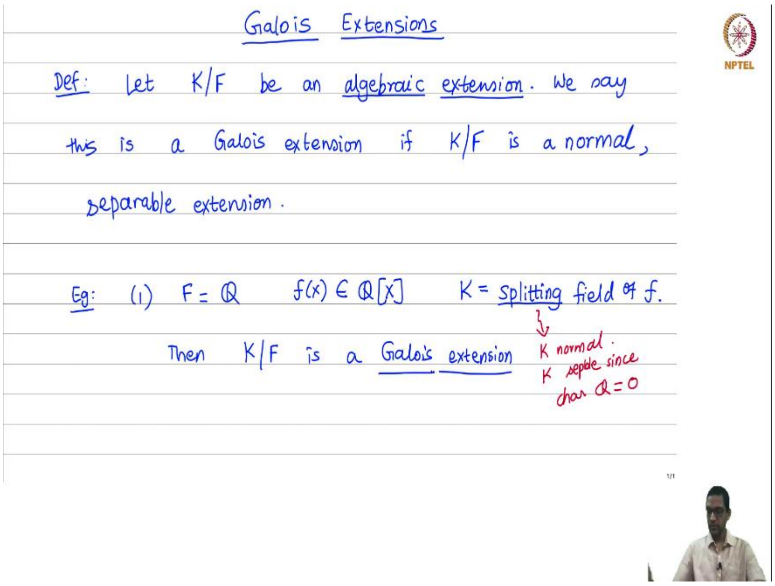
Algebra II
Professor S Viswanath
The Institute of Mathematical Sciences
Lecture 29
Definition and Examples Fixed Fields

(Refer slide time: 00:14)



Galois Extensions

Def: Let K/F be an algebraic extension. We say this is a Galois extension if K/F is a normal, separable extension.

Eg: (1) $F = \mathbb{Q}$ $f(x) \in \mathbb{Q}[x]$ $K =$ splitting field of f.

Then K/F is a Galois extension

K normal.

K sepble since char $\mathbb{Q} = 0$

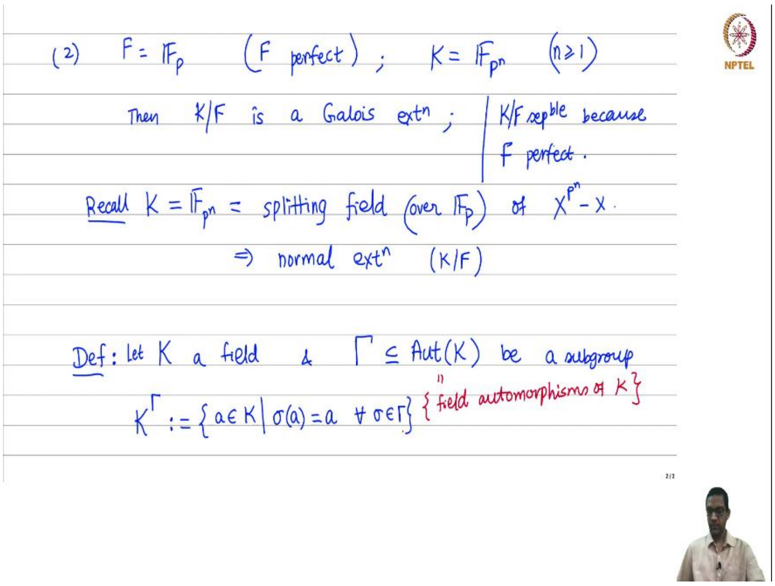
We will talk about Galois extensions today. So, first the definition, let K be an algebraic extension, let K over F be an algebraic extension. We say that this is Galois, we say this is a Galois extension, if it has two properties number one, K over F is a normal extension and number two, if it is a separable extension. So, we talked about both these adjectives already, when is an extension called normal? When is an extension called separable? And if an extension has both these properties then it is called a Galois extension, if it is a normal separable extension.

And notice here that we do not really require that K over F should be a finite extension and so on. All we demand is that to begin with, that it should be an algebraic extension, could be an infinite or finite extension. But of course, eventually, we will restrict ourselves to a more in-depth analysis of the finite Galois extensions. But the definition is completely general. And so, quickly let us see the examples.

So, if I take my base field F to be the field Q, and if I take any polynomial fx in Qx and if I define K to be the splitting field of this polynomial. So, what I can do is to take K, define K to be the splitting field of this polynomial f, then K over F is automatically Galois, K over F is a Galois extension. Why is this? We just need to check the two adjectives. The two properties it is supposed to have because it is a splitting field of a polynomial, it is normal.

So, recall this is one of the definitions or characterizations of a normal extension. So, this tells you that K is normal. And K is separable comes for free, because recall Q is a characteristic 0 field. And we talked about this when we talked about separable extensions and so on. Any algebraic extension over a characteristic 0 field is automatically separable. So, K is separable, separable since characteristic of Q0. And recall we also have a version of this for characteristic p, in that case, we require the field to be perfect, so sorry, Galois extension.

(Refer slide time: 03:26)



(2) $F = \mathbb{F}_p$ (F perfect) ; $K = \mathbb{F}_{p^n}$ $(n \geq 1)$

Then K/F is a Galois extⁿ ; | K/F sep^ble because F perfect.

Recall $K = \mathbb{F}_{p^n}$ = splitting field (over $\mathbb{F}_p$) of $X^{p^n} - X$.

⇒ normal extⁿ (K/F)

Def: let K a field & $\Gamma \subseteq \mathrm{Aut}(K)$ be a subgroup

$K^{\Gamma} := \{a \in K \mid \sigma(a) = a \ \forall \sigma \in \Gamma\}$ {field automorphisms of K}

So now, let us look at a second example, which is for finite fields. If I take F to be Fp, then recall this case it has finite characteristic, but recall that F is perfect. And that meant that the Frobenius map is an automorphism of the field. And in this case, again, we have seen the following that you will get separability for free, if K is algebraic extension of F then separability is automatic, because the definition of separability is that every irreducible polynomial, so you take any element of the extension field, its minimal irreducible polynomial over the base field must be a separable polynomial, must have distinct roots.

And if F is perfect, then we have seen that any irreducible polynomial is automatically separable. So, this, this just comes from our lecture on separable polynomials and so on. So, in this case again, so let me take my field K to be the field Fp to the n, let us say, for any n greater than or equal to 1, I will take K also to be the finite field with p to the n elements now. Then K over F is a Galois extension. Why is it a Galois extension?

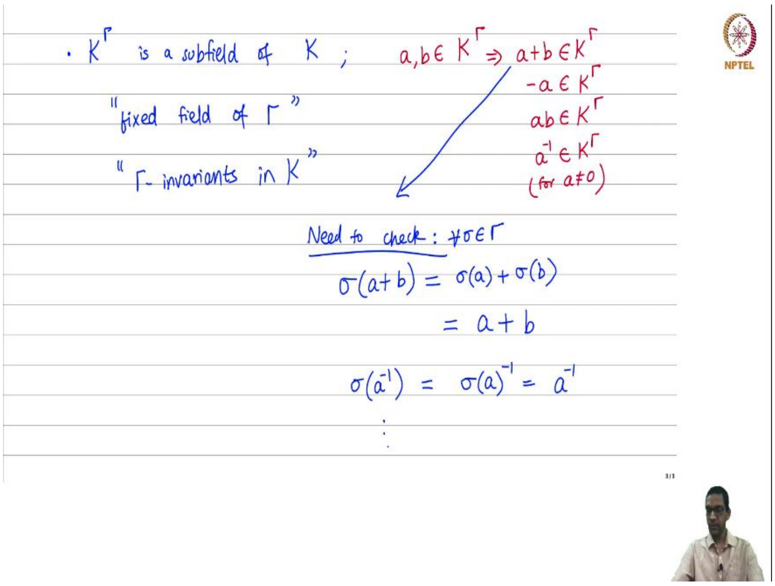
Well, as I just said, separability K is separable because F is a perfect field, and K is of course, in this case a finite extension of F. So, it is definitely an algebraic extinction. So, this is the automatic property. The normality is what we need to check. So, can we realize K as the splitting field of some polynomial, but recall, that is exactly how the finite fields were constructed. Recall from the lecture on finite fields, recall K, which is Fp to the n is nothing but the splitting field over, so and the base field here is Fp of the polynomial x to the p to the n minus x.

In fact, that is exactly how finite fields are constructed as splitting fields of this particular polynomial. So it is therefore normal. So, which implies this is a normal extension. What is the normal extension? K over F. And so, we have both properties. It is so I should have said here again, it is a separable extension. So, it has both properties, so it is Galois. Now, you know, we could talk about lots more examples, but for the moment, let is first look at some equivalent characterizations of Galois extensions for that I need a definition.

So, let me say if K is a field, let K be a field and look at the set AutK, which is the set of all field automorphisms of K. So, when I say Aut of K, I will always mean K is a field. So, I am thinking of this as a set of all maps from K to K, which are field automorphisms. So, field automorphisms of K. And so, I take a field and I take a subgroup.

So, let me call the subgroup as gamma, let gamma be a subgroup of the group of automorphisms, the automorphisms form a group as always. So, if I take gamma sub group, then the definition is the following. So, let K be field gamma be a sub group, then we write K superscript gamma, K gamma to be the set of all elements of K which are fixed by every element of gamma. So, sigma of a should be a, and this should be true for every sigma and gamma.

(Refer slide time: 07:37)



- K^{Γ} is a subfield of K ;

"fixed field of Γ"

"Γ- invariants in K"

$a, b \in K^{\Gamma} \Rightarrow a+b \in K^{\Gamma}$

$-a \in K^{\Gamma}$

$ab \in K^{\Gamma}$

$a^{-1} \in K^{\Gamma}$

(for $a \neq 0$)

Need to check : $\forall \sigma \in \Gamma$

$$\sigma(a+b) = \sigma(a) + \sigma(b)$$
$$= a + b$$

$$\sigma(a^{-1}) = \sigma(a)^{-1} = a^{-1}$$

$$\vdots$$

So, this K gamma then is, so let us check the following, simple property, K gamma is in fact a field. Well, it is actually a subfield of K. This is a subfield of the ambient field K. So, let us check this. So, what is it that we need to check? We need to check the properties of a subfield; what all do we need? Well, if you have two elements a and b, in the subset, when is the subset a subfield?

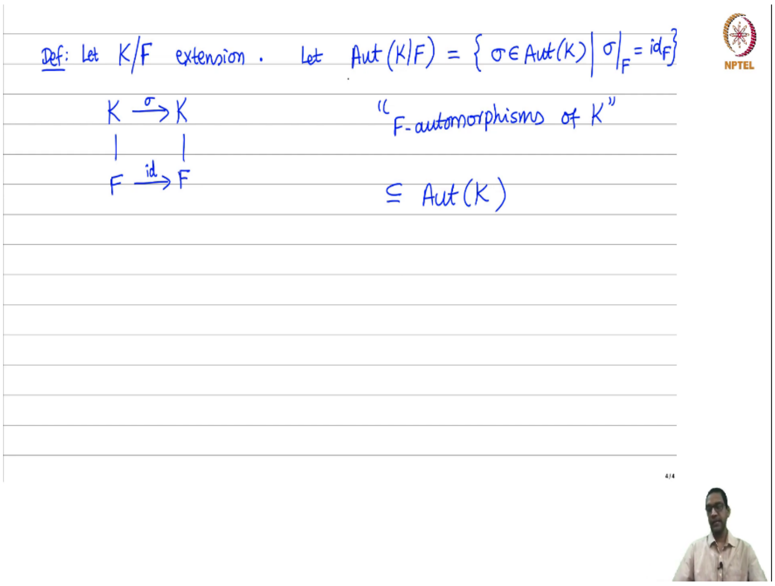
If you take two elements a and b, then you have to check that a plus b is in the subset. The algebraic, sorry the additive inverse minus a in the subset the product is there. And the multiplicative inverse is there. This is for a not equal to 0. So, it is closed under taking under addition, multiplication, and additive inverses and multiplicative inverses. Now I will just take a couple of these properties. They are all very easy. So how do you check this for instance.

So, to check that a plus b is in K gamma, you need to check the following whether every element of gamma fixes the element a plus b. So, you apply sigma to a plus b, sigma is an element of gamma. So, you need to check the following for every sigma and gamma, I need to check that sigma of a plus b equals a plus b, but sigma of a plus b is just sigma a plus sigma b, because sigma is an automorphism of the field and both a and b come from K gamma. Therefore, they are fixed by sigma. So that shows that a plus b is also fixed by sigma.

Similarly, let us check the last one, if I had to check that a inverse belongs to K gamma, I need to apply sigma to a inverse but again sigma is an automorphism. Therefore, we have the following properties, sigma a inverses sigma a the whole inverse, but sigma a is just a, because a belongs to K gamma. So, and so on, you can you can just check the other two properties similarly. So, this is a sub field and this is usually what is called the fixed field of gamma.

So, this is called the fixed field of this subgroup gamma or sometimes called the field of gamma invariants, the subfield of gamma invariance. So, you will see all these terms used. Now observe, we did not really use the fact that gamma is a subgroup for any of this. In fact, if you just take any subset, this will still work the same way, it will turn out to be a subfield. But we will almost always only be interested in the case when gamma is a subgroup. That is what is going to occur again and again when we study Galois theory.

(Refer slide time: 10:38)



<u>Def</u>: Let K/F extension. Let $Aut(K/F) = \{ \sigma \in Aut(K) \mid \sigma|_F = id_F \}$

$$\begin{tikzcd} K \arrow[r, "\sigma"] \arrow[d, dash] & K \arrow[d, dash] \\ F \arrow[r, "id"] & F \end{tikzcd}$$

"F-automorphisms of K"

$\subseteq Aut(K)$

Now, let me define another notion. So, I just talked about the group of automorphisms. Now, if K is an extension of F, so K over F, let K be an extension of F, then we define let Aut K over F denote the set of all field automorphisms of K, which has the following property that when you restrict them to F, it just gives you the identity map on F. So, this, in fact, came up earlier when we talked about normal extensions, and so on.

So, these are exactly the maps from K to K, the sigma's, which when you restrict to the base field, is just the identity on the base field. So, they fix the base field. So, this is called Aut K over F, sometimes called the group of F automorphisms of K. And observe that this is a subgroup of Aut K, Aut K is all field automorphisms, even ones which do not fix F pointwise. But when we think about extension fields having K and F, then the natural notion really is that of Aut K over F automorphisms, which fix the base field.