Function Field Extensions and The Fundamental Equality

Unit 16

Gil Cohen

January 1, 2025

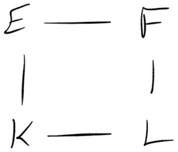
Overview

Function field extensions

Definition 1

Let F/L, E/K be function fields. We say that F/L is an extension of E/K if

- $E \subseteq F$
- $K \subseteq L$
- $L \cap E = K$.



We would like to study the relation between the prime divisors of F/L and those of E/K.

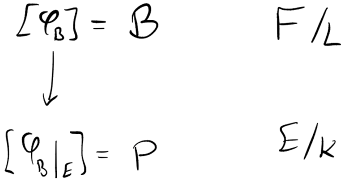
Prime divisors and places in function field extensions

Let $\mathfrak{P}$ be a prime divisor of F/L. Consider a corresponding place $\varphi_{\mathfrak{P}}$, and note that $(\varphi_{\mathfrak{P}})|_E$ is a place of E.

Assume further that $(\varphi_{\mathfrak{P}})|_E$ is a nontrivial place. Then, $(\varphi_{\mathfrak{P}})|_E$ is a place of E/K (as it is also trivial on $L \supseteq K$).

Denote the prime divisor of E/K that corresponds to $(\varphi_{\mathfrak{P}})|_E$ by $\mathfrak{p}$.

We say that $\mathfrak{P}$ lies over $\mathfrak{p}$, and that $\mathfrak{p}$ lies under $\mathfrak{P}$, and denote this by $\mathfrak{P}/\mathfrak{p}$.



Valuations in function field extensions

Consider the valuation $\upsilon_{\mathfrak{P}}$ of F/L that corresponds to $\mathfrak{P}$, and recall that

$$\upsilon_{\mathfrak{P}}(\mathsf{F}^{\times}) = \mathbb{Z}.$$

Now,

$$\upsilon_{\mathfrak{P}}(\mathsf{E}^{\times}) \leq \upsilon_{\mathfrak{P}}(\mathsf{F}^{\times})$$

and so either $\upsilon_{\mathfrak{P}}(\mathsf{E}^{\times}) = 0$ or $\upsilon_{\mathfrak{P}}(\mathsf{E}^{\times}) = e\mathbb{Z}$ for some integer $e \geq 1$.

The case $\upsilon_{\mathfrak{P}}(\mathsf{E}^{\times}) = 0$ cannot occur since, per our assumption, $\exists x \in \mathsf{E}^{\times}$ s.t. $\varphi_{\mathfrak{P}}(x) = \infty$ and so $\upsilon_{\mathfrak{P}}(x) < 0$.

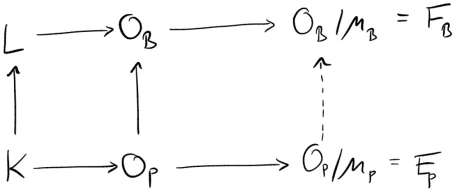
The valuation $\upsilon_{\mathfrak{p}}$ of E/K that corresponds to $\mathfrak{p}$ is then given by

$$\upsilon_{\mathfrak{p}} = \frac{1}{e} \cdot \upsilon_{\mathfrak{P}}|_{\mathsf{E}}.$$

The integer e is denoted by $e(\mathfrak{P}/p)$ or by $e_{\mathsf{F}/\mathsf{E}}(\mathfrak{P})$, or sometimes simply by $e(\mathfrak{P})$, and is called the ramification index of $\mathfrak{P}/\mathfrak{p}$.

Valuation rings, places, and residue fields in extensions

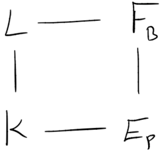
Let $\mathcal{O}_{\mathfrak{P}}$ be the valuation ring of $\mathfrak{P}$ in F, and denote its maximal ideal by $\mathfrak{m}_{\mathfrak{P}}$. Similarly define $\mathcal{O}_{\mathfrak{p}}$ and $\mathfrak{m}_{\mathfrak{p}}$, and recall that $\mathcal{O}_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{P}} \cap \mathsf{E}$ and $\mathfrak{m}_{\mathfrak{p}} = \mathfrak{m}_{\mathfrak{P}} \cap \mathsf{E}$.



Since $\mathfrak{m}_{\mathfrak{p}} = \mathfrak{m}_{\mathfrak{P}} \cap \mathsf{E} \subseteq \mathfrak{m}_{\mathfrak{P}}$ we have that the right "square" is commutative. As the left square is also commutative we have that the "big rectangle" is commutative.

Valuation rings, places, and residue fields in extensions

By the above discussion we know that the following diagram is commutative.



We call $[F_{\mathfrak{P}} : E_p]$ the relative degree of $\mathfrak{P}$ over $\mathfrak{p}$ and denote it by $f(\mathfrak{P}/\mathfrak{p})$. As the above diagram commutes, we have that

$$[L : K] \cdot \deg \mathfrak{P} = f(\mathfrak{P}/\mathfrak{p}) \cdot \deg \mathfrak{p},$$

where, potentially, some of the extensions above may be infinite.

Overview

A little lemma

Lemma 2

Let L/K *be a finite field extension, and* x *transcendental over* L*. Then,*

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

Left as an exercise.

Finiteness in extensions

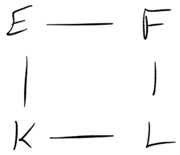
Lemma 3

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

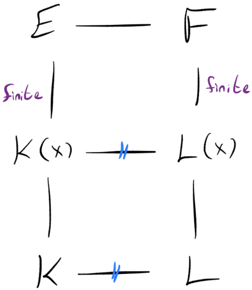
1. L/K *is finite*
2. F/E *is finite*
3. $F_{\mathfrak{P}}/E_{\mathfrak{p}}$ *is finite (that is,* $f(\mathfrak{P}/\mathfrak{p}) < \infty$*.)*

Proof.

We start with (1) $\iff$ (2). Take $x \in E \setminus K$. Then, $x \in F \setminus L$. Indeed, if $x \in L$ then $x \in E \cap L = K$ in contradiction.



Finiteness in extensions



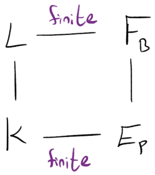
Proof.

Thus, x is transcendental over K and over L, and so

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

The proof of (1) $\iff$ (2) follows by the diagram.

Finiteness in extensions



Proof.

The proof of (1) $\iff$ (3) follows from the above diagram.

Remark. Lemma 3 also holds when we replace "finite" with "algebraic" everywhere.

Definition 4

A function field extension F/L of E/K is called finite if F/E is finite (equivalently, L/K is finite). It is called algebraic if F/E is algebraic (equivalently, L/K is algebraic).

Finiteness in extensions

Claim 5

Let F/E be an algebraic extension and φ a non-trivial place of F. Then, $\varphi|_E$ is a nontrivial place of E.

Proof.

We prove the contrapositive: assume $\varphi|_E$ is trivial and we will show φ is trivial.

Observe that it suffices to prove the above for finite extensions.

Indeed, having done so, take any $x \in \mathrm{F}$. As x is algebraic over E, $\mathrm{E}(x)/\mathrm{E}$ is a finite extension. Thus,

$$\begin{aligned} \varphi|_{\mathrm{E}} \text{ is trivial} \quad &\Longrightarrow \quad \varphi|_{\mathrm{E}(x)} \text{ is trivial} \\ &\Longrightarrow \quad \varphi(x) \neq \infty. \end{aligned}$$

As this holds for all $x \in \mathrm{F}$ we conclude that φ is trivial.

Finiteness in extensions

Proof.

So we assume F/E is finite. Let v be a valuation corresponding to φ. Then, $v(\mathsf{F}^\times)$ is an ordered group, and

$$0 = v(\mathsf{E}^\times) \leq v(\mathsf{F}^\times).$$

By a result we proved,

$$[v(\mathsf{F}^\times) : v(\mathsf{E}^\times)] \leq [\mathsf{F} : \mathsf{E}] < \infty,$$

and so $v(\mathsf{F}^\times)$ is finite.

However, we proved that the only finite ordered group is 0, and so φ is trivial. □

Overview

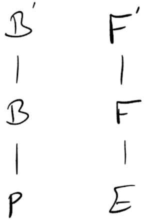
Ramification index and residual degrees in towers

The following lemma is left as an exercise.

Lemma 6

Let F/L *be an algebraic extension of* E/K*, and let* F′/L′ *be an algebraic extension of* F/L*. Let* $\mathfrak{p}$ *be a prime divisor of* E/K*,* $\mathfrak{P}$ *a prime divisor of* F/L *that lies above* $\mathfrak{p}$*, and let* $\mathfrak{P}'$ *be a prime divisor of* F′/L′ *lying over* $\mathfrak{P}$*. Then,*

$$f(\mathfrak{P}'/\mathfrak{p}) = f(\mathfrak{P}'/\mathfrak{P}) \cdot f(\mathfrak{P}/\mathfrak{p}),$$
$$e(\mathfrak{P}'/\mathfrak{p}) = e(\mathfrak{P}'/\mathfrak{P}) \cdot e(\mathfrak{P}/\mathfrak{p}).$$



Overview

Refining the notation

Let F/L be an algebraic extension of E/K, and take $x \in \mathsf{E}$. When considering a principle divisor (x) one should distinct between the divisor as a divisor of F/L and as a divisor of E/K.

To this end, we extend our notation and write $(x)_{\mathsf{F}}$ and $(x)_{\mathsf{E}}$, respectively. Similarly we have $(x)_{\mathsf{F},0}$ and $(x)_{\mathsf{E},0}$ for distinguishing between the zero divisors, and $(x)_{\mathsf{F},\infty}$ and $(x)_{\mathsf{E},\infty}$ for the pole divisors.

A useful lemma

Lemma 7

Let E/K *be a function field, and* $\mathfrak{p}$ *a prime divisor of* E/K*. Then,* $\exists x \in \mathrm{E} \setminus \mathrm{K}$ *and* $k \geq 1$ *integer s.t.*

$$(x)_{\mathrm{E},\infty} = k\mathfrak{p}.$$

The Lemma readily follows by the strong approximation theorem, however, for sports, we'll prove it based only on Riemann's Theorem.

Proof.

Denote the genus of E/K by g. By Riemann's Theorem, for n sufficiently large,

$$\dim n\mathfrak{p} \geq \deg n\mathfrak{p} + 1 - g \geq n + 1 - g \geq 2.$$

Thus, $\exists x \in \mathrm{E} \setminus \mathrm{K}$ s.t.

$$(x)_{\mathrm{E}} + n\mathfrak{p} \geq 0,$$

and so $(x)_{\mathrm{E},\infty} = k\mathfrak{p}$ for some $0 \leq k \leq n$.

As $x \notin \mathrm{K}$, x has a pole and so $k \geq 1$. □

Prime divisors above

Lemma 8

Let F/L *be an algebraic extension of* E/K *and let* $\mathfrak{p}$ *be a prime divisor of* E/K*. Then, the set of prime divisors of* F/L *lying over* $\mathfrak{p}$ *is finite and nonempty.*

Proof.

By Lemma 7, $\exists x \in \mathsf{E} \setminus \mathsf{K}$ s.t.

$$(x)_{\mathsf{E},\infty} = k\mathfrak{p}$$

for some $k \geq 1$. We now consider x as an element of F and write

$$(x)_{\mathsf{F},\infty} = \sum_{i=1}^{r} m_i \mathfrak{P}_i,$$

where $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ are distinct prime divisors of F/L, and $m_1, \ldots, m_r \geq 1$ are integers.

Prime divisors above

Proof.

Note that $r \geq 1$. Indeed, otherwise x has no pole as an element of F and so $x \in \mathsf{L}$. As $x \in \mathsf{E}$ we conclude that

$$x \in \mathsf{L} \cap \mathsf{E} = \mathsf{K}$$

which contradicts the fact that $x \in \mathsf{E} \setminus \mathsf{K}$.

We turn to prove that $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ are precisely the prime divisors of F/L that lie over $\mathfrak{p}$.

In one direction, if $\mathfrak{P}$ lies over $\mathfrak{p}$ then, as $\upsilon_{\mathfrak{p}}(x) < 0$, we have that

$$\upsilon_{\mathfrak{P}}(x) = e(\mathfrak{P}/\mathfrak{p})\upsilon_{\mathfrak{p}}(x) < 0.$$

Therefore, $\mathfrak{P} \in \{\mathfrak{P}_1, \ldots, \mathfrak{P}_r\}$.

Prime divisors above

Proof.

In the other direction, take $\mathfrak{P} = \mathfrak{P}_i$ for some i. Thus, $v_{\mathfrak{P}}(x) < 0$.

As we assume F/E is algebraic, Claim 5 guarantees the existence of a prime divisor $\mathfrak{q}$ of E/K lying under $\mathfrak{P}$.

We have that

$$v_{\mathfrak{q}}(x) = \frac{1}{e(\mathfrak{P}/\mathfrak{q})} v_{\mathfrak{P}}(x) < 0,$$

and so $\mathfrak{q}$ participates in $(x)_{E,\infty} = k\mathfrak{p}$, and so $\mathfrak{q} = \mathfrak{p}$. □

Overview

The fundamental equality

Theorem 9

Let F/L *be a finite extension of* E/K*. Let* $\mathfrak{p}$ *be a prime divisor of* E/K*. Then,*

$$[\mathrm{F} : \mathrm{E}] = \sum_{\mathfrak{P}/\mathfrak{p}} e(\mathfrak{P}/\mathfrak{p}) f(\mathfrak{P}/\mathfrak{p}).$$

Proof.

Let $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ be the prime divisors lying over $\mathfrak{p}$.

By inspecting the proof of the Lemma 8, we see that $\exists x \in \mathrm{E} \setminus \mathrm{K}$ s.t.

$$(x)_{\mathrm{E},\infty} = k\mathfrak{p},$$

$$(x)_{\mathrm{F},\infty} = \sum_{i=1}^{r} m_i \mathfrak{P}_i.$$

The fundamental equality

Proof.

$$(x)_{\mathsf{E},\infty} = k\mathfrak{p} \qquad (x)_{\mathsf{F},\infty} = \sum_{i=1}^{r} m_i \mathfrak{P}_i.$$

We proved that

$$[\mathsf{F} : \mathsf{L}(x)] = \deg(x)_{\mathsf{F},\infty} = \sum_{i=1}^{r} m_i \deg \mathfrak{P}_i.$$

Now,

$$m_i = -v_{\mathfrak{P}_i}(x) = -v_{\mathfrak{p}}(x) \cdot e(\mathfrak{P}_i/\mathfrak{p}) = k \cdot e(\mathfrak{P}_i/\mathfrak{p}).$$

Thus,

$$[\mathsf{F} : \mathsf{L}(x)] = k \sum_{i=1}^{r} e(\mathfrak{P}_i/\mathfrak{p}) \deg \mathfrak{P}_i$$

The fundamental equality

Proof.

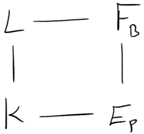
$$[\mathsf{F} : \mathsf{L}(x)] = k \sum_{i=1}^{r} e(\mathfrak{P}_i/\mathfrak{p}) \deg \mathfrak{P}_i$$

Since $[\mathsf{L} : \mathsf{K}] = [\mathsf{L}(x) : \mathsf{K}(x)]$ we have that

$$\begin{aligned}[\mathsf{F} : \mathsf{K}(x)] &= [\mathsf{F} : \mathsf{L}(x)][\mathsf{L}(x) : \mathsf{K}(x)] \\ &= k \sum_{i=1}^{r} e(\mathfrak{P}_i/\mathfrak{p})[\mathsf{L} : \mathsf{K}] \deg \mathfrak{P}_i.\end{aligned}$$

Recall that

$$[L : K] \deg \mathfrak{P} = f(\mathfrak{P}/\mathfrak{p}) \deg \mathfrak{p}.$$



The fundamental equality

Proof.

So far,

$$[\mathsf{F} : \mathsf{K}(x)] = k \sum_{i=1}^{r} e(\mathfrak{P}_i/\mathfrak{p})[\mathsf{L} : \mathsf{K}] \deg \mathfrak{P}_i,$$

$$[L : K] \deg \mathfrak{P} = f(\mathfrak{P}/\mathfrak{p}) \deg \mathfrak{p}.$$

Thus,

$$[\mathsf{F} : \mathsf{K}(x)] = k \deg \mathfrak{p} \sum_{i=1}^{r} e(\mathfrak{P}_i/\mathfrak{p}) f(\mathfrak{P}_i/\mathfrak{p}).$$

Recall that

$$[\mathsf{E} : \mathsf{K}(x)] = \deg(x)_{\mathsf{E},\infty} = k \deg \mathfrak{p},$$

and so

$$[\mathsf{F} : \mathsf{E}] = \frac{[\mathsf{F} : \mathsf{K}(x)]}{[\mathsf{E} : \mathsf{K}(x)]} = \sum_{i=1}^{r} e(\mathfrak{P}_i/\mathfrak{p}) f(\mathfrak{P}_i/\mathfrak{p}).$$

Overview

Example

We consider again our example F/K where $\mathsf{F} = \mathsf{K}(x, y)$ and

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

In the problem set you will show that $\mathsf{F}/\mathsf{K}(x)$ is indeed a function field when $\operatorname{char} \mathsf{K} \neq 2$.

We will use the fundamental equality to investigate prime divisors of F by consider the finite function field extension $\mathsf{F}/\mathsf{K}(x)$.

Example

Let $\mathfrak{P}$ be a prime divisor lying over $\mathfrak{p}_\infty$ of $\mathsf{K}(x)$. Then,

$$2v_{\mathfrak{P}}(y) = v_{\mathfrak{P}}(y^2) = v_{\mathfrak{P}}(x^3 - x).$$

But

$$v_{\mathfrak{P}}(x^3 - x) = e(\mathfrak{P}/\mathfrak{p}_\infty) \cdot v_\infty(x^3 - x) = -3 \cdot e(\mathfrak{P}/\mathfrak{p}_\infty).$$

$\implies e(\mathfrak{P}/\mathfrak{p}_\infty)$ is even. By the fundamental equality,

$$e(\mathfrak{P}/\mathfrak{p}_\infty) \leq [\mathsf{F} : \mathsf{K}(x)] = 2,$$

and so

$$e(\mathfrak{P}/\mathfrak{p}_\infty) = 2.$$

The fundamental equality then implies that $\mathfrak{P}$ is the only place lying over $\mathfrak{p}_\infty$ and that $f(\mathfrak{P}/\mathfrak{p}_\infty) = 1$.

Example

Let us explore prime divisors over $\mathfrak{p}_0$ of $\mathsf{K}(x)$. Let $\mathfrak{P}$ be a prime divisor lying over $\mathfrak{p}_0$. Then,

$$2v_{\mathfrak{P}}(y) = v_{\mathfrak{P}}(y^2) = v_{\mathfrak{P}}(x^3 - x) = e(\mathfrak{P}/\mathfrak{p}_0) \cdot v_0(x^3 - x) = 1 \cdot e(\mathfrak{P}/\mathfrak{p}_0).$$

By the fundamental equality,

$$e(\mathfrak{P}/\mathfrak{p}_0) \leq [\mathsf{F} : \mathsf{K}(x)] = 2.$$

Together with the above equation, we conclude

$$e(\mathfrak{P}/\mathfrak{p}_0) = 2.$$

The fundamental equality then implies that $\mathfrak{P}$ is the only place lying over $\mathfrak{p}_0$ and that $f(\mathfrak{P}/\mathfrak{p}_0) = 1$. We denote this place by $\mathfrak{P}_0$.

The same is the case for $\mathfrak{p}_1, \mathfrak{p}_{-1}$.

Example

What about places over $\mathfrak{p}_2$? Let's try to use the same trick: Let $\mathfrak{P}$ be a prime divisor lying over $\mathfrak{p}_2$. Then,

$$2v_{\mathfrak{P}}(y) = v_{\mathfrak{P}}(y^2) = v_{\mathfrak{P}}(x^3 - x) = e(\mathfrak{P}/\mathfrak{p}_2) \cdot v_2(x^3 - x) = e(\mathfrak{P}/\mathfrak{p}_2) \cdot 0,$$

and we cannot conclude anything about $e(\mathfrak{P}/\mathfrak{p}_2)$ in this way.

Example

We will later develop tools to study places over a place. In our case, it turns out that $e(\mathfrak{P}/\mathfrak{p}_2) = 1$ but there are two cases:

1. If $T^2 - 6 \in \mathsf{K}[T]$ is irreducible then there is a unique $\mathfrak{P}/\mathfrak{p}_2$, and $f(\mathfrak{P}/\mathfrak{p}_2) = 2$; otherwise
2. There are two distinct places over $\mathfrak{p}_2$ each with $f(\mathfrak{P}/\mathfrak{p}_2) = 1$.

So the arithmetic of the underlying field K plays a role. E.g., for $\mathsf{K} = \mathbb{F}_7$ we are in case (1) whereas for $\mathsf{K} = \mathbb{F}_5$ we are in case (2).

Example

There is nothing sacred about x. Consider now the function field extension $F/K(y)$.

Let's find the places $\mathfrak{P}'$ over $\mathfrak{q}_\infty$ of $K(y)$. Our starting point is

$$\upsilon_{\mathfrak{P}'}(y^2) = \upsilon_{\mathfrak{P}'}(x^3 - x).$$

Now,

$$\upsilon_{\mathfrak{P}'}(y^2) = e(\mathfrak{P}'/\mathfrak{q}_\infty) \cdot \upsilon_\infty(y^2) = -2e(\mathfrak{P}'/\mathfrak{q}_\infty) = -2e.$$

Thus,

$$\begin{aligned} -2e &= \upsilon_{\mathfrak{P}'}(x^3 - x) \\ &\geq \min(\upsilon_{\mathfrak{P}'}(x^3), \upsilon_{\mathfrak{P}'}(x)) \\ &= \min(3\upsilon_{\mathfrak{P}'}(x), \upsilon_{\mathfrak{P}'}(x)). \end{aligned}$$

Example

So far

$$\begin{aligned}-2e &= v_{\mathfrak{P}'}(x^3 - x) \\ &\geq \min(v_{\mathfrak{P}'}(x^3), v_{\mathfrak{P}'}(x)) \\ &= \min(3v_{\mathfrak{P}'}(x), v_{\mathfrak{P}'}(x)).\end{aligned}$$

But $-2e < 0$ and so $v_{\mathfrak{P}'}(x) < 0$, and so we have by the strict triangle inequality that

$$-2e = 3v_{\mathfrak{P}'}(x) \quad \Longrightarrow \quad e = e(\mathfrak{P}'/\mathfrak{q}_\infty) = 3,$$

where we used the fundamental equality.

Thus, there is a single prime divisor $\mathfrak{P}'/\mathfrak{q}_\infty$ with $e = 3, f = 1$.

Example

Since

$$-2e = 3v_{\mathfrak{P}'}(x)$$

and $e = 3$, we can conclude that

$$v_{\mathfrak{P}'}(x) = -2,$$

but recall that in general

$$[\mathrm{F} : \mathrm{K}(x)] = \deg(x)_\infty$$

but $[\mathrm{F} : \mathrm{K}(x)] = 2$ (recall $y^2 = x^3 - x$) and so

$$(x)_\infty = 2\mathfrak{P}'.$$

In fact,

$$(x) = 2\mathfrak{P}_0 - 2\mathfrak{P}'.$$

Exercise. Find (y).