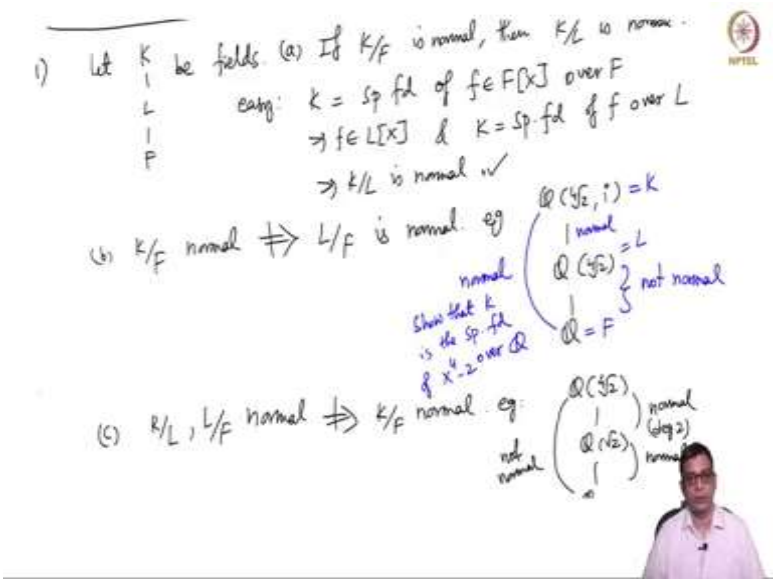
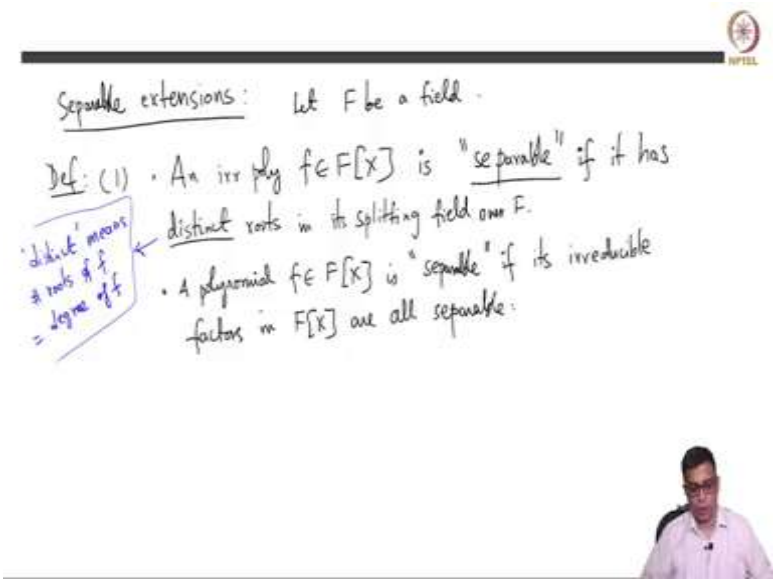
Introduction to Galois Theory
Professor Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute
Lecture 18
Separable Extension – Part 1

(Refer Slide Time: 00:38)



Welcome back, in the last video we in the last few videos in fact, we looked at Galois extensions. We also defined the notion of normal extensions. And I did a couple of problems sessions, problem sessions in the last two videos, where we looked at some properties of normal extensions, and also characterized normal extensions, understood how normal extensions behave in a tower of three fields. And I introduced you an important relation between Galois groups of extensions, when you have a tower of three fields.

(Refer Slide Time: 00:58)



So today, let us introduce any very important notion called separable extensions. Separable extensions are very important. And this, in fact, gives us a very convenient way of checking if something is Galois or not. So in this video, I will introduce to you, maybe you have read these things in a course on field theory. So, but I need some basic definitions and properties of this. And once we finish this in the next video, we will get back to Galois extensions.

So in this video, it is going to be sort of a review, if you have seen separable extensions. If you have not seen separable extensions, this is going to be a very quick introduction to them. So, let us start with an arbitrary field. So, let capital F be any field. So, I am going to give you some definitions first. First definition is an irreducible polynomial, so I am going to shorten it like this, over the given field is called separable if it has distinct roots in its splitting field.

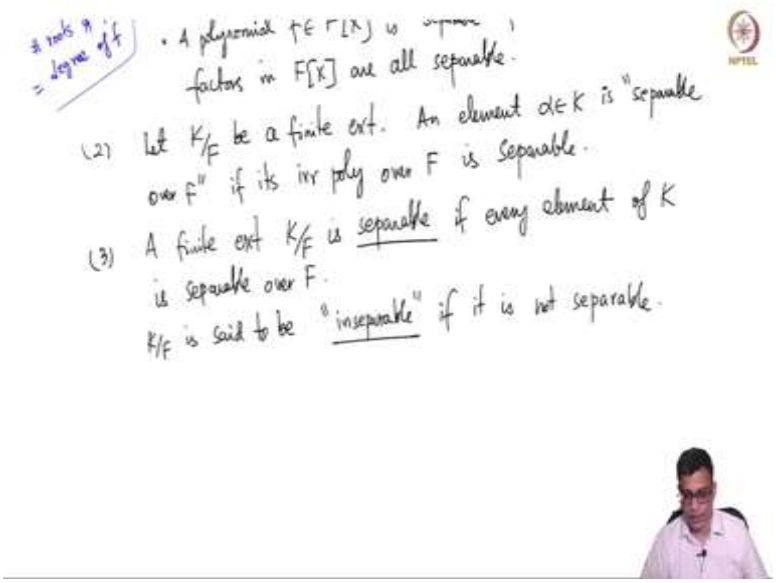
So remember that this may not have roots in the given field itself. But wherever it has roots, we know that it has a splitting field. So we might as well consider that. It is called separable if it has distinct roots in its splitting field. Just a remark about what distinct means. So, distinct means as many roots as its degree, number of roots of F equals the degree of f.

So, I will do a few examples later on. But this is a very common phenomenon. So in fact, most polymers that you are used to, if you work with characteristic zero, for example, every polymer has this property. So it is difficult to find a polynomial, which does not have this property, but they do exist.

So, I am going to come to that after I complete the definitions. I give you some examples. Just before I go to the second definition, though we rarely talk about a polynomial being separable, I want to define that for, to be able to state the next theorem most conveniently. So polynomial, I have now omitted the irreducibility condition. So here I take irreducible. Now I am just taking any polynomial is separable.

If, I do not want to say it has different roots, because it may have multiple roots, but I want its irreducible factors to be, so the polynomial may not be irreducible, but it will factor into reducible polynomials in FX are all separable. So the polynomial itself may not have distinct roots, but we want its irreducible factors to be separable. I will give you an example to illustrate this.

(Refer Slide Time: 4:30)

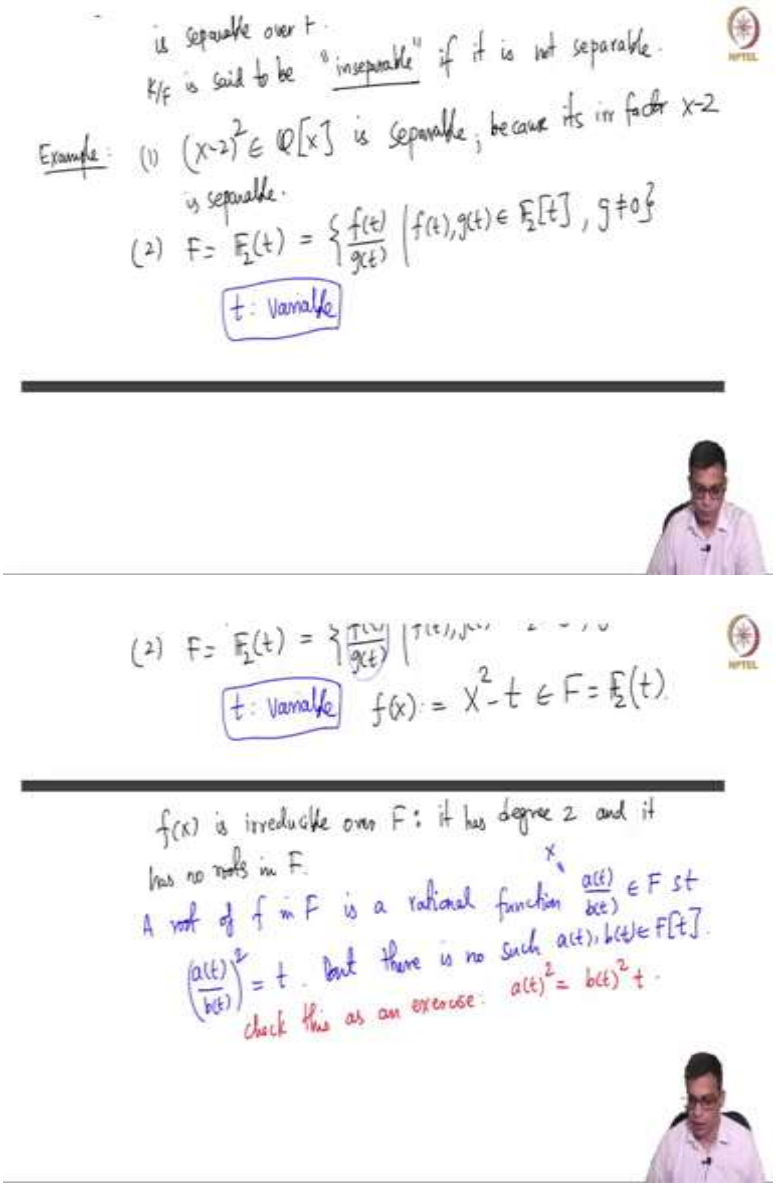


Now, next definition is that a finite extension, of fields of course, always is separable. Actually, let me just first define what it means for an element to be separable. So, let K over F be a finite extension. In this course, we are only going to look at finite extensions of fields. An element alpha and K is separable over F.

I have defined in one, I have defined the notion of a polynomial being separable, now I am defining an element being separable, an element is separable over f if its irreducible polynomial over capital F is separable. A finite extension is always algebraic, so its, this element will have an irreducible polynomial. If that is reduced, separable then the element itself is said to be separable.

Finally, a finite extension this you can now guess, K over F is separable if every element of K is separable over F, simple definition just like algebraic extensions, if every element is separable, we say the extension is separable. K over F is said to be inseparable, so the antonym is inseparable if it is not separable, that means, even one element is not separable. So, just like the antonym for algebraic is transcendental, so we say that is extension is inseparable if it is not separable.

(Refer Slide Time: 6:36)



So now before I discuss some properties, I will give you just very quickly one or two examples. So, for example, if you take is separable, though, it does not have as many roots as its degree, here the degree is two but it has only one root, because its irreducible factors,

which is only one actually is separable. Just to illustrate that, for irreducible polynomial to be separable, all you need is distinct roots.

For an arbitrary polynomial to be separable, you need to look at its irreducible factors. A more interesting example, in fact, every polynomial of QX is separable, as we will discuss very soon. But a more interesting example is this. So, let us take F to be the rational function field over the finite field F 2. So this is all ratios of polynomials like this, in the polynomial ring and of course, g must be nonzero.

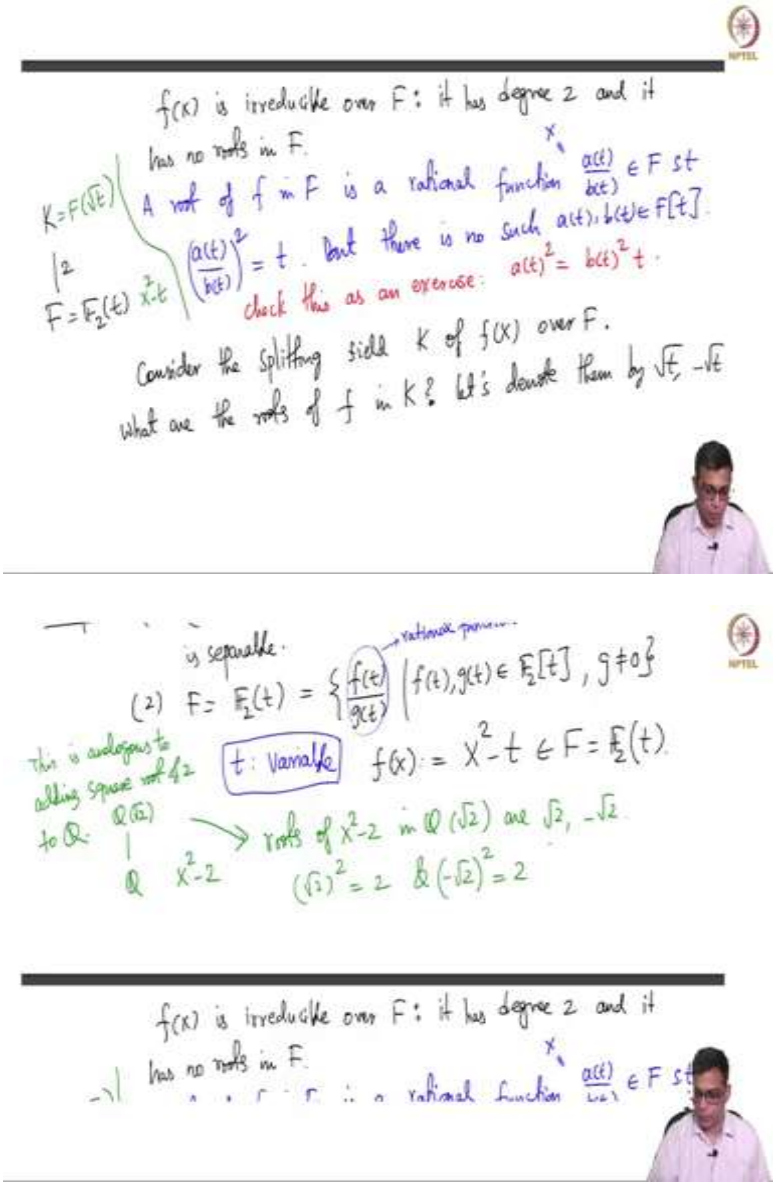
So here T is a variable, so T is a variable. So in this field, so this is a very big characteristic to field. So, in this field, let us consider, so x will refer now to the variable, so let us take f to be, f x to be X square minus t in F, which remember, is F2 round bracket T. So in this polynomial, you take this, so it is easy to see that f is irreducible over capital F.

So, this is a bit confusing, but if you just pause and think for a minute, it will become clear to you. It is irreducible because it has degree 2. And as we discussed some time back any degree 2 polynomial is irreducible, if and only if it has no roots, it has degree 2, and it has no roots in capital F. That is clear, because what is a root of, a root of f in capital F is a rational function.

So this such things are called rational functions. So it is like rational numbers, which are ratios of integers, rational function is a ratio of polynomials. So a root of f is a rational function. Let us say AT by BT. I have taken f here, so I should really use some other letters, at by bt in F, such that, you plug in this equal to x right, at by bt whole square is equal to T, but there is no such at bt in the polynomial.

So, this is something you can check as an exercise because just consider degree of such an expression. Check this as an exercise, if there is such a thing, what you will have is at square equals bt square times t. So, you cannot have any polynomials, 2 polynomials at bt, which have this property. So, this is not possible, that means at or bt such that at or bt whole square equals t does not exist. That means, this polynomial here has no roots in capital F, that means it is irreducible in capital F t, or capital F. But what are the roots of this?

(Refer Slide Time: 10:54)



Now consider the splitting field. So, these are very crucial example. So, it is important for you to understand this, I am going to describe this in detail. Consider the splitting field of K of f x over capital F. So, you have capital F, which is f t round bracket T, and K is a splitting field. And remember, this is not equal to K because f has no roots in F.

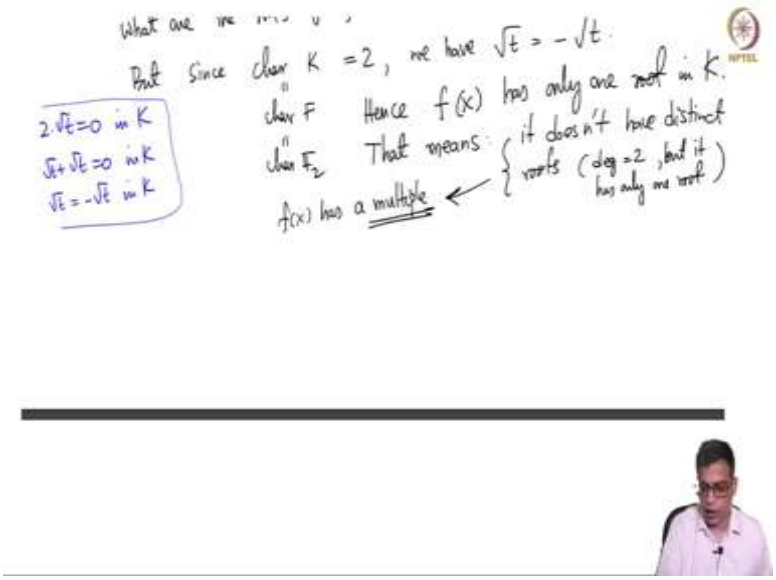
So, this must be degree 2, because you are adding a degree, roots of a degree 2 polynomial, which is irreducible, and once you add a root this is something that we know, all other roots are added. So, this is degree two. What is this field K? And we also remember that every polynomial or every field has a splitting field. So, K exists is something that we know.

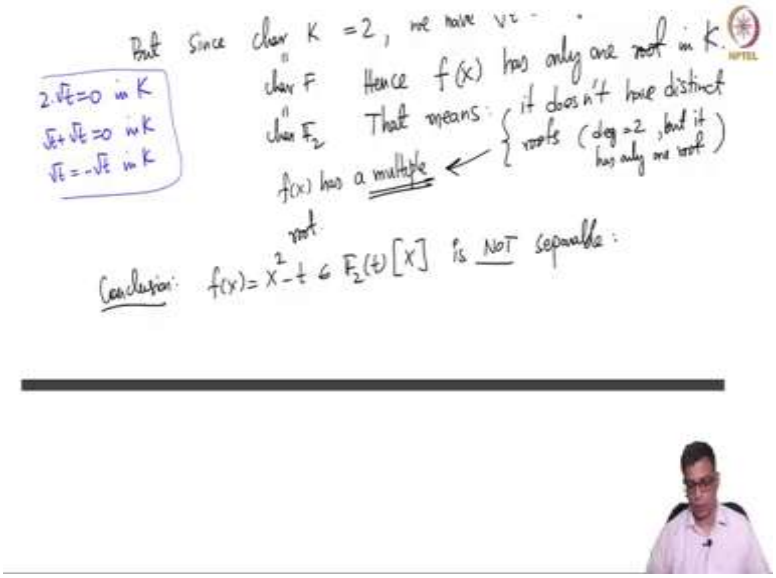
So, what are the roots of F and K? See this is exactly like, so I will just, though the situation is somewhat unfamiliar to you, this is exactly similar to this is analogous to adding roots, let us say square root of let us say 2 Q. So, what we really do there is Q, you take x square minus two remember roots of x square minus 2 are square roots of 2, so that is a square root of two. So, adjoin this.

So, here you take the square roots of the polynomial x square minus T and you adjoin root. So, it is convenient to denote the roots by root 2 t because that is what they are, they are square roots of t. So, what are the roots of capital F small f and capital K, let us denote them by, and you would have root 2 and minus root t.

This is where, so here for example, roots are, so let me just roots of x square minus 2 in Q root 2 R minus root, because, root 2 square is 2 and minus root 2 square is 2. So, they are the two rules remember a polynomial or field can have at most as many roots as the degree, so here degree is 2 and there are 2 roots, one and two. Here also there is degree 2 and there will be at most 2 roots but now I claim that there is exactly one root in fact.

(Refer Slide Time: 14:01)



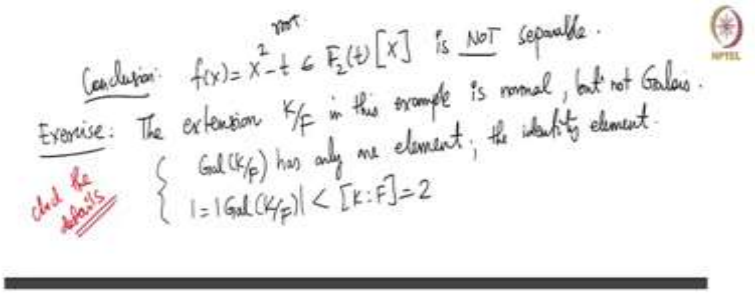


But since, characteristic of K which is of course, characteristic of f, which is characteristic of F 2 is 2, we must have root 2 equals minus root, root t equals minus root t. So, in this field 2 times anything is 0. So 2 times root t is 0 in K. So, 2 times root t is 0 in K, that means root t plus root t is 0 in K, that means root t equals minus root t in K. That means root t equals minus root t and hence fx has only one root in K.

That means, it does not have, I am just writing the various equivalent statements, does not have distinct roots because this came up earlier when we talked about some examples of normal extensions. And I hinted to you why they will not be Galois in general, it does not have distinct roots, degree is 2, but it has only one root.

So, that means it does not have distinct roots or yet another way of saying this is f has a multiple root. So any root that repeats at least twice is called a multiple root. So the conclusion of all this, so all this is to conclude fx, which is x square minus t, which is a polynomial in one variable over the field F2 t is not separable, it is not separable, because it is irreducible and it has only one root, it must have two roots for it to be separable, so, it is not.

(Refer Slide Time: 16:19)

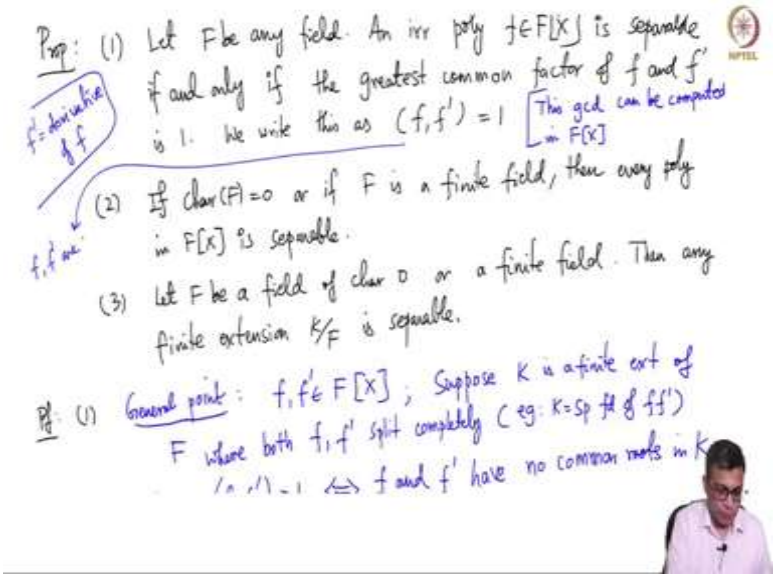


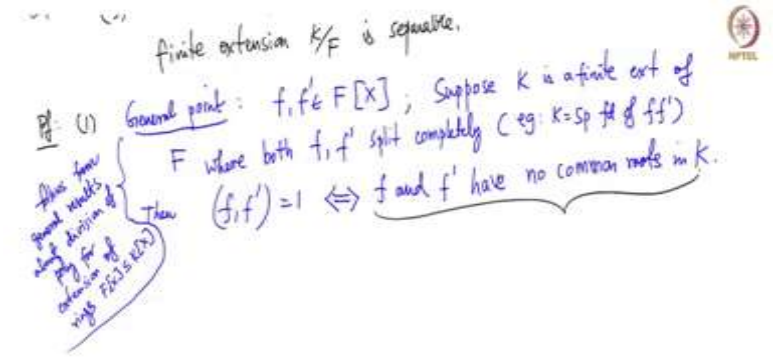
So as an exercise and I will come back to this in detail later. But right now I want to move on. So I will leave this as an exercise at this moment, the extension K over F, K over F being this K over F, in this example, that means, f is this, K is the splitting field of x square minus t, is normal. This is by definition, because it is a splitting field of a polynomial, but not Galois. It is normal, but it is not Galois.

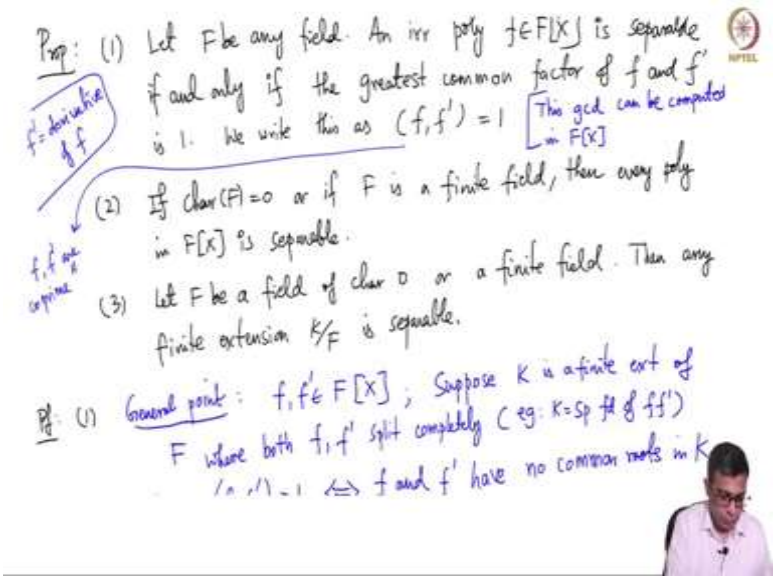
Because if you consider the automorphisms of K over F, I claim that it has only one element, the identity element, because it must send root t to another root of its irreducible polynomial. But there is only one such namely root t, minus root t is also equal to root t. So, the Galois group has only one element, so one equals the cardinality of the Galois group, which is less than the index of the degree of the extension.

So, in fact, I have done this exercise but check the details. If there is anything that is not clear to you check the details. So, you have here an example of a normal but not Galois extension, we will see soon how to provide the missing ingredient, which is exactly separability. So, here the polynomial in question is not separable.

(Refer Slide Time: 18:14)







So, before we go on to that theorem that I want to prove, which is a crucial theorem about Galois extensions, let me introduce some properties of separable extensions because these are useful anyway to keep in mind. So propositions, so I am going to write this as a proposition, one first part is an irreducible polynomial.

So f is any field, an irreducible polynomial small f is separable, so, if and only if the greatest common factor of f and f prime, which is the derivative of f, is one. So, we write this as the GCD. So, is usually denoted by f comma f prime in brackets. So, f prime is the derivative of f, the formal derivative of a polynomial in one variable, you know how to do that.

So, that is the first way, first part of the proposition, it is a good way to check if something is separable or not, you simply look at its derivative and compute the GCD. And this GCD, the point is this GCD, so this GCD can be computed in f itself. So, this I will explain again in the proof, but you do not need to compute, you do not need to see the factor and if, you know that the factor completely then you can easily look at the common factors and see the GCD, but you can actually do that in F itself.

So, now the second part of the proposition which is actually useful for us is if characteristic of F is 0 or if F is a finite field, then every polynomial in FX is separable, so separability is no condition at all if you have a characteristic 0 field or a finite field. And the third statement is a immediate consequence of two, but I want to write this because it is useful to keep this in mind. Let F be a field of characteristic 0 or a finite field.

So, F is either characteristic 0 field or it is a finite field. Then any finite extension of F is separable. So, separability is no condition at all again if you have a field of characteristics 0 or a finite field. So, 3 of course (())(21:29) from 2, so I am going to prove one and two. So, let me quickly prove this as I said my goal here is not to do this in a comprehensive manner, but give you a quick idea of how to prove this.

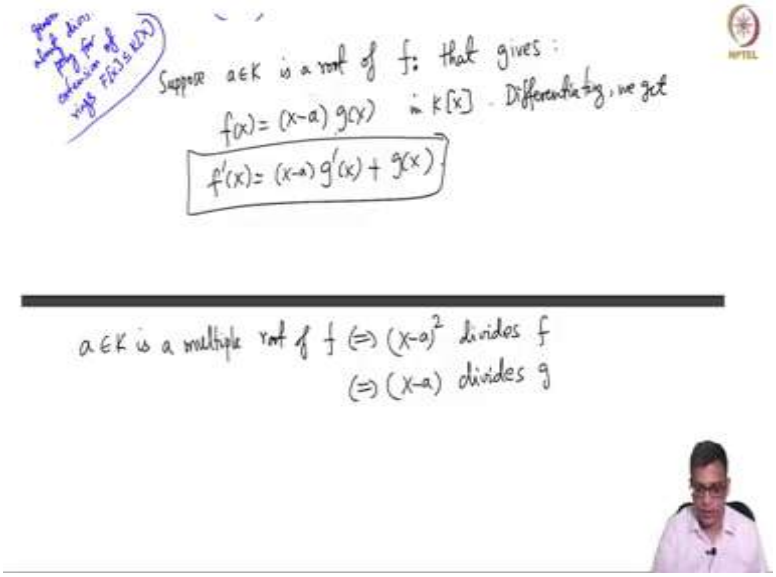
So, again this is something that you could have seen in any course on field theory. So, just prove one the crucial idea is the following. Suppose, a in F, so the point is this is a general point, so which I will write first. So, we have f and f prime are in the polynomial ring over capital F. Suppose, K is a finite extension of f where mode f and f prime split completely.

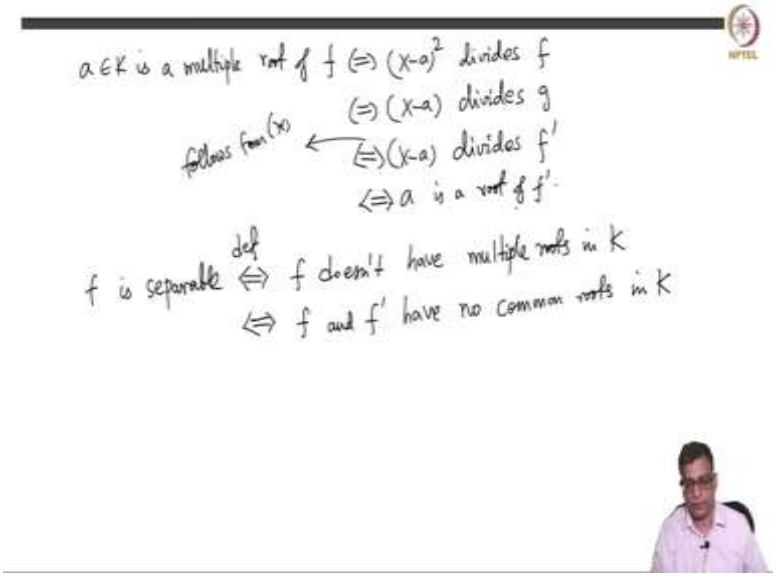
For example, you can take a to b splitting field of f times f prime, so f and f prime are both going to factor completely into linear polynomials in K. Then GCD, so I will just write this as f comma f prime is one which is the terminology that I am following here. So, if the greatest common factor is one means GCD is one in bracket f comma f prime in bracket one, if and only if f and f prime have no common roots.

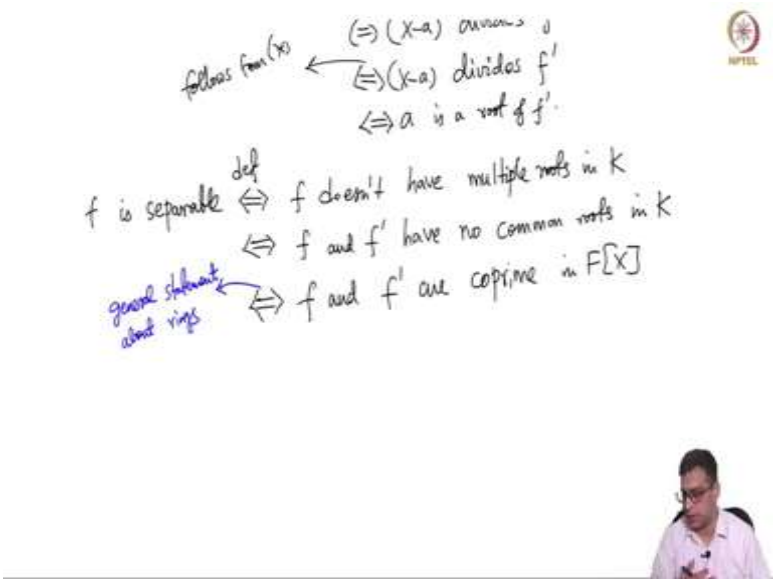
So they may not have roots in f, but they will have roots in K for some arbitrary, I mean some particular extension K. And if they have no common roots there, they have to be irreducible, they have to be co-prime. So this is really called co-prime. We say f and f prime or co-prime. That is the terminology.

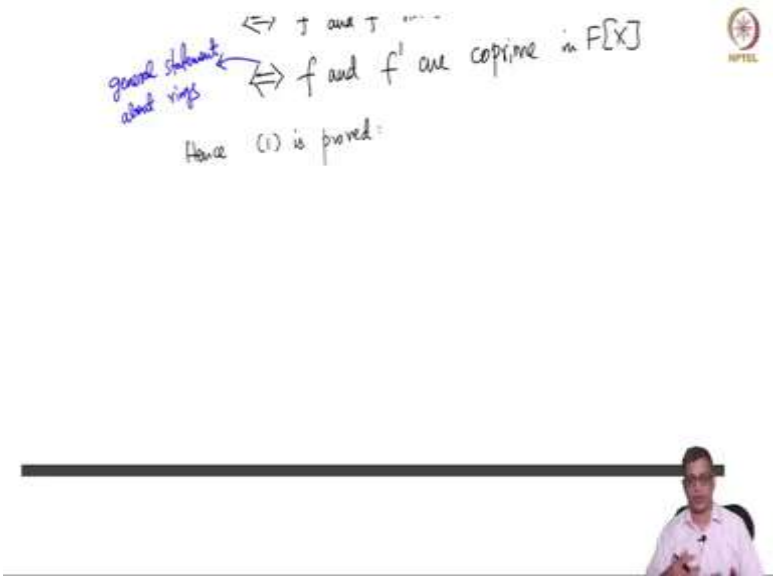
So this is some general ring theory statement. So this is from some general results about division of polynomials for extensions of rings, fx containing K. So I do not want to spend time on this. This is a general statement. So I might as well work with the splitting field of f times f prime and see if they have a common root. So I will really study this.

(Refer Slide Time: 24:45)









So suppose a in K is a root of, let me we start with the root of f. So that means that gives, so here I am really working in capital K x, that gives f x equals x minus a times gx. This is, this is the meaning of a being a root that means x minus a divides fx, differentiating both sides, we get f prime x is equal to the product rule, you take formal derivation of polynomials follows the usual derivative rules. So this is x minus a times the derivative of g plus gx times the derivative of x minus a, which is one.

So, this is the, the important equation that I want to analyse. So now, I claim that a in K is a multiple root. What is the meaning of multiple routes, so that means x minus a square divides f, because you must have a root appear at least twice in its factorization in a splitting field.

So, this means x minus a whole square divides F, but this means x minus a divides g because x minus a is one factor like this. So, g must also have a factor of x minus a. And I claim that this is if and only if, these two are just definitions, but this, the last statement is the consequence of this equation, because x minus a divides g, that means x minus a divides the right hand side here, so divides f prime.

On the other hand if I have x minus a divides f prime that means x minus a divides f, this as well as of course, it divides this, so it divides g, so this is a, this implication follows from start. But if x minus a divides f prime, that is clearly same as a is a root of f prime. So, a is a root of f prime. So, now, this is the statement, so a is a multiple root of f if and only if a is a root of f prime.

So, that means, so now let me just write down a series of things, f is separable, f is separable if and only if f does not have multiple roots in K, this is the definition. It does not have roots multiple roots in a splitting field. But of course, it does not have multiple routes in any field where it has roots, it need not be splitting field, because one its roots or what its roots are.

So, whether it is splitting field or some extension of splitting field, you get the same statement. So it does not have multiple roots in K. That means f and f prime have no common roots because a is a multiple root of F means a is a root of f prime. Now if nothing is a multiple root of f, then it cannot be root of a, every root of a f is not a multiple root of f, that means that root is not a root of f prime, that means f and f prime have no common roots in K.

This implies f and f prime are co-prime in fx itself, this as I said is a general ring theory statement that I started this proof with. So, this is something that you can look up somewhere else. This is just a simple fact that you can find for example in Artin's book, Michael Artin's book. So, if they have no common roots in K in the base field itself they cannot be, they cannot have a non-constant common factor.

So that means they are co-prime, so this exactly means, so hence, so I think one is proved. So, one is proved. So let me stop this video here because it has already been time. I will stop this and continue with the proof of the remaining two parts in the next video. Thank you.