Journal of Number Theory **72**, 110–136 (1998)
Article No. NT982251

The Group of Automorphisms of the Function Fields of the Curve $x^n + y^m + 1 = 0$

Aristides I. Kontogeorgis*

Department of Mathematics, University of Crete, Heraclion 71409, Crete, Greece
E-mail: kontogar@talos.cc.uch.gr

Communicated by P. Roquette

Received September 10, 1997

We will study the group of automorphisms of the function fields of the curves $x^n + y^m + 1 = 0$, for $n \neq m$. This groups is bigger than $\mu(n) \times \mu(m)$ in case $m \mid n$. If moreover $n-1$ is a power of the characteristic, then the group order exceeds the Hurwitz bound.

1. INTRODUCTION

Let n, m be natural numbers. We will work over an algebraically closed field k whose characteristic p does not divide n and m. Denote by $F_{n,m}$ the function field of the affine curve $x^n + y^m + 1 = 0$. If the genus of $F_{n,m}$ is greater than one then it is well known that the group of automorphisms of $F_{n,m}$ is finite. The aim of this paper is the determination of the group of automorphisms $G_{n,m}$ of the function fields $F_{n,m}$, with genus $g > 1$. It is obvious that the group $\mu(n) \times \mu(m)$, where $\mu(n)$ is the cyclic group of the nth roots of unity, is a subgroup of $G_{n,m}$. The question is if there are more automorphisms. Leopoldt [Le], in arbitrary characteristic, and Tzermias [Tz], in characteristic zero, studied the automorphism group of the Fermat curves, $m = n$. Hyperelliptic curves in zero characteristic were studied by Brandt and Stichtenoth [B–S]. We will exclude these curves from our considerations and assume that $n > 2$. Our tools can not handle the curve with $n = 4$, $m = 3$ which was recently studied in a paper of Klassen and Schaefer [K–S]. Without loss of generality we may also assume that $n > m$ and for the sake of simplicity we suppose that $ch(k) \neq 2, 3$. With the above restrictions we shall prove the following:

* Supported by a grant from I.K.Y.

0022-314X/98 $25.00

THEOREM 1. *The automorphism group* $G_{n,m}$ *of the above curves is* $G_{n,m} = \mu(n) \times \mu(m)$ *if* $m \nmid n$. *In case* $m \mid n$ *and* $n-1$ *is not a power of the characteristic of* k, *the group of automorphisms* $G_{n,m}$ *admits a presentation*

$$G_{n,m} = \langle \sigma, \tau / \sigma^{2m} = 1, \tau^n = 1, \sigma^3 \tau^{-1} = \tau\sigma, \sigma^2 \tau = \tau \sigma^2 \rangle,$$

where the automorphisms σ, τ *are given by*

$$(\sigma(x) = \xi / x, \sigma(y) = y / x^{n/m}) \qquad (\tau(x) = \xi x, \tau(y) = y),$$

where ξ *denotes a primitive* n*th root of unity. Moreover* $G_{n,m}$ *is given as a central extension*

$$1 \to \mu(m) \to G_{n,m} \to D_n \to 1,$$

where D_n *denotes the dihedral group of order* $2n$. *This extension splits if and only if* m *is odd. In this case* $G_{n,m} \cong \mu(m) \times D_n$. *In case* $m \mid n$ *and* $n - 1 = q$ *is a power of the characteristic the group of automorphisms is given as a central extension*

$$1 \to \mu(m) \to G_{n,m} \to \mathrm{PGL}(2, q) \to 1.$$

As in the previous case this extension splits if and only if m *is odd. If* m *is odd* $G_{n,m} \cong \mu(m) \times \mathrm{PGL}(2, q)$. *In case* m *is even the cohomology class* $\alpha \in H^2(\mathrm{PGL}(2, q), \mu(m))$ *corresponding to the above extension is given by*

$$\alpha = res^{-1}_{\mathrm{PGL}(2,q) \to H_2}(\beta),$$

where H_2 *is anyone* 2*-Sylow subgroup,* 2^{f+1} *is its order and* $\beta \in H^2(H_2, \mu(m))$ *is the cohomology class corresponding to the subextension*

$$1 \to \mu(m) \to \pi^{-1}(H_2) \to H_2 \to 1.$$

The group $\pi^{-1}(H_2)$ *admits the following presentation in terms of generators and relations,*

$$\pi^{-1}(H_2) = \begin{cases} \langle R, S / R^{2^f} = S^{2m} = 1, S^3 R^{-1} = RS, \ S^2 R = R S^2 \rangle, \\ \qquad \text{if} \quad 2^f \mid q + 1 = n, \\ \langle R, S / R^{2^f m} = S^2 = 1, S R S^{-1} = R^r \rangle, \\ \qquad \text{if} \quad 2^f \mid q - 1, \end{cases}$$

where r *is the unique solution* $\mathrm{mod}\ 2^f m$ *of the system* $r \equiv 1 \bmod m$, $r \equiv -1 \bmod 2^{f+1}$.

In case of characteristic zero the problem is easy since there is no wild ramification, and the calculation of the automorphism group can be done by bounding its order using the Riemann–Hurwitz formula. In case of arbitrary characteristic, we owe very much to the ideas of Leopoldt [Le]. The case $m \mid n$ and $n-1$ is a power of the characteristic, appears in Henn's paper [He] and is a counterexample of the ordinary Hurwitz bound of the group of automorphisms.

We should keep in mind that the above curve models might be singular at infinity. We will work in the language of places, which correspond to algebraic points at some non-singular projective model of our curve.

2. THE FIELD $F_{n,m}$ AS A KUMMER EXTENSION OF $k(x)$ AND $k(y)$

Let $F_{n,m}$ be the function field of the curve $x^n + y^m + 1 = 0$. $F_{n,m}$ is a Kummer algebraic extension over the $k(x)$ and $k(y)$, or equivalently a cyclic double ramified covering of $\mathbb{P}^1(k)$.

Let $P_{(x=a)}$ ($P_{(y=b)}$ respectively) be the place of $k(x)$ ($k(y)$ respectively) corresponding to the point $x=a$ ($y=b$ respectively) of $\mathbb{P}^1(k)$. We calculate the ramification places using Kummer's criterion ([St] III.7.3, p. 110). The minimal polynomial of the separable extension $[F_{n,m}\colon k(x)]$ is $T^m + (x^n+1)$. Denote by v_p the valuation of $k(x)$ corresponding to place P:

$$v_P(x^n+1) = v_P\left(\prod_{i=1}^{n} (x-\zeta_i)\right) = \begin{cases} 1 & \text{if} \quad P = P_{(x=\zeta_i)} \\ -n & \text{if} \quad P = P_{(x=\infty)} \\ 0 & \text{otherwise;} \end{cases}$$

hence the number r_P of places above P and the corresponding ramification indices e_p are

$$r_P = \begin{cases} 1 & \text{if } P = P_{(x=\zeta_i)} \\ (n,m) & \text{if } P = P_{(x=\infty)} \\ m & \text{otherwise} \end{cases} \qquad e_P = \begin{cases} m & \text{if } P = P_{(x=\zeta_i)} \\ \dfrac{m}{(n,m)} & \text{if } P = P_{(x=\infty)} \\ 1 & \text{otherwise} \end{cases}$$

where $(\zeta_i)_{i=1,\ldots,n}$ are the nth roots of -1. For symmetry reasons between m and n we have

$$r_P = \begin{cases} 1 & \text{if } P = P_{(y=\varepsilon_j)} \\ (n,m) & \text{if } P = P_{(y=\infty)} \\ n & \text{otherwise} \end{cases} \qquad e_P = \begin{cases} n & \text{if } P_{(y=\varepsilon_j)} \\ \dfrac{n}{(n,m)} & \text{if } P_{(y=\infty)} \\ 1 & \text{otherwise} \end{cases}$$

where $(\varepsilon_j)_{j=1,\dots,m}$ are the mth roots of -1. The principal divisors of the two generating functions x, y of the field $F_{n,m}$ are

$$(x)=P_{(x=0)}-P_{(x=\infty)}=\sum_{i=1}^{m}\alpha_i-\frac{m}{(n,m)}\sum_{j=1}^{(n,m)}\gamma_j$$

$$(y)=P_{(y=0)}-P_{(y=\infty)}=\sum_{i=1}^{n}\beta_i-\frac{n}{(n,m)}\sum_{j=1}^{(n,m)}\delta_j,$$

where α_i, γ_j, β_i, δ_j are the extensions, in $F_{n,m}$, of the places $P_{(x=0)}$, $P_{(x=\infty)}\in k(x)$ and $P_{(y=0)}$, $P_{(y=\infty)}\in k(y)$, respectively. We can see, using the defining equation of the curve, that $\gamma_k=\delta_k$. Moreover the different of the separable extension $F_{n,m}/k(x)$ is

$$D(F_{n,m}/k(x))=(m-1)\sum_{i=1}^{n}\beta_i+\left(\frac{m}{(n,m)}-1\right)\sum_{j=1}^{(n,m)}\gamma_j;$$

therefore according to ([Ha], p. 455):

$$\begin{aligned}(dx)&=D(F_{n,m}/k(x))-2(x)_\infty\\&=(m-1)\sum_{i=1}^{n}\beta_i+\left(\frac{m}{(n,m)}-1\right)\sum_{j=1}^{(n,m)}\gamma_j-2\frac{m}{(n,m)}\sum_{j=1}^{(n,m)}\gamma_j.\end{aligned}$$

So we conclude that $2g-2=\deg(dx)=nm-n-m-(n,m)$. A basis for the space of holomorphic differentials of the field $F_{n,m}$ is given by

$$x^iy^j\omega,\qquad (i,j)\in I,$$

where I is the set of indices

$$I:=\left\{(i,j)\in\mathbb{N}^2:\frac{2g-2}{(n,m)}-\frac{im+nj}{(n,m)}\geqslant 0\right\},\tag{1}$$

and

$$\omega:=\frac{dx}{my^{m-1}}=-\frac{dy}{nx^{n-1}}.$$

Indeed, the divisor of the above differential is

$$(\omega)=\frac{2g-2}{(n,m)}\sum_{k=1}^{(n,m)}\gamma_i$$

and

$$(x^i y^j \omega) = \left[\frac{2g-2}{(n,m)} - \frac{im+nj}{(n,m)} \right] \sum_{k=1}^{(n,m)} \gamma_k;$$

hence all the above differentials are holomorphic. Furthermore they are linearly independent and Towse[1] [To] proves that $|I| = g$.

3. CALCULATION OF POLE AND GAP NUMBERS

Define for a place P of the function field $F_{n,m}$ the Weierstrass semigroup

$$E(P) := \{ v \in \mathbb{N} \colon \exists f \in F_{n,m} / (f)_\infty = vP \}.$$

The elements of $E(P)$ are called the pole numbers at P and the elements of $\mathbb{N} \backslash E(P)$ are called the gaps at P. For every divisor D of the function field $F_{n,m}$ we define the finite dimensional k vector space $\mathscr{L}(D) := \{ f \colon (f) + D \geqslant 0 \}$. Set $\ell(D) := \dim_k \mathscr{L}(D)$. Observe that $s \in E(P)$ if and only if $\ell(sP) = \ell((s-1)P) + 1$.

The objective of this section is to calculate a part of the set $E(P)$ for the places $P = \alpha_1$ or β_1. Notice that all α_s, $s = 1, ..., m$, β_t, $t = 1, ..., n$ have the same Weierstrass semigroup. The sets

$$x^i y_1^j \omega \qquad \text{or} \qquad x_1^i y^j \omega \quad (i, j) \in I,$$

where $x_1 = x - \zeta_1$, $y_1 = y - \varepsilon_1$, are also two basis for the space of holomorphic differentials. Moreover it holds

$$v_{\alpha_1}(x^i y_1^j \omega) = i + nj, \qquad v_{\beta_1}(x_1^i y^j \omega) = mi + j.$$

The Riemann–Roch theorem implies that

$$\begin{aligned} s \in E(P) &\Leftrightarrow \ell(sP) = \ell((s-1)P) + 1 \\ &\Leftrightarrow \ell(W - (s-1)P) - \ell(W - sP) = 0, \end{aligned}$$

where W is a canonical divisor of $F_{n,m}$. We take as W the divisor of ω. The dimension of the space $\mathscr{L}(W - sP)$ can be interpreted as the number of linearly independent holomorphic differentials which have a zero at place P of order $\geqslant s$, since

$$\mathscr{L}(W - sP) := \{ f \colon (f) \geqslant -(\omega) + sP \} = \{ (f\omega) \geqslant sP \}.$$

[1] Towse's method does not aply when $m \mid n$, but we can check that this result is also true in this case.

On the other hand, from (1) we have $0 \leqslant i < n$ and $0 \leqslant j < m$, for $(i, j) \in I$, which gives us that the functions

$$\Phi_n : \begin{cases} I \to \mathbb{N} \\ (i, j) \mapsto i + nj + 1 \end{cases} \qquad \Psi_m : \begin{cases} I \to \mathbb{N} \\ (i, j) \mapsto mi + j + 1 \end{cases}$$

are "one to one." Hence the valuations $v_{a_1}(x^i y_1^i \omega)$ take different values for different (i, j) and the same holds for the valuations $v_{\beta_1}(x_1^i y^j \omega)$, so the valuation of an arbitrary holomorphic differential is

$$v_{a_1}\left\{\sum_{(i, j) \in I} \lambda_{i, j} x_1^i y^j \omega\right\} = \min_{\lambda_{i, j} \neq 0} v_{a_1}(\lambda_{i, j} x_1^i y^j \omega) = \min_{(i, j) \text{ such that } \lambda_{i, j} \neq 0} \{i + nj\}.$$

Thus

$$\ell(W - s\alpha_1) = |\{i + nj \geqslant s, (i, j) \in I\}|$$

and similarly

$$\ell(W - s\beta_1) = |\{mi + j \geqslant s, (i, j) \in I\}|.$$

We conclude that $\ell(W - (s-1)\alpha_1) \neq \ell(W - s\alpha_1)$; if and only if there exist $(i, j) \in I : i + nj = s - 1$. The cardinal number of the set $\{i + nj + 1, (i, j) \in I\} = \Phi_n(I)$ is g, so the gaps at place α_1 are $\Phi_n(I)$. Similarly the gaps at place β_1 are $\Psi_n(I)$.

"Small" gap numbers are enough for our needs. We restrict ourselves to gaps at place α_1 which are images, under the function Φ_n, of the set $I_1 = \{(i, 0) \in I\}$. According to (1), $(i, 0) \in I_1$ if and only if

$$i \leqslant n - 1 - \frac{n + (n, m)}{m}. \tag{2}$$

Divide $n + (n, m)$ by m: $n + (n, m) = \kappa m + r$, where $0 \leqslant r < m$. If we set

$$t := \begin{cases} n - \kappa & \text{in case} \quad r = 0 \\ n - \kappa - 1 & \text{in case} \quad r > 0 \end{cases},$$

then from (2) we conclude that $i \leqslant t - 1$. Moreover $n + 1 = \Phi_n((0, 1))$ is a gap for a_1. Finally, the structure of gap and pole numbers of α_1 up to $n + 1$ is

$$0, \ \underbrace{1, 2, ..., t,}_{gaps} \qquad \underbrace{t + 1, ..., n,}_{pole\ numbers} \qquad \underbrace{n + 1,}_{gap} .... \tag{3}$$

Similarly for $P=\beta_1$ we calculate the part of $E(\beta_1)$ which are of the form $\Psi_n((0,j))$, $(0,j)\in I$. Divide $m+(n,m)$ by $n: m+(n,m)=\lambda n+v$, $0\leqslant v<n$. Since $m<n$, λ must be zero or one. As in the study of $E(\alpha_1)$ if we set

$$t' := \begin{cases} m-\lambda & \text{in case} \quad v=0 \\ m-\lambda-1 & \text{in case} \quad v>0 \end{cases}$$

then $j\leqslant t'-1$. Observe that $\lambda=1$ if and only if $v=0$; hence $t'+1=m$ and the structure of gap and pole numbers of β_1, up to $m+1$ is

$$0, \underbrace{1, 2, \ldots, m-1,}_{gaps} \quad \underbrace{m}_{pole\ number}, \quad \underbrace{m+1,}_{gap} \ldots. \tag{4}$$

LEMMA 2. *Let $n=m\kappa_1+r_1$, $0\leqslant r_1<m$, be the division of n by m. The number t is equal to $n-\kappa_1-1$. Furthermore if $m+1<n$ then $m<t+1$. In case $m+1=n$ we have $m=t+1$.*

Proof. There are two cases:

1. $m\mid n$ so $(n,m)=m$. This means that $\kappa=\kappa_1+1$ and $r=0$; thus $t=n-\kappa_1-1$.

2. $m\nmid n$ so $(n,m)<m$. Obviously

$$n+(n,m)=\kappa_1 m+r_1+(n,m).$$

We distinguish the following subcases:

- If $r_1+(n,m)=m$, then $\kappa=\kappa_1+1$, $r=0$ and so $t=n-\kappa_1-1$.
- If $r_1+(n,m)<m$, then $\kappa=\kappa_1$, $r>0$ and so $t=n-\kappa_1-1$.
- The case $r_1+(n,m)>m$ can never happen since $(n,m)\mid r_1$.

At last the inequality $m<t+1$ is equivalent to $(m-r_1)/(m-1)<\kappa_1$, since $m>1$. The left hand side of the above inequality is less than one unless $r_1=0, 1$. So $(m-r_1)/(m-1)\geqslant\kappa_1$ only if $\kappa_1=1$ and $r_1=0, 1$ (recall that $n>m$ so $\kappa_1\geqslant 1$). Hence the equality $t+1=m$ holds if and only if $n=m+1$. ∎

LEMMA 3. *There is no automorphism σ such that: $\sigma(\alpha_i)=\beta_j$.*

Proof. For every place P and for every automorphism $\sigma\in G$ $E(P)=E(\sigma P)$. To prove the assertion we notice that $E(\alpha_1)\neq E(\beta_1)$. Indeed, $m\in E(\beta_1)$ and if $m+1<n$ then by Lemma 2, $m<t+1$ so $m\notin E(\alpha_1)$. In case $m+1=n$, $n\notin E(\beta_1)$ but $n\in E(\alpha_1)$. ∎

LEMMA 4. *If P is a place of $F_{n,m}$ and $P \notin \{\{\alpha_i\}_{i=1,\dots,m} \cup \{\beta_j\}_{j=1,\dots,n} \cup \{\gamma_k\}_{k=1,\dots(n,m)}\}$ then for every automorphism $\sigma \in Aut(F_{n,m})$ holds that $\sigma(P) \notin \{\beta_j\}_{j=1,\dots,n}$.*

Proof. We will prove that $E(P) \neq E(\beta_j)$. For this we will work in $\mathcal{L}(W)^*$, i.e., the space of linear forms:

$$\Phi\colon \mathcal{L}(W) \to k.$$

The place P restricts to finite places $P_{(x=a)}$, $P_{(y=b)}$ of the function fields $k(x)$, $k(y)$, respectively. We set $\tilde{x}=x-a$, $\tilde{y}:=y-b$. The set $\{\tilde{x}^i\tilde{y}^j\omega, (i,j)\in I\}$ forms a basis for the vector space of holomorphic differentials, so every holomorphic differential ω_1 can be written as

$$\omega_1 = \sum_{(i,j)\in I} \gamma_{i,j}\tilde{x}^i\tilde{y}^j\omega, \qquad \gamma_{i,j}\in k.$$

Let T be a local uniformiser of the valuation ring at P. The functions $\tilde{x}$, $\tilde{y}$ can be expressed as formal power series of T:

$$\tilde{x} = \sum_{k\geqslant 1} a_k T^k, \qquad \tilde{y} = \sum_{l\geqslant 1} b_l T^l.$$

Moreover, since the place P is not ramified over the fields $k(x)$, $k(y)$ we have $a_1 b_1 \neq 0$. The s powers of the power series $\tilde{x}$, $\tilde{y}$ are denoted by

$$\tilde{x}^s = \sum_{k\geqslant 1} a_k^{(s)} T^k, \qquad \tilde{y}^s = \sum_{l\geqslant 1} b_l^{(s)} T^l$$

and from the multiplication law of power series we compute

$$\begin{array}{llll} a_k^{(s)} = b_k^{(s)} = 0, & \text{if } k<s\neq 0 & a_k^{(0)} = b_k^{(0)} = 1 & \text{if } k=0 \\ a_s^{(s)} = a_1^s,\, b_s^{(s)} = b_1^s, & \text{if } k=s\neq 0 & a_k^{(0)} = b_k^{(0)} = 0 & \text{if } k>0. \end{array} \tag{5}$$

Define the linear forms

$$\Phi^{(s)} := \begin{cases} \mathcal{L}(W) \to k \\ \omega_1 \mapsto \langle \omega_1, \Phi^{(s)} \rangle := \sum_{(i,j)\in I} \gamma_{i,j}\phi_{i,j}^{(s)}, \end{cases}$$

where

$$\phi_{i,j}^{(s)} := \sum_{k+l=s} a_k^{(i)} b_l^{(j)}, \qquad (i,j)\in I. \tag{6}$$

The arbitrary holomorphic differential is written

$$\omega_1 = \left(\sum_{s \geqslant 0} \langle \omega_1, \Phi^{(s)} \rangle \, T^s \right) \omega.$$

From the selection of the place P we have that $P \nmid (\omega)$ so the vector space $\mathscr{L}(W - sP)$ is characterized by the equations: $0 = \langle \omega, \Phi^{(s_1)} \rangle$, $\forall 0 \leqslant s_1 \leqslant s-1$. It is clear that

$$\mathscr{L}(W - s_1 P) = \operatorname{Ker} \Phi^{(s_1 - 1)} |_{\mathscr{L}(W - (s_1 - 1)\, P)} < \mathscr{L}(W - (s_1 - 1)\, P).$$

Thus $\mathscr{L}(W - (s-1)\, P) \neq \mathscr{L}(W - sP)$ if and only if $\Phi^{(s-1)}$ is linearly independent from the forms $\Phi^{(s_1)}$, $0 \leqslant s_1 \leqslant s-2$; therefore,

$$s \in E(P) \Leftrightarrow \exists \xi_0, ..., \xi_{s-2} \colon \Phi^{(s-1)} = \sum_{k=0}^{s-2} \xi_k \Phi^{(k)}.$$

Notice that every linear form $\Phi^{(s)}$ corresponds to a $1 \times g$ matrix, namely

$$\Phi^{(s)} \leftrightarrow (\phi^{(s)}_{(0,0)}, \phi^{(s)}_{(1,0)}, ..., \phi^{(s)}_{(t-1,0)}, ..., \phi^{(s)}_{(i,j)}, ...) \qquad (i, j) \in I.$$

By (6) and (5) we have that

$$\phi^{(s)}_{i,0} = \sum_{k+l=s} = a^{(i)}_k b^{(0)}_l = a^{(i)}_s,$$

so a left upper square block of the matrix of the first $t-1$ forms is as in the following table.

	$(0,0)$	$(1,0)$	$\cdots$	$(t-1,0)$	$\cdots$
$s=0$	1	0	$\cdots$	0	
$s=1$	$*$	a_1		0	
$\vdots$	$\vdots$	$\vdots$	$\ddots$	0	
$s=t-1$	$*$	$*$		a_1^{t-1}	$*$
$\vdots$	$*$	$*$		$\vdots$	$\ddots$

Hence the first $t-1$ forms $\Phi^{(s)}$ are linearly independent so $1, ..., t \notin E(P)$. In case $m+1 < n$ our assertion is proved. Indeed, $m \in E(\beta_i)$ and by Lemma 2 we have that $m < t+1$ so $m \notin E(P)$ and $E(P) \neq E(\beta_i)$.

Suppose now that $n = m+1$. In order to prove that $E(P) \neq E(\beta)$ we have to calculate a larger part of the semigroup $E(P)$. This calculation is complicated for general n, m. We will use a theorem of Leopoldt concerning function fields of the "allgemein Fermatschen Typus."

THEOREM 5. *Let F/k be a function field with a model in $\mathbb{A}^2(k)$ given by an irreducible polynomial $F_n(x, y) = 0$ of degree $n \geqslant 4$ without any singularities at finite points or at infinity. If P is a place such that $P \nmid (x)_\infty$, $(y)_\infty$, $\mathrm{Diff}(F/k(y)$, $\mathrm{Diff}(F/k(x))$ then $\ell(vP) = 1$ for $v = 0, ..., n-2$. Moreover $\ell((n-1)P) = 2$ if and only if*

$$\text{whenever } \tilde{x} - \theta\tilde{y} \equiv 0 \bmod P^2 \text{ then } \tilde{x} - \theta\tilde{y} \equiv 0 \bmod P^{n-1},$$

where $\theta \in k$, and $\tilde{x} = x - a$, $\tilde{y} = y - b$, $a = x(P)$, $b = y(P)$.

Proof. This is Satz 4 of Leopoldt's paper ([Le], p. 267) together with the characterization of the "allgemein Fermatschen Typus" function fields, in terms of their plane models, done in the discussion in ([Le], pp. 262–263). ∎

Observe that the function fields $F_{m+1,m}$ are function fields of this type since the plane model given by $x^{m+1} + y^m + 1 = 0$ is not singular at the finite points or at infinity. The place $P \nmid (x)_\infty$, $(y)_\infty$, $\mathrm{Diff}(F/k(y)$, $\mathrm{Diff}(F/k(x))$, so Theorem 5 gives us $t + 1 = n - 1 \in E(P)$ if and only if

$$\text{whenever } \tilde{x} - \theta\tilde{y} \equiv 0 \bmod P^2 \text{ then } \tilde{x} - \theta\tilde{y} \equiv 0 \bmod P^{t+1}. \tag{7}$$

Set $y_* := \tilde{y}/b$, $x_* := \tilde{x}/a$ where $a = x(P)$, $b = y(P)$ the algebraic points corresponding to the place P. The defining polynomial $x^{m+1} + y^m + 1$ of the curve can be transformed into

$$(1 + y_*)^m - 1 = \theta_*[(1 + x_*)^{m+1} - 1], \qquad \theta_* = -\frac{a^{m+1}}{b^m} \neq 0, \infty.$$

Therefore, using the binomial theorem we obtain

$$my_* - \theta_*(m+1)\, x_* = -\sum_{v=2}^{m} \left[\binom{m}{v} y_*^v - \theta_* \binom{m+1}{v} x_*^v \right] + \theta_* s_*^n. \tag{8}$$

The elements x_*, y_* are local uniformisers at the place P, so from (8)

$$y_* - \theta_* \frac{m+1}{m} x_* \equiv 0 \qquad \bmod P^2. \tag{9}$$

Assume that $n \geqslant 4$ and $t + 1 = n - 1 \in E(P)$; then using (7) and (9) we have

$$y_* - \theta_* \frac{m+1}{m} x_* \equiv 0 \qquad \bmod P^{t+1}. \tag{10}$$

Notice also that from (9) we have $y_*^v - \theta_*^v(m+1/m)\, x_*^v \equiv 0 \bmod P^v$; therefore using the right hand side of (8) we have the following conditions:

$$\binom{m}{v} \frac{(m+1)^v}{m^v} \theta_*^v - \theta_* \binom{m+1}{v} = 0 \qquad \text{for} \quad v = 1, ..., t+1 = n-1 = m. \tag{11}$$

In case $m > 3(11)$ for $v = 2$ gives

$$\binom{m}{2} \frac{(m+1)^2}{m^2} \theta_*^2 - \theta_* \binom{m+1}{2} = 0.$$

Since $p \nmid m$, $m+1$, $\binom{m+1}{2} \neq 0$ hence $\binom{m}{2} \neq 0$ as well. This gives us $p \nmid m-1$ and so $\theta_* = m^2/(m-1)(m+1)$. We proceed to the next coefficient $v = 3$. We have

$$\binom{m}{3} \frac{(m+1)^3}{m^3} \theta_*^3 - \theta_* \binom{m+1}{3} = 0$$

from which follows that $1 \equiv 0 \bmod p$, a contradiction. Therefore $t+1 = n-1 = m \notin E(P)$ so $E(P) \neq E(\beta)$. We have used that $p \neq 2, 3$ and that $3 < n-1$. So our argument does not work for the curves $x^4 + y^3 + 1 = 0$, $x^3 + y^2 + 1 = 0$ and $x^2 + y + 1 = 0$. We are not interested in the two last curves which have genera 1 and 0, respectively. Klassen and Schaefer [K–S], proved that the curve $x^4 + y^3 + 1 = 0$ has 48 automorphisms.

4. LOCAL STUDY

From now on we will denote by G the group of automorphisms, by F the Fermat function field $F_{n,m}$ and by $G(\beta)$ the decomposition subgroup of G at the place β, where $\beta = \beta_i$ for some $i = 1, ..., n$. Denote by P_ζ the restriction of the place β to the rational function field $k(x)$. The decomposition subgroup is equal to the inertia group $G(\beta) = G_0(\beta)$, since the field of definition k is algebraic closed. We will prove that

$$G(\beta) = \begin{cases} \mu(m) & \text{if} \quad m \nmid n \\ C_{2m} & \text{if} \quad m \mid n,\ n-1 \text{ not a } p\text{-power}, \\ \mathscr{E}_q \rtimes C_{m(q-1)} & \text{if} \quad m \mid n,\ n-1 = q \text{ is a } p\text{-power} \end{cases}$$

where C_x denotes a cyclic group of order x, and $\mathscr{E}_q$ denotes an elementary abelian group of order q.

From the study of the gap structure at the place β we see that the space $\mathscr{L}(m\beta)$ is two dimensional and a basis is given by $\{1, 1/(x-\zeta)\}$. the group $G(\beta)$ leaves the space $\mathscr{L}(m\beta)$ invariant. So $\sigma(1/(x-\zeta)) = \mu + \lambda(1/(x-\zeta))$, $\mu, \lambda \in k$. This gives us that every automorphism $\sigma \in G(\beta)$ leaves the field $k(x)$ invariant. Denote by $\bar{G}(P_\zeta)$ the image of the restriction map

$$Res: \begin{cases} G(\beta) \to \bar{G}(P_\zeta) \\ \sigma \mapsto Res_{k(x)}\, \sigma \end{cases}.$$

Obviously the kernel of the restriction is $\mu(m) \lhd G(\beta)$.

A generating radicand of F over $k(x)$ is of the form $y^\ell z$ where $(\ell, m) = 1$ and $z \in k(x)$ ([Ha1] p. 38). For all $\sigma \in G(\beta)$, $\sigma(k(x)) = k(x)$, so $\sigma(y)$ is also a generating radicand for the extension $F/k(x)$. So $\sigma(y) = y^{\ell_\sigma} z_\sigma$ for an element z_σ in $k(x)$. Let τ be a generator of the cyclic group $\mu(m) = Gal(F/k(x))$. Observe that

$$\sigma^{-1}\tau\sigma = \tau^{\ell_\sigma} \qquad \forall \sigma \in G(\beta). \tag{12}$$

Denote by $G_1(\beta)$ the first ramification group of β. The group $G(\beta) = G_0(\beta)$ can be written as a semidirect product of a cyclic group $E := G_0(\beta)/G_1(\beta)$ of order prime to p by the p-group $G_1(\beta)$. denote by π the projection $G_0(\beta) \to G_0(\beta)/G_1(\beta)$. Take π in both sides of (12)

$$\pi(\sigma^{-1}) \cdot \pi(\tau) \cdot \pi(\sigma) = \pi(\tau)^{\ell_\sigma} \qquad \forall \sigma \in G(\beta).$$

Since E is abelian and $ord(\pi(\tau)) = ord(\tau) = m$ we have that $\ell_\sigma \equiv 1 \bmod m$ so

$$\sigma\tau = \tau\sigma.$$

Moreover, since $\ell_\sigma \equiv 1 \bmod m$, all automorphisms σ of F extending the arbitrary $\sigma_0 \in \bar{G}(P_\zeta)$ are of the form

$$\sigma(y) = \theta_\sigma \cdot y \cdot z_{\sigma_0} \qquad \sigma(x) = \sigma_0(x), \tag{13}$$

where $z_{\sigma_0} \in k(x)$ and θ_σ ranges over the mth roots of unity. This gives us that

$$k(x) \ni z_\sigma^m = \left(\frac{\sigma(y)}{y}\right)^m = \frac{\sigma(x^n+1)}{x^n+1}.$$

Conversely, if $\sigma_0 \in PGL(2, k)$, $\sigma_0(P_\zeta) = P_\zeta$ and $\sigma_0(x^n+1)/(x^n+1) = z_{\sigma_0}^m$ is an mth power for some $z_{\sigma_0} \in k(x)$, then the automorphisms σ of F given by

$$\sigma(y) = \theta y z_{\sigma_0}, \qquad \sigma(x) = \sigma_0(x),$$

are extending σ_0. We have proved the following

LEMMA 6. *Let P_ζ be the restriction of the place β in $k(x)$. An element $\sigma_0 \in PGL(2,k)$ such that $\sigma_0(P_\zeta)=P_\zeta$ is extendible into an automorphism of F if and only if $\sigma(x^m+1)$ differs from x^n+1 by an mth power factor z^m only. The extensions of σ_0 to F are given by* (13).

According to Lemma 6 we have to determine those automorphisms σ of $k(x)$ which leave P_ζ fixed and for which

$$\sigma(x)^n+1=z^m\cdot(x^n+1) \qquad \text{with} \quad z\in k(x). \tag{14}$$

It suffices to know that this relation holds up to a constant factor in $k(x)$, because k is algebraically closed and each element in k is an mth power. Thus instead of (14) we require the relation

$$\sigma(x)^n+1=c\cdot z^m\cdot(x^n+1) \qquad \text{with} \quad c\in k,\, z\in k(x). \tag{15}$$

This is equivalent to the corresponding relation for the principal divisors of the functions involved. The principal divisor of x^n+1 is (denote for simplicity $P_{\zeta_i}=P_{(x=\zeta_i)}$)

$$(x^n+1)=\sum_{1\leqslant i\leqslant n} P_{\zeta_i}-nP_\infty. \tag{16}$$

Notice that every automorphism σ of $k(x)$ which is extendible to F permutes the places of $k(x)$ which are ramified in $F/k(x)$ with the same degree.

The ramified places for $F/k(x)$ are, first, the points P_{ζ_i}, which have common ramification degree m. Second, the point P_∞ has ramification degree $m/(n,m)$.

LEMMA 7. *Every automorphism $\sigma\in G(\beta)$ that fixes P_∞ is the identity.*

Proof. Let $\sigma_0=\sigma|_{k(x)}$, such that $\sigma(P_\infty)=P_\infty$. Then from (16) we have that the principal divisors of the functions $\sigma(x^n+1)$, x^n+1 are equal; thus (15) holds with $z\in k$. Moreover since σ_0 leaves P_∞ fixed we have

$$\sigma_0(x)=a+bx \qquad \text{with} \quad a,b\in k,\, b\neq 0.$$

Consequently,

$$\sigma(x)^n+1=(a+bx)^n+1=c\cdot(x^n+1).$$

We expand the left hand side according to the binomial formula. Since $p\nmid n$ there is at least one intermediate binomial coefficient $\binom{n}{i}\neq 0$, where

$0 < i < n$. Comparing the coefficient of x^i on both sides of the above equation we see that

$$\binom{n}{i} a^{n-i} b^i = 0$$

which gives $a = 0$, i.e., $\sigma(x) = bx$. Hence σ leaves not only P_∞ fixed but also P_0. So σ_0 fixes three points of $k(x)$ and consequently $\sigma = 1$. ∎

To study $\bar{G}(P_\zeta)$ we have to distinguish three cases:

Case (i). $1 < (n, m) < m$. In this case, P_∞ is the only place of $k(x)$ which has ramification degree $m/(n, m)$; hence P_∞ is fixed under every extendible automorphism σ_0 which fixes P_ζ. So by lemma 7 we have that $\bar{G}(P_\zeta) = 1$.

Case (ii). $(n, m) = m$, i.e., $m \mid n$. In this case a nontrivial extendible automorphism σ of $k(x)$ which fixes P_ζ is given by

$$\sigma(x) = \frac{\zeta^2}{x}, \tag{17}$$

where $\zeta^n = -1$. For, since $\zeta^{2n} = 1$ we have

$$\sigma(x)^n + 1 = \frac{1}{x^n} + 1 = \frac{1 + x^n}{x^n}.$$

We see that (15) holds with $c = 1$ and $z = 1/x^{n/m}$; note that $m \mid n$ in Case (ii). The automorphism given by (17) permutes P_∞ and P_0.

Every other automorphism $\sigma \in \bar{G}(P_\zeta)$ permutes the primes P_{ζ_i} because these are precisely the primes which ramify in F, with ramification degree m. We put

$$P_\eta = \sigma(P_\infty)$$

with $\eta \notin \{\zeta_1, ..., \zeta_n\}$. We assume that $\eta \neq \infty$ because otherwise P_∞ is fixed under σ and hence $\sigma = 1$ by Lemma 7. We compute

$$\begin{aligned}\sum_{1 \leqslant i \leqslant n} \sigma(P_{\zeta_i}) - n\sigma(P_\infty) &= \sum_{1 \leqslant i \leqslant n} P_{\zeta_i} - nP_\eta \\ &= n(P_\infty - P_\eta) + \sum_{1 \leqslant i \leqslant n} P_{\zeta_i} - nP_\infty.\end{aligned}$$

Here, $P_\infty - P_\eta$ is the principal divisor of the function $1/(x-\eta)$. It follows that (15) holds with $z=(1/(x-\eta))^{n/m}$. (Recall that $m \mid n$ in Case (ii).) On the other hand, since $\sigma(P_\infty)=P_\eta$ we see that σ is of the form

$$\sigma(x)=\frac{a+bx}{x-\eta}. \tag{18}$$

Substituting in (15) and multiplying with $(x-\eta)^n$ we obtain

$$(a+bx)^n+(x-\eta)^n=c\cdot(x^n+1) \tag{19}$$

as a necessary and sufficient condition for σ to be extendible to F. As above, let $0<i<n$ such that $\binom{n}{i}\neq 0$. Comparing coefficients of x^i on both sides of (19) we see that

$$a^{n-i}b^i=-(-\eta)^{n-i}. \tag{20}$$

If $\eta=0$ then $a\neq 0$ (otherwise $\sigma=1$) and thus $b=0$. Since σ leaves P_ζ fixed, the specialization $x\mapsto\zeta$ implies $\sigma(x)\mapsto\zeta$ which means $a=\zeta^2$. Hence if $\eta=0$ we obtain the involution already found in (17).

Now assume that $\eta\neq 0$; then $a\neq 0$ and $b\neq 0$ according to (20). Suppose that there exists an i such that both $\binom{n}{i}\neq 0$ and $\binom{n}{i+1}\neq 0$. Then Eq. (20) holds simultaneously for i and $i+1$. Taking quotients we have that $ab^{-1}=-\eta$ and so in view of (18), $\sigma(x)=b(x-\eta)/(x-\eta)=b$, a contradiction. Hence, if there should exist a nontrivial automorphism $\sigma\in\bar{G}(P_\zeta)$, which is different from the involution (17) there do not exist two successive intermediate binomial coefficients $\binom{n}{i}$, $\binom{n}{i+1}$ which are both $\neq 0$.

Lemma 8. *If for all $i=1,\ldots,n-2$,*

$$\binom{n}{i}\neq 0\Rightarrow\binom{n}{i+1}=0$$

and $p\nmid n$ then $n=1+q$ where q is a p-power.

Proof. Denote by $a=\sum a_i p^i$, $b=\sum b_i p^i$, $0\leqslant a_i, b_i<p$, the p-adic expansions of two integer numbers a, b. if $a_i\leqslant b_i$ for all i then we write $a\leqslant_p b$. It is known that $\binom{n}{i}\neq 0$ if and only if $i\leqslant_p n$ ([Sch], p. 73). Let $n=n_0+n_1q_1+\cdots+n_sq_s$ be the p-adic expansion of n, where $q_i=p^{s_i}$ and $0<n_i<0$. Observe that $q_i\leqslant_p n$ and $1+q_1\leqslant_p n$ so $\binom{n}{q_i}\neq 0$ and $\binom{n}{1+q_i}\neq 0$. From the condition of the lemma we have that $n-2<q_i$. Since the characteristic is prime to n, $s=1$ and $n-1=q_1$. ∎

Using Lemma 8 we deduce that *in Case* (ii), *if* $n-1$ *is not a power of the characteristic* p, *then* $\bar{G}(P_\zeta)$ *is of order* 2, *containing only the involution given by* (17).

It remains to discuss Case (ii) when $n-1=q$ is a p-power. It is convenient to replace the Kummer radicand by another radicand for $F/k(x)$ which will be easier to handle. Let us put

$$t := \frac{\zeta}{x-\zeta}; \qquad \text{hence} \quad x = \zeta \cdot \frac{t+1}{t} \tag{21}$$

and

$$u := -t^n(x^n+1). \tag{22}$$

Since $m \mid n$, we have that t^n is an mth power and hence u is an admissible radicand for the Kummer extension $F/k(x)$. Without any restriction of generality we might assume that $\zeta = \zeta_1$. The principal divisor of u is

$$\begin{aligned}(u) &= n \cdot (t) + (x^n+1) = n(P_\infty - P_\zeta) + \sum_{1 \leqslant i \leqslant n} P_{\zeta_i} - nP_\infty \\ &= \sum_{2 \leqslant i \leqslant n} P_{\zeta_i} - (n-1)\, P_\zeta.\end{aligned}$$

Now we know in Case (ii) that the P_{ζ_i} are permuted under $\sigma \in \bar{G}(P_\zeta)$, and P_ζ is kept fixed. Hence the principal divisor of u is fixed under σ.

By definition of t we have $k(x) = k(t)$, and the pole of t is P_ζ. The element u has P_ζ as only pole, of order $n-1=q$. Consequently, u is a polynomial in t, of degree q. It is easy to compute that polynomial explicitly, using (21) and (22), keeping in mind that $n = q+1$:

$$u = -t^n\left(\frac{\zeta^n (t+1)^n}{t^n} + 1\right) = (t+1)^n - t^n = t^q + t + 1.$$

It is convenient to change the variable t so that the form of the above polynomial is simplified. Namely, we put $t = a_1 + b_1 t_1$ with $a_1, b_1 \in k$ such that $a_1^q + a_1 = -1$ and $b_1^q = -b_1$, with $b_1 \neq 0$. Then we put $u_1 = -b_1^{-1} u$ and have

$$u_1 = t_1^q - t_1.$$

Now let us change notation: we write t instead of t_1 and u instead of u_1. We have seen that, *in Case* (ii) *with* $n = q+1$ *there exists a generator* t *of* $k(x) = k(t)$ *which has* P_ζ *as its pole, and such that the polynomial* $u = t^q - t$

is a radicand for $F/k(t)$. *The principal divisor of* u *is kept fixed under every* $\sigma \in \bar{G}(P_\zeta)$.

Now every $\sigma \in \bar{G}(P_\zeta)$ leaves the pole of t fixed and hence is of the form

$$\sigma(t) = a + bt,$$

with $a, b \in k$ and $b \neq 0$. Such an automorphism is in $\bar{G}(P_\zeta)$ if and only if $\sigma(u) = cu$ where $0 \neq c \in k$, which means

$$\sigma(t)^q - \sigma(t) = (a+bt)^q - (a+bt) = c \cdot (t^q - t),$$

with $c \neq 0 \in k$. This yields the conditions

$$a^q = a, \qquad c = b, \qquad b^q = b.$$

Hence, *in Case* (ii) *with* $n = q+1$, *the group* $\bar{G}(P_\zeta)$ *consists precisely of those transformations* $t \mapsto a + bt$ *whose coefficients* a, b *are contained in the field* $\mathbb{F}_q$ *of* q*-elements. This group is isomorphic to the group of matrices*

$$\begin{pmatrix} 1 & 0 \\ a & b \end{pmatrix} \qquad \textit{with} \quad a, b \in \mathbb{F}_q,\ b \neq 0.$$

In particular we see that the order of $\bar{G}(P_\zeta)$ *is* $(q-1)q$.

Case (iii). $(n, m) = 1$. In this case the $n+1$ places $P_{\zeta_1}, ..., P_{\zeta_n}, P_\infty$ are precisely the places which are ramified in F, and they all have ramification degree m. Every $\sigma \in \bar{G}(P_\zeta)$ leaves P_ζ fixed and hence permutes the $P_{\zeta_2}, ..., P_{\zeta_n}, P_\infty$.

Let $\sigma(P_\infty) = P_\eta$. If $\eta = \infty$ then from Lemma 7 we see that $\sigma = 1$. Now suppose $\sigma \neq 1$ which means that $\eta \in \{\zeta_2, ..., \zeta_n\}$. The principal divisor of $x^n + 1$ is mapped under σ onto the divisor

$$\sum_{1 \leqslant i \leqslant n} \sigma(P_{\zeta_i}) - nP_\eta.$$

In the above sum the term P_η does not appear, whereas one term P_∞ appears. If we subtract from this the principal divisor of $x^n + 1$ then we obtain

$$\left(\frac{\sigma(x^n+1)}{x^n+1}\right) = (n+1)(P_\infty - P_\eta). \tag{23}$$

The right hand side is the principal divisor of the function $(1/(x-\eta))^{n+1}$. On the other hand, we know that the right hand side is the divisor of the mth power of such a function. We obtain

$$m \mid n+1$$

as a necessary condition for the existence of a nontrivial automorphism in $\bar{G}(P_\zeta)$.

Equation (23) gives us that

$$\sigma(x)^n = \frac{c(x^n+1)-(x-\eta)^{n+1}}{(x-\eta)^{n+1}}, \qquad \text{where} \quad c \in k.$$

The principal divisor of the polynomial $f(x) := c(x^n+1)-(x-\eta)^{n+1}$, which is of degree $n+1$, is

$$\sum_{1 \leqslant i \leqslant n} A_i + P_\eta - (n+1)\, P_\infty,$$

where A_i, P_η are the places, not necessarily different, corresponding to the roots of $f(x)$. On the other hand the principal divisor of $(x-\eta)^{n+1}$ is $(n+1)(P_\eta - P_\infty)$ and this gives us that the principal divisor of $\sigma(x)^n$ is

$$(\sigma(x)^n) = \sum_{1 \leqslant i \leqslant n} A_i - nP_\eta.$$

Therefore the polynomial $f(x)$ has a multiple root of order n. Let ρ be this root; then

$$f(x) = c(x^n+1)-(x-\eta)^{n+1} = c_1 \cdot (x-\eta)(x-\rho)^n, \tag{24}$$

for some $c_1 \in k$. We distinguish two cases:

Case (a). $\rho = 0$. Then (24) becomes

$$c(x^n+1)-(x-\eta)^{n+1} = c_1(x-\eta)\, x^n = c_1 x^{n+1} - c_1 \eta x^n. \tag{25}$$

We extract the left hand side using the binomial formula

$$\begin{aligned} c(x^n+1)-(x-\eta)^{n+1} = & -x^{n+1} + (-(n+1)(-\eta)+c)\, x^n \\ & - \sum_{i=1}^{n-1} \binom{n+1}{i} (-\eta)^{n+1-i} x^i + c - (-\eta)^{n+1}. \end{aligned}$$

By comparing the coefficients of the x^{n+1} in both sides of (25) we obtain $c_1 = -1$. By comparing the coefficients of x^n and the constant term we have that $c = \eta$. Furthermore for all $i = 1, ..., n$ we have that

$$\binom{n+1}{i} = 0,$$

which in view of the nonvanishing criterion of a binomial coefficient given in Lemma 8 gives us that $n+1 = q$ is a power of the characteristic p. But this is impossible since $m \mid n+1$ and $(m, p) = 1$.

Case (b). $\rho \neq 0$. We observe that $(x-\rho)^{n-1}$ divides the polynomial

$$g(x) := (n+1)\, f(x) - \frac{df(x)}{dx}(x-\eta) = c(x^n + n\eta x^{n-1} + (n+1)).$$

Moreover we have that η is a root of $g(x)$, since $\eta^n = -1$, so for a constant c' we have

$$c(x^n + n\eta x^{n-1} + (n+1)) = c'(x-\eta)(x-\rho)^{n-1}. \tag{26}$$

By comparing the coefficients of x^n in both sides of (26) we deduce that $c' = c$. Comparing the coefficients of x and x^2 in both sides of (26) we obtain

$$(-\rho)^{n-2}\,(-\rho - \eta(n-1)) = 0 \Rightarrow -\rho = (n-1)\,\eta \tag{27}$$

and

$$(-\rho)^{n-3}\left(-\eta\binom{n-1}{2} - \rho(n-1)\right) = 0. \tag{28}$$

We substitute (27) into (28) to get

$$(-\rho)^{n-3}\,\eta\,\frac{(n-1)\,n}{2} = 0,$$

a contradiction, since from (27) $n-1 \neq 0$ (recall that we have assumed for the characteristic $p \neq 2$ and $p \nmid n$).

We have found so far all the elements in group $G(\beta)$. This group is of order

$$|\bar{G}(P_\zeta)| \cdot |\mu(m)| = \begin{cases} m & \text{if } \; m \nmid n \\ 2m & \text{if } \; m \mid n \text{ and } n-1 \text{ is not a } p \text{ power.} \\ mq(q-1) & \text{if } \; m \mid n \text{ and } n-1 = q \text{ is a } p \text{ power} \end{cases}$$

Moreover, in the first two cases the order of $G(\beta)$ is prime to the characteristic of the field p (recall that we have assumed $p \neq 2$), so $G(\beta)$ is isomorphic to a cyclic group of order m (respectively $2m$). In last case the group $G(\beta)$ is the semidirect product of a cyclic group of order $m(q-1)$ by a normal elementary abelian group of order q [Se, p. 68].

5. STRUCTURE OF THE GROUP OF AUTOMORPHISMS

Denote by $O(\beta, G)$ the orbit of the place β under the action of G. In this section we will calculate the order of $|G|$ counting the order of $O(\beta, G)$. We have determined which places of F cannot be in the orbit of β (Lemmata 3 and 4); therefore

$$O(\beta, G) \subseteq \{\beta_1, \beta_2, ..., \beta_n, \gamma_1, \gamma_2, ..., \gamma_{(n,m)}\}.$$

Notice that all $\beta_i \in O(\beta, G)$ for all $i = 1, ..., n$ and if $\gamma_{i_0} \in O(\beta, G)$ for some i_0 then $\gamma_i \in O(\beta, G)$ for all places γ_i $i = 1, ..., (n, m)$ above P_∞.

Case (1). Suppose that $m \mid n$. The involution σ given by (17) sends a place γ_i over P_∞ to some place α_j over P_0. This gives us that $O(\beta, G) = \{\beta_1, \beta_2, ..., \beta_n\}$, for if there was a $\tau \in G$ such that $\tau(\beta) = \gamma_i$ then $\tau\sigma(\beta) = \alpha_j$ which is impossible due to Lemma 3. Therefore the order of G, in this case, is given by

$$|G| = |G : G(\beta)| \cdot |G(\beta)| = |0(\beta, G)| \cdot |G(\beta)|$$
$$= \begin{cases} 2nm & \text{if} \quad n-1 \text{ is not a power of } p \\ nmq(q-1) & \text{if} \quad n-1 \text{ is a power of } p. \end{cases}$$

Case (2). Suppose now that $m \nmid n$. Then $|O(\beta, G)| = n$ or $n + (n, m)$. Suppose that $|O(\beta, G)| = n + (n, m)$ and let $H := \mu(n) \times \mu(m)$. Obviously the order of the orbit of β under the action of H is $|O(\beta, H)| = |H : H(\beta)| = n$. We have proved that $|G(\beta)| = \mu(m) = |H(\beta)|$ so

$$\frac{n + (n, m)}{n} = \frac{|G : G(\beta)|}{|H : H(\beta)|} = \frac{|G|}{|H|} \in \mathbb{N}.$$

From the left hand side of the above equation we obtain that $n \mid (n, m)$, a contradiction since $n > m$. So $|O(\beta, G)| = n$ and the group G has order

$$|G| = |O(\beta, G)| \cdot |G(\beta)| = nm.$$

We will now give a group theoretic description of the group of automorphisms. Suppose first that $m \nmid n$. In this case the group G is the direct product of the groups $\mu(n)$ and $\mu(m)$, since $|G| = n \cdot m$ and $\mu(n) \times \mu(m) \geqslant G$.

Suppose now that $m \mid n$. Observe first that $\mu(m) < Z(G)$. Indeed, let G_1 be the subgroup of G generated by all products $x \cdot y$, $x \in G(\beta)$, $y \in \mu(n)$ The group $G_1 < G$ has at least $|G(\beta)| \cdot |\mu(n)| = |G|$ elements, since $G(\beta) \cap \mu(n) = 1$. So $|G_1| = |G|$ and obviously $G_1 = G$. This gives us the desired result, because the elements of $\mu(m)$ are commuting with elements of $G(\beta)$ and $\mu(n)$.

Since $\mu(m) \lhd G$ every automorphism $\sigma \in G$ can be restricted into an automorphism of the rational function field $k(x) = F^{\mu(m)}$. Thus the restriction map given above can be extended to a map

$$\mathscr{F}: \begin{cases} G \to \mathscr{F}(G) < PGL(2, k) \\ \sigma \mapsto res_{k(x)}\, \sigma. \end{cases}$$

Obviously the kernel of $\mathscr{F}$ is $\ker \mathscr{F} = \mu(m)$. We distinguish two more cases:

Case (i). $n-1$ is not a power of p. Then according to the calculation of the order of G, the order of $\mathscr{F}(G)$ is $2n$. Notice that the group $\mathscr{F}(G)$ contains the cyclic group $\mu(n)$ generated by $\tau_0 \colon x \mapsto \zeta^2 x$ and the involution $\sigma_0 \colon x \mapsto \zeta^2/x$. Since $\sigma_0 \notin \langle \tau_0 \rangle = \mu(n)$ and $\sigma_0 \tau_0 = \tau_0^{-1} \sigma_0$, the group generated by σ_0, τ_0 is a dihedral group of order $2 \cdot n$. This is the order of the group $\mathscr{F}(G)$, so $\mathscr{F}(G) \cong D_n$ and the group G is given as a central extension of D_n with abelian kernel $\mu(m)$.

The decomposition group is generated by

$$\sigma: \begin{cases} y \mapsto \dfrac{y}{x^{n/m}} \\[2ex] x \mapsto \dfrac{\zeta^2}{x} \end{cases}$$

since σ is of order $2m$. the group $\mu(n) < G$ is generated by

$$\tau: \begin{cases} y \mapsto y \\ x \mapsto \zeta^2 x \end{cases}$$

and we can check that the group G admits a presentation

$$\langle \sigma, \tau / \sigma^{2m} = 1, \tau^n = 1, \sigma^3 \tau^{-1} = \tau\sigma, \sigma^2 \tau = \tau \sigma^2 \rangle.$$

Observe that if a central extension with abelian kernel splits, i.e., it corresponds to the trivial cohomology class, then G is the direct product of the groups involved. We will prove that the extension

$$1 \to \mu(n) \to G \to D_n \to 1 \tag{29}$$

splits, i.e., $G \cong \mu(n) \times D_n$ if and only if m is odd.

Suppose first that m is odd. We will use the fact that the map

$$H^2(D_n, \mu(m)) = \bigoplus_{p \mid 2n} H^2(D_n, \mu(m))_p \to \bigoplus_{p \mid 2n} H^2(H_p, \mu(m))$$

$$a = \sum_{p \mid 2n} a_p \mapsto \sum_{p \mid 2n} res_{(D_n \to H_p)}\, a_p,$$

where H_p runs through all p-Sylow subgroups of D_n is injective [Wei, p. 93]. If $p = 2$ then $(|H_2|, m) = 1$ so $res_{(D_n \to H_2)}\, a_2 = 1$ by the Zassenhaus theorem [Hu, p. 126]. On the other hand if H_p is a p-Sylow subgroup for $p \neq 2$, then $res_{(D_n \to H_p)} a_p = 1$ since $H_p < \mu(n)$ and the subextension

$$1 \to \mu(m) \to G_1 \to \mu(n) \to 1$$

splits.

In case m is even the extension which gives G does not split. For this consider the subgroup generated by the involution σ given by (17) and the subextension given by the following diagram:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mu(m) & \longrightarrow & G & \xrightarrow{\pi} & D_n & \longrightarrow & 1 \\ & & \| & & \uparrow & & \uparrow & & \\ 1 & \longrightarrow & \mu(m) & \longrightarrow & \pi^{-1}(\langle\sigma\rangle) & \longrightarrow & \langle\sigma\rangle & \longrightarrow & 1 \end{array}$$

Let $a \in H^2(D_n, \mu(m))$ be the cohomology class which corresponds to the extension G. To the subextension $\pi^{-1}(\langle\sigma\rangle)$ corresponds the cohomology class $res_{(D_n \to \langle\sigma\rangle)}\, a$ [Wei, p. 213]. But $\pi^{-1}(\langle\sigma\rangle) = G(\beta)$ which is a cyclic group of order $2m$. So $res_{(D_n \to \langle\sigma\rangle)}\, a \neq 1$ since a cyclic group of order $2m$ is not isomorphic to $\mu(m) \times \langle\sigma\rangle$ in case $2 \mid m$.

Case (ii). $n - 1 = p^s = q$, is a power of the characteristic. We claim that $\mathscr{F}(G) < PGL(2, q^2)$. We take as generator of the field $k(x)$ the element t defined above. We have proved that $\mathscr{F}(G(\beta)) = \bar{G}(P_\zeta)$ is a group of Möbius transformations of the form $t \mapsto a + bt$, $a, b \in \mathbb{F}_q \subset \mathbb{F}_{q^2}$. Elements in $\mu(n)$ are defined over $\mathbb{F}_{q^2}$ as well. Indeed, in the change of coordinates $x \mapsto t$ we have involved ζ, a_1, b_1 which are in $\mathbb{F}_{q^2}$ since

$$b_1^q = -b_1 \Rightarrow b_1^{q^2} = b_1 \qquad (q \text{ is odd})$$

$$\zeta^n = -1 \Rightarrow \zeta^{q+1} = -1 \Rightarrow \zeta^q = -\frac{1}{\zeta} \Rightarrow \zeta^{q^2} = \zeta$$

$$a_1^q = -1 - a_1 \Rightarrow a_1^{q^2} = (-1 - a_1)^q = (-1)^q + (-1)^q a_1^q = a_1,$$

therefore the change of coordinates $x \mapsto t$ is a Möbius transformation in $PGL(2, q^2)$. On the other hand $\mathcal{F}(\mu(n))$ is generated by the automorphism $x \mapsto \zeta^2 x$ which is in $PGL(2, q^2)$.

The order of $\mathcal{F}(G)$ is $q(q-1)(q+1)$. We will prove that the unique subgroup of $PGL(2, q^2)$ of order $q(q-1)(q+1)$ is $PGL(2, q)$. For this we will use the following characterization of subgroups of projective linear groups found in [V–M, p. 165].

THEOREM 9. *The group $PGL(2, p^f)$ has only the following subgroups*:

1. *Elementary abelian p-groups*
2. *Cyclic groups of order t with $t \mid p^f \pm 1$.*
3. *Dihedral groups of order $2t$, $t \mid p^f \pm 1$.*
4. *Groups isomorphic to A_4, S_4, A_5.*
5. *Semidirect products of elementary abelian groups of order p^r with cyclic groups of order t, where $t \mid p^r - 1$ and $t \mid p^f - 1$.*
6. *Groups isomorphic to* $\mathrm{PSL}(2, p^r)$ *and* $\mathrm{PGL}(2, p^r)$ *where $r \mid f$.*

We will use this theorem and the fact that $|\mathcal{F}(G)| = q(q^2-1)$, where $q = p^s$ is a power of the characteristic, to describe the group structure of $\mathcal{F}(G)$. First $\mathcal{F}(G)$ is not a p-group, so it is not an elementary abelian group. Suppose that $\mathcal{F}(G)$ is isomorphic to a cyclic group of order t, $t \mid p^f \pm 1$. Then $|\mathcal{F}(G)| = p^s(p^{2s}-1)$ divides $p^f \pm 1$, a contradiction, since $p \nmid 1$. For the same reason $\mathcal{F}(G)$ is not a dihedral group. The three groups A_4, S_4, A_5 have order less than or equal to 60. On the other hand $|\mathcal{F}(G)| = q(q^2-1) \geqslant 120$ since $p \geqslant 5$. So $\mathcal{F}(G) \not\cong A_4, S_4, A_5$. Suppose now that $\mathcal{F}(G)$ is the semidirect product of an elementary abelian group of order p^r with a cyclic group of order $t = p^{s-r}(p^{2s}-1)$. The number t must divide both $p^r - 1$ and $p^f - 1$, which is again a contradiction. Finally if $\mathcal{F}(G) \cong \mathrm{PSL}(2, p^r)$ then $r \mid f = 2s$ and

$$|\mathrm{PSL}(2, r)| = \frac{(p^{2r}-1)\, p^r}{2} = (p^{2s}-1)\, p^s,$$

another contradiction. The only remaining possibility for $\mathrm{Im}(\mathcal{F}) \cong \mathrm{PGL}(2, q)$.

The group G is a central extension of $\mathrm{PGL}(2, q)$ with kernel $\mu(m)$ given by the exact sequence

$$1 \to \mu(m) \to G \xrightarrow{\pi} \mathrm{PGL}(2, q) \to 1. \tag{30}$$

Using the universal coefficient theorem, the values of the Schur multiplier $H_2(\mathrm{PGL}(2, q), \mathbb{Z})$ and the abelianization of $\mathrm{PGL}(2, q)$ [Br, p. 26] we can compute

$$H^2(\mathrm{PGL}(2, q), \mu(m)) = \begin{cases} 0 & \text{if} \quad m \equiv 1 \bmod 2 \\ \mathbb{Z}_2 \oplus \mathbb{Z}_2 & \text{if} \quad m \equiv 0 \bmod 2. \end{cases}$$

This gives us that for m odd the group G is isomorphic to

$$G \cong \mu(m) \times \mathrm{PGL}(2, q).$$

For m even the situation is more complicated. To describe the structure of G it is enough to determine the cohomology class $a \in H^2(\mathrm{PGL}(2, q), \mu(m))$ which corresponds to the central extension (30). The restriction map

$$\begin{aligned} \mathbb{Z}_2 \otimes \mathbb{Z}_2 &= H^2(\mathrm{PGL}(2, q), \mu(m)) \\ &= H^2(\mathrm{PGL}(2, q), \mu(m))_{(2)} \to H^2(H_2, \mu(m)), \end{aligned}$$

to anyone 2-Sylow subgroup H_2 of $\mathrm{PGL}(2, q)$, is injective [Wei, p. 93]. Therefore the cohomology class $\alpha \in H^2(\mathrm{PGL}(2, q), \mu(m))$ is determined by the cohomology class $\beta := res_{\mathrm{PGL}(2, q) \to H_2}(\alpha)$ of the corresponding sub-extension

$$1 \to \mu(m) \to \pi^{-1}(H_2) \to H_2 \to 1. \tag{31}$$

To calculate the cohomology class $\beta \in H^2(H_2, \mu(m))$ we will describe first the structure of the group $\pi^{-1}(H_2)$. From Theorem 9, since the characteristic $p \neq 2$, we have that H_2 is isomorphic to a dihedral group D_k, $k = 2^f$. Observe that $(q-1, q+1) = 2$ since $2 \,|m|\, q+1$. So $k = 2^f$, for $f > 1$ divides either $q-1$ or $q+1$ (recall that the order of $\mathrm{PGL}(2, q) = q(q-1)(q+1)$). Moreover, it is known that in the extension $k(x)/k(x)^{\mathrm{PGL}(2, q)}$ only two places p_1, p_2 of $k(x)^{\mathrm{PGL}(2, q)}$ ramify, with corresponding ramification indices $e_1 = q(q-1)$ and $e_2 = q+1$. The places of $k(x)$ over p_1 are $P_{\zeta_1}, \ldots, P_{\zeta_n}$ and the set of places of $k(x)$ over p_2 are in the orbit $O(\mathrm{PGL}(2, q), P_{(x=0)})$ of $P_{(x=0)}$ under the action of $\mathrm{PGL}(2, q)$.

Suppose that the group H_2 is given in terms of generators and relations as

$$H_2 = \langle \rho, \sigma / \rho^{2^f} = \sigma^2 = (\rho\sigma)^2 = 1 \rangle.$$

The element $\rho \in H_2$ of order 2^f fixes a place over p_1 or p_2. We distinguish the following two cases: (notice that if $f = 1$, the two cases coincide)

Case (a). $2^f | q+1=n$. Then ρ fixes two places of $k(x)$, which belong to the $O(\mathrm{PGL}(2,q), P_{(x=0)})$. We can choose the 2-Sylow subgroup H_2 to be a subgroup of the group $D_n=\langle \sigma_0, \tau_0\rangle$ defined above. Therefore $\pi^{-1}(H_2)$ admits a presentation

$$\langle R, S / R^{2^f} = S^{2m} = 1, S^3 R^{-1} = RS, S^2 R = RS^2 \rangle.$$

Let ϕ be a section of H_2 in $\pi^{-1}(H_2)$, defined by $\phi(\rho^i \sigma^j) = R^i S^j$. The representative cocycle, which corresponds to the section ϕ, of the cohomology class β is given by

$$b = \begin{cases} H_2 \times H_2 \to \mu(m) \\ (x, y) \mapsto \phi(x)\,\phi(y)\,\phi(xy)^{-1}. \end{cases}$$

For $x=\rho^i\sigma^j$, $y=\rho^{i'}\sigma^{j'}$, arbitrary elements of H_2 we calculate

$$b(x,y) = \begin{cases} 0 & \text{if } \ j=0 \\ S^{2i'} & \text{if } \ j\neq 0 \end{cases}$$

(recall that $\mu(m)=\langle S^2\rangle$).

Case (b). $2^f | q-1$. In this case ρ fixes two places among the P_{ζ_i}. The group $\pi^{-1}(\langle\rho\rangle)$ is a subgroup of the decomposition group $G(\beta_i)$ for some i. Since $(ord(\pi^{-1}(\langle\rho\rangle)), p)=1$ we have that $\pi^{-1}(\langle\rho\rangle)$ is cyclic so we can choose a preimage $R\in\pi^{-1}(\rho)$ of order $2^f m$ in $\pi^{-1}(H_2)$. Observe that $\pi^{-1}(\langle\sigma\rangle$ is abelian and isomorphic to $\mu(m)\times\langle\sigma\rangle$, since σ fixes a place $k(x)$ which does not ramify in the extension $F/k(x)$. Therefore we can choose $S\in\pi^{-1}(\sigma)$, such that $S^2=1$. Since $[\pi^{-1}(H_2):\langle R\rangle]=2$ the group $\langle R\rangle$ is normal in $\pi^{-1}(H_2)$. This gives us the relation $SRS^{-1}=S^r$, for some r. The group $\pi^{-1}(H_2)$ is given by

$$\pi^{-1}(H_2) = \langle R, S / R^{2^f m} = S^2 = 1, SRS^{-1} = S^r \rangle.$$

To determine r we notice first that $R^{2^f}\in\mu(m)$; hence

$$R^{2^f} = SR^{2^f}S^{-1} = R^{r2^f}, \qquad \text{so} \quad R \equiv 1 \bmod m.$$

Moreover

$$SRS^{-1}R = R^{r+1} \in \mu(m), \qquad \text{so} \quad r \equiv -1 \bmod 2^f.$$

The above system, since $(2^f, m)=2$, has two solutions modulo $2^f m$, r_0 and $r_1 = r_0 + 2^{f-1}m$.

The fixed places of every element in H_2 of the form $\sigma\rho^i$, are in $O(\mathrm{PGL}(2,q), P_{(x=0)})$. So $\sigma\rho^i$ is a conjugate with the involution $x \overset{\tau_o^{n/2}}{\mapsto} \zeta^n x$ in

$\mu(n)$. We have that the groups $\pi^{-1}(\langle \rho\sigma^i \rangle) \cong (\langle \sigma \rangle) \cong \mu(m) \times \mathbb{Z}_2$. Since, $(m, 2) = 2$, every preimage of every element in H_2 of the form $\rho\sigma^i$ has order t such that $(t, 2) = 2$. On the other hand $(SR)^2 = S^{r+1}$ has order

$$\frac{2^f m}{(r+1, m2^f)} = \frac{m}{\left(\dfrac{r+1}{2^f}, m\right)}$$

which must be odd. So $((r+1)/2^f, m) = 2$ which gives us that 2^{f+1} divides $r+1$. 2^{f+1} cannot divide both solutions r_0 and r_1. So r is uniquely determined mod $2^f m$ as the solution of the system

$$r \equiv 1 \bmod m, \qquad r \equiv -1 \bmod 2^{f+1}.$$

Let ϕ be the section of H_2 in $\pi^{-1}(H_2)$ defined in part (a). In this case the representative cocycle is given by

$$b(\rho^i\sigma^j, \rho^{i'}\sigma^{j'}) = \begin{cases} 1 & \text{if } \ j = 0 \\ R^{i'(r+1)} & \text{if } \ j = 1 \end{cases}$$

(recall that $2^f \mid r+1$ and $\mu(m) = \langle R^{2^f} \rangle$).

ACKNOWLEDGMENTS

I express my gratitude to my advisor, Jannis A. Antoniadis, for his continued support, guidance, and encouragement. I am indebted also to Professor P. Roquette for the valuable suggestions he made for the improvement of my manuscript. Finally I thank the Greek national Scholarship Foundation (I.K.Y.) for their financial support.

REFERENCES

[B–S] R. Brandt and H. Stichtenoth, Die Automorphismengruppen Hyperelliptischer Kurben, *Manuscripta Math.* **55** (1986), 83–92.

[Br] R. Brandt, "Über die Automorphismengruppen von algebraischen Funktionenkörper," Ph.D. thesis, Universität-Gesamthochschule Essen, 1988.

[Ha] H. Hasse, "Zahlentheorie," Akademie-Verlag, Berlin, 1969.

[Ha1] H. Hasse, Theorie der relativ-zyklischen algebraischen Funtionenkörper, insbesondere bei endlichen Konstantenkörper, *J. Reine Angew. Math.* **172** (1934), 37–54.

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

[Hu] B. Huppert, "Endliche Gruppen I," Grundlehren der Mathematischen Wissenschaften, Band 134, Springer-Verlag, Berlin, 1967.

[K–S] M. J. Klassen and E. F. Schaefer, Arithmetic and geometry of the curve $y^3 + 1 = x^4$, *Acta Arithmetica* **74** (1996), 241–257.

[Le] H. W. Leopoldt, Über die Automorphismengruppe des Fermatkörpers, *J. Number Theory* **56** (1996), 256–282.

[Se] J. P. Serre, "Local Fields," Graduate Texts in Mathematics, Vol. 67, Springer-Verlag, New York, 1979.

[Sch] F. K. Schmidt, Die Wronskische Determinante in beliebigen differenzierbaren Funktionenkörpern, *Math. Z* **45** (1939), 62–74.

[St] H. Stichtenoth, "Algebraic Function Fields and Codes," Universitext, Springer-Verlag, Berlin, 1993.

[To] C. W. Towse, "Weierstrass Points on Cyclic Covers of the Projective Line," Ph.D. thesis, Brown University, 1993.

[Tz] P. Tzermias, The group of automorphisms of the Fermat curve, *J. Number Theory* **53** (1995), 173–178.

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

[Wei] E. Weiss, "Cohomology of Groups," Academic Press, New York, 1969.