On the Different of Abelian Extensions of Global Fields

G. Frey, M. Perret, H. Stichtenoth

0. Introduction

Let q be a power of some prime number p, and let $\mathbf{F}_q$ be the field with q elements. Coding theorists are interested in explicitly described function fields over $\mathbf{F}_q$ having a large number of $\mathbf{F}_q$-rational places (or, equivalently, irreducible complete smooth algebraic curves over $\mathbf{F}_q$ with many $\mathbf{F}_q$-rational points). For small values of the genus, such function fields are often abelian extensions of the rational function field $\mathbf{F}_q(z)$. For instance, this is the case for Hermitian curves, some Fermat curves, and some Artin-Schreier extensions of $\mathbf{F}_q(z)$. Moreover, one way to exhibit families of function fields $E/\mathbf{F}_q$ of genus growing to infinity and having *good asymptotic behaviour* (i.e., the ratio (number of rational places/genus) has a limit > 0), is to construct a tower of function fields $E_0 \subseteq E_1 \subseteq E_2 \ldots$ over $\mathbf{F}_q$, each step E_{i+1}/E_i being Galois with an abelian Galois group. In other words, *solvable* extensions may have a good asymptotic behaviour, cf. [3].

One aim of our paper is to show that *abelian* extensions E_i/F (where F is some fixed function field over $\mathbf{F}_q$, and $\mathbf{F}_q$ is assumed to be the full constant field of F and all $E_i, i \geq 1$) are *asymptotically bad* (i.e., the ratio (number of rational places/genus) tends to 0 as the genus of $E_i/\mathbf{F}_q$ goes to infinity).

It should be pointed out that our method uses only elementary results from Hilbert's ramification theory, cf. [2,4], and the finiteness of the residue class fields. In the case of global fields, one may also use class field theory in order to obtain some results of this paper.

1. Hilbert's Ramification Theory for Locally Abelian Extensions

In this section, we consider the following situation. K is some field, $o \subseteq K$ a discrete valuation ring and $\wp \subseteq o$ the maximal ideal of o. Let L/K be a *finite abelian field extension* with Galois group G (i.e. L/K is Galois, and its Galois group G is abelian). Let $\mathcal{O} \subseteq L$ be a discrete valuation ring of L with $o \subseteq \mathcal{O}$ and maximal ideal $\mathcal{P}$, hence $\wp = \mathcal{P} \cap o$. Throughout section 1, we suppose that *$\mathcal{O}$ is the only discrete valuation ring of L containing o*. Let $k := o/\wp$ and $l := \mathcal{O}/\mathcal{P}$ denote the residue class fields of o resp. $\mathcal{O}$. Then l/k is a finite field extension, and we shall always assume *that l/k is separable.* We choose some $\mathcal{P}$-prime element $\pi \in \mathcal{P}$ (i.e., $\mathcal{P}$ is the principal ideal generated by π), and consider the groups

$$G_0 := \{\sigma \in G \mid \sigma x \equiv x \mod \mathcal{P} \text{ for all } x \in \mathcal{O}\}$$

and, for $i \geq 1$,

$$G_i := \{\sigma \in G_0 \mid \sigma\pi \equiv \pi \mod \mathcal{P}^{i+1}\}.$$

It is well-known that the definition of G_i is independent of the choice of π, and $G \supseteq G_0 \supseteq G_1 \supseteq \ldots \supseteq G_n = \{1\}$ for sufficiently large $n \geq 1$, see [2,4]. The factor groups $\mathcal{P}^i/\mathcal{P}^{i+1}$ (for $i \geq 0$) are considered as vector spaces over l via

$$(x + \mathcal{P}) \cdot (a + \mathcal{P}^{i+1}) := xa + \mathcal{P}^{i+1} \qquad (x \in \mathcal{O}, a \in \mathcal{P}^i),$$

and G acts on $\mathcal{P}^i/\mathcal{P}^{i+1}$ by

$$\tau(a + \mathcal{P}^{i+1}) := \tau(a) + \mathcal{P}^{i+1}$$

(in order to see that this action is well-defined observe that $\mathcal{O}$ is the only extension of o in L, hence $\tau(\mathcal{P}) = \mathcal{P}$ for all $\tau \in G$). We set

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

Clearly, X_i is a k-subspace of $\mathcal{P}^i/\mathcal{P}^{i+1}$.

Proposition 1: The dimension of X_i as a vector space over k is at most one.

Proof: By Hilbert's ramification theory l/k is a normal field extension. Due to our assumption l/k being separable we obtain that l/k is Galois. Moreover, any automorphism τ_0 in the Galois group of l/k is induced by some $\tau \in G$, i.e. $\tau_0(x + \mathcal{P}) = \tau(x) + \mathcal{P}$ for any $x + \mathcal{P} \in \mathcal{O}/\mathcal{P} = l$, see [2]. In order to prove the proposition we can assume that $X_i \neq \{0\}$. We choose $a + \mathcal{P}^{i+1} \in X_i$ with $a \in \mathcal{P}^i \backslash \mathcal{P}^{i+1}$. Since $\mathcal{P}^i/\mathcal{P}^{i+1}$ is a one-dimensional vector space over l (this is obvious) we have for all $a_1 + \mathcal{P}^{i+1} \in X_i$: $a_1 + \mathcal{P}^{i+1} = (c + \mathcal{P}) \cdot (a + \mathcal{P}^{i+1})$ for some $c \in \mathcal{O}$. For any $\tau \in G$, the following holds:

$$\begin{aligned}(c + \mathcal{P}) \cdot (a + \mathcal{P}^{i+1}) &= a_1 + \mathcal{P}^{i+1} = \tau(a_1 + \mathcal{P}^{i+1}) \\ &= \tau(c + \mathcal{P}) \cdot \tau(a + \mathcal{P}^{i+1}) = \tau(c + \mathcal{P}) \cdot (a + \mathcal{P}^{i+1}),\end{aligned}$$

consequently $\tau(c + \mathcal{P}) = c + \mathcal{P}$ for any $\tau \in G$. Thus $c + \mathcal{P}$ is invariant under any automorphism of l/k, i.e. $c + \mathcal{P} \in k$. This proves Proposition 1. ∎

It is well known that the mappings

$$\psi : \begin{cases} G_0/G_1 \longrightarrow & l^* \\ \sigma \longrightarrow & \frac{\sigma\pi}{\pi} \mod \mathcal{P} \end{cases}$$

resp. for $i \geq 1$

$$\varphi_i : \begin{cases} G_i/G_{i+1} \longrightarrow & \mathcal{P}^i/\mathcal{P}^{i+1} \\ \sigma \longrightarrow & \frac{\sigma\pi}{\pi} - 1 \mod \mathcal{P}^{i+1} \end{cases}$$

are embeddings of G_0/G_1 into the multiplicative group of l (resp. of G_i/G_{i+1} into the additive group $\mathcal{P}^i/\mathcal{P}^{i+1}$), and the definition of ψ and φ_i is independent of the choice of the prime element π. For our purposes, the following refinement is essential:

Proposition 2: Under the hypotheses of this section, the image of ψ is contained in k^*, and the image of φ_i is contained in X_i for any $i \geq 1$.

Proof: (a) Let $\sigma \in G$. We have to show that $\tau_0(\psi(\sigma)) = \psi(\sigma)$ for all τ_0 in the Galois group of l/k. As before, τ_0 is induced by some $\tau \in G$, and we obtain

$$\tau_0(\psi(\sigma)) = \tau_0\Big(\frac{\sigma\pi}{\pi} + \mathcal{P}\Big) = \frac{\tau(\sigma\pi)}{\tau(\pi)} + \mathcal{P} = \frac{\sigma(\tau(\pi))}{\tau(\pi)} + \mathcal{P} = \psi(\sigma)$$

(we have used that G is abelian and $\tau(\pi)$ is a $\mathcal{P}$-prime element as well).
(b) An analogous argument proves that $\varphi_i(\sigma) \in X_i$ for any $\sigma \in G_i$. ∎

We recall some facts from ramification theory. Let $f = f(\mathcal{P} \mid \wp) = [l : k]$ denote the *residue class degree* and $e := e(\mathcal{P} \mid \wp)$ the *ramification index* of $\mathcal{P}$ over $\wp$, i.e. $\wp\mathcal{O} = \mathcal{P}^e$. Since $\mathcal{O}$ is the only extension of o in L and l/k is separable, we have $e \cdot f = [L : K]$. Let $s := \mathrm{char}(k)$ be the characteristic of the residue class field and $g_i := \mathrm{ord}\, G_i$ for any $i \geq 0$. Then G_1 is the unique s-Sylow subgroup of G_0, and $g_0 = e$. The extension $\mathcal{P} \mid \wp$ is said to be *tame* if $g_1 = 1$ (hence $(s, e) = 1$), otherwise $\mathcal{P} \mid \wp$ is *wildly ramified.*

Let $W \subseteq k^*$ be the group of roots of unity in k. If W is finite, we set $w := \#W$.

Corollary 3: In addition to the hypotheses of this section, suppose that k contains only finitely many roots of unity. If $\mathcal{P} \mid \wp$ is tame then $e \leq w$.

Proof: Consider the map $\psi : G_0 \to l^*$ as before. Since $G_1 = 1, \psi$ is a monomorphism. By Proposition 2, the image of ψ is contained in W. ∎

In order to obtain a similar estimate for the ramification index also in the case of wild ramification, we introduce the following notion: an integer $i \geq 0$ is called a *jump* (for $\mathcal{P} \mid \wp$) if $G_i \neq G_{i+1}$.

Corollary 4: In addition to the hypotheses of this section, assume that k is a finite field. Then $e \leq (\#k)^r$ where r denotes the number of jumps.

Proof: $e = g_0 = (g_0/g_1) \cdot (g_1/g_2) \cdot \ldots \cdot (g_n/g_{n+1})$ where n is chosen such that $g_{n+1} = 1$. Proposition 1 and 2 yield $g_i/g_{i+1} \leq \#k$ for any $i \geq 0$. The corollary follows immediately. ∎

Hilbert's formula [2,4] states that the *different exponent* $d := d(\mathcal{P} \mid \wp)$ is given by

$$d = \sum_{i \geq 0} (g_i - 1).$$

This formula can be restated as follows. We consider the set $\{\nu_1, \ldots, \nu_r\}$ of jumps (where $0 \leq \nu_1 < \nu_2 < \ldots < \nu_r$ and r is the number of jumps) and set

$$t_1 := \nu_1 + 1; \quad t_i := \nu_i - \nu_{i-1} \quad \text{for} \quad i = 2, \ldots, r.$$

Then

$$d = \sum_{i=1}^{r} t_i(g_{\nu_i} - 1).$$

Since G is abelian, the Hasse-Arf theorem [2] applies. It yields

$$t_i \cdot g_{\nu_i} \equiv 0 \mod e$$

for $i = 1, \ldots, r$. Combining this with Hilbert's formula we obtain

Proposition 5: Under the hypotheses of this section, the different exponent d satisfies the estimate

$$d \geq \frac{1}{2} re$$

where r denotes the number of jumps.

Proof:

$$d = \sum_{i=1}^{r} t_i g_{\nu_i}(1 - g_{\nu_i}^{-1})$$

$$\geq \frac{1}{2} \cdot \sum_{i=1}^{r} t_i g_{\nu_i} \geq \frac{1}{2} re$$

by the Hasse-Arf theorem. ∎

2. The Different of Abelian Extensions of Global Fields

In this section, F denotes a *global field*. This means that either F is a *number field*, or F is an *algebraic function field of one variable* over a finite field $\mathbf{F}_q$ (we assume that $\mathbf{F}_q$ is the full constant field of F). A *place* of F is the maximal ideal of a discrete valuation ring of F. If $\wp$ is a place of F, its corresponding valuation ring will be denoted by $o_\wp$. The residue class field $o_\wp/\wp$ is a finite field, and in the function field case we have $\mathbf{F}_q \subseteq o_\wp$. The *degree* of $\wp$ is defined by

$$\deg \wp := \log \#(o_\wp/\wp)$$

(in the number field case, log is taken with respect to the basis $e = 2,718\ldots$; if F is a function field over $\mathbf{F}_q$, we take $\log = \log_q$ - the logarithm with respect to the basis q). The definition of the degree is extended to *divisors* of F (a divisor is a formal finite sum of places) by linearity.

Let E/F be an ***abelian extension*** of F and $\mathrm{Gal}(E/F)$ be its Galois group. If $\wp$ is a place of F, there are $g = g(\wp)$ places $\mathcal{P}_1, \ldots, \mathcal{P}_g$ of E lying over $\wp$ (i.e. $\wp \subseteq \mathcal{P}_\nu$). All of them have the same ramification index $e(\wp) := e(\mathcal{P}_\nu \mid \wp)$ and the same residue class degree $f(\wp) := f(\mathcal{P}_\nu \mid \wp)$, and we have $e(\wp) \cdot f(\wp) \cdot g(\wp) = [E : F]$. For an extension $\mathcal{P} = \mathcal{P}_\nu$ of $\wp$ in E/F, we consider the ***decomposition group***

$$G(\wp) := G(\mathcal{P} \mid \wp) := \{\sigma \in \mathrm{Gal}(E/F) \mid \sigma\mathcal{P} = \mathcal{P}\}$$

(this is independent of the choice of the extension $\mathcal{P}$ since E/F is abelian), and the ***decomposition field*** $Z = Z(\wp)$, i.e. $F \subseteq Z \subseteq E$ and $G(\wp) = \mathrm{Gal}(E/Z)$.

There exists the unique ***maximal unramified subextension*** $F \subseteq M \subseteq E$. This means that all places of F are unramified in M/F, and M is a maximal subfield of E with this property. Let $S := S(E/F)$ be the set of places of F which are ramified in E/F (it is well-known that S is finite).

Lemma 6: With the notations as above, we have

$$\sum_{\wp \in S} \log e(\wp) \geq \log[E : F] - \log[M : F].$$

Proof: For any $\wp \in S$, let $G_0(\wp) \subseteq G$ be the ***inertia group*** of $\wp$, see [2,4]. Its order is $e(\wp)$, and if $U \subseteq G$ is the subgroup of G generated by all $G_0(\wp)$ (with $\wp \in S$), then M is the fixed field of U. Therefore $\mathrm{ord}\ U = [E : M] = [E : F]/[M : F]$. Since G is abelian,

$$\mathrm{ord}\quad U \leq \prod_{\wp \in S} \mathrm{ord}\quad G(\wp) = \prod_{\wp \in S} e(\wp).$$

Taking logarithms yields the assertion of the lemma. ∎

Let $\mathcal{D}(E/F)$ be the ***different*** of E/F. The main result of this section is the following:

Theorem 7: Suppose that E/F is an abelian extension of global fields and $F \subseteq M \subseteq E$ is the maximal unramified subextension. In the function field case we assume, in addition, that E and F have the same constant field $\mathbf{F}_q$. Then the degree of the different $\mathcal{D}(E/F)$ satisfies

$$\deg \mathcal{D}(E/F) \geq \frac{1}{2}[E : F] \cdot (\log[E : F] - \log[M : F]).$$

Proof: For $\wp \in S$, let $d(\wp)$ be the different exponent of a place $\mathcal{P}$ of E lying over $\wp$, and $r(\wp)$ be the number of jumps, cf. section 1 (observe that we can apply the results of section 1 if F is replaced by the decomposition field $Z(\wp)$). We obtain

$$\begin{aligned}
\deg \mathcal{D}(E/F) &= \sum_{\mathfrak{p}\in S}\sum_{\mathcal{P}|\mathfrak{p}} d(\mathcal{P})\cdot \deg \mathcal{P} \\
&= \sum_{\mathfrak{p}\in S} g(\mathcal{P})\cdot d(\mathcal{P})\cdot f(\mathcal{P})\cdot \deg \mathfrak{p} \\
&\geq \frac{1}{2}\sum_{\mathfrak{p}\in S} g(\mathcal{P})\cdot r(\mathcal{P})\cdot e(\mathcal{P})\cdot f(\mathcal{P})\cdot \deg \mathfrak{p} \qquad \text{(by Proposition 5)} \\
&= \frac{1}{2}[E:F]\cdot \sum_{\mathfrak{p}\in S} r(\mathcal{P})\cdot \deg \mathfrak{p} \\
&\geq \frac{1}{2}[E:F]\cdot \sum_{\mathfrak{p}\in S} \log e(\mathcal{P}) \qquad \text{(by Corollary 4)} \\
&\geq \frac{1}{2}[E:F]\cdot (\log[E:F] - \log[M:F]) \qquad \text{(by Lemma 6).}
\end{aligned}$$

■

3. Abelian Extensions of Function Fields Are Asymptotically Bad

We want to prove a slightly more general result than we announced in the introduction. For an algebraic function field $E/\mathbf{F}_q$ (with $\mathbf{F}_q$ as its full constant field) we set

$$\begin{aligned}
g(E) &= \text{genus of} \quad E \\
N(E) &= \text{number of rational places of} \quad E/\mathbf{F}_q.
\end{aligned}$$

If E/F is a Galois extension with Galois group G, we let G' be the ***commutator subgroup*** of G. The fixed field $E^{ab} \supseteq F$ of G' is the ***maximal abelian extension*** of F contained in E. In particular, if G is abelian, $G' = \{1\}$ and $E^{ab} = E$.

Theorem 8: Let $F/\mathbf{F}_q$ be an algebraic function field and $(E_\nu)_{\nu\geq 1}$ be a sequence of extension fields of F with the following properties:

(i) $\mathbf{F}_q$ is the full constant field of F and all E_ν.
(ii) E_ν/F is Galois with Galois group G_ν.
(iii) $\text{ord}\,(G_\nu/G'_\nu) \longrightarrow \infty$ as $\nu \longrightarrow \infty$.

Then the quotient $N(E_\nu)/g(E_\nu)$ tends to zero as $\nu \longrightarrow \infty$.

Proof: There is a constant h (the class number of F) such that any abelian unramified extension M/F with the same constant field $\mathbf{F}_q$ is of degree $[M:F] \leq h$, cf. [1]. We consider the maximal abelian extension $F_\nu \subseteq E_\nu$ of F contained in E_ν. By (iii), the degree $n_\nu := [F_\nu : F] \longrightarrow \infty$ as $\nu \longrightarrow \infty$, and the degree d_ν of the different $\mathcal{D}(F_\nu/F)$ satisfies the estimate

$$d_\nu \geq \frac{1}{2} n_\nu (\log n_\nu - \log h)$$

by Theorem 7. The Hurwitz genus formula yields

$$\begin{aligned} g(F_\nu) &\geq n_\nu (g(F) - 1) + \frac{1}{2} d_\nu \\ &\geq n_\nu (g(F) - 1 + \frac{1}{4} (\log n_\nu - \log h)). \end{aligned}$$

On the other hand, we have the trivial estimate $N(F_\nu) \leq n_\nu \cdot N(F)$, hence

$$\frac{N(F_\nu)}{g(F_\nu)} \leq \frac{N(F)}{g(F) - 1 + \frac{1}{4} (\log n_\nu - \log h)} \longrightarrow 0$$

for $\nu \longrightarrow \infty$. Eventually, since $N(E_\nu) \leq [E_\nu : F_\nu] \cdot N(F_\nu)$ and $g(E_\nu) \geq [E_\nu : F_\nu](g(F_\nu) - 1) \geq \frac{1}{2}[E_\nu : F_\nu] \cdot g(F_\nu)$ (observe that $g(F_\nu) \longrightarrow \infty$ for $\nu \longrightarrow \infty$), we obtain $N(E_\nu)/g(E_\nu) \longrightarrow 0$. ∎

References

[1] *Artin, E. and Tate, J.:* Class field theory. New York - Amsterdam 1967

[2] *Serre, J.P.:* Corps locaux. Paris 1962

[3] *Serre, J.P.:* Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini. C.R. Acad.Sc. Paris, t. 296 (1983), 397-402

[4] *Zariski, O. and Samuel P.:* Commutative Algebra, Vol. I. Princeton 1958

Gerhard Frey
Institut für Experimentelle Mathematik
Universität GHS Essen
Ellernstr. 29, D-4300 Essen 12
Germany

Marc Perret
Equipe Arithmétique et Théorie de l'Information
CIRM, Luminy Case 916
F-13288 Marseille Cedex 9
France

Henning Stichtenoth
Fachbereich 6, Universität GHS Essen
D-4300 Essen 1
Germany