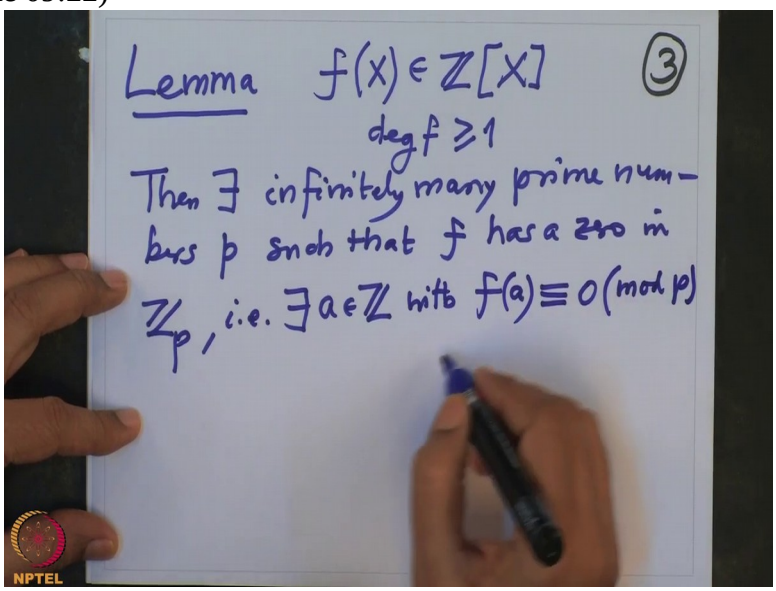
of f is bigger equal to 1.

(Refer Slide Time 08:30)



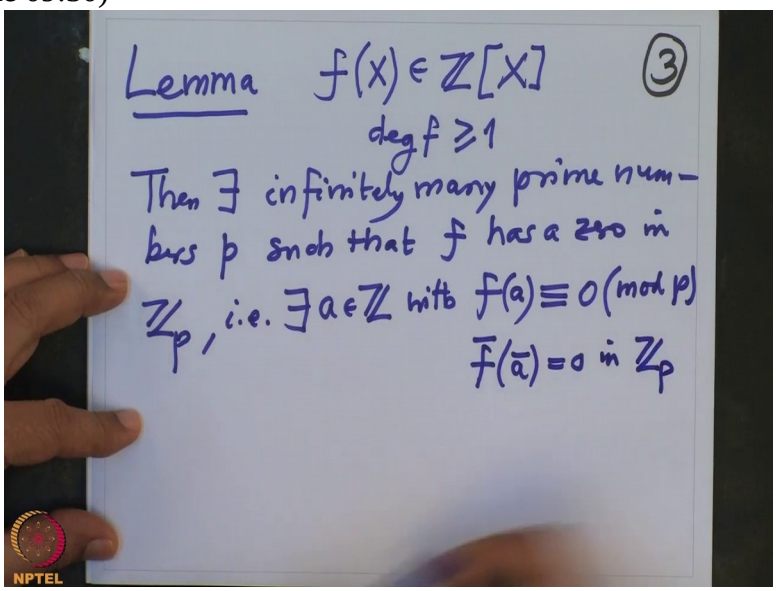
So then there exist infinitely many primes, prime numbers p such that f has a 0 in $\mathbb{Z}_p$. So that means there exists an integer a in $\mathbb{Z}$ with $f(a)$ is congruent to 0 mod p.

(Refer Slide Time 09:22)



So this means f of, f bar of a bar is 0 in Z mod p

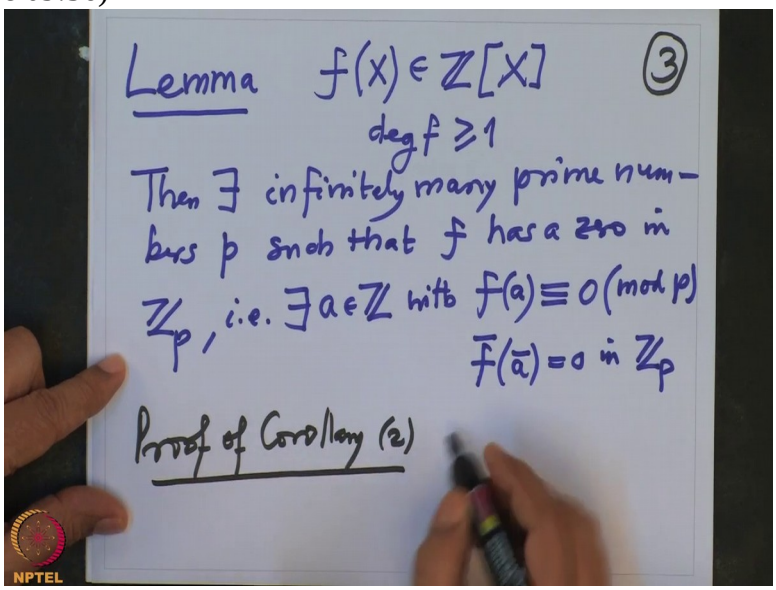
(Refer Slide Time 09:30)



where bar means denoting mod p.

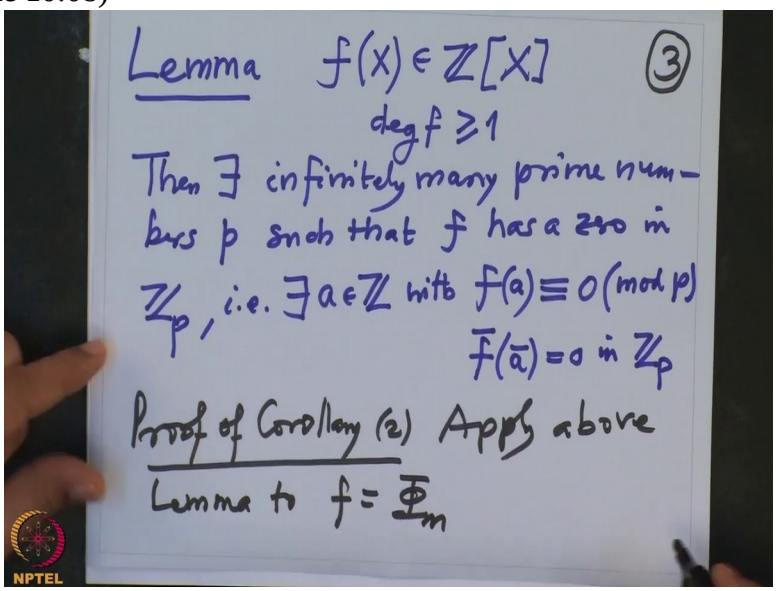
So if I prove this lemma the corollary follows because we are going to apply this lemma to that Φ_n . So proof of corollary 2, apply

(Refer Slide Time 09:56)



above lemma to the polynomial f equal to Φ_n .

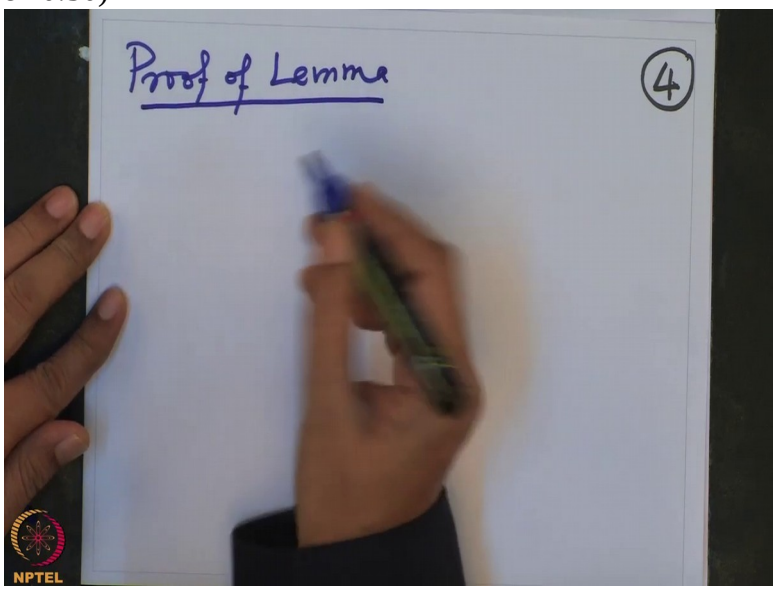
(Refer Slide Time 10:08)



And therefore it is clear. I have to prove the lemma only. Lemma is very easy to prove. Let us prove lemma. Lemma is very, very easy to prove.

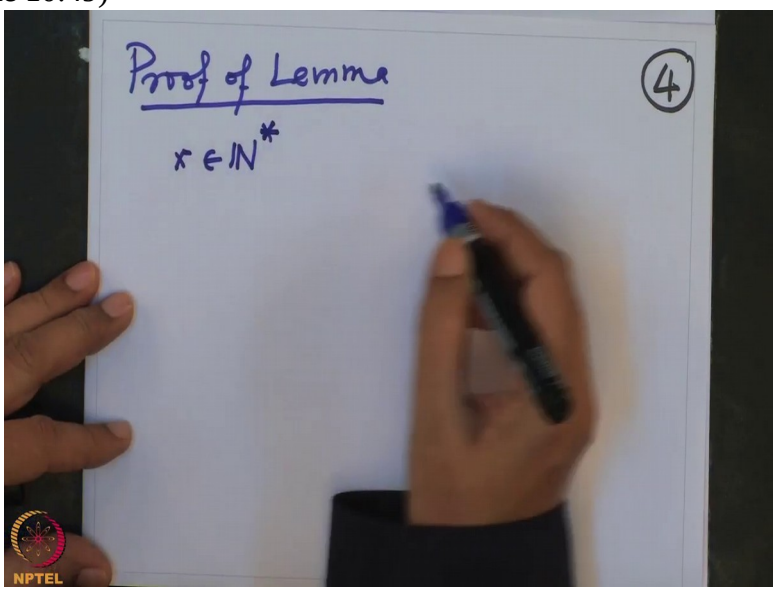
So proof of lemma. What is it you want to prove? You want

(Refer Slide Time 10:30)



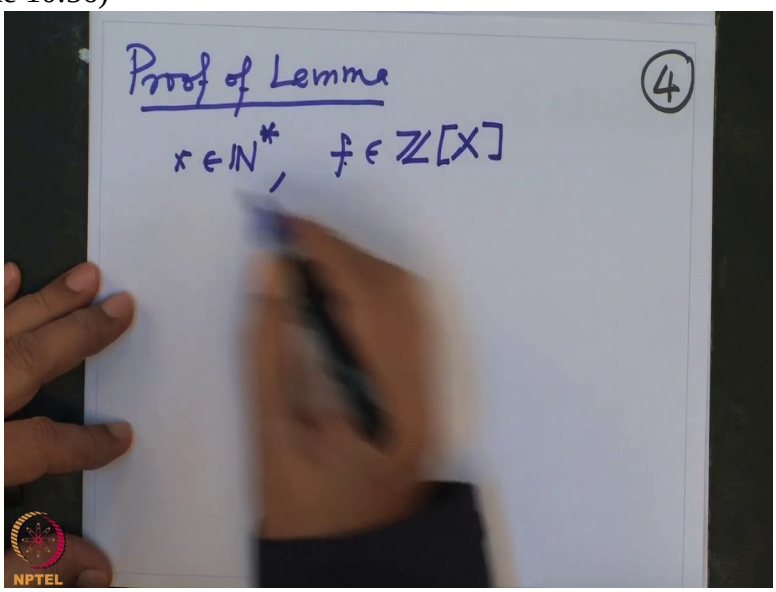
to produce infinitely many primes so that f has a 0 mod p, alright. That means what? That means, so I take a natural number, x is a natural number, arbitrary natural number non-zero,

(Refer Slide Time 10:49)



and I will get, I had a polynomial f in integer coefficients. So I look at

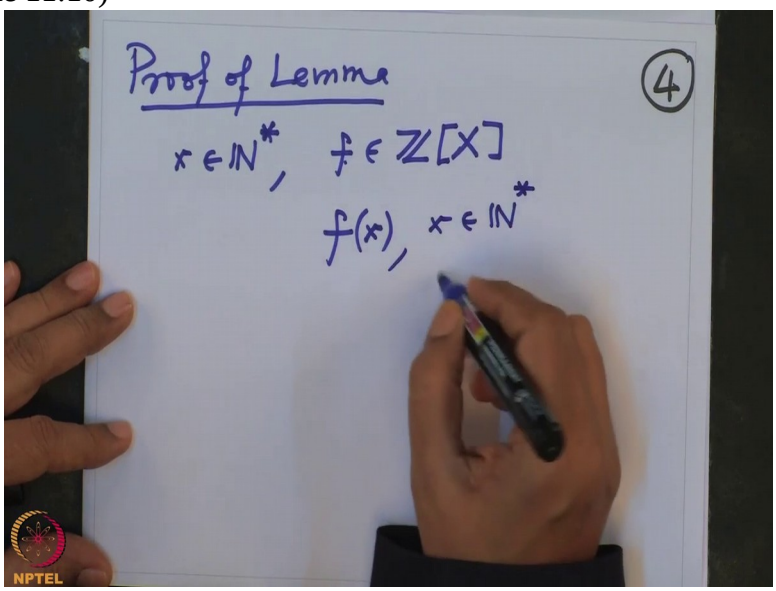
(Refer Slide Time 10:56)



the value of $f(x)$, so $f(x)$. This is some integer and x is varying. So there are many, many integers.

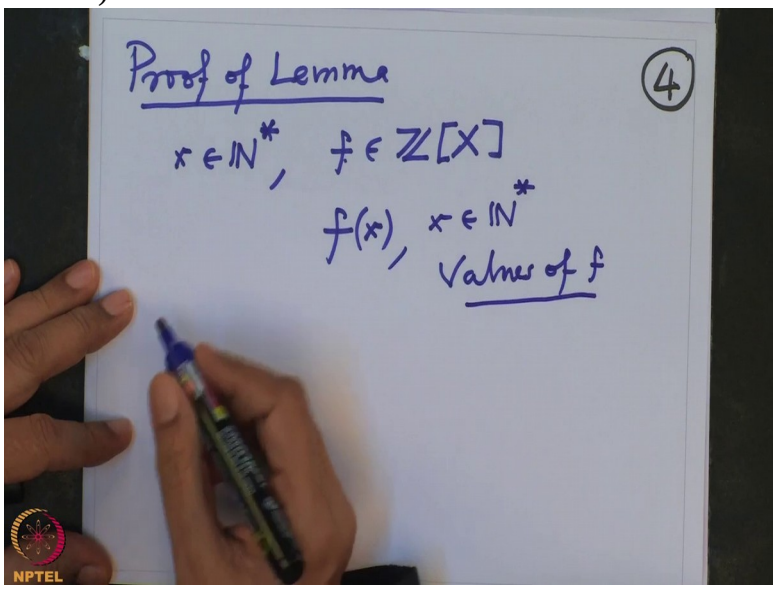
So look at these values, all the values. These are values

(Refer Slide Time 11:10)



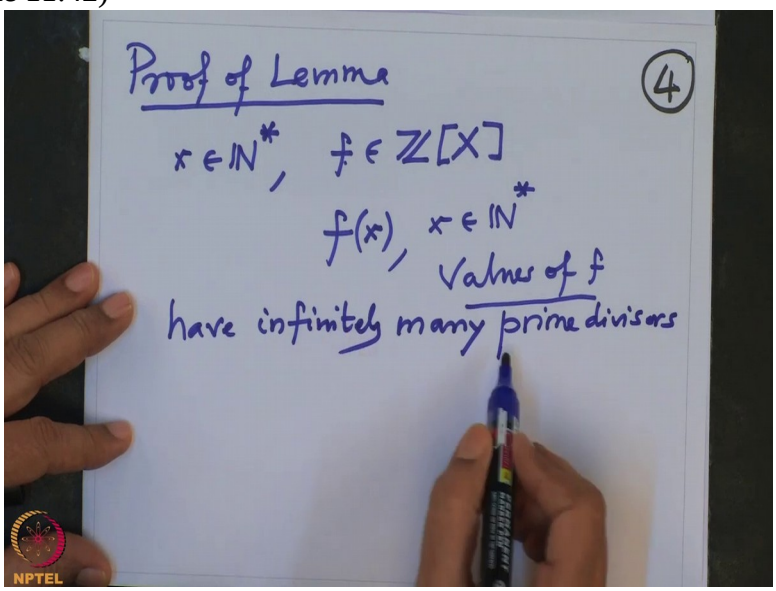
of f. They are integers.

(Refer Slide Time 11:15)



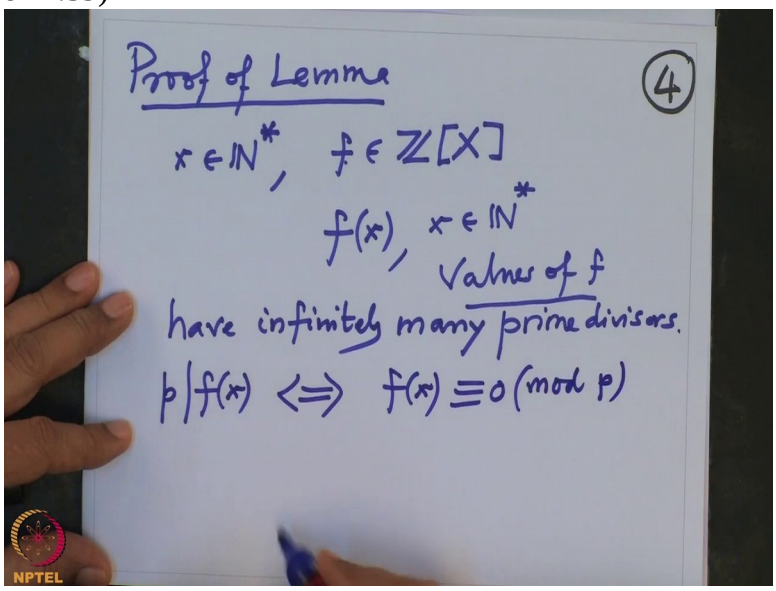
I want to show that they have infinitely many divisors. So these values have infinitely many prime divisors. That will produce, so

(Refer Slide Time 11:42)



if p is, so this will prove the lemma because if p divides $f(x)$, that is equivalent to saying $f(x)$ is congruent to 0 mod p.

(Refer Slide Time 11:59)

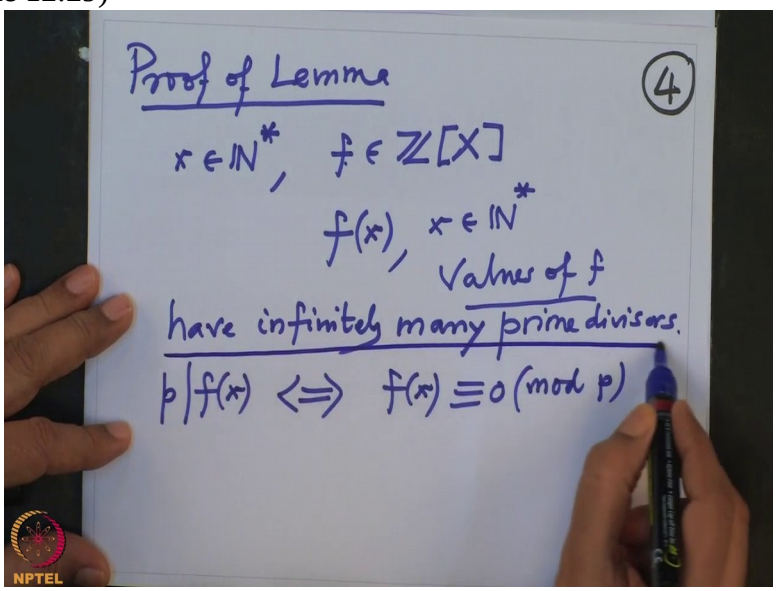


So this p is a required prime.

So if I, values are, the x is varying then values are varying. But this has infinitely many prime divisors. When I say this has infinitely many prime divisors means they are prime numbers, p infinite in number which divide $f(x)$ for some x. So therefore that will prove the lemma.

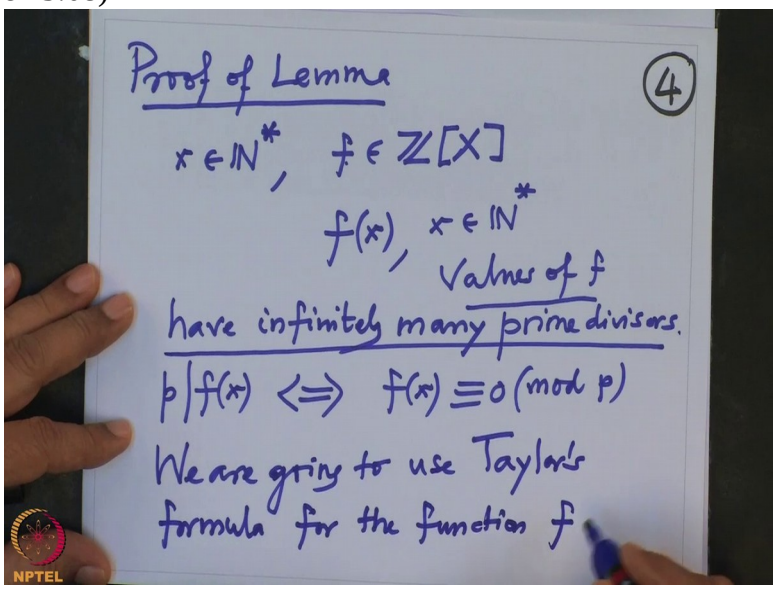
And how do you check this statement? You have

(Refer Slide Time 12:29)



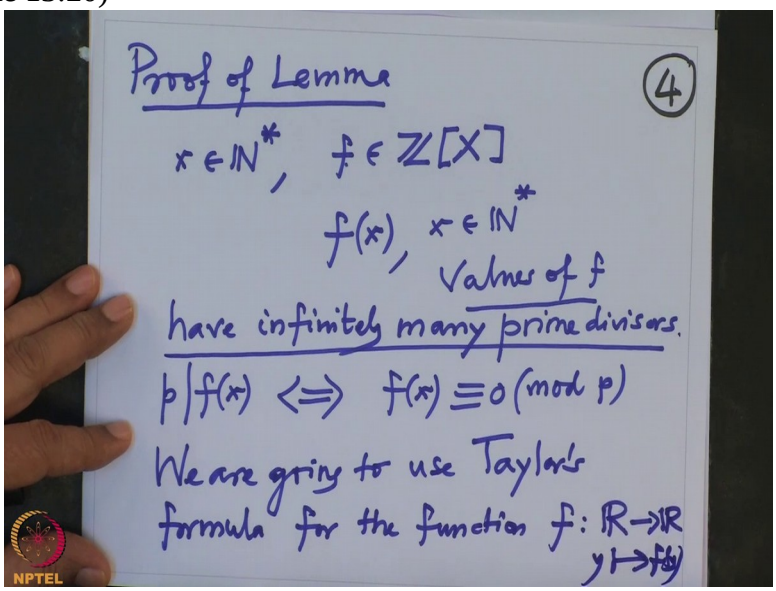
infinitely many prime divisors. So that is because, let us look at, look at, I am going to use the Taylor's formula. So we are going to use, we are using, going to use Taylor's formula. I will recall that formula for the function f. f is a polynomial.

(Refer Slide Time 13:08)



So f is a, so you can think of, f is a function from wherever, from real number to real numbers. Any real number y, this is $f(y)$.

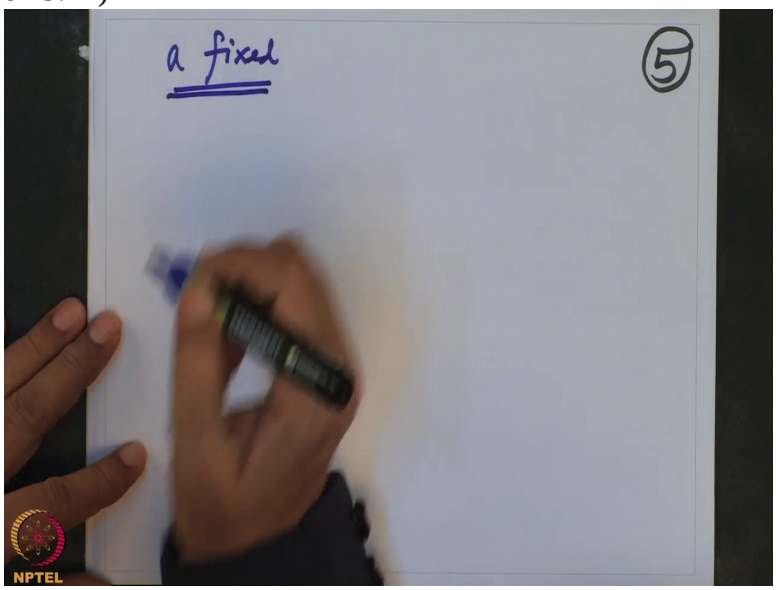
(Refer Slide Time 13:20)



This is a polynomial function. So it is differentiable function. So Taylor's formula makes sense. And what do we do with the Taylor's formula? Let us write down that.

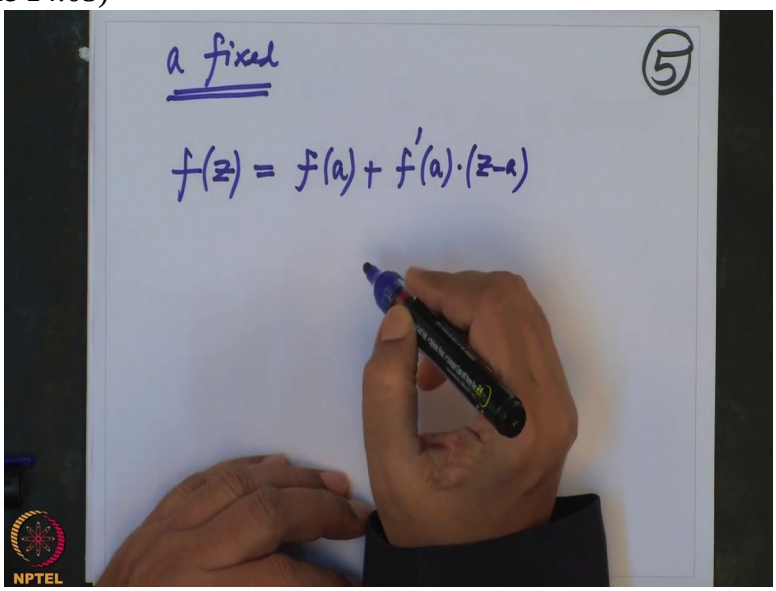
So that means if I fix a, I will fix a, a is fixed, and Taylor's expansion at a I am taking.

(Refer Slide Time 13:44)



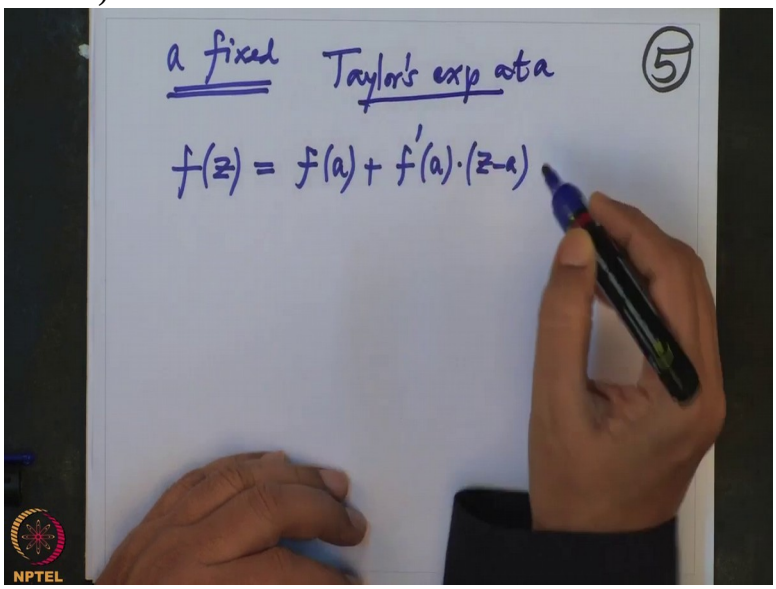
That means I have to write $f(z)$ equal to what? $f(a)+f'(a)(z-a)+\ldots$

(Refer Slide Time 14:05)



I am looking Taylor's expansion at a.

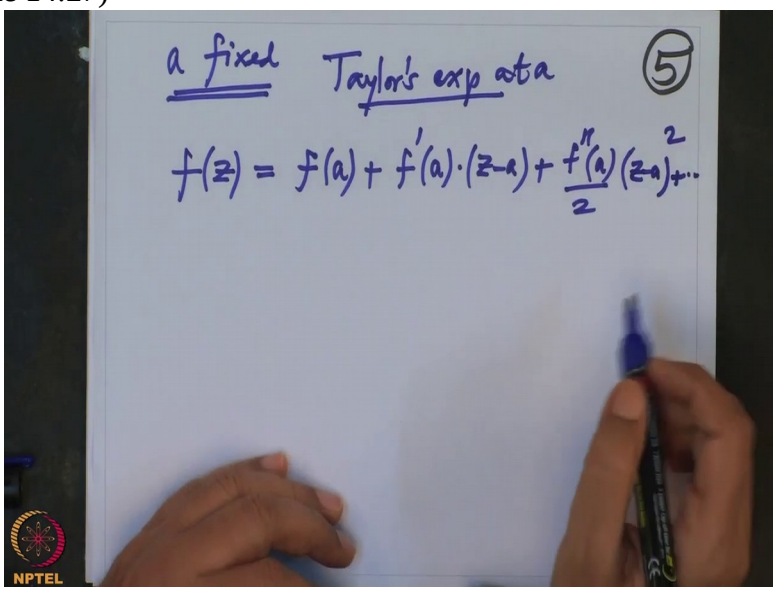
(Refer Slide Time 14:17)



Plus $\frac{f''(a)}{2}(z-a)^2$, and so on.

This is a Taylor's

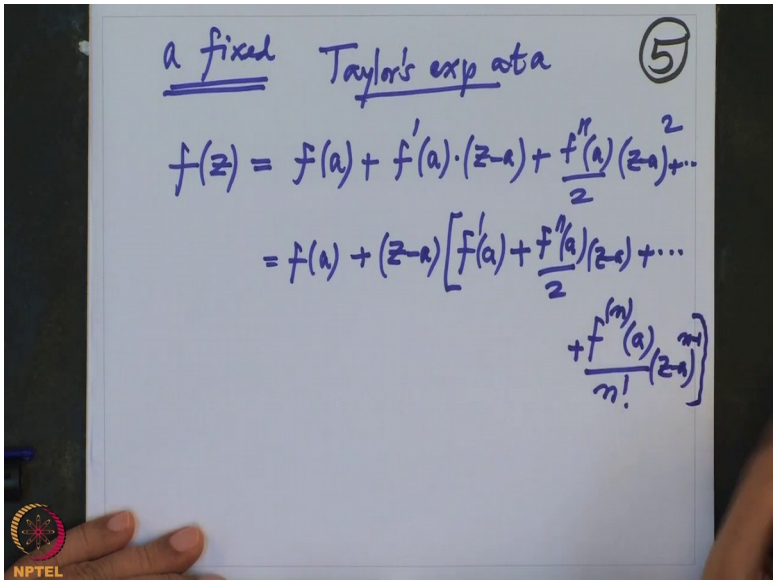
(Refer Slide Time 14:27)



expansion. Now in this I am going to look at only the first term, so that is $f(a)$. And the remaining terms have $z-a$ as a factor. And this will not go on forever, because f is a polynomial. So this is actually a polynomial. So this has only finitely many terms.

So from here, I am going to take $z-a$ common. And what is inside then? $f'(a)+\frac{f''(a)}{2}(z-a)^2$, and how long it will go on? It will not go on more than the degree. So once it reaches nth derivative of f evaluated at $\frac{a}{n!}$ and then $(z-a)^{n-1}$ and after that the derivative will be

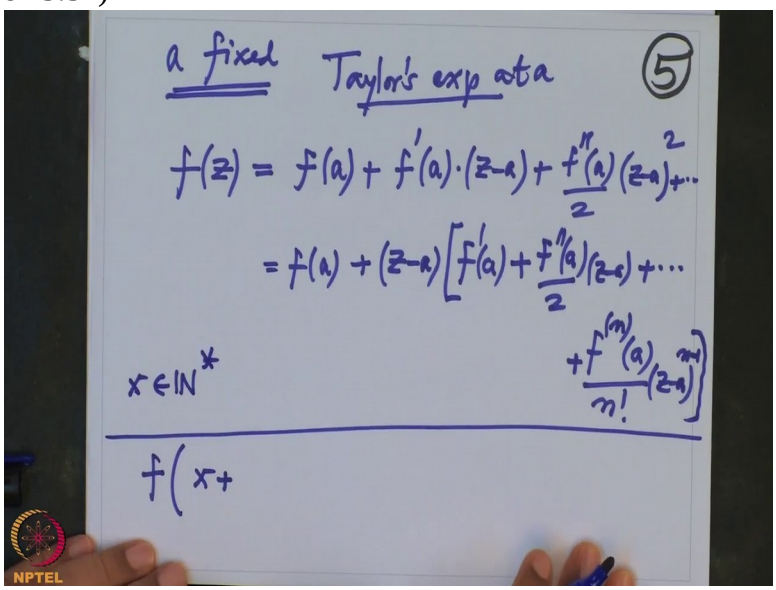
(Refer Slide Time 15:20)



0. So the other terms will be 0.

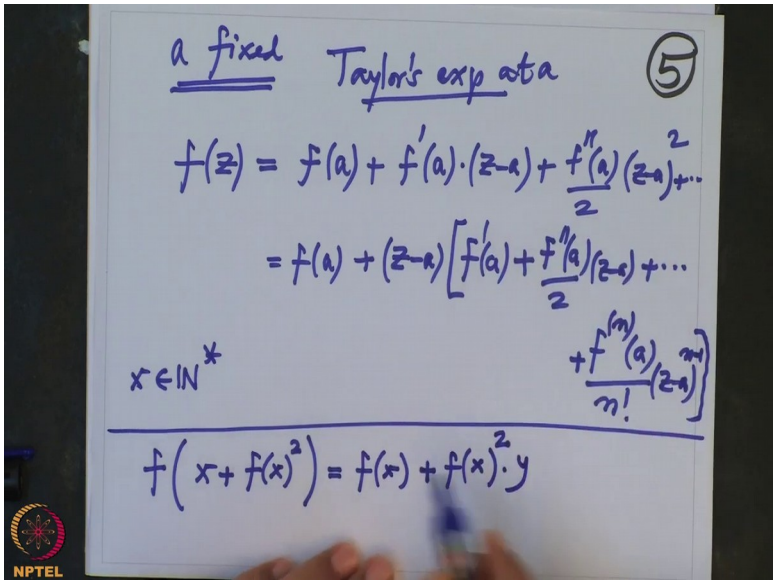
So it is this, actually. So therefore this, we, I am going to use this. So how am I using it? I am using it to the following, following formula. So I am going to take z equal to $f(z)$ I will take x +, I have given, I take any x in

(Refer Slide Time 15:52)



natural numbers. And then x and take $f(x)^2$. Then the Taylor's expansion of this will be, if you stare at it, it will be $f(x)+f(x)^2 y$, this, the remaining

(Refer Slide Time 16:13)

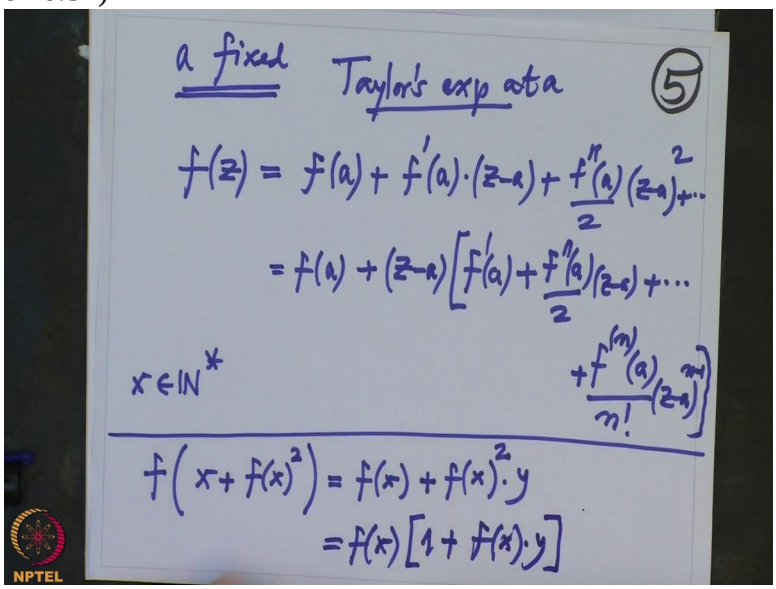


term I have omitted.

So I have taken what, is clear. This is my, a is my x. And y is my z, see I want, so once I adjust like that, you find suitable y so that this expansion there. Now what do I want? I want, as x varies this $f(x)$ has more and more prime divisors.

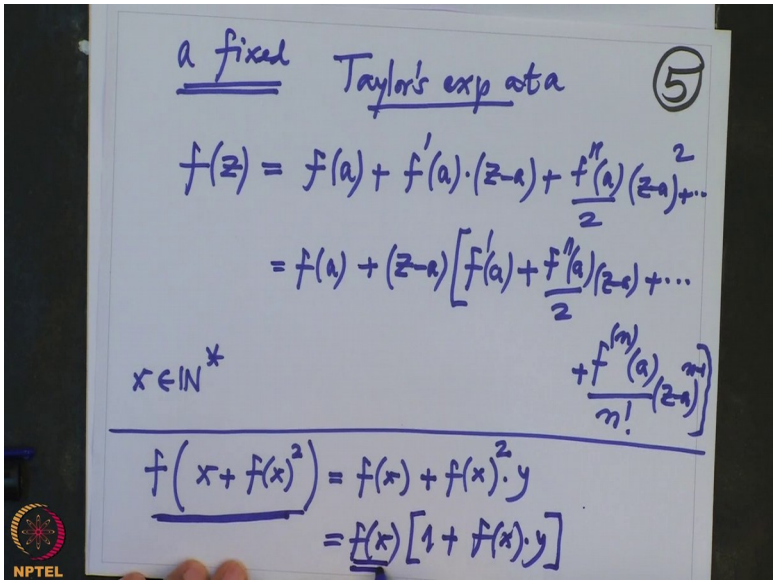
So this is what, this is $f(x)1+f(x)y$.

(Refer Slide Time 16:52)



Now this is also value, this is also value of f.

(Refer Slide Time 17:00)

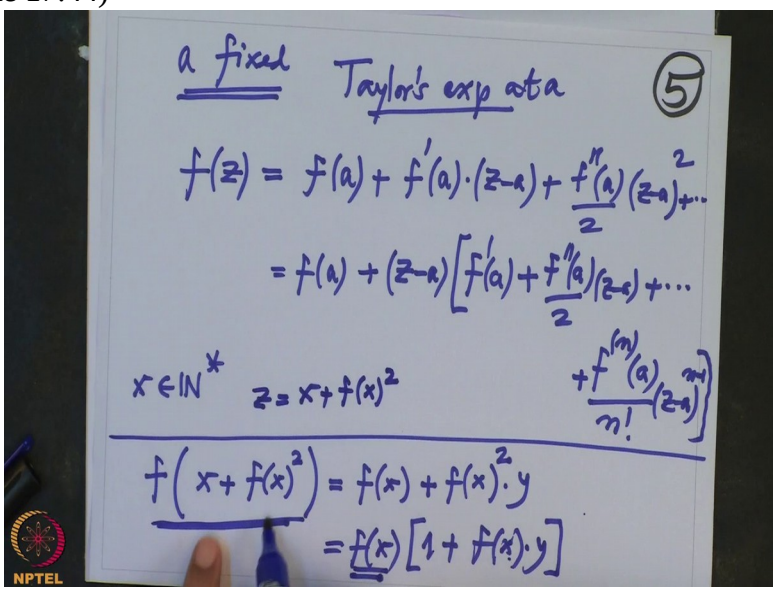


So this is value of f. This is also value of f. But this value is $f(x)$ times this. And this and this, they are co-prime. You see, this is, I have made them co-prime.

So the prime divisors of this will be new prime divisors. So they are also prime divisors of this value then. So if I vary the values then I am getting new and new prime divisors. And this will, this is true for any x. So every time I will get a new value.

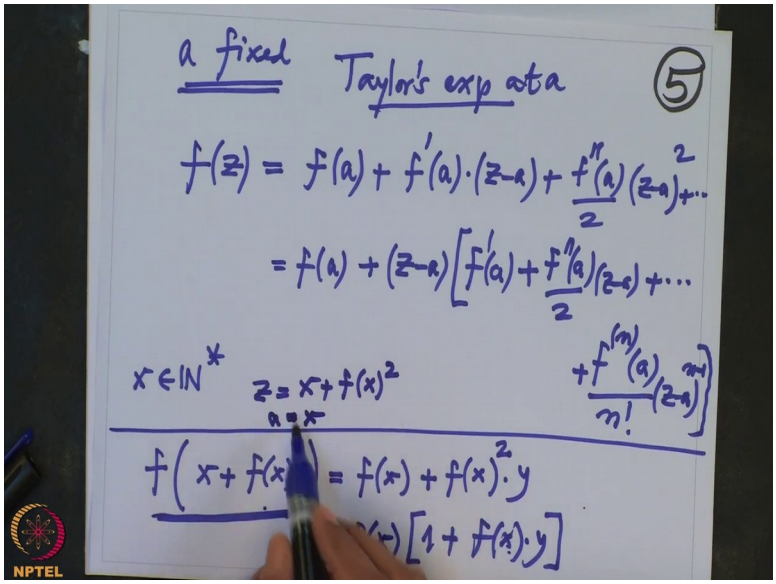
So this one, I have applied above formula to z equal to $x+f(x)^2$. If I put above, z equal to

(Refer Slide Time 17:44)



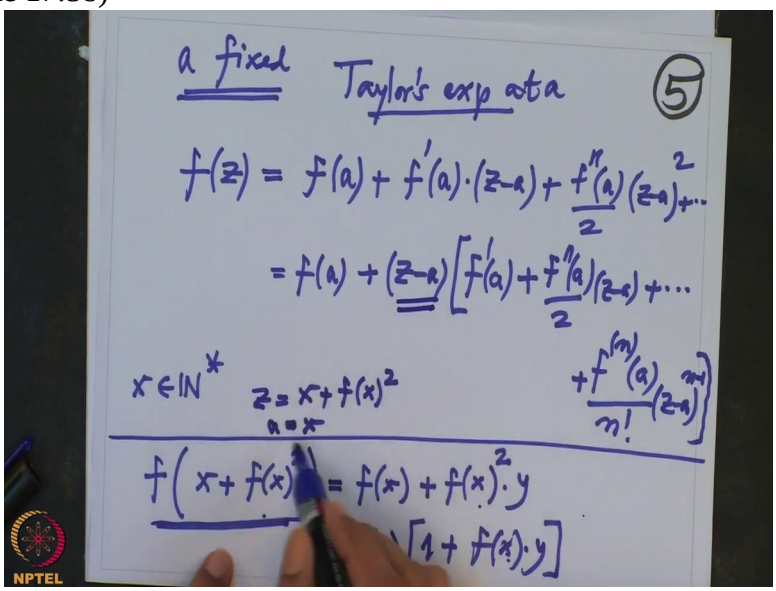
$x+f(x)$, this is this side, and a is x.

(Refer Slide Time 17:50)



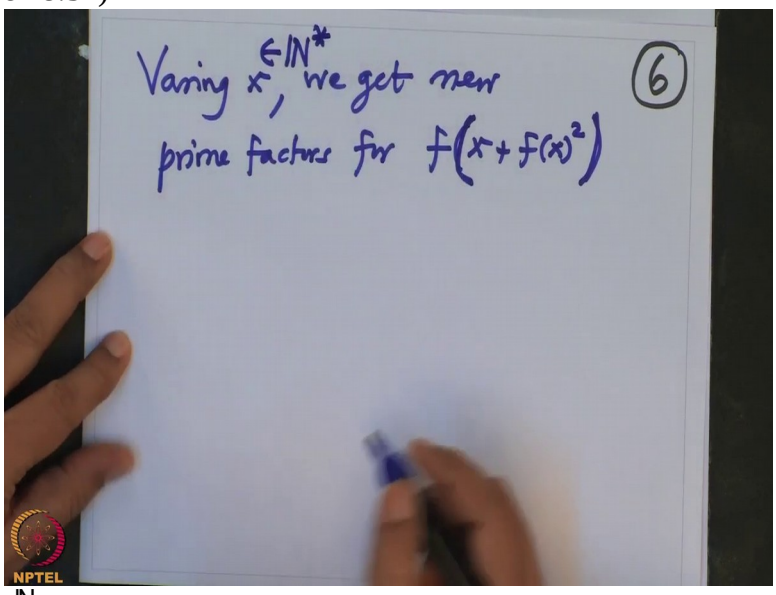
So you see that this is that $f(z)$. And $f(x)$ is $f(a)$. And what is this term then, $z-a$?

(Refer Slide Time 17:58)



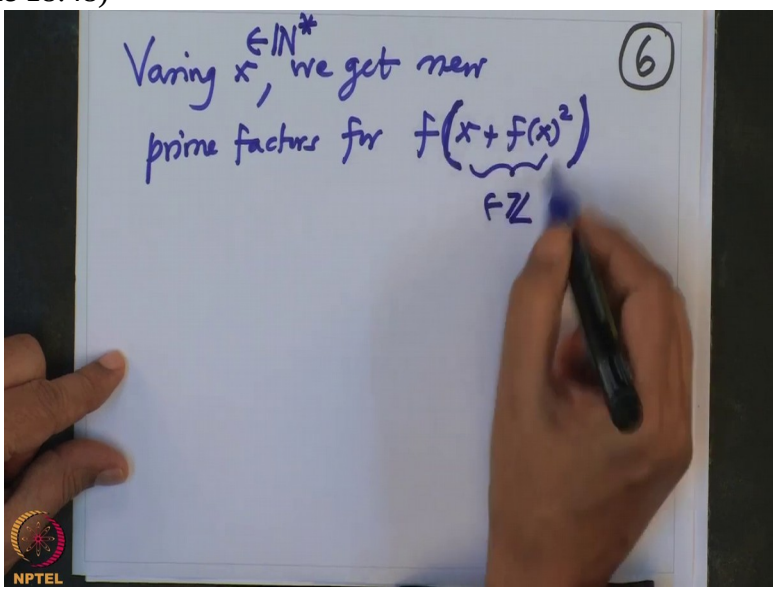
$z-a$ is what? That is precisely, this x will get canceled, $f(x)^2$. And the remaining is y. So it is that. So that proves that, so this proves that when I vary, so varying x we get new prime factors for $f(x)+f(x)^2$ and x is varying in $\mathbb{N}^*$.

(Refer Slide Time 18:37)



And then this is $\mathbb{N}$ because f is a polynomial with integer coefficient. This is also integer. And then,

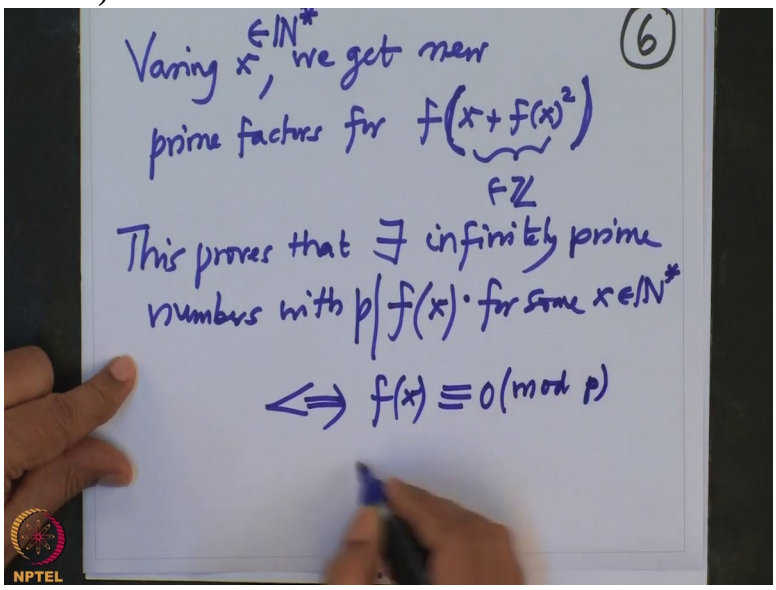
(Refer Slide Time 18:48)



that is also an integer.

So I get, these are integers. And they are known to have factors. So that proves that, so this proves that there exists infinitely many primes, prime numbers with p divides, $p|x$ for some x in natural number. This equation is equivalent to saying $f(x)$ is congruent to 0 mod p

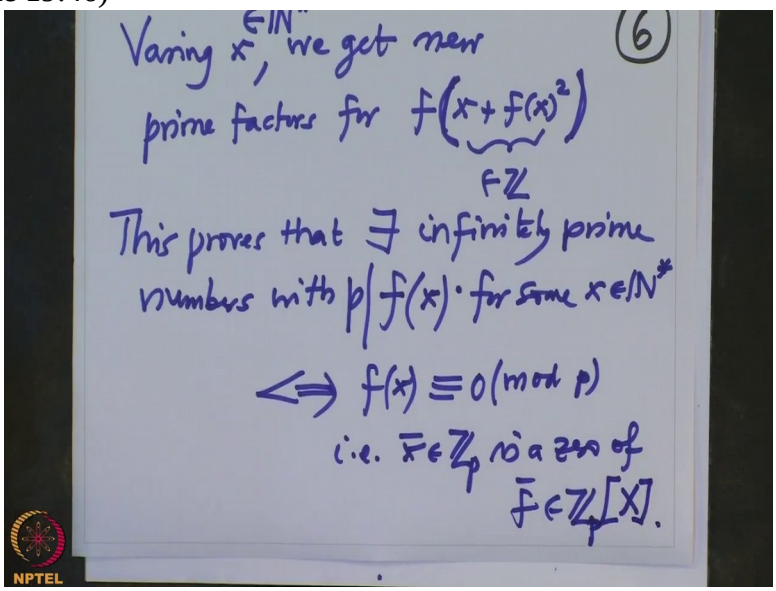
(Refer Slide Time 19:30)



that is $\bar{x}$ in $\mathbb{Z}_p$ is a 0 of $\bar{f} \in \mathbb{Z}_p[X]$.

That is what we wanted

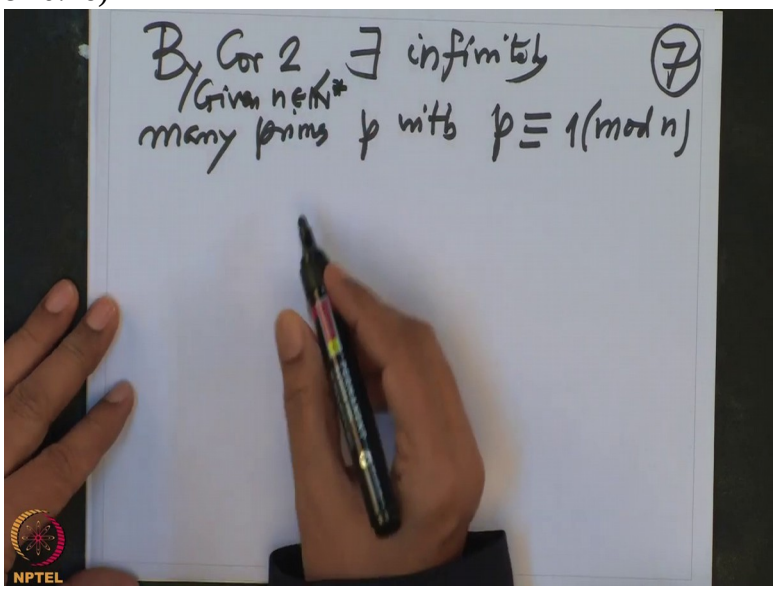
(Refer Slide Time 19:46)



to prove. And we noted therefore that, this we applied to f equal to Φ_n , that cyclotomic polynomial. So that proves that corollary, alright.

Now I want to also note the following, this one the last corollary. So what was the last corollary? There are, by corollary 2, there are infinitely many primes, many primes p with, p congruent to 1 mod n. n is given. So given n, natural number, non-zero natural number,

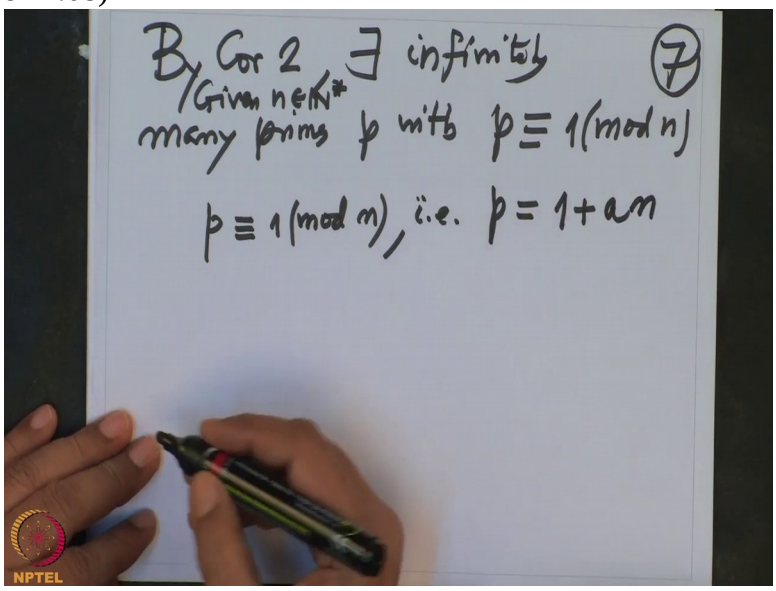
(Refer Slide Time 20:46)



you can find p so that p is congruent to 1 mod n. So how will the p look like?

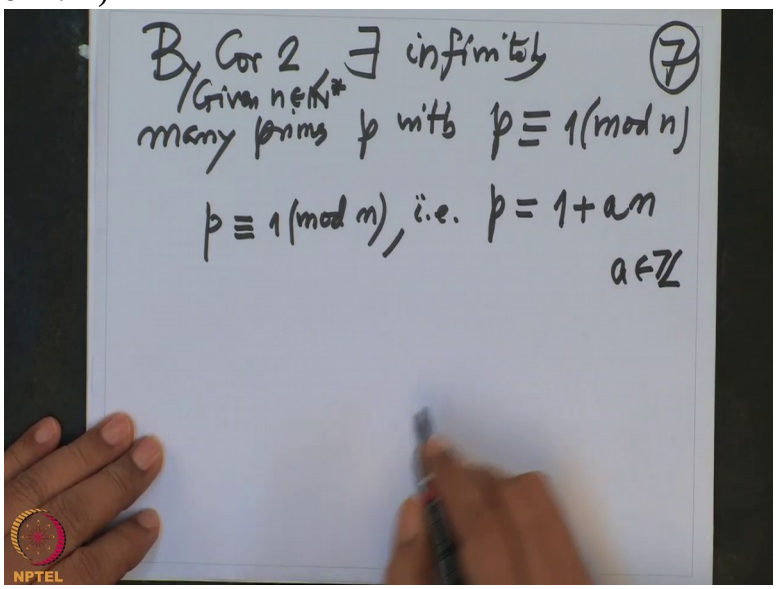
So that means p will look like congruent to 1 mod n. That is same thing as saying, that is p is of the form, 1 plus some multiple of n

(Refer Slide Time 21:08)



where a is an integer.

(Refer Slide Time 21:14)

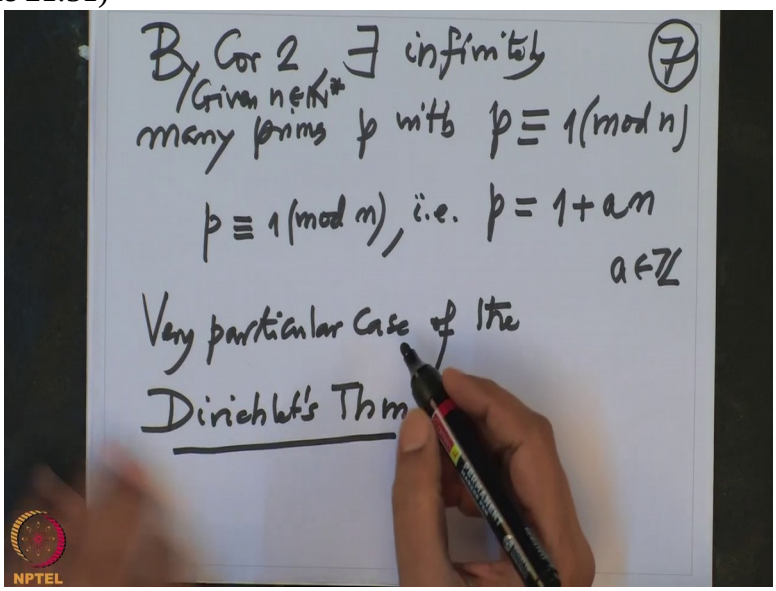


So there are many, many primes with this condition. But that means they are in arithmetic progression.

If you arrange these integers in a increasing order, they are in arithmetic progression. So this is a very particular, this statement is a very particular case of the following theorem which was due to Dirichlet, Dirichlet's theorem in number theory.

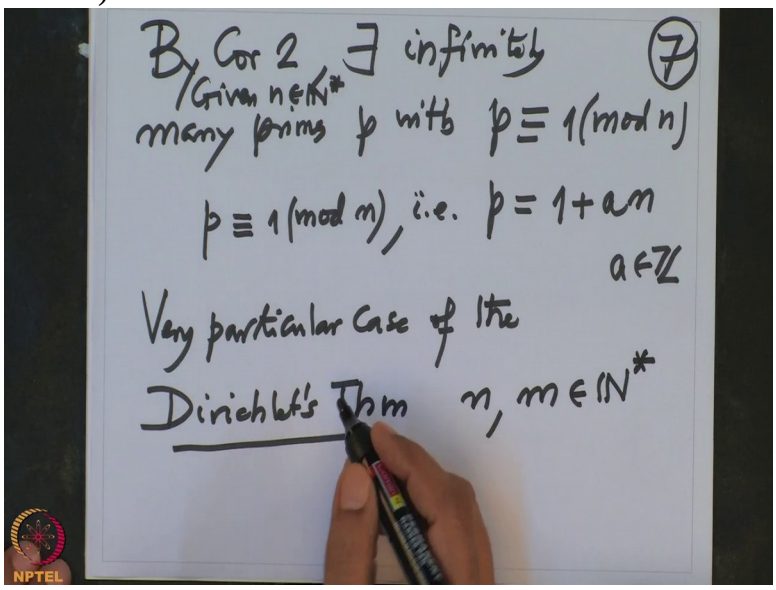
What does it say?

(Refer Slide Time 21:51)



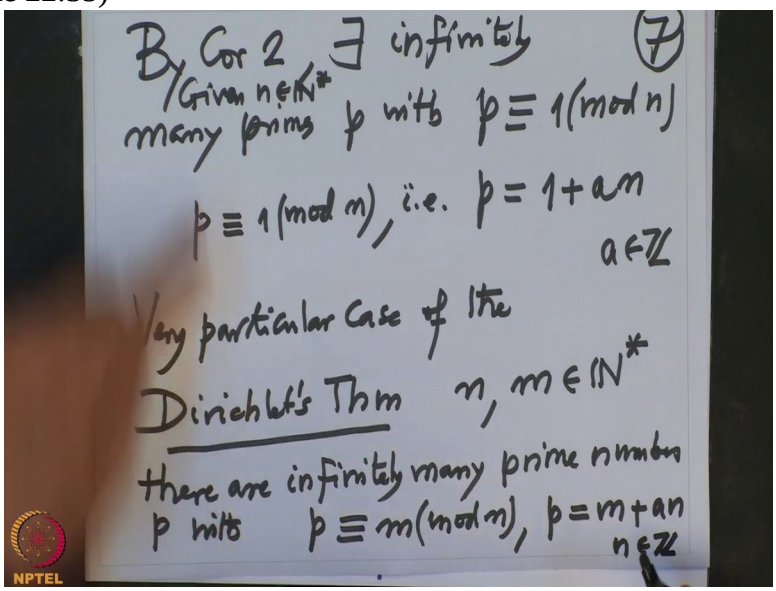
It says that, given 2 natural numbers n and m, both non-zero natural numbers,

(Refer Slide Time 22:00)



there are infinitely many primes; prime numbers p with p is congruent to m mod n. That means what? That is p is of the form, m plus a n where n is an integer.

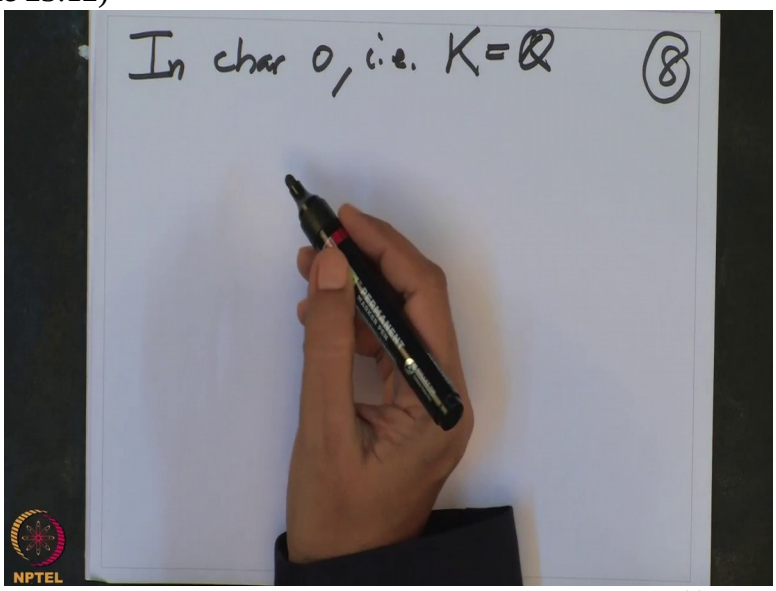
(Refer Slide Time 22:35)



the corollary 2 is m equal to 1. And m is any number. So this is a difficult theorem which is not so easy to prove. But it has, it is a very fundamental theorem in number theory. So we have proved very particular case of this which is very, very useful for the Galois Theory purpose, Ok. That was one comment.

So in characteristic 0, 0, that is when I take K equal to $\mathbb{Q}$, this case.

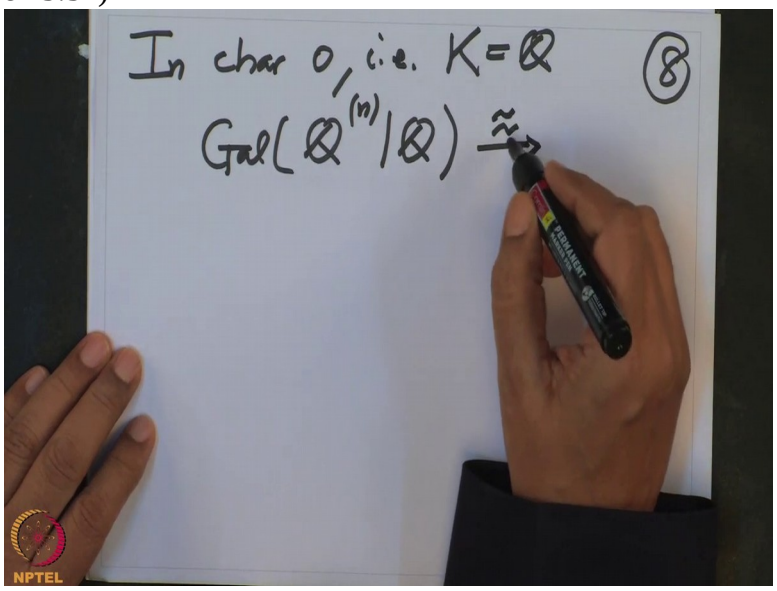
(Refer Slide Time 23:12)



Then what did we prove that? We prove that the Galois group of $\mathbb{Q}^{(n)}$ over $\mathbb{Q}$, this is a cyclotomic field extension.

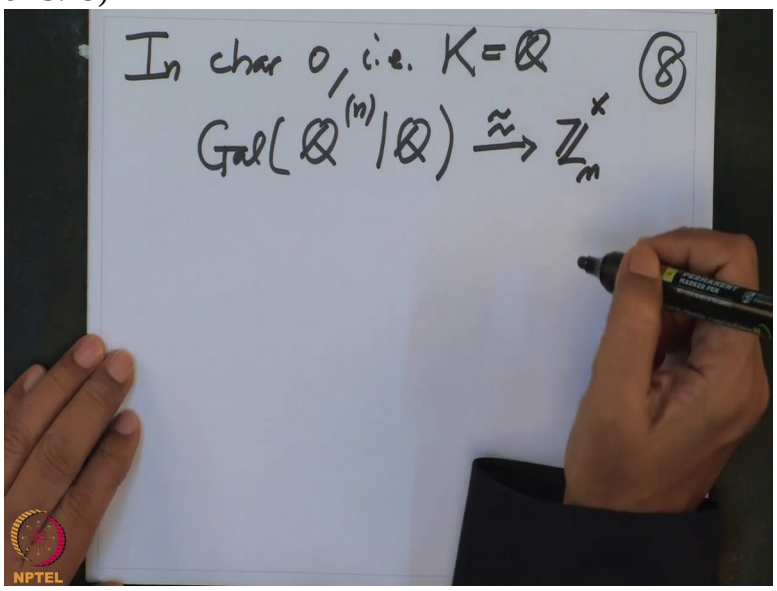
This Galois group is isomorphic in a canonical way to,

(Refer Slide Time 23:31)



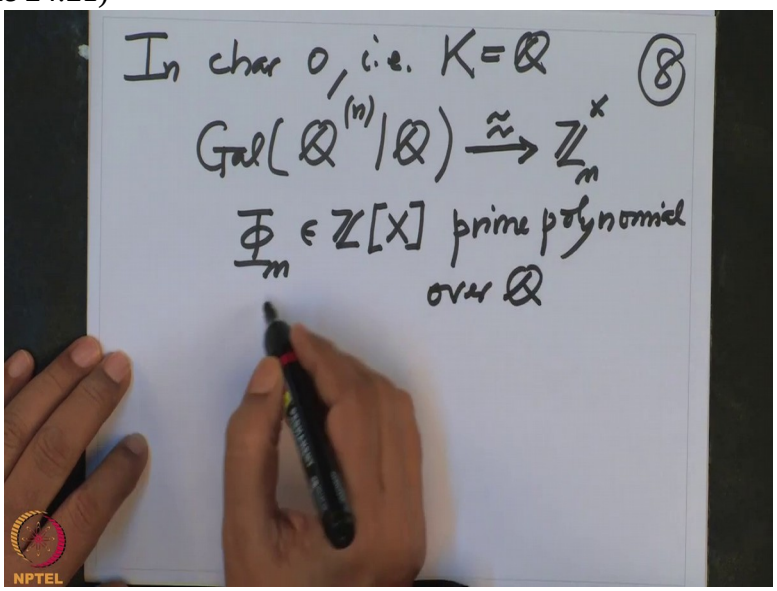
canonical is not the word here because I composed with, the automorphism groups of the roots of unity, that is canonical but identifying that with $\mathbb{Z}_n^x$, that was not canonical.

(Refer Slide Time 23:49)



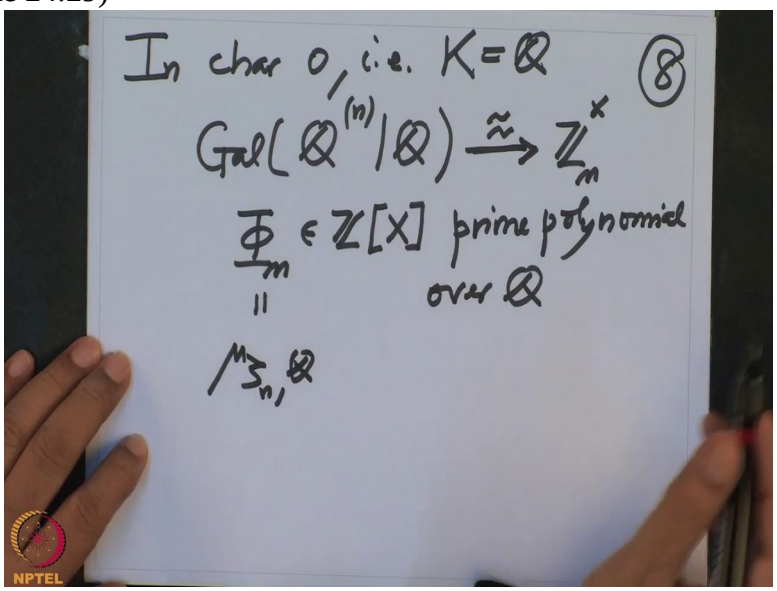
So this is not canonical. But anyway we know it is an isomorphism here. This group is isomorphic to this group. That is what we prove in characteristic 0. And the proof, the main important step in the proof was to prove that this Φ_n , cyclotomic polynomial which is a polynomial with integers, this is prime polynomial in, prime polynomial over $\mathbb{Q}$.

(Refer Slide Time 24:21)



And that is therefore the irreducible, that is therefore the minimal polynomial of ζ_n over $\mathbb{Q}$ and we know this is a Galois

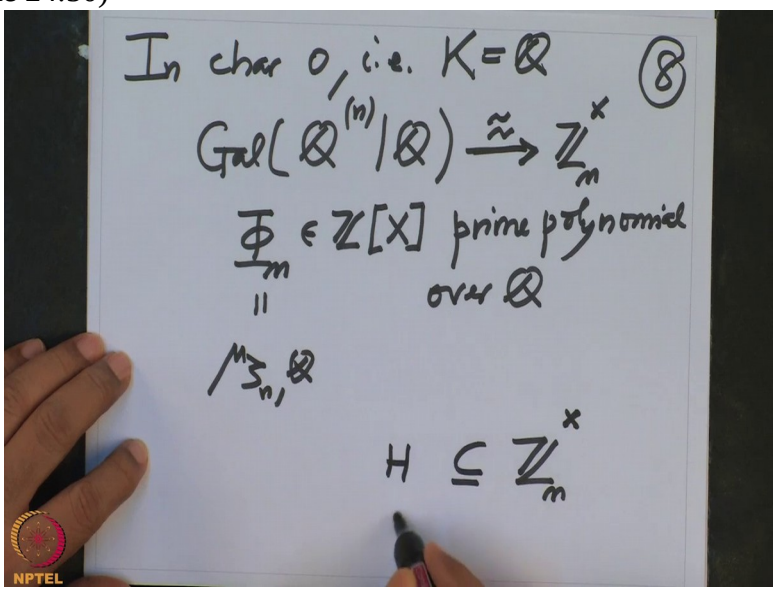
(Refer Slide Time 24:29)



extension and Galois group also we know. Ok now if I take any subgroup, so $\mathbb{Z}_n^x$, this is, this group is a Galois group of cyclotomic field $\mathbb{Q}^{(n)}$ over $\mathbb{Q}$.

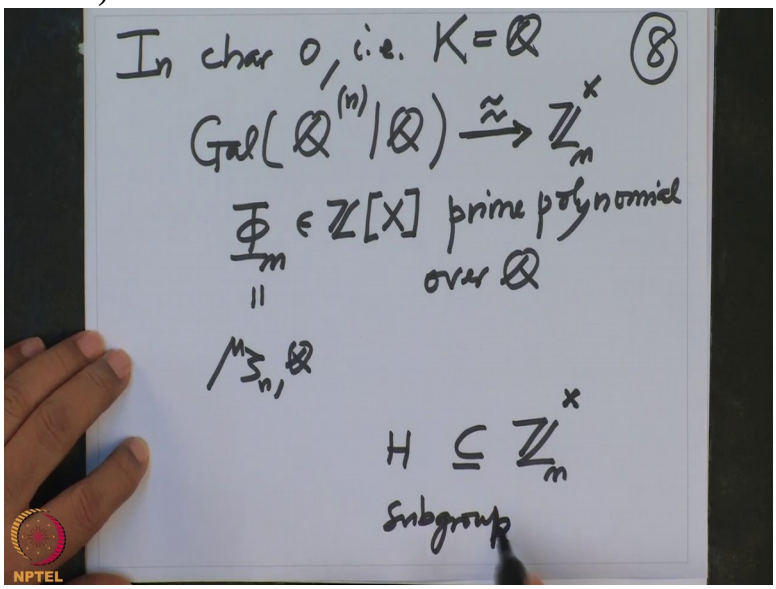
So if I take any subgroup H,

(Refer Slide Time 24:50)



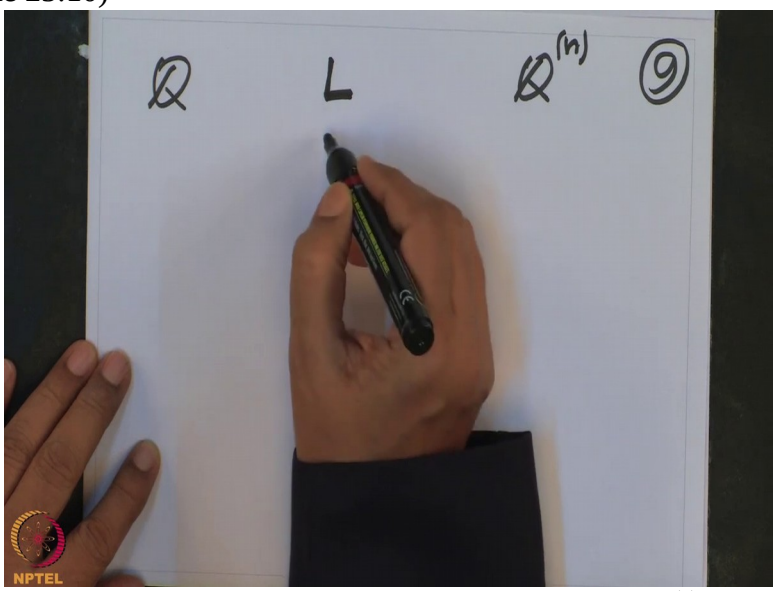
subgroup

(Refer Slide Time 24:55)



then what can I do? Look at, $\mathbb{Q}$ is here. $\mathbb{Q}^{(n)}$ is here. And I have taken the field now here inside. I should call it L probably, L.

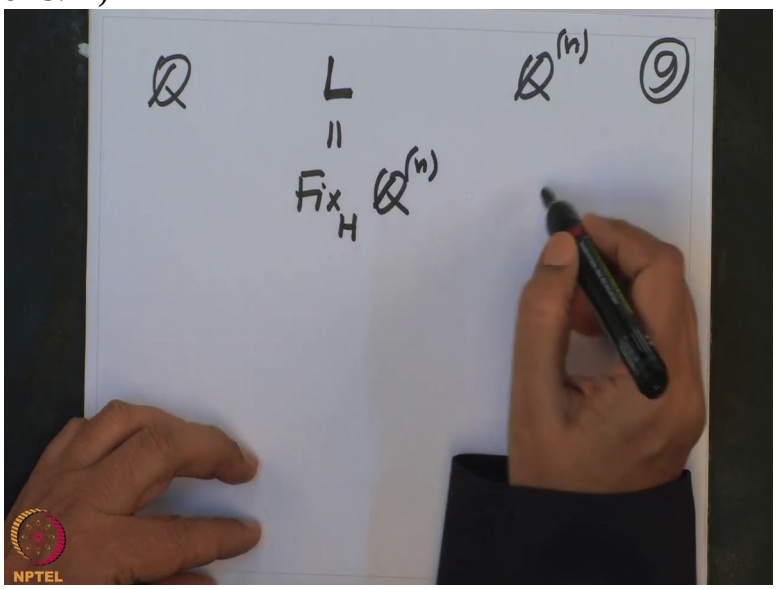
(Refer Slide Time 25:10)



This is precisely a fix field of H under the action of fix field of H $\mathbb{Q}^{(n)}$.

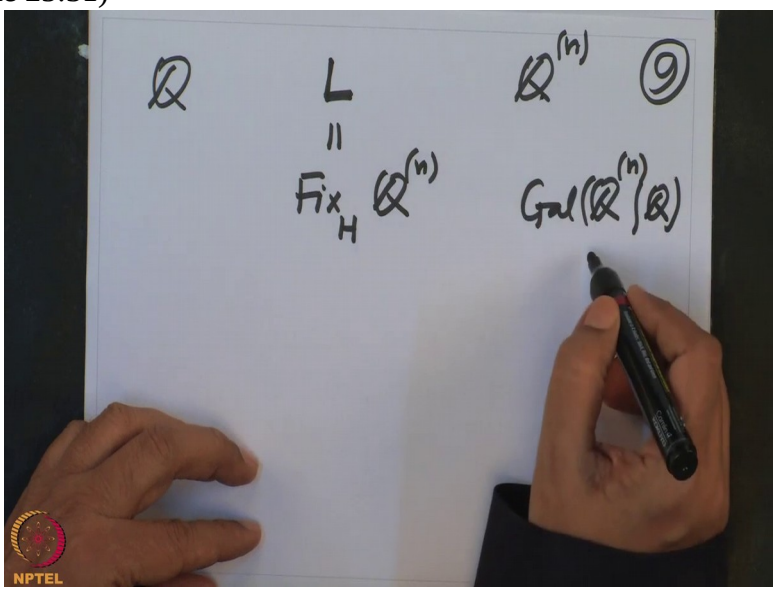
See the

(Refer Slide Time 25:22)



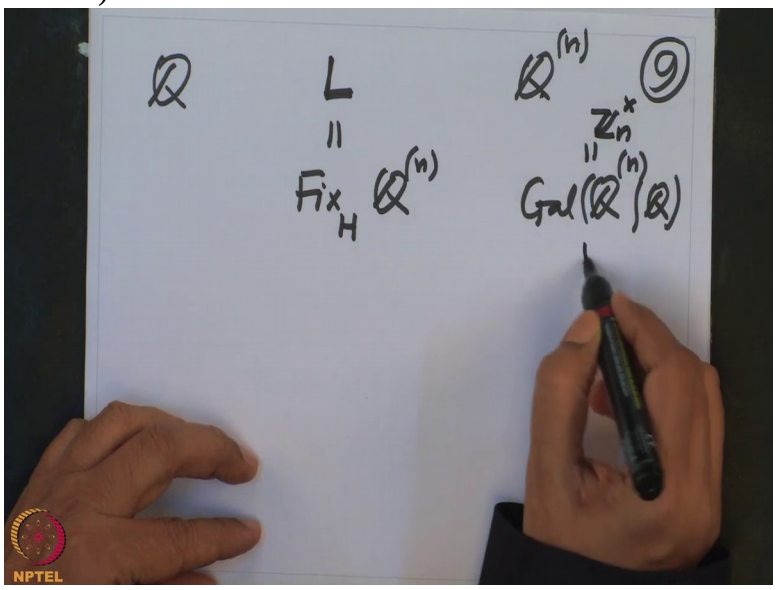
Galois group, $\mathbb{Q}^{(n)}$ over $\mathbb{Q}$, this group is operating on this field and therefore,

(Refer Slide Time 25:31)



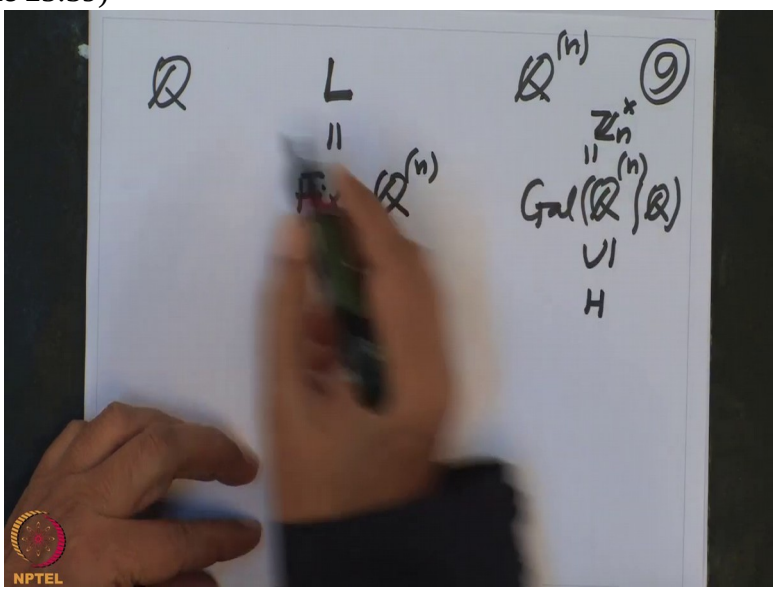
and H is a subgroup here. So this was $\mathbb{Z}_n^x$,

(Refer Slide Time 25:37)



H is a subgroup here. So I can take

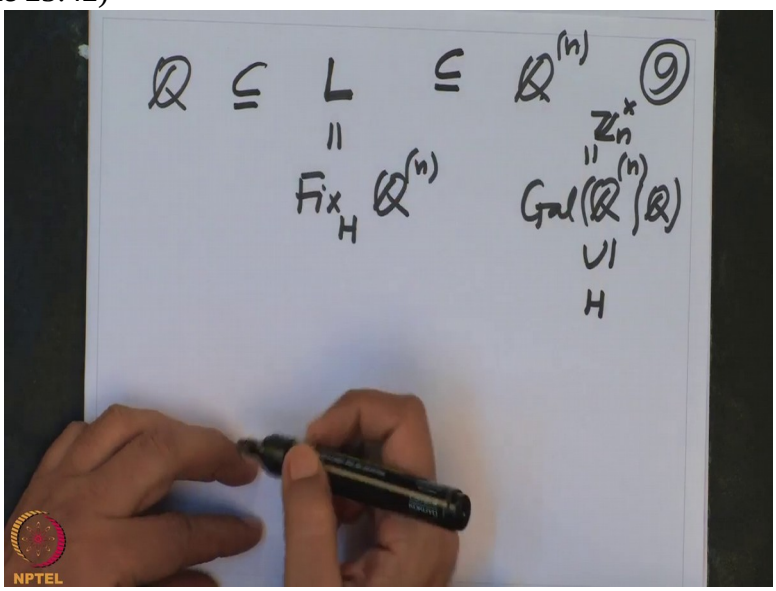
(Refer Slide Time 25:39)



a fix field.

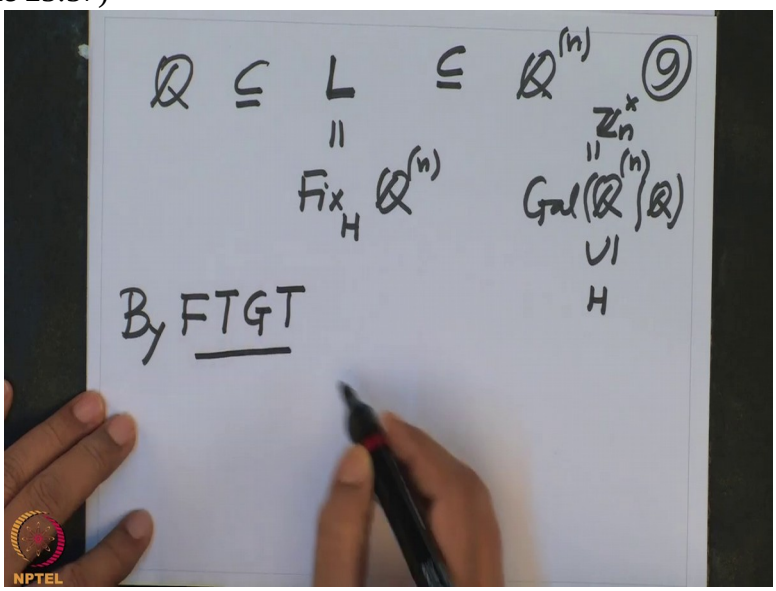
So the fix field is in-between.

(Refer Slide Time 25:42)



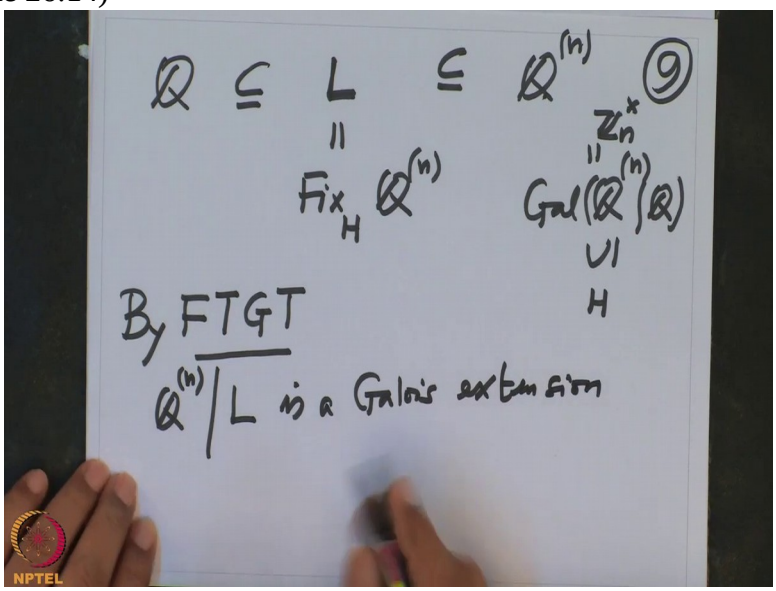
And in the fundamental theorem of Galois theory we saw that this extension by fundamental, I will keep writing, fundamental theorem of Galois theory (FTGT),

(Refer Slide Time 25:57)



this one $\mathbb{Q}^{(n)}$ over L is Galois, is a Galois extension.

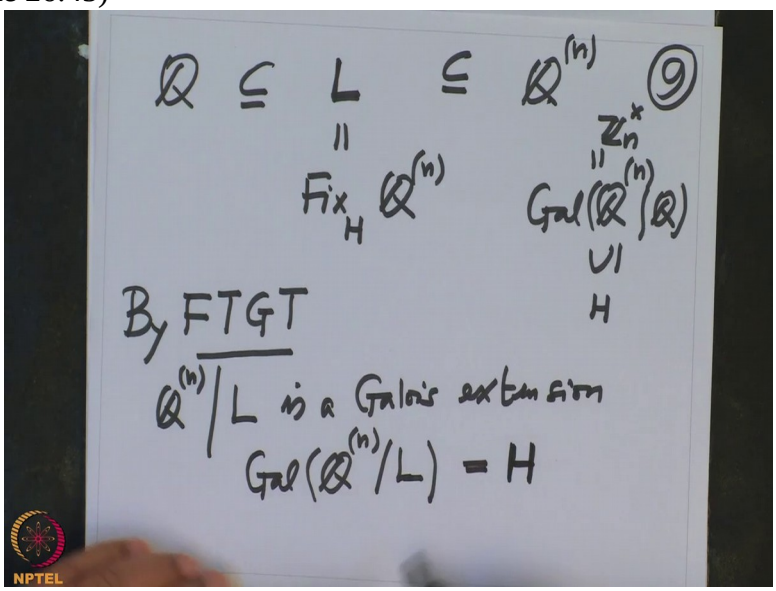
(Refer Slide Time 26:14)



And also what is the order?

Order of the Galois group, so Gal of this, I think I have not checked this when I just proved they are bijective maps. But I will prove now that the Galois group of this over this is, is precisely H. That also

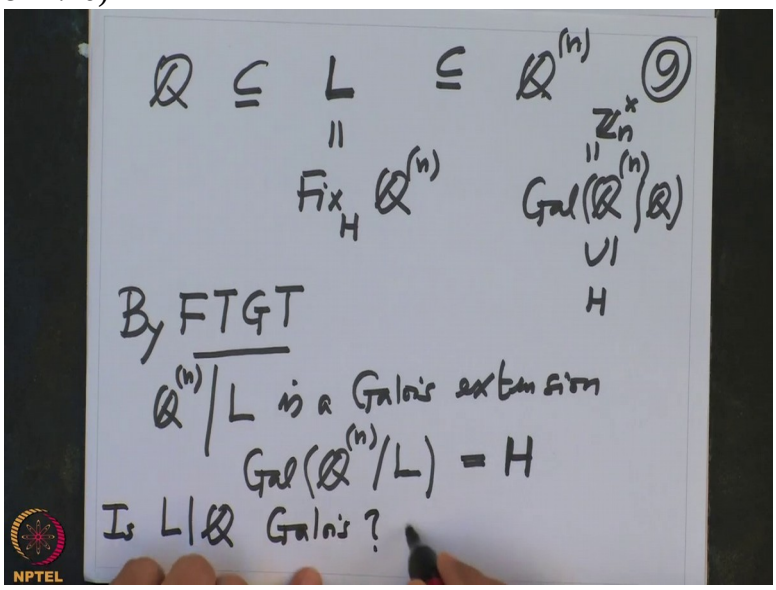
(Refer Slide Time 26:45)



you have checked.

So H, take the fixed field and go, then you get H is a Galois group. Therefore H occurs as a Galois group of $\mathbb{Q}^{(n)}$ over L but now one may ask what about this, L over Q? Is it Galois? Is this extension Galois? And if yes,

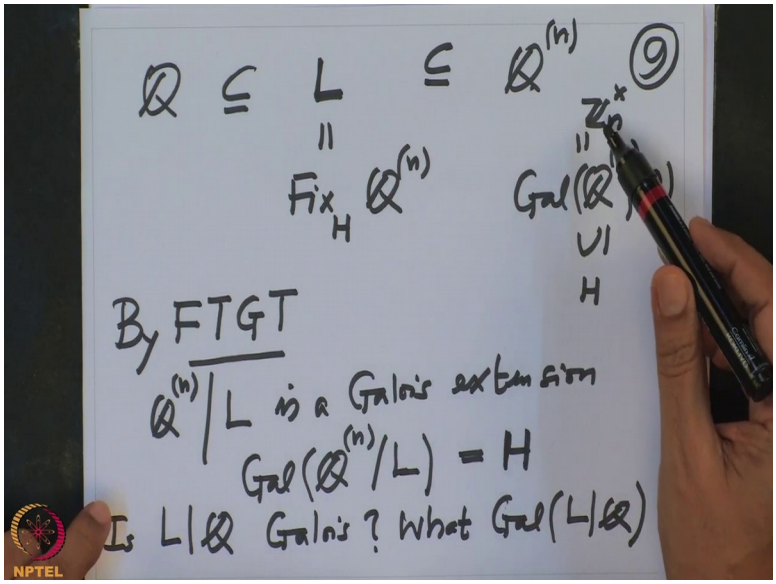
(Refer Slide Time 27:10)



is Galois group of L over $\mathbb{Q}$?

And I will prove in this case, the answer is yes and this Galois group L over $\mathbb{Q}$ is nothing but $\mathbb{Z}_n^x$ modulo of group H. Here the group H is subgroup; it is a subgroup of abelian group.

(Refer Slide Time 27:33)



So H is normal. So the quotient group makes sense. So this question has answer, yes. And this Galois group is nothing but the quotient of the Galois group by the subgroup H. And this I will make it more precise in the next lecture. Next lecture I will check that this extension is Galois and the group is the coefficient.

So that means we need to analyze in a, under the Galois correspondence, when will the fixed field be Galois over the base field? And this we will analyze, that if and only, the subgroup is abelian, subgroup is normal. This is what I will start doing from the next lecture.

Also I want to now decide which group occur as a Galois group over $\mathbb{Q}$? And this is a very important problem. Still the answer is not completely known

(Refer Slide Time 28:47)

and therefore it is of much interest.

And next lecture I will say more things about this. Thank you