ELEMENTARY ABELIAN P-EXTENSIONS OF ALGEBRAIC FUNCTION FIELDS AND THE HASSE-ARF THEOREM

APPROVED BY

Assoc. Prof. Dr. Cem Güneri ....
(Thesis Supervisor)

Prof. Dr. Alev Topuzoğlu ....

Assist. Prof. Dr. Seher Tutdere ....

DATE OF APPROVAL: 06.01.2017

ELEMENTARY ABELIAN P-EXTENSIONS OF ALGEBRAIC FUNCTION FIELDS AND THE HASSE-ARF THEOREM

by

SEZEL ALKAN

Submitted to the Graduate School of Engineering and Natural Sciences
in partial fulfillment of
the requirements for the degree of
Master of Science

Sabancı University
Fall 2016

ELEMENTARY ABELIAN P-EXTENSIONS OF ALGEBRAIC FUNCTION FIELDS AND THE HASSE-ARF THEOREM

APPROVED BY

Assoc. Prof. Dr. Cem Güneri (Thesis Supervisor)	....
Prof. Dr. Alev Topuzoğlu	....
Assist. Prof. Dr. Seher Tutdere	....

DATE OF APPROVAL: January 6, 2017

ELEMENTARY ABELIAN P-EXTENSIONS OF ALGEBRAIC FUNCTION FIELDS AND THE HASSE-ARF THEOREM

Sezel Alkan

Mathematics, Master Thesis, 2017

Thesis Supervisor: Assoc. Prof. Dr. Cem Güneri

Keywords: Function field extension, elementary abelian extension, ramification, rational place, genus

Abstract

This thesis starts with the basic properties of elementary abelian p-extensions of function fields. Ramification structure and the genus computation for such extensions are presented first. When the constant field is finite, number of rational places of function fields is finite and this number is bounded by the Hasse-Weil bound. However for large genus, this bound is weak. Therefore, when a sequence of function field extensions with growing genera is considered, the growth of the ratio of the number of rational places to the genera in the sequence is of interest. Following the work of Frey-Perret-Stichtenoth, we show that the limit of this ratio is zero if a sequence of elementary abelian p-extensions are considered. Hasse-Arf Theorem gives information about the jumps in the higher ramification group filtration of a function field extension. We also present the proof of this theorem for elementary abelian p-extensions, which is due to Garcia and Stichtenoth.

CEBİRSEL FONKSİYON CİSİMLERİNİN ELEMENTER ABELYEN P GENİŞLEMELERİ VE HASSE-ARF TEOREMİ

Sezel Alkan

Matematik, Yüksek Lisans Tezi, 2017

Tez Danışmanı: Doç. Dr. Cem Güneri

Anahtar Kelimeler: Fonksiyon cismi genişlemesi, elementer abelyen genişleme, dallanma, rasyonel yer, cins.

Özet

Bu tezde ilk olarak fonksiyon cisimlerinin elementer abelyen p-genişlemelerinin temel özellikleri sunulmuştur. Bu tür genişlemeler için dallanma yapısı ve cinsin hesaplanması gösterilmiştir. Sabit cismi sonlu olduğunda fonksiyon cisminin rasyonel nokta sayısı da sonludur. Bu durumda rasyonel nokta sayısı Hasse-Weil sınırı ile sınırlıdır. Ancak cins büyük olduğunda bu sınır zayıftır. Bu sebeple cinsi büyüyen bir fonksiyon cismi genişlemeleri dizisi ele alındığında, dizideki rasyonel noktaların sayısının cinslere oranının nasıl büyüdüğü önemlidir. Frey-Perret-Stichtenoth çalışmasını takip ederek, dizideki fonksiyon cismi genişlemeleri elementer abelyen p-genişlemeleri olduğu durumda bu oranın limitinin sıfır olduğu gösterilmiştir. Hasse-Arf Teoremi, fonksiyon cismi genişlemesinin üst dallanma grupları filtrasyonundaki sıçramalar hakkında bilgi verir. Tezde bu teoremin elementer abelyen p-genişlemeleri için Garcia ve Stichtenoth tarafından yapılmış bir ispatı da sunulmuştur.

to my parents

Acknowledgements

First of all, I would like to thank my supervisor Cem Güneri for his help and guidance. I would like to give special thanks to Henning Stichtenoth. It has been an honor to learn function fields from him. Moreover, I want to thank all other members of the faculty for providing a warm and friendly environment.

Table of Contents

1

Preliminaries

In this section, we fix some notation and state a few results which will be used in the following sections. Our notation follows that of [S]. We assume that the reader is familiar with the theory of algebraic function fields. Throughout, we will use

- K for a perfect field with characteristic $p > 0$;
- F, E, E_i, $\ldots$ for algebraic function fields over K;
- P, P' for places of a function field and $degP$ for the degree of the place P;
- $\mathbb{P}_F$ for the set of places of F;
- v_P for the discrete valuation associated to the place P;
- $g(F)$ for the genus of the function field F.

Let us consider a finite extension E/F of function fields and a place P of F. For any place $P' \in \mathbb{P}_E$ lying above P, we write $P'|P$. Let $e(P'|P)$ and $f(P'|P)$ denote the ramification index and the relative degree of P' over P, respectively. Then we have

$$\sum_{P'|P} e(P'|P)f(P'|P) = [E : F],$$

which is called the Fundamental Equality [S, Theorem 3.1.11]. In particular, if E/F is a Galois extension, then $e(P) := e(P'|P) = e(P''|P)$ and $f(P) := f(P'|P) = f(P''|P)$ for any two places $P', P'' \in \mathbb{P}_E$ lying over P. Hence, we have $e(P)f(P)g(P) = [E : F]$, where $g(P)$ denotes the number of places of E lying over P.

The extension $P'|P$ is said to be ramified if $e(P'|P) > 1$; otherwise it is called unramified. Moreover, we say that P is totally ramified in E/F if $e(P'|P) = [E : F]$ for some $P'|P$. Clearly, in that case there is only one place lying over P.

Suppose that the extension E/F is separable, as well. Let $d(P'|P)$ denote the different exponent of $P'|P$. Then $d(P'|P) \geq 0$, and in addition $d(P'|P) = 0$ for almost all $P \in \mathbb{P}_F$ and $P'|P$. Thus, we have a divisor

$$\mathrm{Diff}(E/F) := \sum_{P\in\mathbb{P}_F} \sum_{P'|P} d(P'|P)P'$$

of E, called the different of E/F. Note that $d(P'|P) \geq e(P'|P) - 1$ for all $P'|P$ and equality holds if and only if the characteristic of F does not divide $e(P'|P)$. In particular, $d(P'|P) = 0$ if the extension $P'|P$ is unramified.

The genus of E can be determined by the genus of F and the different $\mathrm{Diff}(E/F)$. More precisely,

$$2g(E) - 2 = [E : F](2g(F) - 2) + deg(\mathrm{Diff}(E/F)).$$

This is called the Hurwitz Genus Formula [S, Theorem 3.4.13]. Here we also assumed E and F have the same constant field.

Now let E/F be a cyclic extension with $[E : F] = p = char(F)$. Then there exist elements $y \in E$, $a \in F$ such that

$$E = F(y) \quad \text{and} \quad y^p - y = a,$$

and the Galois group of E/F is generated by the automorphism σ defined by

$$\sigma(y) = y + 1.$$

Conversely, for any $a \in F$, either all the roots of the polynomial $\varphi(t) = t^p - t - a$ are in F or it is irreducible. In the latter case, $F(y)/F$ is a cyclic extension of degree p, where y is a root of $\varphi(t)$.

The extensions described above are called Artin-Schreier extensions. Artin-Schreier extensions are the simplest examples of elementary abelian p-extensions which have Galois group isomorphic to $(\mathbb{Z}/p\mathbb{Z})^n$ for some n. This thesis presents the basic structure of elementary abelian p-extensions and also the proof of Hasse-Arf Theorem for these extensions.

2

Basics of Elementary Abelian p-Extensions

In this section we give some basic properties of elementary abelian p-extensions of algebraic function fields, which are generalizations of Artin-Schreier extensions. Let us recall the definition of such extensions.

Definition 2.1. An extension E/F of function fields is called an *elementary abelian p-extension* if it is Galois with $Gal(E/F)$ an elementary abelian p-group, or equivalently if $Gal(E/F) \simeq (\mathbb{Z}/p\mathbb{Z})^n$ for some n.

The following theorem shows that elementary abelian p-extensions of a field F with characteristic $p > 0$ and additive subgroups of that field are closely related. It is stated in [GS] without a proof.

Theorem 2.2. *Let F be a field of characteristic p and $U \subseteq F$ be an additive subgroup of F with*

$$ord(U) = p^n \quad and \quad U \cap \wp(F) = \{0\},$$

where $\wp : u \mapsto u^p - u$ is the Artin-Schreier operator. Then $F(\wp^{-1}(U))$ is an elementary abelian p-extension of degree p^n.

To prove Theorem 2.2, we need the following facts.

Lemma 2.3. *[GO, Lemma 2.3] Let F be a field of characteristic p and $a, b \in F$. Suppose that an Artin-Schreier extension E/F can be defined by two distinct ways:*

$$E = F(y) \quad with \quad y^p - y = a,$$

$$E = F(z) \quad with \quad z^p - z = b.$$

Then there exist some $c \in F$ and $\alpha \in \mathbb{F}_p \setminus \{0\}$ such that

$$b - \alpha a = c^p - c.$$

Lemma 2.4. *[L, Corollary 1.15] Let $E_1, \ldots, E_n$ be Galois extensions of F with Galois groups $G_1, \ldots, G_n$. Suppose that*

$$E_i \cap (E_1 \cdots E_{i-1}) = F$$

for each $1 < i \leq n$. Then the Galois group of $E_1 \cdots E_n$ is isomorphic to $\prod_{i=1}^n G_i$.

Now we prove the theorem.

Proof of Theorem 2.2. Note that $y \in \wp^{-1}(U)$ if and only if $y^p - y - u = 0$ for some $u \in U$. Then $F(\wp^{-1}(U))$ is the splitting field of the set of polynomials

$$\{t^p - t - u \in F[t] \mid u \in U\}$$

over F. Furthermore, as each polynomial of this set is separable over F the extension $F(\wp^{-1}(U))/F$ is Galois.

Since $U \subseteq F$ is an additive subgroup of the field F of characteristic $p > 0$ we can consider U as a vector space over $\mathbb{F}_p$. As $ord(U) = p^n$, there exist $u_1, u_2, \ldots, u_n \in U$ such that

$$U = \mathbb{F}_p u_1 \oplus \mathbb{F}_p u_2 \oplus \ldots \oplus \mathbb{F}_p u_n.$$

For each u_i, $1 \leq i \leq n$ we can find $y_i \in F(\wp^{-1}(U))$ such that $y_i^p - y_i = u_i$. We claim that $F(\wp^{-1}(U)) = F(y_1, y_2, \ldots, y_n)$. Clearly, $F(y_1, y_2, \ldots, y_n) \subseteq F(\wp^{-1}(U))$. For the proof of the opposite inclusion, we take $u \in U$. It is enough to show that $F(\wp^{-1}(u)) \subseteq F(y_1, y_2, \ldots, y_n)$. We have

$$u = k_1 u_1 + k_2 u_2 + \ldots + k_n u_n$$

for some $k_i \in \mathbb{F}_p$. Let

$$y = k_1 y_1 + k_2 y_2 + \ldots + k_n y_n \in F(\wp^{-1}(U)).$$

Applying the Artin-Schreier operator $\wp$ to both sides of the equation we obtain

$$\begin{aligned}
\wp(y) &= \wp(k_1 y_1 + k_2 y_2 + \ldots + k_n y_n) \\
&= (k_1 y_1 + k_2 y_2 + \ldots + k_n y_n)^p - (k_1 y_1 + k_2 y_2 + \ldots + k_n y_n) \\
&= k_1 y_1^p + k_2 y_2^p + \ldots + k_n y_n^p - k_1 y_1 - k_2 y_2 - \ldots - k_n y_n \\
&= k_1(y_1^p - y_1) + k_2(y_2^p - y_2) + \ldots + k_n(y_n^p - y_n) \\
&= k_1 u_1 + k_2 u_2 + \ldots + k_n u_n \\
&= u.
\end{aligned}$$

Hence, $y = k_1 y_1 + k_2 y_2 + \ldots + k_n y_n$ is a root of the polynomial $t^p - t - u \in F[t]$. Observe that the other roots of $t^p - t - u$ are $y + \mu$, where $\mu \in \mathbb{F}_p \setminus \{0\}$. Hence all the roots of $t^p - t - u$ live in $F(y_1, y_2, \ldots, y_n)$, which implies that $F(\wp^{-1}(u)) \subseteq F(y_1, y_2, \ldots, y_n)$. Since $u \in U$ is arbitrary, we have $F(\wp^{-1}(U)) \subseteq F(y_1, y_2, \ldots, y_n)$.

Note that $y_i \notin F$ for any i, since otherwise $\wp(y_i) = y_i^p - y_i = u_i \in \wp(F)$ and this contradicts the assumption $U \cap \wp(F) = \{0\}$, as $u_i \neq 0$. Hence, $F(y_i)/F$ is a degree p (Artin-Schreier) extension for all $1 \leq i \leq n$.

Now we prove the following equality:

$$[F(y_1, \ldots, y_i) : F(y_1, \ldots, y_{i-1})] = p \quad \text{for all} \quad 1 < i \leq n. \tag{2.1}$$

Assume that $[F(y_1, \ldots, y_i) : F(y_1, \ldots, y_{i-1})] = 1$ for some $1 < i \leq n$. We have seen that $[F(y_i) : F] = p$ with $y_i^p - y_i = u_i$. If $F \subseteq F(y_i) \subseteq F(y_1, \ldots, y_{i-1})$, then there exists $\tilde{y} \in F(y_1, \ldots, y_{i-1})$ such that $F(y_i) = F(\tilde{y})$ and $\tilde{y}^p - \tilde{y} = u$ for some $u \in \oplus_{k=1}^{i-1} \mathbb{F}_p u_k$. Then by [GO, Lemma 1.2], we conclude that

$$u_i - \alpha u = c^p - c$$

for some $\alpha \in \mathbb{F}_p \setminus \{0\}$ and $c \in F$. Since $U \cap \wp(F) = \{0\}$, $u_i - \alpha u = 0$, or $u_i = \alpha u$. This is a contradiction to the linear independence of $\{u_1, \ldots, u_n\}$, hence our claim holds. Therefore, $[F(\wp^{-1}(U)) : F] = [F(y_1, y_2, \ldots, y_n) : F] = p^n$.

To complete the proof, we show that the extension $F(\wp^{-1}(U)) = F(y_1, y_2, \ldots, y_n)$ of F is elementary abelian.

Clearly, $F(y_1, y_2, \ldots, y_n)$ is the compositum of the fields $F(y_i)$, $1 \leq i \leq n$ satisfying $[F(y_i) : F] = p$. Furthermore, $F(y_i) \cap F(y_1, \ldots, y_{i-1}) = F$ for every $1 < i \leq n$, by the previous paragraph. Then by Lemma 2.4,

$$Gal(F(y_1, y_2, \ldots, y_n)/F) \simeq \prod_{i=1}^{n} Gal(F(y_i)/F).$$

Since each $F(y_i)/F$ is an Artin-Schreier extension, we have $Gal(F(y_i)/F) \simeq \mathbb{Z}/p\mathbb{Z}$ for all $1 \leq i \leq n$ and this gives the desired result. □

The converse of Theorem 2.2 also holds. The proof we provide is similar to that of [AA].

Theorem 2.5. *Let E/F be an elementary abelian p-extension of degree p^n. Then*

$$E = F(\wp^{-1}(U))$$

for some additive subgroup $U \subseteq F$ with

$$ord(U) = p^n \quad \textit{and} \quad U \cap \wp(F) = \{0\}. \tag{2.2}$$

Proof. Since E/F is an elementary abelian p-extension of degree p^n, the Galois group of E/F is

$$G := Gal(E/F) = \prod_{i=1}^{n} G_i,$$

where each G_i is a cyclic group of order p. For each $1 \leq i \leq n$, let E_i be the fixed field of the subgroup

$$H_i := G_1 \times \ldots \times G_{i-1} \times \{id\} \times G_{i+1} \times \ldots \times G_n$$

of G. As H_i is a normal subgroup of G (since G is abelian), E_i/F is Galois and

$$Gal(E_i/F) \simeq G/H_i \simeq G_i,$$

implying that

$$[E_i : F] = ord(Gal(E_i/F)) = ord(G_i) = p.$$

Then there exist $u_i \in F$ and $y_i \in E_i$ such that

$$E_i = F(y_i) \quad \text{and} \quad y_i^p - y_i = u_i.$$

Hence, as in the proof of Theorem 2.2, we get

$$E_1 \cdots E_n = F(y_1, \ldots, y_n) = F(\wp^{-1}(U)),$$

where U is the additive subgroup of F generated by $u_1, \ldots, u_n$.

Let us prove that $ord(U) = p^n$. For this it is sufficient to show that the set $\{u_1, \ldots, u_n\}$ is linearly independent over $\mathbb{F}_p$. Assume the contrary. Then there exist $c_1, \ldots, c_n \in \mathbb{F}_p$, not all 0, such that $\sum_{i=1}^n c_i u_i = 0$. Assume without loss of generality that $c_1 \neq 0$. We have

$$\begin{aligned} 0 = \sum_{i=1}^n c_i u_i &= \sum_{i=1}^n c_i (y_i^p - y_i) \\ &= \sum_{i=1}^n c_i y_i^p - \sum_{i=1}^n c_i y_i \\ &= (\sum_{i=1}^n c_i y_i)^p - \sum_{i=1}^n c_i y_i. \end{aligned} \tag{2.3}$$

Let $y := \sum_{i=1}^n c_i y_i$. From (2.3) we get $y^p = y$, i.e. $y \in \mathbb{F}_p$. As $c_1 \neq 0$, we have

$$y_1 = c_1^{-1}(y - \sum_{i=2}^n c_i y_i).$$

Hence,

$$y_1 \in E_1 \cap (E_2 \cdots E_n). \tag{2.4}$$

Since $E_2 \cdots E_n$ is the fixed field of the subgroup

$$H := \bigcap_{i=2}^n H_i = G_1 \times \{id\} \times \ldots \times \{id\}$$

of G and E_1 is the fixed field of H_1, we conclude that $E_1 \cap (E_2 \cdots E_n)$ is the fixed field of the smallest subgroup of G containing H_1 and H, which is G. So $E_1 \cap (E_2 \cdots E_n) = F$. This implies by (2.4) that $y_1 \in F$, contradicting $[F(y_1) : F] = p$. Hence, $\{u_1, \ldots, u_n\}$ is linearly independent over $\mathbb{F}_p$, and $ord(U) = p^n$.

We will now show that $U \cap \wp(F) = \{0\}$. Let $x \in U \cap \wp(F)$. Then

$$x = \sum_{i=1}^{n} \alpha_i u_i = z^p - z$$

for some $z \in F$ and $\alpha_i \in \mathbb{F}_p$. Thus,

$$z^p - z = \sum_{i=1}^{n} \alpha_i u_i = \sum_{i=1}^{n} \alpha_i (y_i^p - y_i) = (\sum_{i=1}^{n} \alpha_i y_i)^p - \sum_{i=1}^{n} \alpha_i y_i$$

or equivalently

$$\sum_{i=1}^{n} \alpha_i y_i - z = (\sum_{i=1}^{n} \alpha_i y_i)^p - z^p = (\sum_{i=1}^{n} \alpha_i y_i - z)^p,$$

implying that $w := \sum_{i=1}^{n} \alpha_i y_i - z \in \mathbb{F}_p$. Suppose that $x \neq 0$. Then $\alpha_j \neq 0$ for some $1 \leq j \leq n$, and by the argument used in proving $ord(U) = p^n$, we have

$$y_j = \alpha_j^{-1}(w + z - \sum_{\substack{i \neq j, \\ 1 \leq i \leq n}} \alpha_i y_i) \in E_j \cap (E_1 \cdots E_{j-1} \cdot E_{j+1} \cdots E_n) = F,$$

i.e. $y_j \in F$. This is a contradiction to $[F(y_j) : F] = p$. Hence $x = 0$ and $U \cap \wp(F) = \{0\}$.

We have shown that $E_1 \cdots E_n = F(\wp^{-1}(U))$ satisfies (2.2). Then by Theorem 2.2 we obtain that $F(\wp^{-1}(U))/F$ is an elementary abelian p-extension of degree p^n. Finally, since $F(\wp^{-1}(U)) = E_1 \cdots E_n \subseteq E$ and $[E : F] = p^n$, we have

$$E = E_1 \cdots E_n = F(\wp^{-1}(U)).$$

□

Since an elementary abelian p-extension E/F is finite and Galois, there exists $y \in E$ such that $E = F(y)$. In the following theorem, under some assumptions, we find such an element and its minimal polynomaial over F. First, let us introduce some special type of polynomials.

Definition 2.6. A polynomial of the form

$$a(t) = a_n t^{p^n} + a_{n-1} t^{p^{n-1}} + \ldots + a_t t^p + a_0 t \in F[t]$$

is called an *additive polynomial* over F.

Note that $a(t)$ is separable if and only if $a_0 \neq 0$. Moreover, since F has characteristic $p > 0$,

$$a(x + y) = a(x) + a(y) \tag{2.5}$$

for any $x, y \in E$, where E is an arbitrary extension of F.

Proposition 2.7. *Let E/F be an elementary abelian p-extension of degree p^n and $a(t) \in F[t]$ be a separable, monic, additive polynomial of degree p^n. Suppose that*

$$W := \{\alpha \mid a(\alpha) = 0\} \subseteq F.$$

Then there exists an element $y \in E$ with $E = F(y)$ whose minimal polynomial over F is given by

$$\varphi(t) = a(t) - z \in F[t], \quad \textit{for some} \quad z \in F.$$

In particular, if $\mathbb{F}_{p^n} \subseteq F$, then $y \in E$ can be chosen such that its minimal polynomial is $\varphi(t) = t^{p^n} - t - z \in F[t]$, with $z \in F$.

Proof. We have seen that there exist $y_1, \ldots, y_n \in E$ such that

$$E = F(y_1, \ldots, y_n) \quad \text{with} \quad y_i^p - y_i \in F,$$

for all $1 \leq i \leq n$. Now we will find generators of $Gal(E/F)$ by extending the generators of the Artin-Schreier extensions $F(y_i)/F$, $1 \leq i \leq n$, to $E = F(y_1, \ldots, y_n)$. Define the automorphisms σ_i, $1 \leq i \leq n$, of E over F by

$$\sigma_i(y_i) = y_i + 1, \quad \sigma_i(y_j) = y_j \quad \text{for} \quad j \neq i.$$

It can easily be seen that these are actually automorphisms of E/F. In order to prove σ_i's generate $Gal(E/F)$, it is enough to show that they are linearly independent over $\mathbb{F}_p$. Suppose not, then

$$\sigma_1^{\nu_1} \circ \sigma_2^{\nu_2} \circ \ldots \circ \sigma_n^{\nu_n} = id$$

for some $\nu_i \in \mathbb{F}_p$, not all $\nu_i = 0$. We can assume $\nu_1 \neq 0$. Since $\sigma_1^{\nu_1} = \sigma_n^{-\nu_n} \circ \ldots \circ \sigma_2^{-\nu_2}$, we obtain

$$y_1 + \nu_1 = \sigma_1^{\nu_1}(y_1) = \sigma_n^{-\nu_n} \circ \ldots \circ \sigma_2^{-\nu_2}(y_1) = y_1.$$

This is a contradiction because $\nu_1 \neq 0$. Hence, σ_i's generate $Gal(E/F)$.

By (2.5), W is an additive subgroup of F. Since $a(t) \in F[t]$ is separable and $deg(a(t)) = p^n$, $ord(W) = p^n$. Thus,

$$W = \bigoplus_{i=1}^{n} \mathbb{F}_p w_i$$

for some $w_i \in W \subseteq F$.

Define $y := \sum_{i=1}^{n} w_i y_i$, and let $\sigma \in Gal(E/F)$. There are $\mu_1, \mu_2, \ldots, \mu_n \in \mathbb{F}_p$ such that

$$\sigma = \sigma_1^{\mu_1} \circ \sigma_2^{\mu_2} \circ \ldots \circ \sigma_n^{\mu_n}. \tag{2.6}$$

Then we have

$$\sigma(y) = \sigma(\sum_{i=1}^{n} w_i y_i) = \sum_{i=1}^{n} w_i \sigma(y_i) = \sum_{i=1}^{n} w_i (y_i + \mu_i) = y + \sum_{i=1}^{n} \mu_i w_i. \tag{2.7}$$

Hence,

$$\begin{aligned} \sigma(y) = y &\Leftrightarrow \sum_{i=1}^{n} \mu_i w_i = 0 \\ &\Leftrightarrow \mu_i = 0 \quad \text{for all} \quad 1 \leq i \leq n \\ &\Leftrightarrow \sigma = id. \end{aligned}$$

This implies that $F(y) = E$. To see this, suppose that $F(y) \subsetneqq E$. Then there exists $id \neq \gamma \in Gal(E/F(y)) \subseteq Gal(E/F)$, but this is not possible as $\gamma(y) = y$ implies $\gamma = id$ by the above argument. Therefore, $F(y) = E$.

Next, we find the minimal polynomial of y over F. Let $a(y) = z$, and $\sigma \in Gal(E/F)$ is an arbitrary automorphism. We assume σ has a combination as in (2.6). Then we have

$$\begin{aligned} \sigma(z) &= \sigma(a(y)) \\ &= a(\sigma(y)) \\ &= a(y + \sum_{i=1}^{n} \mu_i w_i) \qquad \text{(by (2.7))} \\ &= a(y) + a(\sum_{i=1}^{n} \mu_i w_i) \\ &= z + 0 \qquad (\text{since } \sum_{i=1}^{n} \mu_i w_i \in W) \\ &= z. \end{aligned}$$

Thus, $\sigma(z) = z$ for all $\sigma \in Gal(E/F)$, and this is equivalent to $z \in F$. Therefore, $\varphi(t) := a(t) - z \in F[t]$. Now we have y is a root of the monic polynomial $\varphi(t) \in F[t]$. Moreover, as $[F(y) : F] = [E : F] = p^n$ and $deg(\varphi(t)) = p^n$, the irreducibility is clear. Then $\varphi(t) \in F[t]$ is the minimal polynomial of y over F.

Finally, suppose that $\mathbb{F}_{p^n} \subseteq F$. Then the set of roots of the separable additive polynomial $a(t) := t^{p^n} - t \in F[t]$ is exactly $\mathbb{F}_{p^n}$, which is in F by assumption. Hence, the rest follows. □

From now on, we present fundamental concepts of elementary abelian p-extensions of function fields such as ramification, different exponents and genera. Let us note that the following proposition is stated in a more general setting in [S, Proposition 3.7.10] but its proof is omitted.

Proposition 2.8. *Consider an algebraic function field F/K with constant field K. Suppose that there exists an element $u \in F \setminus K$ which satisfies:*

$$\textit{for every place } P \in \mathbb{P}_F \textit{ with } v_P(u) < 0,\ gcd(p, v_P(u)) = 1.$$

Let $E = F(y)$ with

$$a(y) = u,$$

where $a(t) \in K[t]$ is a separable, monic, additive polynomial of degree p^n which has all its roots in K. Then

(a) E/F is a Galois extension of degree p^n and $Gal(E/F)$ is isomorphic to the additive group

$$W := \{\alpha \mid a(\alpha) = 0\} \subseteq K,$$

i.e. $Gal(E/F) \simeq (\mathbb{Z}/p\mathbb{Z})^n$.

(b) K is algebraically closed in E.

(c) Poles of u in F are totally ramified in E/F and the other places of F are unramified.

(d) Let $P \in \mathbb{P}_F$ be a pole of u with valuation $v_P(u) =: -m_P$. Then the different exponent $d(P'|P)$ of the extension P' of P in E is

$$d(P'|P) = (p^n - 1)(m_P + 1).$$

(e) The genus $g(E)$ of E is

$$g(E) = p^n g(F) + \frac{p^n - 1}{2}(-2 + \sum_{\substack{v_P(u)<0,\\ P\in\mathbb{P}_F}} (m_P + 1) degP),$$

where $g(F)$ is the genus of F and m_P is as in (d).

Proof. (a) Since $u \in F \setminus K$, u has at least one pole in F [S, Corollary 1.1.20] . So we can find a place $P \in \mathbb{P}_F$ such that

$$v_P(u) =: -m_P, \quad \text{with} \quad m_P > 0.$$

Let $P' \in \mathbb{P}_E$ be a place lying over P and $e := e(P'|P)$ be the ramification index of P' over P. As $a(t) \in K[t]$ is a monic, additive polynomial of degree p^n, we have

$$a(y) = y^{p^n} + a_{n-1}y^{p^{n-1}} + \ldots + a_1 y^p + a_0 y$$

for some $a_i \in K$. Since $a(y) = u$, we have

$$v_{P'}(a(y)) = v_{P'}(u) = ev_P(u) = e(-m_P) < 0. \tag{2.8}$$

This implies $v_{P'}(y) < 0$, using the triangle inequality. Then by the strict triangle inequality [S, Lemma 1.1.11] we obtain

$$v_{P'}(a(y)) = \min\{p^i v_{P'}(y) \mid 0 \leq i \leq n\} = p^n v_{P'}(y). \tag{2.9}$$

We conclude from (2.8) and (2.9) that

$$-em_P = v_{P'}(a(y)) = p^n v_{P'}(y). \tag{2.10}$$

In particular, $p^n \mid -em_P$. Since $gcd(p, m_P) = 1$ by assumption, we have $p^n \mid e$ which implies $e \geq p^n$. Then by the Fundamental Equality we obtain

$$[E : F] \geq e \geq p^n. \tag{2.11}$$

On the other hand, as y is a root of the polynomial $\varphi(t) := a(t) - u \in F[t]$ and $deg(\varphi(t)) = p^n$, we have $[E : F] = [F(y) : F] \leq p^n$. Therefore, $[E : F] = p^n$.

Now we show that the extension E/F is Galois. The rest of the proof of part (a) will be essentially showing the converse of Proposition 2.7. As an immediate consequence of the above argument, $\varphi(t)$ is the minimum polynomial of y over F. For any $\alpha \in W$ we have

$$\begin{aligned} \varphi(y + \alpha) &= a(y + \alpha) - u \\ &= a(y) + a(\alpha) - u \\ &= u + 0 - u = 0. \end{aligned}$$

Then for every $\alpha \in W \subseteq K$ the element $y + \alpha$ is a root of the polynomial $\varphi(t) \in F[t]$. Since $a(t) \in K[t]$ is separable, we see that $ord(W) = p^n$. We also know $deg(\varphi(t)) = p^n$. Hence, these are all the roots of $\varphi(t)$ and $E = F(y)$ is the splitting field of the separable polynomial $\varphi(t)$ over F, i.e. E/F is Galois.

It remains to show that $Gal(F(y)/F)$ is isomorphic to the additive subgroup

$$W = \{\alpha \mid a(\alpha) = 0\}$$

of K. For each $\sigma \in Gal(F(y)/F)$, $\sigma(y)$ is a root of the polynomial $\varphi(t)$. Thus, $\sigma(y) = y + \alpha$ for some $\alpha \in W$. Since α is uniquely determined by σ, we have a bijection

$$\phi\colon Gal(F(y)/F) \;\; \to W, \quad \sigma \;\; \mapsto \alpha.$$

Finally, we show that ϕ is a group homomorphism. Let $\sigma_1, \sigma_2 \in Gal(F(y)/F)$. Then $\sigma_1(y) = y + \alpha_1$ and $\sigma_2(y) = y + \alpha_2$ for some $\alpha_1, \alpha_2 \in W$. Hence, we have

$$(\sigma_1 \circ \sigma_2)(y) = \sigma_1(\sigma_2(y)) = \sigma_1(y + \alpha_2) = \sigma_1(y) + \sigma_1(\alpha_2) = (y + \alpha_1) + \alpha_2.$$

Therefore, ϕ sends $\sigma_1 \circ \sigma_2$ to the sum $\alpha_1 + \alpha_2$. This completes the proof of (a).

(b) Suppose that K is not algebraically closed in E. Then $K' \supsetneq K$, where K' is the constant field of E. Let $[K' : K] =: d$. By [S, Lemma 3.6.2], we have

$$d = [K' : K] = [FK' : F].$$

This implies $[E : FK'] = p^n/d$, as $[E : F] = p^n$. Now by the proof of (a), there exists a place $P \in \mathbb{P}_F$ which is totally ramified in E/F (see (2.11)). Let $P' \in \mathbb{P}_E$ be the extension of P in E. Then

$$e(P'|P) = [E : F] = p^n.$$

Set $P_{FK'} := P' \cap FK'$. Clearly, $P_{FK'}$ is a place of FK'. As FK'/F is a constant field extension, the place P is unramified in FK'/F [S, Theorem 3.6.3(a)], so $e(P_{FK'}|P) = 1$. Then we have

$$e(P'|P) = e(P'|P_{FK'})e(P_{FK'}|P) = e(P'|P_{FK'}),$$

implying that $e(P'|P_{FK'}) = p^n$. This is a contradiction, since $[E : FK'] = p^n/d$ for some $d > 1$ and $e(P'|P_{FK'}) \leq [E : FK']$ by the Fundamental Equality. Hence K is also the constant field of E.

(c) We already know that the poles of u are totally ramified in E/F (see the proof of (a)). Suppose that $P \in \mathbb{P}_F$ is not a pole of u, so $v_P(u) \geq 0$, i.e. $u \in \mathcal{O}_P$, where $\mathcal{O}_P$ denotes the valuation ring of P. We also know

$$a(t) = t^{p^n} + c_{n-1}t^{p^{n-1}} + \ldots + c_1 t^p + c_0 t \in K[t] \subseteq \mathcal{O}_P[t],$$

which implies that

$$\varphi(t) = a(t) - u \in \mathcal{O}_P[t].$$

Then by [S, Theorem 3.5.10(a)], for every extension P' of P in E we have

$$0 \leq d(P'|P) \leq v_{P'}(\varphi'(y)) = v_{P'}(c_0) = 0.$$

Hence, $d(P'|P) = 0$. Therefore, $e(P'|P) = 1$ for each $P' \in \mathbb{P}_E$ lying over P, i.e. P is unramified.

(d) Let $x \in F$ be a prime element at the place P. Since P is totally ramified in E/F, we have

$$v_{P'}(x) = e(P'|P)v_P(x) = p^n,$$

where P' is the extension of P in E. We want to find a prime element at the place P'. Using (2.10), we see that $v_{P'}(y) = -m_P$. By assumption $gcd(p, m_P) = 1$. Then also $gcd(p^n, m_P) = 1$, and so we can find integers $i, j \geq 0$ such that

$$1 = ip^n - jm_P.$$

We define $z := x^i y^j$. Then we have

$$\begin{aligned} v_{P'}(z) &= i v_{P'}(x) + j v_{P'}(y) \\ &= i p^n - j m_P = 1, \end{aligned}$$

i.e. z is a prime element at the place $P' \in \mathbb{P}_E$. Hence, by [S, Proposition 3.5.12]

$$E = F(z) \quad \text{and} \quad d(P'|P) = v_{P'}(\psi'(z)),$$

where $\psi(t) \in F[t]$ is the minimal polynomial of z over F. We have

$$\psi(t) = \prod_{\sigma \in G} (t - \sigma(z)),$$

with $G := Gal(E/F)$. Let us define a polynomial $h(t) := \prod_{\sigma \neq id} (t - \sigma(z)) \in E[t]$. Trivially, $\psi(t) = (t - z)h(t)$. Then $\psi'(t) = h(t) + (t - z)h'(t)$, implying that

$$\psi'(z) = h(z) = \prod_{\sigma \neq id} (z - \sigma(z)).$$

Therefore,

$$d(P'|P) = v_{P'}(\psi'(z)) = v_{P'}(\prod_{\sigma \neq id} (z - \sigma(z))) = \sum_{\sigma \neq id} v_{P'}(z - \sigma(z)).$$

Now we show that

$$v_{P'}(z - \sigma(z)) = m_P + 1$$

for all $id \neq \sigma \in G$. Let $\sigma_0 \in G \setminus \{id\}$. Then $\sigma_0(y) = y + \alpha$ for some $\alpha \in W \setminus \{0\}$. So

$$\begin{aligned} z - \sigma_0(z) &= x^i y^j - x^i (\sigma_0(y))^j \qquad (\text{ since}\, x \in F\ ) \\ &= x^i y^j - x^i (y + \alpha)^j \\ &= x^i y^j - x^i \sum_{k=0}^{j} \binom{j}{k} y^{j-k} \alpha^k \\ &= -x^i \sum_{k=1}^{j} \binom{j}{k} y^{j-k} \alpha^k . \end{aligned}$$

Since $v_{P'}(y) = -m_P < 0$, the strict triangle inequality gives

$$v_{P'}(y^{j-1}) < v_{P'}(y^{j-k})$$

for $k > 1$. Moreover, note that $\binom{j}{1} = j \neq 0$ in the constant field K (since $ip^n - jm_P = 1$) and again α is a nonzero element of K by assumption. Then we obtain

$$\begin{aligned} v_{P'}(z - \sigma_0(z)) &= v_{P'}\left(-x^i \sum_{k=1}^{j} \binom{j}{k} y^{j-k} \alpha^k \right) \\ &= v_{P'}(x^i) + v_{P'}\left(\binom{j}{1} \alpha y^{j-1} \right) \\ &= v_{P'}(x^i) + v_{P'}(y^{j-1}) \\ &= ip^n + (j-1)(-m_P) \\ &= (ip^n - jm_P) + m_P = 1 + m_P. \end{aligned}$$

Hence, we conclude that

$$d(P'|P) = \sum_{\sigma \neq id} v_{P'}(z - \sigma(z)) = (p^n - 1)(m_P + 1),$$

as $ord(G \setminus \{id\}) = p^n - 1$.

(e) We have proved that a place $P \in \mathbb{P}_F$ is either unramified in E/F, in which case $d(P'|P) = 0$, or totally ramified in the extension E/F. We have also proved in (d) that if $P \in \mathbb{P}_F$ is totally ramified in E/F, then

$$d(P'|P) = (p^n - 1)(m_P + 1).$$

Furthermore, since the constant field of E is K by (b), the Hurwitz Genus Formula yields

$$\begin{aligned} 2g(E) - 2 &= [E : F](2g(F) - 2) + \sum_{P \in \mathbb{P}_F} \sum_{P'|P} d(P'|P) degP' \\ &= p^n(2g(F) - 2) + \sum_{\substack{v_P(u)<0, \\ P \in \mathbb{P}_F}} (p^n - 1)(m_P + 1) degP' \end{aligned}$$

or equivalently

$$g(E) = p^n g(F) + \frac{p^n - 1}{2}(-2 + \sum_{\substack{v_P(u)<0, \\ P \in \mathbb{P}_F}} (m_P + 1) degP').$$

Finally, let P be a place of F with $v_P(u) < 0$. Then since P is totally ramified in E/F, using the Fundamental Equality we obtain

$$degP' = [F_{P'} : K] = [F_{P'} : F_P][F_P : K] = 1degP = degP,$$

where P' is the extension of P in E (here $F_{P'}$ and F_P denote the residue class fields of P' and P, respectively). This finishes the poof of (e). □

There is a more general way to compute the genus of an elementary abelian p-extension of a function field, which uses the genera of some intermediate fields. Before showing this, we need a lemma.

Lemma 2.9. *Let E/F be an elementary abelian p-extension of degree p^n. Then the number of intermediate fields $F \subseteq L \subseteq E$ with $[L : F] = p$ is $\frac{p^n-1}{p-1}$.*

Proof. Since the extension E/F is Galois, there is a one to one correspondence between the intermediate fields $F \subseteq L \subseteq E$ with $[L : F] = p$ and the subgroups of $Gal(E/F)$ of order p^{n-1}. Because $Gal(E/F)$ is an elementary abelian group of order p^n, we can regard it as a vector space over $\mathbb{F}_p$ of dimension n. Hence the number of $n-1$ dimensional subspaces of $Gal(E/F)$ will give the desired number, which is well-known:

$$\frac{(p^n - 1)(p^n - p)\ldots(p^n - p^{(n-1)-1})}{(p^{n-1} - 1)(p^{n-1} - p)\ldots(p^{n-1} - p^{(n-1)-1})}, \tag{2.12}$$

After cancellations we see (2.12) is equal to $\frac{p^n-1}{p-1}$, and this completes the proof. □

Theorem 2.10. *Let F/K be an algebraic function field with constant field K, and let E be an elementary abelian p-extension of $F$of degree p^n with the same constant field. Assume that $E_1, \dots, E_t$ are the intermediate fields $F \subseteq E_i \subseteq E$ with $[E_i : F] = p$, $1 \leq i \leq t$ (here $t = \frac{p^n-1}{p-1}$ by Lemma 2.9). Then the genus $g(E)$ of E is given by*

$$g(E) = \sum_{i=1}^{t} g(E_i) - \frac{p}{p-1}(p^{n-1} - 1)g(F).$$

The proof of Theorem 2.10 is due to Garcia and Stichtenoth [GS]. It depends heavily on the following fact which can be found in [K, Theorem 1].

Theorem 2.11. *Suppose that we have a relation*

$$\sum_{H \subseteq G} r_H \varepsilon_H = 0 \in \mathbb{Q}[G],$$

where $G := Gal(E/F)$ and $\varepsilon_H := \frac{1}{ord(H)} \sum_{\sigma \in H} \sigma \in \mathbb{Q}[G]$ for any subgroup $H \subseteq G$. Then the same relation exists between the genera. More precisely,

$$\sum_{H \subseteq G} r_H g(E_H) = 0,$$

where E_H is the fixed field of the subgroup $H \subseteq G$ and $g(E_H)$ is the genus of E_H.

Now we can prove Theorem 2.10.

Proof of Theorem 2.10. Let $H_i := Gal(E/E_i)$, $1 \leq i \leq t$, i.e. H_i is the subgroup of $Gal(E/F)$ corresponding to the intermediate field E_i. We choose a non-identity element σ of $Gal(E/F)$, and we claim that σ is contained in exactly $\frac{p^{n-1}-1}{p-1}$ of the subgroups H_i. Observe that $Gal(E/F)/\langle\sigma\rangle$ is a vector space over $\mathbb{F}_p$ of

$$\dim(Gal(E/F)/\langle\sigma\rangle) = \dim(Gal(E/F)) - \dim(\langle\sigma\rangle) = n - 1.$$

By the same method which we used in (2.12), we see that $Gal(E/F)/\langle\sigma\rangle$ has $\frac{p^{n-1}-1}{p-1}$ subspaces of dimension $n-2$. This means that $Gal(E/F)$ has precisely $\frac{p^{n-1}-1}{p-1}$ subspaces of dimension $n-1$ containing σ, or equivalently, among the $\frac{p^n-1}{p-1}$ subgroups of $Gal(E/F)$ having order p^{n-1} (namely H_i's), $\frac{p^{n-1}-1}{p-1}$ subgroups contain σ. This proves the claim. Clearly, $id \in H_i$ for all $1 \leq i \leq t$. Let us also denote $G := Gal(E/F)$. Then we have

$$\begin{aligned}
p^{n-1} \cdot \sum_{i=1}^{t} \varepsilon_{H_i} &= \sum_{i=1}^{t} \sum_{\sigma \in H_i} \sigma \\
&= (\frac{p^n-1}{p-1}) \cdot id + (\frac{p^{n-1}-1}{p-1}) \cdot \sum_{\sigma \in G \setminus \{id\}} \sigma \\
&= (\frac{p^n-1}{p-1} - \frac{p^{n-1}-1}{p-1}) \cdot id + (\frac{p^{n-1}-1}{p-1}) \cdot \sum_{\sigma \in G} \sigma \\
&= (\frac{p^n - p^{n-1}}{p-1}) \cdot id + (\frac{p^{n-1}-1}{p-1}) p^n \cdot \varepsilon_G.
\end{aligned}$$

Dividing the equations above by p^{n-1}, we obtain

$$\sum_{i=1}^{t} \varepsilon_{H_i} = (\frac{p-1}{p-1}) \cdot id + \frac{p}{p-1}(p^{n-1}-1) \cdot \varepsilon_G. \tag{2.13}$$

Since $id = \varepsilon_{\{id\}}$, (2.13) is equivalent to

$$\varepsilon_{\{id\}} = \sum_{i=1}^{t} \varepsilon_{H_i} - \frac{p}{p-1}(p^{n-1}-1) \cdot \varepsilon_G.$$

Then by Theorem 2.11, we conclude

$$g(E) = \sum_{i=1}^{t} g(E_i) - \frac{p}{p-1}(p^{n-1}-1) g(F).$$

□

3

Hasse-Arf Theorem for Elementary Abelian p-Extensions

Let E/F be a finite Galois extension of algebraic function fields, and let the characteristic of F be $p > 0$, as usual. In this section, we will introduce the higher ramification groups, and then we will prove the Hasse-Arf Theorem in the particular case where $Gal(E/F)$ is an elementary abelian p-group.

Definition 3.1. Let F and E be as above. Suppose that P is a place of F and P' is an extension of P in E. Then for every $i \geq -1$, the *i-th ramification group* of the extension $P'|P$ is defined to be

$$G_i(P'|P) := \{\sigma \in G \mid v_{P'}(\sigma(z) - z) \geq i + 1 \text{ for all } z \in \mathcal{O}_{P'}\},$$

where $G := Gal(E/F)$ and $\mathcal{O}_{P'}$ is the valuation ring of the place P'.

Indeed, $G_i(P'|P)$ is a subgroup of G. To see this, let $\sigma_1, \sigma_2 \in G_i(P'|P)$ and $z \in \mathcal{O}_{P'}$. Then by the triangle equality we have

$$\begin{aligned} v_{P'}((\sigma_1 \circ \sigma_2)(z) - z) &= v_{P'}(\sigma_1(\sigma_2(z)) - \sigma_2(z) + \sigma_2(z) - z) \\ &\geq \min\{v_{P'}(\sigma_1(\sigma_2(z)) - \sigma_2(z)), v_{P'}(\sigma_2(z) - z)\} \\ &\geq i + 1, \end{aligned}$$

as both $v_{P'}(\sigma_1(\sigma_2(z)) - \sigma_2(z)) \geq i+1$ and $v_{P'}(\sigma_2(z) - z) \geq i+1$. So $\sigma_1 \circ \sigma_2 \in G_i(P'|P)$. Note that, here we have also used that $\sigma_2(z) \in \mathcal{O}_{P'}$ for any $z \in \mathcal{O}_{P'}$.

Denote by $G_i := G_i(P'|P)$ the i-th ramification group of the extension $P'|P$. It is easy to see that G_i's form a decreasing sequence

$$G \supseteq G_0 \supseteq G_1 \supseteq G_2 \supseteq \dots \tag{3.1}$$

of subgroups of G and $G_m = \{id\}$ for m big enough.

The next result shows that this sequence helps to understand the structure of G. For a proof, see [S, Proposition 3.5.8].

Proposition 3.2. *With the notation as above we have:*

(*a*) *$ord(G_0) = e(P'|P)$ and G_1 is a normal subgroup of G_0. Further, G_1 is a p-group and G_0/G_1 is cyclic of order relatively prime to p.*

(*b*) *For all $i \geq 1$, G_{i+1} is a normal subgroup of G_i and G_i/G_{i+1} is an elementary abelian p-group.*

Before stating the famous Hasse-Arf Theorem, we will give a definition.

Definition 3.3. Let $s \geq 0$ be an integer. We call s a *jump* of the extension $P'|P$ if $G_s \supsetneq G_{s+1}$.

Theorem 3.4. *(Hasse-Arf Theorem). Assume G is an abelian p-group and maintain the other notation as above. Let $P'|P$ be totally ramified, and let $s < t$ be two subsequent jumps of $P'|P$, which means that*

$$G_s \supsetneq G_{s+1} = \ldots = G_t \supsetneq G_{t+1}.$$

Then we have

$$t \equiv s \pmod{(G : G_t)}.$$

A proof of Theorem 3.4, due to Arf in a general case, can be found in [A]. The rest of the section is devoted to the proof of Theorem 3.4 in the particular case where G is an elementary abelian p-group. The proof is due to Garcia and Stichtenoth [GaSt]. It only uses the following well-known facts.

Corollary 3.5. *(Transitivity of the Different Exponents) [S, Corollary 3.4.12]. Let $L \supseteq E \supseteq F$ be a tower of finite separable function field extensions. Suppose that $P'' \supseteq P' \supseteq P$ are places of L, E and F, respectively. Then*

$$d(P''|P) = e(P''|P')d(P'|P) + d(P''|P').$$

Theorem 3.6. *(Hilbert's Different Formula) [S, Theorem 3.8.7]. As before, E/F is a finite Galois extension of algebraic function fields and $P' \in \mathbb{P}_E$ is an extension of the place $P \in \mathbb{P}_F$ in E. Then we have*

$$d(P'|P) = \sum_{i=0}^{\infty}(ord(G_i(P'|P)) - 1).$$

Note that for an unramified place P of F, we have $G_0 = \{id\}$ by Proposition 3.2(a). Therefore, $G_i = \{id\}$ for all $i \geq 0$ in this case. If a place $P \in \mathbb{P}_F$ is totally ramified, then by Proposition 3.2(a), (3.1) becomes

$$G = G_0 = G_1 \supseteq G_2 \supseteq G_3 \supseteq \ldots.$$

Now we state Hasse-Arf Theorem in the case we will prove.

Theorem 3.7. *Assume that G is an an elementary abelian p-group and maintain the other notation as above. Let $P'|P$ be totally ramified, and let $s < t$ be two subsequent jumps of $P'|P$. Then we have*

$$t \equiv s \pmod{(G : G_t)}.$$

Proof. Let $s_1, \ldots, s_m$ denote all jumps of the extension $P'|P$ in order. Then

$$0 < s_1 < \ldots < s_m$$

and $G_i = \{id\}$ for all $i > s_m$. We show by induction that

$$s_{n+1} \equiv s_n \pmod{(G : G_{s_{n+1}})}$$

for all $1 \le n \le m-1$. For $n = 1$, we have

$$G = G_0 = G_1 = \ldots = G_{s_1} \supsetneq G_{s_1+1} = \ldots = G_{s_2} \supsetneq G_{s_2+1} \supseteq \ldots .$$

Since G is an elementary abelian p-group, we can consider it as a vector space over $\mathbb{F}_p$; then so is the quotient G/G_{s_2+1}. Clearly, G_{s_2}/G_{s_2+1} is a subspace of G/G_{s_2+1}. Then there exists a subspace H of G such that

$$G/G_{s_2+1} = (G_{s_2}/G_{s_2+1}) \oplus (H/G_{s_2+1}).$$

It is easy to see that, H, regarded as a subgroup of G, satisfies the following equalities:

$$G_{s_2+1} \subseteq H \subseteq G, \qquad H \cap G_{s_2} = G_{s_2+1}, \qquad ord(H) = ord(G_{s_2+1})(G : G_{s_2}). \tag{3.2}$$

Let E_H be the fixed field of H and $Q := P' \cap E_H$. By definition of ramification groups, we have

$$G_i(P'|Q) = H \cap G_i(P'|P) = H \cap G_i$$

for all $i \ge 0$. Then Hilbert's Different Formula yields

$$d(P'|P) = (s_1+1)(ord(G)-1) + (s_2 - s_1)(ord(G_{s_2})-1) + \sum_{k>s_2}(ord(G_k)-1).$$

Similarly, we have

$$\begin{aligned} d(P'|Q) &= (s_1+1)(ord(H \cap G)-1) + (s_2-s_1)(ord(H \cap G_{s_2})-1) \\ &\quad + \sum_{k>s_2}(ord(H \cap G_k)-1) \\ &= (s_1+1)(ord(H)-1) + (s_2-s_1)(ord(G_{s_2+1})-1) \\ &\quad + \sum_{k>s_2}(ord(G_k)-1). \end{aligned}$$

By the transitivity of different exponents, we conclude

$$\begin{aligned} d(P'|P) - d(P'|Q) &= e(P'|Q)d(Q|P) \\ &= ord(H)d(Q|P) \equiv 0 \pmod{ord(H)}. \end{aligned}$$

Here we have also used the fact that $Q \in \mathbb{P}_{E_H}$ is totally ramified in E, which is a consequence of the total ramification of the place P in E. Then subtracting the above equations we obtain

$$(s_1 - s_2)(ord(G_{s_2}) - ord(G_{s_2+1})) \equiv (s_1 + 1)(ord(G) - ord(H)) \pmod{ord(H)},$$

which implies

$$(s_1 - s_2)(ord(G_{s_2}) - ord(G_{s_2+1})) \equiv 0 \ (\mathrm{mod}\ ord(H)). \tag{3.3}$$

Clearly, (3.3) is equivalent to

$$(s_1 - s_2)ord(G_{s_2+1})((G_{s_2} : G_{s_2+1}) - 1) \equiv 0 \ (\mathrm{mod}\ ord(H)). \tag{3.4}$$

By (3.2), we know that $ord(H) = ord(G_{s_2+1})(G : G_{s_2})$, so (3.4) becomes

$$(s_1 - s_2)((G_{s_2} : G_{s_2+1}) - 1) \equiv 0 \ (\mathrm{mod}\ (G : G_{s_2})).$$

Finally, since $(G_{s_2} : G_{s_2+1}) - 1$ and $(G : G_{s_2})$ are relatively prime, we obtain

$$s_1 - s_2 \equiv 0 \ (\mathrm{mod}\ (G : G_{s_2})).$$

Hence, the proof of the first step is complete. Now suppose that $1 < n \leq m - 1$ and

$$s_{j+1} \equiv s_j \ (\mathrm{mod}\ (G : G_{s_{j+1}})) \tag{3.5}$$

for all $1 \leq j < n$. We will show

$$s_{n+1} \equiv s_n \ (\mathrm{mod}\ (G : G_{s_{n+1}})).$$

For convenience, let $s := s_n$ and $t := s_{n+1}$. Then we have the sequence

$$G = G_0 = G_1 \supseteq \ldots \supseteq G_s \supsetneq G_{s+1} = \ldots = G_t \supsetneq G_{t+1} \supseteq \ldots .$$

By exactly the same method as in the proof of the first step, we can find a subgroup $K \subseteq G$ such that

$$G_{t+1} \subseteq K \subseteq G, \quad K \cap G_t = G_{t+1}, \quad ord(K) = ord(G_{t+1})(G : G_t). \tag{3.6}$$

Let E_K be the fixed field of K and $Q_1 := P' \cap E_K$ be the restriction of P' to E_K. Using Hilbert's Different Formula we obtain

$$\begin{aligned} d(P'|P) = (s_1 + 1)(ord(G) - 1) + \sum_{j=1}^{n-1}(s_{j+1} - s_j)(ord(G_{s_{j+1}}) - 1) \\ + (t - s)(ord(G_t) - 1) + \sum_{l>t}(ord(G_l) - 1), \end{aligned}$$

and also as $G_i(P'|Q_1) = K \cap G_i$,

$$d(P'|Q_1) = (s_1+1)(ord(K)-1) + \sum_{j=1}^{n-1}(s_{j+1}-s_j)(ord(K \cap G_{s_{j+1}})-1)$$
$$+ (t-s)(ord(G_{t+1})-1) + \sum_{l>t}(ord(G_l)-1).$$

Since $d(P'|P) - d(P'|Q_1) = e(P'|Q_1)d(Q_1|P) = ord(K)d(Q_1|P)$, taking the difference of the two equations we conclude

$$(s-t)(ord(G_t) - ord(G_{t+1})) \equiv \sum_{j=1}^{n-1}(s_{j+1}-s_j)(ord(G_{s_{j+1}}) - ord(K \cap G_{s_{j+1}})) \quad (3.7)$$

modulo $ord(K)$. Now by induction hypothesis, for every j with $1 \leq j < n$ there exists some $c_j \in \mathbb{Z}$ such that

$$s_{j+1} - s_j = c_j(G : G_{s_{j+1}}).$$

Then we have

$$(s_{j+1}-s_j)ord(G_{s_{j+1}}) = c_j(G : G_{s_{j+1}})ord(G_{s_{j+1}}) = c_j ord(G)$$

and

$$\begin{aligned}(s_{j+1}-s_j)ord(K \cap G_{s_{j+1}}) &= c_j(G : G_{s_{j+1}})ord(K \cap G_{s_{j+1}}) \\ &= c_j(G : G_{s_{j+1}})\frac{ord(K)ord(G_{s_{j+1}})}{ord(K \cdot G_{s_{j+1}})} \\ &= c_j\frac{ord(G)}{ord(K \cdot G_{s_{j+1}})}ord(K).\end{aligned}$$

This implies

$$\sum_{j=1}^{n-1}(s_{j+1}-s_j)(ord(G_{s_{j+1}}) - ord(K \cap G_{s_{j+1}})) \equiv 0 \pmod{ord(K)}.$$

So we conclude from (3.7) that

$$(s-t)(ord(G_t) - ord(G_{t+1})) \equiv 0 \pmod{ord(K)}. \quad (3.8)$$

In what follows, we will just repeat the argument which we used in the proof of the first step. By (3.8), we have

$$(s-t)ord(G_{t+1})((G_t : G_{t+1}) - 1) \equiv 0 \pmod{ord(K)}.$$

Since $ord(K) = ord(G_{t+1})(G : G_t)$ by (3.6), we have

$$(s-t)((G_t : G_{t+1}) - 1) \equiv 0 \pmod{(G : G_t)},$$

and this completes the proof, as $(G_t : G_{t+1}) - 1$ and $(G : G_t)$ are relatively prime. □

More generally, let the extension $P'|P$ be ramified (not necessarily totally ramified). We consider the fixed field E_{G_0} of G_0. Let $P_1 := P' \cap E_{G_0}$. Then $P_1 \in \mathbb{P}_{E_{G_0}}$ is totally ramified in E [S, Theorem 3.8.2], and $G_i(P'|P_1) = G_i(P'|P)$ for all $i \geq 0$, by definition of ramification groups. Hence, by the argument used in proving Theorem 3.7, we obtain

$$t \equiv s \pmod{(G_0 : G_t)},$$

where $s < t$ are two subsequent jumps of $P'|P$.

4

Asymptotic Theory of Elementary Abelian p-Extensions

Let $\mathbb{F}_q$ be a finite field with $q = p^s$ elements, where s is a positive integer, and let $F/\mathbb{F}_q$ be an algebraic function field with constant field $\mathbb{F}_q$. Function fields over finite fields is a subject of interest, not only due to theoretical reasons but also due to their relation to coding theory. One of the central problems is the number of rational places. This number is bounded by the celebrated Hasse-Weil bound ([S, Theorem 5.2.3]), although the bound is big when the genus is big. Moreover, again partly due to coding theoretic reasons, the growth of the number of rational places relative to genus in an infinite sequence of function fields over finite fields (of growing genera) is of interest too. When this ratio for a given sequence has a positive limit, the sequence said to be asymptotically good.

Suppose that E_i/F are abelian extensions with

$$F \subseteq E_1 \subseteq E_2 \subseteq \ldots,$$

and $\mathbb{F}_q$ is the constant field of each $E_i, i \geq 1$, as well. The aim of this section is to show that the genus of E_i increases much faster than the number of its rational places as $[E_i : F]$ goes to infinity, which is a disappointing result. The proof of this fact will use Hasse-Arf Theorem. Since we proved Hasse-Arf for elementary abelian p-extensions, we will formulate the results only for such extensions. The general (abelian) case can be seen in [FPS].

In the following, we will assume that E/F is an extension of function fields with Galois group $G = Gal(E/F)$ an elementary abelian p-group. Let P be a place of $F/\mathbb{F}_q$, and let P' be the only place of $E/\mathbb{F}_q$ lying over P. Moreover, let $F_P := \mathcal{O}_P/P$ and $E_{P'} := \mathcal{O}_{P'}/P'$ denote the residue class fields of P and P', respectively.

Lemma 4.1. *Under the above assumptions we have:*

(a) *The field extension $E_{P'}/F_P$ is Galois.*

(b) *Every $\sigma \in G$ induces an automorphism $\bar{\sigma}$ of $E_{P'}/F_P$ given by*

$$\bar{\sigma}(x + P') = \sigma(x) + P',$$

where $x + P' \in \mathcal{O}_{P'}/P' = E_{P'}$, and each automorphism of $E_{P'}/F_P$ arises in this way.

Note that the above lemma holds even the constant field is not finite. For a proof, see [S, Theorem 3.8.2].

Now we consider the factor groups $(P')^i/(P')^{i+1}, i \geq 1$. We have the following lemma.

Lemma 4.2. *For each $i \geq 1$, the factor group $(P')^i/(P')^{i+1}$ is a vector space over $E_{P'}$ via the multiplication*

$$(x + P')(a + (P')^{i+1}) := xa + (P')^{i+1},$$

where $x \in \mathcal{O}_{P'}$, $a \in (P')^i$. The dimension of $(P')^i/(P')^{i+1}$ over $E_{P'}$ is one.

Proof. It is straightforward to show that the scalar multiplication is well-defined and $(P')^i/(P')^{i+1}$ is an $E_{P'}$-vector space.

In order to prove $(P')^i/(P')^{i+1}$ is a one-dimensional vector space over $E_{P'}$, we choose a nonzero element $a + (P')^{i+1} \in (P')^i/(P')^{i+1}$. So $a \in (P')^i \setminus (P')^{i+1}$. Let π be a prime element at the place P'. Then by [S, Theorem 1.1.6(b)], $a = \pi^i u$ for some unit $u \in (\mathcal{O}_{P'})^*$. Now let $y + (P')^{i+1} \in (P')^i/(P')^{i+1}$ be an arbitrary element. We can assume $y \neq 0$. Then $y = \pi^j v$ for some $j \geq i$ and $v \in (\mathcal{O}_{P'})^*$. Hence, we have

$$\begin{aligned} y + (P')^{i+1} &= \pi^j v + (P')^{i+1} \\ &= (\pi^{j-i} v u^{-1} + P')(\pi^i u + (P')^{i+1}) \\ &= (\pi^{j-i} v u^{-1} + P')(a + (P')^{i+1}). \end{aligned}$$

As $v_{P'}(\pi^{j-i} v u^{-1}) = j - i \geq 0$, we conclude that $\pi^{j-i} v u^{-1} + P' \in \mathcal{O}_{P'}/P' = E_{P'}$, and the result follows. □

Define a map from $G \times (P')^i/(P')^{i+1}$ to $(P')^i/(P')^{i+1}$ by

$$(\sigma, a + (P')^{i+1}) \mapsto \sigma(a) + (P')^{i+1} =: \sigma(a + (P')^{i+1}). \qquad (4.1)$$

As P is a place of F and $\sigma \in G = Gal(E/F)$, we have $\sigma(P) = P$. Then $\sigma(P')$ is a place of E lying over P. By assumption P' is the only place of E lying over P. Hence, $\sigma(P') = P'$ and (4.1) makes sense. For $i \geq 1$, we set

$$X_i := \{a + (P')^{i+1} \in (P')^i/(P')^{i+1} \mid \sigma(a + (P')^{i+1}) = a + (P')^{i+1} \text{ for all } \sigma \in G\}.$$

It is easy to check that X_i is an F_P-subspace of $(P')^i/(P')^{i+1}$.

Proposition 4.3. *X_i as a vector space over F_P has dimension at most one.*

Proof. Suppose that $X_i \neq \{0\}$ and choose an element $0 \neq a + (P')^{i+1} \in X_i$. Then by Lemma 4.2, for every $a_1 + (P')^{i+1} \in X_i$ there exists some $c \in \mathcal{O}_{P'}$ such that

$$a_1 + (P')^{i+1} = (c + P')(a + (P')^{i+1}).$$

We need to show that $c + P' \in F_P$. Let $\sigma \in G$. Then

$$\begin{aligned}(c+P')(a+(P')^{i+1}) &= a_1 + (P')^{i+1} \\ &= \sigma(a_1 + (P')^{i+1}) \\ &= \sigma((c+P')(a+(P')^{i+1})) \\ &= \sigma(ca + (P')^{i+1}) \\ &= \sigma(ca) + (P')^{i+1} \\ &= \sigma(c)\sigma(a) + (P')^{i+1} \\ &= (\sigma(c)+P')(\sigma(a)+(P')^{i+1}) \\ &= \bar{\sigma}(c+P')\sigma(a+(P')^{i+1}) \\ &= \bar{\sigma}(c+P')(a+(P')^{i+1}).\end{aligned}$$

Hence, $\bar{\sigma}(c+P') = c+P'$ for all $\sigma \in G$. So using Lemma 4.1 we can conclude $c+P' \in E_{P'}$ is invariant under the automorphisms of $E_{P'}/F_P$, and this implies $c + P' \in F_P$. □

Next we consider the map

$$\begin{aligned}\psi\colon G_0 &\to (E_{P'})^* \\ \sigma &\mapsto \frac{\sigma(\pi)}{\pi} + P',\end{aligned}$$

and for $i \geq 1$, the maps

$$\begin{aligned}\varphi_i\colon G_i &\to (P')^i/(P')^{i+1} \\ \sigma &\mapsto \frac{\sigma(\pi)}{\pi} - 1 + (P')^{i+1},\end{aligned}$$

where π is a prime element at the place P' and $G_0, G_1, \ldots$ are defined as in Section 3. Then ψ is a well-defined homomorphism from G_0 to the multiplicative group of $E_{P'}$ with kernel G_1. In particular, it is independent of the choice of the prime element. For details we refer to [S, Proposition 3.8.5]. With a slight adjustment of the proof of [S, Proposition 3.8.5], one can also show that φ_i is a homomorphism from G_i to the additive group of $(P')^i/(P')^{i+1}$ and $ker(\varphi_i) = G_{i+1}$. We omit the proof.

Proposition 4.4. *With the notation above, we have:*

(a) The image of ψ is contained in $(F_P)^*$.

(b) For all $i \geq 1$, $Im(\varphi_i) \subseteq X_i$.

Proof. For the proof of (a), see [FPS, Proposition 2]. The proof of (b) is similar to that of (a). Let $a + (P')^{i+1} \in Im(\varphi_i)$ with $i \geq 1$. Then $a + (P')^{i+1} = \varphi_i(\tau)$ for some $\tau \in G_i$.

Thus, for all $\sigma \in G$ we obtain

$$\begin{aligned}
\sigma(a + (P')^{i+1}) &= \sigma(\varphi_i(\tau)) \\
&= \sigma(\frac{\tau(\pi)}{\pi} - 1 + (P')^{i+1}) \\
&= \frac{\sigma(\tau(\pi))}{\sigma(\pi)} - 1 + (P')^{i+1} \\
&= \frac{\tau(\sigma(\pi))}{\sigma(\pi)} - 1 + (P')^{i+1} \qquad \text{(since G is abelian)} \\
&= \varphi_i(\tau) \qquad \text{(because $\sigma(\pi)$ is a prime at P')} \\
&= a + (P')^{i+1},
\end{aligned}$$

which implies $a + (P')^{i+1} \in X_i$. □

Note that the results we obtained till now are valid independent of the finiteness of the constant field. In the following we need a finite constant field.

Corollary 4.5. *Let $e(P'|P)$ be the ramification index of P' over P. Then we have*

$$e(P'|P) \leq (ord(F_P))^r, \tag{4.2}$$

where P, P' and F_P are defined as above, and r is the number of jumps of the extension $P'|P$.

Proof. The field F_P is finite, as F is a function field over a finite field. For $i \geq 0$, let $g_i := ord(G_i)$. We know by Proposition 3.2 that $g_0 = e(P'|P)$. Then since $g_n = 1$ for sufficiently large n, we have

$$e(P'|P) = g_0 = (g_0/g_1)(g_1/g_2)\dots(g_{n-1}/g_n).$$

Now using Proposition 4.4 we see that $g_0/g_1 \leq ord(F_P)$. Since X_i is an F_P vector space with dimension at most one (Proposition 4.3) and $Im(\varphi_i) \subseteq X_i$ (Proposition 4.4), we can also see that $g_i/g_{i+1} \leq ord(F_P)$ for all $1 \leq i \leq n-1$. Moreover, as $g_i/g_{i+1} = 1$ in the case i is not a jump, we obtain (4.2). □

The following proposition, which is due to Frey, Perret and Stichtenoth [FPS], gives an estimate for the different exponent $d(P'|P)$.

Proposition 4.6. *Under the assumptions of this section, we have*

$$d(P'|P) \geq \frac{1}{2} re(P'|P),$$

where r is the number of jumps of $P'|P$.

Proof. Let $0 \leq s_1 < \ldots < s_r$ denote the jumps of $P'|P$, and let $g_i := ord(G_i)$ for $i \geq 0$, as before. Since G is an elementary abelian p-group, for each $1 < i \leq r$ we have

$$(s_i - s_{i-1})g_{s_i} = k_i g_0 \tag{4.3}$$

for some positive integer k_i, by the Hasse-Arf Theorem. As $ord(G_0) = g_0 = e(P'|P)$, (4.3) becomes

$$(s_i - s_{i-1})g_{s_i} = k_i e(P'|P), \tag{4.4}$$

where $k_i \in \mathbb{Z}^+$ and $1 < i \leq r$. Then using Hilbert's Different Formula we obtain

$$\begin{aligned}
d(P'|P) &= \sum_{i=0}^{\infty}(g_i - 1) \\
&= \sum_{i=0}^{s_1}(g_i - 1) + \sum_{i=s_1+1}^{\infty}(g_i - 1) \\
&= (s_1 + 1)(g_{s_1} - 1) + \sum_{j=2}^{r}(s_j - s_{j-1})(g_{s_j} - 1) \\
&= (s_1 + 1)g_{s_1}(1 - g_{s_1}^{-1}) + \sum_{j=2}^{r}(s_j - s_{j-1})g_{s_j}(1 - g_{s_j}^{-1}) \\
&= (s_1 + 1)e(P'|P)(1 - g_{s_1}^{-1}) + \sum_{j=2}^{r}k_j e(P'|P)(1 - g_{s_j}^{-1}) \qquad \text{(by (4.4))} \\
&\geq \frac{1}{2}re(P|P').
\end{aligned}$$

In the last inequality we used the fact that $g_{s_i} > 1$ for all $1 \leq i \leq r$, as s_i is a jump. □

Note that Proposition 4.6 remains true in the case P' is not the only extension of the place P.

Now we consider the ramification group

$$G_0(P_i|P) = \{\sigma \in G \mid v_{P_i}(\sigma(z) - z) \geq 1 \text{ for all } z \in \mathcal{O}_{P_i}\},$$

where P_i is one of the extensions of P in E. Let $g(P)$ be the number of places lying over P. Since E/F is a Galois extension, for each $j = 1, \ldots, g(P)$ there exists an automorphism $\sigma \in G$ such that $P_j = \sigma(P_i)$. Then as G is abelian, we conclude that $G_0(P) := G_0(P_i|P)$ is independent of the choice of the extension P_i. Here we have used $G_0(\tau(P_i)|P) = \tau^{-1}G_0(P_i|P)\tau$ for all $\tau \in G$ [S, p.130]. Let T_P be the fixed field of $G_0(P)$. Then T_P is the maximal subextension of F where P is unramified [S, Theorem 3.8.3(c)]. Therefore, the field $M := \cap_{P \in \mathcal{S}} T_P$ is the maximal unramified subextension of F, where $\mathcal{S}$ denotes the set of ramified places of F in E/F. Note that $\mathcal{S}$ is a finite set (for a proof see [S, Corollary 3.5.5]).

Lemma 4.7. *With the notations above, we have*

$$\sum_{P\in\mathcal{S}} log_q e(P) \geq log_q[E:F] - log_q[M:F].$$

Proof. The subgroup corresponding to intermediate field M is $Gal(E/M) = \prod_{P\in\mathcal{S}} G_0(P)$, which is the subgroup generated by all $G_0(P)$'s with $P \in \mathcal{S}$. Then since G is abelian and $ord(G_0(P)) = e(P)$ for all $P \in \mathcal{S}$, we have

$$[E:M] = ord(Gal(E/M)) \leq \prod_{P\in\mathcal{S}} ord(G_0(P)) = \prod_{P\in\mathcal{S}} e(P).$$

Finally, as $[E:M] = [E:F]/[M:F]$, by taking logarithms we obtain the desired inequality. □

We can now prove an important estimate for the degree of the different Diff(E/F).

Theorem 4.8. *Let E/F be an elementary abelian p-extension of function fields having the same constant field $\mathbb{F}_q$, and let $F \subseteq M \subseteq E$ be the maximal unramified subextension. Then the degree of the different Diff(E/F) satisfies*

$$deg(Diff(E/F)) \geq \frac{1}{2}[E:F](log_q[E:F] - log_q[M:F]).$$

Proof. Let P be a place of F, and let us consider the group $G_{-1}(P'|P)$, where P' is an extension of P in E. It is easy to show that

$$G_{-1}(P'|P) = \{\sigma \in G \mid \sigma(P') = P'\}.$$

Clearly, $G_{-1}(P'|P) \subseteq G_0(P)$. Similar to $G_0(P)$, it is independent of the choice of the extension P'. Let Z_P be the fixed field of $G_{-1}(P) := G_{-1}(P'|P)$, and let $P_Z := P' \cap Z_P$. Then the place P_Z of Z_P has only one extension in E.

Using Hilbert's Different Formula we see that

$$d(P'|P) = \sum_{i=0}^{\infty}(ord(G_i(P'|P)) - 1) = d(P'|P_Z). \tag{4.5}$$

Moreover,

$$e(P'|P) = e(P'|P_Z) \quad \text{and} \quad f(P'|P) = f(P'|P_Z), \tag{4.6}$$

since $e(P_Z|P) = f(P_Z|P) = 1$ [S, Theorem 3.8.2]. Now let $\mathcal{S}$ denotes the set of ramified place of F in E, and let $r(P)$ be the number of jumps for $P'|P$. Note that $d(P) := d(P'|P) = d(P''|P)$ for any two places $P', P'' \in \mathbb{P}_E$ lying over P, since the extension E/F is Galois [S, Corollary 3.7.2(c)]. Then we have

$$\begin{aligned}
deg(\text{Diff}(E/F)) &= \sum_{P\in\mathcal{S}}\sum_{P'|P} d(P)degP' \\
&= \sum_{P\in\mathcal{S}} g(P)d(P)degP' \\
&= \sum_{P\in\mathcal{S}} g(P)d(P_Z)degP' \qquad \text{(by (4.5))} \\
&\geq \frac{1}{2}\sum_{P\in\mathcal{S}} g(P)r(P_Z)e(P_Z)degP' \qquad \text{(by Proposition 4.6)} \\
&= \frac{1}{2}\sum_{P\in\mathcal{S}} g(P)r(P_Z)e(P)degP' \qquad \text{(by (4.6))} \\
&= \frac{1}{2}\sum_{P\in\mathcal{S}} g(P)r(P_Z)e(P)f(P)degP \\
&= \frac{1}{2}[E:F]\sum_{P\in\mathcal{S}} r(P_Z)degP \\
&= \frac{1}{2}[E:F]\sum_{P\in\mathcal{S}} r(P_Z)degP_Z \qquad \text{(by (4.6))} \\
&= \frac{1}{2}[E:F]\sum_{P\in\mathcal{S}} log_q(q^{degP_Z})^{r(P_Z)} \\
&\geq \frac{1}{2}[E:F]\sum_{P\in\mathcal{S}} log_q e(P_Z) \qquad \text{(by Corollary 4.5)} \\
&= \frac{1}{2}[E:F]\sum_{P\in\mathcal{S}} log_q e(P) \qquad \text{(by (4.6))} \\
&\geq \frac{1}{2}[E:F](log_q[E:F]-log_q[M:F]) \qquad \text{(by Lemma 4.7)}
\end{aligned}$$

and this gives the estimate that we want. □

We are ready to prove the main result of this section. Let us note that $N(F)$ denotes the number of rational places, i.e. the number of degree one places of $F/\mathbb{F}_q$.

Theorem 4.9. *Let $F/\mathbb{F}_q$ be an algebraic function field, and let $(E_v)_{v\geq 1}$ be a sequence of elementary abelian p-extensions of F with the same constant field F_q. Then the quotient $N(E_v)/g(E_v)$ goes to zero as $[E_v:F]\to\infty$.*

Proof. By Theorem 4.8, for each $v\geq 1$ we have

$$deg(\text{Diff}(E_v/F)) \geq \frac{1}{2}[E_v:F](log_q[E_v:F]-log_q[M:F]), \tag{4.7}$$

where $F\subseteq M\subseteq E_v$ is the maximal unramified subextension. Any unramified abelian extension M_0/F with constant field $\mathbb{F}_q$ is of degree $[M_0:F]\leq h$, where h is the class number of F (see [AT]). Let us note that class number is defined as the order of the group of divisor classes of degree zero. Then (4.7) becomes

$$deg(\text{Diff}(E_v/F)) \geq \frac{1}{2}[E_v:F](log_q[E_v:F]-log_q h), \tag{4.8}$$

where h is the class number of F. The Hurwitz Genus Formula for E_v/F gives

$$2g(E_v) - 2 = [E_v : F](2g(F) - 2) + deg(\text{Diff}(E_v/F)).$$

So we obtain

$$\begin{aligned} g(E_v) &\geq [E_v : F](g(F) - 1) + \frac{1}{2} deg(\text{Diff}(E_v/F)) \\ &\geq [E_v : F](g(F) - 1) + \frac{1}{4}[E_v : F](log_q[E_v : F] - log_q h) \qquad \text{(by (4.8))} \end{aligned}$$

for each $v \geq 1$. Moreover, $N(E_v) \leq [E_v : F]N(F)$ by the Fundamental Equality. Hence for every $v \geq 1$,

$$\frac{N(E_v)}{g(E_v)} \leq \frac{N(F)}{g(F) - 1 + \frac{1}{4}(log_q[E_v : F] - log_q h)}$$

holds. Since the right hand side of the inequality goes to zero as $[E_v : F] \to \infty$, the result follows.

□

Bibliography

[AA] Álvaro G.R., Arnoldo T.H., Elementary abelian p-extensions and curves with many points, *Rev. Acad. Colomb. Cienc.,* **36**, 243-252 (2012).

[A] Arf C., Untersuchungen über reinverzweigte Erweiterungen diskret bewerteter perfekter Körper, *J. Reine Angew. Math.,* **181**, 1-44 (1940).

[AT] Artin E., Tate J., *Class Field Theory,* New York - Amsterdam, 1967.

[FPS] Frey G., Perret M., Stichtenoth H., On the Different of Abelian Extensions of Global Fields, *Lecture Notes in Math., Springer, Berlin,* **1518**, 26-32 (1992).

[GS] Garcia A., Stichtenoth H., Elementary abelian p-extensions of algebraic function fields, *Manuscr. Math.,* **72**, 67-79 (1991).

[GaSt] Garcia A., Stichtenoth H., Some Remarks on the Hasse-Arf Theorem, *Contemporary Mathematics,* **461**, 141-146 (2008).

[GO] Güneri C., Özbudak F., Weil-Serre Type Bounds for Cyclic Codes, *IEEE Trans. on Inf. Theory,* **54**, 5381-5395 (2008).

[K] Kani E., Relations between the genera and between the Hasse-Witt invariants of Galois coverings of curves, *Canad. Math. Bull.,* **28**, 321-327 (1985).

[L] Lang S., *Algebra,* Springer-Verlag, New York, 2002.

[S] Stichtenoth H., *Algebraic Function Fields and Codes,* Springer-Verlag, Berlin Heidelberg, 2009.