Compositio Mathematica **120:** 137–170, 2000.

On Subfields of the Hermitian Function Field

ARNALDO GARCIA[1],* HENNING STICHTENOTH[2]*
and CHAO-PING XING[3]*
[1]*Instituto de Matématica Pura e Aplicada IMPA, 22460-320 Rio de Janeiro RJ, Brazil.*
e-mail: garcia@impa.br
[2]*Universität GH Essen, FB 6, Mathematik u. Informatik, 45117 Essen, Germany.*
e-mail: stichtenoth@uni-essen.de
[3]*Department of Mathematics, University of Science and Technology of China, Hefei, Anhui 230026, P.R. China; and Department of Information Systems and Computer Science, The National University of Singapore, 10 Lower Kent Ridge Crescent, Singapore 119260.*
e-mail: xingcp@iscs.nus.edu.sg

(Received: 8 May 1998; accepted in final form: 14 September 1998)

Abstract. The Hermitian function field $H = K(x, y)$ is defined by the equation $y^q + y = x^{q+1}$ (q being a power of the characteristic of K). Over $K = \mathbb{F}_{q^2}$ it is a maximal function field; *i.e.* the number $N(H)$ of $\mathbb{F}_{q^2}$-rational places attains the Hasse–Weil upper bound $N(H) = q^2+1+2g(H)\cdot q$. All subfields $K \subsetneqq E \subseteq H$ are also maximal. In this paper we construct a large number of nonrational subfields $E \subseteq H$, by considering the fixed fields $H^{\mathcal{G}}$ under certain groups $\mathcal{G}$ of automorphisms of H/K. Thus we obtain many integers $g \geqslant 0$ that occur as the genus of some maximal function field over $\mathbb{F}_{q^2}$.

Mathematics Subject Classifications (1991): 11Gxx, 14Gxx

Key words: function fields, rational places, finite fields.

1. Introduction

Let K be a finite field, F/K an algebraic function field over K of genus $g(F)$. By the Hasse–Weil theorem, the number $N(F)$ of rational places of F/K is bounded by $N(F) \leqslant \#K + 1 + 2g(F) \cdot \sqrt{\#K}$. The function field is said to be *maximal* if $N(F)$ attains this upper bound. We are interested in the following question: Which integers $g \geqslant 0$ happen to be the genus of some maximal function field over K?

Suppose that the cardinality of K is not a square and that F/K is maximal. From the equality $N(F) = \#K + 1 + 2g(F) \cdot \sqrt{\#K}$ follows that $g(F) = 0$, hence F is the rational function field over K. Therefore we will always assume that $\#K$ is a square. We fix some notation.

* The first and second authors were partially supported by GMD-CNPq, the third author was supported by DFG.

p is a prime number.
$q = p^n$ is some power of p (with $n \geqslant 1$).
$K = \mathbb{F}_{q^2}$ is the finite field with q^2 elements.
$K^\times = K \setminus \{0\}$ is the multiplicative group of K.
F is a function field over K, and K is algebraically closed in F.
$g(F)$ is the genus of F/K.
$N(F)$ is the number of rational places (places of degree one) of F/K.
$\mathbb{P}(F)$ is the set of all places of F/K.

By definition, F/K is maximal if and only if

$$N(F) = q^2 + 1 + 2g(F) \cdot q. \tag{1.1}$$

Our main problem can be stated as follows: Describe the set

$$\Gamma(q^2) = \{g \geqslant 0 \mid \text{there exists a maximal function field } F/K \text{ of genus } g(F) = g\}. \tag{1.2}$$

A well-known example of a maximal function field over $K = \mathbb{F}_{q^2}$ is the *Hermitian* function field H; it is defined by

$$H = K(x, y) \quad \text{with } y^q + y = x^{q+1}. \tag{1.3}$$

The genus of H is $g(H) = q(q-1)/2$, the number of rational places is $N(H) = q^3+1 = q^2+1+2g(H)\cdot q$, cf. [St 1, VI.4.4]. One can show that any function field over K of genus $g > q(q-1)/2$ is not maximal, and that the Hermitian function field is the only maximal function field of genus $g = q(q-1)/2$. In particular, $\Gamma(q^2)$ is a finite set. More precisely, one knows that

$$\Gamma(q^2) \subseteq [0, (q-1)^2/4] \cup \{q(q-1)/2\}, \tag{1.4}$$

see [R–St], [X–St], [F–T].

Any subfield $E \subseteq F$ of a maximal function field F/K (with $K \subsetneqq E$) is maximal [La], so all subfields of the Hermitian function field H provide examples of maximal function fields over K. In this paper we will construct systematically a large variety of subfields $E \subseteq H$ which can be obtained as fixed fields of some subgroups of the automorpism group $\mathcal{A}ut(H)$. We will determine the genera of these subfields E (thus finding many numbers $g \in \Gamma(q^2)$), and in some cases we will describe E explicitly by generators and equations.

2. Places and Automorphisms of H

We recall some known facts about the Hermitian function field H (as defined in (1.3)) that we will use in subsequent sections, cf. [St 1, VI.4.4].

https://doi.org/10.1023/A:1001736016924 Published online by Cambridge University Press

The extension $H/K(x)$ is Galois of degree $[H: K(x)] = q$. The pole of x in $K(x)$ is totally ramified in H, and we denote by $P_\infty \in \mathbb{P}(H)$ the unique pole of x in H; *i.e.* x has pole divisor $(x)_\infty = qP_\infty$. All other rational places of $K(x)$ split completely in $H/K(x)$, thus we have $N(H) = 1 + q^3$ rational places in H/K.

We will also need the number of places of H/K of degree 2 and 3.

LEMMA 2.1. *For all* $r \geqslant 1$ *let* $B_r = \#\{P \in \mathbb{P}(H) \mid \deg P = r\}$. *Then*

$$B_1 = N(H) = q^3 + 1; \qquad B_2 = 0; \qquad B_3 = \tfrac{1}{3}q^3(q+1)(q^2-1).$$

Proof. It is clear that $B_1 = N(H) = q^3 + 1$. From the maximality of H/K follows that the numerator $L_H(t)$ of the Zeta function of H is

$$L_H(t) = \prod_{i=1}^{2g(H)} (1 - \omega_i t),$$

with $\omega_i = -q$ for $i = 1, \ldots, 2g(H)$. Setting

$$S_r := \sum_{i=1}^{2g(H)} \omega_i^r = (-1)^r (q-1) q^{r+1},$$

we obtain [St 1, V.2.9] for $r \geqslant 2$:

$$B_r = \frac{1}{r} \sum_{d \mid r} \mu\left(\frac{r}{d}\right)(q^{2d} - S_d).$$

(μ denotes the Möbius function.) In particular,

$$\begin{aligned} B_2 &= \tfrac{1}{2}(-(q^2 - S_1) + (q^4 - S_2)) \\ &= \tfrac{1}{2}(-q^2 - (q-1)q^2 + q^4 - (q-1)q^3) = 0, \end{aligned}$$

and

$$\begin{aligned} B_3 &= \tfrac{1}{3}(-(q^2 - S_1) + (q^6 - S_3)) \\ &= \tfrac{1}{3}(-q^2 - (q-1)q^2 + q^6 + (q-1)q^4) = \tfrac{1}{3}q^3(q+1)(q^2-1). \qquad \square \end{aligned}$$

The automorphism group of the Hermitian function field,

$$\mathcal{A} := \mathcal{A}ut(H) = \{\sigma\colon H \to H \mid \sigma \text{ is an automorphism of } H/K\}$$

is extremely large [St 3], [Le]. It is isomorphic to the projective unitary group $\mathrm{PGU}(3, q^2)$ and has order

$$\operatorname{ord} \mathcal{A} = q^3(q^2-1)(q^3+1). \tag{2.1}$$

We describe $\mathcal{A}$ in some detail: The subgroup

$$\mathcal{A}(P_\infty) = \{\sigma \in \mathcal{A} \mid \sigma P_\infty = P_\infty\} \subseteq \mathcal{A}$$

consists of all automorphisms σ with

$$\begin{aligned} &\sigma(x) = ax + b, \qquad \sigma(y) = a^{q+1}y + ab^q x + c, \\ &a \in K^\times, \quad b \in K, \quad c^q + c = b^{q+1}. \end{aligned} \tag{2.2}$$

It has order

$$\text{ord } \mathcal{A}(P_\infty) = q^3(q^2 - 1). \tag{2.3}$$

Let

$$\mathcal{A}_1(P_\infty) = \{\sigma \in \mathcal{A}(P_\infty) \mid \sigma x = x + b \text{ for some } b \in K\}.$$

Then $\mathcal{A}_1(P_\infty)$ is the unique p-Sylow subgroup of $\mathcal{A}(P_\infty)$, it contains all automorphisms with

$$\begin{aligned} &\sigma x = x + b, \qquad \sigma y = y + b^q x + c, \\ &b \in K, \quad c^q + c = b^{q+1}, \end{aligned} \tag{2.4}$$

and its order is

$$\text{ord } \mathcal{A}_1(P_\infty) = q^3. \tag{2.5}$$

The factor group $\mathcal{A}(P_\infty)/\mathcal{A}_1(P_\infty)$ is cyclic of order $q^2 - 1$; it is generated by the automorphism $\epsilon \in \mathcal{A}(P_\infty)$ with

$$\epsilon(x) = ax, \qquad \epsilon(y) = a^{q+1}y, \tag{2.6}$$

where $a \in K$ is a primitive $(q^2 - 1)$th root of unity.

Another automorphism $\omega \in \mathcal{A}$ is given by

$$\omega(x) = \frac{x}{y}, \qquad \omega(y) = \frac{1}{y}. \tag{2.7}$$

This element ω is an involution (i.e. $\text{ord}(\omega) = 2$), and $\mathcal{A}$ is generated by $\mathcal{A}(P_\infty)$ and ω; i.e.

$$\mathcal{A} = \langle \mathcal{A}(P_\infty), \omega \rangle . \tag{2.8}$$

Let $\mathcal{G} \subseteq \mathcal{A}$ be a subgroup of $\mathcal{A}$; we denote by $H^{\mathcal{G}}$ its fixed field,

$$H^{\mathcal{G}} = \{z \in H \mid \sigma z = z \quad \text{for all} \quad \sigma \in \mathcal{G}\}.$$

https://doi.org/10.1023/A:1001736016924 Published online by Cambridge University Press

Then $H/H^{\mathcal{G}}$ is a Galois extension of degree $[H\colon H^{\mathcal{G}}] = \mathrm{ord}(\mathcal{G})$, and $\mathcal{G}$ is the Galois group of $H/H^{\mathcal{G}}$. Since $2g(H) = q(q-1)$, the Hurwitz genus formula gives

$$q^2 - q - 2 = \mathrm{ord}(\mathcal{G}) \cdot (2g(H^{\mathcal{G}}) - 2) + \deg \mathrm{Diff}(H/H^{\mathcal{G}}), \tag{2.9}$$

where $\mathrm{Diff}(H/H^{\mathcal{G}})$ is the different of $H/H^{\mathcal{G}}$. For a place $P \in \mathbb{P}(H)$ let $Q = P \cap H^{\mathcal{G}}$ be the restriction of P to $H^{\mathcal{G}}$, and we denote by

$$e(Q) := e(P|Q) \quad (\text{resp. } d(Q) := d(P|Q))$$

the ramification index (resp. the different exponent) of $P|Q$. Thus

$$\deg \mathrm{Diff}(H/H^{\mathcal{G}}) = \mathrm{ord}(\mathcal{G}) \cdot \sum_{Q \in \mathbb{P}(H^{\mathcal{G}})} \frac{d(Q)}{e(Q)} \cdot \deg Q,$$

and we obtain from (2.9) that

$$q^2 - q - 2 = \mathrm{ord}(\mathcal{G}) \cdot \left(2g(H^{\mathcal{G}}) - 2 + \sum_{Q \in \mathbb{P}(H^{\mathcal{G}})} \frac{d(Q)}{e(Q)} \cdot \deg Q \right). \tag{2.10}$$

PROPOSITION 2.2. *The fixed field $H^{\mathcal{A}}$ is rational, and exactly two places of $H^{\mathcal{A}}$ are ramified in H. One of the ramified places is the place $Q_\infty := P_\infty \cap H^{\mathcal{A}}$; this place is wildly ramified in $H/H^{\mathcal{A}}$ with ramification index*

$$e(Q_\infty) = e(P_\infty \mid Q_\infty) = q^3(q^2 - 1)$$

and different exponent

$$d(Q_\infty) = d(P_\infty \mid Q_\infty) = q^5 + q^2 - q - 2.$$

The conjugates of P_∞ under $\mathcal{A}$ are exactly all rational places of H.

The other ramified place is the place $\tilde{Q} := \tilde{P} \cap H^{\mathcal{A}}$, where $\tilde{P} \in \mathbb{P}(H)$ is any place of degree three. This place $\tilde{Q}$ is a rational place of $H^{\mathcal{A}}$, and it is tamely ramified in $H/H^{\mathcal{A}}$ with $e(\tilde{Q}) = e(\tilde{P}|\tilde{Q}) = q^2 - q + 1$. The conjugates of $\tilde{P}$ under $\mathcal{A}$ are exactly all places of H of degree three.

Proof. As the extension $H/K(x)$ is Galois, $H^{\mathcal{A}}$ is contained in $K(x)$, and hence $H^{\mathcal{A}}$ is also rational. In order to determine the ramification index and the different exponent of $P_\infty \mid Q_\infty$ we use Hilbert's ramification theory, cf. [St 1, Ch.III.8]. By definition, the group $\mathcal{A}(P_\infty) = \{\sigma \in \mathcal{A} \mid \sigma P_\infty = P_\infty\}$ is the decomposition group of $P_\infty \mid Q_\infty$, so

$$e(P_\infty \mid Q_\infty) = \mathrm{ord}\, \mathcal{A}(P_\infty) = q^3(q^2 - 1)$$

https://doi.org/10.1023/A:1001736016924 Published online by Cambridge University Press

by (2.3) (note that $\mathcal{A}(P_\infty)$ is also the inertia group since $\deg P_\infty = 1$).

The different exponent $d(P_\infty \mid Q_\infty)$ can be calculated as follows: Let v_{P_∞} be the discrete valuation of H associated to P_∞, and choose a P_∞-prime element t, i.e. $v_{P_\infty}(t) = 1$. For $1 \neq \sigma \in \mathcal{A}(P_\infty)$ set

$$i(\sigma) = v_{P_\infty}(\sigma(t) - t); \tag{2.11}$$

then

$$d(P_\infty \mid Q_\infty) = \sum_{1 \neq \sigma \in \mathcal{A}(P_\infty)} i(\sigma)$$

by [St 1, Prop. III.5.12 and Thm. III.8.8]. In our situation we have (2.2)

$$\sigma(x) = ax + b, \qquad \sigma(y) = a^{q+1}y + ab^q x + c,$$

with $a \in K \setminus \{0\}$ and $b \in K$, and we can choose the prime element $t = x/y$. So

$$\begin{aligned} i(\sigma) &= v_{P_\infty}\left(\frac{ax+b}{a^{q+1}y + ab^q x + c} - \frac{x}{y}\right) \\ &= v_{P_\infty}((ax+b)y - x(a^{q+1}y + ab^q x + c)) - 2v_{P_\infty}(y) \\ &= v_{P_\infty}((a - a^{q+1})xy - ab^q x^2 + by - cx) + 2(q+1) \\ &= \begin{cases} 1, & \text{if } a \neq 1, \\ 2, & \text{if } a = 1 \text{ and } b \neq 0, \\ q+2, & \text{if } a = 1 \text{ and } b = 0 \text{ (and } c \neq 0). \end{cases} \end{aligned} \tag{2.12}$$

Hence

$$\begin{aligned} d(P_\infty | Q_\infty) &= (q^2 - 2) \cdot q^3 + (q^2 - 1) \cdot q \cdot 2 + (q-1)(q+2) \\ &= q^5 + q^2 - q - 2. \end{aligned}$$

As the number of conjugates of P_∞ under $\mathcal{A}$ is equal to the index $(\mathcal{A} : \mathcal{A}(P_\infty)) = q^3 + 1 = N(H)$, all rational places of H are $\mathcal{A}$-conjugate. Now all assertions of Proposition 2.2 concerning P_∞ are settled.

We substitute $e(Q_\infty)$ and $d(Q_\infty)$ into formula (2.10) and find after some computation that

$$\sum_{Q \neq Q_\infty} \frac{d(Q)}{e(Q)} \cdot \deg Q = \frac{q^2 - q}{q^2 - q + 1}. \tag{2.13}$$

This implies that exactly one place $\tilde{Q} \in \mathbb{P}(H^{\mathcal{A}})$ with $\tilde{Q} \neq Q_\infty$ ramifies in $H/H^{\mathcal{A}}$, that $\deg \tilde{Q} = 1$ and that $\tilde{Q}$ is tamely ramified (otherwise the left-hand side of (2.13) would be $\geqslant 1$). Moreover it follows that $e(\tilde{Q}) = q^2 - q + 1$ (since $d(\tilde{Q}) = e(\tilde{Q}) - 1$).

In order to show that any place $\tilde{P} \in \mathbb{P}(H)$ lying above $\tilde{Q}$ has degree three, we consider the group $\mathcal{B} :=$ inertia group of $\tilde{P}$ in $H/H^{\mathcal{A}}$. The group $\mathcal{B}$ is cyclic of order $\operatorname{ord}(\mathcal{B}) = q^2 - q + 1$. Let $\tilde{R} = \tilde{P} \cap H^{\mathcal{B}}$ be the restriction of $\tilde{P}$ to the fixed field $H^{\mathcal{B}}$ of $\mathcal{B}$. As all places of H/K of degree one lie above Q_∞, and as there are no places of degree two (by Lemma 2.1), we conclude that

$$\deg \tilde{R} = \deg \tilde{P} \geqslant 3. \tag{2.14}$$

The Hurwitz genus formula (2.10), applied to the extension $H/H^{\mathcal{B}}$, yields

$$q^2 - q - 2 = (q^2 - q + 1)\left(2g(H^{\mathcal{B}}) - 2 + \sum_{R \in \mathbb{P}(H^{\mathcal{B}})} \frac{e(R) - 1}{e(R)} \deg R\right).$$

From this equation and (2.14) we conclude easily that $g(H^{\mathcal{B}}) = 0$, that $\tilde{R}$ is the only ramified place in $H/H^{\mathcal{B}}$, and that $\deg \tilde{R} = \deg \tilde{P} = 3$.

The number of places of H lying above the place $\tilde{Q} = \tilde{P} \cap H^{\mathcal{A}}$ is equal to

$$\frac{\operatorname{ord}(\mathcal{A}) \cdot \deg \tilde{Q}}{e(\tilde{P}|\tilde{Q}) \cdot \deg \tilde{P}} = \frac{q^3(q^2 - 1)(q^3 + 1)}{(q^2 - q + 1) \cdot 3} = \tfrac{1}{3} q^3 (q + 1)(q^2 - 1),$$

and this is exactly the number of places of H of degree three, by Lemma 2.1. Hence all places of H of degree three are conjugate under $\mathcal{A}$, and Proposition 2.2 is completely proved. □

In the proof of Proposition 2.2 we have also established:

COROLLARY 2.3. *Let $\tilde{P} \in \mathbb{P}(H)$ be a place of degree three and $\mathcal{B} \subseteq \mathcal{A}$ be the inertia group of $\tilde{P}$ with respect to the extension $H/H^{\mathcal{A}}$. Then the fixed field $H^{\mathcal{B}}$ is rational, the extension $H/H^{\mathcal{B}}$ is cyclic of degree $[H\colon H^{\mathcal{B}}] = q^2 - q + 1$, and $\tilde{P}$ is totally ramified in $H/H^{\mathcal{B}}$. All other places of $H^{\mathcal{B}}$ are unramified in $H/H^{\mathcal{B}}$.*

There is another useful description of the Hermitian function field $H = K(x, y)$ as follows: Choose elements $a, b \in K$ such that $a^q + a = b^{q+1} = -1$, and set

$$u = \frac{y + a}{x}, \qquad v = \frac{b(y + a + 1)}{x}.$$

Then $H = K(u, v)$, and one checks easily that

$$u^{q+1} + v^{q+1} + 1 = 0. \tag{2.15}$$

https://doi.org/10.1023/A:1001736016924 Published online by Cambridge University Press

3. The Fixed Fields of p-Subgroups $\mathcal{U} \subseteq \mathcal{A}$

We maintain all notations from Section 2. Let $\mathcal{U} \subseteq \mathcal{A}$ be a p-subgroup of $\mathcal{A}$. We consider the fixed field $H^{\mathcal{U}}$ of H under $\mathcal{U}$ and want to determine its genus $g(H^{\mathcal{U}})$.

Since $\mathcal{A}_1(P_\infty)$ is a p-Sylow subgroup of $\mathcal{A}$ and any two p-Sylow subgroups are conjugate, we will assume w.l.o.g. that $\mathcal{U} \subseteq \mathcal{A}_1(P_\infty)$. We identify an automorphism $\sigma \in \mathcal{A}_1(P_\infty)$ with the pair $\sigma = [b, c] \in K \times K$ where

$$\sigma x = x + b, \qquad \sigma y = y + b^q x + c \quad \text{and} \quad c^q + c = b^{q+1}, \tag{3.1}$$

see (2.4). The group operation on such pairs is then given by

$$[b_1, c_1] \cdot [b_2, c_2] = [b_1 + b_2, b_1 b_2^q + c_1 + c_2]. \tag{3.2}$$

The identity is the pair $[0, 0]$, the inverse of $[b, c]$ is $[b, c]^{-1} = [-b, b^{q+1} - c]$. The map $\varphi\colon \mathcal{U} \to K$ given by

$$\varphi([b, c]) = b \tag{3.3}$$

is a homomorphism into the additive group of K and we set

$$\mathcal{V}_{\mathcal{U}} = \mathrm{Im}(\varphi), \qquad \mathcal{W}_{\mathcal{U}} = \{c \in K \mid [0, c] \in \mathcal{U}\}. \tag{3.4}$$

These are additive subgroups of K, and $\mathcal{W}_{\mathcal{U}} \simeq \mathrm{Ker}(\varphi)$. Hence

$$\text{ord } \mathcal{U} = p^{v+w}, \quad \text{where } p^v = \text{ord } \mathcal{V}_{\mathcal{U}} \quad \text{and} \quad p^w = \text{ord } \mathcal{W}_{\mathcal{U}}. \tag{3.5}$$

Now we determine the genus $g(H^{\mathcal{U}})$. It is easily seen that P_∞ is the only place of H which is ramified in the extension $H/H^{\mathcal{U}}$, the Hurwitz genus formula (2.10) then yields

$$q^2 - q - 2 = \text{ord } \mathcal{U} \cdot \big(2g(H^{\mathcal{U}}) - 2\big) + d(P_\infty), \tag{3.6}$$

where $d(P_\infty)$ denotes the different exponent of P_∞ in the extension $H/H^{\mathcal{U}}$. We have (with $i(\sigma)$ as in (2.11))

$$\begin{aligned} d(P_\infty) &= \sum_{1 \neq \sigma \in \mathcal{U}} i(\sigma) \\ &= 2(\text{ord } \mathcal{U} - \text{ord } \mathcal{W}_{\mathcal{U}}) + (q + 2)(\text{ord } \mathcal{W}_{\mathcal{U}} - 1) \\ &= 2(p^{v+w} - p^w) + (q + 2)(p^w - 1) \end{aligned} \tag{3.7}$$

by (2.12). Substituting this into (3.6), we obtain

$$g(H^{\mathcal{U}}) = \tfrac{1}{2} p^{n-v}(p^{n-w} - 1). \tag{3.8}$$

In particular, $H^{\mathcal{U}}$ is a rational function field if and only if one of the following (pairwise equivalent) conditions holds

(i) $\mathrm{ord}(W_{\mathcal{U}}) = q$.

https://doi.org/10.1023/A:1001736016924 Published online by Cambridge University Press

(ii) $\mathcal{U} \supseteq \{[0, c] \mid c^q + c = 0\}$.
(iii) $H^{\mathcal{U}} \subseteq K(x)$.

PROPOSITION 3.1. *Let $q = p^n$ and $\mathcal{U}$ be a p-subgroup of $\mathcal{A}$ such that the fixed field $H^{\mathcal{U}}$ is not rational. Then $g(H^{\mathcal{U}}) = \frac{1}{2}p^{n-v}(p^{n-w} - 1)$, with $0 \leqslant w \leqslant n-1$ and $0 \leqslant v \leqslant n$.*

Proof. Since $g(H^{\mathcal{U}})$ is an integer, all assertions follow immediately from (3.8). □

We show now that the above numerical conditions on v and w are also sufficient for the existence of such a subfield of H, if the characteristic of K is odd.

THEOREM 3.2. *Let $q = p^n$ with $p \neq 2$, and let $g \geqslant 1$ be an integer. Then the following assertions are equivalent.*

(i) *There exists a p-subgroup $\mathcal{U} \subseteq \mathcal{A}$ such that $g = g(H^{\mathcal{U}})$.*
(ii) *There are integers v, w such that $0 \leqslant w \leqslant n-1$, $0 \leqslant v \leqslant n$ and $g = \frac{1}{2}p^{n-v}(p^{n-w} - 1)$.*

Proof. It remains to show that (ii) implies (i). One checks immediately that the set $\mathcal{C} = \{[b, c] \in \mathcal{A}_1(P_\infty) \mid b \in \mathbb{F}_q\}$ is an Abelian subgroup of $\mathcal{A}_1(P_\infty)$ of order $\operatorname{ord} \mathcal{C} = q^2$. For $j \geqslant 1$ and $[b, c] \in \mathcal{A}_1(P_\infty)$ holds

$$[b, c]^j = \left[jb, jc + \frac{j(j-1)}{2} b^{q+1} \right]. \tag{3.9}$$

Since the characteristic p of K is odd, we conclude that all nontrivial automorphisms $\sigma \in \mathcal{A}_1(P_\infty)$ have order p. It follows that $\mathcal{C}$ is a $\mathbb{F}_p$-vector space of dimension $2n$. The space

$$\mathcal{Z} = \{[0, c] \in \mathcal{A}_1(P_\infty) \mid c^q + c = 0\}$$

is an n-dimensional subspace of $\mathcal{C}$ (in fact, $\mathcal{Z}$ is the center of $\mathcal{A}_1(P_\infty)$). We choose $\mathbb{F}_p$-subspaces $\mathcal{V}, \mathcal{W} \subseteq \mathcal{C}$ with

$$\mathcal{W} \subseteq \mathcal{Z}, \qquad \dim_{\mathbb{F}_p} \mathcal{W} = w, \qquad \mathcal{V} \cap \mathcal{Z} = 0 \quad \text{and} \quad \dim_{\mathbb{F}_p} \mathcal{V} = v.$$

Then $\mathcal{U} = \mathcal{V} \cdot \mathcal{W}$ is a subgroup of $\mathcal{A}_1(P_\infty)$ such that $\mathcal{W}_{\mathcal{U}} \simeq \mathcal{W}$ and $\mathcal{V}_{\mathcal{U}} \simeq \mathcal{V}$ (notation as in (3.4)). Hence, the genus of $H^{\mathcal{U}}$ is $g(H^{\mathcal{U}}) = \frac{1}{2}p^{n-v}(p^{n-w} - 1)$ by Proposition 3.1. □

In the case $\operatorname{char}(K) = 2$, the situation is slightly different.

THEOREM 3.3. *Let $q = 2^n$, and let $g \geqslant 1$ be an integer. Then the following assertions are equivalent.*

(i) *There exists a 2-subgroup $\mathcal{U} \subseteq \mathcal{A}$ such that $g = g(H^{\mathcal{U}})$.*

https://doi.org/10.1023/A:1001736016924 Published online by Cambridge University Press

(ii) $g = 2^{n-v-1} \cdot (2^{n-w} - 1)$ *with* $0 \leqslant v \leqslant n-1$ *and* $0 \leqslant w \leqslant n-1$, *and there exist additive subgroups* $\mathcal{V} \subseteq K$ *and* $\mathcal{W} \subseteq \mathbb{F}_q$ *of orders* $\operatorname{ord} \mathcal{V} = 2^v$ *and* $\operatorname{ord} \mathcal{W} = 2^w$, *such that* $\mathcal{V}^{q+1} = \{b^{q+1} \mid b \in \mathcal{V}\}$ *is contained in* $\mathcal{W}$.

Proof. (i) $\Rightarrow$ (ii): Let $\mathcal{U} \subseteq \mathcal{A}$ be a 2-group whose fixed field $H^{\mathcal{U}}$ is not rational. We can assume that $\mathcal{U} \subseteq \mathcal{A}_1(P_\infty)$. Define $\mathcal{V} = \mathcal{V}_{\mathcal{U}}$ and $\mathcal{W} = \mathcal{W}_{\mathcal{U}}$ as in formulas (3.4), and let $\operatorname{ord} \mathcal{V} = 2^v$, $\operatorname{ord} \mathcal{W} = 2^w$. By (3.8) the genus of $H^{\mathcal{U}}$ is $g(H^{\mathcal{U}}) = 2^{n-v-1}(2^{n-w} - 1)$. Since $g(H^{\mathcal{U}})$ is a positive integer, we conclude that $0 \leqslant v \leqslant n-1$ and $0 \leqslant w \leqslant n-1$. It remains to prove that $\mathcal{W} \subseteq \mathbb{F}_q$ and $\mathcal{V}^{q+1} \subseteq \mathcal{W}$. Let $c \in \mathcal{W}$. Then $[0, c] \in \mathcal{A}_1(P_\infty)$ and, therefore, $c^q + c = 0$ by (3.1). Since q is even, it follows that $c \in \mathbb{F}_q$. Finally, let $b \in \mathcal{V}$. Choose an element $d \in K$ such that $[b, d] \in \mathcal{U}$. Then $[b, d]^2 = [0, b^{q+1}] \in \mathcal{U}$, hence $b^{q+1} \in \mathcal{W}$.

(ii) $\Rightarrow$ (i): We note that the set $\mathcal{Z} = \{[0, c] \mid c \in \mathbb{F}_q\} = \{\sigma^2 \mid \sigma \in \mathcal{A}_1(P_\infty)\}$ is the center of $\mathcal{A}_1(P_\infty)$ (this is easily checked). Assume now that $\mathcal{V} \subseteq K$ and $\mathcal{W} \subseteq \mathbb{F}_q$ are additive subgroups of orders 2^v and 2^w such that $0 \leq w < n$ and $\mathcal{V}^{q+1} \subseteq \mathcal{W}$. We show by induction on v (for fixed $\mathcal{W}$) that there is a subgroup $\mathcal{U} \subseteq \mathcal{A}_1(P_\infty)$ with $\mathcal{V}_{\mathcal{U}} = \mathcal{V}$ and $\mathcal{W}_{\mathcal{U}} = \mathcal{W}$.

The case $v = 0$ is trivial: in this case we set $\mathcal{U} := \{[0, c] \mid c \in \mathcal{W}\}$. Suppose now that $v > 0$. Let $\mathcal{V}_0 \subseteq \mathcal{V}$ be a subgroup of order 2^{v-1}. By induction hypothesis there is a subgroup $\mathcal{U}_0 \subseteq \mathcal{A}_1(P_\infty)$ with $\mathcal{V}_{\mathcal{U}_0} = \mathcal{V}_0$ and $\mathcal{W}_{\mathcal{U}_0} = \mathcal{W}$. Choose an element $b \in \mathcal{V} \setminus \mathcal{V}_0$ and an element $c \in K$ with $c^q + c = b^{q+1}$, and let $\beta = [b, c]$. For all elements $\gamma = [b_0, c_0] \in \mathcal{U}_0$ we have that

$$(\beta\gamma)^2 = [b + b_0, *]^2 = [0, (b + b_0)^{q+1}]$$

lies in $\mathcal{U}_0$ (because $\mathcal{V}^{q+1} \subseteq \mathcal{W}$). Now we claim that

$$\beta \cdot \mathcal{U}_0 = \mathcal{U}_0 \cdot \beta. \tag{3.10}$$

In order to prove this, consider the product $\beta \cdot \gamma$ with some $\gamma \in \mathcal{U}_0$. Since $\beta^4 = \gamma^4 = [0, 0]$ and all squares are in the center of $\mathcal{A}_1(P_\infty)$, we find that

$$\begin{aligned} \beta\gamma &= \beta\gamma(\beta\gamma^4\beta^3) = (\beta\gamma)^2\gamma^3\beta^3 \\ &= \gamma^3 \cdot (\beta\gamma)^2 \cdot \beta^2 \cdot \beta \in \mathcal{U}_0 \cdot \mathcal{U}_0 \cdot \mathcal{U}_0 \cdot \beta = \mathcal{U}_0\beta. \end{aligned}$$

This implies (3.10) and shows that $\mathcal{U} := \mathcal{U}_0 \cup \beta \cdot \mathcal{U}_0$ is a subgroup of $\mathcal{A}_1(P_\infty)$. It is easily checked that $\mathcal{V}_{\mathcal{U}} = \mathcal{V}$ and $\mathcal{W}_{\mathcal{U}} = \mathcal{W}$, as desired. □

COROLLARY 3.4. *Let $q = 2^n$. Then we have*

(i) *If there exists a 2-subgroup $\mathcal{U} \subseteq \mathcal{A}$ such that the fixed field $H^{\mathcal{U}}$ has genus $g(H^{\mathcal{U}}) = 2^{n-v-1} \cdot (2^{n-w} - 1) \neq 0$ then there is a 2-subgroup $\mathcal{U}' \subseteq \mathcal{A}$ with*

$$g(H^{\mathcal{U}'}) = 2^{n-v'-1}(2^{n-w} - 1), \quad \text{for all } v' \text{ with } 0 \leqslant v' \leqslant v.$$

(ii) *For all integers v, w with $0 \leqslant v \leqslant w < n$ there is a 2-subgroup $\mathcal{U} \subseteq \mathcal{A}$ such that $g(H^{\mathcal{U}}) = 2^{n-v-1}(2^{n-w} - 1)$.*

(iii) *Suppose that v and w satisfy the following conditions:*

$$w|n,\ w|v,\ v|2n,\ 1 \leqslant v < n \text{ and } \left.\frac{2^v - 1}{2^w - 1}\ \right|\ (2^n + 1).$$

Then there exists a 2-subgroup $\mathcal{U} \subseteq \mathcal{A}$ such that

$$g(H^{\mathcal{U}}) = 2^{n-v-1}(2^{n-w} - 1).$$

Proof. (i) If $g(H^{\mathcal{U}}) = 2^{n-v-1}(2^{n-w} - 1)$ then ord $\mathcal{V}_{\mathcal{U}} = 2^v$, ord $\mathcal{W}_{\mathcal{U}} = 2^w$ and $\mathcal{V}_{\mathcal{U}}^{q+1} \subseteq \mathcal{W}_{\mathcal{U}}$. For all $v' \leqslant v$ there is a subgroup $\mathcal{V}' \subseteq \mathcal{V}_{\mathcal{U}}$ of order $2^{v'}$, and clearly $(\mathcal{V}')^{q+1} \subseteq \mathcal{W}_{\mathcal{U}}$. By Theorem 3.3 there exists a 2-subgroup $\mathcal{U}' \subseteq \mathcal{A}$ with $g(H^{\mathcal{U}'}) = 2^{n-v'-1}(2^{n-w} - 1)$.

(ii) First choose an additive subgroup $\mathcal{W} \subseteq \mathbb{F}_q$ of order 2^w. As $b^{q+1} = b^2$ for all $b \in \mathbb{F}_q$, the mapping $b \mapsto b^{q+1}$ is an isomorphism of the additive group $\mathbb{F}_q$ onto itself. Hence there is, for all $v \leqslant w$, a subgroup $\mathcal{V} \subseteq \mathbb{F}_q$ of order 2^v with $\mathcal{V}^{q+1} \subseteq \mathcal{W}$. Now apply Theorem 3.3.

(iii) The conditions on v and w imply that $\mathbb{F}_{2^w} \subseteq \mathbb{F}_{2^v} \subseteq \mathbb{F}_{2^{2n}} = K$. The norm mapping $\nu\colon \mathbb{F}_{2^v} \to \mathbb{F}_{2^w}$ is given by $\nu(b) = b^{(2^v-1)/(2^w-1)}$, and the assumption $(2^v - 1)/(2^w - 1) \mid (2^n + 1)$ implies that $(\mathbb{F}_{2^v})^{2^n+1} \subseteq \mathbb{F}_{2^w}$. Now we can apply Theorem 3.3 with $\mathcal{V} = \mathbb{F}_{2^v}$ and $\mathcal{W} = \mathbb{F}_{2^w}$. □

Remark 3.5. Here we want to indicate how hard it is to find a 2-subgroup $\mathcal{U} \subseteq \mathcal{A}$ with $v > w$. If $w = 0$, that means $\mathcal{W}_{\mathcal{U}} = \{0\}$, the condition $\mathcal{V}_{\mathcal{U}}^{q+1} \subseteq \mathcal{W}_{\mathcal{U}}$ implies $v = 0$.

Now suppose that $w = 1$, that means $\mathcal{W}_{\mathcal{U}} = \{0, \alpha\}$ for some $\alpha \in \mathbb{F}_q^*$. If $v > 0$ we then fix an element $b \in \mathcal{V}_{\mathcal{U}} \backslash \{0\}$. For another element $b_1 \in \mathcal{V}_{\mathcal{U}} \backslash \{0, b\}$, we have

$$(b + b_1)^{q+1} = b^{q+1} + b_1^{q+1} + b\, b_1^q + b^q\, b_1.$$

Using the condition $\mathcal{V}_{\mathcal{U}}^{q+1} \subseteq \mathcal{W}_{\mathcal{U}} = \{0, \alpha\}$, we must have

$$\alpha = b\, b_1^q + b^q\, b_1. \tag{3.11}$$

We multiply Equation (3.11) by b and by b_1, obtaining

$$b^2\, b_1^q + \alpha b_1 = \alpha b \quad \text{and} \quad \alpha b + b^q\, b_1^2 = \alpha b_1.$$

https://doi.org/10.1023/A:1001736016924 Published online by Cambridge University Press

Hence $b^q b_1^2 = b^2 b_1^q$ and $(b_1/b)^{q/2} = b_1/b$. We then conclude that $b_1/b \in \mathbb{F}_{q/2} \cap \mathbb{F}_{q^2} = \mathbb{F}_{2^d}$, with

$$d = \gcd(n-1, 2n) = \begin{cases} 1, & \text{if } n \text{ even} \\ 2, & \text{if } n \text{ odd.} \end{cases}$$

This shows that $v \leqslant 2$ and $v = 2$ occurs only if n is odd.

We have then shown that there is no 2-subgroup $\mathcal{U} \subseteq \mathcal{A}$ with genus as below.

$$g(H^{\mathcal{U}}) = \begin{cases} 2^s(2^n - 1) & \text{with } 0 \leqslant s \leqslant n-2. \\ 2^s(2^{n-1} - 1) & \text{with } n \text{ even and } 0 \leqslant s \leqslant n-3. \\ 2^s(2^{n-1} - 1) & \text{with } n \text{ odd and } 0 \leqslant s \leqslant n-4. \end{cases}$$

4. The Fixed Fields of Subgroups of $\mathcal{A}(P_\infty)$

As in Section 2, we denote by

$$\mathcal{A}(P_\infty) = \{\sigma \in \mathcal{A} = \mathcal{A}ut(H/K) \mid \sigma P_\infty = P_\infty\}$$

the decomposition group of P_∞ in the Galois extension $H/H^{\mathcal{A}}$. Any $\sigma \in \mathcal{A}(P_\infty)$ acts as follows

$$\sigma(x) = ax + b, \qquad \sigma(y) = a^{q+1}y + ab^q x + c,$$

$$a \in K^\times, \quad b \in K, \qquad c^q + c = b^{q+1}.$$

For convenience we will indentify σ with this triple $[a, b, c]$, so

$$\mathcal{A}(P_\infty) = \{[a, b, c] \mid a \in K^\times, b \in K, c^q + c = b^{q+1}\}.$$

The group structure of $\mathcal{A}(P_\infty)$ is given by

$$[a_1, b_1, c_1] \cdot [a_2, b_2, c_2] = [a_1a_2, a_2b_1 + b_2, a_2^{q+1}c_1 + a_2b_2^q b_1 + c_2]. \tag{4.1}$$

The identity is the triple $[1, 0, 0]$, the inverse of $[a, b, c]$ is

$$[a, b, c]^{-1} = [a^{-1}, -a^{-1}b, a^{-(q+1)}c^q]. \tag{4.2}$$

The unique p-Sylow subgroup of $\mathcal{A}(P_\infty)$ is the group

$$\mathcal{A}_1(P_\infty) = \{[1, b, c] \mid b \in K, c^q + c = b^{q+1}\}.$$

Our aim is to determine the genus of the fixed fields of H with respect to subgroups of $\mathcal{A}(P_\infty)$. Let us fix some notation for the rest of this section.

https://doi.org/10.1023/A:1001736016924 Published online by Cambridge University Press

$$\begin{aligned}
&\mathcal{G} \subseteq \mathcal{A}(P_\infty) \text{ is a subgroup of } \mathcal{A}(P_\infty).\\
&\mathcal{U}_{\mathcal{G}} = \mathcal{G} \cap \mathcal{A}_1(P_\infty) \text{ is the unique } p\text{-Sylow subgroup of } \mathcal{G}.\\
&\mathcal{V}_{\mathcal{G}} = \{b \in K \mid \text{there is some } c \in K \text{ such that } [1, b, c] \in \mathcal{G}\}.\\
&\mathcal{W}_{\mathcal{G}} = \{c \in K \mid [1, 0, c] \in \mathcal{G}\}.\\
&\operatorname{ord} \mathcal{G} = m \cdot p^u \text{ with } (m, p) = 1.\\
&\operatorname{ord} \mathcal{V}_{\mathcal{G}} = p^v, \qquad \operatorname{ord} \mathcal{W}_{\mathcal{G}} = p^w.
\end{aligned} \tag{4.3}$$

As we have considered p-groups already in Section 3, we will always assume in this Section that $\mathcal{G}$ is not a p-group, so

$$\operatorname{ord} \mathcal{G} = m \cdot p^u \quad \text{with } (m, p) = 1, \quad m > 1 \quad \text{and} \quad u = v + w \geqslant 0.$$

The Hurwitz genus formula (2.9) for the Galois extension $H/H^{\mathcal{G}}$ yields

$$q^2 - q - 2 = \operatorname{ord} \mathcal{G} \cdot (2g(H^{\mathcal{G}}) - 2) + \sum_{P \in \mathbb{P}(H)} d_{\mathcal{G}}(P) \cdot \deg P, \tag{4.4}$$

where $d_{\mathcal{G}}(P)$ is the different exponent of P with respect to $H/H^{\mathcal{G}}$.

The place P_∞ is totally ramified in $H/H^{\mathcal{G}}$. Using the transitivity of the different exponent in the extension $H^{\mathcal{G}} \subseteq H^{\mathcal{U}_{\mathcal{G}}} \subseteq H$, we obtain from Equation (3.7) that

$$\begin{aligned}
d_{\mathcal{G}}(P_\infty) &= 2(p^u - 1) + q(p^w - 1) + p^u(m - 1)\\
&= p^u(m + 1) + q(p^w - 1) - 2\\
&= \operatorname{ord} \mathcal{G} + p^u + qp^w - q - 2.
\end{aligned} \tag{4.5}$$

Let $S = \{P \in \mathbb{P}(H) \mid \deg P = 1 \ \text{ and } \ P \neq P_\infty\}$. It is easily seen that the only places $P \in \mathbb{P}(H) \setminus \{P_\infty\}$ which ramify in $H/H^{\mathcal{G}}$ are in S, and they are tamely ramified. Denoting by $e_{\mathcal{G}}(P)$ the ramification index of P in $H/H^{\mathcal{G}}$, we obtain from (4.4) and (4.5)

$$q(q - p^w) - p^u = \operatorname{ord} \mathcal{G} \cdot (2g(H^{\mathcal{G}}) - 1) + \sum_{P \in S} (e_{\mathcal{G}}(P) - 1). \tag{4.6}$$

For tamely ramified places of degree one, ramification theory [St 1, III] yields

$$e_{\mathcal{G}}(P) - 1 = \#\{\sigma \in \mathcal{G} \setminus \{1\} \mid \sigma P = P\}.$$

Hence we obtain that

$$\sum_{P \in S} (e_{\mathcal{G}}(P) - 1) = \sum_{1 \neq \sigma \in \mathcal{G}} N_S(\sigma) \tag{4.7}$$

with $N_S(\sigma) := \#\{P \in S \mid \sigma P = P\}$, for $\sigma \in \mathcal{G} \setminus \{1\}$. Before we can determine $N_S(\sigma)$, we need some preparation. For $a \in K^\times$ denote by $\operatorname{ord}(a)$ the multiplicative order of a.

LEMMA 4.1. *Let* $\sigma = [a, b, c] \in \mathcal{A}(P_\infty)$ *with* $a \neq 1$. *Then we have*

(i) *If* $\operatorname{ord}(a)$ *is not a divisor of* $q + 1$, *then* $\operatorname{ord}(\sigma) = \operatorname{ord}(a)$.

https://doi.org/10.1023/A:1001736016924 Published online by Cambridge University Press

(ii) *If* $\mathrm{ord}(a)$ *divides* $q+1$, *then*

$$\mathrm{ord}(\sigma) = \begin{cases} \mathrm{ord}(a), & \text{if } c = ab^{q+1}/(a-1). \\ p \cdot \mathrm{ord}(a), & \text{otherwise}. \end{cases}$$

Proof. Let $\tau := [1, e, f]$ with

$$e := b/(a-1) \quad \text{and} \quad f^q + f = e^{q+1}.$$

Then $\tau^{-1} = [1, -e, f^q]$, and one checks that

$$\tau^{-1}\sigma\tau = [a, 0, c^*] \quad \text{with } c^{*q} + c^* = 0.$$

(i) If $\mathrm{ord}(a)$ does not divide $q+1$, let $f^* := c^*/(a^{q+1}-1)$. Then

$$f^{*q} + f^* = \frac{c^{*q}}{(a^{q+1}-1)^q} + \frac{c^*}{a^{q+1}-1} = \frac{1}{a^{q+1}-1}(c^{*q} + c^*) = 0.$$

So $\tau^* := [1, 0, f^*]$ is in $\mathcal{A}_1(P_\infty)$, and

$$\begin{aligned} \tau^{*-1} \cdot [a, 0, c^*] \cdot \tau^* &= [a, 0, a^{q+1} f^{*q} + c^* + f^*] \\ &= [a, 0, -a^{q+1} f^* + f^* + c^*] = [a, 0, 0]. \end{aligned}$$

We have thus shown that σ is conjugate to the automorphism $[a, 0, 0]$, hence

$$\mathrm{ord}(\sigma) = \mathrm{ord}([a, 0, 0]) = \mathrm{ord}(a).$$

(ii) Now we assume that $a^{q+1} = 1$. With the same choice of $\tau = [1, e, f]$ as above we find that $\sigma^* := \tau^{-1}\sigma\tau = [a, 0, c^*]$ with

$$\begin{aligned} c^* &= f^q + f + c - ab^q e - ae^{q+1} + e^q b \\ &= e^{q+1} - ae^{q+1} - ab^q e + e^q b + c \\ &= \frac{b^{q+1}}{(a-1)^{q+1}}(1-a) - ab^q \cdot \frac{b}{a-1} + b \cdot \frac{b^q}{(a-1)^q} + c \\ &= \frac{-b^{q+1}}{a^q - 1} - \frac{ab^{q+1}}{a-1} + \frac{b^{q+1}}{a^q - 1} + c \\ &= c - \frac{a}{a-1} b^{q+1}. \end{aligned}$$

Hence $c^* = 0$ iff $c = ab^{q+1}/(a-1)$. One checks easily that the order of $\sigma^* = [a, 0, c^*]$ is

$$\mathrm{ord}(\sigma^*) = \begin{cases} \mathrm{ord}(a), & \text{if } c^* = 0, \\ p \cdot \mathrm{ord}(a), & \text{if } c^* \neq 0. \end{cases}$$

https://doi.org/10.1023/A:1001736016924 Published online by Cambridge University Press

Since $\mathrm{ord}(\sigma) = \mathrm{ord}(\sigma^*)$, Lemma 4.1 is completely proved. □

LEMMA 4.2. *Let* $\sigma = [a, b, c] \in \mathcal{A}(P_\infty)$ *with* $\sigma \neq 1$. *Then*

$$N_S(\sigma) = \begin{cases} 0, & \textit{if } p \textit{ divides } \mathrm{ord}(\sigma). \\ q, & \textit{if } \mathrm{ord}(\sigma) \textit{ divides } q+1. \\ 1, & \textit{otherwise}. \end{cases}$$

Proof. (i) Suppose that $\mathrm{ord}(\sigma)$ is divisible by p. As all $P \in S$ are tame in the extension $H/H^{\mathcal{A}(P_\infty)}$, we conclude that $\sigma P \neq P$ for all $P \in S$, i.e. $N_S(\sigma) = 0$.

(ii) Suppose that $\sigma \neq 1$ and $\mathrm{ord}(\sigma)$ divides $q + 1$. The proof of Lemma 4.1 (ii) shows that σ is conjugate in $\mathcal{A}(P_\infty)$ to $\sigma^* = [a, 0, 0]$ with $\mathrm{ord}(a) = \mathrm{ord}(\sigma)$ dividing $q + 1$. Then $N_S(\sigma) = N_S(\sigma^*)$, and $1 \neq \sigma^* \in \mathrm{Gal}(H/K(y))$. In the extension $H/K(y)$ exactly q places $P \in S$ are ramified (namely the zeros of $y^q + y$), and they are totally ramified. Thus $N_S(\sigma^*) = q$.

(iii) Now we assume that $\mathrm{ord}(\sigma) = s$ with $s \mid (q^2 - 1)$ but s does not divide $q+1$. By Lemma 4.1(i), σ is conjugate in $\mathcal{A}(P_\infty)$ to $\sigma^* = [a, 0, 0]$ with $\mathrm{ord}(a) = s$ (in particular $a^{q+1} \neq 1$). For $(\alpha, \beta) \in K \times K$ with $\beta^q + \beta = \alpha^{q+1}$ there is a unique place $P_{\alpha,\beta} \in S$ which is a common zero of $x - \alpha$ and $y - \beta$, and all places $P \in S$ can be described in this manner. We have

$$\sigma^*(P_{\alpha,\beta}) = P_{\alpha,\beta} \Leftrightarrow P_{\alpha,\beta} \text{ is a common zero of } \sigma^*(x-\alpha) \text{ and } \sigma^*(y-\beta).$$

Since $\sigma^*(x - \alpha) = ax - \alpha = a(x - \alpha) + \alpha(a - 1)$ and $\sigma^*(y - \beta) = a^{q+1}y - \beta = a^{q+1}(y - \beta) + \beta(a^{q+1} - 1)$, it follows that

$$\begin{aligned} \sigma^*(P_{\alpha,\beta}) = P_{\alpha,\beta} &\Leftrightarrow \alpha(a-1) = \beta(a^{q+1}-1) = 0 \\ &\Leftrightarrow \alpha = \beta = 0. \end{aligned}$$

Hence $N_S(\sigma) = N_S(\sigma^*) = 1$. □

LEMMA 4.3. *Notations as in* (4.3). *Let* $a_0 \in K^\times$, $\mathrm{ord}(a_0) = s > 1$ *and* $s|m$.

(i) *If* $s \nmid (q + 1)$, *then there are exactly* p^u *elements* $\sigma \in \mathcal{G}$ *of the form* $\sigma = [a_0, *, *]$ *having order* s.
(ii) *If* $s \mid (q+1)$ *then there are exactly* p^v *elements* $\sigma \in \mathcal{G}$ *of the form* $\sigma = [a_0, *, *]$ *having order* s.

Proof. The mapping

$$\rho : \begin{cases} \mathcal{G} & \to K^\times \\ \sigma = [a, b, c] & \mapsto a \end{cases}$$

is a homomorphism, its kernel is the p-Sylow subgroup $\mathcal{U}_{\mathcal{G}}$ of $\mathcal{G}$ of order p^u, its image is the unique subgroup of $K^\times$ of order m. Since $\mathrm{ord}(a_0) = s$ is a divisor of m, there exists an automorphism $\sigma_0 = [a_0, b_0, c_0] \in \mathcal{G}$. The coset $\sigma_0 \cdot \mathcal{U}_{\mathcal{G}}$ is then

$$\sigma_0 \cdot \mathcal{U}_{\mathcal{G}} = \{[a, b, c] \in \mathcal{G} \mid a = a_0\}.$$

https://doi.org/10.1023/A:1001736016924 Published online by Cambridge University Press

(i) Suppose that s is not a divisor of $q+1$. It follows that all elements $\sigma \in \sigma_0 \cdot \mathcal{U}_{\mathcal{G}}$ have order s, by Lemma 4.1(i).
(ii) Now we assume that s divides $q+1$. For each $b' \in \mathcal{V}_{\mathcal{G}}$ we fix an element $c' \in K$ such that $[1, b', c'] \in \mathcal{G}$; then every $\sigma \in \sigma_0 \cdot \mathcal{U}_{\mathcal{G}}$ can be uniquely represented as

$$\sigma = [a_0, b_0, c_0] \cdot [1, b', c'] \cdot [1, 0, c] = [a_0, b_0 + b', *],$$

with $b' \in \mathcal{V}_{\mathcal{G}}$ and $c \in \mathcal{W}_{\mathcal{G}}$. By Lemma 4.1, there is at most one element $\sigma \in \mathcal{G}$ of order s with $\sigma = [a_0, b_0 + b', *]$ if a_0 and $b := b_0 + b'$ are given. The proof of Lemma 4.3(ii) will be finished when we show the following assertion:

CLAIM. *Let* $\sigma = [a_0, b, c'] \in \mathcal{G}$ *and* $\mathrm{ord}(a_0) = s$ *be a divisor of* $q+1$*. Then there exists an element* $\tilde{\sigma} \in \mathcal{G}$ *of order* s *such that* $\tilde{\sigma} = [a_0, b, \tilde{c}]$.

Proof. If $\mathrm{ord}(\sigma) = s$ we take $\tilde{\sigma} = \sigma$. Otherwise, $\mathrm{ord}(\sigma) = p \cdot s$ by Lemma 4.1. For all $j \geqslant 1$ holds

$$[a_0, b, *]^j = \left[a_0^j, \frac{a_0^j - 1}{a_0 - 1} \cdot b, * \right].$$

Choose $t \geqslant 1$ with $p \cdot t \equiv 1 \bmod s$. Then

$$\tilde{\sigma} := [a_0, b, *]^{pt} = \left[a_0, \frac{a_0 - 1}{a_0 - 1} b, * \right] = [a_0, b, *]$$

is an element of $\mathcal{G}$ of order s whose first components are a_0 and b, as desired. □

THEOREM 4.4. *Let* $\mathcal{G} \subseteq \mathcal{A}(P_\infty)$ *be a subgroup of order* $m \cdot p^u$ *with* $m > 1$*, and define* v, w *as in* (4.3)*. Let* $d := \gcd(m, q+1)$*. Then the fixed field* $H^{\mathcal{G}}$ *has genus*

$$g(H^{\mathcal{G}}) = \frac{p^n - p^w}{2mp^u} (p^n - (d-1)p^v).$$

Proof. There are exactly $d-1$ elements $1 \neq a_0 \in K^\times$ with

$$\mathrm{ord}(a_0) \mid m \quad \text{and} \quad \mathrm{ord}(a_0) \mid (q+1),$$

and there are exactly $m-d$ elements $a_0 \in K^\times$ with

$$\mathrm{ord}(a_0) \mid m \quad \text{and} \quad a_0^{q+1} \neq 1.$$

Now we obtain from Lemma 4.2 and Lemma 4.3

$$\begin{aligned} \sum_{1 \neq \sigma \in \mathcal{G}} N_S(\sigma) &= (d-1)p^v q + (m-d)p^u \\ &= \mathrm{ord}\, \mathcal{G} + d(qp^v - p^u) - qp^v. \end{aligned}$$

https://doi.org/10.1023/A:1001736016924 Published online by Cambridge University Press

Formulas (4.6) and (4.7) imply that

$$q(q-p^w)-p^u = 2g(H^{\mathcal{G}})\cdot mp^u + d(qp^v - p^u) - qp^v.$$

Substituting $q=p^n$ and $u=v+w$, the result follows. □

Not for all choices of v, w and m with $0 \leqslant w \leqslant n$, $0 \leqslant v \leqslant 2n$ and $m \mid (q^2-1)$ there exists a subgroup $\mathcal{G} \subseteq \mathcal{A}(P_\infty)$ of order $m \cdot p^{v+w}$, with ord $\mathcal{V}_{\mathcal{G}} = p^v$ and ord $\mathcal{W}_{\mathcal{G}} = p^w$. For example if $d=\gcd(m, q+1) > 1$, then there is no such a subgroup having $v > n$ and $w < n$. We will not give necessary and sufficient conditions on v, w and m in the general case but we restrict ourselves to special cases. Let

$$\mathcal{G}_0 := \{[a,0,c] \mid a \in K^\times \quad \text{and} \quad c^q + c = 0\}. \tag{4.8}$$

This is a subgroup of $\mathcal{A}(P_\infty)$ of order $q(q^2-1)$, its fixed field is the rational function field $H^{\mathcal{G}_0} = K(z)$ with $z = x^{q^2-1}$.

COROLLARY 4.5. *Let $\mathcal{G} \subseteq \mathcal{G}_0$ be a subgroup of order* ord $\mathcal{G} = m \cdot p^u$, *with* $(m,p)=1$. *Then the fixed field $H^{\mathcal{G}}$ has genus*

$$g(H^{\mathcal{G}}) = \frac{1}{2m}(p^n+1-d)(p^{n-u}-1),$$

where $d = \gcd(m, q+1)$.

Proof. Note that $\mathcal{V}_{\mathcal{G}} = 0$ for $\mathcal{G} \subseteq \mathcal{G}_0$, hence $u=w$ and $v=0$. The result follows immediately from Theorem 4.4. □

PROPOSITION 4.6. *Let $m \geqslant 1$, $d \geqslant 1$ and $0 \leqslant u \leqslant n$ be integers with the following properties.*

(i) $m \mid (q^2-1)$ *and* $d = \gcd(m, q+1)$.
(ii) $s := \min\{r \geqslant 1 \mid p^r \equiv 1 \bmod (m/d)\}$ *is a divisor of* u.

Then there exists a subgroup $\mathcal{G} \subseteq \mathcal{G}_0$ of order $m \cdot p^u$, and hence there exists a subfield $E \subseteq H$ with

$$g(E) = \frac{1}{2m}(p^n+1-d)(p^{n-u}-1).$$

Proof. Let $a \in K^\times$ be an element with $a^m = 1$, and let $\alpha := a^{q+1}$. Then

$$\alpha^{m/d} = 1, \quad \text{with } d = \gcd(m, q+1).$$

It follows that $\alpha \in \mathbb{F}_{p^s}$ where s is defined by (ii). Moreover we know that $q \equiv 1 \bmod (m/d)$ (since $m \mid (q^2-1)$), hence $\mathbb{F}_{p^s} \subseteq \mathbb{F}_q$. The set $\mathcal{T} = \{c \in$

https://doi.org/10.1023/A:1001736016924 Published online by Cambridge University Press

$K \mid c^q + c = 0\}$ is a one-dimensional $\mathbb{F}_q$-vector space, hence it is a vector space over $\mathbb{F}_{p^s}$ of dimension n/s. Since $0 \leqslant u/s \leqslant n/s$, we can find an $\mathbb{F}_{p^s}$-subspace $\mathcal{W} \subseteq \mathcal{T}$ of dimension u/s; then $\mathcal{W}$ is an additive subgroup of $\mathcal{T}$ of order p^u. Let

$$\mathcal{G} := \{[a, 0, c] \mid a^m = 1 \quad \text{and} \quad c \in \mathcal{W}\}.$$

Then $\mathcal{G}$ is a subgroup of $\mathcal{G}_0$: in fact, if $[a_1, 0, c_1]$ and $[a_2, 0, c_2]$ are elements of $\mathcal{G}$, then

$$[a_1, 0, c_1] \cdot [a_2, 0, c_2] = [a_1 a_2, 0, a_2^{q+1} c_1 + c_2]$$

is in $\mathcal{G}$ because $a_2^{q+1} \in \mathbb{F}_{p^s}$ and $\mathcal{W}$ is an $\mathbb{F}_{p^s}$-module. The order of $\mathcal{G}$ is obviously $m \cdot p^u$, as desired. □

Remark 4.7. One can show that all subgroups $\mathcal{G} \subseteq \mathcal{G}_0$ satisfy the numerical conditions of Proposition 4.6.

COROLLARY 4.8. *Suppose that* $m \mid (q+1)(p-1)$. *Then for all* u *with* $0 \leqslant u \leqslant n$ *there exists a subgroup* $\mathcal{G} \subseteq \mathcal{G}_0$ *such that*

$$g(H^{\mathcal{G}}) = \frac{1}{2m}(p^n + 1 - d)(p^{n-u} - 1),$$

where $d = \gcd(m, q+1)$. *In particular, if* $m \mid (q+1)$, *then*

$$g(H^{\mathcal{G}}) = \frac{1}{2}\left(\frac{p^n + 1}{m} - 1\right)(p^{n-u} - 1).$$

Proof. The condition $m \mid (q+1)(p-1)$ implies that m/d is a divisor of $p-1$, hence $s = 1$ (with s as in Proposition 4.6(ii)). Now all assertions of Corollary 4.8 follow immediately. □

The following special case of Proposition 4.6 is often useful.

COROLLARY 4.9. *For any divisor* m *of* $q^2 - 1$ *there exists a subgroup* $\mathcal{G} \subseteq \mathcal{G}_0$ *such that*

$$g(H^{\mathcal{G}}) = \frac{1}{2m}(p^n + 1 - d)(p^n - 1),$$

where $d = \gcd(m, q+1)$.

Proof. Set $u = 0$ in Proposition 4.6. □

5. The Fixed Fields of Some Tame Subgroups of $\mathcal{A}$

We call a subgroup $\mathcal{G} \subseteq \mathcal{A}$ tame if the extension $H/H^{\mathcal{G}}$ is tame; i.e. the ramification index of any place $P \in \mathbb{P}(H)$ in the extension $H/H^{\mathcal{G}}$ is relatively prime to the characteristic p of K. In particular, if p does not divide the order of $\mathcal{G}$ then $\mathcal{G}$ is tame.

In this section we will determine the genus $g(H^{\mathcal{G}})$ for a large number of tame subgroups $\mathcal{G} \subseteq \mathcal{A}$. We start with

THEOREM 5.1. *Let $\tilde{P} \in \mathbb{P}(H)$ be a place of degree 3, and let $\mathcal{B} \subseteq \mathcal{A}$ be the inertia group of $\tilde{P}$ with respect to the field extension $H/H^{\mathcal{A}}$. The group $\mathcal{B}$ is cyclic of order $q^2 - q + 1$, and for any integer $r \geqslant 1$ dividing $q^2 - q + 1$ there exists a unique subgroup $\mathcal{G} \subseteq \mathcal{B}$ of order $\operatorname{ord} \mathcal{G} = r$. The genus of the fixed field $H^{\mathcal{G}}$ is then*

$$g(H^{\mathcal{G}}) = \frac{s-1}{2}, \quad \textit{with } s = \frac{q^2 - q + 1}{r}.$$

Proof. The group $\mathcal{B}$ is cyclic of order $q^2 - q + 1$, and $\tilde{P}$ is the only place of H that ramifies in the extension $H/H^{\mathcal{B}}$, see Corollary 2.3. Let $r \geqslant 1$ be a divisor of $q^2 - q + 1$ and $\mathcal{G} \subseteq \mathcal{B}$ denote the unique subgroup of $\mathcal{B}$ of order r. Since $\tilde{P}$ is totally ramified in $H/H^{\mathcal{G}}$, the different of $H/H^{\mathcal{G}}$ is

$$\operatorname{Diff}(H/H^{\mathcal{G}}) = (r-1) \cdot \tilde{P}.$$

The Hurwitz genus formula for $H/H^{\mathcal{G}}$ yields

$$q^2 - q - 2 = r(2g(H^{\mathcal{G}}) - 2) + (r-1) \cdot \deg \tilde{P}.$$

As $\deg \tilde{P} = 3$, Theorem 5.1 follows immediately. □

Next we prove a general formula for the genus $g(H^{\mathcal{G}})$, where $\mathcal{G} \subseteq \mathcal{A}$ is any tame subgroup of $\mathcal{A}$.

PROPOSITION 5.2. *Let $\mathcal{G} \subseteq \mathcal{A}$ be a tame subgroup of $\mathcal{A}$ satisfying the following hypothesis.*

$$\textit{All } P \in \mathbb{P}(H) \textit{ with } \deg P > 1 \textit{ are unramified in } H/H^{\mathcal{G}}. \qquad (*)$$

Then the genus of $H^{\mathcal{G}}$ is

$$g(H^{\mathcal{G}}) = 1 + \frac{1}{2 \cdot \operatorname{ord} \mathcal{G}} \cdot \left(q^2 - q - 2 - \sum_{1 \neq \sigma \in \mathcal{G}} N(\sigma) \right),$$

where $N(\sigma)$ is defined as

$$N(\sigma) := \#\{P \in \mathbb{P}(H) \mid \deg P = 1 \textit{ and } \sigma P = P\}. \qquad (5.1)$$

Proof. Denote by $e(P)$ the ramification index of a place $P \in \mathbb{P}(H)$ in the extension $H/H^{\mathcal{G}}$. By hypothesis $(*)$, the degree of the different $\mathrm{Diff}(H/H^{\mathcal{G}})$ is

$$\begin{aligned}\deg \mathrm{Diff}(H/H^{\mathcal{G}}) &= \sum_{P\in\mathbb{P}(H);\deg P=1} (e(P)-1)\\ &= \sum_{P\in\mathbb{P}(H);\deg P=1}\ \sum_{1\neq\sigma\in\mathcal{G};\sigma P=P} 1 = \sum_{1\neq\sigma\in\mathcal{G}} N(\sigma).\end{aligned}$$

Hence the Hurwitz genus formula (2.9) implies Proposition 5.2. □

We will apply Proposition 5.2 to various tame subgroups $\mathcal{G} \subseteq \mathcal{A}$. First we will consider subgroups of the group $\mathcal{C} := \langle\epsilon,\omega\rangle \subseteq \mathcal{A}$ which is generated by the automorphims ϵ and ω given by (2.6) and (2.7):

$$\epsilon(x) = ax, \qquad \epsilon(y) = a^{q+1}y \quad \text{and} \quad \omega(x) = x/y, \qquad \omega(y) = 1/y.$$

Here $a \in K$ is a primitive (q^2-1)th root of unity. Any $\sigma \in \mathcal{C}$ is of the form

$$\sigma(x) = cx, \qquad \sigma(y) = c^{q+1}y \quad \text{with} \ \ c \in K^{\times},$$

or

$$\sigma(x) = c\cdot x/y, \qquad \sigma(y) = c^{q+1}\cdot 1/y \quad \text{with} \ \ c \in K^{\times}.$$

Hence $\mathrm{ord}(\mathcal{C}) = 2(q^2-1)$, and $\mathcal{C}$ is tame if $\mathrm{char}(K) \neq 2$.

Moreover, hypothesis $(*)$ from Proposition 5.2 holds for $\mathcal{C}$ (in order to prove this, consider ramification in the subextensions $H^{\mathcal{C}} = K(y^{q-1}+y^{-(q-1)}) \subseteq K(y^{q-1}) \subseteq K(y) \subseteq H$).

LEMMA 5.3. *Assume that* $\mathrm{char}(K) \neq 2$.

(i) *Let* $\sigma \in \mathcal{C}$ *with* $\sigma(x) = cx$, $\sigma(y) = c^{q+1}y$ *and* $1 \neq c \in K^{\times}$. *Then*

$$N(\sigma) = \begin{cases} 2, & \text{if } c^{q+1} \neq 1.\\ q+1, & \text{if } c^{q+1} = 1.\end{cases}$$

(ii) *Let* $\sigma \in \mathcal{C}$ *with* $\sigma(x) = c\cdot x/y$, $\sigma(y) = c^{q+1}\cdot 1/y$ *and* $c \in K^{\times}$. *Then*

$$N(\sigma) = \begin{cases} q+1, & \text{if } c \in \mathbb{F}_q\\ 0, & \text{if } c \notin \mathbb{F}_q \text{ and } c^{(q^2-1)/2} = 1.\\ 2, & \text{if } c \notin \mathbb{F}_q \text{ and } c^{(q^2-1)/2} = -1.\end{cases}$$

Proof. (i) This is a consequence of Lemma 4.2 (note that $N(\sigma) = 1 + N_S(\sigma)$, because $N_S(\sigma)$ does not count the place P_∞).

https://doi.org/10.1023/A:1001736016924 Published online by Cambridge University Press

(ii) Now we determine $N(\sigma)$ for an automorphism $\sigma \in \mathcal{C}$ given by $\sigma(x) = c \cdot x/y$ and $\sigma(y) = c^{q+1} \cdot 1/y$, with $c \in K^\times$. The places $P \in \mathbb{P}(H)$ of degree one are $P = P_\infty$ and, for any pair $(\alpha, \beta) \in K \times K$ with $\beta^q + \beta = \alpha^{q+1}$, the unique common zero $P = P_{\alpha,\beta}$ of $x - \alpha$ and $y - \beta$. Obviously $\sigma(P_\infty) \neq P_\infty$ and $\sigma(P_{0,0}) \neq P_{0,0}$. For the remaining places $P_{\alpha,\beta}$ holds $\beta \neq 0$, and we have for such a place

$$\begin{aligned} \sigma(P_{\alpha,\beta}) = P_{\alpha,\beta} &\Leftrightarrow \sigma(x)(P_{\alpha,\beta}) = \alpha \quad \text{and} \quad \sigma(y)(P_{\alpha,\beta}) = \beta \\ &\Leftrightarrow c \cdot \alpha/\beta = \alpha \quad \text{and} \quad c^{q+1}/\beta = \beta \\ &\Leftrightarrow \alpha(c\beta^{-1} - 1) = 0 \quad \text{and} \quad \beta^2 = c^{q+1}. \end{aligned}$$

So we have to count all pairs $(\alpha, \beta) \in K \times K^\times$ satisfying

$$\beta^q + \beta = \alpha^{q+1}, \beta^2 = c^{q+1} \quad \text{and} \quad \alpha(c\beta^{-1} - 1) = 0 \tag{5.2}$$

One checks that (5.2) has precisely the following solutions $(\alpha, \beta) \in K \times K^\times$:

Case 1. $c \in \mathbb{F}_q$. Then $\beta = c$ and $\alpha^{q+1} = 2c$.

Case 2. $c \notin \mathbb{F}_q$ and $c^{(q^2-1)/2} = 1$. There are no solutions of (5.2).

Case 3. $c \notin \mathbb{F}_q$ and $c^{(q^2-1)/2} = -1$. Then $\alpha = 0$ and $\beta = \pm c^{(q+1)/2}$. □

THEOREM 5.4. *Assume that* $\operatorname{char}(K) \neq 2$. *Let m be a divisor of $q^2 - 1$ and let $b \in K$ be an element of order m. Consider the group $\mathcal{G} := \langle \lambda, \omega \rangle \subseteq \mathcal{C}$ that is generated by the automorphisms λ and ω, where*

$$\lambda(x) = bx, \qquad \lambda(y) = b^{q+1}y \quad \textit{and} \quad \omega(x) = x/y, \qquad \omega(y) = 1/y.$$

Let $d := \gcd(m, q+1)$, $\tilde{d} := \gcd(m, q-1)$ *and*

$$\delta := \begin{cases} 0, & \textit{if } m \textit{ divides } (q^2-1)/2. \\ m, & \textit{otherwise}. \end{cases}$$

Then the fixed field $H^{\mathcal{G}}$ has genus

$$g(H^{\mathcal{G}}) = \frac{1}{4m}((q+1)(q-1-d-\tilde{d}) + 2(m+d) - \delta).$$

Proof. The group $\mathcal{G}$ has order $2m$; it consists of the following automorphisms σ_c and τ_c where

$$\sigma_c(x) = cx, \qquad \sigma_c(y) = c^{q+1}y, \quad c^m = 1,$$

https://doi.org/10.1023/A:1001736016924 Published online by Cambridge University Press

and

$$\tau_c(x) = c \cdot x/y, \qquad \tau_c(y) = c^{q+1} \cdot 1/y, \quad c^m = 1.$$

From Lemma 5.3(i) follows

$$\sum_{c^m=1, c\neq 1} N(\sigma_c) = (q+1)(d-1) + 2(m-d).$$

The number of elements $c \in \mathbb{F}_q$ with $c^m = 1$ is $\tilde{d} = \gcd(m, q-1)$. Now we distinguish two cases.

Case 1. m divides $(q^2-1)/2$. We see from Lemma 5.3 that in this case

$$\sum_{c^m=1} N(\tau_c) = \tilde{d}(q+1).$$

Case 2. m does not divide $(q^2-1)/2$. Now there are exactly $m/2$ elements $c \in K$ with $c^m = 1$ and $c^{(q^2-1)/2} = -1$, and all of them are in $K \setminus \mathbb{F}_q$. Hence Lemma 5.3 yields in this case

$$\sum_{c^m=1} N(\tau_c) = 2 \cdot m/2 + \tilde{d}(q+1) = \tilde{d}(q+1) + m.$$

In both cases we find that

$$\sum_{1\neq\sigma\in\mathcal{G}} N(\sigma) = (q+1)(d+\tilde{d}-1) + 2(m-d) + \delta,$$

with

$$\delta = \begin{cases} 0, & \text{if } m \text{ divides } (q^2-1)/2. \\ m, & \text{otherwise}. \end{cases}$$

Proposition 5.2 yields now the desired formula for the genus $g(H^{\mathcal{G}})$. □

EXAMPLE 5.5. (char$(K) \neq 2$).

https://doi.org/10.1023/A:1001736016924 Published online by Cambridge University Press

(i) *For any even divisor m of $q-1$, there is a subfield $E \subseteq H$ of genus*

$$g(E) = \frac{1}{4m}(q-1)(q-1-m).$$

(ii) *For any odd divisor m of $q-1$, there is a subfield $E \subseteq H$ of genus*

$$g(E) = \frac{1}{4m}(q-1)(q-m).$$

(iii) *For any even divisor m of $q+1$, there is a subfield $E \subseteq H$ of genus*

$$g(E) = \frac{1}{4m}(q-3)(q+1-m).$$

(iv) *For any odd divisor m of $q+1$, there is a subfield $E \subseteq H$ of genus*

$$g(E) = \frac{1}{4m}((q-3)(q+1-m)+q+1).$$

Proof. We use notations as in Theorem 5.4.

(i) Let m be an even divisor of $q-1$. Then $d = \gcd(m, q+1) = 2$, $\delta = 0$ and $\tilde{d} = \gcd(m, q-1) = m$. By Theorem 5.4 the genus of $E := H^{\mathcal{G}}$ is

$$g(E) = \frac{1}{4m}((q+1)(q-1-2-m)+2(m+2)) = \frac{1}{4m}(q-1)(q-1-m).$$

(ii) If m is an odd divisor of $q-1$, then $d = \gcd(m, q+1) = 1$, $\tilde{d} = \gcd(m, q-1) = m$ and $\delta = 0$. The genus of $E := H^{\mathcal{G}}$ is in this case

$$g(E) = \frac{1}{4m}((q+1)(q-1-1-m)+2(m+1)) = \frac{1}{4m}(q-1)(q-m).$$

The proofs of (iii) and (iv) are similar. □

We consider another class of subgroups $\mathcal{G} \subseteq \mathcal{C}$ in the following example:

EXAMPLE 5.6. (char$(K) \neq 2$). *Let m be an even divisor (resp. odd divisor) of $q-1$. Then there exists a subfield $E \subseteq H$ of genus*

$$g(E) = \begin{cases} \dfrac{(q-1)^2}{4m} \left(\textit{resp. } \dfrac{q(q-1)}{4m}\right), & \textit{if } q \equiv 1 \bmod 4, \\ \dfrac{(q-1)^2+2m}{4m} \left(\textit{resp. } \dfrac{q(q-1)+2m}{4m}\right), & \textit{if } q \equiv 3 \bmod 4. \end{cases}$$

Proof. Consider the following subgroup $\mathcal{G}_0 \subseteq \mathcal{A}$:

$$\mathcal{G}_0 := \{\sigma \in \mathcal{A} \mid \sigma(x) = ax, \sigma(y) = a^{q+1}y \text{ with } a^m = 1\}.$$

https://doi.org/10.1023/A:1001736016924 Published online by Cambridge University Press

Choose an element $b \in K$ such that $b^{q-1} = -1$ and define an automorphism $\rho \in \mathcal{A}$ by

$$\rho(x) = b \cdot x/y\,, \qquad \rho(y) = b^{q+1} \cdot 1/y.$$

It is easily verified that $\mathcal{G} := \mathcal{G}_0 \cup \rho\mathcal{G}_0$ is a subgroup of $\mathcal{C}$ of order ord $\mathcal{G} = 2m$. We get from Lemma 5.3(i):

$$\sum_{1\neq\sigma\in\mathcal{G}_0} N(\sigma) = (q+1) + (m-2)\cdot 2 = q - 3 + 2m, \text{ if } m \text{ is even, (resp.}$$

$$\sum_{1\neq\sigma\in\mathcal{G}_0} N(\sigma) = (m-1)\cdot 2, \text{ if } m \text{ is odd).}$$

The automorphisms $\tau \in \mathcal{G} \setminus \mathcal{G}_0$ are given by $\tau = \rho \circ \sigma$ with $\sigma \in \mathcal{G}_0$, hence

$$\tau(x) = ab \cdot x/y, \qquad \tau(y) = (ab)^{q+1} \cdot 1/y \text{ with } a^m = 1.$$

Since $ab \notin \mathbb{F}_q$ and

$$(ab)^{(q^2-1)/2} = (a^{q-1})^{(q+1)/2} \cdot (b^{q-1})^{(q+1)/2} = 1 \cdot (-1)^{(q+1)/2},$$

it follows from Lemma 5.3(ii) that

$$N(\tau) = \begin{cases} 0, & \text{for } q \equiv 3 \bmod 4. \\ 2, & \text{for } q \equiv 1 \bmod 4. \end{cases}$$

Therefore

$$\sum_{1\neq\sigma\in\mathcal{G}} N(\sigma) = \begin{cases} q - 3 + 2m, \ (\text{resp. } 2m-2) & \text{for } q \equiv 3 \bmod 4. \\ q - 3 + 4m, \ (\text{resp. } 4m-2) & \text{for } q \equiv 1 \bmod 4. \end{cases}$$

Now we apply Proposition 5.2 and obtain the desired formula for the genus $g(H^{\mathcal{G}})$. □

Many other tame subgroups $\mathcal{G}$ of $\mathcal{A}$ can be constructed if we represent the Hermitian function field as in (2.15): $H = K(u, v)$ with $u^{q+1} + v^{q+1} + 1 = 0$. All rational places $P \in \mathbb{P}(H)$ can then be described in the following manner.

(i) $P = Q_{\alpha,\beta}$ with $\alpha, \beta \in K$,

$$u(P) = \alpha, \qquad v(P) = \beta \quad \text{and} \quad \alpha^{q+1} + \beta^{q+1} + 1 = 0.$$

(ii) $P = Q_\alpha$ with $\alpha \in K$,

$$u(P) = v(P) = \infty, \qquad \left(\frac{u}{v}\right)(P) = \alpha \quad \text{and} \quad \alpha^{q+1} + 1 = 0.$$

https://doi.org/10.1023/A:1001736016924 Published online by Cambridge University Press

Let $\zeta \in K$ be a primitive $(q+1)$th root of unity and consider the automorphisms σ_1 and $\sigma_2 \in \mathcal{A}$ with

$$\sigma_1(u) = \zeta u, \qquad \sigma_1(v) = v, \quad \text{and} \quad \sigma_2(u) = u, \qquad \sigma_2(v) = \zeta v.$$

These maps generate a tame Abelian subgroup $\mathcal{D} = \langle \sigma_1, \sigma_2 \rangle \subseteq \mathcal{A}$,

$$\mathcal{D} = \{\sigma_1^i \sigma_2^j \mid i, j \in \mathbb{Z}/(q+1)\mathbb{Z}\}, \tag{5.3}$$

which is isomorphic to $\mathbb{Z}/(q+1)\mathbb{Z} \times \mathbb{Z}/(q+1)\mathbb{Z}$. The fixed field $H^{\mathcal{D}}$ of $\mathcal{D}$ is rational, namely $H^{\mathcal{D}} = K(u^{q+1}) = K(v^{q+1})$, and it is easily seen that only rational places of H are ramified in $H/H^{\mathcal{D}}$ (hence hypothesis $(*)$ from Proposition 5.2 holds for all subgroups $\mathcal{G} \subseteq \mathcal{D}$).

LEMMA 5.7. *Let* $1 \neq \sigma = \sigma_1^i \sigma_2^j \in \mathcal{D}$ *with* $i, j \in \mathbb{Z}/(q+1)\mathbb{Z}$. *Then*

$$N(\sigma) = \begin{cases} q+1 & \text{if } i = 0 \text{ or } j = 0 \text{ or } i = j, \\ 0 & \text{otherwise}. \end{cases}$$

Proof. For $i = 0$ we have $\sigma = \sigma_2^j \in \mathrm{Gal}(H/K(u))$. In the extension $H/K(u)$ exactly the $q+1$ zeros of v are ramified, hence $N(\sigma_2^j) = q+1$. In a similar manner one shows that $N(\sigma_1^j) = N((\sigma_1\sigma_2)^j) = q+1$ for $j \neq 0$ (observe that $(\sigma_1\sigma_2)^j \in \mathrm{Gal}(H/K(u/v))$). Now let $\sigma = \sigma_1^i \sigma_2^j$ with $i, j \neq 0$ and $i \neq j$. We have to show that none of the places $P = Q_{\alpha,\beta}$ resp. $P = Q_\alpha$ is invariant under σ.

Case (i). $P = Q_{\alpha,\beta}$. Assume that $\sigma P = P$. Then $\alpha = u(P) = (\sigma u)(P) = \zeta^i \alpha$, hence $\alpha = 0$. Moreover $\beta = v(P) = (\sigma v)(P) = \zeta^j \beta$, hence $\beta = 0$. This conflicts with the condition $\alpha^{q+1} + \beta^{q+1} + 1 = 0$.

Case (ii). $P = Q_\alpha$. Assume that $\sigma P = P$. Then

$$\alpha = \left(\frac{u}{v}\right)(P) = \left(\frac{\sigma u}{\sigma v}\right)(P) = \zeta^{i-j}\alpha.$$

As $i \neq j$ it follows that $\alpha = 0$ which is a contradiction to $\alpha^{q+1} + 1 = 0$. □

THEOREM 5.8. *Let* $\mathcal{G}$ *be a subgroup of* $\mathcal{D}$ (*as defined in* (5.3)). *Then*

$$g(H^{\mathcal{G}}) = 1 + \frac{(q+1)(q+1-r_1-r_2-r_3)}{2r},$$

with $r = \mathrm{ord}(\mathcal{G})$, $r_1 = \mathrm{ord}(\mathcal{G} \cap \langle \sigma_1 \rangle)$, $r_2 = \mathrm{ord}(\mathcal{G} \cap \langle \sigma_2 \rangle)$ *and* $r_3 = \mathrm{ord}(\mathcal{G} \cap \langle \sigma_1\sigma_2 \rangle)$.

Proof. Since $\langle \sigma_1 \rangle \cap \langle \sigma_2 \rangle = \langle \sigma_1 \rangle \cap \langle \sigma_1\sigma_2 \rangle = \langle \sigma_2 \rangle \cap \langle \sigma_1\sigma_2 \rangle = \{1\}$, we obtain from Lemma 5.7 that

$$\sum_{1 \neq \sigma \in \mathcal{G}} N(\sigma) = ((r_1 - 1) + (r_2 - 1) + (r_3 - 1)) \cdot (q+1).$$

https://doi.org/10.1023/A:1001736016924 Published online by Cambridge University Press

The result follows now from Proposition 5.2. □

EXAMPLE 5.9. *Let a, b be integers. Define*

$$d := \gcd(q+1, a, b), \qquad d_1 := \gcd(q+1, a),$$

$$d_2 := \gcd(q+1, b) \quad \textit{and} \quad d_3 := \gcd(q+1, a-b).$$

Then there exists a subgroup $\mathcal{G} \subseteq \mathcal{D}$ such that

$$g(H^{\mathcal{G}}) = 1 + \tfrac{1}{2}(d(q+1) - d_1 - d_2 - d_3).$$

Proof. We consider the cyclic group $\mathcal{G} \subseteq \mathcal{D}$ which is generated by the automorphism $\sigma := \sigma_1^a \sigma_2^b$. Then

$$\mathrm{ord}(\mathcal{G}) = (q+1)/d, \qquad \mathrm{ord}(\mathcal{G} \cap \langle\sigma_1\rangle) = d_2/d,$$

$$\mathrm{ord}(\mathcal{G} \cap \langle\sigma_2\rangle) = d_1/d \quad \text{and} \quad \mathrm{ord}(\mathcal{G} \cap \langle\sigma_1\sigma_2\rangle) = d_3/d.$$

The result now follows from Theorem 5.8. □

EXAMPLE 5.10. *Let $c \geqslant 1$ be an odd divisor (resp. even divisor) of $(q+1)$. Then there exists a subfield $H_0 \subseteq H$ such that H/H_0 is cyclic of degree $[H : H_0] = c$ and*

$$g(H_0) = 1 + \frac{(q-2)(q+1)}{2c} \left(\textit{resp. } g(H_0) = 1 + \frac{(q-3)(q+1)}{2c} \right).$$

Moreover the extension H/H_0 is unramified if c is odd.

Proof. Let $q+1 = a \cdot c$ and $b := 2a$. With notations as in Example 5.9 (i.e., $\mathcal{G}$ is the cyclic group generated by $\sigma_1^a \sigma_2^{2a}$), we have

$$\begin{aligned} &d = d_1 = d_2 = d_3 = a, && \text{if } c \text{ is odd,} \\ &d = d_1 = d_3 = a;\ d_2 = 2a, && \text{if } c \text{ is even.} \end{aligned}$$

The formula for the genus $g(H_0)$ now follows from Example 5.9. If c is an odd divisor of $(q+1)$ then H/H_0 is unramified because $d = d_1 = d_2 = d_3 = a$ in this case and hence

$$\mathcal{G} \cap \langle\sigma_1\rangle = \mathcal{G} \cap \langle\sigma_2\rangle = \mathcal{G} \cap \langle\sigma_1\sigma_2\rangle = \{1\}.$$ □

EXAMPLE 5.11. *Let $a, b \geqslant 1$ be divisors of $q+1$, and let $d := \gcd(a, b)$. Then there exists a subgroup $\mathcal{G} \subseteq \mathcal{D}$ such that $g(H^{\mathcal{G}}) = 1 + \frac{1}{2}(ab - a - b - d)$.*

Proof. In this case we choose the subgroup $\mathcal{G} \subseteq \mathcal{D}$ that is generated by σ_1^a and σ_2^b. Then

$$\mathrm{ord}(\mathcal{G}) = (q+1)^2/ab, \qquad \mathrm{ord}(\mathcal{G} \cap \langle\sigma_1\rangle) = (q+1)/a,$$

$$\mathrm{ord}(\mathcal{G} \cap \langle\sigma_2\rangle) = (q+1)/b \quad \text{and} \quad \mathrm{ord}(\mathcal{G} \cap \langle\sigma_1\sigma_2\rangle) = (q+1)/\mathrm{lcm}(a,b).$$

The result follows from Theorem 5.8. □

We give yet another example of a tame subgroup $\mathcal{E} \subseteq \mathcal{A}$. Let $H = K(u,v)$ be generated as above, i.e. $u^{q+1} + v^{q+1} + 1 = 0$. Consider the automorphisms τ and $\rho \in \mathcal{A}$ given by

$$\tau(u) = v, \qquad \tau(v) = u, \quad \text{and} \quad \rho(u) = \frac{v}{u}, \qquad \rho(v) = \frac{1}{u}.$$

Then $\tau^2 = \rho^3 = 1$ and $\tau^{-1}\rho\tau = \rho^2$, hence

$$\mathcal{E} := \langle\tau, \rho\rangle \tag{5.4}$$

is a group of order 6 isomorphic to the symmetric group $\mathcal{S}_3$. For $p \neq 2, 3$ this is a tame subgroup of $\mathcal{A}$.

EXAMPLE 5.12. *The genus of the fixed field of $\mathcal{E}$ is*

$$g(H^{\mathcal{E}}) = \begin{cases} \frac{1}{12}(q^2 - 4q + 3) & \text{for } q \equiv 1 \bmod 6, \\ \frac{1}{12}(q^2 - 4q + 7) & \text{for } q \equiv 5 \bmod 6. \end{cases}$$

Proof. The automorphism τ fixes exactly the places $P = Q_{\alpha,\alpha}$ with $2\alpha^{q+1}+1 = 0$, hence $N(\tau) = q + 1$. One checks easily that

$$N(\rho) = \begin{cases} 2 & \text{if } q \equiv 1 \bmod 6, \\ 0 & \text{if } q \equiv 5 \bmod 6. \end{cases}$$

As all elements of order 2 in $\mathcal{E}$ are conjugate to τ, we obtain

$$\begin{aligned} \sum_{1 \neq \sigma \in \mathcal{E}} N(\sigma) &= 3 \cdot N(\tau) + N(\rho) + N(\rho^2) \\ &= 3(q+1) + 2N(\rho) \\ &= \begin{cases} 3q + 7 & \text{if } q \equiv 1 \bmod 6, \\ 3q + 3 & \text{if } q \equiv 5 \bmod 6. \end{cases} \end{aligned}$$

The claim follows now from Proposition 5.2. □

https://doi.org/10.1023/A:1001736016924 Published online by Cambridge University Press

6. Supplementary Remarks

In Section 1 we defined the set $\Gamma(q^2) = \{g \geqslant 0 \mid$ there is a maximal function field over $\mathbb{F}_{q^2}$ of genus $g\}$, and we remarked that

$$g \in \Gamma(q^2) \Rightarrow g \leqslant \frac{(q-1)^2}{4} \quad \text{or} \quad g = \frac{q(q-1)}{2}. \tag{6.1}$$

The genera of subfields of the Hermitian function field $H/\mathbb{F}_{q^2}$ are in $\Gamma(q^2)$. Combining (6.1) with the results of this paper, we obtain.

Remark 6.1. For $q \leqslant 16$ holds

$$\Gamma(2^2) = \{0, 1\}, \qquad \Gamma(3^2) = \{0, 1, 3\};$$

$$\Gamma(4^2) = \{0, 1, 2, 6\}; \qquad \Gamma(5^2) = \{0, 1, 2, 3, 4, 10\};$$

$$\{0, 1, 2, 3, 5, 7, 9, 21\} \subseteq \Gamma(7^2) \subseteq [0, 9] \cup \{21\};$$

$$\{0, 1, 2, 3, 4, 6, 7, 9, 10, 12, 28\} \subseteq \Gamma(8^2) \subseteq [0, 12] \cup \{28\};$$

$$\{0, 1, 2, 3, 4, 6, 8, 9, 12, 16, 36\} \subseteq \Gamma(9^2) \subseteq [0, 16] \cup \{36\};$$

$$\{0, 1, 2, 3, 4, 5, 7, 9, 10, 11, 13, 15, 18, 19, 25, 55\} \subseteq \Gamma(11^2) \subseteq [0, 25] \cup \{55\};$$

$$\{0, 2, 3, 6, 9, 12, 15, 18, 26, 36, 78\} \subseteq \Gamma(13^2) \subseteq [0, 36] \cup \{78\};$$

$$\{0, 1, 2, 4, 6, 8, 12, 24, 28, 40, 56, 120\} \subseteq \Gamma(16^2) \subseteq [0, 56] \cup \{120\}.$$

Proof. We give the details only for $q = 5$ and $q = 8$; the other cases are similar.

$q = 5$: $\Gamma(5^2) \subseteq \{0, 1, 2, 3, 4, 10\}$ follows from (6.1). By Corollary 4.9 the Hermitian function field $H/\mathbb{F}_{25}$ contains subfields of genus 0, 1, 2, 4 and 10, and Theorem 5.1 provides a subfield of genus 3.

$q = 8$: $\Gamma(8^2) \subseteq [0, 12] \cup \{28\}$ follows from (6.1). By Corollary 4.9 the Hermitian function field over $\mathbb{F}_{64}$ contains subfields of genus 0, 1, 4, 7 and 28. Corollary 3.4 gives subfields of H of genus $g = 2^{2-v}(2^{3-w}-1)$ for $(v, w) = (0, 0), (0, 1), (0, 2), (1, 1), (1, 2), (2, 2)$ and $(2, 1)$, so 1, 2, 3, 4, 6, 12, 28 are in $\Gamma(8^2)$. Theorem 5.1 provides a subfield of genus $(19-1)/2 = 9$, and Theorem 5.8 yields a subfield of genus 10 (taking $r = 3$ and $r_1 = r_2 = r_3 = 1$, with notations as in Theorem 5.8). □

All entries in the tables of Remark 6.1 come from subfields of the Hermitian function field. We can add the entry $g = 1$ for $q = 13$, since $1 \in \Gamma(q^2)$ for all q, see

https://doi.org/10.1023/A:1001736016924 Published online by Cambridge University Press

[Se]. The results of Remark 6.1 for $q = 2, 3, 4, 5$ and 9 are known [Se], [X–St], [G–V 8]. For $q = 8$ the fact that $9 \in \Gamma(8^2)$ seems to be new [G–V 8].

It is known that $\{0, 1, 2\} \subseteq \Gamma(q^2)$ for all sufficiently large q, see [Se]. For an arbitrary integer $a \geqslant 0$ we can prove a weaker result

Remark 6.2. Given an integer $a \geqslant 0$, there exist infinitely many q with $a \in \Gamma(q^2)$.

Proof. Choose q such that $q \equiv -1 \bmod (2a+1)$ holds. Then $m := (q^2-1)/(2a+1)$ is a divisor of q^2-1 and $\gcd(m, q+1) = (q+1)/(2a+1)$. By Corollary 4.9 there is a subfield E of H of genus

$$g = \frac{1}{2m}\left(q+1-\frac{q+1}{2a+1}\right)(q-1) = a. \qquad \square$$

In many cases one can easily describe the fixed field $E = H^{\mathcal{G}}$ (for a group $\mathcal{G}$ of automorphisms of the Hermitian function field H) in terms of generators of E. Here are some examples.

EXAMPLE 6.3 (cf. Corollary 4.9). *Consider $H = \mathbb{F}_{q^2}(x, y)$ with $y^q + y = x^{q+1}$ and the automorphism ϵ of $H/\mathbb{F}_{q^2}$ given by $\epsilon(x) = ax$, $\epsilon(y) = a^{q+1}y$, where a is a primitive (q^2-1)th root of unity. Then $\operatorname{ord}(\epsilon) = q^2-1$, and for any $m \mid (q^2-1)$ there is a unique subgroup $\mathcal{G} \subseteq \langle\epsilon\rangle$ of order m. The fixed field $E = H^{\mathcal{G}}$ can be generated by two functions z, t satisfying the irreducible equation*

$$z^n = t(t+1)^{q-1}, \quad \text{with } n := (q^2-1)/m.$$

Proof. Let $t := y^{q-1}$; then $H = \mathbb{F}_{q^2}(x, y) = \mathbb{F}_{q^2}(x, t)$ with

$$x^{q^2-1} = (y^q + y)^{q-1} = y^{q-1}(y^{q-1}+1)^{q-1} = t(t+1)^{q-1}.$$

Setting $z := x^m$ we obtain $E = H^{\mathcal{G}} = \mathbb{F}_{q^2}(z, t)$ and $z^n = t(t+1)^{q-1}$. $\square$

EXAMPLE 6.4 (cf. also [La] and [L, p. 40]). *Here we give equations for some other maximal curves. Let the Hermitian function field be represented by its Fermat equation:*

$$v^{q+1} = (-1)\cdot\left(u^{q+1}+1\right). \qquad (6.2)$$

We will consider two cases and in both cases we will have that u^{q+1} belongs to the function field of the maximal curve considered and hence Theorem 5.8 *applies to both cases.*

Case 1. Let $k \in \mathbb{N}$ and $m|(q+1)$. Multiplying Equation (6.2) by u^{km}, we get

$$z^m + t^k\left(t^{\frac{q+1}{m}}+1\right) = 0, \qquad (6.3)$$

https://doi.org/10.1023/A:1001736016924 Published online by Cambridge University Press

where $z = u^k \cdot v^{\frac{q+1}{m}}$ and $t = u^m$.

Equation (6.3) is the equation of a maximal curve over $\mathbb{F}_{q^2}$ with genus g given by (see [St 1, Prop. III.7.3])

$$2g = \frac{q+1}{m}(m-1) - (\delta_1 + \delta_2 - 2),$$

where $\delta_1 = \gcd(m, k)$ and $\delta_2 = \gcd\left(m, \frac{q+1}{m} + k\right)$.

The field $K(z, t)$ is the fixed field of the group $\mathcal{G}$ inside $\mathcal{D}$ (notations as in (5.3)) of order $q + 1$ corresponding to pairs (i, j) with

$$i \equiv 0 \left(\operatorname{mod} \frac{q+1}{m}\right) \quad \text{and} \quad \frac{mi}{q+1} \cdot k + j \equiv 0 (\operatorname{mod} m).$$

Case 2: Let k and b be two natural numbers. Raising Equation (6.2) to the kth power and then multiplying by $u^{b(q+1)}$, we get

$$z^{m_1} = (-1)^k t^{bm} \cdot (t^m + 1)^k, \tag{6.4}$$

where m_1 and m are divisors of $(q + 1)$, $z = (u^b v^k)^{\frac{q+1}{m_1}}$ and $t = u^{\frac{q+1}{m}}$.

Equation (6.4) is the equation of a maximal curve over $\mathbb{F}_{q^2}$ with genus g given by (see [St 1, Prop. III.7.3]) $2g = m(m_1 - \delta_1) - (\delta_2 + \delta_3 - 2)$, where $\delta_1 = \gcd(m_1, k)$, $\delta_2 = \gcd(m_1, bm)$ and $\delta_3 = \gcd(m_1, (b + k)m)$.

In this case, the field $K(z, t)$ is the fixed field of the group $\mathcal{G}$ of the order $(q + 1)^2/mm_1$ corresponding to pairs (i, j) with

$$i \equiv 0 \ (\operatorname{mod} m) \quad \text{and} \quad ib + jk \equiv 0 \ (\operatorname{mod} m_1). \qquad \square$$

Remark 6.5. Defining equations for the fields $H^{\mathcal{G}}$, where $\mathcal{G} \subseteq \mathcal{A}$ is a nonabelian tame subgroup of $\mathcal{A}$ as considered in Theorem 5.4, are related to Chebyshev polynomials; for details we refer to [G–S].

Remark 6.6. Subfields of the Hermitian function field cover almost all examples of maximal function fields that we found in the literature, see [D–H], [D–S–V], [G–V, 1–8], [I], [La], [M–K], [Se], [St 1], [W 1,2].

Except at the end of Section 5 and in Example 6.4 we have not used the fact that the Hermitian function field H can be given by a Fermat equation.

$$H = K(u, v) \quad \text{with} \quad u^{q+1} + v^{q+1} + 1 = 0.$$

There is a natural subgroup $\mathcal{F}$ of the automorphism group $\mathcal{A}$ to consider here. It consists of the elements $\sigma(u) = au + bv$ and $\sigma(v) = cu + dv$ satisfying:

$$a^{q+1} + c^{q+1} = 1, \qquad b^{q+1} + d^{q+1} = 1 \quad \text{and} \quad a^q b + c^q d = 0.$$

https://doi.org/10.1023/A:1001736016924 Published online by Cambridge University Press

It can be shown that the order of this subgroup $\mathcal{F}$ is equal to $(q^3 - q) \cdot (q + 1)$. It would be interesting to determine the genera of fixed fields of subgroups of this group $\mathcal{F}$. At the end of Section 5 we have considered subgroups with $b = c = 0$. Here we will consider two further examples:

EXAMPLE 6.7 (char $K \neq 2$). *For two elements $b, c \in K$ with $b^{q+1} = c^{q+1} = 1$, let σ be the automorphism given by:*

$$\sigma(u) = bv \quad \text{and} \quad \sigma(v) = cu.$$

We then have that

$$\sigma^{2n}(u) = (bc)^n \cdot u \quad \text{and} \quad \sigma^{2n}(v) = (bc)^n \cdot v;$$
$$\sigma^{2n+1}(u) = (bc)^n \cdot bv \quad \text{and} \quad \sigma^{2n+1}(v) = (bc)^n \cdot cu.$$

Denoting by M the multiplicative order of the element bc, we have that the cyclic subgroup of $\mathcal{F}$ generated by σ has order equal to $2M$. Since we assumed that char $K \neq 2$, *the cyclic group $\langle\sigma\rangle$ is tame. Denoting by $N(\sigma_1)$ the number of fixed points of an automorphism $\sigma_1 \in \langle\sigma\rangle$, one can check that:*

$$N(\sigma^{2n}) = q + 1, \text{ for } n = 1, 2, \ldots, M - 1, \quad \text{and}$$
$$N(\sigma^{2n+1}) = \begin{cases} 2, & \text{if } (q+1)/M \text{ is odd,} \\ q + 1, & \text{if } M \text{ is odd and } n = (M-1)/2, \\ 0, & \text{otherwise.} \end{cases}$$

Now it follows from Proposition 5.2 that the genus g of the fixed field of $\langle\sigma\rangle$ is given by:

$$4Mg = \begin{cases} (q+1)(q-1) - (q-1)M, & \text{if } (q+1)/M \text{ odd,} \\ (q+1)(q-1) - (q-3)M, & \text{if } (q+1)/M \text{ even and } M \text{ even,} \\ (q+1)(q-2) - (q-3)M, & \text{if } M \text{ odd.} \end{cases}$$

If M is odd the genus formula above coincides with the one in Example 5.5(iv). *If M is even and M is a proper divisor of $(q+1)$, then the genus formula above does not coincide with the one given in Example* 5.5(iii). □

EXAMPLE 6.8 (char $K \neq 2$). *Let m be a divisor of $(q + 1)$. We have m^2 automorphisms of H of the form below.*

$$\sigma(u) = bv \quad \text{and} \quad \sigma(v) = cu, \quad \text{with } b^m = c^m = 1. \tag{6.5}$$

These automorphisms generate a subgroup $\mathcal{G}$ of $\mathcal{F}$ having $2m^2$ elements; the other m^2 elements being of the form below.

$$\tau(u) = bu \quad \text{and} \quad \tau(v) = cv, \quad \text{with } b^m = c^m = 1. \tag{6.6}$$

https://doi.org/10.1023/A:1001736016924 Published online by Cambridge University Press

Since char$(K) \neq 2$, *we have that* $\mathcal{G}$ *is tame. The number of fixed points* $N(\tau)$ *for automorphisms* τ *as in* (6.6) *above is easily seen to satisfy (see Lemma* 5.7*):*

$$N(\tau) = \begin{cases} q+1, & \text{if } b = 1 \text{ and } c \neq 1. \\ q+1, & \text{if } c = 1 \text{ and } b \neq 1. \\ q+1, & \text{if } b = c \neq 1. \\ 0, & \text{otherwise}. \end{cases}$$

Hence summing over τ *as in* (6.6), *we get*

$$\sum_{1 \neq \tau} N(\tau) = 3(m-1)(q+1). \tag{6.7}$$

It remains to determine $N(\sigma)$ *for automorphisms* σ *as in* (6.5) *above. For these automorphisms we have:*

$$N(\sigma) = \begin{cases} q+1, & \text{if } bc = 1. \\ 2, & \text{if } (bc)^{\frac{q+1}{2}} = -1. \\ 0, & \text{otherwise}. \end{cases}$$

Hence summing over σ *as in* (6.5), *we get*

$$\sum_{\sigma} N(\sigma) = \begin{cases} m(q+1), & \text{if } (q+1)/m \text{ is even}. \\ m(q+1+m), & \text{if } (q+1)/m \text{ is odd}. \end{cases} \tag{6.8}$$

It now follows from (6.7), (6.8) *and Proposition* 5.2 *that the genus* $g = g(H^{\mathcal{G}})$ *is given by:*

$$4m^2 g = \begin{cases} 4m^2 + (q+1)(q+1-4m), & \text{if } (q+1)/m \text{ is even}. \\ 3m^2 + (q+1)(q+1-4m), & \text{if } (q+1)/m \text{ is odd}. \end{cases}$$

Particularly interesting is the case $m = 2$. *In this case the group* $\mathcal{G}$ *is the dihedral group with 8 elements and we have:*

$$g = \begin{cases} (q-3)^2/16, & \text{if } q \equiv 3 \bmod 4. \\ (q-1)(q-5)/16, & \text{if } q \equiv 1 \bmod 4. \end{cases}$$ □

The following remark was communicated to us by J.-P. Serre:

Remark 6.9. The natural action of $\mathcal{A} = \mathcal{A}ut(H)$ on the l-adic Tate module of the Hermitian curve (where l is a prime number not dividing q) gives rise to a representation $\rho\colon \mathcal{A} \to \mathrm{GL}_{2g}(\mathbb{Q}_l)$. The corresponding character χ is irreducible and has values in $\mathbb{Q}$. For a subgroup $\mathcal{B} \subseteq \mathcal{A}$, the genus $g(H^{\mathcal{B}})$ is given by

$$2g(H^{\mathcal{B}}) = \frac{1}{\text{ord } \mathcal{B}} \cdot \sum_{\sigma \in \mathcal{B}} \chi(\sigma).$$

https://doi.org/10.1023/A:1001736016924 Published online by Cambridge University Press

This formula comes from the orthogonality relations for characters of irreducible representations, applied to the restriction $\chi|_{\mathcal{B}}$ and to the identity $\mathrm{id}_{\mathcal{B}}$.

As an example, consider the case $q = 8$ and a subgroup $\mathcal{B} = \langle\sigma\rangle \subseteq \mathcal{A}$ of order 3. The values of the character χ can be found in the Atlas of finite groups [C, p. 64]. Depending on the type of σ one has $\chi(\sigma) = -7$ or $\chi(\sigma) = -1$ or $\chi(\sigma) = 2$. Hence

$$g(H^{\mathcal{B}}) = \tfrac{1}{6}(\chi(\mathrm{id}) + \chi(\sigma) + \chi(\sigma^2)) = \tfrac{1}{6}(56 + 2 \cdot \chi(\sigma)),$$

and therefore $g(H^{\mathcal{B}}) = 7$ or 9 or 10. The case $g(H^{\mathcal{B}}) = 9$ corresponds to our Theorem 5.1; the other cases are special cases of Example 5.11.

References

[C] Conway, J. H. *et al.*: *Atlas of Finite Groups*, Clarendon Press, Oxford, 1985.

[D–H] Davenport, H. and Hasse, H.: Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen, *J. Reine Angew. Math.* **172** (1934), 151–182.

[D–S–V] Duursma, I., Stichtenoth, H. and Voss, C.: Generalized Hamming weights for duals of BCH codes, and maximal algebraic function fields, In: R. Pellikaan, M. Perret, S. G. Vladut (eds), *Arithmetic, Geometry and Coding Theory*, Proceedings Luminy (1993), De Gruyter, Berlin, 1996, pp. 53–65.

[F–T 1] Fuhrmann, R. and Torres, F.: The genus of curves over finite fields with many rational points, *Manuscr. Math.* **89** (1996), 103–106.

[F–T 2] Fuhrmann, R. and Torres, F.: On curves over finite fields with many rational points. International Centre for Theoretical Physics Preprint IC/96/47, Trieste, 1996.

[F–G–T] Fuhrmann, R., Garcia, A. and Torres, F.: On maximal curves, *J. Number Theory* **67** (1997), 29–51.

[G–S] Garcia, A. and Stichtenoth, H.: On Chebyshev polynomials and maximal curves, Preprint 1998.

[G–V 1] van der Geer, G. and van der Vlugt, M.: Weight distributions for a certain class of codes and maximal curves, *Discr. Math.* **106/107** (1992), 209–218.

[G–V 2] van der Geer, G. and van der Vlugt, M.: Fibre products of Artin–Schreier curves and generalized Hamming weights of codes, *J. Comb. Theory A* **70** (1995), 337–348.

[G–V 3] van der Geer, G. and van der Vlugt, M.: Curves over finite fields of characteristic 2 with many rational points, *C.R. Acad. Sci. Paris, Ser. I* **317** (1993), 693–597.

[G–V 4] van der Geer, G. and van der Vlugt, M.: Generalized Hamming weights of codes and curves over finite fields with many points, in *Israel Math. Conf. Proc.* **9** (1996), 417–432.

[G–V 5] van der Geer, G. and van der Vlugt, M.: Generalized Reed-Muller Codes and Curves with Many Points, Preprint 1997.

[G–V 6] van der Geer, G. and van der Vlugt, M.: Quadratic forms, generalized Hamming weights of codes and curves with many points, *J. Number Theory* **59** (1966), 20–36.

[G–V 7] van der Geer, G. and van der Vlugt, M.: How to construct curves over finite fields with many points, In: F. Cortona (ed.), *Arithmetic Geometry*, Cambridge Univ. Press, Cambridge, 1997, pp. 169–189.

[G–V 8] van der Geer, G. and van der Vlugt, M.: *Tables for the Function* $N_q(g)$, Jan. 1998. ttp://www.wins.uva.nl/˜geer.

[I] Ibukiyama, T.: On rational points of curves of genus 3 over finite fields. *Tohoku Math. J.* 45 (1993) 311–329.

[L] Lang, S.: *Introduction to Algebraic and Abelian Functions*, 2nd edn, Springer-Verlag, Berlin, Heidelberg, 1982.

[La] Lachaud, G.: Sommes d'Eisenstein et nombre de points de certaines courbes algébriques sur les corps finis, *C.R. Acad. Sci. Paris* **305** (1987), 729–732.

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

[M–K] Miura, S. and Kamiya, N.: Geometric Goppa codes on some maximal curves and their minimum distance, *Proc. IEEE Workshop on Information Theory*, Susono-shi, Japan, June (1993), pp. 85–86.

[N–X] Niederreiter, H. and Xing, C. P.: Drinfeld modules of rank 1 and algebraic curves with many rational points II, *Acta Arith*. **81** (1997), 81–100.

[R–St] Rück, H. G. and Stichtenoth, H.: A Characterization of Hermitian Function Fields over Finite Fields, *J. Reine Angew. Math.* **457** (1994), 185–188.

[Se] Serre, J.-P.: Résumé des cours de 1983–1984, In: *Ann. Collège de France*, 1984, pp. 79–83.

[St 1] Stichtenoth, H.: *Algebraic Function Fields and Codes*, Springer-Verlag, Berlin, 1993.

[St 2] Stichtenoth, H.: Algebraic–geometric codes associated to Artin–Schreier extensions of $\mathbb{F}_q(z)$, In: *Proc. 2nd Int. Workshop on Algebra and Combin. Coding Theory*, Leningrad (1990), pp. 203–206.

[St 3] Stichtenoth, H.: Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik I, II, *Arch. Math.* **24** (1973), 524–544 and 615–631.

[W 1] Wolfmann, J.: Nombre de points rationnels de courbes algébriques sur des corps finis associées à des codes cycliques, *C.R. Acad. Sci. Paris, Sér. I* **305** (1987), 345–348.

[W 2] Wolfmann, J.: The number of points on certain algebraic curves over finite fields, *Comm. Algebra* **17** (1989), 2055–2060.

[X–St] Xing, C. P. and Stichtenoth, H.: The genus of maximal function fields over finite fields, *Manuscr. Math.* **86** (1995), 217–224.