ACTA ARITHMETICA
120.1 (2005)

Number of rational places of subfields of the function field of the Deligne–Lusztig curve of Ree type

by

Emrah Çakçak and Ferruh Özbudak (Ankara)

1. Introduction. Let $\mathbb{F}_q$ be a finite field with q elements and $\overline{\mathbb{F}}_q$ denote its algebraic closure. Let $\mathcal{X}$ be a Deligne–Lusztig curve of Ree type defined over $\mathbb{F}_q$, $q = 3^{2s+1}$, $s \geq 1$, and F be its function field. Then $F/\mathbb{F}_q$ is $\mathbb{F}_q(x, y_1, y_2)$ defined by the system of equations

$$y_1^q - y_1 = x^{q_0}(x^q - x), \quad y_2^q - y_2 = x^{2q_0}(x^q - x), \tag{1.1}$$

where $q_0 = 3^s$. For the function field F, we have the following properties ([H-P], [P]):

(P1) $F/\mathbb{F}_q$ has genus $g = \frac{3}{2}\, q_0(q-1)(q+q_0+1)$.

(P2) The automorphisms in $G = \mathrm{Aut}(F\overline{\mathbb{F}}_q/\overline{\mathbb{F}}_q)$ are $\mathbb{F}_q$-rational and G is a Ree group of order

$$q^3(q-1)(q^3+1) = 8q^3\,\frac{q-1}{2}\,\frac{q+1}{4}\,(q+3q_0+1)(q-3q_0+1).$$

(P3) $F/\mathbb{F}_q$ has q^3+1 rational places on which G acts as a permutation group.

(P4) The L-polynomial ([S, V.1.14]) of F is

$$L(t) = (1+3q_0t+qt^2)^{q_0(q^2-1)}(1+qt^2)^{q_0(q-1)(q+3q_0+1)/2}.$$

(P5) For any integer $m \geq 1$, the number of rational places of $F\mathbb{F}_{q^m}/\mathbb{F}_{q^m}$ is

$$N_m = q^m + 1 - q_0 q^{m/2}(q-1)\left[(q+3q_0+1)\cos\frac{m\pi}{2} + 2(q+1)\cos\frac{5m\pi}{6}\right].$$

In particular $F\mathbb{F}_{q^m}/\mathbb{F}_{q^m}$ is maximal if and only if $m \equiv 6 \bmod 12$.

Note that properties (P1), (P2) and (P3) uniquely determine F (see [H-P]).

Throughout this paper, F will denote $\mathbb{F}_q(x, y_1, y_2)$ defined in (1.1) and G its automorphism group $\mathrm{Aut}(F/\mathbb{F}_q)$. For a subgroup $H \leq G$, we denote by

2000 *Mathematics Subject Classification*: 11R58, 11G20, 14G15.

F^H its fixed subfield

$$F^H = \{z \in F \mid \sigma z = z \text{ for all } \sigma \in H\}.$$

In [C-O], we have determined the genera of a large family of subfields $\mathbb{F}_q \subsetneq F^H \subsetneq F$ corresponding to subgroups $H \leq G$. Function fields with many rational places are interesting and have many applications to coding theory and related areas ([T-V], [S], [N-X]). A function field E of genus $g(E)$ with full constant field $\mathbb{F}_q$ is called *optimal* if it has as many rational places as possible among the function fields of genus $g(E)$ with full constant field $\mathbb{F}_q$. It is well known that F is an optimal function field. We will show that some subfields of F also have many rational places. Using the methods of [C-O], it is easy to determine the number of rational places under degree 1 places of F for the subfields constructed in [C-O]. However, for most of the subgroups $H \leq G$, there will be rational places of F^H below higher degree places of F (cf. [C-O, Remark 4.38]).

In this paper we determine the exact number of rational places of some subfields of the form F^H. We also determine the genera corresponding to subgroups of the normalizer of a 3-Sylow subgroup of G, which was not considered in [C-O]. We note that, as the L-polynomial of F has two irreducible factors, the knowledge of the genus and the number of rational places of a subfield of F enables us to determine its L-polynomial completely (see Remark 7.2).

Let $E/\mathbb{F}_q$ be a function field and $H \leq \mathrm{Aut}(E/\mathbb{F}_q)$ be a subgroup of the automorphism group $\mathrm{Aut}(E/\mathbb{F}_q)$. In Section 4, under some assumptions, we introduce a method in order to compute the number of rational places of E^H below higher degree places of E. This method allows us to determine the exact number of rational places of F^H for some $H \leq G$. In particular we determine the number of rational places corresponding to subgroups of the normalizer of a 3-Sylow subgroup of G or to subgroups of a dihedral group D of order $2(q-1)$ in G.

The paper is organized as follows. In Section 2, we give some basic observations on the number of rational places of the subfields of $E^H \leq E$ of a function field $E/\mathbb{F}_q$ corresponding to subgroups $H \leq \mathrm{Aut}(E/\mathbb{F}_q)$. In Section 3 we determine the number of rational places below degree 6 places of F and hence, for an involution κ, we determine the number of rational places of F^H and $F^{\langle\kappa\rangle\times H}$, where H is an elementary Abelian 3-group in the centralizer of κ. We introduce our method and compute the number of rational places below higher degree places of F in Section 4. Then we determine the genera and the number of rational places of the subfields corresponding to subgroups of the normalizer of a 3-Sylow subgroup of G. Section 6 considers the subfields corresponding to subgroups of the dihedral group D. We give some numerical examples in Section 7, including some function fields with

the best known number of rational places (cf. [G-V]). Moreover we find a *new entry* for the table [G-V] and we determine its explicit defining equations.

2. Some general observations. Let E be a function field over $\mathbb{F}_q$ and $H \leq \mathrm{Aut}(E/\mathbb{F}_q)$ be a subgroup of the automorphism group of E over $\mathbb{F}_q$. In this section we give some basic observations on the number of rational places of E^H.

For $m \geq 1$, let B_m denote the set of degree m places of E. We can determine $|B_m|$ using the L-polynomial of E. For each $m \geq 1$, $\mathrm{Aut}(E/\mathbb{F}_q)$ and hence H acts on B_m. Let $\boldsymbol{\mathcal{O}}(H, m)$ denote the set of orbits of the action of H on B_m. We have

$$|B_m| = \sum_{\mathcal{O} \in \boldsymbol{\mathcal{O}}(H,m)} |\mathcal{O}|. \tag{2.1}$$

For any orbit $\mathcal{O} \in \boldsymbol{\mathcal{O}}(H, m)$, we have

$$Q_1, Q_2 \in \mathcal{O} \;\Rightarrow\; Q_1 \cap E^H = Q_2 \cap E^H.$$

We call $P = Q_1 \cap E^H$ the *place of* E^H *under the orbit* $\mathcal{O}$. Conversely, for any place P of E^H, there is a uniquely determined integer $m \geq 1$ and a uniquely determined orbit $\mathcal{O} \in \boldsymbol{\mathcal{O}}(H, m)$ such that P is the place of E^H under the orbit $\mathcal{O}$. We call $\mathcal{O}$ the *orbit of* E *over the place* P.

Let $\mathcal{O} \in \boldsymbol{\mathcal{O}}(H, m)$ be an orbit, $Q_1, Q_2 \in \mathcal{O}$ be places in $\mathcal{O}$ and P be the place of E^H under the orbit $\mathcal{O}$. As E/E^H is a Galois extension, we have $e(Q_1|P) = e(Q_2|P)$, $f(Q_1|P) = f(Q_2|P)$ and

$$|\mathcal{O}| = \frac{|H|}{f(Q_1|P)e(Q_1|P)}. \tag{2.2}$$

Moreover if P is a rational place of E^H, then we have a tower of subgroups $H_0(Q) \leq H_{-1}(Q) \leq H$ such that

$$H_{-1}(Q)/H_0(Q) \cong \mathbb{Z}_m, \tag{2.3}$$

where $H_{-1}(Q)$ and $H_0(Q)$ are the decomposition and inertia groups of a place $Q \in \mathcal{O}$ of the orbit $\mathcal{O}$ of E over P.

We denote the number of rational places of E^H by $N(E^H)$. For $m \geq 1$, $N(E^H, m)$ denotes the number of rational places of E^H under the orbits of $\boldsymbol{\mathcal{O}}(H, m)$. Then we have

$$N(E^H) = \sum_{m=1}^{\infty} N(E^H, m).$$

We note that for $g \in \mathrm{Aut}(E/\mathbb{F}_q)$ and $m \geq 1$,

$$N(E^H, m) = N(E^{gHg^{-1}}, m).$$

Consider now the function field F defined by (1.1) and let H be a subgroup of $G = \mathrm{Aut}(F/\mathbb{F}_q)$. The number $N(F^H, 1)$ can be calculated using the action of G on the degree 1 places of F (see [C-O, Examples 4.39, 4.40]). It follows from property (P5) of Section 1 that there is no degree 2 or degree 3 place of F. Again using the action of G on the degree 6 places of F we show how to compute $N(F^H, 6)$ in Section 3. In Section 4 we introduce a method to compute, under some assumptions, the number of rational places below unramified places of degree $m > 1$ for a function field E and apply this method to F.

3. Rational places below degree 6 places. Let F be the function field defined by (1.1). Let H be a subgroup of $G = \mathrm{Aut}(F/\mathbb{F}_q)$ containing elements of order 6. In this section we compute $N(F^H, 6)$, the number of rational places of F^H below degree 6 places of F. We show that the methods of [C-O] can be used for determining the number of rational places of subfields below degree 6 places of F, as in the case of degree 1 places of F. There is no degree 2 or degree 3 place of F. To determine the number of rational places below degree m places with $m \notin \{1, 2, 3, 6\}$, we will need another method introduced in Section 4. Let κ be an involution of G. Then the centralizer $C(\kappa)$ of κ can be written as $C(\kappa) = \langle\kappa\rangle \times L'$, where L' is the unique subgroup of $C(\kappa)$ isomorphic to $\mathrm{PSL}(2, q)$ (cf. Subsection 4.1 in [C-O]). In this section, we also compute the number of rational places of the function fields $F^{\langle\kappa\rangle}$, F^H and $F^{\langle\kappa\rangle\times H}$ for all elementary Abelian 3-groups $H \le L'$.

First we recall some group-theoretical notions that will be used throughout the paper ([Ro], [C-O]). Let B be a finite group. A *Hall subgroup* A of B is a subgroup with $\gcd(|A|, |B : A|) = 1$. If A is an Abelian Hall subgroup of B, then every subgroup of order dividing $|A|$ is contained in a conjugate of A. The Ree group G has cyclic Hall subgroups of orders $(q-1)/2$, $(q+1)/4$, $q+3q_0+1$ and $q-3q_0+1$. A finite group Γ is called a *Frobenius group* if it has a subgroup $W \le \Gamma$ with $\langle 1\rangle \ne W \ne \Gamma$ such that

$$W \cap W^\sigma = \langle 1\rangle \quad \text{for all } \sigma \in \Gamma \setminus W,$$

where $W^\sigma = \sigma W \sigma^{-1}$. Then

$$K = \Gamma \setminus \bigcup_{\sigma\in\Gamma} (W^\sigma \setminus \langle 1\rangle)$$

is a normal subgroup of Γ such that $\Gamma = KW$ and $W \cap K = \langle 1\rangle$. K is called the *Frobenius kernel* and W is called a *Frobenius complement*. The Frobenius kernel K is uniquely determined by the conditions above and W is uniquely determined up to K-conjugacy.

Now we fix some notation that will be used throughout the section. From [C-O, Theorem 3.5] we know that there is a one-to-one correspondence between the degree 6 places of F and the Hall subgroups of order $q-3q_0+1$.

Let K be a Hall subgroup of order $q-3q_0+1$ and $N(K)$ be its normalizer. From property (6) in [C-O, Proposition 2.3] (see also [L-N]) we know that $N(K)$ is a Frobenius group with kernel K and a cyclic Frobenius complement of order 6. The number of distinct Frobenius complements in $N(K)$ is $q-3q_0+1$. Let W be one of these Frobenius complements. Let θ be the unique involution of W and W_3 the subgroup of order 3 of W. We have

$$N(K) = KW \quad \text{and} \quad W \leq C(\theta),$$

where $C(\theta)$ is the centralizer of θ in G. Let V be the 3-Sylow subgroup of $C(\theta)$ containing W_3.

LEMMA 3.1. *We have*

$$N(W) = \langle\theta\rangle \times V$$

where $N(W)$ is the normalizer of W in G.

Proof. If $g = \theta v$ with $v \in V$, we have

$$\begin{aligned} gWg^{-1} &= \theta v W v^{-1}\theta \\ &= \theta W \theta \quad \text{as } V \text{ is Abelian and } V \leq C(\theta) \\ &= W. \end{aligned}$$

Next we will prove the other direction, i.e. that

$$N(W) \leq \langle\theta\rangle \times V.$$

Let $g \in G$ satisfy $gWg^{-1} = W$. Then $g\theta g^{-1} = \theta$ and $gW_3g^{-1} = W_3$. Let U be the 3-Sylow subgroup of G containing W_3 (or equivalently containing V). We have $g \in C(\theta)$ and from property (9) in [C-O, Proposition 2.3] we deduce that $g \in N(W_3) \leq N(U)$. We have (see [C-O, Theorem 4.9(i)])

$$C(\theta) \cap N(U) = VT,$$

where $T \leq G$ is a cyclic group of order $q-1$ containing θ. Therefore $g \in VT$. Let $\tau \in T$ be an element of order $(q-1)/2$. Then g can be written as

$$g = \tau^i \theta^j v$$

where $v \in V$, $0 \leq i < (q-1)/2$ and $j = 0, 1$. We want to show that $\tau^i = 1$. Since $\langle\theta\rangle \times V \leq N(W)$, we have

$$gWg^{-1} = \tau^i W \tau^{-i},$$

which implies $\tau^i W_3 \tau^{-i} = W_3$. Let $h_3 \in W_3 \setminus \{1\}$. Then

$$\tau^i h_3 \tau^{-i} = h_3 \quad \text{or} \quad \tau^i h_3 \tau^{-i} = h_3^2.$$

So either $h_3 \in C_U(\tau^i)$ or $h_3 \in C_U(\tau^{2i})$. But from property (8) in [C-O, Proposition 2.3] (see also [W]) and since $\gcd(|\tau^i|, 2) = 1$, we have $\tau^i = 1$. ∎

LEMMA 3.2. *Let K_1 be a Hall subgroup of G of order $q - 3q_0 + 1$ and W_1 be a Frobenius complement of the normalizer $N(K_1)$ of K_1. Then there exist $g \in G$ and $t \in K$ such that*

$$K_1 = gKg^{-1} \quad \text{and} \quad W_1 = gtW(gt)^{-1}.$$

Conversely, for each $g \in G$ and $t \in K$, $K_1 = gKg^{-1}$ is a Hall subgroup of order $q - 3q_0 + 1$ with $W_1 = gtWt^{-1}g^{-1}$ being a Frobenius complement of the normalizer $N(K_1)$ of K_1.

Proof. Since all Hall subgroups of G of order $q - 3q_0 + 1$ are conjugate in G, there exists $g \in G$ such that $K_1 = gKg^{-1}$. Let W_1 be a Frobenius complement of the normalizer $N(K_1)$ of K_1. Then $g^{-1}W_1g$ is a Frobenius complement of $N(K)$. Since all Frobenius complements of $N(K)$ are conjugate by means of a $t \in K$, we have

$$W = t^{-1}(g^{-1}W_1g)t$$

for some $t \in K$. This is equivalent to

$$W_1 = gtW(gt)^{-1}.$$

We prove the converse similarly. ∎

COROLLARY 3.3. *W is also a Frobenius complement of the normalizer of a conjugate K_1 of K with $K \neq K_1$ if and only if there exists $g \in N(W) \setminus N(K)$, in which case $K_1 = gKg^{-1}$.*

Proof. Assume that K_1 is a Hall subgroup of G of order $q - 3q_0 + 1$ and $K_1 \neq K$. We have $K_1 = gKg^{-1}$ for some $g \in G$ and $g \notin N(K)$. Assume also that W is a Frobenius complement of the normalizer of K_1 as well. By Lemma 3.2 there exists $t \in K$ such that $(gt) \in N(W)$. Let $g_1 = gt$. By Lemma 3.1, we have $g_1 \in \langle\theta\rangle \times V$ and obviously $g_1 \notin N(K)$.

Conversely assume that $g \in N(W)$ and $g \notin N(K)$. Let $K_1 = gKg^{-1}$. Then W is a Frobenius complement of the normalizer of K_1 as well and $K_1 \neq K$. ∎

LEMMA 3.4. *We have*

$$N(K) \cap N(W) = W.$$

Proof. We know that $W \leq N(K) = KW$ and $W \leq N(W)$. But $|N(K)| = 6(q - 3q_0 + 1)$ and $|N(W)| = 2q$ (by Lemma 3.1) so that $\gcd(|N(K)|, |N(W)|) = 6 = |W|$, which finishes the proof. ∎

PROPOSITION 3.5. *Let $\{a_1W, \ldots, a_kW\}$ be the set of all left cosets of W in $N(W)$ and hence $k = q/3$. Then $\{a_1Ka_1^{-1}, \ldots, a_kKa_k^{-1}\}$ is the set of all distinct Hall subgroups in G of order $q - 3q_0 + 1$ with W being a Frobenius complement of their normalizers.*

Proof. By Corollary 3.3 we need only consider the conjugates aKa^{-1} of K with elements $a \in N(W)$. For $a_1, a_2 \in N(W)$, we have

$$\begin{aligned} a_1 K a_1^{-1} = a_2 K a_2^{-1} &\Leftrightarrow a_1^{-1} a_2 K a_2^{-1} a_1 = K \\ &\Leftrightarrow a_1^{-1} a_2 \in N(K) \cap N(W) \\ &\Leftrightarrow a_1^{-1} a_2 \in W \quad \text{by Lemma 3.4.} \end{aligned}$$

This completes the proof. ∎

We recall that for a given Hall subgroup K_1 of G of order $q-3q_0+1$, there are $q - 3q_0 + 1$ distinct Frobenius complements in $N(K_1)$. Now we consider the union of all of these Frobenius complements over all Hall subgroups of G of order $q - 3q_0 + 1$.

COROLLARY 3.6. *The number of Frobenius complements corresponding to Hall subgroups of G of order $q - 3q_0 + 1$ is*

$$\frac{(q^3+1)q^2(q-1)}{2}.$$

Proof. The number of Hall subgroups of G of order $q - 3q_0 + 1$ is the number of degree 6 places of F, which is

$$\frac{q^3(q-1)(q+1)(q+3q_0+1)}{6}$$

(see [C-O]). The normalizer of each of these Hall subgroups has exactly

$$q - 3q_0 + 1$$

distinct Frobenius complements.

By Proposition 3.5, each Frobenius complement corresponding to some Hall subgroup of G is a Frobenius complement of exactly $q/3$ distinct Hall subgroups of G of order $q - 3q_0 + 1$. Therefore the number of Frobenius complements corresponding to Hall subgroups of G of order $q - 3q_0 + 1$ is

$$\frac{\frac{q^3(q-1)(q+3q_0+1)}{6}(q - 3q_0 + 1)}{q/3} = \frac{(q^3+1)q^2(q-1)}{2}. \ ∎$$

PROPOSITION 3.7. *Any cyclic subgroup of order 6 in G is a Frobenius complement of exactly $q/3$ distinct Hall subgroups of order $q - 3q_0 + 1$.*

Proof. Let S be the set of all subgroups of order 6 in G. Any $W_1 \in S$ can be written as $W_1 = \langle \theta_1 \rangle \times W_{3,1}$ where θ_1 is an involution of G, and $W_{3,1} \leq G$ is a subgroup of order 3 which is contained in a 3-Sylow subgroup V_1 of $C(\theta_1)$.

There exists a unique involution of G fixing any two distinct rational places of F (cf. [C-O, Proposition 2.5(i)]). Moreover each involution of G fixes exactly $q+1$ rational places of F (cf. [C-O, Proposition 2.5(iii)]). There-

fore the number of involutions in G is

$$\frac{\binom{q^3+1}{2}}{\binom{q+1}{2}} = \frac{(q^3+1)q^3}{(q+1)q}.$$

Let θ_1 be an involution of G. The number of 3-Sylow subgroups of $C(\theta_1)$ is $q+1$ and each of them has $(q-1)/2$ subgroups of order 3 (cf. [C-O, Proposition 4.8 and Theorem 4.11]). Hence

$$|S| \le \frac{(q^3+1)q^3}{(q+1)q}\,(q+1)\,\frac{q-1}{2} = \frac{(q^3+1)q^2(q-1)}{2}. \tag{3.1}$$

Using Corollary 3.6 we observe that the right hand side of (3.1) is equal to the number of Frobenius complements corresponding to Hall subgroups of G of order $q-3q_0+1$. Therefore we have equality in (3.1) and any element of S is a Frobenius complement for exactly $q/3$ distinct Hall subgroups of G of order $q-3q_0+1$ (see also Proposition 3.5). ∎

Proposition 3.7 implies that for any subgroup $W \le H$ of order 6 there are $q/3$ degree 6 places P such that $W \le H_{-1}(P)$. As the results of this section will be used in Section 5, we show in the following lemma that for H a subgroup of the normalizer of a 3-Sylow subgroup, two distinct cyclic subgroups of H of order 6 cannot be contained in the decomposition group of the same degree 6 place.

LEMMA 3.8. *Let W_1 and W_2 be two distinct cyclic subgroups of order 6 in the normalizer of a 3-Sylow subgroup of G. Then there is no Hall subgroup K_1 of G of order $q-3q_0+1$ such that*

$$W_1 \subseteq N(K_1) \quad \textit{and} \quad W_2 \subseteq N(K_1).$$

Proof. Assume the contrary. Then W_2 is the conjugate of W_1 by a nonidentity element of K_1. Since both W_1 and W_2 are contained in the normalizer of the same 3-Sylow subgroup of G, they both fix the same rational place of F and do not fix any other rational place. But no nonidentity element of K_1 fixes a rational place, hence a contradiction. ∎

Let H be a subgroup of the normalizer of a 3-Sylow subgroup of G, and let $n_6(H)$ be the number of distinct cyclic subgroups of order 6 of H. Then from Proposition 3.7 and Lemma 3.8, there are $n_6(H)q/3$ degree 6 places P such that $|H_{-1}(P)| = 6$ (note that the extension F/F^H is unramified at degree 6 places). So $N(F^H, 6)$ is calculated as

$$N(F^H, 6) = \frac{6}{|H|}\, n_6(H)\, \frac{q}{3}. \tag{3.2}$$

Let κ be an involution of G and L' be the subgroup of $C(\kappa)$ isomorphic to $\mathrm{PSL}(2,q)$. There exists an elementary Abelian subgroup $H \le L'$ with $|H| = 3^f$ if and only if $1 \le f \le 2s+1$.

THEOREM 3.9. *For $1 \le f \le 2s+1$, let H be an elementary Abelian subgroup $H \le L'$ with $|H| = 3^f$ and for $f = 0$ let $H = \langle 1 \rangle$. For the number of rational places of F^H and $F^{\langle \kappa \rangle \times H}$ we have*

$$N(F^H) = 1 + \frac{q^3}{3^f}, \tag{3.3}$$

$$N(F^{\langle \kappa \rangle \times H}) = 1 + \frac{q}{3^f} + \frac{q^3 - q}{2 \cdot 3^f} + \frac{q(3^f - 1)}{2 \cdot 3^f}. \tag{3.4}$$

Proof. From [C-O, Subsection 4.1.1] we know that all rational places of F split completely in F/F^H except a place P which is totally ramified. Then

$$N(F^H, 1) = 1 + \frac{q^3}{3^f}.$$

There is no cyclic subgroup in H of order distinct from 3. We recall that F has no degree 3 places, which follows from property (P5) in Section 1. Therefore

$$N(F^H) = N(F^H, 1).$$

Let $\{P_0, \dots, P_q\}$ be the rational places of F fixed by κ and assume that H fixes P_0, without loss of generality. From [C-O, Subsection 4.1.1] we know $e(P_i | P_i \cap F^{\langle \kappa \rangle \times H}) = 2$, $f(P_i | P_i \cap F^{\langle \kappa \rangle \times H}) = 1$ for $1 \le i \le q$. Moreover the rational places of F distinct from $P_0, \dots, P_q$ split in $F/F^{\langle \kappa \rangle \times H}$. Therefore

$$N(F^{\langle \kappa \rangle \times H}, 1) = 1 + \frac{q}{3^f} + \frac{q^3 - q}{2 \cdot 3^f}.$$

There are $(3^f - 1)/2$ distinct subgroups of degree 6 in $\langle \kappa \rangle \times H$. Therefore using (3.2) we get

$$N(F^{\langle \kappa \rangle \times H}, 6) = \frac{q(3^f - 1)}{2 \cdot 3^f}.$$

The result follows from the observation that $N(F^{\langle \kappa \rangle \times H}) = N(F^{\langle \kappa \rangle \times H}, 1) + N(F^{\langle \kappa \rangle \times H}, 6)$. ∎

Recall that the genera of F^H and $F^{\langle \kappa \rangle \times H}$ in (3.3) and (3.4) are (cf. [C-O])

$$g(F^H) = \frac{1}{2}\left[\frac{3q_0 q^2 + q^2 - q}{3^f} - 3q_0\right],$$

$$g(F^{\langle \kappa \rangle \times H}) = \frac{1}{4}\left[\frac{3q_0 q^2 + q^2 - 2q}{3^f} - 3q_0 + 1\right].$$

4. Rational places below unramified higher degree places. Let E be a function field over a finite field $\mathbb{F}_q$ and $H \le \mathrm{Aut}(E/\mathbb{F}_q)$ be a subgroup of the automorphism group of E over $\mathbb{F}_q$. In this section we develop a method to compute $N(E^H, m)$, the number of rational places of E^H below the degree m places of E. The problem here is that, even if the ramification structure of

the extension E/E^H is known, the computation of the decomposition group $H_{-1}(P)$ at an unramified place P of E is difficult. Our method uses the defining equations of the function field $E/\mathbb{F}_q$ and the explicit descriptions of the automorphisms in H.

Assume that the function field $E/\mathbb{F}_q$ (with $\mathbb{F}_q$ its full constant field) is defined as

$$E = \mathbb{F}_q(z_0, z_1, \ldots, z_n)$$

where $z_0, \ldots, z_n$ satisfy the equations

$$F_i(z_0, \ldots, z_n) = 0, \quad i = 1, \ldots, r, \tag{4.1}$$

where, for each $i = 1, \ldots, r$, $F_i(Z_0, \ldots, Z_n)$ is a polynomial over $\mathbb{F}_q$ in the variables $Z_0, \ldots, Z_n$. Let $m > 1$ be an integer. We want to compute $N(E^H, m)$, so we assume E contains places of degree m (otherwise $N(E^H, m) = 0$ trivially). We need the following definition.

Definition 4.1. For $r \geq 1$, $n \geq 0$, let $R_i(Z_0, \ldots, Z_n)$, $i = 1, \ldots, r$, be rational functions over $\mathbb{F}_q$ in the independent variables $Z_0, \ldots, Z_n$. Then, for $m \geq 1$, we call an $n+1$-tuple $(\zeta_0, \ldots, \zeta_n) \in \mathbb{F}_{q^m}^{n+1}$ a *purely* $\mathbb{F}_{q^m}$*-solution* of the set of equations $\{R_i(Z_0, \ldots, Z_n) = 0 \mid i = 1, \ldots, r\}$ if $R_i(\zeta_0, \ldots, \zeta_n) = 0$ for each $i = 1, \ldots, r$ and the set $\{\zeta_0, \ldots, \zeta_n\} \subseteq \mathbb{F}_{q^m}$ is not contained in a smaller subfield of $\mathbb{F}_{q^m}$. Note that if $(\zeta_0, \ldots, \zeta_n)$ is a purely $\mathbb{F}_{q^m}$-solution of a set of equations defined over $\mathbb{F}_q$ then the m distinct $\mathbb{F}_q$-conjugates

$$(\zeta_0, \ldots, \zeta_n), (\zeta_0^q, \ldots, \zeta_n^q), \ldots, (\zeta_0^{q^{m-1}}, \ldots, \zeta_n^{q^{m-1}})$$

are also purely $\mathbb{F}_{q^m}$-solutions.

We make the following assumptions on the degree m places of E:

A1 Any degree m place P of E is unramified in the extension E/E^H.

A2 For any degree m place P of E and for each $i = 0, \ldots, r$, we have $z_i \in \mathcal{O}_P$.

A3 For each purely $\mathbb{F}_{q^m}$-solution $(\zeta_0, \ldots, \zeta_n) \in \mathbb{F}_{q^m}^{n+1}$ of the defining equations of $E/\mathbb{F}_q$, $F_i(Z_0, \ldots, Z_n), i = 1, \ldots, r$, there is a unique degree 1 place P of the constant field extension $E.\mathbb{F}_{q^m}$ with $z_0 - \zeta_0, z_1 - \zeta_1, \ldots$ $\ldots, z_n - \zeta_n \in P$.

Let P be a degree m place of E. From assumption **A1**, the place P^H of E^H below P is a degree 1 place of E^H if and only if $H_{-1}(P)$ is cyclic of order m, in which case $H_{-1}(P)$ is generated by an element $\sigma \in H$ acting as the Frobenius morphism on the residue field $\mathcal{O}_P/P$:

$$\sigma(z) \equiv z^q \bmod P \quad \text{for all } z \in \mathcal{O}_P,$$

where σ is called the *Frobenius substitution* of P (see [Se]). So we assume that H contains elements of order m (otherwise $N(E^H, m) = 0$ again). Now, given an element $\tau \in H$ of order m, we want to find the number of degree m

places P such that $H_{-1}(P) = \langle\tau\rangle$. If $H_{-1}(P) = \langle\tau\rangle$, then some generator of the cyclic group $\langle\tau\rangle$ is the Frobenius substitution of P. So we first find a method to find the number of degree m places P such that $H_{-1}(P) = \langle\tau\rangle$ and τ is the Frobenius substitution of P. Repeating the procedure for each element in H of order m will determine the number $N(E^H, m)$.

LEMMA 4.2. *Let $E = \mathbb{F}_q(z_0, z_1, \ldots, z_n)$ be a function field over $\mathbb{F}_q$ defined by the equations* (4.1). *Let $\tau \in \mathrm{Aut}(E/\mathbb{F}_q)$ be an automorphism of order $m > 1$ and H be a subgroup of $\mathrm{Aut}(E/\mathbb{F}_q)$ containing τ. Assume that, for each $i = 0, \ldots, n$, we can write the element $\tau(z_i)$ explicitly as*

$$\tau(z_i) = T_i(z_0, \ldots, z_n)$$

where $T_i(Z_0, \ldots, Z_n)$ is a known rational function over $\mathbb{F}_q$ in $n+1$ variables. Assume moreover that the degree m places of E satisfy assumptions **A1**, **A2** *and* **A3**. *Then there is a one-to-one correspondence between the sets of $\mathbb{F}_q$-conjugate purely $\mathbb{F}_{q^m}$-solutions*

$$\{(\zeta_0, \ldots, \zeta_n), (\zeta_0^q, \ldots, \zeta_n^q), \ldots, (\zeta_0^{q^{m-1}}, \ldots, \zeta_n^{q^{m-1}})\}$$

of the set of equations

$$F_i(Z_0, \ldots, Z_n) = 0, \quad i = 1, \ldots, r, \tag{4.2}$$

$$T_i(Z_0, \ldots, Z_n) - Z_i^q = 0, \quad i = 0, \ldots, n, \tag{4.3}$$

and the degree m places P of E such that $H_{-1}(P) = \langle\tau\rangle$ and τ is the Frobenius substitution of P. In particular the number of such places is equal to the number of purely $\mathbb{F}_{q^m}$-solutions of the equations (4.2), (4.3) *divided by m.*

Proof. Let P be a degree m place of E. Observe that the statement

$$H_{-1}(P) = \langle\tau\rangle \text{ and } \tau \text{ is the Frobenius substitution of } P$$

is equivalent to

$$\tau(z)(P) = \tau(z) + P = z^q + P = z^q(P) \quad \text{for each } z \in \mathcal{O}_P. \tag{4.4}$$

From assumption **A2** and the fact that $z_0, \ldots, z_n$ generates E over $\mathbb{F}_q$, $\mathcal{O}_P/P$ is generated by $z_0(P), \ldots, z_n(P)$ as a field over $\mathbb{F}_q$. So (4.4) holds if and only if

$$\tau(z_i)(P) = z_i^q(P) \quad \text{for each } i = 0, \ldots, n. \tag{4.5}$$

Consider now the constant field extension $E_m = E.\mathbb{F}_{q^m}$ and let $P_1, \ldots, P_m$ be the degree 1 places of E_m extending P. Let z_i be any of $z_0, \ldots, z_n$. From assumption **A2**, z_i does not have a pole at a degree m place of E. As $\tau \in \mathrm{Aut}(E/\mathbb{F}_q)$ maps degree m places to degree m places, $\tau(z_i)$ is an element of $\mathcal{O}_P$ and also of $\mathcal{O}_{P_j}$ for each $j = 1, \ldots, m$. So we have

$$\tau(z_i)(P) = z_i^q(P) \quad \text{iff} \quad \tau(z_i)(P_j) = z_i^q(P_j) \text{ for some } j = 1, \ldots, m,$$

in which case $\tau(z_i)(P_j) = z_i^q(P_j)$ for each $j = 1, \ldots, m$.

For each $i = 0, \ldots, n$ and $j = 1, \ldots, m$ we can identify $z_i(P_j)$ with a unique value $\zeta_{i,j} \in \mathbb{F}_{q^m} \subset E_m$ such that $\zeta_{i,j} = \zeta_{i,j}(P_j) = z_i(P_j)$. So (4.5) holds if and only if

$$T_i(\zeta_{0,j}, \ldots, \zeta_{n,j}) = \zeta_{i,j}^q \quad \text{for each } i = 0, \ldots, n \text{ and } j = 1, \ldots, m, \tag{4.6}$$

equivalently if and only if the tuples $(\zeta_{0,j}, \ldots, \zeta_{n,j})$, $j = 1, \ldots, m$, are solutions of the equations (4.3). Observe that the tuples $(\zeta_{0,j}, \ldots, \zeta_{n,j})$, $j = 1, \ldots, m$, are $\mathbb{F}_q$-conjugate purely $\mathbb{F}_{q^m}$-solutions of the defining equations (4.2) of $E/\mathbb{F}_q$. Now assumption **A3** implies that there is a one-to-one correspondence between the sets of $\mathbb{F}_q$-conjugate purely $\mathbb{F}_{q^m}$-solutions

$$\{(\zeta_0, \ldots, \zeta_n), (\zeta_0^q, \ldots, \zeta_n^q), \ldots, (\zeta_0^{q^{m-1}}, \ldots, \zeta_n^{q^{m-1}})\}$$

of the equations (4.2) and the degree m places of E. Restricting this correspondence to the solutions of the equations (4.3) will settle the result. ∎

Given an element $\tau \in H$ of order m, let $M(\tau)$ denote the number of degree m places P of E such that $H_{-1}(P) = \langle \tau \rangle$ and τ is the Frobenius substitution of P. This number can be calculated using Lemma 4.2 provided the corresponding number of $\mathbb{F}_{q^m}$-solutions in Lemma 4.2 can be calculated. Now, for any degree m place P with $H_{-1}(P) = \langle \tau \rangle$ there is a unique integer l, $1 \le l < m$, with $\gcd(l, m) = 1$ such that τ^l is the Frobenius substitution of P. Therefore the number of degree m places P with $H_{-1}(P) = \langle \tau \rangle$ is

$$\sum_{\substack{1 \le l < m \\ \gcd(m,l)=1}} M(\tau^l)$$

and the number of degree m places P with $|H_{-1}(P)| = m$ can be written as:

$$\sum_{\substack{\tau \in H \\ |\tau| = m}} M(\tau).$$

Now, assume that P is a degree m place of E with $|H_{-1}(P)| = m$ (equivalently the place of E^H below P is rational). Then, since P is unramified in the extension E/E^H (by assumption **A1**), the orbit of H containing P has $|H|/m$ elements. Therefore the number $N(E^H, m)$ is calculated as

$$N(E^H, m) = \frac{m}{|H|} \sum_{\substack{\tau \in H \\ |\tau| = m}} M(\tau). \tag{4.7}$$

Unfortunately, this method may be difficult to apply in general. First, one needs to know explicitly the elements $\tau(z_0), \ldots, \tau(z_n)$ for every auto-

morphism $\tau \in H$ of order m. Even in that case, it may be hard to find the number of solutions of the equations (4.2), (4.3) in Lemma 4.2.

Now, we shall apply the method described above to the function field F. Let G_{P_∞} be the subgroup of G fixing the place P_∞, the pole of x. From [P], we know explicitly the automorphisms in G_{P_∞} (see (5.1) in Section 5). So in what follows, we will consider automorphisms of distinct orders in G_{P_∞}. In particular we will compute $M(\tau)$ for elements $\tau \in G_{P_\infty}$ of order $m \mid (q-1)$ with $m > 2$, $m = 9$ and $m = 6$.

Let $m \mid (q-1)$, $m > 2$, $\tau \in G_{P_\infty}$ be an element of order m and $H \leq G$ be a subgroup containing τ. From [C-O, Theorem 2.6], τ fixes one more place P_0 of F. As the value of $M(\tau)$ does not change by taking a conjugate of τ, we shall assume that P_0 is the common zero of x, y_1 and y_2. Then, from [P], τ is written as

$$\tau(x) = \alpha x, \quad \tau(y_1) = \alpha^{q_0+1} y_1, \quad \tau(y_2) = \alpha^{2q_0+1} y_2, \tag{4.8}$$

where $\alpha \in \mathbb{F}_q^\times$ and $|\alpha| = m$. Let us check that the degree m places of F satisfy assumptions **A1**–**A3**. Since $m \notin \{1, 6\}$, any degree m place is unramified in the extension F/F^H, so **A1** is satisfied. Now, each of x, y_1 and y_2 has a unique pole, P_∞, which is rational. So **A2** is also satisfied. To check **A3**, it is enough to check whether the affine curve defined by equations (1.1) is nonsingular. Therefore **A3** also holds. Now by Lemma 4.2, $M(\tau)$ is equal to the number of purely $\mathbb{F}_{q^m}$-solutions of the equations

$$\begin{aligned} Y_1^q - Y_1 - X^{q_0}(X^q - X) &= 0, \\ Y_2^q - Y_2 - X^{2q_0}(X^q - X) &= 0, \\ \alpha X - X^q &= 0, \\ \alpha^{(q_0+1)} Y_1 - Y_1^q &= 0, \\ \alpha^{(2q_0+1)} Y_2 - Y_2^q &= 0, \end{aligned} \tag{4.9}$$

divided by m. We have:

Proposition 4.3. *The set of nonzero solutions (in $\overline{\mathbb{F}}_q^3$) of the system (4.9) is given by*

$$\mathcal{S} = \left\{ (X, Y_1, Y_2) \in \overline{\mathbb{F}}_q^3 \;\middle|\; X^{q-1} = \alpha,\ Y_1 = \frac{\alpha - 1}{\alpha^{q_0+1} - 1} X,\ Y_2 = \frac{\alpha - 1}{\alpha^{2q_0+1} - 1} X \right\}.$$

The set $\mathcal{S}$ has $q-1$ elements and each solution in $\mathcal{S}$ is purely $\mathbb{F}_{q^m}$. Therefore, for any $\tau \in G$ of order $|\tau| = m$, with $m \mid (q-1)$, $m > 2$, we have

$$M(\tau) = \frac{q-1}{m}.$$

Proof. It is easy to see that $\mathcal{S}$ is indeed the set of nonzero solutions of the system (4.9) and that $\mathcal{S}$ has $q-1$ elements. For each $X \in \overline{\mathbb{F}}_q$ with

$X^{q-1} = \alpha$, the smallest i with $X^{q^i} = X$ is m. So each solution in $\mathcal{S}$ is purely $\mathbb{F}_{q^m}$. The last assertion follows from Lemma 4.2. ∎

Let us now consider the case $m = 9$. So let $\tau \in G_{P_\infty}$ be an element of order 9 and $H \leq G$ be a subgroup containing τ. So the automorphism τ can be explicitly written as

$$\begin{aligned} \tau(x) &= x + \beta, \\ \tau(y_1) &= y_1 + \beta^{q_0} x + \gamma, \\ \tau(y_2) &= y_2 - \beta^{q_0} y_1 + \beta^{2q_0} x + \delta, \end{aligned} \tag{4.10}$$

where $\beta, \gamma, \delta \in \mathbb{F}_q$ and $\beta \neq 0$. It is easy to check that the degree 9 places of F satisfy assumptions **A1**–**A3**. By Lemma 4.2, $M(\tau)$ is equal to the number of purely $\mathbb{F}_{q^9}$-solutions of the equations

$$Y_1^q - Y_1 - X^{q_0}(X^q - X) = 0, \tag{4.11}$$

$$Y_2^q - Y_2 - X^{2q_0}(X^q - X) = 0, \tag{4.12}$$

$$X + \beta - X^q = 0, \tag{4.13}$$

$$Y_1 + \beta^{q_0} X + \gamma - Y_1^q = 0, \tag{4.14}$$

$$Y_2 - \beta^{q_0} Y_1 + \beta^{2q_0} X + \delta - Y_2^q = 0, \tag{4.15}$$

divided by 9. Let $\mathrm{Tr}(\cdot)$ denote the absolute trace of an element of $\mathbb{F}_q$. We have:

Proposition 4.4. *The system of equations* (4.11), ..., (4.15) *has solutions over* $\overline{\mathbb{F}}_q$ *if and only if*

$$\mathrm{Tr}(\beta^{-(q_0+1)}\gamma) = s \bmod 3, \quad \text{where } q_0 = 3^s, \tag{4.16}$$

and in that case the solution set of the system is given by

$$\begin{aligned} \mathcal{S} = \{(X, Y_1, Y_2) \in \overline{\mathbb{F}}_q^3 \mid \\ \beta^{-3}X^3 - (\beta^{-1}X + 1 - (\beta^{-(q_0+1)}\gamma)^3 - (\beta^{-(q_0+1)}\gamma)^{3q_0}) = 0, \\ Y_1 - \beta^{-q_0}(\beta^{2q_0}X - X^{2q_0}\beta + \delta) = 0,\ Y_2^q - (Y_2 + X^{2q_0}\beta) = 0\}. \end{aligned}$$

The set $\mathcal{S}$ *has* $3q$ *elements and each solution in* $\mathcal{S}$ *is purely* $\mathbb{F}_{q^9}$. *Therefore, for* $\tau \in G_{P_\infty}$ *defined by* (4.10), $\beta \neq 0$, *we have*

$$M(\tau) = \begin{cases} q/3 & \text{if } \mathrm{Tr}(\beta^{-(q_0+1)}\gamma) = s, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. From (4.11), (4.13) and (4.14) we get

$$\beta^{-q_0} X^{q_0} = \beta^{-1} X + \beta^{-(q_0+1)}\gamma. \tag{4.17}$$

Equation (4.17) together with (4.13) gives

$$\beta^{-3}X^3 = \beta^{-1}X + 1 - (\beta^{-(q_0+1)}\gamma)^3 - (\beta^{-(q_0+1)}\gamma)^{3q_0}, \tag{4.18}$$

and calculating $\beta^{-q_0}X^{q_0}$ using (4.18), we get

$$\beta^{-q_0}X^{q_0} = \beta^{-1}X + \beta^{-(q_0+1)}\gamma + s - \mathrm{Tr}(\beta^{-(q_0+1)}\gamma). \tag{4.19}$$

Now equating the right hand sides of (4.17) and (4.19), we conclude

$$\mathrm{Tr}(\beta^{-(q_0+1)}\gamma) = s. \tag{4.20}$$

So if $\mathrm{Tr}(\beta^{-(q_0+1)}\gamma) \neq s$ then the system (4.11), ..., (4.15) has no solution. Let us assume that (4.20) holds. Let $X = \chi$ be a solution of (4.18). Then the other two solutions are $\chi + \beta$ and $\chi + 2\beta$. Any of the three solutions of (4.18) also satisfies (4.13), and the smallest extension of $\mathbb{F}_q$ containing solutions of (4.13) is $\mathbb{F}_{q^3}$. From (4.12), (4.13), (4.15) and (4.17), we get

$$Y_1 = \beta^{-q_0}(\beta^{2q_0}X - X^{2q_0}\beta + \delta). \tag{4.21}$$

Using equations (4.12) and (4.13) we get

$$Y_2^q = Y_2 + X^{2q_0}\beta. \tag{4.22}$$

So any solution of the system of equations (4.11), ..., (4.15) is an element of $\mathcal{S}$. We leave it to the reader to check that any element of $\mathcal{S}$ satisfies equations (4.11), ..., (4.15).

For each solution $X = \chi$, $\chi + \beta$ or $\chi + 2\beta$ of (4.18), the solution for Y_1 is uniquely determined from (4.21) and is also an element of $\mathbb{F}_{q^3}$. The equation (4.22) has q distinct solutions for Y_2. So $\mathcal{S}$ has $3q$ distinct elements.

Using (4.17), we get

$$X^{2q_0} + (X^{2q_0})^q + (X^{2q_0})^{q^2} = 2\beta^{2q_0},$$

and combining with (4.22) we get $Y_2^{q^3} = Y_2 + 2\beta^{2q_0}$ and $Y_2^{q^9} = Y_2$. Therefore if X is replaced by χ, $\chi + \beta$ or $\chi + 2\beta$ in (4.22) then any of the q solutions for Y_2 is in $\mathbb{F}_{q^9}$, and $\mathbb{F}_{q^9}$ is the smallest extension of $\mathbb{F}_q$ containing them. So any solution in $\mathcal{S}$ is purely $\mathbb{F}_{q^9}$. The last assertion follows from Lemma 4.2. ∎

Now we shall show how to compute $N(F^H, m)$ when $m = 6$ by using the method described in this section. Observe that any two cyclic subgroups of order 6 in G are conjugate. Indeed any cyclic subgroup of order 6 is a Frobenius complement of a Hall subgroup of order $q - 3q_0 + 1$ (cf. Proposition 3.7). Since Frobenius complements of the same Hall subgroup of order $q - 3q_0 + 1$ are conjugate and the Hall subgroups of order $q - 3q_0 + 1$ are conjugate, we see that any two cyclic subgroups of order 6 are also conjugate (cf. Lemma 3.2). So we will consider the cyclic subgroup $\langle\tau\rangle$ generated by the following element:

$$\tau(x) = -x, \quad \tau(y_1) = y_1 + 1, \quad \tau(y_2) = -y_2, \tag{4.23}$$

and then compute $M(\tau)$ and $M(\tau^5)$. Note that the definition of τ^5 differs only at y_1, namely $\tau^5(x) = -x$, $\tau^5(y_2) = -y_2$ and $\tau^5(y_1) = y_1 - 1$. We

assume that the extension F/F^H is unramified at degree 6 places, so that the degree 6 places of F satisfy assumptions **A1**–**A3**. Consider the equations

$$Y_1^q - Y_1 - X^{q_0}(X^q - X) = 0, \tag{4.24}$$

$$Y_2^q - Y_2 - X^{2q_0}(X^q - X) = 0, \tag{4.25}$$

$$-X - X^q = 0, \tag{4.26}$$

$$Y_1 + \gamma - Y_1^q = 0, \tag{4.27}$$

$$-Y_2 - Y_2^q = 0, \tag{4.28}$$

where $\gamma = 1$ or -1. Then by Lemma 4.2, $M(\tau)$ (resp. $M(\tau^5)$) is equal to the number of purely $\mathbb{F}_{q^6}$-solutions of the equations (4.24), ..., (4.28) with $\gamma = 1$ (resp. $\gamma = -1$) divided by 6. We have:

PROPOSITION 4.5. *The system of equations* (4.24), ..., (4.28) *with* $\gamma = 1$ (*resp.* $\gamma = -1$) *has solutions over* $\overline{\mathbb{F}}_q$ *if and only if* s *is odd* (*resp.* s *is even*) *and in that case the solution set of the system is given by*

$$\mathcal{S} = \{(X, Y_1, Y_2) \in \overline{\mathbb{F}}_q^3 \mid X^2 = -1,\ Y_1^q - Y_1 = \gamma,\ Y_2 = -X\}.$$

The set $\mathcal{S}$ *has* $2q$ *elements and each solution in* $\mathcal{S}$ *is purely* $\mathbb{F}_{q^6}$. *Therefore, for* τ *defined by* (4.23), *we have*

$$M(\tau) = \begin{cases} q/3 & \text{if } s \text{ is odd,} \\ 0 & \text{if } s \text{ is even,} \end{cases}$$

$$M(\tau^5) = \begin{cases} q/3 & \text{if } s \text{ is even,} \\ 0 & \text{if } s \text{ is odd.} \end{cases}$$

In particular, for any cyclic subgroup of H *of order* 6, *the number of degree* 6 *places* P *of* F *such that* $H_{-1}(P) = \langle \tau \rangle$ *is* $q/3$.

Proof. From (4.24), (4.26) and (4.27) we get

$$X^{q_0+1} = \gamma. \tag{4.29}$$

Raising (4.29) to the power $q_0 - 1$, we get

$$X^{q_0^2} = X,$$

which implies

$$X^q = X^3. \tag{4.30}$$

The equations (4.26) and (4.30) give

$$X^3 = -X. \tag{4.31}$$

The nonzero solutions of (4.31) are ω and $-\omega \in \mathbb{F}_{q^2}$ where $\omega^2 = -1$. It is easy to check that ω and $-\omega$ satisfy (4.26). Replacing X with ω or $-\omega$ in (4.24) we get

$$Y_1^q - Y_1 = (-1)^{s+1}, \tag{4.32}$$

which together with (4.27) implies $\gamma = (-1)^{s+1}$. Hence, for $\gamma = 1$ (resp.

$\gamma = -1$) the system has solutions iff s is odd (resp. s is even). Assume $\gamma = (-1)^{s+1}$. Replacing X with ω or $-\omega$ in (4.25) and combining with (4.28), we get $Y_2 = -X$. So the solutions of the system (4.24), ..., (4.28) satisfy

$$X^2 = -1, \tag{4.33}$$

$$Y_1^q - Y_1 = \gamma, \tag{4.34}$$

$$Y_2 = -X. \tag{4.35}$$

Now the system (4.33)–(4.35) has $2q$ solutions over $\overline{\mathbb{F}}_q$. Moreover any solution of (4.33) is purely $\mathbb{F}_{q^2}$ and any solution of (4.34) is purely $\mathbb{F}_{q^3}$, so that any solution of (4.33)–(4.35) is purely $\mathbb{F}_{q^6}$. ∎

REMARK 4.6. Using Proposition 3.7 and Lemma 3.8, we already know how to compute $N(F^H, 6)$. Nevertheless we prefer to keep Proposition 4.5, which uses a different method and gives an application of Lemma 4.2.

5. Normalizer of a 3-Sylow subgroup. In this section we compute the number of rational places of subfields of F fixed by subgroups of the normalizer of a 3-Sylow subgroup of G. Let U be a 3-Sylow subgroup of $G = \mathrm{Aut}(F/\mathbb{F}_q)$ and $N(U)$ be its normalizer. We assume U fixes the place P_∞, the pole of x. Then the automorphisms in $N(U) = \{\psi_{\alpha,\beta,\gamma,\delta} \mid \alpha \in \mathbb{F}_q^*,\ \beta,\gamma,\delta \in \mathbb{F}_q\}$ are explicitly written as (see [P])

$$\psi_{\alpha,\beta,\gamma,\delta} = \begin{cases} x \mapsto \alpha x + \beta, \\ y_1 \mapsto \alpha^{q_0+1} y_1 + \alpha\beta^{q_0} x + \gamma, \\ y_2 \mapsto \alpha^{2q_0+1} y_2 - \alpha^{q_0+1}\beta^{q_0} y_1 + \alpha\beta^{2q_0} x + \delta. \end{cases} \tag{5.1}$$

The group $N(U)$ is of order $q^3(q-1)$ and is written as $N(U) = UT$ where T is cyclic of order $q-1$. It follows from property (7) in [C-O, Proposition 2.3] that U has order q^3 and U has trivial intersection with its conjugates. Its center $Z(U)$ is elementary Abelian of order q, U is of class 3, and U contains a normal elementary Abelian subgroup U_1 of order q^2 containing $Z(U)$ which is both the derived group and the Frattini subgroup of U. The members of $U - U_1$ have order 9, their cubes forming $Z(U) - \langle 1\rangle$ (see [C-O]). Let us assume that T fixes the place P_0, the common zero of x, y_1 and y_2. Then we have

$$\begin{aligned} T &= \{\psi_{\alpha,0,0,0} \mid \alpha \in \mathbb{F}_q^*\}, & U_1 &= \{\psi_{1,0,\gamma,\delta} \mid \gamma,\delta \in \mathbb{F}_q\}, \\ U &= \{\psi_{1,\beta,\gamma,\delta} \mid \beta,\gamma,\delta \in \mathbb{F}_q\}, & Z(U) &= \{\psi_{1,0,0,\delta} \mid \delta \in \mathbb{F}_q\}. \end{aligned} \tag{5.2}$$

Let H be a subgroup of $N(U)$ of order $|H| = n3^{b+c+d}$ where $n \mid (q-1)$ and $0 \le b,c,d \le 2s+1$. Let $|H \cap U_1| = 3^{c+d}$ and $|H \cap Z(U)| = 3^d$. Unfortunately, the possible values of n, b, c, d are not all known. Recall that $N(F^H, m)$ is the number of rational places of F^H under the degree m places

of F. Let us now find for which values of $m > 1$, $N(F^H, m)$ can be nonzero. Since any place P of degree $m > 1$ is unramified in the extension F/F^H, $H_{-1}(P)$ is a cyclic group. So let us find the order of elements in $N(U)$. Let $\kappa = \psi_{-1,0,0,0}$ be the involution of T. Let us first consider the elements in the subset $S_1 = U.(T \setminus \{\kappa\}) = \{\psi_{\alpha,\beta,\gamma,\delta} \mid \alpha \neq -1\}$. Observe that any element in $S_1 \setminus U$ is contained in some conjugate of T. So, for any $\psi \in S_1$, we have $|\psi| = 3$, 9 or m where $m \mid (q-1)$, $m \neq 2$. Let us now consider the subset $S_2 = U.\{\kappa\} = \{\psi_{-1,\beta,\gamma,\delta}\}$. By (5.1), the orders of elements in S_2 are

$$|\psi_{-1,\beta,-\beta^{q_0+1},\delta}| = 2 \quad \text{for } \beta, \delta \in \mathbb{F}_q,$$
$$|\psi_{-1,\beta,\gamma,\delta}| = 6 \quad \text{for } \beta, \gamma, \delta \in \mathbb{F}_q \text{ and } \gamma \neq -\beta^{q_0+1}.$$

In particular we have:

LEMMA 5.1. *Let $H = S_1 \sqcup S_2$ be the disjoint decomposition of H as defined above. The set of orders of the elements in S_1 is $\{3, 9\} \cup \{m : m \neq 2$ and m divides $q-1\}$ and the set of orders of the elements in S_2 is $\{2, 6\}$.*

Now, F does not have any degree 2 or degree 3 place. Therefore we need only compute $N(F^H, m)$ for $m = 6$ or 9 or $m \mid (q-1)$, $m > 2$. For the case $m = 6$ we will use the results of Section 3, and for the cases $m = 9$ and $m \mid (q-1)$, $m > 2$ we shall use the results of Section 4. Let us first prove a result on the number of elements of distinct orders in H.

PROPOSITION 5.2. *Assume that $n > 1$. Then H has a cyclic subgroup T_H of order n, which is contained in a conjugate of T such that $H = T_H U_H$ where $U_H = U \cap H$. Moreover, T_H normalizes U_H and $n \mid \gcd(3^b - 1, 3^c - 1, 3^d - 1, q-1)$. If $n \neq 2$, then T_H has 3^{b+c+d} distinct conjugates in H and for any $m \mid n$, $m > 2$, H has $3^{b+c+d}\phi(m)$ distinct elements of order m, $\phi(\cdot)$ being Euler's Phi function. In the case $2 \mid n$, let κ be the involution of T_H. The order of the centralizer $C_{U_H}(\kappa)$ of κ in U_H is 3^c, and H has 3^{b+d} distinct involutions and $3^{b+d}(3^c - 1)$ distinct elements of order 6.*

Proof. We first prove that H has an element of order n. As U_H is the only 3-Sylow subgroup of H, U_H is normal in H. Therefore H/U_H is a subgroup of $N(U)/U$ which is isomorphic to the cyclic group T. Then H/U_H is a cyclic group of order n and there exists $\sigma \in H$ such that $\sigma^n \in U_H$ and $\sigma^i \notin U_H$ for $1 \leq i < n$. Since $U_H \leq U$, the order of σ is either n, $3n$ or $9n$. Using Lemma 5.1 and the equality $\gcd(q-1, 3) = 1$, we deduce that the order of σ is n if $n \neq 2$ and is either 2 or 6 if $n = 2$. Taking σ^3 if necessary, we choose and fix $\sigma \in H$ such that $|\sigma| = n$.

Let $T_H = \langle \sigma \rangle$ be the cyclic group generated by σ. Since T is an Abelian Hall subgroup of $N(U)$, T_H is contained in a conjugate of T (cf. [C-O, Theorem 2.1]). Note that T_H normalizes U_H and $T_H \cap U_H = \langle 1 \rangle$. Then we have $H = T_H U_H$.

Recall that a *characteristic subgroup* of a group is invariant under the group automorphisms. Note that the derived group U_1 and the center $Z(U)$ are characteristic subgroups of U. Moreover T and hence T_H normalizes U. Therefore T_H also normalizes U_1 and $Z(U)$.

If $2 \nmid n$, then σ (respectively σ^2 if $2 \mid n$) acts without a fixed point on the nonidentity elements of U by conjugation (cf. [C-O, Proposition 2.3(8)]). Let $k = n$ if $2 \nmid n$ and $k = n/2$ if $2 \mid n$. Therefore $k \mid (|U_H| - 1) = 3^{b+c+d} - 1$, $k \mid (|U_1 \cap H| - 1) = 3^{c+d} - 1$ and $k \mid (|Z(U) \cap H| - 1) = 3^d - 1$, or equivalently $k \mid \gcd(3^b - 1, 3^c - 1, 3^d - 1)$. As $\gcd(2, (q-1)/2) = 1$, $4 \nmid n$ and hence $n \mid \gcd(3^b - 1, 3^c - 1, 3^d - 1)$.

For the case $n \neq 2$ and $m \mid n$ with $m > 2$, we now determine the number of distinct elements in H of order m. It follows from [C-O, Proposition 2.3(8)], that σ does not commute with a nonidentity element of U_H. So T_H has $|U_H| = 3^{b+c+d}$ distinct conjugates in H. Therefore in this case H has $3^{b+c+d}\phi(m)$ distinct elements of order m.

Finally, we consider the case $2 \mid n$. It follows from properties (7) and (8) of [C-O, Proposition 2.3] that for any $u_1 \in U_1$ there exist $v \in C_U(\kappa)$ and $z \in Z(U)$ such that $u_1 = vz$. For $u_1 \in H \cap U_1$, let $v \in C_U(\kappa)$ and $z \in Z(U)$ be such that $u_1 = vz$. As $\kappa z \kappa \in Z(U)$ and $\kappa(\kappa z \kappa z)\kappa = \kappa z \kappa z$, using property (8) of [C-O, Proposition 2.3] we obtain $\kappa z \kappa = z^{-1}$. Since U_1 is an elementary Abelian 3-group, this implies that $\kappa u_1 \kappa = vz^{-1} \in H \cap U_1$, $v \in C_{U_H}(\kappa)$ and $z \in H \cap Z(U)$. Therefore $H \cap U_1 = C_{U_H}(\kappa) \times (H \cap Z(U))$ and $|C_{U_H}(\kappa)| = 3^c$.

Any involution θ of H is a conjugate of κ by an element of U_H. Therefore $|C_{U_H}(\theta)| = 3^c$ for any involution of H and the number of distinct involutions in H is $3^{b+c+d}/3^c$. Each involution θ of H commutes with exactly $3^c - 1$ elements of order 3 in H, namely the nonidentity elements of $C_{U_H}(\theta)$. Therefore there are $3^{b+d}(3^c - 1)$ elements of order 6 in this case. ∎

First we compute $N(F^H, 6)$ and we assume that $2 \mid |H|$. As $\phi(6) = 2$, by Proposition 5.2, H has $3^{b+d}(3^c - 1)/2$ distinct cyclic subgroups of order 6. So from (3.2), we have

$$N(F^H, 6) = \frac{6}{|H|} \cdot \frac{3^{b+d}(3^c - 1)}{2} \cdot \frac{q}{3} = \frac{q(3^c - 1)}{3^c n}. \tag{5.3}$$

Let us now calculate the number $N(F^H, m)$ where $m \mid n$, $m > 2$. So assume $n > 2$ and let $m \mid n$, $m > 2$. From Proposition 4.3, for each element $\tau \in H$ of order m, $M(\tau) = (q-1)/m$. So we need only find the number of elements of order m in H. Using Proposition 5.2 and (4.7) we get

$$N(F^H, m) = \frac{m}{|H|} \cdot 3^{b+c+d}\phi(m) \cdot \frac{q-1}{m} = \frac{q-1}{n}\,\phi(m). \tag{5.4}$$

Consider now the case $m = 9$. Unfortunately, we cannot give a formula for $N(F^H, 9)$ in terms of n, b, c, d. Note that the number of elements of

order 9 in H is $3^{b+c+d}-3^{c+d}$. Let $\widetilde{n}_9(H)$ be the number of order 9 elements in H which satisfy the condition (4.16) in Proposition 4.4, i.e.

$$\widetilde{n}_9(H) = |\{\psi_{1,\beta,\gamma,\delta} \in H \mid \beta \neq 0,\ \mathrm{Tr}(\beta^{-(q_0+1)}\gamma) = s\}|. \tag{5.5}$$

Then, by Proposition 4.4, $M(\tau) = q/3$ for $\widetilde{n}_9(H)$ elements of order 9 in H and $M(\tau) = 0$ for the remaining elements of order 9. So from (4.7) the number $N(F^H, 9)$ is calculated as

$$N(F^H, 9) = \frac{9}{|H|}\,\widetilde{n}_9(H)\,\frac{q}{3}. \tag{5.6}$$

Now, we are ready to calculate the number of rational places of F^H:

THEOREM 5.3. *Let U be the 3-Sylow subgroup of G fixing the place P_∞, the pole of x, U_1 the derived subgroup of U, $Z(U)$ the center of U and $N(U)$ the normalizer of U in G. Let H be a subgroup of $N(U)$. Assume the order of H is $|H| = n3^{b+c+d}$ where $n \mid \gcd(q-1, 3^b-1, 3^c-1, 3^d-1)$, $0 \le b, c, d \le 2s+1$, $|H \cap U_1| = 3^{c+d}$ and $|H \cap Z(U)| = 3^d$. Let $N(F^H)$ and $g(F^H)$ denote the number of rational places and the genus of F^H respectively. Let $\widetilde{n}_9(H)$ be defined by* (5.5). *We have*:

(i) *if $n = 1$ then*

$$N(F^H) = 1 + \frac{q^3}{3^{b+c+d}} + \frac{3}{3^{b+c+d}}\,\widetilde{n}_9(H)q,$$
$$g(F^H) = \frac{1}{2\cdot 3^{b+c+d}} \cdot 3q_0(q^2 + qq_0 - 3^{c+d} - q_0 3^d);$$

(ii) *if $n > 1$ and $2 \nmid n$ then*

$$N(F^H) = 2 + \frac{q^3 - 3^{b+c+d}}{n3^{b+c+d}} + \frac{3}{n3^{b+c+d}}\,\widetilde{n}_9(H)q + \frac{q-1}{n}\,(n-1),$$
$$g(F^H) = \frac{1}{2n3^{b+c+d}} \cdot 3q_0(q^2 + qq_0 - 3^{c+d} - q_0 3^d);$$

(iii) *if $n > 1$ and $2 \mid n$ then*

$$N(F^H) = 2 + \frac{2(q/3^c - 1)}{n} + \frac{q^3 - q3^{b+d}}{n3^{b+c+d}} + \frac{3}{n3^{b+c+d}}\,\widetilde{n}_9(H)q + \frac{q(3^c-1)}{3^c n} + \frac{q-1}{n}\,(n-2),$$
$$g(F^H) = \frac{1}{2n3^{b+c+d}}\,[3q_0(q^2 + qq_0 - 3^{c+d} - q_0 3^d) - 3^{b+c+d}(q/3^c - 1)].$$

Proof. Recall that for a subgroup $H \le N(U)$, F^H may have rational places below places of F of degree 1, 9, 6 or m where $m \mid n$, $m > 2$. So the number of rational places of F^H is computed from

$$N(F^H) = N(F^H, 1) + N(F^H, 9) + N(F^H, 6) + \sum_{\substack{m \mid n \\ m > 2}} N(F^H, m). \tag{5.7}$$

If $n = 1$ or 2, the last sum in (5.7) is equal to 0. Otherwise, from (5.4), we have

$$\sum_{\substack{m|n\\ m>2}} N(F^H, m) = \frac{q-1}{n} \sum_{\substack{m|n\\ m>2}} \phi(m)$$

where

$$\sum_{\substack{m|n\\ m>2}} \phi(m) = \begin{cases} n-1 & \text{if } 2 \nmid n, \\ n-2 & \text{if } 2 \mid n. \end{cases} \tag{5.8}$$

Observe also that $N(F^H, 6) = 0$ if $2 \nmid n$. As $N(F^H, 6)$ and $N(F^H, 9)$ are computed in (5.3) and (5.6) respectively, we need to calculate $N(F^H, 1)$ and $g(F^H)$ in each case. So we need to find the ramifications at rational places. The place P_∞ is fully ramified in the extension F/F^H and the different exponent at P_∞ is

$$d_{P_\infty} = (n3^{b+c+d} - 1) + (3^{b+c+d} - 1) + 3q_0(3^{c+d} - 1) + q(3^d - 1).$$

If $n > 2$, each cyclic group of order n in H fixes P_∞ and one more rational place of F. In the case $2 \mid n$, each involution in H fixes P_∞ and q more places. Moreover, two distinct involutions in H do not fix the same place except P_∞ (cf. [C-O, Proposition 2.5(i)]). Let $g = \frac{3}{2}q_0(q-1)(q+q_0+1)$ be the genus of F and g_H be the genus of F^H.

In the following, in each case, we list the ramified places of F, write $N(F^H, 1)$ and state the Riemann–Hurwitz formula from which $g(F^H)$ is calculated:

(i) If $n = 1$ then only P_∞ is ramified and we have

$$N(F^H, 1) = 1 + \frac{q^3}{3^{b+c+d}},$$
$$2g - 2 = |H|(2g_H - 2) + d_{P_\infty}.$$

(ii) If $n > 1$ and $2 \nmid n$ then

- P_∞ is fully ramified,
- 3^{b+c+d} places are ramified with ramification index n,
- $q^3 - 3^{b+c+d}$ places are unramified.

We have

$$N(F^H, 1) = 1 + 1 + \frac{q^3 - 3^{b+c+d}}{n3^{b+c+d}},$$
$$2g - 2 = |H|(2g_H - 2) + d_{P_\infty} + 3^{b+c+d}(n-1).$$

(iii) If $n > 1$ and $2 \mid n$ then

- P_∞ is fully ramified,

- 3^{b+c+d} places are ramified with ramification index n,
- $q3^{b+d} - 3^{b+c+d} = 3^{b+d}(q - 3^c)$ more places are ramified with ramification index 2,
- $q^3 - q3^{b+d}$ places are unramified.

We have

$$N(F^H, 1) = 1 + 1 + \frac{2(q/3^c - 1)}{n} + \frac{q^3 - q3^{b+d}}{n3^{b+c+d}},$$
$$2g - 2 = |H|(2g_H - 2) + d_{P_\infty} + 3^{b+c+d}(n-1) + 3^{b+d}(q - 3^c). \blacksquare$$

Unfortunately, we do not know all the possible values of n, b, c, d in Theorem 5.3. Now we construct some subgroups of $N(U)$ with all possible values of n, c and d for the case $b = 0$. First we give some properties for some elements of $N(U)$. Let $\alpha_1, \alpha_2, \alpha \in \mathbb{F}_q \setminus \{0\}$ and $\gamma_1, \gamma_2, \gamma, \delta_1, \delta_2, \delta \in \mathbb{F}_q$. The following properties are easy consequences of (5.1):

$$\begin{aligned} \psi_{\alpha_1,0,0,0} \circ \psi_{\alpha_2,0,0,0} &= \psi_{\alpha_1\alpha_2,0,0,0}, \\ \psi_{1,0,\gamma_1,\delta_1} \circ \psi_{1,0,\gamma_2,\delta_2} &= \psi_{1,0,(\gamma_1+\gamma_2),(\delta_1+\delta_2)}, \\ \psi_{\alpha^{-1},0,0,0} \circ \psi_{1,0,\gamma,\delta} &= \psi_{1,0,\gamma\alpha^{q_0+1},\delta\alpha^{2q_0+1}} \circ \psi_{\alpha^{-1},0,0,0}. \end{aligned} \tag{5.9}$$

For integers $c, d \le 2s+1$, let $e = \gcd(c, d, 2s+1)$. Note that

$$\gcd(3^c - 1, 3^d - 1, q - 1) = 3^e - 1.$$

Let $\{\gamma_1, \dots, \gamma_{c/e}\}$ and $\{\delta_1, \dots, \delta_{d/e}\}$ be $\mathbb{F}_{3^e}$-linearly independent subsets of $\mathbb{F}_q$. The set

$$S = \{\psi_{1,0,(\gamma_1\alpha_{1,1}+\gamma_2\alpha_{1,2}+\cdots+\gamma_{c/e}\alpha_{1,c/e}),(\delta_1\alpha_{2,1}+\delta_2\alpha_{2,2}+\cdots+\delta_{d/e}\alpha_{2,d/e})} \mid \alpha_{1,1}, \dots, \alpha_{1,c/e}, \alpha_{2,1}, \dots, \alpha_{2,d/e} \in \mathbb{F}_{3^e}\}$$

is a subset of $N(U)$ of size 3^{c+d}. Moreover using (5.9) we observe that S is a subgroup of U_1 with $|S \cap Z(U)| = 3^d$.

For $n \mid (3^e - 1)$, let α_0 be an element of $\mathbb{F}_{3^e} \setminus \{0\}$ of multiplicative order n. Let

$$H = \{\psi_{\alpha_0^i,0,0,0} \circ \psi \mid 1 \le i \le n \text{ and } \psi \in S\}. \tag{5.10}$$

Using (5.9) we observe that H is a subgroup of $N(U)$ of order $n3^{c+d}$. It is easy to observe that $H = T_H U_H$, where $U_H = S$ and

$$T_H = \{\psi_{\alpha_0^i,0,0,0} \mid 1 \le i \le n\}.$$

In the following corollary, we give the number of rational places and the genera of the subfields F^H of F with H as in (5.10).

Corollary 5.4. *Let $0 \le c, d \le 2s+1$ and $n \mid \gcd(q-1, 3^c-1, 3^d-1)$. Then $N(U)$ has a subgroup H, given in* (5.10), *of order $n3^{c+d}$ where*

$$|H \cap U| = |H \cap U_1| = 3^{c+d} \quad \textit{and} \quad |H \cap Z(U)| = 3^d.$$

We have:

(i) *if* $n = 1$ *then*

$$N(F^H) = 1 + \frac{q^3}{3^{c+d}},$$
$$g(F^H) = \frac{1}{2 \cdot 3^{c+d}} \cdot 3q_0(q^2 + qq_0 - 3^{c+d} - q_0 3^d);$$

(ii) *if* $n > 1$ *and* $2 \nmid n$ *then*

$$N(F^H) = 2 + \frac{q^3 - 3^{c+d}}{n3^{c+d}} + \frac{q-1}{n}(n-1),$$
$$g(F^H) = \frac{1}{2n3^{c+d}} \cdot 3q_0(q^2 + qq_0 - 3^{c+d} - q_0 3^d);$$

(iii) *if* $n > 1$ *and* $2 \mid n$ *then*

$$N(F^H) = 2 + \frac{2(q/3^c - 1)}{n} + \frac{q^3 - q3^d}{n3^{c+d}} + \frac{q(3^c - 1)}{3^c n} + \frac{q-1}{n}(n-2),$$
$$g(F^H) = \frac{1}{2n3^{c+d}}\,[3q_0(q^2 + qq_0 - 3^{c+d} - q_0 3^d) - 3^{c+d}(q/3^c - 1)].$$

In Section 7, for $q = 27$ we give more examples, including some examples with $b \neq 0$.

REMARK 5.5. We note that Theorem 3.9 corresponds to the very special subcase of Corollary 5.4 with $d = 0$ and $n \in \{1, 2\}$.

6. Dihedral groups of order $2(q-1)$. Let F be the function field defined by (1.1) and G be its automorphism group $\mathrm{Aut}(F/\mathbb{F}_q)$. Let T_2 be a Hall subgroup of order $(q-1)/2$ and D be the normalizer of T_2, which is a dihedral group of order $2(q-1)$ (cf. property (5) in [C-O, Proposition 2.3]). Let T be the cyclic group of order $q-1$ in D. Let κ be the involution of T. We note that D is a subgroup of the centralizer $C(\kappa)$ of κ and $C(\kappa) = \langle\kappa\rangle \times L'$, where L' is the unique subgroup of $C(\kappa)$ isomorphic to $\mathrm{PSL}(2, q)$ (cf. Subsection 4.1 in [C-O]). There exists a dihedral subgroup D' of L' such that

$$D = \langle\kappa\rangle \times D'.$$

In this section we determine the number of rational places of a subfield F^H fixed by a subgroup $H \leq D$. We note that any dihedral subgroup of G of order $2n$ with $n \mid (q-1)$ is contained in a conjugate of D (cf. [C-O, Theorem 2.4, property (5) in Proposition 2.3 and Remark 2.2]).

As $H \leq D$ and $\gcd(2(q-1), q - 3q_0 + 1) = 1$, the degree 6 places, so the nonrational places of F, are unramified in the extension F/F^H. Any cyclic subgroup of D is either of degree 2 or contained in T. Since F has no degree 2 place, $N(H, m)$ can be nonzero only for integers $m \neq 2$ dividing $q - 1$.

If the order of H is 2, then $N(F^H) = N(F^H, 1)$. Assume that the order of H is greater than 2. So H is either a cyclic subgroup of T of order n or a dihedral subgroup of order $2n$ with $n|(q-1)$. If H is a cyclic subgroup of T, then it is also a subgroup of the normalizer $N(U)$ of a 3-Sylow subgroup U of G and its number of rational places is already determined in Corollary 5.4 (corresponding to the case $c = d = 0$ in Corollary 5.4). We assume that H is a dihedral group with $|H| = 2n$ and $n \,|\, (q-1)$.

Let P_∞ and P_0 be the places of F corresponding to the pole of x, and to the common zero of x, y_1 and y_2 respectively in (1.1). There exists a conjugate of T fixing P_0 and P_∞ (cf. [C-O, Remark 2.2 or Proposition 2.5]). Therefore we assume, without loss of generality, that T fixes P_0 and P_∞. For $m > 2$ and $m \,|\, n$, H has a unique cyclic subgroup of order m and the number of distinct elements of order m in H is $\phi(m)$, where $\phi(\cdot)$ is Euler's Phi function. The number $N(F^H, m)$ will be determined using the results of Section 4. It follows from (4.7) and Proposition 4.3 that

$$N(F^H, m) = \frac{q-1}{|H|}\,\phi(m).$$

Now we are ready to calculate the number $N(F^H)$ of rational places of F^H.

THEOREM 6.1. *For $n \,|\, (q-1)$, there exists a dihedral subgroup of order $2n$. For a dihedral subgroup H of order $2n$ with $n \,|\, (q-1)$ we have*:

(i) *if $2 \nmid n$, then*

$$N(F^H) = 1 + \frac{q+1}{2} + \frac{q^3-1}{2n} + \frac{q-1}{2n}\,(n-1),$$
$$g(F^H) = \frac{1}{4n}\,(q-1)(3q_0q + q + 3q_0 - n);$$

(ii) *if $2 \,|\, n$, then*

$$N(F^H) = 1 + \frac{q-1}{n} + \frac{q+1}{2} + \frac{q^3-q}{2n} + \frac{q-1}{2n}\,(n-2),$$
$$g(F^H) = \frac{1}{4n}\,(q-1)(3q_0q + q + 3q_0 - n - 1).$$

Proof. We have

$$N(F^H) = N(F^H, 1) + \sum_{\substack{m|n \\ m>2}} N(F^H, m), \tag{6.1}$$

and using (5.8) we get

$$\sum_{\substack{m|n \\ m>2}} N(F^H, m) = \begin{cases} \dfrac{q-1}{2n}\,(n-1) & \text{if } 2 \nmid n, \\ \dfrac{q-1}{2n}\,(n-2) & \text{if } 2 \,|\, n. \end{cases} \tag{6.2}$$

When $2 \nmid n$, the number of involutions in H is n and none of them fixes P_0 or P_∞. So there are $n(q+1)$ more ramified places with ramification index 2.

Therefore, we have

$$N(F^H,1) = 1 + (q+1) + \frac{q^3 - 1 - n(q+1)}{2n}. \tag{6.3}$$

In the case $2 \mid n$, H has $n+1$ involutions and exactly one of them fixes the places P_0 and P_∞. So $(q-1)+n(q+1)$ places are ramified with ramification index 2. We have

$$N(F,1) = 1 + \frac{q-1}{n} + (q+1) + \frac{q^3 - 1 - (q - 1 + n(q+1))}{2n}. \tag{6.4}$$

Using (6.1)–(6.4) we calculate the number of rational places in both cases. The genus in each case is computed in [C-O, page 153]). ∎

7. Examples. Let $F = \mathbb{F}_{27}(x, y_1, y_2)$ be the function field over $\mathbb{F}_{27}$ defined by

$$y_1^{27} - y_1 = x^3(x^{27} - x), \quad y_2^{27} - y_2 = x^6(x^{27} - x),$$

let $G = \mathrm{Aut}(F/\mathbb{F}_{27})$ be its automorphism group, $N(U)$ the normalizer of a 3-Sylow subgroup $U < G$, and $D < G$ a dihedral subgroup of order 52. In this section, we give the number of rational places $N(F^H)$ and the genus $g(F^H)$ of subfields F^H fixed by various subgroups of $N(U)$ and D.

Let $H \le N(U)$ be a subgroup of order $|H| = n3^{b+c+d}$, with $n \mid 26$ and $0 \le b, c, d \le 3$ where $|H \cap U_1| = 3^{c+d}$ and $|H \cap Z(U)| = 3^d$ as in Section 5, and let $\widetilde{n}_9(H)$ be defined by (5.5) (here we assume U fixes the place P_∞, the pole of x). The following examples are a consequence of Theorem 3.9:

- H with $n = 2$, $b = 0$, $c = 0$, $d = 0$, $\widetilde{n}_9(H) = 0$:
  $N(F^H) = 9856$, $g(F^H) = 1800$.
- H with $n = 1$, $b = 0$, $c = 3$, $d = 0$, $\widetilde{n}_9(H) = 0$:
  $N(F^H) = 730$, $g(F^H) = 117$.
- H with $n = 2$, $b = 0$, $c = 3$, $d = 0$, $\widetilde{n}_9(H) = 0$:
  $N(F^H) = 379$, $g(F^H) = 65$.

Using Corollary 5.4 we obtain the following examples:

- H with $n = 26$, $b = 0$, $c = 0$, $d = 0$, $\widetilde{n}_9(H) = 0$:
  $N(F^H) = 784$, $g(F^H) = 139$.
- H with $n = 1$, $b = 0$, $c = 1$, $d = 3$, $\widetilde{n}_9(H) = 0$:
  $N(F^H) = 244$, $g(F^H) = 36$.
- H with $n = 1$, $b = 0$, $c = 3$, $d = 1$, $\widetilde{n}_9(H) = 0$:
  $N(F^H) = 244$, $g(F^H) = 40$.
- H with $n = 2$, $b = 0$, $c = 0$, $d = 3$, $\widetilde{n}_9(H) = 0$:
  $N(F^H) = 379$, $g(F^H) = 52$.

Using Theorem 5.3 and constructing subgroups of $N(U)$ with $b \neq 0$ explicitly, we obtain the following examples:

- H with $n=1$, $b=1$, $c=1$, $d=3$, $\widetilde{n}_9(H)=81$: $N(F^H)=109$, $g(F^H)=12$.
- H with $n=2$, $b=1$, $c=1$, $d=2$, $\widetilde{n}_9(H)=18$: $N(F^H)=145$, $g(F^H)=19$.
- H with $n=1$, $b=1$, $c=0$, $d=3$, $\widetilde{n}_9(H)=27$: $N(F^H)=271$, $g(F^H)=39$.
- H with $n=1$, $b=2$, $c=2$, $d=3$, $\widetilde{n}_9(H)=729$: $N(F^H)=37$, $g(F^H)=1$.

Let now H be a subgroup of D. From the results in Section 6, the following examples are obtained:

- $|H|=2\cdot 2$, dihedral: $N(F^H)=4942$, $g(F^H)=897$.
- $|H|=2\cdot 13$, dihedral: $N(F^H)=796$, $g(F^H)=133$.
- $|H|=2\cdot 26$, dihedral: $N(F^H)=406$, $g(F^H)=63$.

We note that the examples above with genera $12, 36, 39, 40$ are function fields with the best known number of rational places (cf. [G-V]). Moreover the example with genus 19 is a *new entry* for the table of [G-V]. In the following we work out this example and moreover we determine its explicit defining equations for the corresponding function field.

EXAMPLE 7.1. Let H be the subgroup of G generated by $\psi=\psi_{1,1,\gamma+2,0}$ and $\kappa=\psi_{2,0,0,0}$ where $\gamma\in\mathbb{F}_{27}$ with $\mathrm{Tr}(\gamma)\neq 0$. By explicit computations we get

$$\begin{aligned} H\cap U &= \langle \psi_{1,1,2,0}, \psi_{1,0,\gamma,0}, \psi_{1,0,0,1}, \psi_{1,0,0,\gamma}\rangle\,,\\ H\cap U_1 &= \langle \psi_{1,0,\gamma,0}, \psi_{1,0,0,1}, \psi_{1,0,0,\gamma}\rangle\,,\\ H\cap Z(U) &= \langle \psi_{1,0,0,1}, \psi_{1,0,0,\gamma}\rangle\,. \end{aligned}$$

Moreover the elements $\psi_{1,\beta',\gamma',\delta'}$ in H satisfying $\beta'\neq 0$ and $\mathrm{Tr}((\beta')^{-(q_0+1)}\gamma')=1$ are

$$\begin{aligned} &\psi_{1,k,\gamma+2,i+j\gamma}, \quad i,j=0,1,2,\ k=1,2, \qquad \text{when } \mathrm{Tr}(\gamma)=1,\\ &\psi_{1,k,2\gamma+2,i+j\gamma}, \quad i,j=0,1,2,\ k=1,2, \qquad \text{when } \mathrm{Tr}(\gamma)=2. \end{aligned}$$

Therefore we have $n=2$, $b=1$, $c=1$, $d=2$, $\widetilde{n}_9(H)=18$ and from Theorem 5.3 it follows that $g(F^H)=19$, $N(F^H)=145$. We first find defining equations for the function field $F^{H\cap U_1}$. Let $w_1, w_2\in F$ be given by

$$w_1=y_1^3-\gamma^2 y_1, \qquad w_2=y_2^9-\frac{\gamma^9-\gamma}{\gamma^3-\gamma}\,y_2^3+\frac{\gamma^9-\gamma^3}{\gamma^3-\gamma}\,y_2.$$

The elements of $H\cap U_1$ fix x, w_1, w_2. Moreover $F^{H\cap U_1}=\mathbb{F}_{27}(x,w_1,w_2)$ where

$$\begin{aligned} w_1^9+\gamma^{18}w_1^3+\gamma^{24}w_1-x^3(x^{27}-x)=0,\\ w_2^3+\frac{\gamma-\gamma^3}{\gamma^9-\gamma^3}\,w_2-x^6(x^{27}-x)=0. \end{aligned}$$

Now we will determine defining equations for the function field $F^{H\cap U}$. Let $\overline{\psi}$ be the restriction of $\psi_{1,1,2,0}$ to the function field $\mathbb{F}_{27}(x, w_1, w_2)$. We have

$$\begin{aligned}\overline{\psi}(x) &= x + 1,\\ \overline{\psi}(w_1) &= w_1 + x^3 - \gamma^2 x + \gamma^2 + 2,\\ \overline{\psi}(w_2) &= w_2 - w_1^3 + \frac{\gamma^7 - \gamma}{\gamma^3 - \gamma}\, w_1 + x^9 - \frac{\gamma^9 - \gamma}{\gamma^3 - \gamma}\, x^3 + \frac{\gamma^9 - \gamma^3}{\gamma^3 - \gamma}\, x.\end{aligned}$$

Let $u, v_1, v_2 \in F^{H\cap U_1}$ be given by

$$\begin{aligned}u &= x^3 - x,\\ v_1 &= w_1 - x^4 - (\gamma^2 + 1)x^2,\\ v_2 &= w_2 + x w_1^3 - \frac{\gamma^7 - \gamma}{\gamma^3 - \gamma}\, x w_1 + x^{11} - \frac{\gamma^9 - \gamma}{\gamma^3 - \gamma}\, x^5 + \frac{\gamma^9 - \gamma^3}{\gamma^3 - \gamma}\, x.\end{aligned}$$

Then $\overline{\psi}$ and so the restriction of each element in $H \cap U$ to $\mathbb{F}_{27}(x, w_1, w_2)$ fixes u, v_1 and v_2. Moreover $F^{H\cap U} = \mathbb{F}_{27}(u, v_1, v_2)$ where

$$v_1^9 + \gamma^{18} v_1^3 + \gamma^{24} v_1 + u^{12} + (\gamma^{18} - 1)u^6 + (\gamma^{24} + 1)u^2 = 0,$$

$$v_2^3 + \frac{\gamma - \gamma^3}{\gamma^9 - \gamma^3}\, v_2 + \frac{\gamma - \gamma^3}{\gamma^9 - \gamma^3}\, u v_1^3 + \gamma^{24} u v_1 - \frac{\gamma - \gamma^3}{\gamma^9 - \gamma^3}\, u^5 + \frac{\gamma^7 - \gamma^9}{\gamma^9 - \gamma^3}\, u^3 - u = 0.$$

Let $\overline{\kappa}$ be the restriction of $\kappa = \psi_{2,0,0,0}$ to the function field $\mathbb{F}_{27}(u, v_1, v_2)$. Then $\overline{\kappa}(u) = -u$, $\overline{\kappa}(v_1) = v_1$ and $\overline{\kappa}(v_2) = -v_2$. Let $t = u^2$, $z_1 = v_1$ and $z_2 = uv_2$. Then $\overline{\kappa}$, and hence the restriction of each element of H to $\mathbb{F}_{27}(u, v_1, v_2)$, fixes t, z_1 and z_2. Therefore $F^H = \mathbb{F}_{27}(t, z_1, z_2)$ with its explicit defining equations

$$z_1^9 + \gamma^{18} z_1^3 + \gamma^{24} z_1 + t^6 + (\gamma^{18} - 1)t^3 + (\gamma^{24} + 1)t = 0,$$

$$z_2^3 + \frac{\gamma - \gamma^3}{\gamma^9 - \gamma^3}\, t z_2 + \frac{\gamma - \gamma^3}{\gamma^9 - \gamma^3}\, t^2 z_1^3 + \gamma^{24} t^2 z_1 - \frac{\gamma - \gamma^3}{\gamma^9 - \gamma^3}\, t^4 + \frac{\gamma^7 - \gamma^9}{\gamma^9 - \gamma^3}\, t^3 - t^2 = 0.$$

REMARK 7.2. Let E be a subfield of F with full constant field $\mathbb{F}_q$. Let $N(E)$ and $g(E)$ denote the number of rational places and genus of E. In this remark we determine the L-polynomial $L_E(t)$ of E completely, using $N(E)$ and $g(E)$. The L-polynomial $L(t)$ of F is given in property (P4) of Section 1. We note that the polynomials $1 + 3q_0 t + qt^2$ and $1 + qt^2$ are irreducible in $\mathbb{Z}[t]$. Using [La] we observe that $L_E(t)$ divides $L(t)$ and hence

$$L_E(t) = (1 + 3q_0 t + qt^2)^a (1 + qt^2)^b. \tag{7.1}$$

Moreover,

$$2a + 2b = 2g(E) \tag{7.2}$$

and as the coefficient of t in $L_E(t)$ is $3q_0 a$ we have

$$N(E) = q + 1 + 3q_0 a \tag{7.3}$$

(cf. [S, Theorem V.1.15]). Using (7.1)–(7.3) we obtain

$$L_E(t) = (1 + 3q_0t + qt^2)^{(N(E)-q-1)/3q_0}(1 + qt^2)^{g(E)-(N(E)-q-1)/3q_0}.$$

Acknowledgements. The authors would like to thank the anonymous referee for useful suggestions.

The second author is partially supported by the Turkish Academy of Sciences in the framework of Young Scientists Award Programme (F.Ö./TÜBA-GEBIP/2003-13).

References

[C-O] E. Çakçak and F. Özbudak, *Subfields of the function field of the Deligne–Lusztig curve of Ree type*, Acta Arith. 115 (2004), 133–180.

[G-V] G. van der Geer and M. van der Vlugt, *Tables of curves with many points*, available at http://www.science.uva.nl/~geer/tables-mathcomp15.ps.

[H-P] J. P. Hansen and J. P. Pedersen, *Automorphism groups of Ree type*, *Deligne–Lusztig curves and function fields*, J. Reine Angew. Math. 440 (1993), 99–109.

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

[L-N] V. M. Levchuk and Ya. N. Nuzhin, *Structure of Ree groups*, Algebra Logic 24 (1985), 16–26 (transl. from: Algebra Logika 24 (1985), 26–41).

[N-X] H. Niederreiter and C. Xing, *Rational Points on Curves over Finite Fields*: *Theory and Applications*, Cambridge Univ. Press, Cambridge, 2001.

[P] J. P. Pedersen, *A function field related to the Ree group*, in: Lecture Notes in Math. 1518, Springer, Berlin, 1992, 122–131.

[Ro] D. J. S. Robinson, *A Course in the Theory of Groups*, Springer, New York, 1993.

[Se] J.-P. Serre, *Local Fields*, Grad. Texts in Math. 67, Springer, New York, 1979.

[S] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, Berlin, 1993.

[T-V] M. A. Tsfasman and S. G. Vlăduţ, *Algebraic-Geometric Codes*, Kluwer, Dordrecht, 1991.

[W] H. N. Ward, *On Ree's series of simple groups*, Trans. Amer. Math. Soc. 121 (1966), 62–89.

Institute of Applied Mathematics and Department of Mathematics
Middle East Technical University
İnönü Bulvarı
06531, Ankara, Turkey
E-mail: cakcak@metu.edu.tr
ozbudak@math.metu.edu.tr

Received on 15.3.2005
and in revised form on 27.7.2005 (4959)