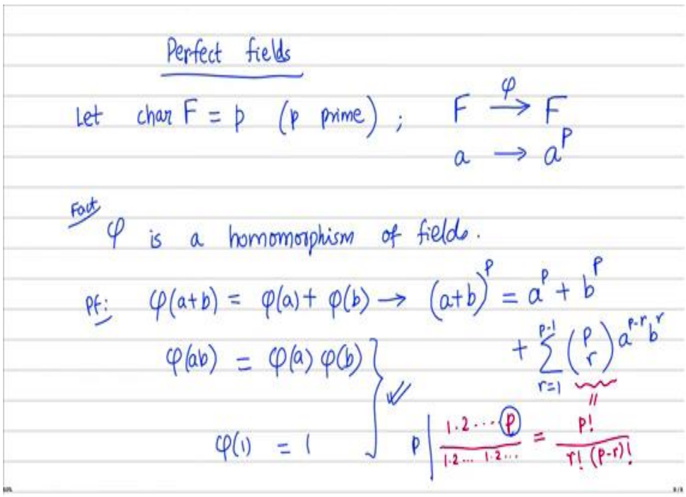
Algebra II
Professor S Viswanath
The Institute of Mathematical Sciences
Lecture 28
Perfect Fields, Separable Extensions

(Refer Slide Time: 00:15)



Perfect fields

Let char $F = p$ (p prime) ; $F \xrightarrow{\varphi} F$, $a \to a^p$

Fact: φ is a homomorphism of fields.

Pf: $\varphi(a+b) = \varphi(a) + \varphi(b) \to (a+b)^p = a^p + b^p + \sum_{r=1}^{p-1} \binom{p}{r} a^{p-r} b^r$

$\varphi(ab) = \varphi(a)\varphi(b)$

$\varphi(1) = 1$

$p \mid \frac{1\cdot 2 \cdots \boxed{p}}{1\cdot 2 \ldots \; 1 \cdot 2 \ldots} = \frac{p!}{r!\,(p-r)!}$

And we will see, how this is motivated by this problem or this example that I talked about of having irreducible, which are not separable. So, what is the perfect field? So, let me just quickly define this. So, suppose F is a field of characteristic p, this only makes sense, let us say for characteristic p fields, p is a prime. So, the computation that we just did with three actually works in general. So, this is, so let us do the following.

Let us take the map from the field F to itself, let us call it phi, which is the following. It takes every element of the field and maps it to its pth power, p being a prime here. Now observe that this map is actually a field homomorphism. So, claim or observation, fact; observe phi is a homomorphism of fields. Well, what do we have to check? We just have to check that it maps a b, phi maps, a plus b to phi a plus phi b, phi maps the product a b to phi a, phi b maps inverses to inverses, maps 1 to 1.

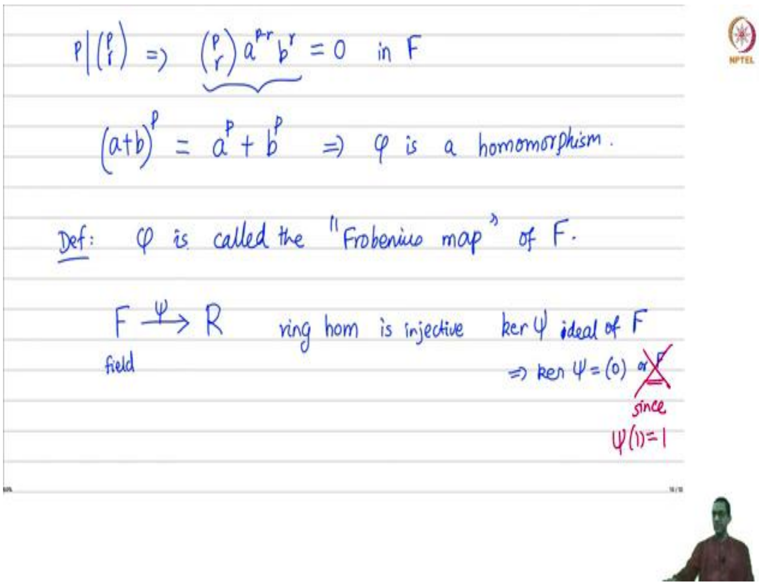
Now, observe that well, I guess inverses to inverses is not necessary. If you have checked that it maps 1 to 1. So, let us just erase this. So, we just need to check that phi satisfies these properties. Now, well, really, these two properties are more or less obvious from the definition, it sends a b to a b whole power p, which is a power p, b power p.

So, these two are more or less obvious, the only thing one needs to check really is this property. So, let us do that. So, let us compute a plus b whole power p. And observe this is more or less like the computation we did with three, which is, there are two terms, which are just a power p plus b power p, and then lots of cross terms which come from the binomial expansion. But all of them look like this.

What are the cross terms? It is p choose r, or p see r, x power r, well not x here, it is a power something, b power the complimentary exponent, this is r going from 1 to p minus 1. Now observe that this p choose r, this term over here is in fact divisible by p. Why? Well, what does this look like? This is a factorial of p divided by the factorial of r times the factorial of p minus r. And since r and p minus r are both numbers strictly between 1, I mean they are numbers between 1 and p minus 1, they are strictly smaller than p.

So, when you sort of write out this factorials, the numerator will have all numbers 1, 2, 3, till p, the denominators will again be like a product of some, it is a product of one factorial, the product of another factorial, but the bottom does not involve the term p, it only involves terms which are strictly smaller than p. So, this, this p on the numerator will survive the cancellation. So, at the at the end of this, this cancellation, you are still going to be left with this p. So, p divides the answer, that is the point, so p divides this quotient.

(Refer Slide Time: 04:08)



$$p \mid \binom{p}{r} \Rightarrow \underbrace{\binom{p}{r} a^{p-r} b^{r}}_{} = 0 \quad \text{in } F$$

$$(a+b)^p = a^p + b^p \Rightarrow \varphi \text{ is a homomorphism.}$$

Def: φ is called the "Frobenius map" of F.

$F \xrightarrow{\psi} R$ ring hom is injective ker ψ ideal of F

field

$\Rightarrow \ker \psi = (0)$ or $\cancel{F}$

since

$\psi(1) = 1$

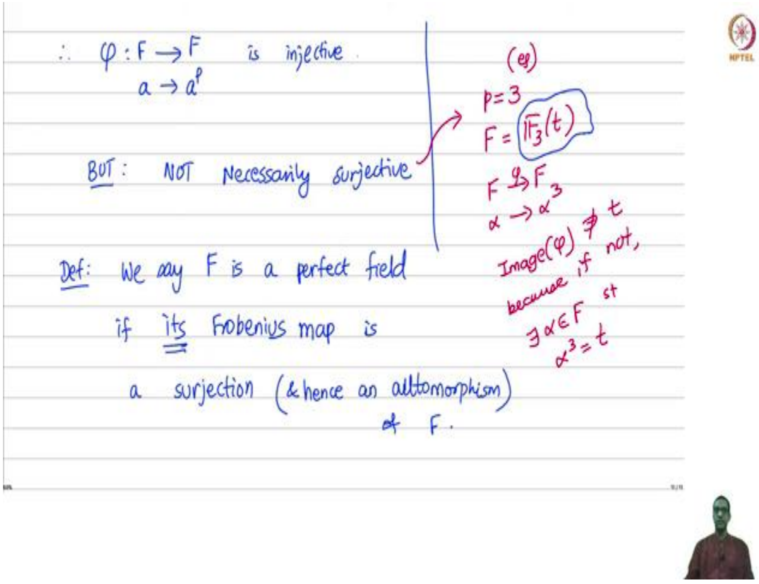
And so p choose r is a multiple of p. So therefore, so p divides p choose r implies that term is 0, p choose r, a power something, b power something is 0 in this field F. Why? Because F has characteristic p, and this is therefore, since this is a multiple of p. This is just the 0 element in the field F. So that is what characteristic p means, p times any element of the field is just 0. So therefore, you are only left with the two terms at the end, a power p and b power p. So, this just shows that phi is a homomorphism.

And this has a name, so definition or notation nomenclature phi is called the Frobenius map. So, we call this the Frobenius map of F, for each field of characteristic p, you have this map at a going to a power p. And observe that because it is a homomorphism between two fields, what you certainly know is that phi is injective.

In fact, more generally recall, if I have a field F, and I have a homomorphism, from that field to any ring, I mean, think of both as rings. But if the left-hand side is a field, then if the domain is a field, then any ring homomorphism is necessarily injective. So, ring homomorphism, from a field to a ring must be injective.

Why is that? Because the kernel recall is an ideal. So, the kernel of this, let us call it psi, is an ideal of the left-hand side, but a field has no ideas other then 0. So, this means that, well, there is also the whole ideal, if you wish, kernel of 0 can be 0, or the whole thing, but it cannot be the whole thing because 1 maps to 1. It cannot be this, since by definition, a homomorphism is required to map 1 to 1. So, any ring homomorphism is necessarily injective, if you are going from a field to some other ring, because the field does not have any ideals.

(Refer Slide Time: 06:45)



$\therefore$ $\varphi : F \to F$ is injective.
$a \to a^p$

BUT: NOT Necessarily surjective

Def: We say F is a perfect field if its Frobenius map is a surjection (& hence an alltomorphism) of F.

(eg)
$p=3$
$F = \boxed{\mathbb{F}_3(t)}$
$F \xrightarrow{\varphi} F$
$\alpha \to \alpha^3$
$\text{Image}(\varphi) \not\ni t$
because if not, $\exists\, \alpha \in F$ st $\alpha^3 = t$

Now, since this Frobenius map phi is a map from a field to itself, what we therefore conclude is that therefore, the Frobenius map from F to F is definitely injective, a going to a power p is injective. But and this is important, keep in mind, but not necessarily surjective. This, need not be a surjection.

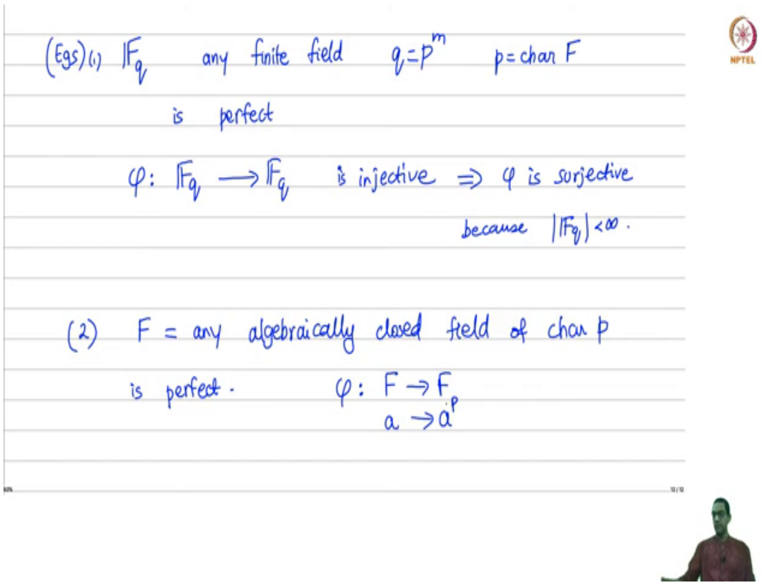
And in fact, that is exactly the example we just talked about. So, if it seems slightly unfamiliar, notice that the example we just gave, so let us take the example p equals 3, let us take the field F to be F3 of t, where t is the indeterminate, this the field of rational functions, and the Frobenius map, which is you know, every everything going to its cubed. So, what is a map from F to F? It sends every alpha to its cube.

So, this is the Frobenius map, observe that the image of this Frobenius map does not contain the element t of the field. Why is that? Because if it did, then there would exist, because if not, then you claim that I mean, you would conclude that there is some element of F, such that alpha cube equals t. And that is exactly what we just showed is not possible. You write alpha a t by bt and show that a t by bt whole cube equal t is impossible, you cannot find such polynomials a t and bt. So, the example we just talked about is in fact something which shows that the Frobenius map is not a surjection. But at least it is injective in all cases.

Now, here is the beauty of this whole thing. So, let us make a little definition here. If the Frobenius map is subjective, so we say that the field F is perfect, we say F is a perfect field, if it is Frobenius map is a surjection. If its Frobenius map is, well if it is a surjection it is already an injection remember. So, saying it is a surjection is the same as saying it is an isomorphism. So, let me write it as a surjection, is a surjection and hence an isomorphism.

Well isomorphism from the field to itself, so that is what we call an automorphism, hence an automorphism of the field F. So, if the Frobenius is surjective, as well as being injective, then we say that F is a perfect field. So, we have just seen an example of an imperfect field, the field F3 of t is not perfect, because it is Frobenius map is not a surjection.

(Refer Slide Time: 10:14)



(Egs) (1) $\mathbb{F}_q$ any finite field $q=p^m$ $p = \text{char } F$

is perfect

$\varphi : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ is injective $\Rightarrow \varphi$ is surjective

because $|\mathbb{F}_q| < \infty$.

(2) F = any algebraically closed field of char p

is perfect. $\varphi : F \to F$, $a \to a^p$

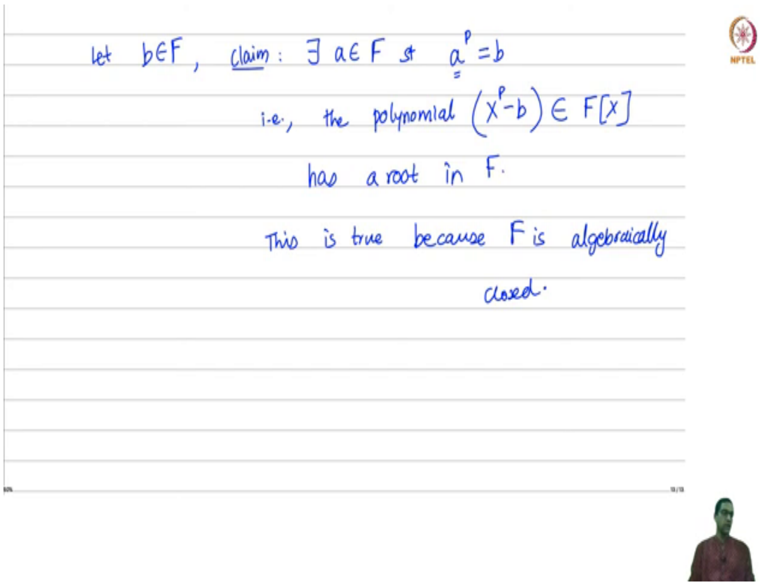
But I mean, are there examples of perfect fields? Well, there is one nice class of examples, obvious class of examples, which are just a finite fields. So, let us look at Fq, any finite field. What is q here? q is some power of the prime p here, say p power m, p is the characteristic of the field, any finite field is necessarily perfect.

Here is an important example, which is any finite field is perfect. Why? Well, we call the Frobenius is an injection. The Frobenius map from Fq to itself is always an injection, is injective. But injective just means it is a one-to-one function. But if you have a finite field, then one to one automatically implies onto, you have an injective map from a set of some 10 elements. Well, 10 is not a powerful prime, let us say I have the finite field F16, from a set of 16 elements to itself, I have an injective map, then that map also has to be subjective,

So, this is a consequence of the finiteness. So, this implies phi is automatically surjective as well, because F is finite. This is of course not true. If you have an infinite field, you cannot conclude an injective map is automatically surjective. So, this is one example. Well, what are other examples of infinite fields, which are necessarily perfect?

Well, you can take algebraically closed fields. So here is the second example. So, suppose F is any algebraically, closed field of characteristic p, close field of some finite characteristic, let us say characteristic p, then this automatically perfect. Why? Because, well, this time, the reason is slightly different. So, let us look at the map phi from F to F, which is every element going to a power p. And we want to claim that this map is surjective.

(Refer Slide Time: 12:38)



let $b \in F$, claim: $\exists\, a \in F$ st $\underline{\underline{a}}^p = b$

i.e., the polynomial $(x^p - b) \in F[x]$

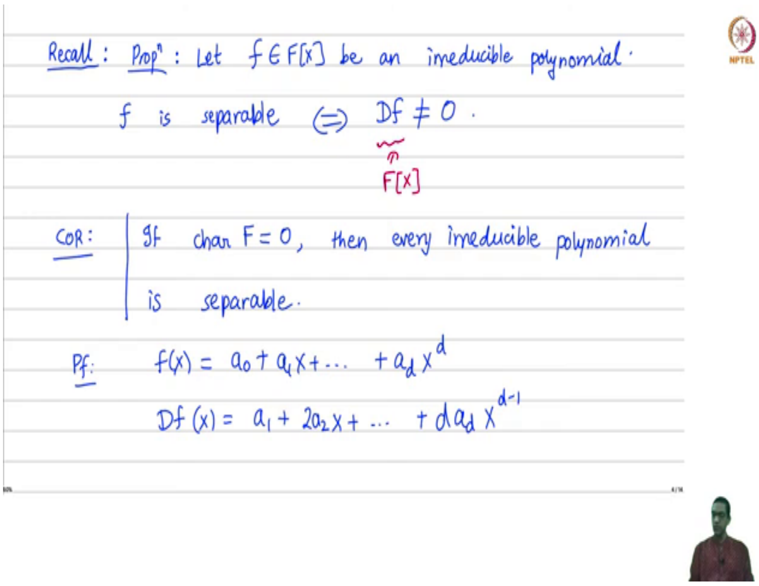
has a root in F.

This is true because F is algebraically closed.

Well, what does that mean? Take any element of F, let b in F, the claim is that there exists an element a in F, such that a power p will give me this element b i.e., let us rephrase it as follows. This is the same as saying that the polynomial, so let us look at the polynomial x power p minus b.

So, look at this polynomial, it is a polynomial with coefficients in the field F, this polynomial has a root in F, that is exactly what this element a would be, it would be a root of this polynomial, but F is algebraically closed, and I have a polynomial with coefficients in F. Well, this is true, because F is algebraically closed, the polynomial has a root, but this is true. This is true, because F is algebraically closed. So, you have now seen two examples of perfect fields, one are the finite fields and the other is the class of algebraically closed fields of finite characteristic.

(Refer Slide Time: 14:30)



Recall: Prop^n: Let $f \in F[x]$ be an irreducible polynomial.

f is separable $\iff$ $\underbrace{Df}_{\substack{\cap \\ F[x]}} \neq 0$.

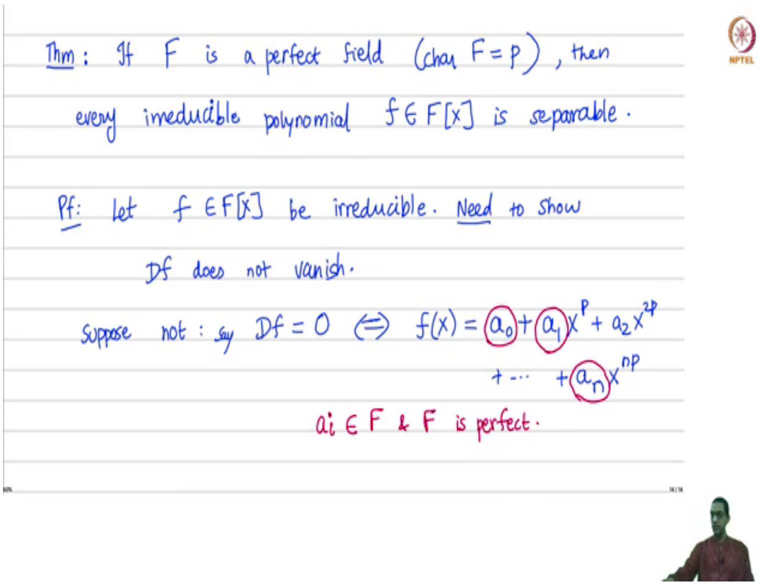
COR: If char $F = 0$, then every irreducible polynomial is separable.

Pf: $f(x) = a_0 + a_1 x + \dots + a_d x^d$

$Df(x) = a_1 + 2a_2 x + \dots + d a_d x^{d-1}$

And what is the point of introducing this this new notion? Well, recall all this began, because we constructed an example. So, we said, let us go back up. We said that over a characteristic 0 field, there we are, so if the field has characteristic 0, then a polynomial being irreducible implies it is separable. If the field has characteristic p irreducibility, does not imply separability. But here is the importance of this perfectness assumption.

(Refer Slide Time: 14:46)



Thm: If F is a perfect field (char $F = p$), then every irreducible polynomial $f \in F[x]$ is separable.

Pf: Let $f \in F[x]$ be irreducible. Need to show Df does not vanish.

Suppose not: say $Df = 0 \iff f(x) = \boxed{a_0} + \boxed{a_1} x^p + a_2 x^{2p} + \dots + \boxed{a_n} x^{np}$

$a_i \in F$ & F is perfect.

That is the little theorem or proposition for us, which is that, if F is perfect, however, if F is a perfect field, and let us assume the characteristic is called p, say the characteristic is some prime p, if F is a perfect field, then the same fact holds, then every irreducible is automatically separable, every irreducible polynomial f in Fx is necessarily separable.

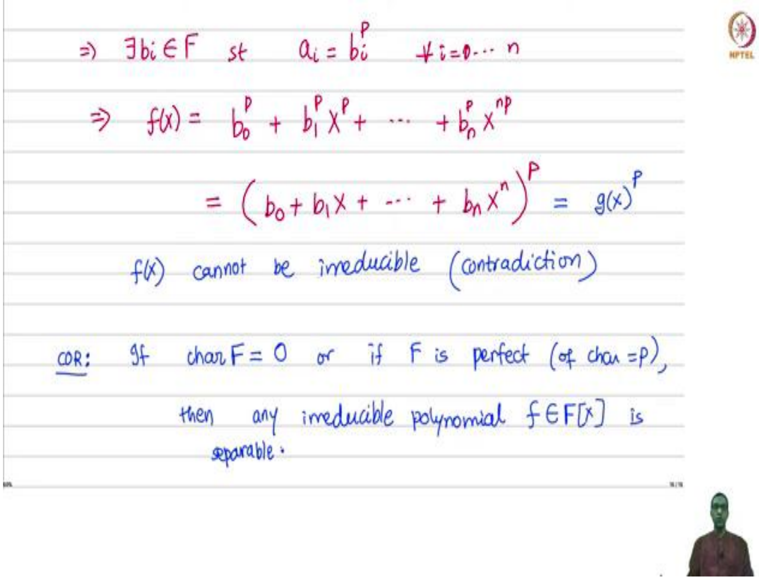
So, let us prove this. So, what do we need to do? Let us take f to be irreducible. So, let f, f of x be an element of Fx, be irreducible. To show it is separable, we need to show that its derivative is not 0. So, recall, need to show, so, we already had this proposition that for an irreducible polynomial separability is the same as derivative not vanishing, so need to show derivative of F does not vanish.

So, suppose not, let us proceed by contradiction, suppose not, let us write, so, suppose the derivative say the derivative vanishes, then we have seen this before in the earlier lectures on repeated roots, if the derivative vanishes, then it means that the only coefficients of f which survive are the multiples of p and f must have the following form, should look like a naught plus some a1x power p plus some a2x power to 2p and so on.

Some let us say, ar x power r, let us say an x power np. This is the only way in which the derivative can vanish. In fact, it is if no Df, why? Because if you just compute the derivative, if you take x power r, what happens is it becomes r x to the r minus 1 and that term vanishing can only happen if r is a multiple of p, if r is not a multiple of p, that term does not vanish.

So, the only non-vanishing terms which can occur the monomials which can occur in Fx are the ones x power 0, x power p, 2p, 3p and so on. So, this again, you have seen before. Now, so, this is what we know f should have the following form. But where does the perfectness assumption now come in? How does that help us? So, recall all these a0, a1 and so on are all elements of the base field. So, all the ai's are after all elements from the field F and F is known to be perfect for F is assumed to be perfect.

(Refer Slide Time: 18:24)



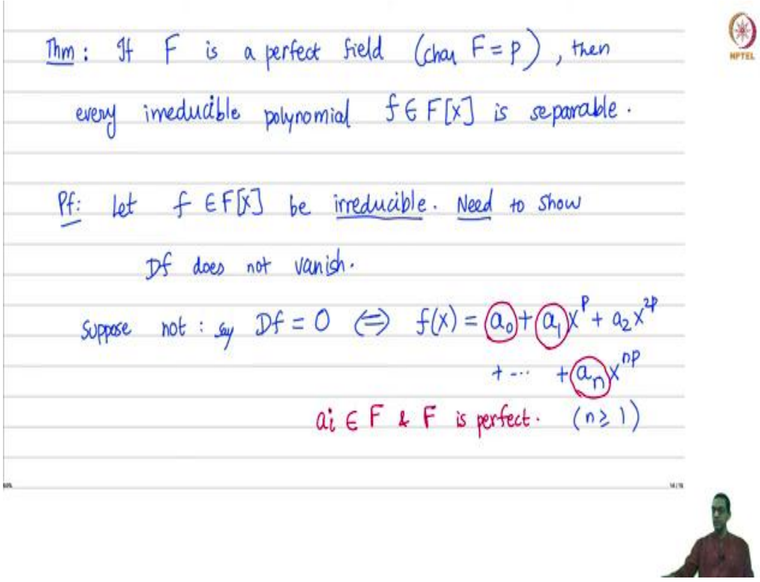
$\Rightarrow \exists\, b_i \in F$ st $a_i = b_i^p \quad \forall\, i = 0 \cdots n$

$\Rightarrow f(x) = b_0^p + b_1^p x^p + \cdots + b_n^p x^{np}$

$= \left(b_0 + b_1 x + \cdots + b_n x^n\right)^p = g(x)^p$

$f(x)$ cannot be irreducible (contradiction)

COR: If char $F = 0$ or if F is perfect (of char $= p$), then any irreducible polynomial $f \in F[x]$ is separable.



Thm: If F is a perfect field (char $F = p$), then every irreducible polynomial $f \in F[x]$ is separable.

Pf: Let $f \in F[x]$ be irreducible. Need to show Df does not vanish.

Suppose not: say $Df = 0 \iff f(x) = \boxed{a_0} + \boxed{a_1} x^p + a_2 x^{2p} + \cdots + \boxed{a_n} x^{np}$

$a_i \in F$ & F is perfect. $(n \geq 1)$

What does that mean? It means that the Frobenius map is an isomorphism which means that for each ai, I can find a corresponding bi. I mean, I can find many of them maybe, but at least one bi exists, there exists bi such that ai is the pth power of bi. So, this is for all i equals 1 to n. So, what does that do for us?

It enables us to rewrite the polynomial F as follows. So, instead of a0, so, this is for 0 to n. So, instead of a0 here, I will rewrite it as b0 power p; instead of a1, I will write it as b1 power p x power p and so on, b n power p, x power np. Let us go up and check, this is how F looked, I have just changed all the a's into the corresponding powers of pth powers of the b's.

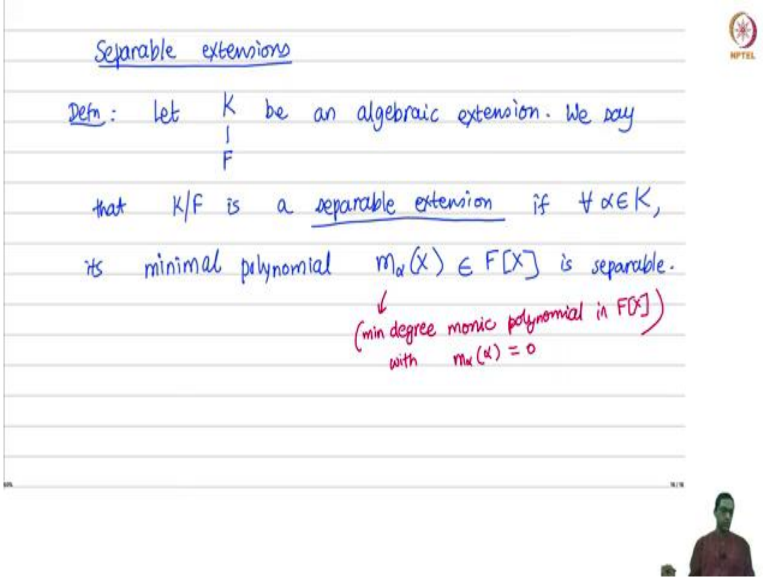
And now, again by the calculation we have done before using the fact that the field has characteristic 0, this is just b0 plus b1x plus dot dot dot bn x power n the whole power p. Now observe that this polynomial, now that we have written in this form, this polynomial cannot be irreducible. It is straightaway obvious that f of x cannot be irreducible. Well, why not?

Because it factors obviously, as the pth power of some other polynomial, this looks like some gx power p, where gx is some polynomial and that means that F is not irreducible. So, notice here that, by the way that n is at least 1. So, to begin with F is not a constant polynomial. So, I should have said n here is at least 1, the degree is at least p in some sense, you cannot have a constant F here, because I have assumed F is irreducible to begin.

So, the point is the F has been shown to be a power of g and that of course means F is not irreducible, that is a contradiction. So, that proves what we wanted, which is that, if I have an irreducible polynomial with coefficients in a perfect field, then that polynomial is automatically separable.

And so, as some consolation to the failure of separability in general for irreducible, if characteristic of the field is 0 or if the characteristic is p, but it is separable or F is perfect sorry, if characteristic of F is 0 or if F is a perfect field, perfect of some finite characteristic of characteristic p, then you conclude that any irreducible polynomial f in Fx is automatically separable. So, in particular, this holds for finite fields as well.

(Refer Slide Time: 22:01)



Separable extensions

Defn: let $\begin{matrix} K \\ | \\ F \end{matrix}$ be an algebraic extension. We say

that K/F is a separable extension if $\forall \alpha \in K$,

its minimal polynomial $m_\alpha(X) \in F[X]$ is separable.

$\downarrow$

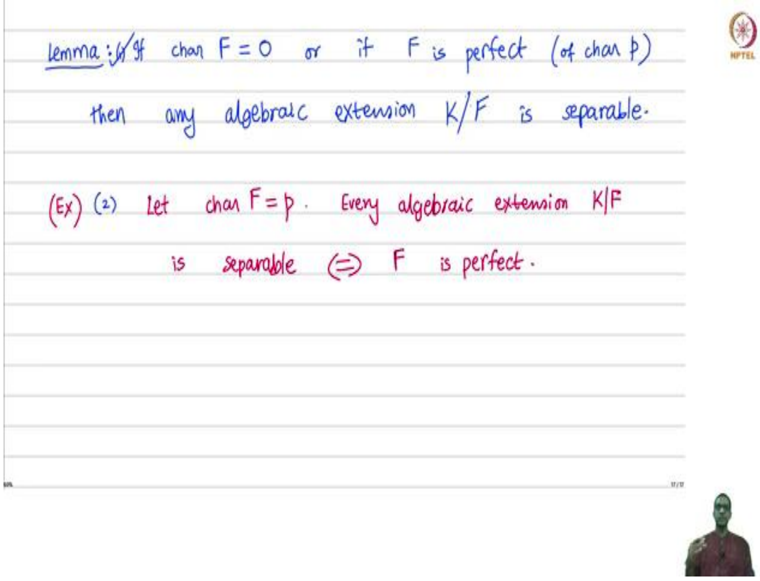
(min degree monic polynomial in F[X] with $m_\alpha(\alpha) = 0$)

Now, finally, coming to the point that we began at the very beginning, just to talk about separable extensions. So, so far we talked about separable polynomials, when do we call an extension separable? So, let us talk about separable extensions. So, the definition is the following, we say that let K be an algebraic extension. So, K over F be an algebraic extension.

We say that this extension K over F is separable, we say that it is a separable extension So, we assume to begin with that it is algebraic, only for algebraic extensions that we will define this notion. So, we say it is a separable extension, if for every element alpha in K its minimal polynomial, so, look at its minimal polynomial m alpha of x. So, what is the minimal polynomial? So, I am talking about the minimal degree monic irreducible polynomial with coefficients in the base field.

So, what is the minimal polynomial here, which I mean minimal degree monic polynomial in Fx is necessarily irreducible with alpha as a root. So, this is just the generator of the ideal on which alpha vanishes, if it is minimal polynomial m alpha of x in Fx is separable. So, we talked about separable polynomials before. Now what we are saying is, an extension is said to be separable, if for every element of the extension, the minimal polynomial of that element over the base field is a separable polynomial.

(Refer Slide Time: 24:22)

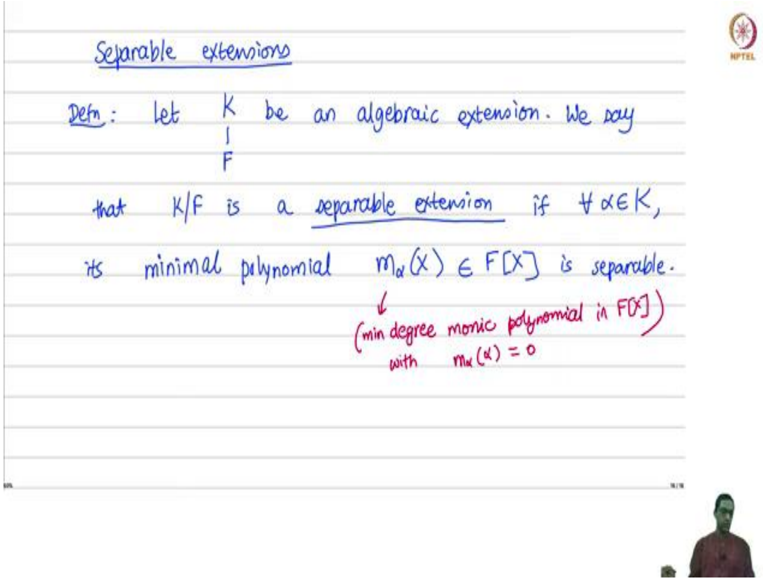


Lemma: If char $F = 0$ or if F is perfect (of char p)

then any algebraic extension K/F is separable.

(Ex) (2) Let char $F = p$. Every algebraic extension $K|F$

is separable $\Longleftrightarrow$ F is perfect.



Separable extensions

Defn: let $\begin{array}{c}K\\ |\\ F\end{array}$ be an algebraic extension. We say that K/F is a separable extension if $\forall \alpha \in K$, its minimal polynomial $m_\alpha(x) \in F[X]$ is separable.

$\downarrow$ (min degree monic polynomial in $F[X]$ with $m_\alpha(\alpha) = 0$)

So, let us quickly write out a corollary to our discussion of perfect fields and so on. The nice thing here is that recall, if F has characteristic 0 or if it is perfect, then any irreducible polynomial is automatically separable. So that gives us a rich class of examples of separable extensions. In fact, if the characteristic of the bass field is either 0 or if F is perfect, of some finite characteristic then any algebraic extension is automatically separable.

So, then any algebraic extension K over F is separable. Why is that? Because for every alpha, so what is it that we need? You take any alpha in K and look at its minimal polynomial, the minimal polynomial is always irreducible and irreducible polynomials are automatically separable, provided you have this hypothesis, that the characteristic is either 0 or the field is perfect. So, this is a rich class of example.

So, for example, if your base field is a finite field, then any algebraic extension of a finite field is necessarily a separable extension. Or if you take the field of rational numbers, then any extension of q, any algebraic extension of q is automatically separable. So, this is this is some nice thing to keep in mind. And in fact, the converse is also true. And so, let me just state that for now. So, we have already proved this in more or less as a consequence of what we said earlier.

So, I am not going to prove the second part of this lemma. I am just going to leave this as an as an exercise, maybe we will talk about it later in maybe the problem-solving sessions. If, front of the converse is true as well, if, so let characteristic of F be some prime p then the converse holds every algebraic extension K of F is separable if and only if F is perfect. So, it is really an equivalent statement. The field being perfect is exactly the property that says that all algebraic extensions are always separable extensions.