

Kummer Extensions

Unit 25

Gil Cohen

May 22, 2022

Overview

- 1 Galois review - cyclic extensions
- 2 No ramification in constant field extensions
- 3 Kummer extensions
- 4 Certain quadratic extensions
- 5 Tame cyclic extensions of $K(x)$

Recall that a Galois extension F/K is called **cyclic** if $\text{Gal}(F/K)$ 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

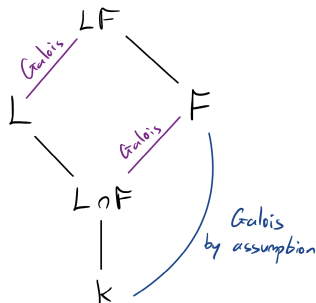
Lemma 2

Let $K \subseteq L, F$ be fields s.t. F/K is a finite Galois extension. Then LF/L is Galois and

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

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

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

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

$$LF = F(S)$$

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

Cyclic extensions

Proof. (Proof of Lemma 2)

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

Let $f(x) \in K[x]$ 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 $g(x) \in L[x]$ be the minimal polynomial of a over L . Since $K \subseteq L$ 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 $g(x) \in F[x]$, and so

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

Now,

$$LF = LK(a) = L(a),$$

and so

$$[LF : L] = [L(a) : L] = \deg g(x). \quad (1)$$

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

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

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

$$\begin{aligned}\varphi : \text{Gal}(LF/L) &\rightarrow \text{Gal}(F/(L \cap F)) \\ \sigma &\mapsto \sigma|_F\end{aligned}$$

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

As

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

we have that φ is also onto. Thus,

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



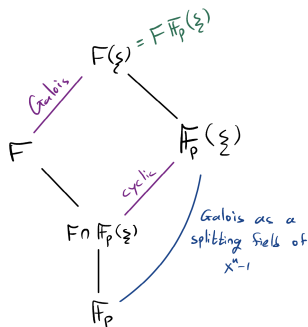
Cyclic extensions

Proof. (Proof of Lemma 1)

We have that

$$F(\zeta) = F\mathbb{F}_p(\zeta).$$

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



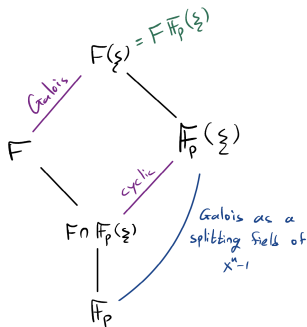
Cyclic extensions

Proof. (Proof of Lemma 1)

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

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

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,

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

Proof.

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

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

where $\mu_n \subseteq E$ 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.

Proof.

Thus, F/E is Galois and an element $\sigma \in \text{Gal}(F/E)$ 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 $\sigma_\zeta \in \text{Gal}(F/E)$ s.t. $\sigma_\zeta(a) = \zeta a$. Thus,

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

Cyclic extensions

Proof.

Moreover, the map

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

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 $a \in F$ s.t. $a^n \in E$ and $F = E(a)$.

Let σ be a generator of the cyclic group $\text{Gal}(F/E)$. It can be shown that the elements of $\text{Gal}(F/E)$ are linearly independent over E (even over \bar{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 $F = E(a)$ and that $a^n \in E$.

As $\zeta \in E$ we have that

$$\begin{aligned} \sigma(a) &= \sum_{j=0}^{n-1} \zeta^j \sigma^{j+1}(t) = \zeta^{-1} \sum_{j=0}^{n-1} \zeta^{j+1} \sigma^{j+1}(t) \\ &= \zeta^{-1} \sum_{j=0}^{n-1} \zeta^j \sigma^j(t) = \zeta^{-1} a. \end{aligned}$$

Cyclic extensions

Proof.

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

$$\{a, \zeta^{-1}a, \dots, (\zeta^{-1})^{n-1}a\} = \{a, \zeta a, \dots, \zeta^{n-1}a\}.$$

Thus, the minimal polynomial of a over E is

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

Thus, $F = E(a)$ and $a^n \in E$. □

Overview

- 1 Galois review - cyclic extensions
- 2 No ramification in constant field extensions
- 3 Kummer extensions
- 4 Certain quadratic extensions
- 5 Tame cyclic extensions of $K(x)$

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 $F = EL$. Then, for every $\mathfrak{P} \in \mathbb{P}(F)$ lying over some $\mathfrak{p} \in \mathbb{P}(E)$ we have

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

Proof.

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

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

As $\alpha \in L$, 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.

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

But $\alpha \in L$ and so $\varphi'(\alpha) \in L$. Hence,

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

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

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



Overview

- 1 Galois review - cyclic extensions
- 2 No ramification in constant field extensions
- 3 Kummer extensions**
- 4 Certain quadratic extensions
- 5 Tame cyclic extensions of $K(x)$

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 $\text{Gal}(F/E)$ 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 $\mathfrak{p} \in \mathbb{P}(E)$ and $\mathfrak{P} \in \mathbb{P}(F)$ lying over \mathfrak{p} . Let

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

Then,

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

Moreover, if L is the constant field of F and g_F, g_E are the genera of E/K and F/L , respectively then

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

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

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

By assumption,

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

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 $p = \text{char}(K)$ 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 $\ell \in \mathbb{Z}$.

Kummer Extensions

Proof.

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

Take $t \in E$ s.t. $v_p(t) = \ell$, 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,

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

and so

$$v_{\mathfrak{p}}(y_1) = v_p(u_1) = 0.$$



Proof.

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

Observe that

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

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

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

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 $F = E(y_1)$. As F/E is separable, by a theorem we proved,

$$d(\mathfrak{P}/\mathfrak{p}) \leq v_{\mathfrak{P}}(\psi'(y_1)).$$

Proof.

So far we have that $d(\mathfrak{K}/\mathfrak{p}) \leq v_{\mathfrak{p}}(\psi'(y_1))$. Now,

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

and so

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

so

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

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

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

Kummer Extensions

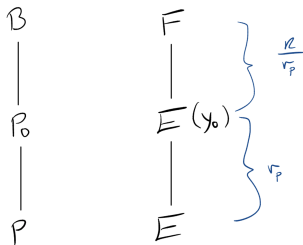
Proof.

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

$$y_0 = y^{n/r_p}$$

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

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

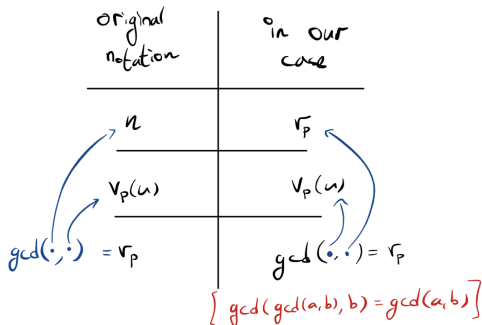


Kummer Extensions

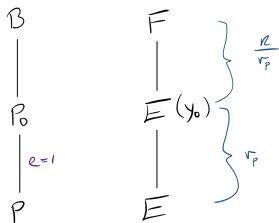
Proof.

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

$$e(p_0/p) = 1.$$



Kummer Extensions



Proof.

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

Moving on to consider $F/E(y_0)$ we first note that

$$r_p \cdot v_{p_0}(y_0) = v_{p_0}(y_0^{r_p}) = v_{p_0}(u) = e(p_0/p) \cdot v_p(u) = v_p(u),$$

and so

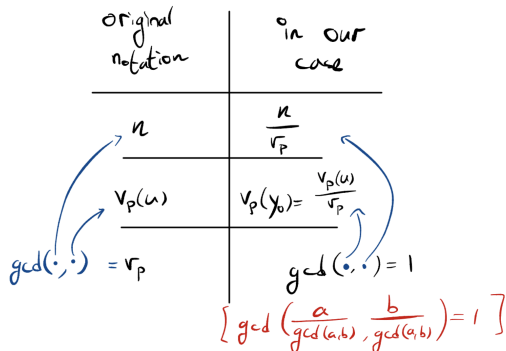
$$v_{p_0}(y_0) = \frac{v_p(u)}{r_p}.$$

Kummer Extensions

Proof.

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

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

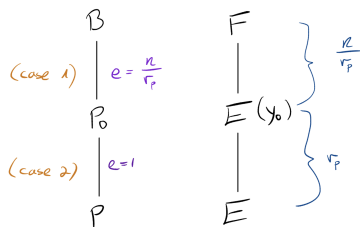


Kummer Extensions

Proof.

In summary we obtained the information depicted 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

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

Thus,

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

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

$$\begin{aligned}\sum_{\mathfrak{P}/\mathfrak{p}} \deg \mathfrak{P} &= \frac{1}{e(\mathfrak{p})} \cdot \deg \left(\sum_{\mathfrak{P}/\mathfrak{p}} e(\mathfrak{P}/\mathfrak{p}) \mathfrak{P} \right) \\ &= \frac{1}{e(\mathfrak{p})} \cdot \deg \text{Con}_{F/E}(\mathfrak{p}).\end{aligned}$$

In a previous unit we proved that

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

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

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

Proof.

Recall we showed that

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

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

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

Proof.

We summarize

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

Now, by the Hurwitz Genus Formula,

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

and so

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

Corollary 7

Let E/K be a function field and

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

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

Assume further that

$$\exists q \in \mathbb{P}(E) \quad \gcd(v_q(u), n) = 1.$$

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

$$g_F = 1 + n \cdot (g_E - 1) + \frac{1}{2} \sum_{p \in \mathbb{P}(E)} (n - r_p) \deg p.$$

Proof.

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

Otherwise,

$$v_q(u) = v_q(w^d) = d \cdot v_q(w),$$

which would imply $d \mid v_q(u)$ in contradiction to $\gcd(v_q(u), n) = 1$.

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

$$E \subseteq EL \subseteq F.$$

Kummer Extensions

Proof.

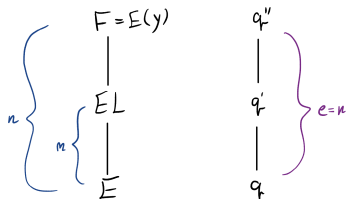
Let $q'' \in \mathbb{P}(F)$ be the prime divisor lying over q . Note that q'' is unique as

$$e(q''/q) = \frac{n}{r_q} = \frac{n}{\gcd(n, v_q(u))} = n.$$

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

$$e(q'/q) = 1$$

as no ramification occurs in constant field extensions per Lemma 4



Kummer Extensions

Proof.

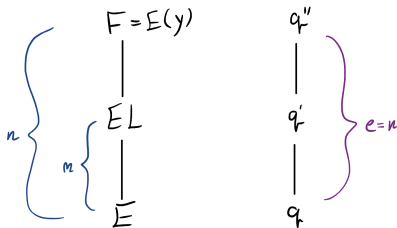
On the other hand, as $m \mid n$ and $\gcd(n, v_q(u)) = 1$ we have that

$$\gcd(m, v_q(u)) = 1.$$

Thus, by Theorem 6,

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

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



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

- 1 Galois review - cyclic extensions
- 2 No ramification in constant field extensions
- 3 Kummer extensions
- 4 Certain quadratic extensions**
- 5 Tame cyclic extensions of $K(x)$

Certain quadratic extensions

Lemma 8

Let $F = K(x, y)$ where

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

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

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

Certain quadratic extensions

Proof.

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

$$\gcd(v_q(f(x)), n) = \gcd(1, 2) = 1.$$

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

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

As for the genus, note that

$$r_q = \gcd(n, v_q(f(x))) = \gcd(2, 1) = 1,$$

$$r_\infty = \gcd(n, v_\infty(f(x))) = \gcd(2, -m) = \gcd(2, m).$$

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

$$r_p = \gcd(n, v_p(f(x))) = \gcd(2, 0) = 2.$$

Certain quadratic extensions

Proof.

$$\begin{aligned}r_q &= 1, \\r_\infty &= \gcd(2, m), \\r_p &= 2 \quad \text{otherwise.}\end{aligned}$$

By Corollary 7,

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

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

$$\begin{aligned}g_F &= -1 + \frac{1}{2} (1 \cdot \deg q + (2 - \gcd(2, m)) \cdot \deg p_\infty) \\&= -1 + \frac{1}{2} (m + (2 - \gcd(2, m))).\end{aligned}$$

Certain quadratic extensions

Proof.

Hence,

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



Overview

- 1 Galois review - cyclic extensions
- 2 No ramification in constant field extensions
- 3 Kummer extensions
- 4 Certain quadratic extensions
- 5 Tame cyclic extensions of $K(x)$

Tame cyclic extensions of $K(x)$

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

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

where

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

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 $[F : K(x)] = n$;
- 2 If K contains an n -th root of unity, $F/K(x)$ is cyclic.
- 3 The prime divisors that correspond to $p_1(x), \dots, p_s(x)$ in $\mathbb{P}(K(x))$ are totally ramified in $F/K(x)$.
- 4 All prime divisors \mathfrak{q} lying over $\mathfrak{p}_\infty \in \mathbb{P}(K(x))$ 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 $F/K(x)$.
- 6 Finally, the genus g of $F/K(x)$ 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, $\text{char}(K)$ 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 $v_{\mathfrak{p}_i}(u) = n_i$ 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.

Tame cyclic extensions of $K(x)$

Proof.

Now,

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

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

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

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

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, $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ totally ramify in $F/K(x)$.

Tame cyclic extensions of $K(x)$

Proof.

For every $\mathfrak{q} \in \mathbb{P}(F)$ lying over \mathfrak{p}_∞ , 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 $\mathfrak{p}_1, \dots, \mathfrak{p}_s, \mathfrak{p}_\infty$, we have that $r_{\mathfrak{p}} = n$ and so

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

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

Tame cyclic extensions of $K(x)$

Proof.

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

By Corollary 7,

$$\begin{aligned}g &= 1 + n \cdot (g_{K(x)} - 1) + \frac{1}{2} \sum_{p \in \mathbb{P}(E)} (n - r_p) \deg p \\&= 1 - n + \frac{1}{2} \left((n - d) \cdot 1 + \sum_{i=1}^s (n - 1) \deg p_i \right) \\&= \frac{n-1}{2} \left(-1 + \sum_{i=1}^s \deg p_i(x) \right) - \frac{d-1}{2}.\end{aligned}$$

□