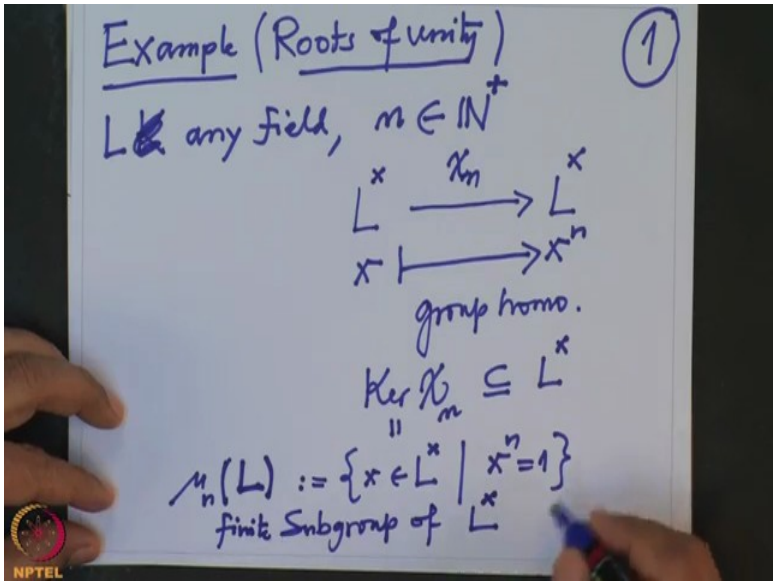
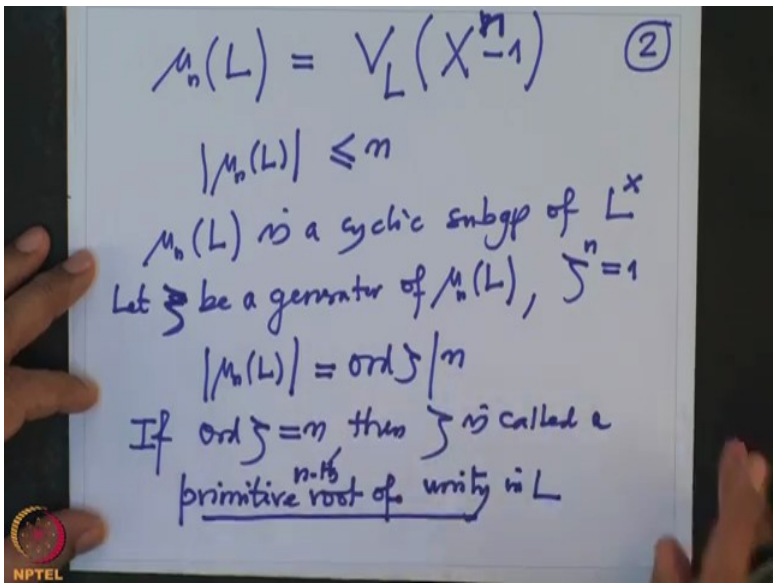
Galois Theory
Professor Dilip P Patil
Department of Mathematics
Indian Institute of Science, Bangalore
Lecture 22
Construction of Finite Fields

We have seen that finite subgroups of the unit group of a field are cyclic and we want to consider one important example where we will use these facts to describe what is called roots of unity.

(Refer Slide Time: 0:45)



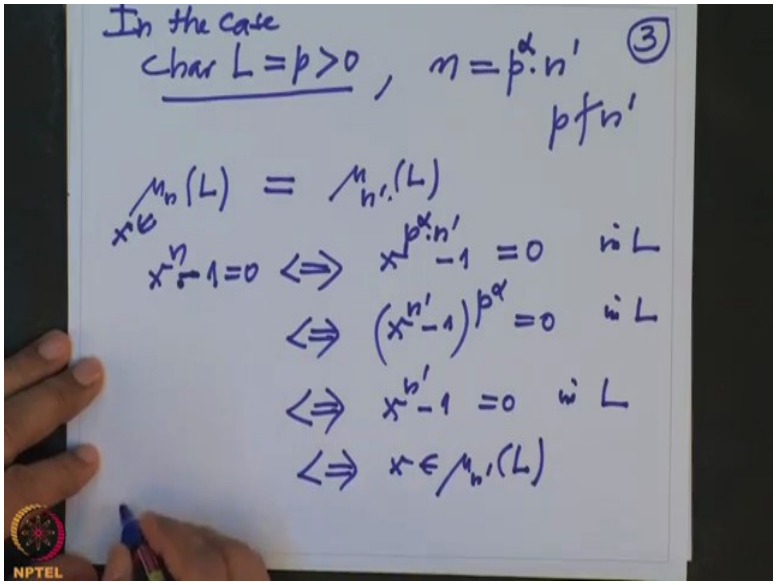
(Refer Slide Time: 03:15)



So let me write this as an example roots of unity, so let K be any field and n be a positive natural number, actually I want to call not K but L, L any field and n be any positive natural number then look at the unit group of L and we have a natural map here namely the power map n, x goes to x^n , this is the power map, this map obviously is a group homomorphism, so therefore it makes central talk about kernel let me call it χ_n , so kernel of χ_n these is a subgroup of L^x and these subgroup is precisely all those elements $x \in L^x$ such that x^n is identity, so these is also these are precisely the n-th roots of 1, so these is denoted by $\mu_n(L)$ it depends on n and it depends on field L, so these is a subgroup of L^x and in fact it is a finite subgroup in fact the cardinality of $\mu_n(L)$ is at most n because $\mu_n(L)$ is precisely in our earlier notation if you remember $\mu_n(L)$ is same as $V_L(X^n - 1)$ they are precisely the zeros of these polynomial, so it is.

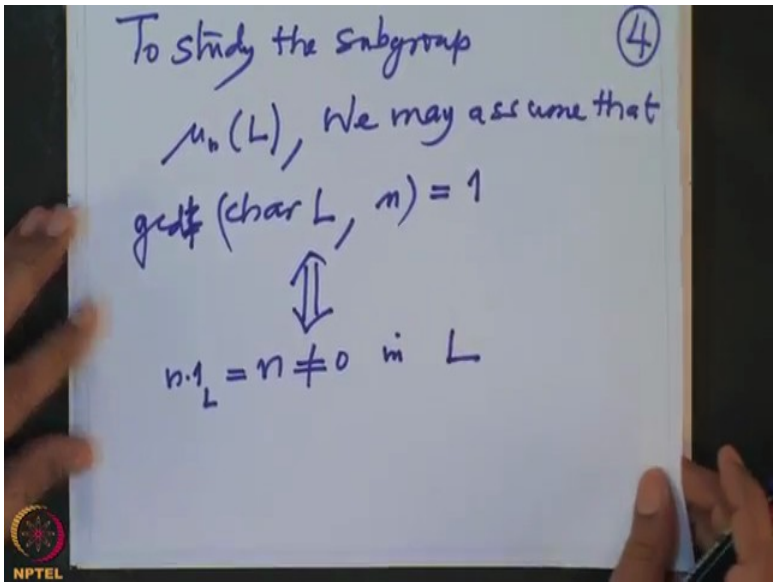
And these cardinality less equal to n, so cardinality of $\mu_n(L)$ is less equal to n, so therefore it is a finite subgroup of L^x so we know it is cyclic, so $\mu_n(L)$ is a cyclic subgroup of L^x so if let ζ be a generator of $\mu_n(L)$ then first of all note that ζ^n is 1 that is by definition of $\mu_n(L)$ and order of therefore order of ζ will divide n and these is order of ζ is same as cardinality of $\mu_n(L)$ so when the order is n if order of ζ is exactly n then ζ is called a primitive root of unity, primitive n-th root of unity in L, note that the primitive unity is defined only when the order is precisely n so it is in this case when one talks about primitive n-th root that means $\mu_n(L)$ has order n and ζ is the generator of $\mu_n(L)$.

(Refer Slide Time: 05:57)



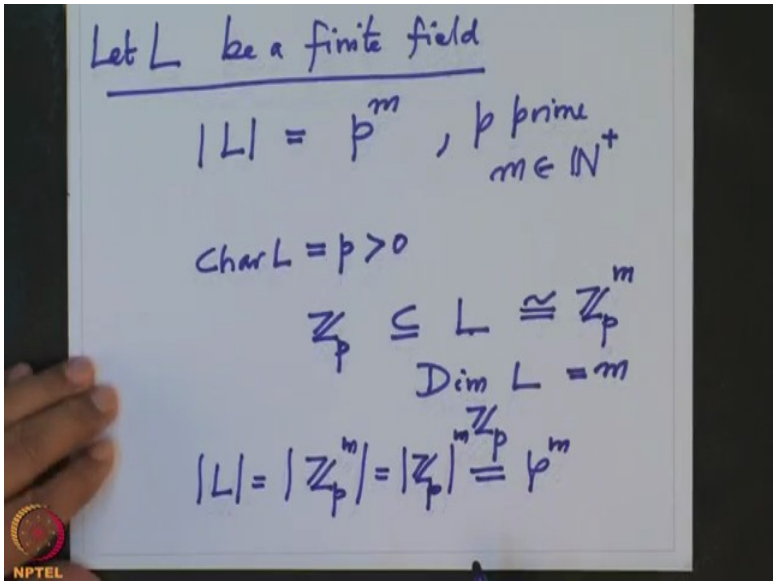
So if the note if characteristic is p what happens if characteristic of the field is p which is positive in the case you write is given n as take out as much power of p can come out $p^{\alpha}n'$ where p does not divide n' then $\mu_n(L)$ and $\mu_{n'}(L)$ they are same because when somebody belongs here x belongs here means what that means x^n is equal to 1 or $x^n - 1$ is zero but these is equivalent to saying $x^{p^{\alpha}n'} - 1$ is zero these is equivalent to saying $(x^{n'} - 1)^{p^{\alpha}}$ is zero and the zero is all are in L but L is a field so these is equivalent to saying $x^{n'} - 1$ is zero in L, so that is equivalent to saying x is in $\mu_{n'}(L)$, so the groups are not changing if you through away the if you cancel the power of the characteristic from n, So therefore one may we may assume there for to study.

(Refer Slide Time: 07:39)



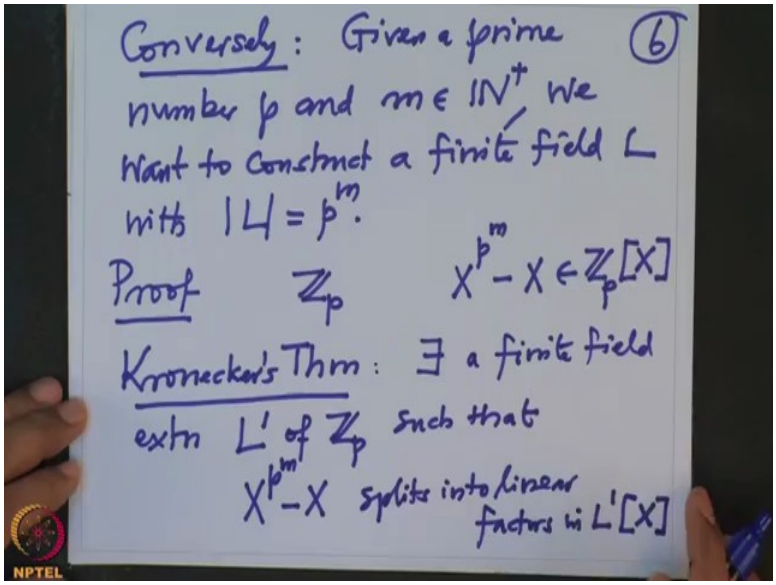
So I will note it down very important reduction so to study the subgroup $\mu_n(L)$ we may assume that p, the characteristic of L and n are co-prime, the gcd of these is 1 already characteristic zero we do not have to assume anything, characteristic p we have to assume p does not divide 1 but these can be neatly written as these is equivalent to saying n is not equal to zero in L when you say n that means the n times 1 these is not zero in L that is where when if the characteristic is positive if the characteristic is positive if the characteristic zero these is always true so that is a very important reduction to study the roots of unity and (I will come) we will come back to it when we construct field extensions whose the Galois group precisely this group, ok alright.

(Refer Slide Time: 09:10)



So now we want to I want to come back to a proof where the structure of the finite fields or L, L be a finite field then first of all we note we last time also we noted that the cardinality of L must be power of a prime numbers p^m where p is prime and m is non zero natural number, these is because we know that the characteristic of finite field must be a positive characteristic L must be p positive and then L will contain a prime field $\mathbb{Z}_p$ and because L is finite dimension of L as a $\mathbb{Z}_p$ vector space it is positive m finite dimensional vector space so therefore these L will be isomorphic as a vector space to $\mathbb{Z}_{p^m}$ in particular cardinality of L must be cardinality of $\mathbb{Z}_{p^m}$ which is $\mathbb{Z}_p$ cardinality power m so which is p^m so we proved that if you have a finite field the cardinality is nothing but power of a prime number p.

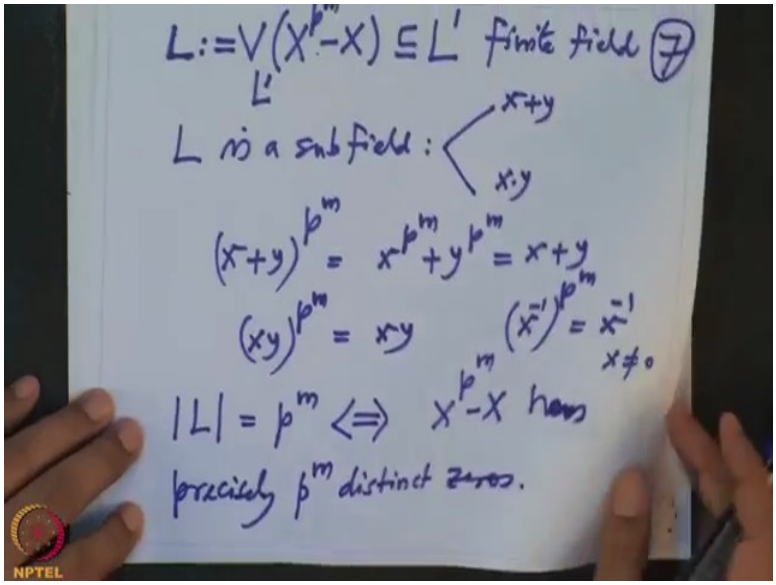
(Refer Slide Time: 10:55)



Conversely I want to prove that if I have any finite field no conversely I want to so conversely given p given a prime number p and a positive natural number m we want to construct a finite field L with cardinality p^m , for m equal to 1 it is obviously the field we can take is $\mathbb{Z}_p$, ok. So proof so we have given p so that means we have given $\mathbb{Z}_p$ and then you look a we therefore can look at the polynomial $X^{p^m} - X$ these is a polynomial think of these is a polynomial over $\mathbb{Z}_p[X]$, alright.

Now, I want to used Kronecker's theorem, Kronecker's theorem says that given any polynomial or any field I can find a bigger field so that all zeros of that field of the that polynomial lies in that field, so by Kronecker's theorem there exists a field extension finite field extension L' of $\mathbb{Z}_p$ such that $X^{p^m} - X$ these polynomial splits into linear factors in $L'[X]$ and these is a finite field extension of these so in particular L' is also finite, alright.

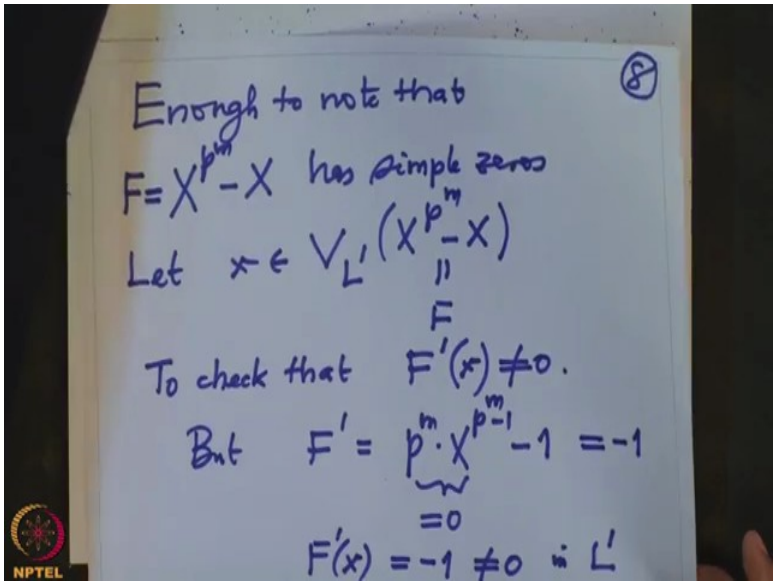
(Refer Slide Time: 13:37)



So L' is also finite field and anyway I want to consider the all the zeros of the these polynomial, so zeros of these polynomial $V(X^{p^m}-X)$ in L', so these set I want to call it L so they are the zeros of these polynomial and they are precisely ok will worry about how many are there but right now we checked that these actually form a sub field so for that I have to checked that so we will checked that L is a sub field so for these I have to checked it is closed under addition and also multiplication and inverses of course, so that means if x is a zero of these, y is a zero of these then $x+y$ is also zero of these that is what we have to check (but) for that is very easy $(x+y)^{p^m}$ these is because a characteristic is p, $x^{p^m}+y^{p^m}$ but x^{p^m} is x and y^{p^m} is y, so therefore this similarly this and also x inverse power p^m equal to x inverse, that is we don't have to checked this because for these is when x is not zero, so it is a subfield, alright.

Now if I want to claim that the cardinality of L is precisely p^m but to check that I have to checked that these polynomial so to these is if and only if the polynomial $X^{p^m}-X$ has precisely p^m distinct zeros, that means I have to checked that these polynomial all the zeros are simple.

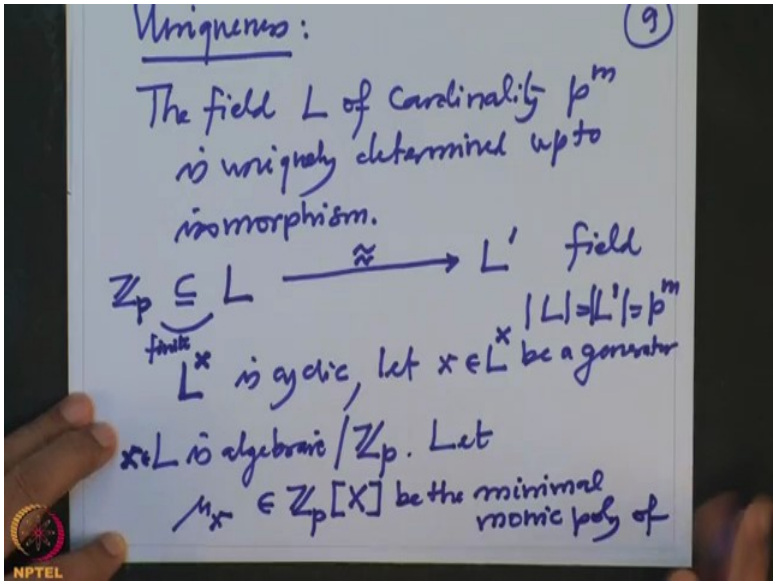
(Refer Slide Time: 16:12)



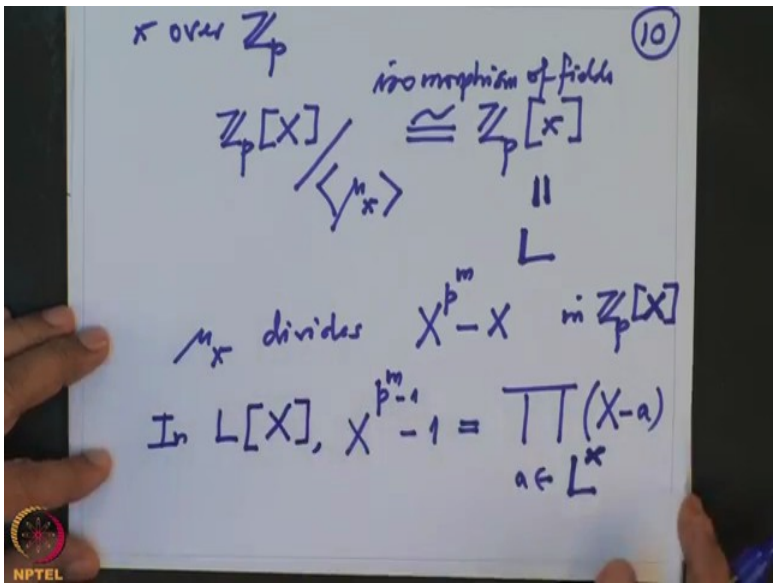
So to check this so it is enough to note that the polynomial $X^{p^m} - X$ has simple zeros that means no repeated zeros and how does one check that when I should differentiate and checked whether that is a zero of these, so let x be a zero of these polynomial let us called these polynomial as F and I want to check now to check that if I take F' and evaluated these small x this is not zero but what is F' we have to differentiate these polynomial with respect to X but p is a characteristic so these is $p^m X^{p^m-1} - 1$ but these is zero p is zero therefore these is zero so these is -1 .

So therefore $F'(x) = -1$ it is constant, so an -1 cannot be -1 is not zero in L therefore we have checked that these polynomial has only simple zeros and it has precisely therefore p^m zeros so that checked that the zero set of these polynomial in arbitrary field extension where these polynomial splits has precisely $n = p^m$ elements and that is a required field.

(Refer Slide Time: 18:19)



(Refer Slide Time: 21:33)



Now we auto prove the uniqueness, so uniqueness that means we want to prove that if I have 2 fields of the cardinality p^m then they are isomorphic, so suppose so I will write a statement first the field L of cardinality p^m is uniquely determined up to isomorphism, ok that means what that means if I have two fields L and L' fields with the same cardinality p^m then I want to find an isomorphism yes, alright.

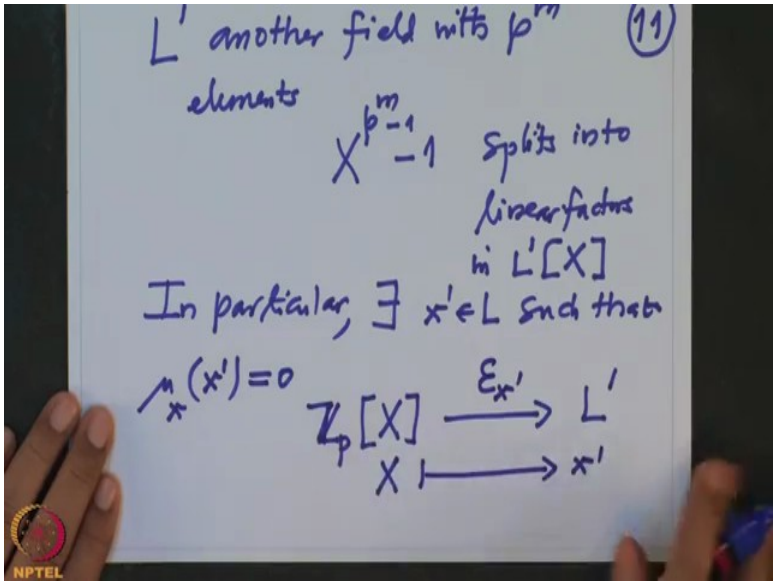
So let us look at L^x now L is a finite field so these is a finites of group of L^x so these groups is cyclic we have proved it, so let x in L^x be a generator, ok now these L contains $\mathbb{Z}_p$ because characteristic is p, characteristic has to be p you know we have noted that if

the power is the cardinalities power of p then p has to be the characteristic so it will contain the field $\mathbb{Z}_p$ and because these L is a finite field these extension is a finite extension in fact finite of degree m and in particular there for algebraic L is algebraic over $\mathbb{Z}_p$, so in particular these element x which is a generator of L^x is algebraic of $\mathbb{Z}_p$.

So let μ_x be a μ_x belonging to $\mathbb{Z}_p[X]$ be the minimal monic polynomial of x or $\mathbb{Z}_p$ alright, so what is L so now therefore what do we know or the property of minimal polynomial that is when I take $\mathbb{Z}_p[X]$ mode ideal generated by μ_x these is isomorphic to $\mathbb{Z}_p$ adjoin x these is precisely remember the evaluation map the polynomials evaluating at these small x the kernel is precisely generated by the minimal monic polynomial and the image is precisely the subfield generated by x.

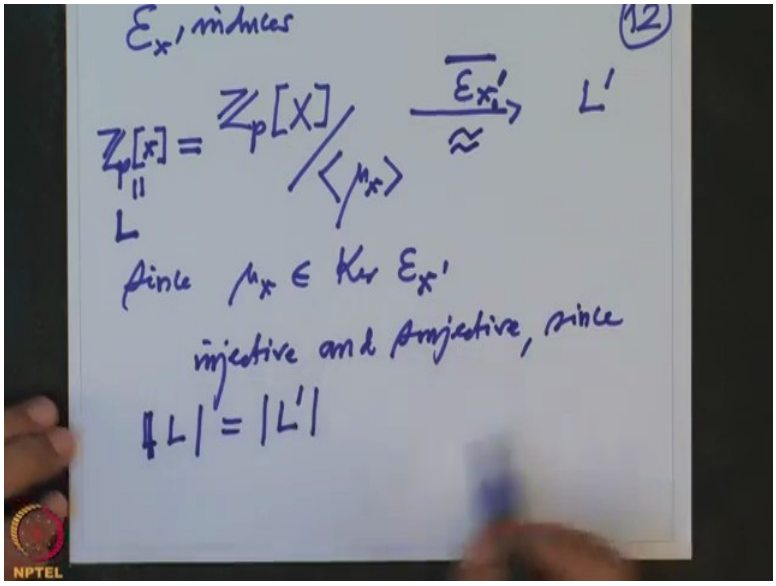
So these is a field and these is an isomorphism of fields, alright but these is what because x is a generator these is precisely L, x is a generator of L^x means every element of L^x are the powers of x and therefore in particular they are polynomials in x so these field is precisely L alright. Now we know that these polynomial μ_x is 1 and the look at the other polynomial $X^{p^m}-X$ these is the polynomial where x also satisfy because x is an element in L so therefore μ_x these polynomial is in the kernel therefore μ_x has to divide μ_x divides these polynomial in $\mathbb{Z}_p[X]$ in $\mathbb{Z}_p[X]$ because these is polynomial where x satisfies and these is another polynomial where X this is minimal so therefore these has to divide these here but when I these polynomial has all roots in L therefore when you threw away X take a common factor $X^{p^m-1}-1$ these polynomial is precisely the product of $X-a$ where a varies in L^x because when I threw away X we get these polynomial has distinct roots when I threw away when X you get a polynomial of degree p^m-1 and L^x also has m elements so all linear factors will occur there because so these polynomial splits like these in $L[X]$, these splitting is in $L[X]$ these.

(Refer Slide Time: 25:07)



Now let us take the L' was another field, L' another field with p^m elements and we have noted that these polynomial $X^{p^m-1}-1$ these splits into linear factors in $L'[X]$ also so therefore and μ was the factor of these therefore we know there exists so in particular there exists $x' \in L$ such that $\mu_x(x')$ is zero because μ was a factor of these μ was a factor of $X^{p^m}-X$ therefore will be 1 and X is not zero so x' will be a zero of these μ and then we have these map look at the map $\mathbb{Z}_p[X]$ to L' the map is evaluation map $\epsilon_{x'}$ so X capital X go to x' then obviously these μ goes to zero, so therefore we will get so these will induce.

(Refer Slide Time: 27:21)



These ϵ_x induces $\mathbb{Z}_p[X]$ modulo ideal generated by μ_x to L' because μ is in the kernel of these max since μ_x belong to kernel of ϵ_x but now these is a field these we know these is precisely $\mathbb{Z}_p[x]$ small x but these is precisely L so these is a field and these goes inside these L', so these map these ϵ_x these map bar these map is injective because these is a field from a field it cannot have kernel field has no ideal other than zero and itself so these may have be injective and also surjective because surjectivity will follow from the fact that both L and L' have the same cardinality so pigeonhole principle will tell you in injective map same cardinality set has to have bijectivity.

So since cardinality of L equal to cardinality of L' so therefore these is actually an isomorphism because it is bijective maps (so it is isomor) so that proves our claim that L and L' are isomorphic.

So remember that we have proved two very important observation today namely one was every finite subgroup of group of units of a field is cyclic and we have used that track to check that any two finite fields of the same cardinality are isomorphic and cardinality of a finite field can only be power of a prime and any two such fields are isomorphic, so we have also constructed them explicitly how to construct and the (constructor) construction is by using the polynomial $X^{p^m} - X$ and we will continue in the next lecture some more consequences I want to deduce from this observations, thank you.