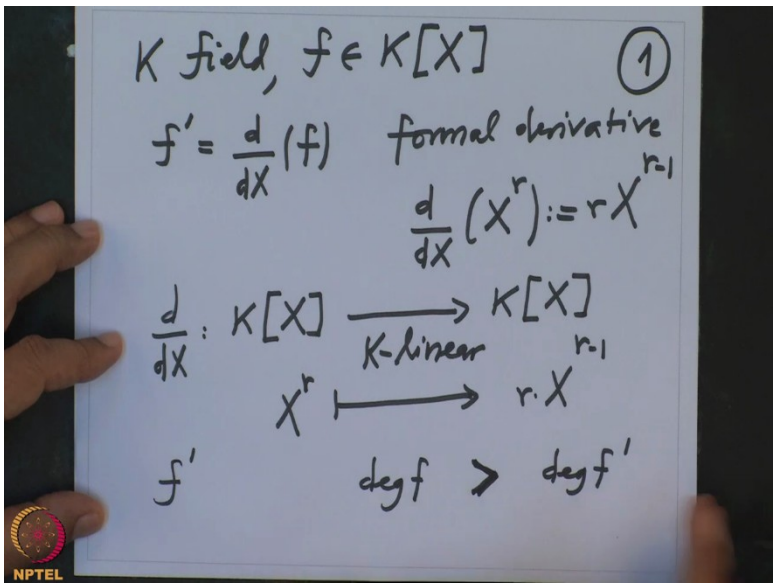
Galois Theory
Professor Dilip P. Patil
Department of Mathematics
Indian Institute of Science Bangalore
Lecture 55
Perfect fields

Okay, last lecture we have been seeing about field extension, Galois group, and normal extensions. Today I want to start with separable extensions and to do separable extensions I 1st digress little bit on the separable polynomials so let us recall that.

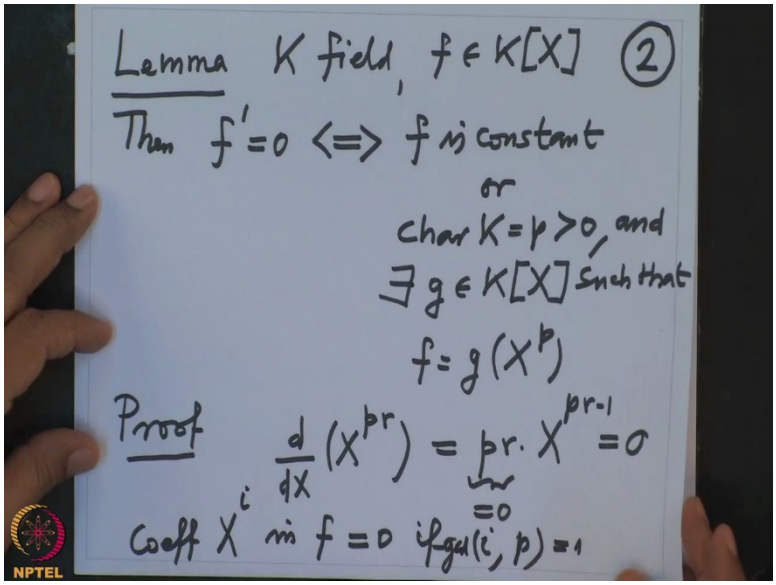
(Refer Slide Time: 0:58)



We have also used this terminology before so let K be a field, so this is our base field and f is a polynomial with coefficients in X with coefficients in K. So recall that when I write f' that is by definition $\frac{d}{dx}$ of f, this is formal derivative of f that simply means you just use the formulas like $\frac{d}{dx}$ of the powers of X^r that is by definition $r X^{r-1}$ and use the linearity. So this $\frac{d}{dx}$ is a linear map from the polynomial ring in one variable over K to itself, this is K linear where the bases element here that X^r that goes to $r X^{r-1}$ and extended linearly.

So therefore given any polynomial f, we have another polynomial f' and the degree of f and degree of f', so the degree of f will strictly be less than degree of f'. It might happen it is much less, it might so let us list some of the easy facts about this.

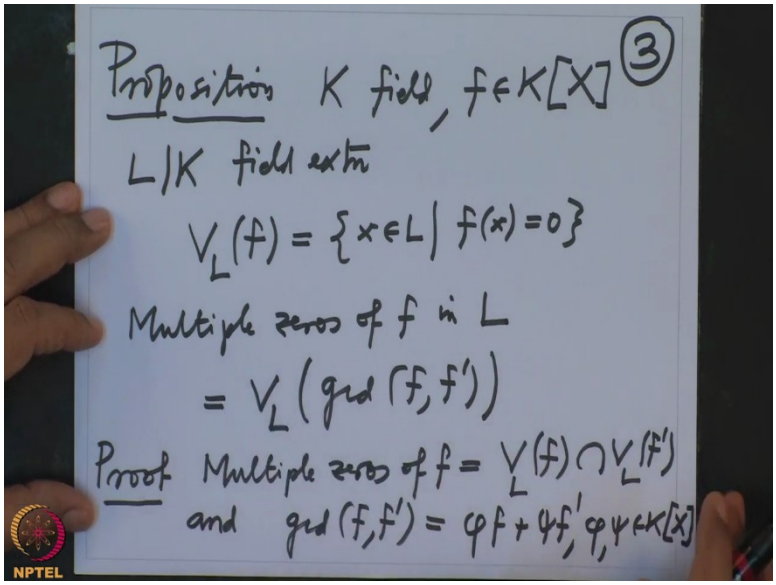
(Refer Slide Time: 2:51)



So for example, let us write it as lemma so K field and f belongs to $K[X]$, then f' is 0 if and only if f is either constant, f is constant or characteristic of the field K is p which is positive and there exist a polynomial g in $K[X]$ such that f will be equal to g of X power p. So only the powers of X^p are surviving as coefficients in the polynomial f, only the coefficients of powers of X^p are nonzero, other coefficients are 0. This is very simple proof, this follows immediately from the fact that if I differentiate $\frac{d}{dx}$ of X^{pr} , this is $pr\,X^{pr-1}$, but p is characteristic so this is 0 therefore this is a 0 power.

So therefore, if f' is 0 it cannot have X^i coefficient of X^i in f is 0 if i and p are co-prime, GCD is 1 because if i and p are co-prime, this i when I differentiate this, this is i times X^{i-1} and i is non-zero in the field because it is co-prime to p therefore it is immediate from this this equivalence so I leave the details to verify they are very easy. Okay now also immediate from this is the following so another proposition.

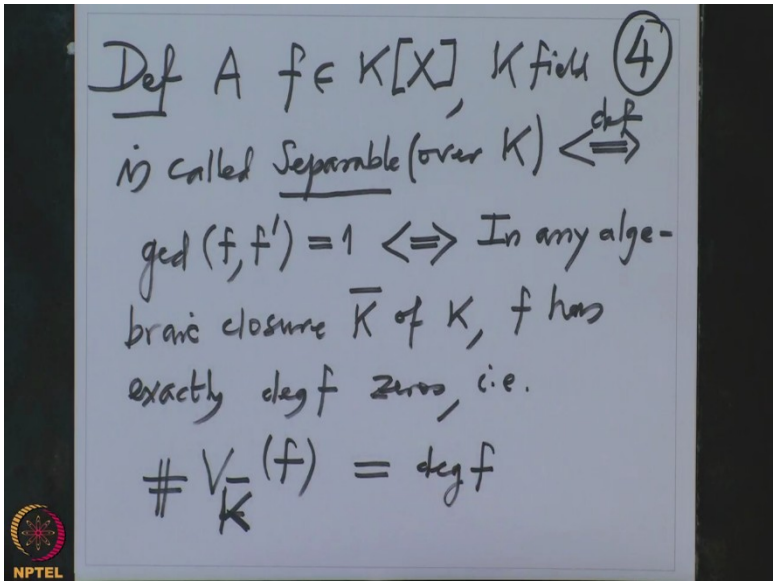
(Refer Slide Time: 5:13)



This says the following, if we have a polynomial K field and f is a polynomial in $K[X]$, remember that our goal in this course is always to study zeros of a polynomial so and that includes multiple zeros. Now I am going to reduce the study to the simple zeros so therefore we want to state some easy facts about when the zeros can be multiples. So and suppose L over K is field extension and we are looking at the zeros of $f \in L$, these zeros and among them I look at the multiple zeros so the multiple this is the set of zeros $x \in L$ such that $f(x)$ is 0. We know that there are utmost degree f times as many as degree f utmost and among them multiple zeros, so multiple zeros of $f \in L$, this set so this is precisely the set of zeros of L in L of the GCD so this is also clear.

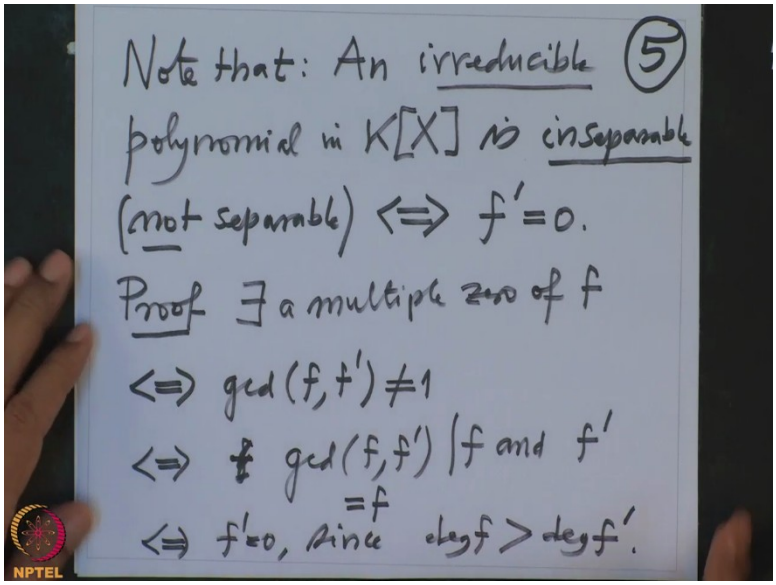
So proof, so we know multiple zeros are precisely the common zeros of f and f' so these multiple zeros of f, this is precisely $V_L(f) \cap V_L(f')$. And also we know this equality will follow from this equality and the fact that GCD of f and f', we can always write it as a $K[X]$ linear combination of f and f', where Phi and Psi are some polynomials in $K[X]$, both these equalities will give you this so I will leave that details to the verification, alright.

(Refer Slide Time: 8:01)



Now let us recall when do you call so definition, a polynomial f in $K[X]$, where K is a field is called separable over K, I will drop this over K always saying, it will be understood from the context I write, this is separable if and only if that this is the definition that GCD of f and f' is a unit that is 1 alright. But this is equivalent to saying obviously that in any algebraic closure $\overline{K}$ of K, f has exactly degree f zeros that is in symbols cardinality of the zero set of f in $\overline{K}$ is precisely equal to degree of f, this is then we call the polynomial to be separable over K, alright.

(Refer Slide Time: 9:48)

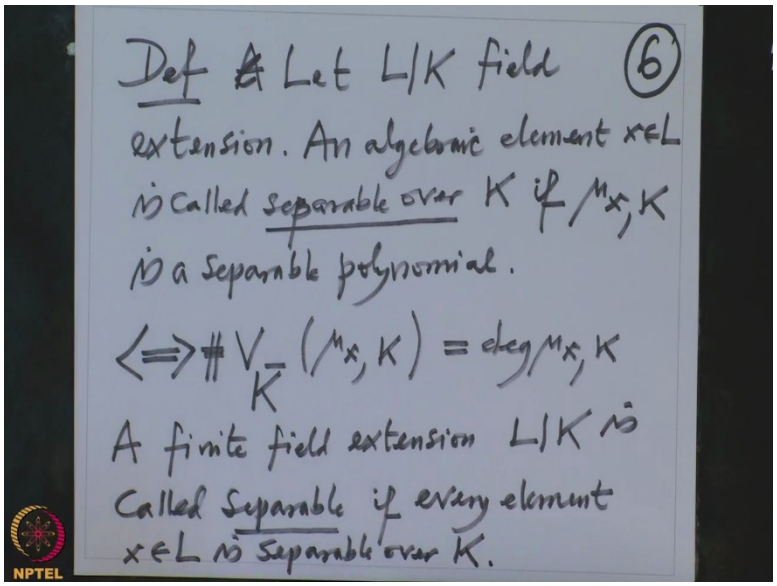


So first of all easy consequence so note that an irreducible polynomial in $K[X]$ is inseparable, when I say inseparable that means not separable if and only if f' = 0. This is

easy because if f' is not 0 then the GCD will be if it is inseparable then the GCD has to be non-constant polynomial therefore f' is 0 alright. So okay let me write proof, I have to check that I have given that the polynomial is inseparable, inseparable means so there exist a multiple zero of f.

When do there exist multiple 0? That is if and only if GCD of f and f' is nonzero, not equal to 1 that is what we have seen in this earlier proposition, this proposition is precisely it is a multiple 0 is precisely the common 0 of f and f' and that is equivalent to saying GCD is non-constant polynomials that is precisely inseparable definition but this GCD is non-one means that is if and only if GCD has to divide both f and f', but that will mean and if f is irreducible so that will mean that the only possibility for GCD equal to f and then f has to divide f', but by the degree ground that we will say that f' is 0 since degree of f is strictly bigger than degree of f'. So therefore inseparability of a polynomial is simply tested by computing the derivative of that polynomial and checking whether the derivative is 0 or not 0, alright.

(Refer Slide Time: 13:00)

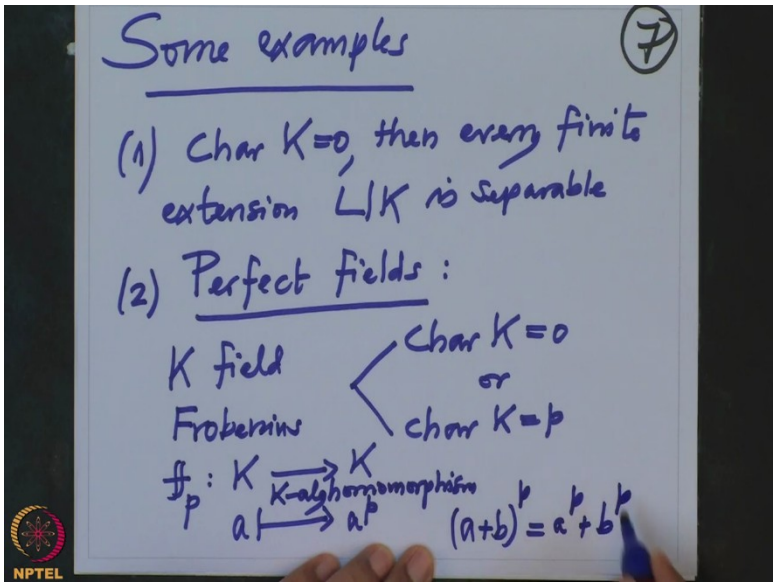


So we know about the polynomial being inseparable, so now I want to define so another definition, a finite field extension is not necessary, let L over K be any field extension, may not be an algebraic. So an algebraic element x in L is called separable over K if the minimal polynomial of x over K is a separable polynomial. But we know this is equivalent to saying that the zeros of μ in $\overline{K}$, this cardinality is precisely equal to the degree of $\mu_{x,K}$, this is what we call the element to be separable and we will call the finite field extension L

over K is called separable if every element is separable, every element x in K is separable over K.

So before we go onto the theorems about separable extension, I would like to give examples of a algebraic extensions which are separable or examples of the field K where every algebraic extension of K is separable, so those are precisely called perfect fields so some examples.

(Refer Slide Time: 15:46)

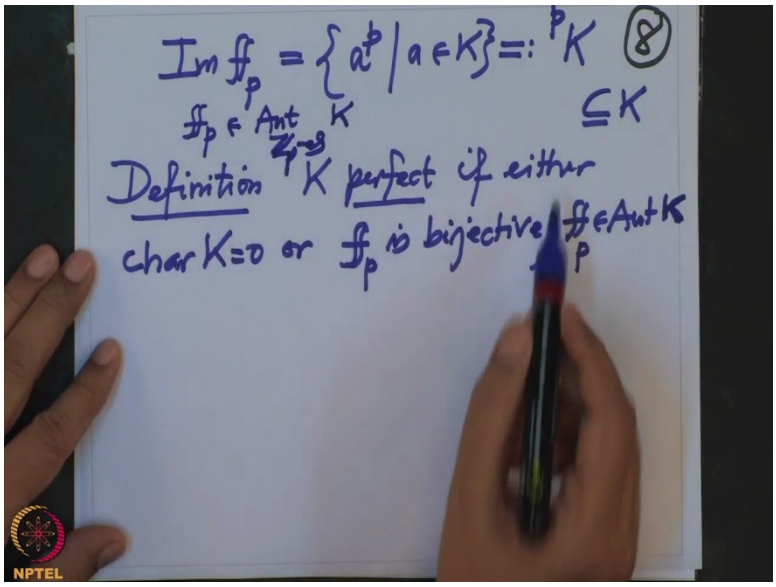


First of all, if characteristic K is 0 then every finite extension L over K is separable that is very clear because in case of characteristic 0 irreducible polynomial cannot be inseparable that we have seen because inseparability is equivalent to saying that the derivative is 0 but that can only happen when the field when the polynomial is a constant polynomial, so characteristic 0 case every finite extension is separable. Now 2, so called perfect field so this is what I want to digress on perfect fields.

So first the definition and then we will check that the fields are perfect okay so perfect field means so we have a field K and there are 2 possibilities for this, characteristic K is 0 or characteristic K equal to p and in this case we would like every characteristic 0 field to be perfect, so let me complete the definition. So an characteristic p K we have this Frobenius map f_p, f_p is from K to K, the map is any a going to a^p , remember this is called Frobenius and this is a K algebra automorphism that is clear because we have to check that respect to addition and multiplication, multiplication is obvious and addition because we

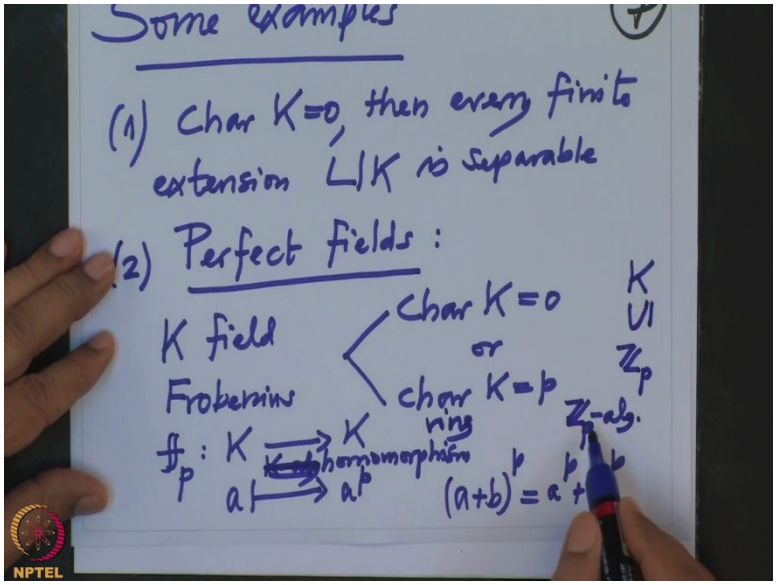
know it is a characteristic is p therefore a + b when you expand by binomials we get $a^p + b^p$ so that shows that this is a K algebra automorphism.

(Refer Slide Time: 18:38)



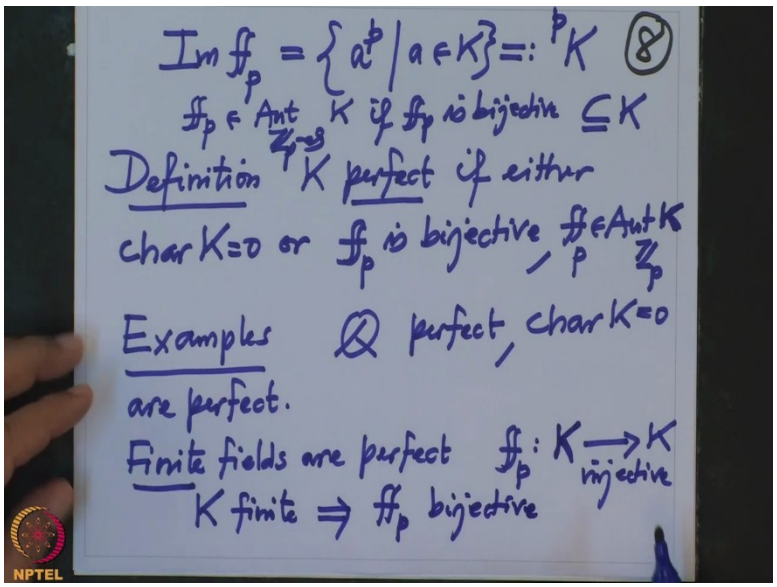
And therefore we can talk about the image of this, the image of this Frobenius in f, these are precisely the elements p powers of elements in k, this is also I will denote it by ^pK , I will denote p on this side because if I write it on this side one might get mistake with K power p which is the vector space of dimension p that is not what we mean here, this is the p powers of elements from a so therefore this is clearly containing K and now we say that K is perfect so definition K is perfect if either characteristic of K is 0 or f_p is bijective that means this means f_p belongs to Aut K.

(Refer Slide Time: 19:59)



I made mistake by saying here this is not a K algebra automorphism, this is a ring automorphism. All that one can say that this is a $\mathbb{Z}_p$ algebra automorphism $\mathbb{Z}_p$ algebra automorphism because characteristic is P therefore K will contain $\mathbb{Z}_p$ as a subfield and as a $\mathbb{Z}_p$ algebra it is a $\mathbb{Z}_p$ algebra automorphism.

(Refer Slide Time: 20:47)

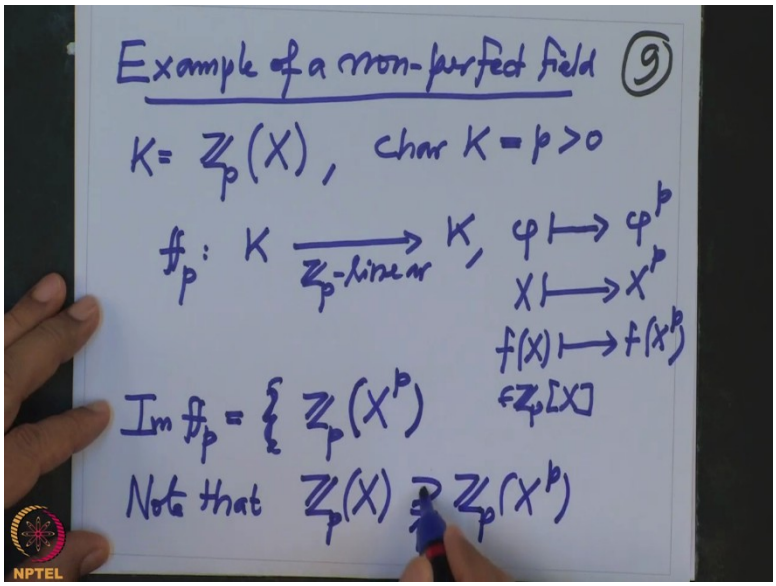


So this frobenius is an element in this f_p is an element in Aut $\mathbb{Z}_p$ algebra K if it is surjective this is $\mathbb{Z}_p$, this is if f_p is bijective, but because it is a field it is always Injective and therefore surjectivity of f_p is more important alright, so that is field is called perfect if either characteristic is 0 or frobenius is a bijective map equivalently f_p is an automorphism of $\mathbb{Z}_p$ algebra okay alright. Now we want to so first of all some examples

of perfect field, so examples so $\mathbb{Q}$ is perfect or any other characteristic 0 fields are perfect, finite fields are perfect finite fields no matter what their characteristic is, finite fields are perfect.

This is simply because we have to check that f_p is surjective so if K is a finite set, I know because K is a field and this is a ring automorphism, this is always injective and to test surjectivity in case of finite, if K is finite it is enough to check that it is injective. So K is finite so the pigeon hole principle will tell that f_p is actually bijective so therefore by definition finite fields are perfect, alright.

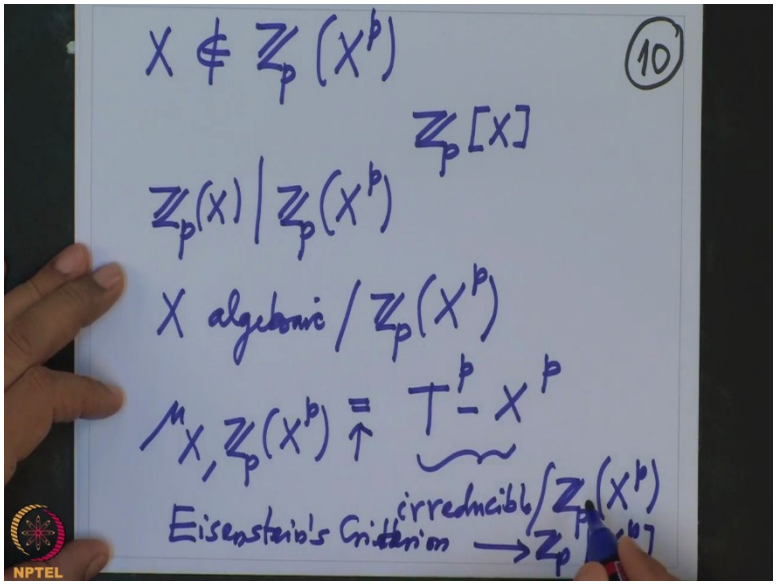
(Refer Slide Time: 22:48)



At least 1 example of a non-perfect field, so example of a non-perfect field. Okay that is now you take for example, you take $\mathbb{Z}_p$ and take rational function field in one variable this is my field K, note that the characteristic is K characteristic is p positive okay. And now let us look at the frobenius. Frobenius f_p this is a map from K to K any f in a rational function Phi going to ϕ^p , in particular X is going to X^p and if I have a polynomial $f(X)$ it is then going to f of X power p because this map is $\mathbb{Z}_p$ linear so polynomial has coefficients in $\mathbb{Z}_p$, this is the polynomial in coefficients in $\mathbb{Z}_p$ therefore by linearity it is X. I know where X go therefore I know where the whole polynomial will go so that is it.

So therefore I say the image of f_p is precisely you take all rational functions and take, so image of f_p is precisely $\mathbb{Z}_p(X^p)$, they are rational functions in the p power of X.

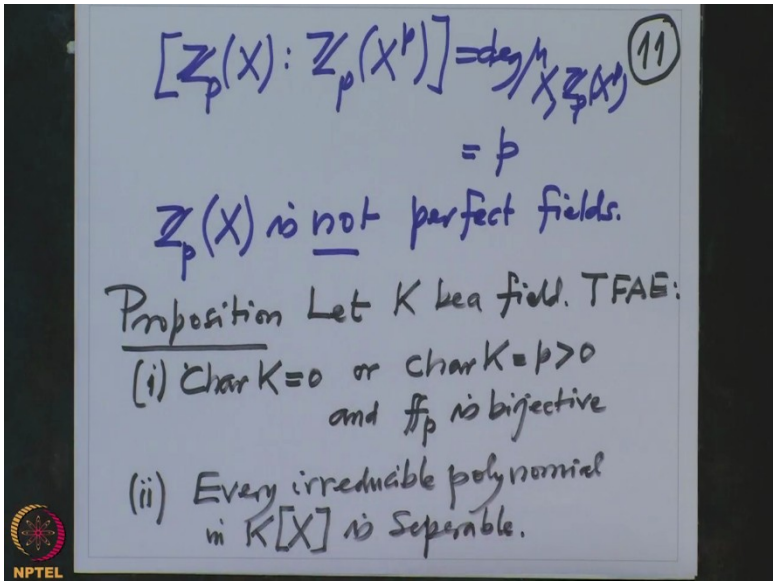
(Refer Slide Time: 25:35)



Now note that $\mathbb{Z}_p(X)$ this contains this field $\mathbb{Z}_p(X^p)$ and this is I claim that this is nontrivial so this is not equality here because for that we just have to check that X does not belong to $\mathbb{Z}_p(X^p)$, this just follows from the prime decomposition in $\mathbb{Z}_p(X)$ so I will not say more about this but we know now we have we have this field extension, this is a proper field extension this over $\mathbb{Z}_p(X^p)$. And the element X is algebraic over $\mathbb{Z}_p(X^p)$ and what is the minimal polynomial? Minimal polynomial of X over $\mathbb{Z}_p(X^p)$, this is $T^p - X^p$, T is a variable I am using because I do not want to use the variable X again.

And this polynomial is irreducible obviously, how do you check this equality? This equality you can simply check this X is clearly 0 of this polynomial and this polynomial is irreducible over $\mathbb{Z}_p(X^p)$ and to check it is irreducible over this, enough to note that this is irreducible over $\mathbb{Z}_p(X^p)$ and for that you can use Eisenstein's criterion we apply it here, it is irreducible and therefore over rational function field of that, quotient field of this is precisely this therefore it is irreducible that is for say minimal polynomial.

(Refer Slide Time: 27:26)



So therefore this degree extension the degree of this extension field is precisely the degree of the minimal polynomial μ_x over $\mathbb{Z}_p(X^p)$ but this is precisely p so the degree is p so therefore frobenius map images not the whole but it is not too bad, it is only a PDV extension, so therefore what we check is $\mathbb{Z}_p[X]$ is not perfect. And I would not I would not like to write one characterisation of perfect field which will be more important for us so let me state it so proposition; let K be a field then the following are equivalent. 1, either characteristic K is 0 or characteristic is positive p positive and f_p is bijective, this is the definition of perfect.

And 2nd, every irreducible polynomial in $K[X]$ is separable, we will see the proof of this soon when we come back after the break we will see the proof of this proposition and then we will continue about our study of separable extensions. And the main goal in this lecture will be to prove that separable extension has a primitive element like we have proved earlier Galois extensions have a primitive element and now we are proving a weaker theorem that separable extensions have a primitive element. This proposition we will prove after the break and we will continue separability, thank you.