

Algebra II
Professor S Viswanath
The Institute of Mathematical Sciences
Lecture 27
Separable Polynomials

(Refer Slide Time: 00:16)

Separable extensions

Def: let $f \in F[X]$. We say f is separable if it has no repeated roots in any field extension K of F .

$K =$ splitting field of f (or any field extn of F over which f splits)

$f(x) = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n)$



Let us talk about Separable Extensions. So, this is a special property of field extensions. But before we talk about the extensions themselves, let us talk about separable polynomials. So, this is a notion which you have seen already. This is just the idea of having repeated roots or not having repeated roots. So, let me define it formally, let f be a polynomial with coefficients in a field capital F , let us say F is in $F[X]$. We say f is separable, polynomial f is separable, if it does not have repeated roots, if it has no repeated roots in any field extension of capital F . So, in any field extension of K of F .

And of course, to check if, so suppose you are given a polynomial f to check if it is separable or not is, well, where is the best place to check? If you for example, take K to be let us say, the splitting field of f . So, suppose K is the splitting field of f . Or you take K to be, let us say the algebraic closure of the base field, capital F , definitely, over which the polynomial f splits. So, in fact, you can take this or any field extension of F over which f splits completely into linear factors.

So, it is sort of enough to check. So, to check if a polynomial is separable, you just have to check whether it has repeated roots in this particular extension. And well, why is that? Because, of course, here f splits as a product of x minus, so into distinct, but not necessarily distinct into linear factors completely. And if no two of the alphas are equal in K , then the



you can be sure that you will not have repeated roots of f in any other field extension. And, well, what is the, well, what have you seen before about polynomials with repeated roots?

(Refer Slide Time: 03:08)

Recall: Proposition: f is separable $\Leftrightarrow (f, Df) = (1)$
ie f and Df are relatively prime

Also: Discriminant of f $\Delta(f) = \left[\prod_{i < j} (\alpha_i - \alpha_j) \right]^2$
= polynomial in the coeffs of $f(x)$.

f separable $\Leftrightarrow \Delta(f) \neq 0$





Separable extensions

Def: Let $f \in F[X]$. We say f is separable if it has no repeated roots in any field extension K of F .

K = splitting field of f (or any field extn of F over which f splits)

$f(x) = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n)$



So, recall, we have criterion, well, there are two different criteria that you have seen in the earlier lectures. So, to check if a polynomial is separable, you do not really need to go to some, splitting field and check if you have distinct root there, you can just do this checking without leaving the base field at all. And that is the proposition or the theorem.

So, recall the derivative of criterion, recall the earlier proposition, which says that f has no repeated roots, which in our new terminology, f is separable, if and only if the GCD if you take the polynomial f and its derivative, so what is called D of f , if the greatest common

divisor of these two is just 1, if these two are relatively prime, i.e., so in this case, I mean this notation is the ideal generated by f and Df .

But you can also think in terms of just elements, they do not have any common factors, i.e., f , and its derivative Df , are relatively prime. And this is an if and only if condition. So, recall, the derivative here is the formal derivative for polynomial defined by saying the derivative of x power n is just nx to be n minus 1. So, I sort of encourage you to go back and look at the earlier lectures on repeated roots to recall the definitions and properties.

Now, this was the criterion which tells you when a polynomial is separable, you just have to check if the polynomial and its derivative have a common factor or not. And this you can just do in the base field, this is just a calculation in f of x , just compute the GCD by, say the Euclidean algorithm. And also recall a second way of doing this, so we will not really use this, but recall there was this notion of a discriminant of f .

So, this was defined as, well you can just take the product of the various roots, let us say i not equal to j or i less than j and take the square of the roots of the polynomial. So of course, as written, this is something which you can compute in the splitting field or the algebraic closure, because that is where all the roots are going to be present. But the, I mean, a priori, the answer is in K , some splitting field, but we know that the function that we have constructed here is a symmetric function of the roots.

And therefore, this is actually some turn out to be some polynomial in the coefficients, so polynomial in the coefficients of the given polynomial of x . And here is the second criterion for separability. Recall f is separable, meaning it has all distinct roots, is the same as saying this discriminant Δ does not vanish, Δ is not 0. And this Δ of f , this is some particular element of the base field, which turns out to be some polynomial function of the coefficients. So, this is another way of computing or determining if f is separable, just by staying within the field of definition, need not go to some splitting field.

(Refer Slide Time: 06:57)

(Eg) a) $f(x) = (x^3-1) = (x-1)(x-\omega)(x-\omega^2) \in \mathbb{C}[x]$
 $F = \mathbb{Q}$

b) $f(x) = x^3-1 = (x-1)^3$ 1,1,1
 $F = \mathbb{F}_3$

And of course, you probably seen a bunch of examples back in the earlier lecture when repeated roots were discussed. So here are some quick examples, if I take $f(x)$ to be $x^3 - 1$, for instance, and I think of my base field as the field of rational numbers. So, this is a separable polynomial, because let us say I go up to the algebraic closure. So, this is the expansion over let us say, the complex numbers, or you can take the algebraic closure of \mathbb{Q} , it does not matter.

So, once you pass to some extension field, and where it splits completely, there you can check, there if it has distinct roots, then this is a separable polynomial. So here is an example of a separable polynomial and here is a non-example of a separable polynomial, the very same polynomial, but considered over the finite field \mathbb{F}_3 , where as you know, it just splits as $x - 1$ the whole cube. So, this is the expansion over \mathbb{F}_3 and of course, this is not separable, because the root 1 is repeated thrice.

(Refer Slide Time: 08:17)

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

f is separable $\Leftrightarrow Df \neq 0$.

Cor: If $\text{char } F = 0$, then every irreducible polynomial is separable.

Pf: $f(x) = a_0 + a_1x + \dots + a_dx^d$
 $Df(x) = a_1 + 2a_2x + \dots + da_dx^{d-1}$

So, here are some examples and non-examples and what will be important for us is again a fact that was proved during the earlier lecture on repeated roots, recall the following proposition as well or theorem, which says, gives you yet another criterion for separability, but this time for irreducible polynomials. So, let f in $F[x]$ be an irreducible polynomial, in this case separability is much easier. So, let me state it as f is a separable polynomial, if and only if its derivative is not 0, it is not the 0 polynomial. Recall the Df the derivative is again a polynomial in $F[x]$. So, what we are saying is that this this polynomial Df .

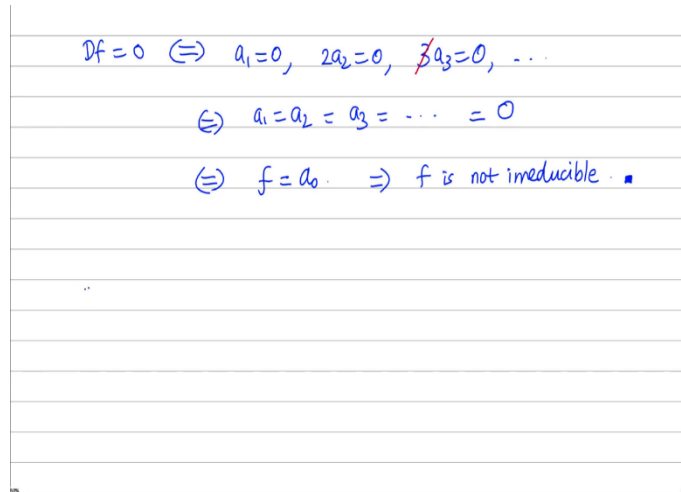
So, this is recall some polynomial in $F[x]$, this is not the 0 polynomial. So, that is equivalent to separability non vanishing of the derivative. And recall this was proved, sort of by showing that and by using the previous criterion that separability is the same as F and Df having a common factor, but Df is strictly smaller, is of strictly smaller degree than F and so they cannot really have a common factor. I mean, if F is irreducible, the only factors of F are 1 and F .

So, if Df has strictly smaller degree, there is really no way it can share a common factor with F , unless Df is the 0 polynomial. So that is how this was proved. So again, here I am referring back to the earlier lecture and corollary is that in characteristic 0, if the characteristic of the field is 0, then the derivative cannot vanish. So, then every irreducible polynomial is automatically separable, every irreducible polynomial F is automatically separable.

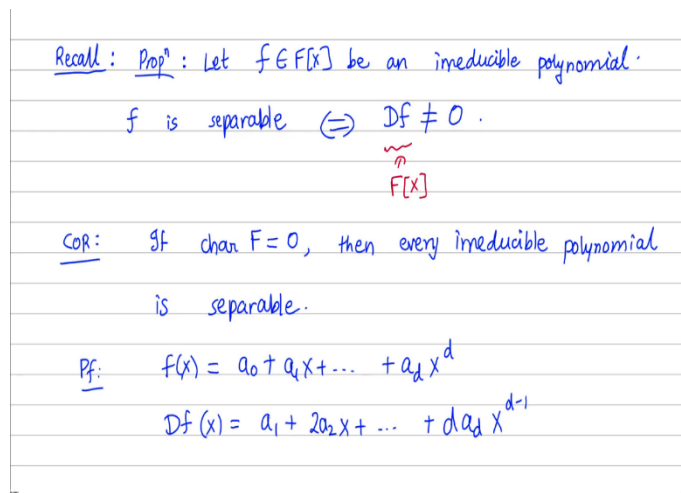
Why is this? Well, if you write out a polynomial, so when can the, I mean the derivative can never vanish. So, proof if the polynomial f looks like, a_0 plus a_1x and so on plus some, let us say it is a degree d polynomial ax^d to the d , then the derivative df of x just looks like a_1 plus

$2a_2x$ plus etc., etc., d ad x to the d minus 1. And the only way in which this can be 0, is if a_1 , a_2 , a_3 are all 0. And here observe you are using the characteristic zero hypotheses, because saying that some multiple of $a_2 = 0$ is saying is the same as saying that a_2 is 0.

(Refer Slide Time: 11:44)



$Df = 0 \Leftrightarrow a_1 = 0, 2a_2 = 0, \cancel{3}a_3 = 0, \dots$
 $\Leftrightarrow a_1 = a_2 = a_3 = \dots = 0$
 $\Leftrightarrow f = a_0 \Rightarrow f$ is not irreducible. ■

Recall: Propⁿ: Let $f \in F[x]$ be an irreducible polynomial.
 f is separable $\Leftrightarrow Df \neq 0$.
 $\underbrace{F[x]}_n$
Cor: If $\text{char } F = 0$, then every irreducible polynomial is separable.
Pf: $f(x) = a_0 + a_1x + \dots + a_dx^d$
 $Df(x) = a_1 + 2a_2x + \dots + da_dx^{d-1}$



So, observe that the derivative can be 0, if and only if the following equations are true a_1 is 0, $2a_2$ is 0, $3a_3$ is 0, and so on. But then this is the same as saying a_1 is 0, a_2 is 0, a_3 is 0 etc. Because you can sort of cancel, so for example, $3a_3$ is 0, means a_3 is 0, yes, the field has characteristic 0. If the field had characteristic 3, for example, then $3a_3$ is 0 is always true, you cannot conclude that a_3 is 0 from there.

So now, where does this this leave us? This says that this is the same as saying that f is a constant. This is like our classic statement from, say analysis, which says that the only

polynomials with derivatives 0 are just the constants, this holds over characteristic 0 fields. But of course, a constant cannot be irreducible. If f is a constant, but then constants are not irreducible, it is their unit.

So, this is, observe in this case f is not irreducible. So, the conclusion that we wanted, if f is irreducible, then it is automatically separable. So that is what we have managed to show. Because if f is irreducible, then it cannot be a constant. So that is a nice fact for characteristic 0 that irreducibility automatically implies separability, irreducible polynomials must have non repeated roots. Whereas the, the same thing is not true over characteristic p as we just said.

(Refer Slide Time: 13:35)

If $\text{char } F = p$ (p prime)

Then, it is no longer true that irreducible polynomials are separable!

(Eg) $F = \mathbb{F}_3(t) = \left\{ \frac{a(t)}{b(t)} : a, b \in \mathbb{F}_3[t], b \neq 0 \right\}$

field of rational functions over \mathbb{F}_3

char 3



So, let us now consider the next situation which is what if f has characteristic p , if characteristic of f is a prime p , so p is some prime number here. So, this is the positive characteristic case, then this factor is no longer true. Then it is no longer true that irreducible are separable, irreducible polynomials are automatically separable. So, one has to be a little careful in arbitrary characteristic.

And here is an example to show that one has to be a little careful when dealing with the case of finite characteristic. So, let us take the field F to be the following. So, I will take \mathbb{F}_3 but I will also adjoin this variable t to it. So, what is \mathbb{F}_3 of t ? So, t is just some indeterminate here. So, what is \mathbb{F}_3 of t ? This is the set of all rational functions. So, this is the field of rational functions in the variable t , which means it is polynomial divided by polynomial.

So, what are a and b ? They are both polynomials with coefficients in F_3 and the denominator is not 0. So, b is not the 0 polynomial. So, this is the field of rational functions. So, it is a field. And it is in fact, still a field of characteristic 3. It is a field of rational functions. So, if you take any element of this field, and you take 3 times that, then that is just 3 times a over b , but 3 times a is just the 0 polynomial. So F_3 of t is still have of characteristic 3. So, it is a field of rational functions over the field of F_3 . And this is still a characteristic 3 field. So, I should say F is a characteristic 3 field. Now, I claim that in this characteristic 3 field, you can find irreducible polynomials, which have repeated roots.

(Refer Slide Time: 15:55)

$$f(x) = x^3 - t \quad \textcircled{1} \quad f \text{ is irreducible}$$

$$\text{If not, then } f(x) = (x - \alpha)g(x) \quad \deg g = 2$$

$$\text{for some } \alpha \in \mathbb{F}_3(t) \Rightarrow \alpha = \frac{a(t)}{b(t)}, b \neq 0$$

$$f(\alpha) = 0 \Rightarrow \alpha^3 = t \Rightarrow \left(\frac{a(t)}{b(t)}\right)^3 = t$$

$$\Rightarrow (a(t))^3 = t(b(t))^3$$

$$a(t) = a_0 + a_1 t + \dots \quad (a(t))^3 = a_0^3 + (a_1 t)^3 + (a_2 t^2)^3 + \dots + 3(\text{cross terms}) \rightarrow 0 \text{ in } F$$



What is an example? So here is the simplest example. Let us take f of x to be the polynomial x cubed minus t . So, recall, t is now, it is an element of the field, it is an element of f . So, this is a polynomial of degree 3, x is the variable, t is like a constant. So, we'll claim number 1, that f is irreducible. Let us check this. So, if f is reducible, then what can you conclude? So, proof of irreducibility, if not, then, well, it is a polynomial of degree 3. So, it has to split into two pieces. Let us say it splits, it is not irreducible, then at least one of the two factors must have degree 1.

In other words, then there exists, so how does f split then, f splits like this, let us say f of x must split as, some degree one piece into some possibly degree two piece. So, degree of g is 2 we can say. So, g may or may not be irreducible. But I know for sure there is one linear term. And what is α here? For some α in the base field, the base field here is F_3 of t .

In other words, α looks like some a of t by b of t , some rational function, b is not 0. And so, f of α is 0, therefore, because f of x is x minus α into gx , if you plug in α

equal to 0, what you are going to get? If you plug in alpha for x, you are going to get 0. This just means that alpha is the root of the original equation. So alpha cubed equals t. Therefore, this is going to give us a contradiction. This is like saying the polynomial at divided by bt this is a rational function, when you take this and you cube it, it just gives you t.

Why is this not possible? Because, well, let us rewrite it. It is a t cubed equals t times bt cubed. And if you sort of see what these two sides look like, well, a t cubed a is well, if you cube a polynomial, what do you get in this case? Well, a polynomial looks like this, a t is some a0 plus a1t, and so on. If you cube it, it is like the calculation we just did. I mean, we talked about this polynomial x cubed minus 1. So, a t cubed is just going to give you, well a0 cubed plus a1t the whole cubed plus a2t square the whole cubed and so on.

And then there will also be lots of cross terms. So, when you do this expansion, you are also going to get a 3 a naught square, a1t plus 3 whatever a naught something and so on. But all the cross terms are all going to look like three times something. So, these are these are going to be the cross terms in the expansion. And they are all 0. Why because this is recall everything is over the field F3, F3 of t. So, or you can say that, as we just observed three times any element of f is just 0, f the field F3 of t is of characteristic three.

(Refer Slide Time: 19:41)

$$a(t)^3 = a_0^3 + a_1^3 t^3 + a_2^3 t^6 + \dots$$

$$t b(t)^3 = t b_0^3 + b_1^3 t^4 + b_2^3 t^7 + \dots$$

② $Df = 3x^2 = 0$ in $F[x]$. $\Rightarrow f(x)$ is not separable!

$f(x) = x^3 - t$ ① f is irreducible

If not, then $f(x) = (x - \alpha)g(x)$ $\deg g = 2$

for some $\alpha \in \mathbb{F}_3(t) \Rightarrow \alpha = \frac{a(t)}{b(t)}, b \neq 0$

$f(\alpha) = 0 \Rightarrow \alpha^3 = t \Rightarrow \left(\frac{a(t)}{b(t)}\right)^3 = t$

$\Rightarrow (a(t))^3 = t(b(t))^3$

$a(t) = a_0 + a_1t + \dots$ $(a(t))^3 = a_0^3 + (a_1t)^3 + (a_2t^2)^3 + \dots$
 $+ 3 \text{ (cross terms)} \rightarrow 0 \text{ in } \mathbb{F}$



Recall: Propⁿ: Let $f \in \mathbb{F}[x]$ be an irreducible polynomial.

f is separable $\Leftrightarrow Df \neq 0$.

$\underbrace{Df}_{\in \mathbb{F}[x]} \neq 0$

Cor: If $\text{char } \mathbb{F} = 0$, then every irreducible polynomial is separable.

Pf: $f(x) = a_0 + a_1x + \dots + a_dx^d$

$Df(x) = a_1 + 2a_2x + \dots + da_dx^{d-1}$



So, these terms are 0. So, the element $a t^3$ in the field \mathbb{F} just works out to be something like this. So, this is a_0^3 plus $a_1^3 t^3$, and so on. So, it is a polynomial, which only involves the powers, t^0, t^3, t^6, t^9 and so on, this is $a t^3$, sorry. Well, the same thing holds for $b t^3$. It is again going to involve only, $b_1^3 t^3$ and so on. But now I am going to multiply it by t , because what I know is that $a t^3$ is supposed to equal t times $b t^3$. Now we can see the contradiction, because now the right-hand side has powers of t , which look like t^1, t^4, t^7 , and so on.

So, these are all powers of t congruent to 1 modulo 3. And so, these two can never be equal. There is just no way these two can be the same answer, unless, of course, all the a 's and b 's are 0, but we have assumed that these are not. So that argument concludes the proof of irreducibility of this polynomial f .

Now, it is easy to see that f is not separable. Why? Well, we already have a criterion for separability. If you have an irreducible polynomial here, so let us go back and look at our proposition. So, what is the proposition? Say, if you have an irreducible polynomial, then checking separability is very easy. It is separable if and only if its derivative does not match.

So, we have already shown that this polynomial is irreducible $x^3 - t$. Let us show that its derivative vanishes. So, let us compute its derivative. It is just $3x^2$. Recall the t is a constant here. So, well, the derivative is just $3x^2$, but that is of course, just 0 in polynomial f of x . So, the derivative here is just 0.

So, what does that imply? That says that this polynomial is not separable, symbolize polynomial f of x , and which is exactly what we do. So, if you have a field of finite characteristic, then irreducible polynomials do not automatically become separable. But there is this one sort of nice exception or a special case when this holds, so those are what are called perfect fields.