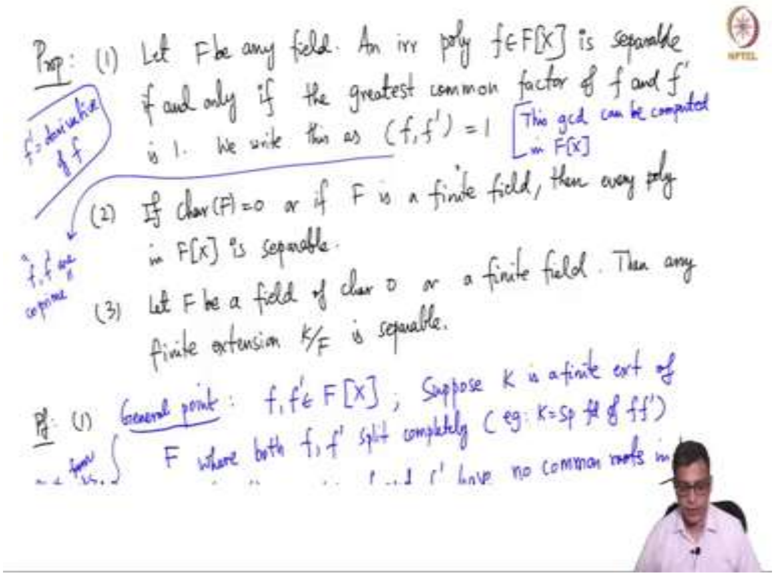
Introduction to Galois Theory
Professor Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute
Lecture 19
Separable Extension – Part 2

(Refer Slide Time: 00:41)



Prop: (1) Let F be any field. An irr poly $f \in F[X]$ is separable if and only if the greatest common factor of f and f' is 1. We write this as $(f, f') = 1$ [This gcd can be computed in $F[X]$

f' = derivative of f

"f, f' are coprime"

(2) If $\mathrm{char}(F) = 0$ or if F is a finite field, then every poly in $F[X]$ is separable.

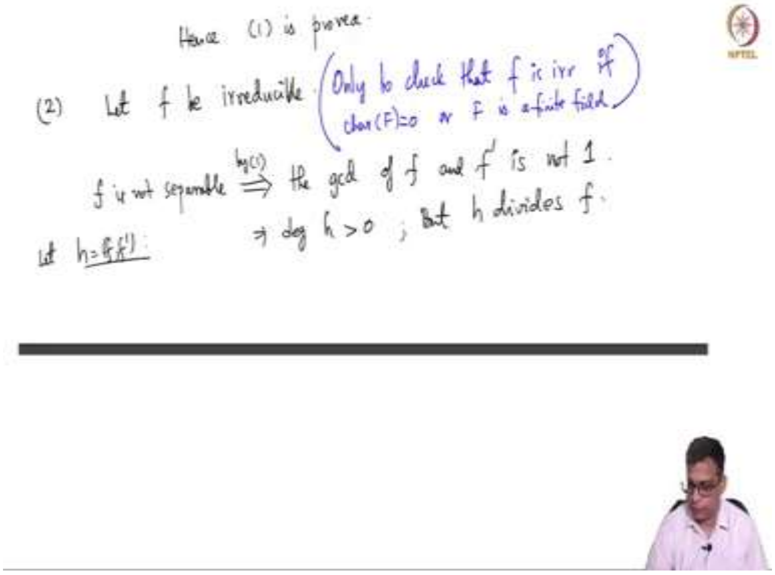
(3) Let F be a field of char 0 or a finite field. Then any finite extension K/F is separable.

Pf: (1) General point: $f, f' \in F[X]$; Suppose K is a finite ext of F where both f, f' split completely (eg: $K = $ Sp fd of ff')

f and f' have no common roots in

Welcome back, in the last video I defined separable extensions. I first define what it means for a polynomial to be separable then for an element in an extension field to be separable. And finally, what it means for the extension itself to be separable. We looked at some examples of inseparable polynomials and then we are in the middle of proving this proposition and we just proved that to verify if a polynomial is separable or not, all you need to do is verify the greatest common divisor of that polynomial in its derivative.

(Refer Slide Time: 00:52)

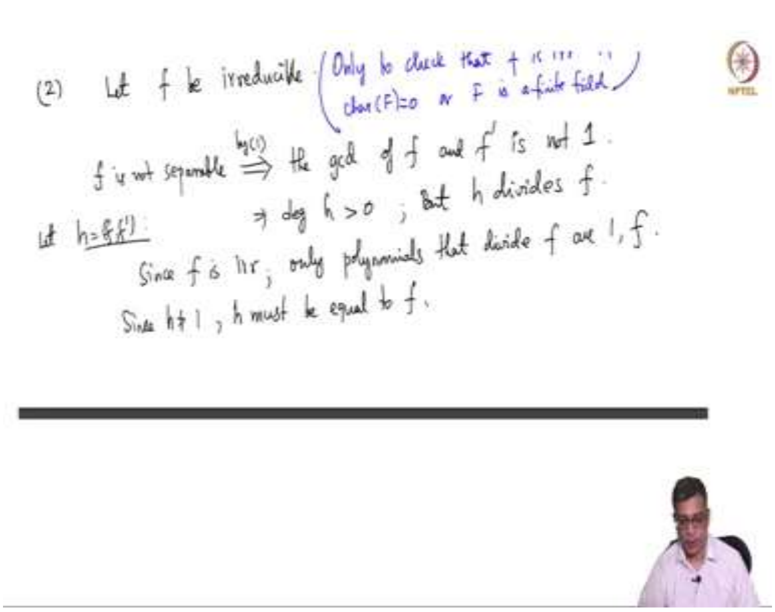


Hence (1) is proved.

(2) Let f be irreducible. (Only to check that f is irr if char$(F)=0$ or F is a finite field)

f is not separable $\overset{\text{by}(1)}{\Longrightarrow}$ the gcd of f and f' is not 1.

Let $\underline{h = (f, f')}$. $\Rightarrow$ deg $h > 0$; But h divides f.



(2) Let f be irreducible. (Only to check that f is irr if char$(F)=0$ or F is a finite field)

f is not separable $\overset{\text{by}(1)}{\Longrightarrow}$ the gcd of f and f' is not 1.

Let $\underline{h = (f, f')}$. $\Rightarrow$ deg $h > 0$; But h divides f.

Since f is irr, only polynomials that divide f are $1, f$.

Since $h \neq 1$, h must be equal to f.

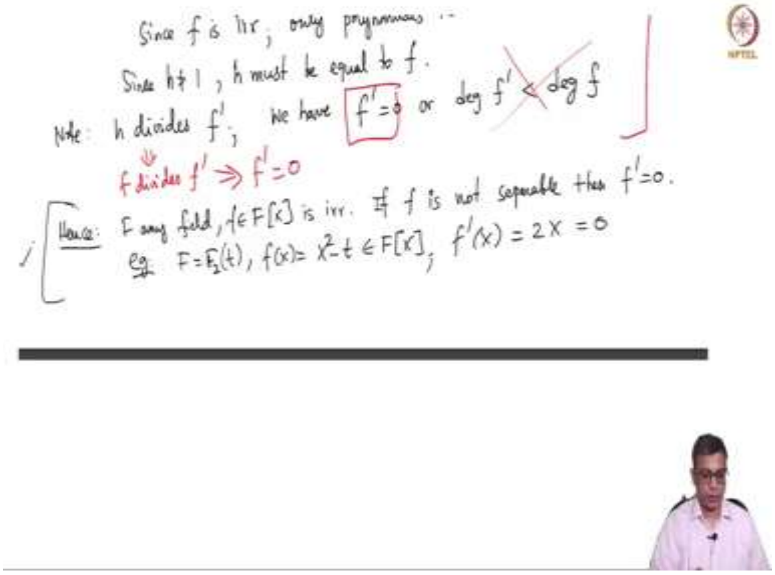
And the second part and third part now we will prove, so continuing the proof So, the first observation is that let f be irreducible, so that is going to be the situation now. So, second statement is every polynomial is separable if the field has characteristic 0 or that it is a finite field. So, now that means, irreducible factorization of every element has a property that every irreducible polynomial appearing in the factorization is separable.

So, we need to only prove that it is separable, so only to check that f is irreducible, if characteristic of f is 0 or f is a finite field. That is the goal. So, we are going to start with an arbitrary irreducible polynomial. Now, using the statement one, we have to think about a little bit. So, what is the first, suppose f is not separable. This implies by 1, the GCD of f and f prime is not 1, but whatever the GCD is, so let us say h is the GCD, let h be the GCD.

So, degree of his positive, so that it, GCD is not constant means it is a non-constant polynomial, but h divides f being the greatest common divisor it is a divisor to begin with. So, h divides f, but since f is irreducible only polynomials that divide f are, what is an irreducible polynomial, it means it has no proper factors that means no factors other than 1 and f, but h is just not equal to 1 is what we concluded, h must be equal to f, it is f.

So, GCD is a positive degree polynomial, but the only positive degree polynomial that divides f is f because f is irreducible. So, f is irreducible is very important for this argument.

(Refer Slide Time: 3:36)



Since f is irr; only polynomials ...

Since $h \neq 1$, h must be equal to f.

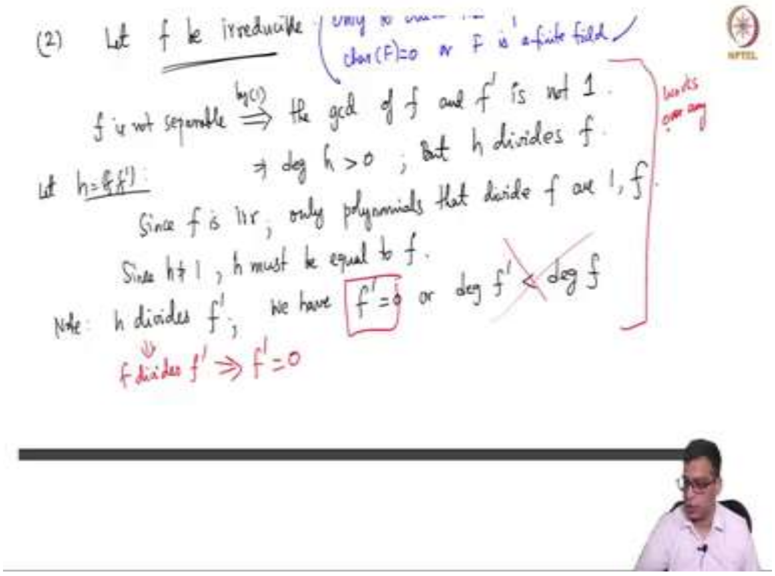
Note: h divides f'; we have $\boxed{f'=0}$ or $\cancel{\deg f' < \deg f}$

$\Downarrow$

f divides $f' \Rightarrow f'=0$

Hence: F any field, $f \in F[x]$ is irr. If f is not separable then $f'=0$.

eg. $F = \mathbb{F}_2(t)$, $f(x) = x^2 - t \in F[x]$; $f'(x) = 2x = 0$



(2) Let f be irreducible (only to show ... char(F)=0 or F is a finite field ✓

f is not separable $\overset{\text{by(1)}}{\Longrightarrow}$ the gcd of f and f' is not 1.

Let $h = (f, f')$: $\Rightarrow \deg h > 0$; But h divides f.

Since f is irr, only polynomials that divide f are 1, f.

Since $h \neq 1$, h must be equal to f.

Note: h divides f'; we have $\boxed{f'=0}$ or $\cancel{\deg f' < \deg f}$

$\Downarrow$

f divides $f' \Rightarrow f'=0$

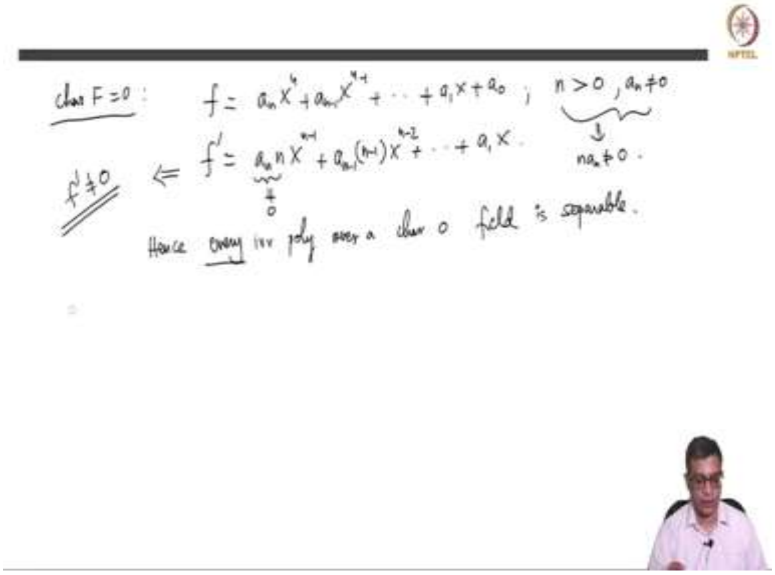
works over any

But then h divides, now note that h divides f prime also, but degree of f prime. So, we have two possibilities, either f prime is 0 or degree of f prime is strictly less than degree of f. In general, if you take a polynomial its derivative will have degree strictly less than degree of f or maybe it becomes 0, we do not want to talk about degree of 0 polynomial.

So, we separate these two cases, but we just can rule this out now, because h divides f prime, f divides f prime. So, it cannot be a smaller degree polynomial. So, f must be 0, f prime must be 0. So, that means, so where are we now, if you have a irreducible polynomial and this argument works over any field.

So, the conclusion is f is any field, small f is an irreducible polynomial. If f is not separable then f prime is 0. So, recall, in the example that we discussed in the last video, sorry, F is this small f of x which is x square minus t in capital F square bracket x, then f prime of x is 0. So, P is a constant now, so the derivative is 0, 2 x is 0, so because characteristic 2 is 0.

(Refer Slide Time: 5:31)



$\underline{\text{char } F = 0}$: $f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 x + a_0$; $\underbrace{n > 0 , a_n \neq 0}_{\Downarrow}$ $n a_n \neq 0$.

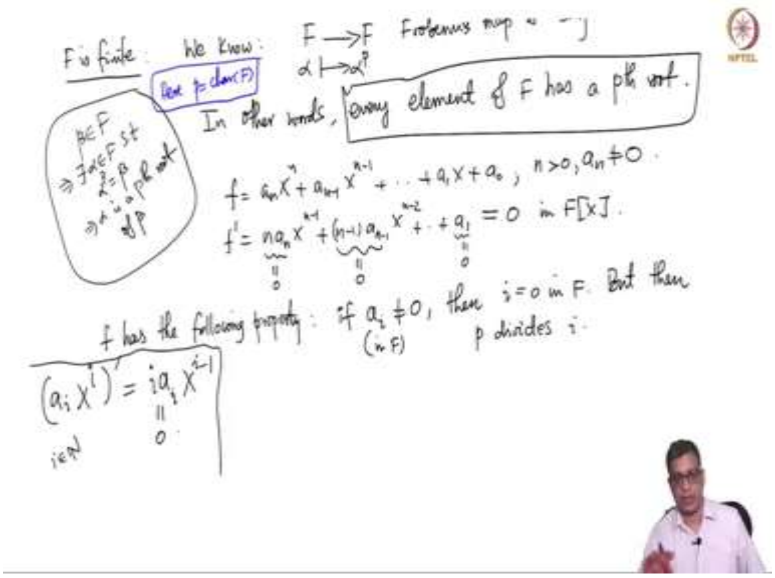
$\underline{\underline{f' \neq 0}} \Leftarrow f' = \underbrace{a_n}_{\neq 0} n X^{n-1} + a_{n-1}(n-1) X^{n-2} + \cdots + a_1 X$.

Hence $\underline{\text{every}}$ irr poly over a char 0 field is separable.

Now, let us assume that characteristic of F is 0, I have to consider two cases. In general, what is f, f is like this, so and n is positive because f is an irreducible polynomial. An irreducible polynomial or a field must have positive degree, because constants are not called irreducible, they are units. So, this is a n x n like this. Then what is f prime? So, this is a n, n times x n minus 1. Now note that a n, a n is also not 0, because we always write the last, highest coefficient, it must exist, so a n is nonzero.

So that means a n n is nonzero and hence f prime is nonzero. So, it just cannot happen that f prime is zero if characteristic is 0. So, as long as you have a positive degree polynomial, f prime cannot be zero. Hence, every irreducible polynomial over a characteristic 0 field is separable and hence every polynomial itself. So this cannot happen for characteristic 0 positive degree polynomial.

(Refer Slide Time: 7:07)



F is finite. We know: $F \to F$ Frobenius map is 1-1 (here $p = \mathrm{char}(F)$), $\alpha \mapsto \alpha^p$

In other words, $\boxed{\text{every element of } F \text{ has a } p\text{th root.}}$

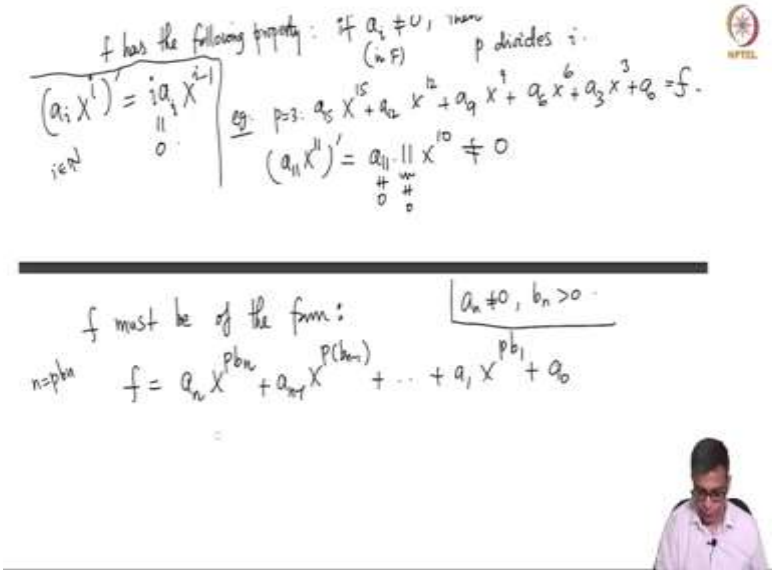
$\beta \in F \Rightarrow \exists \alpha \in F$ st $\alpha^p = \beta \Rightarrow \alpha$ is a pth root of β

$f = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$, $n > 0, a_n \neq 0$.

$f' = \underbrace{n a_n}_{\overset{\shortparallel}{0}} X^{n-1} + \underbrace{(n-1) a_{n-1}}_{\overset{\shortparallel}{0}} X^{n-2} + \dots + \underbrace{a_1}_{\overset{\shortparallel}{0}} = 0$ in $F[X]$.

f has the following property: if $\underset{(\text{in } F)}{a_i \neq 0}$, then $i = 0$ in F. But then p divides i.

$(a_i X^i)' = \underset{\overset{\shortparallel}{0}}{i a_i} X^{i-1}$, $i \in \mathbb{N}$



f has the following property: if $\underset{(\text{in } F)}{a_i \neq 0}$, then p divides i.

$(a_i X^i)' = \underset{\overset{\shortparallel}{0}}{i a_i} X^{i-1}$, $i \in \mathbb{N}$

eg: $p = 3$: $a_{15} X^{15} + a_{12} X^{12} + a_9 X^9 + a_6 X^6 + a_3 X^3 + a_0 = f$.

$(a_{11} X^{11})' = \underset{\neq 0}{a_{11}} \cdot \underset{\neq 0}{11} X^{10} \neq 0$

f must be of the form: $\boxed{a_n \neq 0, b_n > 0}$

$n = pb_n$ $f = a_n X^{pb_n} + a_{n-1} X^{p(b_{n-1})} + \dots + a_1 X^{pb_1} + a_0$

Now, let us, and as we saw in this example, it can happen in positive characteristic, but we will now argue that it cannot happen in finite fields. So assume that F is finite. And the fact that we need is the following the Frobenius map from F to F is surjective or on to, that means, you take alpha to alpha power p, it is an onto map clearly, because it is an injective map. Because any field map is injective, you have a finite set.

So injective map from a finite set itself is surjective always, simply counting will tell you that. So in other words, every element of F has a Pth root, which is the crucial statement that I am going to use, every element of F has a Pth root. Remember, that fails here, here, P is an element of capital F, and t does not have a square root, as we argued in the last video, so it does not have a square root or Pth root in p equal 2 case.

So, but for finite fields, that is not the case, every element has a Pth root, because you take any element of capital F, it is an image of this map, if you take beta in capital F, there exists alpha in capital F, such that alpha power P equals beta. So that means alpha is a Pth root of beta, so every element of a finite field has a Pth root. By the way, P is the characteristic here of F. So here, P equals characteristic of F, every finite field will have positive characteristic and that characteristic is a prime number, so P is that Prime, so I should have said that here.

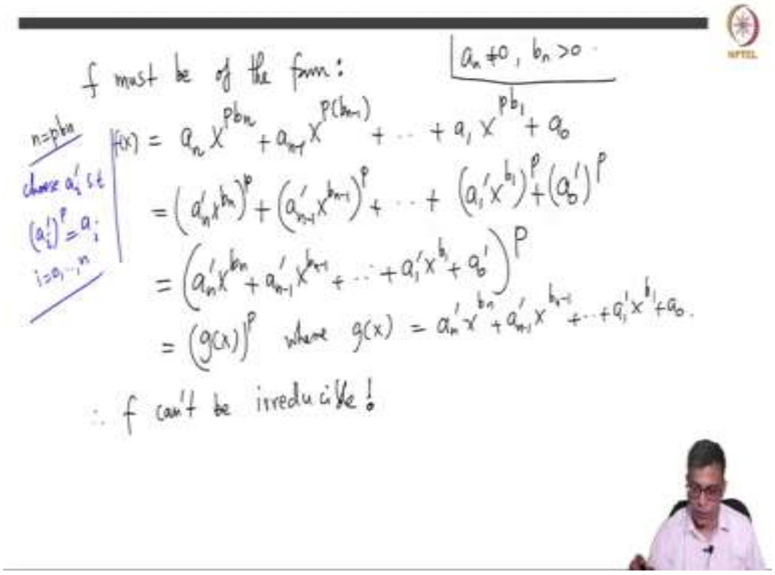
So P is the characteristic of f. And now going back to this, let us analyse when it can happen that f prime is 0. I am just rewriting what I had earlier. So f prime is a n x n minus 1, n a n x n minus 1, n minus 1, a n minus 1, x n minus 2, a 1. So suppose this is 0 in FX, because that must be the case. If you have that f is not separable.

So this of course, as before, n is positive and a n is nonzero in the field, but n times n is 0. So this is 0. This is 0, this is 0. So, that means f has a property that has the following property, if a i is nonzero, then i times. So, what is the coefficient of x power i, so if you have a a i, x power i, you differentiate this, you get i times ai x power i minus i 1, so, this is 0 because a polynomial is zero means all the coefficients are 0. So, this is 0, but ai is not 0 in F, of course, that means, i must be 0, so i is 0 in F, but then in terms of i is an integer, so i is an integer here is a positive integer.

So, that means, p divides i. So, only coefficients or only terms that can survive in F are terms whose degree is a multiple of P, for example, if p is 3, you can, you must have x power 6 or let us say x power 15 something plus something times x power 12, plus something times x power 9, plus something times x power 6, plus something times x cubed plus constant. This must be f because, if it has any other term, which is not, whose degree is not a multiple, for example, if it has degree 11, then the derivative will be whatever is the coefficient.

So, this of course is a 15. So, I should just write that here, so that this is a 15, this is a 12, this a 9, this is a 6, this is a 3, and this is a 0, because if you have a anything else, for example, this, this will be a 11 times 11 times x power 10. But this is not 0, because this is not 0, this is not 0. If that is not 0, then we have a contradiction. So, only terms that survive, that exist in f are multiples whose degrees are multiples of P.

(Refer Slide Time: 12:24)



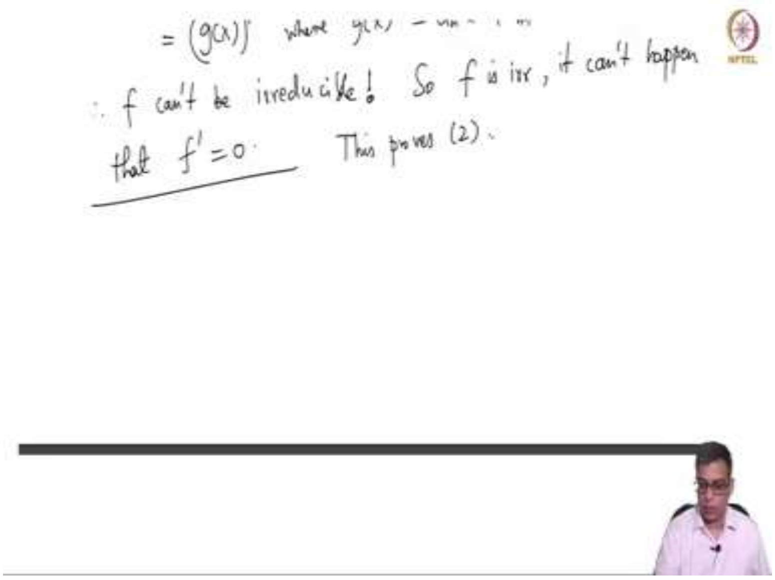
f must be of the form: $\boxed{a_n \neq 0,\ b_n > 0}$

$n = pb_n$

choose a_i' s.t. $(a_i')^p = a_i$, $i = 0, \dots, n$

$$f(x) = a_n x^{pb_n} + a_{n-1} x^{p(b_{n-1})} + \dots + a_1 x^{pb_1} + a_0$$
$$= (a_n' x^{b_n})^p + (a_{n-1}' x^{b_{n-1}})^p + \dots + (a_1' x^{b_1})^p + (a_0')^p$$
$$= (a_n' x^{b_n} + a_{n-1}' x^{b_{n-1}} + \dots + a_1' x^{b_1} + a_0')^P$$
$$= (g(x))^p \text{ where } g(x) = a_n' x^{b_n} + a_{n-1}' x^{b_{n-1}} + \dots + a_1' x^{b_1} + a_0.$$

$\therefore$ f can't be irreducible!



$= (g(x))^p$ where ...

$\therefore$ f can't be irreducible! So f is irr, it can't happen that $f' = 0$. This proves (2).

So, f must be like, f must be of the form. So, I am going to write it like this F equals a n x power P bn. So, a n or n, I am and writing is P b n. So, n must be divisible by P, and then I will simply write it like this a 1 x power P times b 1 plus a 0. So, maybe some of these are 0, but I just want to write compactly like this. So, a n is nonzero, of course, n is positive.

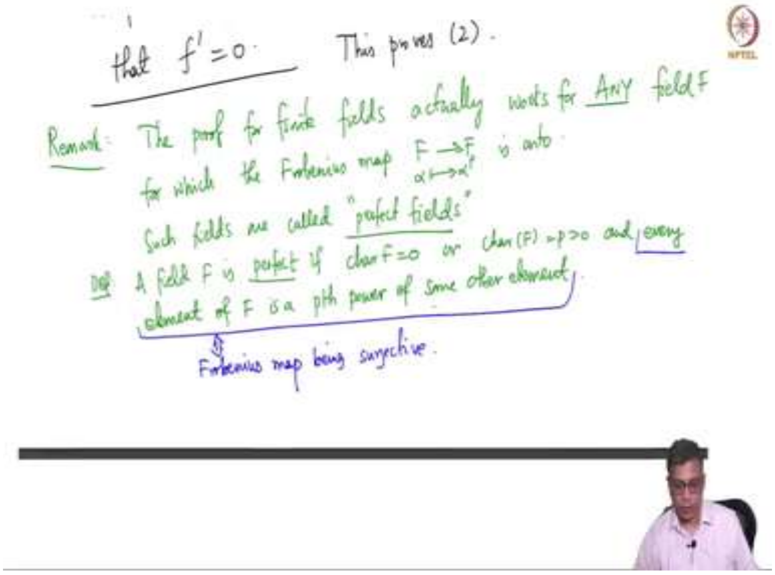
So, that means b n is positive, the degree is P b n, degree is divisible by P, the next term also has degree divisible by P. So, of course, here, it will be in the case of 3 for example is 15. This will be 12. So, 3 times 5, 3 times 3, 3 times 3 and so on. But then, here is where we use the fact that a n has a Pth root. So, choose a i prime such that a i prime power P is a i, every a i has a Pth root. So, I can write this now as a i prime x power b n times p, plus a n minus 1 prime x power b n minus 1 times P, plus a 1 prime times x power b 1 times P plus a 0 prime.

So, I do this for every i from 0 to n, sorry, 0 to n, this is the. So then a i prime. So this should be a n, a n prime P x power, b power n power P is a n prime power P which is a n, x power b n p, so that is good. Now using the binomial theorem that has the in characteristic P there are no mixed terms, I can simply write this as the whole power P.

So this is a nice thing with characteristic P. So, if you expand this by binomial theorem, all the mixed terms will have coefficients divisible by P, so they will go away. So this will simply be equal to this term. But this means this is g power P, where, so let me write this as, where, of course, gx is a n x bn, a n minus 1 prime x b n minus 1, a 1 prime x b 1 plus a 0.

What is a now conclusion? f x is equal to g x power P, so f cannot be irreducible. By definition of irreducibility, f is a multiple of gx P times with itself. So, f is g power P. So, f cannot be irreducible. So, no irreducible polynomial over a finite field can have derivative equal to 0 in other words. So, if f is irreducible it cannot happen that f prime is 0, that is all. So, every polynomial over a field which is a finite field is separable. So, this proves.

(Refer Slide Time: 16:28)



that $f' = 0$. This proves (2).

Remark: The proof for finite fields actually works for ANY field F for which the Frobenius map $\begin{array}{c} F \to F \\ \alpha \mapsto \alpha^p \end{array}$ is onto.

Such fields are called "perfect fields"

Def: A field F is perfect if char F = 0 or char(F) = p > 0 and every element of F is a pth power of some other element.

$\Updownarrow$

Frobenius map being surjective.

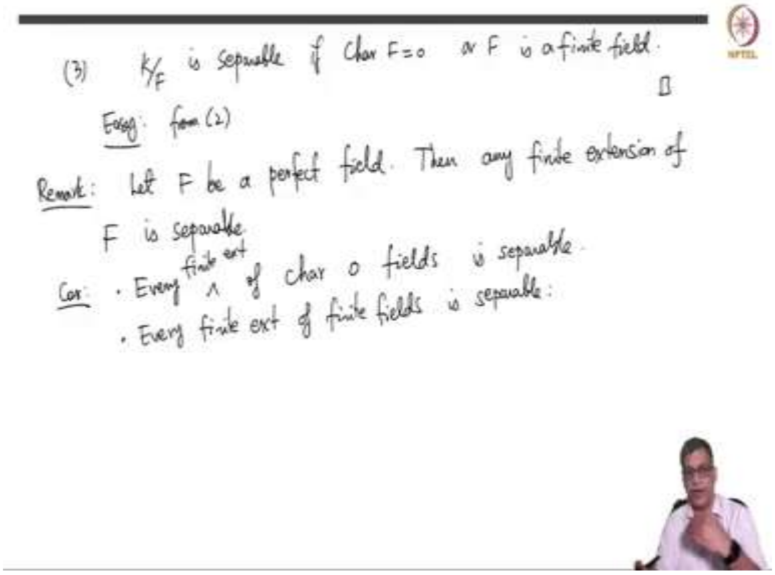
Now, I will remark the same proof, the proof for finite fields actually works for any field for which, for any field F, for which the Frobenius map is onto, such fields are called in fact, perfect fields are either characteristic 0, so actually the definition a field F is perfect if characteristic F is 0 or every element of F is a Pth power.

This is just another way of writing. So, let me be a bit more careful -- or characteristic of F is P and every element of f is a Pth power of some other element. So, every element of F is a

Pth power of some other element, this last statement is, this is equal to Frobenius map being surjective. Is equivalent to Frobenius being surjective or onto. So, perfect field is a field which has characteristic 0 or every element is a Pth power.

And remember, we have never used the fact that we are dealing with a finite field really, we are only, we have only used it when we did this. And in the case of finite fields, this is a trivial observation because it is a finite set. But if you are dealing let us say for with a field of characteristic P, P positive, but not a finite field, but for which every element is a Pth power, then the argument still works and such fields do exist.

(Refer Slide Time: 19:08)



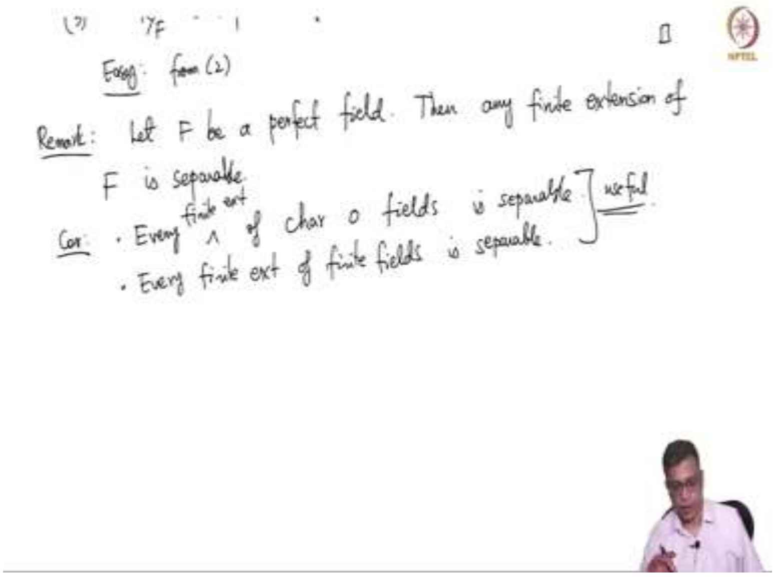
(3) K/F is separable if Char $F = 0$ or F is a finite field. □

Easy: from (2)

Remark: Let F be a perfect field. Then any finite extension of F is separable.

Cor: • Every finite ext of char 0 fields is separable.

• Every finite ext of finite fields is separable.



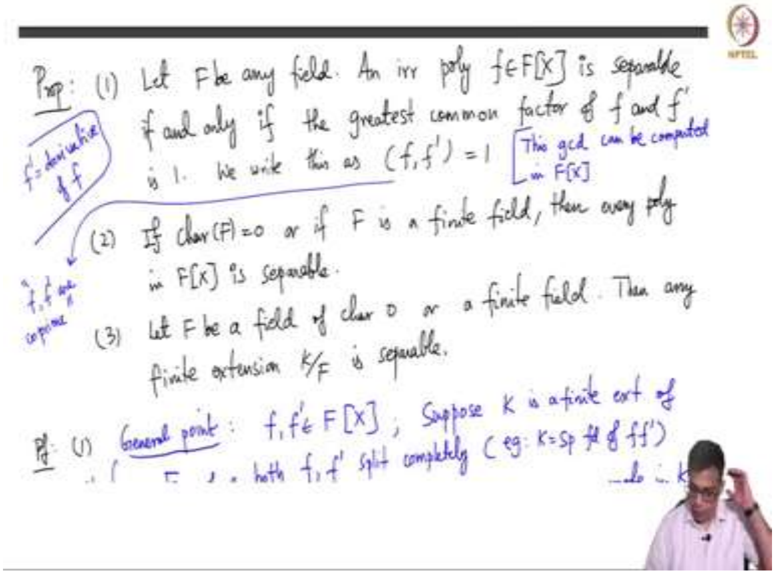
(3) K/F □

Easy: from (2)

Remark: Let F be a perfect field. Then any finite extension of F is separable.

Cor: • Every finite ext of char 0 fields is separable.] useful

• Every finite ext of finite fields is separable.



Prop: (1) Let F be any field. An irr poly $f \in F[X]$ is separable if and only if the greatest common factor of f and f' is 1. We write this as $(f, f') = 1$ [This gcd can be computed in F[X]

f' = derivative of f

"f, f' are coprime"

(2) If $\text{char}(F) = 0$ or if F is a finite field, then every poly in F[X] is separable.

(3) Let F be a field of char 0 or a finite field. Then any finite extension K/F is separable.

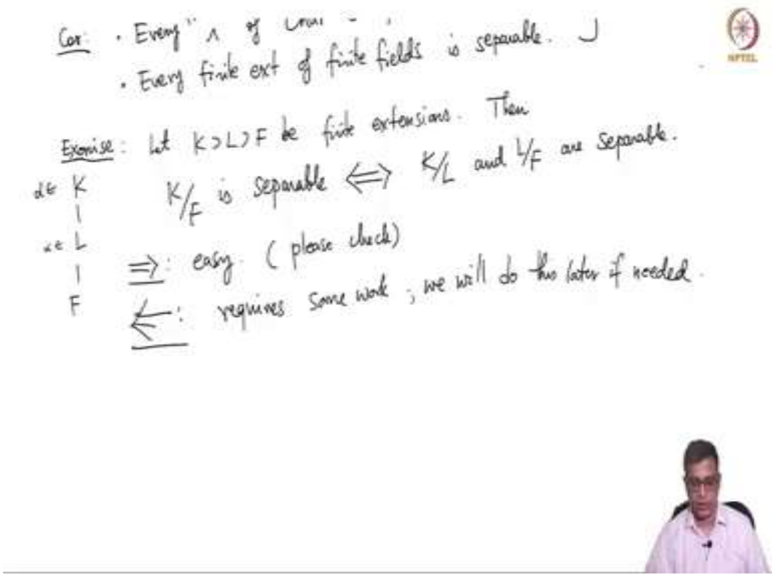
Pf: (1) General point: $f, f' \in F[X]$; Suppose K is a finite ext of F s.t. both f, f' split completely (eg: K = Sp fd of ff')

So, and the final statement is K over F is separable. If characteristic of F is 0 or F is a finite field in fact, now I can simply say F is perfect, but this is easy. This is easy from 2. So, I will not write anything. Let me just go back to the proposition statement. So, every element, every polynomial is separable. So now if you take an extension K over F, where F is characteristic 0 or a finite field and you take an alpha and K, it is irreducible polynomial is separable by two.

So the alpha is separable and hence the extension is separable. So the conclusion is, so this finishes the proof of the proposition, but I want to end the, I mean this discussion about separability with this remark. Let F be a finite field, then any finite extension of F, sorry, let F be a perfect field, then any finite extension of F is separable. So, K over F is separable if the base is separable, if the base is a perfect field.

So, as an example every extension, I mean this is a trivial corollary of Q, every extension of characteristic 0 fields is separable and every finite extension of course, finite and every finite extension has finite fields, of course, I do not need finite here because any extension of finite fields must be finite, because the field itself is finite. So, there is a finite basis. This is useful to keep in mind, because most of the time when we are dealing with characteristic 0 and finite fields separability is no additional condition it is automatically there.

(Refer Slide Time: 21:52)



Cor: · Every " ∧ of [illegible]. · " is separable.

· Every finite ext of finite fields is separable.

Exercise: Let $K \supset L \supset F$ be finite extensions. Then

K/F is separable $\Leftrightarrow$ K/L and L/F are separable.

$$\begin{tikzcd} \alpha\in K \arrow[d, dash] \\ \alpha\in L \arrow[d, dash] \\ F \end{tikzcd}$$

$\Rightarrow$: easy. (please check)

$\Leftarrow$: requires some work; we will do this later if needed.

And finally, let me end this with an exercise. Part of it that you can do now as an exercise, part of it that you cannot do now, will be done later when we need this in the later part of the course, we will do this. So, let K containing L containing F be fine finite field, finite extensions, so you have K, L and F. Then K over F is separable if and only if K over L and L over F are separable.

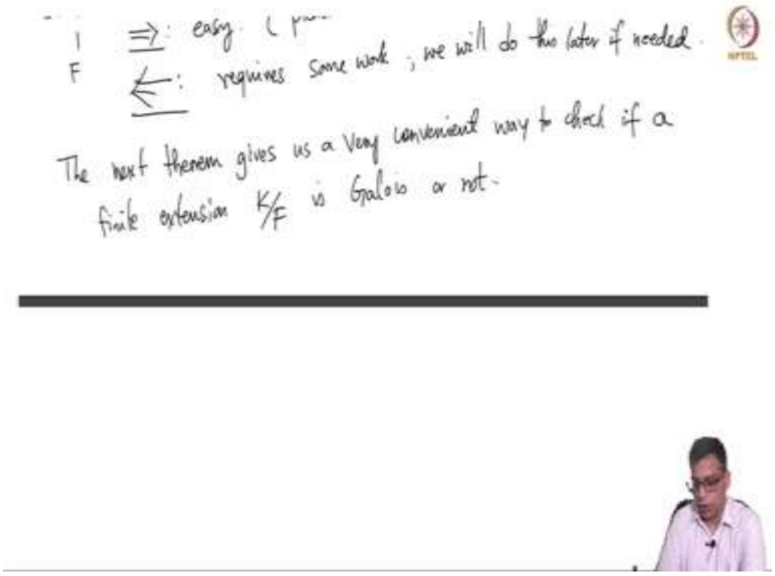
So, this is somewhat like algebraic extensions. So, if you replace word algebraic, if you replace the word separable by algebraic it will be true. So, here, and this is unlike normal extensions, if K over F is normal does not mean L over F is normal, but it is true for separable. So, this part is easy.

Because if K over F is separable, let us take an alpha and K, its irreducible polynomial over F is algebra sorry, its irreducible polynomial over F has distinct roots, is separable, but then irreducible polynomial of alpha over L is a factor of alpha over F. I am going to over this orally, so that I mean you have something to do, so this is an exercise.

So, irreducible polynomial of alpha in K over L divides the irreducible polynomial of alpha over F. If the irreducible polynomial of alpha over F is separable, any factor is separable, so K over L is separable, alpha is separable over L in other words. On the other hand, if you take alpha here, its irreducible polynomial over F will be same as, its, I mean alpha's irreducible polynomial, when you consider alpha as an element of K. So, this is even more easy.

So, alpha is separable over L. So, this, I will let you check, I mean, this is just wordplay nothing more than that. And this requires some work. And we will do this later. Let me say if needed because I am not sure if we will use this but right now we are not going to use this. So, I will omit the proof because it requires some proof, but I think this is a nice statement and that we should prove later. So, I will come back to this at a later part of the course. So, and but it is a nice statement to keep in mind because this is a property of separable extensions in traverse.

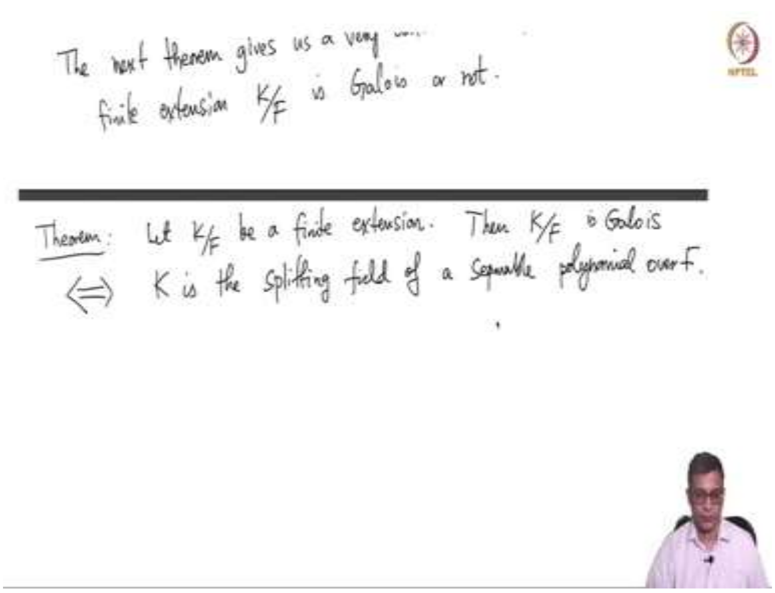
(Refer Slide Time: 24:32)



$|$ $\Rightarrow$: easy (p

F $\Leftarrow$: requires some work, we will do this later if needed.

The next theorem gives us a very convenient way to check if a finite extension K/F is Galois or not.



The next theorem gives us a very

finite extension K/F is Galois or not.

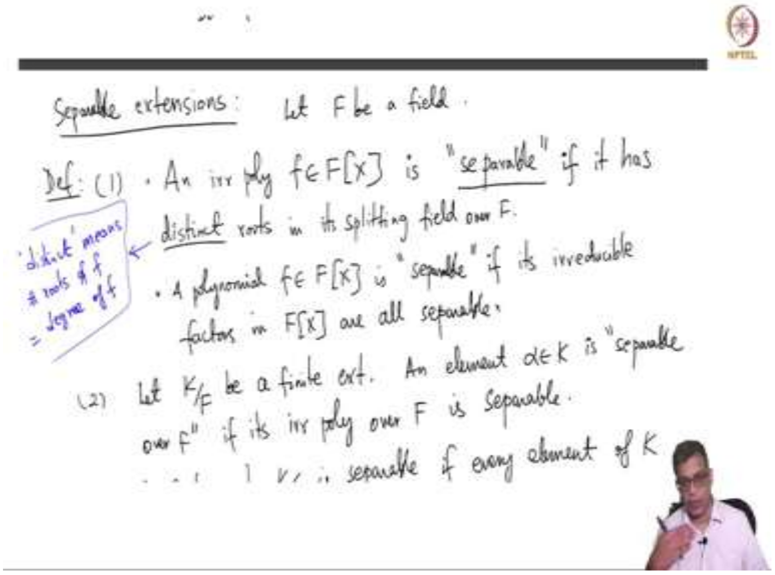
Theorem: Let K/F be a finite extension. Then K/F is Galois $\Leftrightarrow$ K is the splitting field of a separable polynomial over F.

So, now, let us state the theorem that I want to prove next, because I, that proof will take a bit of time, so I want to state it and then start the proof in the next video. So the main theorem that we want to prove now is going to give us a very convenient way of check if an extension, if a finite extension of fields is Galois or not? And the statement is the following. So, let me give you the statement. I will stop the video after writing the statement, and we will start the next video with the proof.

Let K over F be a finite extension, then it gives a characterization of Galois extensions. So, then K over F is Galois if and only if K is a splitting field of a separable polynomial over capital F. See, if you omit the word separable here, this cannot be true statement because K is the splitting filed of a polynomial over F is the meaning of K over F being normal. And as we saw in the example of F to t, FX normal extensions are not Galois in general.

So, you cannot omit the word separable, then the statement is not true, but if you put a separable polynomial, then you have the equivalence with Galois extensions. So, an extension is Galois if and only if it is a splitting field of a separable polynomial over F. So, let me stop this video here. And in the next video, we will recover, we will start with the proof.

(Refer Slide Time: 26:43)



Separable extensions: Let F be a field.

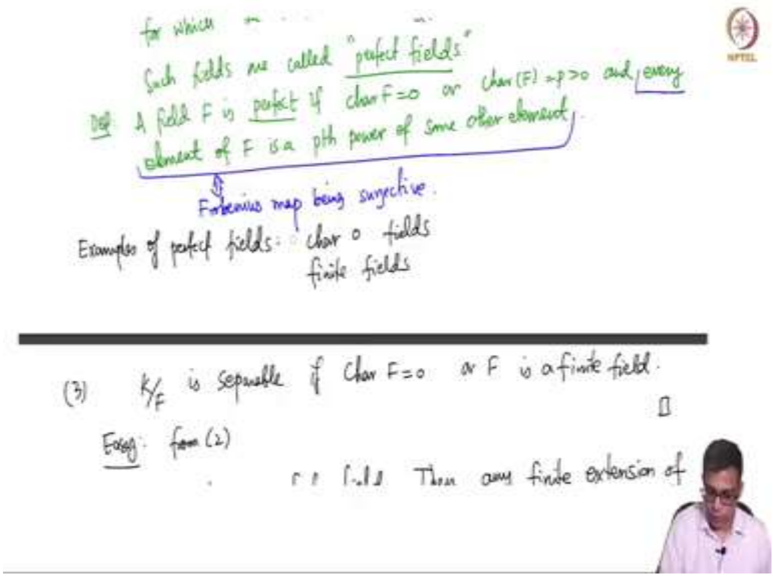
Def: (1) • An irr poly $f \in F[x]$ is "separable" if it has distinct roots in its splitting field over F.

'distinct' means # roots of f = degree of f

• A polynomial $f \in F[x]$ is "separable" if its irreducible factors in $F[x]$ are all separable.

(2) Let K/F be a finite ext. An element $\alpha \in K$ is "separable over F" if its irr poly over F is separable.

[illegible] is separable if every element of K



for which

Such fields are called "perfect fields"

Def: A field F is perfect if char $F=0$ or char$(F) = p > 0$ and every element of F is a pth power of some other element.

$\Updownarrow$

Frobenius map being surjective.

Examples of perfect fields: char 0 fields
finite fields

(3) K/F is separable if Char $F=0$ or F is a finite field. □

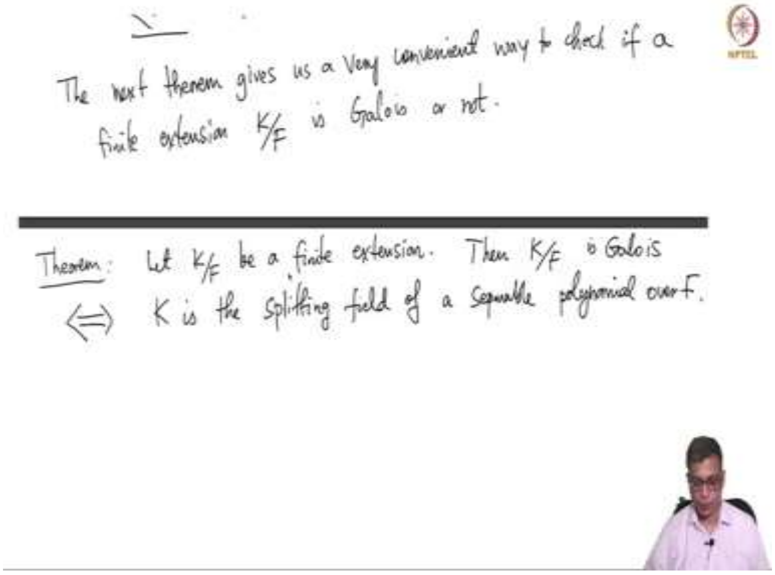
Exag: from (2)

[illegible] Then any finite extension of

Just to recap what we did in the last two videos, I defined the notion of separable extensions. These are extensions where every element is separable that means, every element has the property that its irreducible polynomial is separable, which further means, that irreducible polynomial has distinct roots in an arbitrary extension where it has roots, for example, in the splitting field of that polynomial. And then we learned how to characterize separability of a polynomial using its derivative.

And then using the characterization, we noted that and this is the final statement is the most important for us, if you have a characteristic 0 field or a finite field, then any extension, any finite extension is separable. And in fact that statement is true for perfect fields of which the 2 cases that we are interested in are examples. So, examples of perfect fields, characteristic 0 fields, and finite fields so these are two examples of perfect fields, over any perfect field any finite extension is separable.

(Refer Slide Time: 27:54)



The next theorem gives us a very convenient way to check if a finite extension K/F is Galois or not.

Theorem: Let K/F be a finite extension. Then K/F is Galois $\Longleftrightarrow$ K is the splitting field of a separable polynomial over F.

And now the next order of business for us is to prove this very important theorem, which characterizes Galois extensions in a way that is more practical and will be useful for us when we try to determine if a given extension is Galois or not. So, let me stop this video now. And in the next video, we will prove this theorem. Thank you.