Transcendence Degree One Function Fields Over a Finite Field with Many Automorphisms

Gábor Korchmáros, Maria Montanucci and Pietro Speziali

Abstract

Let \( \mathbb{K} \) be the algebraic closure of a finite field \( \mathbb{F}_q \) of odd characteristic \( p \). For a positive integer \( m \) prime to \( p \), let \( F = \mathbb{K}(x, y) \) be the transcendence degree 1 function field defined by \( y^q + y = x^m + x^{-m} \). Let \( t = x^{m(q-1)} \) and \( H = \mathbb{K}(t) \). The extension \( F|H \) is a non-Galois extension. Let \( K \) be the Galois closure of \( F \) with respect to \( H \). By Stichtenoth [17], \( K \) has genus \( g(K) = (qm-1)(q-1) \), \( p \)-rank (Hasse-Witt invariant) \( \gamma(K) = (q-1)^2 \) and a \( K \)-automorphism group of order at least \( 2q^2m(q-1) \). In this paper we prove that this subgroup is the full \( K \)-automorphism group of \( K \); more precisely \( \text{Aut}_K(K) = Q \times D \) where \( Q \) is an elementary abelian \( p \)-group of order \( q^2 \) and \( D \) has a index 2 cyclic subgroup of order \( m(q-1) \). In particular, \( \sqrt{m} | \text{Aut}_K(K) | > g(K)^{3/2} \), and if \( K \) is ordinary (i.e. \( g(K) = \gamma(K) \)) then \( |\text{Aut}_K(K)| > q^{3/2} \). On the other hand, if \( G \) is a solvable subgroup of the \( K \)-automorphism group of an ordinary, transcendence degree 1 function field \( L \) of genus \( g(L) \geq 2 \) defined over \( \mathbb{K} \), then \( |\text{Aut}_K(K)| \leq 34(g(L)+1)^{3/2} < 68\sqrt{2}g(L)^{3/2} \); see [12]. This shows that \( K \) hits this bound up to the constant \( 68\sqrt{2} \).

Since \( \text{Aut}_K(K) \) has several subgroups, the fixed subfield \( F^N \) of such a subgroup \( N \) may happen to have many automorphisms provided that the normalizer of \( N \) in \( \text{Aut}_K(K) \) is large enough. This possibility is worked out for subgroups of \( Q \).

1 Introduction

Let \( L \) be a transcendence degree one function field defined over an algebraically closed field \( \mathbb{K} \), i.e. \( L = \mathbb{K}(\mathcal{X}) \) where \( \mathcal{X} \) is an algebraic curve defined over \( \mathbb{K} \). It is well known that if \( L \) is neither rational, nor elliptic then the \( \mathbb{K} \)-automorphism group \( \text{Aut}(L) \) of \( L \) is finite. More precisely, \( |\text{Aut}(L)| \leq 16g(L)^4 \) with just one exception, namely the Hermitian function field \( H = H(x, y), y^q + y = x^3 + x^{-3} \) with \( q = p^k \) whose genus equals \( \frac{1}{2}q(q-1) \) and \( K \)-automorphism group has order \( (q^3+1)q^3(q^2-1) \); see [15]. This bound was refined by Henn in [9] and for special families of curves in [3][4][5][8].

In [12] the authors investigated the case where \( L \) is ordinary, i.e. its genus and \( p \)-rank coincide, and they showed for this case that if \( G \) is a solvable subgroup of \( \text{Aut}(L) \) then

\[
|G| \leq 34(g(L)+1)^{3/2} < 68\sqrt{2}g(L)^{3/2}.
\]

By Stichtenoth [17], the Galois closure \( K \) of \( F|H \) where \( F = \mathbb{K}(x, y) \) with \( y^q + y = x^m + x^{-m} \) where \( q = p^k \), \( m \) is a positive integer prime to \( p \), \( H = \mathbb{K}(x^{m(q-1)}) \), has genus \( g(K) = (q-1)(qm-1) \), \( p \)-rank \( \gamma(K) = (q-1)^2 \) and size of the Galois group \( |\text{Gal}(K|H)| \geq q^2m(q-1) \). For \( m = 1 \), \( K \) is ordinary and it provides an example hitting the bound (1), up to the constant term.

In Section [5] we prove that this subgroup is almost the full \( \mathbb{K} \)-automorphism group of \( K \); more precisely \( \text{Aut}_K(K) = Q \times D \) where \( Q \) is an elementary abelian \( p \)-group of order \( q^2 \) and \( D \) has a index 2 cyclic subgroup of order \( m(q-1) \). Moreover, \( Q \) is defined over \( \mathbb{F}_{q^2} \) while \( D \) is defined over \( \mathbb{F}_{q^r} \) where \( r \) is the smallest positive
integer such that \( m(q-1) \mid (q^r-1) \). We also give an explicit representation for \( K \) showing that \( K = \mathbb{K}(x, y, z) \) with \( y^q + y = x^m + x^{-m} \) and \( z^q + z = x^m \).

Since \( \text{Aut}_{\mathbb{K}}(K) \) has several subgroups, the fixed subfield \( P^N \) of some of such subgroups \( N \) may happen to have many automorphisms provided that the normalizer of \( N \) in \( \text{Aut}_{\mathbb{K}}(K) \) is large enough. In Section 6, this possibility is worked out for subgroups of \( \Delta \).

\section{Background and Preliminary Results}

In this paper, \( \mathbb{K} \) denotes an algebraically closed field of odd characteristic \( p \). Let \( L \) denote a transcendence degree 1 function field with constant field \( \mathbb{K} \); equivalently let \( L \) denote the function field \( \mathbb{K}(X) \) of a (projective, non-singular, geometrically irreducible, algebraic) curve \( \mathcal{X} \) defined over \( \mathbb{K} \). The subject of our paper is the group of automorphisms \( \text{Aut}_{\mathbb{K}}(L) \) of \( L \) which fix \( \mathbb{K} \) elementwise, and we begin by collecting basic facts and known results on \( \text{Aut}_{\mathbb{K}}(L) \) that will be used in our proofs. For more details, the reader is referred to [10] and [16].

For a subgroup \( G \) of \( \text{Aut}_{\mathbb{K}}(L) \), the fixed field \( L^G \) of \( L \) is the subfield of \( L \) fixed by every element in \( G \). The field extension \( L|L^G \) is Galois of degree \( |G| \). Take a place \( \bar{P} \) of \( L^G \) together with a place \( P \) of \( L \) lying over \( \bar{P} \), that is, let \( P \) be an extension of \( \bar{P} \) to \( L \). The integer \( e = e(P|\bar{P}) \) defined by \( v_P(x) = e v_{\bar{P}}(x) \) for all \( x \in L^G \) is the \textit{ramification index} of \( P|\bar{P} \), and \( P|\bar{P} \) is \textit{unramified} if \( e(P|\bar{P}) = 1 \), otherwise it is \textit{ramified}. If \( P|\bar{P} \) is ramified then is either \textit{wild} or \textit{tame} ramified according as \( p \) divides \( e(P|\bar{P}) \) or not. Furthermore, \( P \) is \textit{ramified in} \( L|L^G \) if \( P|\bar{P} \) is ramified for at least one place \( P \) of \( L \), otherwise \( P \) is \textit{unramified in} \( L|L^G \), and the adjective wild or tame is used for \( P \) according as at least one or none of the places \( P \) of \( L \) lying over \( \bar{P} \) is wild or tame. Also, a place \( \bar{P} \) of \( L^G \) is \textit{totally ramified} in \( L|L^G \) if there is just one extension \( P \) of \( \bar{P} \) in \( L \), and if this occurs then \( e(P|\bar{P}) = |G| \). Moreover, \( L|L^G \) is an \textit{unramified extension} if no extension of \( P \) to \( L \) is ramified; otherwise \( L|L^G \) is an \textit{unramified extension}. If each extension \( P|\bar{P} \) is tame then \( L|L^G \) is a \textit{tame Galois extension}; otherwise it is a \textit{wild Galois extension}.

On the set \( \mathcal{P} \) of all places of \( L \), \( G \) has a faithful action. For \( P \in \mathcal{P} \), the \textit{stabilizer} \( G_P \) of \( P \) in \( G \) is the subgroup of \( G \) consisting of all elements of \( G \) fixing \( P \). A necessary and sufficient condition for a place \( P \in \mathcal{P} \) to be ramified is \( |G_P| > 1 \), the ramification index \( e_P \) being equal to \( |G_P| \). The \textit{G-orbit} of \( P \in \mathcal{P} \) consists of the images of \( P \) under the action of \( G \) on \( \mathcal{P} \), and it is a \textit{long or short} orbit according as \( G_P \) is trivial or not. If \( o \) is a \( G \)-orbit then \( |o| = |G|/|G_P| \) for any place \( P \in o \). If no \( G \)-orbit is short then no nontrivial element in \( G \) fixes a place in \( \mathcal{P} \), that is, \( L|L^G \) is an unramified Galois extension, and the converse also holds.

Assume now that \( L \) is neither rational nor elliptic. Then \( L \) has genus \( g(L) \geq 2 \), and \( G \) is finite with a finite number of short orbits on \( \mathcal{P} \). For an integer \( i \geq -1 \), the \( i \)-th ramification group \( G_P^{(i)} \) of the extension \( P|\bar{P} \) is defined to be

\[
G_P^{(i)} = \{ g \in G \mid \text{ord}_P(g(z) - z) \geq i + 1, \text{ for all } z \in O_P \},
\]

where \( O_P \) is the local ring at \( P \) in \( L \). These ramification groups are normal subgroups of \( G_P \) and they form a decreasing chain \( G_P = G_P^{(0)} \geq G_P^{(1)} \geq \cdots \geq \{1\} \). Here \( G_P^{(0)} = G_P \) whereas \( G_P^{(1)} \) is the (unique) Sylow \( p \)-subgroup of \( G_P \), and \( G_P = G_P^{(1)} \rtimes C \) where the complement \( C \) in the semidirect product \( G_P^{(1)} \rtimes C \) is cyclic. The Hurwitz genus formula states that

\[
2g(L) - 2 = |G|(2g(L^G) - 2) + \sum_{P \in \mathcal{P}_L} d_P.
\]
where \( g(L^G) \) is the genus of \( L^G \), and

\[
d_p = \sum_{i \geq 0}(|G_p^{(i)}| - 1). \tag{3}
\]

Let \( \gamma(L) \) denote the \( p \)-rank (equivalently, the Hasse-Witt invariant of \( L \)). If \( S \) is a \( p \)-subgroup of \( \text{Aut}_K(L) \) then the Deuring-Shafarevich formula, see [18] or [10, Theorem 11,62], states that

\[
\gamma - 1 = |S|(\bar{\gamma} - 1) + \sum_{i=1}^{k}(|S| - \ell_i), \tag{4}
\]

where \( \gamma(L^S) \) is the \( p \)-rank of \( L^S \) and \( \ell_1, \ldots, \ell_k \) denote the sizes of the short orbits of \( S \). Both the Hurwitz and Deuring-Shafarevich formulas hold true for rational and elliptic curves provided that \( G \) is a finite subgroup.

A subgroup of \( \text{Aut}_K(L) \) is a \( p' \)-group (or a prime to \( p \)) group if its order is prime to \( p \). A subgroup \( G \) of \( \text{Aut}_K(L) \) is tame if the 1-point stabilizer of any point in \( G \) is \( p' \)-group. Otherwise, \( G \) is non-tame (or wild). Every \( p' \)-subgroup of \( \text{Aut}_K(L) \) is tame, but the converse is not always true. If \( G \) is tame then the classical Hurwitz bound \( |G| \leq 84(g(L) - 1) \) holds, but for non-tame groups this is far from being true. The Stichtenoth bound \( |G| \leq 16g(L)^4 \) holds for any \( L \) with \( g(L) \geq 2 \) other than the Hermitian function field.

From Group Theory, we use the following three deep results, see [19, 6, 7].

**Lemma 2.1** (Dickson’s classification of finite subgroups of the projective linear group \( \text{PGL}(2, \mathbb{K}) \)). The finite subgroups of the group \( \text{PGL}(2, \mathbb{K}) \) are isomorphic to one of the following groups:

(i) prime to \( p \) cyclic groups;
(ii) elementary abelian \( p \)-groups;
(iii) prime to \( p \) dihedral groups;
(iv) the alternating group \( A_4 \);
(v) the symmetric group \( S_4 \);
(vi) the alternating group \( A_5 \);
(vii) the semidirect product of an elementary abelian \( p \)-group of order \( p^h \) by a cyclic group of order \( n > 1 \) with \( n \mid (q - 1) \);
(viii) \( \text{PSL}(2, p^f) \);
(ix) \( \text{PGL}(2, p^f) \).

**Lemma 2.2** (Feith-Thompson theorem). Every finite group of odd order is solvable.

**Lemma 2.3** (Alperin-Gorenstein-Walter theorem). If \( \Gamma \) is a finite simple group of 2-rank two (i.e. \( \Gamma \) contains no elementary abelian subgroup of order 8), then one of the following holds:

(i) The Sylow 2-subgroups of \( \Gamma \) are dihedral, and \( \Gamma \) is isomorphic to either \( \text{PSL}(2, n) \) with an odd prime power \( n \geq 5 \), or to the alternating group \( A_7 \).
(ii) The Sylow 2-subgroups of \( \Gamma \) are semi-dihedral and \( \Gamma \) is isomorphic to either \( \text{PSL}(3, n) \) with an odd prime power \( n \equiv -1 \text{ (mod 4)}, \) or to \( \text{PSU}(3, n), n \equiv 1 \text{ (mod 4)}, \) or to the Mathieu group \( M_{11} \).
(iii) The Sylow 2-subgroups of $\Gamma$ are wreathed, and $\Gamma$ is isomorphic to either PSL$(3,n)$ with an odd prime power $n \equiv 1 \pmod{4}$, or to PSU$(3, n), n \equiv -1 \pmod{4}$, or to PSU$(3, 4)$.

(iv) $\Gamma$ isomorphic to PSU$(3,4)$.

From now on, $K$ is the algebraic closure of a finite field $\mathbb{F}_q$ of odd order $q = p^h$ with $h \geq 1$, $m \geq 1$ is an integer prime to $p$, $F = K(x, y)$ is the transcendency degree 1 function field defined by $y^q + y = x^m + x^{-m}$, $t = x^{m(q-1)}$ and $H$ is the rational subfield $K(t)$ of $F$.

3 Galois closure of $F|H$

Let $F$ and $H$ be as defined in Section 1. Our first step is to give an explicit presentation of the Galois closure of $F|H$.

**Proposition 3.1.** The Galois closure of $F|H$ is $K(x, y, z)$ with

$$y^q + y = x^m + \frac{1}{x^m}, \quad (5)$$

$$z^q + z = x^m. \quad (6)$$

**Proof.** Let $K$ denote the function field $K(x, y, z)$ given by (5) and (6). We show first that $K$ contains a subfield isomorphic to an Artin-Mumford function field. For this, let $s = z - y$. Then (6) reads

$$s^q + s = y^q + y - (z^q + z) = \frac{1}{x^m},$$

whence by (6)

$$s^q + s = \frac{1}{z^q + z}. \quad (7)$$

The function field $L = K(x, s, z)$ with (5) and (7) is a subfield of $K$. Actually, $K = L$ as $y = z - s$, and $AM = K(s, z)$ with (7) is an Artin-Mumford subfield of $K$. Also,

$$[L : H] = [K : H] = [K : F] [F : H] = q^2 m (q-1).$$

It remains to show that Aut$(L)$ has a subgroup of order $q^2 m (q-1)$ fixing $t$. Take a positive integer $r$ for which $m|(q^r - 1)$. Let $\mathcal{V}$ be the subgroup of $\mathbb{F}_q^*$ consisting of all elements $v$ such that $v^m \in \mathbb{F}_q^*$. Obviously, $\mathcal{V}$ is a cyclic group of order $(q-1)m$.

For $\alpha, \beta \in \mathbb{F}_q^*$ with Tr$(\alpha) = \alpha^q + \alpha = 0$, Tr$(\beta) = \beta^q + \beta = 0$, and $v \in \mathcal{V}$, let $\varphi_{\alpha, \beta, v}(x, s, z)$ denote the $K$-automorphism of $K$

$$\varphi_{\alpha, \beta, v}(x, s, z) = (vx, v^{-m}s + \alpha, vmz + \beta). \quad (8)$$

Then $\varphi_{\alpha, \beta, v}(s)^q + \varphi_{\alpha, \beta, v}(s) = v^{-m}(s^q + s)$, and $\varphi_{\alpha, \beta, v}(z)^q + \varphi_{\alpha, \beta, v}(z) = v^m(z^q + z)$. This shows that (7) is left invariant by $\varphi_{\alpha, \beta, v}(x, s, z)$. Furthermore, $\varphi_{\alpha, \beta, v}(x)^m = vmx^m$. Let

$$\Phi := \{ \varphi_{\alpha, \beta, v} : v \in \mathcal{V}, \alpha^q + \alpha = 0, \beta^q + \beta = 0 \}.$$

A straightforward computation shows that

$$\varphi_{\alpha, \beta, v} \circ \varphi_{\alpha', \beta', v'} = \varphi_{v^{-m} \alpha' + \alpha, v^m \beta' + \beta, vm}.$$
and hence \( \Phi \) is a subgroup of \( \text{Aut}_K(L) \) of order \( q^2m(q - 1) \). Furthermore,

\[
\varphi_{\alpha,\beta,v}(t) = \varphi_{\alpha,\beta,v}(x^{m(q-1)}) = ((\varphi_{\alpha,\beta,v}(x))^{m})_{q-1} = v^{m(q-1)}x^{m(q-1)} = t.
\]

Since \([L : H] = [K : H] = q^2m(q - 1)\), the claim follows.

Our proof of Proposition 3.1 also gives the following result.

**Lemma 3.2.** The Galois group of the Galois closure \( K \) of \( F|H \) is \( \Phi \).

4 Some subgroups of \( \text{Aut}_K(K) \)

From Lemma 3.2, \( \Phi \) is a subgroup of \( \text{Aut}_K(K) \) of order \( q^2m(q - 1) \). Actually, \( \text{Aut}_K(K) \) is larger than \( \Phi \).

**Lemma 4.1.** \( |\text{Aut}_K(K)| \geq 2q^2m(q - 1) \).

**Proof.** Let

\[
\xi : (x, s, z) \mapsto \left( \frac{1}{x}, z, s \right).
\]

By a straightforward computation, \( \xi \in \text{Aut}_K(F) \), and \( \xi \notin \Phi \) is an involution. Since \( \xi \varphi_{\alpha,\beta,v} \xi = \varphi_{\beta,\alpha,v}^{-1} \) for every \( \varphi_{\alpha,\beta,v} \in \Phi \), the normalizer of \( \Phi \) contains \( \xi \). Thus, \( |\Phi, \xi| = 2q^2m(q - 1) \) by Lemma 3.2.

From the proof of Lemma 4.1, \( G = \Phi \times \langle \xi \rangle \) is a subgroup of \( \text{Aut}_K(K) \). Our main goal is to prove that \( G = \text{Aut}_K(K) \). The proof needs several results on the structure of \( \text{Aut}_K(K) \) which are stated and proven below. For this purpose, the following subgroups of \( \text{Aut}_K(K) \) are useful.

(i) \( \Psi := \{ \varphi_{\alpha,\alpha,1} | \alpha^q + \alpha = 0 \} \) of order \( q \).

(ii) \( \Delta := \{ \varphi_{\alpha,\beta,1} | \alpha^q + \alpha = \beta^q + \beta = 0 \} \) of order \( q^2 \).

(iii) \( W := \{ \varphi_{0,0,v} | v^m = 1 \} \) of order \( m \).

(iv) \( V := \{ \varphi_{0,0,v} | v \in V \} \) of order \( (q - 1)m \).

(v) \( M := \{ \varphi_{\alpha,\beta,v} \in \Phi | v^m = 1 \} \).

Obviously, both \( \Delta \) and \( \Psi \) are elementary abelian \( p \)-groups while both \( V \) and \( W \) are prime to \( p \) cyclic groups.

**Proposition 4.2.** \( K|F \) is an unramified Galois extension of degree \( q \). Furthermore, \( g(K) = (q - 1)(qm - 1) \) and \( \gamma(K) = (q - 1)^2 \).

**Proof.** We show that \( F = K^\Psi \). From \( \varphi_{\alpha,\alpha,1}(x, s, z) = (x, s + \alpha, z + \alpha) \),

\[
\varphi_{\alpha,\alpha,1}(y) = \varphi_{\alpha,\alpha,1}(z - s) = \varphi_{\alpha,\alpha,1}(z) - \varphi_{\alpha,\alpha,1}(s) = z + \alpha - (s + \alpha) = z - s = y.
\]

Moreover, \( \varphi_{\alpha,\alpha,1}(x) = x \). Therefore, \( K^\Psi \) contains \( F \). Since \([K : F] = q\) this yields \( F = K^\Psi \) whence the first claim follows. We show that no nontrivial element in \( \Psi \) fixes a place of \( K \). From the definition of \( \Psi \), every \( \psi \in \Psi \) leaves the Artin-Mumford subfield \( AM = \mathbb{K}(s, z) \) invariant. By a straightforward computation, if \( \psi \) is nontrivial, then it fixes no place of \( AM \). But then \( \psi \) fixes no place of \( L \), and hence \( K|F \) is unramified. Therefore, the Hurwitz genus formula and the Deuring-Shafarevich formula yield the second claim.

5
Proposition 4.2 has the following corollary.

**Corollary 4.3.** A necessary and sufficient condition for $F$ to be ordinary, i.e. $g(F) = \gamma(F)$, is $m = 1$.

**Lemma 4.4.** $\Delta$ is an (elementary abelian) Sylow $p$-subgroup of $\text{Aut}_K(K)$.

**Proof.** Let $S$ be a Sylow $p$-subgroup of $\text{Aut}_K(K)$ containing $\Delta$. From Nakajima’s bound [13] Theorem 1, see also [10] Theorem 11.84,

$$|S| \leq \frac{p^r}{p-2}(\gamma(X) - 1) = \frac{p^r}{p-2}(q^2 - 2q) < pq^2,$$

whence $|S| = q^2$. □

**Remark 4.5.** From the proof of Lemma 4.4 if $q = p$ then $K$ hits the Nakajima’s bound.

**Lemma 4.6.** The subgroups $\Delta$, $W$, $V$, $\Phi$ of $G$ have the following properties:

(i) $\Delta$ is a normal subgroup of $G$.

(ii) $W$ is a subgroup of the center $Z(\Phi)$ of $\Phi$.

(iii) $\Phi = \Delta \rtimes V$.

(iv) $G = \Delta \rtimes (V \rtimes \langle \xi \rangle)$.

**Proof.** By a direct computation,

$$\varphi^{-1}_{\alpha_1,\beta_1,v_1} \circ \varphi_{\alpha_1,\beta_1,v_1} = \varphi(\alpha_1v_1^{-m} + a)v_1^{-m - \alpha_1v_1^{-m}}(\beta_1v_1^{m} + \beta)v_1^{m - \beta_1v_1^{m}},$$

for every $\varphi_{\alpha_1,\beta_1,v_1} \in \Phi$ and $\varphi_{\alpha_1,\beta_1} \in \Delta$. Also, $\xi \circ \varphi_{\alpha_1,\beta_1} \circ \xi = \varphi_{-\alpha_1,-\beta_1}$. Therefore (i) holds. Furthermore, (ii) is proven by a straightforward computation. Since $\Delta$ is a normal subgroup of $G$, and $|\Delta|$ is prime to $|V|$, we have $\langle \Delta, V \rangle = \Delta V = \Delta \rtimes V$. Moreover, $|\Delta V| = |\Delta||V| = |\Phi|$. Thus, $\Phi = \Delta \rtimes V$. From this, (iv) also follows. □

**Lemma 4.7.** The action of $\Delta$ on the set $P$ of places of $K$ has exactly two short orbits both of length $q$.

**Proof.** From the Deuring-Shafarevich formula,

$$q^2 - 2q = \gamma(K) - 1 = |\Delta|\gamma(K^\Delta) - 1 + d,$$

with $d = \sum_{i=1}^{\gamma(K)}(q^2 - \lambda_i)$ where $\lambda_1, \ldots, \lambda_r$ are the lengths of the $r$ short orbits of $\Delta$ in its action on $P$. Since $|\Delta| = q^2$, Equation (9) taken mod $q^2$ yields that $d \geq q^2 - 2q$. Therefore, $\gamma(K^\Delta) = 0$ and hence

$$q^2 - 2q = -q^2 + d.$$

Thus $i \leq 2$ and [9] reads $q^2 - 2q = -q^2 + q^2 - \lambda_1 + q^2 - \lambda_2 = q^2 - (\lambda_1 + \lambda_2)$. whence $\lambda_1 + \lambda_2 = 2q$, that is, $\lambda_1 = \lambda_2 = q$. □

For each point $P$ in a short orbit of $\Delta$, the fact that $\Delta$ is abelian together with Lemma 4.7 yield the stabilizer $\Delta_P$ to have order $q$.

**Lemma 4.8.** For two points $P_1, P_2$ from different short orbits of $\Delta$, the stabilizers $\Delta_{P_1}$ and $\Delta_{P_2}$ have trivial intersection.
Proof. By absurd, $\Delta_{p_1}$ fixes as many as $2q$ places of $K$. The Deuring-Shafarevich formula applied to $\Delta_{p_1}$ yields that $q = 1 - \gamma$ where $\gamma$ is the $p$-rank of $K^\Delta_{p_1}$. But this cannot actually occur as $q > 2$. 

**Lemma 4.9.** Let $\Omega$ be a short orbit of $\Aut_K(K)$ containing both short orbits of $\Delta$. Then $\Omega$ is the unique non-tame short orbit of $\Aut_K(K)$. 

**Proof.** Take a place $P \in \mathcal{P}$ outside $\Omega$. By absurd, the stabilizer of $P$ in $\Aut_K(K)$ contains a non-trivial $p$-subgroup. Let $S_p$ be a Sylow $p$-subgroup containing that subgroup. Lemma 4.11 together with claim (i) of Proposition 4.6 yields that $S_p = \Delta$. Now, the proof follows from Lemma 4.7. 

The following results provide characterizations of the short orbits of $\Delta$. 

**Lemma 4.10.** $W$ fixes each place in the short orbits of $\Delta$. 

**Proof.** By Lemma 4.6, $\Delta \times W$ is an abelian group. From Lemmas 4.7 and 4.8, $\Delta \times W$ induces a permutation group on both short orbits of $\Delta$. The nucleus of the permutation representation of $\Delta \times W$ on any of them has order $qm$ and hence it contains $W$, the unique subgroup of $\Delta \times W$ of order $m$. 

**Lemma 4.11.** $\text{Supp}(\text{div}(s)_\infty)$ and $\text{Supp}(\text{div}(z)_\infty)$ are the short orbits of $\Delta$. 

**Proof.** From the proof of Proposition 3.7 the subfield $K^W$ is the Artin-Mumford function field $AM = \mathbb{K}(s, z)$ with (7). By (ii) of Lemma 4.6 the centralizer of $W$ in $\Aut_K(K)$ contains $\Delta$. Since $W \cap \Delta = \{1\}$, the restriction of the action of $\Delta$ on $AM$ is a subgroup of $\Aut_K(AM)$. On the other hand, $AM$ is the function field of the plane algebraic curve $\mathcal{C}$ of affine equation $(X^q + X)(Y^q + Y) = 1$ which has only two singular points, namely $X_\infty$ and $Y_\infty$, both ordinary singularities of multiplicity $q$. On the set of places, that is, branches of $\mathcal{C}$, $\Delta$ has a faithful action. Further, the unique Sylow $p$-subgroup $S_p$ of $\Aut_K(\mathcal{C})$ has order $q^2$ and a subgroup of $S_p$ of order $q$ fixes each of the $q$ places centered at $X_\infty$ and acts transitively on the set of the $q$ places centered at $Y_\infty$. Another subgroup of $S_p$ of order $q$ acts in the same way if the roles of the places centered at $X_\infty$ and $Y_\infty$ are interchanged. In particular, $\Delta = S_p$, and $\Delta$ has exactly two short orbits each of length $q$. In terms of $AM$, $\text{div}(s)_\infty$ is the sum of the $q$ places centered at $X_\infty$. This together with Lemma 4.11 shows that the places of $M$ lying over these $q$ places in the extension $K|AM$ form a short orbit of $\Delta$. Similarly, $\text{div}(z)_\infty$ is the sum of the $q$ places centered at $X_\infty$, and the places of $K$ lying over the $q$ places centered at $Y_\infty$ form a short orbit of $\Delta$. From Lemma 4.7 $\text{div}(s)_\infty$ and $\text{div}(z)_\infty$ are the short orbits of $\Delta$. 

From now on $\Omega_1$ and $\Omega_2$ denote the two short orbits of $\Delta$ as given in Lemma 4.7. Up to a change of notation, $\text{div}(s)_0 = \Omega_1$ and $\text{div}(s)_\infty = \Omega_2$. A byproduct of the proof of Lemma 4.11 is the following result. 

**Lemma 4.12.** The stabilizer of any point $P \in \Omega_1$ in $\Delta$ consists of all $\varphi_{\alpha,0,1}$ with $\alpha^q + \alpha = 0$. The same holds for $P \in \Omega_2$ and $\varphi_{0,\beta,1}$ with $\beta^q + \beta = 0$. 

We prove another result on the zeroes and poles of $x$. 

**Lemma 4.13.** The zeroes of $x$, as well as the poles of $x$, have the same multiplicity. 

**Proof.** From Lemma 4.11 any zero of $x$ is a point of $\Omega_1$. Since $\Delta$ fixes $x$, and $\Omega_1$ is an orbit of $\Delta$, the claim follows for the zeroes of $x$. The same argument works for the poles of $x$ whenever $\Omega_1$ is replaced by $\Omega_2$. Since $|\Omega_1| = |\Omega_2|$, we also have that the multiplicity of any zero of $x$ is equal to that of any pole of $x$. 

**Lemma 4.14.** The subfield $K^\Delta$ of $K$ is rational. 

7
Proof. For a place $P \in \Omega_1 \cup \Omega_2$, let $U$ be a subgroup of $\text{Aut}_K(K)$ fixing $P$ whose order $u$ is prime to $p$. Then $U$ is a cyclic group. Suppose that $U$ centralizes $\Delta_P$. Then $U\Delta_P$ is an abelian group of order $uq$. Furthermore, the first $u + 1$ ramification groups coincide, that is, $\Delta_P^{(0)} = \Delta_P^{(1)} = \ldots = \Delta_P^{(u)}$, see [10, Lemma 11.75 (iv)]. Since $\Delta_P = \Delta_P^{(0)}$ has order $q$ by Lemma 4.15, the Hurwitz genus formula applied to $\Delta$ gives

$$2g(K) - 2 \geq q(2g(K^\Delta) - 2) + 2q(q - 1)(u + 1)$$

By (ii) of Lemma 4.6 and Lemma 4.10, $U$ may be assumed to contain $W$. Then $2q^2(u + 1) \geq 2q^2(m + 1)$. This together with $2g(K) - 2 = 2(q^2m - qm - q)$ yields $g(K^\Delta) = 0$. \qed

The proof of Lemma 4.14 also gives the following result.

Lemma 4.15. The centralizer of $\Delta$ in $\text{Aut}_K(K)$ is $\Delta \times W$.

5 Main result

Our goal is to prove the following result.

Theorem 5.1. Let $K$ be the Galois closure of the extension $F|H$ where $F = F(x, y)$ with $y^q + y = x^m + x^{-m}$, and $H = \mathbb{K}(x^{m(q-1)})$. Then $\text{Aut}_K(K) = \Delta \rtimes (C_{m(q-1)} \rtimes \langle \xi \rangle)$ where $\Delta$ is an elementary abelian normal subgroup of order $q^2$, $C_{m(q-1)}$ is a cyclic subgroup and $\xi$ is an involution.

In the proof we treat two cases separately depending upon the abstract structures of minimal normal subgroups of $\text{Aut}_K(K)$.

5.1 Case I: $\text{Aut}_K(K)$ contains a solvable minimal normal subgroup

Lemma 5.2. If $N$ is a normal elementary abelian subgroup of $\text{Aut}_K(K)$ of order prime to $p$ then either $N \leq W$ or $|N| \equiv |N \cap W| + 1$ (mod $p$).

Proof. By (ii) of Lemma 4.9 the conjugate of every element in $N \setminus N \cap W$ by any element of $\Delta$ is also in $N \setminus N \cap W$. Assume on the contrary that $|N| - |N \cap W| \not\equiv 1$ (mod $p$). Then some element $u \in N \setminus N \cap W$ coincides with its own conjugate by any element of $\Delta$. Equivalently, $u$ centralizes $\Delta$. By Lemma 4.7, $u$ preserves $\Omega_1$ (and $\Omega_2$). Since $u$ has prime order different from $p$, $u$ fixes a place in $\Omega_1$. For $U = \langle u \rangle$, the argument used in the proof of Lemma 4.14 shows that $U$ is contained in $W$, a contradiction. \qed

Next, the possibility of the existence of some subgroup of $\text{Aut}_K(K)$ which is not contained in

$$G = \Phi \rtimes \langle \xi \rangle$$

is investigated.

Lemma 5.3. Let $H$ be a subgroup of $\text{Aut}_K(K)$ which is not contained in $G$. Then the centralizer of $H$ does not contain $W$.

Proof. As already observed in the proof of Lemma 4.11 the subfield $K^W$ is the Artin-Mumford function field $AM = \mathbb{K}(s, z)$ with $[\mathbb{K}:AM]$. By absurd, $HW/W$ is a subgroup of $\text{Aut}(AM)$. Since $|\text{Aut}(AM)| = 2(q - 1)q^2$, see [19, Theorem 7] for $q = p$ and [13, Theorem 5.3] for any $q$, and $G/W$ is a subgroup of $\text{Aut}(AM)$, the latter subgroup is the whole $\text{Aut}(AM)$. Therefore $HW/W$ is contained in $G/W$. But then $HW \leq G$ and hence $H \leq G$, a contradiction. \qed
From Proposition 4.6, \( M = \Delta \times W \). Therefore, \( M \) is an abelian subgroup of \( \Phi \) of order \( q^2m \), and \(|M| = q^2m > (q - 1)(qm - 1) = \varphi(K)\). Let \( R \) be the subgroup of \( G \) generated by \( M \) and \( \xi \). Then \( R = M \times \langle \xi \rangle \) as the normalizer of \( M \) in \( G \) contains \( \xi \).

**Lemma 5.4.** If \( N \) is an elementary abelian normal \( 2 \)-subgroup of \( \text{Aut}_K(K) \) then \( N = \{1, \varphi_{0,0,-1}\} \).

**Proof.** By definition, \( \xi \) and \( \varphi_{0,0,-1} \) are contained in \( G \). Since both \( \xi \) and \( \varphi_{0,0,-1} \) are involutions and commute, they generate an elementary abelian subgroup \( S \) of \( G \) of order 4. Let \( U \) be a subgroup of \( \text{Aut}_K(K) \) of order \( d = 2^n \geq 2 \). From the Hurwitz genus formula applied to \( U \),

\[
2\varphi(K) - 2 = 2^n(2\varphi(K^U) - 2) + \sum_{i=1}^k (2^n - \ell_i)
\]

where \( \ell_1, \ldots, \ell_k \) are the short orbits of \( U \) on the set \( P \) of all places of \( K \). Since \( \varphi(K) = (q - 1)(qm - 1) \) is even, and hence \( 2\varphi(K) - 2 \equiv 2 \pmod{4} \), while \( 2^n(2\varphi(K^U) - 2) \equiv 0 \pmod{4} \), some \( \ell_i \) \((1 \leq i \leq k)\) must be either 1 or 2. Therefore, \( U \) or a subgroup of \( U \) of index 2 fixes a point of \( \mathcal{X} \) and hence is cyclic. From [11] Chapter I, Satz 14.9, \( U \) is either cyclic, or the direct product of a cyclic group by a group of order 2, or a generalized quaternion group, or dihedral, or semidihedral, or a modular maximal-cyclic group (also called type (3) with Huppert’s notation). In particular, \( U \) contains no elementary abelian subgroup of order 8. By absurd, let \( N \) be a elementary abelian normal \( 2 \)-subgroup of \( \text{Aut}_K(K) \) which is not contained in \( G \). Then \( N \) has order 2 or 4. In the former case, \( N \) is in \( Z(\text{Aut}_K(K)) \) and hence \( N \) together with \( S \) generate an elementary abelian group of order 8, a contradiction. If \(|N| = 4 \) and \( N \cap S = \{1\} \) then some non-trivial element of \( s \in S \) commutes with each element of \( N \), and hence \( N \) together with \( s \) generate an elementary abelian group of order 8, again a contradiction. If \( N \cap S = \{1, u\} \) then \( u \in Z(G) \) and hence \( u = \varphi_{0,0,-1} \). Since \(|N| - |N \cap S| = 2 \), Lemma 5.2 yields \( N < W \) a contradiction. Therefore, \( N < G \), and hence \( N \) is a subgroup of \( V \times \langle \xi \rangle \). Since \( V \) is cyclic, \( N \) contains \( \varphi_{0,0,-1} \). If \(|N| = 4 \) then \( N \) has two elements outside \( W \). But this is impossible by Lemma 5.2.

**Remark 5.5.** The proof of Lemma 5.4 also shows that \( \text{Aut}_K(K) \) contains no elementary abelian group of order 8.

**Lemma 5.6.** Any solvable minimal normal subgroup of \( \text{Aut}_K(K) \) is contained in \( R \).

**Proof.** Let \( N \) be a solvable minimal normal subgroup of \( \text{Aut}_K(K) \). Then \( N \) is an elementary abelian group of order \( r^h \) with a prime \( r \geq 2 \) and \( h \geq 1 \). If \( r = p \) then \( N \) is contained in \( \Delta \) by Lemma 4.4. Therefore \( r \neq p \) is assumed. By Lemma 5.2, the case \( r = 2 \) is dismissed, as well.

We investigate the subfield \( K^N \). The quotient group \( \bar{M} = M/N \) is a subgroup of \( \text{Aut}_K(K^N) \). Since \( p \neq r \), we have \( \Delta \cap N = \{1\} \) and \( M \cap N = W \cap N \leq W \). Furthermore, \( \bar{M} = M/(M \cap N) \cong \Delta W/(W \cap N) \). The Hurwitz genus formula applied to \( N \) yields \( \varphi(K) - 1 \geq |N|/\varphi(K^N) - 1 \).

We show that the \( \ell \)-rank \( \gamma(K^N) \) of \( K^N \) is positive. If \( \gamma(K^N) = 0 \) by absurd, any nontrivial \( \ell \)-subgroup of \( \text{Aut}_K(K^N) \) has exactly one fixed place, see [10] Lemma 11.129]. Let \( \hat{P} \) be the unique fixed place of \( \Delta = \Delta N/N \) viewed as a subgroup of \( \text{Aut}_K(K^N) \). Then the \( \Delta \)-orbit of \( \hat{P} \) in the extension \( K\bar{M}^N \) contains \( \Omega_1 \cup \Omega_2 \). Furthermore, since \( N \) is a normal subgroup of \( \text{Aut}_K(K) \), \( \Omega \) is the union of \( \Delta \)-orbits. By Lemma 4.1, each \( \Delta \)-orbit other than \( \Omega_1 \) and \( \Omega_2 \) has size \( q^2 \). Therefore, \( q \) divides \( |\Omega| \). Since \( |\Omega| \) divides \( |N| \), this yields that \( q \) divides \( N \), a contradiction. As a consequence, \( K^N \) is not rational.

We show that \( K^N \) is neither elliptic. For a place \( P \in \Omega_1 \), all ramification groups \( N_i^{(i)} \) of \( N \) at \( P \) have odd order, and hence \( d_P = \sum_i (N_i^{(i)} - 1) \) is even. Let \( \theta \) be the \( \Delta \)-orbit containing \( P \). Then, \( |N_P|/|\theta| = |N| \).
Take a Sylow 2-subgroup \( S \) of \( G \) containing a Sylow 2-subgroup \( S_P \) of \( G_P \). Since \( \xi, \varphi_{0,0,-1} \) are two distinct involutions which commute, \( S \) is not cyclic. Therefore \( S \neq S_P \), as \( S \) does not fix \( P \). Thus \( |S| \) does not divide \( |G_P| \) showing that the \( G \)-orbit of \( P \) must have even length. This yields that \( \sum_{p \in P} d_p \) is divisible by four.

On the other hand, \( 2g(K) - 2 = 2(q^2m - qm - q) \) is twice an odd number, a contradiction.

Therefore, \( g(K^N) \geq 2 \). From the Nakajima bound, see [14], or [10, Theorem 11.84] applied to \( \hat{\Delta} \),

\[
q^2 \leq \frac{p}{2}(\gamma(K^N) - 1) \leq \frac{p}{2}(g(K^N) - 1)
\]

whence

\[
g(K^N) - 1 \geq \begin{cases} 
3 & \text{when } q = 3, \\
15 & \text{when } q > 3.
\end{cases}
\] (10)

From \( |M| \geq g(K) - 1 \),

\[
4|M| \geq 4(g(K) - 1) \geq 4|N|(g(K^N) - 1) = |N|(4g(K^N) + 4 - 8)
\] (11)

which yields

\[
4|M| \geq |N||M| - 8|N|.
\] (12)

From \( |N|(g(K^N) - 1) \leq (g(K) - 1) \leq |M| \),

\[
4 \geq \frac{|N|}{|M|} \cdot \frac{|M|}{|M \cap N|} - \frac{8|N|}{|M \cap N|} = \frac{|N|}{|M \cap N|} - \frac{8}{g(K^N) - 1}.
\] (13)

This and (10) yield

\[
\frac{|N|}{|W \cap N|} \leq \begin{cases} 
6 & \text{when } q = 3, \\
4 & \text{when } q > 3.
\end{cases}
\] (14)

Since \( W \cap N \leq N \) we have \( |W \cap N| = r^w \) for some \( 0 \leq w \leq h \). By (10) and Lemma 5.2, this is only possible when either \( r = 3 \) and \( p \neq 3 \), or \( r = 5 \) and \( q = 3 \), or \( w = h \). In the latter case, \( W \cap N = N \) whence \( N \leq W < R \), and the claim is proven. If \( r = 3 \) and hence \( |N| = 3 \) or \( |N| = 9 \) according as \( N \cap W = \{1\} \) or \( |N \cap W| = 3 \), Lemma 5.2 shows that \( N \leq W < R \). The same argument works for \( r = 5 \), \( |N| = 5, 25 \), and \( |N \cap W| = 1, 5 \).

Lemma 5.7. If a normal subgroup \( N \) of \( \Phi \) is contained in \( \Delta \) then \( N \) coincides with \( \Delta \).

Proof. Take \( \varphi_{\alpha,\beta,1} \in N \) for some \( \alpha \neq 0 \), \( \beta \neq 0 \). Since \( v \) has order \( m(q - 1) \) in \( F_q \). \( v^m \) is a primitive element of \( F_q \). Since \( N \) is normal in \( \text{Aut}_F(K) \), \( \varphi_{0,0,v}^{-1} \circ \varphi_{\alpha,\beta,1} \circ \varphi_{0,0,v} \in N \). From

\[
\varphi_{0,0,v}^{-1} \circ \varphi_{\alpha,\beta,1} \circ \varphi_{0,0,v}(x, s, z) = (x, s + v^m \alpha, z + v^{-m} \beta),
\]

\[
\varphi_{0,0,v}^{-1} \circ \varphi_{\alpha,\beta,1} \circ \varphi_{0,0,v} = \varphi_{v^m \alpha, v^{-m} \beta, 1}.
\]

Since \( v^m \) is a primitive element of \( F_q \), \( N \) contains each \( \varphi_{\alpha',\beta',1} \) whenever \( \alpha' = \omega \alpha, \beta' = \omega^{-1} \beta \) with \( \omega \in F_q^* \). Thus \( |N| \geq q \). Moreover if \( \alpha_i = \omega_i \alpha \) and \( \beta_i = \omega_i^{-1} \beta \), where \( \omega_i \in F_q^* \) and \( i = 1, 2 \) then \( N \) contains \( \varphi_{\alpha_i,\beta_i,1} = \varphi_{(\omega_1 + \omega_2) \alpha, (\omega_1^{-1} + \omega_2^{-1}) \beta, 1} \). To count the elements in \( N \), observe that \( (\omega + \omega')^{-1} = \omega^{-1} + \omega'^{-1} \) only occurs whenever \( \omega' = \omega \) is a root of the quadratic polynomial \( \omega x + \omega^2 + x^2 \). For a fixed \( \omega \), this shows that at least \( (q - 1) - 2 = q - 3 \) possible choices for \( \omega' \) provide different elements in \( N \). Thus, \( |N| \geq q + (q - 1)(q - 3) = q^2 - 3(q - 1) \).

By absurd, \( N \) is a proper subgroup of \( \Delta \). Then \( q^2 - 3(q - 1) \leq \frac{q^2}{p} \), which is only possible for \( q = p = 3 \). In this case, since \( \psi \circ \varphi_{\alpha,\beta,1} \circ \psi \in N \) we find \( q - 1 \) more elements in \( N \) of the form \( \varphi_{\alpha',\beta',1} \), where \( \alpha' = \omega \alpha \) and \( \beta' = \omega \beta \) for \( \omega \in F_q^* \). Thus, \( |N| \geq q^2 - 2(q - 1) = 5 \). Since \( \frac{q^2}{p} = 3 \) the claim also holds in this case. \( \square \)
Lemma 5.8. Let $N$ be a normal subgroup $M$ of $R$. If $|N| = r^h$, with an odd prime $r$ different from $p$, then $N$ is a subgroup of $W$.

Proof. From $[R : M] = 2$, $N$ is a subgroup of $M = \Delta \times W$. Since $N \cap \Delta = \{1\}$, this is only possible when $N < W$.

Lemmas 5.4, 5.6, 5.7, 5.8 have the following corollary.

Lemma 5.9. Let $N$ be a solvable minimal normal subgroup of $\text{Aut}_K(K)$. Then either

(i) $N = \Delta$, and $|N| = q^2$,

(ii) $N < W$, and $|N| = r$ with a prime $r$ different from $p$.

Lemma 5.10. If $\text{Aut}_K(K)$ has a solvable minimal normal subgroup then $\Delta$ is a normal subgroup of $\text{Aut}_K(K)$.

Proof. We may assume that (ii) of Lemma 5.9 holds. Then $N = \langle \varphi_{0,0,w} \rangle$ with $w^r = 1$. Therefore, the fixed places of $N$ are the zeroes and poles of $x$. From Lemma 4.11 these points form $\Omega_1 \cup \Omega_2$. Hence $\text{Aut}_K(K)$ preserves $\Omega_1 \cup \Omega_2$. Therefore, the conjugate $\Delta'$ of $\Delta$ by any $h \in \text{Aut}_K(K)$ has its two short orbits $\Omega_1'$ and $\Omega_2'$ contained in $\Omega_1 \cup \Omega_2$. Actually, $\Omega_1' \cup \Omega_2' = \Omega_1 \cup \Omega_2$. From this we infer that $\Delta = \Delta'$. Take any place $P \in \Omega_1$. Then $|\Delta_P| = |\Delta'_P| = q$. Then both $\Delta_P$ and $\Delta'_P$ are contained in the unique $p$-subgroup $S_P$ of the stabilizer of $P$ in $\text{Aut}_K(K)$, see [10] (ii)a Theorem 11.49. If $\Delta'_P \neq \Delta_P$ then $|S_P| > q$. Let $S$ be a Sylow $p$-subgroup of $\text{Aut}_K(K)$. By Lemma 4.3 $S$ is conjugate to $\Delta$ in $\text{Aut}_K(K)$. But this is impossible as $|\Delta_Q| \leq q$ for any $Q \in \Delta'$ by Lemma 4.7. The same argument works for any place in $\Omega_2$. Since $\Delta_P$ and $\Delta_Q$, with $P \in \Omega_1, Q \in \Omega_2$, generate $\Delta$, it turns out that $\Delta'$ is also generated by $\Delta_P$ and $\Delta_Q$. Thus $\Delta = \Delta'$.

Lemma 5.11. If $\text{Aut}_K(K)$ has a solvable minimal normal subgroup then $W$ is a normal subgroup of $\text{Aut}_K(K)$.

Proof. We may assume that (ii) of Lemma 5.9 holds. From Lemma 4.15, $\Delta \times W$ is a normal subgroup of $\text{Aut}_K(K)$. Since $|\Delta|$ and $|W|$ are coprime, the assertion follows.

Theorem 5.12. If $\text{Aut}_K(K)$ has a minimal normal subgroup which is solvable then $\text{Aut}_K(K) = G$. In particular $|\text{Aut}_K(K)| = 2q^2(q - 1)m$.

Proof. As usual, the factor group $\text{Aut}_K(K)/\Delta$ is viewed as a subgroup of $\text{Aut}_K(K \Delta)$. Since $\xi$ interchanges $\Omega_1$ and $\Omega_2$, Lemma 4.7 yields that $\text{Aut}_K(K \Delta)$ has an orbit of length 2 consisting of the points lying under $\Omega_1$ and $\Omega_2$ in the field extension $K|\Delta$. From Lemma 4.14 $K \Delta$ is rational. Hence $\text{Aut}_K(K \Delta)$ is isomorphic to a subgroup of $\text{PGL}(2, K)$. From the classification of subgroups of $\text{PGL}(2, K)$, $\text{Aut}_K(K \Delta)$ is a dihedral group. This shows that $\text{Aut}_K(K)$ contains a (normal) subgroup $T$ of index 2 such that $T = \Delta \times C$ with a cyclic group $C$. Observe that $T$ is the subgroup of $\text{Aut}_K(K)$ which preserves both $\Omega_1$ and $\Omega_2$. Hence $W \leq T$. From Lemma 5.11, $CW$ is a group. Since its order $|C||W|/|C \cap W|$ is prime to $p$, this yields $W \leq C$. Therefore, the assertion follows from Lemma 5.8.

5.2 Case II: $\text{Aut}_K(K)$ contains no solvable minimal normal subgroup

For the rest of the paper we assume that $\text{Aut}_K(K)$ has no solvable minimal normal subgroup. In particular, $O(\text{Aut}_K(K))$ is trivial, that is, $\text{Aut}_K(K)$ is an odd-core free group. Therefore, any minimal normal subgroup $N$ of $\text{Aut}_K(K)$ is the direct product of pairwise isomorphic non-abelian simple groups. Since $\text{Aut}_K(K)$ has no elementary abelian subgroup of order 8, see the proof of Lemma 5.4 this direct product has just one factor, that is, $N$ itself is a non-abelian simple group. The possibilities for $N$ are listed below.
Lemma 5.13. If no minimal normal subgroup of $\text{Aut}_G(K)$ is solvable, and $N$ is a non-abelian minimal normal subgroup of $\text{Aut}_G(K)$, then $\Delta$ is contained in $N$.

Proof. Since $N$ is a normal subgroup, its centralizer $C(N)$ in $\text{Aut}_G(K)$ is also a normal subgroup of $\text{Aut}_G(K)$. Actually $C(N)$ is trivial. In fact, on one hand, $C$ has odd order, since an involution in $\text{Aut}_G(K)$ together with an elementary abelian group of $N$ of order 4 would generate an elementary abelian group of order 8 contradicting the claim in Remark 5.5. On the other hand, groups of odd order are solvable by the Feith-Thompson theorem. By conjugation, every $d \in \Delta$ defines a permutation on $N$, and hence $\Delta$ has a permutation representation on $N$. Its kernel is contained in the centralizer $C(N)$, and hence is trivial, that is, the permutation representation is faithful. Therefore, $\Delta$ is isomorphic to a subgroup $D$ of the automorphism group $\text{Aut}(N)$ of $N$.

We show that $D \cap N \neq \{1\}$. By absurd, $\text{Aut}(N)/N$ contains the subgroup $DN/N \cong D$. Then case (I) does not occur since $\text{Aut}(N) \cong \text{PSL}(2, q)$ while the factor group $\text{PSL}(2, q)/\text{PGL}(2, q)$ is cyclic and $[\text{PGL}(2, q) : \text{PSL}(2, q)] = 2$, and hence the odd order subgroups of $\text{Aut}(N)/N$ are all cyclic. In case (II), $\text{Aut}(N) \cong \text{PGL}(3, q)$ while the factor group $\text{PGL}(3, q)/\text{PSL}(3, q)$ is cyclic and $[\text{PGL}(3, q) : \text{PSL}(3, q) : 3] = 1, 3$ according as $q \equiv \pm 1 \pmod{3}$. Therefore, an odd order subgroup of $\text{Aut}(N)/N$ is an elementary abelian group of order $q^2$ only for $q = 3$ and $q \equiv 1 \pmod{3}$. Furthermore, if $q \equiv 1 \pmod{3}$ then $|N|$ also divisible by 3. Therefore, case (ii) does not occur either. Case (III) can be ruled out with the same argument replacing the condition $q \equiv \pm 1 \pmod{3}$ with $q \equiv \mp 1 \pmod{3}$. In cases (IV), $|\text{Aut}(N)/N| = 2$ and $|\text{Aut}(N)/N| = 1$ respectively, and they contain no nontrivial subgroups of odd order.

The nontrivial subgroup $D \cap N$ is contained in a Sylow $p$-subgroup $S_p$ of $N$. Since $N$ is a normal subgroup of $\text{Aut}_G(K)$, Lemma 5.13 yields that $D \cap N$ is a subgroup of $\Delta$. Since $D \cap N$ is a normal subgroup of $G$, Lemma 4.4 shows that $D \cap N = \Delta$. Therefore, $\Delta < N$. \hfill \Box

Proposition 5.14. $\text{Aut}_G(K)$ has a minimal normal solvable subgroup.

Proof. By absurd, $\text{Aut}_G(K)$ has no minimal solvable subgroup, and hence it has a minimal normal simple subgroup isomorphic to one of the five simple groups listed above. From the proof of Lemma 5.13 the centralizer of $N$ in $\text{Aut}_G(K)$ is trivial. Therefore, we have a monomorphism $\tau : \text{Aut}_G(K) \rightarrow \text{Aut}(N)$ defined by the map which takes $g \in \text{Aut}_G(K)$ to the automorphism $\tau(g)$ of $N$ acting on $N$ by conjugation with $g$. Since $\tau$ maps $N$ into a normal subgroup $\tau(N)$ of $\text{Aut}(N)$ and $\Delta < N$ by Lemma 5.13 we have that $\tau(N)$ has a subgroup isomorphic to $\Delta$.

In Case (I), $\tau(N) = \text{PSL}(2, q)$, and $\bar{q} = q^2$ by Lemma 4.4 and the classification of subgroups of $\text{PSL}(2, q)$. From Lemma 4.15 the centralizer of $\Delta$ in $\text{Aut}_G(K)$ contains an element of order prime to $p$. Obviously, the same holds for $\tau(\Delta)$ where $\tau(\Delta) < \tau(N) \cong \text{PSL}(2, q)$. But this is impossible since $\text{Aut}(\text{PSL}(2, q)) = \text{PGL}(2, q)$ and any subgroup of $\text{PGL}(2, q)$ of order $q$ coincides with its own centralizer in $\text{PGL}(2, q)$.

In Case (II), $\tau(N) = \text{PSL}(3, q)$ and $q$ must be a divisor of $q - 1$. The latter claim follows from the fact that $\text{PSL}(3, q)$ has order $q^3(q^2 + q + 1)(q + 1)/12$ with $q = 3, 1$ according as $q \equiv \pm 1 \pmod{3}$ where its subgroups of order $q^2$ are not abelian while its subgroups of order $q + 1$ and of order $q + 1$
are cyclic. Therefore, \(\tau(\Delta)\) is a Sylow subgroup contained in a subgroup which is the direct product of two cyclic groups of order \(\bar{q} - 1\). Since \(\bar{q} - 1\) is even, this shows that the centralizer of \(\tau(\Delta)\) in \(PSL(3, \bar{q})\) contains an elementary abelian subgroup of order 4. Since \(\tau\) is a monomorphism, the same holds for the centralizer of \(\Delta\) in \(\text{Aut}_{\bar{K}}(K)\). But this contradicts Lemma 4.15.

Case (III) can be ruled out with the argument used for Case (II) whenever \(\bar{q} - 1\) and \(\bar{q} + 1\) are interchanged.

In Cases (IV) and (V), we have \(\text{Aut}(N) = S_7\) and \(\text{Aut}(N) = M_{11}\) respectively. The only Sylow subgroups of \(N\) whose orders are square numbers have order 9, and they coincide with their own centralizers in \(\text{Aut}(N)\) contradicting Lemma 4.15.

\[
\text{Case (III) can be ruled out with the argument used for Case (II) whenever } \bar{q} - 1 \text{ and } \bar{q} + 1 \text{ are interchanged.}
\]

\[
\text{In Cases (IV) and (V), we have } \text{Aut}(N) = S_7 \text{ and } \text{Aut}(N) = M_{11} \text{ respectively. The only Sylow subgroups of } N \text{ whose orders are square numbers have order 9, and they coincide with their own centralizers in } \text{Aut}(N) \text{ contradicting Lemma 4.15.}
\]

6 Some Galois subcovers of \(K\)

We investigate the possibility that some Galois subcovers of the Galois closure \(K\) of \(F|H\) are of the same type of \(K\) with different defining pair \((q, m)\) of parameters. More precisely, we consider the family of all function fields \(\bar{F}(x, y)\) with \(y^q + y = x^m + x^{-m}\) where \(\bar{q} = p^k\), \(\bar{m}\) is any positive integer prime to \(p\), and find sufficient conditions on the parameters \(\bar{q}\) and \(\bar{m}\) ensuring that the Galois closure \(\bar{K}\) of the extension \(\bar{F}|H\) be isomorphic to a subfield of \(K^H\) for a subgroup \(H\) of \(\text{Aut}_{\bar{K}}(K)\).

First we point out that this can really occur.

**Proposition 6.1.** For any divisor \(d\) of \(m\), let \(C\) be the subgroup of \(W\) of order \(d\), and set \(\bar{m} = m/d\). Then the subfield \(K^C\) of \(K\) is \(\bar{K}(t, s, z)\) with (7) and

\[
z^q + z = t^\bar{m},
\]

and \(K^C\) is isomorphic to \(\bar{F}\) for \(\bar{q} = q\) and \(\bar{m}\).

**Proof.** The rational function \(t = x^d\) is fixed by \(C\). Since \([\bar{K}(K): \bar{K}(K^C)] = d\) and \(\bar{K}(t, s, z) \subset K^C\), the claim follows.

Next we show examples with \(\bar{q} < q\) arising from subfields of \(\bar{F}_q\). For this purpose, we need a slightly different representation for \(K\) and its \(\bar{K}\)-automorphism group. Take two nonzero elements \(\mu, \theta \in \bar{K}\) such that \(\mu^q + \mu = 0\) and \(\theta^m = -\mu^{-1}\), and define \(x' = \theta^{-1}x\), \(s' = \mu^{-1}s\), \(z' = \mu z\). Then \(K = \bar{K}(x', s', z')\) with

\[
s'^q - s' = \frac{1}{z'^q - z'},
\]

and

\[
z'^q - z' = x'^m.
\]

In fact, from (7),

\[
1 = (s^q + s)(z^q + z) = (\mu^q s^q + \mu s')(\mu^{-q} z'^q + \mu^{-1} z') = (s'^q - s')(z'^q - z'),
\]

while, from (6),

\[
-\mu^{-1} x'^m = x^m = z^q + z = -\mu^{-1}(z'^q - z').
\]

Let \(\bar{F}_q\) the smallest Galois extension of \(\bar{F}_q\) such that \(m \mid (q^r - 1)\). For \(\alpha', \beta' \in \bar{F}_q\) and \(v^m(q-1) = 1\) with \(v \in \bar{F}_q\), let

\[
\varphi_{\alpha', \beta', v}(x', s', z') = (v' x', -v'^{-m} s' + \alpha', -v'^m z' + \beta').
\]
Lemma 6.2. The genus and $p$-rank of $K_{\tilde{\Delta}}$ are

$$g(K_{\tilde{\Delta}}) = \left(\frac{q}{\bar{q}} - m - 1\right)\left(\frac{q}{\bar{q}} - 1\right), \quad \text{and} \quad \gamma(K_{\tilde{\Delta}}) = \left(\frac{q}{\bar{q}} - 1\right)^2.$$ 

Proof. From Lemma 4.14 $K_{\Delta}$ is rational and the different in the Hurwitz genus formula applied to $\Delta$ is

$$\sum_{p \in P} \sum_{i=0}^{m} (|\Delta_p^{(i)}| - 1) = 2g(K) - 2 + q^2 = 2q(m+1)(q-1),$$

where $P$ is the set of all places of $K$. On the other hand, $\Delta_P$ is nontrivial if and only if $P \in \Omega_1 \cup \Omega_2$. From Lemma 4.10 $W \times \Delta_P$ fixes $P$, and hence for any $P \in \Omega_1 \cup \Omega_2$, $q = \Delta_P^{(0)} = \Delta_P^{(1)} = \cdots = \Delta_P^{(m)}$; see [10] Lemma 11.75 (i). Also $|\Omega_1| + |\Omega_2| = 2q$ and $|\Delta_P| = q$. Therefore, $\Delta_P^{(i)}$ is trivial for every $i > m$. By the properties of the subgroups $\Delta_1$ and $\Delta_2$, this yields for any point $P \in \Omega_1 \cup \Omega_2$ that $\bar{q} = \tilde{\Delta}_P^{(0)} = \tilde{\Delta}_P^{(1)} = \cdots = \tilde{\Delta}_P^{(m)}$ but $\tilde{\Delta}_P^{(i)}$ is trivial for $i > m$. Therefore, the different in the Hurwitz genus formula applied to $\tilde{\Delta}$ is

$$\sum_{p \in P} \sum_{i=0}^{m} (|	ilde{\Delta}_P^{(i)}| - 1) = 2g(K) - 2 + 2q^2 = 2q(m+1)(\bar{q} - 1),$$

Thus,

$$2(qm - 1)(q - 1) = \bar{q}^2(2g(K_{\tilde{\Delta}}) - 2) + 2q(m+1)(\bar{q} - 1),$$

whence the first claim follows. Moreover, from the Deuring-Shafarevic formula applied to $\tilde{\Delta}$,

$$(q - 1)^2 - 1 = \bar{q}^2(\gamma(K_{\tilde{\Delta}}) - 1) + \frac{2q}{\bar{q}}(\bar{q}^2 - \bar{q}),$$

whence the second claim follows. \qed
Proposition 6.3. Let $q = q^k$ with $k \geq 1$. Then $K^\Delta = \mathbb{K}(x', t, w)$ with
\[
\begin{align*}
    w + w^q + \ldots + w^{q^{k-1}} &= x'^{-m}, \\
    t + t^q + \ldots + t^{q^{k-1}} &= x'^m.
\end{align*}
\]
Furthermore, $\text{Aut}_E(K^\Delta)$ has a subgroup $\tilde{G}$ of order $2(q/\bar{q})^2 m(\bar{q}-1)$ with $\tilde{G} = (\Delta/\bar{\Delta}) \rtimes (C_m(q-1) \rtimes \langle \xi \rangle)$.

Proof. First we show that $K^\Delta = \mathbb{K}(x', t, w)$ with $t = s^q - s'$, and $w = z^q - z'$. By direct computation, both $t$ and $x'$ are fixed by $\Delta$. Hence $\mathbb{K}(x', t, w) \subseteq K^\Delta$. Also $[K : K^\Delta] = q^2$. On the other hand, both extensions $K|\mathbb{K}(x', s, w)$ and $\mathbb{K}(x', s, w)|\mathbb{K}(x', t, w)$ are (Artin-Schreier extensions) of degree $\bar{q}$,
\[
[K : \mathbb{K}(x', t, w)] = [K : \mathbb{K}(x', s, w)] \cdot [\mathbb{K}(x', s, w) : \mathbb{K}(x', t, w)] = \bar{q} \cdot \bar{q} = q^2.
\]
Therefore $K^\Delta = \mathbb{K}(x', t, w)$. Since $z^q - z' = z^q - z^q^{k-1} + z^{q^2-1} - \ldots + z^{q^k-1} - z^q - z' = \sum_{i=0}^{k-1} w^{q^i}$, and this remains true when $z'$ and $w$ are replaced by $s'$ and $t$, the first claim follows. The second claim can be deduced from $\text{Aut}_E(K)$ taking for $\tilde{G}$ the normalizer of $\Delta$. Alternatively, a direct computation shows that the following maps are elements of $\text{Aut}_E(K^\Delta)$:
\[
\varphi_{\alpha, \beta, v}(x', t, w) = (vx', v^{-m}t + \alpha', v^m w + \beta) \quad \text{with} \quad T_{\bar{q}^r|\bar{q}^s}(\alpha) = T_{\bar{q}^r|\bar{q}^s}(\beta) = 0, \quad \text{and} \quad v^m(\bar{q}-1) = 1, \quad \text{and} \quad \xi(x', t, w) = (x'^{-1}, w, t). \quad \text{These generate a group} \quad \tilde{G} \quad \text{with the properties in the second claim.}
\]

Corollary 6.4. If $q = q^2$ then $K^\Delta$ is isomorphic to $F$ with parameters $(\bar{q}, m)$.

From Lemma 6.2 for every $q = q^k$ with $k \geq 1$, $K^\Delta$ has the same genus and $p$-rank of the function field $F$ with parameters $(q/\bar{q}, m)$. Moreover, from Proposition 6.3 $K^\Delta = \mathbb{K}(x', t, w)$ with
\[
\begin{align*}
    (w + w^q + \ldots + w^{q^{k-1}})(t + t^q + \ldots + t^{q^{k-1}}) &= 1, \\
    t + t^q + \ldots + t^{q^{k-1}} &= x'^m,
\end{align*}
\]
and $\text{Aut}_E(K^\Delta)$ has a subgroup $\tilde{G}$ of order $2(q/\bar{q})^2 m(\bar{q}-1)$ with
\[
\tilde{G} = (\Delta/\bar{\Delta}) \rtimes (C_m(q-1) \rtimes \langle \xi \rangle) = (\Delta/\bar{\Delta}) \rtimes (C_m(q-1) \rtimes \langle \xi \rangle)
\]
where the subgroup $\tilde{W} = \Delta/\bar{\Delta} \rtimes C_m(q-1)$ consists of all maps $\varphi_{\alpha, \beta, v}(x', t, w) = (vx', v^{-m}t + \alpha, v^m w + \beta)$ with $T_{\bar{q}^r|\bar{q}^s}(\alpha) = T_{\bar{q}^r|\bar{q}^s}(\beta) = 0$, $v^m(\bar{q}-1) = 1$, whereas $\xi(x', t, w) = (x'^{-1}, w, t)$. In particular, the subgroup $C_m$ consisting of all maps $\varphi_{0,0,v}$ with $v^m = 1$ is the center $Z(\tilde{W})$ of $\tilde{W}$, and $C_m$ is a normal subgroup of $\tilde{G}$.

By Corollary 6.4, if $q = q^2$ then $K^\Delta$ and $F$ with parameter $(q/\bar{q}, m)$ are isomorphic. Our aim is to prove that the converse also holds.

For this purpose, it is useful to view $\mathbb{K}(x', t, w)$ as a degree $m$ Kummer extension of the function field $L = \mathbb{K}(t, w)$ where $(w + w^q + \ldots + w^{q^{k-1}})(t + t^q + \ldots + t^{q^{k-1}}) = 1$. Since $L$ is the fixed field of $C_m$, and $C_m$ is a normal subgroup of $G$, the factor group $G/C_m$ is a subgroup of $\text{Aut}(L)$. By direct computation, $G/C_m$ contains the subgroup $\Delta^*$ consisting all maps $\varphi_{\alpha, \beta}(t, w) = (t + \alpha, w + \beta)$ with $T_{\bar{q}^r|\bar{q}^s}(\alpha) = T_{\bar{q}^r|\bar{q}^s}(\beta) = 0$ as well as the involution $\xi^*(t, w) = (w, t)$, and the subgroup $\bar{G}_{\bar{q}-1} = \{\eta^*(t, w) = (\lambda^m t, \lambda^{-1} w)|\lambda^{\bar{q}-1} = 1\}$. Therefore, $\tilde{G}/C_m \cong (\Delta^* \rtimes C_{\bar{q}-1}) \rtimes (\xi^*)$. Furthermore, $\Delta^*$ has two short orbits $\Omega_1^* \text{ and } \Omega_2^*$, the former consisting of all places centered at the infinite point $W_{\infty}$ of the curve $(W + W^q + \ldots + W^{q^{k-1}})(T + T^q + \ldots + T^{q^{k-1}}) = 1$, the latter one of those centered at the other infinite point $T_{\infty}$. Both points at infinity are ordinary singular
points with multiplicity \( q/\bar{q} \). Now look at \( \mathbb{K}(t, w)/\mathbb{K}(t) \) as a generalized Artin-Schreier extension of degree \( q/\bar{q} \). Then the (unique) zero of \( t \) is totally ramified while each pole of \( t \) is totally unramified. More precisely, \( \text{div}(t)_0 = (q/\bar{q})P \), while \( \text{div}(t)_\infty = \sum_{i=1}^{q/\bar{q}} T_i \) with \( \Omega_1 = \{ T_1, \ldots, T_{q/\bar{q}} \} \) where \( P \) is the place corresponding to the unique branch centered at \( W_\infty \) whose tangent has equation \( T = 0 \). By a direct computation, \( C_{\bar{q}-1} \) fixes \( P \) and acts transitively on the remaining \( q/\bar{q} - 1 \) places in \( \Omega_1 \). Analogous results hold for \( w \) and \( \Omega_2 \). Hence \( C_{\bar{q}-1} \) fixes a unique point in \( \Omega_2 \) and acts transitively on the remaining \( q/\bar{q} - 1 \) places in \( \Omega_2 \).

**Lemma 6.5.** Let \( C \leq \text{Aut}_L(\mathbb{K}) \) be a cyclic group containing \( C_{\bar{q}-1} \). If \( C \) is in the normalizer \( N_{\text{Aut}_L(\mathbb{K})}(\Delta^*) \) and leaves both short orbits of \( \Delta \) invariant, then \( C = C_{\bar{q}-1} \).

**Proof.** Let \( C = \langle c \rangle \). Then \( c \) preserves both \( \Omega_1^* \). Since \( c \) commutes with \( C_{\bar{q}-1} \), it fixes \( P \). Thus \( t \) and the image \( c(t) \) of \( t \) by \( c \) have the same poles and the same zero. Therefore, \( c(t) = \rho t \) with some \( \rho \in \mathbb{K}^* \). Analogously, \( c(w) = \sigma w \) with some \( \sigma \in \mathbb{K}^* \). By a straightforward computation, this yields \( \rho = \sigma \) and \( \rho^{\bar{q}-1} = 1 \). Hence \( c \) has order at most \( \bar{q} - 1 \) and the claim holds. \( \square \)

**Corollary 6.6.** Let \( q = \bar{q}^k \). Then \( k \leq 2 \) is the necessary and sufficient condition for \( K^{\Delta} \) to be isomorphic to \( F \) with parameter \( (q/\bar{q}, m) \).

**Proof.** By Corollary 6.4 we only have to prove the necessary condition. By absurd, \( K^{\Delta} \) and \( F \) with parameter \( (q/\bar{q}, m) \) have isomorphic \( K \)-automorphism groups. From Theorem 5.1, \( \text{Aut}_K(K^{\Delta}) \) has a cyclic group of order \( q/\bar{q} - 1 \) contained in the normalizer of \( \Delta \). From the discussion after Corollary 6.4, this yields the existence of a cyclic group \( C \) of the same order \( q/\bar{q} - 1 \) satisfying the hypotheses in Lemma 6.5. Therefore, \( q/\bar{q} - 1 \leq \bar{q} - 1 \) whence \( k \leq 2 \). \( \square \)

**Remark 6.7.** From Corollary 6.4, a tower \( \mathbb{K}(x) \subset F_1 \subset \cdots \subset F_i \subset \cdots \) arises where \( q = p^{2^i} \) and \( F_i \) is a function field isomorphic to \( \mathbb{K}(x, y, z) \) defined by \( y^q + y = x^m + x^{-m} \) and \( z^q + z = x^m \). By Theorem 5, \[
\lim_{i \to \infty} \frac{|\text{Aut}_L(F_i)|}{g(F_i)^{3/2}} = \frac{2}{\sqrt{m}}.
\]

**References**

[1] J.L. Alperin, R. Brauer and D. Gorenstein, Finite simple groups of 2-rank two, *Scripta Math.* **29** (1973), 191-214.

[2] J.L. Alperin, R. Brauer and D. Gorenstein, Finite groups with quasi-dihedral and wreathed Sylow 2-subgroups, *Trans. Amer. Math. Soc.* **151** (1970), 1-261.

[3] M. Giulietti and G. Korchmáros, Large 2-groups of automorphisms of algebraic curves over a field of characteristic 2, *J. Algebra* **427** (2015), 264-294.

[4] M. Giulietti and G. Korchmáros, Automorphism groups of algebraic curves with p-rank zero, *J. Lond. Math. Soc.* **81** (2010), 277-296.

[5] M. Giulietti and G. Korchmáros, Algebraic curves with a large non-tame automorphism group fixing no point, *Trans. Amer. Math. Soc.* **362** (2010), 5983-6001.

[6] D. Gorenstein and J.H. Walter, The characterization of finite groups with dihedral Sylow 2-subgroups. I. *J. Algebra* **2** (1965), 85-151.
[7] D. Gorenstein and J.H. Walter, The characterization of finite groups with dihedral Sylow 2-subgroups. II. *J. Algebra* 2 (1965), 218-270.

[8] R. Guralnick, B. Malmskog and R. Pries, The automorphism groups of a family of maximal curves, *J. Algebra* 361 (2012), 92-106.

[9] H.-W. Henn, Funktionenkörper mit grosser Automorphismengruppe, *J. Reine Angew. Math.* 302 (1978), 96–115.

[10] J.W.P. Hirschfeld, G. Korchmáros and F. Torres, *Algebraic Curves over a Finite Field*, Princeton Series in Applied Mathematics, Princeton, (2008).

[11] B. Huppert, *Endliche Gruppen. I*, Grundlehren der Mathematischen wissenschaften 134, Springer, Berlin, 1967, xii+793 pp.

[12] G. Korchmáros and M. Montanucci, Ordinary algebraic curves with many automorphisms in positive characteristic, arXiv:1610.05252, 2016.

[13] G. Korchmáros and M. Montanucci, The Geometry of the Artin-Schreier-Mumford Curves over an Algebraically Closed Field, arXiv: 1612.05912, 2016.

[14] S. Nakajima, p-ranks and automorphism groups of algebraic curves, *Trans. Amer. Math. Soc.* 303 (1987), 595-607.

[15] H. Stichtenoth, Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. II. Ein spezieller Typ von Funktionenkörpern, *Arch. Math.* 24 (1973), 615–631.

[16] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, Berlin, 1993, x+260 pp.

[17] H. Stichtenoth, Private communications, 2016.

[18] F. Sullivan, p-torsion in the class group of curves with many automorphisms, *Arch. Math.* 26 (1975), 253–261.

[19] R.C. Valentini and M.L. Madan, A Hauptsatz of L.E. Dickson and Artin–Schreier extensions, *J. Reine Angew. Math.* 318 (1980), 156–177.

[20] J.H. Walter, The characterization of finite groups with abelian Sylow 2-subgroups, *Ann. of Math.* 89 (1969), 405-514.