Università degli studi di Roma 'Sapienza'
Facoltà di Scienze Matematiche Fisiche e Naturali
Dottorato in Matematica

An upper bound for the genus of a curve without points of small degree

Claudio Stirpe

Dottorando XXIII ciclo

Anno Accademico 2010/2011

To Pio Parisi sj.

Contents

Chapter 1

Introduction

Let X be a smooth, projective, absolutely irreducible curve over the finite field $\mathbb{F}_q$ and let K be the function field of X. For any integer $n > 0$ let a_n denote the number of places of K of degree n. Then $N_n = \sum_{d|n} da_d$ is the number of rational points over the constant field extension $K\mathbb{F}_{q^n}$. The Weil inequality (see [16]) states that

$$|N_n - q^n - 1| \leq 2gq^{n/2},$$

where g is the genus of the curve. A search for curves with many points, motivated by applications in coding theory, showed that this bound is optimal when the genus g is small compared to q (see [6] for further details). When g is large compared to q sharper estimates hold (see for example [10] for an asymptotic result or

also [15] Chapter V). A similar problem arises from finding curves without points of degree n when n is a positive integer. In particular when X has no points over $\mathbb{F}_{q^n}$ then $g \geq \frac{q^n-1}{2q^{n/2}}$. The genus 2 case was already considered in [11]. Moreover in a recent paper, E. Howe, K. Lauter and J. Top [9] show that the previous bound is not always sharp when $n = 1$ and $g = 3$ or 4. In the same paper they cite an unpublished result of P. Clark and N. Elkies that states that for every fixed prime p there is a constant $C_p > 0$ such that for any integer $n > 0$, there is a projective curve over $\mathbb{F}_p$ of genus $g \leq C_p n p^n$ without places of degree smaller than n.

In this paper we prove that this bound is not optimal. In fact we prove the following result.

Theorem 1.1. For any prime p there is a constant $C_p > 0$ such that for any $n > 0$ and for any power q of p there is a projective curve over $\mathbb{F}_q$ of genus $g \leq C_p q^n$ without points of degree strictly smaller than n.

We show the existence of such curves by means of class field theory. The basic facts and definitions about this topic are showed in the third Chapter. In the second Chapter we give the basic definitions and results about the arithmetic of function fields. In

the forth Chapter we generalize a result in [1] about the number of ray class field extensions with given conductor $\mathfrak{m}$ and we use it in order to prove the bound of Clark and Elkies. In the last Chapter the sharper estimate of Theorem 1.1 is proved. A table of examples for $q = 2$ and $n < 20$ is also given.

Acknowledgements

I am grateful to Prof. René Schoof, Università di Roma 'Tor Vergata', for his patience and support. Part of this work was done when I was a visiting student at the Mathematical Institute at Leiden University.

Chapter 2

Background and notation

By a curve over $\mathbb{F}_q$ we mean a smooth, projective, geometrically irreducible curve over the finite field $\mathbb{F}_q$ of characteristic p. Let X be such a curve and let K be the associated function field. The field K is a finite extension of $\mathbb{F}_q(x)$ where x is a transcendental element over $\mathbb{F}_q$ (see [15] Appendix B for more details). The constant field of K is the maximal finite extension of $\mathbb{F}_q$ in K.

Let Y be a curve with associated function field L. A morphism $f : Y \to X$ is a covering of X if it is surjective and separable (see [15] Appendix A). A covering is abelian if the associated extension L/K is Galois with abelian Galois group. The degree of the extension is called the degree of the covering.

A place of K is a maximal ideal P in some discrete valuation

ring $O_P \subseteq K$ (i.e. a principal domain in K with exactly one non-zero maximal ideal). The degree of a place is the degree of the residue field $\mathcal{F}_P = O_P/P$.

To every place is associated a discrete valuation that is denoted by v_P (see [15] Chapter I). Let L/K be an extension of K and let Q (resp. P) be a place of L (resp. K). We write $Q|P$ and we say Q lies over P if $Q \cap K = P$. The valuation v_P can be extended in a unique way to a discrete valuation v_Q over Q. Then the two valuation are related as follows: there is a positive integer $e(Q|P) > 0$ such that $v_Q(x) = e(Q|P)v_P(x)$ for all $x \in K$. A place Q over P is unramified if $e(Q|P) = 1$. Otherwise it is ramified. A ramified place $Q|P$ is wild if $p|e(Q|P)$ and is tame otherwise. A place P of K is unramified in L/K if all the places Q over P are unramified, otherwise it is ramified. The extension L/K is unramified if all the places of K are unramified, otherwise it is ramified. Let $f(Q|P)$ denote the degree $[\mathcal{F}_Q : \mathcal{F}_P]$ of the field extension $\mathcal{F}_Q/\mathcal{F}_P$, then we have the well-known formula $\sum_{Q|P} f(Q|P)e(Q|P) = [L : K]$. If L/K is a Galois extension then $f(Q|P) = f(Q'|P)$ and $e(Q|P) = e(Q'|P)$ for any place Q and Q' in L over P so we get the simpler formula $ref = n$, where n is the degree $[L : K]$, the integer e is $e(Q|P)$, the integer f is

$f(Q|P)$ and r is the number of places Q of L over P. In the sequel we say that a place P is totally inert if $f = n$, is totally split if $r = n$ and is totally ramified is $e = n$. Similarly P is partially inert if $f > 1$, is partially split if $r > 1$ and is partially ramified if $e > 1$.

The next Lemma is an elementary tool when we want to compute the ramification index in the compositum of two function fields.

Lemma 2.1 (Abhyankar's Lemma)**.** Let K'/K be a finite separable extension of function fields such that $K' = K_1K_2$ is the compositum of two function fields K_1 and K_2 with $K \subseteq K_1$ and $K \subseteq K_2$. Let P' be a place of K' and let $P = P' \cap K$ and $P_i = P' \cap K_i$ be the places under P' in K and K_i for $i = 1, 2$. If at least one of the extensions $P_1|P$ or $P_2|P$ is tame, then $e(P'|P) = lcm\{e(P_1|P), e(P_2|P)\}$.

It follows from the previous Lemma that the compositum of two unramified extensions is still unramified.

A divisor $\sum_P n_P P$ is a finite formal sum of places. A divisor is effective if $n_P \geq 0$ for every place P. There is a partial ordering relation $D \leq D'$ whenever $D' = \sum n'_P P$ has coefficients $n_P \leq n'_P$

for every place P. The degree of D is the integer $\sum_P n_P deg(P)$. The support $Supp(D)$ of D is the set of places P such that $n_P \neq 0$.

We refer to [15] for the definition of the divisor $Diff(L/K)$. This notion is important because of the following Lemma.

Lemma 2.2 (Hurwitz Genus Formula)**.** Let K be a function field of genus g_K with constant field $\mathbb{F}_q$ and let L/K be a finite separable extension with constant field $\mathbb{F}_{q^d}$. Then the genus of L is given by

$$2g_L - 2 = \frac{[L:K]}{d}(2g_K - 2) + deg(Diff(L/K)). \qquad (2.1)$$

We need only the following result for computing the degree of the different.

Lemma 2.3 (Dedekind's Different Theorem)**.** Let

$$Diff(L/K) = \sum_P \sum_{P'|P} d(P'|P)P'$$

be the different of L/K, where P ranges over the places of K and P' over the places of L. Then $d(P'|P) \geq e(P'|P) - 1$ and equality holds if and only if the place $P'|P$ is not wild ramified. In particular $d(P'|P) = 0$ if and only if $P'|P$ is unramified.

The set of the places of K is denoted by $\mathcal{P}_K$ and the set of divisors of K is denoted by $\mathcal{D}_K$. The degree zero divisors are

denoted by $\mathcal{D}_K^0$. We can associate to every element $z \in K$ its principal divisor $(z) \in \mathcal{D}_K^0$. The set of principal divisors is denoted by $Prin(K)$. It is a well-known fact that the order of the quotient group $\mathcal{D}_K^0/Prin(K)$, denoted by h_K, is finite and it is called the divisor class number of K (see [15], Chapter V).

Let L/K be a finite Galois extension.

Definition 2.1. Let Q be a place of L and $P = Q \cap K$ the place of K under Q. The decomposition group of Q is the stabilizer of Q in L

$$D(Q|P) = \{\sigma \in Gal(L/K) |\ \sigma(Q) = Q\}.$$

The fixed field of $D(Q|P)$ in L is called the decomposition field of Q.

Let $\sigma \in Gal(L/K)$. We define an isomorphism

$$\overline{\sigma} : O_Q/Q \to O_{\sigma(Q)}/\sigma(Q)$$

by

$$\overline{\sigma}(\overline{z}) = \overline{\sigma(z)}, \qquad z \in O_Q,$$

where $\overline{z} \in \mathcal{F}_Q = O_Q/Q$ is the residue class of z in $\mathcal{F}_Q$ and $\overline{\sigma(z)} \in \mathcal{F}_{\sigma(Q)}$ is the residue class in $\mathcal{F}_{\sigma(Q)}$. When $\sigma \in D(Q|P)$, the image $\overline{\sigma}$ belongs to the subgroup $Gal(\mathcal{F}_Q/\mathcal{F}_P)$.

Proposition 2.1. Let Q be a place of L and let $P = Q \cap K$. The following sequence is exact

$$1 \to I(Q|P) \to D(Q|P) \to Gal(\mathcal{F}_Q/\mathcal{F}_P) \to 1,$$

where $I(Q|P)$ is the kernel of the map $\sigma \to \overline{\sigma}$ restricted to $D(Q|P)$. Moreover $|D(Q|P)| = e(Q|P)f(Q|P)$ and $|I(Q|P)| = e(Q|P)$.

Definition 2.2. The group $I(Q|P)$ of Proposition 2.1 is the inertia group of Q.

If $Q|P$ is unramified then $I(Q|P) = \{1\}$ and $D(Q|P)$ is a cyclic group isomorphic to $Gal(\mathcal{F}_Q/\mathcal{F}_P)$. In particular there is a generator $\Phi \in D(Q|P)$ such that the image $\overline{\Phi}$ in $Gal(\mathcal{F}_Q/\mathcal{F}_P)$ is the Frobenius morphism $z \to z^u$ for $z \in \mathcal{F}_Q$, where $u = q^{deg(P)}$ is the cardinality of $\mathcal{F}_P$. This element $\Phi \in D(Q|P)$ is called the Frobenius automorphism $Frob(Q|P)$ of Q.

Let $Q'|P$ be a place of L over P distinct from Q. Then $Q' = \sigma(Q)$ for at least one $\sigma \in Gal(L/K)$ and so $I(Q'|P) = \sigma I(Q|P)\sigma^{-1}$ and $D(Q'|P) = \sigma D(Q|P)\sigma^{-1}$. Moreover $Frob(Q'|P) = \sigma Frob(Q|P)\sigma^{-1}$. In particular when $Gal(L/K)$ is an abelian group we get $I(Q|P) = I(Q'|P)$ and similarly $D(Q|P) = D(Q'|P)$ and $Frob(Q|P) = Frob(Q'|P)$ so we can define without ambiguity the Frobenius automorphism and the decomposition group at

P as $Frob(P) = Frob(Q|P)$ and $D(P) = D(Q|P)$ respectively.

Proposition 2.2. Let L/K be an abelian extension and M be a subfield of L containing K. For any place P of K we denote by $Frob(P)$ the Frobenius automorphism in $Gal(L/K)$. Then P is totally split in M/K if and only if $Frob(P) \in Gal(L/M)$.

The following Lemma (see [12], Theorem 1) is an explicit version of the well-known Chebotarev Theorem (see [5] Chapter 2).

Lemma 2.4. [Explicit version of the Chebotarev Theorem] Let $C \subseteq G$ be a conjugacy class in the Galois Group $G = Gal(M_2/M_1)$ of a finite extension M_2/M_1. Assume that the constant field of M_1 and M_2 are the same. Let $\pi_C(d)$ be the number of places P over M_1 of degree d such that the coniugacy class $[Frob(P)]$ is C and let $\pi(d)$ is the number of unramified places P of M_1 of degree d. Let $\psi_C(d) = \sum_{r|d} r\pi_C(r)$ and $\psi(d) = \sum_{r|d} r\pi(r)$. Then $\psi_C(d)$ is bounded by

$$|\psi_C(d) - \frac{|C|}{|G|}\psi(d)| \leq 2g_{M_2}\frac{|C|}{|G|}q^{d/2} + deg(D),$$

where D is the divisor given by the formal sum of all the ramified places of M_1.

Proof. Let $\chi : G \to \mathbb{C}^*$ be a class function of G. For any unramified place P of M_1 and for any integer $n \geq 0$ we define

$\chi(P^n) = \chi([Frob(P)]^n)$ as the evaluation by χ of the n-power of the conjugacy class of the Frobenius automorphism of P. When P is ramified we define

$$\chi(P^n) = \frac{1}{e(P)} \sum_{\omega \in I(P'|P)} \chi([\omega\sigma(P')]^n),$$

where P' is a place of M_2 over P and $\sigma(P')$ is an element of the decomposition group $D(P'|P)$ such that its image $\overline{\sigma}$ in $Gal(\mathcal{F}_{P'}/\mathcal{F}_P)$, as in Proposition 2.1, is the Frobenius morphism. It is easy to see that $\chi(P^n)$ is well-defined. We say that χ is averaged over the ramified places. We define

$$\psi_\chi(d) = \sum_{r|d} \sum_{deg(P)=r} \chi(P^{d/r}),$$

where P runs over the places of M_1.

We denote by $\hat{G}$ the set of irreducible characters of G and by

$$\zeta_{M_i}(t) = \prod_{P \in \mathcal{P}_{M_i}} (1 - t^{deg(P)})^{-1}$$

the zeta function of M_i for $i = 1, 2$. By the Riemann hypothesis for curves the polynomial $\zeta_{M_i}(t)(1-t)(1-qt)$ of degree $2g_{M_i}$ (see [15] Chapter V) is equal to

$$\prod_{j=1}^{g_i} (1 - \alpha_{i,j}t)(1 - \overline{\alpha}_{i,j}t)$$

for suitable algebraic integers $\alpha_{i,j}$ such that $|\alpha_{i,j}| = \sqrt{q}$, where g_i is the genus of M_i.

For a given a character $\chi \in \hat{G}$ we define the L-function $L(t,\chi)$ as 1 when $t = 0$ and

$$\frac{d}{dt}\log(L(t,\chi)) = \sum_{r=1}^{\infty} \psi_\chi(r) t^{r-1},$$

when $|t| < \frac{1}{q}$. This series is absolutely convergent for $|t| < \frac{1}{q}$ so $L(t,\chi)$ admit an analytic continuation to the whole complex plane.

It is easy to see that $\zeta_{M_1}(t) = L(t,\chi_0)$, where χ_0 is the trivial character, as one can easily verify by using the Taylor series for the logarithm of $\zeta_{M_1}(t)$. In a similar way we can verify the relation

$$\frac{d}{dt}\log\zeta_{M_2}(t) = \sum_{\chi\in\hat{G}} \frac{d}{dt}\log L(t,\chi)^{\chi(1)}.$$

It follows that

$$\zeta_{M_2}(t) = \zeta_{M_1}(t) \prod_{\chi\in\hat{G},\ \chi\neq\chi_0} L(t,\chi)^{\chi(1)}.$$

When $\chi \in \hat{G}$ is not the trivial character, the L-function $L(t,\chi)$ is a polynomial (see [16]). By the Riemann hypothesis, this polynomial can be written as $\prod_{h=1}^{k}(1-\beta_h t)$ with $|\beta_h| = \sqrt{q}$ for $h = 1,\ldots,k$ and the degree k of $L(t,\chi)$ is bounded by $k \leq 2g_{M_2}$.

It follows that

$$\frac{d}{dt}\log(L(t,\chi)) = \sum_{r=1}^{\infty}\psi_\chi(r)t^{r-1} = \sum_{r=1}^{\infty}(\sum_{i=1}^{k}\beta_i^r)t^r$$

and so

$$|\psi_\chi(r)| \leq deg(L(t,\chi))\sqrt{q^r} \leq 2g_{M_2}\sqrt{q^r}.$$

By the orthogonality relations for irreducible characters

$$\sum_{\chi\in\hat{G}}\overline{\chi(C)}\sum_{deg(P)|d}\chi(P) = \sum_{[Frob(P)]=C}|\mathcal{C}_G(C)| = \frac{|G|}{|C|}\psi_C(d),$$

where P runs over the unramified places of M_1 and $\mathcal{C}_G(C)$ is the centralizer of C in G.

Similarly, when P is a ramified place, the sum $\sum_{\chi\in\hat{G}}\overline{\chi(C)}\chi(P)$ is bounded by $\frac{G}{C}$ so we can estimate

$$|\frac{|G|}{|C|}\psi_C(d) - \psi(d)| \leq |\sum_{\chi\neq\chi_0}\sum_{P\notin Supp(D)}\overline{\chi(C)}\chi(P)| + \sum_{P\in Supp(D)}\frac{|G|}{|C|}$$

$$\leq \sum_{\chi\neq 1}\sqrt{q^{d/2}}\chi(1)deg(L(t,\chi)) + \sum_{P\in Supp(D)}\frac{|G|}{|C|}$$

$$\leq 2g_{M_2}\sqrt{q^{d/2}} + \frac{|G|}{|C|}|D|,$$

and the Lemma follows. □

Chapter 3

Class field theory

3.1 Main definitions

In this section we introduce the Artin map and the ray class group. The explicit construction of ray class fields by means of Carlitz modules will be showed in the next section.

Definition 3.1. Let Q be a place of L lying over the place P of K. We define, for every integer $n \geq -1$, the n-th ramification group $G_n(Q|P)$ as

$$G_n(Q|P) = \{\sigma \in Gal(L/K) |\ v_Q(\sigma(x)-x) \geq n+1 \text{ for all } x \in O_Q\}.$$

It follows by the definition that $G_{-1}(Q|P) = D(Q|P)$ and $G_0(Q|P) = I(Q|P)$.

When $Q' = \sigma(Q)$ for a certain $\sigma \in Gal(L/K)$ then $G_n(Q'|P) =$

$\sigma G_n(Q|P)\sigma^{-1}$ for all $n \geq -1$. It follows that, when L/K is an abelian extension, the group $G_n(Q|P)$ coincide with $G_n(Q'|P)$ for every place Q' over P and for every $n \geq -1$. In this case we can also denote $G_n(Q|P)$ by $G_n(P)$.

We can extend the previous definition to any real number $u \geq -1$ by

$$G_u(Q|P) = G_{[u]}(Q|P),$$

where $[u]$ is the integral part of u. Let $g_i = |G_i(Q|P)|$ be the order of the group $G_i(Q|P)$ for $i \geq -1$. We define a real function $\phi : [-1, +\infty) \to [-1, +\infty)$ such that $\phi(u) = u$ for $-1 \leq u \leq 0$ and

$$\phi(u) = \frac{1}{g_0}(g_1 + g_2 + \ldots + g_{[u]} + (u - [u])g_{[u]+1}),$$

for $u \geq 0$. It is very easy to see that the function ϕ is continuous, strictly increasing, piecewise linear and concave on $[-1, +\infty)$. We denote by ψ the inverse function. Then ψ is continuous, piecewise linear, strictly increasing and convex on $[-1, +\infty)$.

Lemma 3.1. The real number $\psi(n)$ is an integer for any integer $n \geq -1$.

Proof. The Lemma is trivial for $n = -1$ and $n = 0$. For $n > 0$ let

u be the real number $\psi(n)$. Then

$$g_0\phi(u) = g_0 n = g_0 + \ldots + g_{[u]} + (u - [u])g_{[u]+1},$$

by definition of ϕ. It follows that

$$u - [u] = \frac{1}{g_{[u]+1}}(g_0 n - g_0 - \ldots - g_{[u]}).$$

But $G_{[u]+1}(Q|P)$ is a subgroup of $G_i(Q|P)$ for $i < [u]+1$ so $u-[u]$ is an integer by the Lagrange Theorem, so u is an integer. □

A partial converse of the previous Lemma is the following.

Proposition 3.1 (Hasse-Arf Theorem)**.** Let $n \geq -1$ be an integer. Assume $G_n(Q|P) \neq G_{n+1}(Q|P)$. Then $\phi(n)$ is an integer.

Definition 3.2. We define the upper ramificaton group $G^u(Q|P) = G_{\psi(u)}(Q|P)$.

The completion of K with respect to the valuation v_P is unique and we denote it by $\hat{K}_P$. The corresponding valuation is also denoted by v_P. In the sequel U_P denotes the unit elements in O_P. We denote by $\hat{O}_P$ and $\hat{U}_P$ the valuation ring of $\hat{K}_P$ and the group of units of $\hat{O}_P$, respectively. It is easy to check that $\hat{O}_P = \{x \in \hat{K}_P |\ v_P(x) \geq 0\}$. The n-th unit group is defined as

$$\hat{U}_P^{(n)} = \{x \in \hat{U}_P |\ v_P(x-1) \geq n\},$$

when $n > 0$ and $\hat{U}_P^{(0)} = \hat{U}_P$.

Assume now M is a complete field with respect to the valuation v. Let L/M be a finite abelian extension. There is a map

$$\theta_{L/M} : M^* \to Gal(L/M),$$

called the local Artin reciprocity map, that satisfies:

1. $Ker(\theta_{L/M}) = N_{L/M}(L^*)$, where $N_{L/M}$ is the norm map;
2. if L/M is unramified then $\theta_{L/M}(x) = Frob(P)^{v(x)}$ for all $x \in M^*$;
3. the image of $U_M^{(n)}$, the n-th unit group of M, is the upper ramification group $G^n(L/M)$ for all $n \geq 0$.

We are going to define a global Artin map of a function fields extension L/K in terms of the local Artin map $\theta_{\hat{L}_Q/\hat{K}_P}$, where P runs over the places of K and Q is a place of L over P.

Definition 3.3. The adele ring of K is the set

$$\mathbb{A}_K = \{(x_P)_P, x_P \in \hat{K}_P | \, x_P \in \hat{O}_P \text{ for all but finitely many places}\}.$$

Where P runs over the set $\mathcal{P}_K$ of places of K.

The field K is canonically embedded in the adele ring $\mathbb{A}_K$ via the diagonal morphism.

Definition 3.4. The unit group J_K of $\mathbb{A}_K$

$$J_K = \{(x_P)_P, x_P \in \hat{K}_P^* |\ x_P \in \hat{U}_P \text{ for all but finitely many places}\}.$$

is called the idele group of K.

The idele group J_K is a topological group. A base for the topology is given by the neighborhoods of the unity

$$\prod_{P \in S} \hat{K}_P^* \times \prod_{P \notin S} \hat{U}_P,$$

where S is a finite set of $\mathcal{P}_K$.

The multiplicative group K^* is canonically embedded in J_K.

Definition 3.5. The quotient group $C_K = J_K/K^*$ is the idele class group of K.

The class group is a topological group with respect to the quotient topology.

Let L/K a finite abelian extension of K. We define the global Artin reciprocity map $\theta_{L/K} : J_K \to Gal(L/K)$ as the product of the local Artin reciprocity $\theta_{\hat{L}_Q/\hat{K}_P}$, where P runs over the places of K and Q is a place of L over P. The map $\theta_{L/K}$ is well-defined because $Gal(\hat{L}_Q/\hat{K}_P) \cong D(Q|P) = D(P)$ (see [13] Chapter 2) and so $\theta_{\hat{L}_Q/\hat{K}_P}$ does not depend on the choice of Q.

The multiplicative group K^* is contained in the kernel of $\theta_{L/K}$ so we can define an homomorphism

$$(\cdot, L/K) : C_K \to Gal(L/K)$$

induced by the global Artin reciprocity. We call $(\cdot, L/K)$ the norm residue symbol of L/K. We describe the kernel of this homomorphism.

The norm map $N_{L/K} : L^* \to K^*$ can be extended to a morphism

$$N_{J_L/J_K} : J_L \to J_K$$

such that the idele $(x_Q)_{Q\in\mathcal{P}_L}$ is sent to $(\prod_{Q|P} N_{L/K}(x_Q))_{P\in\mathcal{P}_K}$.

Let $\mathcal{N}_K^L = (K^* N_{J_L/J_K}(J_L))/K^* \subseteq C_K$. Then $\mathcal{N}_K^L$ is a finite index subgroup of C_K.

Theorem 3.1 (Artin Reciprocity)**.** For any finite abelian extension L/K there is a canonical isomorphism $C_K/\mathcal{N}_K^L \cong Gal(L/K)$ induced by the norm residue symbol.

For any open subgroup M of C_K of finite index there is a finite abelian extension L/K such that $\mathcal{N}_K^L = M$.

Moreover $L_1 \subseteq L_2$ if and only if $\mathcal{N}_K^{L_2} \subseteq \mathcal{N}_K^{L_1}$.

In the sequel we use ray class fields for constructing curves. Let S be a finite non-empty set of places and let $\mathfrak{m} = \sum n_P P$ be

an effective divisor of the function field K with support disjoint from S. The S-congruence subgroup modulo $\mathfrak{m}$ is the subgroup

$$J_S^{\mathfrak{m}} = \prod_{P \in S} \hat{K}_P^* \times \prod_{P \notin S} \hat{U}_P^{(n_P)}.$$

Definition 3.6. A ray class group is a subgroup $C_S^{\mathfrak{m}}$ of C_K of the form

$$C_S^{\mathfrak{m}} = (K^* J_S^{\mathfrak{m}})/K^*$$

where $J_S^{\mathfrak{m}}$ is a S-congruence subgroup modulo $\mathfrak{m}$.

The index of $C_S^{\mathfrak{m}}$ in C_K is finite (see [13] Chapter 2 Section 4). We denote by $K_S^{\mathfrak{m}}$ the function field associated to the subgroup $C_S^{\mathfrak{m}}$ by the previous theorem.

The conductor of an abelian extension L/K is the divisor

$$\sum_P c_P P,$$

where P runs over the ramified places of K and c_P is the least integer u such that the upper ramification group $G^u(\hat{L}_Q/\hat{K}_P)$ is trivial for any $Q|P$ (see [13] Chapter 2 Section 3).

Theorem 3.2 (Conductor Theorem)**.** The function field $K_S^{\mathfrak{m}}$ is the largest abelian extension of K with conductor $\mathfrak{f}$ such that $\mathfrak{f} \leq \mathfrak{m}$ and such that every place of S splits completely.

We end this section with a very useful tool that we will use in the sequel.

Definition 3.7. Let K be a complete field according to the valuation v and let $g(z) = \sum_{i=0}^{d} g_i z^i$ be a polynomial in K with $d \geq 1$ such that $g_0 \neq 0$ and $g_d \neq 0$. The Newton polygon of g is the lower convex hull in $\mathbb{R} \times \mathbb{R}$ of the points $(i, v(g_i))$ for all $0 \leq i \leq d$ with $g_i \neq 0$.

The following Lemma shows that Newton polygons are useful for computing the roots of irreducible polynomials in algebraic extensions. We will use it in order to compute the ramification index of a place P.

Lemma 3.2. Let K be a complete field according to the valuation v. Let $g(z)$ be a polynomial in K and let $I \subseteq \mathbb{R} \times \mathbb{R}$ be the segment of the Newton polygon of g joining $(i, v(g_i))$ and $(j, v(g_j))$ with $i < j$. Let $m = \frac{v(i)-v(j)}{i-j}$ be the slope of I and assume that the slopes in the intervals $[i-1, i]$ and $[j, j+1]$ are different from m. Then there are exactly $t = j - i$ distinct roots $\alpha_1, \ldots, \alpha_t$ of $g(z)$ in K^{ac} with $v_L(\alpha_1) = \cdots = v_L(\alpha_t) = -m$, where L is the splitting field of $\alpha_1, \ldots, \alpha_t$ and v_L is the unique extension of v to L.

Moreover the polynomial $h(z) = \prod_{i=1}^{t}(z - \alpha_i)$ is a polynomial

in $K[z]$ and $h(z)|g(z)$.

We are going to see the case $K = \mathbb{F}_q(x)$ in more details in the next section.

3.2 Carlitz modules

In the sequel we denote by R the polynomial ring $\mathbb{F}_q[x]$ contained in the rational function field K and by K^{ac} an algebraic closure of K.

Let $\alpha \in End_{\mathbb{F}_q}(K^{ac})$ the endomorphism $\alpha(y) = y^q + xy$, for $y \in K^{ac}$. We define the ring endomorphism $\phi : R \to End_{\mathbb{F}_q}(K^{ac})$ by

$$\phi(f(x))(y) = f(\alpha)(y),$$

for $y \in K^{ac}$. In this way K^{ac} is an R-module and the action of $f \in R$ is

$$f(y) = \phi(f)(y),$$

for $y \in K^{ac}$. In the sequel, when there is no ambiguity, we denote the action $\phi(f)(y)$ simply by y^f.

The following properties are obvious

Lemma 3.3. Let y and z be elements in K^{ac}. For any $a \in \mathbb{F}_q$ and f, $g \in R$ we have:

1. $y^a = ay$;

2. $y^{f+g} = y^f + y^g$;

3. $(y^f)^g = y^{fg}$;

4. $(y+z)^f = y^f + z^f$.

When $f \in R$ and n is an integer, we define the polynomial $[f, n]$ by the following properties

1. $[f, n] = 0$ if $f = 0$ or if $n < 0$ or $n > deg(f)$;

2. $[f, 0] = f$;

3. $[x^{d+1}, n] = x[x^d, n] + [x^d, n-1]^q$;

4. $[af+bg, n] = a[f, n]+b[g, n]$, for any a, $b \in \mathbb{F}_q$ and f, $g \in R$.

The proof of the following Lemma follows directly from the properties of $[f, n]$.

Lemma 3.4. Let $f \in R$ be a polynomial of degree $n > 0$. Then $[f, i]$ is well-defined for any integer i. Moreover

$$deg([f, i]) = (d-i)q^i$$

for $0 \leq i \leq d$ and

$$y^f = \sum_{i=0}^{d} [f, i] y^{q^i}$$

for all $y \in K^{ac}$.

Definition 3.8. Let f be a non-zero polynomial in R. The subset $\Lambda_f = \{y \in K^{ac} |\ y^f = 0\}$ of K^{ac} is a Carlitz module. The splitting field $K(\Lambda_f)$ is called the cyclotomic function field over K with modulus f.

The set Λ_f is an R-submodule of K^{ac}. The derivative of the polynomial y^f with respect to y is f by the previous Lemma so the extension $K(\Lambda_f)/K$ is finite and separable. Moreover $K(\Lambda_f)/K$ is a Galois extension because the action of $\sigma \in Gal(K^{ac}/K)$ on y commutes with the action of f.

Lemma 3.5. Let $f \in R$ be an irreducible monic polynomial and $n > 0$ be an integer. Then Λ_{f^n} is a cyclic R-module isomorphic to $R/(f^n)$.

Proof. Before we assume $n = 1$. Let d be the degree of f. Then Λ_f has exactly q^d elements in K^{ac}. Moreover Λ_f is a $R/(f)$ module, but $R/(f)$ is a finite field with q^d elements so $\Lambda_f \cong R/(f)$ is a cyclic R-module.

Now assume the result holds for $n-1$. Consider $\Lambda_{f^{n-1}} \cong R/(f^{n-1})$. Then $\Lambda_{f^{n-1}}$ is a cyclic module generated by λ. We get a morphism $\beta : \Lambda_{f^n} \to \Lambda_{f^{n-1}}$ by $\beta(y) = y^f$. Then the kernel of β is Λ_f. There is an element $z \in K^{ac}$ such that $z^f = \lambda$ so

$z \in \Lambda_{f^n}$ and β is surjective. Moreover such z does not belong to $\Lambda_{f^{n-1}}$. We show that z generates Λ_{f^n}. Let y be an element of Λ_{f^n}. Then $y^f = \lambda^g$ for a suitable $g \in R$ because $y^f \in \Lambda_{f^{n-1}}$. So $y^f = (z^f)^g = (z^g)^f$ and $y - z^g \in \Lambda_f$. But Λ_f is generated by $z^{f^{n-1}}$ so $y - z^g = (z^{f^{n-1}})^h$ for a suitable $h \in R$. It follows that $y = z^g + z^{hf^{n-1}} = z^{g+hf^{n-1}}$ and z generates Λ_{f^n}. Finally the morphism $g \to z^g$ is clearly an R-module isomorphism between $R/(f^n)$ and Λ_{f^n}. □

We have a similar result for f reducible.

Lemma 3.6. Let f, $g \in R$ two monic polynomials and let h be the greatest common divisor $\gcd(f, g)$. Then $\Lambda_f \cap \Lambda_g = \Lambda_h$.

Proof. It follows from the properties stated in Lemma 3.3 and from the Bézout identity for the greatest common divisor. □

Corollary 3.1. Let f and g be two monic coprime polynomials in R. Then $\Lambda_{fg} = \Lambda_f + \Lambda_g$.

Proof. Of course $\Lambda_f + \Lambda_g \subseteq \Lambda_{fg}$. But $|\Lambda_{fg}| = q^{deg(f)+deg(g)} = |\Lambda_f + \Lambda_g|$ because $\Lambda_f \cap \Lambda_g = \Lambda_1 = \{0\}$ by the previous Lemma so the inclusion is an equality. □

Corollary 3.2. Let $f \in R$ be a non-zero monic polynomial. Then Λ_f is a cyclic module isomorphic to $R/(f)$.

Proof. Write the factorization of $f = \prod_{i=1}^{k} f_i^{n_i}$ in irreducible polynomials. Then $\Lambda_f = \Lambda_{f_1^{n_1}} + \ldots + \Lambda_{f_k^{n_k}}$ by the previous Corollary. But $\Lambda_{f_i{}^{n_i}}$ is a cyclic R-module generated by, say, λ_i for $i = 1, 2, \ldots, k$ so $\lambda = \lambda_1 + \ldots + \lambda_k$ is a generator of Λ_f. □

Now we can compute the Galois group of the extension $K(\Lambda_f)/K$. Let $\prod_{i=1}^{k} f_i^{n_i}$ be the factorization in irreducibles of the monic polynomial $f \in R$ and let $U(f) = (R/(f))^*$ be the group of units in $R/(f)$. Then $U(f)$ is a multiplicative group. Its order $u(f)$ is

$$u(f) = q^{deg(f)} \prod_{i=1}^{k} (1 - q^{-deg(f_i)}).$$

Lemma 3.7. Let $f \in R$ be a monic irreducible polynomial and $n > 0$ be a positive integer. Then the degree $[K(\Lambda_{f^n}) : K]$ is equal to $u(f^n)$ and the Galois group $Gal(K(\Lambda_{f^n})/K)$ is isomorphic to $U(f^n)$. Moreover the place P corresponding to f is totally ramified in $K(\Lambda_{f^n})/K$ and all the other finite places are unramified.

Proof. Let λ be a generator of Λ_{f^n}. We show that λ^g is an other generator of Λ_{f^n} if and only if $\gcd(f, g) = 1$.

When $\gcd(f, g) \neq 1$ then $f|g$ so $\lambda^g \in \Lambda_{f^{n-1}}$ so g is not a generator of Λ_{f^n}.

When $\gcd(f, g) = 1$ then $af + bg = 1$ for suitable a and b in R. So $\lambda = \lambda^{bg} = (\lambda^g)^b$ and λ^g is a generator.

It follows that λ^g is a root of the polynomial $c(z) = \frac{z^{f^n}}{z^{f^{n-1}}}$ in $K^{ac}[z]$. But

$$\deg(c(z)) = q^{\deg(f^n)} - q^{deg(f^{n-1})} = q^{deg(f^n)}(1 - q^{-deg(f)}) = u(f^n)$$

so

$$c(z) = \prod_{g \in U(f^n)} (z - \lambda^g) \tag{3.1}$$

and

$$f = \frac{f^n}{f^{n-1}} = c(0) = (-1)^{u(f^n)} \prod_{g \in U(f^n)} \lambda^g. \tag{3.2}$$

Let Q be a place of $K(\Lambda_{f^n})$ over the place P of K corresponding to the irreducible polynomial f and let $e = e(Q|P)$ be the ramification degree of the place P in $K(\Lambda_{f^n})/K$. Then $e = v_Q(f) = \sum_{g \in U(f)} v_Q(\lambda^g) \geq u(f^n)$ because $\lambda^{f^n} = 0$ and so $v_Q(\lambda) \geq 1$ and $v_Q(\lambda^g) \geq 1$ for any $g \in U(f)$. It follows that $e \geq u(f)$. But $e \leq [K(\Lambda_{f^n}) : K] \leq deg(c) = u(f)$ so the equality holds.

The morphism from $Gal(K(\Lambda_{f^n})/K)$ to the set of generators of Λ_{f^n} which sends $\sigma \in Gal(K(\Lambda_{f^n})/K)$ to $\sigma(\lambda)$ is injective, because λ is a generator of Λ_{f^n}, and surjective because a polynomial h determines an automorphism $\sigma(z) = z^h$ in $Gal(K(\Lambda_{f^n})/K)$ if and only if $h \in U(f^n)$. So

$$Gal(K(\Lambda_{f^n})/K) \cong U(f^n).$$

Finally let g be an irreducible prime polynomial in R prime to f. Let S be a place of $K(\Lambda_{f^n})$ over the place of K corresponding to (g). We show that $v_S(\lambda) \geq 0$. In fact if $v_S(\lambda) < 0$ then, by Lemma 3.4,

$$v_S(\lambda^{f^n}) = v_S(\lambda^{q^{\deg(f^n)}}) < 0,$$

because $v_S([f^n, i]) = 0$ for $i = 0, \ldots, \deg(f^n)$. But $\lambda^{f^n} = 0$ so we get a contradiction. In a similar way we get that $v_S(\lambda^h) \geq 0$ for any $h \in R$.

We apply the Lemma 3.4 to the relation $c(z)z^{f^{n-1}} = z^{f^n}$ and we get $c'(z)z^{f^{n-1}} + c(z)f^{n-1} = f^n$. It follows that

$$c'(\lambda)\lambda^{f^{n-1}} = f^n$$

and so the valuation

$$v_S(c'(\lambda)) = v_S(f^n) - v_S(\lambda^{f^{n-1}}) = -v_S(\lambda^{f^{n-1}}) \leq 0.$$

But $v_S(c'(\lambda)) \geq 0$ because $v_S(\lambda) \geq 0$ so the equality follows. It follows from [4], Chapter I, Section 4, that the place S is not ramified. □

Lemma 3.8. Let f and g be two monic coprime polynomials in R. Then $K(\Lambda_{fg})$ is the compositum field $K(\Lambda_f)K(\Lambda_g)$.

Proof. It follows from Corollary 3.1 and 3.2. □

Corollary 3.3. Let $f \in R$ be a monic polynomial.

1. The degree $[K(\Lambda_f) : K]$ is equal to $u(f)$ and

$$Gal(K(\Lambda_f)/K) \cong (R/(f))^*.$$

2. Let $g \in R$ be an irreducible monic polynomial and let P the finite place corresponding to g. Then P is unramified in $K(\Lambda_f)/K$ if g does not divide f. In this case the Frobenius morphism $Frob(P) \in Gal(K(\Lambda_f)/K)$ satisfies

$$Frob(P)(\lambda) = \lambda^g,$$

where λ is a generator of Λ_f as R-module. The inertia degree of P in $K(\Lambda_f)/K$ is the multiplicative order of the image of g in $R/(f)$.

3. If $g \in R$ is an irreducible monic polynomial that divides f then the corresponding place P is ramified in $K(\Lambda_f)/K$ and the ramification degree is equal to $u(g^n)$ where g^n is the maximum power of g such that g^n divides f. The inertia degree $f(P)$ of the place P in $K(\Lambda_f)/K$ is equal to the multiplicative order of the image of g in the quotient group $R/(\frac{f}{g^n})$.

Proof. The first part follows from the last two Lemmas.

For the second part, we know by definition that

$$Frob(P)(\lambda) \equiv \lambda^{q^{\deg g}} \mod Q,$$

where Q is a place of $K(\Lambda_f)$ over the place P. In particular $\lambda^g \equiv Frob(P)(\lambda) \mod Q$ by Lemma 3.4 and by property 3 of $[g, i]$. By Lemma 3.7 we know that $Frob(P)(z) = z^h$ for a suitable polynomial $h \in U(f)$. We have to show that $\lambda^h \equiv \lambda^g \mod Q$ implies $h = g$. But this follows from the equation (3.1), in fact if we take the derivative of both sides then

$$f = c'(z) = \sum_{t' \in R/(f)} \prod_{t \neq t'} (z - \lambda^t)$$

and valuating $c(z)'$ in $z = \lambda^g$ we get

$$f = \prod_{t \in R/(f), t \neq \overline{g}} (\lambda^g - \lambda^t) \neq 0,$$

where $\overline{g}$ is the image of g in $R/(f)$. Then

$$g \not| f$$

implies that

$$\lambda^t \not\equiv \lambda^g \mod Q$$

whenever $t \not\equiv \overline{g}$ in $R/(f)$. So

$$Frob(P)(z) = z^g$$

and the inertia degree is the order of the Frobenius automorphism in $Gal(K(\Lambda_f)/K)$. By Lemma 3.7 the order of $Frob(P)$ is the order of $\overline{g}$ in $R/(f)$.

Finally if $f = g^n g'$ and $\gcd(g, g') = 1$, then P is totally ramified in $K(\Lambda_{g^n})/K$ and unramified in $K(\Lambda_{g'})/K$. The result follows from part 2 and from the previous Lemma. □

A different result holds for the infinite place P_∞.

Proposition 3.2. Let $f \in R$ be a monic irreducible polynomial of degree d. Then the infinite place P_∞ is partially ramified in $K(\Lambda_f)/K$. The inertia group $I(P_\infty)$ has order $e(P_\infty) = q-1$ and there are $\frac{q^d-1}{q-1}$ places over P_∞ so $f(P_\infty) = 1$ and $I(P_\infty) = D(P_\infty)$.

Proof. Let Q be a place of $K(\Lambda_f)$ over the place P_∞. Let λ be a generator of Λ_f and let L be the completion of $K(\Lambda_f)$ over the place Q. Let Q' be the place of L over Q. Let $c(z)$ be the minimal polynomial of λ in K. Then $e(Q'|P_\infty) = e(Q|P_\infty) = e(P_\infty)$ because the extension is Galois and

$$c(z) = c_0 + c_1 z^{q-1} + \ldots + c_d z^{q^d-1}$$

with $c_i \in R$ and $\deg(c_i) = (d-i)q^i$ for $i = 0, \ldots, d$ by Lemma 3.4. So the Newton polygon over L has vertexes

$$(q^i - 1, v_{Q'}(c_i)) = (q^i - 1, -(d-i)q^i e(P_\infty)),$$

for $i = 0, 1, \ldots, d$. We apply the Lemma 3.2 to the segment I connecting $(0, -de(P_\infty))$ and $(q-1, -(d-1)qe(P_\infty))$ so there are exactly $q-1$ roots $\alpha_1, \ldots, \alpha_{q-1} \in L^{ac}$ of $c(z)$ of valuation $e(P_\infty)\frac{q(d-1)-d}{q-1}$. But $q(d-1)-d \equiv d-1-d \equiv -1 \mod q-1$ so $q-1|e(P_\infty)$.

Let F be the completion of K respect to the valuation v_{P_∞}. We apply Lemma 3.2 to the polynomial $c(z)$ over the field F. The polynomial $h(z) = \prod_{i=1}^{q-1}(z-\alpha_i)$ belongs to $F[z]$ and $h(z)|c(z)$. But the extension F/K is Galois so $c(z)$ splits in factors of degree $q-1$ and there are at least $\frac{q^d-1}{q-1}$ places in $K(\Lambda_f)$ over P_∞. It follows that $e(P_\infty) = q-1$. □

Corollary 3.4. Let $f \in R$ be a monic irreducible polynomial and let $n > 0$ be a positive integer. Then the place P_∞ is partially ramified in $K(\Lambda_{f^n})/K$. The inertia group $I(P_\infty)$ has order $e(P_\infty) = q-1$ and there are $\frac{u(f^n)}{q-1}$ places over P_∞ so $f(P_\infty) = 1$ and $I(P_\infty) = D(P_\infty)$. In particular the constant field of $K(\Lambda_{f^n})$ is $\mathbb{F}_q$.

Proof. Similar to Corollary 3.3. □

From now on, given a monic polynomial $f \in R$, we consider the subfield $K(\Lambda_f)^{I(P_\infty)}$ fixed by $I(P_\infty)$, where $I(P_\infty)$ is the in-

ertia group of P_∞. By the previous Corollary, the extension $K(\Lambda_f)^{I(P_\infty)}/K$ is a Galois extension of degree $\frac{u(f)}{q-1}$, unramified outside the finite places dividing f, such that the infinite place P_∞ is completely split. In other words $K(\Lambda_f)^{I(P_\infty)}$ is the ray class field $K^{\mathfrak{f}}_{P_\infty}$, where the divisor $\mathfrak{f} \in \mathcal{D}_K$ is the set of zeros of f that is the sum with multeplicities of the places corresponding to the irreducible polynomials dividing f.

Example 3.1. Let $q = 2$ and $f = x^3 + x + 1$. Then

$$y^f = y^8 + (x^4 + x^2 + x)y^4 + (x^4 + x^3 + x^2 + 1)y^2 + (x^3 + x + 1)y.$$

Let $z \in K^{ac}$ be a non-zero element in Λ_f. So

$$z^7 + (x^4 + x^2 + x)z^3 + (x^4 + x^3 + x^2 + 1)z + (x^3 + x + 1) = 0.$$

Then $K(\Lambda_f) = K^{\mathfrak{f}}_{P_\infty} = \mathbb{F}_q(x, z)$ and the function field extension $K^{\mathfrak{f}}_{P_\infty}/K$ has degree $u(f) = 2^3(1 - \frac{1}{8}) = 7$. By the Hurwitz genus formula (2.1), the genus of $K^f_{P_\infty}$ is

$$g = 1 - u(f) + \frac{1}{2}deg(f)(u(f) - 1) = 3$$

because the place $\mathfrak{f}$ is totally ramified and the ramification is tame.

A similar construction holds when P_∞ is not the infinite place. We will see in a later section that we can get finitely many different field extensions (see Theorem 4.1).

When K is not the rational function field, the previous construction can be generalized by means of Drinfeld modules, see [8] for further details.

In the sequel we will often use the following formulas for the degree and the genus of a ray class field extension of an arbitrary function field K (see [2] Chapter 2, Section 5).

Theorem 3.3. Let K be a function field over the constant field $\mathbb{F}_q$ of genus g_K and let h_K be the divisor class number of K. Let S be a place of degree d and $\mathfrak{m} = \sum_{i=1}^{k} m_i P_i$ be an effective divisor of K where P_i are distinct places of degree n_i for $i = 1, ..., k$ such that $S \notin Supp(\mathfrak{m})$ and $k \geq 0$ is a non negative integer (we set $\mathfrak{m} = 0$ when $k = 0$). Then the ray class field $K_S^{\mathfrak{m}}$ is a function field over $\mathbb{F}_{q^d}$. The degree $[K_S^{\mathfrak{m}} : K]$ is equal to

$$dh_K \prod_{i=1}^{k} \frac{(q^{n_i} - 1)q^{(m_i-1)n_i}}{q-1}$$

if $k > 0$ and dh_K otherwise. The genus $g_{K_S^{\mathfrak{m}}}$ of $K_S^{\mathfrak{m}}$ is given by

$$g_{K_S^{\mathfrak{m}}} = 1 + h_K(g_K - 1), \tag{3.3}$$

if $deg(\mathfrak{m}) \leq 1$,

$$g_{K_S^{\mathfrak{m}}} = 1 + \frac{h_K(q^n - 1)(g_K - 1)}{q-1} + \frac{h_K n(q^n - q)q^{n(m-1)}}{2(q-1)}, \tag{3.4}$$

if $k = 1$, the degree of P is n and $\mathfrak{m} = mP$ with $deg(\mathfrak{m}) > 1$,

$$g_{K_S^{\mathfrak{m}}} = 1+\frac{h_K \prod_i (q^{n_i}-1)}{2(q-1)}(2g_K-2+deg(\mathfrak{m})-\sum_i \frac{deg(P_i)q^{(m_i-1)n_i}}{q^{n_i}-1}), \tag{3.5}$$

otherwise.

Chapter 4

Ray class fields

In the sequel K is a function field with constant field $\mathbb{F}_q$.

It is a well-known fact that the maximal unramified abelian extension of K is infinite because it contains all the possible constant field extension. From now on we consider only unramified abelian extensions of K with constant field $\mathbb{F}_q$. Let $h = h_K$ be the divisor class number of K. Then h is the degree of every maximal unramified abelian extension of K with constant field $\mathbb{F}_q$. There are exactly h such extensions of K (see [1], Chapter 8). We denote them by $K_1^0, \ldots, K_h^0$.

In this section we prove a similar result concerning also ramified extensions and point out some consequences.

Theorem 4.1. Let $\mathfrak{m} = \sum_{i=1}^{t} m_i P_i$ be an effective divisor and

let n_i be the degree of P_i for $i = 1, \ldots, t$. We set $\mathfrak{m} = 0$ if $t = 0$. We set also $d = \frac{h_K}{q-1} \prod_{i=1}^{t} (q^{n_i} - 1) q^{(m_i - 1)n_i}$ if $t > 0$ and $d = h_K$ otherwise. Then there are exactly d abelian extensions of K of degree d with conductor $\mathfrak{m}$ and constant field $\mathbb{F}_q$.

As before we denote such extensions by $K_1^{\mathfrak{m}}, \ldots, K_d^{\mathfrak{m}}$. There is no conflict with the previous notation because the result concerning unramified extensions can be seen as a special case of the previous Theorem.

Proof. In order to apply the Artin reciprocity Theorem 3.1 we construct suitable subgroups of the Class group C_K.

Let U_0 be the subset of J_K given by

$$U_0 = \{(x_P)_{P \in \mathcal{P}_K} \in J_K | x_P \in \hat{U}_P^* \text{ for all places } P \in \mathcal{P}_K\}$$

and let $U_{\mathfrak{m}}$ be the subset of U_0 given by

$$U_{\mathfrak{m}} = \{(x_P)_{P \in \mathcal{P}_K} \in U_0 | x_P \equiv 1 \mod t_i^{m_i} \text{ for all } i = 1, \ldots, t\},$$

where t_i is an element in K_{P_i} with $v_{P_i}(t_i) = 1$ for $i = 1, \ldots, t$. As before we set $U_{\mathfrak{m}} = U_0$ if $\mathfrak{m} = 0$. The field K^* is canonically embedded in J_K and we denote it again with K^* as in the previous Chapter. Let $C_{\mathfrak{m}} = U_{\mathfrak{m}}/(K^* \cap U_{\mathfrak{m}})$ be the classes of $U_{\mathfrak{m}}$ in C_K.

Let D_0 be the subgroup of C_K of classes of ideles $x = (x_P)_{P \in \mathcal{P}_K}$ such that the divisor

$$Div(x) = \sum_{P \in \mathcal{P}_K} v_P(x_P)P$$

has degree 0. It follows from the definition of idele that $Div(x)$ is a finite sum for all non zero $x \in J_K$ and D_0 is well-defined because the principal divisors have degree 0. Moreover $U_0 \subseteq D_0$.

The following sequence is exact (see [1], Chapter 8):

$$0 \to D_0 \to C_K \to \mathbb{Z} \to 0, \tag{4.1}$$

where the map $C_K \to \mathbb{Z}$ is the degree of the divisor and it is surjective by the Schmidt Theorem (see [15], Chapter V). Let D be a divisor of degree 1. It is very easy to construct a class $x \in J_K$ such that $Div(x) = D$. Let $[x] \in C_K$ be the class of x in C_K. The subgroup generated by $C_{\mathfrak{m}} \cup [x]$ in C_K has finite index $c = |D_0/C_{\mathfrak{m}}| = \frac{h_K}{q-1} \prod_{i=1}^{t} (q^{n_i} - 1) q^{(m_i - 1)n_i}$ if $t > 0$ and $c = h_K$ if $t = 0$. In particular $c = d$. Let $a_1, \ldots, a_d$ be the representatives of the cosets of $C_{\mathfrak{m}}$ in D_0. Then the subgroups B_i of C_K generated by $C_{\mathfrak{m}} \cup ([x] + a_i)$ are d distinct subgroups of C_K of index d such that the image onto $\mathbb{Z}$ in (4.1) is surjective.

Let $K_1^{\mathfrak{m}}, \ldots, K_d^{\mathfrak{m}}$ be the function fields corresponding to the subgroups $B_1, \ldots, B_d$ by the Artin map. By Theorem 3.1 they

are abelian extensions of K of degree d. The constant field is $\mathbb{F}_q$ by Theorem 3.1 because B_i contains the element $[x]+a_i$ of degree 1 for $i = 1, \ldots, d$ and so it is not contained in the norm group $\mathcal{N}_K^{\mathbb{F}_{q^j}K}$ for any $j > 1$. Moreover they are unramified outside $\mathfrak{m}$ by Theorem 3.2.

We show that $K_1^{\mathfrak{m}}, \ldots, K_d^{\mathfrak{m}}$ are all the abelian extensions of K satisfying the hypothesis of the Theorem. Let L/K be an other such extension and let G be the Galois group of L/K. Let M be the norm group $\mathcal{N}_K^L$. By Theorem 3.1 G is isomorphic to C_K/M and M is a subgroup of C_K of index d containing $C_{\mathfrak{m}}$ such that there is an idele $y \in J_K$ such that the class $[y]$ is in M and $deg(Div(y)) = 1$. Then $D - Div(y)$ has degree 0 and so $[x] - [y]$ belongs to one coset $a_i + C_{\mathfrak{m}}$ for a suitable $i \in \{1, 2, \ldots, d\}$. But $M' = C_{\mathfrak{m}} \cup [y]$ is a subgroup of $M \cap B_i$ and the index of M' in C_K is d so $M = M' = B_i$ and $L = K_i^{\mathfrak{m}}$. □

Remark 4.1. The proof of the previous Theorem shows that the extensions $K_1^{\mathfrak{m}}, K_2^{\mathfrak{m}}, \ldots, K_d^{\mathfrak{m}}$ of K are all contained in the constant field extension of degree d of any one of them, say $K_1^{\mathfrak{m}}\mathbb{F}_{q^d}$. In fact the compositum of function fields $K_i^{\mathfrak{m}}K_j^{\mathfrak{m}}$ corresponds to the intersections $B_{i,j} = B_i \cap B_j$ in C_K by the Artin reciprocity map

for $i, j \in \{1, \ldots, d\}$. The image of the valuation of $B_{i,j}$ by the degree map in (4.1) is a subgroup of $\mathbb{Z}$ of finite index $d'|d$. In particular $K_i^{\mathfrak{m}} K_j^{\mathfrak{m}} = K_i^{\mathfrak{m}} \mathbb{F}_{q^{d'}}$.

Remark 4.2. When the quotient group $D_0/C_{\mathfrak{m}}$ is cyclic we can say something more about the subextensions of $K_i^{\mathfrak{m}}$ containing K for $i = 1, \ldots, d$. In fact let l be a divisor of d. Then there is only one subgroup G of $D_0/C_{\mathfrak{m}}$ of index l. Let g_1, ..., g_l be the cosets representatives of G in $D_0/C_{\mathfrak{m}}$. We denote by F_i the fields corresponding by the Artin reciprocity map to the subgroups G_i of C_K generated by $G \cup ([x]+g_i)$ for $i = 1, \ldots, l$. The field extensions F_i/K are all the abelian extensions of degree l unramified outside $\mathfrak{m}$ with constant field $\mathbb{F}_q$ for $i = 1, \ldots, l$.

Corollary 4.1. Let $\mathfrak{m}$ be an effective divisor and d a positive integer as in the previous Theorem. Let P be a place of K of degree d', let l be the positive integer $\gcd(d, d')$ and $P_i|P$ be a place of $K_i^{\mathfrak{m}}$ over P for $i \in \{1, \ldots, d\}$. If $D_0/C_{\mathfrak{m}}$ is a cyclic group then $f(P_i|P) = 1$ in at most l such extensions $K_i^{\mathfrak{m}}/K$.

Proof. Assume that the place P is totally split in $K_i^{\mathfrak{m}}/K$ for at least one $i \leq d$, otherwise the proof would be trivial. Then P is split in $K_j^{\mathfrak{m}}/K$ for $j \neq i$ if and only if P is totally split in

the compositum $K_i^{\mathfrak{m}}K_j^{\mathfrak{m}}/K$. But $K_i^{\mathfrak{m}}K_j^{\mathfrak{m}} = K_i^{\mathfrak{m}}\mathbb{F}_{q^a}$ for a suitable integer $a|d$ by Remark 4.1. By the properties of the constant field extensions this is possible only when $a|d'$ and so $a|l$ and $K_j^{\mathfrak{m}} \subseteq K_i^{\mathfrak{m}}\mathbb{F}_{q^l}$.

It follows from the proof of the previous Theorem that

$$l \cdot ([x] + a_i) \subseteq B_j$$

and so $l \cdot (a_i - a_j) \in C_{\mathfrak{m}}$ and the class of $l \cdot a_j$ in the quotient group $D_0/C_{\mathfrak{m}}$ is the class of $l \cdot a_i$. It is very easy to see that when $D_0/C_{\mathfrak{m}}$ is a cyclic group generated by g the only classes a_j such that the class of $l \cdot a_j$ is the same class of $l \cdot a_i$ are the classes of the elements $a_i + \frac{td}{l} \cdot g$ for $t = 0, \ldots, l-1$ so there are at most l such classes $a_j \in D_0/C_{\mathfrak{m}}$ and there are at most l corresponding fields extensions by the previous Theorem. □

Remark 4.3. When $D_0/C_{\mathfrak{m}}$ is not a cyclic group the Theorem does not hold. As an example consider $\mathfrak{m}$ be a sum of two places of degree m of the rational function field $\mathbb{F}_q(x)$. Then a place P of degree d' with $\frac{q^m-1}{q-1}|d'$ can be split in all the d extensions $K_i^{\mathfrak{m}}/K$ where $d = \frac{(q^m-1)^2}{q-1}$.

The previous Corollary can be generalized in the following result.

Corollary 4.2. Assume the quotient group $D_0/C_{\mathfrak{m}}$ be cyclic as in Corollary 4.1 and let s be a prime dividing d and let t be the maximal power of s dividing d. Let F_i/K be the extensions of degree t for $i = 1, \ldots, t$ as in the Remark 4.2. Let P be a place of K of degree d' and $P_i|P$ be a place of F_i over P. Let l be the $\gcd(d', t)$ and let $c \geq 0$ be the exponent such that $\frac{t}{l} = s^c$. Assume $c \geq 1$. Then for each positive integer $j \leq c$, the integer s^j divides $f(P_i|P)$ in at least $l(s^c - s^{j-1})$ such extensions F_i/K.

Proof. Let j' denote the number ls^{c-j+1} and E_1/K, ..., $E_{j'}/K$ be the extensions of K unramified outside $\mathfrak{m}$ of degree j' over K by Corollary 4.1. If $s^j \not| f(P_i|P)$ for a certain $i \in \{1, \ldots, t\}$ then the Frobenius $Frob(P)$ of P in F_i/K has order dividing s^{j-1}. Let $E_{i'}/K$ be the only subfield of F_i of degree j' over K and let $P'_{i'}$ be the place under P_i in $E_{i'}$. Then $Frob(P'_{i'}) = Frob(P_i)^{j-1} = 1$ so $f(P'_{i'}|P) = 1$. By Corollary 4.1 there are at most l such extensions E_i/K such that $f(P'_i|P) = 1$, say, E_1/K, ..., E_l/K. There are exactly s^{j-1} extensions F_i/K over each $E_{i'}$ so $s^j \not| f(P_i|P)$ in at most ls^{j-1} extensions F_i/K and the Corollary follows. □

Remark 4.4. In the previous Corollary when $j = c$ we obtain that $\frac{t}{l}$ does not divide $f(P_i|P)$ in atmost $\frac{t}{s}$ extensions F_i/K.

4.1 An other proof of the Clark Elkies bound

When K is the rational function field $\mathbb{F}_q(x)$, we get as a Corollary a result similar to the one of Clark and Elkies cited in [9].

In what follows we denote by a_d the number of places of $\mathbb{F}_q(x)$ of degree d. Of course we have $\sum_{d<n} a_d \leq 1 + \sum_{d=1}^{n} \frac{q^d}{d} \leq \frac{q^n-1}{q-1}$ but this bound is too rough.

Lemma 4.1. The number of places of $\mathbb{F}_q(x)$ of degree strictly smaller than n is at most $q \cdot \frac{q^n}{n}$ when $n \geq 1$.

Proof. We prove it by induction over n. When $n = 1$ the result is trivial. When $n = 2$ we have

$$a_1 = q + 1 \leq \frac{q(q+1)}{2} \leq q \cdot \frac{q^2}{2}$$

and the result holds for every $q \geq 2$. When $n = 3$ there are

$$a_1 + a_2 = q + 1 + \frac{q^2 - q}{2} = \frac{q^2 + q + 2}{2} \leq q \cdot \frac{q^3}{3}$$

places of degree smaller than 3 and the result still holds when $q \geq 2$.

Suppose that $\sum_{d<n} a_d \leq q \cdot \frac{q^n}{n}$, then

$$\sum_{d<n+1} a_d \leq q \cdot \frac{q^n}{n} + \frac{q^n}{n} = (q+1)\frac{q^n}{n} \leq q \cdot \frac{q^{n+1}}{n+1}$$

when $n \geq 3$. □

Corollary 4.3. For any finite field $\mathbb{F}_q$ there is a positive integer n_0 such that, for any $n > n_0$, there is a projective curve over $\mathbb{F}_q$ of genus $g < \frac{(n-2)q^n}{2(q-1)}$ without points of degree strictly smaller than n.

Proof. Let $\mathfrak{m}$ be a finite place of $K = \mathbb{F}_q(x)$ of degree $n > 1$ corresponding to the polynomial $f \in \mathbb{F}_q[x]$ and let $d = \frac{q^n-1}{q-1}$. The quotient group $D_0/C_{\mathfrak{m}}$ is isomorphic to $\mathbb{F}_q[x]^*/(f)$ (see also [14], Chapter 1). In particular $D_0/C_{\mathfrak{m}}$ is a cyclic group. By Remark 4.2 there are d distinct totally ramified subextensions $K_i^{\mathfrak{m}}$ of K of degree d with constant field $\mathbb{F}_q$ for $i = 1, \ldots, d$.

We count the number of ray class field extensions $K_i^{\mathfrak{m}}/K$ with at least one partially split place P of degree $deg(P) < n$ and $f(P_i|P) < \frac{n}{deg(P)}$ where P_i is a place of $K_i^{\mathfrak{m}}$ over P.

Let t be a positive integer smaller than n such that $t|d$. Let P be a place of K of degree $d' < n$ and let $l = \gcd(t, d')$. By Corollary 4.1 there are at most l extensions $K_i^{\mathfrak{m}}/K$ for $i = 1, \ldots, d$ such that P is totally split in a subextension of degree t and so $f(P_i|P) \leq \frac{d}{t}$. We sum the number of all these possible subextensions with (potentially) at least one place of degree smaller than n for all P of degree d' and t dividing d. There are at most $\frac{q \cdot q^{n/t}}{n/t}$ places of degree smaller than $\frac{n}{t}$ so there is at least one $K_i^{\mathfrak{m}}$ without

place of degree smaller than n whenever

$$\sum_{t|k,\, t<n} \sum_{d'=1}^{[n/t]} \gcd(t, d') a_{d'} < d \tag{4.2}$$

But the last formula holds when n is large because the left hand side in (4.2) is smaller than

$$\sum_{t|k,\, t<n} t \cdot \frac{q \cdot q^{n/t}}{n/t} \leq$$

$$\frac{q \cdot q^n}{n} + \sum_{t=2}^{n-1} t \cdot \frac{q \cdot q^{n/t}}{n/t} \leq$$

$$\frac{q \cdot q^n}{n} + 2q(n-2)\frac{q^{n/2}}{n/2},$$

where the last inequality follows from

$$t \cdot \frac{q^{n/t}}{n/t} \leq 2 \cdot \frac{q^{n/2}}{n/2}$$

whenever $t \geq 2$ and n is large. In particular we get

$$\sum_{t|k,\, t<n} \sum_{d'=1}^{[n/t]} \gcd(d', t) a_{d'} \leq \frac{q \cdot q^n}{n} + 4q \cdot q^{n/2} < \frac{q^n - 1}{q - 1} = d,$$

when n is large.

The divisor class number of the rational function field is 1, by the Hurwitz genus formula (2.1), so the genus g of $K_i^{\mathfrak{m}}$ may be computed by the formula (3.4)

$$g = 1 - \frac{q^n - 1}{q - 1} + \frac{n(q^n - q)}{2(q-1)} = \frac{nq^n - 2q^n - nq + 2q}{2(q-1)} < \frac{(n-2)q^n}{2(q-1)}.$$

The result now follows. □

Remark 4.5. It is very easy to estimate the integer n_0. In fact one can prove that $n_0 = [6\log_q(9/4)] < 14$ is a possible value of n_0.

Example 4.1. We set $q = 2$ and $n = 2$. Let $\mathfrak{m}$ be the place

$$\mathfrak{m} = (x^3 + x + 1)$$

of $K = \mathbb{F}_2(x)$. There are 7 distinct, totally ramified at $\mathfrak{m}$, subextensions $K_i^{\mathfrak{m}}/K$ of degree 7 with constant field $\mathbb{F}_2$. These fields, up to the order, satisfy $K_i^{\mathfrak{m}} \subseteq K_{S_i}^{\mathfrak{m}}$ where $S_1 = \{(x)\}$, $S_2 = \{(x+1)\}$, $S_3 = \{(x^2+x+1)\}$, $S_4 = \{(x^4+x+1)\}$, $S_5 = \{(x^4+x^3+1)\}$, $S_6 = \{(x^4+x^3+x^2+x+1)\}$ and $S_7 = \{(\frac{1}{x})\}$ is the infinite place.

The reader can easily check that all the places of degree prime to 7 split exactly in one of the extensions $K_i^{\mathfrak{m}}$ given above, see also the following Example. We have already seen in the Example 3.1 that the genus of $K_i^{\mathfrak{m}}$ is 3 for $i = 1, \ldots, 7$.

In this manner we obtain three distinct curves (corresponding to the function fields $K_4^{\mathfrak{m}}$, $K_5^{\mathfrak{m}}$ and $K_6^{\mathfrak{m}}$) of genus 3 without points of degree 1 or 2. These examples of curves without points of degree 1 or 2 are the ones with the smallest genus.

Example 4.2. In the previous Example we check that the place $P = (x^3 + x^2 + 1)$ is split in $K_3^{\mathfrak{m}}/K$. Let $z \in \hat{K}_P^* \subseteq J$ be the

element

$$z = \frac{(x^3+x^2+1)^2}{(x^2+x+1)^3}.$$

By the local Artin map z corresponds to

$$Frob(P)^{v_P(z)} = Frob(P)^2 \in D(P) \subseteq Gal(K_3^{\mathfrak{m}}/K)$$

because P is unramified in $K_3^{\mathfrak{m}}/K$. By Proposition 2.2 it is enough to see that $Frob(P)$ is the trivial automorphism but z is in the kernel of the Artin map via the embedding $\hat{K}_P^* \subseteq J_K$ because $z \equiv 1 \mod x^3+x+1$ so $[z]$, the class of z in C_K, belongs to $C_{S_3}^{\mathfrak{m}}$ as in Definition 3.6. So the Frobenius automorphism at P is trivial. The result follows from Proposition 2.2.

Example 4.3. We set $q = 2$ and $n = 4$. Let $\mathfrak{m}$ be the place (x^4+x+1) of $K = \mathbb{F}_2(x)$. A similar argument as in Example 4.1 above shows that the ray class field of conductor $\mathfrak{m}$ with constant field $\mathbb{F}_2$ such that the place $P = (x^7+x^4+1)$ splits completely gives a function field of genus 14 without points of degree smaller than n. This is not the best possible, in fact the subextension $F \subseteq K_P^{\mathfrak{m}}$ of degree 5 over K has the same property but the genus is 4. This is the best possible example when $n = 3$ and $q = 2$.

Chapter 5

A refinement of the Clark-Elkies bound

We can improve the result of Corollary 4.3 for large n by considering ray class field extensions of the rational function field with conductor given by a sum of different places.

In the sequel we assume that $K = \mathbb{F}_q(x)$ is the rational function field over $\mathbb{F}_q$. As in the previous section the number of places of degree t of K is denoted by a_t for any integer $t > 0$.

The next Lemma shows that there are many function fields without places of small degree when we consider ray class field extensions of K.

Lemma 5.1. Let $C_1 > 0$ and $C_2 > 0$ be two real constants (not depending on n) with $C_2 < 1$. Let $m > \log_q(n)$ be a prime

number and let $\alpha \leq a_m$ be a positive integer. Let $\mathfrak{q}_1, \ldots, \mathfrak{q}_\alpha$ be distinct places of K of degree m and let $\mathfrak{m}$ be the divisor $\sum_{i=1}^{\alpha} \mathfrak{q}_i$. We set $d = \frac{(q^m-1)^\alpha}{q-1}$. Let $K_1^{\mathfrak{m}}, \ldots, K_d^{\mathfrak{m}}$ be the abelian extensions of degree d unramified outside $\mathfrak{m}$ as in Theorem 4.1. Then there is a constant n_0 such that when $n > n_0$ and $\alpha > C_1 \frac{n}{\log_q(n)}$ then there are at least $C_2 d$ function field extensions $K_i^{\mathfrak{m}}$ of K such that the inertia index $f(P_i|P)$ is greater than $\frac{n}{deg(P)}$ whenever P is a place of K of degree $deg(P) < \frac{n}{\log_q(n)}$ and P_i is a place of $K_i^{\mathfrak{m}}$ over P.

In the proof we use a well known Lemma and a trivial consequence.

Lemma 5.2. Let s and m be odd prime numbers and let q be a prime power such that $s | \frac{q^m-1}{q-1}$ but $s \not| q-1$. Then $s = 2am + 1$ for a suitable integer $a > 0$. In particular $s > 2m$.

Corollary 5.1. There is a constant $c_q > 0$ such that when $m > c_q$ is a prime then there are at most m distinct primes dividing $\frac{q^m-1}{q-1}$ and these primes are all greater than $2m$.

Proof of Lemma 5.1. Let i be an element in $\{1, \ldots, d\}$ such that $K_i^{\mathfrak{m}}/K$ is a function field extension with $f(P_i|P) < \frac{d}{deg(P)}$ for at least one place P of K of degree smaller than $\frac{n}{\log_q(n)}$. As in the proof of Corollary 4.3 we estimate the number of such extensions.

Let k be the integer $\frac{q^m-1}{q-1}$. Let j be an integer in $\{1,\dots,\alpha\}$ and let t be a power of a prime number s such that t divides k. Consider the subextensions of $K_i^{\mathfrak{q}_j} \subseteq K_i^{\mathfrak{m}}$ totally ramified in $\mathfrak{q}_j$ of degree t for $j \in \{1,\dots,\alpha\}$. Let d' denote the degree of P and let $P_{i,j}$ be the place of $K_i^{\mathfrak{q}_j}$ under P_i with $P_{i,j}|P$. Let l be the integer $\gcd(t,d')$. It is easy to see, multiplying all the maximal prime power t dividing k, that if for every prime power divisor t of k the number $\frac{t}{l}$ divides $f(P_{i,j}|P)$ for at least one $j \leq \alpha$ then

$$k|f(P_i|P)\gcd(k,d')$$

and so

$$f(P_i|P) \geq \frac{n}{d'},$$

because $k > n$ and $d' \geq \gcd(k,d')$. It follows that if $f(P_i|P) < \frac{d}{deg(P)}$ then there is at least one prime power t dividing k such that $\frac{t}{l} \not| f(P_{i,j}|P)$ for all $j = \{1,\dots,\alpha\}$. For this reason, given a prime power t dividing k, it will be enough to estimate only the number of extensions $K_i^{\mathfrak{m}}/K$ such that $\frac{t}{l} \not| f(P_{i,j}|P)$ for all $j = 1,\dots,\alpha$.

The extensions $K_i^{\mathfrak{q}_j}/K$ are cyclic for $j \in \{1,\dots,\alpha\}$. By Remark 4.4 there are at most $\frac{t}{s}$ distinct extensions $K_i^{\mathfrak{q}_j}/K$ of degree t totally ramified in $\mathfrak{q}_j$ such that $\frac{t}{l} \not| f(P_{i,j}|P)$. It follows that there are at most $\left(\frac{k}{s}\right)^{\alpha}$ different extensions $K_i^{\mathfrak{q}_1}\cdots K_i^{\mathfrak{q}_\alpha}$ of K such

that $\frac{t}{l} \not| f(P_i|P)$ when P is unramified. So we see that there are at most

$$\frac{d}{s^\alpha}$$

extensions $K_i^{\mathfrak{m}}/K$ with $deg(P_i) < n$.

Now we consider the case $P = \mathfrak{q}_h$, for a certain $h \in \{1, \ldots, \alpha\}$, is a ramified place. We consider $\mathfrak{m}' = \mathfrak{m} - P$. For a similar reasoning as above we get at most

$$\frac{d}{(q^m - 1)s^{\alpha-1}}$$

extensions $K_j^{\mathfrak{m}'}$ for $j \in \{1, \ldots, \frac{(q^m-1)^{\alpha-1}}{q-1}\}$ such that $f(P_j'|P) < \frac{n}{deg(P)}$, where P_j' is a place of $K_j^{\mathfrak{m}'}$ over P. But $K_j^{\mathfrak{m}'} \subseteq K_i^{\mathfrak{m}}$ for $q^m - 1$ suitable $i \in \{1, \ldots, d\}$ and $f(P_j'|P) \leq f(P_i|P)$ so there are at most

$$\frac{d}{s^{\alpha-1}}$$

extensions $K_i^{\mathfrak{m}}/K$ of K with $f(P_i|P) < \frac{n}{deg(P)}$ when $P \in Supp(\mathfrak{m})$ is ramified.

Now we sum the number of all such extensions for all the places P of K, ramified or not, of degree smaller than $\frac{n}{\log_q(n)}$ and for all prime $s|k$. So we prove the following inequality:

$$\sum_{s|k} \sum_{i=1}^{\alpha} \frac{d}{s^{\alpha-1}} + \sum_{deg(P) < \frac{n}{\log_q(n)}} \sum_{s|k} \frac{d}{s^\alpha} < (1 - C_2)d, \qquad (5.1)$$

where P runs over the unramified places of K of degree smaller than $\frac{n}{\log_q(n)}$. The left hand side in (5.1) is bounded by

$$\alpha \sum_{s|k} \frac{d}{s^{\alpha-1}} + q \cdot q^{\frac{n}{\log_q(n)}} \sum_{s|k} \frac{d}{s^{\alpha}}, \tag{5.2}$$

by (4.1). So we prove that

$$\alpha \sum_{s|k} \frac{1}{s^{\alpha-1}} + q \cdot q^{\frac{n}{\log_q(n)}} \sum_{s|k} \frac{1}{s^{\alpha}} < 1 - C_2. \tag{5.3}$$

By Corollary 5.1 there are at most m distinct prime numbers s dividing k and all such s are greater than $2m$ by Lemma 5.2 when m is large so the left hand side in (5.3) is smaller than $1 - C_2$ whenever

$$m\alpha \frac{1}{(2m)^{\alpha-1}} + mq^{\frac{n}{\log_q(n)}} \frac{q}{(2m)^{\alpha}} < 1 - C_2,$$

or, also,

$$(2m)^{\alpha} > \frac{qm}{1 - C_2}(2m\alpha + q^{\frac{n}{\log_q(n)}}),$$

or also

$$\alpha \log_q(2m) > \log_q(q^{\frac{n}{\log_q(n)}} + 2m\alpha) + \log_q(\frac{m}{1 - C_2}) + 1.$$

It is very easy to check the last inequality in fact the right hand side is smaller than

$$\frac{n}{\log_q(n)} + \log_q(2m\alpha) + \log_q(\frac{m}{1 - C_2}) + 1,$$

because the logarithm is a convex function and

$$\alpha \log_q(2m) \geq \frac{n}{\log_q(n)} + \log_q(2m\alpha) + \log_q(\frac{m}{1-C_2}) + 1$$

when n is large because $\alpha > C_1 \frac{n}{\log_q(n)}$ by hypothesis. □

The proof of the following Lemma follows directly by the Hurwitz genus formula (2.1). It is a generalization of (3.5).

Lemma 5.3. Let $\mathfrak{q}_1, \ldots, \mathfrak{q}_h$ be distinct places of K of degree $t_1, \ldots, t_h$ respectively. Let $p_1, \ldots, p_h$ be positive integers such that $p_i | \frac{q^{t_i}-1}{q-1}$ for $i = 1, \ldots, h$. Let F_i/K be ray class field extensions of degree p_i totally ramified in $\mathfrak{q}_i$ for $i = 1, \ldots, h$. Then the genus g_L of the compositum field $L = F_1 \cdots F_h$ is smaller than

$$g_L \leq \frac{1}{2} \sum_{i=1}^{h} t_i \prod_{j=1}^{h} p_j.$$

Proposition 5.1. Let m and l be distinct prime numbers with l and m greater than $3\log_q(n)$ and let α and β be positive integers with $\alpha \leq a_m$ and $\beta \leq a_l$. Let $C_1 > 0$ be a real constant and let $C_2 > 0$ be a real constant with $C_2 < 1$ as in Proposition 5.1. Let $\mathfrak{q}_1, \ldots, \mathfrak{q}_\alpha$ (resp. $\mathfrak{p}_1, \ldots, \mathfrak{p}_\beta$) be distinct places of K of degree m (resp. l) with $\alpha > C_1 \frac{n}{\log_q(n)}$. Let $\mathfrak{m}$ be the effective divisor $\sum_{i=1}^{\alpha} \mathfrak{q}_i + \sum_{j=1}^{\beta} \mathfrak{p}_j$. Let k_1 and k_2 be the integers $\frac{q^m-1}{q-1}$ and $\frac{q^l-1}{q-1}$

respectively and set $d = \frac{(q^m-1)^\alpha (q^l-1)^\beta}{q-1}$. Assume that k_1 and k_2 are both prime to $q-1$.

Then there is an integer n_0 such that when $n > n_0$ and

$$\frac{C_2}{2} d > \frac{q \cdot q^n}{n},$$

there is a function field extension $K_i^{\mathfrak{m}}/K$ for a certain $i \in \{1, \ldots, d\}$ without places of degree smaller than n.

Proof. We may assume that l and m are smaller than $\frac{n}{\log_q(n)}$ otherwise the proof would be more easy. By Lemma 5.1 there are at least $C_2 d$ function field extensions $K_i^{\mathfrak{m}}/K$ for $i = 1, \ldots, d$ such that $deg(P) f(P_i|P) \geq n$ whenever $deg(P) < \frac{n}{\log_q(n)}$ and P_i is a place over P. In one of these field extensions $K_i^{\mathfrak{m}}$ of K there is a place of degree smaller than n only if there is a place P of K of degree $d' < n$ with $d' \geq \frac{n}{\log_q(n)}$ such that P is totally split in $K_i^{\mathfrak{q}_j}/K$ for all $j \in \{1, \ldots, \alpha\}$ and in $K_i^{\mathfrak{p}_h}/K$ for all $h \in \{1, \ldots, \beta\}$ by Lemma 5.2 where $K_i^{\mathfrak{q}_j}$ and $K_h^{\mathfrak{p}}$ are the ray class fields of K with conductor $\mathfrak{q}_j$ and $\mathfrak{p}_h$, respectively, contained in $K_i^{\mathfrak{m}}$. We are going to estimate the number of such function field extensions $K_i^{\mathfrak{m}}/K$. The rest of the proof is similar to the proof of Corollary 4.3.

For a fixed $j \leq \alpha$ we consider $K_i^{\mathfrak{q}_j}/K$ for $i \in \{1, \ldots, k_1\}$. There are at most $d_1 = \gcd(d', k_1)$ function field extensions $K_i^{\mathfrak{q}_j}/K$ such

that P is totally split by Corollary 4.1. Similarly for a fixed $h \leq \beta$ there are at most $d_2 = \gcd(d', k_2)$ function field extensions $K_i^{\mathfrak{q}_h}/K$ with $i \in \{1, \ldots, k_2\}$ such that P is totally split. We denote by d'' the greatest common divisor $\gcd(q-1, d')$. It follows that there are at most $d_1^{\alpha} d_2^{\beta} d''^{\alpha+\beta-1}$ extensions $K_i^{\mathfrak{m}}/K$ with $i \in \{1, \ldots, d\}$ such that P is totally split.

Let $A_{d_1,d_2,d'}$ be the number of places of K of degree d' totally split in all the subextensions of degree $d_1 d''$ (resp. $d_2 d''$) of the ray class fields $K_i^{\mathfrak{q}_j}$ for $i \in \{1, \ldots, k_1\}$ and $j \in \{1, \ldots, \alpha\}$ (resp. $K_i^{\mathfrak{p}_h}$ for $i \in \{1, \ldots, k_2\}$ and $h \in \{1, \ldots, \beta\}$). Then

$$A_{d_1,d_2,d'} \leq \frac{q^{d'}}{d' d_1^{\alpha} d_2^{\beta} d''^{\alpha+\beta-1}} + 2\frac{g_F}{d_1^{\alpha} d_2^{\beta} d''^{\alpha+\beta-1}} q^{d'/2} + deg(\mathfrak{m})$$

by Lemma 2.4 and so

$$A_{d_1,d_2,d'} \leq \frac{q^{d'}}{d' d_1^{\alpha} d_2^{\beta} d''^{\alpha+\beta-1}} + (q^{d'/2} + 1)(m\alpha + l\beta)$$

by Lemma 5.3.

By the previous Proposition there are at least $C_2 d$ distinct extensions $K_i^{\mathfrak{m}}/K$ such that $f(Q|P)deg(P) > n$ when $deg(P) < \frac{n}{\log_q(n)}$ but there are at most

$$\sum_{d'=\frac{n}{\log_q(n)}}^{n-1} A_{d_1,d_2,d'} d_1^{\alpha} d_2^{\beta} d''^{\alpha+\beta-1}$$

extensions $K_i^{\mathfrak{m}}/K$ with at least one totally split place of degree d' by Lemma 4.1. In particular this number is smaller than

$$\sum_{d'=\frac{n}{\log_q(n)}}^{n-1} \frac{q^{d'}}{d'} + (q^{d'/2}+1)(\alpha m + \beta l) d_1^{\alpha} d_2^{\beta} d''^{\alpha+\beta-1}, \tag{5.4}$$

by Lemma 2.4. But

$$d_1 d'' \leq d' < n < k_1^{1/3}$$

and similarly for $d_2 d''$. Moreover $\alpha m + \beta l < 2\log_q(d)$. It follows that there are at most

$$\sum_{d'=\frac{n}{2\log_q(n)}}^{n-1} \frac{q^{d'}}{d'} + q^{n/2}(\alpha m + \beta l) k_1^{\alpha/3} k_2^{\beta/3} \leq$$

$$\leq q\frac{q^n}{n} + 2nq^{n/2}\log_q(d) d^{1/3}$$

extensions $K_i^{\mathfrak{m}}/K$ such that at least one point of degree $d' < n$ is totally split. The right hand side in the last equation is smaller than $C_2 d$ if

$$q\frac{q^n}{n} < \frac{C_2}{2} d$$

and

$$2nq^{n/2}\log_q(d) d^{1/3} < \frac{C_2}{2} d.$$

The first condition holds by hypothesis, the second one holds when n is large because $d > q^{\frac{n}{\log_q(n)}}$. So there is at least one function field extension $K_i^{\mathfrak{m}}/K$ without places of degree smaller than n. $\square$

In order to prove Theorem 1.1 we choose l and m greater than $3\log_q(n)$ but smaller than $C\log_q(n)$ for a suitable constant $C > 0$ and we find suitable α and β smaller than n with α or β greater than $C_1\frac{n}{\log_q(n)}$ for an other suitable $C_1 > 0$ such that the integer

$$d = \frac{(q^m-1)^\alpha(q^l-1)^\beta}{q-1}$$

is bigger than $4q\frac{q^n}{n}$ but smaller than $C'4q\cdot\frac{q^n}{n}$ for a suitable constant $C' > 1$ (not depending on n). In fact, when $d \leq 4C'q\cdot\frac{q^n}{n}$ then $m\alpha + l\beta \leq n$ when n is large and the genus of $K_i^{\mathfrak{m}}$ is bounded by $g \leq \frac{m\alpha+l\beta}{2}d$ for all $i \in \{1,\ldots,d\}$, by (3.5), so $g \leq \frac{n}{2}d \leq 2C'q\cdot q^n$. We will see that $C' = q$ is a possible choice for C'.

The existence of suitable α and β is proved by the next Lemma.

Lemma 5.4. Let l and m be coprime numbers with $l < m < 2l$. Then there is a constant l_0, such that when $l > l_0$ then for any real number r greater than q^{2m^3} there are two positive integers α and β such that

$$r < \frac{(q^m-1)^\alpha(q^l-1)^\beta}{q-1} < rq. \tag{5.5}$$

Proof. Let R be the real number $\log_q(rq) + \log_q(q-1)$. Taking logarithm of both sides in (5.5) we get the equivalent condition

$$R - 1 < \alpha q_m + \beta q_l \leq R, \tag{5.6}$$

where q_m and q_l denote the real numbers $\log_q(q^m-1)$ and $\log_q(q^l-1)$.

Let $L \subset \mathbb{R}^2$ be the lattice generated by $\mathbf{w_1} = (q_m, 0)$ and $\mathbf{w_2} = (0, q_l)$. The statement of the Lemma is equivalent to say that there is a point of the lattice in the right-upper quarter of the plane between the lines $\{x + y = R + 1\}$ and $\{x + y = R\}$.

We denote by $|\cdot|$ the pseudo-norm over the vector space $\mathbb{R}^2$ given by $|(x, y)| = |x+y|$. This is not a norm because $|(x, -x)| = 0$ also when $x \neq 0$.

We look for an element $\mathbf{v} = h\mathbf{w_1} - k\mathbf{w_2} \in L$ with

$$|\mathbf{v}| < 1 \tag{5.7}$$

$$|\mathbf{v}| > \frac{1}{2} \tag{5.8}$$

and

$$0 < h < k \leq m. \tag{5.9}$$

Let u be an integer and let $\mathcal{F}_u$ be the Farey series of order u, that is the set of the ascending series of the irreducible fractions between 0 and 1 whose denominator does not exceed u. It is a well-known fact (see [7], Chapter III) that when $\frac{h_1}{k_1}$ and $\frac{h_2}{k_2}$ are two consecutive elements of the series then $|h_1k_2 - k_1h_2| = 1$.

When $u = m$ is very easy to see that there is no element $\frac{h}{k} \in \mathcal{F}_u$ such that $\frac{q_l}{q_m} < \frac{h}{k} < \frac{l}{m}$ when m and l are large. In fact for any positive $\epsilon < 1$

$$\frac{l}{m} - \frac{q_l}{q_m} < \epsilon \frac{1}{m(m-1)}, \tag{5.10}$$

when m and l are large. Let $\frac{h}{k} \in \mathcal{F}_m$ the element preceding $\frac{l}{m}$ in $\mathcal{F}_m$. Then

$$\frac{h}{k} < \frac{q_l}{q_m} < \frac{l}{m}.$$

Choose $\mathbf{v} = (-hq_m, kq_l) \in L$.

It follows that $|\mathbf{v}| < 1$ otherwise

$$\frac{q_l}{q_m} - \frac{h}{k} \geq \frac{1}{kq_m} \geq \frac{1}{km} = \frac{l}{m} - \frac{h}{k}.$$

In a similar way we see that $|\mathbf{v}| > \frac{1}{2}$ otherwise

$$\frac{q_l}{q_m} - \frac{h}{k} = \frac{v}{kq_m} < \frac{1}{2kq_m}$$

so

$$\frac{l}{m} - \frac{q_l}{q_m} + \frac{1}{2kq_m} > \frac{l}{m} - \frac{h}{k} = \frac{1}{km}$$

and so

$$\frac{l}{m} - \frac{q_l}{q_m} > \frac{1}{km} - \frac{1}{2kq_m} > \frac{1}{4m(m-1)}$$

contradicting (5.10) with $\epsilon = \frac{1}{4}$.

Let $\mathbf{z} = c\mathbf{w_1}$ be the maximum point of L over the x-axis such that c is a positive integer and $|\mathbf{z}| < R$. If $R - 1 < |\mathbf{z}|$ we choose $\alpha = c$ and $\beta = 0$ and the Lemma follows.

Otherwise consider the points $\mathbf{z}_i = \mathbf{z} + i\mathbf{v} \in L$ for all integers $i > 0$. Then $\mathbf{z}_i$ is in the right-upper quarter if $i < \frac{c}{h}$. Let t be the integer $[\frac{c}{h}] > 0$. We prove that $R < |\mathbf{z}_t|$. In fact by (5.8) $t|\mathbf{v}| > \frac{1}{2}[\frac{c}{h}]$ and so $t|\mathbf{v}| \geq |\mathbf{w_1}| = q_m$ because $R > 2m^3$. So

$$R < (c+1)|\mathbf{w_1}| < |\mathbf{z}_t|. \tag{5.11}$$

Let i be the minimal integer such that $R - 1 < |\mathbf{z}_i|$. Then i is smaller than t by (5.11) and greater than 0 by assumption. Moreover

$$|\mathbf{z}_{i-1}| + 1 < R$$

because i was supposed to be minimal. So R is greater than $|\mathbf{z}_{i-1}| + |\mathbf{v}| = |\mathbf{z}_i|$ by (5.7) and so

$$R - 1 < |\mathbf{z}_i| < R.$$

Let $\alpha = c - ih$ and $\beta = ik$ be the coordinates of $\mathbf{z}_i$. The real number $\alpha q_m + \beta q_l$ verifies (5.6). This concludes the proof. □

Proof of Theorem 1.1. We assume before $q = p$ is a prime.

Choose prime numbers l and m and two positive integers α and β satisfying (5.5) in the previous Lemma with $r = 4p\frac{p^n}{n}$. Such choice of r verifies the hypothesis of the Lemma when n is large and l and m are smaller than $C\log_p(n)$ for a constant $C > 0$. By the Bertrand postulate there are at least two primes smaller than $C\log_p(n)$ when $C \geq 12$ so there are such integers.

It is easy to see that $\alpha < a_m$ and $\beta < a_l$ if l and m are greater than $3\log_p(n)$ otherwise $p^{m\alpha+l\beta}$ would be greater than p^{n^3} and it would not satisfy (5.5). In a similar way we see that α or β is greater than, say, $\frac{1}{48}\frac{n}{\log_p(n)}$ otherwise $p^{m\alpha+l\beta}$ would be smaller than $p^{n/2}$ in contrast with (5.5). So we can apply Proposition 5.1 with $C_1 = \frac{1}{48}$. We get a function field without places of degree smaller than n for all $n > n_0$ for a suitable constant n_0. We have already seen that the genus of such function field is smaller than $\frac{1}{2(p-1)}p^n$ by (3.5). Let C_p be the constant $\frac{1}{2(p-1)}p^{n_0}$. Then there is a function field with constant field $\mathbb{F}_p$ without places of degree smaller than n of genus smaller than $C_p p^n$ for all integer $n > 0$.

Now let $q = p^c$ be a prime power of p. By the previous case there is a function field K of genus $g_K \leq C_p p^{cn} = C_p q^n$ over $\mathbb{F}_p$ without places of degree smaller of cn. The constant field extension $K\mathbb{F}_q$ is a function field over $\mathbb{F}_q$ with the same genus

without places of degree smaller than n. This concludes the proof.

□

5.1 Tables

We list examples of curves over $\mathbb{F}_q$ without points of degree d' such that $d' \leq n$ when $q = 2$ and $n < 20$.

The integer d in the table is the degree of a function field extension $K/\mathbb{F}_q(x)$ of the rational function field with genus g and constant field $\mathbb{F}_q$. In this table the field K is always a subfield of the ray class field $K_S^{\mathfrak{m}}$ of conductor $\mathfrak{m}$. The irreducible polynomials in the forth column correspond to the places in the support of $\mathfrak{m}$ with multiplicity. The polynomial in $\mathbb{F}_q(x)$ corresponding to the place S totally split in $K_S^{\mathfrak{m}}/\mathbb{F}_q(x)$ is showed in the last column.

n	g	d	$\mathfrak{m}$	S
1	2	2	$(x^3+x+1)^2$	(x^3+x^2+1)
2	3	7	(x^3+x+1)	(x^4+x+1)
3	4	5	(x^4+x+1)	(x^7+x^4+1)
5	12	7	$(x^6+x^4+x^3+x+1)$	$(x^8+x^5+x^3+x^2+1)$
7	48	17	$(x^8+x^7+x^6+x+1)$	$(x^9+x^7+x^5+x^2+1)$
8	78	$7\cdot 7$	(x^3+x^2+1, x^3+x+1)	$(x^9+x^7+x^2+x+1)$
9	120	31	$(x^{10}+x^3+1)$	$(x^{11}+x^9+x^7+x^2+1)$
11	362	$15\cdot 7$	$(x^4+x+1, x^6+x^5+x^3+x^2+1)$	$(x^{13}+x^8+x^5+x^3+1)$
12	588	$31\cdot 7$	(x^5+x^2+1, x^3+x+1)	$(x^{13}+x^{12}+x^{10}+x^7+x^4+x+1)$
13	1480	$31\cdot 15$	(x^5+x^2+1, x^4+x+1)	$(x^{14}+x^{13}+x^5+x^4+x^3+x^2+1)$
14	3342	$127\cdot 7$	(x^7+x+1, x^3+x+1)	$(x^{15}+x^{14}+x^{13}+x^7+x^6+x^4+x^2+x+1)$
15	8940	$73\cdot 17$	$(x^9+x^4+1, x^8+x^5+x^3+x^2+1)$	$(x^{16}+x^{14}+x^{13}+x^{11}+x^{10}+x^7+x^4+x+1)$
16	19861	$23\cdot 89$	$(x^{11}+x^6+x^5+x^2+1, x^{11}+x^9+1)$	$(x^{18}+x^{17}+x^{11}+x^9+x^7+x^4+1)$
17	41440	$89\cdot 63$	$(x^{11}+x^9+1, x^6+x+1)$	$(x^{18}+x^{17}+x^{16}+x^{11}+x^9+x^4+1)$
18	89415	$127\cdot 89$	$(x^7+x+1, x^{11}+x^9+1)$	$(x^{19}+x^{18}+x^{15}+x^{14}+x^{11}+x^7+x^3+x+1)$
19	95886	$127\cdot 127$	(x^7+x+1, x^7+x^6+1)	$(x^{20}+x^{19}+x^{15}+x^{14}+x^{13}+x^2+1)$

Bibliography

[1] E. Artin, J. Tate: *Class field theory*. New York, W.A. Benjamin (1967).

[2] R. Auer: *Ray class fields of global function fields with many rational places*. Dissertation at the Oldenburg University, http://oops.uni-oldenburg.de/volltexte/1999/457/pdf/Aueray99.pdf (1999).

[3] R. Auer: *Ray class fields of global function fields with many rational places*. Acta Arithmetica 95, 97-122 (2000).

[4] J.W.S. Cassels, A. Frohlich: *Algebraic number theory*. Academic Press, London (1967).

[5] M. D. Fried, M. Jarden: *Field Arithmetic*. Springer Verlag (1987).

[6] R. Fuhrmann, F. Torres: *The genus of curves over finite fields with many rational points*. Manuscr. Math., 89, 103-106 (1996).

[7] G.H. Hardy, E.M. Wright: *An introduction to the theory of numbers*. Oxford Science Publications, Clarendon (1938).

[8] D. R. Hayes: *Explicit class field theory in global function fields*. Studies in algebra and number theory, Adv. in Math. Suppl. Stud. 6, Academic Press, 173-217 (1979).

[9] H. Howe, K. Lauter, J. Top: *Pointless curves of genus three and four*. Séminaires et congrès, 11, 125-141 (2005).

[10] Y. Ihara: *Some remarks on the number of rational points of algebraic curves over finite fields*. J. Fac. Sci. Univ. Tokyo, 28, 721-724 (1981).

[11] D. Maisner, E. Nart: *Abelian surfaces over finite fields as Jacobians. With an appendix by Everett W. Howe*. Experiment. Math. 11, no. 3, 321-337 (2002).

[12] K. Murty, J. Scherk: *Effective versions of the Chebotarev density theorem for function fields*. Comptes Rendus de

l'Académie des Sciencies (Paris), Série I, Mathématique, 319, No. 6, 523-528 (1994).

[13] H. Niederreiter, C. Xing: *Rational points on curves over finite fields: theory and applications*. Cambridge, Cambridge University Press (2001).

[14] A. Rigato: *Uniqueness of optimal curves over* $\mathbb{F}_2$ *of small genus*. Phd Thesis at Universitá di Roma Tor Vergata, http://dspace.uniroma2.it/dspace/index.jsp (2009).

[15] H. Stichtenoth: *Algebraic function fields and codes*. Berlin, Springer-Verlag (1993).

[16] A. Weil: *Courbes algébriques et variétés abéliennes*. Paris, Hermann (1971).