Ray Class Fields of Global Function Fields with Many Rational Places

Vom Fachbereich Mathematik
der Carl-von-Ossietzky-Universität Oldenburg
zur Erlangung des Grades eines
Doktors der Naturwissenschaften
angenommene Dissertation, vorgelegt von

Roland Auer

aus

Lindau/Bodensee

Erstreferent: Prof. Dr. H.-G. Quebbemann
Korreferent: Prof. Dr. H. Stichtenoth

Tag der mündlichen Prüfung: 16. Juli 1999.

Contents

Introduction

The search for algebraic curves over finite fields $\mathbb{F}_q$ with many rational points or, what amounts to the same, for global function fields with many rational places was motivated by Goppa's algebro-geometric construction of error-correcting codes and initiated by Serre [S2, S3] in the early eighties. Serre was the first to utilize class field theory, among other methods, to exhibit such curves, and he also provided explicit formulas for the maximal numbers $N_q(1)$ and $N_q(2)$ of rational points on curves over $\mathbb{F}_q$ of genus $g = 1$ and 2, respectively.

Until today, no such formula is known for $N_q(g)$ when $g \geq 3$. Instead, the work of many mathematicians has led to large tables, such as in [GV7], documenting the state of the art by giving lower and upper bounds for the numbers $N_q(g)$. The lower bounds are obtained by more or less explicit constructions of curves with many points. Hansen and Stichtenoth [Han, HS, St1], Wirtz [Wi], van der Geer and van der Vlugt [GV1–GV6], Niederreiter and Xing [NX1, NX2, NX5, NX6, NX7] and Shabat [Sh] provided defining equations for such curves, mostly of Artin-Schreier or Kummer type. The present work, which performs class field constructions, follows the theme of research by Schoof [Sf], Lauter [La1, La3] and Niederreiter and Xing [XN, NX2, NX3, NX4, NX7, NX8, NX9]. In particular, it has been influenced by the paper [XN], the methods of which are refined upon in Section 6. Making use of algorithmic number theory, we succeed in improving the mentioned tables in numerous places.

When dealing with class field theory, instead of an algebraic curve X (smooth, projective, absolutely irreducible) defined over a finite field $\mathbb{F}_q$, it is convenient to consider its field $K = \mathbb{F}_q(X)$ of algebraic functions, a global function field with full constant field $\mathbb{F}_q$. The genus of K is that of X, and coverings of X correspond to field extensions of K, the degree of the covering being the degree of the extension. To a point $P \in X$ with minimal field of definition over $\mathbb{F}_q$ say $\mathbb{F}_{q^d}$ we associate the set $\mathfrak{p} \subseteq K$ of all functions vanishing in P and call $\mathfrak{p}$ a place of K. This $\mathfrak{p}$ is the maximal ideal in the discrete valuation ring R consisting of those functions which are regular at P, it corresponds in fact to the whole Frobenius (q-th power map) orbit of P, which contains d points, and it has (residue field) degree $\deg \mathfrak{p} := [R/\mathfrak{p} : \mathbb{F}_q] = d$. In particular, the rational places, i.e. the places of degree 1, of $K|\mathbb{F}_q$ are in 1–1 correspondence with the $\mathbb{F}_q$-rational points on X. In this thesis we shall work with a purely field theoretic definition of a global function field $K|\mathbb{F}_q$ and forget about curves completely. The necessary background is given in Section 1.

The central objects in this work are the ray class fields $K_S^{\mathfrak{m}}$, where S is a non-empty set of places of K and $\mathfrak{m}$ is an S-cycle, i.e. a finite formal sum $\sum m_{\mathfrak{p}}\mathfrak{p}$ of places $\mathfrak{p}$ outside S together with non-negative integer multiplicities $m_{\mathfrak{p}}$. The extension $K_S^{\mathfrak{m}}|K$ can be characterized as the largest abelian extension $L|K$ of conductor $\mathfrak{f}(L|K) \leq \mathfrak{m}$ such that every place $\mathfrak{p} \in S$ splits completely in L (i.e. there are $[L : K]$ places of L lying above $\mathfrak{p}$). Roughly speaking, the conductor measures the "wildness" of ramification at each place of K, thus the S-cycle $\mathfrak{m}$ confines this wildness. For example, if $\mathfrak{m} = \mathfrak{o}$, no ramification is allowed at all, and we obtain the special case of a Hilbert class field $K_S^{\mathfrak{o}}$, whose degree over K equals the S-class number h_S.

The extension $K_S^{\mathfrak{m}}|K$ is always finite. This would no longer be the case if we dropped the splitting condition in the characterization of a ray class field, i.e. if we allowed S to be empty, because the maximal constant field extension $\bar{\mathbb{F}}_q K|K$ is abelian of infinite degree and unramified everywhere. Thinking of ray class fields of number fields, the role of S is usually played by the archimedean primes. For function fields, however, there is no canonical choice of S.

The $K_S^{\mathfrak{m}}$ provide a rather fine classification of the finite abelian extensions of K and are canonical and quite beautiful objects in themselves. Already because of this, they deserve being studied more intimately. We utilize them mainly to produce curves with many points. For example, if S consists of rational places only, then $K_S^{\mathfrak{m}}$ has at least $[K_S^{\mathfrak{m}} : K]\,|S|$ rational places. For suitable choices of S and $\mathfrak{m}$, this number tends to be large compared with the genus of $K_S^{\mathfrak{m}}$, which remains to be calculated.

There are various ways of obtaining the ray class fields. If S consists of exactly one place of K, then $K_S^{\mathfrak{m}}$ can be constructed by adjoining the $\mathfrak{m}$-torsion of a rank 1 Drinfel'd module to the Hilbert class field $K_S^{\mathfrak{o}}$. This gives us a so-called narrow ray class field, whose Galois group over $K_S^{\mathfrak{o}}$ naturally contains $\mathbb{F}_q^*$, and $K_S^{\mathfrak{m}}$ is the subfield fixed by $\mathbb{F}_q^*$. In the general situation, one singles out a place $\mathfrak{q} \in S$ and gains $K_S^{\mathfrak{m}}$ as the subfield of $K_{\{\mathfrak{q}\}}^{\mathfrak{m}}$ fixed by the Frobenius automorphisms of all the other places in S (cf. [XN, NX4]).

Our approach is by class field theory: we define a suitable open subgroup $\mathcal{C}_S^{\mathfrak{m}}$ of finite index in the idèle class group $\mathcal{C}_K$ of K and obtain $K_S^{\mathfrak{m}}$ directly as the class field associated to this subgroup. The Galois group $G(K_S^{\mathfrak{m}}|K)$ is isomorphic to $\mathcal{C}_K/\mathcal{C}_S^{\mathfrak{m}}$. To obtain its order, this time one has to factor out S-units, i.e. algebraic functions having all their poles and zeros in S, instead of Frobenius automorphisms. For the convenience of the reader, we include a brief introduction to class field theory in Section 4 also indicating ideas for the proofs of its main theorems.

It should be mentioned that defining equations for the extensions $K_S^{\mathfrak{m}}|K$ are

only known in very few cases (Propositions 8.4 and 8.9). Surely, one could gain such equations in each single case by calculating the minimal polynomial of a suitable norm from the narrow ray class field in the Drinfel'd module construction. But the necessary calculations as well as the resulting polynomials tend to get very lengthy. The proper method seems to consist in determining (the coefficients of) the equations for small successive Kummer and Artin-Schreier extensions in the fashion of [GV6], and thereby make up the whole of $K_S^{\mathfrak{m}}|K$ step by step.

As was mentioned above, it is important to know the genus of $K_S^{\mathfrak{m}}$. By means of a remarkable genus formula (Theorem 5.8 and Corollary 5.9), the problem is reduced to the determination of the degrees $[K_S^{\mathfrak{m}'} : K]$ for certain $\mathfrak{m}' \leq \mathfrak{m}$. This formula is deduced in Sections 3 and 5 from Hilbert's Different Formula, the Hasse-Arf Theorem and the connection between upper ramification groups and higher unit groups known from local class field theory. Another proof not included in this thesis applies Moebius inversion to the Conductor Discriminant Product Formula and was found by Cohen et al. [CDO].

Unfortunately we only have explicit formulas for the degrees $[K_S^{\mathfrak{m}} : K]$ in very special cases (Theorems 8.1 and 8.5). Therefore we content ourselves with giving algorithms for their computation under the additional assumption that S is finite. The case of mixed S-cycles $\mathfrak{m}$ is only treated for tame ramification, i.e. for $\mathfrak{m}$ of the form $\sum_{\mathfrak{p}\in R} \mathfrak{p}$ with a finite set R of places of K. Instead, from page 40 onwards, we concentrate on ramification at a single place $\mathfrak{p}$ of K. In this situation we introduce the concept of the S-description at $\mathfrak{p}$, a polynomial $\delta(t)$ with non-negative integer coefficients satisfying $\delta(1) - \delta(0) = |S| - 1$. Together with the S-class number h_S it carries the information about the degrees of the extensions $K_S^{m\mathfrak{p}}|K$ for all $m \in \mathbb{N}_0$ (see Theorem 6.4 and the discussion following it).

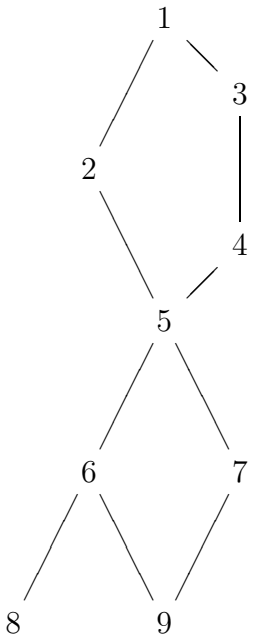
An algorithm for computing these S-descriptions was implemented in KASH, the shell programming language of KANT, a powerful algorithmic number theory tool developed by the Berlin KANT group [K] under the guidance of M. Pohst. By searching through a large number of choices for K, S and $\mathfrak{p}$, in Section 9 we filter out those S-descriptions which lead to ray class fields having many rational places compared with their genera.

Acknowledgements

First of all, I wish to thank F. Heß, who supplied me with a special KASH version capable of dealing with residue fields, who kept supporting me in the programming process by giving valuable advice whenever necessary, and who

discussed with me the problem of finding fundamental S-units, thereby contributing considerably to the progress of Section 2. I am also indebted to C. Dement, P. Kunkel and B. Wittje for a number of error corrections, to P. Harmand for seeing me through my LaTeX and TeX troubles, and especially to K. Roegner for her excellent and thorough proof reading. The thesis benefits from elucidating discussions I enjoyed with N. Manolache, W. Schmale, V. Shabat, P. Stevenhagen, H. Stichtenoth, U. Vetter, B. Wittje and certainly many others. Thank you all for that. Finally, I want to express my gratitude to my supervisor Prof. Dr. H.-G. Quebbemann for his patience and permanent support. He spent hours and hours listening and discussing problems with me and accompanied me through the ups and downs of my research work.

Dependence of Sections



Part I
Global Function Fields

This first part treats certain topics which manage without class field theory. The first section is a very concise introduction to global function fields, and the second discusses the problem of finding S-units. In Section 3 we turn to Hilbert's ramification theory, thereby preparing ourselves for entering Part II.

1 Preliminaries

This section aims at familiarizing the reader with the notation and some basic facts from the theory of algebraic function fields used in this thesis. Apart from some results about completions (for which we shall give instant proof), its whole content is covered by Stichtenoth's book [St2].

The group of a Galois extension $L|K$ is denoted $G(L|K)$. For the notions of a **Dedekind domain**, a **discrete valuation** (here always assumed to be additive and normalized with values in $\mathbb{Z} \cup \{\infty\}$) and a **discrete valuation ring** we refer the reader to e.g. [FJ, pp. 12ff]. If P is a prime element in a factorial domain or a maximal ideal in a Dedekind domain, then we write v_P for the associated discrete valuation on the field of fractions.

Throughout the text, K is a **global function field**, i.e. K is finitely generated and of transcendence degree 1 over a finite field $\mathbb{F}_q$, where q is a power of the characteristic p. We always require that $\mathbb{F}_q$ is the full **constant field** of K, i.e. is algebraically closed in K, and express this circumstance by writing $K|\mathbb{F}_q$.

A **place** of K is the maximal ideal $\mathfrak{p}$ in some discrete valuation ring $R_\mathfrak{p}$ of K. We say that $\mathfrak{p}$ is a **zero** or a **pole** of the function $z \in K$ if $z \in \mathfrak{p}$ or $z \notin R_\mathfrak{p}$, respectively. The constant field $\mathbb{F}_q$ is naturally contained in the (finite) **residue field** $\mathbb{F}_\mathfrak{p} := R_\mathfrak{p}/\mathfrak{p}$ of $\mathfrak{p}$. The **degree** of $\mathfrak{p}$ is defined as $\deg \mathfrak{p} := [\mathbb{F}_\mathfrak{p} : \mathbb{F}_q]$. A place of degree 1 is called a **rational place**. The map $\mathfrak{p} \mapsto v_\mathfrak{p}$ is a 1–1 correspondence between the places and the (discrete) valuations of K. We denote the set of all places of K by $\mathbb{P}_K$ and define $\mathbb{P}_K^d := \{\mathfrak{p} \in \mathbb{P}_K \mid \deg \mathfrak{p} = d\}$ for $d \in \mathbb{N}$.

The free abelian group $\mathcal{D}_K$ on the set $\mathbb{P}_K$ is called the **divisor group** of K. The map $\deg : \mathbb{P}_K \to \mathbb{Z}$ is extended to $\mathcal{D}_K$ by linearity. Its kernel is denoted by $\mathcal{D}_K^0$. A divisor $\mathfrak{m} \in \mathcal{D}_K$ is written as a formal sum $\mathfrak{m} = \sum_{\mathfrak{p} \in \mathbb{P}_K} m_\mathfrak{p} \mathfrak{p}$ with integer coefficients $m_\mathfrak{p}$ and finite **support** $\operatorname{supp} \mathfrak{m} := \{\mathfrak{p} \in \mathbb{P}_K \mid m_\mathfrak{p} \neq 0\}$. If $\mathfrak{n} = \sum_\mathfrak{p} n_\mathfrak{p} \mathfrak{p} \in \mathcal{D}_K$ is another divisor and $m_\mathfrak{p} \leq n_\mathfrak{p}$ for all $\mathfrak{p} \in \mathbb{P}_K$, then we

write $\mathfrak{m} \leq \mathfrak{n}$. The zero element in $\mathcal{D}_K$ is denoted $\mathfrak{o}$, and a divisor $\mathfrak{m} \geq \mathfrak{o}$ is called **effective**.

Each function $z \in K^*$ has only finitely many zeros and poles, hence one can define its **principal divisor** $(z) = (z)_K := \sum_{\mathfrak{p}\in\mathbb{P}_K} v_\mathfrak{p}(z)\mathfrak{p}$. Breaking up (z) into the **zero divisor** $(z)_0 \geq \mathfrak{o}$ and the **pole divisor** $(z)_\infty \geq \mathfrak{o}$ of z such that $(z) = (z)_0 - (z)_\infty$, one has the following

1.1. Theorem. *Let $z \in K \setminus \mathbb{F}_q$. Then* $\deg(z)_0 = \deg(z)_\infty = [K : \mathbb{F}_q(z)]$.

In particular, $\deg(z)_K = 0$ for all $z \in K^*$. The map $(\ ) = (\ )_K : K^* \to \mathcal{D}_K^0$, $z \mapsto (z)$ is a group morphism with kernel $\mathbb{F}_q^*$, hence $(K^*) \simeq K^*/\mathbb{F}_q^*$. The quotient $\mathcal{D}_K^0/(K^*)$ is called the **(divisor) class group** of K. Its order, the **(divisor) class number** h_K, is finite.

For $\mathfrak{m} \in \mathcal{D}_K$, the **Riemann-Roch space** $\mathcal{L}(\mathfrak{m}) := \{z \in K^* \,|\, (z) + \mathfrak{m} \geq \mathfrak{o}\} \cup \{0\}$ is a finite $\mathbb{F}_q$-space, and we set $\dim \mathfrak{m} := \dim_{\mathbb{F}_q} \mathcal{L}(\mathfrak{m})$. The **genus** of K can be defined as the non-negative integer $g_K := \max\{\deg \mathfrak{m} - \dim \mathfrak{m} + 1 \,|\, \mathfrak{m} \in \mathcal{D}_K\}$.

The power series

$$Z_K(t) := \sum_{n=0}^{\infty} A_n t^n \in \mathbb{Z}[[t]] \subseteq \mathbb{C}((t))$$

with $A_n = |\{\mathfrak{m} \in \mathcal{D}_K \,|\, \mathfrak{m} \geq \mathfrak{o},\, \deg \mathfrak{m} = n\}|$ is called the **zeta function** of K. It is actually a rational function, namely $Z_K(t) = \frac{P_K(t)}{(1-t)(1-qt)}$ with **numerator polynomial** $P_K(t) \in \mathbb{Z}[t]$ of degree $2g_K$.

1.2. Theorem. *The numerator polynomial of the zeta function of K satisfies the functional equation*

$$P_K(t) = q^{g_K} t^{2g_K} P_K\left(\tfrac{1}{qt}\right).$$

Moreover, $P_K(1) = h_K$ is the class number of K.

The simplest example of a global function field is that of a **rational function field** $\mathbb{F}_q(x)$ with an indeterminate x over $\mathbb{F}_q$. Extending the degree map $\deg : \mathbb{F}_q[x] \to \mathbb{N}_0 \cup \{-\infty\}$ to the whole of $\mathbb{F}_q(x)$ yields a discrete valuation $v_\infty := -\deg$ on $\mathbb{F}_q(x)$. The place ∞ of $\mathbb{F}_q(x)$ corresponding to v_∞ has degree 1 and is the (only) pole of x. All (discrete) valuations on $\mathbb{F}_q(x)$ are given by the set

$$\{v_P \,|\, P \in \mathbb{F}_q[x] \text{ monic, irreducible}\} \cup \{v_\infty\}.$$

Hence there is a 1–1 correspondence $P \leftrightarrow \mathfrak{p}$ with $v_P = v_\mathfrak{p}$ between the monic irreducibles $P \in \mathbb{F}_q[x]$ and the places $\mathfrak{p} \neq \infty$ of $\mathbb{F}_q(x)$. In this correspondence, $\mathfrak{p}$ is the maximal ideal in the localization of $\mathbb{F}_q[x]$ at P, and the principal divisor of P is $(P) = \mathfrak{p} - (\deg P)\infty$, thus $\deg \mathfrak{p} = \deg P$. A rational function field has genus 0 and trivial divisor class group. Conversely, each global function field of genus 0 is a rational function field.

Let $L|\mathbb{F}_{q^d}$ be a finite *separable* extension of $K|\mathbb{F}_q$. In other words, L is a global function field containing K with full constant field of degree $d \in \mathbb{N}$ over that of K, and L^p does not contain K. Let $\mathfrak{q}$ be a place of L; then $\mathfrak{q} \cap K =: \mathfrak{p}$ is a place of K. We say that $\mathfrak{q}$ lies **above** $\mathfrak{p}$ and write $\mathfrak{q}|\mathfrak{p}$. The canonical inclusion $\mathbb{F}_\mathfrak{p} \subseteq \mathbb{F}_\mathfrak{q}$ is compatible with the inclusions $\mathbb{F}_q \subseteq \mathbb{F}_\mathfrak{p}$ and $\mathbb{F}_q \subseteq \mathbb{F}_{q^d} \subseteq \mathbb{F}_\mathfrak{q}$, and $[\mathbb{F}_\mathfrak{q} : \mathbb{F}_\mathfrak{p}]$ is called the **inertia degree** of $\mathfrak{q}|\mathfrak{p}$. Note that, by definition, $[\mathbb{F}_\mathfrak{q} : \mathbb{F}_\mathfrak{p}] \deg \mathfrak{p} = d \deg \mathfrak{q}$. The restriction $v_\mathfrak{q}|_K$ equals $e \cdot v_\mathfrak{p}$ for some positive integer $e =: e(\mathfrak{q}|\mathfrak{p})$, called the **ramification index** of $\mathfrak{q}|\mathfrak{p}$. These numbers satisfy the following

1.3. Fundamental Equality. *Let $\mathfrak{p} \in \mathbb{P}_K$, then*

$$\sum_{\mathfrak{q}|\mathfrak{p}} e(\mathfrak{q}|\mathfrak{p})[\mathbb{F}_\mathfrak{q} : \mathbb{F}_\mathfrak{p}] = [L : K],$$

where the sum is over all places $\mathfrak{q}$ of L lying above $\mathfrak{p}$.

We say that $\mathfrak{q}|\mathfrak{p}$ is **ramified** if $e(\mathfrak{q}|\mathfrak{p}) > 1$, otherwise $\mathfrak{q}|\mathfrak{p}$ is called **unramified**. If $e(\mathfrak{q}|\mathfrak{p}) = [L : K]$, then ($\mathfrak{q}$ is the only place of L above $\mathfrak{p}$ and) we say that $\mathfrak{q}|\mathfrak{p}$ (or $\mathfrak{p}$) is **totally ramified** (in L). We call $\mathfrak{p}$ unramified in L if $\mathfrak{q}|\mathfrak{p}$ is unramified for all $\mathfrak{q} \in \mathbb{P}_L$ above $\mathfrak{p}$. The extension $L|K$ itself is called unramified if all places of K are unramified in L. A place $\mathfrak{p}$ of K is said to **split completely** in L if there are $[L : K]$ places of L above $\mathfrak{p}$ (necessarily each with ramification index and inertia degree equal to 1).

The **different exponent** $d(\mathfrak{q}|\mathfrak{p})$ of $\mathfrak{q}|\mathfrak{p}$ (for a definition see [St2, p. 82]) is always $\geq e(\mathfrak{q}|\mathfrak{p}) - 1$ and $= 0$ iff $\mathfrak{q}|\mathfrak{p}$ is unramified. Since only finitely many places of K ramify in L, one can define the **different** $\sum_{\mathfrak{q} \in \mathbb{P}_L} d(\mathfrak{q}|\mathfrak{q} \cap K)\mathfrak{q} \in \mathcal{D}_L$ of $L|K$. There is a norm map for divisors

$$N_{L|K} : \begin{array}{ccc} \mathcal{D}_L & \to & \mathcal{D}_K \\ \sum_{\mathfrak{q} \in \mathbb{P}_L} m_\mathfrak{q} \mathfrak{q} & \mapsto & \sum_{\mathfrak{p} \in \mathbb{P}_K} \sum_{\mathfrak{q}|\mathfrak{p}} m_\mathfrak{q} [\mathbb{F}_\mathfrak{q} : \mathbb{F}_\mathfrak{p}] \mathfrak{p}. \end{array}$$

We note that $\deg N_{L|K} \mathfrak{m} = d \deg \mathfrak{m}$ for $\mathfrak{m} \in \mathcal{D}_L$. The norm behaves nicely on principal divisors in that $N_{L|K}(z)_L = (N_{L|K} z)_K$ for any $z \in L$, where $N_{L|K}$ on the right hand side denotes the usual norm of elements (see [CF, p. 75]).

Defining the **discriminant** $\mathfrak{d}(L|K) \in \mathcal{D}_K$ as the norm of the different of $L|K$, the genus formula in [St2, p. 88] reads:

1.4. Hurwitz Genus Formula. *In the above situation, the genera of K and L satisfy the relation*

$$d \cdot (g_L - 1) = [L : K](g_K - 1) + \frac{1}{2} \deg \mathfrak{d}(L|K).$$

The special case of $L = K(\mathbb{F}_{q^d}) = \mathbb{F}_{q^d}K$ is called the **constant field extension** of degree d over K. It is Galois with group $G(L|K) \simeq G(\mathbb{F}_{q^d}|\mathbb{F}_q)$. For any place $\mathfrak{p}$ of K and $\mathfrak{q}$ of L above $\mathfrak{p}$, one has $e(\mathfrak{q}|\mathfrak{p}) = 1$ and $\mathbb{F}_\mathfrak{q} = \mathbb{F}_{q^d}\mathbb{F}_\mathfrak{p}$, i.e. there are exactly $r := \gcd(d, \deg \mathfrak{p})$ places $\mathfrak{q}$ of L lying above $\mathfrak{p}$, each of which has degree $\deg \mathfrak{q} = \deg \mathfrak{p}/r$. By the Hurwitz Genus Formula, L has the same genus as K.

If $\mathfrak{p}$ is any place of K, then the **absolute value** map $K \to \mathbb{R}_+$, $z \mapsto |z|_\mathfrak{p} := q^{-(\deg \mathfrak{p})v_\mathfrak{p}(z)}$ defines a metric on K. (Two functions $z, z' \in K$ are close to each other if $v_\mathfrak{p}(z - z')$ is large.) In this way, K is made into a metrical field, i.e. addition, multiplication and the inversion $z \mapsto z^{-1}$ are continuous w.r.t. the defined topology. By the usual construction of "Cauchy sequences modulo zero sequences", we obtain a complete field $K_\mathfrak{p}$ naturally containing K as a dense subfield, and by these properties it is uniquely determined up to K-isomorphism. $K_\mathfrak{p}$ is called the **completion** of K at $\mathfrak{p}$. The topological closure $\bar{\mathfrak{p}}$ of $\mathfrak{p}$ in $K_\mathfrak{p}$ is the maximal ideal in the discrete valuation ring $R_{\bar{\mathfrak{p}}} := \bar{R}_\mathfrak{p}$, the topological closure of $R_\mathfrak{p}$ in $K_\mathfrak{p}$. The residue field $\mathbb{F}_{\bar{\mathfrak{p}}} = R_{\bar{\mathfrak{p}}}/\bar{\mathfrak{p}}$ is naturally isomorphic with $\mathbb{F}_\mathfrak{p}$ and $v_{\bar{\mathfrak{p}}}|_K = v_\mathfrak{p}$. Thus we can identify $\mathbb{F}_{\bar{\mathfrak{p}}}$ with $\mathbb{F}_\mathfrak{p}$, and there is no ambiguity in writing $v_\mathfrak{p}$ instead of $v_{\bar{\mathfrak{p}}}$. Now and then we shall need the following form of the

1.5. Weak Approximation Theorem. *Let $S \subseteq \mathbb{P}_K$ be finite, and, for each $\mathfrak{p} \in S$, let a (positive) integer $m_\mathfrak{p}$ and an element $z_\mathfrak{p} \in K_\mathfrak{p}$ be given. Then there exists $z \in K$ such that $v_\mathfrak{p}(z - z_\mathfrak{p}) \geq m_\mathfrak{p}$ for all $\mathfrak{p} \in S$.*

This theorem is readily derived from its non-complete variant in [St2, p. 11] using the fact that K is dense in $K_\mathfrak{p}$. An application of this theorem will usually be referred to in the text as "weak approximation".

We return to the situation of a finite separable extension $L|K$. Let $\mathfrak{q} \in \mathbb{P}_L$ lie above $\mathfrak{p} \in \mathbb{P}_K$. The natural inclusion $K_\mathfrak{p} \subseteq L_\mathfrak{q}$ is compatible with the inclusions $K \subseteq K_\mathfrak{p}$ and $K \subseteq L \subseteq L_\mathfrak{q}$, and one has $L_\mathfrak{q} = K_\mathfrak{p}L$. The "local extension" $L_\mathfrak{q}|K_\mathfrak{p}$ has degree

$$[L_\mathfrak{q} : K_\mathfrak{p}] = e(\mathfrak{q}|\mathfrak{p})[\mathbb{F}_\mathfrak{q} : \mathbb{F}_\mathfrak{p}].$$

In particular, considering the constant field extension $L = \mathbb{F}_{q^d}K$ of degree $d := \deg \mathfrak{p}$ over K, we see that $\mathbb{F}_{\mathfrak{p}} = \mathbb{F}_{\mathfrak{q}} = \mathbb{F}_{q^d} \subseteq L \subseteq L_{\mathfrak{q}} = K_{\mathfrak{p}}$. This inclusion obviously identifies each residue class $\alpha \in \mathbb{F}_{\mathfrak{p}} = \mathbb{F}_{\bar{\mathfrak{p}}}$ with one of its representatives in $R_{\bar{\mathfrak{p}}} \subseteq K_{\mathfrak{p}}$ and is therefore independent of the choice of $\mathfrak{q}$.

Given a sequence of elements $z_n \in K_{\mathfrak{p}}$, $n \in \mathbb{N}$, the corresponding sequence $(s_m)_{m\in\mathbb{N}_0}$ of partial sums $s_m := \sum_{n=1}^{m} z_n$ is Cauchy (and hence converges in $K_{\mathfrak{p}}$) iff $\lim_{n\to\infty} z_n = 0$, i.e. iff $v_{\mathfrak{p}}(z_n)$ tends to ∞. The limit of the sequence $(s_m)_{m\in\mathbb{N}_0}$ is denoted $\sum_{n=1}^{\infty} z_n$. An element $\pi \in K_{\mathfrak{p}}$ satisfying $v_{\mathfrak{p}}(\pi) = 1$, i.e. $\bar{\mathfrak{p}} = R_{\bar{\mathfrak{p}}}\pi$, is called a **uniformizer** at $\mathfrak{p}$. The structure of $K_{\mathfrak{p}}$ is as follows (cf. [H, p. 155]).

1.6. Proposition. *Let $\mathfrak{p}$ be a place of K and $\pi \in K_{\mathfrak{p}}$ a uniformizer at $\mathfrak{p}$. Then*

$$K_{\mathfrak{p}} = \mathbb{F}_{\mathfrak{p}}((\pi)) = \left\{ \sum_{n=m}^{\infty} \alpha_n \pi^n \;\middle|\; m \in \mathbb{Z} \text{ and } \alpha_n \in \mathbb{F}_{\mathfrak{p}} \text{ for all } n \right\}.$$

*For each $z \in K_{\mathfrak{p}}$, the coefficients $\alpha_n \in \mathbb{F}_{\mathfrak{p}}$ of the **expansion** $z = \sum_n \alpha_n \pi^n$ at $\mathfrak{p}$ in π are uniquely determined by z; moreover, $\alpha_n = 0$ for all $n < m := v_{\mathfrak{p}}(z)$, and $\alpha_m \in \mathbb{F}_{\mathfrak{p}}^*$ is the residue class of z/π^m if $z \neq 0$.*

Proof. The proposition is probably better known in the case of $\mathfrak{p} \in \mathbb{P}_K^1$, for which a proof is given in [St2, p. 143]. (Although there the proposition is only formulated with the uniformizer chosen inside K, the argument given works for any choice of $\pi \in K_{\mathfrak{p}}$.) We reduce the general case of $\mathfrak{p} \in \mathbb{P}_K^d$ with $d \in \mathbb{N}$ to the former by considering the constant field extension $L := \mathbb{F}_{q^d}K$ of degree d over K. Choose a place $\mathfrak{q}$ of L above $\mathfrak{p}$. Because $e(\mathfrak{q}|\mathfrak{p}) = [\mathbb{F}_{\mathfrak{q}} : \mathbb{F}_{\mathfrak{p}}] = 1$, we have $v_{\mathfrak{p}} = v_{\mathfrak{q}}$ on $K_{\mathfrak{p}} = L_{\mathfrak{q}}$, and π is a uniformizer at $\mathfrak{q} \in \mathbb{P}_L^1$ as well. Now, everything follows from the first case. □

Expansions can in many cases be determined very easily from the defining equation of a function field as the following examples show.

1.7. Example. (a) Consider the function field $K := \mathbb{F}_2(x, y)$ where x is an indeterminate over $\mathbb{F}_2$ and $y^2 + y = x^3(x + 1)^2$. By [St2, p. 115], the pole ∞ of x is the only place of $\mathbb{F}_2(x)$ ramified in K, the different exponent being $d(\mathfrak{p}_0|\infty) = 6$, where $\mathfrak{p}_0 \in \mathbb{P}_K^1$ is the place above ∞. Therefore $g_K = 2$ according to the Hurwitz Genus Formula 1.4. The other rational places of K are $\mathfrak{p}_1 := (0, 1)$, $\mathfrak{p}_2 := (1, 0)$, $\mathfrak{p}_3 := (1, 1)$ and $\mathfrak{p}_4 := (0, 0)$, where (α, β) with $\alpha, \beta \in \mathbb{F}_2$ denotes the common zero of $x - \alpha$ and $y - \beta$. Since $\mathbb{P}_K^2$ is empty, $Z_K(t) = 1 + 5t + 15t^2 + \cdots$. Hence $P_K(t) = (1 - 3t + 2t^2)Z_K(t) =$

$1 + 2t + 2t^2 + 4t^3 + 4t^4$ and $h_K = P_K(1) = 13$ according to Theorem 1.2. For later purposes we need expansions at $\mathfrak{p}_4$. Let us take x as a uniformizer. Using the defining equation for K, we obtain

$$y = x^3 + x^5 + y^2 = x^3 + x^5 + x^6 + x^{10} + x^{12} + x^{20} + x^{24} + x^{40} + \cdots,$$

from which we can compute the expansion of any $z \in K = \mathbb{F}_2(x) \oplus \mathbb{F}_2(x)y$ at $\mathfrak{p}_4$ in x.

(b) In the rational function field $K = \mathbb{F}_8(x)$, consider the zero $\mathfrak{p} \in \mathbb{P}_K^2$ of $\pi := x^2 + x + 1$. Write $\mathbb{F}_8^* = \langle\alpha\rangle$ with $\alpha^3 = \alpha + 1$. Then the residue class $\omega := (\alpha x + \alpha^5) + \mathfrak{p} \in \mathbb{F}_\mathfrak{p}$ satisfies $\omega^9 = \alpha$, $\omega^{21} = x + \mathfrak{p}$ and $\mathbb{F}_\mathfrak{p}^* = \langle\omega\rangle$. From $x + \omega^{21} = \pi + (x + \omega^{21})^2 \in \bar{\mathfrak{p}} \subseteq K_\mathfrak{p}$ we derive the expansion

$$x = \omega^{21} + \pi + \pi^2 + \pi^4 + \pi^8 + \pi^{16} + \pi^{32} + \pi^{64} + \pi^{128} + \cdots$$

of x at $\mathfrak{p}$. □

In the course of this work we shall perform several calculations within global function fields $K|\mathbb{F}_q$. Each of these is obtainable from a rational function field $\mathbb{F}_q(x)$ by at most two successive extensions of Kummer or Artin-Schreier type, whence the genus and the places of K can be determined according to the corresponding theorems in [St2]. However, since these are not the only calculations we have to do, we shall make use of KANT/KASH, a powerful number theory tool (for details see [K]), also capable of dealing with global function fields. It requires a global function field to be input in the form $K = \mathbb{F}_q(x, y)$, where y must be integral over the polynomial ring $\mathbb{F}_q[x]$. It will then decompose places in $K|\mathbb{F}_q(x)$ and compute the genus of K.

Let $\mathfrak{p} \in \mathbb{P}_K$ and let $\pi \in K_\mathfrak{p}$ be a uniformizer at $\mathfrak{p}$. There are certain subgroups of $K_\mathfrak{p}^*$ which will play an important role in our computations concerning ray class fields, viz. the **unit group**

$$U_\mathfrak{p}^{(0)} = U_\mathfrak{p} := R_{\bar{\mathfrak{p}}}^* = \left\{\alpha_0 + \alpha_1\pi + \alpha_2\pi^2 + \cdots \;\middle|\; \alpha_0 \in \mathbb{F}_\mathfrak{p}^*,\ \alpha_1, \alpha_2, \ldots \in \mathbb{F}_\mathfrak{p}\right\}$$

and, for any postive integer n, the n-th **one-unit group** at $\mathfrak{p}$,

$$U_\mathfrak{p}^{(n)} := 1 + \bar{\mathfrak{p}}^n = \left\{1 + \alpha_n\pi^n + \alpha_{n+1}\pi^{n+1} + \cdots \;\middle|\; \alpha_n, \alpha_{n+1}, \ldots \in \mathbb{F}_\mathfrak{p}\right\}.$$

The first one-unit group $U_\mathfrak{p}^{(1)}$ is simply called *the* one-unit group. We note that we have a canonical isomorphism $\mathbb{F}_\mathfrak{p}^* \simeq U_\mathfrak{p}/U_\mathfrak{p}^{(1)}$, $\alpha \mapsto \alpha U_\mathfrak{p}^{(1)}$ and that, for positive integers $m \le n$, the factor group

$$U_\mathfrak{p}^{(m)}/U_\mathfrak{p}^{(n)} = \left\{(1 + \alpha_m\pi^m + \cdots + \alpha_{n-1}\pi^{n-1})U_\mathfrak{p}^{(n)} \;\middle|\; \alpha_m, \ldots, \alpha_{n-1} \in \mathbb{F}_\mathfrak{p}\right\}$$

has $q^{(n-m)\deg\mathfrak{p}}$ elements.

2 S-Units

Let $K|\mathbb{F}_q$ be as before. We are concerned here with objects depending on a *non-empty* set $S \subseteq \mathbb{P}_K$ of places of K. The S-units will play an important role in our treatment of the ray class fields. Some tools to compute them are developed in the following.

Let $\mathcal{D}_S$ be the group of divisors of K with support in S, and $\mathcal{D}_S^0 := \mathcal{D}_S \cap \mathcal{D}_K^0$. We write $\deg S$ for the (positive) greatest common divisor of the degrees of the places in S; hence $\deg(\mathcal{D}_S) = \mathbb{Z} \deg S$.

Denote by $\mathcal{O}_S = \bigcap_{\mathfrak{p} \notin S} R_\mathfrak{p}$ the ring of **S-integral functions** in K, i.e. those functions which have poles only in S. The group $\mathcal{O}_S^*$ of invertible elements in $\mathcal{O}_S$ is called the group of **S-units**. By [FJ, p. 22] and [St2, p. 69] the map $S \mapsto \mathcal{O}_S$ is a 1–1 correspondence between the non-empty subsets of $\mathbb{P}_K$ and the Dedekind domains with field of fractions K. Accordingly, $\mathcal{O}_S$ is a Dedekind domain. Its ideal class group, $\mathcal{C}\ell(\mathcal{O}_S)$, which will be referred to as the **S-class group**, is, as usual, defined as the quotient of the group of non-zero fractional ideals of $\mathcal{O}_S$ by its subgroup of principal ideals $z\mathcal{O}_S$ with $z \in K^*$. It has finite order $h_S := |\mathcal{C}\ell(\mathcal{O}_S)|$, called the **$S$-class number**.

The following proposition provides the connection between the S-class group and the group of S-units (cf. [Ro1]).

2.1. Proposition. *The S-class group $\mathcal{C}\ell(\mathcal{O}_S)$ is naturally isomorphic to $\mathcal{D}_K/(\mathcal{D}_S + (K^*))$, and the sequence*

$$0 \to \mathcal{D}_S^0/(\mathcal{O}_S^*) \to \mathcal{D}_K^0/(K^*) \to \mathcal{D}_K/(\mathcal{D}_S + (K^*)) \stackrel{\deg}{\to} \mathbb{Z}/\mathbb{Z}\deg S \to 0$$

is exact.

Proof. The canonical map $\mathcal{D}_K \to \mathcal{C}\ell(O_S)$ taking a divisor $\sum m_\mathfrak{p}\mathfrak{p}$ to the class of the fractional ideal $\prod_{\mathfrak{p} \notin S}(\mathfrak{p} \cap \mathcal{O}_S)^{m_\mathfrak{p}}$ is surjective with kernel $\mathcal{D}_S + (K^*)$. The exactness of the sequence follows (from left to right) from the facts $(\mathcal{O}_S^*) = \mathcal{D}_S^0 \cap (K^*)$, $\mathcal{D}_S^0 + (K^*) = \mathcal{D}_K^0 \cap (\mathcal{D}_S + (K^*))$, $\mathcal{D}_K^0 + \mathcal{D}_S = \{\mathfrak{m} \in \mathcal{D}_K \mid \deg \mathfrak{m} \in \mathbb{Z} \deg S\}$ and $\deg \mathbb{P}_K = 1$ (F. K. Schmidt's Theorem, see [FJ, p. 32] or [St2, p. 164]). □

The index $(\mathcal{D}_S^0 : (\mathcal{O}_S^*))$ is called the **S-regulator** and is denoted by reg_S. More generally, for any subgroup U of finite index in $\mathcal{O}_S^*$ we define its regulator $\mathrm{reg}\, U$ as the index $(\mathcal{D}_S^0 : (U))$; hence $\mathrm{reg}_S = \mathrm{reg}\, \mathcal{O}_S^*$.

2.2. Corollary. *We have $\mathrm{reg}_S h_S = h_K \deg S$, and $(\mathcal{O}_S^*) \simeq \mathcal{O}_S^*/\mathbb{F}_q^*$ is a free abelian group of rank $|S| - 1$ (Dirichlet's Unit Theorem).*

We now turn to the practical computation of S-units. It is reasonable to restrict to the case of S being finite (and non-empty).

We call a family of functions $u_i \in K^*$, $i \in I$, **(multiplicatively) independent (over $\mathbb{Z}$)** if they are linearly independent in the $\mathbb{Z}$-module K^*. Obviously, $(u_i)_{i\in I}$ are independent if and only if the corresponding family of principal divisors $(u_i) \in \mathcal{D}_K^0$ are $\mathbb{Z}$-linearly independent.

In all the examples that we shall treat in this thesis, it is not hard to find $s := |S| - 1$ independent S-units $u_1, \ldots, u_s$ simply by guessing. (A general algorithm, which does this automatically, is currently being implemented in KASH.) However, the principal divisors $(u_1), \ldots, (u_s)$ found in this way sometimes do not generate all of $(\mathcal{O}_S^*)$. In order to check if they do and, if they do not, to see how to produce other S-units generating larger subgroups of $\mathcal{O}_S^*$, it is useful to determine the regulator.

2.3. Lemma. *Let $s := |S|-1 \in \mathbb{N}_0$ and write $S = \{\mathfrak{p}_0, \ldots, \mathfrak{p}_s\}$. Let $u_1, \ldots, u_s$ be independent S-units, U the subgroup of $\mathcal{O}_S^*$ generated by them, and $A_0 := (v_{\mathfrak{p}_j}(u_i))_{1\le i,j\le s} \in \mathbb{Z}^{s\times s}$. Then*

$$\operatorname{reg} U = \frac{\deg S}{\deg \mathfrak{p}_0} \left|\det A_0\right| .$$

This is a slight improvement compared to a result by Schörnig [Sg, p. 53], who only made use of the fact that $\operatorname{reg} U$ divides $|\det A_0|$. Note that Schörnig's definition of the regulator differs from ours by the factor $\prod_{j=0}^{s} \deg \mathfrak{p}_j / \deg S$.

Proof. Set $d_j := \deg\{\mathfrak{p}_0, \ldots, \mathfrak{p}_j\}$ and $b_j := d_{j-1}/d_j$. Applying the submodule basis construction from the proof in [Wa, p. 3] of the well-known theorem on free modules over a principal ideal domain shows that there exists an upper triangular matrix $B \in \mathbb{Z}^{s\times s}$ having $b_1, \ldots, b_s$ on its diagonal such that

$$(\mathfrak{b}_1, \ldots, \mathfrak{b}_s) := (\mathfrak{p}_0, \ldots, \mathfrak{p}_s) \begin{pmatrix} * \\ B \end{pmatrix}$$

is a $\mathbb{Z}$-basis for $\mathcal{D}_S^0$. Since $\Phi : \mathcal{D}_S^0 \to \mathbb{Z}^s$, $\sum_{i=0}^{s} c_i\mathfrak{p}_i \mapsto (c_1, \ldots, c_s)$ is injective, we can conclude that

$$(\mathcal{D}_S^0 : (U)) = (\Phi\mathcal{D}_S^0 : \Phi(U)) = \left|\frac{\det A_0}{\det B}\right| = \frac{d_s}{d_0} \left|\det A_0\right| . \quad \square$$

2.4. Remark. In the situation of the lemma, let S' be a non-empty subset of S. Then a $\mathbb{Z}$-basis for $U \cap \mathcal{O}_{S'}$ can be obtained as follows. Assume w.l.o.g. that $S' = \{\mathfrak{p}_0, \ldots, \mathfrak{p}_{s'}\}$ where $s' = |S'| - 1$. Since $\mathbb{Z}$ is euclidean, we can compute $T = (t_{ij})_{1\le i,j\le s} \in \mathrm{GL}_s(\mathbb{Z})$ such that TA_0 is lower triangular. Setting $u_i' := \prod_{j=1}^{s} u_j^{t_{ij}}$, it is easily seen that $u_1', \ldots, u_{s'}'$ form a basis for $U \cap \mathcal{O}_{S'}$.

A basis for $\mathcal{O}_S^*/\mathbb{F}_q^*$ can now be constructed from $u_1, \ldots, u_s$ by applying the following proposition to each prime number l dividing $\operatorname{reg} U$.

2.5. Proposition. *In the situation of the previous lemma we set* $A := (v_{\mathfrak{p}_j}(u_i))_{\substack{1\le i\le s\\ 0\le j\le s}} \in \mathbb{Z}^{s\times(s+1)}$ *and write* $^-$ *to denote reduction modulo a given prime number* $l \in \mathbb{N}$. *Consider the group isomorphism*

$$\mathfrak{u} : \mathbb{Z}^s \to (U) \simeq U, \quad (m_1, \ldots, m_s) \mapsto (u_1^{m_1} \cdots u_s^{m_s}).$$

The pre-images $M := \mathfrak{u}^{-1}((U) \cap (K^{*l}))$ *and* $N := \mathfrak{u}^{-1}((U) \cap l\mathcal{D}_K)$ *satisfy* $l\mathbb{Z}^s \subseteq M \subseteq N$, *hence* $\bar{M} := M/l\mathbb{Z}^s \subseteq \bar{N} := N/l\mathbb{Z}^s \subseteq \mathbb{F}_l^s$.

(a) $\bar{N}$ *is the kernel of* $\mathbb{F}_l^s \to \mathbb{F}_l^{s+1}$, $\nu \mapsto \nu\bar{A}$.

(b) $\bar{M} = 0 \iff l \nmid ((\mathcal{O}_S^*) : (U))$.

(c) *Let* $m \in N$ *and* $z \in K^*$. *Then* $\mathfrak{u}(m) = (z^l)$ *iff* $z \in \mathcal{L}(-\mathfrak{u}(m)/l) \setminus \{0\}$.

(d) *The dimension of* $\bar{N}$ *equals the* l*-rank of* $\mathcal{D}_S^0/(U)$, *which in turn is bounded by* $v_l(\operatorname{reg} U)$.

Proof. Note that $l\mathbb{Z}^s$ is the $\mathfrak{u}$-pre-image of $(U^l) \subseteq (U) \cap (K^{*l})$.

(a) For $m \in \mathbb{Z}^s$, by definition, $mA \in \mathbb{Z}^{s+1}$ is the row vector whose components are the coefficients of the divisor $\mathfrak{u}(m)$. Reduction modulo l shows the assertion.

(b) $l|((\mathcal{O}_S^*) : (U))$ means that there exists $z \in K^*$ satisfying $(z^l) \in (U)$ and $(z) \notin (U)$, i.e. $\mathfrak{u}^{-1}(l(z)) \in M \setminus l\mathbb{Z}^s$.

(c) This is clear from the definition of Riemann-Roch space and because $\mathfrak{u}$ has values in $\mathcal{D}_K^0$.

(d) Recall that the l-rank of an abelian group G is defined as the $\mathbb{F}_l$-dimension of G/lG, and that it is $\le v_l(|G|)$ if G is finite. Now $\mathfrak{u}$ induces a surjective $\mathbb{F}_l$-homomorphism $\mathbb{F}_l^s \to ((U) + l\mathcal{D}_S^0)/l\mathcal{D}_S^0$, whose kernel is $\bar{N}$. Hence

$$\dim_{\mathbb{F}_l} \bar{N} = s - \dim_{\mathbb{F}_l}((U) + l\mathcal{D}_S^0)/l\mathcal{D}_S^0 = \dim_{\mathbb{F}_l} \mathcal{D}_S^0/((U) + l\mathcal{D}_S^0),$$

but $\mathcal{D}_S^0/((U) + l\mathcal{D}_S^0) \simeq \frac{\mathcal{D}_S^0/(U)}{l(\mathcal{D}_S^0/(U))}$. □

The proposition suggests an algorithm that we want to describe briefly and informally in the following. First we determine $\bar{N}$ from the matrix A by means of 2.5(a). In order to find out whether l divides $((\mathcal{O}_S^*) : (U))$, by 2.5(b) it suffices to test the condition

(1) $\quad \mathfrak{u}(m) \in (K^{*l})$

with $\bar{m}$ running through a system of representatives for the orbits $\{\mathbb{F}_l^* \nu \,|\, \nu \in \bar{N} \setminus \{0\}\}$, since $\bar{M}$ is a subspace of $\bar{N}$. These are $(|\bar{N}| - 1)/(l-1)$ tests, so we have an obvious improvement of the algorithm in [Sg, p. 54], which contains a loop over $l^s - 1$ elements. This simplification has the additional advantage that we can choose the vectors m with at least one component, say m_i, equal to 1, so that, in case (1) holds, we simply replace u_i by $z \in \mathcal{L}(-\mathfrak{u}(m)/l) \setminus \{0\}$ and thus obtain a larger subgroup U' of $\mathcal{O}_S^*$ satisfying $(U' : U) = l$, to which we can apply the described procedure anew.

Due to 2.5(c), each test (1) comes down to determining a Riemann-Roch space (of dimension 0 or 1), a task for which a KANT algorithm has been implemented by Heß [He]. If l equals the characteristic p of K, then 1 can be tested much easier, since taking p-th roots in K is a simple exercise in linear algebra. Recall that the p-th power map in characteristic p is an injective ring homomorphism, i.e. a p-th root is unique (if it exists), and that the p-th root of $\alpha \in \mathbb{F}_q$ is $\alpha^{q/p}$.

2.6. Lemma. *Let $(y_1, \ldots, y_n)$ be a basis for the characteristic p field extension $K|k$. We form the transition matrix $W = (w_{ij})_{1 \le i,j \le n} \in k^{n \times n}$ with $y_i^p = \sum_{j=1}^n w_{ij} y_j$.*

(a) *The matrix W is invertible if and only if $K|k$ is separable.*

(b) *Let $u = \sum_{i=1}^n f_i y_i$ and $z = \sum_{i=1}^n g_i y_i$ with $f_1, \ldots, f_n, g_1, \ldots, g_n \in k$. Then $u = z^p$ is equivalent to $(f_1, \ldots, f_n) = (g_1^p, \ldots, g_n^p)W$.*

(c) *The p-th power image of $\mathbb{F}_q(x)$, x an indeterminate of $\mathbb{F}_q$, is $\mathbb{F}_q(x^p)$.*

Proof. **(a)** W is invertible iff $y_1^p, \ldots, y_n^p$ are linearly independent over k, which amounts to saying that K^p and k are linearly disjoint over k^p (here the superscript p denotes p-th power); but this means that $K|k$ is separable.

(b) and **(c)** are immediately verified. □

This lemma can readily be applied to any global function field $K|\mathbb{F}_q$ because, by [St2, p. 128], there always exists $x \in K \setminus \mathbb{F}_q$ such that $K|\mathbb{F}_q(x)$ is separable.

2.7. Example. Let K be the function field $\mathbb{F}_4(x, y)$, where x is an indeterminate over $\mathbb{F}_4$ and

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

Because $u = (y^2 - y)/(x^2 - x)$ satisfies $u^2 - u = \frac{x^2+x+1}{x^2(x-1)}$, K is obtainable from $\mathbb{F}_4(x)$ by two successive Artin-Schreier extensions. Moreover $K|\mathbb{F}_4(x)$ is Galois. The Galois group is generated by the two automorphisms which take

y to $y+1$ and $y+x$, respectively, and hence is abelian of type $(2,2)$. Choose $\alpha \in \mathbb{F}_4 \setminus \mathbb{F}_2$. The following facts are easily verified using [St2, p. 115]. Exactly those places of K associated to x, $x-1$ and the pole ∞ of x are ramified in K, each with ramification index 2 and inertia degree 1, and K has genus 3 and 14 rational places, namely

$$\begin{array}{llll} \mathfrak{p}_0 := (0,\alpha), & \mathfrak{p}_1 := (0,\alpha^2), & \mathfrak{p}_2 := (1,0), & \mathfrak{p}_3 := (1,1), \\ \mathfrak{p}_4 := (\alpha,0), & \mathfrak{p}_5 := (\alpha,1), & \mathfrak{p}_6 := (\alpha,\alpha), & \mathfrak{p}_7 := (\alpha,\alpha^2), \\ \mathfrak{p}_8 := (\alpha^2,0), & \mathfrak{p}_9 := (\alpha^2,1), & \mathfrak{p}_{10} := (\alpha^2,\alpha), & \mathfrak{p}_{11} := (\alpha^2,\alpha^2), \\ \mathfrak{p}_{12}, \mathfrak{p}_{13}, & & & \end{array}$$

where (α,β) with $\alpha,\beta \in \mathbb{F}_4$ denotes the place of K which is the common zero of $x-\alpha$ and $y-\beta$, and $\mathfrak{p}_{12}$ and $\mathfrak{p}_{13}$ are the zeros of y/x and $y/x-1$, respectively, which lie above ∞. Let $S := \{\mathfrak{p}_0, \ldots, \mathfrak{p}_{13}\}$ and "guess" S-units

$$\begin{aligned}(u_1, \ldots, u_{13}) = (&x, x+\alpha, x+\alpha^2, y, y+1, y+\alpha, y+\alpha^2, y+x, \\ &y+x+\alpha, y+\alpha x, y+\alpha x+\alpha, y+\alpha^2 x, y+\alpha^2 x+\alpha);\end{aligned}$$

then

$$A := (v_{\mathfrak{p}_j}(u_i))_{\substack{1\le i\le 13\\ 0\le j\le 13}} = \begin{pmatrix} 2&2&0&0&0&0&0&0&0&0&0&0&0&-2&-2\\ 0&0&0&0&1&1&1&1&0&0&0&0&-2&-2\\ 0&0&0&0&0&0&0&0&1&1&1&1&-2&-2\\ 0&0&1&0&1&0&0&0&1&0&0&0&-1&-2\\ 0&0&0&1&0&1&0&0&0&1&0&0&-1&-2\\ 1&0&0&0&0&0&1&0&0&0&1&0&-1&-2\\ 0&1&0&0&0&0&0&1&0&0&0&1&-1&-2\\ 0&0&0&1&0&0&1&0&0&0&0&1&-2&-1\\ 1&0&0&0&1&0&0&0&0&1&0&0&-2&-1\\ 0&0&0&0&0&0&0&2&0&2&0&0&-2&-2\\ 1&0&1&0&0&1&0&0&0&0&0&1&-2&-2\\ 0&0&0&0&0&2&0&0&0&0&2&0&-2&-2\\ 1&0&0&1&0&0&0&1&1&0&0&0&-2&-2 \end{pmatrix}.$$

Without regard to sign, any 13×13-minor of A (erase one column and compute the determinant) equals 512, which by Lemma 2.3 is the regulator of $U := \langle u_1, \ldots, u_{13}\rangle$. We want to test whether 2 divides $((\mathcal{O}_S^*) : (U))$ by means of Propositon 2.5 and find $\bar{N} = \mathbb{F}_2 e_1 \oplus \mathbb{F}_2 e_{10} \oplus \mathbb{F}_2 e_{12}$, where e_i denotes the i-th canonical basis vector in $\mathbb{F}_2^{13}$. Hence we have to search for squares in the set

$$\begin{aligned} V :=& \{u_1^{m_1} u_{10}^{m_{10}} u_{12}^{m_{12}} \mid (0,0,0) \neq (m_1, m_{10}, m_{12}) \in \{0,1\}^3\} \\ =& \{x, y+\alpha x, y+\alpha^2 x, xy+\alpha x^2, xy+\alpha^2 x^2, \\ & \qquad y^2+xy+x^2, xy^2+x^2 y+x^3\}. \end{aligned}$$

Applying Lemma 2.6 with $(1, y, y^2, y^3)$ as a basis for $K|\mathbb{F}_4(x)$, i.e.

$$W^{-1} = \frac{1}{x^2-x}\begin{pmatrix} x^2-x & 0 & 0 & 0 \\ x^3-1 & x^2+x+1 & 1 & 0 \\ 0 & x^2-x & 0 & 0 \\ 0 & x^3-1 & x^2+x+1 & 1 \end{pmatrix},$$

shows that in fact no element of V is a square in K and hence proves $\mathcal{O}_S^* = \mathbb{F}_4^* U$ and $\mathrm{reg}_S = 512$.

If we have information about the S-class number and the divisor class number, we can determine the regulator reg_S directly or estimate it from below by means of 2.2. One such technique is demonstrated in the following example continued from Section 1.

2.8. Example. Let $K = \mathbb{F}_2(x, y)$ and $\mathfrak{p}_0, \ldots, \mathfrak{p}_4$ as in Example 1.7(a). Suppose $S \subseteq \mathbb{P}_K^1$ contains at least two elements, say $\mathfrak{p} \neq \mathfrak{p}'$, then $\mathfrak{p} - \mathfrak{p}' \in \mathcal{D}_S^0 \setminus (K^*)$ by Theorem 1.1, and consequently $\mathrm{reg}_S > 1$. Let $0 \leq k \leq 4$ and consider the set $S_k := \{\mathfrak{p}_0, \ldots, \mathfrak{p}_k\}$. Then $\mathrm{reg}_{S_k} = h_K = 13$ and $h_{S_k} = 1$ for $k \geq 1$ by Corollary 2.2. We "guess" S_4-units $u_1 := x$, $u_2 := x + 1$, $u_3 := y$ and $u_4 := y + x^2$ and set

$$A := \big(v_{\mathfrak{p}_j}(u_i)\big)_{\substack{1 \leq i \leq 4 \\ 0 \leq j \leq 4}} = \begin{pmatrix} -2 & 1 & 0 & 0 & 1 \\ -2 & 0 & 1 & 1 & 0 \\ -5 & 0 & 2 & 0 & 3 \\ -5 & 0 & 0 & 3 & 2 \end{pmatrix} \text{ and } T := \begin{pmatrix} 13 & 6 & -3 & -2 \\ 5 & 3 & -1 & -1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \in \mathrm{GL}_4(\mathbb{Z}).$$

By Lemma 2.3,

$$TA = \begin{pmatrix} -13 & 13 & 0 & 0 & 0 \\ -6 & 5 & 1 & 0 & 0 \\ -2 & 0 & 1 & 1 & 0 \\ -2 & 1 & 0 & 0 & 1 \end{pmatrix}$$

shows that $\mathcal{O}_{S_4}^* = \langle u_1, u_2, u_3, u_4 \rangle$. Moreover, writing $T = (t_{ij})_{1 \leq i,j \leq 4}$ and setting $u_k' := \prod_{j=1}^4 u_j^{t_{kj}}$, we obtain $\mathcal{O}_{S_k}^* = \langle u_1', \ldots, u_k' \rangle$ according to Remark 2.4. This example is continued in Section 6.

3 Ramification Groups

We shall recall some basics of Hilbert's ramification theory as found in [Nk, pp. 186ff] or [St2, pp. 118ff] and prove an upper index version of Hilbert's Different Formula for abelian extensions by means of the Hasse-Arf Theorem. Although we restrict ourselves to the function field case here, everything in this section, except for Example 3.3 and Corollary 3.5, carries over literally to number fields by merely requiring the "places" (i.e. primes) under consideration to be non-archimedean.

Let $K|\mathbb{F}_q$ be as before, $\bar{K}$ a fixed algebraic closure of K, $L|K$ a finite Galois extension with group $G(L|K)$, $\mathfrak{p}$ a place of K and $\mathfrak{q}$ a place of L lying above $\mathfrak{p}$. It is well-known that $G(L|K)$ acts transitively on the set of all places of L above $\mathfrak{p}$. For $s \in [-1, \infty)$ there is the s-th **lower ramification group** of $\mathfrak{q}|\mathfrak{p}$,

$$G_s(\mathfrak{q}|\mathfrak{p}) := \{\sigma \in G(L|K) \mid v_{\mathfrak{q}}(\sigma z - z) \geq s + 1 \ \forall z \in R_{\mathfrak{q}}\}.$$

We note that $G_{-1}(\mathfrak{q}|\mathfrak{p}) = \{\sigma \in G \,|\, \sigma\mathfrak{q} = \mathfrak{q}\}$ is the **decomposition group** and $G_0(\mathfrak{q}|\mathfrak{p})$ is the **inertia group** of $\mathfrak{q}|\mathfrak{p}$. See [St2, p. 119] for their specific properties. After renumbering by means of the continuous and strictly isotonous bijection

$$\eta = \eta_{\mathfrak{q}|\mathfrak{p}} : \begin{array}{ccc} [-1,\infty) & \to & [-1,\infty) \\ s & \mapsto & \displaystyle\int_0^s \frac{|G_x(\mathfrak{q}|\mathfrak{p})|}{|G_0(\mathfrak{q}|\mathfrak{p})|}dx, \end{array}$$

we get the **upper ramification groups** $G^{\eta(s)}(\mathfrak{q}|\mathfrak{p}) := G_s(\mathfrak{q}|\mathfrak{p})$. (Note that η is the identity in any case on $[-1,0]$.) Whereas, by definition, the lower numbering is stable under modification of the lower field K (see [Nk, p. 187]), the upper numbering is compatible with a change of the upper field (see [Nk, p. 190]):

3.1. Proposition. *For any Galois subextension $L'|K$ of $L|K$ with $\mathfrak{q}' := \mathfrak{q} \cap L'$, the restriction map $G(L|K) \to G(L'|K)$ sends $G^s(\mathfrak{q}|\mathfrak{p})$ onto $G^s(\mathfrak{q}'|\mathfrak{p})$ for all $s \in [-1,\infty)$.*

Analogously we can define the ramification groups of the local extension $L_\mathfrak{q}|K_\mathfrak{p}$, which we denote by $G_s(L_\mathfrak{q}|K_\mathfrak{p})$ and $G^s(L_\mathfrak{q}|K_\mathfrak{p})$ for the moment. Clearly, $G_{-1}(L_\mathfrak{q}|K_\mathfrak{p}) = G^{-1}(L_\mathfrak{q}|K_\mathfrak{p}) = G(L_\mathfrak{q}|K_\mathfrak{p})$. Since the restriction map $G(L_\mathfrak{q}|K_\mathfrak{p}) \to G(L|K)$ is injective and sends $G_s(L_\mathfrak{q}|K_\mathfrak{p})$ onto $G_s(\mathfrak{q}|\mathfrak{p})$ and $G^s(L_\mathfrak{q}|K_\mathfrak{p})$ onto $G^s(\mathfrak{q}|\mathfrak{p})$ for all $s \in [-1,\infty)$ (see [CF, p. 41]), we shall identify these groups with one another and drop the notations $G_s(L_\mathfrak{q}|K_\mathfrak{p})$ and $G^s(L_\mathfrak{q}|K_\mathfrak{p})$ again.

The canonical surjection $G^{-1}(\mathfrak{q}|\mathfrak{p}) \twoheadrightarrow G(\mathbb{F}_\mathfrak{q}|\mathbb{F}_\mathfrak{p})$ has as kernel the inertia group $G^0(\mathfrak{q}|\mathfrak{p})$. Hence, in the case that $\mathfrak{q}|\mathfrak{p}$ is unramified, there is a unique element $\varphi_{\mathfrak{q}|\mathfrak{p}} \in G^{-1}(\mathfrak{q}|\mathfrak{p})$ satisfying

$$\varphi_{\mathfrak{q}|\mathfrak{p}} z \equiv z^{q^{\deg \mathfrak{p}}} \mod \mathfrak{q}$$

for all $z \in R_\mathfrak{q}$, called the **Frobenius automorphism** of $\mathfrak{q}|\mathfrak{p}$ (cf. [CF, p. 164]), which will be used in Section 4. Note that $\varphi_{\sigma\mathfrak{q}|\mathfrak{p}} = \sigma\varphi_{\mathfrak{q}|\mathfrak{p}}\sigma^{-1}$ for $\sigma \in G(L|K)$.

Since $G_s(\sigma\mathfrak{q}|\mathfrak{p}) = \sigma G_s(\mathfrak{q}|\mathfrak{p})\sigma^{-1}$ for any automorphism $\sigma \in G(L|K)$ and $s \in [-1,\infty)$, the orders of the (lower and upper) ramification groups do not depend on the specific choice of $\mathfrak{q}$. Therefore, we can define the **conductor exponent** $f(L,\mathfrak{p})$ of $\mathfrak{p}$ in L as the least integer $m \geq 0$ such that $G^m(\mathfrak{q}|\mathfrak{p})$ is trivial. The effective divisor

$$\mathfrak{f}(L|K) := \sum_{\mathfrak{p} \in \mathbb{P}_K} f(L,\mathfrak{p})\mathfrak{p}$$

of K is called the **conductor** of $L|K$. Because $G^0(\mathfrak{q}|\mathfrak{p})$ is the inertia group of $\mathfrak{q}|\mathfrak{p}$, the places of K occurring in $\mathfrak{f}(L|K)$ are exactly those which ramify in L. The Conductor Lemma in Section 5 below shows that in the abelian case $\mathfrak{f}(L|K)$ is indeed the conductor of $L|K$ in the sense of class field theory.

We also define the **splitting set** $S(L|K) \subseteq \mathbb{P}_K$ of $L|K$ as the set consisting of those places $\mathfrak{p}$ of K which split completely in L. Due to the properties of the decomposition group we have

$$S(L|K) = \big\{\mathfrak{p} \in \mathbb{P}_K \,\big|\, G^{-1}(\mathfrak{q}|\mathfrak{p}) = 1 \text{ for } \mathfrak{q} \in \mathbb{P}_L \text{ above } \mathfrak{p}\big\}. \tag{2}$$

As a consequence of Proposition 3.1, the splitting set and the conductor enjoy the following properties:

3.2. Corollary. *Let L_1 and L_2 be two finite Galois extensions of K within $\bar{K}$.*

(a) *If $L_1 \subseteq L_2$ then $S(L_1|K) \supseteq S(L_2|K)$ and $\mathfrak{f}(L_1|K) \leq \mathfrak{f}(L_2|K)$.*

(b) *Let $L := L_1L_2$. Then $S(L|K) = S(L_1|K) \cap S(L_2|K)$, and $\mathfrak{f}(L|K) = \max\{\mathfrak{f}(L_1|K), \mathfrak{f}(L_2|K)\}$, where the maximum is taken coefficientwise.*

Proof. Let $s \in [-1, \infty)$ and $\mathfrak{p} \in \mathbb{P}_K$.

(a) Choose $\mathfrak{q}_1 \in \mathbb{P}_{L_1}$ and $\mathfrak{q}_2 \in \mathbb{P}_{L_2}$ such that $\mathfrak{q}_2|\mathfrak{q}_1|\mathfrak{p}$. By 3.1, the triviality of $G^s(\mathfrak{q}_2|\mathfrak{p})$ implies that of $G^s(\mathfrak{q}_1|\mathfrak{p})$. Hence $f(L_1, \mathfrak{p}) \leq f(L_2, \mathfrak{p})$ by definition of the conductor exponent.

(b) Choose a place $\mathfrak{q}$ of L above $\mathfrak{p}$ and let $\mathfrak{q}_1 := \mathfrak{q} \cap L_1$ and $\mathfrak{q}_2 := \mathfrak{q} \cap L_2$. From 3.1 we see that $G^s(\mathfrak{q}|\mathfrak{p})$ is trivial iff $G^s(\mathfrak{q}_1|\mathfrak{p})$ and $G^s(\mathfrak{q}_2|\mathfrak{p})$ are trivial. Hence $f(L, \mathfrak{p}) = \max\{f(L_1, \mathfrak{p}), f(L_2, \mathfrak{p})\}$. The assertion on the splitting sets follows with (2). □

As an application we give the following

3.3. Example (Artin-Schreier Extensions). *Let $\wp : \bar{K} \to \bar{K}$, $z \mapsto z^p - z$, be the **Artin-Schreier operator** and define the **Artin-Schreier reduced valuation** of a function $u \in K$ at a place $\mathfrak{p} \in \mathbb{P}_K$ by*

$$v^*_{\mathfrak{p}}(u) := \max\{v_{\mathfrak{p}}(u - \wp t) \,|\, t \in K\} \in \mathbb{Z} \cup \{\infty\}.$$

Let $U \subseteq K$ be finite and $L := K(\wp^{-1}U) \subseteq \bar{K}$.

(a) *For $u \in K$ with $v_{\mathfrak{p}}(u) < 0$ we have the equivalence*

$$v_{\mathfrak{p}}(u) = v^*_{\mathfrak{p}}(u) \iff v_{\mathfrak{p}}(u) \not\equiv 0 \mod p.$$

(b) *The extension $L|K$ has conductor*

$$\mathfrak{f}(L|K) = \sum_{m_\mathfrak{p}>0} (m_\mathfrak{p}+1)\mathfrak{p},$$

where $m_\mathfrak{p} := -\min_{u\in U} v^*_\mathfrak{p}(u)$ for $\mathfrak{p} \in \mathbb{P}_K$.

(c) *The splitting set of $L|K$ is $S(L|K) = \{\mathfrak{p} \in \mathbb{P}_K \mid v^*_\mathfrak{p}(u) > 0 \ \forall u \in U\}$.*

(d) *The degree of $L|K$ is $[L:K] = (V + \wp K : \wp K)$, where $V := \sum_{u\in U} \mathbb{F}_p u$ is the $\mathbb{F}_p$-subspace of K spanned by U.*

Proof. **(a)** See [St2, p. 114].

(b) Let $u \in U$. We show that $K_u := K(\wp^{-1}u) \subseteq L$ satisfies

$$\mathfrak{f}(K_u|K) = \sum_{v^*_\mathfrak{p}(u)<0} \big(1 - v^*_\mathfrak{p}(u)\big)\mathfrak{p}. \tag{3}$$

If $u \in \wp K$, then $K_u = K$ and $v^*_\mathfrak{p}(u) = \infty$ for all $\mathfrak{p} \in \mathbb{P}_K$, and we are done. Otherwise $K_u|K$ is Galois of degree p and we can use Proposition III.7.8 of [St2, p. 115]. Let $\mathfrak{p} \in \mathbb{P}_K$. If $v^*_\mathfrak{p}(u) \geq 0$, then $\mathfrak{p}$ is unramified in L, i.e. $f(K_u, \mathfrak{p}) = 0$. In case $m := -v^*_\mathfrak{p}(u) > 0$, exactly one place $\mathfrak{q} \in \mathbb{P}_{K_u}$ lies over $\mathfrak{p}$ (with $e(\mathfrak{q}|\mathfrak{p}) = p$, i.e. $\mathfrak{p}$ is totally ramified in K_u) and the different exponent equals

$$d(\mathfrak{q}|\mathfrak{p}) = (p-1)(m+1).$$

A comparison with Hilbert's Different Formula (see [St2, p. 124])

$$d(\mathfrak{q}|\mathfrak{p}) = \sum_{n=0}^{\infty} (|G_n(\mathfrak{q}|\mathfrak{p})| - 1)$$

yields $G(K_u|K) = G_0(\mathfrak{q}|\mathfrak{p}) = \cdots = G_m(\mathfrak{q}|\mathfrak{p})$ and $G_{m+1}(\mathfrak{q}|\mathfrak{p}) = 1$. Hence the bijection $\eta_{\mathfrak{q}|\mathfrak{p}}$ is the identity on $[-1, m]$ and $\eta_{\mathfrak{q}|\mathfrak{p}}(s) = m + \frac{s-m}{p}$ for $s \in [m, \infty)$. We conclude that $G^m(\mathfrak{q}|\mathfrak{p}) = G_m(\mathfrak{q}|\mathfrak{p}) = G(K_u|K)$ and $G^{m+1}(\mathfrak{q}|\mathfrak{p}) = G_{m+p}(\mathfrak{q}|\mathfrak{p}) = 1$; hence, $f(K_u, \mathfrak{p}) = m + 1 = 1 - v^*_\mathfrak{p}(u)$ by the definition of the conductor exponent. Thus we have established (3) for all $u \in U$, and the formula for $\mathfrak{f}(L|K)$ follows from 3.2(b) since $L = \prod_{u\in U} K_u$.

(c) Let $\mathfrak{p} \in \mathbb{P}_K$ and $u \in U$. We write $K_u = K(\wp^{-1}u) = K(y)$ with $y \in \wp^{-1}u$ and show

$$v^*_\mathfrak{p}(u) > 0 \iff \mathfrak{p} \in S(K_u|K).$$

Suppose $v_{\mathfrak{p}}^*(u) > 0$. Then there exists $t \in K$ such that $\tilde{y} := y - t$ satisfies $\tilde{y}^p - \tilde{y} = u - \wp t \equiv 0 \mod \mathfrak{p}$. Hence $\mathfrak{p}$ splits completely in $K_u = K(\tilde{y})$ according to [St2, p. 76]. Conversely, suppose $\mathfrak{p}$ splits completely in K_u. Then we can assume $v_{\mathfrak{p}}(u) \geq 0$ by the proof of (b) and, using [St2, pp. 96,76], conclude that $u \equiv \wp t \mod \mathfrak{p}$ for some $t \in R_{\mathfrak{p}}$; hence $v_{\mathfrak{p}}^*(u) \geq v_{\mathfrak{p}}(u - \wp t) > 0$. The assertion follows with 3.2(b).

(d) This is due to the Kummer theory of the operator $\wp$ (also called Artin-Schreier theory, see [Nk, p. 294]). □

By Čebotarev's Density Theorem[1], $S(L|K)$ and, for $[L : K] > 1$, also its complement $\mathbb{P}_K \setminus S(L|K)$ is an infinite set. Another well-known consequence of this deep theorem is the fact that L is uniquely determined by $S(L|K)$ as a finite Galois extension of K. More precisely, sharpening 3.2(a), we have

3.4. Theorem. *Let L_1 and L_2 be finite Galois extensions of K within $\bar{K}$. Then*

$$L_1 \subseteq L_2 \iff S(L_1|K) \supseteq S(L_2|K).$$

Proof. See [CF, p. 362]. □

From this we can derive the following generalization of F. K. Schmidt's Theorem:

3.5. Corollary. *For $d \in \mathbb{N}$, let $S_d = \bigcup_{n=1}^{\infty} \mathbb{P}_K^{nd}$ be the set of all places of $K|\mathbb{F}_q$ whose degree is divisible by d, and $K_d = \mathbb{F}_{q^d}K \subseteq \bar{K}$ the constant field extension of degree d over K. Then $S_d = S(K_d|K)$, $\deg S_d = d$, and K_d is the largest Galois extension L of K within $\bar{K}$ such that $S_d \subseteq S(L|K)$.*

Proof. Clearly, $\mathfrak{p} \in \mathbb{P}_K$ splits completely in $K_d|K$ if and only if d divides $\deg \mathfrak{p}$. To verify the second assertion, set $d' := \deg S_d$. Then $S_d = S_{d'}$, which by Theorem 3.4 implies $K_d = K_{d'}$ and hence $d = d'$. Finally, let $L \subseteq \bar{K}$ be finite Galois over K with $S_d = S(K_d|K) \subseteq S(L|K)$. Then, again by Theorem 3.4, $L \subseteq K_d$. □

In what follows, $L|K$ will be assumed finite *abelian*. The Frobenius automorphism and the ramification groups no longer depend on $\mathfrak{q}$, so we can write $\varphi_{L,\mathfrak{p}}$ instead of $\varphi_{\mathfrak{q}|\mathfrak{p}}$ and $G^s(L, \mathfrak{p})$ instead of $G^s(\mathfrak{q}|\mathfrak{p})$. The subfield of L fixed by $G^s(L, \mathfrak{p})$ is denoted $L^s(\mathfrak{p})$ and called the s-th **upper ramification field**

[1] We do not want to formulate the theorem itself here. Instead, we state some of its consequences which are not essential for what follows but produce illustrative examples.

of $\mathfrak{p}$ in L. In particular, $L^{-1}(\mathfrak{p})$ is the **decomposition field** and $L^0(p)$ is the **inertia field** of $\mathfrak{p}$ in L (cf. [St2, p. 118]). As we shall see later, the upper ramification fields have an interpretation in terms of ray class fields. In view of this, it will turn out useful to have an upper index version of Hilbert's

3.6. Different Formula. *The different exponent of* $\mathfrak{q}|\mathfrak{p}$ *satisfies*

$$\begin{aligned} d(\mathfrak{q}|\mathfrak{p}) &= \sum_{n=0}^{\infty} \left(\left| G^0(L,\mathfrak{p}) \right| - (G^0(L,\mathfrak{p}) : G^n(L,\mathfrak{p})) \right) \\ &= \sum_{n=0}^{\infty} \left([L : L^0(\mathfrak{p})] - [L^n(\mathfrak{p}) : L^0(\mathfrak{p})] \right). \end{aligned}$$

Proof. For convenience, put $G^s := G^s(L,\mathfrak{p})$, $\eta := \eta_{\mathfrak{q}|\mathfrak{p}}$ and $\psi := \eta^{-1}$. Set $t_0 := -1$ and let $0 \le t_1 < \cdots < t_r$ be the (other) **jumps** of the filtration $(G^s)_{s \ge -1}$, i.e. the numbers $s \ge -1$ satisfying $G^{s+\varepsilon} \subsetneq G^s$ for all $\varepsilon > 0$. Obviously, all $\psi(t_i)$ are integers, and $t_0 = -1$ is a jump iff $[\mathbb{F}_{\mathfrak{q}} : \mathbb{F}_{\mathfrak{p}}] > 1$. The bijection η is piecewise linear, its slopes being

$$\eta'(s) = \frac{1}{(G^0 : G^{t_i})} = \frac{t_i - t_{i-1}}{\psi(t_i) - \psi(t_{i-1})}$$

for $\psi(t_{i-1}) < s < \psi(t_i)$ and $i \in \{1, \ldots, r\}$. By the Hasse-Arf Theorem (see [S1, p. 93][2]), the t_i are integers, too; in particular, $t_r = f(L,\mathfrak{p}) - 1$. Substituting the above equation into Hilbert's (lower index) Different Formula (see [St2, p. 124] or [CF, p. 36]) yields

$$\begin{aligned} d(\mathfrak{q}|\mathfrak{p}) &= \sum_{n=0}^{\infty} (|G_n(\mathfrak{q}|\mathfrak{p})| - 1) = \sum_{i=1}^{r} \sum_{s=\psi(t_{i-1})+1}^{\psi(t_i)} \left(\left| G^{t_i} \right| - 1 \right) \\ &= \sum_{i=1}^{r} (\psi(t_i) - \psi(t_{i-1})) \frac{|G^0| - (G^0 : G^{t_i})}{(G^0 : G^{t_i})} \\ &= \sum_{i=1}^{r} (t_i - t_{i-1}) \left(\left| G^0 \right| - (G^0 : G^{t_i}) \right) \\ &= \sum_{i=1}^{r} \sum_{n=t_{i-1}+1}^{t_i} \left(\left| G^0 \right| - (G^0 : G^n) \right) = \sum_{n=0}^{\infty} \left(\left| G^0 \right| - (G^0 : G^n) \right). \quad \square \end{aligned}$$

[2] We prefer Serre's direct proof to one deduced from local class field theory (see [Nk, p. 372] or [CF, p. 157]), which is merely touched upon in our next section.

As an immediate consequence we obtain the following

3.7. Discriminant Formula. *Let* $\mathfrak{f}(L|K) \leq \mathfrak{m} = \sum_{\mathfrak{p}} m_{\mathfrak{p}}\mathfrak{p} \in \mathcal{D}_K$. *Then the discriminant of* $L|K$ *is given by*

$$\mathfrak{d}(L|K) = [L:K]\mathfrak{m} - \sum_{\mathfrak{p}\in\mathbb{P}_K} \Big(\sum_{n=0}^{m_{\mathfrak{p}}-1} [L^n(\mathfrak{p}) : K] \Big)\mathfrak{p}.$$

Proof. Since $L^0(\mathfrak{p})$ is the inertia field of $\mathfrak{p}$ in L, we have $\sum_{\mathfrak{q}|\mathfrak{p}}[\mathbb{F}_{\mathfrak{q}} : \mathbb{F}_{\mathfrak{p}}] = [L^0(\mathfrak{p}) : K]$ for each $\mathfrak{p} \in \mathbb{P}_K$. The discriminant is the norm of the different. Hence $\mathfrak{d}(L|K) = \sum_{\mathfrak{p}} d(L,\mathfrak{p})\mathfrak{p}$ with

$$\begin{aligned} d(L,\mathfrak{p}) &= \sum_{\mathfrak{q}|\mathfrak{p}} [\mathbb{F}_{\mathfrak{q}} : \mathbb{F}_{\mathfrak{p}}] d(\mathfrak{q}|\mathfrak{p}) \\ &= [L^0(\mathfrak{p}) : K] \sum_{n=0}^{m_{\mathfrak{p}}-1} \big([L : L^0(\mathfrak{p})] - [L^n(\mathfrak{p}) : L^0(\mathfrak{p})] \big) \\ &= [L:K]m_{\mathfrak{p}} - \sum_{n=0}^{m_{\mathfrak{p}}-1} [L^n(\mathfrak{p}) : K]. \quad \square \end{aligned}$$

Part II
Ray Class Fields

This part is devoted entirely to the definition and investigation of the central objects of this thesis, the ray class fields $K_S^{\mathfrak{m}}$, where S is a non-empty set of places and $\mathfrak{m}$ an effective divisor of K with support away from S. Their existence is based on (global) class field theory, of which we shall give a brief survey in Section 4.

The extension $K_S^{\mathfrak{m}}|K$ will be characterized as the *largest* abelian extension of K with conductor $\leq \mathfrak{m}$ such that every place in S splits completely. This and other properties of the ray class fields are discussed in Section 5. Here we also see that everything comes down to knowing the degrees $[K_S^{\mathfrak{m}} : K]$, the determination of which is therefore attacked in Section 6.

In the whole of Part II we assume again that $K|\mathbb{F}_q$ is a global function field. Moreover, we fix an algebraic closure $\bar{K}$ of K, inside which all algebraic extensions of K are chosen.

4 Class Field Theory

The purpose of this section is to make available the necessary tools from class field theory. A complete exposition of this theory, as presented in [CF] and [AT], would be beyond the scope of this thesis. Nevertheless, we want to give an impression of how the results depend on each other and how the proofs are arranged. A general introduction to topological groups, which play a central role here, is found e.g. in [Lu].

We recall from Section 1 that for each place $\mathfrak{p}$ of K the multiplicative group $K_{\mathfrak{p}}^*$ is a topological group, in which the subgroups $U_{\mathfrak{p}}^{(n)}$ with $n \in \mathbb{N}_0$ form a basis of open neighbourhoods of 1. The **idèle group** $\mathcal{I}_K$ of K is defined as the restricted topological product of the $K_{\mathfrak{p}}^*$, $\mathfrak{p} \in \mathbb{P}_K$, with respect to their subgroups $U_{\mathfrak{p}}$ (see [CF, p. 68]). In other words,

$$\mathcal{I}_K := \Big\{ (\alpha_{\mathfrak{p}})_{\mathfrak{p}\in\mathbb{P}_K} \in \prod_{\mathfrak{p}\in\mathbb{P}_K} K_{\mathfrak{p}}^* \,\Big|\, \alpha_{\mathfrak{p}} \in U_{\mathfrak{p}} \text{ for almost all } \mathfrak{p} \in \mathbb{P}_K \Big\},$$

and the topology on $\mathcal{I}_K$ is the initial topology induced by the canonical projections $\mathcal{I}_K \twoheadrightarrow K_{\mathfrak{p}}^*$, $\mathfrak{p} \in \mathbb{P}_K$. Therefore, a subset of $\mathcal{I}_K$ is open iff it is a union of sets of the form $\prod_{\mathfrak{p}\in\mathbb{P}_K} V_{\mathfrak{p}}$ with $V_{\mathfrak{p}} \subseteq K_{\mathfrak{p}}^*$ open for all $\mathfrak{p} \in \mathbb{P}_K$ and $V_{\mathfrak{p}} = U_{\mathfrak{p}}$ for almost all $\mathfrak{p} \in \mathbb{P}_K$. It is readily verified that $\mathcal{I}_K$ is a topological group.

The canonical embedding of $K_\mathfrak{p}^*$ into $\mathcal{I}_K$ will be expressed by the symbol $[\ ]_\mathfrak{p}$, i.e. $[z]_\mathfrak{p}$ for $z \in K_\mathfrak{p}^*$ is the idèle $(\dots, 1, z, 1, \dots)$ having z at its $\mathfrak{p}$-th position and 1 elsewhere. Clearly, the morphism $[\ ]_\mathfrak{p}$ preserves the topology, i.e. is a homeomorphism onto its image. The diagonal embedding of K^* into $\mathcal{I}_K$ is considered as inclusion. The factor group $\mathcal{C}_K = \mathcal{I}_K/K^*$ is called the **idèle class group** of K and carries the quotient topology induced from $\mathcal{I}_K$, i.e. the canonical projection $\mathcal{I}_K \twoheadrightarrow \mathcal{C}_K$ is continuous and open.

Let L be finite separable over K. The inclusion $K^* \subseteq L^*$ is extended to idèles by identifying $\alpha = (\alpha_\mathfrak{p})_{\mathfrak{p}\in\mathbb{P}_K} \in \mathcal{I}_K$ with $(\alpha_\mathfrak{q})_{\mathfrak{q}\in\mathbb{P}_L} \in \mathcal{I}_L$, where $\alpha_\mathfrak{q} = \alpha_\mathfrak{p}$ for $\mathfrak{q}|\mathfrak{p}$. Since $L^* \cap \mathcal{I}_K = K^*$, it induces an inclusion $\mathcal{C}_K \subseteq \mathcal{C}_L$. Both inclusions preserve the respective topologies. Also the norm $N_{L|K}$ from L^* to K^* is extended to idèles by the continuous morphism

$$N_{L|K}: \begin{array}{ccc} \mathcal{I}_L & \to & \mathcal{I}_K \\ (\beta_\mathfrak{q})_{\mathfrak{q}\in\mathbb{P}_L} & \mapsto & \left(\prod_{\mathfrak{q}|\mathfrak{p}} N_{L_\mathfrak{q}|K_\mathfrak{p}}\beta_\mathfrak{q}\right)_{\mathfrak{p}\in\mathbb{P}_K} \end{array}$$

(see [CF, p. 75]). Since $N_{L|K}L^* \subseteq K^*$, it induces a norm map $N_{L|K}: \mathcal{C}_L \to \mathcal{C}_K$, which is continuous, too. Finally, the norm is obviously transitive, i.e. if L' is an intermediate field of $L|K$, then $N_{L|K} = N_{L'|K} \circ N_{L|L'}$.

Until the end of this section we assume $L|K$ to be finite abelian. Consider $G(L|K)$ as a topological group equipped with the discrete topology. Class field theory asserts the existence of a canonical group morphism built up from the Frobenius automorphisms defined in Section 3.

4.1. Reciprocity Law. (a) *Let $S \subseteq \mathbb{P}_K$ be a finite set of places of K including all those which ramify in L. Then there is a unique continuous homomorphism*

$$(\ , L|K): \mathcal{I}_K \to G(L|K)$$

such that $(K^*, L|K) = 1$ and

$$(\alpha, L|K) = \prod_{\mathfrak{p}\in\mathbb{P}_K\setminus S} \varphi_{L,\mathfrak{p}}^{v_\mathfrak{p}(\alpha_\mathfrak{p})}$$

for each $\alpha = (\alpha_\mathfrak{p})_{\mathfrak{p}\in\mathbb{P}_K} \in \mathcal{I}_K$ satisfying $\alpha_\mathfrak{p} = 1$ for all $\mathfrak{p} \in S$.

(b) *The map $(\ , L|K)$ is surjective with kernel $K^*N_{L|K}\mathcal{I}_L$.*

(c) *If L' is an intermediate field of $L|K$, then $(\alpha, L'|K) = (\alpha, L|K)|_{L'}$ for all $\alpha \in \mathcal{I}_K$.*

The homomorphism $(\ , L|K)$ is called the **Artin map** or the **norm residue symbol** of $L|K$.

Remarks on the proof. We can follow [CF, pp. 170–193]; only for the part concerning Artin-Schreier extensions we refer to [AT, pp. 29–37].

The uniqueness of $(\ ,L|K)$ follows from the continuity by means of weak approximation and shows that the definition of the Artin map does not depend on the exceptional set S. Also, (c) can easily be derived from this uniqueness, noting that $\varphi_{L',\mathfrak{p}} = \varphi_{L,\mathfrak{p}}|_{L'}$. The behaviour of the Frobenius automorphism in towers, by applying weak approximation once more, implies that $N_{L|K}\mathcal{I}_L$ is contained in the kernel of $(\ ,L|K)$.

In order to prove (b) and the existence of the Artin map one usually employs Galois cohomology. In the beginning the so-called first inequality, stating that $[L : K]$ divides $(\mathcal{C}_K : N_{L|K}\mathcal{C}_L)$, is established for cyclic extensions $L|K$ by determining the Herbrand quotient of $\mathcal{C}_L$ as a $G(L|K)$-module. Assuming the existence of an Artin map, one can now derive that it must be onto for any finite *abelian* extension $L|K$.

The second inequality, $(\mathcal{C}_K : N_{L|K}\mathcal{C}_L)|[L : K]$, can be stated more generally for $L|K$ abelian, because it is easily reduced to the situation where $L|K$ is cyclic of prime degree n and K contains the n-th roots of unity. If $n = p$ is the characteristic, L is an Artin-Schreier extension of K and therefore contained in $\tilde{K} := K(\wp^{-1}K)$. Thinking of $G(\tilde{K}|K)$ as equipped with the Krull topology, one exhibits a homeomorphism[3] $\omega : \mathcal{C}_K/\mathcal{C}_K^p \simeq G(\tilde{K}|K)$ in terms of traces of residues of local differentials and shows, by the aid of the first inequality, that $\omega(N_{L|K}\mathcal{C}_L/\mathcal{C}_K^p) = G(\tilde{K}|L)$, whence $\mathcal{C}_K/N_{L|K}\mathcal{C}_L \simeq G(L|K)$. The case $n \neq p$ is somewhat more technical. This time $L|K$ is a Kummer extension, and the proof of the second inequality uses an intricate interplay between Kummer groups and idèle norms, too difficult to present here. Having shown the second inequality, one can immediately conclude that the Artin map (if it exists) must have the kernel $K^*N_{L|K}\mathcal{I}_L$.

In order to finally prove the existence of the Artin map, $(\ ,L|K)$ is defined as the product of all local Artin maps $(\ ,L_\mathfrak{p}|K_\mathfrak{p})$ with $\mathfrak{p} \in \mathbb{P}_K$, as indicated at the end of this section. By this definition $(\ ,L|K)$ is continuous and also the representation by Frobenius automorphisms as required in (a) verifies trivially. The crucial point is to show that $(\ ,L|K)$ indeed swallows K^*. This is easy for constant field extensions of K and generalizes via an assertion on the Brauer group of K to arbitrary finite abelian extensions. □

Since K^* is contained in its kernel, we can also think of the Artin map

[3] Although not needed for the proof, it should help understanding the Reciprocity Law to verify that $\omega(\ )|_L = (\ ,L|K)$ for all finite subextensions $L|K$ of $\tilde{K}|K$.

$(\ ,L|K)$ as defined on $\mathcal{C}_K$. As such it is continuous, too. Its kernel

$$\mathcal{N}_L := N_{L|K}\mathcal{C}_L = K^* N_{L|K}\mathcal{I}_L/K^*$$

is called the **norm group** of L, and L is called the **class field** associated to this norm group. We note that the Artin map induces an isomorphism

$$\mathcal{C}_K/\mathcal{N}_L \simeq G(L|K).$$

From the Reciprocity Law we can derive some consequences on inclusions of class fields and norm groups.

4.2. Corollary. *Let L_1, L_2 be finite abelian over K. Then*

(a) $L_1 \subseteq L_2 \iff \mathcal{N}_{L_1} \supseteq \mathcal{N}_{L_2}$.

(b) $\mathcal{N}_{L_1L_2} = \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2}$.

(c) $\mathcal{N}_{L_1\cap L_2} = \mathcal{N}_{L_1}\mathcal{N}_{L_2}$.

Proof. We can follow the arguments in [Nk, p. 321]. The implication $\Longrightarrow$ in (a) and the inclusions $\subseteq$ in (b) and $\supseteq$ in (c) follow from the transitivity of the norm. If in (b) conversely $\alpha K^* \in \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2}$ for $\alpha \in \mathcal{I}_K$ then $(\alpha, L_1L_2|K)|_{L_i} = (\alpha, L_i|K) = 1$ for $i \in \{1,2\}$ by 4.1(c), thus $\alpha K^* \in \mathcal{N}_{L_1L_2}$. Using (b) to prove the opposite implication in (a) we see that $\mathcal{N}_{L_1} \supseteq \mathcal{N}_{L_2}$ implies $\mathcal{N}_{L_1L_2} = \mathcal{N}_{L_2}$, thus $[L_1L_2 : K] = [L_2 : K]$ by the Reciprocity Law, whence $L_1 \subseteq L_2$.

It remains to show that $\mathcal{N}_{L_1\cap L_2} \subseteq \mathcal{N} := \mathcal{N}_{L_1}\mathcal{N}_{L_2}$. For $i \in \{1,2\}$, by Galois theory, $(\mathcal{N}, L_i|K) = G(L_i|L_i')$ for some intermediate field L_i' of $L_i|K$, and by the Reciprocity Law, $\mathcal{N}$ is the kernel of $(\ ,L_i'|K)$, i.e. equals $\mathcal{N}_{L_i'}$. Using (a) we conclude $L_1' = L_2' \subseteq L_1 \cap L_2$ and $\mathcal{N} \supseteq \mathcal{N}_{L_1\cap L_2}$. □

4.3. Existence Theorem. *The map $L \mapsto \mathcal{N}_L$ is a 1–1 correspondence between the finite abelian extensions of K (within $\bar{K}$) and the open subgroups of finite index in $\mathcal{C}_K$.*

Remarks on the proof. We follow [CF, pp. 201f]. Clearly the kernel $\mathcal{N}_L = N_{L|K}\mathcal{C}_L$ of the continuous map $(\ ,L|K) : \mathcal{C}_K \to G(L|K)$ is open and of finite index in $\mathcal{C}_K$. Moreover, $\mathcal{N}_L$ is uniquely determined by L according to 4.2(a). Let us call a subgroup $\mathcal{N}$ of $\mathcal{C}_K$ **normic** if it is the norm group $\mathcal{N}_L$ of some abelian extension $L|K$. We note that if $\mathcal{N}$ contains a normic subgroup $\mathcal{N}'$, say with class field L', then $\mathcal{N}$ is itself normic, for, by the Reciprocity Law, $(\mathcal{N}, L'|K)$ is a subgroup of $G(L'|K)$, whose fixed field $L \subseteq L'$ has norm group $\mathcal{N}_L = \mathcal{N}$.

It remains to show that any open subgroup $\mathcal{N}$ of finite index in $\mathcal{C}_K$ is normic. If the index $n = (\mathcal{C}_K : \mathcal{N})$ is a prime number and K contains the n-th roots of unity, this follows from the proof of the Reciprocity Law, or more precisely of the second inequality, where the class field (of a subgroup) of $\mathcal{N}$ was constructed. By a lemma on norm lifts in cyclic extensions one can reduce the general case to the former. □

To conclude this section, we point out the connection between global and local class field theory. Let $\mathfrak{p} \in \mathbb{P}_K$ and denote by $L_\mathfrak{p}$ the completion of L at any one of the places above $\mathfrak{p}$. (They are all $K_\mathfrak{p}$-isomorphic.) By [CF, p. 175], the composed morphism

$$([\ ]_\mathfrak{p}, L|K) : K_\mathfrak{p}^* \hookrightarrow \mathcal{I}_K \twoheadrightarrow G(L|K)$$

has image $G^{-1}(L, \mathfrak{p})$. In the course of the proof of the Reciprocity Law this morphism turned out to be equal to the local norm residue symbol $(\ , L_\mathfrak{p}|K_\mathfrak{p})$, whose definition is given in [CF, p. 140]. By [CF, p. 155] we obtain:

4.4. Theorem. *The homomorphism* $([\ ]_\mathfrak{p}, L|K) : K_\mathfrak{p}^* \to G^{-1}(L, \mathfrak{p})$ *is surjective and maps* $U_\mathfrak{p}^{(n)}$ *onto* $G^n(L, \mathfrak{p})$ *for all* $n \in \mathbb{N}_0$.

In particular, $([U_\mathfrak{p}]_\mathfrak{p}, L|K) = 1$ for all but the finitely many places $\mathfrak{p} \in \mathbb{P}_K$ which ramify in L. Hence for each $\alpha = (\alpha_\mathfrak{p}) \in \mathcal{I}_K$, by continuity,

$$(\alpha, L|K) = \prod_{\mathfrak{p} \in \mathbb{P}_K} ([\alpha_\mathfrak{p}]_\mathfrak{p}, L|K),$$

and the product is finite.

5 Definition and Properties

Pursuing the program we announced in the beginning of this part, our next task is to find a suitable open subgroup of finite index in $\mathcal{C}_K$ such that its class field has the desired properties. Reflecting on Theorem 4.4 encourages us to give the following definitions.

Let S be a set of places of K. By an **S-cycle** we mean an effective divisor of K with support disjoint from S. Let $\mathfrak{m} = \sum_\mathfrak{p} m_\mathfrak{p}\mathfrak{p}$ be such an S-cycle. Then we define the **S-congruence subgroups mod $\mathfrak{m}$**,

$$\mathcal{I}_S^\mathfrak{m} := \left(\prod_{\mathfrak{p} \in S} K_\mathfrak{p}^* \times \prod_{\mathfrak{p} \in \mathbb{P}_K \setminus S} U_\mathfrak{p}^{(m_\mathfrak{p})} \right) \cap \mathcal{I}_K \quad \text{and} \quad \mathcal{C}_S^\mathfrak{m} := K^* \mathcal{I}_S^\mathfrak{m} / K^*,$$

of $\mathcal{I}_K$ and $\mathcal{C}_K$, respectively. (Here intersection with $\mathcal{I}_K$ is only necessary, of course, when S is infinite.) For an arbitrary effective divisor $\mathfrak{n} = \sum_\mathfrak{p} n_\mathfrak{p}\mathfrak{p}$ of K we set $\mathcal{I}^\mathfrak{n} := \mathcal{I}^\mathfrak{n}_{\mathbb{P}_K \setminus \operatorname{supp}\mathfrak{n}}$ and define

$$\phi(\mathfrak{n}) := \prod_{\mathfrak{p}\in\mathbb{P}_K} (U_\mathfrak{p} : U_\mathfrak{p}^{(n_\mathfrak{p})}) = \prod_{\mathfrak{p}\in\operatorname{supp}\mathfrak{n}} (q^{\deg\mathfrak{p}} - 1)q^{(n_\mathfrak{p}-1)\deg\mathfrak{p}}.$$

We note some elementary properties of the congruence subgroups.

5.1. Remark. *Let $S \subseteq \mathbb{P}_K$ and $\mathfrak{m} = \sum_\mathfrak{p} m_\mathfrak{p}\mathfrak{p}$ be an S-cycle.*

(a) *If $T \subseteq S$ and $\mathfrak{n} \geq \mathfrak{m}$ is a T-cycle, then $\mathcal{I}^\mathfrak{n}_T \subseteq \mathcal{I}^\mathfrak{m}_S$ and $\mathcal{C}^\mathfrak{n}_T \subseteq \mathcal{C}^\mathfrak{m}_S$.*

(b) *If $T \subseteq \mathbb{P}_K$ and $\mathfrak{n}$ is a T-cycle, then $\mathcal{I}^\mathfrak{m}_S\mathcal{I}^\mathfrak{n}_T = \mathcal{I}^{\min\{\mathfrak{m},\mathfrak{n}\}}_{S\cup T}$, where the minimum is taken coefficientwise.*

(c) *The congruence subgroups $\mathcal{I}^\mathfrak{n}_\emptyset$ and $\mathcal{C}^\mathfrak{n}_\emptyset$ with $\mathfrak{n}$ running through all effective divisors of K form a basis of open neighbourhoods of 1 in $\mathcal{I}_K$ and $\mathcal{C}_K$, respectively.*

(d) *Both $\mathcal{I}^\mathfrak{m}_S$ and $\mathcal{C}^\mathfrak{m}_S$ are open.*

(e) *We have $\mathcal{I}^\mathfrak{o}_S/\mathcal{I}^\mathfrak{m}_S \simeq \prod_\mathfrak{p} U_\mathfrak{p}/U_\mathfrak{p}^{(m_\mathfrak{p})}$ and $(\mathcal{I}^\mathfrak{o}_S : \mathcal{I}^\mathfrak{m}_S) = \phi(\mathfrak{m})$.*

(f) *The index $(\mathcal{C}_K : \mathcal{C}^\mathfrak{n}_\emptyset)$ is infinite for every effective divisor $\mathfrak{n}$ of K.*

(g) *$K^*\mathcal{I}^\mathfrak{n} = \mathcal{I}_K$ for any $\mathfrak{n} \geq \mathfrak{o}$.*

(h) *$\mathcal{I}^\mathfrak{m}_S$ is topologically generated by its subgroups $[K^*_\mathfrak{p}]_\mathfrak{p}$, $\mathfrak{p} \in S$, and $[U_\mathfrak{p}^{(m_\mathfrak{p})}]_\mathfrak{p}$, $\mathfrak{p} \in \mathbb{P}_K \setminus S$.*

Proof. **(a)**–**(e)** are obvious.

(f) Choosing a place $\mathfrak{p} \in \mathbb{P}_K \setminus \operatorname{supp}\mathfrak{n}$, the homomorphism $K^*_\mathfrak{p} \to \mathcal{I}_K/K^*\mathcal{I}^\mathfrak{n}_\emptyset$ induced by the embedding $[\ ]_\mathfrak{p}$ has kernel $U_\mathfrak{p}$. But $K^*_\mathfrak{p}/U_\mathfrak{p} \simeq \mathbb{Z}$.

(g) This is merely an idèlic reformulaton of the Weak Approximation Theorem 1.5.

(h) Let $\alpha = (\alpha_\mathfrak{p})_{\mathfrak{p}\in\mathbb{P}_K} \in \mathcal{I}^\mathfrak{m}_S$ and $\mathfrak{n} = \sum_\mathfrak{p} n_\mathfrak{p}\mathfrak{p}$ be an effective divisor of K. Then the set $T := \{\mathfrak{p} \in \mathbb{P}_K \mid \alpha_\mathfrak{p} \notin U_\mathfrak{p}^{(n_\mathfrak{p})}\}$ is finite and $\alpha \equiv \prod_{\mathfrak{p}\in T}[\alpha_\mathfrak{p}]_\mathfrak{p} \mod \mathcal{I}^\mathfrak{n}_\emptyset$. Thus the assertion follows by (b). □

Because of 5.1(f) we require S to be *non-empty* from now on. In a moment we shall see that under this assumption the index of $\mathcal{C}^\mathfrak{m}_S$ in $\mathcal{C}_K$ is indeed finite. In order to obtain an ideal theoretic interpretation of the corresponding factor group, we introduce the **S-class group mod $\mathfrak{m}$**, $\mathcal{C}\ell^\mathfrak{m}(\mathcal{O}_S)$, defined as the

quotient of the group of fractional ideals of $\mathcal{O}_S$ prime to $\mathfrak{m}$ by its subgroup of principal ideals $z\mathcal{O}_S$ with $z \in K^* \cap \mathcal{I}^{\mathfrak{m}}$. Note that $\mathcal{C}\ell^{\mathfrak{o}}(\mathcal{O}_S) = \mathcal{C}\ell(\mathcal{O}_S)$ is the usual S-class group defined in Section 2.

5.2. Proposition. *Let $S \subseteq \mathbb{P}_K$ be non-empty and $\mathfrak{m}$ an S-cycle.*

(a) *$\mathcal{C}\ell^{\mathfrak{m}}(\mathcal{O}_S)$ is naturally isomorphic to $\mathcal{C}_K/\mathcal{C}_S^{\mathfrak{m}}$.*

(b) *The sequence*

$$\mathcal{O}_S^* \to \mathcal{I}_S^{\mathfrak{o}}/\mathcal{I}_S^{\mathfrak{m}} \to \mathcal{I}_K/K^*\mathcal{I}_S^{\mathfrak{m}} \to \mathcal{I}_K/K^*\mathcal{I}_S^{\mathfrak{o}} \to 1$$

is exact.

(c) *$(\mathcal{C}_K : \mathcal{C}_S^{\mathfrak{m}})$ is finite.*

Proof. **(a)** The natural homomorphism $\mathcal{I}^{\mathfrak{m}} \to \mathcal{C}\ell^{\mathfrak{m}}(\mathcal{O}_S)$ mapping the idèle $(\alpha_{\mathfrak{p}})_{\mathfrak{p}\in\mathbb{P}_K} \in \mathcal{I}^{\mathfrak{m}}$ to the class of the fractional $\mathcal{O}_S$-ideal $\prod_{\mathfrak{p}\in\mathbb{P}_K\setminus S}(\mathfrak{p}\cap\mathcal{O}_S)^{v_{\mathfrak{p}}(\alpha_{\mathfrak{p}})}$ is onto with kernel $\mathcal{I}_S^{\mathfrak{m}}(K^* \cap \mathcal{I}^{\mathfrak{m}}) = K^*\mathcal{I}_S^{\mathfrak{m}} \cap \mathcal{I}^{\mathfrak{m}}$. Consequently, $\mathcal{C}\ell^{\mathfrak{m}}(\mathcal{O}_S) \simeq K^*\mathcal{I}^{\mathfrak{m}}/K^*\mathcal{I}_S^{\mathfrak{m}} = \mathcal{I}_K/K^*\mathcal{I}_S^{\mathfrak{m}}$ by 5.1(g).

(b) We have $\mathcal{O}_S^* = K^* \cap \mathcal{I}_S^{\mathfrak{o}}$, implying $\mathcal{O}_S^*\mathcal{I}_S^{\mathfrak{m}}/\mathcal{I}_S^{\mathfrak{m}} = (K^*\mathcal{I}_S^{\mathfrak{m}} \cap \mathcal{I}_S^{\mathfrak{o}})/\mathcal{I}_S^{\mathfrak{m}}$, which is the exactness at $\mathcal{I}_S^{\mathfrak{o}}/\mathcal{I}_S^{\mathfrak{m}}$. The exactness at the other groups is even simpler.

(c) This follows from (b) since both $\mathcal{I}_S^{\mathfrak{o}}/\mathcal{I}_S^{\mathfrak{m}}$ and $\mathcal{I}_K/K^*\mathcal{I}_S^{\mathfrak{o}} \simeq \mathcal{C}\ell(\mathcal{O}_S)$ are finite. □

According to the Existence Theorem 4.3, we can now define $K_S^{\mathfrak{m}}$ as the class field associated to the congruence subgroup $\mathcal{C}_S^{\mathfrak{m}}$ and call it the **S-ray class field mod $\mathfrak{m}$**. By 4.1(b) we have an isomorphism

$$G(K_S^{\mathfrak{m}}|K) \simeq \mathcal{I}_K/K^*\mathcal{I}_S^{\mathfrak{m}} \simeq \mathcal{C}_K/\mathcal{C}_S^{\mathfrak{m}} \simeq \mathcal{C}\ell^{\mathfrak{m}}(\mathcal{O}_S).$$

We remark that $K_S^{\mathfrak{o}}$ is the **Hilbert class field** of $\mathcal{O}_S$ in the sense of Rosen [Ro2] (with the slight generalization that we allow S to be infinite). Moreover, in case S consists of exactly one place, an explicit construction of $K_S^{\mathfrak{m}}$ in terms of rank 1 Drinfel'd modules has been carried out by Hayes [Hay]. This special case is treated in an example at the end of this section.

As a consequence of our remark about the congruence subgroups we obtain the following

5.3. Corollary. *Let S and T be non-empty subsets of $\mathbb{P}_K$, $\mathfrak{m}$ an S-cycle and $\mathfrak{n}$ a T-cycle.*

(a) *If $S \supseteq T$ and $\mathfrak{m} \le \mathfrak{n}$, then $K_S^{\mathfrak{m}} \subseteq K_T^{\mathfrak{n}}$.*

(b) *$K_S^{\mathfrak{m}} \cap K_T^{\mathfrak{n}} = K_{S\cup T}^{\min\{\mathfrak{m},\mathfrak{n}\}}$.*

(c) *If $S \supseteq T$, $\mathfrak{m} \leq \mathfrak{n}$ and $\mathfrak{n}$ is also an S-cycle, then $[K_S^{\mathfrak{n}} : K_S^{\mathfrak{m}}] \leq [K_T^{\mathfrak{n}} : K_T^{\mathfrak{m}}]$.*

Proof. **(a)** This is clear from 5.1(a) and 4.2(a).

(b) By 5.1(b) we have $\mathcal{C}_S^{\mathfrak{m}}\mathcal{C}_T^{\mathfrak{n}} = \mathcal{C}_{S\cup T}^{\min\{\mathfrak{m},\mathfrak{n}\}}$, so that the assertion follows from 4.2(c) and the definition of the ray class fields.

(c) By 4.1(c), the norm residue symbol $(\ ,K_S^{\mathfrak{n}}|K)$ induces an isomorphism $K^*\mathcal{I}_S^{\mathfrak{m}}/K^*\mathcal{I}_S^{\mathfrak{n}} \simeq G(K_S^{\mathfrak{n}}|K_S^{\mathfrak{m}})$, and likewise for T instead of S. Because of 5.1(b), the natural map $K^*\mathcal{I}_T^{\mathfrak{m}}/K^*\mathcal{I}_T^{\mathfrak{n}} \to K^*\mathcal{I}_S^{\mathfrak{m}}/K^*\mathcal{I}_S^{\mathfrak{n}}$ is onto. □

Next we want to investigate some extremality properties of the ray class fields.

5.4. Conductor Lemma. *Let $L|K$ be finite abelian and let S be any non-empty subset of $S(L|K)$. Then $\mathfrak{f}(L|K)$ is the smallest S-cycle $\mathfrak{m}$ such that L is contained in $K_S^{\mathfrak{m}}$.*

Proof. Let $\mathfrak{m} = \sum_{\mathfrak{p}} m_{\mathfrak{p}}\mathfrak{p}$ be an S-cycle. By the definition of the conductor exponent and Theorems 4.4 and 4.1(b), for each $\mathfrak{p} \in \mathbb{P}_K$ we have the equivalence

$$f(L,\mathfrak{p}) \leq m_{\mathfrak{p}} \iff G^{m_{\mathfrak{p}}}(L,\mathfrak{p}) = 1 \iff [U_{\mathfrak{p}}^{(m_{\mathfrak{p}})}]_{\mathfrak{p}} \subseteq K^*N_{L|K}\mathcal{I}_L,$$

and moreover $\mathfrak{p} \in S$ implies $G^{-1}(L,\mathfrak{p}) = 1$, i.e. $[K_{\mathfrak{p}}^*]_{\mathfrak{p}} \subseteq K^*N_{L|K}\mathcal{I}_L$. Since $K^*N_{L|K}\mathcal{I}_L$ is open, hence closed, by 5.1(h) and 4.2(a) the above facts can be summarized as

$$\mathfrak{f}(L|K) \leq \mathfrak{m} \iff \mathcal{I}_S^{\mathfrak{m}} \subseteq K^*N_{L|K}\mathcal{I}_L \iff \mathcal{C}_S^{\mathfrak{m}} \subseteq \mathcal{N}_L \iff L \subseteq K_S^{\mathfrak{m}},$$

which is what we had to show. □

We deduce the following characterization of the ray class fields.

5.5. Proposition. *Let S be a non-empty set of places of K and $\mathfrak{m}$ an S-cycle. Then $K_S^{\mathfrak{m}}$ is the largest abelian extension L of K such that $S \subseteq S(L|K)$ and $\mathfrak{f}(L|K) \leq \mathfrak{m}$. Moreover, $\mathbb{F}_{q^d}$ with $d := \deg S$ is the full constant field of $K_S^{\mathfrak{m}}$.*

Proof. Let $L|K$ be finite abelian. By the lemma, $S \subseteq S(L|K)$ and $\mathfrak{f}(L|K) \leq \mathfrak{m}$ imply $L \subseteq K_S^{\mathfrak{m}}$. Conversely, let $L \subseteq K_S^{\mathfrak{m}}$. Then $\mathfrak{f}(L|K) \leq \mathfrak{m}$ is also clear from the Conductor Lemma, and it remains to show that $S \subseteq S(L|K)$. Indeed, $\mathfrak{p} \in S$ implies $[K_{\mathfrak{p}}^*]_{\mathfrak{p}} \subseteq \mathcal{I}_S^{\mathfrak{m}} \subseteq K^*N_{L|K}\mathcal{I}_L$ by 4.2(a); hence, from Theorem 4.4 it follows that $G^{-1}(L,\mathfrak{p}) = ([K_{\mathfrak{p}}^*]_{\mathfrak{p}}, L|K) = 1$, i.e. $\mathfrak{p} \in S(L|K)$.

As for the second assertion, recall that the constant field extension $K_d = \mathbb{F}_{q^d}K$ of degree d over K is unramified and $S \subseteq S(K_d|K)$. This implies $\mathbb{F}_{q^d} \subseteq K_d \subseteq K_S^{\mathfrak{o}} \subseteq K_S^{\mathfrak{m}}$. On the other hand, in order that $\mathbb{F}_{q^{d'}}$ for some $d' \in \mathbb{N}$ be contained in $K_S^{\mathfrak{m}}$, d' must divide the degree of every place in $S(K_S^{\mathfrak{m}}|K) \supseteq S$, so that $d'|d$. □

Recall that a rational function field has trivial divisor class group. So by 2.1 we obtain the following

5.6. Corollary. *Let $K = \mathbb{F}_q(x)$ be a rational function field and $S \subseteq \mathbb{P}_K$ non-empty. Then $h_S = \deg S =: d$ and the Hilbert class field $K_S^{\mathfrak{o}} = \mathbb{F}_{q^d}K = \mathbb{F}_{q^d}(x)$ is again a rational function field.*

If we choose S large enough, it may happen that the S-ray class field does not even depend on the modulus $\mathfrak{m}$, as we see in our next

5.7. Corollary. *With notation as in Corollary 3.5, we have $K_{S_d}^{\mathfrak{m}} = K_d$ and $\mathcal{C}\ell^{\mathfrak{m}}(\mathcal{O}_{S_d}) \simeq \mathbb{Z}/d\mathbb{Z}$ for any S_d-cycle $\mathfrak{m}$; in particular, $h_{S_d} = d$.*

Proof. The equality $K_{S_d}^{\mathfrak{m}} = K_d$ follows from 3.5 and the previous proposition. We conclude that $\mathcal{C}\ell^{\mathfrak{m}}(\mathcal{O}_{S_d}) \simeq G(K_{S_d}^{\mathfrak{m}}|K) = G(K_d|K) \simeq \mathbb{Z}/d\mathbb{Z}$. □

Given a place $\mathfrak{p}$ and an effective divisor $\mathfrak{m}$ of K whose $\mathfrak{p}$-th coefficient is $m_\mathfrak{p}$, we set $\mathfrak{m} \setminus \mathfrak{p} := \mathfrak{m} - m_\mathfrak{p}\mathfrak{p}$. With this notation, we can write down the remarkable fact that the ramification fields of the S-ray class field mod $\mathfrak{m}$ are the S-ray class fields mod $\mathfrak{m}'$ for certain $\mathfrak{m}' \leq \mathfrak{m}$.

5.8. Theorem. *Let S be a non-empty set of places of K, $\mathfrak{m}$ an S-cycle and L an intermediate field of $K_S^{\mathfrak{m}}|K$. For any place $\mathfrak{p}$ of K and any $n \in \mathbb{N}_0$ we have*

$$L^n(\mathfrak{p}) = L \cap K_S^{\mathfrak{m}\setminus\mathfrak{p}+n\mathfrak{p}} \quad \text{and} \quad L^{-1}(\mathfrak{p}) = L \cap K_{\{\mathfrak{p}\}}^{\mathfrak{m}\setminus\mathfrak{p}} = L \cap K_{S\cup\{\mathfrak{p}\}}^{\mathfrak{m}\setminus\mathfrak{p}}.$$

In particular, writing $\mathfrak{m} = \sum_\mathfrak{p} m_\mathfrak{p}\mathfrak{p}$, the discriminant of $K_S^{\mathfrak{m}}|K$ is

$$\mathfrak{d}(K_S^{\mathfrak{m}}|K) = [K_S^{\mathfrak{m}} : K]\mathfrak{m} - \sum_\mathfrak{p}\Bigg(\sum_{n=0}^{m_\mathfrak{p}-1}[K_S^{\mathfrak{m}\setminus\mathfrak{p}+n\mathfrak{p}} : K]\Bigg)\mathfrak{p}.$$

Proof. Consider an arbitrary intermediate field L' of $L|K$. By Propositions 3.1 and 5.5 we obtain the following equivalence of conditions on L':

$$\begin{aligned} L' \subseteq L^n(\mathfrak{p}) &\iff G(L|L') \supseteq G^n(L,\mathfrak{p}) \iff G^n(L',\mathfrak{p}) = 1 \iff \\ n \geq f(L',\mathfrak{p}) &\iff \mathfrak{m}\setminus\mathfrak{p} + n\mathfrak{p} \geq \mathfrak{f}(L'|K) \iff L' \subseteq K_S^{\mathfrak{m}\setminus\mathfrak{p}+n\mathfrak{p}}. \end{aligned}$$

Similarly,

$$\begin{aligned} L' \subseteq L^{-1}(\mathfrak{p}) &\iff G^{-1}(L',\mathfrak{p}) = 1 \iff \mathfrak{p} \in S(L'|K) \\ &\iff L' \subseteq K_{\{\mathfrak{p}\}}^{\mathfrak{m}\setminus\mathfrak{p}} \iff L' \subseteq K_{S\cup\{\mathfrak{p}\}}^{\mathfrak{m}\setminus\mathfrak{p}}. \end{aligned}$$

The last identity follows from the Discriminant Formula 3.7 since $\mathfrak{f}(K_S^{\mathfrak{m}}|K) \leq \mathfrak{m}$. □

Together with the Disriminant Formula 3.7, Proposition 5.5 and the Hurwitz Genus Formula 1.4, we deduce the following

5.9. Corollary. *Let $S \subseteq \mathbb{P}_K$ be non-empty, $\mathfrak{p} \in \mathbb{P}_K \setminus S$ and L an intermediate field of $K_S^{m\mathfrak{p}}|K_S^{(m-1)\mathfrak{p}}$ for some $m \in \mathbb{N}$. Then the genera of K and L are related as*

$$(g_L - 1)\deg S = [L:K]\big(g_K - 1 + \tfrac{m}{2}\deg\mathfrak{p}\big) - \frac{1}{2}\sum_{n=0}^{m-1}[K_S^{n\mathfrak{p}} : K]\deg\mathfrak{p}.$$

Thus computation of the discriminant (and thereby of the genus) of ray class field extensions amounts to determining their degrees. This has already been seen by Cohen et al. [CDO] in the number field case. As an illustration we give the following

5.10. Example (Ray Class Fields à la Hayes). *Assume that S consists of exactly one place of degree $d \in \mathbb{N}$. Let $\mathfrak{m}$ be an S-cycle, $h = h_K$ the (divisor) class number and $g = g_K$ the genus of K. Then*

(a) *$[K_S^{\mathfrak{o}} : K] = hd$ and $[K_S^{\mathfrak{m}} : K] = \frac{hd\phi(\mathfrak{m})}{q-1}$ for $\mathfrak{m} \neq \mathfrak{o}$.*

(b) *The genera of the S-ray class fields are given by*

$$g_{K_S^{\mathfrak{m}}} = \begin{cases} 1 + h(g-1) & \text{if } \deg\mathfrak{m} \leq 1, \\ 1 + \frac{hq^{(m-1)n}(q^n-1)(g-1)}{q-1} + \frac{hn}{2}\frac{mq^{mn}-(m+1)q^{(m-1)n}-q+2}{q-1} & \\ \qquad \text{if } \mathfrak{m} = m\mathfrak{p} \text{ with } \mathfrak{p} \in \mathbb{P}_K^n \text{ and } m,n \in \mathbb{N}, & \\ 1 + \frac{h}{2}\frac{\phi(\mathfrak{m})}{q-1}\Big(2g - 2 + \deg\mathfrak{m} - \sum_{\mathfrak{p}\in\operatorname{supp}\mathfrak{m}}\frac{\deg\mathfrak{p}}{\phi(\mathfrak{p})}\Big) & \text{if } |\operatorname{supp}\mathfrak{m}| > 1. \end{cases}$$

Note that the genus of $K_S^{\mathfrak{m}}$ does not depend on d but on g, h and $\mathfrak{m}$ only.

Proof. **(a)** By Proposition 2.1, $|S| = 1$ implies $h_S = hd$ and $\mathcal{O}_S^* = \mathbb{F}_q^*$, which is mapped injectively into $\mathcal{I}_S^{\mathfrak{o}}/\mathcal{I}_S^{\mathfrak{m}}$ when $\mathfrak{m} \neq \mathfrak{o}$. Hence the degree formulas follow from Proposition 5.2 and 5.1(e).

(b) Note that $K_S^{\mathfrak{m}}$ has the full constant field $\mathbb{F}_{q^d}$ according to Proposition 5.5. For $\mathfrak{m} \in \mathbb{P}_K^1$ we have $\phi(\mathfrak{m}) = q - 1$, hence $K_S^{\mathfrak{m}} = K_S^{\mathfrak{o}}$ by (a). Since $K_S^{\mathfrak{o}}|K$ is unramified, its discriminant is $\mathfrak{o}$. Hence the assertion in case $\deg\mathfrak{m} \leq 1$ follows from the Hurwitz Genus Formula 1.4.

For the other two cases, write $\mathfrak{m} = \sum_{\mathfrak{p}} m_{\mathfrak{p}}\mathfrak{p}$ and let $\mathfrak{p} \in \operatorname{supp}\mathfrak{m}$. Then

$$\begin{aligned}\sum_{n=1}^{m_{\mathfrak{p}}-1} [K_S^{\mathfrak{m}\setminus\mathfrak{p}+n\mathfrak{p}} : K] &= \frac{hd}{q-1}\sum_{n=1}^{m_{\mathfrak{p}}-1} \phi(\mathfrak{m}) q^{(1-m_{\mathfrak{p}})\deg\mathfrak{p}} q^{(n-1)\deg\mathfrak{p}} \\ &= \frac{hd}{q-1}\frac{\phi(\mathfrak{m})}{\phi(\mathfrak{p})}(1-q^{(1-m_{\mathfrak{p}})\deg\mathfrak{p}}).\end{aligned}$$

If $\mathfrak{m} = m\mathfrak{p}$ with $\mathfrak{p} \in \mathbb{P}_K^n$ and $m, n \in \mathbb{N}$, then $\mathfrak{m} \setminus \mathfrak{p} = \mathfrak{o}$, so (a) and the discriminant formula in Theorem 5.8 yield

$$\begin{aligned}\mathfrak{d}(K_S^{\mathfrak{m}}|K) &= \frac{hd\phi(m\mathfrak{p})}{q-1} m\mathfrak{p} - \Big(hd + \frac{hd}{q-1}\frac{\phi(m\mathfrak{p})}{\phi(\mathfrak{p})}\big(1-q^{(1-m)n}\big)\Big)\mathfrak{p} \\ &= \frac{hd}{q-1}\big(mq^{(m-1)n}(q^n-1) - q + 1 - q^{(m-1)n} + 1\big)\mathfrak{p}.\end{aligned}$$

If $\mathfrak{p}$ is not the only place in $\operatorname{supp}\mathfrak{m}$, then $[K_S^{\mathfrak{m}\setminus\mathfrak{p}} : K] = \frac{hd}{q-1}\frac{\phi(\mathfrak{m})}{\phi(\mathfrak{p})} q^{(1-m_{\mathfrak{p}})\deg\mathfrak{p}}$, whence

$$\mathfrak{d}(K_S^{\mathfrak{m}}|K) = \frac{hd\phi(\mathfrak{m})}{q-1}\mathfrak{m} - \sum_{\mathfrak{p}\in\operatorname{supp}\mathfrak{m}} \frac{hd}{q-1}\frac{\phi(\mathfrak{m})}{\phi(\mathfrak{p})}\mathfrak{p}.$$

In both cases the genus of $K_S^{\mathfrak{m}}$ turns out as asserted by applying the Hurwitz Genus Formula 1.4. □

As soon as S consists of more than one place, the determination of the degrees is much more difficult. We shall dedicate the next section to working out this problem.

6 Computation of Degrees

In view of the previous section (especially Theorem 5.8), our task is to determine the degrees $[K_S^{\mathfrak{m}} : K]$ for a fixed non-empty subset S of $\mathbb{P}_K$, which for practical reasons is now assumed to be *finite*, and for a varying S-cycle $\mathfrak{m}$. We divide the problem into three steps by considering two intermediate fields of $K_S^{\mathfrak{m}}|K$, namely the Hilbert class field $K_S^{\mathfrak{o}}$ and the field $K_S^{\tilde{\mathfrak{m}}}$ with

$$\tilde{\mathfrak{m}} := \sum_{\mathfrak{p}\in\operatorname{supp}\mathfrak{m}} \mathfrak{p}.$$

By Proposition 5.2(a) the extension $K_S^{\mathfrak{o}}|K$ has group $G(K_S^{\mathfrak{o}}|K) \simeq \mathcal{C}\ell(\mathcal{O}_S)$. Its order h_S can be determined via Corollary 2.2 after a computation of $\mathcal{O}_S^*$

and the divisor class number h_K of K. In the next section we shall learn about yet another method to determine (or at least estimate) h_S when S contains "many" rational places, which may also help us with the S-units.

As for the second step, $G(K_S^{\tilde{\mathfrak{m}}}|K_S^{\mathfrak{o}})$ is by 5.2(b) isomorphic to $\mathcal{I}_S^{\mathfrak{o}}/\mathcal{O}_S^*\mathcal{I}_S^{\tilde{\mathfrak{m}}}$. Therefore the degree $[K_S^{\tilde{\mathfrak{m}}} : K_S^{\mathfrak{o}}]$ divides $\phi(\tilde{\mathfrak{m}})/(q-1)$ (cf. also Example 5.10), and can be determined as follows (for technical reasons we exclude the trivial case of $\mathfrak{m} = \mathfrak{o}$). Let $s := |S| - 1 \in \mathbb{N}_0$, and suppose we have computed S-units $u_1, \ldots, u_s$ such that $\mathcal{O}_S^* = \langle \alpha, u_1, \ldots, u_s \rangle$, where α is a generator of $\mathbb{F}_q^*$. Write $R := \operatorname{supp} \mathfrak{m} = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ with $r = |R| \in \mathbb{N}$. For each $j \in \{1, \ldots, r\}$ we set $d_j := q^{\deg \mathfrak{p}_j} - 1$ and $c_j := d_j/(q-1)$ and choose a generator ω_j of $\mathbb{F}_{\mathfrak{p}_j}^*$ such that $\omega_j^{c_j} = \alpha$. Let $D = (d_{ij})_{1 \le i,j \le r} \in \mathbb{Z}^{r \times r}$ with

$$d_{ij} := \begin{cases} d_j & \text{for } 1 \le i = j < r, \\ c_j & \text{for } i = r, \\ 0 & \text{otherwise,} \end{cases}$$

be the matrix obtained from the diagonal matrix with entries $d_1, \ldots, d_r$ by replacing the last row with $(c_1, \ldots, c_r)$. Note that the sacrificed row $(0, \ldots, 0, d_r) \in \mathbb{Z}^r$ is a $\mathbb{Z}$-linear combination of the rows of D. Since $S \cap R = \emptyset$, there exists an $A = (a_{ij})_{\substack{1 \le i \le s \\ 1 \le j \le r}} \in \mathbb{Z}^{s \times r}$ such that $\omega_j^{a_{ij}} = u_i + \mathfrak{p}_j \in \mathbb{F}_{\mathfrak{p}_j}$ for all $i \in \{1, \ldots, s\}$ and $j \in \{1, \ldots, r\}$. The (non-canonical) surjective group morphism

$$\begin{aligned} \mathbb{Z}^r \to \mathcal{I}_S^{\mathfrak{o}}/\mathcal{I}_S^{\tilde{\mathfrak{m}}} &\simeq \prod_{j=1}^{r} \mathbb{F}_{\mathfrak{p}_j}^* \\ (a_1, \ldots, a_r) &\mapsto (\omega_j^{a_j})_{1 \le j \le r} \end{aligned}$$

gives rise to the exact sequence

$$0 \to N \to \mathbb{Z}^r \to \mathcal{I}_S^{\mathfrak{o}}/\mathcal{O}_S^*\mathcal{I}_S^{\tilde{\mathfrak{m}}} \to 1,$$

where N is the subgroup of $\mathbb{Z}^r$ generated by the rows of the matrix $\binom{A}{D} \in \mathbb{Z}^{(s+r)\times r}$ of rank r. After some row transformations $T = (t_{ij})_{1 \le i,j \le s+r} \in \mathrm{GL}_{s+r}(\mathbb{Z})$, we find a $B \in \mathbb{Z}^{r \times r}$ with $T\binom{A}{D} = \binom{0}{B}$. Because $G(K_S^{\tilde{\mathfrak{m}}}|K_S^{\mathfrak{o}}) \simeq \mathbb{Z}^r/N$, it now follows that

$$[K_S^{\tilde{\mathfrak{m}}} : K_S^{\mathfrak{o}}] = |\det B| .$$

At the same time we have found a basis for the group $K^* \cap \mathcal{I}_S^{\tilde{\mathfrak{m}}}$, which is needed in step three below.

6.1. Lemma. *With notation as above, the S-units*

$$\tilde{u}_i := \alpha^{t_{i,s+r}} \prod_{k=1}^{s} u_k^{t_{ik}}, \quad 1 \le i \le s,$$

form a basis of the free abelian group $K^* \cap \mathcal{I}_S^{\tilde{\mathfrak{m}}} = \mathcal{O}_S^* \cap \mathcal{I}_S^{\tilde{\mathfrak{m}}}$.

Proof. For $i \in \{1, \dots, s\}$ and $j \in \{1, \dots, r\}$ we have $\sum_{k=1}^{s} t_{ik} a_{kj} + t_{i,s+r} c_j \equiv 0 \bmod d_j$ by definition of T; hence,

$$\tilde{u}_i + \mathfrak{p}_j = \omega_j^{t_{i,s+r} c_j} \prod_{k=1}^{s} \omega_j^{t_{ik} a_{kj}} = 1.$$

This shows $\tilde{u}_1, \dots, \tilde{u}_s \in \mathcal{I}_S^{\tilde{\mathfrak{m}}}$.

Conversely, suppose $u = \alpha^{t_0} \prod_{k=1}^{s} u_k^{t_k} \in \mathcal{O}_S^*$ with $t_0, \dots, t_s \in \mathbb{Z}$ is contained in $\mathcal{I}_S^{\tilde{\mathfrak{m}}}$. Then there are $t_{s+1}, \dots, t_{s+r} \in \mathbb{Z}$ such that

$$t_0 c_j + \sum_{k=1}^{s} t_k a_{kj} + t_{s+j} d_j = 0 \quad \forall j \in \{1, \dots, r\}.$$

Thus $t := (t_1, \dots, t_{s+r-1}, t_0)$ satisfies $t \binom{A}{D} = 0$. Putting $\tilde{t} = (\tilde{t}_1, \dots, \tilde{t}_{s+r}) := tT^{-1}$, from

$$\tilde{t} \begin{pmatrix} 0 \\ B \end{pmatrix} = \tilde{t} T \begin{pmatrix} A \\ D \end{pmatrix} = t \begin{pmatrix} A \\ D \end{pmatrix} = 0$$

we can conclude $\tilde{t}_{s+1} = \cdots = \tilde{t}_{s+r} = 0$ since the rows of B are linearly independent. Therefore

$$\prod_{i=1}^{s} \tilde{u}_i^{\tilde{t}_i} = \prod_{i=1}^{s} \Big(\alpha^{\tilde{t}_i t_{i,s+r}} \prod_{k=1}^{s} u_k^{\tilde{t}_i t_{ik}} \Big) = \alpha^{t_0} \prod_{k=1}^{s} u_k^{t_k} = u.$$

It remains to show that $K^* \cap \mathcal{I}_S^{\tilde{\mathfrak{m}}} = \mathcal{O}_S^* \cap \mathcal{I}_S^{\tilde{\mathfrak{m}}}$ is free of rank s. The morphism $K^* \cap \mathcal{I}_S^{\tilde{\mathfrak{m}}} \to \mathcal{D}_K$, $u \mapsto (u)$ has kernel $\mathbb{F}_q^* \cap \mathcal{I}_S^{\tilde{\mathfrak{m}}} = 1$, since we have assumed $\tilde{\mathfrak{m}} \neq \mathfrak{o}$. Therefore, by 2.2, $K^* \cap \mathcal{I}_S^{\tilde{\mathfrak{m}}} \simeq (K^* \cap \mathcal{I}_S^{\tilde{\mathfrak{m}}}) \subseteq (\mathcal{O}_S^*)$ is free of rank $\le s$. On the other hand, for any common multiple d of $d_1, \dots, d_r$, we have ${\mathcal{O}_S^*}^d \subseteq \mathcal{I}_S^{\tilde{\mathfrak{m}}}$, from which it follows that $((\mathcal{O}_S^*) : (K^* \cap \mathcal{I}_S^{\tilde{\mathfrak{m}}})) \le ((\mathcal{O}_S^*) : d(\mathcal{O}_S^*)) = s^d < \infty$. □

The rest of this section is devoted to the treatment of step three, the extension $K_S^{\mathfrak{m}} | K_S^{\tilde{\mathfrak{m}}}$. The Reciprocity Law tells us that

$$G(K_S^{\mathfrak{m}} | K_S^{\tilde{\mathfrak{m}}}) \simeq K^* \mathcal{I}_S^{\tilde{\mathfrak{m}}} / K^* \mathcal{I}_S^{\mathfrak{m}} \simeq \mathcal{I}_S^{\tilde{\mathfrak{m}}} / (K^* \cap \mathcal{I}_S^{\tilde{\mathfrak{m}}}) \mathcal{I}_S^{\mathfrak{m}}. \tag{4}$$

Writing $\mathfrak{m} = \sum_{\mathfrak{p}} m_{\mathfrak{p}}\mathfrak{p}$, we see that $\mathcal{I}_S^{\tilde{\mathfrak{m}}}/\mathcal{I}_S^{\mathfrak{m}} \simeq \prod_{\mathfrak{p}\in\operatorname{supp}\mathfrak{m}} U_{\mathfrak{p}}^{(1)}/U_{\mathfrak{p}}^{(m_{\mathfrak{p}})}$ is a p-group. We need to know what the structure of the groups $U_{\mathfrak{p}}^{(1)}/U_{\mathfrak{p}}^{(n)}$ with $\mathfrak{p} \in \mathbb{P}_K$ and $n \in \mathbb{N}$ is. In order to answer this question it is useful to agree upon some notation. Recall that p is the characteristic of K. For any real $a > 0$, let

$$\lceil a \rceil_p := \min\{p^l \mid a \le p^l, l \in \mathbb{N}_0\}$$

be the least p-power integer $\ge a$. Moreover denote by $\mathbb{N}_p^* := \mathbb{N} \setminus p\mathbb{Z}$ the set of positive integers prime to p and by $n^* := n/p^{v_p(n)} \in \mathbb{N}_p^*$ the non-p-part of $n \in \mathbb{N}$. The following proposition could easily be derived from Hasse's One Unit Theorem in [H, p. 227]. For reasons of constructiveness, however, we write down a direct proof.

6.2. Proposition. *Let $\mathfrak{p}$ be a place of K, $\pi \in K_{\mathfrak{p}}$ a uniformizer at $\mathfrak{p}$, B an $\mathbb{F}_p$-basis of $\mathbb{F}_{\mathfrak{p}}$ and $n \in \mathbb{N}$.*

(a) *For each $j \in \mathbb{N}$ and $\beta \in \mathbb{F}_{\mathfrak{p}}^*$, the coset $(1+\beta\pi^j)U_{\mathfrak{p}}^{(n)} \in U_{\mathfrak{p}}^{(1)}/U_{\mathfrak{p}}^{(n)}$ has order $\lceil n/j \rceil_p$.*

(b) *There is a decomposition*

$$U_{\mathfrak{p}}^{(1)}/U_{\mathfrak{p}}^{(n)} = \prod_{\substack{j\in\mathbb{N}_p^* \\ \beta\in B}} \left\langle (1+\beta\pi^j)U_{\mathfrak{p}}^{(n)} \right\rangle$$

as a direct product of cyclic subgroups.

Proof. **(a)** For $l \in \mathbb{N}_0$, one has $(1+\beta\pi^j)^{p^l} = 1 + \beta^{p^l}\pi^{jp^l} \in U_{\mathfrak{p}}^{(n)}$ iff $p^l \ge n/j$.

(b) Let H be the subgroup of $U_{\mathfrak{p}}^{(1)}/U_{\mathfrak{p}}^{(n)}$ generated by all cosets $(1+\beta\pi^j)U_{\mathfrak{p}}^{(n)}$ with $j \in \mathbb{N}_p^*$ and $\beta \in B$. We prove that

$$U_{\mathfrak{p}}^{(m)}/U_{\mathfrak{p}}^{(n)} \subseteq H$$

for $m \in \{1, \dots, n\}$ by induction on $n-m$. For $m = n$ there is nothing to show. Let $1 \le m < n$ and $u \in U_{\mathfrak{p}}^{(m)}$. Set $l := v_p(m)$, then $u \equiv 1 + \omega^{p^l}\pi^m \mod U_{\mathfrak{p}}^{(m+1)}$ for some $\omega \in \mathbb{F}_{\mathfrak{p}}$. Writing $\omega = \sum_{\beta\in B} a_\beta\beta$ with $a_\beta \in \{0, \dots, p-1\}$, we see that

$$\prod_{\beta\in B}(1+\beta\pi^j)^{a_\beta} \equiv 1 + \omega\pi^j \mod U_{\mathfrak{p}}^{(j+1)}$$

with $j := m^* \in \mathbb{N}_p^*$; hence,

$$\prod_{\beta\in B}(1+\beta\pi^j)^{a_\beta p^l} \equiv (1+\omega\pi^j)^{p^l} \equiv u \mod U_{\mathfrak{p}}^{(m+1)}.$$

By the induction hypothesis, $U_{\mathfrak{p}}^{(m+1)}/U_{\mathfrak{p}}^{(n)} \subseteq H$, from which we may conclude $uU_{\mathfrak{p}}^{(n)} \in H$. So we have proved $U_{\mathfrak{p}}^{(1)}/U_{\mathfrak{p}}^{(n)} = H$. Since $(U_{\mathfrak{p}}^{(1)} : U_{\mathfrak{p}}^{(n)}) = q^{(n-1)\deg \mathfrak{p}}$, the directness of the product follows from (a) and part (b) of the next lemma. □

6.3. Lemma. *The positive integers* $\left\lceil \frac{m}{j} \right\rceil_p$ *with* $m, j \in \mathbb{N}$ *satisfy the following properties.*

(a) $\left\lceil \frac{m+1}{j} \right\rceil_p \Big/ \left\lceil \frac{m}{j} \right\rceil_p = \begin{cases} p & \text{if there is } l \in \mathbb{N}_0 \text{ such that } m = jp^l, \\ 1 & \text{otherwise.} \end{cases}$

(b) $\prod_{j \in \mathbb{N}_p^*} \left\lceil \frac{m}{j} \right\rceil_p = p^{m-1}$.

Proof. **(a)** Clearly, $\left\lceil \frac{m+1}{j} \right\rceil_p = \left\lceil \frac{m}{j} \right\rceil_p$ unless $\frac{m}{j} = p^l$ for some $l \in \mathbb{N}_0$, in which case $\left\lceil \frac{m+1}{j} \right\rceil_p = p^{l+1} = p\left\lceil \frac{m}{j} \right\rceil_p$.

(b) By induction on m. The assertion is trivial for $m = 1$. Write $m = ip^l$ with $i := m^* \in \mathbb{N}_p^*$ and $l := v_p(m)$, then

$$\prod_{j \in \mathbb{N}_p^*} \left\lceil \frac{m+1}{j} \right\rceil_p = \left\lceil \frac{m+1}{i} \right\rceil_p \prod_{j \in \mathbb{N}_p^* \setminus \{i\}} \left\lceil \frac{m}{j} \right\rceil_p = p \prod_{j \in \mathbb{N}_p^*} \left\lceil \frac{m}{j} \right\rceil_p = p^m$$

by (a) and the induction hypothesis. □

For simplicity we restrict to the case of $|\operatorname{supp} \mathfrak{m}| = 1$, i.e. $\tilde{\mathfrak{m}} =: \mathfrak{p} \in \mathbb{P}_K \setminus S$. In this case the result is as follows.

6.4. Theorem. *Let* $\mathfrak{p} \in \mathbb{P}_K \setminus S$. *There are* $s = |S| - 1$ *positive integers* $n_1, \ldots, n_s$ *depending only on* S *and* $\mathfrak{p}$ *such that*

$$\left[K_S^{m\mathfrak{p}} : K_S^{\mathfrak{p}}\right] = q^{(m-1)\deg \mathfrak{p}} \Big/ \prod_{i=1}^{s} \left\lceil \frac{m}{n_i} \right\rceil_p$$

for all $m \in \mathbb{N}$.[4]

With $n_1, \ldots, n_s$ as in the theorem we define the polynomial

$$\delta := \frac{q^{\deg \mathfrak{p}} - 1}{(q-1)[K_S^{\mathfrak{p}} : K_S^{\mathfrak{o}}]} + \sum_{i=1}^{s} t^{n_i} = \sum_{n \in \mathbb{N}_0} \delta_n t^n \in \mathbb{Z}[t]$$

[4] In general, all degrees $[K_S^{\mathfrak{m}} : K_S^{\tilde{\mathfrak{m}}}]$, for $\operatorname{supp} \mathfrak{m}$ within a fixed set $R \subseteq \mathbb{P}_K \setminus S$ of r places, can be given in terms of (a tree of at most) $\sum_{i=1}^{s} r^i$ positive integers. A complete exposition of this result would make this section even more technical than it is already.

and set $\delta^{(m)} := \sum_{l=0}^{v_p(m)} \delta_{m/p^l} = |\{i \in \{1,\dots,s\} \mid n_i \le m,\ n_i^* = m^*\}|$ for $m \in \mathbb{N}$ and $\delta^{(0)} := \delta_0$. From 6.4 and 6.3(a) we derive the recursive degree formula

$$(5) \qquad \left[K_S^{(m+1)\mathfrak{p}} : K_S^{m\mathfrak{p}}\right] = q^{\deg \mathfrak{p}}/p^{\delta^{(m)}} \quad \forall m \in \mathbb{N},$$

which is more convenient for practical computations. Since the coefficients δ_n, $n \in \mathbb{N}_0$, of δ can be reconstructed out of the numbers $\delta^{(m)}$, $m \in \mathbb{N}_0$, from (5) we see that δ is uniquely determined by S and $\mathfrak{p}$. We call $\delta_{S,\mathfrak{p}} := \delta$ the **S-description at $\mathfrak{p}$**. Note that $\delta_{S,\mathfrak{p}}(1) - \delta_{S,\mathfrak{p}}(0) = s = |S| - 1$. Together with 5.3(c) we obtain the following

6.5. Corollary. *Let $\emptyset \neq S' \subseteq S$. Then $\delta_{S',\mathfrak{p}}^{(m)} \le \delta_{S,\mathfrak{p}}^{(m)}$ for all $m \in \mathbb{N}_0$.*[5]

Before we enter the proof of Theorem 6.4, we want to take a closer look at the structure of $U_{\mathfrak{p}}^{(1)}$. As usual we denote by $\mathbb{Z}_p = \varprojlim_l \mathbb{Z}/p^l\mathbb{Z}$ the ring of p-adic integers, the completion of $\mathbb{Z}$ at v_p. Identifying $u \in U_{\mathfrak{p}}^{(1)}$ with the family $(uU_{\mathfrak{p}}^{(n)})_{n\in\mathbb{N}}$, we can write

$$U_{\mathfrak{p}}^{(1)} = \varprojlim_n U_{\mathfrak{p}}^{(1)}/U_{\mathfrak{p}}^{(n)}.$$

Since $U_{\mathfrak{p}}^{(1)}/U_{\mathfrak{p}}^{(n)}$ is naturally a module over $\mathbb{Z}/\lceil n\rceil_p\mathbb{Z}$, and thereby a fortiori a $\mathbb{Z}_p$-module, the definition of $u^a := \left((uU_{\mathfrak{p}}^{(n)})^a\right)_{n\in\mathbb{N}}$ for $u \in U_{\mathfrak{p}}^{(1)}$ and $a \in \mathbb{Z}_p$ makes $U_{\mathfrak{p}}^{(1)}$ a $\mathbb{Z}_p$-module (cf. [H, pp. 215ff]). For the proof of 6.4 it is important to know how linear independence in $U_{\mathfrak{p}}^{(1)}$ over $\mathbb{Z}$ and $\mathbb{Z}_p$ are related.

6.6. Theorem (Kisilevsky). *Let I be a set. A family $(u_i)_{i\in I}$ of one-units $u_i \in U_{\mathfrak{p}}^{(1)}$, $i \in I$, is independent over $\mathbb{Z}$ iff it is independent over $\mathbb{Z}_p$.*

Proof. See [Ki]. □

By Proposition 6.2 and with π and B as therein, for each $n \in \mathbb{N}$ there is a (non-canonical) group isomorphism

$$\begin{array}{rccl} & U_{\mathfrak{p}}^{(1)}/U_{\mathfrak{p}}^{(n)} & \to & \mathcal{Z}^{(n)} := \displaystyle\prod_{j\in\mathbb{N}_p^*} \left(\mathbb{Z}/\mathbb{Z}\lceil n/j\rceil_p\right)^B \\ \zeta^{(n)} : & \displaystyle\prod_{\substack{j\in\mathbb{N}_p^*\\ \beta\in B}} (1+\beta\pi^j)^{c_{j\beta}} U_{\mathfrak{p}}^{(n)} & \mapsto & \left(c_{j\beta} + \mathbb{Z}\lceil n/j\rceil_p\right)_{\substack{j\in\mathbb{N}_p^*\\ \beta\in B}}. \end{array}$$

[5] Moreover, one has $\deg \delta_{S',\mathfrak{p}} \le \deg \delta_{S,\mathfrak{p}}$. But we shall not prove this here.

Passing to projective limits on both sides yields an isomorphism $\zeta : U_{\mathfrak{p}}^{(1)} \simeq \mathcal{Z} := \varprojlim_n \mathcal{Z}^{(n)} = \mathbb{Z}_p^{\mathbb{N}_p^* \times B}$ of $\mathbb{Z}_p$-modules (cf. Hasse's One-Unit Theorem in [H, p. 227]), which makes the diagram

$$\begin{array}{ccc} U_{\mathfrak{p}}^{(1)} & \xrightarrow{\ \zeta\ } & \mathcal{Z} \\ \big\downarrow & & \big\downarrow{\scriptstyle (n)} \\ U_{\mathfrak{p}}^{(1)}/U_{\mathfrak{p}}^{(n)} & \xrightarrow{\ \zeta^{(n)}\ } & \mathcal{Z}^{(n)} \end{array}$$

commutative for all $n \in \mathbb{N}$. Here ${}^{(n)}$ means the canonical projection $\mathcal{Z} \twoheadrightarrow \mathcal{Z}^{(n)}$.

A crucial role in the proof of Theorem 6.4 is played by the map

$$\begin{array}{rccl} & \mathcal{Z} & \to & \mathbb{N} \cup \{\infty\} \\ \nu : & (z_{j\beta})_{\substack{j \in \mathbb{N}_p^* \\ \beta \in B}} & \mapsto & \min\{jp^{v_p(z_{j\beta})} \mid j \in \mathbb{N}_p^*, \beta \in B\}, \end{array}$$

where we agree that $\nu(0) = p^\infty = \infty$. It satisfies the following properties.

6.7. Lemma. *Let $z, z' \in \mathcal{Z}$, $a \in \mathbb{Z}_p$ and $m \in \mathbb{N}$. Then*

(a) $\nu(az) = p^{v_p(a)}\nu(z)$.

(b) $\nu(z + z') \geq \min\{\nu(z), \nu(z')\}$.

(c) *The subgroup of $\mathcal{Z}^{(m)}$ generated by $z^{(m)}$ has order $\left|\left\langle z^{(m)} \right\rangle\right| = \lceil m/\nu(z) \rceil_p$.*

(d) $z^{(m)} = 0$ *if and only if* $m \leq \nu(z)$.

(e) *If $m > \nu(z)$ then $\nu(z)$ can be read from $z^{(m)}$.*

Proof. Write $z = (z_{j\beta})_{\substack{j \in \mathbb{N}_p^* \\ \beta \in B}}$ and $z' = (z'_{j\beta})_{\substack{j \in \mathbb{N}_p^* \\ \beta \in B}}$.

(a) $\nu(az) = \min\{jp^{v_p(a)}p^{v_p(z_{j\beta})} \mid j \in \mathbb{N}_p^*, \beta \in B\} = p^{v_p(a)}\nu(z)$.

(b) $\nu(z + z') \geq \min\{jp^{v_p(z_{j\beta})}, jp^{v_p(z'_{j\beta})} \mid j \in \mathbb{N}_p^*, \beta \in B\} = \min\{\nu(z), \nu(z')\}$.

(c) Write $z^{(m)} = \left(c_{j\beta} + \mathbb{Z}\lceil m/j \rceil_p\right)_{\substack{j \in \mathbb{N}_p^* \\ \beta \in B}}$ with $c_{j\beta} \in \mathbb{Z}$. For $j \in \mathbb{N}_p^*$ and $\beta \in B$, we then have $z_{j\beta} \equiv c_{j\beta} \mod \lceil m/j \rceil_p$, and therefore $c_{j\beta} + \mathbb{Z}\lceil m/j \rceil_p \in \mathbb{Z}/\mathbb{Z}\lceil m/j \rceil_p$ has order

$$\left|\left\langle c_{j\beta} + \mathbb{Z}\lceil m/j \rceil_p \right\rangle\right| = \max\{1, \lceil m/j \rceil_p / p^{v_p(c_{j\beta})}\} = \left\lceil m/(jp^{v_p(z_{j\beta})}) \right\rceil_p.$$

It follows that

$$\left|\left\langle z^{(m)} \right\rangle\right| = \max_{\substack{j \in \mathbb{N}_p^* \\ \beta \in B}} \left\lceil m/(jp^{v_p(z_{j\beta})}) \right\rceil_p = \lceil m/\nu(z) \rceil_p$$

by definition of ν.

(d) This is deduced from (c) and entails (e). □

After these preparations we can finally give the

Proof of Theorem 6.4. By Lemma 6.1, $U_{S,\mathfrak{p}} := \mathcal{O}_S^* \cap U_\mathfrak{p}^{(1)} = K^* \cap \mathcal{I}_S^\mathfrak{p}$ is free of rank s, say with basis[6] $(u_1, \dots, u_s)$. Set $z_i = (z_{ij\beta})_{\substack{j \in \mathbb{N}_p^* \\ \beta \in B}} := \zeta(u_i)$ for $i \in \{1, \dots, s\}$. According to Kisilevsky's Theorem 6.6, $u_1, \dots, u_s$ and hence also $z_1, \dots, z_s \in \mathcal{Z}$ are $\mathbb{Z}_p$-linearly independent. We can assume w.l.o.g. that

$$\nu(z_1) = n_1 := \min_{1 \le i \le s} \nu(z_i).$$

Write $n_1 = j_1 p^l$ with $j_1 := n_1^*$ and $l := v_p(n_1)$. By definition of ν, there is $\beta_1 \in B$ such that $v_p(z_{1j_1\beta_1}) = l$. For $i \in \{2, \dots, s\}$ we have $l \le v_p(z_{ij_1\beta_1})$ and can therefore define

$$\tilde{z}_i := z_i - \frac{z_{ij_1\beta_1}}{z_{1j_1\beta_1}} z_1 \in \mathcal{Z}.$$

Replacing $z_2, \dots, z_s$ by $\tilde{z}_2, \dots, \tilde{z}_s$ yields a direct decomposition

$$\left\langle z_1^{(m)}, \dots, z_s^{(m)} \right\rangle = \left\langle z_1^{(m)} \right\rangle \oplus \left\langle \tilde{z}_2^{(m)}, \dots, \tilde{z}_s^{(m)} \right\rangle$$

for all $m \in \mathbb{N}$, while $\left\langle z_1^{(m)} \right\rangle \simeq \mathbb{Z}/\mathbb{Z}\left\lceil m/n_1 \right\rceil_p$ by Lemma 6.7(c). We note that $\nu(\tilde{z}_i) \ge \nu(z_i) \ge n_1$ for $i \in \{2, \dots, s\}$ and that $\tilde{z}_2, \dots, \tilde{z}_s$ are again $\mathbb{Z}_p$-linearly independent. Hence we can apply the same procedure to $\tilde{z}_2, \dots, \tilde{z}_s$ once more and so on. In this way, we obtain positive integers $n_1 \le \dots \le n_s$ such that

$$U_{S,\mathfrak{p}} U_\mathfrak{p}^{(m)} / U_\mathfrak{p}^{(m)} \simeq \left\langle z_1^{(m)}, \dots, z_s^{(m)} \right\rangle \simeq \prod_{j=1}^{s} \mathbb{Z}/\mathbb{Z}\left\lceil \tfrac{m}{n_i} \right\rceil_p$$

and, consequently,

$$[K_S^{m\mathfrak{p}} : K_S^\mathfrak{p}] = (U_\mathfrak{p}^{(1)} : U_{S,\mathfrak{p}} U_\mathfrak{p}^{(m)}) = q^{(m-1)\deg \mathfrak{p}} \Big/ \prod_{i=1}^{s} \left\lceil \frac{m}{n_i} \right\rceil_p$$

for all $m \in \mathbb{N}$ by the isomorphism (4) on page 38. □

[6] In fact it would suffice to assume $\langle u_1, \dots, u_s \rangle$ of finite index prime to p in $U_{S,\mathfrak{p}}$.

The previous proof describes an algorithm for determining the positive integers $n_1 \leq \cdots \leq n_s$. In practice we shall perform it with some "precision" $n \in \mathbb{N}$, i.e. we apply it to $z_1^{(n)}, \ldots, z_s^{(n)}$ rather than to $z_1, \ldots, z_s$. By Lemma 6.7(e) this works fine, if we chose $n > n_s$ (which we cannot know beforehand). Otherwise, it is impossible to finish with the algorithm because of 6.7(d), and we have to redo the computations with larger precision. We shall illustrate this algorithm in an

6.8. Example. We continue Example 2.8 and retain the notation therein. Let $k \in \{0, \ldots, 3\}$. We want to determine the S_k-description at $\mathfrak{p} := \mathfrak{p}_4$. Note that $U_{\mathfrak{p}}^{(0)} = U_{\mathfrak{p}}^{(1)}$ and $\delta_{S_k,\mathfrak{p}}^{(0)} = 1$. It will suffice to work with "precision" $n = 6$. We abbreviate $(a + 8\mathbb{Z}, b + 2\mathbb{Z}, c + 2\mathbb{Z}) \in \mathcal{Z}^{(6)}$ by $\begin{pmatrix} a & b & c \end{pmatrix}$ and let

$$\zeta^{(6)} : \begin{array}{rcl} U_{\mathfrak{p}}^{(1)}/U_{\mathfrak{p}}^{(6)} & \to & \mathcal{Z}^{(6)} \\ (1+x)^a(1+x^3)^b(1+x^5)^c U_{\mathfrak{p}}^{(6)} & \mapsto & \begin{pmatrix} a & b & c \end{pmatrix} \end{array}$$

be the group isomorphism defined above. The expansion of y at $\mathfrak{p}$ in x has been determined in Example 1.7(a). Using the constructive proof of Proposition 6.2, we compute the "matrix"

$$C := \left(\zeta^{(6)}(u_i/x^{v_{\mathfrak{p}}(u_i)} U_{\mathfrak{p}}^{(6)})\right)_{1 \leq i \leq 4} = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 2 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix} \in (\mathcal{Z}^{(6)})^4.$$

Let $T_k \in \mathbb{Z}^{k \times 4}$ consist of the first k rows of T. Then

$$\left(\zeta^{(6)}(u_i' U_{\mathfrak{p}}^{(6)})\right)_{1 \leq i \leq 3} = T_3 C = \begin{pmatrix} 6 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \in (\mathcal{Z}^{(6)})^3.$$

Applying the algorithm of the previous proof yields $\delta_{S_1,\mathfrak{p}} = 1 + t^2$, $\delta_{S_2,\mathfrak{p}} = 1 + t^2 + t^5$ and $\delta_{S_3,\mathfrak{p}} = 1 + t + t^3 + t^5$. By means of Theorem 6.4 or formula (5) we can now calculate the degrees $[K_{S_k}^{m\mathfrak{p}} : K] = [K_{S_k}^{m\mathfrak{p}} : K_{S_k}^{\mathfrak{p}}]$ for any $m \in \mathbb{N}$. The genera are obtained from Corollary 5.9. For $m \in \mathbb{N}_0$ we put $K^{(m)} := K_{S_2}^{m\mathfrak{p}}$. Note that $\mathfrak{p} = \mathfrak{p}_4$ ramifies totally and $\mathfrak{p}_0$, $\mathfrak{p}_1$, $\mathfrak{p}_2$ split completely in $K^{(m)}$. From $[K_{S_3}^{2\mathfrak{p}} : K] = 1 < 2 = [K_{S_2}^{2\mathfrak{p}} : K]$ we conclude by Proposition 5.5 that $\mathfrak{p}_3 \notin S(K^{(m)}|K)$ and, consequently,

$$N_{K^{(m)}} := \left|\mathbb{P}^1_{K^{(m)}}\right| = 1 + 3[K^{(m)} : K]$$

for $m \geq 2$. The genus and number of rational places of $K^{(m)}$ with $m \in \{2, \ldots, 17\}$ are given in the following table.

$q = 2$										
m	2-3	4-6	7	8-9	10-11	12	13	14	15	16-17
$[K^{(m)} : K]$	2	4	8	16	32	64	128	256	512	1024
$g_{K^{(m)}}$	4	10	28	68	164	388	868	1892	4068	8676
$N_{K^{(m)}}$	7	13	25	49	97	193	385	769	1537	3073

In the previous example, $K^{(4)}$ has the maximal number of rational places possible for a function field $L|\mathbb{F}_2$ of genus 10, and $K^{(7)}$ and $K^{(8)}$ have more rational places than any example $L|\mathbb{F}_2$ of genus 28 and 68 found before. We shall further pursue this method of producing global function fields with many rational places in Part III.

Part III
Many Rational Places

As announced in the title, we are now trying to find global function fields K for which the number

$$N_K := \left|\mathbb{P}_K^1\right|$$

is large. In view of our preceding investigations, we are searching for such fields among ray class fields. This is done systematically in Section 9.

Before, in the next section, we turn to the question of how large N_K can be. In connection with this problem we shall discuss an upper bound for S-class numbers as well. In Section 8 we shall treat certain ray class fields of the rational function field with many rational places.

7 Upper Bounds

Let $K|\mathbb{F}_q$ be as before. In 1948 Weil proved the famous function field analogue of the Riemann Hypothesis, stating that the inverse roots $\omega_1, \ldots, \omega_{2g_K}$ of the numerator polynomial $P_K(t) = \prod_{i=1}^{2g_K}(1-\omega_i t)$ all have absolute value $|\omega_i| = \sqrt{q}$ (see [St2, Ch. V]). As an immediate consequence one obtains the so-called **Hasse-Weil bound** for the number of rational places

$$N_K \leq q + 1 + 2g_K\sqrt{q}. \tag{6}$$

In case equality holds, we call K **maximal**. Obviously, K can only be maximal if $g_K = 0$ or if q is a square. A consideration involving the constant field extension of degree 2 (see [St2, p. 182]) shows that in addition one must have $g_K \leq (q - \sqrt{q})/2$. In fact (for each square q), the Hermitian function field (see [St2, p. 198]) is a maximal function field of genus $(q-\sqrt{q})/2$. Stichtenoth and Xing [SX] conjectured a large gap below this genus and showed that there are indeed smaller values of g_K, for which K cannot be maximal. Finally Fuhrmann and Torres [FT] succeeded in completing the proof of this conjecture.

7.1. Theorem (Fuhrmann and Torres). *Let $K|\mathbb{F}_q$ be maximal. Then either $g_K = (q - \sqrt{q})/2$ or $g_K \leq (\sqrt{q} - 1)^2/4$.*

For non-square q, Serre [S2] could improve (6). We denote by $\lfloor a \rfloor$ the integer part of $a \in \mathbb{R}$.

7.2. Theorem (Serre). *For any $K|\mathbb{F}_q$ we have:*

(a) $N_K \le q + 1 + g_K\lfloor 2\sqrt{q}\rfloor$.

(b) *If $N_K = q + g_K\lfloor 2\sqrt{q}\rfloor$ then $g_K = 1$ or $g_K = 2$.*

Proof. **(a)** See [St2, pp. 180f].

(b) This is proven in [S5, pp. 5–11a] with the aid of a theorem by Siegel on totally positive algebraic integers. □

The bound in 7.2(a) is called the **Serre bound**. Combining 7.2(b) with 7.1, we obtain:

7.3. Corollary. *If q is a square ≥ 16 and $(\sqrt{q}-1)^2/4 < g_K \ne (q-\sqrt{q})/2$, then $N_K \le q - 1 + 2g\sqrt{q}$.*

The maximum number of rational places a global function field of genus $g \in \mathbb{N}_0$ with full constant field $\mathbb{F}_q$ can have is denoted $N_q(g)$. We call $K|\mathbb{F}_q$ **optimal** if $N_K = N_q(g_K)$. Note that, trivially, $N_q(0) = q + 1$. Also $N_q(1)$ and $N_q(2)$ have been determined in general. (For details see [S3].) For larger g, the precise value of $N_q(g)$ is still unknown in most cases. An overview of what is known about $N_q(g)$ for $g \le 50$ and q a not too large power of 2 or 3 is given in [GV7].

For large genera one can improve the above bounds by means of the so-called explicit Weil formulas (see [St2, p. 183]): Each polynomial $\psi(t) = c_1 t + \cdots + c_m t^m \in \mathbb{R}[t]$ with $c_1, \ldots, c_m \ge 0$ satisfying

$$1 + \psi(t) + \psi(t^{-1}) \ge 0 \quad \forall t \in \mathbb{C} \text{ with } |t| = 1$$

(write $\psi \gg 0$ for short) provides an estimate

$$g_K \ge (N_K - 1)\psi(q^{-1/2}) - \psi(q^{1/2}). \tag{7}$$

The maximization of the right hand side of (7) over all $\psi \gg 0$ goes back to an unpublished manuscript of Oesterlé's, given to Serre [S6, pp. 29–37a]. In the following we shall give an outline of this result, which is also presented in [Sf] and [Th].

First note that, for each $m \in \mathbb{N}$, the map

$$F_m : \begin{array}{ccc} [\frac{\pi}{m+1}, \frac{\pi}{m}] & \to & [0,1] \\ \varphi & \mapsto & -\dfrac{\cos\frac{m+1}{2}\varphi}{\cos\frac{m-1}{2}\varphi} \end{array}$$

is an isotonous homeomorphism because it has derivative $F'_m(\varphi) = (\sin m\varphi + m\sin\varphi)/(2\cos^2\frac{m-1}{2}\varphi)$. Next we define a map

$$\vartheta_q : [q+1,\infty) \to [0,1)$$

piecewise as follows. Given a real number $N \geq q+1$, let $m \geq 2$ be the unique integer such that $N \in [q^{m/2}+1, q^{(m+1)/2}+1)$ and set

$$u := \frac{1}{\sqrt{q}}\,\frac{q^{(m+1)/2} - N + 1}{N - 1 - q^{(m-1)/2}} \in (0,1].$$

Then we define $\vartheta_q(N) := \cos(F_m^{-1}(u))$. It is easily verified that ϑ_q is again an isotonous homeomorphism. Finally we claim that also

$$\gamma_q : \begin{array}{rcl} [q+1,\infty) & \to & [0,\infty) \\ N & \mapsto & 1 + \dfrac{(\sqrt{q}\vartheta_q(N)-1)N}{q - 2\sqrt{q}\vartheta_q(N) + 1}. \end{array}$$

is strictly increasing. The isotony of γ_q on $[q^2+1,\infty)$ is evident since $\vartheta_q(q^2+1) = 1/\sqrt{2} \geq 1/\sqrt{q}$. A direct computation shows that

$$\gamma_q(N) = (N-q-1)/(2\sqrt{q}) \quad \text{for } N \in [q+1, q^{3/2}+1] \tag{8}$$

and

$$\begin{aligned} \gamma_q(N) = \tfrac{1}{4q}\Big(&N - q^2 - 1 \\ &+ \sqrt{(8q+1)N^2 - (18q^2+16q+2)N + q^4 + 8q^3 + 18q^2 + 8q + 1}\Big) \\ &\text{for } N \in [q^{3/2}+1, q^2+1], \end{aligned} \tag{9}$$

whence we see that γ_q is strictly increasing on $[q+1, q^2+1]$ as well.

7.4. Theorem (Oesterlé). *Suppose that $N_K \geq q+1$. Then $g_K \geq \gamma_q(N_K)$. For $q \geq 3$ (but not always for $q = 2$), $\gamma_q(N_K)$ is the maximum of the right hand side of (7) over all $\psi \gg 0$.*

Proof. See [Th, pp. 45-63]. □

Let $\bar{N}_q := \gamma_q^{-1} : [0,\infty) \to [q+1,\infty)$ be the inverse map. Then clearly

$$N_q(g) \leq \bar{N}_q(g) \quad \forall g \in \mathbb{N}_0. \tag{10}$$

We call this estimate the **Oesterlé bound**. Equation (8) implies $\bar{N}_q(g) = q+1+2g\sqrt{q}$, i.e. the Oesterlé bound coincides with the Hasse-Weil bound, for $g \in [0, (q-\sqrt{q})/2]$. Furthermore, from (9) we deduce

$$(11)\quad \bar{N}_q(g) = q+1+\tfrac{1}{2}\Big(\sqrt{(8q+1)g^2+4(q^2-q)g}-g\Big)$$
$$\text{for } g \in \big[\tfrac{1}{2}(q-\sqrt{q}), \sqrt{\tfrac{q}{2}}(q-1)\big].$$

The right hand side of (11) is also known as the **Ihara bound** for $N_q(g)$ and has been directly and more elegantly established for all $g \in \mathbb{N}_0$ in [I].

7.5. Example. (a) We want to find a good upper bound for $N_7(3)$. The Hasse-Weil bound and the Serre bound both say $N_7(3) \le 23$. From (11) we see that

$$22 < \bar{N}_7(3) = (3\sqrt{113}+13)/2 < 23.$$

Since $N_7(3) \ne 22$ by 7.2(b) we can conclude $N_7(3) \le 21$. The exact value of $N_7(3)$, as determined by Serre [S4], is 20.

(b) By (11) we have $\bar{N}_4(3) = 5+\frac{1}{2}(\sqrt{441}-3) = 14$. This shows that the global function field in Example 2.7 is optimal and that $N_4(3) = 14$.

For non-empty $S \subseteq \mathbb{P}_K$, the S-class number h_S can be estimated by applying Oesterlé's Theorem to the Hilbert class field of $\mathcal{O}_S$.

7.6. Proposition. *Assume that $K|\mathbb{F}_q$ has genus $g \ge 1$ and that $S \subseteq \mathbb{P}_K$ contains at least $N > (\sqrt{q}-1)(g-1)$ rational places. Then*

$$h_S \le \hbar_q(g,N) := \vartheta_q^{-1}(t)/N \quad \textit{with} \quad t := \frac{N+(q+1)(g-1)}{\sqrt{q}(N+2g-2)}.$$

Proof. The restrictions on g and N ensure that $1/\sqrt{q} \le t < 1$, whereby $\hbar_q$ is well-defined. Let $K' := K_S^{\mathfrak{o}}$ be the Hilbert class field of $\mathcal{O}_S$. By Proposition 5.5, its field of constants is again $\mathbb{F}_q$, and the extension $K'|K$ is unramified of degree $[K' : K] = h_S$. Hence $g' := g_{K'} = 1+h_S(g-1)$ by 1.4. Moreover, $N' := N_{K'} \ge h_S N$ since every place of S splits completely in $K'|K$. For $N' \le q+1$, the claim of the proposition is obvious. Assume $N' \ge q+1$. Then, by Oesterlé's Theorem,

$$\frac{g-1}{N} \ge \frac{g'-1}{N'} \ge \frac{\gamma_q(N')-1}{N'} = \frac{\sqrt{q}\vartheta_q(N')-1}{q-2\sqrt{q}\vartheta_q(N')+1}.$$

Isolating $\vartheta_q(N')$ in this inequality results in $\vartheta_q(N') \le t$, from which, by the isotony of ϑ_q, we conclude the assertion. □

From the following lemma, which also helps us compute the bounds $\hbar_q(g,N)$, we see that ϑ_q^{-1} is piecewise a $\mathbb{Q}(\sqrt{q})$-rational function.

7.7. Lemma. *For each $n \in \mathbb{N}$, define a polynomial*

$$f_n(t) := \sum_{i=0}^{\lfloor n/2 \rfloor} \tfrac{n}{n-i}\tbinom{n-i}{i}(-2t-2)^{\lfloor n/2 \rfloor - i} \in \mathbb{Z}[t].$$

(a) *The f_n satisfy $f_{n-1}+f_n = f_{n+1}$ if n is even, and $f_{n-1}(t) - 2(t+1)f_n(t) = f_{n+1}(t)$ if n is odd.*

(b) *Let $t \in \left[\cos\frac{\pi}{m}, \cos\frac{\pi}{m+1}\right]$ with $2 \le m \in \mathbb{N}$. Then*

$$\vartheta_q^{-1}(t) = 1 + \frac{q^{(m+1)/2} + q^{m/2}u}{1+\sqrt{q}u} \quad \textit{with} \quad u := \frac{f_{m+1}(t)}{f_{m-1}(t)}.$$

Proof. **(a)** This is verified using $\frac{n-1}{n-i}\binom{n-i}{i-1} + \frac{n}{n-i}\binom{n-i}{i} = \frac{n+1}{n+1-i}\binom{n+1-i}{i}$.

(b) Using (a) and the formula $\cos\frac{n-1}{2}\varphi + \cos\frac{n+1}{2}\varphi = 2\cos\frac{\varphi}{2}\cos\frac{n}{2}\varphi$, one can show by induction that

$$(-1)^{\lfloor n/2 \rfloor}\cos\tfrac{n}{2}\varphi = \begin{cases} \frac{1}{2}f_n(\cos\varphi) & \text{if } n \text{ is even,} \\ (\cos\frac{\varphi}{2})f_n(\cos\varphi) & \text{if } n \text{ is odd,} \end{cases}$$

for all $n \in \mathbb{N}$ and $\varphi \in \mathbb{R}$. Writing $t = \cos\varphi$ with $\varphi \in \left[\frac{\pi}{m+1}, \frac{\pi}{m}\right]$, it follows that $F_m(\varphi) = f_{m+1}(t)/f_{m-1}(t)$. Hence the assertion is clear from the definition of ϑ_q. □

7.8. Example. By means of 7.7(a) we obtain

$$\begin{aligned}
&f_1(t) = 1, \quad f_2(t) = -2t, \quad f_3(t) = -2t+1, \quad f_4(t) = 4t^2-2,\\
&f_5(t) = 4t^2-2t-1, \quad f_6(t) = -8t^3+6t, \quad f_7(t) = -8t^3+4t^2+4t-1,\\
&f_8(t) = 16t^4-16t^2+2, \quad f_9(t) = 16t^4-8t^3-12t^2+4t+1,\\
&f_{10}(t) = -32t^5+40t^3-10t,\\
&f_{11}(t) = -32t^5+16t^4+32t^3-12t^2-6t+1,\\
&f_{12}(t) = 64t^6-96t^4+36t^2-2, \quad \ldots
\end{aligned}$$

(a) Let K and S be as in Example 2.7. By Lemma 7.7 we have

$$14\hbar_4(3,14) = \vartheta_4^{-1}\left(\tfrac{2}{3}\right) = 1 + \frac{16+8u}{1+2u} \text{ with } u = \frac{f_4(2/3)}{f_2(2/3)} = \frac{1}{6}$$

since $\frac{2}{3} \in [\cos\frac{\pi}{3}, \cos\frac{\pi}{4}]$. Hence $h_S \le \hbar_4(3,14) = 1$ according to Proposition 7.6. By Corollary 2.2, we can therefore conclude that K has divisor class number $h_K = \mathrm{reg}_S = 512$.

(b) Let $K = \mathbb{F}_3(x,y)$ where x is an indeterminate over $\mathbb{F}_q$ and y satisfies the Artin-Schreier equation $y^3 - y = x^7 - x^5$. The numbers of places of K up to degree $g_K = 6$ are given by $\left(\left|\mathbb{P}_K^d\right|\right)_{1\le d\le 6} = (10, 9, 0, 18, 36, 108)$. Hence $Z_K(t) = 1 + 10t + 64t^2 + 310t^3 + 1273t^4 + 4648t^5 + 15700t^6 + \cdots$,

$$\begin{aligned} P_K(t) = (1 - 4t + 3t^2)Z_K(t) &= 1 + 6t + 27t^2 + 84t^3 + 225t^4 + 486t^5 \\ &\quad + 927t^6 + 1458t^7 + 2025t^8 + 2268t^9 + 2187t^{10} + 1458t^{11} + 729t^{12} \end{aligned}$$

and $h_K = P_K(1) = 11881$ according to Theorem 1.2. Let $S \subseteq \mathbb{P}_K$ contain at least 5 rational places. We want to show that then $h_S = 1$. We have $t := \frac{5}{9}\sqrt{3} \in [\cos\frac{\pi}{11}, \cos\frac{\pi}{12}]$ and $u := f_{12}(t)/f_{10}(t) = \frac{1633}{6525}\sqrt{3}$, consequently,

$$\vartheta_3^{-1}(t) = 1 + \frac{3^6 + 3^5\sqrt{3}u}{1 + \sqrt{3}u} = \frac{993101}{1904}$$

by Lemma 7.7. From Proposition 7.6 we obtain $h_S \le \hbar_3(6,5) = \vartheta_3^{-1}(t)/5 = 993101/9520 < 105$. Since, on the other hand, h_S divides $h_K = 109^2$, we can conclude that $h_S = 1$. □

8 Rational Function Field

Let $K = \mathbb{F}_q(x)$, where x is an indeterminate over $\mathbb{F}_q$. For convenience we again fix an algebraic closure $\bar{K}$, in which all algebraic extensions of K considered here, especially the ray class fields, are assumed to lie.

Throughout this section we assume that $S \subseteq \mathbb{P}_K^1$ is non-empty and that $\mathfrak{p} \in \mathbb{P}_K^1 \setminus S$ is another rational place. Note that under these assumptions we have $h_S = h_K = 1$ and $\mathcal{I}_S^{\mathfrak{o}}/\mathcal{O}_S^*\mathcal{I}_S^{\mathfrak{p}} \simeq U_{\mathfrak{p}}/\mathbb{F}_q^* U_{\mathfrak{p}}^{(1)} = 1$, hence $K_S^{\mathfrak{p}} = K$ by Proposition 5.2. For $\alpha \in \mathbb{F}_q$ denote by $\mathfrak{p}_\alpha$ the zero of $x - \alpha$. After a transformation of the variable x we can assume that $\mathfrak{p} = \infty$ is the pole of x and that $\mathfrak{p}_0 \in S$.

We shall consider two special situations in this section. First we restrict to the case $q = p$, and in the end we allow q to be an arbitrary p-power again but

require $|S| = q$. In both cases we shall explicitly give the S-description at $\mathfrak{p}$ and provide defining equations for the first few ray class fields.

From now on we assume $q = p$ and set $A := \{\alpha \in \mathbb{F}_p^* \,|\, \mathfrak{p}_\alpha \in S\}$. Then $|A| = |S| - 1 =: s \in \{0, \dots, p-1\}$.

8.1. Theorem. *Under the above conditions, the S-description at $\mathfrak{p}$ equals*

$$\delta_{S,\mathfrak{p}} = \sum_{n=0}^{s} t^n.$$

The proof depends on the following

8.2. Lemma. *Let $U_{S,\mathfrak{p}} := \mathcal{O}_S^* \cap U_\mathfrak{p}^{(1)}$. Then $U_\mathfrak{p}^{(1)} = U_{S,\mathfrak{p}} U_\mathfrak{p}^{(s+1)}$.*

Proof of the lemma. Write $A = \{\alpha_1, \dots, \alpha_s\}$ and take $\pi := 1/x$ as a uniformizer at $\mathfrak{p} = \infty$. Then $U_{S,\mathfrak{p}} = \langle 1 - \alpha_1\pi, \dots, 1 - \alpha_s\pi \rangle$. By Proposition 6.2, it suffices to show that the product

$$\prod_{i=1}^{s} \left\langle (1 - \alpha_i\pi) U_\mathfrak{p}^{(s+1)} \right\rangle \subseteq U_\mathfrak{p}^{(1)} / U_\mathfrak{p}^{(s+1)}$$

is direct. To this end, let $c_1, \dots, c_s \in \{0, \dots, p-1\}$ and write

$$y := \prod_{i=1}^{s} (1 - \alpha_i\pi)^{c_i} = \sum_{n \in \mathbb{N}_0} \sigma_n \pi^n$$

with $1 = \sigma_0, \sigma_1, \sigma_2, \dots \in \mathbb{F}_p$. For $j \in \mathbb{N}$, set $\beta_j := \sum_{i=1}^{s} c_i \alpha_i^j$ and recall Newton's Formulas

$$n\sigma_n + \sum_{j=1}^{n} \beta_j \sigma_{n-j} = 0 \quad \forall n \in \mathbb{N}. \tag{12}$$

Now we assume that $y \in U_\mathfrak{p}^{(s+1)}$, i.e. $\sigma_1 = \cdots = \sigma_s = 0$. By (12) it follows inductively that $\beta_1 = \cdots = \beta_s = 0$. In other words, $(c_1, \dots, c_s)$, viewed as a vector in $\mathbb{F}_p^s$, lies in the kernel of the matrix $(\alpha_i^j)_{1 \le i,j \le s} \in \mathrm{GL}_s(\mathbb{F}_p)$, i.e. $c_1 = \cdots = c_s = 0$. □

Proof of the theorem. Write $\delta_{S,\mathfrak{p}} = 1 + \sum_{n \in \mathbb{N}} \delta_n t^n$ with $\delta_1, \delta_2, \dots \in \{0, 1\}$. By the lemma we know that $K_S^{(s+1)\mathfrak{p}} = K_S^\mathfrak{p}$. According to the recursive degree formula (5) in Section 6, this implies $\delta_{S,\mathfrak{p}}^{(m)} = 1$ for $m \in \{1, \dots, s\}$, which in turn yields $\delta_1 = \cdots = \delta_s = 1$. Since $\delta_{S,\mathfrak{p}}(1) = s+1$, we obtain the assertion. □

Note that $\mathfrak{p}$ is totally ramified in $K_S^{m\mathfrak{p}}$ for all $m \in \mathbb{N}_0$ since $K_S^{\mathfrak{o}} = K$ is the inertia field of $\mathfrak{p}$ in $K_S^{m\mathfrak{p}}$. Furthermore, if $S' \subseteq \mathbb{P}_K^1$ satisfies $|S'| - 1 > s$, then $K_{S'}^{(s+2)\mathfrak{p}} = K \subsetneq K_S^{(s+2)\mathfrak{p}}$ according to Theorem 8.1. Consequently for all $m \geq s+2$, by Proposition 5.5, $S = S(K_S^{m\mathfrak{p}}|K) \cap \mathbb{P}_K^1$ and therefore $K_S^{m\mathfrak{p}}$ has exactly

$$N_{K_S^{m\mathfrak{p}}} = 1 + [K_S^{m\mathfrak{p}} : K](s+1)$$

rational places. The genus can be calculated by means of 5.9.

8.3. Example. For $p = q \in \{5, 7\}$ and different values of $s = |S| - 1$ and m we compute genus and number of rational places of the ray class fields $K_S^{m\mathfrak{p}}$. As an orientation we include (the integer part of) the Oesterlé bound in the following tables.

$q = 5$												
s	1	2	3	4	1	2	3	4	1	2	3	4
m	3	4	5-6	7	4	5-6	7	8	5-6	7	8	9
$[K_S^{m\mathfrak{p}} : K]$	5	5	5	5	25	25	25	25	125	125	125	125
$g_{K_S^{m\mathfrak{p}}}$	2	4	6	10	22	34	56	70	172	284	356	420
$N_{K_S^{m\mathfrak{p}}}$	11	16	21	26	51	76	101	126	251	376	501	626
$\lfloor \bar{N}_5(g_{K_S^{m\mathfrak{p}}}) \rfloor$	14	19	25	34	60	83	125	150	324	506	622	723

$q = 7$												
s	1	2	3	4	5	6	1	2	3	4	5	6
m	3	4	5	6	7-8	9	4	5	6	7-8	9	10
$[K_S^{m\mathfrak{p}} : K]$	7	7	7	7	7	7	49	49	49	49	49	49
$g_{K_S^{m\mathfrak{p}}}$	3	6	9	12	15	21	45	69	93	117	162	189
$N_{K_S^{m\mathfrak{p}}}$	15	22	29	36	43	50	99	148	197	246	295	344
$\lfloor \bar{N}_7(g_{K_S^{m\mathfrak{p}}}) \rfloor$	22	32	42	52	60	77	140	198	254	311	413	472

We want to write the first few $K_S^{m\mathfrak{p}}$ as Artin-Schreier extensions in the sense of Example 3.3. Recall the definition of $\mathbb{N}_p^* = \mathbb{N} \setminus p\mathbb{Z}$ from Section 6.

8.4. Proposition. *For $s < n \in \mathbb{N}$ we set*

$$u_n := x^{n-s} \prod_{\alpha \in A} (x - \alpha).$$

Let $m \in \{\tilde{s}+1, \ldots, p(\tilde{s}+1)\}$ with $\tilde{s} := s$ if $s < p-1$ and $\tilde{s} := p$ if $s = p-1$.[7] *Then*

$$K_S^{m\infty} = K(\wp^{-1}u_n \,|\, n \in \mathbb{N}_p^*, \tilde{s} < n < m).$$

[7] It is not hard to derive from the proof of 6.4 that if m is larger than this, then $G(K_S^{m\infty}|K)$ is no longer of exponent p, i.e. $K_S^{m\infty}|K$ can no longer be written as an Artin-Schreier extension in the sense of 3.3.

Proof. Set $J := \{n \in \mathbb{N}_p^* \,|\, \tilde{s} < n < m\}$ and $L := K(\wp^{-1}u_n \,|\, n \in J)$. By 3.3(b) and (c), the extension $L|K$ has conductor $\mathfrak{f}(L|K) \leq m\infty$ and splitting set $S \subseteq S(L|K)$; hence, $L \subseteq K_S^{m\infty}$ according to Proposition 5.5. We show equality by comparing degrees. Set

$$V := \sum_{n\in J} \mathbb{F}_p u_n \subseteq \mathbb{F}_p[x];$$

then we have $\deg u \in J \subseteq \mathbb{N}_p^*$ for all $u \in V \setminus \{0\}$. Therefore $V \cap \wp K = V \cap \wp\mathbb{F}_p[x] = 0$, thus

$$\log_p[L : K] = \dim_{\mathbb{F}_p} V = |J|$$

by 3.3(d). For $n \in \mathbb{N}$, Theorem 8.1 and the recursive degree formula (5) yield $[K_S^{(n+1)\infty} : K_S^{n\infty}] = p$ if $s < n^*$ and $K_S^{(n+1)\infty} = K_S^{n\infty}$ otherwise. Hence

$$\log_p[K_S^{m\infty} : K] = |\{n \in \mathbb{N} \,|\, s < n^*, n < m\}|\,.$$

The inclusion $\{n \in \mathbb{N} \,|\, s < n^*, n < m\} \subseteq J$ holds due to the restrictions on m. □

Now we turn to a different situation. We let $q = p^e$ with $e \in \mathbb{N}$ arbitrary and take S as large as possible under the general assumptions of this section, i.e. $S = \mathbb{P}_K^1 \setminus \{\mathfrak{p}\}$. In this case, the S-description at $\mathfrak{p}$ has been explicitly determined by Lauter [La3]. We present her result in the following.

Take $Q := \{1, \ldots, q-1\} \subseteq \mathbb{Z}$ as a set of representatives for the cyclic group $\mathbb{Z}/(q-1)\mathbb{Z} \simeq \mathbb{F}_q^*$. Via this latter isomorphism (and independent of its specific form), the group $G := G(\mathbb{F}_q|\mathbb{F}_p)$ acts on Q. Clearly, two elements n and n' of Q lie in the same G-orbit $Gn = Gn'$ iff $n' \equiv p^l n \mod q-1$ for some $l \in \mathbb{N}_0$. For $n \in \mathbb{N}$ we define

$$e_n := \begin{cases} |Gn| & \text{if } n \in Q \text{ and } n = \min Gn, \\ 0 & \text{otherwise.} \end{cases}$$

Note that if $e_n > 0$, then $n \in \mathbb{N}_p^* \cap Q$ and e_n divides $e = |G|$. Some other facts concerning the numbers e_n are collected in Lemma 8.7 below.

8.5. Theorem (Lauter). *Under the above assumptions with $|S| = q$, the S-description at $\mathfrak{p}$ is*

$$\delta_{S,\mathfrak{p}} = 1 + \sum_{n\in\mathbb{N}} e_n t^n$$

Proof. See [La3]. □

Thus the recursive degree formula (5) simplifies to

$$(13)\quad \left[K_S^{(m+1)\mathfrak{p}} : K_S^{m\mathfrak{p}}\right] = q/p^{e_{m^*}} \quad \forall m \in \mathbb{N}.$$

By Galois theory, for each $l \in \mathbb{N}_0$ we choose an extension $L_l|K$ of degree p^l such that L_l is an intermediate field of $K_S^{m\mathfrak{p}}|K_S^{(m-1)\mathfrak{p}}$ for some $m \in \mathbb{N}$. The genus g_{L_l} of L_l can be computed by means of 5.9. According to 5.8, the inertia field of $\mathfrak{p}$ in L_l is $L_l^0(\mathfrak{p}) = L_l \cap K_S^{\mathfrak{o}} = K$; hence, $\mathfrak{p}$ is totally ramified in L_l. Therefore

$$(14)\quad N_{L_l} = 1 + p^l q \quad \forall l \in \mathbb{N}_0.$$

In fact, for small l, the L_l tend to have many rational places compared to their genera.

8.6. Example. Let $q = 16$. Then the G-orbits in Q are

$$\{1,2,4,8\},\ \{3,6,9,12\},\ \{5,10\},\ \{7,11,13,14\} \text{ and } \{15\}.$$

Hence $\delta_{S,\mathfrak{p}} = 1 + 4t + 4t^3 + 2t^5 + 4t^7 + t^{15}$ by Lauter's Theorem. The degrees of the extensions $K_S^{m\mathfrak{p}}|K$, as computed by means of (13) for the first few values of m, are as follows

m	0–5	6–9	10	11	12–13	14–15	16–17	18	19	20	21	22
$[K_S^{m\mathfrak{p}} : K]$	1	4	64	2^8	2^{12}	2^{16}	2^{19}	2^{23}	2^{27}	2^{31}	2^{33}	2^{37}

Using (14) and the genus formula of Corollary 5.9, we obtain the genera and numbers of rational places of the fields L_l for $1 \le l \le 11$ in the table below, the last row of which gives (the integer part of) the Oesterlé bound.

$q = 16$											
l	1	2	3	4	5	6	7	8	9	10	11
g_{L_l}	2	6	22	54	118	246	534	1110	2390	4950	10070
N_{L_l}	33	65	129	257	513	1025	2049	4097	8193	16385	32769
$\lfloor \bar{N}_{16}(g_{L_l}) \rfloor$	33	65	150	309	590	1135	2271	4496	9211	18489	36503

8.7. Lemma. *Write $q = p^e$ with $e \in \mathbb{N}$.*

(a) *We have $e_{q-1} = 1$, $e_n = 0$ for $q - q/p \le n < q - 1$, and $e_{q-1-q/p} = e$.*

(b) *Let e be even and $r := \sqrt{q}$. Then $e_n = e$ for $n \in \{1, \dots, 2r\} \setminus (p\mathbb{Z} \cup \{r+1\})$. Moreover, $e_{r+1} = e/2$ and $e_{2r+1} = 0$.*

(c) *Let e be odd and $r := \sqrt{pq}$. Then $e_n = e$ for $n \in \{1, \dots, r\} \setminus p\mathbb{Z}$ and $e_n = 0$ for $n \in \{r, \dots, r+p\}$.*

Proof. **(a)** Clearly, the G-orbit of $q-1$ is $G(q-1)=\{q-1\}$; hence $e_{q-1}=1$. Let $q-q/p \le n < q-1$. Then $q \ne p$ and $p-1 \le n' := pn-(p-1)(q-1) < q-1$. Hence $n' \in Gn$, and from $n-n' = (p-1)(q-1-n) > 0$ we conclude that $e_n = 0$. Finally let $n := q-1-q/p$. Then

$$p^l n = p^l(q-1-q/p) \equiv q-1-p^{l-1} \mod q-1$$

for all $l \in \{1,\dots,e\}$. Thus $Gn = \{q-1-p^{l-1} \mid 1 \le l \le e\}$ has e elements and minimum n.

(b) Let $n \in \{1,\dots,2r\} \setminus p\mathbb{Z}$. Then

$$n \le p^l n \in \{p^l,\dots,2q/p-p^l\} \subseteq Q \text{ for } 0 \le l < e/2.$$

In particular, Gn has at least $e/2$ elements. Now let $e/2 \le l < e$ and write $n = a + p^{e-l}b$ with $a \in \{1,\dots,p^{e-l}-1\}$ and $b \in \{0,\dots,2p^{l-e/2}-1\}$. Then

$$n' := p^l n-(q-1)b = p^l a + b \in \{p^l,\dots,q-1-(r-2)p^{l-e/2}\} \subseteq Q.$$

Thus again $n < 2r \le pr < p^l \le n'$ for $e/2 < l < e$. If $l = e/2$, then $n = a + rb$ and $n' = ra + b$ with $a \in \{1,\dots,r-1\}$ and $b \in \{0,1\}$; hence $n'-n = (r-1)(a-b) \ge 0$, and $n' = n$ only for $a = b = 1$, i.e. for $n = r+1$. This shows $n = \min Gn$ and $|Gn| > e/2 \iff n \ne r+1$.

Finally we have $p^{e/2}(2r+1) = 2q + r \equiv r+2 \mod q-1$; hence $e_{2r+1} = 0$.

(c) Let $n \in \{1,\dots,r\} \setminus p\mathbb{Z}$. Then

$$n \le p^l n \in \{p^l,\dots,q-p^l\} \subseteq Q \text{ for } 0 \le l < (e-1)/2.$$

In particular, $|Gn| = e$. Now let $(e+1)/2 \le l < e$ and write $n = a + p^{e-l}b$ with $a \in \{1,\dots,p^{e-l}-1\}$ and $b \in \{0,\dots,2p^{l-(e-1)/2}-1\}$. Then

$$n < p^l \le p^l a + b = p^l n-(q-1)b \le q-1-(r-p)p^{l-(e-1)/2};$$

hence $n = \min Gn$. As for the second assertion, let $n \in \{r+1,\dots,r+p-1\}$. Then $p^{(e-1)/2}n-q+1 = r(n-r)/p+1 < r+1 \le n$, hence $e_n = 0$. □

As in the lemma, we set $r := \sqrt{q}$ or $\sqrt{pq}$ according to whether q is a square or not. From (13) and 8.7(b) and (c) we conclude $K_S^{(r+1)\mathfrak{p}} = K$. Furthermore we obtain two canonical fields, namely $K_S^{(r+2)\mathfrak{p}}$ and $K_S^{(2r+2)\mathfrak{p}}$ of degree r and rq over K if q is a square, and $p-1$ canonical fields $K_S^{(r+i+1)\mathfrak{p}}$ with $1 \le i < p$ of degree q^i over K in case q is non-square. Below we shall give defining equations for these canonical fields. Their genera and those of the intermediate fields L_l introduced above are easily computed by means of 5.9.

8.8. Proposition. *Write $q = p^e$ with $e \in \mathbb{N}$.*

(a) *If e is even, then* $g_{L_l} = \begin{cases} \frac{r}{2}(p^l - 1) & \text{for } 0 \le l \le e/2, \\ \frac{r}{2}(2p^l - r - 1) & \text{for } e/2 \le l \le 3e/2. \end{cases}$

(b) *If e is odd, then*

$$g_{L_l} = \frac{1}{2}\left(p^l(r+i-1) - r - \frac{q^i - q}{q-1}\right)$$

for $(i-1)e \le l \le ie$ with $1 \le i < p$.

Proof. **(a)** If $0 \le l \le e/2$, then L_l is an intermediate field of $K_S^{(r+2)\mathfrak{p}} | K_S^{(r+1)\mathfrak{p}}$, whence $g_{L_l} = 1 + p^l \frac{r}{2} - \frac{r+2}{2} = \frac{r}{2}(p^l - 1)$ by Corollary 5.9. For $e/2 \le l \le e/3$, L_l is an intermediate field of $K_S^{(2r+2)\mathfrak{p}} | K_S^{(2r+1)\mathfrak{p}}$, thus $g_{L_l} = 1 + p^l r - \frac{1}{2}(r+2+q) = \frac{r}{2}(2p^l - r - 1)$ by 5.9.

(b) If $(i-1)e \le l \le ie$ with $i \in \{1, \dots, p-1\}$, then L_l is an intermediate field of $K_S^{(r+i)\mathfrak{p}} | K_S^{(r+i+1)\mathfrak{p}}$, thus $g_{L_l} = 1 + p^l \frac{r+i-1}{2} - \frac{1}{2}\big(r + 1 + \sum_{j=1}^{i-1} q^j\big) = \frac{1}{2}\big(p^l(r+i-1) - r - \frac{q^i - q}{q-1}\big)$ by 5.9. □

In particular, if e is even, then $L_0, \dots, L_{e/2}$ are maximal, and moreover, according to [RS], $L_{e/2} = K_S^{(r+2)\mathfrak{p}}$ is a Hermitian function field. If e is odd and $p = 2$ or $p = 3$, then $K_S^{(r+p)\mathfrak{p}} = L_{(p-1)e,S}$ is optimal (cf. [S3]). There is also a connection with Deligne-Lusztig curves which has been elucidated by [La2]. The following equations have already been found by Pedersen [Ped] and Hansen and Stichtenoth [HS] in special cases (cf. also [GS1, GS2]).

8.9. Proposition. (a) *Assume that $r := \sqrt{q} \in \mathbb{N}$ and let $y, z \in \bar{K}$ satisfy $y^r + y = x^{r+1}$ and $z^q - z = x^{2r}(x^q - x)$. Then*

$$K_S^{(r+2)\infty} = K(y) \quad \text{and} \quad K_S^{(2r+2)\infty} = K(y, z).$$

(b) *Assume that $r := \sqrt{pq} \in \mathbb{N}$ and let $y_1, \dots, y_{p-1} \in \bar{K}$ satisfy $y_i^q - y_i = x^{ir/p}(x^q - x)$. Then*

$$K_S^{(r+i+1)\infty} = K(y_1, \dots, y_i) \quad \text{for} \quad i \in \{1, \dots, p-1\}.$$

Proof. Write $q = p^e$ with $e \in \mathbb{N}$ and let $\wp : \bar{K} \to \bar{K}$ be the Artin-Schreier operator as defined in Example 3.3. For $z \in \bar{K}$ and $\beta \in \mathbb{F}_q$, define $z^\beta := \sum_{j=0}^{e-1} (\beta z)^{p^j}$. Then, clearly,

$$\wp z^\beta = \beta(z^q - z). \tag{15}$$

(a) By [St2, p. 203], the extension $K(y)|K$ has degree r, and $S(K(y)|K)$ contains S. Define the $\mathbb{F}_p$-space $\Gamma := \{\gamma \in \mathbb{F}_q \,|\, \gamma^r + \gamma = 0\} = \{\beta^r - \beta \,|\, \beta \in \mathbb{F}_q\} \simeq \mathbb{F}_q/\mathbb{F}_r \simeq \mathbb{F}_r$ and set

$$y_\gamma := -\sum_{j=0}^{e/2-1} (\gamma y)^{p^j}$$

for $\gamma \in \Gamma$; then $\wp y_\gamma = -(\gamma y)^r + \gamma y = \gamma x^{r+1}$. Since $\Gamma x^{r+1} \cap \wp K = 0$, from 3.3 we can conclude $K(y) = K(y_\gamma \,|\, \gamma \in \Gamma)$ and $\mathfrak{f}(K(y)|K) = (r+2)\infty$. Hence $K_S^{(r+2)\infty} = K(y)$ by the characterization of the ray class fields in Proposition 5.5. For $\beta \in \mathbb{F}_q$ we have $\wp z^\beta = \beta x^{2r}(x^q - x) =: u_\beta$ by (15), and

$$t_\beta := \sum_{j=0}^{e/2-1} \left(\beta^r x^{r+2}\right)^{p^j}$$

satisfies $\wp t_\beta = \beta x^{q+2r} - \beta^r x^{r+2}$, implying $\tilde{u}_\beta := u_\beta - \wp t_\beta = \beta^r x^{r+2} - \beta x^{2r+1}$ and thus $v_\infty^*(u_\beta) = v_\infty(\tilde{u}_\beta) = -(2r+1)$ by 3.3(a). Because the $\mathbb{F}_p$-space

$$\tilde{V} := \Gamma x^{r+1} \oplus \{\tilde{u}_\beta \,|\, \beta \in \mathbb{F}_q\}$$

has rq elements and $\tilde{V} \cap \wp K = 0$, from 3.3(b)–(d) we obtain $K(y,z) = K(y_\gamma, z^\beta \,|\, \gamma \in \Gamma, \beta \in \mathbb{F}_q)$, $\mathfrak{f}(K(y,z)|K) = (2r+2)\infty$ and $S \subseteq S(K(y,z)|K)$. Therefore, again by 5.5, $K_S^{(2r+2)\infty} = K(y,z)$.

(b) Let $i \in \{1, \ldots, p-1\}$. Then $K_i := K(y_1, \ldots, y_i)$ has degree $[K_i : K] \le q^i$ over K. For $\beta \in \mathbb{F}_q$ we have $\wp y_i^\beta = \beta x^{ir/p}(x^q - x) =: u_{i\beta}$ by (15), and

$$t_{i\beta} := \sum_{j=0}^{(e-3)/2} \left(\beta^r x^{r+i}\right)^{p^j}$$

satisfies $\wp t_{i\beta} = \beta x^{q+ir/p} - \beta^r x^{r+i}$, implying $\tilde{u}_{i\beta} := u_{i\beta} - \wp t_{i\beta} = \beta^r x^{r+i} - \beta x^{ir/p+1}$ and thus $v_\infty^*(u_{i\beta}) = v_\infty(\tilde{u}_{i\beta}) = -(r+i)$ by 3.3(a). Since the $\mathbb{F}_p$-space

$$\tilde{V}_i := \{\tilde{u}_{j\beta} \,|\, 1 \le j \le i, \beta \in \mathbb{F}_q\}$$

has q^i elements and $\tilde{V}_i \cap \wp K = 0$, applying 3.3(b)–(d) shows that $K_i = K(y_j^\beta \,|\, 1 \le j \le i, \beta \in \mathbb{F}_q)$, $[K_i : K] = q^i$, $\mathfrak{f}(K_i|K) = (r+i+1)\infty$ and $S \subseteq S(K_i|K)$. Therefore $K_S^{(r+i+1)\infty} = K_i$ according to Proposition 5.5. □

9 Tables of Examples

Global function fields with many rational places have been constructed before by Serre [S2–S6], Hansen and Stichtenoth [Han, HS, St1], Wirtz [Wi], Schoof [Sf], van der Geer and van der Vlugt [GV1–GV7], Lauter [La1, La3], Niederreiter and Xing [XN,NX1–NX9], Shabat [Sh], Garcia, Stichtenoth and Xing [GSX, GS3], Doumen [Do], Özbudak and Stichtenoth [OS], and certainly many others. They use various methods, some of which are quite similar to the ones introduced in this work.

In this section we want to reproduce or, where possible, improve some of the known results by means of ray class field extensions. As a reference point we take the tables in [GV7] and consider function fields of genus up to 50 over $\mathbb{F}_q$ for $q \in \{2, 3, 4, 8, 9\}$. We refrain from also listing the results for larger values of q obtained in [Au] by employing a special method for determining the degrees of ray class fields over a rational function field, that we did not discuss here.

As before, we start with a global function field $K|\mathbb{F}_q$ of "small" genus g_K having "sufficiently" many rational places, which is given by an explicit equation. We choose a non-empty subset $S \subseteq \mathbb{P}_K^1$ and a place $\mathfrak{p} \in \mathbb{P}_K \setminus S$ and consider the intermediate fields L of $K_S^{m\mathfrak{p}}|K_S^{(m-1)\mathfrak{p}}$ for $m \in \mathbb{N}$. From Section 6 and Corollaries 2.2 and 5.9 we recall the formulas

$$h_S \operatorname{reg}_S = h_K, \tag{16}$$

$$\big[K_S^{\mathfrak{o}} : K\big] = h_S, \quad \big[K_S^{\mathfrak{p}} : K_S^{\mathfrak{o}}\big] = \frac{q^{\deg \mathfrak{p}} - 1}{(q-1)\delta_{S,\mathfrak{p}}^{(0)}}, \tag{17}$$

$$\big[K_S^{(m+1)\mathfrak{p}} : K_S^{m\mathfrak{p}}\big] = q^{\deg \mathfrak{p}}/p^{\delta_{S,\mathfrak{p}}^{(m)}} \quad \forall m \in \mathbb{N} \tag{18}$$

and

$$g_L = 1 + [L:K]\big(g_K - 1 + \tfrac{m}{2}\deg \mathfrak{p}\big) - \frac{1}{2}\sum_{n=0}^{m-1} [K_S^{n\mathfrak{p}} : K] \deg \mathfrak{p}. \tag{19}$$

By Theorem 5.8, the inertia degree of $\mathfrak{p}$ in L is $[K_S^{\mathfrak{o}} : K_{S\cup\{\mathfrak{p}\}}^{\mathfrak{o}}] = h_S/h_{S\cup\{\mathfrak{p}\}}$. Therefore L has

$$N_L \geq [L:K]\,|S| + \begin{cases} h_S & \text{if } h_S = h_{S\cup\{\mathfrak{p}\}} \text{ and } \deg \mathfrak{p} = 1 \\ 0 & \text{otherwise} \end{cases} \tag{20}$$

rational places, and equality holds iff $S = S(L|K) \cap \mathbb{P}_K^1$.

Now the computations are arranged as follows. First we calculate h_K via $P_K(t)$ by counting all places of K up to degree g_K. Next we "guess" S_0-units $u_1, \dots, u_s$ with $s = |S_0| - 1$, where S_0 is either equal to or (due to the specific equation for K) slightly larger than $\mathbb{P}_K^1$. We verify that the upper bound $\hbar_q(g_K, N_K)$ for h_{S_0} established in Proposition 7.6 is less than 2 and that $\operatorname{reg}\langle u_1, \dots, u_s\rangle = h_K$ and thereby prove $\mathcal{O}_{S_0}^* = \mathbb{F}_q^* \times \langle u_1, \dots, u_s\rangle$. By means of Remark 2.4, Lemma 2.3 and equation (16) we then obtain h_S and a $\mathbb{Z}$-basis of $\mathcal{O}_S^*/\mathbb{F}_q^*$ for any non-empty subset $S \subseteq \mathbb{P}_K^1$.

These calculations are performed automatically by a program written in KANT/KASH. Also the algorithms for computing S-descriptions discussed in Section 6 have been implemented in KASH. By (17), (18) and (19) we can then calculate the genera of the intermediate fields L. The program is in fact fast enough to run through all non-empty subsets S of $\mathbb{P}_K^1 \setminus \{\mathfrak{p}\}$, so that we can always take $S = S(L|K) \cap \mathbb{P}_K^1$ and achieve equality in (20).

The whole procedure is applied to several examples of ground fields $K|\mathbb{F}_q$, the results for each q being summarized in a corresponding $N_q(g)$-table. In each example, $K|\mathbb{F}_q$ is defined via an equation, in which x means an indeterminate over $\mathbb{F}_q$ and y is algebraic over $\mathbb{F}_q(x)$. Furthermore the relevant data of the ground field $K|\mathbb{F}_q$ are provided. These are the field invariants g_K, N_K and h_K, the set S_0 containing $\mathbb{P}_K^1$, a small table of S_0-units together with their valuations at all $\mathfrak{p} \in S_0$, the S_0-regulator and the bound $\hbar_q(g_K, N_K)$. While the rational places are specified by the table of S_0-units, other places $\mathfrak{p}$, which are possibly needed, are given in the form $\mathfrak{p} = (z_0, \dots)$, meaning that $\mathfrak{p}$ is the common zero of $z_0, \dots$ in $\mathbb{P}_K$. Finally the S-class numbers and S-descriptions leading to an entry in the corresponding $N_q(g)$-table are listed, each S being labelled with its cardinality $|S|$ and a small letter in parantheses.

Every $N_q(g)$-table is superscribed by the corresponding value of q. In its second column it provides a lower and an upper bound, connected by a hyphen, for the number $N_q(g)$ with g given in the first column, or a single value if these bounds coincide. Except for some cases in which explicit improvements have been achieved by Serre [S2–S5] or Lauter [La4], the upper bound is (the integer part of) the Oesterlé bound $\bar{N}_q(g)$; it is thereby the same as in the tables of [GV7]. The lower bound given here is always greater than or equal to the one in those tables, and it is realized by a certain field L of genus $g_L = g$ as outlined above. The last three columns give reference to how this field L is obtained. The column entitled "K,S" gives the number of the example, from which the ground field K is taken, and the label of a set S in this example satisfying $S = S(L|K) \cap \mathbb{P}_K^1$. The last column tells us the conductor of $L|K$ in the form $\mathfrak{f}(L|K) = m\mathfrak{p}$ with $\mathfrak{p} \in \mathbb{P}_K$ and $m \in \mathbb{N}_0$. Thus L is any intermediate

field of $K_S^{m\mathfrak{p}}|K_S^{(m-1)\mathfrak{p}}$ other than $K_S^{(m-1)\mathfrak{p}}$ (or of $K_S^{\mathfrak{o}}|K$ if $m=0$) having degree $[L:K]$ as given in the table's fourth column. The lower bound for $N_g(g)$ is set in boldface if our construction by ray class fields improves its previously known value. (Note that many of these improvements have already been added to the tables in [GV7]).

Examples for $q = 2$

9.1. Example. Let $K = \mathbb{F}_2(x)$ and consider the places $\mathfrak{p}_0 = (x)$, $\mathfrak{p}_1 = (x+1)$, $\mathfrak{p}_2 = (1/x)$, $\mathfrak{p}_3 = (x^2+x+1)$, $\mathfrak{p}_4 = (x^4+x+1)$ and $\mathfrak{p}_5 = (x^6+x^3+1)$ of K. The relevant S-class numbers and S-descriptions are given below.

(1a) $S = \{\mathfrak{p}_0\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_2} = 1$, $\delta_{S,\mathfrak{p}_4} = 1$.

(2a) $S = \{\mathfrak{p}_0, \mathfrak{p}_2\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_5} = 9 + t$.

(2b) $S = \{\mathfrak{p}_0, \mathfrak{p}_1\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_2} = 1 + t$.

(3a) $S = \{\mathfrak{p}_0, \mathfrak{p}_1, \mathfrak{p}_2\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_3} = 3 + 2t$.

9.2. Example. Let $K = \mathbb{F}_2(x,y)$ with $y^2 + y = (x^2+x)/(x^2+x+1)$. Then $g_K = 1$ and $N_K = 4$. The set $S_0 := \{\mathfrak{p}_0, \ldots, \mathfrak{p}_5\}$ and S_0-units $u_1, \ldots, u_5$ are given by the following table:

	$\mathfrak{p}_0$	$\mathfrak{p}_1$	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}_4$	$\mathfrak{p}_5$
$u_1 = x$	1	1	0	0	−1	0
$u_2 = x+1$	0	0	1	1	−1	0
$u_3 = x^2+x+1$	0	0	0	0	−2	2
$u_4 = y$	1	0	1	0	0	−1
$u_5 = y+x$	2	0	0	2	−1	−1

We have $\hbar_2(1,4) = 5/4 < 2$ and $\mathrm{reg}\langle u_1, \ldots, u_5\rangle = 4 = h_K$. Apart from the rational places also $\mathfrak{p}_4 = (1/x) \in \mathbb{P}_K^2$, $\mathfrak{p}_5 = (x^2+x+1) \in \mathbb{P}_K^2$ are used. The relevant S-class numbers and S-descriptions are given below.

(2a) $S = \{\mathfrak{p}_0, \mathfrak{p}_2\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_4} = 1 + t$.

9.3. Example. Let $K = \mathbb{F}_2(x,y)$ with $y^2 + y = x^3 + x$. Then $g_K = 1$ and $N_K = 5$. The set $S_0 := \{\mathfrak{p}_0, \ldots, \mathfrak{p}_4\}$ and S_0-units $u_1, \ldots, u_4$ are given by the following table:

	$\mathfrak{p}_0$	$\mathfrak{p}_1$	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}_4$
$u_1 = x$	1	1	0	0	−2
$u_2 = x+1$	0	0	1	1	−2
$u_3 = y$	1	0	2	0	−3
$u_4 = y+x$	2	0	0	1	−3

We have $\hbar_2(1,5) = 1$ and $\mathrm{reg}\langle u_1, \ldots, u_4\rangle = 5 = h_K$. Apart from the rational places also $\mathfrak{p}_5 = (x^3+x+1) \in \mathbb{P}_K^6$, $\mathfrak{p}_6 = (x^7+x+1, y+x^6+x^5+x^2+x) \in \mathbb{P}_K^7$ are used. The relevant S-class numbers and S-descriptions are given below.

(1a) $S = \{\mathfrak{p}_0\}$, $h_S = 5$, $\delta_{S,\mathfrak{p}_4} = 1$.

(5a) $S = \{\mathfrak{p}_0, \mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_5} = 63 + 4t$, $\delta_{S,\mathfrak{p}_6} = 127 + 4t$.

9.4. Example. Let $K|\mathbb{F}_2$ and $\mathfrak{p}_0, \ldots, \mathfrak{p}_4$ be as in Examples 1.7(a), 2.8 and 6.8. We recall that $g_K = 2$, $N_K = 5$ and $h_K = 13$. The relevant S-class numbers and S-descriptions are given below.

(3a) $S = \{\mathfrak{p}_0, \mathfrak{p}_1, \mathfrak{p}_2\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_4} = 1 + t^2 + t^5$.

9.5. Example. Let $K = \mathbb{F}_2(x, y)$ with $y^2 + y = (x^2 + x)/(x^3 + x + 1)$. Then $g_K = 2$ and $N_K = 6$. The set $S_0 := \{\mathfrak{p}_0, \ldots, \mathfrak{p}_6\}$ and S_0-units $u_1, \ldots, u_6$ are given by the following table:

	$\mathfrak{p}_0$	$\mathfrak{p}_1$	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}_4$	$\mathfrak{p}_5$	$\mathfrak{p}_6$
$u_1 = x$	1	1	0	0	−1	−1	0
$u_2 = x + 1$	0	0	1	1	−1	−1	0
$u_3 = x^3 + x + 1$	0	0	0	0	−3	−3	2
$u_4 = y$	1	0	1	0	1	0	−1
$u_5 = y + x$	2	0	0	3	−1	−1	−1
$u_6 = (x^3 + x + 1)y + 1$	0	4	0	1	−2	−3	0

We have $\hbar_2(2, 6) = (893 + 306\sqrt{2})/1262 < 2$ and $\mathrm{reg}\langle u_1, \ldots, u_6\rangle = 19 = h_K$. Apart from the rational places also $\mathfrak{p}_6 = (x^3 + x + 1) \in \mathbb{P}_K^3$ is used. The relevant S-class numbers and S-descriptions are given below.

(1a) $S = \{\mathfrak{p}_1\}$, $h_S = 19$.

(4a) $S = \{\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_4, \mathfrak{p}_5\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_0} = 1 + t + t^3 + t^7$.

(5a) $S = \{\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4, \mathfrak{p}_5\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_0} = 1 + t + t^3 + t^5 + t^7$.

9.6. Example. Let $K = \mathbb{F}_2(x, y)$ with $y^2 + y = (x^3 + x^2)/(x^6 + x^5 + x^3 + x + 1)$. Then $g_K = 3$ and $N_K = 6$. The set $S_0 := \{\mathfrak{p}_0, \ldots, \mathfrak{p}_6\}$ and S_0-units $u_1, \ldots, u_6$ are given by the following table:

	$\mathfrak{p}_0$	$\mathfrak{p}_1$	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}_4$	$\mathfrak{p}_5$	$\mathfrak{p}_6$
$u_1 = x$	1	1	0	0	−1	−1	0
$u_2 = x + 1$	0	0	1	1	−1	−1	0
$u_3 = x^2 + x + 1$	0	0	0	0	−2	−2	2
$u_4 = y$	2	0	1	0	3	0	−3
$u_5 = (x^2 + x + 1)y + 1$	0	1	0	3	0	−2	−1
$u_6 = (x^2 + x + 1)y + x^2$	3	0	0	2	−2	−1	−1

We have $\hbar_2(3, 6) = 195/146 < 2$ and $\mathrm{reg}\langle u_1, \ldots, u_6\rangle = 52 = h_K$. Apart from the rational places also $\mathfrak{p}_6 = (x^2 + x + 1) \in \mathbb{P}_K^2$, $\mathfrak{p}_7 = (x^3 + x^2 + 1) \in \mathbb{P}_K^6$ are used. The relevant S-class numbers and S-descriptions are given below.

(3a) $S = \{\mathfrak{p}_0, \mathfrak{p}_3, \mathfrak{p}_4\}$, $h_S = 4$, $\delta_{S,\mathfrak{p}_7} = 21 + 2t$.

(4a) $S = \{\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_0} = 1 + t + t^5 + t^9$.

9.7. Example. Let $K = \mathbb{F}_2(x, y)$ with $y^3 + (x^2 + x + 1)y^2 + (x^3 + x^2)y = x^2 + x$. Then $g_K = 3$ and $N_K = 7$. The set $S_0 := \{\mathfrak{p}_0, \ldots, \mathfrak{p}_6\}$ and S_0-units $u_1, \ldots, u_6$

are given by the following table:

	$\mathfrak{p}_0$	$\mathfrak{p}_1$	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}_4$	$\mathfrak{p}_5$	$\mathfrak{p}_6$
$u_1 = x$	2	1	0	0	−1	−1	−1
$u_2 = x+1$	0	0	2	1	−1	−1	−1
$u_3 = y$	1	0	1	0	1	−2	−1
$u_4 = y+1$	0	2	0	1	0	−2	−1
$u_5 = y+x$	1	0	0	2	−1	−2	0
$u_6 = y+x^2$	1	0	0	1	−2	2	−2

We have $\hbar_2(3,7) = 911/853 < 2$ and $\operatorname{reg}\langle u_1, \ldots, u_6\rangle = 71 = h_K$. The relevant S-class numbers and S-descriptions are given below.

(6a) $S = \{\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4, \mathfrak{p}_5, \mathfrak{p}_6\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_0} = 1 + t + t^3 + t^5 + t^7 + t^9$.

9.8. Example. Let $K = \mathbb{F}_2(x,y)$ with $y^4 + xy^2 + (x^3+x^2)y = x^7 + x^6 + x^5 + x^4$. Then $g_K = 4$ and $N_K = 8$. The set $S_0 := \{\mathfrak{p}_0, \ldots, \mathfrak{p}_7\}$ and S_0-units $u_1, \ldots, u_7$ are given by the following table:

	$\mathfrak{p}_0$	$\mathfrak{p}_1$	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}_4$	$\mathfrak{p}_5$	$\mathfrak{p}_6$	$\mathfrak{p}_7$
$u_1 = x$	1	1	2	0	0	0	0	−4
$u_2 = x+1$	0	0	0	1	1	1	1	−4
$u_3 = y$	2	1	1	2	0	1	0	−7
$u_4 = y+1$	0	0	0	0	1	0	6	−7
$u_5 = y+x^2$	3	1	1	0	1	0	2	−8
$u_6 = y^2+xy$	3	3	2	2	2	1	1	−14
$u_7 = y^2+xy+x^3+x^2$	2	2	2	1	1	3	3	−14

We have $\hbar_2(4,8) = 1571/1472 < 2$ and $\operatorname{reg}\langle u_1, \ldots, u_7\rangle = 260 = h_K$. The relevant S-class numbers and S-descriptions are given below.

(4a) $S = \{\mathfrak{p}_3, \mathfrak{p}_4, \mathfrak{p}_5, \mathfrak{p}_6\}$, $h_S = 1$, $\delta_{S,p_7} = 1 + t^3 + t^4 + t^9$.

(6a) $S = \{\mathfrak{p}_0, \mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_4, \mathfrak{p}_5, \mathfrak{p}_6\}$, $h_S = 1$, $\delta_{S,p_3} = 1 + t + t^3 + t^5 + t^7 + t^{13}$.

(7a) $S = \{\mathfrak{p}_0, \mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_4, \mathfrak{p}_5, \mathfrak{p}_6, \mathfrak{p}_7\}$, $h_S = 1$, $\delta_{S,p_3} = 1+t+t^3+t^5+t^7+t^9+t^{13}$.

9.9. Example. Let $K = \mathbb{F}_2(x,y)$ with $y^4 + (x^2+x+1)y^2 + (x^2+x)y = x^7 + x^6 + x^5 + x^4$. Then $g_K = 5$ and $N_K = 9$. The set $S_0 := \{\mathfrak{p}_0, \ldots, \mathfrak{p}_8\}$ and S_0-units $u_1, \ldots, u_8$ are given by the following table:

	$\mathfrak{p}_0$	$\mathfrak{p}_1$	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}_4$	$\mathfrak{p}_5$	$\mathfrak{p}_6$	$\mathfrak{p}_7$	$\mathfrak{p}_8$
$u_1 = x$	1	1	1	1	0	0	0	0	−4
$u_2 = x+1$	0	0	0	0	1	1	1	1	−4
$u_3 = y$	3	0	1	0	2	0	1	0	−7
$u_4 = y+x$	1	0	3	0	0	1	0	2	−7
$u_5 = y^2+y$	3	3	1	1	2	2	1	1	−14
$u_6 = y^2+y+x^3+x^2$	2	2	1	1	1	1	3	3	−14
$u_7 = y^2+(x^2+x+1)y$	3	1	1	2	2	1	1	4	−15
$u_8 = y^2+(x^2+x+1)y+x^3+x^2$	2	1	1	3	1	4	2	1	−15

We have $\hbar_2(5,9) = \frac{24230319+1494360\sqrt{2}}{24972319} < 2$ and $\operatorname{reg}\langle u_1, \ldots, u_8\rangle = 975 = h_K$. The relevant S-class numbers and S-descriptions are given below.

(7a) $S = \{\mathfrak{p}_1, \mathfrak{p}_3, \mathfrak{p}_4, \mathfrak{p}_5, \mathfrak{p}_6, \mathfrak{p}_7, \mathfrak{p}_8\}$, $h_S = 1$, $\delta_{S,p_0} = 1+t+t^3+t^5+t^7+t^9+t^{15}$.

(8a) $S = \{\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4, \mathfrak{p}_5, \mathfrak{p}_6, \mathfrak{p}_7, \mathfrak{p}_8\}$, $h_S = 1$, $\delta_{S,p_0} = 1+t+t^3+t^5+t^7+t^9+t^{11}+t^{15}$.

The outgrowth of Examples 9.1–9.9 is gathered in the table below.

$q=2$				
g	$N_2(g)$	K, S	$[L:K]$	$\mathfrak{f}(L\|K)$
6	10	9.3(1a)	10	$2\mathfrak{p}_4$
7	10	9.3(5a)	2	$2\mathfrak{p}_5$
8	11	9.5(5a)	2	$10\mathfrak{p}_0$
9	12	9.1(3a)	4	$4\mathfrak{p}_3$
10	13	9.4(3a)	4	$4\mathfrak{p}_0$
12	14–15	9.1(2a)	7	$\mathfrak{p}_5$
14	15–16	9.1(1a)	15	$\mathfrak{p}_4$
15	17	9.1(2b)	8	$7\mathfrak{p}_2$
16	**17**–18	9.9(8a)	2	$14\mathfrak{p}_0$
17	17–18	9.1(1a)	16	$5\mathfrak{p}_2$
19	20	9.3(5a)	4	$2\mathfrak{p}_5$
20	19–21	9.5(1a)	19	$\mathfrak{o}$

g	$N_2(g)$	K, S	$[L:K]$	$\mathfrak{f}(L\|K)$
22	21–22	9.5(5a)	4	$12\mathfrak{p}_0$
27	**24**–25	9.2(2a)	12	$3\mathfrak{p}_4$
28	**25**–26	9.4(3a)	8	$7\mathfrak{p}_0$
29	25–27	9.7(6a)	4	$14\mathfrak{p}_0$
30	**25**–27	9.8(6a)	4	$12\mathfrak{p}_3$
35	**29**–31	9.8(7a)	4	$16\mathfrak{p}_3$
37	**29**–32	9.9(7a)	4	$14\mathfrak{p}_0$
39	33	9.1(2b)	16	$8\mathfrak{p}_2$
41	**33**–35	9.8(4a)	8	$6\mathfrak{p}_7$
42	**33**–35	9.6(4a)	8	$8\mathfrak{p}_0$
44	**33**–37	9.5(4a)	8	$11\mathfrak{p}_0$
49	36–40	9.6(3a)	12	$\mathfrak{p}_7$
50	40	9.3(5a)	8	$2\mathfrak{p}_6$

Examples for $q = 3$

9.10. Example. Let $K = \mathbb{F}_3(x)$ and consider the places $\mathfrak{p}_0 = (x)$, $\mathfrak{p}_1 = (x-1)$, $\mathfrak{p}_2 = (x+1)$, $\mathfrak{p}_3 = (1/x)$, $\mathfrak{p}_4 = (x^2+1)$ and $\mathfrak{p}_5 = (x^4 - x^3 + x^2 + 1)$ of K. The relevant S-class numbers and S-descriptions are given below.

(2a) $S = \{\mathfrak{p}_0, \mathfrak{p}_2\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_5} = 5 + t$.

(2b) $S = \{\mathfrak{p}_0, \mathfrak{p}_1\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_3} = 1 + t$.

(3a) $S = \{\mathfrak{p}_0, \mathfrak{p}_1, \mathfrak{p}_2\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_3} = 1 + t + t^2$, $\delta_{S,\mathfrak{p}_4} = 4 + 2t$.

9.11. Example. Let $K = \mathbb{F}_3(x, y)$ with $y^2 = x^3 + x^2 - x$. Then $g_K = 1$ and $N_K = 6$. The set $S_0 := \{\mathfrak{p}_0, \ldots, \mathfrak{p}_5\}$ and S_0-units $u_1, \ldots, u_5$ are given by the following table:

	$\mathfrak{p}_0$	$\mathfrak{p}_1$	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}_4$	$\mathfrak{p}_5$
$u_1 = x$	2	0	0	0	0	−2
$u_2 = x - 1$	0	1	1	0	0	−2
$u_3 = x + 1$	0	0	0	1	1	−2
$u_4 = y - 1$	0	0	1	0	2	−3
$u_5 = y - x$	1	0	1	1	0	−3

We have $\hbar_3(1,6) = 7/6 < 2$ and $\operatorname{reg}\langle u_1, \ldots, u_5\rangle = 6 = h_K$. Apart from the rational places also $\mathfrak{p}_6 = (x^2 - x - 1, y + x - 1) \in \mathbb{P}_K^2$ is used. The relevant S-class numbers and S-descriptions are given below.

(2a) $S = \{\mathfrak{p}_0, \mathfrak{p}_4\}$, $h_S = 2$, $\delta_{S,\mathfrak{p}_6} = 1 + t$.

(3a) $S = \{\mathfrak{p}_0, \mathfrak{p}_3, \mathfrak{p}_4\}$, $h_S = 2$, $\delta_{S,\mathfrak{p}_6} = 4 + t + t^2$.

(3b) $S = \{\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_5\}$, $h_S = 2$, $\delta_{S,\mathfrak{p}_0} = 1 + t + t^2$.

(4a) $S = \{\mathfrak{p}_0, \mathfrak{p}_1, \mathfrak{p}_3, \mathfrak{p}_4\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_6} = 4 + t + 2t^2$.

(4b) $S = \{\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_0} = 1 + t + t^2 + t^5$.

(5a) $S = \{\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4, \mathfrak{p}_5\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_0} = 1 + t + t^2 + t^4 + t^5$.

9.12. Example. Let $K = \mathbb{F}_3(x, y)$ with $y^2 = x^3 - x + 1$. Then $g_K = 1$ and $N_K = 7$. The set $S_0 := \{\mathfrak{p}_0, \ldots, \mathfrak{p}_6\}$ and S_0-units $u_1, \ldots, u_6$ are given by the following table:

	$\mathfrak{p}_0$	$\mathfrak{p}_1$	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}_4$	$\mathfrak{p}_5$	$\mathfrak{p}_6$
$u_1 = x$	1	1	0	0	0	0	−2
$u_2 = x - 1$	0	0	1	1	0	0	−2
$u_3 = x + 1$	0	0	0	0	1	1	−2
$u_4 = y - 1$	0	1	0	1	0	1	−3
$u_5 = y - x$	0	0	0	2	1	0	−3
$u_6 = y - x - 1$	0	2	1	0	0	0	−3

We have $\hbar_3(1, 7) = 1$ and $\mathrm{reg}\langle u_1, \ldots, u_6\rangle = 7 = h_K$. Apart from the rational places also $\mathfrak{p}_7 = (x^3 - x + 1) \in \mathbb{P}_K^3$, $\mathfrak{p}_8 = (x^2 + 1) \in \mathbb{P}_K^4$ are used. The relevant S-class numbers and S-descriptions are given below.

(5a) $S = \{\mathfrak{p}_0, \mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_6\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_7} = 13 + 2t + 2t^2$.

(6a) $S = \{\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4, \mathfrak{p}_5, \mathfrak{p}_6\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_0} = 1 + t + t^2 + t^4 + t^5 + t^7$.

(7a) $S = \{\mathfrak{p}_0, \mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4, \mathfrak{p}_5, \mathfrak{p}_6\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_8} = 40 + 4t + 2t^2$.

9.13. Example. Let $K = \mathbb{F}_3(x, y)$ with $y^2 = x^6 - x^2 + 1$. Then $g_K = 2$ and $N_K = 8$. The set $S_0 := \{\mathfrak{p}_0, \ldots, \mathfrak{p}_7\}$ and S_0-units $u_1, \ldots, u_7$ are given by the following table:

	$\mathfrak{p}_0$	$\mathfrak{p}_1$	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}_4$	$\mathfrak{p}_5$	$\mathfrak{p}_6$	$\mathfrak{p}_7$
$u_1 = x$	1	1	0	0	0	0	−1	−1
$u_2 = x - 1$	0	0	1	1	0	0	−1	−1
$u_3 = x + 1$	0	0	0	0	1	1	−1	−1
$u_4 = y - x^3$	0	0	0	1	1	0	−3	1
$u_5 = y - x^3 - 1$	0	2	1	0	0	0	−3	0
$u_6 = y - x^3 + 1$	2	0	0	0	0	1	−3	0
$u_7 = y + x^3 - x + 1$	1	0	2	0	1	0	−1	−3

We have $\hbar_3(2, 8) = 13/11 < 2$ and $\mathrm{reg}\langle u_1, \ldots, u_7\rangle = 35 = h_K$. Apart from the rational places also $\mathfrak{p}_8 = (x^2 + 1, y + 1) \in \mathbb{P}_K^2$ is used. The relevant S-class numbers and S-descriptions are given below.

(2a) $S = \{\mathfrak{p}_2, \mathfrak{p}_4\}$, $h_S = 7$, $\delta_{S,\mathfrak{p}_8} = 1 + t$.

9.14. Example. Let $K = \mathbb{F}_3(x, y)$ with $y^3 - y = (x^2 - 1)/x$. Then $g_K = 2$ and $N_K = 8$. The set $S_0 := \{\mathfrak{p}_0, \ldots, \mathfrak{p}_7\}$ and S_0-units $u_1, \ldots, u_7$ are given by the following table:

	$\mathfrak{p}_0$	$\mathfrak{p}_1$	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}_4$	$\mathfrak{p}_5$	$\mathfrak{p}_6$	$\mathfrak{p}_7$
$u_1 = x$	3	0	0	0	0	0	0	−3
$u_2 = x - 1$	0	1	1	1	0	0	0	−3
$u_3 = x + 1$	0	0	0	0	1	1	1	−3
$u_4 = y$	−1	1	0	0	1	0	0	−1
$u_5 = y - 1$	−1	0	0	1	0	1	0	−1
$u_6 = xy + 1$	0	0	2	0	0	2	0	−4
$u_7 = xy + x + 1$	0	0	0	2	2	0	0	−4

We have $\hbar_3(2,8) = 13/11 < 2$ and $\operatorname{reg}\langle u_1,\dots,u_7\rangle = 36 = h_K$. Apart from the rational places also $\mathfrak{p}_8 = (x^2+1, xy-1) \in \mathbb{P}^2_K$ is used. The relevant S-class numbers and S-descriptions are given below.

(2a) $S = \{\mathfrak{p}_1, \mathfrak{p}_4\}$, $h_S = 12$, $\delta_{S,\mathfrak{p}_8} = 2 + t$.

(4a) $S = \{\mathfrak{p}_1, \mathfrak{p}_3, \mathfrak{p}_4, \mathfrak{p}_5\}$, $h_S = 2$, $\delta_{S,\mathfrak{p}_7} = 1 + t + t^2 + t^7$.

(6a) $S = \{\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4, \mathfrak{p}_5, \mathfrak{p}_6\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_7} = 1 + t + t^2 + t^5 + t^7 + t^8$.

(8a) $S = \{\mathfrak{p}_0, \mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4, \mathfrak{p}_5, \mathfrak{p}_6, \mathfrak{p}_7\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_8} = 4 + 2t + 2t^2 + t^4 + 2t^5$.

9.15. Example. Let $K = \mathbb{F}_3(x,y)$ with $y^3 - y = x^4 - x^2$. Then $g_K = 3$ and $N_K = 10$. The set $S_0 := \{\mathfrak{p}_0,\dots,\mathfrak{p}_9\}$ and S_0-units $u_1,\dots,u_9$ are given by the following table:

	$\mathfrak{p}_0$	$\mathfrak{p}_1$	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}_4$	$\mathfrak{p}_5$	$\mathfrak{p}_6$	$\mathfrak{p}_7$	$\mathfrak{p}_8$	$\mathfrak{p}_9$
$u_1 = x$	1	1	1	0	0	0	0	0	0	−3
$u_2 = x-1$	0	0	0	1	1	1	0	0	0	−3
$u_3 = x+1$	0	0	0	0	0	0	1	1	1	−3
$u_4 = y$	2	0	0	1	0	0	1	0	0	−4
$u_5 = y-1$	0	0	2	0	0	1	0	0	1	−4
$u_6 = y-x$	1	0	0	0	0	2	0	1	0	−4
$u_7 = y-x-1$	0	0	1	0	2	0	1	0	0	−4
$u_8 = y+x$	1	0	0	0	1	0	0	0	2	−4
$u_9 = y+x-1$	0	0	1	1	0	0	0	2	0	−4

We have $\hbar_3(3,10) = (2414+270\sqrt{3})/2531 < 2$ and $\operatorname{reg}\langle u_1,\dots,u_9\rangle = 196 = h_K$. Apart from the rational places also $\mathfrak{p}_{10} = (x^5+x^4-1, y+x^4+x^3+x) \in \mathbb{P}^5_K$ is used. The relevant S-class numbers and S-descriptions are given below.

(5a) $S = \{\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_5, \mathfrak{p}_8, \mathfrak{p}_9\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_0} = 1 + t^2 + t^4 + t^5 + t^{10}$.

(9a) $S = \{\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4, \mathfrak{p}_5, \mathfrak{p}_6, \mathfrak{p}_7, \mathfrak{p}_8, \mathfrak{p}_9\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_0} = 1 + t + t^2 + t^4 + t^5 + t^7 + t^8 + t^{10} + t^{14}$.

(10a) $S = \{\mathfrak{p}_0, \mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4, \mathfrak{p}_5, \mathfrak{p}_6, \mathfrak{p}_7, \mathfrak{p}_8, \mathfrak{p}_9\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_{10}} = 121 + 5t + 4t^2$.

9.16. Example. Let $K = \mathbb{F}_3(x,y)$ with $y^3 - y = (x^3-x)/(x^4-x^2+1)$. Then $g_K = 4$ and $N_K = 12$. The set $S_0 := \{\mathfrak{p}_0,\dots,\mathfrak{p}_{12}\}$ and S_0-units $u_1,\dots,u_{12}$ are given by the following table:

	$\mathfrak{p}_0$	$\mathfrak{p}_1$	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}_4$	$\mathfrak{p}_5$	$\mathfrak{p}_6$	$\mathfrak{p}_7$	$\mathfrak{p}_8$	$\mathfrak{p}_9$	$\mathfrak{p}_{10}$	$\mathfrak{p}_{11}$	$\mathfrak{p}_{12}$
$u_1 = x$	1	1	1	0	0	0	0	0	0	−1	−1	−1	0
$u_2 = x-1$	0	0	0	1	1	1	0	0	0	−1	−1	−1	0
$u_3 = x+1$	0	0	0	0	0	0	1	1	1	−1	−1	−1	0
$u_4 = x^2+1$	0	0	0	0	0	0	0	0	0	−2	−2	−2	3
$u_5 = y$	1	0	0	1	0	0	1	0	0	1	0	0	−2
$u_6 = y-1$	0	0	1	0	1	0	0	1	0	0	0	1	−2
$u_7 = y-x$	3	0	0	0	2	0	0	0	2	−1	−1	−1	−2
$u_8 = y-x-1$	0	0	3	0	0	2	2	0	0	−1	−1	−1	−2
$u_9 = (x^2+1)y+1$	0	1	0	0	1	0	0	3	0	−1	−2	−2	0
$u_{10} = (x^2+1)y-x^2$	1	0	0	0	0	1	0	0	3	−2	−2	−1	0
$u_{11} = (x^2+1)y-x$	3	0	0	0	0	1	0	1	0	−1	−2	−2	0
$u_{12} = (x^2+1)y-x^2-x-1$	0	0	3	1	0	0	0	0	1	−2	−2	−1	0

We have $\hbar_3(4,12) = (610+120\sqrt{3})/759 < 2$ and $\operatorname{reg}\langle u_1,\dots,u_{12}\rangle = 1225 = h_K$. Apart from the rational places also $\mathfrak{p}_{12} = (x^2+1) \in \mathbb{P}_K^2$ is used. The relevant S-class numbers and S-descriptions are given below.

(10a) $S = \{\mathfrak{p}_1,\mathfrak{p}_2,\mathfrak{p}_3,\mathfrak{p}_4,\mathfrak{p}_5,\mathfrak{p}_7,\mathfrak{p}_8,\mathfrak{p}_9,\mathfrak{p}_{10},\mathfrak{p}_{11}\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_0} = 1+t+t^2+t^4+t^5+t^7+t^8+t^{10}+t^{11}+t^{14}$.

The outgrowth of Examples 9.10–9.16 is gathered in the table below.

$q=3$				
g	$N_3(g)$	K, S	$[L:K]$	$\mathfrak{f}(L\|K)$
5	12–13	9.11(4a)	3	$2\mathfrak{p}_6$
7	16	9.10(2a)	8	$\mathfrak{p}_5$
9	19	9.14(6a)	3	$5\mathfrak{p}_7$
10	19–21	9.10(2b)	9	$5\mathfrak{p}_3$
13	24–25	9.14(2a)	12	$\mathfrak{o}$
14	24–26	9.14(8a)	3	$5\mathfrak{p}_8$
15	28	9.10(3a)	9	$6\mathfrak{p}_3$
16	27–29	9.10(3a)	9	$3\mathfrak{p}_4$
17	24–30	9.14(4a)	6	$5\mathfrak{p}_7$
19	28–32	9.15(9a)	3	$12\mathfrak{p}_0$
22	30–36	9.15(10a)	3	$3\mathfrak{p}_{10}$
24	**31**–38	9.16(10a)	3	$14\mathfrak{p}_0$

g	$N_3(g)$	K, S	$[L:K]$	$\mathfrak{f}(L\|K)$
30	37–46	9.11(4b)	9	$8\mathfrak{p}_0$
33	**46**–49	9.15(5a)	9	$4\mathfrak{p}_0$
34	**45**–50	9.12(5a)	9	$3\mathfrak{p}_7$
36	46–52	9.11(5a)	9	$9\mathfrak{p}_0$
37	48–54	9.14(2a)	24	$\mathfrak{p}_8$
39	**48**–56	9.11(2a)	24	$2\mathfrak{p}_6$
43	55–60	9.12(6a)	9	$11\mathfrak{p}_0$
45	**54**–62	9.11(3a)	18	$3\mathfrak{p}_6$
46	55–63	9.10(2b)	27	$6\mathfrak{p}_3$
47	**54**–65	9.11(3b)	18	$6\mathfrak{p}_0$
48	55–66	9.14(6a)	9	$11\mathfrak{p}_7$
49	63–67	9.12(7a)	9	$3\mathfrak{p}_8$
50	56–68	9.13(2a)	28	$\mathfrak{p}_8$

Examples for $q = 4$

Let α be the multiplicative generator of $\mathbb{F}_4^*$ satisfying $\alpha^2 = \alpha + 1$.

9.17. Example. Let $K = \mathbb{F}_4(x)$ and consider the places $\mathfrak{p}_0 = (x)$, $\mathfrak{p}_1 = (x+1)$, $\mathfrak{p}_2 = (x+\alpha)$, $\mathfrak{p}_3 = (x+\alpha^2)$, $\mathfrak{p}_4 = (1/x)$, $\mathfrak{p}_5 = (x^2+x+\alpha)$ and $\mathfrak{p}_6 = (x^3+\alpha)$ of K. The relevant S-class numbers and S-descriptions are given below.

(3a) $S = \{\mathfrak{p}_0,\mathfrak{p}_1,\mathfrak{p}_2\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_4} = 1+2t$.

(3b) $S = \{\mathfrak{p}_1,\mathfrak{p}_2,\mathfrak{p}_3\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_6} = 7+2t$.

(4a) $S = \{\mathfrak{p}_0,\mathfrak{p}_1,\mathfrak{p}_2,\mathfrak{p}_3\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_4} = 1+2t+t^3$, $\delta_{S,\mathfrak{p}_6} = 21+3t$.

(5a) $S = \{\mathfrak{p}_0,\mathfrak{p}_1,\mathfrak{p}_2,\mathfrak{p}_3,\mathfrak{p}_4\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_5} = 5+4t$, $\delta_{S,\mathfrak{p}_6} = 21+4t$.

9.18. Example. Let $K = \mathbb{F}_4(x,y)$ with $y^2+y = x^2/(x+1)$. Then $g_K = 1$ and $N_K = 8$. The set $S_0 := \{\mathfrak{p}_0,\dots,\mathfrak{p}_7\}$ and S_0-units $u_1,\dots,u_7$ are given by the following table:

	$\mathfrak{p}_0$	$\mathfrak{p}_1$	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}_4$	$\mathfrak{p}_5$	$\mathfrak{p}_6$	$\mathfrak{p}_7$
$u_1 = x$	1	1	0	0	0	0	0	−2
$u_2 = x + 1$	0	0	2	0	0	0	0	−2
$u_3 = x + \alpha$	0	0	0	1	1	0	0	−2
$u_4 = x + \alpha^2$	0	0	0	0	0	1	1	−2
$u_5 = y$	2	0	−1	0	0	0	0	−1
$u_6 = y + \alpha$	0	0	−1	1	0	0	1	−1
$u_7 = y + x$	1	0	−1	1	0	1	0	−2

We have $\hbar_4(1, 8) = 9/8 < 2$ and $\operatorname{reg}\langle u_1, \ldots, u_7\rangle = 8 = h_K$. The relevant S-class numbers and S-descriptions are given below.

(3a) $S = \{\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_7\}$, $h_S = 2$, $\delta_{S,\mathfrak{p}_0} = 1 + t + t^3$.

(7a) $S = \{\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4, \mathfrak{p}_5, \mathfrak{p}_6, \mathfrak{p}_7\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_0} = 1 + 2t + 2t^3 + t^5 + t^7$.

9.19. Example. Let $K = \mathbb{F}_4(x, y)$ with $y^2 + y = x^3$. Then $g_K = 1$ and $N_K = 9$. The set $S_0 := \{\mathfrak{p}_0, \ldots, \mathfrak{p}_8\}$ and S_0-units $u_1, \ldots, u_8$ are given by the following table:

	$\mathfrak{p}_0$	$\mathfrak{p}_1$	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}_4$	$\mathfrak{p}_5$	$\mathfrak{p}_6$	$\mathfrak{p}_7$	$\mathfrak{p}_8$
$u_1 = x$	1	1	0	0	0	0	0	0	−2
$u_2 = x + 1$	0	0	1	1	0	0	0	0	−2
$u_3 = x + \alpha$	0	0	0	0	1	1	0	0	−2
$u_4 = x + \alpha^2$	0	0	0	0	0	0	1	1	−2
$u_5 = y$	3	0	0	0	0	0	0	0	−3
$u_6 = y + \alpha$	0	0	1	0	1	0	1	0	−3
$u_7 = y + x$	1	0	0	0	1	0	0	1	−3
$u_8 = y + \alpha x$	1	0	1	0	0	1	0	0	−3

We have $\hbar_4(1, 9) = 1$ and $\operatorname{reg}\langle u_1, \ldots, u_8\rangle = 9 = h_K$. The relevant S-class numbers and S-descriptions are given below.

(2a) $S = \{\mathfrak{p}_0, \mathfrak{p}_1\}$, $h_S = 3$, $\delta_{S,\mathfrak{p}_8} = 1 + t^3$.

9.20. Example. Let $K = \mathbb{F}_4(x, y)$ with $y^2 + y = x^5 + x^4$. Then $g_K = 2$ and $N_K = 9$. The set $S_0 := \{\mathfrak{p}_0, \ldots, \mathfrak{p}_8\}$ and S_0-units $u_1, \ldots, u_8$ are given by the following table:

	$\mathfrak{p}_0$	$\mathfrak{p}_1$	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}_4$	$\mathfrak{p}_5$	$\mathfrak{p}_6$	$\mathfrak{p}_7$	$\mathfrak{p}_8$
$u_1 = x$	1	1	0	0	0	0	0	0	−2
$u_2 = x + 1$	0	0	1	1	0	0	0	0	−2
$u_3 = x + \alpha$	0	0	0	0	1	1	0	0	−2
$u_4 = x + \alpha^2$	0	0	0	0	0	0	1	1	−2
$u_5 = y$	4	0	1	0	0	0	0	0	−5
$u_6 = y + x$	1	0	0	2	1	0	0	1	−5
$u_7 = y + x^2$	2	0	0	1	0	1	1	0	−5
$u_8 = y + \alpha x^3$	3	0	0	0	1	0	2	0	−6

We have $\hbar_4(2, 9) = 57/41 < 2$ and $\operatorname{reg}\langle u_1, \ldots, u_8\rangle = 45 = h_K$. The relevant S-class numbers and S-descriptions are given below.

(4a) $S = \{\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_8\}$, $h_S = 3$, $\delta_{S,\mathfrak{p}_0} = 1 + t + t^3 + t^5$.

9.21. Example. Let $K = \mathbb{F}_4(x, y)$ with $y^2 + y = x/(x^3 + x + 1)$. Then $g_K = 2$ and $N_K = 10$. The set $S_0 := \{\mathfrak{p}_0, \ldots, \mathfrak{p}_{10}\}$ and S_0-units $u_1, \ldots, u_{10}$ are given

by the following table:

	$\mathfrak{p}_0$	$\mathfrak{p}_1$	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}_4$	$\mathfrak{p}_5$	$\mathfrak{p}_6$	$\mathfrak{p}_7$	$\mathfrak{p}_8$	$\mathfrak{p}_9$	$\mathfrak{p}_{10}$
$u_1 = x$	1	1	0	0	0	0	0	0	−1	−1	0
$u_2 = x + 1$	0	0	1	1	0	0	0	0	−1	−1	0
$u_3 = x + \alpha$	0	0	0	0	1	1	0	0	−1	−1	0
$u_4 = x + \alpha^2$	0	0	0	0	0	0	1	1	−1	−1	0
$u_5 = x^3 + x + 1$	0	0	0	0	0	0	0	0	−3	−3	2
$u_6 = y$	1	0	0	0	0	0	0	0	2	0	−1
$u_7 = y + \alpha$	0	0	1	0	0	1	1	0	0	0	−1
$u_8 = y + x$	3	0	0	0	0	1	0	1	−1	−1	−1
$u_9 = (x^3 + x + 1)y + \alpha$	0	0	1	0	0	0	0	3	−1	−3	0
$u_{10} = (x^3 + x + 1)y + x^2$	1	0	0	0	0	2	0	2	−2	−3	0

We have $\hbar_4(2, 10) = 41/34 < 2$ and $\operatorname{reg}\langle u_1, \ldots, u_{10}\rangle = 55 = h_K$. Apart from the rational places also $\mathfrak{p}_{10} = (x^3 + x + 1) \in \mathbb{P}^3_K$ is used. The relevant S-class numbers and S-descriptions are given below.

(3a) $S = \{\mathfrak{p}_1, \mathfrak{p}_8, \mathfrak{p}_9\}$, $h_S = 5$, $\delta_{S,\mathfrak{p}_0} = 1 + t + t^5$.

(4a) $S = \{\mathfrak{p}_0, \mathfrak{p}_1, \mathfrak{p}_8, \mathfrak{p}_9\}$, $h_S = 5$, $\delta_{S,\mathfrak{p}_{10}} = 7 + 2t + t^2$.

(7a) $S = \{\mathfrak{p}_0, \mathfrak{p}_1, \mathfrak{p}_3, \mathfrak{p}_4, \mathfrak{p}_5, \mathfrak{p}_6, \mathfrak{p}_7\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_2} = 1 + 2t + t^3 + 2t^5 + t^7$.

(8a) $S = \{\mathfrak{p}_0, \mathfrak{p}_1, \mathfrak{p}_4, \mathfrak{p}_5, \mathfrak{p}_6, \mathfrak{p}_7, \mathfrak{p}_8, \mathfrak{p}_9\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_{10}} = 21 + 4t + t^2 + 2t^3$.

(9a) $S = \{\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4, \mathfrak{p}_5, \mathfrak{p}_6, \mathfrak{p}_7, \mathfrak{p}_8, \mathfrak{p}_9\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_0} = 1 + 2t + 2t^3 + 2t^5 + t^7 + t^9$.

9.22. Example. Let $K = \mathbb{F}_4(x, y)$ with $y^4 + y = x^3 + x^2 + x$. Then $g_K = 3$ and $N_K = 13$. The set $S_0 := \{\mathfrak{p}_0, \ldots, \mathfrak{p}_{12}\}$ and S_0-units $u_1, \ldots, u_{12}$ are given by the following table:

	$\mathfrak{p}_0$	$\mathfrak{p}_1$	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}_4$	$\mathfrak{p}_5$	$\mathfrak{p}_6$	$\mathfrak{p}_7$	$\mathfrak{p}_8$	$\mathfrak{p}_9$	$\mathfrak{p}_{10}$	$\mathfrak{p}_{11}$	$\mathfrak{p}_{12}$
$u_1 = x$	1	1	1	1	0	0	0	0	0	0	0	0	−4
$u_2 = x + \alpha$	0	0	0	0	1	1	1	1	0	0	0	0	−4
$u_3 = x + \alpha^2$	0	0	0	0	0	0	0	0	1	1	1	1	−4
$u_4 = y$	1	0	0	0	1	0	0	0	1	0	0	0	−3
$u_5 = y + 1$	0	1	0	0	0	1	0	0	0	1	0	0	−3
$u_6 = y + \alpha$	0	0	1	0	0	0	1	0	0	0	1	0	−3
$u_7 = y + x$	2	0	0	0	0	0	1	0	0	0	0	1	−4
$u_8 = y + x + 1$	0	2	0	0	0	0	0	1	0	0	1	0	−4
$u_9 = y + x + \alpha$	0	0	2	0	1	0	0	0	0	1	0	0	−4
$u_{10} = y + \alpha x$	1	0	0	0	0	0	0	2	0	1	0	0	−4
$u_{11} = y + \alpha x + 1$	0	1	0	0	0	0	2	0	1	0	0	0	−4
$u_{12} = y + \alpha x + \alpha$	0	0	1	0	0	2	0	0	0	0	0	1	−4

We have $\hbar_4(3, 13) = 183/163 < 2$ and $\operatorname{reg}\langle u_1, \ldots, u_{12}\rangle = 441 = h_K$. Apart from the rational places also $\mathfrak{p}_{13} = (x^3 + x^2 + 1, y + x^2 + x) \in \mathbb{P}^3_K$ is used. The relevant S-class numbers and S-descriptions are given below.

(10a) $S = \{\mathfrak{p}_1, \mathfrak{p}_4, \mathfrak{p}_5, \mathfrak{p}_6, \mathfrak{p}_7, \mathfrak{p}_8, \mathfrak{p}_9, \mathfrak{p}_{10}, \mathfrak{p}_{11}, \mathfrak{p}_{12}\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_0} = 1 + 2t + 2t^3 + t^5 + 2t^7 + t^9 + t^{11}$.

(10b) $S = \{\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4, \mathfrak{p}_6, \mathfrak{p}_7, \mathfrak{p}_8, \mathfrak{p}_{10}, \mathfrak{p}_{11}, \mathfrak{p}_{12}\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_0} = 1 + 2t + 2t^3 + 2t^5 + 2t^9 + t^{11}$.

(13a) $S = \{\mathfrak{p}_0, \mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4, \mathfrak{p}_5, \mathfrak{p}_6, \mathfrak{p}_7, \mathfrak{p}_8, \mathfrak{p}_9, \mathfrak{p}_{10}, \mathfrak{p}_{11}, \mathfrak{p}_{12}\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_{13}} = 21 + 6t + 5t^3 + t^5$.

9.23. Example. Let $K|\mathbb{F}_4$ and $\mathfrak{p}_0, \ldots, \mathfrak{p}_{13}$ be as in Example 2.7. We recall that $g_K = 3$, $N_K = 4$ and $h_K = 512$. The relevant S-class numbers and S-descriptions are given below.

(10a) $S = \{\mathfrak{p}_0, \mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_4, \mathfrak{p}_5, \mathfrak{p}_7, \mathfrak{p}_8, \mathfrak{p}_9, \mathfrak{p}_{10}, \mathfrak{p}_{13}\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_{12}} = 1 + 2t + 2t^3 + 2t^5 + t^9 + 2t^{11}$.

(11a) $S = \{\mathfrak{p}_0, \mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4, \mathfrak{p}_5, \mathfrak{p}_7, \mathfrak{p}_8, \mathfrak{p}_9, \mathfrak{p}_{10}, \mathfrak{p}_{13}\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_{12}} = 1 + 2t + 2t^3 + 2t^5 + t^7 + t^9 + 2t^{11}$.

(12a) $S = \{\mathfrak{p}_0, \mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4, \mathfrak{p}_5, \mathfrak{p}_6, \mathfrak{p}_7, \mathfrak{p}_8, \mathfrak{p}_9, \mathfrak{p}_{10}, \mathfrak{p}_{11}\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_{12}} = 1 + 2t + 2t^3 + 2t^5 + 2t^7 + 2t^{11} + t^{15}$.

(13a) $S = \{\mathfrak{p}_0, \mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4, \mathfrak{p}_5, \mathfrak{p}_6, \mathfrak{p}_7, \mathfrak{p}_8, \mathfrak{p}_9, \mathfrak{p}_{10}, \mathfrak{p}_{11}, \mathfrak{p}_{13}\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_{12}} = 1 + 2t + 2t^3 + 2t^5 + 2t^7 + t^9 + 2t^{11} + t^{15}$.

The outgrowth of Examples 9.17–9.23 is gathered in the table below.

$q = 4$				
g	$N_4(g)$	K, S	$[L : K]$	$\mathfrak{f}(L\|K)$
4	15	9.18(7a)	2	$6\mathfrak{p}_0$
5	17–18	9.17(4a)	4	$6\mathfrak{p}_4$
6	20	9.17(5a)	4	$2\mathfrak{p}_6$
8	21–24	9.22(10a)	2	$6\mathfrak{p}_0$
9	26	9.18(3a)	8	$3\mathfrak{p}_0$
10	27–28	9.19(2a)	12	$2\mathfrak{p}_8$
11	26–30	9.22(13a)	2	$4\mathfrak{p}_{13}$
12	**29**–31	9.18(7a)	4	$8\mathfrak{p}_0$
13	33	9.17(4a)	8	$6\mathfrak{p}_4$
14	32–35	9.17(4a)	8	$2\mathfrak{p}_6$
19	**37**–43	9.21(9a)	4	$10\mathfrak{p}_0$
20	**40**–45	9.17(5a)	8	$3\mathfrak{p}_6$
21	41–47	9.22(10b)	4	$8\mathfrak{p}_0$
22	**41**–48	9.22(10a)	4	$10\mathfrak{p}_0$
23	**45**–50	9.23(11a)	4	$10\mathfrak{p}_{12}$

g	$N_4(g)$	K, S	$[L : K]$	$\mathfrak{f}(L\|K)$
24	49–52	9.23(12a)	4	$10\mathfrak{p}_{12}$
25	51–53	9.20(4a)	12	$3\mathfrak{p}_0$
27	49–56	9.17(3a)	16	$6\mathfrak{p}_4$
28	**53**–58	9.23(13a)	4	$14\mathfrak{p}_{12}$
31	60–63	9.21(4a)	15	$\mathfrak{p}_{10}$
32	**57**–65	9.18(7a)	8	$10\mathfrak{p}_0$
33	65–66	9.17(4a)	16	$7\mathfrak{p}_4$
34	57–68	9.21(7a)	8	$8\mathfrak{p}_2$
36	64–71	9.21(8a)	8	$3\mathfrak{p}_{10}$
41	65–78	9.21(3a)	20	$3\mathfrak{p}_0$
43	72–81	9.17(3b)	24	$2\mathfrak{p}_6$
45	80–84	9.17(5a)	16	$4\mathfrak{p}_5$
47	**73**–87	9.21(9a)	8	$12\mathfrak{p}_0$
48	**80**–89	9.17(5a)	16	$3\mathfrak{p}_6$
49	81–90	9.23(10a)	8	$10\mathfrak{p}_{12}$

Examples for $q = 8$

Let α be the multiplicative generator of $\mathbb{F}_8^*$ satisfying $\alpha^3 = \alpha + 1$.

9.24. Example. Let $K = \mathbb{F}_8(x)$ and consider the places $\mathfrak{p}_0 = (x)$, $\mathfrak{p}_1 = (x+1)$, $\mathfrak{p}_2 = (x+\alpha)$, $\mathfrak{p}_3 = (x+\alpha^2)$, $\mathfrak{p}_4 = (x+\alpha^3)$, $\mathfrak{p}_5 = (x+\alpha^4)$, $\mathfrak{p}_6 = (x+\alpha^5)$, $\mathfrak{p}_7 = (x+\alpha^6)$, $\mathfrak{p}_8 = (1/x)$, $\mathfrak{p}_9 = (x^2+x+1)$ and $\mathfrak{p}_{10} = (x^3+x+\alpha)$ of K. The relevant S-class numbers and S-descriptions are given below.

(3a) $S = \{\mathfrak{p}_0, \mathfrak{p}_1, \mathfrak{p}_2\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_8} = 1 + 2t$.

(4a) $S = \{\mathfrak{p}_0, \mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_8} = 1 + 3t$.

(4b) $S = \{\mathfrak{p}_0, \mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_4\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_8} = 1 + 2t + t^2$.

(6a) $S = \{\mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4, \mathfrak{p}_5, \mathfrak{p}_6, \mathfrak{p}_7\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_9} = 9 + 4t + t^3$.

(6b) $S = \{\mathfrak{p}_0, \mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4, \mathfrak{p}_5\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_{10}} = 73 + 5t$.

(7a) $S = \{\mathfrak{p}_0, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4, \mathfrak{p}_5, \mathfrak{p}_6, \mathfrak{p}_7\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_9} = 9 + 5t + t^3$.

(8a) $S = \{\mathfrak{p}_0, \mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4, \mathfrak{p}_5, \mathfrak{p}_6, \mathfrak{p}_7\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_8} = 1 + 3t + 3t^3 + t^7$, $\delta_{S,\mathfrak{p}_{10}} = 73 + 7t$.

(9a) $S = \{\mathfrak{p}_0, \mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4, \mathfrak{p}_5, \mathfrak{p}_6, \mathfrak{p}_7, \mathfrak{p}_8\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_9} = 9 + 6t + 2t^3$, $\delta_{S,\mathfrak{p}_{10}} = 73 + 8t$.

The outgrowth of Example 9.24 is gathered in the table below.

$q = 8$				
g	$N_8(g)$	K, S	$[L : K]$	$\mathfrak{f}(L\|K)$
1	14	9.24(7a)	2	$2\mathfrak{p}_9$
2	18	9.24(9a)	2	$2\mathfrak{p}_{10}$
3	24	9.24(6a)	4	$2\mathfrak{p}_9$
6	33–36	9.24(8a)	4	$6\mathfrak{p}_8$
7	33–39	9.24(4a)	8	$4\mathfrak{p}_8$
11	48–54	9.24(6a)	8	$3\mathfrak{p}_9$
14	65	9.24(8a)	8	$6\mathfrak{p}_8$

g	$N_8(g)$	K, S	$[L : K]$	$\mathfrak{f}(L\|K)$
21	72–86	9.24(9a)	8	$4\mathfrak{p}_9$
27	96–103	9.24(6a)	16	$3\mathfrak{p}_9$
29	97–109	9.24(3a)	32	$4\mathfrak{p}_8$
30	96–112	9.24(6b)	16	$2\mathfrak{p}_{10}$
38	129–135	9.24(8a)	16	$8\mathfrak{p}_8$
45	144–156	9.24(9a)	16	$4\mathfrak{p}_9$
46	129–158	9.24(4b)	32	$6\mathfrak{p}_8$
48	**128**–164	9.24(8a)	16	$3\mathfrak{p}_{10}$

Examples for $q = 9$

Let α be the multiplicative generator of $\mathbb{F}_9^*$ satisfying $\alpha^2 = \alpha + 1$.

9.25. Example. Let $K = \mathbb{F}_9(x)$ and consider the places $\mathfrak{p}_0 = (x)$, $\mathfrak{p}_1 = (x-1)$, $\mathfrak{p}_2 = (x+1)$, $\mathfrak{p}_3 = (x-\alpha)$, $\mathfrak{p}_4 = (x-\alpha^2)$, $\mathfrak{p}_5 = (x-\alpha^3)$, $\mathfrak{p}_6 = (x-\alpha^5)$, $\mathfrak{p}_7 = (x-\alpha^6)$, $\mathfrak{p}_8 = (x-\alpha^7)$ and $\mathfrak{p}_9 = (1/x)$ of K. The relevant S-class numbers and S-descriptions are given below.

(2a) $S = \{\mathfrak{p}_0, \mathfrak{p}_1\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_9} = 1 + t$.

(5a) $S = \{\mathfrak{p}_0, \mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_5\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_9} = 1 + 2t + t^2 + t^4$.

(6a) $S = \{\mathfrak{p}_0, \mathfrak{p}_1, \mathfrak{p}_3, \mathfrak{p}_4, \mathfrak{p}_5, \mathfrak{p}_6\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_9} = 1 + 2t + 2t^2 + t^5$.

(7a) $S = \{\mathfrak{p}_0, \mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4, \mathfrak{p}_5, \mathfrak{p}_6\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_9} = 1 + 2t + 2t^2 + t^4 + t^5$.

(9a) $S = \{\mathfrak{p}_0, \mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4, \mathfrak{p}_5, \mathfrak{p}_6, \mathfrak{p}_7, \mathfrak{p}_8\}$, $h_S = 1$, $\delta_{S,\mathfrak{p}_9} = 1 + 2t + 2t^2 + t^4 + 2t^5 + t^8$.

The outgrowth of Example 9.25 is gathered in the table below.

$q = 9$				
g	$N_9(g)$	K, S	$[L : K]$	$\mathfrak{f}(L\|K)$
1	16	9.25(5a)	3	$3\mathfrak{p}_9$
3	28	9.25(9a)	3	$5\mathfrak{p}_9$
12	55–63	9.25(2a)	27	$3\mathfrak{p}_9$
15	64–74	9.25(7a)	9	$6\mathfrak{p}_9$
48	163–180	9.25(6a)	27	$6\mathfrak{p}_9$

List of Symbols

Below we list most of the notation and symbols used in this work. The numbers on the right refer to the page of the definition or of the first occurence.

α a generator of $\mathbb{F}_q^*$ 13

α an idèle of K 27

$\alpha_\mathfrak{p}$ $\mathfrak{p}$-th component of $\alpha \in \mathcal{I}_K$ ... 26

B a basis of $\mathbb{F}_\mathfrak{p}$ over $\mathbb{F}_p$ 41

$\mathbb{C}$ the complex numbers

$\mathbb{C}((t))$ the field of formal Laurent series over $\mathbb{C}$ 9

$\mathcal{C}_K$ idèle class group of K 27

$\mathcal{C}_S^\mathfrak{m}$ S-congruence subgroup mod $\mathfrak{m}$ 30

$\mathcal{C}\ell(\mathcal{O}_S)$ S-class group 14

$\mathcal{C}\ell^\mathfrak{m}(\mathcal{O}_S)$ S-class group mod $\mathfrak{m}$ ... 31

$\mathcal{D}_K$ divisor group of K 8

$\mathcal{D}_K^0$ divisors of degree 0 8

$\mathcal{D}_K^0/(K^*)$ divisor class group of K 9

$\mathcal{D}_S$ S-divisors 14

$\mathcal{D}_S^0$ S-divisors of degree 0 14

deg degree 9

$\deg \mathfrak{m}$ degree of $\mathfrak{m}$ 8

$\deg \mathfrak{p}$ degree of $\mathfrak{p}$ 8

$\deg S$ degree of S 14

$\dim \mathfrak{m}$ dimension of $\mathcal{L}(\mathfrak{m})$ 9

$\mathfrak{d}(L|K)$ discriminant of $L|K$ 11

$d(\mathfrak{q}|\mathfrak{p})$ different exponent of $\mathfrak{q}|\mathfrak{p}$ .. 10

δ a description 40

$\delta^{(m)}$ number derived from δ 41

δ_n n-th coefficient of δ 40

$\delta_{S,\mathfrak{p}}$ S-description at $\mathfrak{p}$ 41

e $= \log_p q$ 54

e_n 0 or length of a G-orbit in Q . 54

$e(\mathfrak{q}|\mathfrak{p})$ ramification index of $\mathfrak{q}|\mathfrak{p}$ .. 10

F_m homeomorphism from $[\frac{\pi}{m+1}, \frac{\pi}{m}]$ onto $[0,1]$ 47

$\mathbb{F}_\mathfrak{p}$ residue field at $\mathfrak{p}$ 8

$\mathbb{F}_\mathfrak{p}((\pi))$ field of expansions in π at $\mathfrak{p}$ 12

$\mathbb{F}_q$ finite field with q elements 8

$\mathbb{F}_{q^d}K$ constant field extension of degree d over K 11

$\mathbb{F}_q(x)$ rational function field 9

$[\mathbb{F}_\mathfrak{q} : \mathbb{F}_\mathfrak{p}]$ inertia degree of $\mathfrak{q}|\mathfrak{p}$ 10

$f(L,\mathfrak{p})$ conductor exponent of $\mathfrak{p}$ in L 20

$f_n(t)$ auxiliary polynomials over $\mathbb{Z}$ 50

$\mathfrak{f}(L|K)$ conductor of $L|K$ 20

G $= G(\mathbb{F}_q|\mathbb{F}_p)$ 54

$G(L|K)$ Galois group of $L|K$ 8

GL_n invertible $n \times n$-matrices

$G^s(L,\mathfrak{p})$ s-th upper ramification group of $\mathfrak{p}$ in L 23

$G_s(\mathfrak{q}|\mathfrak{p})$ s-th lower ramification group of $\mathfrak{q}|\mathfrak{p}$ 19

$G^s(\mathfrak{q}|\mathfrak{p})$ s-th upper ramification group of $\mathfrak{q}|\mathfrak{p}$ 20

$G^0(\mathfrak{q}|\mathfrak{p})$ inertia group of $\mathfrak{q}|\mathfrak{p}$ 20

$G^{-1}(\mathfrak{q}|\mathfrak{p})$ decomposition group of $\mathfrak{q}|\mathfrak{p}$ 20

g_K genus of K 9

γ_q lower bound for the genus 48

h_K divisor class number of K 9

h_S S-class number 14

$\hbar_q$ upper bound for S-class numbers 49

η continuous bijection on $[-1,\infty)$ 20

References

[AT] E. Artin, J. Tate. *Class Field Theory.* Mathematics Lecture Notes Series. Benjamin, Reading Massachusetts, 1967.

[Au] R. Auer. *Ray class fields of global function fields with many rational places.* Preprint at `http://xxx.lanl.gov/find/math/1/auer`, 1998.

[CF] J. W. S. Cassels, A. Fröhlich. *Algebraic Number Theory.* Academic Press, New York, 1967.

[CDO] H. Cohen, F. Diaz y Diaz, M. Olivier. *Computing ray class groups, conductors and discriminants.* In: *Algorithmic Number Theory.* H. Cohen (ed.). Lecture Notes in Computer Science **1122**, Springer, Berlin, (1996) 51–59.

[Do] J. Doumen. Master's thesis. Universiteit Leiden, 1998

[FJ] M. D. Fried, M. Jarden. *Field Arithmetic.* Springer, 1987.

[FT] R. Fuhrmann, F. Torres. *The genus of curves over finite fields with many rational points.* Manuscr. Math. **89**/1 (1996) 103–106.

[GS1] A. Garcia, H. Stichtenoth. *Elementary abelian p-extensions of algebraic function fields.* Manuscr. Math. **72** (1991) 67–79.

[GS2] A. Garcia, H. Stichtenoth. *Algebraic function fields over finite fields with many rational places.* IEEE Trans. Inf. Theory **41**/6 (1995) 1548–1563.

[GS3] A. Garcia, H. Stichtenoth. *A class of polynomials over finite fields.* Preprint, 1998.

[GSX] A. Garcia, H. Stichtenoth. C. P. Xing. *On subfields of the Hermitian function field.* Preprint 1998.

[GV1] G. van der Geer, M. van der Vlugt. *Curves over finite fields of characteristic 2 with many rational points.* C. R. Acad. Sci. Paris **317** (1993) série I, 593–597.

[GV2] G. van der Geer, M. van der Vlugt. *Generalized Hamming weights of codes and curves over finite fields with many rational points.* In: *Isreal Math Conf. Proc.* **9** (1996) 417–432.

[GV3] G. van der Geer, M. van der Vlugt. *Quadratic forms, generalized Hamming weights of codes and curves with many points.* J. Number Theory **59** (1996) 20–36.

[GV4] G. van der Geer, M. van der Vlugt. *How to construct curves over finite fields with many points.* In: *Arithmetic Geometry (Cortona 1984).* F. Catanese (ed.). Cambridge Univ. Press (1997) 169–189.

[GV5] G. van der Geer, M. van der Vlugt. *On generalized Reed-Muller codes and curves with many points.* Report W 97-22, Universiteit Leiden, 1997.

[GV6] G. van der Geer, M. van der Vlugt. *Constructing curves over finite fields with many points by solving linear equations.* Preprint 1997.

[GV7] G. van der Geer, M. van der Vlugt. *Tables of curves with many points.* Preprint at `http://www.wins.uva.nl/~geer`, 1999.

[Han] J. P. Hansen. *Group codes and algebraic curves.* Mathematica Gottingensis, Schriftenreihe SFB Geometrie und Analysis, Heft 9, 1987.

[HS] J. P. Hansen, H. Stichtenoth. *Group codes on certain algebraic curves with many rational points.* Appl. Alg. Eng. Commun. Comp. **1** (1990) 67–77.

[H] H. Hasse. *Number Theory.* Springer, Berlin, 1980.

[Hay] D. R. Hayes. *Explicit class field theory in global function fields.* Stud. Alg. Number Th./Adv. Math. Suppl. Stud. **6** (1979) 173–217.

[He] F. Heß. *Effective construction of Riemann-Roch spaces.* Short communication given at the ICM 1998 in Berlin.

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

[K] The KANT Group. M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, M. Schörnig, K. Wildanger. *KANT V4.* J. Symb. Comp. **24**/3 (1997) 267–283.

[Ki] H. Kisilevsky. *Multiplicative independence in function fields.* J. Number Theory **44** (1993) 352–355.

[La1] K. Lauter. *Ray class field constructions of curves over finite fields with many rational points.* In: *Algorithmic Number Theory.* H. Cohen (ed.). Lecture Notes in Computer Science **1122**, Springer, Berlin (1996) 189–197.

[La2] K. Lauter. *Deligne Lusztig curves as ray class fields.* Preprint at `http://www.mpim-bonn.mpg.de/html/preprints/preprints.html`, 1997.

[La3] K. Lauter. *A formula for constructing curves over finite fields with many rational points.* Preprint at `http://www.mpim-bonn.mpg.de/html/preprints/preprints.html`, 1997.

[La4] K. Lauter. *Non-existence of a curve over* $\mathbb{F}_3$ *of genus* 5 *with* 14 *rational points.* Preprint 1998.

[Lu] D. Lutz. *Topologische Gruppen.* B.I.-Wissenschaftsverlag, Zürich, 1976.

[Nk] J. Neukirch. *Algebraische Zahlentheorie.* Springer, Berlin, 1991.

[NX1] H. Niederreiter, C. P. Xing. *Explicit global function fields over the binary field with many rational places.* Acta Arith. **75**/4 (1996) 383–396.

[NX2] H. Niederreiter, C. P. Xing. *Cyclotomic function fields, Hilbert class fields, and global function fields with many rational places.* Acta Arith. **79**/1 (1997) 59–76.

[NX3] H. Niederreiter, C. P. Xing. *Algebraic curves over finite fields with many rational points.* In: *Proc. Number Theory Conf. (Eger 1996).* W. de Gruyter, Berlin, to appear.

[NX4] H. Niederreiter, C. P. Xing. *Drinfel'd modules of rank 1 and algebraic curves with many rational points II.* Acta Arith. **81** (1997) 81–100.

[NX5] H. Niederreiter, C. P. Xing. *Global function fields with many rational places over the ternary field.* Acta Arith. **83**/1 (1998) 65–86.

[NX6] H. Niederreiter, C. P. Xing. *Global function fields with many rational places over the quinary field.* Demonstratio Math. **30**/4 (1997) 919-930.

[NX7] H. Niederreiter, C. P. Xing. *Global function fields with many rational places over the quinary field II.* Acta Arith. **86**/3 (1998) 277-288.

[NX8] H. Niederreiter, C. P. Xing. *Algebraic curves with many rational points over finite fields of characteristic 2.* In: *Proc. Number Theory Conf. (Zakopane 1997).* W. de Gruyter, Berlin, to appear.

[NX9] H. Niederreiter, C. P. Xing. *A general method of constructing global function fields with many rational places.* Algorithmic Number Theory (Portland 1998), Lect. Notes in Comp. Sci., Springer, Berlin, to appear.

[OS] F. Özbudak, H. Stichtenoth. *Curves with many points and configurations of hyperplanes over finite fields.* Preprint 1998.

[Ped] J. P. Pedersen. *A function field related to the Ree group.* In: *Coding Theory and Algebraic Geometry, Proceedings, Luminy 1991.* H. Stichtenoth, M. A. Tsfasman (eds.). LNM **1518**, Springer, Berlin, 1992.

[Per] M. Perret. *Tours ramifiées infinies de corps de classes.* J. Number Theory **38** (1991) 300–322.

[Ro1] M. Rosen. *S-Units and S-class group in algebraic function fields.* J. Algebra **26** (1973) 98–108.

[Ro2] M. Rosen. *The Hilbert class field in function fields.* Expo. Math. **5** (1987) 365–378.

[RS] H.-G. Rück, H. Stichtenoth. *A characterization of Hermitian function fields over finite fields.* J. reine angew. Math. **457** (1994) 185–188.

[Sf] R. Schoof. *Algebraic curves and coding theory.* UTM **336**, Univ. of Trento, 1990.

[Sg] M. Schörnig. *Untersuchungen konstruktiver Probleme in globalen Funktionenkörpern.* Thesis at the Technische Universität Berlin, 1996.

[S1] J.-P. Serre. *Local Fields.* Springer, New York, 1979.

[S2] J.-P. Serre. *Sur le nombre des points rationelles d'une courbe algébrique sur un corps fini.* C. R. Acad. Sci. Paris **296** (1983) série I, 397–402.

[S3] J.-P. Serre. *Nombres de points des courbes algébrique sur* $\mathbb{F}_q$. Séminaire de Théorie des Nombres de Bordeaux **22** (1982/83).

[S4] J.-P. Serre. *Résumé des cours de 1983–1984.* Annuaire du Collège de France (1984) 79–83.

[S5] J.-P. Serre. *Rational points on curves over finite fields, Part I.* Notes of lectures at Harvard University, 1985.

[S6] J.-P. Serre. *Rational points on curves over finite fields, Part II.* Notes of lectures at Harvard University, 1985.

[Sh] V. Shabat. Unpublished manuscript. University of Amsterdam, 1997/98.

[St1] H. Stichtenoth. *Algebraic geometric codes associated to Artin-Schreier extensions of* $\mathbb{F}_q(z)$. In: *Proc. 2nd Int. Workshop on Alg. and Comb. Coding Theory.* Leningrad (1990) 203–206.

[St2] H. Stichtenoth. *Algebraic Function Fields and Codes.* Springer, Berlin, 1993.

[SX] H. Stichtenoth. C. P. Xing. *The genus of maximal function fields over finite fields.* Manuscr. Math. **86** (1995) 217–224.

[Th] M. Thomas. *Türme und Pyramiden algebraischer Funktionenkörper.* Thesis at the Universität GH Essen, 1997.

[Wa] B. L. van der Waerden. *Algebra.* Volume II. Springer, Berlin, 1991.

[Wi] M. Wirtz. *Konstruktionen und Tabellen linearer Codes.* Thesis at the Westfälische Wilhelms-Universität Münster, 1991.

[XN] C. P. Xing, H. Niederreiter. *Drinfel'd modules of rank 1 and algebraic curves with many rational points.* Report Austrian Academy of Sciences, Vienna, 1996.

Curriculum Vitae

	Roland Auer, geboren am
11.08.1967	in Lindau (Bodensee)
1973–1979	Grundschule und Orientierungsstufe in Osterholz-Scharmbeck
1979–1986	Gymnasium Osterholz-Scharmbeck Abschluß: allgemeine Hochschulreife
1986–1989	Grundstudium Mathematik in Oldenburg (Oldb) Abschluß: Diplom-Vorprüfung
1989–1994	Hauptstudium Mathematik in Oldenburg (Oldb) Abschluß: Diplomprüfung
1996–1999	Doktorand im Fach Mathematik an der C.v.O.-Universität Oldenburg
Staatsbürgerschaft:	österreichisch