# Constant Field Extensions

Unit 28

Gil Cohen

January 19, 2025

# Constant field extensions

**Definition 1 (Constant field extensions)**

Let $E/K$ be a function field, and $L$ a field extension of $K$. Denote

$$F = LE.$$

Assuming $F/L$ is a function field we say that $F/L$ is a constant field extension of $E/K$.

It is not generally true that $F/L$ as defined above is a function field, even assuming $L/K$ is finite. But, as we will show, this is the case if $L/K$ is separable.

Recall that if $K$ is a finite field and $L/K$ is finite, then $L/K$ is separable. Indeed, finite fields are perfect.

# Overview

# Normal closure

**Definition 2**

Let $M/K$ be a field extension, and fix an algebraic closure $\bar{K}$ of $K$ containing $M$. The normal closure $\widehat{M}$ of $M/K$ is the smallest subfield of $\bar{K}$ containing $M$ that is normal over $K$.

Assuming $M/K$ is finite we can write

$$M = K(\alpha_1, \ldots, \alpha_n)$$

for some $\alpha_1, \ldots, \alpha_n \in M$.

Let $\sigma_1, \ldots, \sigma_k$ be the embeddings of $M$ in $\bar{K}$. Then,

$$\widehat{M} = K\left(\{\sigma_i(\alpha_j) \mid i \in [k],\ j \in [n]\}\right).$$

In particular, when $M/K$ is finite so is $\widehat{M}/K$.

# Normal closure

$$\widehat{\mathsf{M}} = \mathsf{K}\left(\{\sigma_i(\alpha_j) \mid i \in [k],\ j \in [n]\}\right).$$

Note further that if $\mathsf{M}/\mathsf{K}$ is separable then $\widehat{\mathsf{M}}/\mathsf{K}$ is Galois. Indeed,

$$\mathsf{M}/\mathsf{K} \text{ is separable} \quad \Longrightarrow \quad \widehat{\mathsf{M}}/\mathsf{K} \text{ is separable}$$

as we only adjoined K-conjugates of elements that are separable over K.

We conclude that $\widehat{\mathsf{M}}/\mathsf{K}$ is Galois as it is also normal. In this case we call $\widehat{\mathsf{M}}$ the Galois closure of $\mathsf{M}/\mathsf{K}$.

# Compositum of purely inseparable extensions

## Lemma 3

*Let* $\mathrm{M}/\mathrm{K}$ *be a field extension and*

$$\mathrm{K} \subseteq \mathrm{E}_1, \mathrm{E}_2 \subseteq \mathrm{M},$$

*where* $\mathrm{E}_1, \mathrm{E}_2$ *are purely inseparable over* $\mathrm{K}$*. Then,* $\mathrm{E}_1\mathrm{E}_2$ *is purely inseparable over* $\mathrm{K}$*.*

## Proof.

The set of purely inseparable elements in a field extension is an intermediate field. Indeed, recall that $a$ is purely inseparable over $\mathrm{K}$ iff $a^{p^{e_a}} \in \mathrm{K}$ for some integer $e_a \geq 0$. So, if $a, b$ are purely inseparable over $\mathrm{K}$ then, for $e = \max(e_a, e_b)$,

$$(a+b)^{p^e} = a^{p^e} + b^{p^e} \in \mathrm{F}.$$

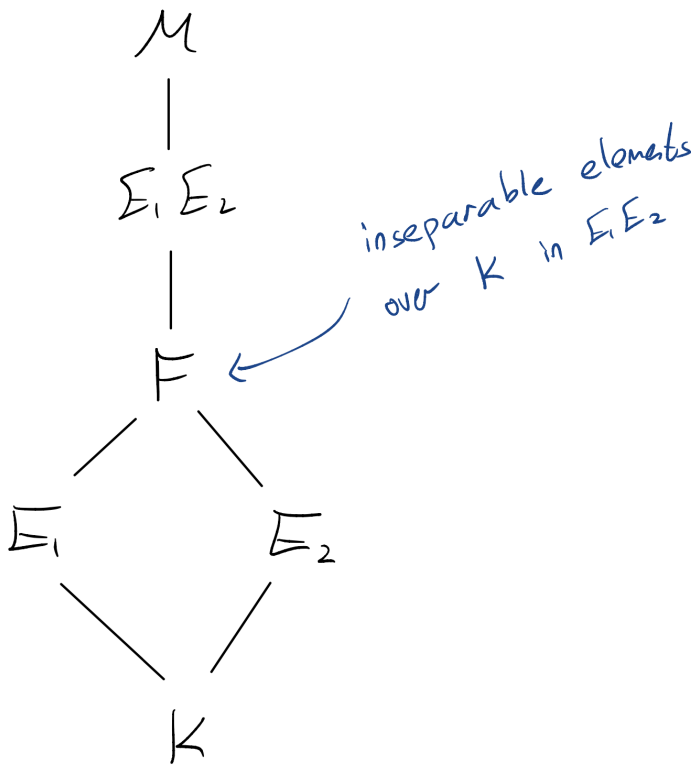
Same for multiplication and inverse.

# Compositum of purely inseparable extensions

**Proof.**

Let F be the field of inseparable elements in $E_1E_2$ over K. Clearly, $E_1 \subseteq F$ and $E_2 \subseteq F$.

But, $E_1E_2$ is the smallest field containing $E_1, E_2$ and so $E_1E_2 = F$. Namely, all elements in $E_1E_2$ are purely inseparable over K.



# The primitive element theorem

Recall

**Theorem 4 (The primitive element theorem)**

*Every finite separable extension is simple.*

Steinitz established the following generalization (note that finite fields are handled differently.)

**Theorem 5**

*Assume* $K$ *is an infinite field. A finite field extension* $M/K$ *is simple iff there are finitely many intermediate fields* $K \subseteq E \subseteq M$.

The latter implies the former as follows: Let $M/K$ be a finite separable extension, and consider the normal closure $\widehat{M}$ of $M/K$. Then, $\widehat{M}/K$ is a finite Galois extension. By Galois Theory, there is a finite number of intermediate fields in $\widehat{M}/K$.

# A variant of the primitive element theorem

**Lemma 6**

*Let* $\mathrm{M}/\mathrm{K}$ *be a finite field extension, and denote* $p = \operatorname{char} \mathrm{K}$*. Then,*

$$[\mathrm{M} : \mathrm{K}]_i = p \quad \Longrightarrow \quad \mathrm{M}/\mathrm{K} \text{ is simple.}$$

Note that the primitive element theorem concludes the same under the assumption $[\mathrm{M} : \mathrm{K}]_i = 1$.

**Proof.**

The assertion is trivial for a finite field K.

Using Steinitz' Theorem (Theorem 5), it suffices to prove that $\mathrm{M}/\mathrm{K}$ has finitely many intermediate fields.

# A variant of the primitive element theorem

**Proof.**

We first show that K has at most one purely inseparable extension

$$K \subsetneq E \subseteq M.$$

Indeed, assume two such extensions $E_1, E_2$ exist. Then,

$$[E_1 : K] = [E_1 : K]_i \geq p$$

(as it is a power of $p$ and $E_1 \neq K$). Thus, since $E_2 \neq E_1$,

$$[E_1E_2 : K] > p.$$

But by Lemma 3, $E_1E_2$ is a purely inseparable extension of K, and so

$$p = [M : K]_i \geq [E_1E_2 : K]_i = [E_1E_2 : K] > p,$$

which is a contradiction.

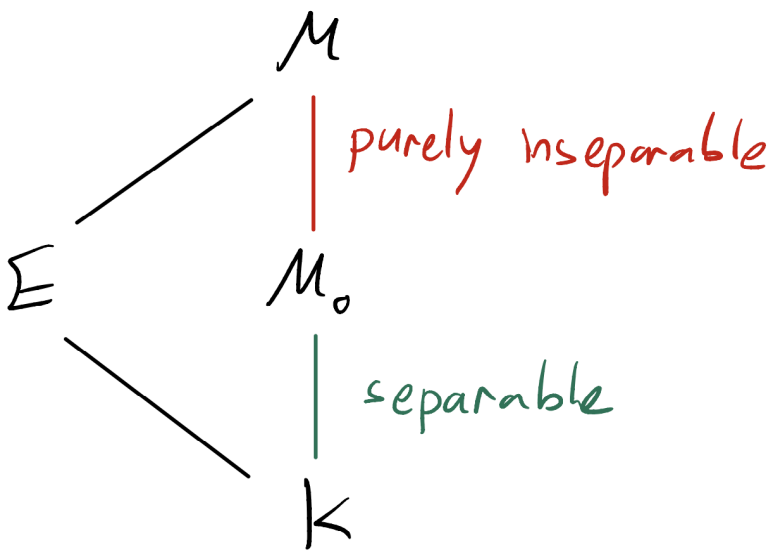
# A variant of the primitive element theorem

**Proof.**

Let $M_0$ be the separable closure of K in M.

Consider now an intermediate field $K \subseteq E \subseteq M$.

Further consider the separable closure of K in E.



# A variant of the primitive element theorem

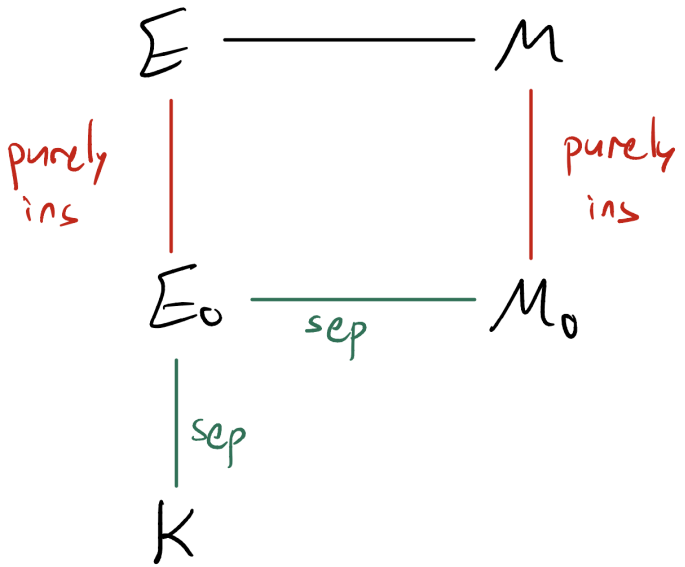
**Proof.**

We have that

$$[M : E_0]_i = \frac{[M : K]_i}{[E_0 : K]_i} = \frac{p}{1} = p.$$

Thus, $E_0$ has at most one purely inseparable extension in M (other than $E_0$), and so we can identify E with $E_0$.

But $M_0/K$ is finite and separable, and so it has only finitely many intermediate fields $E_0$, which completes the proof. □



# Overview

# Separable constant field extensions

**Theorem 7**

*Let* $E/K$ *be a function field and* $L/K$ *finite and separable. Then,* $LE/L$ *is a function field.*

**Proof.**

It suffices to prove that for every non-trivial finite extension $M/L$ (namely, $M \neq L$) it holds that $M \not\subseteq LE$.

Indeed, if $\alpha \in LE \setminus L$ is algebraic over $L$ then we can take

$$M = L(\alpha).$$

$M/L$ is finite and $M \neq L$. But, of course, $M \subseteq LE$, in contradiction.

Moreover, we can assume that $M/L$ has no intermediate fields as otherwise we can descend to one.

In particular, $M/L$ is either separable or purely inseparable.

# Separable constant field extensions

**Proof.**

In the second case, we may assume that

$$[\mathrm{M} : \mathrm{L}]_i = p.$$

Indeed,

$$[\mathrm{M} : \mathrm{L}] = [\mathrm{M} : \mathrm{L}]_i = p^e$$

for some $e \geq 1$. Take $\alpha \in \mathrm{M}$. If $[\mathrm{L}(\alpha) : \mathrm{L}] < p^e$ we can descend to $\mathrm{L}(\alpha)$. Otherwise, the minimal polynomial of $\alpha$ is

$$(T - \alpha)^{p^e} = T^{p^e} - \alpha^{p^e} \in \mathrm{L}[T].$$

Consider $\beta = \alpha^p$. Note that $(T - \beta)^{p^{e-1}} \in \mathrm{L}[T]$ vanishes at $\beta$ and so

$$[\mathrm{L}(\beta) : \mathrm{L}] \leq p^{e-1}.$$

Thus, we can take $\mathrm{L}(\beta)$ instead of M and proceed this way until we get a degree $p$ inseparable extension of L.

# Separable constant field extensions

**Proof.**

In any case,

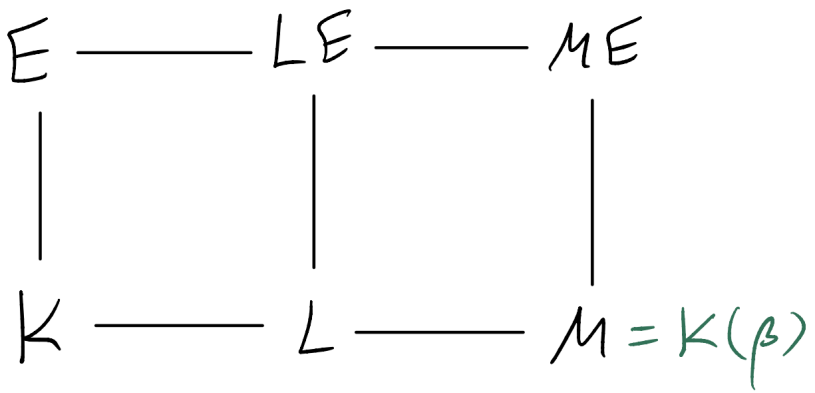
$$[M : L]_i \in \{1, p\},$$

and so, since L/K is separable,

$$[M : K]_i = [M : L]_i \cdot [L : K]_i \in \{1, p\}.$$

The primitive element theorem and its extension given by Lemma 6 imply that M/K is simple, namely, for some $\beta \in M$,

$$M = K(\beta).$$



# Separable constant field extensions

Recall a claim we proved when we talked about normal extensions.

## Claim 8

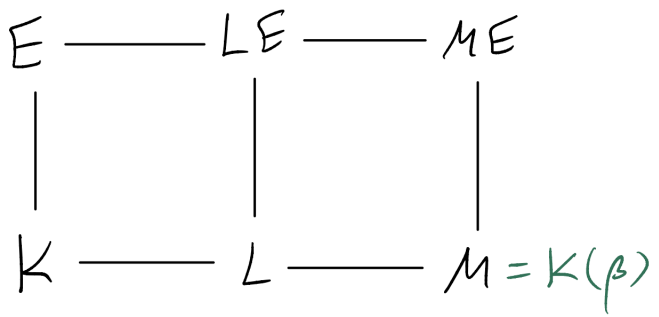
Let E/K be a field extension s.t. K is algebraically closed in E. Then,

$$f \in \mathrm{K}[x] \text{ is irreducible} \quad \Longrightarrow \quad f \text{ is irreducible in } \mathrm{E}[x].$$

With this we return to the proof of Theorem 7.

## Proof. (Proof of Theorem 7)

Let $f(x) \in \mathrm{K}[x]$ be the minimal polynomial of $\beta$ over K. Then, by Claim 8, $f(x)$ is also the minimal polynomial of $\beta$ over E.



# Separable constant field extensions

**Proof.**

Let $f(x) \in \mathsf{K}[x]$ be the minimal polynomial of $\beta$ over K. Then, $f(x)$ is also the minimal polynomial of $\beta$ over E. Thus,

$$\mathsf{ME} = \mathsf{EK}(\beta) = \mathsf{E}(\beta),$$

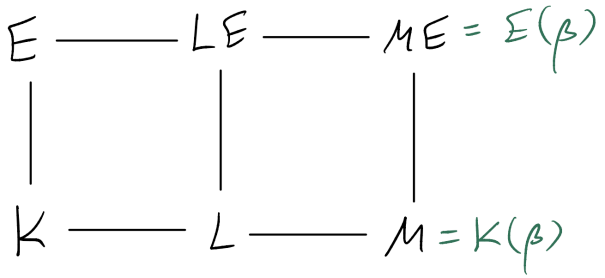
and

$$[\mathsf{ME} : \mathsf{E}] = \deg f = [\mathsf{M} : \mathsf{K}].$$

But, $\mathsf{M} \neq \mathsf{L}$ and so

$$[\mathsf{ME} : \mathsf{E}] = [\mathsf{M} : \mathsf{K}] > [\mathsf{L} : \mathsf{K}] \geq [\mathsf{LE} : \mathsf{E}].$$

Thus, $\mathsf{ME} \neq \mathsf{LE}$, and so $\mathsf{M} \not\subseteq \mathsf{LE}$, as desired.



# Separable constant field extensions

From this point on up until the last part of this unit,

$$F/L = LE/L$$

refers to a constant field extension of $E/K$ where $L$ is a finite separable extension of $K$.

# Separable constant field extensions

## Lemma 9

*Under the above,*

$$[F : E] = [L : K].$$

*Moreover,* $\forall \mathfrak{a} \in \mathcal{D}(E/K)$ *it holds that*

$$\deg_F \mathfrak{a} = \deg_E \mathfrak{a}.$$

## Proof.

Since $L/K$ is separable, $L = K(\alpha)$ for some $\alpha \in L$. Thus,

$$F = LE = E(\alpha).$$

Let $f(x) \in K[x]$ be the minimal polynomial of $\alpha$ over K. By Claim 8, $f(x)$ is irreducible over E, and so

$$[F : E] = [E(\alpha) : E] = \deg f = [K(\alpha) : K] = [L : K].$$

# Separable constant field extensions

**Proof.**

Per our assumption that $L/K$ is finite we have that $F/E$ is finite.

We proved in the previous unit that for a finite extension $F/E$,

$$\deg_F \mathfrak{a} = \frac{[F : E]}{[L : K]} \cdot \deg_E \mathfrak{a}.$$

Thus, in our case,

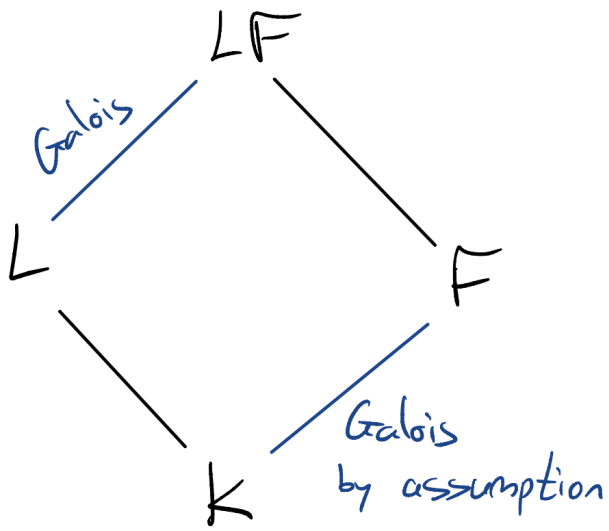
$$\deg_F \mathfrak{a} = \deg_E \mathfrak{a}.$$

# Overview

# A lemma from Galois Theory

## Lemma 10

*Let* $K \subseteq L, F$ *be fields s.t.* $F/K$ *is Galois. Then* $LF/L$ *is Galois.*




## Proof.

The separability of $LF/L$ is clear. Indeed, every element of $F$ is separable over $K$, let alone over $L$. Thus, every element of $LF$ is separable over $L$.

We turn to prove normality.

# A lemma from Galois Theory

**Proof.**

As for normality, recall the characterization of normal extensions as splitting fields.

As $F/K$ is normal, $F$ is the splitting field of

$$\{f_j(x) \in K[x]\}_{j \in J}.$$

Let $S_j \subseteq K$ be the roots of $f_j(x)$, and $S = \cup_j S_j$. Then, $F = K(S)$. But then

$$LF = LK(S) = L(S)$$

is the splitting field of

$$\{f_j(x) \in L[x]\}_{j \in J}.$$

Hence, $LF/L$ is normal. □

# Residue fields under constant field extensions

**Theorem 11**

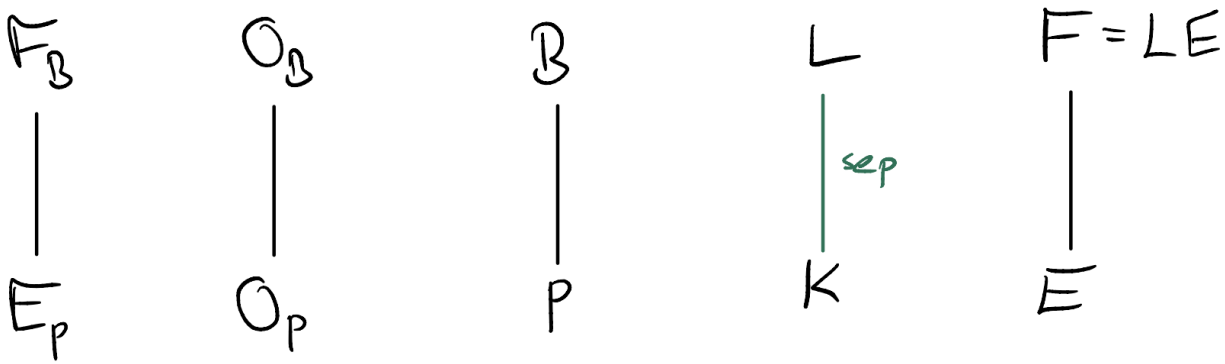
*Let $\mathfrak{P}$ be a prime divisor of $F/L$ lying over $\mathfrak{p}$ in $E/K$. Then,*

$$F_{\mathfrak{P}} = (LE)_{\mathfrak{P}} = LE_{\mathfrak{p}}.$$

**Proof.**

The $\supseteq$ direction follows as both $L, E_{\mathfrak{p}} \subseteq F_{\mathfrak{P}}$.

Take $\bar{z} \in F_{\mathfrak{P}}$. We want to show $\bar{z} \in LE_{\mathfrak{p}}$.



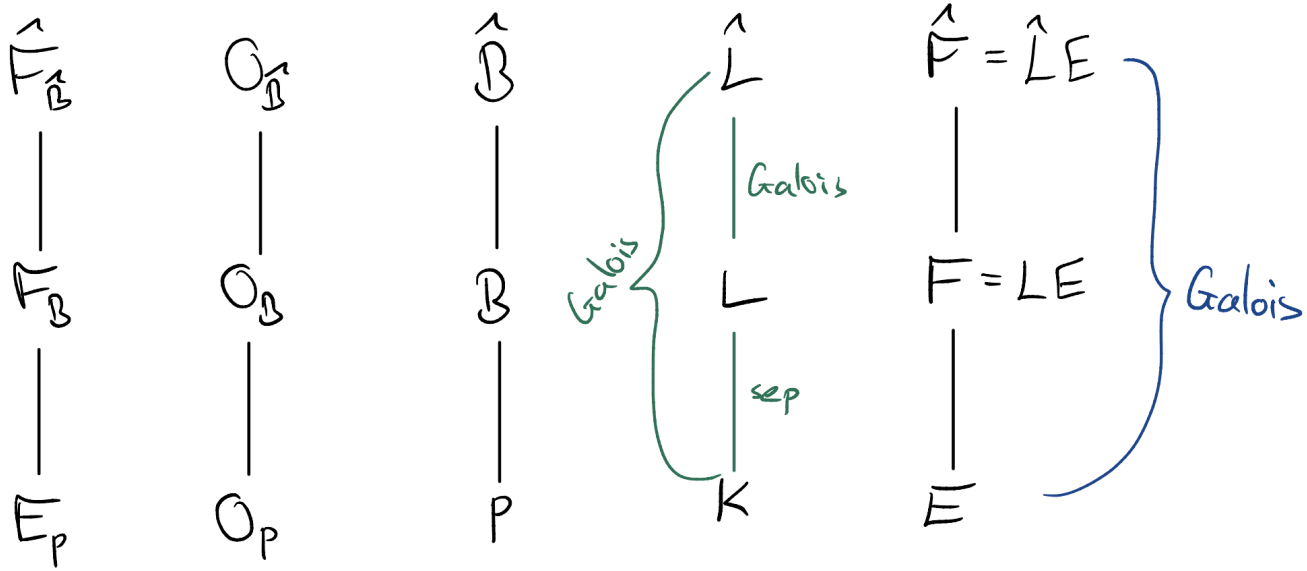
# Residue fields under constant field extensions

**Proof.**

Let $\widehat{L}$ be the normal closure of $L/K$. Recall that $\widehat{L}/K$ is not only normal but also separable since $L/K$ is separable. So $\widehat{L}/K$ is Galois.

By Lemma 10,

$$\widehat{L}/K \text{ is Galois} \quad \Longrightarrow \quad (\widehat{L}E)/(KE) = \widehat{F}/E \text{ is Galois.}$$



# Residue fields under constant field extensions

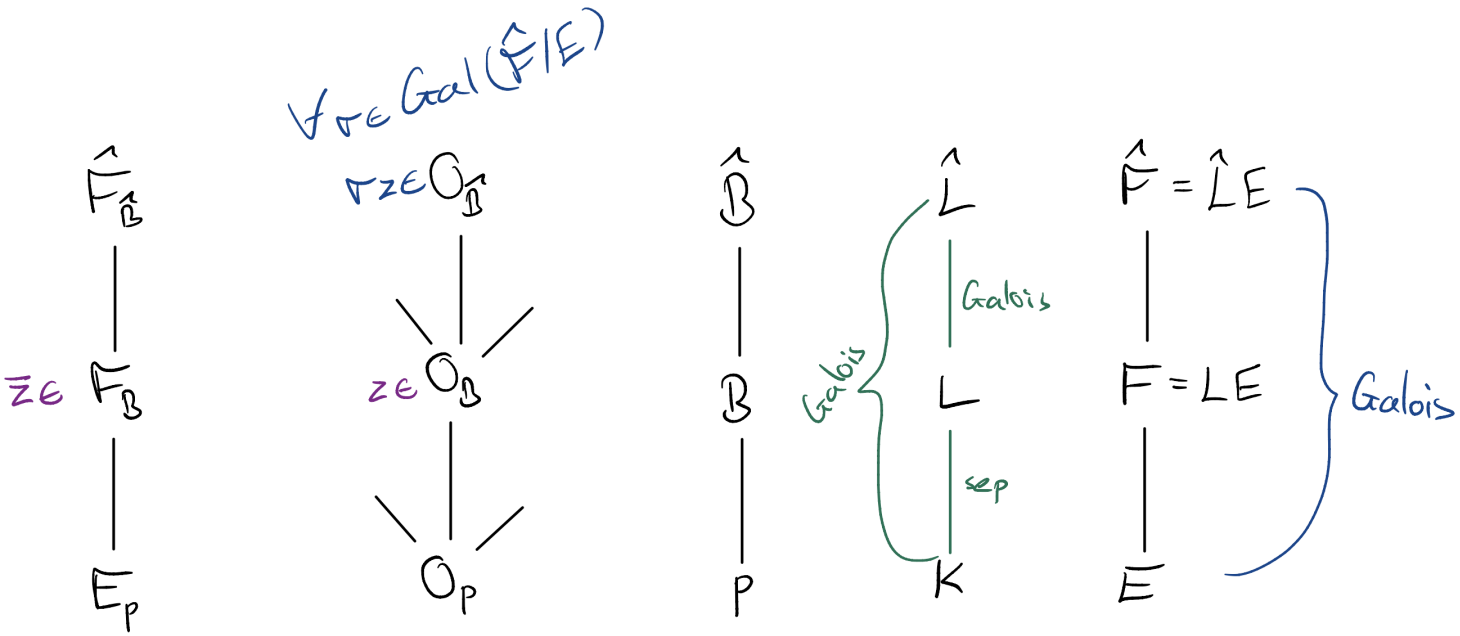
**Proof.**

Fix $\widehat{\mathfrak{P}}/\mathfrak{P}$. We turn to prove that $\bar{z}$ has a representative $z \in \mathcal{O}_{\mathfrak{P}}$ s.t.

$$\forall \sigma \in \mathrm{Gal}(\widehat{\mathrm{F}}/\mathrm{E}) \quad \sigma z \in \mathcal{O}_{\widehat{\mathfrak{P}}}.$$

Let $z' \in \mathcal{O}_{\mathfrak{P}}$ that represents $\bar{z}$. By the WAT, $\exists z \in \mathrm{F}$ s.t.

$$v_{\mathfrak{P}}(z - z') > 0 \quad \text{and} \quad \forall \mathfrak{P}'/\mathfrak{p} \in \mathbb{P}_{\mathrm{F}} \setminus \{\mathfrak{P}\} \quad v_{\mathfrak{P}'}(z) \geq 0.$$



# Residue fields under constant field extensions

**Proof.**

Let $z' \in \mathcal{O}_{\mathfrak{P}}$ that represents $\bar{z}$. By the WAT, $\exists z \in \mathsf{F}$ s.t.

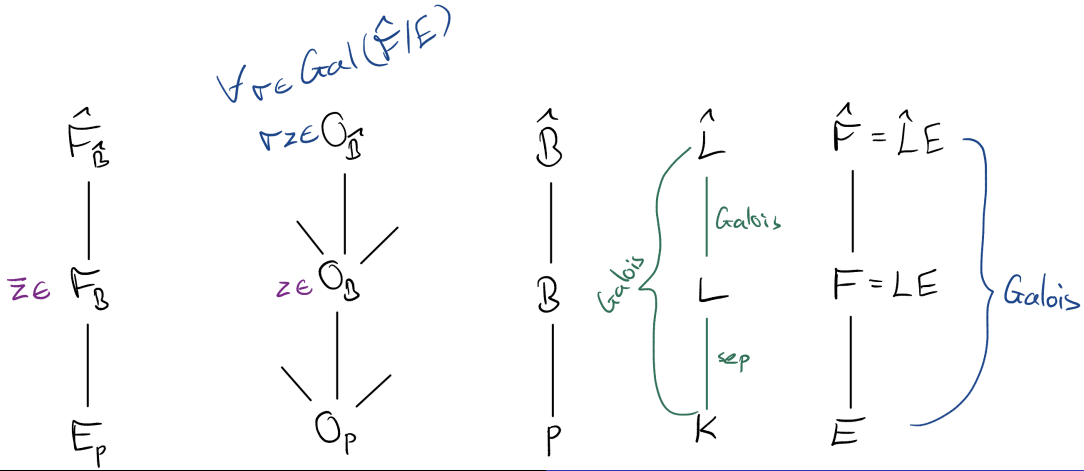
$$v_{\mathfrak{P}}(z - z') > 0 \quad \text{and} \quad \forall \mathfrak{P}'/\mathfrak{p} \in \mathbb{P}_{\mathsf{F}} \setminus \{\mathfrak{P}\} \quad v_{\mathfrak{P}'}(z) \geq 0.$$

Thus, $z$ is also a representative of $\bar{z}$. Moreover,

$$\forall \widehat{\mathfrak{P}}'/\mathfrak{p} \in \mathbb{P}_{\widehat{\mathsf{F}}} \qquad v_{\widehat{\mathfrak{P}}'}(z) \geq 0,$$

and so

$$\forall \sigma \in \mathrm{Gal}(\widehat{\mathsf{F}}/\mathsf{E}) \quad v_{\widehat{\mathfrak{P}}}(\sigma z) = v_{\sigma^{-1}\widehat{\mathfrak{P}}}(z) \geq 0 \quad \Longrightarrow \quad \sigma z \in \mathcal{O}_{\widehat{\mathfrak{P}}}.$$



# Residue fields under constant field extensions

**Proof.**

Denote $n = [\mathrm{L} : \mathrm{K}]$ and let $\alpha$ be a primitive element of $\mathrm{L}/\mathrm{K}$. Then,

$$1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$$

is a basis for $\mathrm{L}/\mathrm{K}$.

By Lemma 9,

$$[\mathrm{F} : \mathrm{E}]_s = [\mathrm{F} : \mathrm{E}] = [\mathrm{L} : \mathrm{K}] = n,$$

so there are precisely $n$ distinct embeddings of $\mathrm{F} \hookrightarrow \widehat{\mathrm{F}}$ over E which we denote by $\sigma_0, \ldots, \sigma_{n-1}$.

We have that

$$\mathrm{F} = \mathrm{LE} = \mathrm{E}(\alpha)$$

and so $1, \alpha, \ldots, \alpha^{n-1}$ is also a basis for $\mathrm{F}/\mathrm{E}$. Thus,

$$z = \sum_{j=0}^{n-1} x_j \alpha^j \qquad x_0, \ldots, x_{n-1} \in \mathrm{E}.$$

# Residue fields under constant field extensions

**Proof.**

$$z = \sum_{j=0}^{n-1} x_j \alpha^j \qquad x_0, \ldots, x_{n-1} \in \mathrm{E}.$$

Thus, for $i = 0, 1, \ldots, n-1$,

$$\sigma_i z = \sum_{j=0}^{n-1} x_j (\sigma_i \alpha)^j.$$

Thus we are looking at a linear system of $n$ equations in $n$ unknowns $x_0, \ldots, x_{n-1}$. The corresponding matrix $A$ satisfies

$$A_{i,j} = (\sigma_i \alpha)^j.$$

Observe that $A$ is a matrix over $\widehat{\mathrm{L}}$. Indeed, $\alpha \in \mathrm{L}$, $(\sigma_i)|_{\mathrm{K}} = \mathrm{id}_{\mathrm{K}}$ and so $(\sigma_i)|_{\mathrm{L}} : \mathrm{L} \to \widehat{\mathrm{L}}$. Thus, $\sigma_i \alpha \in \widehat{\mathrm{L}}$.

# Residue fields under constant field extensions

**Proof.**

$$A_{i,j} = (\sigma_i \alpha)^j \in \widehat{\mathsf{L}}.$$

Note that $A$ is a Vandermonde matrix and so

$$\det A = \prod_{j<\ell} (\sigma_\ell \alpha - \sigma_j \alpha).$$

Since L/K is separable, $\sigma_\ell \alpha \neq \sigma_j \alpha$ for $j \neq \ell$. Indeed, otherwise $\sigma_\ell$ and $\sigma_j$ will be equal on $\mathsf{K}(\alpha) = \mathsf{L}$.

Thus, $\det A \neq 0$ and so $A$ has an inverse $B$ over $\widehat{\mathsf{L}}$. So,

$$\forall 0 \leq j < n \quad x_j = \sum_{i=0}^{n-1} b_{ji} \sigma_i z \in \mathrm{Span}_{\widehat{\mathsf{L}}}(\sigma_0 z, \ldots, \sigma_{n-1} z).$$

But, recall that $x_j \in \mathsf{E}$.

# Residue fields under constant field extensions

**Proof.**

$$\forall j \quad x_j \in \mathsf{E} \cap \mathrm{Span}_{\widehat{\mathsf{L}}}(\sigma_0 z, \ldots, \sigma_{n-1} z).$$

**Recap.** recall that we took $\bar{z} \in \mathsf{F}_{\mathfrak{P}}$ and we wish to prove that $\bar{z} \in \mathsf{LE}_{\mathfrak{p}}$. We further took a representative $z \in \mathcal{O}_{\mathfrak{P}}$ s.t.

$$\sigma_0 z, \ldots, \sigma_{n-1} z \in \mathcal{O}_{\widehat{\mathfrak{P}}}.$$

But $\widehat{\mathsf{L}} \subseteq \mathcal{O}_{\widehat{\mathfrak{P}}}$ and so

$$x_0, \ldots, x_{n-1} \in \mathsf{E} \cap \mathcal{O}_{\widehat{\mathfrak{P}}} = \mathcal{O}_{\mathfrak{p}}.$$

Recall that $z = \sum_{j=0}^{n-1} x_j \alpha^j$ and so

$$\bar{z} = \sum_{j=0}^{n-1} \bar{x}_j \alpha^j \in \mathsf{E}_{\mathfrak{p}}\mathsf{L}.$$

# Overview

# Riemann-Roch spaces in separable constant field extensions

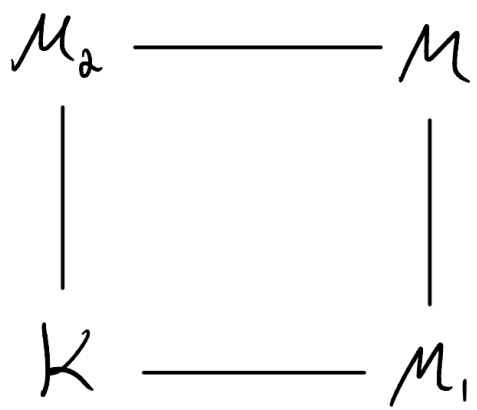
We recall the following basic fact from Galois Theory.

## Claim 12

Let $M_1, M_2$ be two field extensions of a field K, and assume M extend both $M_1$ and $M_2$.

Assume that every set $A_1 \subseteq M_1$ that is linearly independent over K is also linearly independent over $M_2$ (were we think of $A_1 \subseteq M$).

Then, every set $A_2 \subseteq M_2$ that is linearly independent over K is also linearly independent over $M_1$ (where we think of $A_2 \subseteq M$).



**Proof.**

Let $y_1, \ldots, y_n \in M_2$ be linearly independent over K. Take $\alpha_1, \ldots, \alpha_n \in M_1$ s.t.

$$\sum_{i=1}^{n} \alpha_i y_i = 0.$$

We wish to show that $\alpha_1 = \cdots = \alpha_n = 0$.

Let $x_1, \ldots, x_m \in M_1$ be a basis of

$$\mathrm{Span}_K(\alpha_1, \ldots, \alpha_n) \subseteq M_1.$$

Then, for every $i \in [n]$,

$$\alpha_i = \sum_{k=1}^{m} b_{ik} x_k,$$

with $\{b_{ik}\}_{i,k} \subseteq K$.

# Riemann-Roch spaces in separable constant field extensions

**Proof.**

$$\sum_{i=1}^{n} \alpha_i y_i = 0 \qquad \alpha_i = \sum_{k=1}^{m} b_{ik} x_k.$$

So,

$$0 = \sum_{i=1}^{n} \left( \sum_{k=1}^{m} b_{ik} x_k \right) y_i = \sum_{k=1}^{m} \left( \sum_{i=1}^{n} b_{ik} y_i \right) x_k.$$

Recall that Let $x_1, \ldots, x_m \in \mathrm{M}_1$ are linearly independent over K. Thus, per our assumption they are also linearly independent over $\mathrm{M}_2$.

Recall that $\{b_{ik}\}_{i,k} \subseteq \mathrm{K}$ and that $y_1, \ldots, y_n \subseteq \mathrm{M}_2$. Thus, for every $k \in [m]$,

$$\sum_{i=1}^{n} b_{ik} y_i = 0.$$

But $y_1, \ldots, y_n$ are linearly independent over K and so $b_{ik} = 0$, and so $\alpha_1 = \cdots = \alpha_n = 0$.

# Riemann-Roch spaces in separable constant field extensions

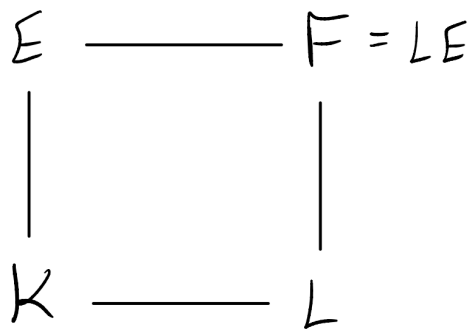
## Corollary 13

*Assume* F/L *is a constant field extension of* E/K *with* L/K *finite and separable.*

*If* $A \subseteq$ E *is linearly independent over* K *then (viewed as a subset of* F*)* $A$ *is linearly independent over* L*.*

## Proof.

By Claim 12, it suffices to prove that if $A \subseteq$ L is linearly independent over K then $A$ is also linearly independent over E.



**Proof.**

Since $L/K$ is separable and finite, $L = K(\alpha)$ for some $\alpha \in L$.

Denote $n = [L : K]$. Then $1, \alpha, \ldots, \alpha^{n-1}$ is a basis for $L/K$. Now,

$$F = EL = E(\alpha)$$

and, as we proved, the minimal polynomial $f$ of $\alpha$ over $K$ is also its minimal polynomial over $E$, and so

$$[F : E] = \deg f = [L : K] = n.$$

Thus, $1, \alpha, \ldots, \alpha^{n-1}$ is also a basis for $F/E$.

# Riemann-Roch spaces in separable constant field extensions

**Proof.**

Now take $\beta_1, \ldots, \beta_m \in \mathrm{L}$ that are linearly independent over K.

Complete this to a basis $\beta_1, \ldots, \beta_n$ of L/K.

Then, there is an invertible matrix $M$ over K that changes bases from $\beta_1, \ldots, \beta_n$ to $1, \alpha, \ldots, \alpha^{n-1}$.

$M$ is also invertible as a matrix over E and so, since $1, \alpha, \ldots, \alpha^{n-1}$ is a basis of F/E then $\beta_1, \ldots, \beta_n$ is also a basis of F/E.

In particular, $\beta_1, \ldots, \beta_m$ are linearly independent over E.

# Riemann-Roch spaces in separable constant field extensions

Recall that if $\mathfrak{a}$ is a divisor of E/K then $\mathrm{Con}(\mathfrak{a})$ is the "respective" divisor in F/L. Indeed, for a prime divisor $\mathfrak{p} \in \mathrm{E/L}$ we defined

$$\mathrm{Con}(\mathfrak{p}) = \sum_{\mathfrak{P}/\mathfrak{p}} e(\mathfrak{P}/\mathfrak{p})\mathfrak{P},$$

and $\mathrm{Con}(\mathfrak{a})$ was extended by linearity.

To keep notation simple, we denote $\mathrm{Con}(\mathfrak{a})$ by $\mathfrak{a}$ and infer from context. In particular, for a divisor $\mathfrak{a}$ of E/K, we use the convention

$$\mathcal{L}_{\mathrm{F}}(\mathfrak{a}) = \mathcal{L}_{\mathrm{F}}(\mathrm{Con}(\mathfrak{a})).$$

**Theorem 14**

*Let $\mathfrak{a}$ be a divisor of* E/K. *Then,*

$$\mathcal{L}_{\mathrm{F}}(\mathfrak{a}) = \mathrm{L}\mathcal{L}_{\mathrm{E}}(\mathfrak{a}) = \mathrm{Span}_{\mathrm{L}}(\mathcal{L}_{\mathrm{E}}(\mathfrak{a})).$$

**Proof.**

We have that

$$\begin{aligned}\mathcal{L}_{\mathsf{E}}(\mathfrak{a}) &= \{x \in \mathsf{E} \mid (x) + \mathfrak{a} \geq 0\} \\ &\subseteq \{x \in \mathsf{F} \mid (x) + \mathfrak{a} \geq 0\} = \mathcal{L}_{\mathsf{F}}(\mathfrak{a}).\end{aligned}$$

Note that the more elaborated way of writing this is as follows:

$$\begin{aligned}\mathcal{L}_{\mathsf{E}}(\mathfrak{a}) &= \{x \in \mathsf{E} \mid (x) + \mathfrak{a} \geq 0\} \\ &= \{x \in \mathsf{E} \mid \mathrm{Con}((x) + \mathfrak{a}) \geq 0\} \\ &= \{x \in \mathsf{E} \mid \mathrm{Con}(x) + \mathrm{Con}\,\mathfrak{a} \geq 0\} \\ &\subseteq \{y \in \mathsf{F} \mid (y) + \mathrm{Con}\,\mathfrak{a} \geq 0\} = \mathcal{L}_{\mathsf{F}}(\mathfrak{a}).\end{aligned}$$

Anyhow, $\mathcal{L}_{\mathsf{E}}(\mathfrak{a}) \subseteq \mathcal{L}_{\mathsf{F}}(\mathfrak{a})$. But $\mathcal{L}_{\mathsf{F}}(\mathfrak{a})$ is an L-vector space, and so

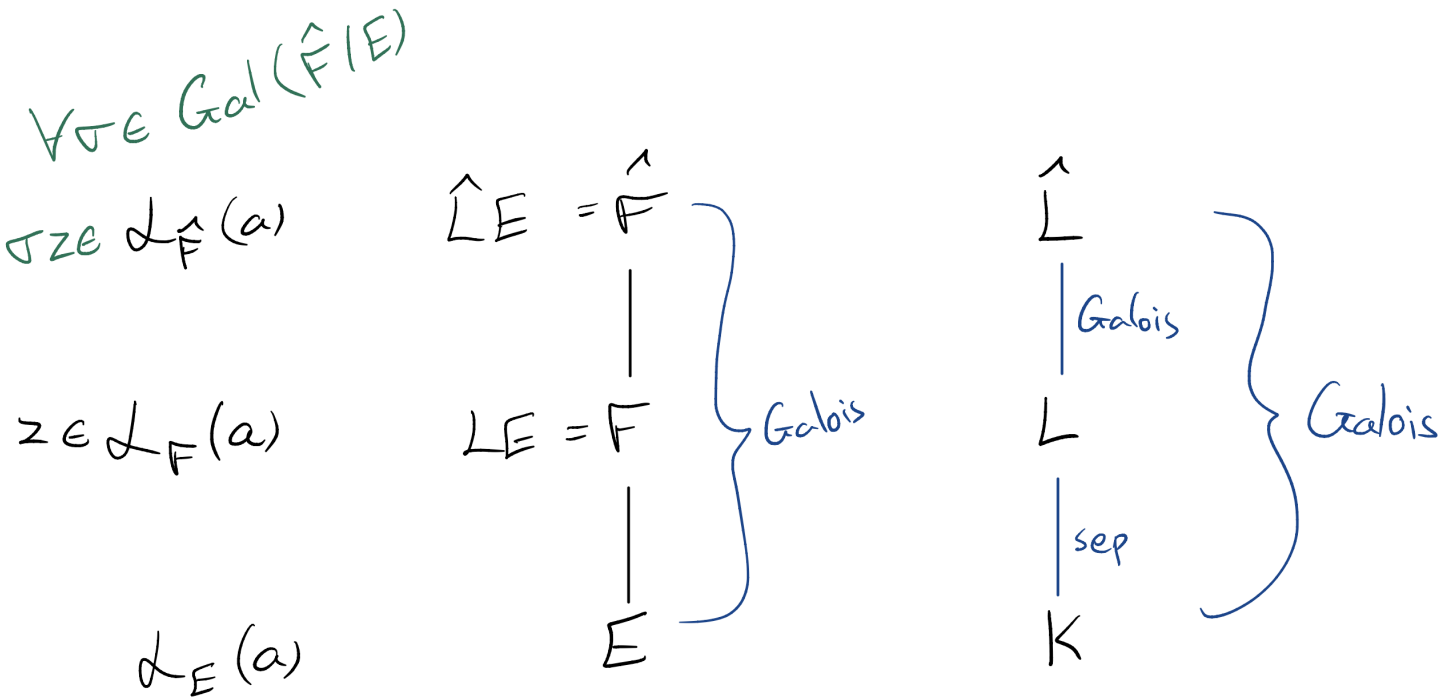
$$\mathsf{L}\mathcal{L}_{\mathsf{E}}(\mathfrak{a}) \subseteq \mathcal{L}_{\mathsf{F}}(\mathfrak{a}).$$

# Riemann-Roch spaces in separable constant field extensions

**Proof.**

We turn to prove the other direction, namely, $\mathcal{L}_F(\mathfrak{a}) \subseteq L\mathcal{L}_E(\mathfrak{a})$. To this end take $z \in \mathcal{L}_F(\mathfrak{a})$ and consider again the Galois closure $\widehat{L}$ of $L/K$. We turn to prove that

$$\forall \sigma \in \mathrm{Gal}(\widehat{F}/E) \quad \sigma z \in \mathcal{L}_{\widehat{F}}(\mathfrak{a}).$$



# Riemann-Roch spaces in separable constant field extensions

**Proof.**

As $z \in \mathcal{L}_F(\mathfrak{a})$,

$$(z) + \mathfrak{a} \geq 0$$

as divisors of $\widehat{F}/\widehat{L}$. Namely,

$$\forall \widehat{\mathfrak{P}} \in \mathbb{P}_{\widehat{F}/\widehat{L}} \quad v_{\widehat{\mathfrak{P}}}(z) + v_{\widehat{\mathfrak{P}}}(\mathfrak{a}) \geq 0.$$

In particular, for every such $\widehat{\mathfrak{P}}$,

$$v_{\sigma^{-1}\widehat{\mathfrak{P}}}(z) + v_{\sigma^{-1}\widehat{\mathfrak{P}}}(\mathfrak{a}) \geq 0.$$

But, $\widehat{F}/E$ is Galois, and so

$$\begin{aligned} v_{\widehat{\mathfrak{P}}}(\mathfrak{a}) &= e(\widehat{\mathfrak{P}}/\mathfrak{p}) v_{\mathfrak{p}}(\mathfrak{a}) \\ &= e(\sigma^{-1}\widehat{\mathfrak{P}}/\mathfrak{p}) v_{\mathfrak{p}}(\mathfrak{a}) \\ &= v_{\sigma^{-1}\widehat{\mathfrak{P}}}(\mathfrak{a}). \end{aligned}$$

# Riemann-Roch spaces in separable constant field extensions

**Proof.**

So far,

$$\forall \widehat{\mathfrak{P}} \quad v_{\sigma^{-1}\widehat{\mathfrak{P}}}(z) + v_{\sigma^{-1}\widehat{\mathfrak{P}}}(\mathfrak{a}) \geq 0.$$

and

$$v_{\widehat{\mathfrak{P}}}(\mathfrak{a}) = v_{\sigma^{-1}\widehat{\mathfrak{P}}}(\mathfrak{a}).$$

Thus,

$$\begin{aligned} v_{\widehat{\mathfrak{P}}}(\sigma z) + v_{\widehat{\mathfrak{P}}}(\mathfrak{a}) &= v_{\sigma^{-1}\widehat{\mathfrak{P}}}(z) + v_{\widehat{\mathfrak{P}}}(\mathfrak{a}) \\ &= v_{\sigma^{-1}\widehat{\mathfrak{P}}}(z) + v_{\sigma^{-1}\widehat{\mathfrak{P}}}(\mathfrak{a}) \geq 0. \end{aligned}$$

That is,

$$(\sigma z) + \mathfrak{a} \geq 0$$

as divisors of $\widehat{F}/\widehat{L}$, and so

$$\sigma z \in \mathcal{L}_{\widehat{F}}(\mathfrak{a}).$$

# Riemann-Roch spaces in separable constant field extensions

**Proof.**

By inspecting the proof of Theorem 11, we can write

$$z = \sum_{j=0}^{n-1} x_j \alpha^j$$

with

$$\begin{aligned} x_j &\in \mathsf{E} \cap \mathrm{Span}_{\widehat{\mathsf{L}}}\left(\left\{\sigma z \mid \sigma \in \mathrm{Gal}(\widehat{\mathsf{F}}/\mathsf{E})\right\}\right) \\ &\subseteq \mathsf{E} \cap \mathcal{L}_{\widehat{\mathsf{F}}}(\mathfrak{a}) \\ &= \mathcal{L}_{\mathsf{E}}(\mathfrak{a}). \end{aligned}$$

Therefore, as $\alpha \in \mathsf{L}$,

$$z \in \mathsf{L}\mathcal{L}_{\mathsf{E}}(\mathfrak{a}).$$

# Riemann-Roch spaces in separable constant field extensions

## Corollary 15

*With the above notations,*

$$\dim_F \mathfrak{a} = \dim_E \mathfrak{a}.$$

## Proof.

By Theorem 14,

$$\mathcal{L}_F(\mathfrak{a}) = L\mathcal{L}_E(\mathfrak{a}) = \mathrm{Span}_L(\mathcal{L}_E(\mathfrak{a})).$$

Now,

$$\dim_F \mathfrak{a} = \dim_L \mathcal{L}_F(\mathfrak{a}) = \dim_L \mathrm{Span}_L(\mathcal{L}_E(\mathfrak{a})),$$
$$\dim_E \mathfrak{a} = \dim_K \mathcal{L}_E(\mathfrak{a}).$$

Thus, we need to show that

$$\dim_K \mathcal{L}_E(\mathfrak{a}) = \dim_L \mathrm{Span}_L(\mathcal{L}_E(\mathfrak{a})).$$

# Riemann-Roch spaces in finite separable constant field extensions

**Proof.**

We need to show that

$$\dim_K \mathcal{L}_E(\mathfrak{a}) = \dim_L \mathrm{Span}_L(\mathcal{L}_E(\mathfrak{a})).$$

Corollary 13 states that if $A \subseteq E$ is linearly independent over K then (viewed as a subset of F) $A$ is linearly independent over L. Taking $A$ to be a basis of $\mathcal{L}_E(\mathfrak{a})$ (over K) yields the $\leq$ direction.

The $\geq$ direction readily follows since there is a basis for $\mathrm{Span}_L(\mathcal{L}_E(\mathfrak{a}))$ (over L) that is contained in $\mathcal{L}_E(\mathfrak{a})$. Such a basis certainly remains independent over K. □

# Overview

# The genus in finite separable constant field extensions

**Theorem 16**

*If* $\mathrm{F}/\mathrm{L}$ *is a finite separable constant field extension of* $\mathrm{E}/\mathrm{K}$ *and the respective genera are* $g_{\mathrm{F}}, g_{\mathrm{E}}$ *then*

$$g_{\mathrm{F}} = g_{\mathrm{E}}.$$

**Proof.**

Take $\mathfrak{p}$ a prime divisor of $\mathrm{E}/\mathrm{K}$ and $k \in \mathbb{N}$ large enough so that

$$\min(\deg_{\mathrm{E}} \mathfrak{a}, \deg_{\mathrm{F}} \mathfrak{a}) \geq k \geq \max(2g_{\mathrm{E}} - 2, 2g_{\mathrm{F}} - 2),$$

where $\mathfrak{a} = k\mathfrak{p}$. By Riemann-Roch,

$$\dim_{\mathrm{E}} \mathfrak{a} = \deg_{\mathrm{E}} \mathfrak{a} + 1 - g_{\mathrm{E}},$$
$$\dim_{\mathrm{F}} \mathfrak{a} = \deg_{\mathrm{F}} \mathfrak{a} + 1 - g_{\mathrm{F}}.$$

# The genus in finite separable constant field extensions

**Proof.**

$$\dim_E \mathfrak{a} = \deg_E \mathfrak{a} + 1 - g_E,$$
$$\dim_F \mathfrak{a} = \deg_F \mathfrak{a} + 1 - g_F.$$

Now, by Lemma 9,

$$\deg_E \mathfrak{a} = \deg_F \mathfrak{a},$$

and by Corollary 15,

$$\dim_E \mathfrak{a} = \dim_F \mathfrak{a}.$$

Therefore, $g_E = g_F$.

# Overview

# Characterization of constant field invariance

## Lemma 17

*Let* $E/K$ *a function field with* $K$ *a perfect field. Let* $L/K$ *be an algebraic extension (finite or infinite) and denote* $F = EL$*. Then,*

1. $L$ *is algebraically closed in* $F$*.*
2. *Any subset of* $E$ *that is* $K$*-linearly independent remains so over* $L$*.*
3. *For every* $x \in E \setminus K$*,*

$$[E : K(x)] = [F : L(x)].$$

## Proof.

We start with Item 1. Take $\gamma \in F$ that is algebraic over $L$. We wish to show $\gamma \in L$. As $F = EL$,

$$\exists \alpha_1, \ldots, \alpha_r \in L \qquad \gamma \in E(\alpha_1, \ldots, \alpha_r).$$

Now $K(\alpha_1, \ldots, \alpha_r)/K$ is finite hence separable, and so $\exists \alpha \in L$ s.t $K(\alpha_1, \ldots, \alpha_r) = K(\alpha)$.

# Characterization of constant field invariance

**Proof.**

Recall that $\gamma$ is algebraic over L and so it is algebraic over K. Indeed, consider the chain $L(\gamma)/L/K$. Thus, $K(\alpha,\gamma)/K$ is finite hence separable, and so

$$\exists \beta \in F \qquad K(\alpha,\gamma) = K(\beta).$$

Adjoining E we get that

$$E(\beta) = E(\alpha,\gamma) = E(\alpha),$$

where the last equality follows since $\gamma \in E(\alpha_1 \ldots, \alpha_r) = E(\alpha)$. Hence,

$$[K(\beta) : K] = \deg f_\beta = [E(\beta) : E] = [E(\alpha) : E] = \deg f_\alpha = [K(\alpha) : K].$$

Thus, $K(\alpha) = K(\beta)$ and so

$$\gamma \in K(\beta) = K(\alpha) \subseteq L.$$

# Characterization of constant field invariance

**Proof.**

We turn to prove Item 2. Take $y_1, \ldots, y_r \in \mathsf{E}$ that are linearly independent over $\mathsf{K}$. Assume that

$$\sum_{i=1}^{r} \gamma_i y_i = 0 \qquad \gamma_1, \ldots, \gamma_r \in \mathsf{L}.$$

We want to show that $\gamma_1 = \cdots = \gamma_r = 0$. Since $\mathsf{K}$ is perfect and $\mathsf{K}(\gamma_1, \ldots, \gamma_r)/\mathsf{K}$ is finite hence separable,

$$\exists \alpha \in \mathsf{L} \qquad \mathsf{K}(\gamma_1, \ldots, \gamma_r) = \mathsf{K}(\alpha).$$

For each $i \in [r]$, write

$$\gamma_i = \sum_{j=0}^{n-1} c_{i,j} \alpha^j \qquad c_{i,j} \in \mathsf{K},$$

where $n = [\mathsf{K}(\alpha) : \mathsf{K}] = \deg f_\alpha$.

# Characterization of constant field invariance

**Proof.**

$$\sum_{i=1}^{r} \gamma_i y_i = 0 \qquad \gamma_1, \ldots, \gamma_r \in \mathsf{L},$$

$$\gamma_i = \sum_{j=0}^{n-1} c_{i,j} \alpha^j \qquad c_{i,j} \in \mathsf{K}.$$

So

$$0 = \sum_{i=1}^{r} \left( \sum_{j=0}^{n-1} c_{i,j} \alpha^j \right) y_i = \sum_{j=0}^{n-1} \left( \sum_{i=1}^{r} c_{i,j} y_i \right) \alpha^j .$$

Recall that $1, \alpha, \ldots, \alpha^{n-1}$ are linearly independent over E since K is algebraically closed in E.

# Characterization of constant field invariance

**Proof.**

$$0 = \sum_{j=0}^{n-1} \left( \sum_{i=1}^{r} c_{i,j} y_i \right) \alpha^j .$$

$1, \alpha, \ldots, \alpha^{n-1}$ are linearly independent over E. Thus, for every $j$,

$$\sum_{i=1}^{r} c_{i,j} y_i = 0.$$

But $c_{i,j} \in \mathrm{K}$ and $y_1, \ldots, y_r$ are linearly independent over K and so $c_{i,j} = 0$, and so are the $\gamma_i$-s.

# Characterization of constant field invariance

**Proof.**

We turn to prove Item 3, namely,

$$\forall x \in \mathrm{E} \setminus \mathrm{K} \qquad [\mathrm{E} : \mathrm{K}(x)] = [\mathrm{F} : \mathrm{L}(x)].$$

The $\geq$ direction follows as we adjoin L to $\mathrm{E}/\mathrm{K}(x)$ and so the degree can only decrease.

As for the other direction, take $z_1, \ldots, z_s \in \mathrm{E}$ that are linearly independent over $\mathrm{K}(x)$. We wish to show these remain linearly independent over $\mathrm{L}(x)$. Otherwise,

$$\sum_{i=1}^{s} f_i(x) z_i = 0 \qquad f_i(x) \in \mathrm{L}[x],$$

where not all $f_i(x)$ zeros. Thus, $\{x^j z_i\}_{i,j}$ are linearly dependent over L, and so, by Item 2, also over K. Thus, $z_1, \ldots, z_s$ are linearly dependent over $\mathrm{K}(x)$ - a contradiction. □

# Characterization of constant field invariance

**Theorem 18**

*Let* $F/L$ *be a finite function field extension of* $E/K$*. Assume* $K$ *is a perfect field. Let* $\bar{K}$ *be an algebraic closure of* $K$ *(containing* $L$*). Then,*

$$[F : E] = [F\bar{K} : E\bar{K}] \cdot [L : K].$$

**Proof.**

First,

$$[F : E] = [F : EL] \cdot [EL : E].$$

Write $L = K(\alpha)$ and recall that $EL = E(\alpha)$ and that

$$[EL : E] = \deg f_\alpha = [L : K],$$

where $f_\alpha$ is the minimal polynomial of $\alpha$ over $K$.

So it remains to prove that

$$[F : EL] = [F\bar{K} : E\bar{K}].$$

# Characterization of constant field invariance

**Proof.**

We wish to prove that

$$[F : EL] = [F\bar{K} : E\bar{K}].$$

Fix $x \in E \setminus L$. By Lemma 17 (taking the constant field extension $E\bar{K}/\bar{K}$ of $EL/L$)

$$[EL : L(x)] = [E\bar{K} : \bar{K}(x)].$$

Similarly, by considering the constant field extension $F\bar{K}/\bar{K}$ of $F/L$,

$$[F : L(x)] = [F\bar{K} : \bar{K}(x)].$$

Thus,

$$[F : EL] = \frac{[F : L(x)]}{[EL : L(x)]} = \frac{[F\bar{K} : \bar{K}(x)]}{[E\bar{K} : \bar{K}(x)]} = [F\bar{K} : E\bar{K}].$$

# Characterization of constant field invariance

## Corollary 19

*Let* $F/L$ *be a finite function field extension of* $E/K$, *with* $K$ *perfect. Assume that* $F = E(y)$ *and that* $\varphi(T) \in E[T]$ *is the minimal polynomial of* $y$ *over* $E$. *Then, TFAE:*

1. $L = K$.
2. $\varphi(T)$ *is irreducible in* $E\bar{K}[T]$.

## Proof.

By Theorem 18,

$$[F : E] = [F\bar{K} : E\bar{K}] \cdot [L : K],$$

and so (1) is equivalent to

$$[F : E] = [F\bar{K} : E\bar{K}].$$

# Characterization of constant field invariance

**Proof.**

So far,

$$(1) \quad \Longleftrightarrow \quad [F : E] = [F\bar{K} : E\bar{K}].$$

But $F = E(y)$ and so

$$[F : E] = [E(y) : E],$$
$$[F\bar{K} : E\bar{K}] = [E\bar{K}(y) : E\bar{K}].$$

So

$$(1) \quad \Longleftrightarrow \quad [E(y) : E] = [E\bar{K}(y) : E\bar{K}].$$

The proof then follows since also

$$(2) \quad \Longleftrightarrow \quad [E(y) : E] = [E\bar{K}(y) : E\bar{K}].$$

# Characterization of constant field invariance

## Corollary 20

*Let* $F/K$ *be a finite extension of* $E/K$, *with* $K$ *perfect. Then, for every algebraic separable extension* $L/K$,

$$[F : E] = [FL : EL].$$

## Proof.

By Theorem 18,

$$[F : E] = [F\bar{K} : E\bar{K}] \cdot [K : K] = [F\bar{K} : E\bar{K}],$$

and (using that $\bar{K} = \bar{L}$),

$$[FL : EL] = [FL\bar{L} : EL\bar{L}] \cdot [L : L] = [F\bar{K} : E\bar{K}].$$

Therefore

$$[F : E] = [FL : EL].$$

# Characterization of constant field invariance

**Definition 21**

A polynomial $\varphi(T) \in \mathrm{K}(x)[T]$ is said to be absolutely irreducible if $\varphi(T)$ is irreducible in $\bar{\mathrm{K}}(x)[T]$.

**Theorem 22**

*Let* $\mathrm{F}/\mathrm{K}$ *be a field extension s.t.* $\mathrm{F} \neq \mathrm{K}$,

$$\mathrm{F} = \mathrm{K}(x, y),$$

*and* $[\mathrm{F} : \mathrm{K}(x)] < \infty$. *Assume* K *is perfect.*

*Let* $\varphi(T) \in \mathrm{K}(x)[T]$ *be the minimal polynomial of* $y$ *over* $\mathrm{K}(x)$. *TFAE:*

1. $\mathrm{F}/\mathrm{K}$ *is a function field;*
2. $\varphi(T)$ *is absolutely irreducible.*

# Characterization of constant field invariance

**Proof.**

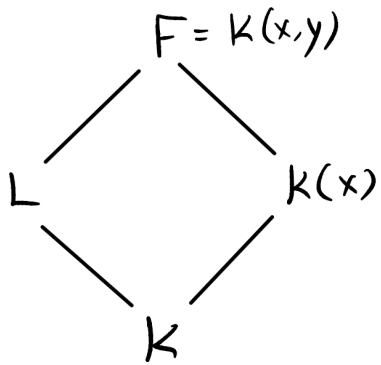
Per our assumption, $F \neq K$, $F = K(x, y)$ and $[F : K(x)] < \infty$. Thus, we need to prove that

$$K \text{ is algebraically closed in } F \iff \varphi(T) \text{ is absolutely irreducible.}$$

Let L be the algebraic closure of K in F. Note that F/L is a function field. Indeed, $F = L(x, y) \neq L$ (as F/K is of transcendence degree 1 and L/K is algebraic) and

$$[F : L(x)] \leq [F : K(x)] < \infty.$$

Moreover, L is algebraically closed in F (as the algebraic closure of K).



# Characterization of constant field invariance

**Proof.**

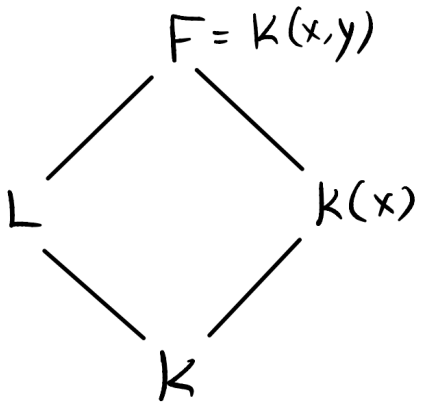
Consider the function field extension $F/L$ over $K(x)/K$. This is a function field extension $x$ is transcendental over $K$ and so

$$L \cap K(x) = K.$$

Since $[F : K(x)] < \infty$, $L/K$ is finite. Indeed,

$$[L : K] = [L(x) : K(x)] = \frac{[F : K(x)]}{[F : L(x)]}.$$

As $K$ is perfect we conclude that $L/K$ is separable.



# Characterization of constant field invariance

**Proof.**

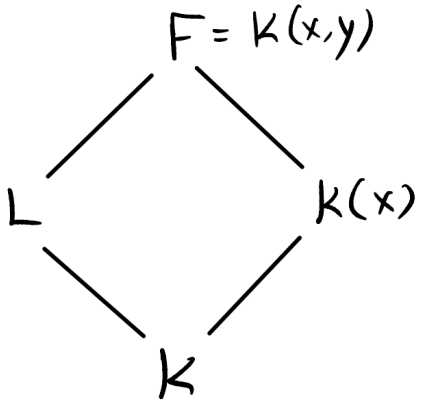
$L/K$ is finite and separable, and so by Corollary 19 (with $E = K(x)$),

$$L = K \iff \varphi(T) \text{ is irreducible in } K(x)\bar{K}[T].$$

The proof follows as

$$K(x)\bar{K} = \bar{K}(x).$$

□



# Example

Consider our running example $\mathrm{F} = \mathrm{K}(x, y)$ where K is a finite field and

$$y^2 = x^3 - x.$$

By Theorem 22, to prove that F/K is a function field, it suffices to prove that

$$T^2 - x^3 + x \in \bar{\mathrm{K}}(x)[T]$$

is irreducible.

If this is not the case then

$$T^2 - x^3 + x = (T + a(x))(T + b(x)),$$

with $a(x), b(x) \in \bar{\mathrm{K}}(x)$.

# Example

$$T^2 - x^3 + x = (T + a(x))(T + b(x)),$$

with $a(x), b(x) \in \bar{\mathrm{K}}(x)$.

But then $a(x) = -b(x)$ and

$$a(x)b(x) = x^3 - x,$$

and so

$$a(x)^2 = x - x^3$$

which forces $a(x) \in \bar{\mathrm{K}}[x]$ and then yields a contradiction by degree considerations.