Journal of Algebra 485 (2017) 310–331

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Generalized Artin–Mumford curves over finite fields

Maria Montanucci [a], Giovanni Zini [b,*]

[a] *Dipartimento di Matematica, Informatica ed Economia, Università degli Studi della Basilicata, Contrada Macchia Romana, 85100 Potenza, Italy*

[b] *Dipartimento di Matematica e Informatica, Università degli Studi di Firenze, Viale Morgagni, 50134 Firenze, Italy*

A R T I C L E I N F O

Article history:
Received 30 December 2016
Available online 24 May 2017
Communicated by Michel Broué

Keywords:
Algebraic curves
Algebraic function fields
Finite fields
Automorphism groups

A B S T R A C T

Let $\mathbb{F}_q$ be the finite field of order $q = p^h$ with $p > 2$ prime and $h > 1$, and let $\mathbb{F}_{\bar{q}}$ be a subfield of $\mathbb{F}_q$. From any two $\bar{q}$-linearized polynomials $L_1, L_2 \in \overline{\mathbb{F}}_q[T]$ of degree q, we construct an ordinary curve $\mathcal{X}_{(L_1,L_2)}$ of genus $\mathfrak{g} = (q-1)^2$ which is a generalized Artin–Schreier cover of the projective line $\mathbb{P}^1$. The automorphism group of $\mathcal{X}_{(L_1,L_2)}$ over the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$ contains a semidirect product $\Sigma \rtimes \Gamma$ of an elementary abelian p-group Σ of order q^2 by a cyclic group Γ of order $\bar{q}-1$. We show that for $L_1 \neq L_2$, $\Sigma \rtimes \Gamma$ is the full automorphism group $\mathrm{Aut}(\mathcal{X}_{(L_1,L_2)})$ over $\overline{\mathbb{F}}_q$; for $L_1 = L_2$ there exists an extra involution and $\mathrm{Aut}(\mathcal{X}_{(L_1,L_1)}) = \Sigma \rtimes \Delta$ with a dihedral group Δ of order $2(\bar{q}-1)$ containing Γ. Two different choices of the pair $\{L_1, L_2\}$ may produce birationally isomorphic curves, even for $L_1 = L_2$. We prove that any curve of genus $(q-1)^2$ whose $\overline{\mathbb{F}}_q$-automorphism group contains an elementary abelian subgroup of order q^2 is birationally equivalent to $\mathcal{X}_{(L_1,L_2)}$ for some separable $\bar{q}$-linearized polynomials L_1, L_2 of degree q. We produce an analogous characterization in the special case $L_1 = L_2$. This extends a result on the Artin–Mumford curves, due to Arakelian and Korchmáros [1].

* Corresponding author.
E-mail addresses: maria.montanucci@unibas.it (M. Montanucci), gzini@math.unifi.it (G. Zini).

http://dx.doi.org/10.1016/j.jalgebra.2017.05.020
0021-8693/

1. Introduction

The Artin–Mumford curve $\mathcal{M}_c$ of genus $(p-1)^2$ defined over a field $\mathbb{F}$ of odd characteristic p is the nonsingular model of the plane curve with affine equation

$$(X^p - X)(Y^p - Y) = c, \quad c \in \mathbb{F}^*. \tag{1}$$

Artin–Mumford curves, especially over non-Archimedean valued fields of positive characteristic, have been investigated in several papers; see [3,2], and [4]. By a result of Cornelissen, Kato and Kontogeorgis [2] valid over any non-Archimedean valued field $(\mathbb{F}, |\cdot|)$ of positive characteristic, if $|c| < 1$ then $\mathrm{Aut}_{\mathbb{F}}(\mathcal{M}_c)$ is the semidirect product

$$(C_p \times C_p) \rtimes D_{p-1}, \tag{2}$$

where C_p is a cyclic group of order p and D_{p-1} is a dihedral group of order $2(p-1)$. This result holds over any algebraically closed field; see [11].

The interesting question whether the genus $(p-1)^2$ together with an automorphism group as in (2) characterize the Artin–Mumford curve has been solved so far only for curves defined over $\mathbb{F}_p$; see [1].

A natural generalization of Artin–Mumford curves arises when the polynomials $X^p - X$ and $Y^p - Y$ in (1) are replaced by separable linearized polynomials L_1, L_2 of equal degree. Our aim is to investigate such generalized Artin–Mumford curves, especially their automorphism groups. To present our results, we need some notation that will also be used throughout the paper.

For an odd prime p and powers $\bar{q} = p^n$ and $q = \bar{q}^m$, $\mathbb{F}_p$, $\mathbb{F}_{\bar{q}}$, $\mathbb{F}_q$ are the finite fields of order p, $\bar{q}$, q; $\mathbb{K}$ is the algebraic closure of $\mathbb{F}_p$; $L_1(T), L_2(T) \in \mathbb{K}[T]$ are separable polynomials of degree q which are $\bar{q}$-linearized. We admit that one, but not both, is $\bar{q}^k$-linearized, for some $k \geq 2$. With this notation, the *generalized Artin–Mumford curve* $\mathcal{X}_{(L_1,L_2)}$ is the nonsingular model of the plane curve with affine equation

$$\mathcal{X}_{(L_1,L_2)}: \quad L_1(X) \cdot L_2(Y) = 1. \tag{3}$$

The family of generalized Artin–Mumford curves is denoted by:

$$\mathcal{S}_{q|\bar{q}} = \big\{ \mathcal{X}_{(L_1,L_2)} \mid L_1(T), L_2(T) \in \mathbb{K}[T],\ \deg(L_1) = \deg(L_2) = q,\ L_1, L_2 \text{ are separable, } \bar{q}\text{-linearized, not both } \bar{q}^k\text{-linearized for any } k \geq 2 \big\}.$$

An interesting feature of a generalized Artin–Mumford curve $\mathcal{X}_{(L_1,L_2)}$ is that its genus only depends on q, namely $\mathfrak{g}(\mathcal{X}_{(L_1,L_2)}) = (q-1)^2$. Also, $\mathcal{X}_{(L_1,L_2)}$ is an ordinary curve, that is, its genus and p-rank are equal. A complete description of the automorphism group of any generalized Artin–Mumford curve is given in the following two theorems.

Theorem 1.1. *The full automorphism group of $\mathcal{X}_{(L,L)}$ is the semidirect product*

$$\Sigma \rtimes \Delta, \tag{4}$$

where

- $\Sigma = \{\tau_{\alpha,\beta} : (X,Y) \mapsto (X+\alpha, Y+\beta) \mid L(\alpha) = L(\beta) = 0\}$ *is an elementary abelian p-group of order q^2;*
- $\Delta = \langle \theta, \xi \rangle$ *is a dihedral group of order $2(\bar{q}-1)$, where $\theta : (X,Y) \mapsto (\lambda X, \lambda^{-1}Y)$ with λ a primitive $(\bar{q}-1)$-th root of unity, and $\xi : (X,Y) \mapsto (Y,X)$.*

Theorem 1.2. *If $L_1 \neq L_2$, the full automorphism group of $\mathcal{X}_{(L_1,L_2)}$ is the semidirect product*

$$\Sigma \rtimes \Gamma, \tag{5}$$

where

- $\Sigma = \{\tau_{\alpha,\beta} : (X,Y) \mapsto (X+\alpha, Y+\beta) \mid L_1(\alpha) = L_2(\beta) = 0\}$ *is an elementary abelian p-group of order q^2;*
- $\Gamma = \langle \theta \rangle$ *is a cyclic group of order $\bar{q}-1$, where $\theta : (X,Y) \mapsto (\lambda X, \lambda^{-1}Y)$ with λ a primitive $(\bar{q}-1)$-th root of unity.*

For $\bar{q} = q$, the size of $\mathrm{Aut}(\mathcal{X}_{(L_1,L_2)})$ is approximately $2(\mathfrak{g}(\mathcal{X}_{(L_1,L_2)})+1)^{3/2}$. Since the groups given in Theorems 1.1 and 1.2 are solvable, $\mathcal{X}_{(L_1,L_2)}$ attains, up to the constant, the bound given in [8].

Our main result is that $\mathrm{Aut}(\mathcal{X}_{(L_1,L_2)})$ together with $\mathfrak{g}(\mathcal{X}_{(L_1,L_2)})$ characterize the curves in $\mathcal{S}_{q|\bar{q}}$. This result can be viewed as a generalization of [1, Theorem 1.1] on Artin–Mumford curves.

Theorem 1.3. *Let $\mathcal{X}$ be a (projective, non-singular, geometrically irreducible, algebraic) curve of genus $\mathfrak{g} = (q-1)^2$ defined over $\mathbb{K}$. If $\mathrm{Aut}(\mathcal{X})$ contains an elementary abelian subgroup E_{q^2} of order q^2, then $\mathcal{X}$ is birationally equivalent over $\mathbb{K}$ to some $\mathcal{X}_{(L_1,L_2)} \in \mathcal{S}_{q|\bar{q}}$, where $\bar{q}$ is the largest power of p such that $\mathrm{Aut}(\mathcal{X})$ contains a cyclic subgroup $C_{\bar{q}-1}$ of order $\bar{q}-1$.*

In the case $L_1 = L_2$, the assumption on the genus can be weakened under a stronger assumption on the automorphism group, as follows.

Theorem 1.4. *Let $\mathcal{X}$ be a curve of genus $\mathfrak{g} \leq (q-1)^2$ defined over $\mathbb{K}$. If $\mathrm{Aut}(\mathcal{X})$ contains a semidirect product $E_{q^2} \rtimes (C_2 \times C_2)$ (where E_{q^2} is elementary abelian of order q^2 and $C_2 \times C_2$ is a Klein four-group), then $\mathcal{X}$ is birationally equivalent over $\mathbb{K}$ to some $\mathcal{X}_{(L,L)} \in$*

$\mathcal{S}_{q|\bar{q}}$, where $\bar{q}$ is the largest power of p such that $\mathrm{Aut}(\mathcal{X})$ *contains a cyclic subgroup $C_{\bar{q}-1}$ of order $\bar{q}-1$.*

In Section 2, preliminary results on automorphism groups of ordinary curves and curves of even genus are collected. In Section 3, we give the proofs of Theorems 1.1 and 1.2, doing so we also show the relevant properties of generalized Artin–Mumford curves; see Lemma 3.1. The proof of Theorems 1.3 and 1.4 is given in Section 4 where additional classification results of independent interest are found, as well. Here we only mention that Theorem 4.2 gives the following characterization.

Theorem 1.5. *Let $\mathcal{Y}$ be a curve of genus $q-1$ defined over $\mathbb{K}$ whose automorphism group* $\mathrm{Aut}(\mathcal{Y})$ *contains an elementary abelian subgroup E_q of order q. Then one of the following holds.*

(I) *$\mathcal{Y}$ is birationally equivalent over $\mathbb{K}$ to the curve $\mathcal{Y}_{L,a}$ with affine equation*

$$L(y) = ax + \frac{1}{x},$$

for some $a \in \mathbb{K}^*$ and $L(T) \in \mathbb{K}[T]$ a separable p-linearized polynomial of degree q. For the curve $\mathcal{Y}_{L,a}$ the following properties hold:

- (i) *$\mathcal{Y}_{L,a}$ is ordinary and hyperelliptic;*
- (ii) *$\mathcal{Y}_{L,a}$ has exactly $2q$ Weierstrass places, which are the fixed places of the hyperelliptic involution μ.*
- (iii) *The full automorphism group* $\mathrm{Aut}(\mathcal{Y}_L)$ *of $\mathcal{Y}_{L,a}$ has order $4q$ and is a direct product $Dih(E_q) \times \langle \mu \rangle$.*

(II) *$p \neq 3$ and $\mathcal{Y}$ is birationally equivalent over $\mathbb{K}$ to the curve $\mathcal{Z}_{\tilde{L},b}$ with affine equation*

$$\tilde{L}(y) = x^3 + bx,$$

for some $a \in \mathbb{K}$ and $\tilde{L}(T) \in \mathbb{K}[T]$ a separable p-linearized polynomial of degree q. For the curve $\mathcal{Z}_{\tilde{L},b}$ the following properties hold:

- (i) *$\mathcal{Z}_{\tilde{L},b}$ has zero p-rank;*
- (ii) $\mathrm{Aut}(\mathcal{Z}_{\tilde{L},b})$ *contains a generalized dihedral subgroup $Dih(E_q) = E_q \rtimes \langle \nu \rangle$.*

Theorem 1.5 provides a generalization of [12, Proposition (2.2) and Corollary (2.3)].

Our proof uses function field theory, especially the Hurwitz genus formula and the Deuring–Shafarevich formula, together with deeper results on finite groups, especially the classification theorem on finite non-abelian simple groups whose Sylow 2-subgroups are dihedral or semidihedral. In doing so we adopt the approach worked out by Giulietti and Korchmáros in [5].

2. Background and preliminary results

We keep the notation used in Introduction. Also, $\mathcal{X}$ is a (projective, non-singular, geometrically irreducible, algebraic) curve of genus $\mathfrak{g} \geq 2$ defined over $\mathbb{K}$, $\mathbb{K}(\mathcal{X})$ is the function field of $\mathcal{X}$, and $\mathrm{Aut}(\mathcal{X})$ is its full automorphism group over $\mathbb{K}$.

For a subgroup G of $\mathrm{Aut}(\mathcal{X})$, let $\bar{\mathcal{X}}$ denote a non-singular model of $\mathbb{K}(\mathcal{X})^G$, that is, a curve with function field $\mathbb{K}(\mathcal{X})^G$, where $\mathbb{K}(\mathcal{X})^G$ consists of all elements of $\mathbb{K}(\mathcal{X})$ fixed by every element in G. Usually, $\bar{\mathcal{X}}$ is called the quotient curve of $\mathcal{X}$ by G and denoted by $\mathcal{X}/G$. The field extension $\mathbb{K}(\mathcal{X})|\mathbb{K}(\mathcal{X})^G$ is Galois of degree $|G|$.

Let Φ be the cover of $\mathcal{X}|\bar{\mathcal{X}}$ where $\bar{\mathcal{X}} = \mathcal{X}/G$. A place P of $\mathbb{K}(\mathcal{X})$ is a ramification place of G if the stabilizer G_P of P in G is nontrivial; the ramification index e_P is $|G_P|$. The G-orbit of P in $\mathbb{K}(\mathcal{X})$ is the subset $o = \{R \mid R = g(P), g \in G\}$ of the set of the places of $\mathbb{K}(\mathcal{X})$, and it is *long* if $|o| = |G|$, otherwise o is *short*. For a place $\bar{Q}$, the G-orbit o lying over $\bar{Q}$ consists of all places P of $\mathbb{K}(\mathcal{X})$ such that $\Phi(P) = \bar{Q}$. If $P \in o$ then $|o| = |G|/|G_P|$ and hence P is a ramification place if and only if o is a short G-orbit. If every non-trivial element in G is fixed–point-free on the set of the places of $\mathbb{K}(\mathcal{X})$, the cover Φ is unramified. For a non-negative integer i, the i-th ramification group of $\mathcal{X}$ at P is denoted by $G_P^{(i)}$ and defined to be

$$G_P^{(i)} = \{\alpha \in G_P \mid v_P(\alpha(t) - t) \geq i + 1\},$$

where t is a local parameter at P; see [10]. Here $G_P^{(0)} = G_P$.

Let $\bar{\mathfrak{g}}$ be the genus of the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/G$. The Hurwitz genus formula [6, Theorem 7.27] gives the following equation

$$2\mathfrak{g} - 2 = |G|(2\bar{\mathfrak{g}} - 2) + \sum_{P \in \mathcal{X}} d_P, \tag{6}$$

where the different d_P at P is given by

$$d_P = \sum_{i \geq 0} (|G_P^{(i)}| - 1), \tag{7}$$

see [6, Theorem 11.70]. Let γ and $\bar{\gamma}$ be the p-ranks of $\mathcal{X}$ and $\bar{\mathcal{X}}$ respectively. The Deuring–Shafarevich formula [6, Theorem 11.62] states that

$$\gamma - 1 = |G|(\bar{\gamma} - 1) + \sum_{i=1}^{k} (|G| - \ell_i) \tag{8}$$

where $\ell_1, \ldots, \ell_k$ are the sizes of the short orbits of G.

A subgroup G of $\mathrm{Aut}(\mathcal{X})$ is *tame* if $\gcd(p, |G|) = 1$, otherwise G is *non-tame*. The stabilizer G_P of a place $P \in \mathcal{X}$ in G is a semidirect product $G_P = Q_P \rtimes U$ where the normal subgroup Q_P is a p-group while the complement U is a tame cyclic group; see [6, Theorem 11.49].

The following result is due to Nakajima; see [9, Theorems 1, 2 and 3] and [6, Lemma 11.75].

Theorem 2.1. *Let $\mathcal{X}$ be a curve with $\mathfrak{g}(\mathcal{X}) \geq 2$ defined over an algebraically closed field of characteristic $p \geq 3$, and H be a Sylow p-subgroup of* $\mathrm{Aut}(\mathcal{X})$*. Then the following hold.*

(I) *When $\gamma(\mathcal{X}) \geq 2$, we have*

$$|H| \leq \frac{p}{p-2}(\gamma(\mathcal{X})-1) \leq \frac{p}{p-2}(\mathfrak{g}(\mathcal{X})-1).$$

(II) *If $\mathcal{X}$ is ordinary (i.e. $\mathfrak{g}(\mathcal{X}) = \gamma(\mathcal{X})$) and $G \leq \mathrm{Aut}(\mathcal{X})$, then $G_P^{(2)} = \{1\}$ and $G_P^{(1)}$ is elementary abelian, for every $P \in \mathcal{X}$.*

(III) *If $\mathcal{X}$ is ordinary then $|\mathrm{Aut}(\mathcal{X})| \leq 84(\mathfrak{g}(\mathcal{X})-1)\mathfrak{g}(\mathcal{X})$.*

(IV) *If $\gamma(\mathcal{X}) = 1$ then H is cyclic.*

The following results are due to Giulietti and Korchmáros; see [5].

Lemma 2.2. ([5, Lemma 4.1]) *Let H be a solvable automorphism group of an algebraic curve $\mathcal{X}$ of genus $\mathfrak{g}(\mathcal{X}) \geq 2$ containing a normal d-subgroup Q of odd order such that $|Q|$ and $[H : Q]$ are coprime. Suppose that a complement U of Q in H is abelian, and that $N_H(U) \cap Q = \{1\}$. If*

$$|H| \geq 30(\mathfrak{g}(\mathcal{X})-1), \tag{9}$$

then $d = p$ and U is cyclic.

The *odd core* $O(G)$ of a group G is its maximal normal subgroup of odd order. If $O(G)$ is trivial, then G is an *odd core-free* group.

Lemma 2.3. ([5, Lemma 6.11]) *Let $\mathcal{X}$ be a curve of even genus, and G be an odd core-free automorphism group of $\mathcal{X}$ with a non-abelian simple minimal normal subgroup M. Up to isomorphism, one of the following cases occurs for some prime d and odd k:*

(i) *$M = PSL(2, d^k) \leq G \leq P\Gamma L(2, d^k)$ with $d^k \geq 5$;*

(ii) *$M = PSL(3, d^k) \leq G \leq P\Gamma L(3, d^k)$ with $d^k \equiv 3 \pmod 4$;*

(iii) *$M = PSU(3, d^k) \leq G \leq P\Gamma U(3, d^k)$ with $d^k \equiv 1 \pmod 4$;*

(iv) *$M = G = A_7$, the alternating group on 7 letters;*

(v) *$M = G = M_{11}$, the Mathieu group on 11 letters.*

Lemma 2.4. ([5, Lemma 6.3]) *If $\mathcal{X}$ is a curve of even genus then* $\mathrm{Aut}(\mathcal{X})$ *has no elementary abelian 2-subgroup of order 8.*

Lemma 2.5. ([5, Lemma 6.4]) *Let $\mathcal{X}$ be a curve of even genus and $G \le \mathrm{Aut}(\mathcal{X})$. If G has a minimal normal subgroup of order 2 then $G = O(G) \rtimes S_2$, where S_2 is Sylow 2-subgroup of G, unless S_2 is a generalized quaternion group.*

For a positive integer d, C_d stands for a cyclic group of order d, D_d for a dihedral group of order $2d$, E_d for an elementary abelian group of order d, and $Dih(E_d)$ for a generalized dihedral group $E_d \rtimes C_2$ of order $2d$.

3. The automorphism group of $\mathcal{X}_{(L_1,L_2)}$

Lemma 3.1. *For the curve $\mathcal{X}_{(L_1,L_2)}$ as in (3), $X_\infty = (1:0:0)$ and $Y_\infty = (0:1:0)$, the following properties hold:*

i) *X_∞ and Y_∞ are q-fold ordinary points;*
ii) *$\mathcal{X}_{(L_1,L_2)}$ is ordinary with $\mathfrak{g}(\mathcal{X}_{(L_1,L_2)}) = \gamma(\mathcal{X}_{(L_1,L_2)}) = (q-1)^2$;*
iii) *If $L_1 \neq L_2$, $\mathrm{Aut}(\mathcal{X}_{(L_1,L_2)})$ contains the subgroup $\Sigma \rtimes \Gamma$ defined in (5);*
iv) *If $L_1 = L_2 = L$, $\mathrm{Aut}(\mathcal{X}_{(L,L)})$ contains the subgroup $\Sigma \rtimes \Delta$ defined in (4);*
v) *In both cases* iii) *and* iv)*, the group Σ is a Sylow p-subgroup of $\mathrm{Aut}(\mathcal{X}_{(L_1,L_2)})$.*
vi) *The quotient curves $\mathcal{X}_{(L_1,L_2)}/\Sigma_x$ and $\mathcal{X}_{(L_1,L_2)}/\Sigma_y$ are rational curves, where $\Sigma_x = \{\tau_{\alpha,\beta} \in \Sigma \mid \beta = 0\}$ and $\Sigma_y = \{\tau_{\alpha,\beta} \in \Sigma \mid \alpha = 0\}$.*

Proof. Let $\bar{P}_{x=\alpha_i}$, with $L_1(\alpha_i) = 0$, be the q distinct zeros and $\bar{P}_{x=\infty}$ be the unique pole of $L(x)$ in $\mathbb{K}(x)$. Then

$$v_{\bar{P}_{x=\alpha_i}}(1/L_1(x)) = -1, \quad v_{\bar{P}_{x=\infty}}(1/L_1(x)) = q,$$

and $1/L_1(x)$ has valuation zero at any other place of $\mathbb{K}(x)$. Thus, the function field $\mathbb{K}(\mathcal{X}_{(L_1,L_2)}) = \mathbb{K}(x,y)$ with $L_1(x) \cdot L_2(y) = 1$, is a generalized Artin–Schreier extension of $\mathbb{K}(x)$ of degree q; see [10, Proposition 3.7.10]. The places $\bar{P}_{x=\alpha_i}$ are totally ramified while any other place is unramified. The genus of $\mathcal{X}_{(L_1,L_2)}$ is given by

$$\mathfrak{g}(\mathcal{X}_{(L_1,L_2)}) = q \cdot \mathfrak{g}(\mathbb{K}(x)) + \frac{q-1}{2} \cdot (-2+2q) = (q-1)^2.$$

The places $P_{x=\alpha_i}$ lying over $\bar{P}_{x=\alpha_i}$, $i = 1, \ldots, q$, are the poles of y and they are centered at Y_∞. The unique zero of y is place $P_{x=\infty}$ lying over $\bar{P}_{x=\infty}$. Analogously, x has q distinct poles $P_{y=\beta_i}$, with $L_2(\beta_i) = 0$, which are simple and centered at X_∞, and a unique zero $P_{y=\infty}$. Note that $P_{x=\infty} = P_{y=0}$ and $P_{y=\infty} = P_{x=0}$. Let $\Sigma = \{\tau_{\alpha,\beta} : (X,Y) \mapsto (X+\alpha, Y+\beta) \mid L_1(\alpha) = L_2(\beta) = 0\}$. By direct computation Σ is an elementary abelian p-subgroup of $\mathrm{Aut}(\mathcal{X}_{(L_1,L_2)})$ of order q^2. From Theorem 2.1(I), Σ is a Sylow p-subgroup of $\mathrm{Aut}(\mathcal{X}_{(L_1,L_2)})$. Thus the Galois group of $\mathbb{K}(x,y)|\mathbb{K}(x)$ is contained in Σ up to conjugation, and hence $\mathbb{K}(x,y)^\Sigma$ is rational. By direct computation Σ has at least two short orbits of length q, namely

$$\Omega_x = \{P_{y=\beta} \mid L_2(\beta) = 0\}, \quad \Omega_y = \{P_{x=\alpha} \mid L_1(\alpha) = 0\}.$$

From the Deuring–Shafarevich formula (8) applied to the extension $\mathbb{K}(x,y)|\mathbb{K}(x,y)^{\Sigma}$,

$$q^2 - 2q = \mathfrak{g}(\mathcal{X}_{(L_1,L_2)}) - 1 \geq \gamma(\mathcal{X}_{(L_1,L_2)}) - 1 \geq q^2(0-1) + 2(q^2 - q) = q^2 - 2q.$$

Therefore the curve $\mathcal{X}_{(L_1,L_2)}$ is ordinary. By direct checking, if $L_1 \neq L_2$, then Σ and Γ are subgroups of $\mathrm{Aut}(\mathcal{X}_{(L_1,L_2)})$, Γ normalizes Σ, and $\Gamma \cap \Sigma = \{1\}$. Analogously, if $L_1 = L_2$, then Σ and Δ are subgroups of $\mathrm{Aut}(\mathcal{X}_{(L_1,L_2)})$, Δ normalizes Σ, and $\Delta \cap \Sigma = \{1\}$.

In order to prove vi), set $\eta = L_1(x)$. Then $\mathbb{K}(\eta, y) \subseteq \mathbb{K}(\mathcal{X}_{(L_1,L_2)})^{\Sigma_x}$. Since $[\mathbb{K}(\mathcal{X}_{(L_1,L_2)}) : \mathbb{K}(\eta, y)] \leq q$, this implies $\mathbb{K}(\mathcal{X}_{(L_1,L_2)})^{\Sigma_x} = \mathbb{K}(\eta, y)$ and

$$\mathcal{X}_{(L_1,L_2)}/\Sigma_x : \ L_2(y) = \frac{1}{\eta}.$$

This shows that $\mathcal{X}_{(L_1,L_2)}/\Sigma_x$ is rational, and the same holds for $\mathcal{X}_{(L_1,L_2)}/\Sigma_y$. □

The following result follows from the proof of Lemma 3.1.

Corollary 3.2. *The group Σ has exactly two short orbits Ω_x and Ω_y, both of length q. Namely,*

$$\Omega_x = \{P_{y=\beta} \mid L_2(\beta) = 0\}, \quad \Omega_y = \{P_{x=\alpha} \mid L_1(\alpha) = 0\}.$$

Moreover $\mathbb{K}(x,y)^{\Sigma}$ is rational and the principal divisors of the coordinate functions are given by

$$(x) = q\,P_{y=0} - \sum_{P \in \Omega_y} P, \quad (y) = q\,P_{x=0} - \sum_{P \in \Omega_x} P.$$

Lemma 3.3. *Let C be a cyclic subgroup of $\mathrm{Aut}(\mathcal{X}_{(L_1,L_2)})$ containing $\Gamma = \langle\theta\rangle$, where $\theta : (X,Y) \mapsto (\lambda X, \lambda^{-1} Y)$ with λ a primitive $(\bar{q}-1)$-th root of unity. Suppose that C is contained in the normalizer N of Σ in $\mathrm{Aut}(\mathcal{X}_{(L_1,L_2)})$. Then $C = \Gamma$.*

Proof. First of all we observe that $C \cap \Sigma = \{1\}$. In fact by direct checking Γ does not commute with any non-trivial p-element $\tau_{\alpha,\beta} \in \Sigma$. From Lemma 3.1 v), C is tame. Since $C \leq N$, C is isomorphic to an automorphism group $\bar{C}$ of $\mathcal{X}_{(L_1,L_2)}/\Sigma$. Denote by $\bar{\Gamma}$ the subgroup of $PGL(2,\mathbb{K})$ which is isomorphic to Γ. Moreover, from Corollary 3.2, C acts on $\Omega_x \cup \Omega_y$, and $\bar{C} \leq PGL(2,\mathbb{K})$ as $\mathcal{X}_{(L_1,L_2)}/\Sigma$ is rational. From [7, Hauptsatz 8.27] both $\bar{C}$ and $\bar{\Gamma}$ fix exactly two places on $\mathcal{X}_{(L_1,L_2)}/\Sigma$ which are then the two places $\bar{P}_x$ and $\bar{P}_y$ lying under Ω_x and Ω_y respectively. Hence, from Corollary 3.2, C fixes the pole divisors of x and y. From the Orbit stabilizer theorem C fixes at least one place in Ω_x and one place in Ω_y. By direct computation Γ fixes $P_{x=0} \in \Omega_y$ and $P_{y=0} \in \Omega_x$, acting semiregularly on $\Omega_x \setminus \{P_{y=0}\}$ and $\Omega_y \setminus \{P_{x=0}\}$. Thus, C fixes $P_{y=0}$ and $P_{x=0}$ and hence the zero divisors of x and y are preserved by C from Corollary 3.2. This implies that the generator c of C has the form $c: (x, y) \mapsto (\gamma x, \delta y)$, for some $\gamma, \delta \in \mathbb{K}$. By direct computation $\gamma^{\bar{q}-1} = \delta^{\bar{q}-1} = 1$, and so $C = \Gamma$. $\square$

Corollary 3.4. *Let C be a cyclic subgroup of the normalizer N of Σ in $\mathrm{Aut}(\mathcal{X}_{(L_1,L_2)})$ such that $(\bar{q}-1) \mid |C|$ and $|C| \mid (q-1)$. Then $C = \Gamma$.*

3.1. Proof of Theorem 1.1

In this section, $L_1 = L_2 = L$ and we refer to Σ and Δ as defined in Theorem 1.1. For $q = p$ Theorem 1.1 was proved in [1, Theorem 1.1]. Thus, we suppose that $q > p$.

Lemma 3.5. *The normalizer N of Σ in $\mathrm{Aut}(\mathcal{X}_{(L,L)})$ is $N = \Sigma \rtimes \Delta$.*

Proof. From Corollary 3.2, $\bar{N} = N/\Sigma$ is a tame subgroup of $PGL(2, \mathbb{K})$ containing a dihedral group $\bar{\Delta}$ which is isomorphic to $\Delta = \Gamma \rtimes \langle \xi \rangle$, where $\Gamma = \langle \theta \rangle$. Now we show that there are no involutions in $N \setminus (\Sigma \rtimes \Delta)$. Let $\iota \in N$ be an involution and let $\bar{\iota}$ be the induced involution in $PGL(2, \mathbb{K})$. Denote by $\bar{P}_x$ and $\bar{P}_y$ the places lying under Ω_x and Ω_y respectively. From [7, Hauptsatz 8.27] there exists a unique involution in $PGL(2, \mathbb{K})$ fixing $\bar{P}_x$ and $\bar{P}_y$, and it is induced by $\theta^{(\bar{q}-1)/2}$. Thus, if $\iota \notin \Gamma$ then ι switches Ω_x and Ω_y. From Corollary 3.2, ι maps x to $a(y + \alpha)$ and y to $b(x + \beta)$ where $a, b \in \mathbb{K}$ and $L(\alpha) = L(\beta) = 0$. Since the order of ι is equal to 2, we have that $\alpha = \beta = 0$ and $\alpha = \beta \in \{-1, 1\}$. Hence, $\iota = \xi$ or $\iota = \theta^{(\bar{q}-1)/2} \cdot \xi$, and so $\iota \in \Delta$. From [7, Hauptsatz 8.27], one of the following holds:

(1) $\bar{N}$ is isomorphic either to A_4 or S_4 or A_5.
(2) $\bar{N}$ is isomorphic to a dihedral group D_d of order $2d$.

Suppose $\bar{N} \cong A_4$. If $\bar{q} \neq 3$, $\bar{\Delta}$ is not contained in $\bar{N}$. If $\bar{q} = 3$ then $\bar{N}$ is not tame, a contradiction.

Suppose $\bar{N} \cong S_4$. In this case $\bar{q} = 3$, which is impossible as $\bar{N}$ is tame, or $\bar{q} = 5$, which is impossible as $\bar{N}$ contains more than the 5 involutions contained in $\bar{\Delta} \cong D_8$.

Suppose that $\bar{N} \cong A_5$. Then as before $\bar{q} = 3$ which is not possible.

Therefore, case (2) occurs. From Lemma 3.3, $d = \bar{q} - 1$ and the claim follows. $\square$

In order to prove that $\mathrm{Aut}(\mathcal{X}_{(L,L)}) = N$, several cases are distinguished according to the structure of the minimal normal subgroups of $\mathrm{Aut}(\mathcal{X}_{(L,L)})$. Recall that every finite group admits a minimal normal subgroup, which is either elementary abelian or a direct product of isomorphic simple groups.

Lemma 3.6. *If $\mathrm{Aut}(\mathcal{X}_{(L,L)})$ has a minimal normal subgroup E_{d^k} which is an elementary abelian d-group, then $\mathrm{Aut}(\mathcal{X}_{(L,L)})$ admits an elementary abelian minimal normal subgroup M which is a p-group.*

Proof. Assume that $d \neq p$. Since Σ normalizes E_{d^k} and $\gcd(d,p)=1$, we have $H = \langle \Sigma, E_{d^k}\rangle = E_{d^k} \rtimes \Sigma$. From Lemma 2.2, either $|E_{d^k} \rtimes \Sigma| < 30(\mathfrak{g}(\mathcal{X}_{(L,L)})-1)$ or $N_H(\Sigma) \cap E_{d^k} = E_{d^h} \neq \{1\}$ with $0 < h \leq k$.

- Assume that $N_H(\Sigma) \cap E_{d^k} = E_{d^h} \neq \{1\}$ with $0 < h \leq k$. From Lemma 3.5, $E_{d^h} \leq \Delta$ up to conjugation and hence $d^h = 4$ or $h = 1$. If $d^h = 4$, then $E_{d^h} = E_{d^k} = \langle \xi \rangle \times \langle \theta^{\frac{\bar{q}-1}{2}} \rangle$ from Lemma 2.4. By direct checking E_{d^k} does not commute with Σ, a contradiction. Hence $E_{d^h} = C_d \leq C_{\bar{q}-1}$. If $d = 2$ then $\mathrm{Aut}(\mathcal{X}_{(L,L)}) = O(\mathrm{Aut}(\mathcal{X}_{(L,L)})) \rtimes S_2$ by Lemma 2.5. Thus $O(\mathrm{Aut}(\mathcal{X}_{(L,L)}))$ contains a minimal normal subgroup of $\mathrm{Aut}(\mathcal{X}_{(L,L)})$, and we can assume d to be odd. Assume that $d \neq p$ is odd. Since $C_d \leq \Gamma$ and E_{d^k} is abelian, we have that E_{d^k} fixes $P_{y=0}$ and $P_{x=0}$, and acts on $\Omega_x \setminus \{P_{y=0}\}$ and $\Omega_y \setminus \{P_{x=0}\}$. Arguing as in the proof of Lemma 3.3, $E_{d^k} \leq \Gamma$. Hence $E_{d^k} = C_d$ which cannot commute with Σ, a contradiction.
- Assume that $|E_{d^k} \rtimes \Sigma| < 30(\mathfrak{g}(\mathcal{X}_{(L,L)})-1)$. By direct computation $d^k < 30$. Since no subgroup of Σ commutes with E_{d^k} we have that Σ is isomorphic to a subgroup of $GL(k,d)$. If $d^k \neq 27$ then $GL(k,d)$ has no elementary abelian subgroup of odd square order. If $d^k = 27$ then $d = p = 3$, a contradiction. □

Remark 3.7. We have shown in Lemma 3.6 that $\mathrm{Aut}(\mathcal{X}_{(L,L)})$ does not admit elementary abelian normal d-subgroups for $d \neq p$ odd. If $\mathrm{Aut}(\mathcal{X}_{(L,L)})$ admits an elementary abelian normal 2-subgroup then it also admits a minimal normal p-subgroup.

Proposition 3.8. *If* $\mathrm{Aut}(\mathcal{X}_{(L,L)})$ *admits an elementary abelian minimal normal subgroup* M*, then* $\mathrm{Aut}(\mathcal{X}_{(L,L)}) = \Sigma \rtimes \Delta$.

Proof. From Lemma 3.6, we can assume that $M \leq \Sigma$. Let $\tilde{\Sigma}$ be a Sylow p-subgroup of $\mathrm{Aut}(\mathcal{X}_{(L,L)})$. Then $M \subseteq \Sigma \cap \tilde{\Sigma}$. For any $\tau_{\alpha\beta} \in M$ and $\sigma \in \mathrm{Aut}(\mathcal{X}_{(L,L)})$, we have $\sigma(\tau_{\alpha\beta}) = \tau_{\alpha'\beta'}$ for some α', β'. Therefore σ acts on the poles of x and on the poles of y, that is, σ acts on Ω_y and on Ω_x. Suppose by contradiction that there exists ω in $\Sigma \setminus \tilde{\Sigma}$ fixing a place $P \in \Omega_x \cup \Omega_y$. Then $\mathrm{Aut}(\mathcal{X}_{(L,L)})$ admits a Sylow p-subgroup $\bar{\Sigma}$ containing ω and the stabilizer $\tilde{\Sigma}_P$ of P in $\tilde{\Sigma}$. Thus the order of $\bar{\Sigma}_P$ is strictly greater than the order of $\tilde{\Sigma}_P$, a contradiction. This proves that $\Sigma_P = \tilde{\Sigma}_P$ for all $P \in \Omega_x \cup \Omega_y$, and hence $\Sigma = \tilde{\Sigma}$. The claim follows from Lemma 3.5. □

Proposition 3.9. $\mathrm{Aut}(\mathcal{X}_{(L,L)})$ *admits an elementary abelian minimal normal subgroup.*

Proof. Suppose by contradiction that $\mathrm{Aut}(\mathcal{X}_{(L,L)})$ admits no elementary abelian minimal normal subgroup. Thus, $\mathrm{Aut}(\mathcal{X}_{(L,L)})$ is odd-core free. In fact if $O(\mathrm{Aut}(\mathcal{X}_{(L,L)})) \neq \{1\}$ then $O(\mathrm{Aut}(\mathcal{X}_{(L,L)}))$ contains a minimal normal subgroup which is then elementary abelian by the Feit–Thompson theorem. From Lemma 2.3 one of the following cases occurs:

(i) $M := PSL(2, d^k) \trianglelefteq \mathrm{Aut}(\mathcal{X}_{(L,L)}) \le P\Gamma L(2, d^k)$. In this case $\Sigma/(\Sigma \cap M)$ is isomorphic to a subgroup of $P\Gamma L(2, d^k)/PSL(2, d^k)$. Since $[PGL(2, d^k) : PSL(2, d^k)] = 2$ and $P\Gamma L(2, d^k)/PGL(2, d^k)$ is cyclic of order k, we have that $\Sigma/(\Sigma \cap M)$ is cyclic. Then either $\Sigma/(\Sigma \cap M) = \{1\}$ or $\Sigma/(\Sigma \cap M) = C_p$. When r is an odd prime, the Sylow r-subgroups of $PSL(2, d^k)$ are cyclic unless $r = d$. Since $q > p$, this implies that $d = p$ and either $d^k = q^2$ or $d^k = q^2/p$. In both cases, arguing as in the proof of Proposition 3.8, we have that any element of $\mathrm{Aut}(\mathcal{X}_{(L,L)})$ normalizing $\Sigma \cap M$ normalizes the whole group Σ. Therefore from [7, Hauptsatz 8.27] $\mathrm{Aut}(\mathcal{X}_{(L,L)})$ contains a cyclic group of order $q^2 - 1$ or $q^2/p - 1$ normalizing Σ, a contradiction to Lemma 3.5.

(ii) $M := PSL(3, d^k) \trianglelefteq \mathrm{Aut}(\mathcal{X}_{(L,L)}) \le P\Gamma L(3, d^k)$. We have $[PGL(3, d^k) : PSL(3, d^k)] \in \{1, 3\}$ and $P\Gamma L(3, d^k)/PGL(3, d^k)$ is cyclic of order k. Hence $\Sigma/(\Sigma \cap M)$ is cyclic. Then either $\Sigma/(\Sigma \cap M) = \{1\}$ or $\Sigma/(\Sigma \cap M) = C_p$. If $d = p$ then a contradiction is obtained since a Sylow d-subgroup of $PSL(3, d^k)$ is not abelian. If either $\gcd(3, d^k - 1) = 1$, or $\gcd(3, d^k - 1) = 3$ and $p \ne 3$, then a contradiction follows from Lemma 2.1. Suppose that $\gcd(3, d^k - 1) = 3$ and $p = 3$. In this case a contradiction is obtained because the Sylow 3-subgroup of M is not abelian (see [7, Satz 7.2]), and hence cannot be contained in Σ.

(iii) $M := PSU(3, d^k) \trianglelefteq \mathrm{Aut}(\mathcal{X}_{(L,L)}) \le P\Gamma U(3, d^k)$. We have $[PGL(3, d^k) : PSL(3, d^k)] \in \{1, 3\}$ and $P\Gamma L(3, d^k)/PGL(3, d^k)$ is cyclic of order k. Hence $\Sigma/(\Sigma \cap M)$ is cyclic. Then either $\Sigma/(\Sigma \cap M) = \{1\}$ or $\Sigma/(\Sigma \cap M) = C_p$. If $d = p$ then a contradiction is obtained since a Sylow d-subgroup of $PSL(3, d^k)$ is not abelian. If either $\gcd(3, d^k + 1) = 1$, or $\gcd(3, d^k + 1) = 3$ and $p \ne 3$, then a contradiction follows from Lemma 2.1. Suppose that $\gcd(3, d^k + 1) = 3$ and $p = 3$. In this case a contradiction is obtained because the Sylow 3-subgroup of M is not abelian (see [6, Theorem A.10 Case (iii)]), and hence cannot be contained in Σ.

(iv) $\mathrm{Aut}(\mathcal{X}_{(L,L)}) = A_7$. Since $|A_7| = 2^3 \cdot 3^2 \cdot 5 \cdot 7$, we have $q = 3 = p$, which is impossible.

(v) $\mathrm{Aut}(\mathcal{X}_{(L,L)}) = M_{11}$. Since $|M_{11}| = 2^4 \cdot 3^2 \cdot 5 \cdot 11$, we have $q = 3 = p$, which is impossible. $\square$

From Propositions 3.8 and 3.9, Theorem 1.1 follows.

3.2. Proof of Theorem 1.2

In this section, $L_1 \ne L_2$ and we refer to Σ and Γ as defined in Theorem 1.2.

Lemma 3.10. *The normalizer N of Σ in $\mathrm{Aut}(\mathcal{X}_{(L_1,L_2)})$ is $N = \Sigma \rtimes \Gamma$.*

Proof. From Corollary 3.2, $\bar{N} = N/\Sigma$ is a tame subgroup of $PGL(2, \mathbb{K})$ containing a cyclic group $\bar{\Gamma}$ which is isomorphic to Γ. Arguing as in the proof of Lemma 3.5, N has no involution other than $\theta^{(\bar{q}-1)/2}$, because by direct checking $\xi : (x, y) \mapsto (y, x)$ is not in $\mathrm{Aut}(\mathcal{X}_{(L_1,L_2)})$. From [7, Hauptsatz 8.27], one of the following holds:

(1) $\bar{N}$ is isomorphic either to A_4 or S_4 or A_5.
(2) $\bar{N}$ is isomorphic to a cyclic group C_d.

Arguing as in the proof of Lemma 3.5, Case (1) is not possible because $\bar{N}$ is tame and it contains only one involution. Therefore, case (2) occurs. From Lemma 3.3, $d = \bar{q} - 1$ and the claim follows. □

The proofs of the following results are analogous to the ones of Lemma 3.6, Proposition 3.8, and Proposition 3.9, and are omitted.

Lemma 3.11. *If* $\mathrm{Aut}(\mathcal{X}_{(L_1,L_2)})$ *has a minimal normal subgroup* E_{d^k} *which is an elementary abelian d-group, then* $\mathrm{Aut}(\mathcal{X}_{(L_1,L_2)})$ *admits an elementary abelian minimal normal subgroup* M *which is a p-group.*

Proposition 3.12. *If* $\mathrm{Aut}(\mathcal{X}_{(L_1,L_2)})$ *admits an elementary abelian minimal normal subgroup, then* $\mathrm{Aut}(\mathcal{X}_{(L_1,L_2)}) = \Sigma \rtimes \Gamma$.

Proposition 3.13. $\mathrm{Aut}(\mathcal{X}_{(L_1,L_2)})$ *admits an elementary abelian minimal normal subgroup.*

From Propositions 3.12 and 3.13, Theorem 1.2 follows.

4. Curves with automorphism group containing E_{q^2}

We need the following result on curves admitting E_{q^2} as an automorphism group.

Proposition 4.1. *For a curve* $\mathcal{X}$ *defined over* $\mathbb{K}$, *assume that one of the following holds.*

(A) $\mathcal{X}$ *has genus* $\mathfrak{g} \le (q-1)^2$ *and the automorphism group* $\mathrm{Aut}(\mathcal{X})$ *has a subgroup* $H = E_{q^2} \rtimes (C_2 \times C_2)$.
(B) $\mathcal{X}$ *has genus* $\mathfrak{g} = (q-1)^2$ *and the automorphism group* $\mathrm{Aut}(\mathcal{X})$ *has a subgroup* $H = E_{q^2}$.

Let $\{M_i\}_i$ *be the set of subgroups of* E_{q^2} *of order* q. *Then the following hold.*

(1) $\mathcal{X}$ *is an ordinary curve of genus* $(q-1)^2$;
(2) *Up to relabeling the indices, the cover* $\mathcal{X} \mid \mathcal{X}/M_i$ *is unramified for each* $i \ne 1,2$;
(3) E_{q^2} *has only two short orbits* Ω_1 *and* Ω_2 *on* $\mathcal{X}$, *each of size* q. *The places of* Ω_i *share the same stabilizer* M_i *for* $i \in \{1,2\}$, *and* $M_1 \ne M_2$. *Moreover,* $\mathcal{X}/M_1$ *and* $\mathcal{X}/M_2$ *are rational.*

Proof. Let $\mathfrak{g}$ and γ, $\bar{\mathfrak{g}}$ and $\bar{\gamma}$, be the genus and p-rank of $\mathcal{X}$, $\bar{\mathcal{X}} := \mathcal{X}/E_{q^2}$ respectively. Also, denote by $k \in \mathbb{N}$ the number of short orbits of E_{q^2} on $\mathcal{X}$, by Ω_i $(1 \le i \le k)$ the i-th short orbit of E_{q^2}, by $\ell_i \in \{p, p^2, \dots, q^2/p\}$ the length of Ω_i, and by M_i the stabilizer of a given place $P_i \in \Omega_i$ in E_{q^2}, of size q^2/ℓ_i. Note that M_i coincides with the stabilizer in E_{q^2} of any place in Ω_i, because E_{q^2} acts on the fixed places of its normal subgroup M_i.

(A) Case $\mathfrak{g} \leq (q-1)^2$ and $H := E_{q^2} \rtimes (C_2 \times C_2) \leq \mathrm{Aut}(\mathcal{X})$.

If $\gamma = 0$, then every element of E_{q^2} fixes exactly one place of $\mathcal{X}$ from [6, Lemma 11.129]. Since E_{q^2} is abelian all elements of E_{q^2} have the same fixed place P, which is fixed also by H. Thus, H/E_{q^2} is cyclic by [6, Theorem 11.49], a contradiction to $H/E_{q^2} \cong C_2 \times C_2$. If $\gamma = 1$ then E_{q^2} is cyclic by Theorem 2.1 (IV), a contradiction. Hence $\gamma \geq 2$. The Deuring–Shafarevich formula (8) applied to E_{q^2} yields

$$\gamma - 1 = q^2(\bar{\gamma} - 1) + \sum_{i=1}^{k}(q^2 - \ell_i). \tag{10}$$

If $k = 0$ then $\bar{\gamma} = (\gamma-1)/q^2 + 1 > 1$, and hence $q^2 \leq \gamma - 1 \leq \mathfrak{g} - 1 \leq q^2 - 2q$, a contradiction. Therefore $\bar{\gamma} \leq 1$ and $k \geq 1$.

Assume that $\bar{\gamma} = 1$. The Riemann–Hurwitz formula together with $\bar{\mathfrak{g}} \geq \bar{\gamma}$ yields $\bar{\mathfrak{g}} = 1$. If $k \geq 2$ then $\gamma - 1 \geq 2(q^2 - q^2/p)$ by equation (10), a contradiction to $\gamma \leq \mathfrak{g}$. This yields $k = 1$. Since $C_2 \times C_2$ normalizes E_{q^2} which has a unique short orbit Ω_1, the induced group $\bar{C}_2 \times \bar{C}_2$ fixes one place of the elliptic curve $\bar{\mathcal{X}}$. From [6, Theorem 11.94 (ii)] and its proof, $\bar{C}_2 \times \bar{C}_2$ is cyclic, a contradiction.

Therefore $\bar{\gamma} = 0$. If $k \geq 3$ then equation (10) together with $\mathfrak{g} \geq \gamma$ yields a contradiction. If $k = 1$ then equation (10) reads $2 \geq \gamma = 1 - \ell_1$, a contradiction. Thus $k = 2$ and equation (10) reads

$$\gamma = q^2 + 1 - (\ell_1 + \ell_2).$$

We prove that $\bar{\mathfrak{g}} = 0$. From the Riemann–Hurwitz formula (6) applied to $\mathcal{X} \to \bar{\mathcal{X}}$ we have that

$$q^2\bar{\mathfrak{g}} \leq \ell_1 + \ell_2 - 2q \leq 2\frac{q^2}{p} - 2q,$$

which implies $\bar{\mathfrak{g}} = 0$. Since $C_2 \times C_2$ normalizes E_{q^2}, the induced group $\bar{C}_2 \times \bar{C}_2$ is a subgroup of $PGL(2, \mathbb{K})$ acting on the two places $\bar{P}_1$ and $\bar{P}_2$ lying under Ω_1 and Ω_2. From [7, Hauptsatz 8.27], $\bar{C}_2 \times \bar{C}_2$ switches $\bar{P}_1$ and $\bar{P}_2$ and hence $\ell_1 = \ell_2 = \ell$. Let $P \in \Omega_i$. From [6, Lemma 11.75 (v)] either $(E_{q^2})_P^{(2)}$ is trivial, or $(E_{q^2})_P^{(2)} = E_{q^2}$, or $1 < |(E_{q^2})_P^{(2)}| = \cdots = |(E_{q^2})_P^{(2)}| < q^2$. By direct checking with the Riemann–Hurwitz formula applied to $\mathcal{X} \to \bar{\mathcal{X}}$, the second and the third case are not possible; hence $(E_{q^2})_P^{(2)}$ is trivial for all P, which implies $\ell = q$. Now the Deuring–Shafarevich formula yields $\gamma = (q-1)^2 \geq \mathfrak{g}$; hence, $\gamma = \mathfrak{g} = (q-1)^2$ and the claim *(1)* follows. Since M_i, $i = 1, 2$, is the stabilizer in E_{q^2} of any place in Ω_i, we have that any other subgroup M_j of order q of E_{q^2}, $j \neq 1, 2$, has no fixed place, and thus the claim *(2)* is proved. Finally, for $i = 1, 2$, denote by $\mathfrak{g}_i$ the genus of the curve $\mathcal{X}/M_i$. By the Riemann–Hurwitz formula (6) applied to the cover $\mathcal{X} \to \mathcal{X}/M_i$,

$$2\mathfrak{g} - 2 = 2(q^2 - 2q) \geq 2q(\mathfrak{g}_i - 1) + 2q(q - 1). \tag{11}$$

Hence $\mathfrak{g}_i = 0$ for $i = 1, 2$ and equality holds in (11). This proves that M_i has no fixed place out of Ω_i, and so $M_1 \neq M_2$.

(B) Case $\mathfrak{g} = (q-1)^2$ and $H := E_{q^2} \leq \mathrm{Aut}(\mathcal{X})$.
Suppose $\gamma = 0$. Then by [6, Lemma 11.129] every element of H fixes exactly one place, which is the same place P for all of them. The Riemann–Hurwitz formula (6) applied to the cover $\mathcal{X} \to \mathcal{X}/H$ yields $\bar{\mathfrak{g}} = 0$, $H_P^{(2)} \neq \{1\}$, and

$$\sum_{i=2}^{\infty}(|H_P^{(i)}| - 1) = 2(q-1)^2. \tag{12}$$

From [6, Th. 11.78], $\mathcal{X}/H_P^{(2)}$ is rational; hence, the Riemann–Hurwitz formula applied to $\mathcal{X} \to \mathcal{X}/H_P^{(2)}$ yields

$$\sum_{i=2}^{\infty}(|H_P^{(i)}| - 1) = 2q^2 - 4q + 2|H_P^{(2)}|. \tag{13}$$

Equations (12) and (13) provide a contradiction to $H_P^{(2)} \neq \{1\}$. Suppose $\gamma = 1$. Then H is cyclic by Theorem 2.1 (IV), a contradiction.
Therefore $\gamma \geq 2$. As in Case (A), $\bar{\gamma} \leq 1$ and $k \geq 1$; also, if $\bar{\gamma} = 1$, then $k = 1$.
Suppose $\bar{\gamma} = 1$ and $k = 1$. From $\mathfrak{g} \geq \gamma$ and the Deuring–Shafarevich formula applied to $\mathcal{X} \to \bar{\mathcal{X}}$ we have $\bar{\mathfrak{g}} = 1$ and $\ell_1 \geq 2q$; hence, pq divides ℓ_1. The Riemann–Hurwitz formula applied to $\mathcal{X} \to \bar{\mathcal{X}}$ reads

$$2(q-1)^2 - 2 = q^2(2 \cdot 0 - 2) + \ell_1 \sum_{i=0}^{\infty}(|H_P^{(i)}| - 1)$$

for any P in Ω_1. This implies that ℓ_1 divides q, a contradiction to $pq \mid \ell_1$.
Therefore $\bar{\gamma} = 0$. Arguing as in the proof of Proposition 4.1 we have $k = 2$, $\gamma = q^2 + 1 - (\ell_1 + \ell_2)$, and $\bar{\mathfrak{g}} = 0$. From the Riemann–Hurwitz formula applied to $\mathcal{X} \to \bar{\mathcal{X}}$,

$$2(\ell_1 + \ell_2) - 4q = \ell_1 c_1 + \ell_2 c_2 \geq 0, \tag{14}$$

where $c_j := \sum_{i=2}^{\infty}(|H_{P_j}^{(i)}| - 1) \geq 0$ for $j = 1, 2$. From Equation (14), the integers ℓ_1 and ℓ_2 cannot be multiple of pq at the same time. Hence $\ell_1 \leq q$ or $\ell_2 \leq q$; say $\ell_1 \leq q$. We have $|H_{P_1}^{(2)}| < q^2/\ell_1$ and $|H_{P_2}^{(2)}| < q^2/\ell_2$; otherwise, Equation (14) would imply $2(\ell_1 + \ell_2) - 4q \geq q^2 - \ell_1$ or $2(\ell_1 + \ell_2) - 4q \geq q^2 - \ell_2$, which is impossible because $\ell_1 \leq q$ and $\ell_2 \leq q^2/p$. Therefore, for $j = 1, 2$, c_j is a multiple of p (possibly zero) from [6, Lemma 11.75 (v)]. Suppose $\ell_2 \geq pq$. As $c_2 \neq 2$, Equation (14) implies that ℓ_2 divides $[4q+(c_1-2)\ell_1]$; hence, p divides $[2(2q/\ell_1-1)]$, a contradiction. Therefore, $\ell_2 \leq q$. Thus, from Equation (14), $\ell_1 = \ell_2 = q$. The rest of the claim follows as in Case (A). $\square$

Theorem 4.2 provides a characterization which generalizes a result by van der Geer and van der Vlugt; see [12, Proposition 2.2 and Corollary 2.3].

Theorem 4.2. *Let $\mathcal{Y}$ be a curve of genus $q-1$ defined over $\mathbb{K}$ whose automorphism group* $\mathrm{Aut}(\mathcal{Y})$ *contains an elementary abelian subgroup E_q of order q. Then one of the following holds.*

(I) *$\mathcal{Y}$ is birationally equivalent over $\mathbb{K}$ to the curve $\mathcal{Y}_{L,a}$ with affine equation*

$$L(y) = ax + \frac{1}{x}, \tag{15}$$

for some $a \in \mathbb{K}^*$ and $L(T) \in \mathbb{K}[T]$ a separable p-linearized polynomial of degree q. For the curve $\mathcal{Y}_{L,a}$ the following properties hold:
- (i) *$\mathcal{Y}_{L,a}$ is ordinary and hyperelliptic;*
- (ii) *$\mathcal{Y}_{L,a}$ has exactly $2q$ Weierstrass places, which are the fixed places of the hyperelliptic involution μ.*
- (iii) *The full automorphism group* $\mathrm{Aut}(\mathcal{Y}_L)$ *of $\mathcal{Y}_{L,a}$ has order $4q$ and is a direct product $Dih(E_q) \times \langle\mu\rangle$.*

(II) *$p \neq 3$ and $\mathcal{Y}$ is birationally equivalent over $\mathbb{K}$ to the curve $\mathcal{Z}_{\tilde{L},b}$ with affine equation*

$$\tilde{L}(y) = x^3 + bx, \tag{16}$$

for some $a \in \mathbb{K}$ and $\tilde{L}(T) \in \mathbb{K}[T]$ a separable p-linearized polynomial of degree q. For the curve $\mathcal{Z}_{\tilde{L},b}$ the following properties hold:
- (i) *$\mathcal{Z}_{\tilde{L},b}$ has zero p-rank;*
- (ii) $\mathrm{Aut}(\mathcal{Z}_{\tilde{L},b})$ *contains a generalized dihedral subgroup $Dih(E_q) = E_q \rtimes \langle\nu\rangle$.*

Proof. The proof is divided in several steps.

- We show that $\mathcal{Y}_{L,a}$ as in (15) has genus $q-1$ and $\mathrm{Aut}(\mathcal{Y}_{L,a})$ contains a subgroup $Dih(E_q) \times \langle\mu\rangle$.
  Let $\bar{P}_0$ and $\bar{P}_\infty$ be the zero and pole of x in $\mathbb{K}(x)$, respectively. Then $\mathbb{K}(\mathcal{Y})|\mathbb{K}(x)$ is a generalized Artin–Schreier extension ([10, Proposition 3.7.10]) which ramifies exactly over the simple poles $\bar{P}_0$ and $\bar{P}_\infty$ of $ax + \frac{1}{x}$. Hence, $g(\mathcal{Y}_{L,a}) = q-1$. The maps

$$E_q = \{\tau_\alpha : (x,y) \mapsto (x, y+\alpha) \mid L(\alpha) = 0\},$$
$$\nu : (x,y) \mapsto (-x,-y), \quad \mu : (x,y) \mapsto (1/(ax), y), \tag{17}$$

generate an automorphism group $Dih(E_q) \times \langle \mu \rangle = (E_q \rtimes \langle \nu \rangle) \times \langle \mu \rangle$ of order $4q$ of $\mathcal{Y}_{L,a}$.

- We show that $\mathcal{Y}_{L,a}$ is ordinary and hyperelliptic with hyperelliptic involution μ, and that the Weierstrass places of $\mathcal{Y}_{L,a}$ are exactly the $2q$ fixed places of μ.
  Let P_0 and P_∞ be the places of $\mathcal{Y}$ lying over $\bar{P}_0$ and $\bar{P}_\infty$. The group E_q and the involution ν fix P_0 and P_∞, while the involution μ interchanges P_0 and P_∞. Let $\bar{\mathcal{Y}} = \mathcal{Y}/E_q$ and $\mathcal{Y}' = \mathcal{Y}/\langle \mu \rangle$. The Riemann–Hurwitz formula applied to the cover $\mathcal{Y} \to \bar{\mathcal{Y}}$ shows that $\bar{\mathcal{Y}}$ is rational and P_0, P_∞ are the unique fixed places of any element of E_q. Thus, the Deuring–Shafarevich formula applied to $\mathcal{Y} \to \bar{\mathcal{Y}}$ shows that $\mathcal{Y}$ has p-rank $q-1$; hence, $\mathcal{Y}$ is ordinary. Let $\bar{P}_1$ and $\bar{P}_2$ be the distinct zeros of ax^2+1 in $\mathbb{K}(x)$, and $P_1^1, \ldots, P_1^q$ and $P_2^1, \ldots, P_2^q$ be the distinct places of $\mathcal{Y}$ lying over $\bar{P}_1$ and $\bar{P}_2$. By direct checking, μ fixes $P_1^1, \ldots, P_1^q, P_2^1, \ldots, P_2^q$. Then the Riemann–Hurwitz formula applied to $\mathcal{Y} \to \mathcal{Y}'$ shows that μ has no other fixed places and $\mathcal{Y}'$ is rational; hence, $\mathcal{Y}$ is hyperelliptic with hyperelliptic involution μ. Since $2q > 4$, the $2q$ fixed places of μ are Weierstrass places of $\mathcal{Y}$ from [6, Theorem 11.112]. Moreover, $\mathcal{Y}$ has exactly $2q$ Weierstrass places from [6, Theorem 7.103].
- We show that $\mathcal{Z}_{\tilde{L},b}$ as in (16) has zero p-rank and admits an automorphism group $Dih(E_q)$.
  The curve $\mathcal{Z}_{\tilde{L},b}$ admits the automorphism group $Dih(E_q) = E_q \rtimes \langle \nu \rangle$, where

$$E_q = \{\tau_\alpha : (x,y) \mapsto (x, y+\alpha) \mid M(\alpha) = 0\}, \quad \nu : (x,y) \mapsto (-x,-y).$$

  From [6, Lemma 12.1 (f)], $\mathcal{Z}_{\tilde{L},b}$ has zero p-rank.
- Let $\mathcal{Y}$ be a curve of genus $q-1$ admitting an automorphism group E_q with λ fixed places. We show that, if $\lambda = 1$, then $p \neq 3$ and $\mathcal{Y}$ is birationally equivalent to some $\mathcal{Z}_{M,b}$.
  Let $\bar{\mathcal{Y}} = \mathcal{Y}/E_q$. The Riemann–Hurwitz formula applied to $\mathcal{Y} \to \bar{\mathcal{Y}}$ shows that $\bar{\mathcal{Y}}$ has genus zero and

$$2(q-1) = \sum_{i=2}^{\infty} (|(E_q)_P^{(i)}| - 1) + \sum_i \ell_i d_{P_i}, \tag{18}$$

  where ℓ_i are the lengths of the short orbits Ω_i of E_q other than $\{P\}$ and P_i is a place of Ω_i; hence, the second summation in Equation (18) is multiple of p. From [6, Lemma 11.75 (v)], the first summation in (18) is the sum of a multiple of p and $j(q-1)$, where j is the largest integer such that $(E_q)_P^{(j+1)} = E_q$. Thus $j = 2$, $E_q = \ldots = (E_q)_P^{(3)}$, $(E_q)_P^{(4)} = \{1\}$, and $\{P\}$ is the unique short orbit of E_q. Let $x \in \mathbb{K}(\bar{\mathcal{Y}})$ with $\mathbb{K}(\bar{\mathcal{Y}}) = \mathbb{K}(x)$ and $\bar{P}$ be the place of $\bar{\mathcal{Y}}$ lying under P. Up to conjugation in $\mathrm{Aut}(\bar{\mathcal{Y}}) \cong PGL(2,\mathbb{K})$, $\bar{P}$ is the simple pole of x. Since $\mathbb{K}(\mathcal{Y})|\mathbb{K}(x)$ is a generalized Artin–Schreier extension ([10, Proposition 3.7.10]), $\mathbb{K}(\mathcal{Y})$ is defined as $\mathbb{K}(x,y)$ by $M(y) = h(x)$, where $M(T) \in \mathbb{K}[T]$ is a separable p-linearized polynomial of degree q and $h(x) \in \mathbb{K}(x)$. Since P is the unique ramified place in $\mathbb{K}(x,y)|\mathbb{K}(x)$, Proposition 3.7.10 in [10] implies that $h(x)$ is a polynomial function in $\mathbb{K}[x]$ and, in order for the genus of $\mathcal{Y}$ to be $q-1$, the valuation of x at P is -3 and coprime to p. Hence, $h(T) \in \mathbb{K}[T]$ has degree 3 and $p \neq 3$. Up to a linear transformation in x, we can assume that $h(x)$ has the form $x^3 + bx + c$; up to a translation in y, we can then assume that $c = 0$.

- Let $\mathcal{Y}$ be a curve of genus $q-1$ admitting an automorphism group E_q with λ fixed places. We show that, if $\lambda \neq 1$, then $\mathcal{Y}$ is birationally equivalent to some $\mathcal{Y}_{L,a}$.
Let $\bar{\mathcal{Y}} = \mathcal{Y}/E_q$ with genus $\bar{\mathfrak{g}}$. From the Riemann–Hurwitz formula applied to $\mathcal{Y} \to \bar{\mathcal{Y}}$,
$$2q-4 = q(2\bar{\mathfrak{g}}-2) + 2\lambda(q-1) + \sum_{i=1}^{\lambda}\sum_{j=2}^{\infty}(|(E_q)_{Q_i}^{(j)}|-1) + \sum_i \ell_i d_{P_i}, \tag{19}$$
where $Q_1,\ldots,Q_\lambda$ are the fixed places of E_q, ℓ_i are the lengths of the short orbits of E_q other than $\{Q_1\},\ldots,\{Q_\lambda\}$, and P_i is a place of the i-th short orbit. Note that ℓ_i is a multiple of p. If $\lambda = 0$, then Equation (19) yields a contradiction modulo p. Then $\lambda \geq 2$. Hence, from Equation (19), $\bar{\mathfrak{g}} = 0$, $\lambda = 2$, and E_q has no short orbits other than the two fixed places P and Q. Let $x \in \mathbb{K}(\bar{\mathcal{Y}})$ with $\mathbb{K}(\mathcal{Y}) = \mathbb{K}(x)$. Since $\mathbb{K}(\mathcal{Y})|\mathbb{K}(x)$ is a generalized Artin–Schreier extension ([10, Proposition 3.7.10]), $\mathbb{K}(\mathcal{Y})$ is defined as $\mathbb{K}(x,y)$ by $L(y) = h(x)$, for some separable p-linearized polynomial $L(T) \in \mathbb{K}[T]$ of degree q. Also, from [10, Proposition 3.7.10], P and Q are the unique poles of $h(x)$, and they are simple poles. Up to conjugation in $\mathrm{Aut}(\bar{\mathcal{Y}}) \cong PGL(2,\mathbb{K})$, $\bar{P}$ and $\bar{Q}$ are the zero and the pole of x. Therefore, $h(x) = (x-r)(x-s)/x$ for some $r,s \in \mathbb{K}$. Up to formal replacement of x and y with rsx and $y+\delta$, where $\delta \in \mathbb{K}$ satisfies $L(\delta) = -r-s$, the equation $L(y) = h(x)$ is the equation defining the curve $\mathcal{Y}_{L,rs}$.
- Finally, we show that $\mathrm{Aut}(\mathcal{Y}_{L,a})$ is the group $Dih(E_q) \times \langle\mu\rangle = (E_q \rtimes \langle\nu\rangle) \times \langle\mu\rangle$ described in (17).
Let $\mathcal{Y}' = \mathcal{Y}/\mu$. Then $\mathrm{Aut}(\mathcal{Y}')$ contains the group $G' \cong \mathrm{Aut}(\mathcal{Y})/\langle\mu\rangle$ induced by $\mathrm{Aut}(\mathcal{Y})$, and in particular the subgroup $E_q' \rtimes \langle\nu'\rangle \cong E_q \rtimes \langle\nu\rangle$ induced by $E_q \rtimes \langle\nu\rangle$. The group E_q' is a Sylow p-subgroup of G', because E_q is a Sylow p-subgroup of $\mathrm{Aut}(\mathcal{Y})$ from Theorem 2.1 (II). From [6, Theorem 11.98] and [7, Haptsatz 8.27], either $G' \cong \mathrm{PSL}(2,q)$, or $G' \cong \mathrm{PGL}(2,q)$, or $G' = E_q' \rtimes C_m'$, where C_m' is cyclic of order m with $m \mid (q-1)$.
Assume that G' contains a subgroup $E_q' \rtimes C_m'$ with $m \mid (q-1)$. Up to conjugation, E_q' is the group induced by E_q as in (17). Let C be a tame subgroup of $\mathrm{Aut}(\mathcal{Y})$ inducing C_m'. Since C normalizes E_q, C acts on the two places of $\mathcal{Y}$ fixed by E_q and acts on the other orbits of E_q; since C commutes with μ, C acts on the fixed places of μ, which form two orbits of E_q. Thus, the group $\bar{C} \cong C$ induced by C on the rational curve $\bar{\mathcal{Y}} = \mathcal{Y}/E_q$ acts on two couples of places. From [7, Satz 8.5], $\bar{C}$ has two fixed places and no other short orbits on $\bar{\mathcal{Y}}$; hence, $\bar{C}$ has order 2. This implies $m = 2$. For $q-1 > 2$ the Lemma is then proved, because both $\mathrm{PGL}(2,q)$ and $\mathrm{PSL}(2,q)$ contain subgroups $E_q \rtimes C_{q-1}$ of order $q(q-1)$; see [7, Hauptsatz 8.27] and [11].

Assume $q = 3$. The case $G' \cong \mathrm{PSL}(2,3)$ is not possible, since $\mathrm{PSL}(2,3)$ contains no subgroup $Dih(E_3)$. Suppose $G' \cong \mathrm{PGL}(2,3)$. Let ρ' be an element of G' of order 4, and $\rho \in G$ an element of order 4 inducing ρ'. From [7, Sätze 8.2 and 8.4] and [11], ρ' does not fix the place P' of $\mathcal{Y}'$ lying under the fixed places P, Q of E_q. Hence, P and Q are in a long orbit of ρ. Therefore, ρ' has a short orbit of length 2 on $\mathcal{Y}'$. This is impossible, since from [7, Satz 8.5] (see also [11]) ρ' has two fixed places and no other short orbits on $\mathcal{Y}'$. We conclude that $G' = E'_q \rtimes C'_m$, and $m = 2$ follows as above. The Lemma is thus proved. □

Proposition 4.3. *For a curve $\mathcal{X}$ defined over $\mathbb{K}$, assume that one of the following holds.*

(A) *$\mathcal{X}$ has genus $\mathfrak{g} \leq (q-1)^2$ and $\mathrm{Aut}(\mathcal{X})$ contains a subgroup $H = E_{q^2} \rtimes (C_2 \times C_2)$;*
(B) *$\mathcal{X}$ has genus $\mathfrak{g} = (q-1)^2$ and $\mathrm{Aut}(\mathcal{X})$ contains a subgroup $H = E_{q^2}$.*

Then E_{q^2} has a subgroup T of order q such that the quotient curve $\mathcal{X}/T$ is birationally equivalent over $\mathbb{K}$ to the curve $\mathcal{Y}_{L,a}$ in (15), for some $a \in \mathbb{K}^*$ and $L(T) \in \mathbb{K}[T]$ a separable p-linearized polynomial of degree q.

Proof. From Proposition 4.1, $\mathcal{X}$ is ordinary of genus $(q-1)^2$ and E_{q^2} admits a subgroup T of order q such that the cover $\mathcal{X} \to \mathcal{X}/T$ is unramified. From the Riemann–Hurwitz formula and the Deuring–Shafarevich formula applied to $\mathcal{X} \to \mathcal{X}/T$, the curve $\mathcal{X}/T$ is ordinary of genus $q-1$. Since T is normal in E_{q^2}, $\mathrm{Aut}(\mathcal{X}/T)$ contains a subgroup $E_{q^2}/T \cong E_q$. From Theorem 4.2, $\mathcal{X}/T$ is birationally equivalent over $\mathbb{K}$ to $\mathcal{Y}_{L,a}$ for some a and L. □

Proposition 4.4. *Let $\mathcal{X}$ be a curve admitting an automorphism group E_{q^2} such that, for some $E_q \leq E_{q^2}$ the quotient curve $\mathcal{X}/E_q$ has affine equation*

$$L(y) = ax + \frac{1}{x},$$

for some $a \in \mathbb{K}^*$ and $L(T) \in \mathbb{K}[T]$ a separable p-linearized polynomial of degree q. Then the following hold:

(1) *$\mathbb{K}(\mathcal{X}/E_{q^2}) = \mathbb{K}(x)$.*
(2) *If $\mathcal{X}$ is an ordinary curve with genus $(q-1)^2$, then E_{q^2} contains a subgroup M of order q different from E_q such that the quotient curve $\mathcal{X}/M$ has affine equation*

$$\tilde{L}(z) = b + \frac{1}{x},$$

for some $z \in \mathbb{K}(\mathcal{X})$, $b \in \mathbb{K}$, and $\tilde{L}(T) \in \mathbb{K}[T]$ a separable p-linearized polynomial of degree q.

Proof. Since $[\mathbb{K}(\mathcal{X}):\mathbb{K}(x)] = q^2 = [\mathbb{K}(\mathcal{X}):\mathbb{K}(\mathcal{X}/E_{q^2})]$, it is enough to prove that $\tau(x) = x$ for any $\tau \in E_{q^2} \setminus E_q$. Since τ and E_q commute, τ induces an automorphism τ' of $\mathbb{K}(x,y)$. If τ' is trivial then $\tau(x) = x$ and *(1)* follows. Otherwise, τ' has order p. Clearly $E_{q^2}/E_q \cong \tilde{E}_q$, where $\tilde{E}_q$ is an elementary abelian subgroup of $\mathrm{Aut}(\mathcal{Y}_L)$ of order q. Arguing as in the proof of Theorem 1.1, $\mathrm{Aut}(\mathcal{Y}_L)$ has a unique elementary abelian group F of order q, namely

$$F = \{\tau_\alpha :\ (x,y) \mapsto (x, y+\alpha) \mid L(\alpha) = 0\},$$

and hence $F = \tilde{E}_q$. Hence $\tau(x) = x$ for every $\tau \in E_{q^2} \setminus E_q$ and (1) follows. From *(1)*, $\mathbb{K}(\mathcal{X}/E_{q^2}) = \mathbb{K}(x)$, that is, $\mathcal{X}/E_{q^2} = \mathbb{P}^1(\mathbb{K})$. The curve $\mathcal{Y}_L$ is the quotient curve $\mathcal{X}_{(L,L)}/H$, where

$$H = \{\tau_{\alpha,\alpha} :\ (x,y) \mapsto (x+\alpha, y+\alpha) \mid L(\alpha) = 0\}.$$

In fact it is sufficient to consider the functions $\eta, \theta \in \mathbb{K}(\mathcal{X}_{(L,L)})$ with $\eta = L(y)$ and $\theta = x + y$. By direct checking $L(\theta) = \eta + 1/\eta$ and $\mathbb{K}(\mathcal{X}_{(L,L)}/H) = \mathbb{K}(\eta,\theta)$. Since $\mathcal{X}_{(L,L)}$ is an ordinary curve of genus $(q-1)^2$ and the cover $\mathcal{X}_{(L,L)} \to \mathcal{X}_{(L,L)}/H$ is unramified, from the Deuring–Shafarevich formula and the Riemann–Hurwitz formula, we have that $\mathcal{Y}_L$ is an ordinary curve of genus $\mathfrak{g}' = q-1$. The Deuring–Shafarevich formula applied to E_q shows that the extension $\mathbb{K}(\mathcal{X})|\mathbb{K}(\mathcal{Y}_L)$ is unramified. Let P_0 and P_∞ be respectively the zero and pole of x in $\mathbb{K}(x)$. Then P_0 and P_∞ are totally ramified in the extension $\mathbb{K}(\mathcal{Y}_L)|\mathbb{K}(x)$ and no other place of $\mathbb{P}^1(\mathbb{K})$ ramifies; see [10, Proposition 3.7.10]. Therefore, both P_0 and P_∞ split completely in $\mathcal{X}$. Let M be the stabilizer in E_{q^2} of a place Q_∞ of $\mathcal{X}$ lying over P_∞. We show that P_∞ is unramified in the extension $\mathbb{K}(\mathcal{X}/M)|\mathbb{K}(x)$. Note that $|M| = q$, since P_∞ splits in q distinct places in $\mathcal{X}$. Furthermore, since E_{q^2} is abelian, each place of $\mathcal{X}$ lying over P_∞ has the same stabilizer M. Therefore, P_∞ splits completely in $\mathcal{X}/M$. Applying the Riemann–Hurwitz formula to the extension $\mathbb{K}(\mathcal{X})|\mathbb{K}(\mathcal{X}/M)$ yields

$$2(q-1)^2 - 2 \geq q(2\mathfrak{g}(\mathcal{X}/M) - 2) + 2q(q-1).$$

Thus $\mathfrak{g}(\mathcal{X}/M) = 0$. Clearly $[\mathbb{K}(\mathcal{X}/M) : \mathbb{K}(x)] = q$, since

$$q^2 = [\mathbb{K}(\mathcal{X}) : \mathbb{K}(x)] = [\mathbb{K}(\mathcal{X}) : \mathbb{K}(\mathcal{X}/M)][\mathbb{K}(\mathcal{X}/M) : \mathbb{K}(x)] = q[\mathbb{K}(\mathcal{X}/M) : \mathbb{K}(x)].$$

From the Deuring–Shafarevich formula applied to the extension $\mathbb{K}(\mathcal{X}/M)|\mathbb{K}(x)$, we have that $\mathbb{K}(x)$ has only one place that ramifies in $\mathbb{K}(\mathcal{X}/M)|\mathbb{K}(x)$, and this place must be P_0.

We prove that the quotient curve $\mathcal{X}/M$ has affine equation

$$\tilde{L}(z) = b + \frac{1}{x},$$

for some $z \in \mathbb{K}(\mathcal{X})$, $b \in \mathbb{K}$, and $\tilde{L}(T) \in \mathbb{K}[T]$ a separable p-linearized polynomial of degree q. Since $\mathbb{K}(\mathcal{X}/M)|\mathbb{K}(x)$ is a generalized Artin–Schreier extension ([10, Proposition 3.7.10]), we have that $\mathbb{K}(\mathcal{X}/M) = \mathbb{K}(x,y)$ where $\tilde{L}(y) = f(x)/g(x)$ for some separable p-linearized polynomial $\tilde{L}(T) \in \mathbb{K}[T]$ of degree q and $f(x)/g(x) \in \mathbb{K}(x)$. Recall that P_0 is the unique pole of $f(x)/g(x)$, and it is a simple pole.

- Suppose that $\deg(f) > \deg(g)$. Then $f(x)/g(x)$ has a pole at P_∞, a contradiction.
- Suppose that $\deg(f) = \deg(g) > 0$. Let $g(x) = x \cdot r(x)^p$ with $r(x) \in \mathbb{K}[x]$, then $f(x) = (x+\alpha)s(x)^p$ with $\alpha \in \mathbb{K}$ and $s(x) \in \mathbb{K}[x]$. If $r(x)$ has a zero β, then by [10, Proposition 3.7.10] it is easily checked that $f(x)/g(x)$ has a corresponding pole of multiplicity at least $p-1$, a contradiction. Therefore, $g(x) = \beta x$ and $f(x) = x + \alpha$, $\alpha, \beta \in \mathbb{K}$. Applying a linear transformation to x, the claim follows.
- Suppose that $\deg(f) < \deg(g)$ and $\deg(g) > 0$. Then, arguing as in the previous case, $f(x) = \alpha$ and $g(x) = \beta x$ with $\alpha, \beta \in \mathbb{K}$. Applying a linear transformation to x, the claim follows.
- Suppose that $\deg(g) = 0$. This is impossible since P_0 is a pole of $f(x)/g(x)$. $\square$

4.1. Proof of Theorems 1.3 and 1.4

We keep our notation introduced in the previous sections. From Proposition 4.3, E_{q^2} contains a subgroup T of order q such that the quotient curve $\mathcal{X}/T$ is the curve $\mathcal{Y}_{L,a}$ with affine equation

$$L(y) = ax + \frac{1}{x},$$

for some $a \in \mathbb{K}^*$ and $L(T) \in \mathbb{K}[T]$ a separable p-linearized polynomial of degree q. Let $\mathbb{K}(x,y)$ be the function field $\mathbb{K}(\mathcal{X}/T)$. From Proposition 4.1, the p-rank of $\mathcal{X}$ is $\gamma = \mathfrak{g} = (q-1)^2$. Thus by Proposition 4.4, $\mathbb{K}(\mathcal{X})$ has a subfield $\mathbb{K}(x,z)$ defined by

$$\tilde{L_1}(z) = b + \frac{1}{x},$$

for some $z \in \mathbb{K}(\mathcal{X})$, $b \in \mathbb{K}$, and $\tilde{L_1}(T) \in \mathbb{K}[T]$ a separable p-linearized polynomial of degree q. Hence, the compositum $\mathbb{K}(x,y,z)$ of $\mathbb{K}(x,y)$ and $\mathbb{K}(x,z)$ is a subfield of $\mathbb{K}(\mathcal{X})$ such that

$$\begin{cases} L(y) = ax + \frac{1}{x}, \\ L_1(z) = b + \frac{1}{x}. \end{cases} \tag{20}$$

Therefore, $\mathbb{K}(x,y,z) = \mathbb{K}(y,z)$ with

$$(L_1(z) - b)L(y) - (L_1(z) - b)^2 = a. \tag{21}$$

From Proposition 4.4, $\mathbb{K}(x,z) = \mathbb{K}(\mathcal{X})^M$ and $\mathbb{K}(x,y) = \mathbb{K}(\mathcal{X})^T$, where $M \neq T$ is an elementary abelian p-subgroup of E_{q^2} of order q. Thus,

$$Gal(\mathbb{K}(\mathcal{X}) \mid \mathbb{K}(y,z)) = Gal(\mathbb{K}(\mathcal{X}) \mid \mathbb{K}(\mathcal{X}/M)) \cap Gal(\mathbb{K}(\mathcal{X}) \mid \mathbb{K}(\mathcal{X}/T)) = M \cap T.$$

Since the cover $\mathcal{X} \to \mathcal{X}/T$ is unramified, we have $M \cap T = \{1\}$ and hence $\mathbb{K}(\mathcal{X}) = \mathbb{K}(y,z)$.

Remark 4.5. Every p-element of $\mathrm{Aut}(\mathcal{X})$ is an element of E_{q^2}.

Proof. Let σ be a p-element of $\mathrm{Aut}(\mathcal{X})$. By Nakajima's bound, Theorem 2.1 (I), $|\langle E_{q^2}, \sigma\rangle| \leq q^2 = |E_{q^2}|$. Therefore $\sigma \in E_{q^2}$. $\square$

Let $z' = z - \delta$, with $L_1(\delta) = b$. Then $\mathbb{K}(y,z) = \mathbb{K}(y,z')$ where

$$L_1(z')L(y) - L_1(z')^2 = a. \tag{22}$$

Up to a $\mathbb{K}$-scaling of z' and y, we can assume that both L_1 and L are monic. Let $\mathcal{Z}$ be the plane curve with affine equation $L_1(Z')L(Y) - L_1(Z')^2 = a$. By Remark 4.5 and Proposition 4.1,

$$E_{q^2} = \{\tau_{\alpha,\beta} : (y,z') \mapsto (y+\alpha, z'+\beta) \mid L(\alpha) = L_1(\beta) = 0\} \leq \mathrm{Aut}(\mathcal{Z})$$

has exactly two short orbits Ω_1 and Ω_2, which have length q and are centered at the points at infinity $P_1 = (1:1:0)$ and $P_2 = (1:0:0)$, respectively. The q distinct tangent lines to $\mathcal{Z}$ at P_1 have equation $\ell_i : Y - Z' = \epsilon_i$, $i = 1,\ldots,q$, and the intersection multiplicity at P_1 of $\mathcal{Z}$ and ℓ_i is equal to the intersection multiplicity at P_1 of the curve $\mathcal{W} : L(Y) - L_1(Z') = 0$ with the line ℓ_i. Since $\mathcal{W}$ has degree q, this implies that $\mathcal{W}$ splits into linear factors $\ell_1, \ell_2, \ldots, \ell_q$. Therefore $L(Y) - L_1(Z') = L_2(Y - Z')$ for some separable p-linearized polynomial $L_2(T) \in \mathbb{K}[T]$ of degree q. Thus, Equation (22) is the equation (3) defining $\mathcal{X}_{(L_1,L_2)}$, up to the formal replacement of $y - z'$ with Y and of z' with bX, where $b^q = a$.

Let $\bar{q}$ be the largest power of p such that $\mathrm{Aut}(\mathcal{X})$ contains a cyclic subgroup C of order $\bar{q} - 1$. Up to conjugation in $\mathrm{Aut}(\mathcal{X})$, C contains the group

$$\Gamma = \{(X,Y) \mapsto (X+\alpha, Y+\beta) \mid L_1(\alpha) = L_2(\beta) = 0\}.$$

Then $\mathcal{X} \in \mathcal{S}_{q|\bar{q}}$ from Theorems 1.1 and 1.2. Thus, Theorem 1.3 is proved.

If $L_1 \neq L_2$, then from Theorem 1.2 $\mathcal{X}_{(L_1,L_2)}$ does not admit any automorphism group $C_2 \times C_2$. Thus, also Theorem 1.4 is proved.

Acknowledgments

This research was supported by the Italian Ministry MIUR, Strutture Geometriche, Combinatoria e loro Applicazioni, PRIN 2012 prot. 2012XZE22K, and by GNSAGA of the Italian INdAM. The authors would like to thank Nazar Arakelian and Gábor Korchmáros for useful comments and suggestions.

References

[1] N. Arakelian, G. Korchmáros, A characterization of the Artin–Mumford curve, J. Number Theory 154 (2015) 278–291.

[2] G. Cornelissen, F. Kato, Equivariant deformation of Mumford curves and of ordinary curves in positive characteristic, Duke Math. J. 166 (2003) 431–470.

[3] G. Cornelissen, F. Kato, Discontinuous groups in positive characteristic and automorphisms of Mumford curves, Math. Ann. 320 (2001) 55–85.

[4] G. Cornelissen, F. Kato, Mumford curves with maximal automorphism group, Proc. Amer. Math. Soc. 132 (2004) 1937–1941.

[5] M. Giulietti, G. Korchmáros, Algebraic curves with many automorphisms, arXiv:1702.08812.

[6] J.W.P. Hirschfeld, G. Korchmáros, F. Torres, Algebraic Curves over a Finite Field, Princeton Ser. Appl. Math., Princeton, 2008.

[7] B. Huppert, Endliche Gruppen. I, Grundlehren Math. Wiss., vol. 134, Springer, Berlin, 1967, xii+793 pp.

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

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

[10] H. Stichtenoth, Algebraic Function Fields and Codes, 2nd edn., Grad. Texts in Math., vol. 254, Springer, Berlin, 2009.

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

[12] G. van der Geer, M. van der Vlugt, Kloosterman sums and the p-torsion of certain Jacobians, Math. Ann. 290 (1991) 549–563.