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

Contents

Introduction 4

I Global Function Fields 8
1 Preliminaries 8
2 $S$-Units 14
3 Ramification Groups 19

II Ray Class Fields 26
4 Class Field Theory 26
5 Definition and Properties 30
6 Computation of Degrees 36

III Many Rational Places 46
7 Upper Bounds 46
8 Rational Function Field 51
9 Tables of Examples 59

List of Symbols 73
References 76
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 $K_m^S$, where $S$ is a non-empty set of places of $K$ and $m$ is an $S$-cycle, i.e. a finite formal sum $\sum m_p p$ of places $p$ outside $S$ together with non-negative integer multiplicities $m_p$. The extension $K_m^S|K$ can be characterized as the largest abelian extension $L|K$ of conductor $f(L|K) \leq m$ such that every place $p \in S$ splits completely in $L$ (i.e. there are $[L : K]$ places of $L$ lying above $p$). Roughly speaking, the conductor measures the “wildness” of ramification at each place of $K$, thus the $S$-cycle $m$ confines this wildness. For example, if $m = 0$, no ramification is allowed at all, and we obtain the special case of a Hilbert class field $K_o^S$, whose degree over $K$ equals the $S$-class number $h_S$.

The extension $K_m^S|K$ 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 $\overline{F}_q K|K$ 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 $K_m^S$ 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 $K_m^S$ has at least $[K_m^S : K]|S|$ rational places. For suitable choices of $S$ and $m$, this number tends to be large compared with the genus of $K_m^S$, 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 $K_m^S$ can be constructed by adjoining the $m$-torsion of a rank 1 Drinfel’d module to the Hilbert class field $K_o^S$. This gives us a so-called narrow ray class field, whose Galois group over $K_o^S$ naturally contains $\overline{F}_q^*$, and $K_m^S$ is the subfield fixed by $\overline{F}_q^*$. In the general situation, one singles out a place $q \in S$ and gains $K_m^S$ as the subfield of $K_m^q$ 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 $C_m^S$ of finite index in the idèle class group $C_K$ of $K$ and obtain $K_m^S$ directly as the class field associated to this subgroup. The Galois group $G(K_m^S|K)$ is isomorphic to $C_K/C_m^S$. 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 $K_m^S|K$ 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 $K_S^m|K$ step by step.

As was mentioned above, it is important to know the genus of $K_S^m$. By means of a remarkable genus formula (Theorem 5.8 and Corollary 5.9), the problem is reduced to the determination of the degrees $[K_S^{m'} : K]$ for certain $m' \leq m$. 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 $[K_S^m : K]$ 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 $m$ is only treated for tame ramification, i.e. for $m$ of the form $\sum_{p \in R} p$ with a finite set $R$ of places of $K$. Instead, from page 40 onwards, we concentrate on ramification at a single place $p$ of $K$. In this situation we introduce the concept of the $S$-description at $p$, 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 $K_S^m|K$ 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 $p$, 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
Introduction

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

![Dependency Diagram]

1

3

2

4

5

6

7

8

9
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 $p$ in some discrete valuation ring $R_p$ of $K$. We say that $p$ is a zero or a pole of the function $z \in K$ if $z \in p$ or $z \notin R_p$, respectively. The constant field $\mathbb{F}_q$ is naturally contained in the (finite) residue field $\mathbb{F}_p := R_p/p$ of $p$. The degree of $p$ is defined as $\deg p := [\mathbb{F}_p : \mathbb{F}_q]$. A place of degree 1 is called a rational place. The map $p \mapsto v_p$ 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 $\mathbb{P}_K^d := \{p \in \mathbb{P}_K \mid \deg p = d\}$ for $d \in \mathbb{N}$.

The free abelian group $D_K$ on the set $\mathbb{P}_K$ is called the divisor group of $K$. The map $\deg : \mathbb{P}_K \rightarrow \mathbb{Z}$ is extended to $D_K$ by linearity. Its kernel is denoted by $D_K^0$. A divisor $m \in D_K$ is written as a formal sum $m = \sum_{p \in \mathbb{P}_K} m_p p$ with integer coefficients $m_p$ and finite support $\text{supp } m := \{p \in \mathbb{P}_K \mid m_p \neq 0\}$. If $n = \sum n_p p \in D_K$ is another divisor and $m_p \leq n_p$ for all $p \in \mathbb{P}_K$, then we
write \( m \leq n \). The zero element in \( D_K \) is denoted \( o \), and a divisor \( m \geq o \) is called effective.

Each function \( z \in K^* \) has only finitely many zeros and poles, hence one can define its principal divisor \( (z) = (z)_K := \sum_{p \in \mathcal{P}_K} v_p(z)p \). Breaking up \( (z) \) into the zero divisor \( (z)_0 \geq o \) and the pole divisor \( (z)_\infty \geq o \) 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 \( (\ ) = (\ )_K : K^* \to D^0_K \), \( z \mapsto (z) \) is a group morphism with kernel \( \mathbb{F}_q^* \), hence \( (K^*) \simeq K^*/\mathbb{F}_q^* \). The quotient \( D^0_K / (K^*) \) is called the (divisor) class group of \( K \). Its order, the (divisor) class number \( h_K \), is finite.

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

The power series
\[
Z_K(t) := \sum_{n=0}^{\infty} A_n t^n \in \mathbb{Z}[t] \subseteq \mathbb{C}((t))
\]
with \( A_n = |\{ m \in D_K \mid m \geq o, \deg m = n \}| \) 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
\[
P_K(t) = q^{g_K} t^{2g_K} P_K \left( \frac{1}{qt} \right).
\]
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 \( \infty \) of \( \mathbb{F}_q(x) \) corresponding to \( v_\infty \) has degree 1 and is the (only) pole of \( x \). All (discrete) valuations on \( \mathbb{F}_q(x) \) are given by the set
\[
\{ v_P \mid P \in \mathbb{F}_q[x] \text{ monic, irreducible} \} \cup \{ v_\infty \}.
\]
Hence there is a 1–1 correspondence $P \leftrightarrow p$ with $v_P = v_p$ between the monic irreducibles $P \in \mathbb{F}_q[x]$ and the places $p \neq \infty$ of $\mathbb{F}_q(x)$. In this correspondence, $p$ is the maximal ideal in the localization of $\mathbb{F}_q[x]$ at $P$, and the principal divisor of $P$ is $(P) = p - (\deg P)\infty$, thus $\deg p = \deg P$. 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 $L|\mathbb{F}_q$ 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 $q$ be a place of $L$; then $q \cap K =: p$ is a place of $K$. We say that $q$ lies above $p$ and write $q|p$. The canonical inclusion $\mathbb{F}_q \subseteq \mathbb{F}_p$ is compatible with the inclusions $\mathbb{F}_q \subseteq \mathbb{F}_q^zd$ and $[\mathbb{F}_q : \mathbb{F}_p]$ is called the inertia degree of $q|p$. Note that, by definition, $[\mathbb{F}_q : \mathbb{F}_p]\deg p = d\deg q$. The extension $v_q|K$ equals $e \cdot v_q$ for some positive integer $e = e(q|p)$, called the ramification index of $q|p$. These numbers satisfy the following

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

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

where the sum is over all places $q$ of $L$ lying above $p$.

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

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

$$N_{L|K} : \mathcal{D}_L \rightarrow \mathcal{D}_K \quad \sum_{q|p} m_q q \rightarrow \sum_{p \in \mathbb{P}_K} \sum_{q|p} m_q [\mathbb{F}_q : \mathbb{F}_p]p.$$  

We note that $\deg N_{L|K} m = d \deg m$ for $m \in \mathcal{D}_L$. 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 $L = K(F_q^d) = F_q^d K$ is called the constant field extension of degree $d$ over $K$. It is Galois with group $G(L|K) \simeq G(F_q^d|F_q)$. For any place $p$ of $K$ and $q$ of $L$ above $p$, one has $e(q|p) = 1$ and $F_q = F_q^d F_p$, i.e. there are exactly $r := \gcd(d, \deg p)$ places $q$ of $L$ lying above $p$, each of which has degree $\deg q = \deg p/r$. By the Hurwitz Genus Formula, $L$ has the same genus as $K$.

If $p$ is any place of $K$, then the absolute value map $K \to \mathbb{R}_+, z \mapsto |z|_p := q^{-(\deg p) v_p(z)}$ defines a metric on $K$. (Two functions $z, z' \in K$ are close to each other if $v_p(z - z')$ 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 $K_p$ naturally containing $K$ as a dense subfield, and by these properties it is uniquely determined up to $K$-isomorphism. $K_p$ is called the completion of $K$ at $p$. The topological closure $\bar{p}$ of $p$ in $K_p$ is the maximal ideal in the discrete valuation ring $R_p := \bar{R}_p$, the topological closure of $R_p$ in $K_p$. The residue field $F_p = R_p/\bar{p}$ is naturally isomorphic with $F_p$ and $v_p|K = v_p$. Thus we can identify $F_p$ with $F_{\bar{p}}$, and there is no ambiguity in writing $v_p$ instead of $v_{\bar{p}}$. 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 $p \in S$, let a (positive) integer $m_p$ and an element $z_p \in K_p$ be given. Then there exists $z \in K$ such that $v_p(z - z_p) \geq m_p$ for all $p \in S$.

This theorem is readily derived from its non-complete variant in [St2, p. 11] using the fact that $K$ is dense in $K_p$. 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 $q \in \mathbb{P}_L$ lie above $p \in \mathbb{P}_K$. The natural inclusion $K_p \subseteq L_q$ is compatible with the inclusions $K \subseteq K_p$ and $K \subseteq L \subseteq L_q$, and one has $L_q = K_p L$. The “local extension” $L_q|K_p$ has degree

$$[L_q : K_p] = e(q|p)[F_q : F_p].$$
In particular, considering the constant field extension \( L = \mathbb{F}_q \sigma K \) of degree \( d := \deg \mathfrak{p} \) over \( K \), we see that \( \mathbb{F}_p = \mathbb{F}_q = \mathbb{F}_q^d \subseteq L \subseteq L_q = K_p \). This inclusion obviously identifies each residue class \( \alpha \in \mathbb{F}_p = \mathbb{F}_p \) with one of its representatives in \( R_p \subseteq K_p \) and is therefore independent of the choice of \( q \).

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

1.6. Proposition. Let \( \mathfrak{p} \) be a place of \( K \) and \( \pi \in K_p \) a uniformizer at \( \mathfrak{p} \). Then

\[
K_p = \mathbb{F}_p((\pi)) = \left\{ \sum_{n=m}^{\infty} \alpha_n \pi^n \mid m \in \mathbb{Z} \text{ and } \alpha_n \in \mathbb{F}_p \text{ for all } n \right\}.
\]

For each \( z \in K_p \), the coefficients \( \alpha_n \in \mathbb{F}_p \) of the expansion \( z = \sum_{n=1}^{\infty} \alpha_n \pi^n \) at \( \mathfrak{p} \) in \( \pi \) are uniquely determined by \( z \); moreover, \( \alpha_n = 0 \) for all \( n < m := v_p(z) \), and \( \alpha_m \in \mathbb{F}_p^* \) is the residue class of \( z/\pi^m \) 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 \( \pi \in K_p \).) 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 \( L := \mathbb{F}_q \sigma K \) of degree \( d \) over \( K \). Choose a place \( q \) of \( L \) above \( \mathfrak{p} \). Because \( e(q|\mathfrak{p}) = [\mathbb{F}_q : \mathbb{F}_p] = 1 \), we have \( v_p = v_q \) on \( K_p = L_q \), and \( \pi \) is a uniformizer at \( q \in \mathbb{P}_L^1 \) 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 \( \infty \) of \( x \) is the only place of \( \mathbb{F}_2(x) \) ramified in \( K \), the different exponent being \( d(p_0|\infty) = 6 \), where \( p_0 \in \mathbb{P}_K^1 \) is the place above \( \infty \). Therefore \( g_K = 2 \) according to the Hurwitz Genus Formula 1.4. The other rational places of \( K \) are \( p_1 := (0,1), p_2 := (1,0), p_3 := (1,1) \) and \( p_4 := (0,0) \), where \((\alpha, \beta)\) with \( \alpha, \beta \in \mathbb{F}_2 \) denotes the common zero of \( x - \alpha \) and \( y - \beta \). Since \( \mathbb{F}_2^d \) is empty, \( Z_K(t) = 1 + 5t + 15t^2 + \cdots \). Hence \( P_K(t) = (1 - 3t + 2t^2)Z_K(t) = \)
1 Preliminaries

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 \( p_1 \). 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 \( p_1 \) in \( x \).

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

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

\[
U_p^{(0)} = U_p := \mathbb{P}_p^* = \{ \alpha_0 + \alpha_1 \pi + \alpha_2 \pi^2 + \cdots \mid \alpha_0 \in \mathbb{F}_p^*, \alpha_1, \alpha_2, \ldots \in \mathbb{F}_p \}
\]

and, for any positive integer \( n \), the \( n \)-th one-unit group at \( p \),

\[
U_p^{(n)} := 1 + \mathbb{P}_p^n = \{ 1 + \alpha_n \pi^n + \alpha_{n+1} \pi^{n+1} + \cdots \mid \alpha_n, \alpha_{n+1}, \ldots \in \mathbb{F}_p \}.
\]

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

\[
U_p^{(m)}/U_p^{(n)} = \{ (1 + \alpha_m \pi^m + \cdots + \alpha_{n-1} \pi^{n-1})U_p^{(n)} \mid \alpha_m, \ldots, \alpha_{n-1} \in \mathbb{F}_p \}
\]

has \( q(n-m) \deg p \) elements.
2 S-Units

Let $K|\mathbb{P}_q$ 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 $D^0_S := D_S \cap D^0_K$. We write $\deg S$ for the (positive) greatest common divisor of the degrees of the places in $S$; hence $\deg(D_S) = \mathbb{Z}\deg S$.

Denote by $O_S = \bigcap_{\mathfrak{p} \in S} \mathcal{R}_\mathfrak{p}$ the ring of $S$-integral functions in $K$, i.e. those functions which have poles only in $S$. The group $O^*_S$ of invertible elements in $O_S$ is called the group of $S$-units. By [FJ, p. 22] and [St2, p. 69] the map $S \mapsto O_S$ is a 1–1 correspondence between the non-empty subsets of $\mathbb{P}_K$ and the Dedekind domains with field of fractions $K$. Accordingly, $O_S$ is a Dedekind domain. Its ideal class group, $\mathcal{C}_\ell(O_S)$, 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 $O_S$ by its subgroup of principal ideals $zO_S$ with $z \in K^*$. It has finite order $h_S := |\mathcal{C}_\ell(O_S)|$, 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 $\mathcal{C}(O_S)$ is naturally isomorphic to $D_K/(D_S + (K^*))$, and the sequence

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

is exact.

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

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

2.2. Corollary. We have $\text{reg}_S h_S = h_K \deg S$, and $(O^*_S) \simeq O_S^*/\mathbb{P}_q^*$ 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 $(u_i) \in D^0_K$ 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 $S = \{p_0, \ldots, p_s\}$. Let $u_1, \ldots, u_s$ be independent $S$-units, $U$ the subgroup of $\mathcal{O}_S^*$ generated by them, and $A_0 := (v_{p_j}(u_i))_{1 \leq i,j \leq s} \in \mathbb{Z}^{s \times s}$. Then
\[
\text{reg } U = \frac{\deg S}{\deg p_0} |\det A_0|.
\]
This is a slight improvement compared to a result by Schöning [Sg, p. 53], who only made use of the fact that reg $U$ divides $|\det A_0|$. Note that Schöning’s definition of the regulator differs from ours by the factor $\prod_{j=0}^s \deg p_j / \deg S$.

Proof. Set $d_j := \deg \{p_0, \ldots, p_j\}$ 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
\[
(b_1, \ldots, b_s) := (p_0, \ldots, p_s) \begin{pmatrix} * \\ B \end{pmatrix}
\]
is a $\mathbb{Z}$-basis for $D^0_S$. Since $\Phi : D^0_S \rightarrow \mathbb{Z}^s$, $\sum_{i=0}^s c_i p_i \mapsto (c_1, \ldots, c_s)$ is injective, we can conclude that
\[
(D^0_S : (U)) = (\Phi D^0_S : \Phi(U)) = \frac{|\det A_0|}{|\det B|} = \frac{d_s}{d_0} |\det A_0|.
\]

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 $S' = \{p_0, \ldots, p_{s'}\}$ where $s' = |S'| - 1$. Since $\mathbb{Z}$ is euclidean, we can compute $T = (t_{ij})_{1 \leq i,j \leq s'} \in \text{GL}_s(\mathbb{Z})$ such that $TA_0$ is lower triangular. Setting $u'_1 := \prod_{j=1}^s u'_{ij}$, it is easily seen that $u'_1, \ldots, u'_{s'}$ form a basis for $U \cap \mathcal{O}_{S'}$. 

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

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

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

The pre-images $M := u^{-1}((U) \cap (K^{*l}))$ and $N := u^{-1}((U) \cap lD_K)$ 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 $\mathbb{F}_l^s \rightarrow \mathbb{F}_l^{s+1}$, $\nu \mapsto \nu \bar{A}$.

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

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

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

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

(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 $u(m)$. Reduction modulo $l$ shows the assertion.

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

(c) This is clear from the definition of Riemann-Roch space and because $u$ 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 $\leq v_l(|G|)$ if $G$ is finite. Now $u$ induces a surjective $\mathbb{F}_l$-homomorphism $\mathbb{F}_l^s \rightarrow ((U) + lD_S^0)/lD_S^0$, whose kernel is $\bar{N}$. Hence

$$\dim_{\mathbb{F}_l} \bar{N} = s - \dim_{\mathbb{F}_l}((U) + lD_S^0)/lD_S^0 = \dim_{\mathbb{F}_l} D_S^0/((U) + lD_S^0),$$

but $D_S^0/((U) + lD_S^0) \simeq D_S^0/(lD_S^0)$. \hfill $\square$

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 $((\mathcal{O}_S^s) : (U))$, by 2.5(b) it suffices to test the condition

(1) $u(m) \in (K^{*l})$
with \( \tilde{m} \) running through a system of representatives for the orbits \( \{ \mathbb{F}_l^* \nu \mid \nu \in \bar{N} \setminus \{0\} \} \), 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 \( z \in \mathcal{L}(\mathbf{u}(m)/l) \setminus \{0\} \) 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 \( W = (w_{ij})_{1 \leq i, j \leq n} \in k^{n \times n} \) 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. \( \blacksquare \)

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 $\infty$ 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

$$
\begin{align*}
 p_0 &:= (0, \alpha), & p_1 &:= (0, \alpha^2), & p_2 &:= (1, 0), & p_3 &:= (1, 1), \\
 p_4 &:= (\alpha, 0), & p_5 &:= (\alpha, 1), & p_6 &:= (\alpha, \alpha), & p_7 &:= (\alpha, \alpha^2), \\
 p_8 &:= (\alpha^2, 0), & p_9 &:= (\alpha^2, 1), & p_{10} &:= (\alpha^2, \alpha), & p_{11} &:= (\alpha^2, \alpha^2), \\
 p_{12}, p_{13},
\end{align*}
$$

where $(\alpha, \beta)$ with $\alpha, \beta \in \mathbb{F}_4$ denotes the place of $K$ which is the common zero of $x - \alpha$ and $y - \beta$, and $p_{12}$ and $p_{13}$ are the zeros of $y/x$ and $y/x - 1$, respectively, which lie above $\infty$. Let $S := \{p_0, \ldots, p_{13}\}$ and "guess" $S$-units

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

then

$$
A := \left( v_{p_j}(u_i) \right)_{1 \leq i \leq 13} = \begin{pmatrix}
2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -2 & -2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -2 & -2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -2 & -2 \\
0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & -1 & -2 \\
1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & -2 & -2 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & -2 & -2 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & -2 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & -2 & -1 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & -2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \\
1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0
\end{pmatrix}.
$$

Without regard to sign, any $13 \times 13$-minor of $A$ (erase one column and compute the determinant) equals 512, which by Lemma 2.3 is the regulator of $U := (u_1, \ldots, u_{13})$. We want to test whether 2 divides $((\mathcal{O}_S^* : (U))$ by means of Proposition 2.5 and find $N = \mathbb{F}_2 e_1 \oplus \mathbb{F}_2 e_{10} \oplus \mathbb{F}_2 e_{12}$, 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

$$
V := \{ u_1^m u_{10}^{m_1} u_{12}^{m_2} \mid (0, 0, 0) \neq (m_1, m_{10}, m_{12}) \in \{0, 1\}^3 \}
= \{ x, y + \alpha x, y + \alpha^2 x, xy + \alpha x^2, xy + \alpha^2 x^2,
\begin{align*}
& y^2 + xy + x^2, xy^2 + x^2 y + x^3 \}.
\end{align*}
$$

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

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

Part I – Global Function Fields
shows that in fact no element of $V$ is a square in $K$ and hence proves $O_S^* = F^*_4 U$ and $\text{reg}_S = 512$.

If we have information about the $S$-class number and the divisor class number, we can determine the regulator $\text{reg}_S$ 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 $K = F_2(x, y)$ and $p_0, \ldots, p_4$ as in Example 1.7(a). Suppose $S \subseteq \mathbb{P}_K^1$ contains at least two elements, say $p \neq p'$, then $p - p' \in \mathcal{D}_S \setminus (K^*)$ by Theorem 1.1, and consequently $\text{reg}_S > 1$. Let $0 \leq k \leq 4$ and consider the set $S_k := \{p_0, \ldots, p_k\}$. Then $\text{reg}_{S_k} = h_K = 13$ 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

$$A := (v_{p_j}(u_i))_{0 \leq i \leq 4} = \begin{pmatrix} -2 & 1 & 0 & 0 & 1 \\ -2 & 0 & 1 & 1 & 0 \\ -5 & 0 & 2 & 0 & 3 \\ -5 & 0 & 0 & 3 & 2 \end{pmatrix}$$

and $T := \begin{pmatrix} 13 & 6 & 3 & 3 & -2 \\ 5 & 3 & -1 & -2 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix} \in \text{GL}_4(\mathbb{Z})$.

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 $O_{S_4}^* = \langle u_1, u_2, u_3, u_4 \rangle$. Moreover, writing $T = (t_{ij})_{1 \leq i, j \leq 4}$ and setting $u'_k := \prod_{j=1}^4 t_{kj}$, we obtain $O_{S_k}^* = \langle u'_1, \ldots, u'_k \rangle$ 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 $G(L|K)$, $p$ a place of $K$ and $q$ a place of $L$ lying above $p$. It is well-known that $G(L|K)$ acts transitively on the set of all places of $L$ above $p$. For $s \in [-1, \infty)$ there is the $s$-th lower ramification group of $q|p$,

$$G_s(q|p) := \{ \sigma \in G(L|K) \mid v_q(\sigma z - z) \geq s + 1 \forall z \in R_q \}.$$
We note that $G_{-1}(q|p) = \{ \sigma \in G \mid \sigma q = q \}$ is the \textbf{decomposition group} and $G_0(q|p)$ is the \textbf{inertia group} of $q|p$. See [St2, p. 119] for their specific properties. After renumbering by means of the continuous and strictly isotonous bijection

$$\eta = \eta_{q|p} : [-1, \infty) \to [-1, \infty)$$

$$s \mapsto \int_0^s \frac{|G_x(q|p)|}{|G_0(q|p)|} \, dx,$$

we get the \textbf{upper ramification groups} $G^{\eta(s)}(q|p) := G_s(q|p)$. (Note that $\eta$ 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]):

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

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

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

$$\varphi_{q|p} z \equiv z^{|p\sigma q|p} \pmod{q}$$

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

Since $G_s(\sigma q|p) = \sigma G_s(q|p) \sigma^{-1}$ 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 $q$. Therefore, we can define the \textbf{conductor exponent} $f(L, p)$ of $p$ in $L$ as the least integer $m \geq 0$ such that $G^m(q|p)$ is trivial. The effective divisor

$$f(L|K) := \sum_{p \in \mathcal{P}_L} f(L, p)p$$
3.3. Example (Artin-Schreier Extensions). Let \( K \) be finite and \( \varphi : \bar{K} \to \bar{K}, z \mapsto z^p - z \). We define the Artin-Schreier reduced valuation of a function \( u \in K \) at a place \( p \in \mathbb{P}_K \) by

\[
v_p^*(u) := \max\{v_p(u - \varphi t) \mid t \in K\} \in \mathbb{Z} \cup \{\infty\}.
\]

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

(a) For \( u \in K \) with \( v_p(u) < 0 \) we have the equivalence

\[
v_p(u) = v_p^*(u) \iff v_p(u) \not\equiv 0 \mod p.
\]
(b) The extension \( L|K \) has conductor

\[
f(L|K) = \sum_{m_p > 0} (m_p + 1)p,
\]

where \( m_p := \min_{u \in U} v_p^*(u) \) for \( p \in \mathbb{P}_K \).

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

(d) The degree of \( L|K \) is \( [L:K] = (V + \varphi K : \varphi K) \), 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 \( K_u := K(\varphi^{-1}u) \subseteq L \) satisfies

\[
(3) \quad f(K_u|K) = \sum_{v_p^*(u) < 0} (1 - v_p^*(u))p.
\]

If \( u \in \varphi K \), then \( K_u = K \) and \( v_p^*(u) = \infty \) for all \( p \in \mathbb{P}_K \), 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 \( p \in \mathbb{P}_K \). If \( v_p^*(u) \geq 0 \), then \( p \) is unramified in \( L \), i.e. \( f(K_u,p) = 0 \). In case \( m := -v_p^*(u) > 0 \), exactly one place \( q \in \mathbb{P}_{K_u} \) lies over \( p \) (with \( e(q|p) = p \), i.e. \( p \) is totally ramified in \( K_u \)) and the different exponent equals

\[
d(q|p) = (p - 1)(m + 1).
\]

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

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

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

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

\[
v_p^*(u) > 0 \iff p \in S(K_u|K).
\]
Suppose \( v_p^*(u) > 0 \). Then there exists \( t \in K \) such that \( \tilde{y} := y - t \) satisfies \( \tilde{y}^p - \tilde{y} = u - \wp t \equiv 0 \) mod \( p \). Hence \( p \) splits completely in \( K_u = K(\tilde{y}) \) according to [St2, p. 76]. Conversely, suppose \( p \) splits completely in \( K_u \). Then we can assume \( v_p(u) \geq 0 \) by the proof of (b) and, using [St2, pp. 96, 76], conclude that \( u \equiv \wp t \mod p \) for some \( t \in R_p \); hence \( v_p(u) \geq v_p(u - \wp t) > 0 \). 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 \( S_d = \bigcup_{n=1}^{\infty} \mathbb{P}_K^n \) be the set of all places of \( K|\mathbb{F}_q \) whose degree is divisible by \( d \), and \( K_d = \mathbb{F}_q^d \bar{K} \subseteq \bar{K} \) 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, \( p \in \mathbb{P}_K \) splits completely in \( K_d|K \) if and only if \( d \) divides \( \deg p \). 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 \( q \), so we can write \( \varphi_{L,p} \) instead of \( \varphi_{q,p} \) and \( G^s(L, p) \) instead of \( G^s(q|p) \). The subfield of \( L \) fixed by \( G^s(L, p) \) is denoted \( L^s(p) \) 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 \( p \) in \( L \). In particular, \( L^{-1}(p) \) is the **decomposition field** and \( L^0(p) \) is the **inertia field** of \( p \) 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 \( q\mid p \) satisfies

\[
\begin{align*}
d(q\mid p) &= \sum_{n=0}^{\infty} \left( |G_n(q\mid p)| - (G^0(q\mid p) : G^n(q\mid p)) \right) \\
&= \sum_{n=0}^{\infty} \left( [L : L^0(p)] - [L^n(p) : L^0(p)] \right).
\end{align*}
\]

**Proof.** For convenience, put \( G^s := G^s(L, p) \), \( \eta := \eta_{q\mid p} \) and \( \psi := \eta^{-1} \). Set \( t_0 := -1 \) and let \( 0 \leq t_1 < \cdots < t_r \) be the (other) jumps of the filtration \( (G^s)_{s \geq -1} \), i.e. the numbers \( s \geq -1 \) satisfying \( G^{s+\varepsilon} \not\subseteq G^s \) for all \( \varepsilon > 0 \). Obviously, all \( \psi(t_i) \) are integers, and \( t_0 = -1 \) is a jump iff \([F_q : F_p] > 1\). The bijection \( \eta \) is piecewise linear, its slopes being

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

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, \( t_r = f(L, p) - 1 \). Substituting the above equation into Hilbert's (lower index) Different Formula (see [St2, p. 124] or [CF, p. 36]) yields

\[
\begin{align*}
d(q\mid p) &= \sum_{n=0}^{\infty} (|G_n(q\mid p)| - 1) = \sum_{i=1}^{r} \sum_{s=\psi(t_{i-1})+1}^{\psi(t_i)} (|G^{t_i}| - 1) \\
&= \sum_{i=1}^{r} (\psi(t_i) - \psi(t_{i-1})) \frac{|G^0| - (G^0 : G^{t_i})}{(G^0 : G^{t_i})} \\
&= \sum_{i=1}^{r} (t_i - t_{i-1}) (|G^0| - (G^0 : G^{t_i})) \\
&= \sum_{i=1}^{r} \sum_{n=t_{i-1}+1}^{t_i} (|G^0| - (G^0 : G^n)) = \sum_{n=0}^{\infty} (|G^0| - (G^0 : G^n)).
\end{align*}
\]

\(\square\)

\(^2\)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 $f(L|K) \leq m = \sum_p m_p p \in D_K$. Then the discriminant of $L|K$ is given by

$$d(L|K) = [L : K]m - \sum_{p \in \mathcal{P}_K} \left( \sum_{n=0}^{m_p-1} [L^n(p) : K] \right)p.$$

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

$$d(L,p) = \sum_{q|p}[F_q : F_p]d(q|p)$$

$$= [L^0(p) : K] \sum_{n=0}^{m_p-1} ([L : L^0(p)] - [L^n(p) : L^0(p)])$$

$$= [L : K]m_p - \sum_{n=0}^{m_p-1} [L^n(p) : K]. \quad \square$$
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 $K^m_S$, where $S$ is a non-empty set of places and $m$ 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 $K^m_S|K$ will be characterized as the largest abelian extension of $K$ with conductor $\leq m$ 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 $[K^m_S:K]$, the determination of which is therefore attacked in Section 6.

In the whole of Part II we assume again that $K'|\bar{F}_q$ 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 $p$ of $K$ the multiplicative group $K^*_p$ is a topological group, in which the subgroups $U_p^{(n)}$ 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 $K^*_p$, $p \in \mathbb{P}_K$, with respect to their subgroups $U_p$ (see [CF, p. 68]). In other words,

$$\mathcal{I}_K := \left\{ (\alpha_p)_{p \in \mathbb{P}_K} \in \prod_{p \in \mathbb{P}_K} K^*_p \mid \alpha_p \in U_p \text{ for almost all } p \in \mathbb{P}_K \right\},$$

and the topology on $\mathcal{I}_K$ is the initial topology induced by the canonical projections $\mathcal{I}_K \to K^*_p$, $p \in \mathbb{P}_K$. Therefore, a subset of $\mathcal{I}_K$ is open iff it is a union of sets of the form $\prod_{p \in \mathbb{P}_K} V_p$ with $V_p \subseteq K^*_p$ open for all $p \in \mathbb{P}_K$ and $V_p = U_p$ for almost all $p \in \mathbb{P}_K$. It is readily verified that $\mathcal{I}_K$ is a topological group.
The canonical embedding of $K^*_p$ into $\mathcal{I}_K$ will be expressed by the symbol $[\ ]_p$, i.e. $[z]_p$ for $z \in K^*_p$ is the idèle $(\ldots, 1, z, 1, \ldots)$ having $z$ at its $p$-th position and 1 elsewhere. Clearly, the morphism $[\ ]_p$ 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 $\alpha = (\alpha_p)_{p \in \mathbb{P}_K} \in \mathcal{I}_K$ with $(\alpha_q)_{q \in \mathbb{P}_L} \in \mathcal{I}_L$, where $\alpha_q = \alpha_p$ for $q | p$. 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 $N_{L|K} : \mathcal{I}_L \rightarrow \mathcal{I}_K$ such that $N_{L|K}(\alpha, L|K) = (\prod_{q | p \in \mathbb{P}_K \setminus S} \varphi_{L,p}(\alpha_p) \nu_q(\alpha_q))_{p \in \mathbb{P}_K}$ (see [CF, p. 75]). Since $N_{L|K} L^* \subseteq K^*$, it induces a norm map $N_{L|K} : \mathcal{C}_L \rightarrow \mathcal{C}_K$, 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

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

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

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

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

(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 $(\cdot, L|K)$ 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 $\varphi_{L',p} = \varphi_{L,p}|_{L'}$. The behaviour of the Frobenius automorphism in towers, by applying weak approximation once more, implies that $N_{L|K}\mathfrak{I}_L$ is contained in the kernel of $(\cdot, L|K)$.

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 $\tilde{K} := K(\varphi^{-1}K)$. 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 $K^*N_{L|K}\mathfrak{I}_L$.

In order to finally prove the existence of the Artin map, $(\cdot, L|K)$ is defined as the product of all local Artin maps $(\cdot, L_p|K_p)$ with $p \in \mathbb{P}_K$, as indicated at the end of this section. By this definition $(\cdot, L|K)$ is continuous and also the representation by Frobenius automorphisms as required in (a) verifies trivially. The crucial point is to show that $(\cdot, L|K)$ 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 $\omega(\cdot)|_L = (\cdot, L|K)$ for all finite subextensions $L|K$ of $K|K$.\hfill\square
( , L|K) as defined on \( C_K \). As such it is continuous, too. Its kernel
\[
N_L := N_{L|K} C_L = K^* N_{L|K} \mathcal{I}_L / K^*
\]
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
\[
C_K / N_L \simeq G(L|K).
\]

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) \( L_1 \subseteq L_2 \iff N_{L_1} \supseteq N_{L_2} \).
(b) \( N_{L_1 L_2} = N_{L_1} \cap N_{L_2} \).
(c) \( N_{L_1 \cap L_2} = N_{L_1} N_{L_2} \).

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

It remains to show that \( N_{L_1 \cap L_2} \subseteq N := N_{L_1} N_{L_2} \). For \( i \in \{1, 2\} \), by Galois theory, \( (N, L_i|K) = G(L_i|L') \) for some intermediate field \( L' \) of \( L_i|K \), and by the Reciprocity Law, \( N \) is the kernel of \( (, L'|K) \), i.e. equals \( N_{L'} \). Using (a) we conclude \( L'_1 = L'_2 \subseteq L_1 \cap L_2 \) and \( N \supseteq N_{L_1 \cap L_2} \).

4.3. Existence Theorem. The map \( L \mapsto N_L \) is a 1–1 correspondence between the finite abelian extensions of \( K \) (within \( \bar{K} \)) and the open subgroups of finite index in \( C_K \).

Remarks on the proof. We follow [CF, pp. 201f]. Clearly the kernel \( N_L = N_{L|K} C_L \) of the continuous map \( (, L|K) : C_K \to G(L|K) \) is open and of finite index in \( C_K \). Moreover, \( N_L \) is uniquely determined by \( L \) according to 4.2(a).

Let us call a subgroup \( N \) of \( C_K \) normic if it is the norm group \( N_L \) of some abelian extension \( L|K \). We note that if \( N \) contains a normic subgroup \( N' \), say with class field \( L' \), then \( N \) is itself normic, for, by the Reciprocity Law, \( (N, L'|K) \) is a subgroup of \( G(L'|K) \), whose fixed field \( L \subseteq L' \) has norm group \( N_L = N \).
Part II – Ray Class Fields

It remains to show that any open subgroup $N$ of finite index in $C_K$ is normic. If the index $n = (C_K : N)$ 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 $N$ 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 $p \in P_K$ and denote by $L_p$ the completion of $L$ at any one of the places above $p$. (They are all $K_p$-isomorphic.) By [CF, p. 175], the composed morphism
\[
([\ ]_p, L|K) : K^*_p \rightarrow I_K \rightarrow G(L|K)
\]
has image $G^{-1}(L_p)$. In the course of the proof of the Reciprocity Law this morphism turned out to be equal to the local norm residue symbol $(\ , L_p|K_p)$, whose definition is given in [CF, p. 140]. By [CF, p. 155] we obtain:

4.4. Theorem. The homomorphism $([\ ]_p, L|K) : K^*_p \rightarrow G^{-1}(L_p)$ is surjective and maps $U^{(n)}_p$ onto $G^n(L_p)$ for all $n \in \mathbb{N}_0$.

In particular, $([U_p]|_p, L|K) = 1$ for all but the finitely many places $p \in P_K$ which ramify in $L$. Hence for each $\alpha = (\alpha_p) \in I_K$, by continuity,
\[
(\alpha, L|K) = \prod_{p \in P_K} ([\alpha_p|_p, L|K]),
\]
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 $C_K$ 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 $m = \sum p m_p p$ be such an $S$-cycle. Then we define the $S$-congruence subgroups mod $m$,
\[
I^m_S := \left( \prod_{p \in S} K^*_p \times \prod_{p \in P_K \setminus S} U^{(m_p)}_p \right) \cap I_K \quad \text{and} \quad C^m_S := K^* I^m_S / K^*.
\]
of $\mathcal{I}_K$ and $C_K$, respectively. (Here intersection with $\mathcal{I}_K$ is only necessary, of course, when $S$ is infinite.) For an arbitrary effective divisor $n = \sum_p n_p p$ of $K$ we set $\mathcal{I}_n := \mathcal{I}_{K \setminus \text{supp } n}$ and define

\[ \phi(n) := \prod_{p \in \mathbb{P}_K} (U_p : U_p^{(n_p)}) = \prod_{p \in \text{supp } n} (q^{\deg_p p} - 1)q^{(n_p - 1)\deg_p} \]

We note some elementary properties of the congruence subgroups.

5.1. Remark. Let $S \subseteq \mathbb{P}_K$ and $m = \sum_p m_p p$ be an $S$-cycle.

(a) If $T \subseteq S$ and $n \geq m$ is a $T$-cycle, then $\mathcal{I}_n T \subseteq \mathcal{I}_m S$ and $C_n T \subseteq C_m S$.
(b) If $T \subseteq \mathbb{P}_K$ and $n$ is a $T$-cycle, then $\mathcal{I}_S \mathcal{I}_n = \mathcal{I}_S \min\{m, n\}$, where the minimum is taken coefficientwise.
(c) The congruence subgroups $\mathcal{I}_n \emptyset$ and $C_n \emptyset$ with $n$ running through all effective divisors of $K$ form a basis of open neighbourhoods of $1$ in $\mathcal{I}_K$ and $C_K$, respectively.
(d) Both $\mathcal{I}_S m$ and $C_S m$ are open.
(e) We have $T_S^o / T_S^m \simeq \prod_p U_p / U_p^{(m_p)}$ and $(T_S^o : T_S^m) = \phi(m)$.
(f) The index $(C_K : C_S^m)$ is infinite for every effective divisor $n$ of $K$.
(g) $K^* \mathcal{I}_S = \mathcal{I}_K$ for any $n \geq 0$.
(h) $\mathcal{I}_S^m$ is topologically generated by its subgroups $[K_p^s]_p$, $p \in S$, and $[U_p^{(m_p)}]_p$, $p \in \mathbb{P}_K \setminus S$.

Proof. (a)–(e) are obvious.

(f) Choosing a place $p \in \mathbb{P}_K \setminus \text{supp } n$, the homomorphism $K_p^* \to \mathcal{I}_K / K_p^* \mathcal{I}_S^m$ induced by the embedding $[\ ]_p$ has kernel $U_p$. But $K_p^* / U_p \simeq \mathbb{Z}$.

(g) This is merely an idéal reformulation of the Weak Approximation Theorem 1.5.

(h) Let $\alpha = (\alpha_p)_{p \in \mathbb{P}_K} \in \mathcal{I}_S^m$ and $n = \sum_p n_p p$ be an effective divisor of $K$. Then the set $T := \{p \in \mathbb{P}_K | \alpha_p \notin U_p^{(n_p)}\}$ is finite and $\alpha \equiv \prod_{p \in T} [\alpha_p]_p \mod \mathcal{I}_S^m$. Thus the assertion follows by (b). \qed

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 $C_S^m$ in $C_K$ is indeed finite. In order to obtain an ideal theoretic interpretation of the corresponding factor group, we introduce the $S$-class group mod $m$, $A^m(O_S)$, defined as the
quotient of the group of fractional ideals of $\mathcal{O}_S$ prime to $m$ by its subgroup of principal ideals $z\mathcal{O}_S$ with $z \in K^* \cap I^m$. Note that $\mathcal{A}^m(\mathcal{O}_S) = \mathcal{A}(\mathcal{O}_S)$ is the usual $S$-class group defined in Section 2.

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

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

(b) The sequence

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

is exact.

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

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

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

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

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

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

We remark that $K_S^m$ 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 $K_S^m$ 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 $\mathbb{P}_K$, $m$ an $S$-cycle and $n$ a $T$-cycle.

(a) If $S \supseteq T$ and $m \leq n$, then $K_S^m \subseteq K_T^n$.

(b) $K_S^m \cap K_T^n = K_{ST}^{\min\{m,n\}}$. 

(c) If $S \supseteq T$, $m \leq n$ and $n$ is also an $S$-cycle, then $[K^n_S : K^m_S] \leq [K^n_T : K^m_T]$.

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

(b) By 5.1(b) we have $C^n_S C^n_T = C^{\min(m,n)}_{S,T}$, 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 $(\quad, K^n_S|K)$ induces an isomorphism $K^* T^n_S / K^* T^n_T \cong G(K^n_S|K^n_T)$, and likewise for $T$ instead of $S$. Because of 5.1(b), the natural map $K^* T^n_T / K^* T^n_T \rightarrow K^* T^n_S / K^* T^n_S$ 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 $f(L|K)$ is the smallest $S$-cycle $m$ such that $L$ is contained in $K^m_S$.

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

$f(L, p) \leq m_p \iff g^{mp}(L, p) = 1 \iff [U_p^{(mp)}]_p \subseteq K^* N_{L|K} I_L,$

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

$f(L|K) \leq m \iff T^n_S \subseteq K^* N_{L|K} I_L \iff C^n_S \subseteq N_L \iff L \subseteq K^n_S,$

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 $m$ an $S$-cycle. Then $K^n_S$ is the largest abelian extension $L$ of $K$ such that $S \subseteq S(L|K)$ and $f(L|K) \leq m$. Moreover, $\mathbb{F}_{q^d}$ with $d := \deg S$ is the full constant field of $K^n_S$.

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

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 $\mathbb{F}_{q^d} \subseteq K_d \subseteq K^n_S \subseteq K^n_S$. On the other hand, in order that $\mathbb{F}_{q^d}$ for some $d' \in \mathbb{N}$ be contained in $K^n_S$, $d'$ must divide the degree of every place in $S(K^n_S|K) \supseteq S$, 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 $K^e_S = \mathbb{F}_q dK = \mathbb{F}_q d(x)$ 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 $m$, as we see in our next

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

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

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

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

$$L^n(p) = L \cap K^m_{S,p+np} \quad \text{and} \quad L^{-1}(p) = L \cap K^m_{S,p} = L \cap K^m_{S,p \cup \{p\}}.$$  

In particular, writing $m = \sum_p m_p p$, the discriminant of $K^m_S|K$ is

$$\Delta(K^m_S|K) = [K^m_S : K] m - \sum_p \left( \sum_{n=0}^{m_p-1} [K^m_{S,p+np} : K] p \right).$$

**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 $L'$:

$$L' \subseteq L^n(p) \iff G(L|L') \supseteq G^n(L,p) \iff G^n(L',p) = 1 \iff n \geq f(L',p) \iff m \setminus p + np \geq f(L'|K) \iff L' \subseteq K^m_{S,p+np}.$$  

Similarly,

$$L' \subseteq L^{-1}(p) \iff G^{-1}(L',p) = 1 \iff p \in S(L'|K) \iff L' \subseteq K^m_{S,p} \iff L' \subseteq K^m_{S \cup \{p\}}.$$  

The last identity follows from the Discriminant Formula 3.7 since $f(K^m_S|K) \leq m$. □
Together with the Discriminant 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, $p \in \mathbb{P}_K \setminus S$ and $L$ an intermediate field of $K_S^{mp}|K_S^{(m-1)p}$ for some $m \in \mathbb{N}$. Then the genera of $K$ and $L$ are related as

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

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 $m$ be an $S$-cycle, $h = h_K$ the (divisor) class number and $g = g_K$ the genus of $K$. Then

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

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

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

Note that the genus of $K_S^m$ does not depend on $d$ but on $g$, $h$ and $m$ 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 $\mathcal{O}_S^*/\mathcal{O}_S^*$ when $m \neq o$. Hence the degree formulas follow from Proposition 5.2 and 5.1(e).

(b) Note that $K_S^m$ has the full constant field $\mathbb{F}_q$ according to Proposition 5.5. For $m \in \mathbb{P}_K$, we have $\phi(m) = q - 1$, hence $K_S^m = K_S^g$ by (a). Since $K_S^m|K$ is unramified, its discriminant is $o$. Hence the assertion in case $\deg m \leq 1$ follows from the Hurwitz Genus Formula 1.4.
For the other two cases, write \( m = \sum_p m_p \) and let \( p \in \text{supp} \, m \). Then
\[
\prod_{n=1}^{m_p-1} [K^m_S \backslash \mathfrak{p}^n : K] = \frac{hd}{q-1} \sum_{n=1}^{m_p-1} \phi(m) q^{(1-m_p) \deg \mathfrak{p}} q^{(n-1) \deg \mathfrak{p}} = \frac{hd}{q-1} \phi(m)(1 - q^{(1-m_p) \deg \mathfrak{p}}).
\]

If \( m = mp \) with \( p \in \mathbb{P}^m_K \) and \( m, n \in \mathbb{N} \), then \( m_p = 0 \), so (a) and the discriminant formula in Theorem 5.8 yield
\[
\mathfrak{d}(K^m_S|K) = \frac{hd\phi(mp)}{q-1} mp - \left( \frac{hd}{q-1} \phi(mp)(1 - q^{(1-m)n}) \right) mp = \frac{hd}{q-1} \left( m q^{(m-1)n}(q^n - 1) - q + 1 - q^{(m-1)n} + 1 \right) mp.
\]

If \( p \) is not the only place in \( \text{supp} \, m \), then \( [K^m_S \backslash \mathfrak{p} : K] = \frac{hd \phi(m)}{q-1 \phi(p)} q^{(1-m_p) \deg \mathfrak{p}} \), whence
\[
\mathfrak{d}(K^m_S|K) = \frac{hd\phi(m)}{q-1} \sum_{p \in \text{supp} \, m} \frac{hd}{q-1} \phi(p) \mathfrak{p}.
\]

In both cases the genus of \( K^m_S \) 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 \( [K^m_S : K] \) 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 \( m \). We divide the problem into three steps by considering two intermediate fields of \( K^m_S|K \), namely the Hilbert class field \( K^m_S \) and the field \( K^m_S \) with
\[
\mathfrak{m} := \sum_{p \in \text{supp} \, m} \mathfrak{p}.
\]

By Proposition 5.2(a) the extension \( K^m_S|K \) has group \( G(K^m_S|K) \simeq \mathcal{O}(\mathcal{O}_S) \). 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, $G(K^m_S|K^o_S)$ is by 5.2(b) isomorphic to $I^o_S/O^*_S\tilde{m}$. Therefore the degree $[K^m_S : K^o_S]$ divides $\phi(\tilde{m})/(q - 1)$ (cf. also Example 5.10), and can be determined as follows (for technical reasons we exclude the trivial case of $m = o$). Let $s := |S| - 1 \in \mathbb{N}_0$, and suppose we have computed $S$-units $u_1, \ldots, u_s$ such that $O^*_S = \langle \alpha, u_1, \ldots, u_s \rangle$, where $\alpha$ is a generator of $\mathbb{F}_q^*$. Write $R := \text{supp} m = \{p_1, \ldots, p_r\}$ with $r = |R| \in \mathbb{N}$. For each $j \in \{1, \ldots, r\}$ we set $d_j := q^{\text{deg} p_j} - 1$ and $c_j := d_j/(q - 1)$ and choose a generator $\omega_j$ of $\mathbb{F}_{p_j}^*$ such that $\omega_j^{c_j} = \alpha$. Let $D = (d_{ij})_{1 \leq i,j \leq r} \in \mathbb{Z}^{r \times r}$ with

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

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 $A = (a_{ij})_{1 \leq i,j \leq s,r} \in \mathbb{Z}^{s \times r}$ such that $\omega_j^{a_{ij}} = u_i + p_j \in \mathbb{F}_{p_j}$ for all $i \in \{1, \ldots, s\}$ and $j \in \{1, \ldots, r\}$. The (non-canonical) surjective group morphism

$$\mathbb{Z}^r \to I^o_S/O^*_S\tilde{m} \simeq \prod_{j=1}^{r} \mathbb{F}_{p_j}^*$$

$$(a_1, \ldots, a_r) \mapsto (\omega_j^{a_{ij}})_{1 \leq j \leq r}$$

gives rise to the exact sequence

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

where $N$ is the subgroup of $\mathbb{Z}^r$ generated by the rows of the matrix $A = (A_{ij})_{1 \leq i,j \leq s+r} \in \mathbb{Z}^{(s+r) \times r}$ of rank $r$. After some row transformations $T = (t_{ij})_{1 \leq i,j \leq s+r} \in \text{GL}_{s+r}(\mathbb{Z})$, we find a $B \in \mathbb{Z}^{r \times r}$ with $T(A) = (B)$. Because $G(K^m_S|K^o_S) \simeq \mathbb{Z}^r/N$, it now follows that

$$[K^m_S : K^o_S] = |\text{det } B|.$$ 

At the same time we have found a basis for the group $K^* \cap I^m_S$, which is needed in step three below.
Part II – Ray Class Fields

6.1. Lemma. With notation as above, the $S$-units
\[ \tilde{u}_i := \alpha^{t_{i,s}} \prod_{k=1}^{s} u_{tk}^t, \quad 1 \leq i \leq s, \]
form a basis of the free abelian group $K^* \cap T_S^m = \mathcal{O}_S^* \cap T_S^m$.

Proof. For $i \in \{1, \ldots, s\}$ and $j \in \{1, \ldots, r\}$ we have $\sum_{k=1}^{s} t_{ik}a_{kj} + t_{i,s+r}c_j \equiv 0 \mod d_j$ by definition of $T$; hence,
\[ \tilde{u}_i + p_j = \omega_j^{t_{i,s+r}c_j} \prod_{k=1}^{s} \omega_j^{t_{ik}a_{kj}} = 1. \]
This shows $\tilde{u}_1, \ldots, \tilde{u}_s \in T_S^m$.

Conversely, suppose $u = \alpha^{t_0} \prod_{k=1}^{s} u_{tk}^t \in \mathcal{O}_S^*$ with $t_0, \ldots, t_s \in \mathbb{Z}$ is contained in $T_S^m$. Then there are $t_{s+1}, \ldots, t_{s+r} \in \mathbb{Z}$ such that
\[ t_0c_j + \sum_{k=1}^{s} t_k a_{kj} + t_{s+r}d_j = 0 \quad \forall j \in \{1, \ldots, r\}. \]
Thus $t := (t_1, \ldots, t_{s+r-1}, t_0)$ satisfies $t \binom{A}{D} = 0$. Putting $\hat{t} = (\hat{t}_1, \ldots, \hat{t}_{s+r}) := tT^{-1}$, from
\[ \hat{t} \binom{0}{B} = \hat{t}T \binom{A}{D} = t \binom{A}{D} = 0 \]
we can conclude $\hat{t}_{s+1} = \cdots = \hat{t}_{s+r} = 0$ since the rows of $B$ are linearly independent. Therefore
\[ \prod_{i=1}^{s} \tilde{u}_i^{\hat{t}_i} = \prod_{i=1}^{s} \left( \alpha^{\hat{t}_i t_{i,s}} \prod_{k=1}^{s} u_{tk}^{\hat{t}_ik} \right) = \alpha^{t_0} \prod_{k=1}^{s} u_{tk}^{t_k} = u. \]

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

The rest of this section is devoted to the treatment of step three, the extension $K^*_S|K_S^m$. The Reciprocity Law tells us that
\[ G(K^*_S|K_S^m) \simeq K^* T_S^m / K^* T_S^m \simeq T_S^m / (K^* \cap T_S^m) T_S^m. \]
Writing $m = \sum_p m_p p$, we see that $J_m^n/I_m^n \cong \prod_{p \in \text{supp}(m)} U_p^{(1)}/U_p^{(m_p)}$ is a $p$-group.

We need to know what the structure of the groups $U_p^{(1)}/U_p^{(n)}/p$ with $p \in \mathbb{P}_K$ 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 

$$[a]_p := \min\{p^l | a \leq p^l, l \in \mathbb{N}_0\}$$

be the least $p$-power integer $\geq a$. 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 $p$ be a place of $K$, $\pi \in K_p$ a uniformizer at $p$, $B$ an $\mathbb{F}_p$-basis of $\mathbb{F}_p$ and $n \in \mathbb{N}$.

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

(b) There is a decomposition

$$U_p^{(1)}/U_p^{(n)} = \prod_{j \in \mathbb{N}^*_p} \langle (1 + \beta \pi^j)U_p^{(n)} \rangle$$

as a direct product of cyclic subgroups.

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

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

$$U_p^{(m)}/U_p^{(n)} \subseteq H$$

for $m \in \{1, \ldots, n\}$ by induction on $n - m$. For $m = n$ there is nothing to show.

Let $1 \leq m < n$ and $u \in U_p^{(m)}$. Set $l := v_p(m)$, then $u \equiv 1 + \omega^{p^l} \pi^{m} \mod U_p^{(m+1)}$ for some $\omega \in \mathbb{F}_p$. Writing $\omega = \sum_{\beta \in B} a_\beta \beta$ with $a_\beta \in \{0, \ldots, p - 1\}$, we see that

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

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

$$\prod_{\beta \in B} (1 + \beta \pi^j)^{a_\beta \pi^l} \equiv (1 + \omega \pi^j)^{p^l} \equiv u \mod U_p^{(m+1)}.$$
By the induction hypothesis, $U_p^{(m+1)} / U_p^{(n)} \subseteq H$, from which we may conclude $uU_p^{(n)} \in H$. So we have proved $U_p^{(1)} / U_p^{(n)} = H$. Since $(U_p^{(1)} : U_p^{(n)}) = q^{(n-1) \deg p}$, 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) $\left\lceil \frac{m+1}{j} \right\rceil_p / \left\lceil \frac{m}{j} \right\rceil_p = \begin{cases} p & \text{if there is } l \in \mathbb{N}_0 \text{ such that } m = j p^l, \\ 1 & \text{otherwise.} \end{cases}$

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

(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 $\left| \text{supp } m \right| = 1$, i.e. $\tilde{m} =: p \in \mathbb{P}_K \setminus S$. In this case the result is as follows.

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

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

for all $m \in \mathbb{N}$.

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

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

In general, all degrees $[K_S^m : K_S^n]$, for supp $m$ 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) $\sum_{i=1}^r r^i$ positive integers. A complete exposition of this result would make this section even more technical than it is already.
and set 
\[ \delta^{(m)} := \sum_{l=0}^{v_p(m)} \delta_m / p^l = |\{ i \in \{1, \ldots, s\} | n_i \leq m, n_i^* = m^*\}| \] for \( m \in \mathbb{N} \) and \( \delta^{(0)} := \delta_0 \). From 6.4 and 6.3(a) we derive the recursive degree formula

\[ [K_{S^{(m+1)p}} : K_{S^p}] = q^{\deg_p / p^{\delta^{(m)}}} \quad \forall m \in \mathbb{N}, \] (5)

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

6.5. Corollary. Let \( \emptyset \neq S' \subseteq S \). Then \( \delta^{(m)}_{S', p} \leq \delta^{(m)}_{S, p} \) 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 \( U_{p}^{(1)} \). As usual we denote by \( \mathbb{Z}_p = \lim_{\leftarrow} \mathbb{Z} / p^l \mathbb{Z} \) the ring of \( p \)-adic integers, the completion of \( \mathbb{Z} \) at \( v_p \). Identifying \( u \in U_p^{(1)} \) with the family \( (u U_p^{(n)})_{n \in \mathbb{N}} \), we can write

\[ U_p^{(1)} = \lim_{\leftarrow} U_p^{(1)}/U_p^{(n)}. \]

Since \( U_p^{(1)}/U_p^{(n)} \) is naturally a module over \( \mathbb{Z}/ [n]_p \mathbb{Z} \), and thereby a fortiori a \( \mathbb{Z}_p \)-module, the definition of \( u^a := (u U_p^{(n)})_{n \in \mathbb{N}} \) for \( u \in U_p^{(1)} \) and \( a \in \mathbb{Z}_p \) makes \( U_p^{(1)} \) a \( \mathbb{Z}_p \)-module (cf. [H, pp. 215ff]). For the proof of 6.4 it is important to know how linear independence in \( U_p^{(1)} \) 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 \( u_i \in U_p^{(1)}, i \in I \), is independent over \( \mathbb{Z} \) iff it is independent over \( \mathbb{Z}_p \).

Proof. See [Ki].

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

\[ U_p^{(1)}/U_p^{(n)} \to \mathbb{Z}^{(n)} := \prod_{j \in \mathbb{Z}_p} \left( \mathbb{Z}/ \mathbb{Z}[n/j]_p \right)^B \]

\[ c^{(n)} : \prod_{j \in \mathbb{Z}_p, \beta \in B} (1 + \beta \pi^j) u_j^{(n)} \to \left( c_{j, \beta} + \mathbb{Z}[n/j]_p \right)_{j \in \mathbb{Z}_p, \beta \in B}. \]

---

5Moreover, one has \( \deg \delta_{S', p} \leq \deg \delta_{S, p} \). But we shall not prove this here.
Passing to projective limits on both sides yields an isomorphism \( \zeta : U_p^{(1)} \cong Z := \lim_{\rightarrow} Z^{(n)} = \mathbb{Z}_p^{\mathbb{N}_p \times B} \) of \( \mathbb{Z}_p \)-modules (cf. Hasse’s One-Unit Theorem in [H, p. 227]), which makes the diagram

\[
\begin{array}{ccc}
U_p^{(1)} & \xrightarrow{\zeta} & Z \\
\downarrow & & \downarrow^{(n)} \\
U_p^{(1)}/U_p^{(n)} & \xrightarrow{\zeta^{(n)}} & Z^{(n)}
\end{array}
\]

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

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

\[
\nu : \left( z_{j\beta} \right)_{j \in \mathbb{N}_p} \rightarrow \left( \nu_{j\beta} \right)_{j \in \mathbb{N}_p} \rightarrow \min \left\{ j p^{\nu_p(z_{j\beta})} \mid j \in \mathbb{N}_p, \beta \in B \right\},
\]

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

6.7. Lemma. Let \( z, z' \in Z, a \in \mathbb{Z}_p \) and \( m \in \mathbb{N} \). Then

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

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

(c) The subgroup of \( Z^{(m)} \) generated by \( z^{(m)} \) has order \( \left| \langle z^{(m)} \rangle \right| = \left[ m/\nu(z) \right]_p \).

(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 \( z = \left( z_{j\beta} \right)_{j \in \mathbb{N}_p} \beta \in B \) and \( z' = \left( z'_{j\beta} \right)_{j \in \mathbb{N}_p} \beta \in B \).

(a) \( \nu(az) = \min \left\{ j p^{\nu_p(a)p^{\nu_p(z_{j\beta})}} \mid j \in \mathbb{N}_p, \beta \in B \right\} = p^{\nu_p(a)} \nu(z) \).

(b) \( \nu(z + z') \geq \min \left\{ j p^{\nu_p(z_{j\beta})}, j p^{\nu_p(z'_{j\beta})} \mid j \in \mathbb{N}_p, \beta \in B \right\} = \min \{ \nu(z), \nu(z') \} \).

(c) Write \( z^{(m)} = \left( c_{j\beta} + Z \left[ m/j \right]_p \right)_{j \in \mathbb{N}_p} \beta \in B \), with \( c_{j\beta} \in \mathbb{Z} \). For \( j \in \mathbb{N}_p \) and \( \beta \in B \),

we then have \( z_{j\beta} \equiv c_{j\beta} \mod \left[ m/j \right]_p \), and therefore \( c_{j\beta} + Z \left[ m/j \right]_p \in \mathbb{Z}/\mathbb{Z} \left[ m/j \right]_p \) has order

\[
\left| \left\langle c_{j\beta} + Z \left[ m/j \right]_p \right\rangle \right| = \max \left\{ 1, \left[ m/j \right]_p / p^{\nu_p(c_{j\beta})} \right\} = \left[ m/\left( j p^{\nu_p(z_{j\beta})} \right) \right]_p.
\]

It follows that

\[
\left| \left\langle z^{(m)} \right\rangle \right| = \max \left\{ \left[ m/\left( j p^{\nu_p(z_{j\beta})} \right) \right]_p \mid j \in \mathbb{N}_p, \beta \in B \right\} = \left[ m/\nu(z) \right]_p
\]

by definition of \( \nu \).
(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, $U_{S,p} := \mathcal{O}_S^* \cap U_p^{(1)} = K^* \cap T_p^*$ is free of rank $s$, say with basis$^6$ $(u_1, \ldots, u_s)$. Set $z_i = (z_{ij})_{j \in \mathbb{N}_0^*} := \zeta(u_i)$ for $i \in \{1, \ldots, s\}$. According to Kisilevsky’s Theorem 6.6, $u_1, \ldots, u_s$ and hence also $z_1, \ldots, z_s \in \mathcal{Z}$ are $\mathbb{Z}_p$-linearly independent. We can assume w.l.o.g. that

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

Write $n_1 = j_1 p^l$ with $j_1 := n_1^*$ and $l := v_p(n_1)$. By definition of $\nu$, there is $\beta_1 \in B$ such that $v_p(z_{1j_1\beta_1}) = l$. For $i \in \{2, \ldots, s\}$ we have $l \leq v_p(z_{ij_1\beta_1})$ 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 $z_2, \ldots, z_s$ by $\tilde{z}_2, \ldots, \tilde{z}_s$ yields a direct decomposition

$$\langle \hat{z}_1^{(m)}, \ldots, \hat{z}_s^{(m)} \rangle = \langle \hat{z}_1^{(m)} \rangle \oplus \langle \hat{z}_2^{(m)}, \ldots, \hat{z}_s^{(m)} \rangle$$

for all $m \in \mathbb{N}$, while $\langle \hat{z}_1^{(m)} \rangle \simeq \mathbb{Z}/\mathbb{Z}[m/n_1]_p$ by Lemma 6.7(c). We note that $\nu(\tilde{z}_i) \geq \nu(z_i) \geq n_1$ for $i \in \{2, \ldots, s\}$ and that $\tilde{z}_2, \ldots, \tilde{z}_s$ are again $\mathbb{Z}_p$-linearly independent. Hence we can apply the same procedure to $\tilde{z}_2, \ldots, \tilde{z}_s$ once more and so on. In this way, we obtain positive integers $n_1 \leq \cdots \leq n_s$ such that

$$U_{S,p} U_p^{(m)}/U_p^{(m)} \simeq \langle \hat{z}_1^{(m)}, \ldots, \hat{z}_s^{(m)} \rangle \simeq \prod_{j=1}^s \mathbb{Z}/\mathbb{Z}[m/n_i]_p$$

and, consequently,

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

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

$^6$In fact it would suffice to assume $\langle u_1, \ldots, u_s \rangle$ of finite index prime to $p$ in $U_{S,p}$.
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 \( p := p_4 \). Note that \( U_p^{(6)} = U_p^{(1)} \) and \( \delta_{S_3, p}^{(6)} = 1 \). It will suffice to work with “precision” \( n = 6 \).

We abbreviate \( (a + 8\mathbb{Z}, b + 2\mathbb{Z}, c + 2\mathbb{Z}) \in \mathbb{Z}^{(6)} \) by \( (a \ b \ c) \) and let

\[
\zeta^{(6)} : \ U_p^{(1)} / U_p^{(6)} \to \mathbb{Z}^{(6)} \\
\quad \ (1 + x)^a(1 + x^3)^b(1 + x^5)^c U_p^{(6)} \mapsto (a \ b \ c)
\]

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

\[
C := \left( \zeta^{(6)}(u_i/u_p^{(6)}) \right)_{1 \leq i \leq 4} = \begin{pmatrix}
0 & 0 & 0 \\
1 & 0 & 0 \\
2 & 1 & 1 \\
1 & 1 & 0
\end{pmatrix} \in (\mathbb{Z}^{(6)})^4.
\]

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

\[
\left( \zeta^{(6)}(u_i'U_p^{(6)}) \right)_{1 \leq i \leq 3} = T_3 C = \begin{pmatrix}
6 & 1 & 1 \\
0 & 0 & 1 \\
1 & 0 & 0
\end{pmatrix} \in (\mathbb{Z}^{(6)})^3.
\]

Applying the algorithm of the previous proof yields \( \delta_{S_1, p} = 1 + t^2, \ \delta_{S_2, p} = 1 + t^2 + t^5 \) and \( \delta_{S_3, p} = 1 + t + t^3 + t^5 \). By means of Theorem 6.4 or formula (5) we can now calculate the degrees \( [K_{S_2}^{mp} : K] = [K_{S_2}^{mp} : K_{S_2}^p] \) for any \( m \in \mathbb{N} \). The genera are obtained from Corollary 5.9. For \( m \in \mathbb{N}_0 \) we put \( K^{(m)} := K_{S_2}^{mp} \). Note that \( p = p_4 \) ramifies totally and \( p_0, p_1, p_2 \) split completely in \( K^{(m)} \).

From \( [K_{S_2}^{2p} : K] = 1 < 2 = [K_{S_2}^{2p} : K] \) we conclude by Proposition 5.5 that \( p_3 \notin S(K^{(m)}|K) \) and, consequently,

\[
N_{K^{(m)}} := \left| \mathfrak{p}_K^{1} \right| = 1 + 3[K^{(m)} : K]
\]
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.

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

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

$$N_K \leq q + 1 + 2g_K \sqrt{q}. \quad (6)$$

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. \quad \text{In fact (for each square } q, \text{ the Hermitian function field (see [St2, p. 198]) is a maximal function field of genus } (q - \sqrt{q})/2. \quad \text{Stichtenoth and Xing [SX] conjectured a large gap below this genus and showed that there are indeed smaller values of } g_K, \text{ for which } K \text{ 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 $[a]$ the integer part of $a \in \mathbb{R}$. 
7.2. Theorem (Serre). For any $K|\mathbb{F}_q$ we have:

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

(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 $\geq 16$ and $(\sqrt{q} - 1)^2/4 < g_K \neq (q - \sqrt{q})/2$, then $N_K \leq q - 1 + 2g\sqrt{q}$.

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 $g \leq 50$ 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 $\psi(t) = c_1t + \cdots + c_mt^m \in \mathbb{R}[t]$ with $c_1, \ldots, c_m \geq 0$ satisfying

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

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

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

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

$$F_m : \left[\frac{\pi}{m+1}, \frac{\pi}{m}\right] \to [0, 1] \quad \varphi \mapsto -\frac{\cos \frac{m+1}{2}\varphi}{\cos \frac{m-1}{2}\varphi}$$

would provide an estimate

$$\frac{1}{\cos \frac{m+1}{2}\varphi} \geq \psi(q^{-1/2}) - \psi(q^{1/2}).$$

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

$$F_m : \left[\frac{\pi}{m+1}, \frac{\pi}{m}\right] \to [0, 1] \quad \varphi \mapsto -\frac{\cos \frac{m+1}{2}\varphi}{\cos \frac{m-1}{2}\varphi}$$

would provide an estimate

$$\frac{1}{\cos \frac{m+1}{2}\varphi} \geq \psi(q^{-1/2}) - \psi(q^{1/2}).$$

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].
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 $\vartheta_q$ is again an isotonous homeomorphism. Finally we claim that also

$$\gamma_q : [q + 1, \infty) \to [0, \infty) \qquad N \mapsto 1 + \frac{(\sqrt{q}\vartheta_q(N) - 1)N}{q - 2\sqrt{q}\vartheta_q(N) + 1}$$

is strictly increasing. The isotony of $\gamma_q$ 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

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

and

$$\gamma_q(N) = \frac{1}{4q} \left( N - q^2 - 1 + \sqrt{(8q + 1)N^2 - (18q^2 + 16q + 2)N + q^4 + 8q^3 + 18q^2 + 8q + 1} \right)$$

for $N \in [q^{3/2} + 1, q^2 + 1]$, whence we see that $\gamma_q$ is strictly increasing on $[q + 1, q^2 + 1]$ as well.

### 7.4. Theorem (Oesterlè)

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

$$N_q(g) \leq \bar{N}_q(g) \quad \forall g \in N_0.$$
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

\[
(11) \quad \bar{N}_q(g) = q + 1 + \frac{1}{2} \left( \sqrt{8q + 1}g^2 + 4(q^2 - q)g - g \right)
\]

for \( g \in \left[ \frac{1}{2}(q - \sqrt{q}), \sqrt{\frac{q}{2}}(q - 1) \right] \).

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 \( N_7(3) \leq 23 \). From (11) we see that

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

Since \( N_7(3) \neq 22 \) by 7.2(b) we can conclude \( N_7(3) \leq 21 \). 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 \( g \geq 1 \) and that \( S \subseteq \mathbb{P}_K \) contains at least \( N > (\sqrt{q} - 1)(g - 1) \) rational places. Then

\[
h_S \leq h_q(g, N) := \vartheta_q^{-1}(t)/N \quad \text{with} \quad t := \frac{N + (q + 1)(g - 1)}{\sqrt{q}(N + 2g - 2)}.
\]

**Proof.** The restrictions on \( g \) and \( N \) ensure that \( 1/\sqrt{q} \leq t < 1 \), whereby \( h_q \) is well-defined. Let \( K' := K_S^g \) 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, \( N' := N_{K'} \geq h_S N \) since every place of \( S \) splits completely in \( K'|K \). For \( N' \leq q + 1 \), the claim of the proposition is obvious. Assume \( N' \geq q + 1 \). Then, by Oesterlé’s Theorem,

\[
\frac{g - 1}{N} \geq \frac{g' - 1}{N'} \geq \frac{\gamma_q(N') - 1}{N'} = \frac{\sqrt{q}\vartheta_q(N') - 1}{q - 2\sqrt{q}\vartheta_q(N') + 1}.
\]

Isolating \( \vartheta_q(N') \) in this inequality results in \( \vartheta_q(N') \leq t \), from which, by the isotony of \( \vartheta_q \), we conclude the assertion. \( \square \)
From the following lemma, which also helps us compute the bounds \( h_q(g, N) \), we see that \( \vartheta_q^{-1} \) is piecewise a \( \mathbb{Q}(\sqrt{q}) \)-rational function.

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

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

(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 \( 2 \leq m \in \mathbb{N} \). Then

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

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

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

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

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 \( \vartheta_q \). \( \square \)

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

\[
\begin{align*}
f_1(t) &= 1, 
&f_2(t) = -2t, 
&f_3(t) = -2t + 1, 
&f_4(t) = 4t^2 - 2, 
&f_5(t) = 4t^2 - 2t - 1, 
&f_6(t) = -8t^3 + 6t, 
&f_7(t) = -8t^3 + 4t^2 + 4t - 1, 
&f_8(t) = 16t^4 - 16t^2 + 2, 
&f_9(t) = 16t^4 - 8t^3 - 12t^2 + 4t + 1, 
&f_{10}(t) = -32t^5 + 40t^3 - 10t, 
&f_{11}(t) = -32t^5 + 16t^4 + 32t^3 - 12t^2 - 6t + 1, 
&f_{12}(t) = 64t^6 - 96t^4 + 36t^2 - 2, \ldots
\end{align*}
\]
(a) Let $K$ and $S$ be as in Example 2.7. By Lemma 7.7 we have

$$14\hbar_4(3, 14) = \vartheta_4^{-1}(\frac{3}{4}) = 1 + \frac{16 + 8u}{1 + 2u} \quad \text{with} \quad u = \frac{f_4(2/3)}{f_2(2/3)} = \frac{1}{6}$$

since $\frac{3}{4} \in [\cos \frac{\pi}{3}, \cos \frac{\pi}{4}]$. Hence $h_S \leq h_4(3, 14) = 1$ according to Proposition 7.6. By Corollary 2.2, we can therefore conclude that $K$ has divisor class number $h_K = \text{reg}_S = 512$.

(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 $(\mid P_d \mid )_{1 \leq d \leq 6} = (10, 9, 0, 18, 36, 108)$. Hence $Z_K(t) = 1 + 10t + 64t^2 + 310t^3 + 1273t^4 + 4648t^5 + 15700t^6 + \cdots$

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

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 $t := \frac{5\sqrt{3}}{9} \in [\cos \frac{\pi}{11}, \cos \frac{\pi}{12}]$ and $u := f_{12}(t)/f_{10}(t) = \frac{1633}{6525}\sqrt{3}$, consequently,$$
\vartheta_3^{-1}(t) = 1 + \frac{3^6 + 3^3\sqrt{3}u}{1 + \sqrt{3}u} = \frac{993101}{1904}$$

by Lemma 7.7. From Proposition 7.6 we obtain $h_S \leq h_3(6, 5) = \vartheta_3^{-1}(t)/5 = 993101/9520 < 105$. Since, on the other hand, $h_S$ divides $h_K = 109^2$, we can conclude that $h_S = 1$. \qed

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 $p \in \mathbb{P}_K^1 \setminus S$ is another rational place. Note that under these assumptions we have $h_S = h_K = 1$ and $I_S^q O_S^q I_p^q \simeq U_p/\mathbb{F}_q^* U_p^{(1)} = 1$, hence $K_S^q = K$ by Proposition 5.2. For $\alpha \in \mathbb{F}_q$ denote by $p_\alpha$ the zero of $x - \alpha$. After a transformation of the variable $x$ we can assume that $p = \infty$ is the pole of $x$ and that $p_0 \in S$.

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 $p$ and provide defining equations for the first few ray class fields.

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

8.1. Theorem. Under the above conditions, the $S$-description at $p$ equals

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

The proof depends on the following

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

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

$$\prod_{i=1}^{s} \left( (1 - \alpha_i \pi)U_p^{(s+1)} \right) \subseteq U_p^{(1)}/U_p^{(s+1)}$$

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

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

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

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

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

Proof of the theorem. Write $\delta_{S,p} = 1 + \sum_{n \in \mathbb{N}} \delta_n t^n$ with $\delta_1, \delta_2, \ldots \in \{0, 1\}$. By the lemma we know that $K_{S}^{(s+1)p} = K_{S,p}^{p}$. According to the recursive degree formula (5) in Section 6, this implies $\delta_{S,p}^{(m)} = 1$ for $m \in \{1, \ldots, s\}$, which in turn yields $\delta_1 = \cdots = \delta_s = 1$. Since $\delta_{S,p}(1) = s + 1$, we obtain the assertion.
Note that $p$ is totally ramified in $K_S^{mp}$ for all $m \in \mathbb{N}_0$ since $K_S^0 = K$ is the inertia field of $p$ in $K_S^{mp}$. Furthermore, if $S' \subseteq \mathbb{P}_K^1$ satisfies $|S'| - 1 > s$, then $K_S^{(s+2)p} = K \subseteq K_S^{(s+2)p}$ according to Theorem 8.1. Consequently for all $m \geq s + 2$, by Proposition 5.5, $S = S(K_S^{mp}|K) \cap \mathbb{P}_K^1$ and therefore $K_S^{mp}$ has exactly

$$N_{K_S^{mp}} = 1 + [K_S^{mp}: K](s + 1)$$

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 $K_S^{mp}$. As an orientation we include (the integer part of) the Oesterlé bound in the following tables.

<table>
<thead>
<tr>
<th>$q = 5$</th>
<th>$s$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m$</td>
<td>3</td>
<td>4</td>
<td>5-6</td>
<td>7</td>
<td>4</td>
<td>5-6</td>
<td>7</td>
<td>8</td>
<td>5-6</td>
</tr>
<tr>
<td>$[K_S^{mp}: K]$</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>25</td>
<td>25</td>
<td>25</td>
<td>125</td>
<td>125</td>
<td>125</td>
</tr>
<tr>
<td>$g_{K_S^{mp}}$</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>10</td>
<td>22</td>
<td>34</td>
<td>56</td>
<td>70</td>
<td>172</td>
</tr>
<tr>
<td>$N_{K_S^{mp}}$</td>
<td>11</td>
<td>16</td>
<td>21</td>
<td>26</td>
<td>51</td>
<td>76</td>
<td>101</td>
<td>126</td>
<td>251</td>
</tr>
<tr>
<td>$[N_5(g_{K_S^{mp}})]$</td>
<td>14</td>
<td>19</td>
<td>25</td>
<td>34</td>
<td>60</td>
<td>83</td>
<td>125</td>
<td>150</td>
<td>324</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$q = 7$</th>
<th>$s$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7-8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m$</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>$[K_S^{mp}: K]$</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>49</td>
<td>49</td>
<td>49</td>
<td>49</td>
</tr>
<tr>
<td>$g_{K_S^{mp}}$</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>12</td>
<td>15</td>
<td>21</td>
<td>45</td>
<td>69</td>
<td>93</td>
</tr>
<tr>
<td>$N_{K_S^{mp}}$</td>
<td>15</td>
<td>22</td>
<td>29</td>
<td>36</td>
<td>43</td>
<td>50</td>
<td>99</td>
<td>148</td>
<td>197</td>
</tr>
<tr>
<td>$[N_7(g_{K_S^{mp}})]$</td>
<td>22</td>
<td>32</td>
<td>42</td>
<td>52</td>
<td>60</td>
<td>77</td>
<td>140</td>
<td>198</td>
<td>254</td>
</tr>
</tbody>
</table>

We want to write the first few $K_S^{mp}$ 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 $s = p - 1$.\footnote{It is not hard to derive from the proof of 6.4 that if $m$ is larger than this, then $G(K_S^{mp}|K)$ is no longer of exponent $p$, i.e. $K_S^{mp}|K$ can no longer be written as an Artin-Schreier extension in the sense of 3.3.}

Then

$$K_S^{\infty} = K(\varphi^{-1}u_n | n \in \mathbb{N}_p^*, \tilde{s} < n < m).$$
Proof. Set $J := \{ n \in \mathbb{N}_p^* \mid \tilde{s} < n < m \}$ and $L := K(\wp^{-1}u_n \mid n \in J)$. By 3.3(b) and (c), the extension $L|K$ has conductor $f(L|K) \leq m\infty$ and splitting set $S \subseteq S(L|K)$; hence, $L \subseteq K_S^{\infty\infty}$ 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

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

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

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. $S = \mathbb{F}_K^1 \setminus \{p\}$. In this case, the $S$-description at $p$ 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 $\mathbb{Z}/(q-1)\mathbb{Z} \simeq \mathbb{F}_q^\ast$. 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 $p$ is

$$\delta_{S,p} = 1 + \sum_{n \in \mathbb{N}} e_n t^n$$
Proof. See [La3].

Thus the recursive degree formula (5) simplifies to
\[ K^{(m+1)p} : K^p S = q/p^{e_m} \quad \forall m \in \mathbb{N}. \]

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 \( K^{p^m} | K^{p^{m-1}} \) 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 \( p \) in \( L_l \) is \( L_l^0(p) = L_l \cap K^p = K \); hence, \( p \) is totally ramified in \( L_l \). Therefore
\[ N_{L_l} = 1 + p^l q \quad \forall l \in \mathbb{N}_0. \]

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 \( \delta_{S,p} = 1 + 4t + 4t^3 + 2t^5 + 4t^7 + t^{15} \) by Lauter’s Theorem. The degrees of the extensions \( K^{p^m} | K \), as computed by means of (13) for the first few values of \( m \), are as follows
\[
\begin{array}{|c|c|c|c|c|c|c|c|c|c|c|}
\hline
\hline
[K^{p^m} : K] & 1 & 4 & 64 & 2^8 & 2^{12} & 2^{16} & 2^{19} & 2^{23} & 2^{27} & 2^{31} & 2^{37} & \\
\hline
\end{array}
\]

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 \( 1 \leq l \leq 11 \) in the table below, the last row of which gives (the integer part of) the Oesterlé bound.

\[
\begin{array}{|c|c|c|c|c|c|c|c|c|c|}
\hline
l & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\
\hline
\bar{g}_{L_l} & 2 & 6 & 22 & 54 & 118 & 246 & 534 & 1110 & 2390 & 4950 & 10070 \\
\hline
N_{L_l} & 33 & 65 & 129 & 257 & 513 & 1025 & 2049 & 4097 & 8193 & 16385 & 32769 \\
\hline
[N_{16(g_{L_l})}] & 33 & 65 & 150 & 309 & 590 & 1135 & 2271 & 4496 & 9211 & 18489 & 36503 \\
\hline
\end{array}
\]

8.7. Lemma. Write \( q = p^e \) with \( e \in \mathbb{N} \).
\[(a) \quad \text{We have } e_{q-1} = 1, e_n = 0 \text{ for } q - q/p \leq n < q - 1, \text{ and } e_{q-1-g/p} = e.\]
\[(b) \quad \text{Let } e \text{ be even and } r := \sqrt{q}. \text{ Then } e_n = e \text{ for } n \in \{1, \ldots, 2r\} \setminus (p\mathbb{Z} \cup \{r+1\}). \text{ Moreover, } e_{r+1} = e/2 \text{ and } e_{2r+1} = 0.\]
\[(c) \quad \text{Let } e \text{ be odd and } r := \sqrt{pq}. \text{ Then } e_n = e \text{ for } n \in \{1, \ldots, r\} \setminus p\mathbb{Z} \text{ and } e_n = 0 \text{ for } n \in \{r, \ldots, r+p\}.\]
Proof. (a) Clearly, the $G$-orbit of $q - 1$ is $G(q - 1) = \{q - 1\}$; hence $e_{q-1} = 1$. Let $q - q/p \leq n < q - 1$. Then $q \neq p$ and $p - 1 \leq n':= pn - (p-1)(q-1) < q-1$. 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

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

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

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

$$n \leq p'n \in \{p', \ldots, 2q/p - p'\} \subseteq Q$$

for $0 \leq l < e/2$.

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

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

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

Finally we have

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

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

$$n \leq p'n \in \{p', \ldots, q - p'\} \subseteq Q$$

for $0 \leq l < (e - 1)/2$.

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

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

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

As in the lemma, we set $r := \sqrt{q}$ or $\sqrt[r]{q}$ according to whether $q$ is a square or not. From (13) and 8.7(b) and (c) we conclude $K_S^{(r+1)p} = K$. Furthermore we obtain two canonical fields, namely $K_S^{(r+2)p}$ and $K_S^{(2r+2)p}$ of degree $r$ and $rq$ over $K$ if $q$ is a square, and $p - 1$ canonical fields $K_S^{(r+i)p}$ with $1 \leq i < p$ 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 $L_i$ 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 $g_{L_i} = \begin{cases} \frac{1}{2}(p^i - 1) & \text{for } 0 \leq l \leq e/2, \\ \frac{1}{2}(2p^i - r - 1) & \text{for } e/2 \leq l \leq 3e/2. \end{cases}$

(b) If $e$ is odd, then

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

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

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

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

In particular, if $e$ is even, then $L_0, \ldots, L_{e/2}$ are maximal, and moreover, according to [RS], $L_{e/2} = K_S^{(r+2)p}$ is a Hermitian function field. If $e$ is odd and $p = 2$ or $p = 3$, then $K_S^{(r+p)p} = L_{(p-1)e}$ 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 $y_1, \ldots, y_{p-1} \in \bar{K}$ satisfy $y_i^q - y_i = x^{ir/p}(x^q - x)$. Then

$$K_S^{(r+i+1)\infty} = K(y_1, \ldots, y_i) \quad \text{for} \quad i \in \{1, \ldots, p-1\}.$$
(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 $\Gamma := \{ \gamma \in \mathbb{F}_q \mid \gamma^r + \gamma = 0 \} = \{ \beta^r - \beta \mid \beta \in \mathbb{F}_q \} \cong \mathbb{F}_q / \mathbb{F}_r \cong \mathbb{F}_r$, and set

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

for $\gamma \in \Gamma$; then $\varphi y_\gamma = -(\gamma y)^r + \gamma y = \gamma x^{r+1}$. Since $\Gamma x^{r+1} \cap \varphi K = 0$, from 3.3 we can conclude $K(y) = K(y_\gamma \mid \gamma \in \Gamma)$ and $f(K(y)|K) = (r + 2)\infty$. 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 $\varphi z^\beta = \beta x^{2r}(x^q - x) =: u_\beta$ by (15), and

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

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

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

has $rq$ elements and $\varphi K = 0$, from 3.3(b)-(d) we obtain $K(y, z) = K(y_\gamma, z^\beta \mid \gamma \in \Gamma, \beta \in \mathbb{F}_q)$, $f(K(y, z)|K) = (2r + 2)\infty$ 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 $[K_i : K] \leq q^i$ over $K$. For $\beta \in \mathbb{F}_q$ we have $\varphi y_i^\beta = \beta x^{ir/p}(x^q - x) =: u_{i,\beta}$ by (15), and

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

satisfies $\varphi t_{i,\beta} = \beta x^{q+i/p} - \beta^r x^{r+i}$, implying $\tilde{u}_{i,\beta} := u_{i,\beta} - \varphi t_{i,\beta} = \beta^r x^{r+i} - \beta x^{2r+1}$ 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

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

has $q^i$ elements and $\tilde{V}_i \cap \varphi K = 0$, applying 3.3(b)-(d) shows that $K_i = K(y_j \mid 1 \leq j \leq i, \beta \in \mathbb{F}_q)$, $[K_i : K] = q^i$, $f(K_i|K) = (r + i + 1)\infty$ and $S \subseteq S(K_i|K)$. Therefore $K_S^{(r+i+1)\infty} = K_i$ according to Proposition 5.5. $\square$
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 $S \subseteq \mathbb{P}_1^K$ and a place $p \in \mathbb{P}_K \setminus S$ and consider the intermediate fields $L$ of $K^{mp}_S | K^{(m-1)p}_S$ for $m \in \mathbb{N}$. From Section 6 and Corollaries 2.2 and 5.9 we recall the formulas

$$(16) \quad h_S \text{ reg}_S = h_K,$$

$$(17) \quad [K^o_S : K] = h_S, \quad [K^p_S : K^o_S] = \frac{q^{\deg p} - 1}{(q - 1)^{\delta_{S,p}^{(0)}}},$$

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

and

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

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

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

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 $u_1, \ldots, u_s$ 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 $h_q(g_K, N_K)$ for $h_{S_0}$ established in Proposition 7.6 is less than 2 and that $\text{reg}(u_1, \ldots, u_s) = h_K$ and thereby prove $\mathcal{O}_{S_0}^* = \mathbb{F}_q^* \times \langle u_1, \ldots, u_s \rangle$. 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 $\mathbb{P}_K^1 \setminus \{p\}$, 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 $p \in S_0$, the $S_0$-regulator and the bound $h_q(g_K, N_K)$. While the rational places are specified by the table of $S_0$-units, other places $p$, which are possibly needed, are given in the form $p = (z_0, \ldots)$, meaning that $p$ is the common zero of $z_0, \ldots$ 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 $f(L|K) = mp$ with $p \in \mathbb{P}_K$ and $m \in \mathbb{N}_0$. Thus $L$ is any intermediate
field of $K_S^m|\mathbb{F}_2$ other than $K_S^{(m-1)p}$ (or of $K_S|\mathbb{F}_2$ if $m = 0$) having degree $[L:K]$ as given in the table’s fourth column. The lower bound for $N(g)$ 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 $p_0 = (x), p_1 = (x+1), p_2 = (1/x), p_3 = (x^2 + x + 1), p_4 = (x^4 + x + 1)$ and $p_5 = (x^6 + x^2 + 1)$ of $K$. The relevant $S$-class numbers and $S$-descriptions are given below.

<table>
<thead>
<tr>
<th>$u_1 = x$</th>
<th>$p_0$</th>
<th>$p_1$</th>
<th>$p_2$</th>
<th>$p_3$</th>
<th>$p_4$</th>
<th>$p_5$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$u_2 = x + 1$</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>-1</td>
<td>0</td>
</tr>
<tr>
<td>$u_3 = x^2 + x + 1$</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>-1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$u_4 = y$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-2</td>
<td>2</td>
</tr>
<tr>
<td>$u_5 = y + x$</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>-1</td>
</tr>
</tbody>
</table>

We have $h_2(1, 4) = 5/4 < 2$ and $\text{reg}(u_1, \ldots, u_5) = 4 = h_K$. Apart from the rational places also $p_4 = (1/x) \in \mathbb{F}_2$, $p_5 = (x^2 + x + 1) \in \mathbb{F}_2^2$ are used. The relevant $S$-class numbers and $S$-descriptions are given below.

(2a) $S = \{p_0, p_2\}, h_S = 1, \delta_{S,p_4} = 1 + t$.

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 $S_0 := \{p_0, \ldots, p_5\}$ and $S_0$-units $u_1, \ldots, u_5$ are given by the following table:

<table>
<thead>
<tr>
<th>$u_1 = x$</th>
<th>$p_0$</th>
<th>$p_1$</th>
<th>$p_2$</th>
<th>$p_3$</th>
<th>$p_4$</th>
<th>$p_5$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$u_2 = x + 1$</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>-2</td>
<td>-1</td>
</tr>
<tr>
<td>$u_3 = x^2 + x + 1$</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>-1</td>
<td>0</td>
</tr>
<tr>
<td>$u_4 = y$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-2</td>
<td>2</td>
</tr>
<tr>
<td>$u_5 = y + x$</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>-1</td>
</tr>
</tbody>
</table>

We have $h_2(1, 4) = 5/4 < 2$ and $\text{reg}(u_1, \ldots, u_5) = 4 = h_K$. Apart from the rational places also $p_4 = (1/x) \in \mathbb{F}_2$, $p_5 = (x^2 + x + 1) \in \mathbb{F}_2^2$ are used. The relevant $S$-class numbers and $S$-descriptions are given below.

(2a) $S = \{p_0, p_2\}, h_S = 1, \delta_{S,p_4} = 1 + t$.

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 $S_0 := \{p_0, \ldots, p_4\}$ and $S_0$-units $u_1, \ldots, u_4$ are given by the following table:

<table>
<thead>
<tr>
<th>$u_1 = x$</th>
<th>$p_0$</th>
<th>$p_1$</th>
<th>$p_2$</th>
<th>$p_3$</th>
<th>$p_4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$u_2 = x + 1$</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>-2</td>
</tr>
<tr>
<td>$u_3 = y$</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>-2</td>
</tr>
<tr>
<td>$u_4 = y + x$</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>-3</td>
</tr>
</tbody>
</table>

We have $h_2(1, 5) = 1$ and $\text{reg}(u_1, \ldots, u_5) = 5 = h_K$. Apart from the rational places also $p_5 = (x^3 + x + 1) \in \mathbb{F}_2^2$, $p_6 = (x^7 + x + 1, y + x^6 + x^5 + x^2 + x) \in \mathbb{F}_2^7$ are used. The relevant $S$-class numbers and $S$-descriptions are given below.
(1a) $S = \{p_0\}$, $h_S = 5$, $\delta_{S,p_1} = 1$.

(5a) $S = \{p_0, p_1, p_2, p_3, p_4\}$, $h_S = 1$, $\delta_{S,p_5} = 63 + 4t$, $\delta_{S,p_6} = 127 + 4t$.

9.4. Example. Let $K|\mathbb{F}_2$ and $p_0, \ldots, p_4$ 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) $S = \{p_0, p_1, p_2\}$, $h_S = 1$, $\delta_{S,p_3} = 1 + t^2 + t^5$.

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 $S_0 := \{p_0, \ldots, p_6\}$ and $S_0$-units $u_1, \ldots, u_6$ are given by the following table:

<table>
<thead>
<tr>
<th>$u_1 = x$</th>
<th>$p_0$</th>
<th>$p_1$</th>
<th>$p_2$</th>
<th>$p_3$</th>
<th>$p_4$</th>
<th>$p_5$</th>
<th>$p_6$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$u_2 = x + 1$</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$u_3 = x^3 + x + 1$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>$u_4 = y$</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$u_5 = y + x$</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>$u_6 = (x^3 + x + 1)y + 1$</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>0</td>
</tr>
</tbody>
</table>

We have $h_2(2, 6) = (893 + 306\sqrt{2})/1262 < 2$ and $\text{reg}(u_1, \ldots, u_6) = 19 = h_K$. Apart from the rational places also $p_6 = (x^3 + x + 1) \in \mathbb{P}_K^1$ is used. The relevant $S$-class numbers and $S$-descriptions are given below.

(1a) $S = \{p_1\}$, $h_S = 19$.

(4a) $S = \{p_1, p_2, p_4, p_5\}$, $h_S = 1$, $\delta_{S,p_0} = 1 + t + t^2 + t^3$.

(5a) $S = \{p_1, p_2, p_3, p_4, p_5\}$, $h_S = 1$, $\delta_{S,p_0} = 1 + t + t^3 + t^5 + t^7$.

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 $S_0 := \{p_0, \ldots, p_6\}$ and $S_0$-units $u_1, \ldots, u_6$ are given by the following table:

<table>
<thead>
<tr>
<th>$u_1 = x$</th>
<th>$p_0$</th>
<th>$p_1$</th>
<th>$p_2$</th>
<th>$p_3$</th>
<th>$p_4$</th>
<th>$p_5$</th>
<th>$p_6$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$u_2 = x + 1$</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$u_3 = x^2 + x + 1$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$u_4 = y$</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$u_5 = (x^2 + x + 1)y + 1$</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>$u_6 = (x^2 + x + 1)y + x^2$</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>2</td>
</tr>
</tbody>
</table>

We have $h_2(3, 6) = 195/146 < 2$ and $\text{reg}(u_1, \ldots, u_6) = 52 = h_K$. Apart from the rational places also $p_6 = (x^2 + x + 1) \in \mathbb{P}_K^2$, $p_7 = (x^3 + x^2 + 1) \in \mathbb{P}_K^6$ are used. The relevant $S$-class numbers and $S$-descriptions are given below.

(3a) $S = \{p_0, p_3, p_4\}$, $h_S = 4$, $\delta_{S,p_7} = 21 + 2t$.

(4a) $S = \{p_1, p_2, p_3, p_4\}$, $h_S = 1$, $\delta_{S,p_0} = 1 + t + t^5 + t^9$.

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 $S_0 := \{p_0, \ldots, p_6\}$ and $S_0$-units $u_1, \ldots, u_6$
are given by the following table:

<table>
<thead>
<tr>
<th></th>
<th>( P_0 )</th>
<th>( P_1 )</th>
<th>( P_2 )</th>
<th>( P_3 )</th>
<th>( P_4 )</th>
<th>( P_5 )</th>
<th>( P_6 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( u_1 = x )</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>-1</td>
<td>-1</td>
<td>-1</td>
</tr>
<tr>
<td>( u_2 = x + 1 )</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>-1</td>
<td>-1</td>
<td>-1</td>
</tr>
<tr>
<td>( u_3 = y )</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>-2</td>
<td>-1</td>
</tr>
<tr>
<td>( u_4 = y + 1 )</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>-2</td>
<td>-1</td>
</tr>
<tr>
<td>( u_5 = y + x )</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>-1</td>
<td>-2</td>
<td>0</td>
</tr>
<tr>
<td>( u_6 = y + x^2 )</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>-2</td>
<td>-2</td>
<td>2</td>
</tr>
</tbody>
</table>

We have \( h_2(3,7) = 911/853 < 2 \) and \( \text{reg}(u_1, \ldots, u_6) = 71 = h_K \). The relevant \( S \)-class numbers and \( S \)-descriptions are given below.

(6a) \( S = \{p_1, p_2, p_3, p_4, p_5, p_6\}, h_S = 1, \delta_{S,p_0} = 1 + t + t^3 + t^5 + t^7 + t^9 \).

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 \( S_0 := \{p_0, \ldots, p_7\} \) and \( S_0 \)-units \( u_1, \ldots, u_7 \) are given by the following table:

<table>
<thead>
<tr>
<th></th>
<th>( P_0 )</th>
<th>( P_1 )</th>
<th>( P_2 )</th>
<th>( P_3 )</th>
<th>( P_4 )</th>
<th>( P_5 )</th>
<th>( P_6 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( u_1 = x )</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>( u_2 = x + 1 )</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>-4</td>
</tr>
<tr>
<td>( u_3 = y )</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>( u_4 = y + 1 )</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>6</td>
</tr>
<tr>
<td>( u_5 = y + x^2 )</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>( u_6 = y^2 + xy )</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>( u_7 = y^2 + xy + x^3 + x^2 )</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

We have \( h_2(4,8) = 1571/1472 < 2 \) and \( \text{reg}(u_1, \ldots, u_7) = 260 = h_K \). The relevant \( S \)-class numbers and \( S \)-descriptions are given below.

(4a) \( S = \{p_3, p_4, p_5, p_6\}, h_S = 1, \delta_{S,p_7} = 1 + t^3 + t^4 + t^9 \).

(6a) \( S = \{p_0, p_1, p_2, p_4, p_5, p_6\}, h_S = 1, \delta_{S,p_3} = 1 + t + t^3 + t^5 + t^7 + t^{13} \).

(7a) \( S = \{p_0, p_1, p_2, p_4, p_5, p_6, p_7\}, h_S = 1, \delta_{S,p_3} = 1 + t + t^3 + t^5 + t^7 + t^9 + t^{13} \).

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 \( S_0 := \{p_0, \ldots, p_8\} \) and \( S_0 \)-units \( u_1, \ldots, u_8 \) are given by the following table:

<table>
<thead>
<tr>
<th></th>
<th>( P_0 )</th>
<th>( P_1 )</th>
<th>( P_2 )</th>
<th>( P_3 )</th>
<th>( P_4 )</th>
<th>( P_5 )</th>
<th>( P_6 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( u_1 = x )</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>( u_2 = x + 1 )</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>( u_3 = y )</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>( u_4 = y + x )</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>( u_5 = y^2 + y )</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>( u_6 = y^2 + y + x^3 + x^2 )</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>( u_7 = y^2 + (x^2 + x + 1)y )</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>( u_8 = y^2 + (x^2 + x + 1)y + x^3 + x^2 )</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>4</td>
<td>2</td>
</tr>
</tbody>
</table>

We have \( h_2(5,9) = \frac{24230319 + 1494360 \sqrt{2}}{24972319} < 2 \) and \( \text{reg}(u_1, \ldots, u_8) = 975 = h_K \). The relevant \( S \)-class numbers and \( S \)-descriptions are given below.

(7a) \( S = \{p_1, p_3, p_4, p_5, p_6, p_7, p_8\}, h_S = 1, \delta_{S,p_0} = 1 + t + t^3 + t^5 + t^7 + t^9 + t^{15} \).

(8a) \( S = \{p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8\}, h_S = 1, \delta_{S,p_0} = 1 + t + t^3 + t^5 + t^7 + t^9 + t^{11} + t^{15} \).
The outgrowth of Examples 9.1–9.9 is gathered in the table below.

<table>
<thead>
<tr>
<th>$g$</th>
<th>$N_2(g)$</th>
<th>$K, S$</th>
<th>$[L : K]$</th>
<th>$(L:K)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>10</td>
<td>9.3(1a)</td>
<td>10</td>
<td>$2p_4$</td>
</tr>
<tr>
<td>7</td>
<td>10</td>
<td>9.3(5a)</td>
<td>2</td>
<td>$2p_5$</td>
</tr>
<tr>
<td>8</td>
<td>11</td>
<td>9.5(5a)</td>
<td>2</td>
<td>$10p_0$</td>
</tr>
<tr>
<td>9</td>
<td>12</td>
<td>9.1(3a)</td>
<td>4</td>
<td>$4p_3$</td>
</tr>
<tr>
<td>10</td>
<td>13</td>
<td>9.4(3a)</td>
<td>4</td>
<td>$4p_0$</td>
</tr>
<tr>
<td>12</td>
<td>14–15</td>
<td>9.1(2a)</td>
<td>7</td>
<td>$p_5$</td>
</tr>
<tr>
<td>14</td>
<td>15–16</td>
<td>9.1(1a)</td>
<td>15</td>
<td>$p_1$</td>
</tr>
<tr>
<td>15</td>
<td>17</td>
<td>9.1(2b)</td>
<td>8</td>
<td>$7p_2$</td>
</tr>
<tr>
<td>16</td>
<td>17–18</td>
<td>9.9(8a)</td>
<td>2</td>
<td>$14p_0$</td>
</tr>
<tr>
<td>17</td>
<td>17–18</td>
<td>9.1(1a)</td>
<td>16</td>
<td>$5p_2$</td>
</tr>
<tr>
<td>19</td>
<td>20</td>
<td>9.3(5a)</td>
<td>4</td>
<td>$2p_5$</td>
</tr>
<tr>
<td>20</td>
<td>19–21</td>
<td>9.5(1a)</td>
<td>19</td>
<td>$a$</td>
</tr>
<tr>
<td>22</td>
<td>21–22</td>
<td>9.5(5a)</td>
<td>4</td>
<td>$12p_0$</td>
</tr>
<tr>
<td>27</td>
<td>24–25</td>
<td>9.2(2a)</td>
<td>12</td>
<td>$3p_4$</td>
</tr>
<tr>
<td>28</td>
<td>25–26</td>
<td>9.4(3a)</td>
<td>8</td>
<td>$7p_0$</td>
</tr>
<tr>
<td>29</td>
<td>25–27</td>
<td>9.7(6a)</td>
<td>4</td>
<td>$14p_0$</td>
</tr>
<tr>
<td>30</td>
<td>25–27</td>
<td>9.8(6a)</td>
<td>4</td>
<td>$14p_0$</td>
</tr>
<tr>
<td>35</td>
<td>29–31</td>
<td>9.8(7a)</td>
<td>4</td>
<td>$16p_1$</td>
</tr>
<tr>
<td>37</td>
<td>29–32</td>
<td>9.9(7a)</td>
<td>4</td>
<td>$14p_0$</td>
</tr>
<tr>
<td>39</td>
<td>33</td>
<td>9.1(2b)</td>
<td>16</td>
<td>$8p_2$</td>
</tr>
<tr>
<td>41</td>
<td>33–35</td>
<td>9.8(4a)</td>
<td>8</td>
<td>$6p_7$</td>
</tr>
<tr>
<td>42</td>
<td>33–35</td>
<td>9.6(4a)</td>
<td>8</td>
<td>$8p_0$</td>
</tr>
<tr>
<td>44</td>
<td>33–37</td>
<td>9.5(4a)</td>
<td>8</td>
<td>$11p_0$</td>
</tr>
<tr>
<td>49</td>
<td>36–40</td>
<td>9.6(3a)</td>
<td>12</td>
<td>$p_7$</td>
</tr>
<tr>
<td>50</td>
<td>40</td>
<td>9.3(5a)</td>
<td>8</td>
<td>$2p_6$</td>
</tr>
</tbody>
</table>

**Examples for $q = 3$**

**9.10. Example.** Let $K = \mathbb{F}_3(x)$ and consider the places $p_0 = (x), p_1 = (x - 1), p_2 = (x + 1), p_3 = (1/x), p_4 = (x^2 + 1)$ and $p_5 = (x^4 - x^3 + x^2 + 1)$ of $K$. The relevant $S$-class numbers and $S$-descriptions are given below.

1. $S = \{p_0, p_2\}, h_S = 1, \delta_{S,P_5} = 5 + t$.
2. $S = \{p_0, p_1\}, h_S = 1, \delta_{S,P_3} = 1 + t$.
3. $S = \{p_0, p_1, p_2\}, h_S = 1, \delta_{S,P_3} = 1 + t + t^2, \delta_{S,P_4} = 4 + 2t$.

**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 $S_0 := \{p_0, \ldots, p_5\}$ and $S_0$-units $u_1, \ldots, u_5$ are given by the following table:

<table>
<thead>
<tr>
<th>$u_1 = x$</th>
<th>$p_0$</th>
<th>$p_1$</th>
<th>$p_2$</th>
<th>$p_3$</th>
<th>$p_4$</th>
<th>$p_5$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>3</td>
</tr>
</tbody>
</table>

We have $h_3(1, 6) = 7/6 < 2$ and $\text{reg}(u_1, \ldots, u_5) = 6 = h_K$. Apart from the rational places also $p_6 = (x^2 - x - 1, y + x - 1) \in \mathbb{F}_3^2$ is used. The relevant $S$-class numbers and $S$-descriptions are given below.

1. $S = \{p_0, p_4\}, h_S = 2, \delta_{S,P_6} = 1 + t$.
2. $S = \{p_0, p_3, p_4\}, h_S = 2, \delta_{S,P_3} = 4 + t + t^2$.
3. $S = \{p_1, p_2, p_5\}, h_S = 2, \delta_{S,P_0} = 1 + t + t^2$.
4. $S = \{p_0, p_1, p_3, p_4\}, h_S = 1, \delta_{S,P_6} = 4 + t + 2t^2$. 
9. Tables of Examples

(4b) $S = \{p_1, p_2, p_3, p_4\}$, $h_S = 1$, $\delta_{S, p_0} = 1 + t + t^2 + t^5$.

(5a) $S = \{p_1, p_2, p_3, p_4, p_5\}$, $h_S = 1$, $\delta_{S, p_0} = 1 + t + t^2 + t^4 + t^5$.

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 $S_0 := \{p_0, \ldots, p_6\}$ and $S_0$-units $u_1, \ldots, u_6$ are given by the following table:

<table>
<thead>
<tr>
<th>$u_i$</th>
<th>$p_0$</th>
<th>$p_1$</th>
<th>$p_2$</th>
<th>$p_3$</th>
<th>$p_4$</th>
<th>$p_5$</th>
<th>$p_6$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$u_1 = x$</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-2</td>
</tr>
<tr>
<td>$u_2 = x - 1$</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>-2</td>
</tr>
<tr>
<td>$u_3 = x + 1$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>-2</td>
</tr>
<tr>
<td>$u_4 = y - 1$</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>-3</td>
</tr>
<tr>
<td>$u_5 = y - x$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>-3</td>
</tr>
<tr>
<td>$u_6 = y - x - 1$</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-3</td>
</tr>
</tbody>
</table>

We have $h_3(1, 7) = 1$ and $\text{reg}(u_1, \ldots, u_6) = 7 = h_K$. Apart from the rational places also $p_7 = (x^3 - x + 1) \in \mathbb{F}_3^3$, $p_8 = (x^2 + 1) \in \mathbb{F}_4^4$ are used. The relevant $S$-class numbers and $S$-descriptions are given below.

(5a) $S = \{p_0, p_1, p_2, p_3, p_5, p_6\}$, $h_S = 1$, $\delta_{S, p_7} = 13 + 2t + 2t^2$.

(6a) $S = \{p_1, p_2, p_3, p_4, p_5, p_6\}$, $h_S = 1$, $\delta_{S, p_0} = 1 + t + t^2 + t^4 + t^5 + t^7$.

(7a) $S = \{p_0, p_1, p_2, p_3, p_4, p_5, p_6\}$, $h_S = 1$, $\delta_{S, p_8} = 40 + 4t + 2t^2$.

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 $S_0 := \{p_0, \ldots, p_7\}$ and $S_0$-units $u_1, \ldots, u_7$ are given by the following table:

<table>
<thead>
<tr>
<th>$u_i$</th>
<th>$p_0$</th>
<th>$p_1$</th>
<th>$p_2$</th>
<th>$p_3$</th>
<th>$p_4$</th>
<th>$p_5$</th>
<th>$p_6$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$u_1 = x$</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-1</td>
</tr>
<tr>
<td>$u_2 = x - 1$</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>-1</td>
</tr>
<tr>
<td>$u_3 = x + 1$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>-1</td>
</tr>
<tr>
<td>$u_4 = y - x^3$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>-3</td>
</tr>
<tr>
<td>$u_5 = y - x^3 - 1$</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-3</td>
</tr>
<tr>
<td>$u_6 = y - x^3 + 1$</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>-3</td>
</tr>
<tr>
<td>$u_7 = y + x^3 - x + 1$</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>-1</td>
</tr>
</tbody>
</table>

We have $h_3(2, 8) = 3/11 < 2$ and $\text{reg}(u_1, \ldots, u_7) = 35 = h_K$. Apart from the rational places also $p_8 = (x^2 + 1, y + 1) \in \mathbb{F}_3^2$ is used. The relevant $S$-class numbers and $S$-descriptions are given below.

(2a) $S = \{p_2, p_4\}$, $h_S = 7$, $\delta_{S, p_8} = 1 + t$.

9.14. Example. Let $K = \mathbb{F}_3(x, y)$ with $y^2 - y = (x^2 - 1)/x$. Then $g_K = 2$ and $N_K = 8$. The set $S_0 := \{p_0, \ldots, p_7\}$ and $S_0$-units $u_1, \ldots, u_7$ are given by the following table:

<table>
<thead>
<tr>
<th>$u_i$</th>
<th>$p_0$</th>
<th>$p_1$</th>
<th>$p_2$</th>
<th>$p_3$</th>
<th>$p_4$</th>
<th>$p_5$</th>
<th>$p_6$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$u_1 = x$</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-3</td>
</tr>
<tr>
<td>$u_2 = x - 1$</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-3</td>
</tr>
<tr>
<td>$u_3 = x + 1$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>-3</td>
</tr>
<tr>
<td>$u_4 = y$</td>
<td>-1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>-1</td>
</tr>
<tr>
<td>$u_5 = y - 1$</td>
<td>-1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>-1</td>
</tr>
<tr>
<td>$u_6 = x y + 1$</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>-4</td>
</tr>
<tr>
<td>$u_7 = x y + x + 1$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>-4</td>
</tr>
</tbody>
</table>
We have \( h_3(2, 8) = 13/11 < 2 \) and \( \text{reg}(u_1, \ldots, u_7) = 36 = h_K \). Apart from the rational places also \( p_8 = (x^2 + 1, xy - 1) \in \mathbb{P}_K^2 \) is used. The relevant \( S \)-class numbers and \( S \)-descriptions are given below.

(2a) \( S = \{p_1, p_4\} \), \( h_S = 12 \), \( \delta_{S,p_8} = 2 + t \).

(4a) \( S = \{p_1, p_3, p_4, p_5\} \), \( h_S = 2 \), \( \delta_{S,p_7} = 1 + t + t^2 + t^7 \).

(6a) \( S = \{p_1, p_2, p_3, p_4, p_5, p_6\} \), \( h_S = 1 \), \( \delta_{S,p_7} = 1 + t + t^2 + t^5 + t^7 + t^8 \).

(8a) \( S = \{p_0, p_1, p_2, p_3, p_4, p_5, p_6, p_7\} \), \( h_S = 1 \), \( \delta_{S,p_6} = 4 + 2t + 2t^2 + t^4 + 2t^5 \).

**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 \( S_0 := \{p_0, \ldots, p_9\} \) and \( S_0 \)-units \( u_1, \ldots, u_9 \) are given by the following table:

<table>
<thead>
<tr>
<th>( u_1 = x )</th>
<th>( p_0 )</th>
<th>( p_1 )</th>
<th>( p_2 )</th>
<th>( p_3 )</th>
<th>( p_4 )</th>
<th>( p_5 )</th>
<th>( p_6 )</th>
<th>( p_7 )</th>
<th>( p_8 )</th>
<th>( p_9 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>( u_2 = x - 1 )</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>( u_3 = x + 1 )</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>( u_4 = y )</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>( u_5 = y - 1 )</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>( u_6 = y - x )</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>( u_7 = y - x - 1 )</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>( u_8 = y + x )</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>( u_9 = y + x - 1 )</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
</tbody>
</table>

We have \( h_3(3, 10) = (2414 + 270\sqrt{3})/2531 < 2 \) and \( \text{reg}(u_1, \ldots, u_9) = 196 = h_K \). Apart from the rational places also \( p_{10} = (x^5 + x^4 - 1, y + x^4 + x^3 + x) \in \mathbb{P}_K^5 \) is used. The relevant \( S \)-class numbers and \( S \)-descriptions are given below.

(5a) \( S = \{p_1, p_2, p_5, p_8, p_9\} \), \( h_S = 1 \), \( \delta_{S,p_0} = 1 + t^2 + t^4 + t^5 + t^{10} \).

(9a) \( S = \{p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8, p_9\} \), \( h_S = 1 \), \( \delta_{S,p_0} = 1 + t + t^2 + t^4 + t^5 + t^7 + t^8 + t^{10} + t^{14} \).

(10a) \( S = \{p_0, p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8, p_9\} \), \( h_S = 1 \), \( \delta_{S,p_{10}} = 121 + 5t + 4t^2 \).

**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 \( S_0 := \{p_0, \ldots, p_{12}\} \) and \( S_0 \)-units \( u_1, \ldots, u_{12} \) are given by the following table:

<table>
<thead>
<tr>
<th>( u_1 = x )</th>
<th>( p_0 )</th>
<th>( p_1 )</th>
<th>( p_2 )</th>
<th>( p_3 )</th>
<th>( p_4 )</th>
<th>( p_5 )</th>
<th>( p_6 )</th>
<th>( p_7 )</th>
<th>( p_8 )</th>
<th>( p_9 )</th>
<th>( p_{10} )</th>
<th>( p_{11} )</th>
<th>( p_{12} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-1</td>
<td>-1</td>
<td>-1</td>
<td>0</td>
</tr>
<tr>
<td>( u_2 = x - 1 )</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-1</td>
<td>-1</td>
<td>-1</td>
<td>0</td>
</tr>
<tr>
<td>( u_3 = x + 1 )</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>-1</td>
<td>-1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>( u_4 = y )</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>( u_5 = y - 1 )</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>-2</td>
</tr>
<tr>
<td>( u_6 = y - x )</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-1</td>
<td>1</td>
</tr>
<tr>
<td>( u_7 = y - x - 1 )</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-2</td>
</tr>
<tr>
<td>( u_8 = y + x )</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-2</td>
</tr>
<tr>
<td>( u_9 = y + x - 1 )</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-2</td>
</tr>
<tr>
<td>( u_{10} = (x^2 + 1)y - x^2 )</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>-2</td>
<td>-2</td>
</tr>
<tr>
<td>( u_{11} = (x^2 + 1)y - x )</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-1</td>
<td>-2</td>
<td>-2</td>
</tr>
<tr>
<td>( u_{12} = (x^2 + 1)y - x^2 - x - 1 )</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-2</td>
<td>-2</td>
</tr>
</tbody>
</table>
We have $h_3(4, 12) = (610 + 120\sqrt{3})/759 < 2$ and $\text{reg}\langle u_1, \ldots, u_{12}\rangle = 1225 = h_K$. Apart from the rational places also $p_{12} = (x^2 + 1) \in \mathbb{P}_K^3$ is used. The relevant $S$-class numbers and $S$-descriptions are given below.

$$(10a) \quad S = \{p_1, p_2, p_3, p_4, p_5, p_7, p_9, p_{10}, p_{11}\}, \quad h_S = 1, \quad \delta_{S,p_0} = 1 + t + t^2 + t^4 + t^5 + t^7 + t^8 + t^{10} + t^{11} + t^{14}.$$

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

| $g$ | $N_3(g)$ | $K$, $S$ | $[L : K]$ | $\|L|K|$ | $g$ | $N_3(g)$ | $K$, $S$ | $[L : K]$ | $\|L|K|$ |
|-----|-----------|----------|------------|-----------|-----|-----------|----------|------------|-----------|
| 5   | 12–13     | 9.11(4a) | 3          | $2p_6$    | 30  | 37–46     | 9.11(4b) | 9          | $8p_0$    |
| 7   | 16        | 9.10(2a) | 8          | $p_5$     | 33  | 46–49     | 9.15(5a) | 9          | $4p_0$    |
| 9   | 19        | 9.14(6a) | 3          | $5p_7$    | 34  | 45–50     | 9.12(5a) | 9          | $3p_7$    |
| 10  | 19–21     | 9.10(2b) | 9          | $5p_3$    | 36  | 46–52     | 9.11(5a) | 9          | $9p_0$    |
| 12  | 24–25     | 9.14(2a) | 12         | $\sigma$  | 37  | 48–54     | 9.14(2a) | 24         | $p_8$     |
| 14  | 24–26     | 9.14(8a) | 3          | $5p_8$    | 39  | 48–56     | 9.11(3a) | 24         | $2p_6$    |
| 15  | 28        | 9.10(3a) | 9          | $6p_3$    | 43  | 55–60     | 9.12(6a) | 9          | $11p_0$   |
| 16  | 27–29     | 9.10(3a) | 9          | $3p_4$    | 45  | 54–62     | 9.11(3a) | 18         | $3p_0$    |
| 17  | 24–30     | 9.14(4a) | 6          | $5p_7$    | 46  | 55–63     | 9.10(2b) | 27         | $6p_3$    |
| 19  | 28–32     | 9.15(9a) | 3          | $12p_0$   | 47  | 54–65     | 9.11(3b) | 18         | $6p_0$    |
| 22  | 30–36     | 9.15(10a) | 3         | $3p_{10}$ | 48  | 55–66     | 9.14(6a) | 9          | $11p_7$   |
| 24  | 31–38     | 9.16(10a) | 3         | $14p_0$   | 49  | 63–67     | 9.12(7a) | 9          | $3p_8$    |
| 50  | 56–68     | 9.13(2a) | 28         | $p_8$     | 51  | 68–71     | 9.13(2b) | 9          | $3p_8$    |

Examples for $q = 4$

Let $\alpha$ 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 $p_0 = (x), p_1 = (x + 1), p_2 = (x + \alpha), p_3 = (x + \alpha^2), p_4 = (1/x), p_5 = (x^2 + x + \alpha)$ and $p_6 = (x^3 + \alpha)$ of $K$. The relevant $S$-class numbers and $S$-descriptions are given below.

$$(3a) \quad S = \{p_0, p_1, p_2\}, \quad h_S = 1, \quad \delta_{S,p_4} = 1 + 2t.$$

$$(3b) \quad S = \{p_1, p_2, p_3\}, \quad h_S = 1, \quad \delta_{S,p_6} = 7 + 2t.$$

$$(4a) \quad S = \{p_0, p_1, p_2, p_3\}, \quad h_S = 1, \quad \delta_{S,p_4} = 1 + 2t + t^3, \quad \delta_{S,p_6} = 21 + 3t.$$

$$(5a) \quad S = \{p_0, p_1, p_2, p_3, p_4\}, \quad h_S = 1, \quad \delta_{S,p_5} = 5 + 4t, \quad \delta_{S,p_6} = 21 + 4t.$$

**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 $S_0 := \{p_0, \ldots, p_7\}$ and $S_0$-units $u_1, \ldots, u_7$ are given by the following table:
We have $h_4(1,8) = 9/8 < 2$ and $\langle u_1, \ldots, u_7 \rangle = 8 = h_K$. The relevant $S$-class numbers and $S$-descriptions are given below.

(3a) $S = \{p_1, p_2, p_7\}$, $h_S = 2$, $\delta_{S,p_0} = 1 + t + t^3$.

(7a) $S = \{p_1, p_2, p_3, p_4, p_5, p_6, p_7\}$, $h_S = 1$, $\delta_{S,p_0} = 1 + 2t + 2t^3 + t^5 + t^7$.

**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 $S_0 := \{p_0, \ldots, p_8\}$ and $S_0$-units $u_1, \ldots, u_8$ are given by the following table:

<table>
<thead>
<tr>
<th>$u_1 = x$</th>
<th>$p_0$</th>
<th>$p_1$</th>
<th>$p_2$</th>
<th>$p_3$</th>
<th>$p_4$</th>
<th>$p_5$</th>
<th>$p_6$</th>
<th>$p_7$</th>
<th>$p_8$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$u_2 = x + 1$</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$u_3 = x + \alpha$</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$u_4 = x + \alpha^2$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$u_5 = y$</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$u_6 = y + \alpha$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$u_7 = y + x$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$u_8 = y + \alpha x$</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

We have $h_4(1,9) = 1$ and $\langle u_1, \ldots, u_8 \rangle = 9 = h_K$. The relevant $S$-class numbers and $S$-descriptions are given below.

(2a) $S = \{p_0, p_1\}$, $h_S = 3$, $\delta_{S,p_8} = 1 + t^3$.

**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 $S_0 := \{p_0, \ldots, p_8\}$ and $S_0$-units $u_1, \ldots, u_8$ are given by the following table:

<table>
<thead>
<tr>
<th>$u_1 = x$</th>
<th>$p_0$</th>
<th>$p_1$</th>
<th>$p_2$</th>
<th>$p_3$</th>
<th>$p_4$</th>
<th>$p_5$</th>
<th>$p_6$</th>
<th>$p_7$</th>
<th>$p_8$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$u_2 = x + 1$</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$u_3 = x + \alpha$</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$u_4 = x + \alpha^2$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$u_5 = y$</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$u_6 = y + x$</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$u_7 = y + x^2$</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$u_8 = y + \alpha x^3$</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

We have $h_4(2,9) = 57/41 < 2$ and $\langle u_1, \ldots, u_8 \rangle = 45 = h_K$. The relevant $S$-class numbers and $S$-descriptions are given below.

(4a) $S = \{p_1, p_2, p_3, p_8\}$, $h_S = 3$, $\delta_{S,p_0} = 1 + t + t^3 + t^5$.

**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 $S_0 := \{p_0, \ldots, p_{10}\}$ and $S_0$-units $u_1, \ldots, u_{10}$ are given
by the following table:

<table>
<thead>
<tr>
<th>(u_1 = x)</th>
<th>(p_0)</th>
<th>(p_1)</th>
<th>(p_2)</th>
<th>(p_3)</th>
<th>(p_4)</th>
<th>(p_5)</th>
<th>(p_6)</th>
<th>(p_7)</th>
<th>(p_8)</th>
<th>(p_9)</th>
<th>(p_{10})</th>
</tr>
</thead>
<tbody>
<tr>
<td>(u_2 = x + 1)</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-1</td>
<td>-1</td>
</tr>
<tr>
<td>(u_3 = x + \alpha)</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-1</td>
<td>-1</td>
<td>0</td>
</tr>
<tr>
<td>(u_4 = x + \alpha^2)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>-1</td>
<td>-1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(u_5 = x^3 + x + 1)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>-1</td>
<td>-1</td>
<td>0</td>
</tr>
<tr>
<td>(u_6 = y)</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>(u_7 = y + \alpha)</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-1</td>
</tr>
<tr>
<td>(u_8 = y + x)</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>-1</td>
<td>-1</td>
<td>-1</td>
</tr>
<tr>
<td>(u_9 = (x^3 + x + 1)y + \alpha)</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>-1</td>
<td>-3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(u_{10} = (x^3 + x + 1)y + x^2)</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
</tr>
</tbody>
</table>

We have \(h_4(2,10) = 41/34 < 2\) and \(\text{reg}(u_1, \ldots, u_{10}) = 55 = h_K\). Apart from the rational places also \(p_{10} = (x^3 + x + 1) \in \mathbb{P}_K^3\) is used. The relevant \(S\)-class numbers and \(S\)-descriptions are given below.

(3a) \(S = \{p_1, p_8, p_9\}\), \(h_S = 5\), \(\delta_{S,p_0} = 1 + t + t^5\).

(4a) \(S = \{p_0, p_1, p_8, p_9\}\), \(h_S = 5\), \(\delta_{S,p_{10}} = 7 + 2t + t^2\).

(7a) \(S = \{p_0, p_1, p_3, p_4, p_5, p_6, p_7\}\), \(h_S = 1\), \(\delta_{S,p_2} = 1 + 2t + t^3 + 2t^5 + t^7\).

(8a) \(S = \{p_0, p_1, p_4, p_5, p_6, p_7, p_8, p_9\}\), \(h_S = 1\), \(\delta_{S,p_{10}} = 21 + 4t + t^2 + 2t^3\).

(9a) \(S = \{p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8, p_9\}\), \(h_S = 1\), \(\delta_{S,p_0} = 1 + 2t + 2t^3 + 2t^5 + t^7 + t^9\).  

**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 \(S_0 := \{p_0, \ldots, p_{12}\}\) and \(S_0\)-units \(u_1, \ldots, u_{12}\) are given by the following table:

<table>
<thead>
<tr>
<th>(u_1 = y)</th>
<th>(p_0)</th>
<th>(p_1)</th>
<th>(p_2)</th>
<th>(p_3)</th>
<th>(p_4)</th>
<th>(p_5)</th>
<th>(p_6)</th>
<th>(p_7)</th>
<th>(p_8)</th>
<th>(p_9)</th>
<th>(p_{10})</th>
<th>(p_{11})</th>
<th>(p_{12})</th>
</tr>
</thead>
<tbody>
<tr>
<td>(u_2 = x + \alpha)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>-1</td>
<td></td>
</tr>
<tr>
<td>(u_3 = x + \alpha^2)</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>(u_4 = y)</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>(u_5 = y + 1)</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>(u_6 = y + \alpha)</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>(u_7 = y + x)</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>(u_8 = y + x + 1)</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>(u_9 = y + \alpha x)</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>(u_{10} = y + \alpha x + 1)</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>(u_{11} = y + \alpha x + \alpha)</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>-1</td>
<td></td>
</tr>
</tbody>
</table>

We have \(h_4(3,13) = 183/163 < 2\) and \(\text{reg}(u_1, \ldots, u_{12}) = 441 = h_K\). Apart from the rational places also \(p_{13} = (x^3 + x^2 + 1, y + x^2 + x) \in \mathbb{P}_K^3\) is used. The relevant \(S\)-class numbers and \(S\)-descriptions are given below.

(10a) \(S = \{p_1, p_3, p_5, p_6, p_7, p_8, p_9, p_{10}, p_{11}, p_{12}\}\), \(h_S = 1\), \(\delta_{S,p_0} = 1 + 2t + 2t^3 + t^5 + 2t^7 + t^9 + t^{11}\).

(10b) \(S = \{p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8, p_{10}, p_{11}, p_{12}\}\), \(h_S = 1\), \(\delta_{S,p_0} = 1 + 2t + 2t^3 + 2t^5 + 2t^9 + t^{11}\).
Let \( \alpha \) be the multiplicative generator of \( \mathbb{F}_8 \) satisfying \( \alpha^3 = \alpha + 1 \).

\[ 9.24 \text{ Example. Let } K = \mathbb{F}_8(x) \text{ and consider the places } p_0 = (x), p_1 = (x + 1), p_2 = (x + \alpha), p_3 = (x + \alpha^2), p_4 = (x + \alpha^3), p_5 = (x + \alpha^4), p_6 = (x + \alpha^5), p_7 = (x + \alpha^6), p_8 = (1/x), p_9 = (x^2 + x + 1) \text{ and } p_{10} = (x^2 + x + \alpha) \text{ of } K. \] The relevant \( S \)-class numbers and \( S \)-descriptions are given below.
9 Tables of Examples

(3a) \( S = \{p_0, p_1, p_2\}, h_S = 1, \delta_{S,p_0} = 1 + 2t. \)

(4a) \( S = \{p_0, p_1, p_2, p_3\}, h_S = 1, \delta_{S,p_0} = 1 + 3t. \)

(4b) \( S = \{p_0, p_1, p_2, p_4\}, h_S = 1, \delta_{S,p_0} = 1 + 2t + t^2. \)

(6a) \( S = \{p_2, p_3, p_4, p_5, p_6, p_7\}, h_S = 1, \delta_{S,p_0} = 9 + 4t + t^3. \)

(6b) \( S = \{p_0, p_1, p_2, p_3, p_4, p_5\}, h_S = 1, \delta_{S,p_{10}} = 73 + 5t. \)

(7a) \( S = \{p_0, p_2, p_3, p_4, p_5, p_6, p_7\}, h_S = 1, \delta_{S,p_0} = 9 + 5t + t^3. \)

(8a) \( S = \{p_0, p_1, p_2, p_3, p_4, p_5, p_6, p_7\}, h_S = 1, \delta_{S,p_0} = 1 + 3t + 3t^3 + t^7, \delta_{S,p_{10}} = 73 + 7t. \)

(9a) \( S = \{p_0, p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8\}, h_S = 1, \delta_{S,p_0} = 9 + 6t + 2t^3, \delta_{S,p_{10}} = 73 + 8t. \)

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

| \( q = 8 \) | \( g \) | \( N_S(g) \) | \( K, S \) | \( [L : K] \) | \( f(L|K) \) |
|---|---|---|---|---|---|
| 1 | 14 | 9.24(7a) | 2 | 2p_9 |
| 2 | 18 | 9.24(9a) | 2 | 2p_{10} |
| 3 | 24 | 9.24(6a) | 4 | 2p_9 |
| 6 | 33-36 | 9.24(8a) | 4 | 6p_8 |
| 7 | 33-39 | 9.24(4a) | 8 | 4p_9 |
| 11 | 48-54 | 9.24(6a) | 8 | 3p_9 |
| 14 | 65 | 9.24(8a) | 8 | 6p_8 |

The Examples for \( q = 9 \)

Let \( \alpha \) 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 \( p_0 = (x), p_1 = (x - 1), p_2 = (x + 1), p_3 = (x - \alpha), p_4 = (x - \alpha^2), p_5 = (x - \alpha^3), p_6 = (x - \alpha^5), p_7 = (x - \alpha^6), p_8 = (x - \alpha^7) \) and \( p_9 = (1/x) \) of \( K \). The relevant \( S \)-class numbers and \( S \)-descriptions are given below.

(2a) \( S = \{p_0, p_1\}, h_S = 1, \delta_{S,p_0} = 1 + t. \)

(5a) \( S = \{p_0, p_1, p_2, p_3, p_5\}, h_S = 1, \delta_{S,p_0} = 1 + 2t + t^2 + t^4. \)

(6a) \( S = \{p_0, p_1, p_3, p_4, p_5, p_6\}, h_S = 1, \delta_{S,p_0} = 1 + 2t + 2t^2 + t^5. \)

(7a) \( S = \{p_0, p_1, p_2, p_3, p_4, p_5, p_6\}, h_S = 1, \delta_{S,p_0} = 1 + 2t + 2t^2 + t^4 + t^5. \)

(9a) \( S = \{p_0, p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8\}, h_S = 1, \delta_{S,p_0} = 1 + 2t + 2t^2 + t^4 + 2t^5 + t^8. \)
The outgrowth of Example 9.25 is gathered in the table below.

| $g$  | $N_0(g)$ | $K, S$       | $[L : K]$ | $f(L|K)$ |
|------|----------|--------------|-----------|---------|
| 1    | 16       | 9.25(5a)     | 3         | $3p_9$  |
| 3    | 28       | 9.25(9a)     | 3         | $5p_9$  |
| 12   | 55–63    | 9.25(2a)     | 27        | $3p_9$  |
| 15   | 64–74    | 9.25(7a)     | 9         | $6p_9$  |
| 48   | 163–180  | 9.25(6a)     | 27        | $6p_9$  |
## 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 occurrence.

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\alpha$</td>
<td>a generator of $\mathbb{F}_q^*$</td>
<td>13</td>
</tr>
<tr>
<td>$\alpha$</td>
<td>an idle of $K$</td>
<td>27</td>
</tr>
<tr>
<td>$\alpha_p$</td>
<td>$p$-th component of $\alpha \in \mathcal{I}_K$</td>
<td>26</td>
</tr>
<tr>
<td>$B$</td>
<td>a basis of $\mathbb{F}_p$ over $\mathbb{F}_p$</td>
<td>41</td>
</tr>
<tr>
<td>$\mathbb{C}$</td>
<td>the complex numbers</td>
<td></td>
</tr>
<tr>
<td>$\mathbb{C}((t))$</td>
<td>the field of formal Laurent series over $\mathbb{C}$</td>
<td>9</td>
</tr>
<tr>
<td>$\mathcal{C}_K$</td>
<td>idèle class group of $K$</td>
<td>27</td>
</tr>
<tr>
<td>$\mathcal{C}_S^m$</td>
<td>$S$-congruence subgroup mod $m$</td>
<td>30</td>
</tr>
<tr>
<td>$\mathfrak{O}(\mathcal{O}_S)$</td>
<td>$S$-class group</td>
<td>14</td>
</tr>
<tr>
<td>$\mathfrak{O}^m(\mathcal{O}_S)$</td>
<td>$S$-class group mod $m$</td>
<td>31</td>
</tr>
<tr>
<td>$\mathcal{D}_K$</td>
<td>divisor group of $K$</td>
<td>8</td>
</tr>
<tr>
<td>$\mathcal{D}_K^0$</td>
<td>divisors of degree 0</td>
<td>8</td>
</tr>
<tr>
<td>$\mathcal{D}_K^0/(K^*)$</td>
<td>divisor class group of $K$</td>
<td>9</td>
</tr>
<tr>
<td>$\mathcal{D}_S$</td>
<td>$S$-divisors</td>
<td>14</td>
</tr>
<tr>
<td>$\mathcal{D}_S^0$</td>
<td>$S$-divisors of degree 0</td>
<td>14</td>
</tr>
<tr>
<td>$\text{deg}$</td>
<td>degree</td>
<td>9</td>
</tr>
<tr>
<td>$\text{deg} m$</td>
<td>degree of $m$</td>
<td>8</td>
</tr>
<tr>
<td>$\text{deg} p$</td>
<td>degree of $p$</td>
<td>8</td>
</tr>
<tr>
<td>$\text{deg} S$</td>
<td>degree of $S$</td>
<td>14</td>
</tr>
<tr>
<td>$\text{dim} m$</td>
<td>dimension of $L(m)$</td>
<td>9</td>
</tr>
<tr>
<td>$\delta(L</td>
<td>K)$</td>
<td>discriminant of $L</td>
</tr>
<tr>
<td>$d(q</td>
<td>p)$</td>
<td>different exponent of $q</td>
</tr>
<tr>
<td>$\delta$</td>
<td>a description</td>
<td>40</td>
</tr>
<tr>
<td>$\delta(m)$</td>
<td>number derived from $\delta$</td>
<td>41</td>
</tr>
<tr>
<td>$\delta_n$</td>
<td>$n$-th coefficient of $\delta$</td>
<td>40</td>
</tr>
<tr>
<td>$\delta_{S,p}$</td>
<td>$S$-description at $p$</td>
<td>41</td>
</tr>
<tr>
<td>$e = \log_p q$</td>
<td></td>
<td>54</td>
</tr>
<tr>
<td>$e_n$</td>
<td>0 or length of a $G$-orbit in $Q$</td>
<td>54</td>
</tr>
<tr>
<td>$e(q</td>
<td>p)$</td>
<td>ramification index of $q</td>
</tr>
<tr>
<td>$F_m$</td>
<td>homeomorphism from $[\frac{\pi}{m+1}, \frac{\pi}{m}]$ onto $[0,1]$</td>
<td>47</td>
</tr>
<tr>
<td>$\mathbb{F}_p$</td>
<td>residue field at $p$</td>
<td>8</td>
</tr>
<tr>
<td>$\mathbb{F}_p((\pi))$</td>
<td>field of expansions in $\pi$ at $p$</td>
<td>12</td>
</tr>
<tr>
<td>$\mathbb{F}_q$</td>
<td>finite field with $q$ elements</td>
<td>8</td>
</tr>
<tr>
<td>$\mathbb{F}_q[K]$</td>
<td>constant field extension of degree $d$ over $K$</td>
<td>11</td>
</tr>
<tr>
<td>$\mathbb{F}_q(x)$</td>
<td>rational function field</td>
<td>9</td>
</tr>
<tr>
<td>$[\mathbb{F}_q : \mathbb{F}_p]$</td>
<td>inertia degree of $q</td>
<td>p$</td>
</tr>
<tr>
<td>$f(L,p)$</td>
<td>conductor exponent of $p$ in $L$</td>
<td>20</td>
</tr>
<tr>
<td>$f_n(t)$</td>
<td>auxiliary polynomials over $\mathbb{Z}$</td>
<td>50</td>
</tr>
<tr>
<td>$\mathfrak{j}(L</td>
<td>K)$</td>
<td>conductor of $L</td>
</tr>
<tr>
<td>$G = G(\mathbb{F}_q[\mathbb{F}_p])$</td>
<td></td>
<td>54</td>
</tr>
<tr>
<td>$G(L</td>
<td>K)$</td>
<td>Galois group of $L</td>
</tr>
<tr>
<td>$\text{GL}_n$</td>
<td>invertible $n \times n$-matrices</td>
<td></td>
</tr>
<tr>
<td>$G^a(L,p)$</td>
<td>$s$-th upper ramification group of $p$ in $L$</td>
<td>23</td>
</tr>
<tr>
<td>$G_s(q</td>
<td>p)$</td>
<td>$s$-th lower ramification group of $q</td>
</tr>
<tr>
<td>$G^a(q</td>
<td>p)$</td>
<td>$s$-th upper ramification group of $q</td>
</tr>
<tr>
<td>$G^0(q</td>
<td>p)$</td>
<td>inertia group of $q</td>
</tr>
<tr>
<td>$G^{-1}(q</td>
<td>p)$</td>
<td>decomposition group of $q</td>
</tr>
<tr>
<td>$g_K$</td>
<td>genus of $K$</td>
<td>9</td>
</tr>
<tr>
<td>$\gamma_q$</td>
<td>lower bound for the genus</td>
<td>48</td>
</tr>
<tr>
<td>$h_K$</td>
<td>divisor class number of $K$</td>
<td>9</td>
</tr>
<tr>
<td>$h_S$</td>
<td>$S$-class number</td>
<td>14</td>
</tr>
<tr>
<td>$h_q$</td>
<td>upper bound for $S$-class numbers</td>
<td>49</td>
</tr>
<tr>
<td>$\eta$</td>
<td>continuous bijection on $[-1, \infty)$</td>
<td>20</td>
</tr>
<tr>
<td>Symbol</td>
<td>Description</td>
<td>Page</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td>$\mathcal{I}_K$</td>
<td>idèle group of $K$</td>
<td>26</td>
</tr>
<tr>
<td>$T^n$</td>
<td>large idèle congruence subgroup \mod $n$</td>
<td>31</td>
</tr>
<tr>
<td>$T^n_S$</td>
<td>$S$-idèle congruence subgroup \mod $m$</td>
<td>30</td>
</tr>
<tr>
<td>$K$</td>
<td>global function field</td>
<td>8</td>
</tr>
<tr>
<td>$K_p$</td>
<td>completion of $K$ at $p$</td>
<td>11</td>
</tr>
<tr>
<td>$K^m_S$</td>
<td>$S$-ray class field \mod $m$</td>
<td>32</td>
</tr>
<tr>
<td>$K^a_S$</td>
<td>Hilbert class field of $O_S$</td>
<td>32</td>
</tr>
<tr>
<td>$F_q$</td>
<td>global function field with full constant field $\mathbb{F}_q$</td>
<td>8</td>
</tr>
<tr>
<td>$\tilde{K}$</td>
<td>a fixed algebraic closure of $K$</td>
<td>19</td>
</tr>
<tr>
<td>$(K^*)$</td>
<td>group of invertible elements of $K$</td>
<td>9</td>
</tr>
<tr>
<td>$L$</td>
<td>global function field</td>
<td>10</td>
</tr>
<tr>
<td>$L_l$</td>
<td>field of degree $p^l$ over $\mathbb{F}_q(x)$ in between $K^{m-1}_S/K^{(m-1)p}_S$</td>
<td>55</td>
</tr>
<tr>
<td>$L_p$</td>
<td>completion of $L$ at some $q</td>
<td>p$</td>
</tr>
<tr>
<td>$L_q/K_p$</td>
<td>local extension</td>
<td>11</td>
</tr>
<tr>
<td>$L^s(p)$</td>
<td>$s$-th upper ramification field of $p$ in $L$</td>
<td>23</td>
</tr>
<tr>
<td>$L^0(p)$</td>
<td>inertia field of $p$ in $L$</td>
<td>24</td>
</tr>
<tr>
<td>$L^{-1}(p)$</td>
<td>decomposition field of $p$ in $L$</td>
<td>24</td>
</tr>
<tr>
<td>$L</td>
<td>\mathbb{F}_{q^d}$</td>
<td>extension of $K</td>
</tr>
<tr>
<td>$[L:K]$</td>
<td>degree of $L</td>
<td>K$</td>
</tr>
<tr>
<td>$L_1L_2$</td>
<td>compositum of $L_1$ and $L_2$</td>
<td>24</td>
</tr>
<tr>
<td>$\mathcal{L}(m)$</td>
<td>Riemann-Roch space of $m$</td>
<td>9</td>
</tr>
<tr>
<td>$\max{m,n}$</td>
<td>coefficientwise maximum of $m$ and $n$</td>
<td>21</td>
</tr>
<tr>
<td>$\min{m,n}$</td>
<td>coefficientwise minimum of $m$ and $n$</td>
<td>32</td>
</tr>
<tr>
<td>$m$</td>
<td>a divisor</td>
<td>8</td>
</tr>
<tr>
<td>$m$</td>
<td>tame part $\sum_{p\in\text{supp}_m} p$ of $m$</td>
<td>36</td>
</tr>
<tr>
<td>$m\setminus p$</td>
<td>non-$p$-part of $m$</td>
<td>34</td>
</tr>
<tr>
<td>$N_K$</td>
<td>number of rational places of $K$</td>
<td>46</td>
</tr>
<tr>
<td>$N_L, K$</td>
<td>norm map \mod $K$</td>
<td>10</td>
</tr>
<tr>
<td>$N_L</td>
<td>K(\beta)$</td>
<td>norm of $\beta \in \mathcal{I}_L$</td>
</tr>
<tr>
<td>$N_q(\beta)$</td>
<td>maximum number of rational places for global function fields $K</td>
<td>\mathbb{F}_q$ of genus $q$</td>
</tr>
<tr>
<td>$\tilde{\mathcal{N}}_p$</td>
<td>Oesterlé bound \mod $p$</td>
<td>39</td>
</tr>
<tr>
<td>$\mathbb{N}$</td>
<td>the positive integers</td>
<td>29</td>
</tr>
<tr>
<td>$\mathbb{N}_0$</td>
<td>the non-negative integers</td>
<td>29</td>
</tr>
<tr>
<td>$\mathbb{N}_p^*$</td>
<td>the positive integers prime to $p$</td>
<td>39</td>
</tr>
<tr>
<td>$\delta$</td>
<td>a divisor</td>
<td>8</td>
</tr>
<tr>
<td>$\nu$</td>
<td>valuation-like map on $\mathbb{Z}$</td>
<td>42</td>
</tr>
<tr>
<td>$O_S$</td>
<td>ring of $S$-integral functions</td>
<td>14</td>
</tr>
<tr>
<td>$O_S^*$</td>
<td>group of $S$-units</td>
<td>14</td>
</tr>
<tr>
<td>$(O_S^*)_S$</td>
<td>group of principal $S$-divisors</td>
<td>14</td>
</tr>
<tr>
<td>$\varphi_{q</td>
<td>p}$</td>
<td>Frobenius automorphism of $q</td>
</tr>
<tr>
<td>$\varphi_{L,p}$</td>
<td>Frobenius automorphism of $p$ in $L$</td>
<td>23</td>
</tr>
<tr>
<td>$\phi(m)$</td>
<td>Euler automorphism of $m$</td>
<td>31</td>
</tr>
<tr>
<td>$\mathbb{F}_K$</td>
<td>set of all places of $K$</td>
<td>8</td>
</tr>
<tr>
<td>$\mathbb{P}_K^d$</td>
<td>set of places of $K$ of degree $d$</td>
<td>8</td>
</tr>
<tr>
<td>$P_K(t)$</td>
<td>numerator of $Z_K(t)$</td>
<td>9</td>
</tr>
<tr>
<td>$\mathfrak{p}$</td>
<td>a place</td>
<td>8</td>
</tr>
<tr>
<td>$\mathfrak{p}_\alpha$</td>
<td>the zero of $x - \alpha$</td>
<td>51</td>
</tr>
<tr>
<td>$\mathfrak{p}_j$</td>
<td>place in the support of $m$</td>
<td>37</td>
</tr>
<tr>
<td>$\mathfrak{p}$</td>
<td>topological closure of $p$ in $K_p$</td>
<td>11</td>
</tr>
<tr>
<td>$\pi$</td>
<td>a uniformizer</td>
<td>12</td>
</tr>
</tbody>
</table>
List of Symbols

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\psi(t)$</td>
<td>polynomial over $\mathbb{R}$</td>
<td>47</td>
</tr>
<tr>
<td>$Q$</td>
<td>representatives ${1, \ldots, q-1}$</td>
<td></td>
</tr>
<tr>
<td>$Q$</td>
<td>the rational numbers</td>
<td>8</td>
</tr>
<tr>
<td>$q$</td>
<td>a power of $p$</td>
<td>10</td>
</tr>
<tr>
<td>$q</td>
<td>p$</td>
<td>$q$ lies over $p$</td>
</tr>
<tr>
<td>$R$</td>
<td>support of $m$</td>
<td>37</td>
</tr>
<tr>
<td>$R_p$</td>
<td>discrete valuation ring at $p$</td>
<td>8</td>
</tr>
<tr>
<td>$R_p$</td>
<td>topological closure of $R_p$ in $K_p$</td>
<td>11</td>
</tr>
<tr>
<td>$\mathbb{R}$</td>
<td>the real numbers</td>
<td></td>
</tr>
<tr>
<td>$\mathbb{R}[t]$</td>
<td>polynomial ring over $\mathbb{R}$</td>
<td>47</td>
</tr>
<tr>
<td>$\text{reg}_S$</td>
<td>$S$-regulator</td>
<td>14</td>
</tr>
<tr>
<td>$\text{reg}U$</td>
<td>regulator of $U$</td>
<td>14</td>
</tr>
<tr>
<td>$S$</td>
<td>subset of $\mathbb{P}_K$</td>
<td>14</td>
</tr>
<tr>
<td>$S(L</td>
<td>K)$</td>
<td>splitting set of $L</td>
</tr>
<tr>
<td>$s$</td>
<td>$</td>
<td>S</td>
</tr>
<tr>
<td>$\sum_n \alpha_n \pi^n$</td>
<td>an expansion in $\pi$</td>
<td>8</td>
</tr>
<tr>
<td>$\vartheta_p$</td>
<td>homeomorphism from $[q + 1, \infty)$ onto $[0, 1]$</td>
<td>12</td>
</tr>
<tr>
<td>$U$</td>
<td>subgroup of $O_S^n$</td>
<td>48</td>
</tr>
<tr>
<td>$U_p$</td>
<td>unit group at $p$</td>
<td>13</td>
</tr>
<tr>
<td>$U_p^{(n)}$</td>
<td>$n$-th one-unit group at $p$</td>
<td>13</td>
</tr>
<tr>
<td>$U_p^{(1)}$</td>
<td>the one-unit group at $p$</td>
<td>13</td>
</tr>
<tr>
<td>$u$</td>
<td>a map with values in $(O_S^n)$</td>
<td>16</td>
</tr>
<tr>
<td>$v_l$</td>
<td>$l$-adic valuation</td>
<td>16</td>
</tr>
<tr>
<td>$v_p$</td>
<td>$p$-adic valuation</td>
<td>8</td>
</tr>
<tr>
<td>$v_p$</td>
<td>valuation at $p$</td>
<td>8</td>
</tr>
<tr>
<td>$v_p^\omega$</td>
<td>Artin-Schreier reduced valuation at $p$</td>
<td>21</td>
</tr>
<tr>
<td>$v_\infty$</td>
<td>degree valuation on $\mathbb{F}_q(x)$</td>
<td>9</td>
</tr>
<tr>
<td>$x$</td>
<td>indeterminate over $\mathbb{F}_q$</td>
<td>51</td>
</tr>
<tr>
<td>$y$</td>
<td>algebraic element over $\mathbb{F}_q(x)$</td>
<td>60</td>
</tr>
<tr>
<td>$\mathbb{Z}[t]$</td>
<td>polynomial ring over $\mathbb{Z}$</td>
<td>54</td>
</tr>
<tr>
<td>$\mathbb{Z}[[t]]$</td>
<td>formal power series ring over $\mathbb{Z}$</td>
<td>9</td>
</tr>
<tr>
<td>$Z_K(t)$</td>
<td>zeta function of $K$</td>
<td>9</td>
</tr>
<tr>
<td>$Z_p$</td>
<td>the $\mathbb{Z}_p$-module $\mathbb{Z}_p^n \times B$</td>
<td>42</td>
</tr>
<tr>
<td>$Z(n)$</td>
<td>additive group isomorphic to $U_p^{(1)}/U_p^{(n)}$</td>
<td>41</td>
</tr>
<tr>
<td>$Z$</td>
<td>the integers</td>
<td></td>
</tr>
<tr>
<td>$Z_p$</td>
<td>the $p$-adic integers</td>
<td>41</td>
</tr>
<tr>
<td>$\zeta$</td>
<td>isomorphism $U_p^{(1)} \simeq Z$ of $\mathbb{Z}_p$-modules</td>
<td>42</td>
</tr>
<tr>
<td>$\zeta(n)$</td>
<td>group isomorphism $U_p^{(1)}/U_p^{(n)} \simeq Z(n)$</td>
<td>41</td>
</tr>
<tr>
<td>$(\ )$</td>
<td>principal divisor map</td>
<td>9</td>
</tr>
<tr>
<td>$(z)$</td>
<td>principal divisor</td>
<td>9</td>
</tr>
<tr>
<td>$(z)_0$</td>
<td>divisor of zeros</td>
<td>9</td>
</tr>
<tr>
<td>$(z)_\infty$</td>
<td>divisor of poles</td>
<td>9</td>
</tr>
<tr>
<td>$(n)$</td>
<td>projection of $Z$ onto $Z(n)$</td>
<td>42</td>
</tr>
<tr>
<td>$(\ , L</td>
<td>K)$</td>
<td>Artin map of $L</td>
</tr>
<tr>
<td>$(\ , L_p</td>
<td>K_p)$</td>
<td>Artin map of $L_p</td>
</tr>
<tr>
<td>$[\ ]_p$</td>
<td>embedding of $K_p^*$ into $\mathcal{I}_K$</td>
<td>27</td>
</tr>
<tr>
<td>$\langle u_1, \ldots, u_s \rangle$</td>
<td>group generated by $u_1, \ldots, u_s$</td>
<td></td>
</tr>
<tr>
<td>$m</td>
<td>n$</td>
<td>$m$ divides $n$</td>
</tr>
<tr>
<td>$f</td>
<td>A$</td>
<td>restriction of $f$ to $A$</td>
</tr>
<tr>
<td>$</td>
<td>a</td>
<td>$</td>
</tr>
<tr>
<td>$</td>
<td>S</td>
<td>$</td>
</tr>
<tr>
<td>$</td>
<td>p</td>
<td>$</td>
</tr>
<tr>
<td>$[a]$</td>
<td>integer part of $a$</td>
<td>46</td>
</tr>
<tr>
<td>$[a]_p$</td>
<td>least $p$-power integer $\geq a$</td>
<td>39</td>
</tr>
<tr>
<td>$f \circ g$</td>
<td>composite of maps $f$ and $g$, $f$ after $g$</td>
<td></td>
</tr>
<tr>
<td>$n^*$</td>
<td>non-$p$-part of $n$</td>
<td>39</td>
</tr>
<tr>
<td>$\infty$</td>
<td>pole of $x$ in $\mathbb{F}_q(x)$</td>
<td>9</td>
</tr>
</tbody>
</table>
References


References


References


References


References


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