Kummer Extensions

Unit 25

Gil Cohen

January 22, 2025

Overview

Cyclic extensions

Recall that a Galois extension F/K is called cyclic if $\mathrm{Gal}(F/K)$ is a cyclic group.

Lemma 1

Let F be a field of characteristic p. Let n coprime to p. Let $\zeta \in \bar{F}$ be an n-th primitive root of unity. Then, $F(\zeta)/F$ is a cyclic extension.

For the proof of Lemma 1 we recall the following lemma from Galois Theory.

Cyclic extensions

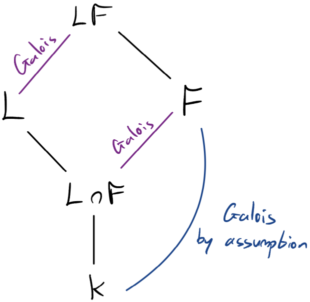
Lemma 2

Let K ⊆ L, F *be fields s.t.* F/K *is a finite Galois extension. Then* LF/L *is Galois and*

$$\mathrm{Gal}(LF/L) \cong \mathrm{Gal}(F/(L \cap F)).$$

In particular,

$$[LF : L] = [F : L \cap F].$$



Proof. (Proof of Lemma 2)

We first show that LF/L is Galois.

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.

As for normality, recall the characterization of normal extensions as splitting fields. Now, as F/K is normal, F is the splitting field of

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

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

$$\mathrm{LF} = \mathrm{F}(S)$$

is the splitting field of $\{f_j(x)\}_{j \in J}$ where we now think of $f_j(x) \in \mathrm{L}[x]$. Hence, LF/L is normal.

Cyclic extensions

Proof. (Proof of Lemma 2)

As F/K is finite and separable, $\mathsf{F} = \mathsf{K}(a)$ for some $a \in \mathsf{F}$.

Let $f(x) \in \mathsf{K}[x]$ be the minimal polynomial of a over K. Since F/K is Galois, $f(x)$ splits completely in F and all its roots are simple.

Let $g(x) \in \mathsf{L}[x]$ be the minimal polynomial of a over L. Since $\mathsf{K} \subseteq \mathsf{L}$ we have that $g(x) \mid f(x)$.

Thus the roots of $g(x)$ is a subset of the roots of $f(x)$ and so they are in F. This implies that $g(x) \in \mathsf{F}[x]$, and so

$$g(x) \in (\mathsf{L} \cap \mathsf{F})[x].$$

Now,

$$\mathsf{LF} = \mathsf{LK}(a) = \mathsf{L}(a),$$

and so

$$[\mathsf{LF} : \mathsf{L}] = [\mathsf{L}(a) : \mathsf{L}] = \deg g(x). \tag{1}$$

Proof. (Proof of Lemma 2)

$g(x)$ is irreducible over L and so certainly over $L \cap K$. Thus,

$$\deg g(x) = [(L \cap F)(a) : L \cap F].$$

As $a \in F$,

$$(L \cap F)(a) \subseteq F.$$

On the other hand,

$$F = K(a) \subseteq (L \cap F)(a),$$

and so $(L \cap F)(a) = F$. Hence,

$$\deg g(x) = [F : L \cap F].$$

With Equation (1), we get

$$[LF : L] = [F : L \cap F].$$

Cyclic extensions

Proof of Lemma 2.

Note that $F/(L \cap F)$ is Galois as F/K is Galois and $K \subseteq L \cap F$.

Consider the restriction homomorphism

$$\varphi : \mathrm{Gal}(LF/L) \to \mathrm{Gal}(F/(L \cap F))$$
$$\sigma \mapsto \sigma|_F$$

φ is a monomorphism. Indeed, assume that $\varphi(\sigma) = \sigma|_F = \mathrm{id}|_F$. As $\sigma|_L = \mathrm{id}|_L$ we have that $\sigma = \mathrm{id}_{LF}$.

As

$$|\mathrm{Gal}(LF/L)| = [LF : L] = [F : L \cap F] = |\mathrm{Gal}(F/(L \cap F))|$$

we have that φ is also onto. Thus,

$$\mathrm{Gal}(LF/L) \cong \mathrm{Gal}(F/(L \cap F)).$$

□

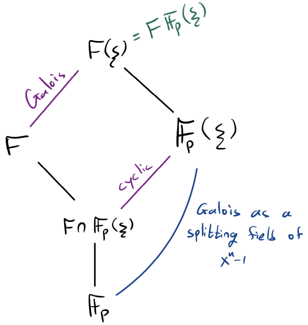
Cyclic extensions

Proof. (Proof of Lemma 1)

We have that

$$F(\zeta) = F\mathbb{F}_{\mathfrak{p}}(\zeta).$$

Now $\mathbb{F}_{\mathfrak{p}}(\zeta)/\mathbb{F}_p$ is Galois as it is the splitting field of the separable polynomial $x^n - 1$ over $\mathbb{F}_p$.



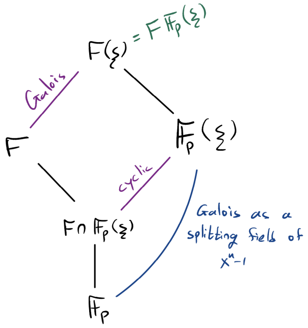
Cyclic extensions

Proof. (Proof of Lemma 1)

By Lemma 2, $F(\zeta)/F$ is Galois. Moreover,

$$\mathrm{Gal}(F(\zeta)/F) \cong \mathrm{Gal}(\mathbb{F}_p(\zeta)/(F \cap \mathbb{F}_p(\zeta))).$$

The RHS is a Galois extension of finite fields and as such it is cyclic. Thus, $F(\zeta)/F$ is cyclic.



Cyclic extensions

Theorem 3

Let E *be a field of characteristic* p*. Let* F/E *be a field extension of degree* n *which is coprime to* p*. Assume that* E *contains an* n*-th primitive root of unity. Then,*

$$\begin{aligned} \mathrm{F}/\mathrm{E} \textit{ is cyclic} \quad &\iff \quad \mathrm{F} = \mathrm{E}(a) \textit{ for some } a \in \mathrm{F} \textit{ s.t. } b \triangleq a^n \in \mathrm{E} \\ &\iff \quad \mathrm{F} \textit{ is the splitting field of } x^n - b \in \mathrm{E}[x]. \end{aligned}$$

Proof.

Assume that $\mathrm{F} = \mathrm{E}(a)$ for $b = a^n \in \mathrm{E}$. Then,

$$x^n - b = x^n - a^n = \prod_{\zeta \in \mu_n} (x - \zeta a),$$

where $\mu_n \subseteq \mathrm{E}$ is the set of n-th roots of unity.

Hence, F is the splitting field over E of the separable polynomial $x^n - b$. The separability follows as p and n are coprime.

Cyclic extensions

Proof.

Thus, F/E is Galois and an element $\sigma \in \mathrm{Gal}(F/E)$ is determined by its action on a. Note that $\sigma(a)$ is also a root of $x^n - b$. Indeed,

$$\sigma(a)^n = \sigma(a^n) = \sigma(b) = b.$$

Thus, $\sigma(a) \triangleq \sigma_\zeta(a) = \zeta a$ for some $\zeta \in \mu_n$.

As we assume that

$$[F : E] = [E(a) : E] = n,$$

$x^n - b$ is the minimal polynomial of a over E. Thus, $\{\zeta a \mid \zeta \in \mu_n\}$ are the E-conjugates of a.

For every conjugate ζa there is $\sigma_\zeta \in \mathrm{Gal}(F/E)$ s.t. $\sigma_\zeta(a) = \zeta a$. Thus,

$$\mathrm{Gal}(F/E) = \{\sigma_\zeta \mid \zeta \in \mu_n\}.$$

Cyclic extensions

Proof.

Moreover, the map

$$\begin{aligned}\mu_n &\to \mathrm{Gal}(\mathrm{F}/\mathrm{E}) = \{\sigma_\zeta \mid \zeta \in \mu_n\} \\ \zeta &\mapsto \sigma_\zeta\end{aligned}$$

is a group isomorphism as can be easily verified. Thus, F/E is cyclic.

In the other direction, assume F/E is cyclic and we ought to find $a \in \mathrm{F}$ s.t. $a^n \in \mathrm{E}$ and $\mathrm{F} = \mathrm{E}(a)$.

Let σ be a generator of the cyclic group Gal(F/E). It can be shown that the elements of Gal(F/E) are linearly independent over E (even over $\bar{\mathrm{E}}$). In particular,

$$\psi = \sum_{j=0}^{n-1} \zeta^j \sigma^j \neq 0,$$

where $\zeta \in \mu_n$ is an n-th primitive root of unity.

Cyclic extensions

Proof.

$$\psi = \sum_{j=0}^{n-1} \zeta^j \sigma^j \neq 0,$$

Let t be s.t. $\psi(t) \neq 0$, and let

$$a \triangleq \psi(t) = \sum_{j=0}^{n-1} \zeta^j \sigma^j(t).$$

We will show that $\mathsf{F} = \mathsf{E}(a)$ and that $a^n \in \mathsf{E}$.

As $\zeta \in \mathsf{E}$ we have that

$$\sigma(a) = \sum_{j=0}^{n-1} \zeta^j \sigma^{j+1}(t) = \zeta^{-1} \sum_{j=0}^{n-1} \zeta^{j+1} \sigma^{j+1}(t)$$

$$= \zeta^{-1} \sum_{j=0}^{n-1} \zeta^j \sigma^j(t) = \zeta^{-1} a.$$

Cyclic extensions

Proof.

So $\sigma(a) = \zeta^{-1}a$ and so the E-Galois conjugates of a are

$$\left\{a, \zeta^{-1}a, \ldots, (\zeta^{-1})^{n-1}a\right\} = \left\{a, \zeta a, \ldots, \zeta^{n-1}a\right\}.$$

Thus, the minimal polynomial of a over E is

$$f(x) = \prod_{j=0}^{n-1}(x - \zeta^j a) = x^n - a^n \in \mathrm{E}[x].$$

Thus, $\mathrm{F} = \mathrm{E}(a)$ and $a^n \in \mathrm{E}$. □

Overview

No ramification in constant field extensions

Lemma 4

Let L/K *be a finite separable extension. Let* E/K *be a function field and consider the constant field extension* F/L *with* $\mathsf{F} = \mathsf{EL}$*. Then, for every* $\mathfrak{P} \in \mathbb{P}(\mathsf{F})$ *lying over some* $\mathfrak{p} \in \mathbb{P}(\mathsf{E})$ *we have*

$$e(\mathfrak{P}/\mathfrak{p}) = 1.$$

Proof.

Let $\alpha \in \mathsf{L}$ be s.t. $\mathsf{L} = \mathsf{K}(\alpha)$. Let $\varphi(T) \in \mathsf{K}[T]$ be the minimal polynomial of α over K. Recall that φ is also the minimal polynomial of α over E.

As $\alpha \in \mathsf{L}$, α is integral over $\mathcal{O}_{\mathfrak{p}}$. Thus, by a result we proved in a previous unit,

$$0 \leq d(\mathfrak{P}/\mathfrak{p}) \leq v_{\mathfrak{P}}(\varphi'(\alpha)).$$

No ramification in constant field extensions

Proof.

$$0 \leq d(\mathfrak{P}/\mathfrak{p}) \leq \upsilon_{\mathfrak{P}}(\varphi'(\alpha)).$$

But $\alpha \in L$ and so $\varphi'(\alpha) \in L$. Moreover, $\varphi'(\alpha) \neq 0$ as α is separable. Hence,

$$\upsilon_{\mathfrak{P}}(\varphi'(\alpha)) = 0.$$

Thus, $d(\mathfrak{P}/\mathfrak{p}) = 0$ and Dedekind's Different Theorem yields

$$e(\mathfrak{P}/\mathfrak{p}) = 1.$$

□

Overview

Kummer Extensions

Definition 5 (Kummer extensions)

Let E/K be a function field where K contains a primitive n-th root of unity ζ. Assume that $n > 1$ is prime to $p = \text{char}(K)$.

Suppose that $u \in E$ is an element satisfying $u \neq w^d$ for all $w \in E$ and $d \mid n$, $d > 1$.

Let $F = E(y)$ with $y^n = u$. Such an extension F/E is called a Kummer extension.

With the notations of Definition 5, by Theorem 3, we have that

1. The polynomial $T^n - u$ is the minimal polynomial of y over E.
2. The extension F/E is Galois of degree n.
3. Gal(F/E) is cyclic and the automorphisms of F/E are given by $\sigma(y) = \zeta y$ for $\zeta \in K$ an n-th root of unity.

Kummer Extensions

With the notation of Definition 5 we have

Theorem 6 (Kummer extensions)

Let $\mathfrak{p} \in \mathbb{P}(\mathsf{E})$ *and* $\mathfrak{P} \in \mathbb{P}(\mathsf{F})$ *lying over* $\mathfrak{p}$. *Let*

$$r_{\mathfrak{p}} = \gcd(n, \upsilon_{\mathfrak{p}}(u)) > 0.$$

Then,

$$e(\mathfrak{P}/\mathfrak{p}) = \frac{n}{r_{\mathfrak{p}}}, \qquad d(\mathfrak{P}/\mathfrak{p}) = \frac{n}{r_{\mathfrak{p}}} - 1.$$

Moreover, if L *is the constant field of* F *and* $g_{\mathsf{F}}, g_{\mathsf{E}}$ *are the genera of* E/K *and* F/L, *respectively then*

$$g_{\mathsf{F}} = 1 + \frac{n}{[\mathsf{L} : \mathsf{K}]} \left(g_{\mathsf{E}} - 1 + \frac{1}{2} \sum_{\mathfrak{p} \in \mathbb{P}(\mathsf{E})} \left(1 - \frac{r_{\mathfrak{p}}}{n}\right) \deg \mathfrak{p} \right).$$

Kummer Extensions

Proof.

We start with the proof regarding $e(\mathfrak{P}/\mathfrak{p})$ and $d(\mathfrak{P}/\mathfrak{p})$ and split the proof to cases according to the value of $r_{\mathfrak{p}}$, starting with the case $r_{\mathfrak{p}} = 1$.

We have that

$$n \cdot \upsilon_{\mathfrak{P}}(y) = \upsilon_{\mathfrak{P}}(y^n) = \upsilon_{\mathfrak{P}}(u) = e(\mathfrak{P}/\mathfrak{p}) \cdot \upsilon_{\mathfrak{p}}(u).$$

By assumption,

$$r_{\mathfrak{p}} = \gcd(n, \upsilon_{\mathfrak{p}}(u)) = 1 \quad \Longrightarrow \quad n \mid e(\mathfrak{P}/\mathfrak{p}).$$

However, by the fundamental equality, $e(\mathfrak{P}/\mathfrak{p}) \leq n$ and so

$$e(\mathfrak{P}/\mathfrak{p}) = n = \frac{n}{r_{\mathfrak{p}}}$$

as desired.

Proof.

As $p = \mathrm{char}(\mathrm{K})$ is prime to $n = e(\mathfrak{P}/\mathfrak{p})$, Dedekind Different Theorem yields

$$d(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{p}) - 1$$

which concludes the proof of the case $r_{\mathfrak{p}} = 1$.

Consider now the case

$$r_{\mathfrak{p}} = \gcd(n, v_{\mathfrak{p}}(u)) = n.$$

We wish to prove that $d(\mathfrak{P}/\mathfrak{p}) = 0$ and $e(\mathfrak{P}/\mathfrak{p}) = 1$.

Note that $v_{\mathfrak{p}}(u) = \ell n$ for some $\ell \in \mathbb{Z}$.

Proof.

So far, $\upsilon_{\mathfrak{p}}(u) = \ell n$ for some $\ell \in \mathbb{Z}$.

Take $t \in E$ s.t. $\upsilon_{\mathfrak{p}}(t) = \ell$, and define

$$y_1 = t^{-1} y,$$
$$u_1 = t^{-n} u.$$

As $y^n = u$,

$$y_1^n = (t^{-1} y)^n = t^{-n} y^n = t^{-n} u = u_1.$$

Thus,

$$\begin{aligned} n \cdot \upsilon_{\mathfrak{P}}(y_1) = \upsilon_{\mathfrak{P}}(y_1^n) = v_{\mathfrak{P}}(u_1) = \upsilon_{\mathfrak{P}}(t^{-n} u) \\ = e(\mathfrak{P}/\mathfrak{p}) \cdot (\upsilon_{\mathfrak{p}}(u) - n \cdot \upsilon_{\mathfrak{p}}(t)) \\ = e(\mathfrak{P}/\mathfrak{p}) \cdot (\ell n - \ell n), \end{aligned}$$

and so

$$\upsilon_{\mathfrak{P}}(y_1) = \upsilon_{\mathfrak{p}}(u_1) = 0.$$

Kummer Extensions

Proof.

So far we have that $y_1^n = u_1$ and $\upsilon_{\mathfrak{P}}(y_1) = \upsilon_{\mathfrak{p}}(u_1) = 0$.

Observe that

$$\psi(T) = T^n - u_1 \in \mathrm{E}[T]$$

is the minimal polynomial of y_1 over E. Indeed, clearly, $\psi(y_1) = 0$. Moreover $y = ty_1$ and so if h is the minimal polynomial of y_1 over E then

$$g(T) = h(t^{-1}T) \in \mathrm{E}[T]$$

vanishes at y. Hence, a degree argument shows that ψ is indeed the minimal polynomial of y_1 over E.

We conclude that $y_1 \in \mathcal{O}'_{\mathfrak{p}}$ and that $\mathrm{F} = \mathrm{E}(y_1)$. As F/E is separable, by a theorem we proved,

$$d(\mathfrak{P}/\mathfrak{p}) \le \upsilon_{\mathfrak{P}}(\psi'(y_1)).$$

Proof.

So far we have that $d(\mathfrak{P}/\mathfrak{p}) \le \upsilon_{\mathfrak{P}}(\psi'(y_1))$. Now,

$$\psi'(T) = nT^{n-1}$$

and so

$$\psi'(y_1) = ny_1^{n-1},$$

so

$$\upsilon_{\mathfrak{P}}(\psi'(y_1)) = (n-1)\upsilon_{\mathfrak{P}}(y_1) = 0,$$

and so $d(\mathfrak{P}/\mathfrak{p}) = 0$.

Dedekind's Different Theorem then implies that $e(\mathfrak{P}/\mathfrak{p}) = 1$ and the proof for the case $r_{\mathfrak{p}} = n$ follows.

Kummer Extensions

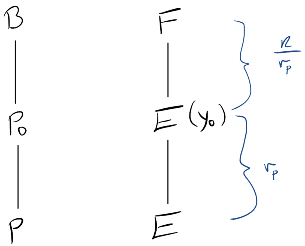
Proof.

We now consider the general case, reducing it to Case 1 and Case 2. To this end, define

$$y_0 = y^{n/r_{\mathfrak{p}}}$$

and consider the intermediate field $\mathrm{E}(y_0)$. Note that $T^{r_{\mathfrak{p}}} - u \in \mathrm{E}[T]$ is the minimal polynomial of y_0 over E and so $[\mathrm{E}(y_0) : \mathrm{E}] = r_{\mathfrak{p}}$. Thus, $[\mathrm{F} : \mathrm{E}(y_0)] = \frac{n}{r_{\mathfrak{p}}}$.

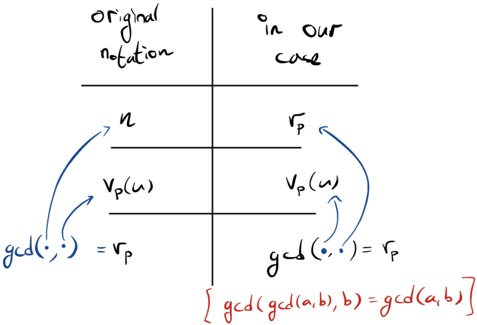
Let $\mathfrak{p}_0 = \mathfrak{P} \cap \mathrm{E}(y_0)$ be the prime divisor lying under $\mathfrak{P}$.



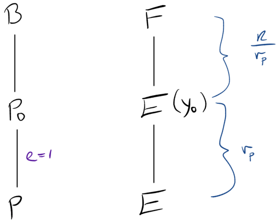
Proof.

We have that $y_0^{r_\mathfrak{p}} = u$ and $r_\mathfrak{p}$ is also the degree $[E(y_0) : E]$. Thus, we can apply Case 2 to $E(y_0)/E$ to conclude that

$$e(\mathfrak{p}_0/\mathfrak{p}) = 1.$$



Kummer Extensions



Proof.

Thus, so far we have concluded the information as depict in the figure.

Moving on to consider $\mathrm{F}/\mathrm{E}(y_0)$ we first note that

$$r_{\mathfrak{p}} \cdot v_{\mathfrak{p}_0}(y_0) = v_{\mathfrak{p}_0}(y_0^{r_{\mathfrak{p}}}) = v_{\mathfrak{p}_0}(u) = e(\mathfrak{p}_0/\mathfrak{p}) \cdot v_{\mathfrak{p}}(u) = v_{\mathfrak{p}}(u),$$

and so

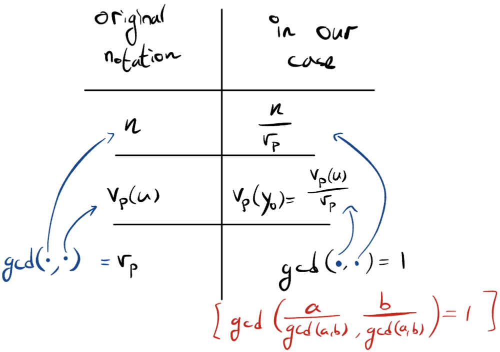
$$v_{\mathfrak{p}_0}(y_0) = \frac{v_{\mathfrak{p}}(u)}{r_{\mathfrak{p}}}.$$

Kummer Extensions

Proof.

We are thus reduced to Case 2 (see figure below). Thus,

$$e(\mathfrak{P}/\mathfrak{p}_0) = \frac{n}{r_{\mathfrak{p}}}.$$

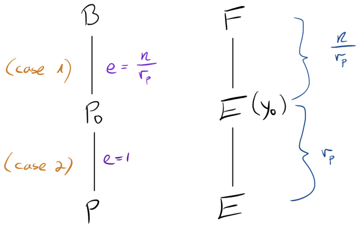


Kummer Extensions

Proof.

In summary we obtained the information depict in the figure. Thus,

$$e(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{p}_0)e(\mathfrak{p}_0/\mathfrak{p}) = \frac{n}{r_\mathfrak{p}}.$$



Proof.

We turn to calculate the genus. Recall that

$$\mathrm{Diff}(\mathrm{F}/E) = \sum_{\mathfrak{p} \in \mathbb{P}(\mathrm{E})} \sum_{\substack{\mathfrak{P}/\mathfrak{p} \\ \mathfrak{P} \in \mathbb{P}(\mathrm{F})}} d(\mathfrak{P}/\mathfrak{p})\mathfrak{P}.$$

Thus,

$$\begin{aligned} \deg \mathrm{Diff}(\mathrm{F}/\mathrm{E}) &= \sum_{\mathfrak{p} \in \mathbb{P}(\mathrm{E})} \sum_{\mathfrak{P}/\mathfrak{p}} d(\mathfrak{P}/\mathfrak{p}) \deg \mathfrak{P} \\ &= \sum_{\mathfrak{p} \in \mathbb{P}(\mathrm{E})} \left(\frac{n}{r_{\mathfrak{p}}} - 1 \right) \sum_{\mathfrak{P}/\mathfrak{p}} \deg \mathfrak{P}. \end{aligned}$$

Kummer Extensions

Proof.

As F/E is Galois, $e(\mathfrak{P}/\mathfrak{p})$ does not depend on $\mathfrak{P}$ but rather only on $\mathfrak{p}$, and so if we denote $e(\mathfrak{P}/\mathfrak{p})$ by $e(\mathfrak{p})$ we get

$$\sum_{\mathfrak{P}/\mathfrak{p}} \deg \mathfrak{P} = \frac{1}{e(\mathfrak{p})} \cdot \deg \left(\sum_{\mathfrak{P}/\mathfrak{p}} e(\mathfrak{P}/\mathfrak{p}) \mathfrak{P} \right)$$
$$= \frac{1}{e(\mathfrak{p})} \cdot \deg \mathrm{Con}_{\mathsf{F}/\mathsf{E}}(\mathfrak{p}).$$

In a previous unit we proved that

$$\deg \mathrm{Con}_{\mathsf{F}/\mathsf{E}}(\mathfrak{p}) = \frac{[\mathsf{F} : \mathsf{E}]}{[\mathsf{L} : \mathsf{K}]} \cdot \deg \mathfrak{p} = \frac{n}{[\mathsf{L} : \mathsf{K}]} \cdot \deg \mathfrak{p},$$

and so, using $e = n/r_{\mathfrak{p}}$, we get

$$\sum_{\mathfrak{P}/\mathfrak{p}} \deg \mathfrak{P} = \frac{1}{e(\mathfrak{p})} \cdot \frac{n}{[\mathsf{L} : \mathsf{K}]} \cdot \deg \mathfrak{p} = \frac{r_{\mathfrak{p}}}{[\mathsf{L} : \mathsf{K}]} \cdot \deg \mathfrak{p}.$$

Proof.

Recall we showed that

$$\deg \mathrm{Diff}(F/E) = \sum_{\mathfrak{p} \in \mathbb{P}(E)} \left(\frac{n}{r_{\mathfrak{p}}} - 1 \right) \sum_{\mathfrak{P}/\mathfrak{p}} \deg \mathfrak{P},$$

and that we took a detour to show that

$$\sum_{\mathfrak{P}/\mathfrak{p}} \deg \mathfrak{P} = \frac{r_{\mathfrak{p}}}{[L:K]} \cdot \deg \mathfrak{p}.$$

Combining these we get

$$\begin{aligned} \deg \mathrm{Diff}(F/E) &= \sum_{\mathfrak{p} \in \mathbb{P}(E)} \frac{n - r_{\mathfrak{p}}}{r_{\mathfrak{p}}} \cdot \frac{r_{\mathfrak{p}}}{[L:K]} \cdot \deg \mathfrak{p} \\ &= \frac{n}{[L:K]} \cdot \sum_{\mathfrak{p} \in \mathbb{P}(E)} \left(1 - \frac{r_{\mathfrak{p}}}{n} \right) \deg \mathfrak{p}. \end{aligned}$$

Kummer Extensions

Proof.

We summarize

$$\deg \mathrm{Diff}(F/E) = \frac{n}{[L:K]} \cdot \sum_{\mathfrak{p} \in \mathbb{P}(E)} \left(1 - \frac{r_{\mathfrak{p}}}{n}\right) \deg \mathfrak{p}.$$

Now, by the Hurwitz Genus Formula,

$$2g_F - 2 = \frac{[F:E]}{[L:K]}(2g_E - 2) + \deg \mathrm{Diff}(F/E),$$

and so

$$g_F = 1 + \frac{n}{[L:K]} \left(g_E - 1 + \frac{1}{2} \sum_{\mathfrak{p} \in \mathbb{P}(E)} \left(1 - \frac{r_{\mathfrak{p}}}{n}\right) \deg \mathfrak{p} \right).$$

Kummer Extensions

Corollary 7

Let E/K *be a function field and*

$$\mathsf{F} = \mathsf{E}(y) \quad \textit{where} \quad y^n = u \in \mathsf{E}.$$

Assume that n *and* $p = \mathrm{char}(\mathsf{K})$ *are coprime and that* K *contains a primitive* n*-th root of unity.*

Assume further that

$$\exists \mathfrak{q} \in \mathbb{P}(\mathsf{E}) \qquad \gcd(v_{\mathfrak{q}}(u), n) = 1.$$

Then,

1. K *is the full constant field of* F *(hence,* F/K *is a function field);*
2. F/E *is cyclic of degree* n*; and*
3. $$g_{\mathsf{F}} = 1 + n \cdot (g_{\mathsf{E}} - 1) + \frac{1}{2} \sum_{\mathfrak{p} \in \mathbb{P}(\mathsf{E})} (n - r_{\mathfrak{p}}) \deg \mathfrak{p}.$$

Proof.

We wish to apply Theorem 6. To this end, we first need to show that $u \neq w^d$ for all $w \in \mathrm{E}$ and $d \mid n$, $d > 1$.

Otherwise,

$$v_{\mathfrak{q}}(u) = v_{\mathfrak{q}}(w^d) = d \cdot v_{\mathfrak{q}}(w),$$

which would imply $d \mid v_{\mathfrak{q}}(u)$ in contradiction to $\gcd(v_{\mathfrak{q}}(u), n) = 1$.

The proof will follow by Theorem 6 once we establish that K is the full constant field of F.

Denote the algebraic closure of K in F by L and consider

$$\mathrm{E} \subseteq \mathrm{EL} \subseteq \mathrm{F}.$$

Kummer Extensions

Proof.

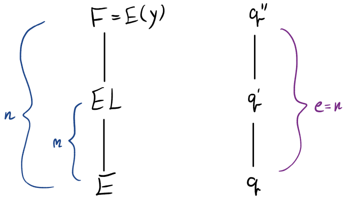
Let $\mathfrak{q}'' \in \mathbb{P}(F)$ be the prime divisor lying over $\mathfrak{q}$. Note that $\mathfrak{q}''$ is unique as

$$e(\mathfrak{q}''/\mathfrak{q}) = \frac{n}{r_{\mathfrak{q}}} = \frac{n}{\gcd(n, \upsilon_{\mathfrak{q}}(u))} = n.$$

Let EL/L be the constant field extension of E/K and let $\mathfrak{q}' \in \mathbb{P}(EL)$ be the prime divisor lying under $\mathfrak{q}''$. Recall that

$$e(\mathfrak{q}'/\mathfrak{q}) = 1$$

as no ramification occurs in constant field extensions per Lemma 4



Proof.

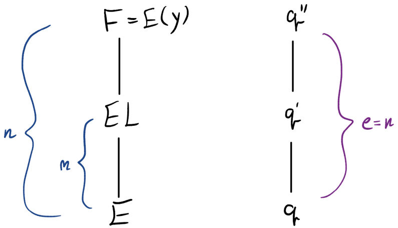
On the other hand, as $m \mid n$ and $\gcd(n, \upsilon_{\mathfrak{q}}(u)) = 1$ we have that

$$\gcd(m, \upsilon_{\mathfrak{q}}(u)) = 1.$$

Thus, by Theorem 6,

$$e(\mathfrak{q}'/\mathfrak{q}) = \frac{m}{\gcd(m, \upsilon_{\mathfrak{q}}(u))} = m.$$

Hence, $m = 1$ and so $\mathsf{L} \subseteq \mathsf{E}$ which implies $\mathsf{L} = \mathsf{K}$.



Remark

In the proof so far we never used the fact that K contains an *n*-th root of unity. Thus, all the results hold except that the extension may not be Galois.

Overview

Certain quadratic extensions

Lemma 8

Let $\mathsf{F} = \mathsf{K}(x, y)$ *where*

$$y^2 = f(x) \in \mathsf{K}[x]$$

and $f(x)$ *is irreducible of degree* m *over* K*. Assume that* K *has odd characteristic. Then,*

1. K *is the full constant field of* F*; and*
2. $\mathsf{F}/\mathsf{K}(x)$ *is cyclic of order* 2 *and has genus*

$$g = \begin{cases} \frac{m-1}{2} & \text{if } m \text{ is odd} \\ \frac{m-2}{2} & \text{otherwise.} \end{cases}$$

Proof.

Since $f(x)$ is irreducible over $\mathsf{K}[x]$, there is a prime divisor $\mathfrak{q}$ in $\mathsf{K}(x)$ that corresponds to $f(x)$, and

$$\upsilon_{\mathfrak{q}}(f(x)) = 1.$$

Certain quadratic extensions

Proof.

Further, $n = [\mathrm{F} : \mathrm{K}(x)] = 2$ and so

$$\gcd(\upsilon_{\mathfrak{q}}(f(x)), n) = \gcd(1, 2) = 1.$$

Moreover, -1 (the 2^{nd} root of unity) is in $\mathrm{K}(x)$ and so, as $\operatorname{char} \mathrm{K}$ is odd, Corollary 7 applies.

Corollary 7 implies that $\mathrm{F}/\mathrm{K}(x)$ is cyclic of order 2 and that K is the full constant field of F.

As for the genus, note that

$$r_{\mathfrak{q}} = \gcd(n, \upsilon_{\mathfrak{q}}(f(x))) = \gcd(2, 1) = 1,$$
$$r_{\infty} = \gcd(n, \upsilon_{\infty}(f(x))) = \gcd(2, -m) = \gcd(2, m).$$

For every other $\mathfrak{p} \in \mathbb{P}(\mathrm{K}(x))$, $\upsilon_{\mathfrak{p}}(f(x)) = 0$ and so

$$r_{\mathfrak{p}} = \gcd(n, \upsilon_{\mathfrak{p}}(f(x))) = \gcd(2, 0) = 2.$$

Certain quadratic extensions

Proof.

$$r_{\mathfrak{q}} = 1,$$
$$r_{\infty} = \gcd(2, m),$$
$$r_{\mathfrak{p}} = 2 \quad \text{otherwise.}$$

By Corollary 7,

$$g_{\mathsf{F}} = 1 + n \cdot (g_{\mathsf{K}(x)} - 1) + \frac{1}{2} \sum_{\mathfrak{p} \in \mathbb{P}(\mathsf{K}(x))} (n - r_{\mathfrak{p}}) \deg \mathfrak{p}.$$

As $n = 2$ and $g_{\mathsf{K}(x)} = 0$,

$$\begin{aligned} g_{\mathsf{F}} &= -1 + \frac{1}{2}\left(1 \cdot \deg \mathfrak{q} + (2 - \gcd(2, m)) \cdot \deg \mathfrak{p}_{\infty}\right) \\ &= -1 + \frac{1}{2}\left(m + (2 - \gcd(2, m))\right). \end{aligned}$$

Certain quadratic extensions

Proof.

Hence,

$$g_{\mathsf{F}} = -1 + \frac{1}{2}\left(m + (2 - \gcd(2, m))\right)$$
$$= \begin{cases} \frac{m-1}{2} & \text{if } m \text{ is odd} \\ \frac{m-2}{2} & \text{otherwise.} \end{cases}$$

□

Overview

Tame cyclic extensions of $\mathsf{K}(x)$

We now consider a function field $\mathsf{F} = \mathsf{K}(x, y)$ s.t.

$$y^n = a \cdot \prod_{i=1}^{s} p_i(x)^{n_i}$$

where

1. $a \neq 0$;
2. The $p_1(x), \ldots, p_s(x) \in \mathsf{K}[x]$ are distinct, irreducible and monic;
3. $n_1, \ldots, n_s \in \mathbb{Z} \setminus \{0\}$;
4. $\mathrm{char}(\mathsf{K}) \nmid n$; and
5. $\forall i \in [s]\ \ \gcd(n, n_i) = 1$.

Lemma 8 is the special case in which $n = 2$, $s = 1$, and $n_1 = 1$ (and also $a = 1$).

Tame cyclic extensions of K(x)

Theorem 9

1. *K is the full constant field of F and* $[F : \mathrm{K}(x)] = n$*;*
2. *If K contains an n-th root of unity,* $\mathrm{F}/\mathrm{K}(x)$ *is cyclic.*
3. *The prime divisors that correspond to* $p_1(x), \ldots, p_s(x)$ *in* $\mathbb{P}(\mathrm{K}(x))$ *are totally ramified in* $\mathrm{F}/\mathrm{K}(x)$*.*
4. *All prime divisors* $\mathfrak{q}$ *lying over* $\mathfrak{p}_\infty \in \mathbb{P}(\mathrm{K}(x))$ *have ramification index* $e(\mathfrak{q}/\mathfrak{p}_\infty) = \frac{n}{d}$ *where*
$$d = \gcd\left(n, \sum_{i=1}^{s} n_i \deg p_i(x)\right).$$
5. *No prime divisor other than those listed above ramify in* $\mathrm{F}/\mathrm{K}(x)$*.*
6. *Finally, the genus g of* $\mathrm{F}/\mathrm{K}(x)$ *is*
$$g = \frac{n-1}{2}\left(-1 + \sum_{i=1}^{s} \deg p_i(x)\right) - \frac{d-1}{2}.$$

Tame cyclic extensions of K(x)

Proof.

We wish to invoke Corollary 7 with

$$u = a \cdot \prod_{i=1}^{s} p_i(x)^{n_i}.$$

We first verify that the hypothesis of Corollary 7 holds.

1. By assumption, char(K) is prime to n;
2. For Item 2, a primitive n-th root of unity is contained in K(x); and
3. If $\mathfrak{p}_i \in \mathbb{P}(K(x))$ is the prime divisor corresponding to $p_i(x)$ then $\upsilon_{\mathfrak{p}_i}(u) = n_i$ which, per assumption, is co-prime to n.

Thus, we can apply Corollary 7 to conclude that

1. K is the full constant field of F;
2. $[F : K(x)] = n$;
3. Assume K contains a primitive n-th root of unity, $F/K(x)$ is cyclic.

Proof.

Now,

$$r_{\mathfrak{p}_i} = \gcd(n, \upsilon_{\mathfrak{p}_i}(u)) = \gcd(n, n_i) = 1,$$

$$r_{\mathfrak{p}_\infty} = \gcd(n, \upsilon_\infty(u)) = \gcd\left(n, \sum_{i=1}^{s} -n_i \deg p_i(x)\right) = d,$$

and for every other prime divisor $\mathfrak{p} \in \mathbb{P}(\mathrm{K}(x))$,

$$r_{\mathfrak{p}} = \gcd(n, \upsilon_{\mathfrak{p}}(u)) = \gcd(n, 0) = n.$$

Corollary 7 then implies that for every $i \in [s]$ and $\mathfrak{P}/\mathfrak{p}_i$,

$$e(\mathfrak{P}/\mathfrak{p}_i) = \frac{n}{r_{\mathfrak{p}_i}} = n,$$

which proves Item 3, namely, $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ totally ramify in $\mathrm{F}/\mathrm{K}(x)$.

Proof.

For every $\mathfrak{q} \in \mathbb{P}(\mathrm{F})$ lying over $\mathfrak{p}_\infty$, Corollary 7 implies that

$$e(\mathfrak{q}/\mathfrak{p}_\infty) = \frac{n}{d},$$

establishing Item 4.

Item 5 follows as for $\mathfrak{p}$ other than $\mathfrak{p}_1, \ldots, \mathfrak{p}_s, \mathfrak{p}_\infty$, we have that $r_\mathfrak{p} = n$ and so

$$e(\mathfrak{P}/\mathfrak{p}) = \frac{n}{n} = 1$$

for all $\mathfrak{P} \in \mathbb{P}(\mathrm{F})$ lying over $\mathfrak{p}$.

Tame cyclic extensions of $\mathsf{K}(x)$

Proof.

We turn to compute the genus g of F. Recall that $r_{\mathfrak{p}_i} = 1$ for all $i \in [s]$, $r_{\mathfrak{p}_\infty} = d$, and $r_{\mathfrak{p}} = n$ for all other $\mathfrak{p} \in \mathbb{P}(\mathsf{K}(x))$.

By Corollary 7,

$$g = 1 + n \cdot (g_{\mathsf{K}(x)} - 1) + \frac{1}{2} \sum_{\mathfrak{p} \in \mathbb{P}(\mathsf{E})} (n - r_{\mathfrak{p}}) \deg \mathfrak{p}$$

$$= 1 - n + \frac{1}{2} \left((n-d) \cdot 1 + \sum_{i=1}^{s} (n-1) \deg p_i \right)$$

$$= \frac{n-1}{2} \left(-1 + \sum_{i=1}^{s} \deg p_i(x) \right) - \frac{d-1}{2}.$$

□