ACTA ARITHMETICA
115.2 (2004)

Subfields of the function field of the Deligne–Lusztig curve of Ree type

by

Emrah Çakçak and Ferruh Özbudak (Ankara)

1. Introduction. Let F be an algebraic function field over a finite field $\mathbb{F}_q$. The number N of rational places of F is bounded by the Hasse–Weil bound

$$|N-(q+1)| \le 2gq^{1/2},$$

where g is the genus of F. For q a square, F is said to be a *maximal* function field if N reaches the Hasse–Weil upper bound, i.e. $N = q+1+2gq^{1/2}$. If F is a maximal function field over $\mathbb{F}_q$, then all subfields $\mathbb{F}_q \subsetneq E \subset F$ are also maximal over $\mathbb{F}_q$ (see [La]). Maximal function fields are also of interest in coding theory ([T-V], [St], [N-X]).

Let X be a Deligne–Lusztig curve of Ree type defined over $\mathbb{F}_q$, $q = 3^{2s+1}$, $s \ge 1$, and F be its function field. Then $F/\mathbb{F}_q$ is isomorphic to $\mathbb{F}_q(x, y_1, y_2)$ defined by

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

$$y_2^q - y_2 = x^{2q_0}(x^q - x), \tag{1.2}$$

where $q_0 = 3^s$. The function field F has the following properties which uniquely determine it ([H-P]):

- $F/\mathbb{F}_q$ has genus $g = \frac{3}{2}q_0(q-1)(q+q_0+1)$.
- 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 $q^3(q-1)(q^3+1)$.
- $F/\mathbb{F}_q$ has q^3+1 $\mathbb{F}_q$-rational places on which G acts as a permutation group.

From now on F will denote $\mathbb{F}_q(x, y_1, y_2)$ defined by (1.1), (1.2) and G its automorphism group $\mathrm{Aut}(F/\mathbb{F}_q)$. F is itself optimal (it has as many $\mathbb{F}_q$-rational places as possible) and any constant field extension $F\mathbb{F}_{q^m}$, $m \equiv 6 \bmod 12$, is maximal ([P]). Let $H \le G$ be a subgroup of G. We denote by

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

F^H its fixed subfield

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

In this paper we construct a large family of subfields $\mathbb{F}_q \subsetneq E = F^H \subseteq F$ using many subgroups $H \leq G$ and we determine their genera. Every such subfield E is maximal over any constant field extension $F\mathbb{F}_{q^m}$, $m \equiv 6 \bmod 12$.

This work is inspired by a recent paper of Garcia, Stichtenoth, and Xing ([G-S-X]), where the subfields of the Hermitian function fields (which are also function fields of Deligne–Lusztig curves associated to the groups $\mathrm{PSU}(3,q)$) are constructed. The case of Deligne–Lusztig curves of Suzuki type is considered by Giulietti, Korchmáros, and Torres in [G-K-T]. Here we note that, together with Ree type studied here, these three families of curves constitute all the curves which are known as Deligne–Lusztig curves.

This paper is organized as follows. In Section 2 we recall the properties of Ree groups that will be needed later. Section 3 deals with the ramification structure of the places of F in the extension F/F^G. The maximal subgroups of G are known (see [L-N]). In Section 4 we consider various subgroups H of maximal subgroups of G and we compute the genera of their fixed subfields F^H. In our computations, we use the properties of Ree groups viewing them as permutation groups acting on the rational places of F in their usual 2-transitive representation.

2. Properties of Ree groups. In this section, we collect some basic properties of Ree groups. For that purpose, let G denote a Ree group $\mathrm{Ree}(q) = {}^2G_2(q)$, $q = 3q_0^2$, $q_0 = 3^s$, $s \geq 1$; it is known that the group G is simple of order $q^3(q-1)(q^3+1)$. Since the integer $q^3(q-1)(q^3+1)$ has the following relatively prime factorization:

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

G has 3-Sylow subgroups of order q^3 and 2-Sylow subgroups of order 8. In addition to these, it is known that there are Hall subgroups in G corresponding to the remaining factors: $\frac{q-1}{2}$, $\frac{q+1}{4}$, $q+3q_0+1$, $q-3q_0+1$. First we recall the basic properties of Hall subgroups. The details can be found in [Ro].

Hall subgroups. A *Hall subgroup* A of a finite group H is a subgroup with $(|A|, |G : A|) = 1$.

THEOREM 2.1 (Wielandt). *Let the finite group H possess a nilpotent Hall subgroup A. Then every subgroup of order dividing $|A|$ is contained in a conjugate of A. In particular, all Hall subgroups of order $|A|$ of H are conjugate.*

REMARK 2.2. Any Hall subgroup A (with $(3,|A|)=1$) of the Ree group is Abelian. So by Theorem 2.1 any subgroup of G of order dividing $|A|$ is contained in a conjugate of A.

We give some properties of subgroups of G. One can get the details from [L-N] and [W].

PROPOSITION 2.3. *For subgroups of G, the following properties hold*:

(1) *A 2-Sylow subgroup of G is a self-centralizing elementary Abelian subgroup of order 8 and its index in the normalizer is 21.*
(2) *2-subgroups of equal order are conjugate in G, in particular all involutions of G are conjugate.*
(3) *The centralizer of an involution in G is isomorphic to $\mathbb{Z}_2 \times \mathrm{PSL}(2,q)$.*
(4) *In G, for each subgroup E of order 4 there exists a cyclic Hall subgroup A_1 of order $(q+1)/4$ and an element ω of order 6 such that $N(E)=N(A_1)=E \rtimes (A_1 \rtimes \langle\omega\rangle)$ and $C(A_1)=E \times A_1$.*
(5) *G has a cyclic Hall subgroup A_0 of order $(q-1)/2$. The group $N(A_0)$ is dihedral of order $2(q-1)$.*
(6) *G has cyclic Hall subgroups A_2 and A_3 of order $q-3q_0+1$ and $q+3q_0+1$ respectively. A_2 and A_3 are respectively the centralizers of their nonidentity elements and are disjoint from their conjugates. The normalizer $N(A_i)$, $i=2,3$, is a Frobenius group with kernel A_i and a cyclic noninvariant factor of order 6.*
(7) *If U is a 3-Sylow subgroup of G, U has order q^3 and is disjoint from 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 $Z(U)-\langle 1\rangle$.*
(8) *The normalizer $N(U)$ is UT, where T is cyclic of order $q-1$. If κ is the involution of T, then $C_U(\kappa)=C_{U_1}(\kappa)$ is elementary Abelian of order q and $C_U(\kappa)\cap Z(U)=\langle 1\rangle$. If τ is an element of T of* (*odd*) *order $(q-1)/2$, then $C_U(\tau^i)=\langle 1\rangle$ for all $\tau^i \neq 1$.*
(9) *Let A be one of the groups U, A_0, A_1, A_2, A_3 and H be a nontrivial subgroup of A, then $N(H) \le N(A)$.*
(10) *The permutation representation of G on the left cosets of $N(U)$ represents G faithfully as a 2-transitive permutation group in such a way that the subgroup fixing three letters has order 2. In what follows*, *this representation will be called the* usual 2-transitive permutation representation *of G.*

The maximal subgroups of G are described by V. M. Levchuk and Ya. N. Nuzhin in [L-N]:

Theorem 2.4. *Maximal subgroups of G are exhausted*, *up to conjugacy*, *by the following*:

(i) $N(U)$, *the normalizer of a* 3-*Sylow subgroup*;
(ii) $C(\kappa)$, *the centralizer of an involution* κ;
(iii) $N(A_i)$, *the normalizer of the subgroup* A_i, $i = 1, 2, 3$, *where* A_i *are cyclic Hall subgroups of order* $(q + 1)/4, q - 3q_0 + 1, q + 3q_0 + 1$, *respectively*;
(iv) $\mathrm{Ree}(m)$, $q = m^p$, *p being a prime.*

It follows from Proposition 2.3(10) that G can be represented faithfully as a 2-transitive permutation group on a set Ω of cardinality $q^3 + 1$. Let P and Q be distinct points in Ω. Denote by G_P and G_{PQ} the subgroups of G fixing the point P and the points P and Q respectively.

Proposition 2.5. *In its usual* 2-*transitive permutation representation on* Ω, G *has the following properties*:

(i) $G_{PQ} = T$, *where* T *is cyclic of order* $q - 1$. *In particular*, G *has a unique involution fixing two points of* Ω.
(ii) *If a nonidentity element* $\kappa \in G_{PQ}$ *fixes more than two points then* κ *is the involution of* T.
(iii) *Any involution of* G *fixes* $q + 1$ *points of* Ω.
(iv) G_P *is the normalizer* $N(U)$ (*which is of order* $q^3(q-1)$) *of a* 3-*Sylow subgroup* U *of* G. *Moreover*, U *acts transitively on the set* $\Omega - \{P\}$.
(v) *The* 3-*Sylow subgroups are in one-to-one correspondence with the points in* Ω.

Proof. For (i)–(iii) we refer to [K-O-S] and [Re]. Since the action of G on Ω is 2-transitive, we have $|G_P| = |G|/|\Omega| = q^3(q - 1)$. Note that $|N(U)| = q^3(q-1)$ for any 3-Sylow subgroup U of G. Hence, using Theorem 2.4, we find that G_P is the normalizer of a 3-Sylow subgroup U of G. If U is not transitive on $\Omega - \{P\}$ then some element τ of U should fix some point $Q \in \Omega - \{P\}$. This implies $\tau \in G_{PQ}$, which contradicts (i) because q^3 is relatively prime to $q - 1$. This also shows that each point of Ω is fixed by a unique 3-Sylow subgroup of G, which establishes (v) (since G acts transitively on Ω and 3-Sylow subgroups are conjugate in G). ∎

Now, we look at the action of G on Ω more closely and obtain some more properties which we need later.

Theorem 2.6. *Let* $1 \neq \sigma \in G$.

(i) *If* $3 \mid |\sigma|$ *then* $\sigma \in N_G(U)$ *for some* 3-*Sylow subgroup*, U, *of* G, *and* σ *fixes a unique point of* Ω.
(ii) *If* $|\sigma| \mid q - 1$ *and* $|\sigma| \neq 2$ *then* σ *is contained in some cyclic subgroup of* G, *of order* $q - 1$, *and* σ *fixes exactly two points of* Ω.

(iii) *If* $|\sigma| = 2$ *then* σ *fixes exactly* $q+1$ *points of* Ω.

In particular, σ *fixes a point of* Ω *if and only if* $|\sigma| \mid q^3(q-1)$.

For the proof of the theorem we need the following:

LEMMA 2.7. *Let* $3 \mid |\sigma|$. *Then* $\sigma \in N_G(U)$ *for some* 3*-Sylow subgroup*, U, *of* G.

Proof. Write the order of σ as $|\sigma| = 3^f m$ with $(3, m) = 1$. Let $\sigma_0 = \sigma^m$ and $\tau_0 = \sigma^{3^f}$. Then $|\sigma_0| = 3^f$, $\sigma_0 \in U$ for some 3-Sylow subgroup U of G, $|\tau_0| = m$ and $\sigma = \sigma_0\tau_0$. Since σ_0 commutes with τ_0, we have

$$\tau_0\sigma_0^i\tau_0^{-1} = \sigma_0^i \quad \text{for all } i.$$

This implies $\tau_0 \in N_G(\langle\sigma_0\rangle)$ and by Proposition 2.3(9), $N_G(\langle\sigma_0\rangle) \subseteq N_G(U)$. So $\tau_0 \in N_G(U)$ and we get $\sigma = \sigma_0\tau_0 \in N_G(U)$. ∎

LEMMA 2.8. *Let* $1 \neq \sigma \in G$ *with* $|\sigma| \mid q-1$. *Then* σ *is contained in some cyclic subgroup of* G, *of order* $q-1$, *and* σ *fixes* (*at least*) *two points of* Ω.

Proof. If $|\sigma| = 2$ then the result follows from Proposition 2.5. So we assume that $|\sigma| \mid q-1$ and $|\sigma| \neq 2$.

Now, let T be the cyclic subgroup of G of order $q-1$, fixing two distinct points $P, Q \in \Omega$ (cf. Proposition 2.5) and T_2 be the subgroup of T of order $(q-1)/2$. As $|\sigma| \mid q-1$ and $|\sigma| \neq 2$, we have $\sigma^2 \neq 1$ and $|\sigma^2| \mid (q-1)/2$. So σ^2 is contained in a cyclic Hall subgroup of order $(q-1)/2$, which should be a conjugate of T_2 (by Remark 2.2). In other words, there is an element $\alpha \in G$ such that $\sigma^2 \in \alpha T_2\alpha^{-1}$. Obviously $\sigma \in N_G(\langle\sigma^2\rangle)$ and by Proposition 2.3(9), $\sigma \in N_G(\alpha T_2\alpha^{-1})$. Observe that $N_G(\alpha T_2\alpha^{-1}) = \alpha N_G(T_2)\alpha^{-1}$. The group $N_G(T_2)$ (and therefore any of its conjugates) is a dihedral group of order $2(q-1)$ by Proposition 2.3(5). A dihedral group, D, of order $2(q-1)$ has a unique cyclic subgroup of order $q-1$, T_D, and any cyclic subgroup C of D with $|C| \neq 2$ is contained in T_D. Therefore $\sigma \in \alpha T\alpha^{-1}$, which is cyclic of order $q-1$, and σ fixes both $\alpha(P)$ and $\alpha(Q)$, where $\alpha(P) \neq \alpha(Q)$. ∎

We are now ready to prove Theorem 2.6.

Proof of Theorem 2.6. Let $1 \neq \sigma \in G$. Assume first that $3 \mid |\sigma|$. Then by Lemma 2.7, $\sigma \in N_G(U)$ for some 3-Sylow subgroup, U, of G, and by Proposition 2.5, σ fixes a point of Ω. Since $(3, q-1) = 1$, again by Proposition 2.5, σ cannot fix two distinct points of Ω. So we proved (i).

Now, any nonidentity element of G which fixes more than two points of Ω should be an involution, and any involution of G fixes $q+1$ points (cf. Proposition 2.5). So (ii) and (iii) follow from Lemma 2.8.

The necessity part of the last assertion of the theorem follows from Proposition 2.5. For the sufficiency, assume $|\sigma| \mid q^3(q-1)$. Then either $3 \mid |\sigma|$

or $|\sigma|\,|\,q-1$. Therefore, (i)–(iii) (proved above) imply that σ should fix a point of Ω. ■

We are now going to show that the representation of the Ree group $G=\mathrm{Aut}(F/\mathbb{F}_q)$ on the set of rational places of F has the same properties as the usual 2-transitive permutation representation of the Ree group G. In fact, we show that these two representations are the same.

PROPOSITION 2.9. *Let G be a finite group of order mn. Let Ω and Ω' be two sets of equal cardinality $|\Omega|=|\Omega'|=n$. Assume that G acts as a transitive permutation group on each of Ω and Ω'. Assume also that subgroups of order m of G are conjugate to each other. Then the actions of G on Ω and Ω' are the same up to relabelling.*

Proof. Denote the points of Ω by $P_0,\ldots,P_{n-1}$. We will label the points of Ω' as $P'_0,\ldots,P'_{n-1}$ in such a way that for each $\tau\in G$ and each $i=0,\ldots,n-1$,

$$\tau(P_i)=P_j\ \Rightarrow\ \tau(P'_i)=P'_j.$$

This will prove the proposition.

Let $H=G_{P_0}$ be the subgroup of G fixing the point P_0 in Ω. Then $|H|=m$. Observe that H fixes a point P' of Ω'. Consider a point $Q'\in\Omega'$ and the subgroup $G_{Q'}$ fixing Q'. Then $|G_{Q'}|=m$ and by assumption $G_{Q'}$ is a conjugate of H. So $H=\alpha G_{Q'}\alpha^{-1}$ for some $\alpha\in G$. This implies that H fixes $\alpha(Q')$. We set

$$P'_0=\alpha(Q').$$

So any element of H fixes P_0 in Ω and P'_0 in Ω'. Since G acts transitively on Ω, there are $\sigma_1,\ldots,\sigma_{n-1}\in G-H$ such that

$$\sigma_i(P_0)=P_i,\qquad i=1,\ldots,n-1.$$

As the elements of each of the cosets $\sigma_i H$ map P_0 to P_i, we have

$$i\neq j\ \Rightarrow\ \sigma_i H\cap\sigma_j H=\emptyset. \tag{2.1}$$

We label the remaining points of the set Ω' as

$$P'_i=\sigma_i(P'_0),\qquad i=1,\ldots,n-1.$$

For $i\neq j$, $P'_i\neq P'_j$ because otherwise we have $\sigma_i(P'_0)=\sigma_j(P'_0)$, which implies $\sigma_i^{-1}\sigma_j(P'_0)=P'_0$ and $\sigma_i^{-1}\sigma_j\in H$, contradicting (2.1). Therefore we have $\Omega'=\{P'_0,\ldots,P'_{n-1}\}$.

Now, let $\tau\in G$, $i\in\{0,\ldots,n-1\}$, and assume that $\tau(P_i)=P_j$ for some $j=0,\ldots,n-1$. As $\sigma_i(P_0)=P_i$ and $\sigma_j(P_0)=P_j$, we have $\sigma_j^{-1}\tau\sigma_i(P_0)=P_0$. So $\sigma_j^{-1}\tau\sigma_i\in H$ and $\sigma_j^{-1}\tau\sigma_i(P'_0)=P'_0$, which implies $\tau\sigma_i(P'_0)=\sigma_j(P'_0)$. Since $\sigma_i(P'_0)=P'_i$ and $\sigma_j(P'_0)=P'_j$, we get $\tau(P'_i)=P'_j$. ■

COROLLARY 2.10. *If the Ree group G acts transitively on a set of cardinality q^3+1, then this action is unique up to relabelling. In particular, the* *representation of* $G = \mathrm{Aut}(F/\mathbb{F}_q)$ *on the set of rational places of* F *is the usual* 2*-transitive representation of* G*.*

Proof. The order of G is $q^3(q-1)(q^3+1)$. Let H be a subgroup of G of order $q^3(q-1)$. By Theorem 2.4, H is the normalizer $N(U)$ of a 3-Sylow subgroup U of G. Also for any two 3-Sylow subgroups U and U' of G, $N(U)$ and $N(U')$ are conjugate in G. Therefore the result follows from Proposition 2.9 and the fact that F has q^3+1 rational places on which $G = \mathrm{Aut}(F/\mathbb{F}_q)$ acts as a transitive permutation group. ∎

3. The ramification structure. In this section, we find the ramified places of F and the associated ramification groups in the extension F/F^G, where $F = \mathbb{F}_q(x, y_1, y_2)$ (defined by (1.1) and (1.2)) and $G = \mathrm{Aut}(F/\mathbb{F}_q)$.

We first recall the definition of ramification groups of a place P of F in the extension F/F^H, where H is any subgroup of G. Let v_P be the discrete valuation of P and O_P be the valuation ring associated to v_P. For each $i \geq -1$, the *ramification groups* of P are defined as

$$H_i(P) = \{\sigma \in H \mid v_P(\sigma(z) - z) \geq i+1 \text{ for each } z \in O_P\}.$$

The *different exponent* of P in the extension F/F^H is

$$d_P = \sum_{i\geq 0}(|H_i(P)| - 1)$$

(see for example [St, III.8.8]). If g and g_H are the genera of F and F^H respectively, then the *Riemann–Hurwitz formula* states that

$$2g-2 = |H|(2g_H - 2) + \sum_{P \text{ is a place of } F} d_P \deg(P).$$

The group G acts on the rational places of F as a transitive permutation group, therefore each rational place is wildly ramified in the extension F/F^G with ramification index $|G|/(q^3+1) = q^3(q-1)$. Moreover if P and Q are two rational places of F, then for each $i \geq -1$ the ramification groups $G_i(P)$ and $G_i(Q)$ are conjugate in G. The *decomposition group* $G_{-1}(P)$ and the *inertia group* $G_0(P)$ of a rational place P are equal and their order is $q^3(q-1)$. The ramification groups for a rational place are computed in [H-P]:

Theorem 3.1. *Let* P *be a rational place of* F *and* $G_i = G_i(P)$ *be the ramification groups of* P *for the extension* F/F^G*. Let* $\nu_0 = 0$, $\nu_1 = 1$, $\nu_2 = 3q_0 + 1$ *and* $\nu_3 = q + 3q_0 + 1$*. Then*:

(i) $G_0 = G_{\nu_0} = N(U)$, *where* U *is a* 3*-Sylow subgroup of* G *and* $N(U)$ *its normalizer in* G,

(ii) $G_1 = G_{\nu_1} = U$ *with* $|U| = q^3$,

(iii) $G_i = U_1$, *where* U_1 *is the derived group of* U *and* $|U_1| = q^2$ *for* $\nu_1 + 1 \leq i \leq \nu_2$,

(iv) $G_i = Z(U)$, *the center of* U, *which is of order* q *for* $\nu_2 + 1 \le i \le \nu_3$,
(v) $G_i = \langle 1 \rangle$ *for* $i \ge \nu_3 + 1$.

Now in order to find the other ramified places, we first consider the extension $\overline{F}/\overline{F}^G$, where $\overline{F} = F\overline{\mathbb{F}}_q$, the constant field extension of $F/\mathbb{F}_q$ with the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$.

We fix the following notation. For any positive integer m, by an $\mathbb{F}_{q^m}$-*rational place* of $\overline{F}$ we mean a place extending a degree 1 place of $F' = F\mathbb{F}_{q^m}$ in the constant field extension $\overline{F}/F'$. If m and n are positive integers with $n \mid m$ then by an $\mathbb{F}_{q^m} \setminus \mathbb{F}_{q^n}$-*rational place* we mean an $\mathbb{F}_{q^m}$-rational place which is not $\mathbb{F}_{q^n}$-rational. For any subgroup H of G and any place P of $\overline{F}$, the H-*orbit* of P will be the set

$$H.P = \{\sigma(P) \mid \sigma \in H\}.$$

Now, we will use the Riemann–Hurwitz formula to determine the non-$\mathbb{F}_q$-rational places of $\overline{F}$ ramified in $\overline{F}/\overline{F}^G$. The ramification groups at an $\mathbb{F}_q$-rational place Q of $\overline{F}$ are given by Theorem 3.1, so the different exponent of Q is

$$d_Q = (q^3(q-1)-1) + (q^3-1) + 3q_0(q^2-1) + q(q-1).$$

The genus of $\overline{F}^G$ is zero (because $\overline{F}^G \subset \overline{F}_q(x)$) and we know that the genus g of $\overline{F}$ is

$$g = \tfrac{3}{2}q_0(q-1)(q+q_0+1).$$

Since all the $\mathbb{F}_q$-rational places of $\overline{F}$ have the same different exponent, the Riemann–Hurwitz formula applied to the extension $\overline{F}/\overline{F}^G$ gives

$$2g - 2 = -2|G| + (q^3+1)d_Q + R,$$

where R is the degree of the part of the different arising from the ramifications at non-$\mathbb{F}_q$-rational places of $\overline{F}$. Computing R, we get

$$R = q^3(q-1)(q^3 + 1 - (q+1)(q+3q_0+1)).$$

Let $B = G_{-1}(Q)$ be the subgroup of G fixing an $\mathbb{F}_q$-rational place Q. The order of this group is $q^3(q-1)$ and the orbit of it at any non-$\mathbb{F}_q$-rational place has $q^3(q-1)$ elements ([P]). Therefore any non-$\mathbb{F}_q$-rational place of $\overline{F}$ is unramified in $\overline{F}/\overline{F}^B$. Let P_1 be a non-$\mathbb{F}_q$-rational place of $\overline{F}$ ramified in $\overline{F}/\overline{F}^G$. Let P_1^B and P^G be the restrictions of P_1 to the fields $\overline{F}^B$ and $\overline{F}^G$ respectively. Let $P_1^B, \ldots, P_t^B$ be the places of $\overline{F}^B$ lying over P^G in $\overline{F}^B/\overline{F}^G$, and let $e_i = e(P_i^B|P^G)$, $i = 1, \ldots, t$, be the corresponding ramification indices. The diagram in Figure 1 summarizes these definitions and notations.

The extension $\overline{F}^B/\overline{F}^G$ is not Galois. On the other hand, if P is a place of $\overline{F}$ extending P^G, then the ramification index $e(P|P^G)$ of P over P^G is equal to $e(P_1|P^G)$ since $\overline{F}/\overline{F}^G$ is Galois. Also if P^B is the restriction of P to $\overline{F}^B$ then the ramification indices $e(P|P^B)$, $e(P_1|P_1^B)$ of P and P_1 over

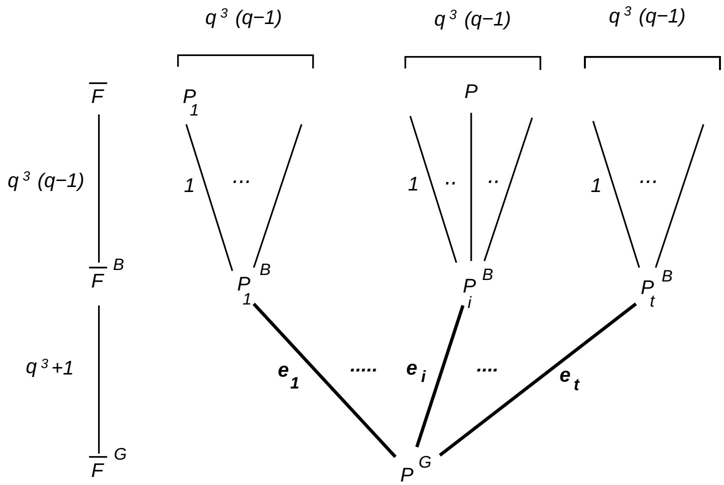

Fig. 1

P^B and P_1^B respectively are both 1. As

$$e(P|P^G) = e(P|P^B)e(P^B|P^G), \qquad e(P_1|P^G) = e(P_1|P_1^B)e(P_1^B|P^G),$$

we get

$$e(P^B|P^G) = e(P_1^B|P_1^G).$$

In other words the ramification indices $e_1, \dots, e_t$ are all equal. So let $e = e_1 = \cdots = e_t$. We have

$$et = q^3 + 1,$$

q^3+1 being the degree of the extension $\overline{F}^B/\overline{F}^G$. In particular e (which is also the ramification index of P_1 over P^G) divides q^3+1 and P_1 is tamely ramified in $\overline{F}/\overline{F}^G$. So the different exponent of P_1 over P^G is $e-1$ and the contribution of all the places of $\overline{F}$ extending P^G to the degree of the different of $\overline{F}/\overline{F}^G$ is $q^3(q-1)t(e-1) = q^3(q-1)(q^3+1-t)$. Comparing this number with R, we see that there is only one ramified place of $\overline{F}^G$ which has a non-$\mathbb{F}_q$-rational extension in $\overline{F}$. As q^3+1 factorizes as $q^3+1 = (q+1)(q+3q_0+1)(q-3q_0+1)$ and $t = (q+1)(q+3q_0+1)$, we get $e = q-3q_0+1$. We summarize the discussion above in the proposition:

PROPOSITION 3.2. *The number of non-$\mathbb{F}_q$-rational places of $\overline{F}$ ramified over $\overline{F}^G$ is $q^3(q-1)(q+1)(q+3q_0+1)$. These places all lie over a single place of $\overline{F}^G$ and their ramification index over that place is $q-3q_0+1$.*

Now we show that the non-$\mathbb{F}_q$-rational places of $\overline{F}$ ramified over $\overline{F}^G$ are exactly the $\mathbb{F}_{q^6} \setminus \mathbb{F}_q$-rational places of $\overline{F}$. In [P] the number N_m of $\mathbb{F}_{q^m}$-rational places of $\overline{F}$ is

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

So the numbers of $\mathbb{F}_{q^2}$-, $\mathbb{F}_{q^3}$- and $\mathbb{F}_{q^6}$-rational places of $\overline{F}$ are

$$N_2 = q^3 + 1, \qquad N_3 = q^3 + 1,$$
$$N_6 = q^3 + 1 + q^3(q-1)(q+1)(q+3q_0+1)$$

respectively. As the number N_1 of $\mathbb{F}_q$-rational places of $\overline{F}$ is q^3+1, $\overline{F}$ has no $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$- and $\mathbb{F}_{q^3} \setminus \mathbb{F}_q$-rational place. Moreover the number of $\mathbb{F}_{q^6} \setminus \mathbb{F}_q$-rational places is equal to the number of non-$\mathbb{F}_q$-rational places of $\overline{F}$ ramified over $\overline{F}^G$. Now if P is an $\mathbb{F}_{q^6} \setminus \mathbb{F}_q$-rational place, every place in the orbit $G.P$ will be so (because the automorphism group $G = \mathrm{Aut}(\overline{F}/\overline{\mathbb{F}}_q)$ is $\mathbb{F}_q$-rational, i.e. every element of G restricts to an automorphism of $F/\mathbb{F}_q$ which will map a degree 6 place of F to a degree 6 place). So we have

$$|G.P| \le N_6 - (q^3+1) < |G|,$$

where $|G.P|$ is the number of elements in the G-orbit of an $\mathbb{F}_{q^6} \setminus \mathbb{F}_q$-rational place P. Therefore every $\mathbb{F}_{q^6} \setminus \mathbb{F}_q$-rational place is ramified in the extension $\overline{F}/\overline{F}^G$. We arrive at the following proposition:

PROPOSITION 3.3. *The non-$\mathbb{F}_q$-rational places of $\overline{F}$ ramified in the extension $\overline{F}/\overline{F}^G$ are exactly the $\mathbb{F}_{q^6} \setminus \mathbb{F}_q$-rational places of $\overline{F}$. Moreover none of these places is $\mathbb{F}_{q^2}$- or $\mathbb{F}_{q^3}$-rational.*

We find the inertia group of an $\mathbb{F}_q^6 \setminus \mathbb{F}_q$-rational place in $\overline{F}/\overline{F}^G$.

LEMMA 3.4. *Let P_1 be an $\mathbb{F}_{q^6} \setminus \mathbb{F}_q$-rational place of $\overline{F}$. Then:*

(i) $G_0(P_1) = M$, *where M is a cyclic Hall subgroup of G with $|M| = q - 3q_0 + 1$.*

(ii) *M fixes exactly six $\mathbb{F}_{q^6} \setminus \mathbb{F}_q$-rational places $P_1, \ldots, P_6$ which are the elements of the $N(M)$-orbit of P_1.*

Proof. The order of the group $G_0(P_1)$ is equal to the ramification index of P_1 in $\overline{F}/\overline{F}^G$:

$$|G_0(P_1)| = q - 3q_0 + 1.$$

Since G contains Hall subgroups of order $q - 3q_0 + 1$, $G_0(P_1)$ is one of them, say M. Consider the $N(M)$-orbit, Ω_1, of P_1. Since $M \lhd N(M)$, any place in Ω_1 is fixed by M. The index of M in $N(M)$ is 6, so M has 6 distinct left cosets in $N(M)$: $\sigma_1 M, \sigma_2 M, \ldots, \sigma_6 M$, $\sigma_i \in N(M)$ and $\sigma_1 = 1$. Clearly Ω_1 has at most 6 elements (corresponding to each coset). Let $P_i = \sigma_i(P_1)$, $i = 2, \ldots, 6$. If $P_i = P_j$ with $i \neq j$ then $\sigma_i^{-1}\sigma_j(P_1) = P_1$ implying $\sigma_i^{-1}\sigma_j \in G_0(P_1) = M$, which is a contradiction because $\sigma_i M$ and $\sigma_j M$ are distinct. So $\Omega_1 = \{P_1, \ldots, P_6\}$ and M fixes the elements of Ω_1.

Let P be an $\mathbb{F}_{q^6} \setminus \mathbb{F}_q$-rational place fixed by M. Since all the $\mathbb{F}_{q^6} \setminus \mathbb{F}_q$-rational places are in the same G-orbit, $P = \sigma(P_1)$ for some $\sigma \in G$. But then $\sigma M \sigma^{-1}$ also fixes P. As $|G_0(P)| = |M| = |\sigma M \sigma^{-1}|$, we have $M = \sigma M \sigma^{-1}$, which implies $\sigma \in N(M)$. Therefore $P \in \Omega_1$. ∎

Now, we will use the results above to find the ramification groups of nonrational places of $F/\mathbb{F}_q$ ramified in F/F^G. First note that the field $\overline{F}^G$ is equal to the compositum $F^G\overline{F}_q$ (since G is $\overline{F}_q$-rational). So $\overline{F}/F$ and $\overline{F}^G/F^G$ are constant field extensions and they are unramified. Therefore the ramified places of F over F^G are exactly the degree 1 places and the degree 6 places. In addition, the ramification index of a degree 6 place of F in F/F^G is $q-3q_0+1$. We have

THEOREM 3.5. *The nonrational places of F ramified in the extension F/F^G are the degree* 6 *places of F and they all lie over a single degree* 1 *place of F^G. For any degree* 6 *place P of F, let $G_{-1}(P)$ and $G_0(P)$ denote its decomposition and inertia groups in F/F^G. Then*:

(i) $G_0(P)=M$, *a cyclic Hall subgroup of order* $q-3q_0+1$ *of* G,
(ii) $G_{-1}(P)=N(M)$, *the normalizer of* M *in* G, *with*

$$|N(M)|=6(q-3q_0+1).$$

Moreover the degree 6 *places of F are in one-to-one correspondence with the Hall subgroups of order* $q-3q_0+1$ *of* G.

Proof. Let P be a degree 6 place of F and $P_1,\dots,P_6$ its extensions in $\overline{F}$. Let $G_0(P_i)$ and $G_0(P)$ denote the inertia groups of P_i and P in $\overline{F}/\overline{F}^G$ and F/F^G respectively. Since $O_P\subset O_{P_i}$ and $\overline{F}/F$ is unramified, for any $\sigma\in G$ and $z\in O_P$ we have

$$v_{P_i}(\sigma(z)-z)\geq 1\ \Rightarrow\ v_P(\sigma(z)-z)\geq 1.$$

So $G_0(P_i)\leq G_0(P)$, but their orders are equal; hence

$$G_0(P)=G_0(P_i),\qquad i=1,\dots,6. \tag{3.1}$$

Set $M=G_0(P)$, which is a cyclic Hall subgroup of order $q-3q_0+1$ of G. By (3.1) and Lemma 3.4, the places $P_1,\dots,P_6$ are in the $N(M)$-orbit of P_1 in $\overline{F}$. So $N(M)$, as a subgroup of $\mathrm{Aut}(F/F^G)$, fixes P:

$$N(M)\leq G_{-1}(P).$$

As $G_0(P)\lhd G_{-1}(P)$ and $N(M)$ is the largest subgroup of G with $M\lhd N(M)$, we get $G_{-1}(P)=N(M)$.

Let P^G denote the restriction of P to F^G. The index $|G_{-1}(P):G_0(P)|=6$ is equal to the relative degree of P over P^G, which implies that P^G is of degree 1 in F^G. The fact that all degree 6 places of F lie over a single place of F^G follows from Proposition 3.2. The last assertion of the theorem follows from:

- $G_0(P)$ does not fix any other degree 6 place (this follows from (3.1) and Lemma 3.4),

- the inertia groups of degree 6 places are conjugate to each other and any conjugate of $G_0(P)$ is the inertia group of a degree 6 place (since the G-orbit of P is the set of degree 6 places in F),
- the Hall subgroups of order $q-3q_0+1$ are conjugate in G. ∎

4. Subfields of F. Every subgroup H of G is contained in a maximal subgroup $\mathcal{M}$ of G. The maximal subgroups of G are given in Theorem 2.4. In this section, for many subgroups H of G we determine the genera of the fixed subfields F^H of F.

The ramification groups in F/F^G are given in Section 3. For any subgroup $H \leq G$, the ramification groups in F/F^H can be calculated using the following theorem (see, for example, [Se, Chapter IV, §1]).

THEOREM 4.1. *Let P be a place of F. For each $i \geq -1$, let $G_i(P)$ be the ramification groups of P in the extension F/F^G and $H_i(P)$ the ramification groups of P in F/F^H. Then*

$$H_i(P) = G_i(P) \cap H \quad \text{for any } i \geq -1.$$

The following theorem gives criteria for membership in the inertia groups $G_0(P)$ of the ramified places P of F in the extension F/F^G:

THEOREM 4.2. *Let σ be a nonidentity element of G. Then σ is in the inertia group $G_0(P)$ of some place P of F if and only if exactly one of the following holds*:

(1) $|\sigma| \mid q^3(q-1)$,
(2) $|\sigma| \mid q-3q_0+1$.

Moreover, if $|\sigma| \mid q-3q_0+1$ and $\sigma \in G_0(P)$, then P is a degree 6 place of F, σ is in some cyclic Hall subgroup of G of order $q-3q_0+1$ and σ is not contained in the inertia group of any other place of F.

In the case $|\sigma| \mid q^3(q-1)$ and $\sigma \in G_0(P)$, P is a degree 1 place of F, $\sigma \in N_G(U)$ for some 3-Sylow subgroup U of G and:

(i) *if $3 \mid |\sigma|$ then σ is not contained in the inertia group of any other place of F*;
(ii) *if $|\sigma| \mid q-1$ and $|\sigma| \neq 2$ then σ is in some cyclic subgroup of G of order $q-1$, and σ is in the inertia group of exactly two places of F which are degree 1 places*;
(iii) *if $|\sigma| = 2$ then σ is in the inertia group of exactly $q+1$ places, all of them being degree 1 places.*

Proof. For a place P of F, $G_0(P) \neq \langle 1 \rangle$ if and only if P is ramified in F/F^G. By Theorems 3.1 and 3.5, the ramified places of F in F/F^G are exactly the degree 1 places and degree 6 places of F. The inertia group of a degree 1 place P is the normalizer $N(U)$ of the corresponding 3-Sylow subgroup U of G and $|N(U)| = q^3(q-1)$ (cf. Theorem 3.1, Proposition 2.5, and Proposition 2.3(8)). The inertia group of a degree 6 place P is the corresponding Hall subgroup M of order $q-3q_0+1$ (cf. Theorem 3.5).

Conversely, assume first that $|\sigma| \mid q-3q_0+1$. By Remark 2.2, $\sigma \in M$ for a Hall subgroup M of order $q-3q_0+1$. Since $(q-3q_0+1, q^3(q-1)) = 1$, σ cannot fix a degree 1 place.

For the case $|\sigma| \mid q^3(q-1)$, the proof follows from Theorem 2.6. ∎

In the rest of this section, Ω will denote the set of degree 1 places $P_0, \ldots, P_{q^3}$ of F. The elements of Ω will be referred to as *points* and G is considered with its usual (faithful, 2-transitive) action on Ω (cf. Corollary 2.10). For two distinct points $P_i, P_j \in \Omega$, G_{P_i} will denote the subgroup of G fixing P_i, and $G_{P_iP_j}$ the subgroup of G fixing both P_i and P_j. Also, for $H \le G$ and $P \in \Omega$, $H.P$ will denote the H-orbit of P, which is the set $\{\sigma(P) \mid \sigma \in H\} \subset \Omega$.

In Subsection 4.1 we find genera of all subfields of F fixed by a subgroup of the centralizer $C(\kappa)$ of an involution κ in G.

4.1. *Centralizer of an involution.* Let κ be an involution of G and $L = C(\kappa)$ be its centralizer. By Proposition 2.3(3), we have

$$L \cong \mathbb{Z}_2 \times \mathrm{PSL}(2,q) \tag{4.1}$$

and $|L| = q(q-1)(q+1)$.

First observe that the $\mathbb{Z}_2$ component in (4.1) is equal to $\langle\kappa\rangle$, since otherwise L would centralize two distinct commuting involutions and should be contained in the normalizer of a subgroup of order 4, which is not the case (see Proposition 2.3(4)). Let us now see that L has a unique subgroup isomorphic to $\mathrm{PSL}(2,q)$. Denote by L' the $\mathrm{PSL}(2,q)$ component in (4.1) and by L'' any subgroup of L isomorphic to $\mathrm{PSL}(2,q)$. Then the order of $L' \cap L''$ should be at least $|\mathrm{PSL}(2,q)|/2$. But by the well known subgroup structure of $\mathrm{PSL}(2,q)$ (see for example Theorem 4.11 below), the only subgroup of order $\ge |\mathrm{PSL}(2,q)|/2$ of $\mathrm{PSL}(2,q)$ is $\mathrm{PSL}(2,q)$ itself, which shows that $L' = L''$. From now on let L' be the subgroup of L which is isomorphic to $\mathrm{PSL}(2,q)$; we have $L = \langle\kappa\rangle \times L' = L' \times \langle\kappa\rangle$.

By Proposition 2.5, κ fixes exactly $q+1$ points, say $P_0, \ldots, P_q$. Let T be the subgroup $G_{P_0P_1}$ fixing P_0 and P_1. By Proposition 2.5, T is cyclic of order $q-1$ and κ is the unique involution of T. Let T_2 be the subgroup of T of order $(q-1)/2$.

We first show that L acts on $P_0, \ldots, P_q$ as a permutation group.

Lemma 4.3. *Any element of G which commutes with κ permutes the fixed points of κ.*

Proof. Let $\sigma \in G$ be such an element, and P_i be a fixed point of κ. Then $\kappa\sigma(P_i) = \sigma\kappa(P_i) = \sigma(P_i)$. So κ fixes $\sigma(P_i)$. ∎

For involutions of G, we have a kind of converse of Lemma 4.3.

LEMMA 4.4. *Any involution of G that permutes any two fixed points of κ commutes with κ.*

Proof. Without loss of generality assume that θ is an involution of G that maps P_0 to P_1. The group $\theta T_2 \theta$ fixes both P_0 and P_1 and $|\theta T_2 \theta| = |T_2|$. Therefore $\theta T_2 \theta = T_2$ and hence $\theta \in N(T_2)$. By Proposition 2.3(5), $N(T_2)$ is a dihedral group of order $2(q-1)$. Since T is cyclic, $T \subset N(T_2)$ as well. Moreover $\theta \notin T$ since θ does not fix neither P_0 nor P_1. Therefore $N(T_2) = \langle \theta, T \rangle$. Let τ be a generator of T. Then $\theta\tau = \tau^{-1}\theta$. As $\kappa = \tau^{(q-1)/2}$ and $(\tau^{(q-1)/2})^{-1} = \tau^{(q-1)/2}$, we get $\theta\kappa = \kappa\theta$. ∎

The following two lemmata will be essential in the genus calculations.

LEMMA 4.5. *Let σ be a nonidentity element of L fixing some point $Q \notin \{P_0, \dots, P_q\}$. Then*:

(i) *σ does not fix any of $P_0, \dots, P_q$,*
(ii) *$|\sigma| = 2$.*

Proof. Let $1 \neq \sigma \in L$ and $\sigma(Q) = Q$ for some $Q \notin \{P_0, \dots, P_q\}$. Let l be a prime dividing $m = |\sigma|$. Assume that $\sigma(P_i) = P_i$ for some $i = 0, 1, \dots, q$. We have

$$\sigma^{m/l}(P_i) = P_i, \quad \sigma^{m/l}(Q) = Q, \quad |\sigma^{m/l}| = l.$$

As $\sigma^{m/l}$ fixes two points (Q and P_i), by Proposition 2.5 we have $l \mid q-1$. Moreover $\sigma^{m/l}$ cannot fix P_j for any $j \neq i$. Otherwise $\sigma^{m/l}$ fixes three distinct points and $\sigma^{m/l}$ should be an involution, indeed it should be κ since there is a unique involution fixing P_i and P_j (cf. Proposition 2.5). However κ does not fix $Q \notin \{P_0, \dots, P_q\}$, which is a contradiction. Hence by Lemma 4.3, $\sigma^{m/l}$ permutes q points ($\{P_0, \dots, P_q\} - \{P_i\}$) without fixing any of them. As $l = |\sigma^{m/l}|$ is prime, this implies $l \mid q$, which is a contradiction because $l \mid q-1$ and $(q, q-1) = 1$.

Therefore σ cannot fix any of $P_0, \dots, P_q$. The same is true for $\sigma^{m/l}$. Then by Lemma 4.3, $\langle \sigma^{m/l} \rangle$ acts without fixed point on $q+1$ points, so $l \mid q+1$. As σ fixes the point Q, $|\sigma| \mid q^3(q-1) = |G_Q|$ (by Proposition 2.5), which implies $l \mid q^3(q-1)$. Since $(q+1, q^3(q-1)) = 2$, we have $l = 2$, but 2 is the greatest power of 2 dividing $q^3(q-1)$, so $|\sigma| = 2$. ∎

LEMMA 4.6. *Let $\kappa_1 \neq \kappa_2$ be two involutions of G. Then*:

(i) *If κ_1 commutes with κ_2 then they cannot fix the same point of Ω.*
(ii) *Assume there is an involution distinct from κ_1 and κ_2 which commutes with both κ_1 and κ_2. Then κ_1 and κ_2 cannot fix the same point.*

Proof. Assume $\kappa_1\kappa_2 = \kappa_2\kappa_1$. Then $|\langle \kappa_1, \kappa_2 \rangle| = 4$. But $|G_P| = q^3(q-1)$ for any $P \in \Omega$ and $4 \nmid q^3(q-1)$, which proves (i).

To show (ii), let κ be the involution with $\kappa_1 \neq \kappa \neq \kappa_2$ commuting with both κ_1 and κ_2. Suppose $\kappa_1(Q) = Q = \kappa_2(Q)$ for some $Q \in \Omega$. Then

$$\kappa_i\kappa(Q) = \kappa\kappa_i(Q) = \kappa(Q) \quad \text{for } i = 1, 2.$$

So κ_1 and κ_2 fixes both Q and $\kappa(Q)$. As κ commutes with κ_1 (and κ_2), by (i), $\kappa(Q) \neq Q$. Recall that G has a unique involution fixing two distinct points (Proposition 2.5); this implies $\kappa_1 = \kappa_2$, which is not the case. ∎

To identify the ramification groups in the extension F/F^L, we also use the following lemma:

LEMMA 4.7. *Let $P \neq Q$ be two points of Ω. Then G has an involution θ with $\theta(P) = Q$.*

Proof. As G acts 2-transitively on Ω, there is an element $\theta \in G$ such that $\theta(P) = Q$ and $\theta(Q) = P$. We will show that θ is indeed an involution of G.

Now, θ^2 fixes both P and Q and by Proposition 2.5, we have

$$|\theta^2| \mid q - 1,$$

implying $|\theta| \mid 2(q-1) = 4\left(\frac{q-1}{2}\right)$. If $|\theta| \nmid q-1$ then $4 \mid |\theta|$, but there is no element of order 4 in G, since 2-Sylow subgroups of G are elementary Abelian (by Proposition 2.3(1)). So $|\theta| \mid q-1$ and by Theorem 2.6, θ fixes (at least) two points P' and Q'. As θ does not fix P and Q, $\{P, Q\} \cap \{P', Q'\} = \emptyset$. This implies that θ^2 fixes four distinct points: P, Q, P', Q'. So by Proposition 2.5, θ^2 is either an involution or the identity of G. If θ^2 is an involution then $|\theta| = 4$, which is not possible. Therefore $\theta^2 = 1$ and θ is an involution. ∎

PROPOSITION 4.8. *The group L has exactly $q+1$ 3-Sylow subgroups each fixing one of $P_0, \ldots, P_q$.*

Proof. Let V be a 3-Sylow subgroup of L. Then V fixes P_j for some $j = 0, 1, \ldots, q$. We will construct $q + 1$ conjugates (in L) of V, each fixing one of $P_0, \ldots, P_q$, and so the list of 3-Sylow subgroups in L will be exhausted (there may be at most $q+1$ 3-Sylow subgroups in L). Let $P_k \in \{P_0, \ldots, P_q\}$ be distinct from P_j and θ be an involution in G with $\theta(P_j) = P_k$. The existence of θ is justified by Lemma 4.7, and $\theta \in L$ by Lemma 4.4.

Now by Proposition 2.5, any 3-Sylow subgroup of G either fixes a point or maps it to q^3 distinct points. Also, by Lemma 4.3, V should permute the points $P_0, \ldots, P_q$. Therefore the V-orbits of P_j and P_k are

$$V.P_j = \{P_j\}, \qquad V.P_k = \{P_0, \ldots, P_q\} - \{P_j\}.$$

In other words, the elements $\sigma\theta$, $\sigma \in V$, maps P_j to q distinct points $\{P_0, \ldots, P_q\} - \{P_j\}$. Hence the groups $\sigma\theta V\theta\sigma^{-1}$, $\sigma \in V$, are q distinct conjugates of V each fixing one of the points in the set $\{P_0, \ldots, P_q\} - \{P_j\}$. ∎

Let V be the 3-Sylow subgroup of L fixing P_0 and let θ be an involution mapping P_0 to P_1. Consider the set

$$\mathcal{L} = VT \cup V\theta VT,$$

where $VT = \{\sigma\tau \mid \sigma \in V,\ \tau \in T\}$ and $V\theta VT = \bigcup_{\sigma\in V} \sigma\theta VT$. It is clear that $|VT| = q(q-1)$ and $|\sigma\theta VT| = q(q-1)$ for any $\sigma \in V$. Let σ_1 and σ_2 be two distinct elements of V. Then

$$\sigma_1\theta(P_0) = \sigma_1(P_1) \neq \sigma_2(P_1) = \sigma_2\theta(P_0).$$

Any element of VT fixes P_0, so the elements of $\sigma_1\theta VT$ map P_0 to $\sigma_1\theta(P_0) = \sigma_1(P_1)$ and those of $\sigma_2\theta VT$ map P_0 to $\sigma_2\theta(P_0) = \sigma_2(P_1)$. This implies

$$\sigma_1\theta VT \cap \sigma_2\theta VT = \emptyset.$$

Also, for any $\sigma \in V$, $\sigma\theta(P_0) = \sigma(P_1) \neq P_0$ and $VT \cap \sigma\theta VT = \emptyset$. Therefore, the number of elements in $\mathcal{L}$ is $q(q-1)(q+1)$, which equals the order of L. Hence

$$L = VT \cup V\theta VT. \tag{4.2}$$

In particular, the subgroup of L fixing P_0 is VT. Since $VT = VT_2 \times \langle\kappa\rangle$, the subgroup of L' fixing P_0 is VT_2.

We are now ready to find the ramification groups of a place fixed by κ in the extension F/F^L:

Theorem 4.9. *Let P be a place fixed by κ, and V the 3-Sylow subgroup of L fixing P. Then the ramification groups in the extension F/F^L are*:

(i) $L_0(P) = N_L(V) = VT$, *where T is a subgroup of L of order $q-1$ fixing P and any one of the remaining places fixed by κ. The order of $L_0(P)$ is $q(q-1)$.*
(ii) $L_i(P) = V$ *with* $|L_i(P)| = q$ *for* $1 \le i \le 3q_0 + 1$.
(iii) $L_i(P) = \langle 1\rangle$ *for* $i \ge 3q_0 + 2$.

Proof. Let U be the 3-Sylow subgroup of G fixing P, $N(U) = UT$ its normalizer, U_1 its derived group and $Z(U)$ its center. Then by Theorem 3.1 the ramification groups of P in the extension F/F^G are:

$$\begin{gathered} G_0(P) = N(U), \qquad G_1(P) = U, \\ G_i(P) = \begin{cases} U_1 & \text{for } 2 \le i \le 3q_0 + 1, \\ Z(U) & \text{for } 3q_0 + 2 \le i \le q + 3q_0 + 1. \end{cases} \end{gathered} \tag{4.3}$$

By Theorem 4.1, $L_i(P) = L \cap G_i(P)$. As V is a 3-Sylow subgroup of L, $L_1(P) = V$. By Proposition 2.3(8), $V \cap U_1 = V$ (since $C_U(\kappa) = C_{U_1}(\kappa)$) and $V \cap Z(U) = \langle 1\rangle$ (since $C_U(\kappa) \cap Z(U) = \langle 1\rangle$), so that

$$L_i(P) = \begin{cases} V & \text{for } 1 \le i \le 3q_0 + 1, \\ \langle 1\rangle & \text{for } i \ge 3q_0 + 2. \end{cases} \tag{4.4}$$

The subgroup of L fixing P is VT from the discussion preceding the theorem. So $L_0(P) = VT$. From the properties of ramification groups (cf. [St, Chap. III]) $L_1(P) \lhd L_0(P)$, so by Proposition 2.3(9), $N_L(V) \leq UT$. Since $L \cap UT = VT$, we get $N_L(V) = VT$. ∎

COROLLARY 4.10. *Let P be a place fixed by κ and H be a subgroup of L. Then the ramification groups $H_i = H_i(P)$ of P in the extension F/F^H are $H_i = L_i(P) \cap H$, $i \geq 0$. In particular $H_i = H_1$ for $2 \leq i \leq 3q_0 + 1$, $H_i = \langle 1 \rangle$ for $i \geq 3q_0 + 2$, and the different exponent of P in F/F^H is given by*

$$d_P = (|H_0| - 1) + (|H_1| - 1) + 3q_0(|H_1| - 1).$$

4.1.1. *The subgroups of L.* The subgroups of $\mathrm{PSL}(2, q)$ are well known by what is commonly called Dickson's Hauptsatz (see [V-M] for a proof involving the ramifications in subfields of the rational function field). When $q = 3^{2s+1}$, $s \geq 1$, this theorem becomes:

THEOREM 4.11 (L. E. Dickson). $\mathrm{PSL}(2, q)$, $q = 3^{2s+1}$, $s \geq 1$, *has only the following subgroups*:

(1) *elementary Abelian 3-groups of order 3^f with $f \leq 2s + 1$;*
(2) *cyclic groups of order n with $n \mid (q \pm 1)/2$;*
(3) *dihedral groups of order $2n$ with $n \mid (q \pm 1)/2$;*
(4) *A_4, alternating group on four letters*;
(5) *semidirect products of elementary Abelian 3-groups of order 3^f with cyclic groups of order n with $f \leq 2s + 1, n \mid 3^f - 1$ and $n \mid (q - 1)/2$;*
(6) $\mathrm{PSL}(2, 3^f)$ *with $f \mid 2s + 1$.*

REMARK 4.12. Let $H \leq L$ be a subgroup with $\kappa \notin H$ and $H \nleq L'$. Then the following isomorphism Φ maps H into L': $\Phi(\alpha) = \alpha$ for each $\alpha \in H \cap L'$ and $\Phi(\beta) = \kappa\beta$ for each $\beta \in H \setminus (H \cap L')$. So H is a subgroup of L which does not contain κ and which is isomorphic to a subgroup of $\mathrm{PSL}(2, q)$. In the subsections below, where we calculate the genera of subfields fixed by subgroups of L', it is easily seen that this property is enough to carry out the calculations. Therefore the genus of F^H is equal to the genus $F^{\Phi(H)}$. So for our purposes, it is enough to consider the subgroups of L' (listed in Theorem 4.11) and their direct products with $\langle \kappa \rangle$.

In each subsection below we will find the genera of the subfields of F corresponding to a distinct (type of) subgroup listed in Theorem 4.11, and its direct product by κ. First observe that since $(|L|, q - 3q_0 + 1) = 1$, if P is a ramified place of F in the extension F/F^H of any subgroup $H \leq L$, then P should be a degree 1 place by Theorem 4.2.

Elementary Abelian 3-groups. Let V' be a 3-group in L' of order 3^f, $f \leq 2s + 1$ and V be the 3-Sylow subgroup of L containing V'. Since the 3-Sylow subgroups are disjoint, only one place P of F is ramified in the extension

$F/F^{V'}$, which is one of the places fixed by κ (see Proposition 4.8). By Theorem 4.9 and Corollary 4.10, the different exponent of this place in $F/F^{V'}$ is

$$d_P = (3^f - 1) + (3^f - 1) + 3q_0(3^f - 1).$$

If we let $g_{V'}$ be the genus of $F^{V'}$ then the Riemann–Hurwitz formula applied to the extension $F/F^{V'}$ gives

$$2g - 2 = 3^f(2g_{V'} - 2) + (3q_0 + 2)(3^f - 1),$$

where $g = \frac{3}{2}q_0(q-1)(q+q_0+1)$ is the genus of F and $g_{V'}$ is computed as

$$g_{V'} = \tfrac{1}{2}\,[3^{-f}(3q_0q^2 + q^2 - q) - 3q_0].$$

Let $H = \kappa \times V'$ and g_H be the genus of F^H. As κ fixes the place P, $\kappa \in H_0(P)$ (the inertia group of P in F/F^H), so $H_0(P) = H$ and the different exponent, d_P^H, of P, in F/F^H becomes

$$d_P^H = (2(3^f) - 1) + (3^f - 1) + 3q_0(3^f - 1).$$

Any element $\sigma \in H$ with $3 \mid |\sigma|$ can fix only one place (cf. Theorem 2.6), which should be P (because $H_0(P) = H$). The group H does not contain any involution other than κ. Also $H - \{\kappa\}$ has no element of order dividing $q-1$. So by Theorem 2.6, the remaining ramified places of F in F/F^H are the q other places fixed by κ, each with ramification index 2. So the Riemann–Hurwitz formula states that

$$2g - 2 = 2(3^f)(2g_H - 2) + (2(3^f) - 1) + (3q_0 + 1)(3^f - 1) + q$$

and we have

$$g_H = \tfrac{1}{4}[3^{-f}(3q_0q^2 + q^2 - 2q) - 3q_0 + 1].$$

In the particular case where $V' = V$, the genus g_V of F^V is

$$g_V = \tfrac{1}{2}(3q_0 + 1)(q - 1)$$

and the genus of $F^{\langle\kappa\rangle \times V}$ equals

$$g_{\kappa V} = \tfrac{1}{4}(3q_0 + 1)(q - 1).$$

Cyclic groups of order dividing $(q+1)/2$. Let C^+ be a subgroup of L' of order $n \mid (q+1)/2$. Assume first that $2 \nmid n$. Then C^+ does not contain any involution and any element of order 3. Also $(n, q-1) = 1$, which implies $C^+ \cap L_0(P) = \langle 1 \rangle$ for all P. So the extension F/F^{C^+} is unramified and

$$2g - 2 = n(2g_{C^+} - 2),$$

where g_{C^+} (the genus of F^{C^+}) is computed as

$$g_{C^+} = \frac{1}{2n}\left(3q_0(q-1)(q+q_0+1) - 2\right) + 1.$$

If $2 \mid n$ then C^+ (being a cyclic group) contains only one involution. So F/F^{C^+} is ramified at $q+1$ places with ramification index 2. Applying the

Riemann–Hurwitz formula $2g-2 = n(2g_{C^+}-2)+q+1$, we get

$$g_{C^+} = \frac{1}{2n}\left(3q_0(q-1)(q+q_0+1)-q-3\right)+1.$$

Consider now the subgroup $H^+ = \langle\kappa\rangle \times C^+$ of L. Again we have two cases. If $2\nmid n$, then H^+ contains only one involution so that

$$2g-2 = 2n(2g_{H^+}-2)+q+1$$

where g_{H^+} is the genus of F^{H^+}, computed as

$$g_{H^+} = \frac{1}{4n}\left(3q_0(q-1)(q+q_0+1)-q-3\right)+1.$$

If $2\,|\,n$ then H^+ has 3 distinct involutions. Since (by Lemma 4.6) distinct involutions of L fix disjoint set of points, F/F^{H^+} is ramified at $3(q+1)$ places of F. In this case, g_{H^+} is computed as

$$g_{H^+} = \frac{1}{4n}\left(3q_0(q-1)(q+q_0+1)-3q-5\right)+1.$$

We consider the following particular cases: if $|C^+| = (q+1)/4$, then the genera of F^{C^+} and $F^{\langle\kappa\rangle\times C^+}$ are

$$g_{C^+} = 6q_0q+2q-6q_0-3, \qquad g_{\kappa C^+} = 3q_0q+q-3q_0-2,$$

respectively, and if $|C^+| = (q+1)/2$, then

$$g_{C^+} = 3q_0q+q-3q_0-2, \qquad g_{\kappa C^+} = \tfrac{1}{2}(3q_0q+q-3q_0-5)+1.$$

Cyclic groups of order dividing $(q-1)/2$. Let $C^- \le L'$ with $n = |C^-|$ dividing $(q-1)/2$. Note that the extension F/F^{C^-} is tame because $3\nmid n$. Let T be the cyclic subgroup of G of order $q-1$, fixing P_0 and P_1. By Remark 2.2, C^- is conjugate to a subgroup of T. So without loss of generality we assume $C^- \le T$. Therefore, the inertia groups of P_0 and P_1, in the extension F/F^{C^-}, are

$$C_0^-(P_0) = V_0T\cap C^- = C^-, \qquad C_0^-(P_1) = V_1T\cap C^- = C^-,$$

where V_0 and V_1 are the 3-Sylow subgroups of L fixing P_0 and P_1 respectively. As $2\nmid(q-1)/2$, C^- does not contain any involution, so F/F^{C^-} is ramified only at the places P_0 and P_1. If g_{C^-} is the genus of F^{C^-}, we have

$$2g-2 = n(2g_{C^-}-2)+2(n-1)$$

and

$$g_{C^-} = \frac{g}{n} = \frac{3}{2n}\,q_0(q-1)(q+q_0+1).$$

Now, let $H^- = \kappa \times C^-$. As $\kappa \in T$, again we have $H^- \le T$. So the extension F/F^{H^-} is ramified at P_0, P_1 with ramification index $2n$, and at $q-1$ other places, fixed by κ, with ramification index 2. If we apply the

Riemann–Hurwitz formula to F/F^{H^-}:

$$2g-2=2n(2g_{H^-}-2)+2(2n-1)+q-1$$

where g_{H^-} is the genus of F^{H^-}, we get

$$g_{H^-}=\frac{1}{4n}(q-1)(3q_0q+q+3q_0-1).$$

When $n=(q-1)/2$, H^- becomes equal to T and the genus of F^T is

$$g_T=\tfrac{1}{2}(3q_0q+q+3q_0-1).$$

Dihedral groups of order $2n$ *with* n *dividing* $(q+1)/2$. Let $D^+\le L'$ be a dihedral subgroup of order $2n$ with $n\,|\,(q+1)/2$. Since $(q+1,q(q-1))=2$, the ramification index of any place of F, in F/F^{D^+}, is at most 2. Let C^+ be the subgroup of D^+ of order n and θ an involution in D^+ which is not contained in C^+. Then

$$D^+=\langle\theta,C^+\rangle.$$

The involutions of D^+ are

(1) the elements in $\{\theta\sigma\mid\sigma\in C^+\}$,
(2) the possible involution of C^+.

So again we have two cases: $2\nmid n$ and $2\,|\,n$. If $2\nmid n$, the number of distinct involutions in D^+ is $n=|C^+|$. So, denoting by g_{D^+} the genus of F^{D^+}, we have

$$2g-2=2n(2g_{D^+}-2)+n(q+1)$$

and we get

$$g_{D^+}=\frac{1}{4n}(q+1)[(3q_0+1)(q-1)-n-1]+1.$$

If $2\,|\,n$, then D^+ has $n+1$ distinct involutions and we have

$$g_{D^+}=\frac{1}{4n}(q+1)[(3q_0+1)(q-1)-n-2]+1.$$

Let $M^+=\langle\kappa\rangle\times D^+\le L$. If $2\nmid n$ then M^+ has $2n+1$ distinct involutions. We have

$$2g-2=4n(2g_{M^+}-2)+(2n+1)(q+1)$$

where g_{M^+} is the genus of F^{M^+}, computed as

$$g_{M^+}=\frac{1}{8n}(q+1)[(3q_0+1)(q-1)-2n-2]+1.$$

In the case $2\,|\,n$, M^+ has $2(n+1)+1=2n+3$ distinct involutions and we get

$$g_{M^+}=\frac{1}{8n}(q+1)[(3q_0+1)(q-1)-2n-4]+1.$$

If $n = (q+1)/4$, we have

$$g_{D^+} = (3q_0+1)(q-1) - (q+1)/4,$$
$$g_{M^+} = \tfrac{1}{2}(3q_0+1)(q-1) - (q+1)/4,$$

and if $n = (q+1)/2$, then

$$g_{D^+} = \tfrac{1}{2}(3q_0+1)(q-1) - (q+1)/4,$$
$$g_{M^+} = \tfrac{1}{4}(3q_0+1)(q-1) - (q+1)/4.$$

Dihedral groups of order $2n$ *with* n *dividing* $(q-1)/2$. Let $D^- \le L'$ be a dihedral subgroup of order $2n$ with $n \,|\, (q-1)/2$. Since $(3, 2n) = 1$, the extension F/F^{D^-} is tame. Let T be the cyclic subgroup of G of order $q-1$, fixing the points P_0 and P_1, and let C^- be the subgroup of D^- of order n. We can assume that $C^- \le T$ by taking a suitable conjugate of D^-. Let θ be an element of D^-, with $\theta \notin C^-$. Then θ is an involution and

$$D^- = \langle \theta, C^- \rangle.$$

The only involution of T is κ, so $\theta \notin T$; moreover, being an involution commuting with κ, θ (and any element of $D^- - C^-$) does not fix any of the points fixed by κ (cf. Lemma 4.6). So, as in the case of cyclic groups of order dividing $(q-1)/2$, the ramification indices of P_0 and P_1, in F/F^{D^-}, are equal to $n = |C^-|$. The other ramified places of F in F/F^{D^-} are those fixed by involutions in D^-. Since $2 \nmid n$, D^- has $n = |C^-|$ involutions, each fixing a disjoint set of $q+1$ points. So the Riemann–Hurwitz formula gives

$$2g - 2 = 2n(2g_{D^-} - 2) + 2(n-1) + n(q+1),$$

where g_{D^-} is the genus of F^{D^-} and we get

$$g_{D^-} = \frac{1}{4n}\,(q-1)(3q_0q + q + 3q_0 - n).$$

Consider now the subgroup $M^- = \langle \kappa \rangle \times D^- \le L$. The ramified places of F in F/F^{M^-} are as follows:

- since $\kappa \in T$, P_0 and P_1 are ramified with ramification index $2n$;
- there are $q-1$ more places, $P_2, \dots, P_q$, fixed by κ, and they are ramified with index 2;
- M^- has $2n$ involutions distinct from κ, each fixing a disjoint set of $q+1$ places (which are also different from $P_0, \dots, P_q$), so that, $2n(q+1)$ more places are ramified with index 2.

Substituting this data in the Riemann–Hurwitz formula,

$$2g - 2 = 4n(2g_{M^-} - 2) + 2(2n-1) + (q-1) + 2n(q+1),$$

where g_{M^-} is the genus of F^{M^-}, we get

$$g_{M^-} = \frac{1}{8n}\,(q-1)(3q_0q + q + 3q_0 - 2n - 1).$$

In the particular case where $n = (q-1)/2$, we have

$$g_{D^-} = \tfrac{1}{4}(6q_0+1)(q+1), \qquad g_{M^-} = \tfrac{1}{4}\cdot 3q_0(q+1).$$

Here we note that, when $n = (q-1)/2$, M^- becomes itself a dihedral group of order $2(q-1)$, generated by the involution θ and the cyclic group T. Moreover, M^- is the normalizer (in G) of the cyclic Hall subgroup $C^- \leq G$ with $|C^-| = (q-1)/2$ (listed in Proposition 2.3(5)).

Semidirect products of elementary Abelian 3-groups with cyclic groups. Let $S = V' \rtimes C^- \leq L'$ be the semidirect product of an elementary Abelian 3-group, $V' \leq L'$, of order 3^f with a cyclic group, $C^- \leq L'$, of order n, with $f \leq 2s+1$, $n \mid 3^f - 1$ and $n \mid (q-1)/2$. Let V be the 3-Sylow subgroup of L' containing V' and T the cyclic subgroup of L, of order $q-1$, containing C^-. Since V' is normal in $S = V' \rtimes C^-$, by Proposition 2.3(9), S is contained in the normalizer $N_L(V)$ of V in L. By Proposition 4.8, V fixes one of the places $P_0, \ldots, P_q$ fixed by κ, and by Theorem 4.9, $N_L(V) = VT$ is the inertia group of that place. So, by taking a suitable conjugate of S, we can assume:

- V (and V') fixes P_0,
- T (and C^-) fixes P_0 and P_1;

in particular, $N_L(V) = VT$ is the inertia group, $L_0(P_0)$, of P_0 in the extension F/F^L. Since $2 \nmid |S|$, S does not contain any involution and the ramifications of F/F^S can occur only at the places fixed by κ. As V' is the only 3-Sylow subgroup of S, only P_0 is wildly ramified. The ramification groups of P_0 in F/F^S are

$$S_0(P_0) = S, \qquad S_i(P_0) = \begin{cases} V' & \text{for } 1 \leq i \leq 3q_0+1, \\ \langle 1 \rangle & \text{for } i \geq 3q_0+2. \end{cases}$$

Therefore the different exponent of P_0 is (cf. Corollary 4.10)

$$d_{P_0} = (3^f n - 1) + (3^f - 1) + 3q_0(3^f - 1).$$

Now the V'-orbit of P_1, $V'.P_1 = \{\sigma(P_1) \mid \sigma \in V'\}$, has 3^f elements, say $V'.P_1 = \{P_1, \ldots, P_{3^f}\}$. Each conjugate of C^- by an element of V', $\sigma C^- \sigma^{-1}$, fixes the place $\sigma(P_1)$. So each place in $V'.P_1$ is tamely ramified in F/F^S with ramification index $n = |C^-|$. Now we will show, using a counting argument, that if $P \neq P_0$ and $P \notin V'.P_1$, then no nonidentity element of S fixes P. Hence the ramified places of F in F/F^S are exactly $P_0, \ldots, P_{3^f}$.

Let $\sigma_1, \sigma_2 \in V'$ be two distinct elements of V'. Then

$$\sigma_i C^- \sigma_i^{-1} \cap V' = \langle 1 \rangle, \qquad i = 1, 2.$$

For $i = 1, 2$, each element of $\sigma_i C^- \sigma_i^{-1}$ fixes both P_0 and $\sigma_i(P_1)$. So any element of $\sigma_1 C^- \sigma_1^{-1} \cap \sigma_2 C^- \sigma_2^{-1}$ fixes P_0, $\sigma_1(P_1)$ and $\sigma_2(P_1)$. As $\sigma_1(P_1) \neq \sigma_2(P_1)$, any element of $\sigma_1 C^- \sigma_1^{-1} \cap \sigma_2 C^- \sigma_2^{-1}$ is either the identity or an involution (because a nonidentity element of G fixing 3 points should be an involution, cf. Proposition 2.5), but S does not contain any involution, so

$$\sigma_1 C^- \sigma_1^{-1} \cap \sigma_2 C^- \sigma_2^{-1} = \langle 1 \rangle.$$

Therefore the number of elements in $\bigcup_{\sigma\in V'}(\sigma C^-\sigma^{-1} - \langle 1\rangle)$ is $|V'|(|C^-|-1) = |S| - |V'|$. So we have

$$S = \bigcup_{\sigma\in V'} (\sigma C^- \sigma^{-1} - \langle 1 \rangle) \cup V',$$

where, for all $\sigma \in V'$, an element in $\sigma C^-\sigma^{-1} - \langle 1\rangle$ fixes only P_0 and $\sigma(P_1)$, and an element of V' fixes only P_0. Hence any element of S fixes either P_0 or an element of $V'.P_1$.

We are ready to compute the genus, g_S, of F^S. We have

$$2g - 2 = 3^f n(2g_S - 2) + d_{P_0} + 3^f(n-1),$$

where $d_{P_0} = 3q_0 3^f - 3q_0 + 3^f n + 3^f - 2$ and we get

$$g_S = \frac{1}{2} \cdot \frac{1}{3^f n} 3q_0(q^2 + qq_0 - q_0 - 3^f).$$

Consider now the subgroup $\langle\kappa\rangle \times S \leq L$. As $\kappa \in T \leq VT$, the different exponent of P_0 in $F/F^{\langle\kappa\rangle\times S}$ is

$$d_{P_0}^{\kappa S} = (2\cdot 3^f n - 1) + (3^f - 1) + 3q_0(3^f - 1).$$

The other ramified places of F in $F/F^{\langle\kappa\rangle\times S}$ are

- the 3^f places fixed by conjugates of $\langle\kappa\rangle \times C^-$, with ramification index $2n$;
- the remaining $q - 3^f$ places fixed by κ, with ramification index 2.

So the Riemann–Hurwitz formula states

$$2g - 2 = 2\cdot 3^f n(2g_{\kappa S} - 2) + d_{P_0}^{\kappa S} + 3^f(2n-1) + (q - 3^f),$$

where $g_{\kappa S}$ denotes the genus of $F^{\kappa\times S}$ and $d_{P_0}^{\kappa S} = 3q_0 3^f - 3q_0 + 2\cdot 3^f n + 3^f - 2$. Then $g_{\kappa S}$ is computed as

$$g_{\kappa S} = \frac{1}{4} \cdot \frac{1}{3^f n}(3q_0 q^2 + q^2 - 2q - 3q_0 3^f + 3^f).$$

When $f = 2s+1$ and $n = (q-1)/2$, we have

$$S = VT_2, \qquad \langle\kappa\rangle \times S = VT,$$

where T_2 is the subgroup of T of order $(q-1)/2$. The genera of F^{VT_2} and F^{VT} are computed as

$$g_{VT_2} = 3q_0 + 1, \qquad g_{VT} = \tfrac{1}{2}(3q_0 + 1)$$

respectively.

The groups isomorphic to $\mathrm{PSL}(2,3^f)$*.* Let L'^f be a subgroup of L' isomorphic to $\mathrm{PSL}(2,3^f)$ with $f \mid 2s+1$. Then

$$|L'^f| = |\mathrm{PSL}(2,3^f)| = \tfrac{1}{2}\cdot 3^f(3^f-1)(3^f+1).$$

If $f=1$, then L'^f is isomorphic to the alternating group on four letters and this case is considered in the next subsection. Therefore we assume here that $f>1$ is an odd integer.

Recall that for any $q=3^{2s+1}$, $s\geq 1$, L has a unique subgroup L' isomorphic to $\mathrm{PSL}(2,q)$ and L' has $q+1$ disjoint 3-Sylow subgroups corresponding to $P_0,\dots,P_q$, the fixed places of κ. Let θ be an involution of L' and assume without loss of generality that $\theta(P_0)=P_1$. Let V be a 3-Sylow subgroup of L' (or equivalently of L) fixing P_0, and T be the subgroup of L fixing P_0 and P_1. Recall the equality (4.2),

$$L = VT \cup V\theta VT.$$

Let T_2 be the subgroup of order $(q-1)/2$ of T. Using the same arguments used to obtain (4.2), we also get

$$L' = VT_2 \cup V\theta VT_2.$$

Note also that L' has $q+1$ disjoint 3-Sylow subgroups corresponding to the fixed places of κ and for the normalizer of V in L' we have $N_{L'}(V)=VT_2$.

Since $f>1$ is odd, considering $\mathrm{Ree}(3^f)$ and by the discussion above, L'^f has 3^f+1 disjoint 3-Sylow subgroups corresponding to $P_0,\dots,P_{3^f}$ among the fixed places of κ. Moreover

$$L'^f = V^fT_2^f \cup V^f\theta^fV^fT_2^f,$$

where V^f is the 3-Sylow subgroup of L'^f fixing P_0, T_2^f is the subgroup, of order $(3^f-1)/2$, fixing P_0 and P_1, and θ^f is an involution of L' such that $\theta^f(P_0)=P_1$. Also $N_{L'^f}(V^f)=V^fT_2^f$, $V^f\leq V$, and $T_2^f\leq T_2$.

Therefore for any $P\in\{P_0,\dots,P_{3^f}\}$, the ramification groups are

$$L_0'^f(P) = V^fT_2^f, \qquad L_i'^f(P) = \begin{cases} V^f & \text{for } 1\leq i\leq 3q_0+1,\\ \langle 1\rangle & \text{for } i\geq 3q_0+2,\end{cases}$$

where V^f is the 3-Sylow subgroup of L'^f fixing P, and T_2^f is the subgroup (of order $(3^f-1)/2$) of L'^f fixing P and all $P_0,\dots,P_{3^f}$. Hence the different exponent of P in $F/F^{L'^f}$ is

$$d_P = \left(\tfrac{1}{2}\cdot 3^f(3^f-1)-1\right) + (3^f-1) + 3q_0(3^f-1).$$

Now, let $\sigma\in L'^f$.

(i) If $3 \mid |\sigma|$ then σ fixes a unique place among $P_0,\dots,P_{3^f}$;

(ii) if $|\sigma| \mid q-1$ and $|\sigma|\neq 2$ then by Theorem 2.6, σ is contained in a cyclic subgroup (of G) of order $q-1$ and from the subgroup structure of $\mathrm{PSL}(2,3^f)$ (cf. Theorem 4.11), σ is contained in a cyclic subgroup of L'^f of order $(3^f-1)/2$, and fixes exactly two places among $P_0,\dots,P_{3^f}$;

(iii) if $|\sigma|=2$ then σ is an involution of L distinct from κ and does not fix any of the places fixed by κ.

Therefore, from Theorem 2.6, if P is a place fixed by κ and $P\notin\{P_0,\dots$ $\dots,P_{3^f}\}$ then P is not ramified in $F/F^{L'^f}$. So the remaining ramified places of F in $F/F^{L'^f}$ are those fixed by involutions of $L'^f\cong\mathrm{PSL}(2,3^f)$.

When t is odd, $\mathrm{PSL}(2,3^t)$ has $3^t(3^t-1)/2$ involutions. So in our case, $f\mid 2s+1$ and L'^f has $3^f(3^f-1)/2$ involutions. Now, we are ready to apply the Riemann–Hurwitz formula to the extension $F/F^{L'^f}$:

$$2g-2=\frac{1}{2}\cdot 3^f(3^f-1)(3^f+1)(2g_{L'^f}-2)+(3^f+1)d_P+\frac{3^f(3^f-1)}{2}(q+1),$$

where $g_{L'^f}$ is the genus of L'^f and

$$d_P=\tfrac{1}{2}\cdot 3^f(3^f-1)+3^f+3q_0(3^f-1)-2.$$

The genus of L'^f is computed as

$$g_{L'^f}=\frac{3q_0(q^2-3^{2f})+q^2-3^{2f}-q+3^f+\frac{1}{2}\cdot 3^f(3^f-1)(3^f-q)}{3^f(3^f-1)(3^f+1)}.$$

Consider now the group $\langle\kappa\rangle\times L'^f$. In $F/F^{\kappa\times L'^f}$, the different exponent of each of the 3^f+1 wildly ramified places will become

$$d_P^\kappa=(3^f(3^f-1)-1)+(3^f-1)+3q_0(3^f-1)$$

(because the inertia group of such a place will be of the form $\langle\kappa\rangle\times(V'\rtimes C^-)$, which is of order $3^f(3^f-1)$). The involution κ will fix $q-3^f$ more places and these will be ramified with ramification index 2. There are $2\,\frac{3^f(3^f-1)}{2}=$ $3^f(3^f-1)$ more involutions in $\kappa\times L'^f$, each fixing $q+1$ points. Then the Riemann–Hurwitz formula gives

$$2g-2=3^f(3^f-1)(3^f+1)(2g_{\kappa L'^f}-2)+(3^f+1)d_P^\kappa+(q-3^f)+3^f(3^f-1)(q+1),$$

where $g_{\kappa L'^f}$, the genus of L'^f, is calculated as

$$g_{\kappa L'^f}=\frac{3q_0(q^2-3^{2f})+q^2-3^{2f}+2(3^f-q)+3^f(3^f-1)(3^f-q)}{2\cdot 3^f(3^f-1)(3^f+1)}.$$

In particular, when $3^f=q$, i.e. $L'^f=L'\cong\mathrm{PSL}(2,q)$, the genus, $g_{L'}$, of the field $F^{L'}$ is $g_{L'}=0$, and as $F^L\subset F^{L'}$, the genus of F^L is also zero.

Groups isomorphic to the alternating group on four letters. Let $\mathcal{A}$ be a subgroup of L' isomorphic to A_4. Then:

(i) $|\mathcal{A}|=12$;

(ii) $\mathcal{A}$ has three distinct involutions $\kappa_1,\kappa_2,\kappa_3$, with $\kappa_1\kappa_2=\kappa_3$;

(iii) $\mathcal{A}$ has four disjoint 3-Sylow subgroups, $V_i', i = 0, 1, 2, 3$, where $V_i' = \kappa_i V_0' \kappa_i$, $i = 1, 2, 3$.

If P_0 is the point fixed by V_0' (which is among the points fixed by κ), then each V_i' fixes $\kappa_i(P_0)$, for $i = 1, 2, 3$. Let us see that

$$P_0 \neq \kappa_i(P_0) \neq \kappa_j(P_0)$$

if $i \neq j$. This will prove that each of the four 3-Sylow subgroups of $\mathcal{A}$ fixes a distinct point.

Since $\kappa \notin \mathcal{A}$, we have $\kappa_i \neq \kappa$ and by Lemma 4.6, $\kappa_i(P_0) \neq P_0$, for each $i = 1, 2, 3$. Suppose that $\kappa_1(P_0) = \kappa_2(P_0) = P_1$. Then

$$\kappa_1\kappa_2(P_0) = \kappa_1(P_1) = P_0,$$

i.e. $\kappa_1\kappa_2$ fixes P_0, but by (ii) above, $\kappa_1\kappa_2 = \kappa_3$ is an involution, and again by Lemma 4.6, $\kappa_1\kappa_2$ cannot fix P_0. So $\kappa_1(P_0) \neq \kappa_2(P_0)$ and similarly

$$i \neq j \ \Rightarrow \ \kappa_i(P_0) \neq \kappa_j(P_0).$$

Therefore, for each $i = 0, \ldots, 3$, V_i fixes a different point, so it is contained in a different 3-Sylow subgroup, U_i, of L. Moreover, only four places of F are wildly ramified in $F/F^{\mathcal{A}}$. If P_i is the place fixed by V_i, then the ramification groups of P_i, in $F/F^{\mathcal{A}}$ are

$$\mathcal{A}_0(P_i) = \mathcal{A}_1(P_i) = \mathcal{A}_2(P_i) = V_i, \qquad \mathcal{A}_3(P_i) = \langle 1 \rangle,$$

and the different exponent of P_i is

$$d_{P_i} = (3-1) + (3-1) + 3q_0(3-1) = 4 + 6q_0.$$

The remaining ramified places of F in $F/F^{\mathcal{A}}$ are the $3(q+1)$ places fixed by the involutions of $\mathcal{A}$. We have

$$2g - 2 = 12(2g_{\mathcal{A}} - 2) + 4(4 + 6q_0) + 3(q+1),$$

where $g_{\mathcal{A}}$ is the genus of $F^{\mathcal{A}}$, calculated as

$$g_{\mathcal{A}} = \frac{1}{24}\,(3q_0q^2 + q^2 + 2q - 27q_0 + 3).$$

If we consider the extension $F/F^{\langle\kappa\rangle\times\mathcal{A}}$, the different exponent of P_i, $i = 0, \ldots, 3$, becomes

$$d_{P_i}^{\kappa} = (6-1) + (3-1) + 3q_0(3-1) = 7 + 6q_0.$$

The remaining $q - 3$ places fixed by κ are ramified in $F/F^{\langle\kappa\rangle\times\mathcal{A}}$, with ramification index 2. The group $\langle\kappa\rangle \times \mathcal{A}$ has six more involutions, each fixing $q+1$ points. So we have

$$2g - 2 = 24(2g_{\kappa\mathcal{A}} - 2) + 4(7 + 6q_0) + (q-3) + 6(q+1),$$

where the genus, $g_{\kappa\mathcal{A}}$, of $F^{\langle\kappa\rangle\times\mathcal{A}}$ is calculated as

$$g_{\kappa\mathcal{A}} = \frac{1}{48}\,(3q_0q^2 + q^2 - 8q - 27q_0 + 15).$$

4.2. *Normalizer of a subgroup of order* $q+3q_0+1$. Let K be a cyclic Hall subgroup of G of order $q+3q_0+1$ and $\Gamma = N_G(K)$. By Proposition 2.3(6), Γ is a Frobenius group with kernel K and a cyclic noninvariant factor of order 6. In this subsection we find the genera of all subfields of F fixed by a subgroup of Γ.

Let us first recall the definition of a Frobenius group and some properties of Frobenius groups (see for example [G-L-S 2] or [Ro]). A finite group Γ is called a *Frobenius group* if it has a subgroup $H \le \Gamma$ with $\langle 1\rangle \ne H \ne \Gamma$ such that

$$H \cap H^\sigma = \langle 1\rangle \qquad \text{for all } \sigma \in \Gamma - H$$

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

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

is a normal subgroup of Γ such that

$$\Gamma = KH, \qquad H \cap K = \langle 1\rangle.$$

K is called the *Frobenius kernel*, H is called a *Frobenius complement* (or a noninvariant factor). The Frobenius kernel K is uniquely determined by the conditions above and H is uniquely determined up to K-conjugacy.

First we find all subgroups of a Frobenius group with cyclic Frobenius kernel of order n and cyclic Frobenius complement of order 6, where $\gcd(n,6)=1$.

PROPOSITION 4.13. *Let M be a Frobenius group with cyclic Frobenius kernel N of order n and cyclic Frobenius complement of order* 6, *where* $\gcd(n,6)=1$. *If $M_1 \le M$ is a subgroup*, *then M_1 is of one of the following types*:

(i) $|M_1| \mid n$ *and* $M_1 \le N$,
(ii) $|M_1| \mid 6$ *and $M_1 \le H$ for a Frobenius complement H of M*,
(iii) $|M_1| = n_1 h_1$ *with* $1 < n_1$, $1 < h_1$, $n_1 \mid n$, $h_1 \mid 6$ *and* $M_1 = N_1 \rtimes H_1$, *where N_1 is the subgroup of N with $|N_1| = n_1$ and H_1 is the subgroup of a Frobenius complement H of M with $|H_1| = h_1$. Moreover M_1 is itself a Frobenius group with Frobenius kernel N_1 and Frobenius complement H_1.*

Proof. It is clear that for any $n_1 \mid n$, $h_1 \mid 6$ and any Frobenius complement H of M, there are cyclic subgroups N_1 of N and H_1 of H with $|N_1| = n_1$ and $|H_1| = h_1$. Conversely for any subgroup M_1 of M with $|M_1| \mid n$ or $|M_1| \mid 6$, we have $M_1 \le N$ or $M_1 \le H$ for a Frobenius complement H of M respectively, by Theorem 2.1. Therefore it remains to consider (iii).

For any subgroup $N_1 \le N$ and $h \in H$, if $g \in N_1$ then $|g| = |hgh^{-1}|$ and hence $hgh^{-1} \in N_1$. Therefore for any nontrivial subgroup $\langle 1\rangle \ne N_1 \le N$

of the Frobenius kernel N and any nontrivial subgroup $\langle 1\rangle \neq H_1 \leq H$ of a Frobenius complement H, $N_1 \rtimes H_1$ is a Frobenius subgroup of M with Frobenius kernel N_1 and Frobenius complement H_1.

Conversely first assume that M_1 is a subgroup of order $2n_1$ with $1 < n_1 \,|\, n$. Let H_1 be a 2-Sylow subgroup of M_1. Then $H_1 \leq H$ for a unique Frobenius complement H of M. If $x \in N - \langle 1\rangle$, then $H_1 \cap xH_1x^{-1} = \langle 1\rangle$. If $x \in M_1 - (N \cup H_1)$, then x is an involution and $x \notin H$, since H has a unique involution. Therefore $H_1 \cap xH_1x^{-1} = \langle 1\rangle$ for any $x \in M_1 - H_1$ and M_1 is a Frobenius group with Frobenius complement H_1. Moreover the Frobenius complement of M_1 is the unique subgroup N_1 of N with $|N_1| = n_1$.

Next assume that M_1 is a subgroup of order $3n_1$ with $1 < n_1 \,|\, n$. Let H_1 be a 3-Sylow subgroup of M_1. Similarly M_1 is a Frobenius group with Frobenius complement H_1 and the subgroup N_1 of N with $|N_1| = n_1$ as the Frobenius kernel.

Now we assume that M_1 is a subgroup of order $6n_1$ with $1 < n_1 < n$ and $n_1 \,|\, n$. Let N_1 be the subgroup of N of order n_1. Let $\{1, \alpha\}$ and $\{1, \beta, \beta^2\}$ be 2-Sylow and 3-Sylow subgroups of M_1. Let $\{1, \alpha\} \subset H$, where $H = \{1, h, \dots, h^5\}$ is the Frobenius complement containing α. Then $\alpha = h^3$ and $\beta = uh^2u^{-1}$ (or $\beta = uh^4u^{-1}$) for $u \in N$. First we consider the case $u \in N_1$. In this case we have $\alpha = h^3 \in M_1$ and $h^2 \in M_1$ (or $h^4 \in M_1$). Therefore $h \in M_1$ and hence $M_1 = N_1 \rtimes H$, which is a Frobenius group with Frobenius kernel N_1 and Frobenius complement H.

We show that the other case $u \in N - N_1$ is impossible. Let $H_1 = \langle \alpha\rangle$. Observe that $N_1 \rtimes \langle \beta\rangle$ is a subgroup of M_1. Moreover $N_1 \rtimes \langle \beta\rangle \cap \{g\alpha : g \in N_1 \rtimes \langle \beta\rangle\} = \emptyset$ and $M_1 = N_1 \rtimes \langle \beta\rangle \cup \{g\alpha : g \in N_1 \rtimes \langle \beta\rangle\}$. Since $N_1 \rtimes \langle \beta\rangle \cap H = \emptyset$, for any $\sigma \in M_1 - H_1$ we have $\sigma H_1 \sigma^{-1} = \langle 1\rangle$. Hence M_1 is a Frobenius group with Frobenius complement H_1 and Frobenius kernel $N_1 \rtimes \langle \beta\rangle$. In particular $\alpha\beta\alpha \in N_1 \rtimes \langle \beta\rangle$.

Note that for any $g \in N$, we have

$$\begin{aligned} \alpha(g\alpha)^2 &= (\alpha g\alpha)g\alpha = g(\alpha g\alpha)\alpha \quad \text{since } N \text{ is Abelian} \\ &= (g\alpha)^2\alpha. \end{aligned}$$

Then $\alpha \in (g\alpha)^{-2}H(g\alpha)^2 \cap H$. Moreover $(g\alpha)^2 \in N$ and hence $(g\alpha)^2 = 1$, since H is a Frobenius complement of M. Therefore $\alpha g = g^{-1}\alpha$.

We have $\alpha = h^3$, $\beta = uh^2u^{-1}$ (or $\beta = uh^4u^{-1}$), and $\alpha\beta\alpha \in N_1 \rtimes \langle \beta\rangle$. Then

$$\begin{aligned} \alpha\beta\alpha &= \alpha(uh^2u^{-1})\alpha & &(\text{or } = \alpha(uh^4u^{-1})\alpha) \\ &= (u^{-1}\alpha)h^2(\alpha u) & &(\text{or } = (u^{-1}\alpha)h^4(\alpha u)) \\ &= u^{-1}h^2u & &(\text{or } = u^{-1}h^4u) \\ &= u^{-2}\beta u^2. \end{aligned}$$

Moreover $\langle\alpha\beta\alpha\rangle$ is a subgroup of order 3 and all subgroups of order 3 in $N_1 \rtimes \langle\beta\rangle$ are exactly $\{\langle v^{-1}\beta v\rangle : v \in N_1\}$. Therefore there exists $v \in N_1$ such that $\{1, u^{-2}\beta u^2, u^{-2}\beta^2 u^2\} = \{1, v^{-1}\beta v, v^{-1}\beta^2 v\}$. We have either $u^{-2}\beta u^2 = v^{-1}\beta v$ or $u^{-2}\beta u^2 = v^{-1}\beta^2 v$. Then either $vu^{-2}\beta u^2 v^{-1} = \beta$ or $vu^{-2}\beta u^2 v^{-1} = \beta^2$. In both cases, $vu^{-2}\langle\beta\rangle u^2 v^{-1} = \langle\beta\rangle$. Moreover $N \rtimes \langle\beta\rangle$ is a Frobenius group with Frobenius kernel N and Frobenius complement $\langle\beta\rangle$. Since $vu^{-2} \in N$ and $vu^{-2}\langle\beta\rangle u^2 v^{-1} = \langle\beta\rangle$, we have $vu^{-2} = 1$ and so $v = u^2$. However $u \in N - N_1$ and $\langle u\rangle = \langle u^2\rangle$, since $\gcd(2, n) = 1$. Hence it is a contradiction that $v = u^2 \in N_1$. ∎

We consider the ramification structure of the extension F/F^{Γ}. The extension F/F^{Γ} is not ramified at the nonrational places of F because $(|\Gamma|, q - 3q_0 + 1) = 1$ (cf. Theorem 3.5). So we need to find the ramified places inside Ω (the set of rational places of F) and the corresponding ramification groups.

The order of Γ is $6(q+3q_0+1)$, so the order of its 3-Sylow subgroups is 3. Let H be a Frobenius complement of Γ. Then H is a cyclic group of order 6. So H contains an involution κ and an element σ of order 3. Assume σ fixes the point P_0. Since σ commutes with κ, from the discussions in Section 4.1, κ (in particular H) also fixes P_0.

We first discuss the wildly ramified places of F in F/F^{Γ}. Recall that the order of the subgroup of G fixing a point of Ω is $q^3(q-1)$. As $(|K|, q^3(q-1)) = 1$, the K-orbit of P_0, $K.P_0 = \{\alpha(P_0) \mid \alpha \in K\}$, has $|K| = q + 3q_0 + 1$ elements, say $P_0, \ldots, P_{q+3q_0}$ (we will show later that κ fixes only P_0 among these points).

THEOREM 4.14. *The wildly ramified places of F in F/F^{Γ} are $P_0, \ldots, P_{q+3q_0}$. The ramification groups of P_0 in F/F^{Γ} are*

$$\Gamma_0(P_0) = H, \qquad \Gamma_i(P_0) = \begin{cases} \langle\sigma\rangle & \text{for } 1 \le i \le 3q_0 + 1, \\ \langle 1\rangle & \text{for } i \ge 3q_0 + 2. \end{cases}$$

The different exponent of P_0 is

$$d_{P_0} = (6-1) + (3-1) + 3q_0(3-1) = 6q_0 + 7.$$

Moreover, for each $i = 1, \ldots, q + 3q_0$, the ramification groups of P_i are conjugates of those of P_0, and the different exponent of P_i is equal to d_{P_0}.

Proof. As $(|\Gamma|, q^3(q-1)) = 6$, H is the (largest) subgroup of Γ fixing P_0, and the assertions about the ramification groups and the different exponent of P_0 follow from Theorem 4.9 and Corollary 4.10.

The wildly ramified places of F will be those fixed by 3-Sylow subgroups of Γ. Any 3-Sylow subgroup of Γ has order 3 and should be a conjugate (in Γ) of $\langle\sigma\rangle$, so it should be contained in a conjugate (in Γ) of H. So the wildly ramified places of F will be those fixed by conjugates of H. As

Γ can be written as the product of its Frobenius kernel and its Frobenius complement, $\Gamma = KH$, any conjugate (in Γ) of H is $\alpha\omega H\omega^{-1}\alpha^{-1} = \alpha H\alpha^{-1}$, where $\alpha \in K$ and $\omega \in H$. In other words, the set of conjugates of H is

$$\{\alpha H\alpha^{-1} \mid \alpha \in K\}.$$

Let $\alpha_1 \neq \alpha_2$ be two elements of K. Then $\alpha_1(P_0) \neq \alpha_2(P_0)$. For $i = 1, 2$, the element of order 3 of $\alpha_i H\alpha_i^{-1}$ is $\alpha_i\sigma\alpha_i^{-1}$, and this element fixes only $\alpha_i(P_0) \in \Omega$. So the groups $\alpha_1 H\alpha_1^{-1}$ and $\alpha_2 H\alpha_2^{-1}$ are distinct. Therefore, H has $q + 3q_0 + 1$ conjugates, each of them fixing a different point among $P_0, \ldots, P_{q+3q_0+1}$. Since any conjugate, $\alpha H\alpha^{-1}$, of H, is the inertia group of $\alpha(P_0)$, the last assertion of the theorem follows. ∎

Now, the ramification index of any tamely ramified place of F in F/F^Γ is 2 (because $(|\Gamma|, q^3(q-1)) = 6$). So we need to find the fixed points of involutions in Γ.

LEMMA 4.15. *The group Γ has exactly $q+3q_0+1$ involutions, each fixing exactly one point among $P_0, \ldots, P_{q+3q_0}$ and q other points of Ω. Moreover, two distinct involutions of Γ cannot fix the same point of Ω.*

Proof. The order of a 2-Sylow subgroups of Γ is 2. Therefore any involution of Γ is a conjugate (in Γ) of κ, so it is contained in a conjugate of H. In the proof of Theorem 4.14, we have also established that H has exactly $q + 3q_0 + 1$ distinct conjugates. From the definition of Frobenius groups, the conjugates of H are disjoint. As each conjugate of H has a unique involution, Γ has exactly $q + 3q_0 + 1$ involutions and (from the proof of Theorem 4.14) each of them fixes one of $P_0, \ldots, P_{q+3q_0}$.

To finish the proof it is enough to show that distinct involutions of Γ cannot fix the same point. Let $\kappa_1 \neq \kappa_2$ be two involutions in Γ. Suppose $\kappa_1(P) = \kappa_2(P) = P$ for some point P of Ω. Then the subgroup of Γ generated by κ_1 and κ_2, $\langle\kappa_1, \kappa_2\rangle$, will also fix P. So $\langle\kappa_1, \kappa_2\rangle \leq G_P$ (and $\langle\kappa_1, \kappa_2\rangle \leq \Gamma$), which implies

$$|\langle\kappa_1, \kappa_2\rangle| \mid 6 = (q^3(q-1), 6(q + 3q_0 + 1)).$$

Obviously the order of the group $\langle\kappa_1, \kappa_2\rangle$ cannot be 2 and 3. So $|\langle\kappa_1, \kappa_2\rangle| = 6$ but this implies that $\langle\kappa_1, \kappa_2\rangle = \Gamma_0(P)$ which is a conjugate of H. No conjugate of H has two distinct involutions, and this contradiction finishes the proof. ∎

From Lemma 4.15, we easily get

THEOREM 4.16. *The number of tamely ramified places of F in the extension F/F^Γ is $q(q + 3q_0 + 1)$, and the ramification index of each of them is* 2.

Any subgroup of Γ is given in Proposition 4.13. In the subsections below we find genera of any subfield of F corresponding to subgroups Γ.

Subgroups of the form $N_1 \rtimes H$ with $|N_1| = n_1 \mid q + 3q_0 + 1$ and $|H| = 6$. $N_1 \rtimes H$ has n_1 disjoint Frobenius complements each fixing a place among the wildly ramified places of F in F/F^{Γ}. The ramification groups of these places in $F/F^{N_1 \rtimes H}$ are the same as their ramification groups in F/F^{Γ}, say $P_0, \dots, P_{n_1-1}$. For any $P \in \{P_0, \dots, P_{n_1-1}\}$, the corresponding Frobenius complement of $N_1 \rtimes H$ fixing P has the unique involution which fixes q other places of Ω. Moreover two distinct involutions of $N_1 \rtimes H$ cannot fix the same place. Therefore the Riemann–Hurwitz formula applied to $F/F^{N_1 \rtimes H}$ gives

$$2g - 2 = 6n_1(2g_{N_1 \rtimes H} - 2) + n_1(6q_0 + 7) + n_1 q,$$

where $g_{N_1 \rtimes H}$ is the genus of $F^{N_1 \rtimes H}$, computed as

$$g_{N_1 \rtimes H} = \frac{3q_0(q-1)(q+q_0+1) - n_1(q+6q_0-5) - 2}{12n_1}.$$

In particular for $N_1 = K$ we have $N_1 \rtimes H = \Gamma$ and $g_{\Gamma} = (q-1)(q_0-1)/4$.

Subgroups of the form $N_1 \rtimes \langle\beta\rangle$ with $|N_1| = n_1 \mid q + 3q_0 + 1$ and $|\beta| = 3$. $N_1 \rtimes \langle\beta\rangle$ has n_1 disjoint Frobenius complements each fixing a unique place $P_0, \dots, P_{n_1-1}$. Let P be one of these places. The ramification groups of P in $F/F^{N_1 \rtimes \langle\beta\rangle}$ are

$$(N_1 \rtimes \langle\beta\rangle)_i(P) = \begin{cases} \langle\beta\rangle & \text{for } 0 \le i \le 3q_0 + 1, \\ \langle 1\rangle & \text{for } i \ge 3q_0 + 2. \end{cases}$$

Therefore its different exponent is

$$d_P = (3-1) + (3-1) + 3q_0(3-1) = 6q_0 + 4.$$

$N_1 \rtimes \langle\beta\rangle$ has no involutions and applying the Riemann–Hurwitz formula to $F/F^{N_1 \rtimes \langle\beta\rangle}$ we get

$$2g - 2 = 3n_1(2g_{N_1 \rtimes \langle\beta\rangle} - 2) + n_1(6q_0 + 4),$$

where $g_{N_1 \rtimes \langle\beta\rangle}$ is the genus of $F^{N_1 \rtimes \langle\beta\rangle}$, computed as

$$g_{N_1 \rtimes \langle\beta\rangle} = \frac{3q_0(q-1)(q+q_0+1) - n_1(6q_0-2) - 2}{6n_1}.$$

In particular for $N_1 = K$ we have $g_{K \rtimes \langle\beta\rangle} = (q-1)q_0/2 - q/3$.

Subgroups of the form $N_1 \rtimes \langle\alpha\rangle$ with $|N_1| = n_1 \mid q + 3q_0 + 1$ and $|\alpha| = 2$. Observe that $\gcd(|N_1 \rtimes \langle\alpha\rangle|, 3) = 1$ and hence there is no wild ramification in $F/F^{N_1 \rtimes \langle\alpha\rangle}$. Since $N_1 \rtimes \langle\alpha\rangle$ has n_1 disjoint Frobenius complements each having a unique involution, the Riemann–Hurwitz formula gives

$$2g - 2 = 2n_1(2g_{N_1 \rtimes \langle\alpha\rangle} - 2) + n_1(q + 1),$$

where $g_{N_1 \rtimes \langle\alpha\rangle}$ is the genus of $F^{N_1 \rtimes \langle\alpha\rangle}$, computed as

$$g_{N_1 \rtimes \langle\alpha\rangle} = \frac{3q_0(q-1)(q+q_0+1) - n_1(q-3) - 3}{4n_1}.$$

In particular for $N_1 = K$ we have $g_{K \rtimes \langle\alpha\rangle} = (3(q+1)q_0 + 1 - 3q)/4$.

Subgroups of the form N_1 *with* $|N_1| = n_1 \mid q + 3q_0 + 1$. Observe that $\gcd(|N_1|, 6) = 1$ and hence the extension F/F^{N_1} is unramified. Therefore the Riemann–Hurwitz formula gives

$$2g - 2 = n_1(2g_{N_1} - 2),$$

where g_{N_1} is the genus of F^{N_1}, computed as

$$g_{N_1} = \frac{3q_0(q-1)(q+q_0+1) + 2n_1 - 2}{2n_1}.$$

In particular for $N_1 = K$ we have $g_K = (3(q+1)q_0 - 2q)/2$.

4.3. *Normalizer of a subgroup of order* $q - 3q_0 + 1$. Let K be a cyclic Hall subgroup of G of order $q - 3q_0 + 1$ and $\Gamma = N_G(K)$. By Proposition 2.3(6), Γ is a Frobenius group with kernel K and a cyclic noninvariant factor of order 6. The properties of the group and its action on Ω (the set of rational places of F) are very similar to those of the normalizer of a Hall subgroup of order $q + 3q_0 + 1$, which we discussed in Section 4.2. So by just imitating the proofs of Theorems 4.14 and 4.16, we get the ramified rational places of F in F/F^{Γ}.

THEOREM 4.17. *F has $q - 3q_0 + 1$ wildly ramified places in F/F^{Γ}. The ramification groups of each wildly ramified place P are*

$$\Gamma_0(P) = H, \qquad \Gamma_i(P) = \begin{cases} \langle\sigma\rangle & \text{for } 1 \le i \le 3q_0 + 1, \\ \langle 1\rangle & \text{for } i \ge 3q_0 + 2, \end{cases}$$

where H is a Frobenius complement of Γ, which is cyclic of order 6, and σ is the element of order 3 of H. The different exponent of P in F/F^{Γ} is

$$d_P = (6-1) + (3-1) + 3q_0(3-1) = 6q_0 + 7.$$

F has $q(q - 3q_0 + 1)$ tamely ramified rational places, each with ramification 2.

Proposition 4.13 gives all subgroups of Γ for this subsection as well. In the following subsections, we find genera of any subfield corresponding to subgroups of Γ.

Subgroups of the form $N_1 \rtimes H$ *with* $|N_1| = n_1 \mid q - 3q_0 + 1$ *and* $|H| = 6$. Note that $N_1 \le K$ and K is a cyclic Hall subgroup of order $q - 3q_0 + 1$. By Theorem 3.5, there exists a degree 6 place Q of F such that K fixes Q. The ramification index of Q in F/F^G is $q - 3q_0 + 1$ and hence by Theorem 4.1, the ramification index of Q in $F/F^{N_1 \rtimes H}$ is n_1. Moreover $N_1 \rtimes H$ has n_1 disjoint Frobenius complements. Each of these gives a unique wildly ramified place P and its different exponent is $d_P = 6q_0 + 7$. Also the involution of each Frobenius complement fixes q other places of Ω. Therefore applying the Riemann–Hurwitz formula to $F/F^{N_1 \rtimes H}$ we get

$$2g - 2 = 6n_1(2g_{N_1 \rtimes H} - 2) + n_1(6q_0 + 7) + n_1 q + 6(n_1 - 1),$$

where $g_{N_1 \rtimes H}$ is the genus of $F^{N_1 \rtimes H}$, computed as

$$g_{N_1 \rtimes H} = \frac{3q_0(q-1)(q+q_0+1) - n_1(q+6q_0+1)+4}{12n_1}.$$

In particular for $N_1 = K$ we have $N_1 \rtimes H = \varGamma$ and $g_\varGamma = (q+1)(q_0+1)/4$.

Subgroups of the form $N_1 \rtimes \langle\beta\rangle$ with $|N_1| = n_1 \mid q-3q_0+1$ and $|\beta| = 3$. As in the previous subsection, there is only one nonrational place Q of F which ramifies in $F/F^{N_1 \rtimes \langle\beta\rangle}$. It is a degree 6 place and its ramification index is n_1. Moreover $N_1 \rtimes \langle\beta\rangle$ has n_1 disjoint Frobenius complements each fixing a unique (rational) place. Let P be one of these places. Then P is wildly ramified with different exponent $d_P = 6q_0+4$. Since $N_1 \rtimes \langle\beta\rangle$ has no involutions, the Riemann–Hurwitz formula gives

$$2g-2 = 3n_1(2g_{N_1 \rtimes \langle\beta\rangle} - 2) + n_1(6q_0+4) + 6(n_1-1),$$

where $g_{N_1 \rtimes \langle\beta\rangle}$ is the genus of $F^{N_1 \rtimes \langle\beta\rangle}$, computed as

$$g_{N_1 \rtimes \langle\beta\rangle} = \frac{3q_0(q-1)(q+q_0+1) - n_1(6q_0+4)+4}{6n_1}.$$

In particular for $N_1 = K$ we have $g_{K \rtimes \langle\beta\rangle} = (q+1)q_0/2 + 2q/3$.

Subgroups of the form $N_1 \rtimes \langle\alpha\rangle$ with $|N_1| = n_1 \mid q-3q_0+1$ and $|\alpha| = 2$. There is only one nonrational place Q of F, of degree 6, ramifying in $F/F^{N_1 \rtimes \langle\alpha\rangle}$ with ramification index n_1. Since $\gcd(|N_1 \rtimes \langle\alpha\rangle|, 3) = 1$, there is no wild ramification. As $N_1 \rtimes \langle\alpha\rangle$ has n_1 distinct involutions, the Riemann–Hurwitz formula gives

$$2g-2 = 2n_1(2g_{N_1 \rtimes \langle\alpha\rangle} - 2) + n_1(q+1) + 6(n_1-1),$$

where $g_{N_1 \rtimes \langle\alpha\rangle}$ is the genus of $F^{N_1 \rtimes \langle\alpha\rangle}$, computed as

$$g_{N_1 \rtimes \langle\alpha\rangle} = \frac{3q_0(q-1)(q+q_0+1) - n_1(q-3)+4}{4n_1}.$$

In particular for $N_1 = K$ we have $g_{K \rtimes \langle\alpha\rangle} = (3q+1)(q_0+1)/4 + 2q_0$.

Subgroups of the form N_1 with $|N_1| = n_1 \mid q-3q_0+1$. F/F^{N_1} is ramified at the degree 6 place Q with the ramification index n_1. Since $\gcd(|N_1|, 6) = 1$, there is no other ramification. Therefore the Riemann–Hurwitz formula gives

$$2g-2 = n_1(2g_{N_1} - 2) + 6(n_1-1),$$

where g_{N_1} is the genus of F^{N_1}, computed as

$$g_{N_1} = \frac{3q_0(q-1)(q+q_0+1) - 4n_1+4}{2n_1}.$$

In particular for $N_1 = K$ we have $g_K = 3q_0(q+3)/2 + 2q$.

4.4. *Normalizer of a subgroup of order* $(q+1)/4$. Let A be a cyclic Hall subgroup of order $(q+1)/4$ and $J = N_G(A)$ be its normalizer in G. By Proposition 2.3(4) and [G-L-S 3, pp. 332–333], the order of J is $6(q+1)$ and we have:

PROPOSITION 4.18. *There is an elementary abelian subgroup $E \le G$ of order 4 and a dihedral subgroup $D \le G$ of order $(q+1)/2$ where $A \le D$, and the elements of E commute with the elements of D, such that $N_G(A)$ is the extension of $E \times D$ by an element of order 3 normalizing both factors and acting without fixed points on E and A.*

We will assume that the groups E and D in the above proposition are subgroups of J and so $E \times D \lhd J$. We will denote $E \times D$ by K. In fact K is the only subgroup of J with order $2(q+1)$. Indeed, we have

LEMMA 4.19. *Let $H \le J$ and write the order of H as $|H| = 2^i a 3^j$, where $a \mid (q+1)/4$. Then H has a subgroup of order $2^i a$ contained in K. In particular if $\gcd(|H|, 3) = 1$ then $H \le K$.*

Proof. First we note that the involutions of J are elements of K. This follows from the fact that K is a normal subgroup of J with index 3. Similarly any element of order dividing $(q+1)/4$ is contained in A. Write the prime decomposition of a as $a = p_1^{m_1} \cdots p_t^{m_t}$. Then for each $i = 1, \ldots, t$, the p_i-Sylow subgroup S_{p_i} of H is contained in some Hall subgroup of G of order $(q+1)/4$. So S_{p_i} is cyclic and contained in A. Therefore H has a subgroup A_H of order a which is contained in K. Also, any 2-Sylow subgroup S_2 of H is contained in K. Now the subgroup generated by A_H and S_2 is the desired subgroup of order $2^i a$. ∎

Here we note that, being the center of K, the first component E of $E \times D$ is also uniquely determined. For the second component, although K contains four distinct dihedral subgroups of order $(q+1)/2$, only one of them is normalized by elements of order 3, which will be discussed below.

From the Sylow theorems, it follows that J has $q+1$ 3-Sylow subgroups and the order of the normalizer of each of them is 6. By Proposition 2.3(4), 3-Sylow subgroups are cyclic of order 6. Notice that any 3-Sylow subgroup V normalizes K, so that $J = K \rtimes V$. In particular, V acts on K by conjugation and since V is a cyclic group generated by some $\sigma \in J$, $|\sigma| = 3$, the fixed points of this action are the elements of K commuting with σ. We have

LEMMA 4.20. *Let $\sigma \in J$ be an element with $|\sigma| = 3$. Then σ commutes with a unique involution $\kappa \in K \setminus E$. Let D be the dihedral subgroup of K generated by κ and A. Then σ normalizes both E and D and acts without fixed points on E and A.*

Proof. The subgroup E is the center of K, and A is the only cyclic subgroup of K of order $(q+1)/4$. So any automorphism of K (in particular conjugation by σ) should map E and A to themselves. Hence $\sigma E\sigma^{-1} = E$ and $\sigma A\sigma^{-1} = A$. Now, for any involution $\kappa \in K \setminus E$, $\sigma\kappa\sigma^{-1}$ is again an involution in $K \setminus E$. The number of involutions in $K \setminus E$ is $q+1$. Since $3 \nmid q+1$, σ should commute with an involution in $K \setminus E$. As $|N_J(\sigma)| = 6$, there is no other element of K commuting with σ, which finishes the proof. ∎

Let $\kappa_0 = 1, \kappa_1, \kappa_2, \kappa_3$ denote the distinct elements of E. From the above lemma, it follows that the distinct conjugates of a 3-Sylow subgroup V of J are

$$\kappa_i\alpha V\alpha^{-1}\kappa_i, \quad i = 0, \ldots, 3, \ \alpha \in A.$$

Let κ be the involution of $K \setminus E$ commuting with the generator σ of V, and D be the dihedral subgroup generated by κ and A. Then, for any $\alpha \in A$, the involution $\alpha^2\kappa \in D$ commutes with $\alpha\sigma\alpha^{-1}$, $\kappa_1\alpha\sigma\alpha^{-1}\kappa_1$, $\kappa_2\alpha\sigma\alpha^{-1}\kappa_2$, $\kappa_3\alpha\sigma\alpha^{-1}\kappa_3$. Since $\gcd((q+1)/4, 2) = 1$, any involution of D can be written as $\alpha^2\kappa$ for some $\alpha \in A$. As D has $(q+1)/4$ involutions and J has $q+1$ 3-Sylow subgroups, we get:

LEMMA 4.21. *The group K has a unique dihedral subgroup D of order $(q+1)/2$ normalized by elements of order 3 in J, and each involution of D is contained in the normalizer of exactly four 3-Sylow subgroups of J which are conjugate under the elements of E.*

From now on D will denote the dihedral subgroup of K, of order $(q+1)/2$, normalized by elements of order 3 in J.

We want to determine the structure of all subgroups of J. If $H \le J$ with $3 \nmid |H|$, then Lemma 4.19 implies $H \le K$ and the subgroups of K can be easily listed. So we need to deal with subgroups H of J with $3 \mid |H|$.

LEMMA 4.22. *Let $H \le J$ with $3 \mid |H|$. Let E_H be the subgroup $H \cap E$ of H. Then E_H is either trivial or equal to E.*

Proof. Let $\sigma \in H$ be an element of order 3. Then by Lemma 4.20, σ acts on E by conjugation and this action does not fix any nontrivial subgroup of E, which proves the lemma. ∎

LEMMA 4.23. *Let $H \le J$ with $3 \mid |H|$. Let $\sigma \in H$ be an element of order 3, $E_H = H \cap E$ and $D_H = H \cap D$. Then*

$$H = (E_H \times D_H) \rtimes \langle\sigma\rangle,$$

in particular $H \cap K = E_H \times D_H$. Moreover:

(i) *If $2 \nmid |D_H|$ then H has $|E_H|\,|D_H|$ 3-Sylow subgroups and the normalizer (in H) of each of them is equal to that subgroup.*
(ii) *If $2 \mid |D_H|$ then H has $\frac{1}{2}|E_H|\,|D_H|$ 3-Sylow subgroups and the order of the normalizer (in H) of each of them is 6. In this case, each*

involution of D_H is contained in the normalizer of exactly $|E_H|$ 3-Sylow subgroups of H.

Proof. To show the first assertion, we need only show that $H \cap K = E_H \times D_H$. Let $B = H \cap K$ and $A_H = H \cap A$. First note that B is either $E_H \times A_H$ or $E_H \times D_1$ where D_1 is a dihedral subgroup generated by A_H and an involution in $K \setminus E$. Now, as $A_H \le D_H$ and $E_H \times D_H \le B$, we need only show that, in the case $B = E_H \times D_1$ with $2 \,|\, |D_1|$, D_H also contains an involution. This is equivalent to showing that B contains an involution κ commuting with σ (then κ should also be in D_H). So assume $B = E_H \times D_1$ with $2 \,|\, |D_1|$. By Lemma 4.22, $E_H = \langle 1 \rangle$ or E. In both cases, since $B \lhd H$, the same counting argument as in the proof of Lemma 4.20 shows that σ commutes with an involution in B. This also shows that if $2 \mid |D_H|$ then $|N_H(\langle \sigma \rangle)| = 6$.

Now by Lemma 4.19 the order of H is $3|E_H|\,|D_H|$. Let V be a 3-Sylow subgroup of H, and n_3 be the number of its conjugates in H. In the case $2 \nmid |D_H|$, Lemma 4.20 implies that $N_H(V) = V$, and (i) follows from the Sylow theorems. When $2 \mid |D_H|$, we have $|N_H(V)| = |N_H(\langle \sigma \rangle)| = 6$ and $n_3 = \frac{1}{2}|E_H|\,|D_H|$. The last assertion follows from Lemma 4.21. ∎

The following theorem gives a complete list of subgroups of J.

THEOREM 4.24. *The group $J = N_G(A)$ has only the following subgroups*:

(i) *subgroups of $E \times D$*,
(ii) *for each subgroup D_1 of D, extensions of $E \times D_1$ by an element of order* 3,
(iii) *for each subgroup D_1 of D, extensions of D_1 by an element of order* 3.

Proof. By Lemmas 4.19 and 4.23, any subgroup of J is one of those listed in (i)–(iii). So we need only show the existence of subgroups listed in (ii) and (iii). Let $D_1 \le D$. In the case $2 \,|\, |D_1|$ let $\sigma \in J$ be an element of order 3 commuting with an involution in D_1 (such a σ exists by Lemma 4.21), otherwise let $\sigma \in J$ be any element of order 3. By Lemma 4.20, σ normalizes both E and A, but since A is cyclic, it also normalizes any subgroup of A. Thus the following are subgroups of J:

$$D_1 \rtimes \langle \sigma \rangle, \qquad (E \times D_1) \rtimes \langle \sigma \rangle. \ ∎$$

Now we determine the ramification structure of F/F^J. The extension F/F^J is not ramified at the nonrational places of F because $\gcd(|J|, q - 3q_0 + 1) = 1$. So we need to find the ramified places inside Ω (the set of rational places of F) and the corresponding ramification groups.

For the wild ramifications of F/F^J, we have:

PROPOSITION 4.25. *The number of wildly ramified places of F in F/F^J is $q+1$. If P is one of them, then the ramification groups of P, in F/F^J are*

$$J_0(P) = N_J(V), \qquad J_i(P) = \begin{cases} V & \text{for } 1 \le i \le 3q_0+1, \\ \langle 1 \rangle & \text{for } i \ge 3q_0+2, \end{cases}$$

where V is a 3-Sylow subgroup of J. The different exponent of P is

$$d_P = (6-1) + (3-1) + 3q_0(3-1) = 6q_0 + 7.$$

Proof. The number of wildly ramified places of F in F/F^J is equal to the number of 3-Sylow subgroups of J, which is $q+1$. For V a 3-Sylow subgroup, since $|N_J(V)|$ is contained in the centralizer of some involution, the other assertions follow from Theorem 4.9 and its corollary. ∎

The ramification index of any tamely ramified place of F in F/F^J is 2 (because $\gcd(|J|, q^3(q-1)) = 6$). So we need to find the places fixed by involutions in J. Now, any involution of J is an element of $E \times D$ (by Lemma 4.19) which is contained in the centralizer of some involution. So Lemma 4.6 of Section 4.1 implies that two distinct involutions of J cannot fix the same place. Since any involution of G fixes $q+1$ places, counting the involutions in J and using Lemma 4.21, we get:

PROPOSITION 4.26. *The tamely ramified places of F in F/F^J are*:

- (i) *the $\frac{q+1}{4}(q-3)$ places fixed by $(q+1)/4$ involutions of D, which are also in the normalizer $N_J(V)$ of a 3-Sylow subgroup V of J,*
- (ii) *the $(3(q+1)/4+3)(q+1)$ places fixed by the remaining $3(q+1)/4+3$ involutions of $E \times D$.*

We want to find the genera of all subfields of F fixed by subgroups of J. The subgroups of $E \times D$ are contained in the centralizer of an involution in E, and were already studied in Section 4.1. So, in this section we shall consider only the subgroups of J listed in (ii) and (iii) of Theorem 4.24. We distinguish here four types of subgroups which will be discussed in the following subsections.

Subgroups of the form A_1, where $A_1 \le A$ is cyclic of order $a_1 \mid (q+1)/4$. Since $\gcd(a_1, q^2(q-1)) = 1$, F/F^{A_1} is unramified and hence by the Riemann–Hurwitz formula we have

$$2g - 2 = a_1(2g_{A_1} - 2),$$

where g_{A_1} is the genus of F^{A_1}, computed as

$$g_{A_1} = \frac{3q_0(q-1)(q+q_0+1) - 2}{2a_1} + 1.$$

In particular for $A_1 = A$ we have $g_A = 6(q-1)q_0 + 2q - 3$.

Subgroups of the form D_1, where $D_1 \le D$ is dihedral of order $2a_1$ with $a_1 \mid (q+1)/4$. Since $\gcd(3, 2a_1) = 1$, there is no wild ramification in F/F^{D_1}. The number of involutions in D_1 is a_1 and hence the Riemann–Hurwitz formula gives

$$2g - 2 = 2a_1(2g_{D_1} - 2) + a_1(q+1),$$

where g_{D_1} is the genus of F^{D_1}, computed as

$$g_{D_1} = \frac{3q_0(q-1)(q+q_0+1) - 2}{4a_1} + 1 - \frac{q+1}{4}.$$

In particular for $D_1 = D$ we have $g_D = 3q_0(q-1) + q - 1 - (q+1)/4$.

Subgroups of the form $E \times A_1$, where $A_1 \le A$ is cyclic of order a_1 dividing $(q+1)/4$. Since $\gcd(4a_1, 3) = 1$, there is no wild ramification in $F/F^{E\times A_1}$. Since $E \times A_1$ has three involutions the Riemann–Hurwitz formula gives

$$2g - 2 = 4a_1(2g_{E\times A_1} - 2) + 3(q+1),$$

where $g_{E\times A_1}$ is the genus of $F^{E\times A_1}$, computed as

$$g_{E\times A_1} = \frac{3q_0(q-1)(q+q_0+1) - 2 - 3(q+1)}{8a_1} + 1.$$

In particular for $A_1 = A$ we have $g_{E\times A} = 3q_0(q-1)/2 - (q-1)/2$.

Subgroups of the form $E \times D_1$, where $D_1 \le D$ is dihedral of order $2a_1$ with $a_1 \mid (q+1)/4$. Since $\gcd(8a_1, 3) = 1$, the extension $F/F^{E\times D_1}$ is unramified. $E \times D_1$ has $4a_1 + 3$ involutions and hence Riemann–Hurwitz formula gives

$$2g - 2 = 8a_1(2g_{E\times D_1} - 2) + (4a_1+3)(q+1),$$

where $g_{E\times D_1}$ is the genus of $F^{E\times D_1}$, computed as

$$g_{E\times D_1} = \frac{3q_0(q-1)(q+q_0+1) - 2 + (4a_1+3)(q+1)}{16a_1} + 1.$$

In particular for $D_1 = D$ we have $g_{E\times D} = (3q_0(q-1)+2)/4 + 2$.

Subgroups of the form $A_1 \rtimes \langle\sigma\rangle$, where $A_1 \le A$ is cyclic of order a_1 dividing $(q+1)/4$ and $\sigma \in J$, $|\sigma| = 3$. By Lemma 4.23, $A_1 \rtimes \langle\sigma\rangle$ has $a_1 = |A_1|$ 3-Sylow subgroups and since $\gcd(|A_1 \rtimes \langle\sigma\rangle|, 2) = 1$, it does not contain any involution. So F has a_1 ramified places (each with index 3) in $F/F^{A_1\rtimes\langle\sigma\rangle}$ and the different exponent of each of them equals $6q_0+4$. The Riemann–Hurwitz formula states

$$2g - 2 = 3a_1(2g_{A_1\rtimes\sigma} - 2) + a_1(6q_0+4),$$

where $g_{A_1\rtimes\sigma}$ is the genus of $F^{A_1\rtimes\langle\sigma\rangle}$, computed as

$$g_{A_1 \rtimes \langle\sigma\rangle} = \frac{3q_0(q-1)(q+q_0+1) - 2 - 4a_1}{6a_1} + 1.$$

In particular for $A_1 = A$ we have $g_{A_1 \rtimes \langle\sigma\rangle} = 2q_0(q-1) - q_0 - 1$.

Subgroups of the form $D_1 \rtimes \langle\sigma\rangle$, where $D_1 \leq D$ is dihedral of order $2a_1$ with $a_1 \mid (q+1)/4$ and $\sigma \in J$, $|\sigma| = 3$. By Lemma 4.23, $D_1 \rtimes \langle\sigma\rangle$ has a_1 3-Sylow subgroups, the order of the normalizer of each of them is 6 and each involution of D_1 is contained in the normalizer of only one 3-Sylow subgroup of $D_1 \rtimes \langle\sigma\rangle$. The last implies that each involution of D_1 fixes one place which is wildly ramified and q other places which are tamely ramified in F/F^J. So F has a_1 wildly ramified places, with different exponent $6q_0+7$ each, and $a_1 q$ tamely ramified places of index 2, in F/F^J. Applying the Riemann–Hurwitz formula we get

$$2g - 2 = 6a_1(2g_{D_1 \rtimes \sigma} - 2) + a_1(6q_0+7) + a_1 q,$$

where $g_{D_1 \rtimes \sigma}$ is the genus of $F^{D_1 \rtimes \langle\sigma\rangle}$, computed as

$$g_{D_1 \rtimes \langle\sigma\rangle} = \frac{3q_0(q-1)(q+q_0+1) - 2 - a_1(6q_0+q+7)}{12a_1} + 1.$$

In particular for $D_1 = D$ we have $g_{D \rtimes \langle\sigma\rangle} = q_0(q-1) - (q - 2q_0 - 1)/4$.

Subgroups of the form $(E \times A_1) \rtimes \langle\sigma\rangle$, where $A_1 \leq A$ is cyclic of order $a_1 \mid (q+1)/4$ and $\sigma \in J$, $|\sigma| = 3$. This subgroup has $4a_1$ 3-Sylow subgroups and three involutions, which implies that F has $4a_1$ wildly ramified places with different exponent $6q_0+4$ and $3(q+1)$ tamely ramified places with index 2. So the Riemann–Hurwitz formula states

$$2g - 2 = (12a_1)(2g_{(E \times A_1) \rtimes \langle\sigma\rangle} - 2) + 4a_1(6q_0+4) + 3(q+1),$$

where $g_{(E \times A_1) \rtimes \langle\sigma\rangle}$ is the genus of $F^{(E \times A_1) \rtimes \langle\sigma\rangle}$, computed as

$$g_{(E \times A_1) \rtimes \langle\sigma\rangle} = \frac{3q_0(q-1)(q+q_0+1) - 2 - 4a_1(6q_0+4) - 3(q+1)}{24a_1} + 1.$$

In particular for $A_1 = A$ we have $g_{(E \times A) \rtimes \langle\sigma\rangle} = (3q_0(q-1) + q - 3)/6 - q_0$.

Subgroups of the form $(E \times D_1) \rtimes \langle\sigma\rangle$, where $D_1 \leq D$ is dihedral of order $2a_1$ with $a_1 \mid (q+1)/4$ and $\sigma \in J$, $|\sigma| = 3$. This subgroup has $4a_1$ 3-Sylow subgroups and hence F has $4a_1$ wildly ramified places. Moreover the different exponent of these places is $6q_0+7$. There are a_1 involutions in D_1 which are also in the normalizer of a 3-Sylow subgroup of J and each of them fixes $q-3$ more places. Also $(E \times D_1) \rtimes \langle\sigma\rangle$ has $3a_1+3$ further involutions which are not in the normalizer of any 3-Sylow subgroup of J. Therefore the Riemann–Hurwitz formula gives

$$\begin{aligned} 2g - 2 = {} & 24a_1(2g_{(E \times D_1) \rtimes \langle\sigma\rangle} - 2) + 4a_1(6q_0+7) + a_1(q-3) \\ & + (3a_1+3)(q+1), \end{aligned}$$

where $g_{(E\times D_1)\rtimes\langle\sigma\rangle}$ is the genus of $F^{(E\times D_1)\rtimes\langle\sigma\rangle}$, computed as

$$g_{(E\times D_1)\rtimes\langle\sigma\rangle} = \frac{3q_0(q-1)(q+q_0+1)-2-4a_1(q+6q_0+7)-3(q+1)}{48a_1}+1.$$

In particular for $D_1 = D$ this subgroups becomes J and we have $g_J = q_0(q-3)/4$.

4.5. *Ree subgroups.* Let $M \le G$ be a Ree subgroup of the form $\mathrm{Ree}(m)$ with $q = m^n$, where n is an odd integer (not necessarily prime) with $n \ge 3$ and $m \ge 27$. In this subsection we find the genus of the subfield of F fixed by M.

REMARK 4.27. Recall that maximal Ree subgroups of G are of the form $\mathrm{Ree}(m)$ with $q = m^n$ and n is a prime. Therefore by Theorem 2.4, the only subgroup of G which would not be considered in the previous subsections or in this subsection is either a subgroup of the normalizer of a 3-Sylow subgroup of G or a subgroup of a Ree subgroup of G of the form $\mathrm{Ree}(3)$.

Let m_0 be defined by $m = 3m_0^2$ and V be a 3-Sylow subgroup of M. Let U be the 3-Sylow subgroup of G containing V. Let $g \in N(U)\cap M$ and $v \in V$. Then $gvg^{-1} \in U\cap M = V$ and hence $N(U)\cap M \le N_M(V)$, where $N_M(V)$ is the normalizer of V in M. By Proposition 2.3(10), for the normalizer $N(V)$ of V in G, we have $N(V) \le N(U)$. Therefore $N_M(V) = N(V)\cap M \le N(U)\cap M$ and hence $N_M(V) = N(U)\cap M$. This implies that for any $g_1, g_2 \in M$,

$$g_1N_M(V) = g_2N_M(V) \ \Leftrightarrow\ g_1N(U) = g_2N(U). \tag{4.5}$$

By the results in Section 2, M has the usual 2-transitive representation of m^3+1 left cosets of $N_M(V)$ in M. Similarly G has the usual 2-transitive representation of q^3+1 left cosets of $N(U)$ in G. By Corollary 2.10, G has the usual 2-transitive representation on the set Ω of rational places of F. In particular any P corresponds to a unique left coset $gN(U)$ in G. Let $\Omega_m \subset \Omega$ be the subset of Ω consisting of the rational places of F corresponding to the left cosets $gN(U)$ with $g \in M \le G$. By (4.5), $|\Omega_m| = m^3+1$ and by Corollary 2.10, M has the usual 2-transitive representation on Ω_m.

THEOREM 4.28. *Let σ be a nonidentity element of M. Then σ fixes a rational place of $P \in \Omega$ if and only if one of the following holds*:

(i) $3 \mid |\sigma|$ *and* $\sigma \in N_M(V)$. *In this case P corresponds to the* 3*-Sylow subgroup U of G containing V and $P \in \Omega_m$.*
(ii) $|\sigma| \mid m-1$ *and* $|\sigma| \ne 2$. *In this case σ fixes exactly two distinct rational places P and P' with $P, P' \in \Omega_m$.*
(iii) $|\sigma| = 2$. *In this case σ fixes exactly $m-1$ distinct rational places from Ω_m and $q-m$ rational places from $\Omega - \Omega_m$.*

Proof. By Theorem 4.2, as $\sigma \in G$, σ fixes a rational place $P \in \Omega$ if and only if either $3 \,|\, |\sigma|$ or $|\sigma| \,|\, m-1$. If $3 \,|\, |\sigma|$, then $\sigma \in N_M(V)$ for some

3-Sylow subgroup V of M and σ fixes exactly one rational place $P \in \Omega_m$ by Theorem 4.2. Similarly if $|\sigma| \mid m-1$ and $|\sigma| \neq 2$, then σ fixes exactly two distinct rational places of Ω_m. If $|\sigma| = 2$, then σ fixes exactly $m-1$ rational places from Ω_m by the usual 2-transitive representation of M on Ω_m, and $q-1$ rational places from Ω by the usual 2-transitive representation of G on Ω. ∎

In computations, we need the following lemmata.

LEMMA 4.29. *The number of involutions of* Ree(m) *is*

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

Proof. Let κ be an involution of M. Then κ fixes exactly $m+1$ rational places $P_0, \dots, P_m$ from Ω_m. Moreover for any two distinct rational places $P, P' \in \Omega_m$, there exists a unique involution of the subgroup $M_{PP'}$ of M fixing P and P'. Since each involution is counted exactly $\binom{m+1}{2}$ times as the involution of any two distinct rational places of its fixed rational places, we get the formula. ∎

LEMMA 4.30. *No two distinct involutions of M can fix the same rational place Q from $\Omega - \Omega_m$.*

Proof. Assume that $\kappa_1 \neq \kappa_2$ are two involutions of M fixing $Q \in \Omega - \Omega_m$. By Lemma 4.6, $\kappa_1\kappa_2 \neq \kappa_2\kappa_1$. Multiplying both sides by $\kappa_1\kappa_2$ we get

$$(\kappa_1\kappa_2)(\kappa_1\kappa_2) \neq (\kappa_1\kappa_2)(\kappa_2\kappa_1) = 1.$$

Then $\kappa_1\kappa_2$ is neither the identity nor an involution and it fixes a rational place $Q \in \Omega - \Omega_m$. This is a contradiction to Theorem 4.28. ∎

Let $P \in \Omega_m$. We compute the ramification groups for P in F/F^M. The inertia group $M_0(P)$ for P in F/F^M is the subgroup of M fixing P. By Proposition 2.5 and Proposition 2.3(8), $M_0(P) = VT_{m-1}$, where V is the 3-Sylow subgroup of M fixing P, and T_{m-1} is the cyclic subgroup of order $m-1$ of M fixing P and any other rational place from Ω_m. Let U be the 3-Sylow subgroup of G containing V. Let U_1 be the derived group of U, and $Z(U)$ be the center of U in G. By Theorems 3.1 and 4.1, for the higher ramification groups of P in the extension F/F^M we have:

(i) $M_1(P) = M \cap U = V$,
(ii) $M_i(P) = V \cap U_1$ for $2 \leq i \leq 3q_0 + 1$,
(iii) $M_i(P) = V \cap Z(U)$ for $3q_0 + 2 \leq i \leq q + 3q_0 + 1$,
(iv) $M_i(P) = \langle 1 \rangle$ for $i \geq q + 3q_0 + 2$.

LEMMA 4.31. *Under the above notations, we have $V \cap U_1 = V_1$, where V_1 is the derived group of V.*

Proof. Recall that

$$U_1 = \langle x^{-1}y^{-1}xy : x, y \in U\rangle, \quad V_1 = \langle x^{-1}y^{-1}xy : x, y \in V\rangle.$$

As $V \le U$, by definition of derived subgroups we have $V_1 \le U_1$ and $V_1 \le V$. It remains to prove that $V \cap U_1 \le V_1$. Assume that there exists $\alpha \in V \cap U_1$ and $\alpha \notin V_1$. As $\alpha \in V - V_1$, by Proposition 2.3(7), the order of α is 9. But $\alpha \in U_1$ as well and U_1 is an elementary Abelian group again by Proposition 2.3(7). Hence the order of α cannot be 9, which is a contradiction. ∎

LEMMA 4.32. *Under the above notations, we have* $V \cap Z(U) = Z(V)$, *where* $Z(V)$ *is the center of* V *in* M.

Proof. For $\alpha \in V \cap Z(U)$, $\alpha \in V$ and $\alpha h = h\alpha$ for any $h \in U$. In particular $\alpha h = h\alpha$ for any $h \in V \le U$. Therefore $\alpha \in Z(V)$. It remains to prove that $Z(V) \le V \cap Z(U)$. Assume that there exists $\alpha \in Z(V)$ such that $\alpha \notin Z(U)$. Since $\alpha \in Z(V) - \langle 1\rangle$, $\alpha = \gamma^3$ for some $\gamma \in V - V_1$ by Proposition 2.3(7). Moreover $V \cap U_1 = V_1$ by Lemma 4.31 and hence $\gamma \notin U_1$. Therefore $\gamma \in U - U_1$ and again by Proposition 2.3(7), $\alpha = \gamma^3 \in Z(U)$. This is a contradiction. ∎

COROLLARY 4.33. *Let* $P \in \Omega_m$. *Let* V *be the* 3*-Sylow subgroup of* M *fixing* P, *and* T_{m-1} *be the cyclic subgroup of* M *fixing* P *and another place of* Ω_m. *Let* V_1 *be the derived subgroup of* V *and* $Z(V)$ *be the center of* V. *The ramification groups of* P *in the extension* F/F^M *are*:

(i) $M_0(P) = VT_{m-1}$,
(ii) $M_1(P) = V$,
(iii) $M_i(P) = V_1$ *for* $2 \le i \le 3q_0 + 1$,
(iv) $M_i(P) = Z(V)$ *for* $3q_0 + 2 \le i \le q + 3q_0 + 1$,
(v) $M_i(P) = \langle 1\rangle$ *for* $i \ge q + 3q_0 + 2$.

Therefore the different exponent d_P *of* P *in* F/F^M *is*

$$\begin{aligned} d_P &= m^3(m-1) - 1 + (m^3 - 1) + 3q_0(m^2 - 1) + q(m-1) \\ &= m^4 + 3q_0(m^2 - 1) + q(m-1) - 2. \end{aligned}$$

For the ramification structure of F/F^M at nonrational places, we need the following lemmata.

LEMMA 4.34. *If* $n \equiv 3 \bmod 6$, *then* $\gcd(|\mathrm{Ree}(m)|, q - 3q_0 + 1) = 1$.

Proof. Note that $m^3 \mid q^3$, $m-1 \mid q-1$ and $|\mathrm{Ree}(m)| = m^3(m-1)(m^3+1)$. Since $\gcd(q^3(q-1), q-3q_0+1) = 1$, we have $\gcd(m^3(m-1), q-3q_0+1) = 1$. It remains to prove that $\gcd(m^3+1, q-3q_0+1) = 1$. Let $n = 3+6k$, where k is a nonnegative integer. Then $q+1 = m^{3(2k+1)}+1$ and hence $m^3+1 \mid q+1$. The assertion follows from the fact that $\gcd(q+1, q-3q_0+1) = 1$. ∎

LEMMA 4.35. *For any odd integer $n \geq 5$ we have*:

(i) *if* $n \equiv 1 \bmod 6$ *with* $(n-1)/6$ *even or* $n \equiv 5 \bmod 6$ *with* $(n-5)/6$ *odd*, *then*

$$m - 3m_0 + 1 \mid q - 3q_0 + 1, \qquad m + 3m_0 + 1 \mid q + 3q_0 + 1;$$

(ii) *if* $n \equiv 1 \bmod 6$ *with* $(n-1)/6$ *odd or* $n \equiv 5 \bmod 6$ *with* $(n-5)/6$ *even*, *then*

$$m - 3m_0 + 1 \mid q + 3q_0 + 1, \qquad m + 3m_0 + 1 \mid q - 3q_0 + 1.$$

Proof. We only give the proof of (i). Note that

$$\begin{aligned} 3m_0^2 &\equiv 3m_0 - 1 \bmod (m - 3m_0 + 1), \\ 3^2 m_0^5 &\equiv m_0 - 1 \bmod (m - 3m_0 + 1), \\ 3^3 m_0^6 &\equiv -1 \bmod (m - 3m_0 + 1). \end{aligned}$$

If $n \equiv 1 \bmod 6$ and $k = (n-1)/6$ is even, then

$$\begin{aligned} q_0 = m_0 3^{3k} m_0^{6k} &\equiv m_0 \bmod (m - 3m_0 + 1), \\ q = 3q_0^2 &\equiv 3m_0^2 \bmod (m - 3m_0 + 1), \\ q - 3q_0 + 1 \equiv 3m_0^2 - 3m_0 + 1 &\equiv 0 \bmod (m - 3m_0 + 1). \end{aligned}$$

If $n \equiv 5 \bmod 6$ and $k = (n-5)/6$ is odd, then

$$\begin{aligned} q_0 = 3^2 m_0^5 3^{3k} m_0^{6k} &\equiv (m_0 - 1)(-1) \bmod (m - 3m_0 + 1), \\ q = 3q_0^2 &\equiv -3m_0 + 2 \bmod (m - 3m_0 + 1), \\ q - 3q_0 + 1 \equiv (-3m_0 + 2) - 3(1 - m_0) + 1 &\equiv 0 \bmod (m - 3m_0 + 1). \end{aligned}$$

Using similar arguments we also get $m + 3m_0 + 1 \mid q + 3q_0 + 1$. ∎

LEMMA 4.36. *The number of distinct Hall subgroups of order* $m - 3m_0 + 1$ *of* $\mathrm{Ree}(m)$ *is*

$$\frac{|\mathrm{Ree}(m)|}{6(m - 3m_0 + 1)} = \frac{m^3(m-1)(m+1)(m + 3m_0 + 1)}{6}.$$

The number of distinct Hall subgroups of order $m + 3m_0 + 1$ *of* $\mathrm{Ree}(m)$ *is*

$$\frac{|\mathrm{Ree}(m)|}{6(m + 3m_0 + 1)} = \frac{m^3(m-1)(m+1)(m - 3m_0 + 1)}{6}.$$

Proof. Let $A_{2,m}$ be a Hall subgroup of order $m - 3m_0 + 1$ in $\mathrm{Ree}(m)$ and $k = |\mathrm{Ree}(m)|/6(m - 3m_0 + 1)$. Any Hall subgroup of order $q - 3q_0 + 1$ in $\mathrm{Ree}(m)$ is of the form $gA_{2,m}g^{-1}$ for some $g \in \mathrm{Ree}(m)$. Let

$$\{N_M(A_{2,m}), a_1 N_M(A_{2,m}), \ldots, a_{k-1} N_M(A_{2,m})\}$$

be the set of left cosets of the normalizer $N_M(A_{2,m})$ of $A_{2,m}$ in $\mathrm{Ree}(m)$. We fix $1, a_1, \ldots, a_{k-1} \in \mathrm{Ree}(m)$. For any $g \in \mathrm{Ree}(m)$, there are uniquely determined elements $a \in \{1, a_1, \ldots, a_{k-1}\}$ and $\alpha \in N_M(A_{2,m})$ such that $g = a\alpha$. Let $\alpha, \beta \in N_M(A_{2,m})$ and $a, b \in \{1, a_1, \ldots, a_{k-1}\}$. Then

$$\begin{aligned}(a\alpha)A_{2,m}(a\alpha)^{-1} = (b\beta)A_{2,m}(b\beta)^{-1} &\Leftrightarrow aA_{2,m}a^{-1} = bA_{2,m}b^{-1}\\ &\Leftrightarrow a^{-1}bA_{2,m}(a^{-1}b)^{-1} = A_{2,m}\\ &\Leftrightarrow a^{-1}b \in N_M(A_{2,m})\\ &\Leftrightarrow a = b.\end{aligned}$$

Hence k is the number of distinct Hall subgroups of order $m - 3m_0 + 1$ in $\mathrm{Ree}(m)$. We use similar arguments for the number of distinct Hall subgroups of order $m + 3m_0 + 1$ of $\mathrm{Ree}(m)$. ■

Now we can identify the ramification structure of F/F^M at nonrational places of F.

THEOREM 4.37. *For $n \geq 3$, if $n \equiv 3 \bmod 6$, then there is no nonrational place of F ramified in F/F^M. For $n \geq 5$:*

(i) *If $n \equiv 1 \bmod 6$ with $(n-1)/6$ even or $n \equiv 5 \bmod 6$ with $(n-5)/6$ odd, then F has exactly $m^3(m-1)(m+1)(m+3m_0+1)/6$ places of degree 6 which ramify in F/F^M. Moreover the ramification index of any of these places is $m - 3m_0 + 1$.*

(ii) *If $n \equiv 1 \bmod 6$ with $(n-1)/6$ odd or $n \equiv 5 \bmod 6$ with $(n-5)/6$ even, then F has exactly $m^3(m-1)(m+1)(m-3m_0+1)/6$ places of degree 6 which ramify in F/F^M. Moreover the ramification index of any of these places is $m + 3m_0 + 1$.*

Proof. F/F^M is ramified at a nonrational place of F if and only if there exists a Hall subgroup A_2 of G with order $q - 3q_0 + 1$ such that $A_2 \cap M \neq \langle 1\rangle$. For $n \geq 3$ and $n \equiv 3 \bmod 6$, as $\gcd(|M|, q - 3q_0 + 1) = 1$ by Lemma 4.34, there is no ramified nonrational place of F in the extension F/F^M. For $n \geq 5$ and $n \equiv 1 \bmod 6$ with $(n-1)/6$ even, each Hall subgroup of M with order $m - 3m_0 + 1$ is in a uniquely determined Hall subgroup of G with order $q - 3q_0 + 1$, since $m - 3m_0 + 1 \mid q - 3q_0 + 1$. Moreover the number of Hall subgroups of M with order $m - 3m_0 + 1$ is $m^3(m-1)(m+1)(m+3m_0+1)/6$ by Lemma 4.36. This completes the proof in this case. The other cases are proved similarly. ■

Now we compute the genus of F^M. The different exponent d_P for any $P \in \Omega_m$ is given by Corollary 4.33 as

$$d_P = (m^4 - 2) + 3q_0(m^2 - 1) + q(m - 1).$$

M has $m^2(m^2 - m + 1)$ distinct involutions and each involution gives $q - m$ extra ramified rational places from $\Omega - \Omega_m$ with ramification index 2 (see Lemmas 4.29 and 4.30).

Case $n \equiv 3 \bmod 6$. By Theorem 4.37 there is no ramification at nonrational places of F in F/F^M. Hence the Riemann–Hurwitz formula applied to F/F^M gives

$$\begin{aligned} 2g-2 = {} & m^3(m-1)(m^3+1)(2g_M-2) \\ & + (m^3+1)((m^4-2)+3q_0(m^2-1)+q(m-1)) \\ & + m^2(m^2-m+1)(q-m), \end{aligned}$$

where g_M is the genus of F^M, computed as

$$\begin{aligned} g_M = \frac{1}{2m^3(m-1)(m^3+1)} & \{3q_0(q-1)(q+q_0+1) \\ & - (m^3+1)(q(m-1)+3q_0(m^2-1)+m^4-2) \\ & - (q-m)m^2(m^2-m+1)-2\}+1. \end{aligned}$$

In particular when $m = 27$ and $q = 3^9$, we have $g_M = 4$.

Case $n \equiv 1 \bmod 6$ *with* $(n-1)/6$ *even or* $n \equiv 5 \bmod 6$ *with* $(n-5)/6$ *odd.* By Theorem 4.37, there are exactly $m^3(m-1)(m+1)(m+3m_0+1)/6$ places of degree 6 which ramify in F/F^M. The ramification index of any of these places is $m-3m_0+1$. Therefore the Riemann–Hurwitz formula gives

$$\begin{aligned} 2g-2 = {} & m^3(m-1)(m^3+1)(2g_M-2) \\ & + (m^3+1)((m^4-2)+3q_0(m^2-1)+q(m-1)) \\ & + m^2(m^2-m+1)(q-m) \\ & + m^3(m-1)(m+1)(m+3m_0+1)(m-3m_0), \end{aligned}$$

where g_M is the genus of F^M, computed as

$$\begin{aligned} g_M = \frac{1}{2m^3(m-1)(m^3+1)} & \{3q_0(q-1)(q+q_0+1) \\ & - (m^3+1)(q(m-1)+3q_0(m^2-1)+m^4-2) \\ & - (q-m)m^2(m^2-m+1) \\ & - m^3(m^2-1)(m+3m_0+1)(m-3m_0)-2\}+1. \end{aligned}$$

In particular when $m = 27$ and $q = 3^{33}$, we have

$$g_M = 1980870811460454688885918495\,93.$$

Case $n \equiv 1 \bmod 6$ *with* $(n-1)/6$ *odd or* $n \equiv 5 \bmod 6$ *with* $(n-5)/6$ *even.* Using Theorem 4.37 as above, the Riemann–Hurwitz formula in this case gives

$$\begin{aligned} 2g-2 = {} & m^3(m-1)(m^3+1)(2g_M-2) \\ & + (m^3+1)((m^4-2)+3q_0(m^2-1)+q(m-1)) \\ & + m^2(m^2-m+1)(q-m) \\ & + m^3(m-1)(m+1)(m-3m_0+1)(m+3m_0), \end{aligned}$$

where g_M is the genus of F^M, computed as

$$\begin{aligned} g_M = \frac{1}{2m^3(m-1)(m^3+1)} &\{3q_0(q-1)(q+q_0+1) \\ &- (m^3+1)(q(m-1)+3q_0(m^2-1)+m^4-2) \\ &- (q-m)m^2(m^2-m+1) \\ &- m^3(m^2-1)(m-3m_0+1)(m+3m_0)-2\}+1. \end{aligned}$$

In particular when $m = 27$ and $q = 3^{15}$, we have $g_M = 67059625$.

REMARK 4.38. For various subgroups $H \leq G$, the action of H on the rational places of F is examined throughout the section. More precisely, for a subgroup $H \leq G$ considered in one of the subsections above, the number of degree 1 places of F ramified in the extension F/F^H and the ramification index of each of them is determined. Using this information, one can easily compute the number of degree 1 places of F^H below the degree 1 places of F. This will give a lower bound on the number of rational places of F^H (see examples below). On the other hand, for most of the subgroups $H \leq G$, there will be rational places of F^H below higher degree places of F, and to find the number of such places is difficult. The task of computing the exact number of rational places of F^H for some of the subgroups $H \leq G$ is considered in another work that we are preparing.

We now give examples on how to calculate the number of rational places of F^H below the rational places of F. For $H \leq G$, let $N(F^H)$ denote the number of degree 1 places of F^H. We give examples among subgroups of the centralizer of an involution. Let $\kappa \in G$ be an involution and L the centralizer of κ in G. Recall that $L = \kappa \times L'$, where L' is the subgroup of L isomorphic to $\mathrm{PSL}(2,q)$ (see Section 4.1).

EXAMPLE 4.39. Let $H = \kappa \times D^+$, where $D^+ \leq L'$ is a dihedral subgroup of order $2n$ with $n \mid (q+1)/2$ and $2 \mid n$. Then $|H| = 4n$ and $8 \mid |H|$. From Section 4.1, there are $(2n+3)(q+1)$ places in F ramified in F/F^H, each of them being a degree 1 place with ramification index 2. So each orbit of H among the ramified places of F has $4n/2$ elements. Therefore H has $(2n+3)(q+1)/2n$ orbits among ramified places of F and $(q^3+1-(2n+3)(q+1))/4n$ orbits among the unramified degree 1 places of F. So

$$N(F^H) \geq \frac{(2n+3)(q+1)}{2n} + \frac{q^3+1-(2n+3)(q+1)}{4n}. \tag{4.6}$$

Note that in the special case of $n = 2$, i.e. when H is a 2-Sylow subgroup of G, we have equality in (4.6).

EXAMPLE 4.40. Let H be a 3-subgroup of L of order $m = 3^f$, $f \leq 2s+1$. From Section 4.1, there is only one place in F (which is a degree 1 place) ramified in F/F^H with ramification index m. In this case also, the number of places of F^H below the degree 1 places of F is equal to the exact number of degree 1 places of F^H. So we have

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

Acknowledgements. We are grateful to the anonymous referee for the encouraging and invaluable detailed comments.

Both authors wish to thank Şükrü Yalçınkaya for very useful conversations during the preparation of the paper.

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

[G-S-X] A. Garcia, H. Stichtenoth and C. P. Xing, *On subfields of the Hermitian function field*, Compositio Math. 120 (2000), 137–170.

[G-K-T] M. Giulietti, G. Korchmáros and F. Torres, *Quotient curves of the Deligne–Lusztig curve of Suzuki type*, preprint 2002, arXiv:math.AG/0206311.

[G-L-S 2] D. Gorenstein, R. Lyons and R. Solomon, *The Classification of the Finite Simple Groups. Number 2*, Amer. Math. Soc., Providence, 1996.

[G-L-S 3] —, —, —, *The Classification of the Finite Simple Groups. Number 3*, Amer. Math. Soc., Providence, 1998.

[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.

[K-O-S] W. M. Kantor, M. E. O'Nan and G. M. Seitz, *2-Transitive groups in which the stabilizer of two points is cyclic*, J. Algebra 21 (1972), 17–50.

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

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

[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, 1992, 122–131.

[Re] R. Ree, *Sur une famille de groupes de permutations doublement transitifs*, Canad. J. Math. 16 (1964), 797–820.

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

[Se] J.-P. Serre, *Local Fields*, Springer, New York, 1979.

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

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

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

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

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

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

Received on 24.6.2003
and in revised form on 8.3.2004 (4564)