Universität des Saarlandes

Fachbereich 9 – Mathematik

Mathematischer Preprint

Cyclotomic Function Fields with Many Rational Places

Alice Keller

Preprint No. 7

Saarbrücken 2000

Universität des Saarlandes

Fachbereich 9 – Mathematik

Cyclotomic Function Fields with Many Rational Places

Alice Keller

Saarland University
Department of Mathematics
Postfach 15 11 50
D–66041 Saarbrücken
Germany
E-Mail: liz@math.uni-sb.de

submitted: 17.01.00

Preprint No. 7

Saarbrücken 2000

Edited by
FB 9 – Mathematik
Im Stadtwald
D–66041 Saarbrücken
Germany

Fax:	+ 49 681 302 4443
e-mail:	preprint@math.uni-sb.de
WWW:	http://www.math.uni-sb.de/

Abstract

Let $A = \mathbb{F}_q[T]$ be the polynomial ring in the variable T and $K = \mathbb{F}_q(T)$ the rational function field over $\mathbb{F}_q$ (the finite field with q elements), and let K_∞ be the completion of K at the place $\infty := \frac{1}{T}$. Furthermore let C be the completion of a fixed algebraic closure of K_∞.

We aim to construct extensions $K \subset K' \subset C$ with many rational places relative to the genus $g(K')$ of K'.

As a first step we consider the cyclotomic fields $K(n)/K$ with $n \in A$, which are generated analogously to the classical cyclotomic fields over $\mathbb{Q}$. Then we consider certain decomposition fields and their intersections. Here we know a lower bound for the number of rational places. We get explicit formulas to calculate the genus, but they depend on the relative position of some subgroups of the muliplicative group $(A/(n))^*$ of the ring $A/(n)$. So the concrete calculation of examples must be done by computer. With a special program we made a systematical search for $q = 2$ and found for fixed genus three new lower bounds.

AMS Subject Classification: 11R18, 11R37, 11R58, 11R60, 11T71, 14H05
Key words: curves with many rational points, abelian extensions of function fields, cyclotomic function fields, function fields with many rational places

Contents

1 Cyclotomic Extensions of K

First we introduce some notations which are used in the whole article.

Definition 1.1 *Let $n \in A$ be a monic polynomial of positive degree. Then there exists a unique factorisation of n in irreducible polynomials, namely:*

$$n = \prod_{\nu=1}^{s} p_\nu^{r_\nu} \ ,$$

with s, r_ν in $\mathbb{N}$ and $p_\nu \in A$ monic, irreducible and pairwise different polynomials of degree ≥ 1. We write for short

$$\begin{array}{llll} d_\nu := deg(p_\nu) \ , & q_\nu := q^{d_\nu} \ , & & \\ n_\nu := p_\nu^{r_\nu} \ , & m_\nu := \dfrac{n}{n_\nu} & \text{and} & \varphi(n) := |(A/(n))^*| \ . \end{array}$$

The extensions $K(n)$ we are looking for are just the splitting fields of the polynomials ρ_n in C which are defined by the following conditions:

1. $\rho_T(X) = TX + X^q$,
2. $\rho_{T^i}(X) = \rho_T(\rho_{T^{i-1}}(X))$,
3. $\rho_{f+g}(X) = \rho_f(X) + \rho_g(X)$ for all $f, g \in, \mathbb{F}_q[T]$
4. $\rho_{cT}(X) = c \cdot \rho_T(X)$ for all $c \in \mathbb{F}_q$.

In other words, $K(n)$ is obtained from K by adjoining the n-torsion of the Carlitz–module ρ (cf. [1, chapter 3]).

Theorem 1.2 *1. The extension $K(n)/K$ is galois and abelian with Galois group $(A/(n))^*$.*

2. Let $n = p^r$ be a primary polynomial, then the extension $K(n)/K$ is totally ramified in $\mathfrak{p} = (p)$ and unramified in all other finite places $\mathfrak{q} \neq \mathfrak{p}$.

3. Let $K_+(n)$ be the fixed field of the embedding $\mathbb{F}_q^* \hookrightarrow (A/(n))^*$.

$$(A/(n))^* \left\{ \begin{array}{c} \left. \begin{array}{c} K(n) \\ | \\ K_+(n) \end{array} \right\} \mathbb{F}_q^* \\ | \\ K \end{array} \right. \quad .$$

Then the place ∞ is totally split in $K_+(n)$ and any place of $K_+(n)$ over ∞ is totally ramified in the extension $K(n)/K_+(n)$.

4. *Let n be the product of s primary factors in A. Then $K(n)$ is the compositum of the fields $K(p_\nu^{r_\nu})$, $\nu = 1, \dots, s$, and all these $K(p_\nu^{r_\nu})$ are linearly disjoint.*

5. *Let $\mathcal{O}(n)$ be the integral closure of A in $K(n)$ and λ a primitive root of ρ_n. Then*

$$\mathcal{O}(n) = A[\lambda] \ .$$

Proof: In [2] as well as in [3].

Corollary 1.3 *The field $\mathbb{F}_q$ is algebraically closed in $K(n)$.*

Remark 1.4 *The theorem shows that the splitting fields of ρ_n have many of the properties of the cyclotomic fields over $\mathbb{Q}$. Therefore they are called* cyclotomic extensions of the rational function field. *The field $K_+(n)$ is the analogue of the maximal real extension of $\mathbb{Q}$ which is contained in the cyclotomic extension. The integral closure $\mathcal{O}(n)$ could be compared with the ring of integers $\mathbb{Z}[\zeta_m]$ for some primitive m-th root of unity ζ_m.*

2 The Genus of $K(n)$

Our aim is now to find a closed formula for the genus $g(K(n))$. Such a formula has been known to several people since about the appearance of [2]. Surprisingly, that formula for the case of a general n has never been published. For special cases, see [4].
First we consider the field $K(p^r)$ and then we can derive the genus of $K(n)$ via induction.
We need some notations:

Definition 2.1 *For a field extension L of K let $S(L)$ be the set of places. Let $\mathcal{O}$ be the integral closure of A in L. Then for any $\mathfrak{q} \in S(L)$ we write $\mathcal{O}_{(\mathfrak{q})}$ for the localization of $\mathcal{O}$ at $\mathfrak{q}$. With $\mathcal{D}(L/K)$ we denote the different of L/K. Let $\mathfrak{p}_\nu := (p_\nu)$ for all $\nu = 1, \dots, s$ and for $1 \le \alpha \le r_\nu$*

$$G(n_\nu)^\alpha := \{b \in (A/(n_\nu))^* \,|\, b \equiv 1 \bmod p_\nu^\alpha\} \ .$$

Furthermore we fix an algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$ and denote the constant field extension by $K'(n) := \overline{\mathbb{F}}_q\, K(n)$.

Later we consider some subextension $K_*(n)$ of $K(n)/K$ for which we will write $K'_*(n) := \overline{\mathbb{F}}_q\, K_*(n)$.
Let $K \subset L \subset K(n)$. For any place $\mathfrak{q} \in S(L)$ and $S(L') \ni \mathfrak{q}'|\mathfrak{q}$ with $L' := \overline{\mathbb{F}}_q\, L$, we write

$$g_i(\mathfrak{q}') := |(G(K'(n)/L'))_i(\mathfrak{q}')| = |(G(K(n)/L))_i(\mathfrak{q})| =: g_i(\mathfrak{q})$$

for the cardinality of the i-th ramification group in the extension $K'(n)/L'$.

Since $\mathbb{F}_q$ is algebraically closed in $K(n)$ neither the genus $g(K(n))$ nor the ramification index $e_{\mathfrak{p}}(K(n)/K)$ change by a constant field extension. The cardinalities of the higher ramification groups are invariant too. So we get:

$$\begin{aligned} [K'(n) : K'] &= [K(n) : K] = \varphi(n) \quad \text{and} \\ e_{\mathfrak{p}'}(K'(n)/K') &= e_{\mathfrak{p}}(K(n)/K) \qquad \text{as well as} \quad g(K'(n)) = g(K(n)) , \end{aligned}$$

where $\mathfrak{p}' \in S(K')$ with $\mathfrak{p}'|\mathfrak{p}$.

Let $p \in A$ be a prime polynomial of degree $d > 0$ and $r > 0$ an integer.
The genus of the field $K(p^r)$ can be calculated by the Riemann–Hurwitz–formula

$$2g(K(p^r)) - 2 = [K(p^r) : K](2g(K) - 2) + \deg \mathcal{D}(K(p^r)/K)).$$

The degree of the different is the sum of degrees of the local differents. For calculating them we can use the cardinalities of the ramification groups (cf. [5, chap. 4, §2]).
We know from 1.2 that ∞ is tamely ramified, so the higher ramification groups are trivial and the local different $\mathcal{D}(K(p^r)_{\mathfrak{Q}}/K_\infty)$ at a place $\mathfrak{Q}$ with $\mathfrak{Q}|\infty$ has degree $q-2$.
Another fact from theorem 1.2 is that $\mathfrak{p} = (p)$ is the only finite ramified place. Since $\mathfrak{p}$ is totally ramified, the ramification index is

$$e_{\mathfrak{p}}(K(p^r)/K) = |(A/\mathfrak{p})^*| = \varphi(p^r) = q^{d(r-1)}(q^d - 1) .$$

For $\mathfrak{P}|\mathfrak{p}$ let $K_{\mathfrak{p}}$ (resp. $K(p^r)_{\mathfrak{P}}$) the completion of K (resp. $K(p^r)$) with respect to $\mathfrak{p}$ (resp. $\mathfrak{P}$). We write $G := G(K(p^r)/K)$ for the Galois group of the extension $K(p^r)/K$.
Then we can the Galois group G of the extension $K(p^r)/K$ identify with the Galois group $G(K(p^r)_{\mathfrak{P}}/K_{\mathfrak{p}})$, which is equal to the decomposition and inertia group.
For all $i \in \mathbb{Z}$ and $i \geq -1$ the i-th ramification group of $\mathfrak{P}$ in $K(p^r)_{\mathfrak{P}}/K_{\mathfrak{p}}$ is

$$G_i := \{\sigma \in G \mid v_{\mathfrak{P}}(\sigma(a) - a) \geq i + 1 \text{ for all } a \in \mathcal{O}_{(\mathfrak{P})}\} .$$

Proposition 2.2 *The ramification groups of $K(p^r)_{\mathfrak{P}}/K_{\mathfrak{p}}$ are*

$$\begin{array}{rcll} G_0 &=& G(K(p^r)_{\mathfrak{P}}/K_{\mathfrak{p}}) \ , & \\ G_i &\cong& G(p^r)^\alpha & \textit{for } q^{d(\alpha-1)} \le i \le q^{d\alpha}-1 \textit{ and } 1 \le \alpha \le r-1 \ , \\ G_i &\cong& G(p^r)^r = \{1\} & \textit{for } q^{d(r-1)} \le i \ . \end{array}$$

Proof: It is clear that $G_0 = T_{\mathfrak{P}}(K(p^r)_{\mathfrak{P}}/K_{\mathfrak{p}}) = G(K(p^r)_{\mathfrak{P}}/K_{\mathfrak{p}})$.
The map

$$\begin{array}{ccc} (A/(p^r))^* & \longrightarrow & G(K(p^r)_{\mathfrak{P}}/K_{\mathfrak{p}}) \\ \overline{b} & \mapsto & \sigma_{\overline{b}} \end{array} \qquad \text{with} \quad \sigma_{\overline{b}}(\lambda_0) = \rho_b(\lambda_0)$$

is well-defined and bijective. For $\overline{b} \in (A/(p^r))^*$ the equations hold:

$$\begin{aligned} \rho_b(\lambda_0) &= b \cdot \lambda_0 + (\dots)\lambda_0^q + \dots + \lambda_0^{q^{deg(b)}} \ , \\ \rho_b(\lambda_0) - \lambda_0 &= \rho_{b-1}(\lambda_0) \ , \\ v_{\mathfrak{P}}(\rho_b(\lambda_0) - \lambda_0) &= v_{\mathfrak{P}}(\rho_{b-1}(\lambda_0)) \ . \end{aligned}$$

Let $b \equiv 1 \bmod p^\alpha$ and $b \not\equiv 1 \bmod p^{\alpha+1}$ for some $0 \le \alpha \le r-1$, then $\rho_{b-1}(\lambda_0)$ is a primitive root of $\rho_{p^{r-\alpha}}$. For we have two Eisenstein polynomials

$$\begin{aligned} f_{p^r}(X) &:= \frac{\rho_{p^r}(X)}{\rho_{p^{r-1}}(X)} = \prod_{\substack{\lambda \in {}_{p^r}\rho \\ \lambda \text{ prim.TP.}}} (X - \lambda) \qquad \text{and} \\ f_{p^{r-\alpha}}(X) &:= \frac{\rho_{p^{r-\alpha}}(X)}{\rho_{p^{r-\alpha-1}}(X)} = \prod_{\substack{\lambda \in {}_{p^{r-\alpha}}\rho \\ \lambda \text{ prim.TP.}}} (X - \lambda) \ , \end{aligned}$$

which are the minimal polynomials for the extension $K(p^r)$ and $K(p^{r-\alpha})$, respectively.
Since $p^\alpha | (b-1)$ and $p^{\alpha+1} \not| \,(b-1)$ there exists $\overline{b'} \in (A/(p^r))^*$, for which we have $b - 1 \equiv b'p^\alpha \bmod p^r$ and $\gcd(b', p) = 1$. We conclude that

$$\begin{aligned} \rho_{p^{r-\alpha}}(\rho_{b-1}(\lambda_0)) &= \rho_{(b-1)p^{r-\alpha}}(\lambda_0) = \rho_{b'p^r}(\lambda_0) = \rho_{p^r}(\rho_{b'}(\lambda_0)) = 0 \quad \text{and} \\ \rho_{p^{r-\alpha-1}}(\rho_{b-1}(\lambda_0)) &= \rho_{b'p^{r-1}}(\lambda_0) \neq 0 \ , \end{aligned}$$

because $\rho_{b'}(\lambda_0)$ is a primitive root of ρ_{p^r}.
Furthermore, $f_{p^{r-\alpha}}(\rho_{b-1}(\lambda_0)) = 0$ and $\rho_{b-1}(\lambda_0)$ is a primitive root of $\rho_{p^{r-\alpha}}$. Keeping in mind that the extension is totally ramified we get

$$v_{\mathfrak{P}}(\rho_{b-1}(\lambda_0)) = \underbrace{[K(p^r)_{\mathfrak{P}} : K(p^{r-\alpha})_{\mathfrak{q}}]}_{q^{d\alpha}} \cdot \underbrace{v_{\mathfrak{q}}(\rho_{b-1}(\lambda_0))}_{1} = q^{d\alpha} \ ,$$

for a prime ideal $\mathfrak{q}|\mathfrak{p}$ in the integral closure of A in $K(p^{r-\alpha})$.
Therefore $\sigma_{\overline{b-1}} \in G_i$ for all $i \leq q^{d\alpha} - 1$ and $\sigma_{\overline{b-1}} \notin G_i$ for $i \geq q^{d\alpha}$. $\square$

It is easily seen that for all $1 \leq \alpha \leq r$ the cardinality of the higher ramification groups is given by $|G(p^r)^\alpha| = q^{d(r-\alpha)}$.

Remark 2.3 *The filtration $\{G(p^r)^\alpha\}$ corresponds to the filtration in upper numbering via the Herbrand φ-function (cf. [5]).*

We write $G(n)$ for $(A/(n))^*$ and identify the Galois group $G(K(n)/K)$ with $G(n)$ under the given isomorphism.
Now we use the above results to calculate the genus via the Riemann–Hurwitz–formula and get

Theorem 2.4 *1. The genus of the field $K(p^r)$ is*

$$g(K(p^r)) = 1 + \frac{1}{2}\varphi(p^r)\left(-2 + \frac{q-2}{q-1} + d\frac{rq^d - r - 1}{q^d - 1}\right) .$$

2. More generally, for any monic polynomial $n \in A$ we get

$$g(K(n)) = 1 + \frac{1}{2}\varphi(n)\left(-2 + \frac{q-2}{q-1} + \sum_{\nu=1}^{s} d_\nu \frac{r_\nu q_\nu - r_\nu - 1}{q_\nu - 1}\right) .$$

Proof: The first part is shown. The second part of the theorem can be proved by induction under using some well–known facts:

1. The Riemann–Hurwitz–formula gives a recursion:

   $$2g(K(n)) - 2 = [K(n) : K(m_\nu)](2g(K(m_\nu)) - 2) + \deg \mathcal{D}(K(n)/K(m_\nu)) .$$

2. $K(n_\nu)$ and $K(m_\nu)$ are linearly disjoint over K and $\mathfrak{p}_\nu$ is the only finite ramified place in $K(n_\nu)/K$, it is unramified in $K(m_\nu)/K$ and totally split in $K'(m_\nu)/K'$ of degree $d_\nu \cdot \varphi(m_\nu)$ (cf. 1.2).

3. For $s \geq 2$ the ramification indices of ∞ in $K(n)/K$ and $K(m_\nu)/K$ are equal.

4. Let $\mathfrak{P} \in S(K(n))$ with $\mathfrak{P}|\mathfrak{p}_\nu$, and let $H_i(\mathfrak{P})$ be the i-th ramification group of $\mathfrak{P}$ in $K(n)/K(m_\nu)$. Then we have

   $$H_i(\mathfrak{P}) = G(K(n)/K(m_\nu)) \cap G_i(\mathfrak{P}) = G_i(\mathfrak{P}) ,$$

   because of $G(K(n)/K(m_\nu)) = G(K(n_\nu)/K) = G(n_\nu)$.

5. So for $s \geq 2$ we have

$$2g(K(n)) - 2 = \varphi(n_\nu)(2g(K(m_\nu)) - 2) + d_\nu \varphi(m_\nu) \sum_{i=0}^{\infty} (g_i(\mathfrak{p}_\nu) - 1) \ .$$

$\square$

3 The Decomposition Field $K_+(n)$

Now we calculate the genus of the decomposition field of the place ∞. We do this from the top and consider the extension $K(n)/K_+(n)$. Since $|\mathbb{F}_q^*| = q-1$, the ramification is tame for all places and all higher ramification groups are trivial. So we have only to calculate the inertia group. For a (fixed) finite place $\mathfrak{P}$ of $K(n)$ with $\mathfrak{P}|\mathfrak{p}_\nu$ for any $\nu = 1, \ldots, s$ the inertia group is

$$T_{\mathfrak{P}}(K(n)/K_+(n)) = T_{\mathfrak{P}}(K(n)/K) \cap G(K(n)/K_+(n)) \ .$$

Because of $T_{\mathfrak{P}}(K(n)/K) \cong G(n_\nu)$ we get

$$T_{\mathfrak{P}}(K(n)/K) \cong \{b \in G(n) \mid b \equiv 1 \bmod m_\nu\}$$

and therefore

$$T_{\mathfrak{P}}(K(n)/K) \cap G(K(n)/K_+(n)) \cong \begin{cases} \mathbb{F}_q^* \ , & \text{for} \quad s = 1 \\ \{1\} \ , & \text{for} \quad s > 1 \end{cases} \ .$$

All $\frac{\varphi(n)}{q-1}$ different places lying over ∞ have the ramification index $q-1$. This proves

Theorem 3.1 *The genus of $K_+(n)$ is*

$$\begin{aligned} g(K_+(n)) &= 1 + \frac{1}{q-1}\left(g(K(n)) - 1 - \frac{1}{2}\left(\varphi(n)\frac{q-2}{q-1} + d_1(q-2)\right)\right) \\ \textit{for } s = 1 \quad & \quad \textit{and} \\ g(K_+(n)) &= 1 + \frac{1}{q-1}\left(g(K(n)) - 1 - \frac{1}{2}\varphi(n)\frac{q-2}{q-1}\right) \quad \textit{for } s > 1 \ . \end{aligned}$$

4 Decomposition Fields and Their Intersections

Let the monic polynomial $n \in A$ now be relatively prime to T and $T-1$. So we can consider the decomposition field of (T) and $(T-1)$, respectively, in $K(n)$. This is no restriction, since for any two rational places (a) and (b) in K there exists a linear transformation which maps these places to (T) and $(T-1)$, respectively, and lets ∞ invariant.
We define $K_T(n)$ and $K_{T-1}(n)$ as the fixed field of the decomposition groups $Z_{(T)}(K(n)/K)$ and $Z_{(T-1)}(K(n)/K)$, respectively. We further put

$$\begin{aligned} K_{T,+}(n) &:= K_T(n) \cap K_+(n) \ , \\ K_{T,T-1}(n) &:= K_T(n) \cap K_{T-1}(n) \ , \\ K_{T,T-1,+}(n) &:= K_{T,T-1}(n) \cap K_+(n) \ . \end{aligned}$$

Now we will calculate the genus for each of these fields.

4.1 The Decomposition Group of a Finite Place

To do that we need an explicit description of the decomposition group of a place $\mathfrak{a} \in S(K)$ of degree α. It is well–known that this group is cyclic and the generator is the Frobenius automorphism, which is described by

$$\sigma(x) \equiv x^{q^\alpha} \bmod \mathfrak{A} \quad \text{for all } x \in \mathcal{O} \ .$$

Here $\mathfrak{A}$ is a prime divisor of $\mathfrak{a}$ in the integral closure $\mathcal{O}$ of A in $K(n)$. From [2, cor. 2.5.] follows

Proposition 4.1 *Let $a \in A$ be a monic, irreducible polynomial prime to n. The Frobenius automorphism of (a) is $\sigma_{\overline{a}}$.*

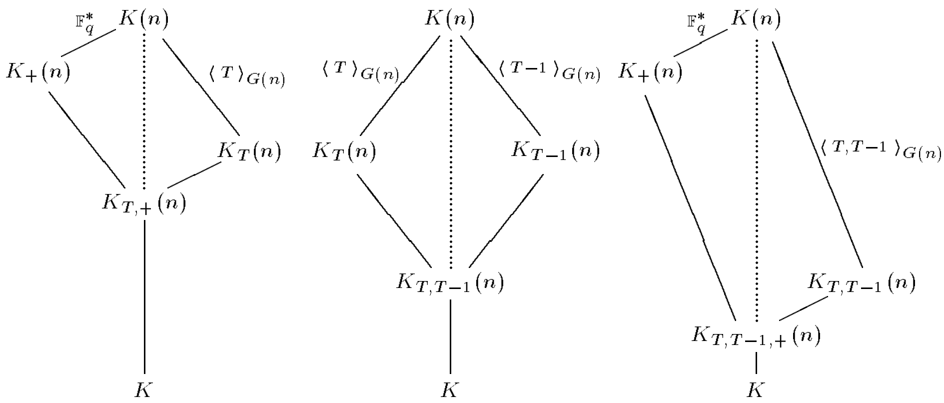
Definition 4.2 *Let $a \in G(n)$. Then $\langle\, a \,\rangle_{G(n)}$ denotes the subgroup of $G(n)$ generated by a.*

In view of our identifications we have for the decomposition group of the places (T) and $(T-1)$:

$$\begin{aligned} Z_{(T)}(K(n)/K) &= \langle \sigma_{\overline{T}} \rangle = \langle\, T \,\rangle_{G(n)} \\ \text{and} \qquad Z_{(T-1)}(K(n)/K) &= \langle \sigma_{\overline{T-1}} \rangle = \langle\, T-1 \,\rangle_{G(n)} \ . \end{aligned}$$

Now we can describe the Galois groups of the extensions.
We have

$$\begin{aligned} G(K(n)/K_{T,+}(n)) &= \langle\, T \,\rangle_{G(n)} \mathbb{F}_q^* \ , \\ G(K(n)/K_{T,T-1}(n)) &= \langle\, T, T-1 \,\rangle_{G(n)} \ , \\ G(K(n)/K_{T,T-1,+}(n)) &= \langle\, T, T-1 \,\rangle_{G(n)} \mathbb{F}_q^* \ . \end{aligned}$$



4.2 The Genus of the Subextensions

Definition 4.3 *For $\alpha = 1, \ldots, r_\nu$ we write $H(n_\nu)^\alpha$ for the embedding of $G(n_\nu)^\alpha$ in $G(n)$ and F_n for $\mathbb{F}_q^*$ regarded as a subgroup of $G(n)$.*

With this notation we have a description of the ramification groups for the different extensions $K(n)/L$, where L is one of the fields $K_T(n)$, $K_{T,+}(n)$, $K_{T,T-1}(n)$ and $K_{T,T-1,+}(n)$. For any $\nu \in \{1, \ldots, s\}$ let $\mathfrak{P}|\mathfrak{p}_\nu$ be a place of L and $q_\nu^{\alpha-1} \leq i \leq q_\nu^\alpha - 1$, then we have

$$\begin{aligned}
(G(K(n)/K_T(n))_i(\mathfrak{P}) &= \langle T \rangle_{G(n)} \cap H(n_\nu)^\alpha \ , \\
(G(K(n)/K_{T,+}(n))_i(\mathfrak{P}) &= \langle T \rangle_{G(n)} F_n \cap H(n_\nu)^\alpha \ , \\
(G(K(n)/K_{T,T-1}(n))_i(\mathfrak{P}) &= \langle T, T-1 \rangle_{G(n)} \cap H(n_\nu)^\alpha \ , \\
(G(K(n)/K_{T,T-1,+}(n))_i(\mathfrak{P}) &= \langle T, T-1 \rangle_{G(n)} F_n \cap H(n_\nu)^\alpha \ .
\end{aligned}$$

Now it follows that the sequences

$$\begin{array}{ccccccccc}
1 & \to & F_n \cap H(n_\nu)^\alpha & \to & F_n & \to & F_{m_\nu p_\nu^\alpha} & \to & 1 \ , \\
1 & \to & \langle T \rangle_{G(n)} \cap H(n_\nu)^\alpha & \to & \langle T \rangle_{G(n)} & \to & \langle T \rangle_{G(m_\nu p_\nu^\alpha)} & \to & 1 \ , \\
1 & \to & \langle T \rangle_{G(n)} F_n \cap H(n_\nu)^\alpha & \to & \langle T \rangle_{G(n)} F_n & \to & \langle T \rangle_{G(m_\nu p_\nu^\alpha)} F_{m_\nu p_\nu^\alpha} & \to & 1 \ , \\
1 & \to & \langle T, T-1 \rangle_{G(n)} \cap H(n_\nu)^\alpha & \to & \langle T, T-1 \rangle_{G(n)} & \to & \langle T, T-1 \rangle_{G(m_\nu p_\nu^\alpha)} & \to & 1
\end{array}$$

are exact. The maps between the groups are the usual injections and projections.

So it is possible to calculate the cardinality of a higher ramification group as the quotient of the cardinalities of two known groups. For a concrete example it is more or less necessary to build the different groups explicitly

and count the elements. So we get explicit formulas which depend on the relative position of $\langle T \rangle_{G(n)}$ and $\langle T-1 \rangle_{G(n)}$, and are therefore difficult to evaluate.
We give two examples.
Let $f \in A$ be a monic polynomial prime to T and $T-1$. Then we define

$$\begin{aligned} \tilde{e}_{T,T-1}(f) &:= |\langle T \rangle_{G(f)} \cap \langle T-1 \rangle_{G(f)}| \,, \qquad & e_{T,T-1}(f) &:= |\langle T, T-1 \rangle_{G(f)}|, \\ \tilde{e}_{T,T-1,+}(f) &:= |\langle T, T-1 \rangle_{G(f)} \cap F_f| \,, \qquad & e_{T,T-1,+}(f) &:= |\langle T, T-1 \rangle_{G(f)} F_f| \,, \end{aligned}$$

and for $s = 1$ we put $\tilde{e}_*(m_\nu) = 1$ and $e_*(m_\nu) := 1$.

Formula 4.4 *The field $K_{T,T-1}(n)$ has genus*

$$\begin{aligned} g(K_{T,T-1}(n)) &= 1 + \frac{1}{e_{T,T-1}(n)} \Bigg(g(K(n)) - 1 - \frac{1}{2} \Bigg[\frac{\varphi(n)}{q-1} \left(\tilde{e}_{T,T-1,+}(n) - 1 \right) \\ &\qquad + \sum_{\nu=1}^{s} \varphi(m_\nu) d_\nu \cdot a_\nu(K'_{T,T-1}(n)) \Bigg] \Bigg) \,, \end{aligned}$$

$$a_\nu(K'_{T,T-1}(n)) = \frac{e_{T,T-1}(n)}{e_{T,T-1}(m_\nu)} - q_\nu^{r_\nu - 1} + (q_\nu - 1) \sum_{\alpha=1}^{r_\nu - 1} q_\nu^{\alpha-1} \frac{e_{T,T-1}(n)}{e_{T,T-1}(m_\nu p_\nu^\alpha)} \,.$$

Formula 4.5 *The genus of $K_{T,T-1,+}(n)$ is*

$$\begin{aligned} g(K_{T,T-1,+}(n)) &= 1 + \frac{1}{e_{T,T-1,+}(n)} \Bigg(g(K(n)) - 1 - \frac{1}{2} \Bigg[\frac{\varphi(n)}{q-1} (q-2) \\ &\qquad + \sum_{\nu=1}^{s} \varphi(m_\nu) d_\nu \cdot a_\nu(K'_{T,T-1,+}(n)) \Bigg] \Bigg) \,, \end{aligned}$$

$$a_\nu(K'_{T,T-1,+}(n)) = \frac{e_{T,T-1,+}(n)}{e_{T,T-1,+}(m_\nu)} - q_\nu^{r_\nu - 1} + (q_\nu - 1) \sum_{\alpha=1}^{r_\nu - 1} \frac{q_\nu^{\alpha-1}\, e_{T,T-1,+}(n)}{e_{T,T-1,+}(m_\nu p_\nu^\alpha)} \,.$$

Remark 4.6 *It is clear that this method can also be used to calculate the ramification groups of the intersection of more than three decomposition fields.*

5 Number of Rational Places

In the subextensions from the top we get lower bounds for the number of rational places.

Let $\mathfrak{p} \in S(K)$ be a rational place. In its decomposition field $\tilde{K}$ in $K(n)/K$, every place over $\mathfrak{p}$ is again rational. So this field has degree of $\tilde{K}/K$ many rational places. Therefore the field L defined as above has – depending on the situation – at least one, two or three times $[L : K]$ many rational places. For $q = 2$ we made explicit calculations to the fields $K_*(n)$ with $deg\,(n) \leq 15$. Here the place ∞ is totally split in $K(n)$ and in any subextension because the inertia group is trivial. Furthermore $\mathbb{F}_2(T)$ has only three rational places and so we got through our systematic search the exact number of rational places in the intersection and not only a lower bound. Comparing our results with the tables published in [8] and [7], this yields three new lower bounds for the number of rational places for fields with fixed genus.

Example 5.1 *For the polynomial* $n = (T^4 + T^3 + 1)(T^4 + T^3 + T^2 + T^1 + 1)$ *with* $\varphi(n) = 225$ *and* $e_T(n) = 15$ *the field* $K_T(n)$ *has the genus* 38 *and* 30 *rational points. A theoretical upper bound is* 33 *(cf. [6]).*

Example 5.2 *The field* $K_{T,T-1}(n)$ *with* $n = (T^3 + T^2 + 1)^3(T^2 + T + 1)^2$ *where* $\varphi(n) = 5376$ *and* $e_{T,T-1}(n) = 336$*, has the genus* 66 *and* 48 *rational places. Here we have* 50 *as an upper bound.*

Example 5.3 *Let* $n = (T^3 + T^2 + 1)^2(T^3 + T + 1)(T^{11} + T^{10} + T^9 + T^7 + 1)$ *then the field* $K_T(n)$ *has the genus* 81 *and* 56 *rational places. For this genus* 59 *is an upper bound for the number of rational places.*

The following table gives our best results. In the first column the genus is written, in the second an upper bound which is taken from [8]. The third column gives the best results which are cited in the tables of [8] and [7]. (In the extensive bibliographies of these two papers, the reader will find many related articles.) The last column contains our best results for each of these genera.

Acknowledgements. This paper comprises the results of my Diplomarbeit, and I would like to thank my teacher, Prof. Dr. E.-U. Gekeler, for his support and Bodo Wack for writing the programs for the systematic search.

g	upper bound	lit.	here
2	6	6	6
5	9	9	8
6	10	10	9
8	11	11	9
9	12	12	12
11	14	14	12
20	21	19	18
21	21	21	21
22	22	21	18
26	25	24	24
28	26	24	24
29	27	25	24
31	28	27	24
32	29	26	24
34	30	27	27
37	32	28	28
38	33	28	30
41	35	32	32
42	35	30	30
48	39	34	32
51	41	36	36
53	42	40	36
54	43	42	42
55	43	36	36
62	48	44	42

g	upper bound	lit.	here
65	50	48	48
66	50	42	48
67	51	44	42
68	51	45	42
69	52	49	48
70	53	46	45
75	56	48	48
76	56	50	45
81	59	48	56
105	73		64
108	75		63
128	87		72
135	91		84
149	99		96
154	101		90
161	105		96
167	109		96
172	112		96
173	112		96
185	119		96
186	119		96
238	148		135
244	151		126
357	212		192
521	298		240

References

[1] Goss, David: Basic Structures of Function Field Arithmetic. Springer. Berlin (1996)

[2] Hayes, D.R.: Explicit class field theory for rational function fields. Trans.Am.Math.Soc. 189, (1974) 77–91

[3] Rust, I. and Scheja, O.: A guide to explicit class field theory in global function fields. Proceedings in Drinfeld Modules, Modular Schemes and Applications. World Scientific Publishing (1997) 44–65

[4] Niederreiter, H. and Xing, C.: Explicit global function fields over the binary field with many rational places. Acta Arith. 75, (1996) 59–76

[5] Serre, J-P.: Local Fields. Springer, New York (1979)

[6] Serre, J-P.: Sur le nombre des points rationnels d'une courbe algèbrique sur un corps fini. C.R.Acad. Sci. Paris Sér. I Math 296 (1983) 397–402

[7] Van der Geer, G. and Van der Vlugt, M.: Tables of curves with many points. Math. comp., electronically published (1999)

[8] Xing, C. and Niederreiter, H.: Drinfeld Modules and Algebraic Curves with Many Rational Points. Mh. Math 127, Springer (1999) 219–241