Journal of Algebra **216,** 665–706 (1999)
Article ID jabr.1998.7804, available online at http://www.idealibrary.com on IDEAL®

The Group of Automorphisms of Cyclic Extensions of Rational Function Fields

Aristides Kontogeorgis

Max-Planck-Institut für Mathematik, Gottfried-Claren Strasse 26, D-53225 Bonn, Germany and Department of Mathematics, University of Crete, Heraclion 71409, Crete, Greece
E-mail: kontogeo@mpim-bonn.mpg.de

Communicated by Walter Feit

Received August 7, 1998

We study the automorphism groups of cyclic extensions of the rational function fields. We give conditions for the cyclic Galois group to be normal in the whole automorphism group, and then we study how the ramification type determines the structure of the whole automorphism group. © 1999 Academic Press

1. INTRODUCTION

A hyperelliptic function field, contains in the center of its group of automorphisms an involution j whose fixed field $F^{(j)}$ is rational. Motivated by this observation Brandt and Stichtenoth [B-S] studied the group G of automorphisms of hyperelliptic function fields, by projecting the automorphism group into the known finite subgroups of $PGL(2,q)$, that constitutes the automorphism group of the rational function field:

$$G \to \frac{G}{\langle j \rangle} < PGL(2,k).$$

As a natural generalization of this we consider cyclic extensions of the rational function field. Let F be such an extension of the rational function field F_0. When $n > 2$ the cyclic group $\mathrm{Gal}(F/F_0)$ is not always a normal subgroup of the automorphism group G. For instance, consider the family of function fields of the curves $x^n + y^m + 1 = 0$, where $n > 4$, $m|n$, and $(p,n) = (p,m) = 1$, $(m,2) = 2$, $p \nmid n-1$. The group $C_n = \mathrm{Gal}(F/k(y))$ is not a normal subgroup of G [Ko].

0021-8693/99 $30.00

R. Brandt [Br] studied the group of automorphisms of function fields which are cyclic central extensions of the rational function field $k(x)$ with $\mathrm{Gal}(F/k(x)) = C_q$, where C_q is a cyclic group of prime order q, prime to the characteristic p of the algebraic closed field k.

Here we generalize further his results to include automorpism groups G of function fields which are cyclic extensions of order n of the rational function field F_0. The constant field k of both function fields F_0 and F is assumed to be algebraically closed of characteristic p, prime to n. We also assume that all ramified places in the Galois extension F/F_0 are ramified completely and that $\mathrm{Gal}(F/F_0)$ is normal in G.

Moreover, following Accola's ideas [Ac] on strongly branched covers, we are able to obtain conditions on the number of ramified places in extension F/F_0, sufficient for the Galois group $\mathrm{Gal}(F/F_0)$ to be normal in the whole automorphism group G. Furthermore, we determine the structure of all such groups of automorphisms in terms of generators and relations when G/C_n is isomorphic to C_n, D_n, A_4, A_5, S_4 or a semidirect product of an elementary Abelian Group by a cyclic one, and in terms of the cohomology class of the group extension in all other cases. The structure of G depends on the ramified places in extensions F/F_0 and F_0/F^G in the following way: Let $A = \{P_1, \dots, P_f\}$ be the set of places of F_0 that are ramified in the extension $F_0/F_0^{G_0}$ and $A_R \subset A$ be the set of places of A which are ramified in F/F_0. The pair $(G_0, A_R \subset A)$ is called the ramification type of the extension F/F_0. It turns out that in most cases the ramification type determines the group structure of the extension G; there are however function fields which are cyclic extensions of the rational function field with the same ramification type, but different automorphism groups.

Finally we are able to prove that for every finite subgroup G_0 of $PGL(2,k)$ we can find a subgroup G_0' of $PGL(2,k)$, isomorphic to G_0 and a cyclic Kummer extension F which realizes every possible ramification type $(G_0', A_R \subset A)$. We also provide a method to write down an equation $y^n = f(x)$ realizing every possible automorphism group.

2. CONDITIONS FOR NORMALITY

Every cyclic cover of the projective line, after a birational transformation, can be written in the form,

$$y^n = \prod_{i=1}^{s} (x - \rho_i)^{d_i}, \qquad d_i \in \mathbb{Z},$$

where $0 < d_i < n$ and $d := \sum_{i=1}^{s} d_i \equiv 0 \mod n$. If the radicand $\prod_{i=1}^{s}(x-\rho_i)^{d_i}$ is not a $\delta|n$ power; i.e., $(n, d_1, \dots, d_s) = 1$, then F is a Kummer extension of F_0 of order n. We study extensions for which the stronger condition $(n, d_i) = 1$ for all $i = 1, \dots, s$, holds.

The function field F is a cyclic Kummer extension of F_0. Denote by v_P the valuation of F_0 corresponding to place P. We have

$$v_P(f(x)) = v_P\left(\prod_{i=1}^{s}(x-\rho_i)^{d_i}\right) = \begin{cases} -d & \text{if } P = P_{x=\infty}, \\ d_i & \text{if } P = P_{x=\rho_i}, \\ 1 & \text{otherwise} \end{cases}$$

and the ramification index e_P is given by the tables: ([St], III.7.3 p. 110])

$$r_P := \begin{cases} (n,d) & \text{if } P = P_{x=\infty} \\ (n,d_i) & \text{if } P = P_{x=\rho_i}, \\ n & \text{otherwise} \end{cases} \qquad e_P = \begin{cases} \dfrac{n}{(n,d)} & \text{if } P = P_{x=\infty} \\ \dfrac{n}{(n,d_i)} & \text{if } P = P_{x=\rho_i} \\ 1 & \text{otherwise} \end{cases}.$$

The conditions $(n, d_i) = 1$ imply that all ramified places in extension F/F_0 are ramified completely. Notice also that we have chosen a curve model such that there is no ramification at infinity, because $n|d$. The genus of the function field F can be computed with the aid of the Riemann−Hurwitz formula:

$$g = \frac{(n-1)(s-2)}{2}.$$

If n is a prime number, then under the assumption $s > 2n$ we have that the extension F/F_0 is strongly branched and, because the group $C_n := \mathrm{Gal}(F/F_0)$ is simple, we can use Corollary 3 of [Ac, p. 321], to deduce that $C_n \lhd G$. We will modify the ideas of Accola to prove:

PROPOSITION 1. *Suppose that a cyclic extension F/F_0 of the rational function field F_0 is ramified completely at s places and $n = |\mathrm{Gal}(F/F_0)|$. If $2n < s$ then $\mathrm{Gal}(F/F_0) \lhd G$, where G is the whole automorphism group.*

Proof. Let T be a generator of C_n and $Q_1, \dots, Q_s$ be the places of F which are fixed under the action of C_n. Denote by $\tilde{T} = \sigma T \sigma^{-1}$ an arbitrary conjugate of T. The fixed places of $\langle \tilde{T} \rangle$ are $\sigma(Q_1), \sigma(Q_2), \dots, \sigma(Q_s)$. Let $\tilde{F}_0 := F^{\langle \tilde{T} \rangle}$ be the fixed field of $\langle \tilde{T} \rangle$. $\tilde{F}_0$ is rational because it is a conjugate field of F_0. Denote by q_i $(i = 1, \dots, s)$, the restrictions of the places $\sigma(Q_i)$ in $\tilde{F}_0$. Because $\tilde{F}_0$ is rational, there are elements f_i in $\tilde{F}_0$, with only one pole at the place q_i, of pole order 1, and moreover

$k(f_i) = \tilde{F}_0$. $\tilde{F}_0$ is a subfield of F and we can consider f_i as an element of F. The divisor of f_i in F is

$$(f_i) = (f_i)_0 - n\sigma(Q_i).$$

Set $h_i := f_i - T \circ f_i$. If h_i is not a constant function then

$$\deg h_i \leq 2 \deg f_i - r_i = 2n - r_i,$$

where $0 \leq r_i \leq \deg f_i$ ($r_i = 0$ or n) is the number of poles of f_i, counting multiplicity, fixed by T. Indeed, for a place P of F, we have

$$v_P(h_i) = v_P(f_i - T \circ f_i) \geq \min\{v_P(f_i), v_P(T \circ f_i)\},$$

so if P is a pole of h_i then P is a pole of f_i or $T \circ f_i$. Moreover if P is a common pole of f_i, $T \circ f_i$ then it is not a pole of h_i.

On the other hand, every fixed place of T which is not a pole of f_i is a root of h_i. So the function h_i has $s - r_i$ roots. Because $2n < s$, we have

$$\deg h_i \leq 2n - r_i < s - r_i \leq \deg h_i,$$

a contradiction. Therefore $h_i \in k$ and because T fixes places which are not poles of f_i we have that $h_i = 0$. This implies that

$$f_i = T(f_i), \qquad \forall i \in \{1, \ldots, s\}.$$

Hence, $f_i \in F_0$, $F_0 = \tilde{F}_0$, and $C_n \lhd G$. ▮

Using the Riemann−Hurwitz formula we find that the above condition is equivalent to

$$(n-1)^2 < g_F,$$

where g_F is the genus of the function field F.

In the case $k = \mathbb{C}$ and $n = p$ is prime, then Victor Gonzalez and Rubi Rodriguez [G-R] have given a better condition. A curve C is a p-cyclic cover of the projective line if and only if it has a g_p^1 base point free linear system. The automorphism group permutes all linear systems of the above form and if the linear system g_p^1 is unique, then the Galois cyclic group $\mathrm{Gal}(C/\mathbb{P}^1)$ is normal in G. A sufficient condition for a linear system g_p^1 to be unique is the inequality:

$$2 \leq p \leq \frac{g}{2} + 1. \tag{1}$$

[A-C], so if (1) holds then $C_p \triangleleft G$.

3. CALCULATION OF THE GROUPS

Let F/F_0 be a cyclic extension with cyclic Galois group C_n of order n prime to the characteristic p and $C_n = \mathrm{Gal}(F/F_0) \triangleleft G$. We form the following short exact sequence,

$$1 \to C_n \to G \overset{\pi}{\to} G_0 \to 1$$

where $G := G/C_n$ is a finite subgroup of $PGL(2,k)$. The group G_0 acts on C_n in the following way: We choose a section of G_0 in G; i.e., for every $\sigma \in G_0$ we choose an element $S \in G$, such that $\pi(S) = \sigma$ and define

$$T^{\sigma} = STS^{-1},$$

where T is a generator of the cyclic group C_n. Because $C_n \triangleleft G$ this action is well defined. Setting $T^{\beta(\sigma)} = T^{\sigma}$ for an integer $\beta(\sigma)$ we can define a homomorphism

$$\beta\colon \begin{cases} G_0 \to \mathrm{Aut}(C_n) \cong \mathbb{Z}_n^* \\ \sigma \mapsto \beta(\sigma) \bmod n \end{cases} \tag{2}$$

We can interpret the action homomorphism β in terms of the generating elements x, y. Notice first that y is a generator of F over F_0, i.e., $F = F_0(y)$. Any other generator of F over F_0 is of the form $y^l B$ where $(l, n) = 1$ and $B \in F_0$ [Ha, p. 38]. Because $C_n \triangleleft F$ we have that for every $S \in G$, $S(F_0) = F_0$ so $S(y)$ is a generator of F_0 over F, hence of the form $S(y) = y^{l(S)}B_S$. By calculation $\beta(\sigma) = l(S)$, where $\sigma = S|_{F_0}$.

Let us consider now the inverse situation: G_0 is an arbitrary finite subgroup of automorphisms of the rational function field F_0. Is it possible to extend every element in G_0, to an automorphism of F? The following proposition gives us a necessary and sufficient condition.

PROPOSITION 2 [Na]. *Let $D = \mathrm{div}(f(x))_0$ be the root divisor of the polynomial $f(x) = y^n$ in the field F_0. Suppose that $\deg(D) = d \equiv 0 \bmod n$ and that $(v_P(D), n) = 1$ for all $P \in \mathrm{supp}(D)$. Let $\sigma \in G_0$ be an automorphism of F_0.*

(a) *The following are equivalent*:

- *For every element σ in G_0 we have that*

$$\sigma(D) \equiv \beta(\sigma) D \bmod n.$$

- *There is an automorphism σ' of the function field F such that $\sigma'|_{F_0} = \sigma$.*

(b) *The following are equivalent*:

- *There is an automorphism σ' of the function field F such that $\sigma'|_{F_0} = \sigma$ and $\sigma' T = T\sigma'$ where T is the generator of the cyclic group* $\mathrm{Gal}(F/F_0)$.
- $\sigma(D) = D$,

where by writing $D \equiv D'$ $\bmod n$, for two divisors with the same support, we mean that $v_P(D) \equiv v_P(D')$ for every $P|D, D'$.

Proof. Let $\sigma \in G_0$ and S be an extension of σ to F. Setting $S(y) = y^{\beta(\sigma)}B_\sigma$ in the defining equation $y^n = f(x)$ of F we get

$$\frac{\sigma(f)}{f^{\beta(\sigma)}} = B_\sigma^n. \tag{3}$$

Equation (3) is equivalent to

$$\sigma\big(\mathrm{div}_0(f)\big) - \beta(\sigma)\big(\mathrm{div}_0(f)\big) \equiv 0 \bmod n,$$

because we have assumed that $n \mid \deg(f)$, i.e., $\mathrm{div}_\infty(f) = n \cdot P_\infty$. Conversely, if $\sigma(\mathrm{div}_0(f)) - \beta(\sigma)\mathrm{div}_0(f) \equiv 0 \bmod n$ then there is a function $B_\sigma \in F_0$, satisfying (3) because the divisor $1/n(\sigma(\mathrm{div}(f)) - \beta(\sigma)\mathrm{div}(f))$ is of degree zero, hence principal.

The second assertion of the proposition is a consequence the first one, because σ, and T are commuting if and only if $\beta(\sigma) = 1$. ▮

The $\mathrm{supp}(D)$ is the set of places of F_0 which are ramified in the extension F/F_0. Because $C_n \lhd G$, every automorphism σ permutes the places in $\mathrm{supp}(D)$. The fixed places of $\mathrm{supp}(D)$ under the action of G_0 are ramified in the extension $F_0/F_0^{G_0}$.

Definition 1. Let G_0 be a finite group of automorphisms of the rational function field F_0 and $A := \{P_1, \dots, P_f\}$ be the set of places of F_0 which are ramified in $F_0/F_0^{G_0}$. Let also $A_R \subset A$ be a G_0 invariant subset of A and $\beta\colon G_0 \to \mathbb{Z}_n^*$ a homomorphism. We will denote by

$$\mathscr{D}_n(G_0, A_R \subset A, \beta) \subset \mathrm{Div}(F_0),$$

the set of effective divisors D of F_0 such that

- G_0 leaves $\mathrm{supp}(D)$ invariant,
- $A \cap \mathrm{supp}(D) = A_R$,
- $(v_P(D), n) = 1$ for all places $P \in \mathrm{supp}(D)$,
- $\sigma(D) \equiv \beta(\sigma)D \bmod n$ for all $\sigma \in G_0$.

Remark 1. Let $D \in \mathscr{D}_n$ $(G_0, A_r \subset A, \beta)$. If $\sigma \in G_0$ fixes a place $P \in \operatorname{supp}(D)$ then $\beta(\sigma) \equiv 1 \bmod n$. Indeed, $\sigma(D) \equiv \beta(\sigma) D \bmod n$ and $v_P(D) \equiv \beta(\sigma) v_P(D) \bmod n$, so $\beta(\sigma) \equiv 1 \bmod n$ because $v_P(D) \in \mathbb{Z}_n^*$.

LEMMA 3. *If for all $\sigma \in G_0$ and for all P such that $\sigma(P) = P$ we have $\beta(\sigma) \equiv 1 \bmod n$, then the set $\mathscr{D}_n(G_0, A_R \subset A, \beta)$ is not empty. Moreover if $\mathscr{D}_n(G_0, A_R \subset A, \beta) \neq \emptyset$ then we can find an effective divisor D in $\mathscr{D}_n(G_0, A_R \subset A, \beta)$ with arbitrary high degree.*

Proof. We will first construct the $\operatorname{supp}(D)$. Pick a place Q_1 of F_0 and consider the orbit $O(Q_1, G_0)$ of Q_1 under the action of G_0. Choose Q_2 not in $O(Q_1, G_0)$ and consider the orbit $O(Q_2, G_0)$. Continuing this way we can construct a set of orbits $O(Q_i, G_0)$ such that

$$O(Q_i, G_0) \cap O\big(Q_j, G_0\big) = \emptyset \quad \text{for } i \neq j,$$

and $A_R \subset \bigcup_{i=1}^{s} O(Q_i, G_0)$. Define the support of D

$$\operatorname{supp}(D) := \bigcup_{i=1}^{s} O(Q_i, G_0).$$

For all $P \in O(Q_i, G_0)$ define $v_P(D) := \lambda(Q_i) \cdot \beta(\sigma)$, where σ is the element of G_0 such that $\sigma(Q_i) = P$, and $1 \leq \lambda(Q_i) < n$ is an integer prime to n. We will later select a suitable $\lambda(Q_i)$ so that $\deg(D) \equiv 0 \bmod n$. The divisor D is well defined because if $\sigma, \sigma' \in G_0$ such that $\sigma(Q_i) = \sigma'(Q_i) = P$ then $\sigma' \cdot \sigma^{-1}(Q_i) = Q_i$, so $\beta(\sigma') \equiv \beta(\sigma) \bmod n$. ▮

DEFINITION 2. Let G_0 be a finite group of automorphisms of the rational function field F_0 and let $A = \{P_1, \dots, P_f\}$, $A_R \subset A$ be as in Definition 1. We say that the ramification type $(G_0, A_R \subset A, \beta)$ is realizable if there exists a cyclic extension F of F_0 defined as at the beginning of Section 2, such that $C_n = \operatorname{Gal}(F/F_0)$ is a normal subgroup of the whole automorphism group G, $G/C_n \supset G_0$ and the set A_R consists of the places of A which are ramified in the extension F/F_0.

PROPOSITION 4. *If the divisor $D \in \mathscr{D}_n$ $(G_0, A_R \subset A, \beta)$ can be constructed so that*

$$\deg D \equiv 0 \bmod n,$$

and the infinite place $P_\infty \notin \operatorname{supp} D$, then the ramification type $(G_0, A_R \subset A, \beta)$ is realizable.

Proof. We set $F = F_0(y)$, where

$$y^n = \prod_{P \in \operatorname{supp}(D)} (x - x(P))^{v_p(D)},$$

and $x(P) \in k$ denotes the finite point of $\mathbb{P}^1(k)$ corresponding to the place P. The assertion follows by Proposition 2. Notice that, in order to ensure $G_0 \lhd G$ we can take $\#\mathrm{supp}(D) > [n/2] + 1$. ∎

In case $\deg D \equiv 0 \bmod n$ but $P_\infty \in \mathrm{supp}\, D$, we can find a Möbius transformation $A \in PGL(2,k)$ such that $P_\infty \notin Q(\mathrm{supp}\, D)$, so the ramification type $(QG_0Q^{-1}, Q(A_R) \subset Q(A), \beta)$ is realizable.

We will now compute the degree of $D \in \mathscr{D}_n\ (G_0, A_R \subset A, \beta)$. Let σ_0 be an arbitrary element in G_0 of order m. The set $\mathrm{supp}(D)$ splits into orbits under the action of σ_0:

$$\mathrm{supp}(D) = \bigcup_{i=1}^{k_{\sigma_0}} O(P_i, \langle \sigma_0 \rangle).$$

Let P be an element of $\mathrm{supp}(D)$, which is not fixed by σ_0. The orbit of P under the action of $\langle \sigma_0 \rangle$ is $O(P, \langle \sigma_0 \rangle) = \{P, \sigma_0(P), \dots, \sigma_0^{m-1}(P)\}$. (Observe that if P is not fixed by the Möbius transformation σ_0 it is not fixed by any power of σ_0.) This orbit corresponds to a divisor,

$$\sum_{i=0}^{m-1} \lambda \beta\left(\sigma_0^i\right) \sigma_0^i(P)$$

of degree modulo p^a:

$$\sum_{i=0}^{m-1} \lambda \beta\left(\sigma_0^i\right) = \begin{cases} \lambda \dfrac{\beta(\sigma_0)^m - 1}{\beta(\sigma_0) - 1} \equiv 0 \bmod p^a & \text{if } \beta(\sigma_0) \not\equiv 1 \bmod p^a, \\ \lambda m \bmod p^a & \text{if } \beta(\sigma_0) \equiv 1 \bmod p^a, \end{cases} \tag{4}$$

for every $p^a \mid n$, $p^{a+1} \nmid n$.

Remark 2. Consider a realizable divisor $D \in \mathscr{D}_n\ (G_0, A_R \subset A, \beta)$, hence of degree $\equiv 0 \bmod n$. If $P \in \mathrm{supp}\, D$ is a fixed place of $\sigma \in G_0$, then $\beta(\sigma) \equiv 1 \bmod n$. If σ has two fixed places P_1, P_2 and $P_1 \in \mathrm{supp}(D)$, $P_2 \notin \mathrm{supp}(D)$, then necessarily we have $(n, m) = 1$, where m is the order of σ. Indeed, the degree of D is

$$\deg(D) = v_{P_1}(D) + \sum \lambda_i m \equiv 0 \bmod n.$$

So $(n,m) | v_{P_1}(D)$, a contradiction unless $(n,m) = 1$.

LEMMA 5. *If there is a* $\sigma \in G_0$ *such that* $\beta(\sigma) \not\equiv 1 \bmod p^a$, *for every prime* $p^a \mid n$, $p^{a+1} \nmid n$, *then every divisor* $D \in \mathscr{D}_n\ (G_0, A_R \subset A, \beta)$ *has degree* $0 \bmod n$.

Proof. σ acts on $\mathrm{supp}(D)$ without fixed points, because $\beta(\sigma) \not\equiv 1 \bmod n$. The desired result follows by Eq. (4). ∎

LEMMA 6. *In case $A_R = \emptyset$; i.e., none of the ramified places in $F_0/F_0^{G_0}$ is ramified in F/F_0 then we can construct a divisor $D \in \mathscr{D}_n\, (G_0, A_R \subset A, \beta)$ of degree* $0 \bmod n$.

Proof. Notice that G_0 acts without fixed points on $\mathrm{supp}(D)$, because $A_R = \emptyset$, so we take even number of orbits $O(Q_i, G_0)$ $i = 1, \dots, r$ and put $\lambda(Q_i) \equiv -\lambda(Q_{r-i}) \bmod n$. This construction implies that $\deg D \equiv 0 \bmod n$.

4. FINITE SUBGROUPS OF $PGL(2,k)$ AS QUOTIENT GROUPS

All finite subgroups of the group of automorphisms of a rational function field are given by:

THEOREM 7 [V-M]. *Let F_0 be a rational function field with an algebraically closed field of constants k of characteristic $p \geq 0$. Suppose that G_0 is a nontrivial finite group of automorphisms of F_0 and $F_1 := F_0^{G_0}$ is the fixed field of G_0. Let r be the number of ramified places of F_1 in the extension F_0/F_1 and $e_1, \dots, e_r$ the corresponding ramification indices. Then G_0 is one of the following groups, with F_0/F_1 having one of the associated ramification types*:

1. *Cyclic group of order relatively prime to p with $r = 2$, $e_1 = e_2 = |G_0|$*
2. *Elementary Abelian p-group with $r = 1$, $e = |G_0|$*
3. *Dihedral group D_m of order $2m$ with $p = 2$, $(p, m) = 1$, $r = 2$, $e_1 = 2$, $e_2 = m$, or $p \neq 2$, $(p, m) = 1$, $r = 3$, $e_1 = e_2 = 2$, $e_3 = m$.*
4. *Alternating group A_4 with $p \neq 2, 3$, $r = 3$, $e_1 = 2$, $e_2 = e_3 = 3$.*
5. *Symmetric group S_4 with $p \neq 2, 3$, $r = 3$, $e_1 = 2$, $e_2 = 3$, $e_3 = 4$.*
6. *Alternating group A_5 with $p = 3$, $r = 2$, $e_1 = 6$, $e_2 = 5$, or $p \neq 2, 3, 5$, $r = 3$, $e_1 = 2$, $e_2 = 3$, $e_3 = 5$.*
7. *Semidirect product of an elementary Abelian p-group of order q with a cyclic group of order m with $m \mid (q-1)$, $r = 2$, $e_1 = |G_0|$, $e_2 = m$.*
8. *$PSL(2, q)$ with $p \neq 2$, $q = p^m$, $r = 2$, $e_1 = \frac{q(q-1)}{2}$, $e_2 = \frac{q+1}{2}$.*
9. *$PGL(2, q)$ with $q = p^m$, $r = 2$, $e_1 = q(q-1)$, $e_2 = q + 1$ where r is the number of places of the field F_1 ramified in F/F_0.*

Remark 3. Because k is algebraically closed, for every place Q of F_0, the inertia group is equal to the decomposition group.

4.1. *Some Cohomology Calculations*

It is well known that the set of all equivalent extensions of the form

$$1 \to C_n \to G \overset{\pi}{\to} G_0 \to 1$$

are classified in terms of the second cohomology group $H^2(G_0, C_n)$ where G_0 acts on C_n by conjugation of an arbitrary section of G_0. If C_n is a trivial G_0 module; i.e., the function β defined in (2) is trivial, then it is easy to compute this cohomology group employing the universal coefficient theorem. Namely, the following formula holds [Br]:

$$H^2(G_0, C_n) \cong \mathrm{Hom}\big(H_2(G_0, \mathbb{Z}), C_n\big) \oplus \mathrm{Ext}\big(H_1(G_0, \mathbb{Z}), C_n\big), \qquad (5)$$

where the G_0 acts trivially on $\mathbb{Z}$. The homology group $H_2(G, \mathbb{Z})$ is the Schur multiplier which is known for all the finite subgroups of $PGL(2, k)$ appearing in Theorem 7. The homology group $H_1(G_0, \mathbb{Z})$ is the Abelianization $G_0/[G_0, G_0]$ of G_0. Using these results we are able to compute the cohomology table, Table I. Notice that two nonequivalent extension sequences might have isomorphic middle groups. For example, all extensions of C_p by C_p, where p is prime are of order p^2, hence Abelian. So there are only two possible middle groups for the extension sequence, namely, C_{2p} and $C_p \times C_p$. On the other hand $H^2(C_p, C_p) \cong \mathbb{Z}_p$.

Denote by $i(G_0, C_n)$ the number of nonisomorphic middle groups obtained by extending the group G_0 by C_n. We have

$$i(G_0, C_n) \le \big| H^2(G_0, C_n) \big|.$$

We state also the proposition which we use later.

TABLE I

Group G_0	$H^2(G_0, C_n)$
C_m	$\mathbb{Z}_{(n,m)}$
D_m	$\begin{cases} 0 & \text{if } (n,2)=1 \\ \mathbb{Z}_2 & \text{if } (n,2)=2, (m,2)=1 \\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 & \text{if } (n,2)=(m,2)=2 \end{cases}$
A_4	$\mathbb{Z}_{(n,2)} \times \mathbb{Z}_{(n,3)}$
A_5	$\mathbb{Z}_{(2,n)}$
S_4	$\mathbb{Z}_{(2,n)} \times \mathbb{Z}_{(2,n)}$
$PSL(2,q)$	$\begin{cases} 1 & \text{if } p=2,\ p^f \neq 4 \\ \mathbb{Z}_{(2,n)} & \text{if } p>2,\ p^f \neq 9,\ p^f = 4, \text{ where } q = p^f \\ \mathbb{Z}_{(6,n)} & \text{if } p^f = 9 \end{cases}$
$PGL(2,q)$	$\mathbb{Z}_{(2,n)} \times \mathbb{Z}_{(2,n)}$

PROPOSITION 8 [Wei, p. 93]. *Let s be the order of G_0. There is an injection*

$$H^2(G_0, A) = \bigoplus_{p|s} H^2(G_0, A)_p \overset{\Phi}{\to} \bigoplus_{p|s} H^2(G_{0p}, A)$$

$$\alpha = \sum_{p|s} \alpha_p \mapsto \sum_{p|s} \operatorname{res}_{(G_0 \to G_{0p})} \alpha_p,$$

where G_{0p} ranges over the p-Sylow subgroups of G_0. Here $H^2(G_0, A)_p$ is the p-part of the finite Abelian group $H^2(G_0, A)$.

4.2. *Cyclic Groups*

We begin our examination of the possible finite groups of the rational function field given in Theorem 7, with the cyclic group. In this section we will prove:

THEOREM 9. *Let $G_0 = G/C_n$ be isomorphic to a cyclic group C_m of order m, prime to the characteristic of the field k. The set A of fixed places of F_0 under the action of G_0 is $A = \{P_1, P_2\}$. The group of automorplhisms G is then isomorphic to*

(a) *C_{nm} is one, at least, of the places P_1, P_2, say P_1, is ramified completely in the extension F/F_0, i.e., when $A_R \neq \emptyset$*

(b) *$C_n \rtimes C_m$ if no place in A is ramified in F/F_0, i.e., $A_R = \emptyset$.*

Proof. (a) In this case, one of the places P_1, P_2, say P_1, is ramified completely in the extension F/F_0. If Q is the unique place of F lying over P_1, then the decomposition subgroup $G(Q)$ is cyclic [Se, p. 68] and equal to G. The group G is Abelian and the map β: $C_m \to \mathbb{Z}_n^*$ is trivial.

(b) In this case none of the two places P_1, P_2 is ramified in F/F_0. Denote by π the natural map π: $G \to G_0$. Let T be a generator of C_n, and S an element of G such that $\pi(S)$ is a generator of the quotient subgroup C_m. The group G is a metacyclic group generated by T, S. Because $\pi(S)^m = 1$ we have that

$$S^m = T^t,$$

for an element $T^t \in C_n$. The function β is determined by its value at the generator $\pi(S)$ of C_m. Let $l := \beta(\pi(S))$. Then

$$T^{\pi(S)} = STS^{-1} = T^{\beta(\pi(S))} = T^l.$$

Consider the subextension diagram, where $G_1 := \pi^{-1}(\ker\beta)$

$$\begin{tikzcd}
1 \arrow[r] & C_n \arrow[r] \arrow[d, equal] & G_1 \arrow[r] \arrow[d] & \ker\beta \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & C_n \arrow[r] & G \arrow[r, "\pi"] & C_m \arrow[r] & 1
\end{tikzcd}.$$

Let $\pi(S)^r$, $r|m$ be a generator of the cyclic group $\ker\beta$. Then

$$l^r = \beta(\pi(S^r)) \equiv 1 \bmod n,$$

and $S^r T S^{-r} = T^{l^r} = T$ so the group $G_1 < G$, which is generated by T and S^r, is Abelian.

We claim that all p-Sylow subgroups of G_1 are isomorphic to $C_{p^{v_1}} \times C_{p^{v_2}}$, where v_1, v_2 are the exponents of p in the decomposition of n and m/r into prime factors. Indeed, let p be a prime divisor of $(n, m/r)$. Denote by G_1^p a p-Sylow subgroup of G_1. Consider the tower of fields

$$\begin{tikzcd}[row sep=small]
 & F \arrow[d, dash] & & \\
 & L := F^{C_{n/p^{v_1}}} \arrow[d, dash] & A_1, \dots, A_{p^{v_1}} \arrow[d, dash] & \text{decomposes completely} \\
G_1^p \Bigg\{ & F_0 \arrow[d, dash] & P_1 \arrow[d, dash] & \text{ramifies completely} \\
 & F_0^{C_{p^{v_2}}} \arrow[d, dash] & p_1 & \\
 & F^{G_1} & &
\end{tikzcd},$$

where p_1 is the restriction of the place P_1 in $F_0^{C_{p^{v_2}}}$, and $A_1, \dots, A_{p^{v_1}}$ are the extensions of the place P_1 of F_0 in $F^{C_{n/p^{v_1}}} =: L$. The Galois group $\mathrm{Gal}(L/F_0) = C_{p^{v_1}}$. If C is a cyclic subgroup of G_1^p containing $\mathrm{Gal}(L/F_0)$,

$$\mathrm{Gal}(L/F_0) \le C \le G_1^p,$$

then $C = \mathrm{Gal}(L/F_0)$. Otherwise, there is an intermediate field

$$L^C < L_T(A_1) < L$$

corresponding to the decomposition group $C(A_1)$ such that A_1 decomposes in the extension $L_T(A_1)/L^C$ and ramifies in the extension $L/L_T(A_1)$. This is impossible, because the subgroups of a cyclic p-group C are completely ordered with respect to inclusion. This remark together with the classification theorem of Abelian groups gives us that $G_1^p = C_{p^{v_1}} \times C_{p^{v_2}}$. Using the classification theorem of Abelian groups once more, we get $G_1 = C_n \times \ker \beta$. This implies

$$\langle T \rangle \cap \langle S^r \rangle = \{1\}. \tag{6}$$

If $S^m = T^t$ then $(S^r)^{m/r} = T^t \in \langle T \rangle \cap \langle S^r \rangle$ so $S^m = 1$ by (6). Hence the group G is given by generators and relations as

$$G = \{S, T \mid S^m = 1, T^n = 1, STS^{-1} = T^l\},$$

where $(l, n) = 1$, $l^r \equiv 1 \bmod n$. We have proven that G is the semidirect product of the groups $C_n \rtimes C_m$ with action given by β. ∎

Remark 4. Notice that if P decomposes in F/F_0 and the other fixed place of G_0 ramifies in F/F_0 then G is cyclic of order $n \cdot |G_0(P)|$. This is possible because in this case $(n, m) = 1$ and $C_n \times C_m \cong C_{nm}$.

COROLLARY 10. *Let G be the group of automorphisms of the function field F and let $G_0 = G/C_n$ be the quotient finite subgroup of F_0. Let also $G_0(P)$ be the decomposition group of a place P of F_0. If $G_0(P)$ is cyclic of order prime to the characteristic p, then the group $G_\pi(P)$ defined as*

$$G_\pi(P) := \{S \in G \colon \pi(S)P = P\},$$

is cyclic of order $n \cdot |G_0(P)|$ in case P is ramified in F/F_0. Otherwise, i.e., in case P is decomposed in F/F_0, $G_\pi(P)$ is the semidirect product of $C_n \rtimes G_0(P)$ with action given by $T^\sigma = T^{\beta(\sigma)}$, where σ is a generator for the cyclic group $G_0(P)$. In first case $\beta(\sigma) \equiv 1 \bmod n$.

We now prove that the following ramification types are realizable by finding a divisor in $\mathscr{D}_n(C_m, A_R \subset A, 1)$ such that $\deg(D) \equiv 0 \bmod n$. We have to consider

(a) $A_R = \{P_1\}$, β is trivial. The arbitrary divisor in $\mathscr{D}_n(C_m, A_R \subset A, 1)$ has the form

$$D = \lambda(P_1)P_1 + \sum_{i=0}^{r} \lambda(Q_i) \sum_{P \in O(Q_i, C_m)} P.$$

We have seen that this situation happens only in case $(n, m) = 1$, so there are integers κ, λ such that $\kappa n + \lambda m = 1$. We take r even, and we set $\lambda(P_1) = 1$, $\lambda(Q_0) = \lambda$, and $\lambda(Q_i) \equiv -\lambda(Q_{r-i+1}) \bmod n$, $i = 1, \dots, r$. This gives us that $\deg D \equiv 0 \bmod n$.

(b) $A_R = \{P_1, P_2\}$, β is trivial. The two orbits $O(P_i, C_m) = \{P_i\}$, $i = 1, 2$ of the fixed places P_1, P_2, are in A_R and $A_R = A = \{P_1, P_2\}$. The arbitrary divisor $D \in \mathscr{D}_n\,(C_m, A_R \subset A, 1)$ is of the form

$$D = \lambda(P_1)P_1 + \lambda(P_2)P_2 + \sum_{i=1}^{r} \lambda(Q_i) \sum_{P \in O(Q_i, C_m)} P,$$

where $Q_i \notin A$ for all $i = 1, \ldots, r$. In order to assure that the above divisor has degree 0 mod n, we set $\lambda(P_1) \equiv -\lambda(P_2) \bmod n$, r to be even and $\lambda(Q_i) \equiv -\lambda(Q_{r-i+1}) \bmod n$.

(c) $A_R = \varnothing$. This case is realizable by Lemma 6.

4.3. *Elementary Abelian Groups*

THEOREM 11. *Let $G_0 = G/C_n$ be isomorphic to an elementary Abelian group $\mathscr{E}_p(t)$ of order p^t, where p is the characteristic of k. The group G is isomorphic to $C_n \rtimes G_0$. Moreover if the unique fixed place P_1 of G_0 is ramified in the extension F/F_0 then G is isomorphic to $C_n \times G_0$.*

Proof. Because $(n, |G_0|) = 1$ the group G is a semidirect product, $G = C_n \rtimes G_0$. The action is given by the function β.

Suppose now that the unique fixed place P_1 of G_0 is ramified in F/F_0. Let Q be the unique place of F lying over P_1. The decomposition group $G(Q) = G$ is equal to the inertia group, because k is algebraically closed. So $G(Q)$ is the semidirect product of a cyclic group of order prime to p with a normal p-group $G_1(Q) = G_0$. Therefore the product is direct. ∎

The arbitrary divisor in $\mathscr{D}_n(G_0, A_R \subset \{P_1\}, \beta)$ is given by

$$D = \sum_{P \in A_R} \lambda(P)P + \sum_{i=1}^{s} \lambda(Q_i) \sum_{P \in O(Q_i, G_0)} P,$$

where $Q_i \notin A$, $i = 1, \ldots, s$. To prove that both ramification types are realizable we must select the above divisor to have degree 0 mod n. In the first case $A_R = \{P_1\}$ and β is trivial, so we take s orbits $O(Q_i, G_0)$ with $\lambda(P_1) = \lambda(Q_i) = 1$, such that

$$\deg(D) = 1 + sp^a \equiv 0 \bmod n,$$

where p^a is the order of G_0. This is always possible, because $(n, p) = 1$. In the second case, $A_R = \varnothing$ and the desired result follows from Lemma 6.

4.4. *Semidirect Products of Cyclic Groups with Elementary Abelian Groups*

In this case $G_0 = G/C_n$ is isomorphic to the semidirect product of an elementary Abelian group $\mathscr{E}_p(t)$ of order p^t, where p is the characteristic of k, with a cyclic group C_m of order m, and $m \mid (p^t - 1)$. In the extension

$F_0/F_0^{G_0}$, two places p_1, p_2 of $F_0^{G_0}$ are ramified with ramification indices $e_1 = |G_0|$ and $e_2 = m$, respectively.

THEOREM 12. *Let $G_0 = G/C_n$ be isomorphic to the semidirect product of an elementary Abelian group $\mathscr{E}_p(t)$ of order p^t, where p is the characteristic of k, with a cyclic group C_m of order m, and $m \mid (p^t - 1)$. The group of automorphisms G is isomorphic to $C_n \rtimes G_0$ if $A_R = \varnothing$ and $\mathscr{E}_p(t) \rtimes C_{nm}$ if $A_R \neq \varnothing$.*

Proof. Although in this case we are interested in elementary Abelian groups of order a power of the characteristic, we prove a more general lemma allowing p to be other than the characteristic.

LEMMA 13. *Denote by $\mathscr{E}_p(t)$ an elementary Abelian p group of order p^t, where p is not necessarily the characteristic. Consider the group $G_0 = \mathscr{E}_p(t) \rtimes C_m$, with $(m, p) = 1$, acting on the rational function field F_0. Suppose that the subextension*

$$1 \to C_n \to \pi^{-1}\big(\mathscr{E}_p(t)\big) \to \mathscr{E}_p(t) \to 1, \tag{7}$$

of the extension

$$1 \to C_n \to G \overset{\pi}{\to} \mathscr{E}_p(t) \rtimes C_m \to 1 \tag{8}$$

splits, i.e., $\pi^{-1}(\mathscr{E}_p(t)) = C_n \rtimes \mathscr{E}_p(t)$. Then G is isomorphic to $C_n \rtimes (\mathscr{E}_p(t) \rtimes C_m)$ if both fixed places of F_0, under the action of C_m, are decomposed in F/F_0 or to $G \cong \mathscr{E}_p(t) \rtimes C_{nm}$ if one of the fixed places of F_0, under the action of C_m, is ramified in F/F_0.

Proof. According to the study of cyclic extensions, we have two possibilities for the group $\pi^{-1}(C_m)$. Thus

$$\pi^{-1}(C_m) \cong C_n \rtimes C_m \quad \text{or} \quad \pi^{-1}(C_m) \cong C_{nm}.$$

If $\pi^{-1}(C_m) \cong C_n \rtimes C_m$ then using the injection Φ defined in Proposition 8:

$$H^2\big(\mathscr{E}_p(t) \rtimes C_m, C_n\big) \overset{\Phi}{\to} \bigoplus_{q \mid |G_0|} H^2\big(H_q, C_n\big),$$

where H_q ranges over the q-Sylow subgroups of G_0, we have that the whole extension (8) splits, because H_q is either a subgroup of $\mathscr{E}_p(t)$ or C_m.

If $\pi^{-1}(C_m) \cong C_{nm}$ then we will show that $G \cong \mathscr{E}_p(t) \rtimes C_{nm}$. Indeed, in this case there is an element $R \in G$ of order nm, which generates a subgroup of G isomorphic to C_{nm}. Because the extension (7) splits we have an embedding

$$j\colon \mathscr{E}_p(t) \hookrightarrow \pi^{-1}\big(\mathscr{E}_p(t)\big) \hookrightarrow G.$$

Moreover $\mathscr{E}_p(t) \cong j(\mathscr{E}_p(t))$ and $\pi^{-1}(\mathscr{E}_p(t)) \lhd G$. Because $C_n \cap \mathscr{E}_p(t) = 1$ we have that $j(\mathscr{E}_p(t)) \lhd G$. On the other hand $j(\mathscr{E}_p(t)) \cap C_{nm} = 1$. Indeed if $x \in j(\mathscr{E}_p(t)) \cap C_{nm}$ then $x^m \in j(\mathscr{E}_p(t)) \cap C_n = 1$ so $x^m = 1$, and $x = 1$ because $(p, m) = 1$. This implies the desired assertion.

We return now to our case, where p is the characteristic of k. Because $(p, n) = 1$, the extension (7) splits. If moreover one of the places fixed by C_m ramifies in F/F_0, then $G \cong \mathscr{E}_p(t) \rtimes C_{nm}$. Otherwise $G \cong C_n \rtimes (\mathscr{E}_p(t) \rtimes C_m)$. ▮

To prove the realization of the ramification type we have to select the arbitrary divisor

$$D = \sum_{P \in A_R} \lambda(P)P + \sum_{i=1}^{s} \lambda(P_i) \sum_{Q \in O(P_i, G_0)} P,$$

of $\mathscr{D}_n(G_0, A_R \subset A, \beta)$ to have degree 0 mod n. Denote by Q the unique place of F_0 above p_1 and by $Q_1, \dots, Q_{p^t}$ the places of F_0 above p_2. Notice also that $O(Q, G_0) = \{Q\}$, $O(Q_1, G_0) = \{Q_1, \dots, Q_{p^t}\}$.

We have the following cases for A_R

(a) $A_R = \varnothing$. This ramification type is realizable by Lemma 6.

(b) $A_R = O(Q, G_0) = \{Q\}$. In this case the function β must be trivial. Observe that the fixed places of C_m are Q, Q' where $Q' \in O(Q_1, G_0)$. Therefore, by Remark 2 we have that $(n, m) = 1$. We set $\lambda(P_i) = 1$, and we choose the number s so that

$$\deg(D) = 1 + s \cdot |G_0| \equiv 0 \bmod n.$$

This is possible because $(|G_0|, n) = (n, m) = 1$.

(c) $A_R = O(Q_1, G_0) = \{Q_1, \dots, Q_{p^t}\}$. Notice that $C_m < \ker \beta$. As before we have $(n, m) = 1$ as a necessary condition for this ramification type to be realizable. The degree of the divisor corresponding to the orbit $O(P_i, G_0)$ is

$$\sum_{P \in O(Q_i, G_0)} v_P(D) \equiv \begin{cases} 0 \bmod p^a & \text{if } \beta(\sigma) \not\equiv 1 \bmod p^a, \\ \lambda |G_0| \bmod p^a & \text{if } \beta(\sigma) \equiv 1 \bmod p^a \end{cases}$$

where $p^a \mid n$, $p^{a+1} \nmid n$. Let $n_0 = \prod_{p|n,\ \beta(\sigma) \equiv 1 \bmod p^a} p^a$. We have to choose an s such that $\deg(D) \equiv 0 \bmod n_0$. We take $\lambda(P) = 1$ for all $P \in \operatorname{supp}(D)$, and because $(n_0, |G_0|)$ divides $(n, mp) = (n, m) = 1$ the equation

$$\deg(D) = p^t + s \cdot |G_0| \equiv 0 \bmod n_0,$$

has a solution mod n_0.

(d) $A_R = O(Q, G_0) \cup O(Q_1, G_0)$. In this case β must be trivial. We set $\lambda(Q) \equiv -1 \bmod n$, $\lambda(P_i) = \lambda(Q_1) \equiv 1 \bmod n$, and we take s, so that

$$\deg(D) = -1 + p^t + s \cdot |G_0| \equiv 0 \bmod n.$$

This is possible because $(n, |G_0|) \mid m$ and $m \mid (p^t - 1)$.

4.5. *Dihedral Groups*

In this section we consider the case $G_0 = G/C_n \cong D_m$. The dihedral group D_m admits the presentation in terms of generators and relations:

$$D_m = \langle a, b \mid a^m = 1, b^2 = 1, ab = ba^{-1} \rangle.$$

The action homomorphism $\beta \colon D_m \to \mathbb{Z}_n^*$ is determined by its values on the generators a and b. Thus

$$\beta \colon \begin{cases} a \mapsto \beta(a) \\ b \mapsto \beta(b) \end{cases}.$$

Because β is a group homomorphism we have that

$$\beta(a)^m \equiv 1 \bmod n, \qquad \beta(b)^2 \equiv 1 \bmod n,$$
$$\beta(a)\beta(b) \equiv \beta(b)\beta(a)^{-1} \bmod n.$$

We claim that $\operatorname{ord}(\beta(a)) \leq 2$. Indeed, if $\operatorname{ord}(\beta(a)) > 2$ then $\operatorname{ord}(\beta(b)) = 1$, because the multiplicative group $\mathbb{Z}_n^*$ is Abelian and cannot contain the dihedral group $D_{\operatorname{ord}(\beta(a))}$. But then $\beta(ab) = \beta(a)\beta(b) = \beta(a)$ a contradiction, because the order of $\beta(ab)$ is at most 2. Furthermore if $\operatorname{ord}(\beta(a)) = 2$ then $2|m$ because $1 = \beta(a^m) = \beta(a)^m$.

There are three cases for $\operatorname{Im}(\beta)$.

$$\operatorname{Im}(\beta) = \{1\} \quad \text{or} \quad \operatorname{Im}(\beta) \cong \mathbb{Z}_2 \quad \text{or} \quad \operatorname{Im}(\beta) \cong V_4.$$

The third case appears only when $m \equiv 0 \bmod 2$. We will need:

LEMMA 14. *Let $n \in N$ and l an integer such that*

$$l^2 - 1 \equiv 0 \bmod n.$$

There are integers $n^+(l), n^-(l)$ *such that*

$$n = \frac{n^+(l) \cdot n^-(l)}{(n^+(l), n^-(l))},$$

where

$$(n^+(l), n^-(l)) = \begin{cases} 2 & \textit{if } n \equiv 0 \bmod 2 \\ 1 & \textit{if } n \equiv 1 \bmod 2 \end{cases},$$

with the additional property:

$$l \equiv 1 \bmod n^+(l) \quad \textit{and} \quad l \equiv -1 \bmod n^-(l).$$

Proof. We simply notice that if p is a prime divisor of n then $p \mid (l^2 - 1) = (l-1)(l+1)$ and p divides both $l-1$ and $l+1$ if and only if $p = 2$. ∎

Remark 5. Because the extensions F/F_0 and $F_0/F_0^{D_m}$ are both Galois, the places P_i of F_0 above a common $p \in F_0^{G_0}$ are either all ramified completely or all decomposed completely in the extension F/F_0.

According to Theorem 7 there are two cases for the ramification type in the extension $F_0/F_0^{G_0}$. We will handle them separately.

Case A. The characteristic of the field k is $p \neq 2$ $(p, m) = 1$. There are three distinct places of $F_1 := F_0^{G_0}$, namely, p_1, p_2, p_3, which are ramified in $F_0/F_0^{G_0}$ with ramification indices $2, 2, m$, respectively. Denote by $P_{1,i}, P_{2,i}, P_{3,j}$, where $i = 0, \dots, m-1$, $j = 0, 1$ the places of F_0 which extend p_1, p_2, p_3.

THEOREM 15. *Let* $G_0 = G/C_n$ *be isomorphic to the dihedral group* D_m, $p \nmid m$ *and* $p \neq 2$. *There are the cases for the structure of the automorphism group* G.

(1). *Suppose that* $\{P_{1,i}\}_{0 \le i < m} \cup \{P_{3,j}\}_{j=0,1} \subset A_R$. *Then* $(n, m) \mid 2$ *and the group of automorphisms* G *admits the presentation in terms of generators and relations,*

$$G = \langle R, S \mid R^2 = S^m,\ S^{nm} = 1,\ RSR^{-1} = S^r \rangle,$$

where r *is a solution of the system of equations*

$$r \equiv 1 \bmod n, \qquad r \equiv -1 \bmod m. \tag{9}$$

If $(n, m) = 1$ *there is only one solution* r. *If* $(n, m) = 2$ *there are two cases*:

- $n \equiv 2 \mod 4$. *In this case, one solution of* (9) *appears when* $\{P_{2,i}\}_{0 \le i < m} \cap A_R = \emptyset$ *and the other when* $\{P_{2,i}\}_{0 \le i < m} \cap A_R \neq \emptyset$.
- $n \equiv 0 \mod 4$. *In this case,* $\{P_{2,i}\}_{0 \le i < m} \cap A_R = \emptyset$ *and we have two possible nonisomorphic groups corresponding to the same ramification type*.

(2) $A_R = \{P_{3,j}\}_{j=1,2}$. *The group* G *is isomorphic to the semidirect product* $C_{nm} \rtimes C_2$.

(3) $A_R = \{P_{1,i}\}_{0 \le i < m} \cup \{P_{2,i}\}_{i=1,\dots,m}$. *In this case,* β *is trivial and* G *is isomorphic to* $C_n \times D_m$ *if* $(n, 2) = 1$ *and* G *is given by*

$$G = \langle R, S \mid R^{2n} = 1, S^m = 1, RSR^{-1} = S^{-1} \rangle,$$

if $(n, m) = 2$.

(4) $A_R = \emptyset$. *In this case* G *is isomorphic to* $C_n \rtimes D_m$, *where the action of* D_m *into* C_n *is given by* β.

(5) $A_R = \{P_{1,i}\}_{0 \le i < m}$. *In this case* G *admits the presentation*:

$$G = \langle R, S \mid R^{2n} = 1, S^m = 1, (RS)^2 = 1 \rangle.$$

Proof. We begin with:

Remark 6. Suppose that $b \in D_m$ fixes the place $P_{1,0}$. The other places $P_{1,i}$ can be enumerated so that $P_{1,i} = a^i P_{1,0}$. The decomposition groups $D_m(P_{1,i})$ of each place $P_{1,i}$ are of the form

$$D_m(P_{1,i}) = D_m(a^i P_{1,0}) = a^i D_m(P_{1,0}) a^{-i} = \langle a^{2i} b \rangle.$$

Every automorphism $ba^k \in D_m$ has two fixed places. A place of the form $P_{1,i}$ is fixed by $ba^k \neq 1$, if and only if $ba^k \in \langle a^{2i} b \rangle$ and because $\operatorname{ord}(a^{2i} b) = 2$ this is equivalent to

$$a^{2i} b = ba^k = a^{-k} b \quad \Leftrightarrow \quad 2i \equiv -k \mod m. \tag{10}$$

If $(m, 2) = 2$ then (10) has two solutions if k is even, and no solution if k is odd. This implies that the two fixed places of the automorphism ba^k restrict to the same place p_1 (if $k \equiv 0 \mod 2$) or p_2 (if $k \equiv 1 \mod 2$). If $(m, 2) = 1$ then (10) has a unique solution, so one of the two fixed places of ba^k restrict to p_1 and the other to p_2.

Suppose that one of the places $P_{3,j}$, say $P_{3,1}$ is ramified in extension F/F_0. Let $Q_{3,1}$ be the unique place of F over $P_{3,1}$. Because $(m, p) = 1$ we have that the decomposition group $G(Q_{3,1})$ is cyclic of order nm. Hence $\beta(a) \equiv 1 \mod n$. Notice that the index $|G : G(Q)| = 2$ so $G(Q) \lhd G$ and G

is a metacyclic group. Let S, R be in G, such that $\pi(R) = b$, $\pi(S) = a$. We may choose $S \in \pi^{-1}(a)$ such that $\langle S \rangle = G(Q)$. Because $G(Q) \lhd G$, there is an integer r such that

$$RSR^{-1} = S^r. \tag{11}$$

Observe that the group C_n is generated by $\langle S^m \rangle$. So from (11) and the action of b on C_n, we have

$$S^{\beta(b)m} = RS^mR^{-1} = S^{rm},$$

which gives us the relation

$$r \equiv \beta(b) \bmod n. \tag{12}$$

Because $G/C_n \cong D_n$, (11) implies

$$RSR^{-1}S = S^{r+1} \in \langle S^m \rangle,$$

and this, in turn, gives us the relation

$$r \equiv -1 \bmod m. \tag{13}$$

The system of equations (12), (13) has solutions if and only if $(n, m) \mid (\beta(b) + 1)$. We distinguish the cases:

1. $\{P_{1,i}\}_{0 \le i < m} \cup \{P_{3,j}\}_{j=0,1} \subset A_R$ so one of the places $P_{1,i}$, $i = 0, \ldots, m-1$, say $P_{1,0}$ is ramified completely in extension F/F_0. Denote by $Q_{1,0}$ the place above $P_{1,0}$. As in Remark 6, we may suppose that $P_{1,0}$ is fixed by $b \in D_m$ (select as generator b of D_m another element of order two if necessary). The decomposition group $G(Q_{1,0})$ is cyclic of order $2n$. Select a generator $R \in \pi^{-1}(b)$ of $G(Q_{1,0})$.

The group C_n is the unique subgroup of order n of the cyclic group $\langle R \rangle$, so it is generated by R^2. Hence $R^2 = S^{mi}$ for some $(i, n) = 1$. We simplify the notation by rechoosing a suitable generator S for the group $G(Q_{3,1})$ such that $R^2 = S^m$. Notice also that $\beta(b) \equiv 1 \bmod n$.

The group G as a metacyclic group is given by the generators and relations

$$G = \langle R, S \mid R^2 = S^m, S^{nm} = 1, RSR^{-1} = S^r \rangle, \tag{14}$$

where r is defined as a solution of the system

$$\begin{aligned} r &\equiv 1 \bmod n, \\ r &\equiv -1 \bmod m. \end{aligned} \tag{15}$$

This system admits (n, m) solutions if and only if $(n, m) \mid 2$. In case $(n, m) = 1$ the solution r is uniquely determined mod nm. In case $(n, m) = 2$ we have two solutions mod nm, namely,

$$r_0, \quad r_1 = r_0 + \frac{nm}{2}.$$

We have already assumed that the places in the orbit of $P_{1,0}$ are ramified completely in F/F_0. It is interesting to see how the ramification type of the places $P_{2,i}$ determines the selection of the root r_0.

Let $P = P_{2,k}$ be a place of F_0 in the orbit of $P_{2,0}$, hence, according to Remark 6, fixed by $ba^i \in D_m$, for some $i \equiv 1 \bmod 2$ (recall that $2|m$). According to Corollary 10, P is decomposed (resp., ramified) if $G_\pi(P) = C_2 \times C_n$ (resp., C_{2n}). The function

$$\Phi_P: \begin{cases} G_\pi(P) & \to \ G_\pi(P) \\ x & \mapsto \ x^2 \end{cases}$$

is a group homomorphism. Because $2|n$, ker $\Phi_P = C_2 \times C_2$ if P is decomposed otherwise (i.e., if P is ramified) ker $\Phi_P = C_2$. By computation,

$$G_\pi(P) = \{RS^{i+sm}, S^{sm} \mid s = 0, \dots, n-1\} \quad \text{for some } i \equiv 1 \bmod 2.$$

The elements $\{1, S^{nm/2}\}$ are in ker Φ_P. Moreover, using (14) we have

$$(RS^{i+sm})^2 = S^{m(1+((r+1)/m)(i+sm))}.$$

Hence P is decomposed in the extension F/F_0 if and only if the equation

$$-(r+1)s \equiv 1 + i\frac{r+1}{m} \bmod n$$

has a solution s. This equation has $(r+1, n) = 2$ different mod n solutions if and only if $(r+1, n) = 2 \mid (1 + i\frac{r+1}{m})$. Because $i \equiv 1 \bmod 2$ we have the equivalence

$$1 + i\frac{r+1}{m} \equiv 0 \bmod 2 \quad \Leftrightarrow \quad \frac{r+1}{m} \not\equiv 0 \bmod 2.$$

If $n \equiv 2 \bmod 4$ then $n/2$ is odd, so 2 divides either $(r_0 + 1)/m$ or $(r_1 + 1)/m = (r_0 + 1)/m + n/2$. Hence, if $n \equiv 2 \bmod 4$ the two solutions of system (15) correspond to the two different ramification types of the places $P_{2,i}$ in extension F/F_0.

If $n \equiv 0 \bmod 4$ then $(r+1)/m \not\equiv 0 \bmod 2$ for both solutions of (15). For if $2 \mid ((r+1)/m)$ then $4 \mid (r+1)$ (recall that $2|m$) and $4|n \mid (r-1)$ so

$4 \mid ((r+1)-(r-1)) = 2$, a contradiction. Therefore, if $n \equiv 0 \mod 4$ then for both solutions of (15) all places $P_{2,i}$ are decomposed in F/F_0.

2. $A_R = \{P_{3,j}\}_{j=1,2}$. In this case the places $P_{i,j}$, $i = 1,2$, $j = 0,\ldots, m-1$ of F_0 are all decomposed in the extension F/F_0. According to Corollary 10,

$$G_\pi(P_{i,j}) \cong C_n \rtimes C_2.$$

We may select a $R \in \pi^{-1}(b)$ such that $R^2 = 1$. The group G is given by

$$\langle R, S \mid S^{nm} = 1, R^2 = 1, RSR^{-1} = S^r \rangle,$$

where r is the solution of the system of Eqs. (11), (12), namely,

$$r \equiv \beta(b) \mod n, \qquad r \equiv -1 \mod m, \tag{16}$$

therefore $(n,m) \mid (\beta(b)+1)$. The group G is a semidirect product

$$C_{nm} \rtimes C_2,$$

with action defined by r. If $(n,m) > 1$ then the system (16) may have more than one solution $\mod nm$ which lead to more than one nonisomorphic automorphism group G.

Suppose now that the places $P_{3,j}$, $j = 1,2$ are not ramified in the extension F/F_0. Then Corollary 10 implies that,

$$G_\pi(P_{3,1}) \cong C_n \rtimes C_m,$$

because $D_m(P_{3,i}) = \langle a \rangle$ is a cyclic group. $G_\pi(P_{3,1})$ has index 2 in G so $C_n \rtimes C_m \triangleleft G$. Let T be a generator of the cyclic group C_n, and S a generator of C_m such that $\pi(S) = a$. If $R \in \pi^{-1}(b)$ because $|G : C_n \rtimes C_m| = 2$ the element $R^2 \in C_n \rtimes C_m$ so $R^2 = T^\mu S^z$. But $\pi(R^2) = a^z$ so $z \equiv 0 \mod m$ and $R^2 = T^\mu$. This gives us

$$R^2SR^{-2} = T^\mu S T^{-\mu} = T^{\mu(1-\beta(a))}S. \tag{17}$$

We may compute the left-hand side of (17) in another way. Because $C_n \rtimes C_m \triangleleft G$ we have

$$RSR^{-1} = T^\lambda S^r,$$

and this gives us

$$R^2SR^{-2} = RT^\lambda S^{-1}R^{-1} = T^{\lambda(\beta(b)-\beta(a))}S. \tag{18}$$

Combining (17) and (18) we get

$$\mu(1-\beta(a)) \equiv \lambda(\beta(b)-\beta(a)) \bmod n. \tag{19}$$

Moreover because $G/\langle T\rangle \cong D_m$ we have

$$RSR^{-1}S = T^{\lambda}S^{r+1} \in \langle T\rangle \quad \text{so } r \equiv -1 \bmod m. \tag{20}$$

Among $T, R, S \in G$ there are the relations,

$$\begin{gathered} S^m = 1, \qquad T^n = 1, \qquad R^2 = T^{\mu}, \qquad RTR^{-1} = T^{\beta(b)}, \\ STS^{-1} = T^{\beta(a)}, \qquad RSR^{-1} = T^{\lambda}S^{-1}, \end{gathered} \tag{21}$$

for some λ, μ satisfying (19). Observe that there are no other relations in the definition of the group G, because the relations (21) define a group of order $2nm$.

We want to simplify the relation $RSR^{-1} = T^{\lambda}S^{-1}$ by choosing another generator $S_1 = T^xS$. We calculate

$$RS_1R^{-1} = RT^xSR^{-1} = T^{x\beta(b)+\lambda}S^{-1} = T^{x(\beta(a)+\beta(b))+\lambda}S_1^{-1}. \tag{22}$$

LEMMA 16. *Let P be a place of F_0 which is fixed by ba. Suppose also that $R^2 = T^{\mu}$. If $2|n$ then*

$$(n, \beta(b)\beta(a)+1) \mid (\lambda + \mu\beta(a)), \tag{23}$$

if and only if P is decomposed in F/F_0. If $(2,n)=1$ then (23) holds in all cases.

Proof. Suppose first that $2|n$. By Corollary (10) we have

$$G_{\pi}(P) = \mathrm{Gal}\big(F/F_0^{\langle ba\rangle}\big) = \begin{cases} C_{2n} & \text{if } P \text{ ramifies in } (F/F_0) \\ C_n \rtimes C_2 & \text{if } P \text{ decomposes in } (F/F_0) \end{cases}.$$

In the first case there is only one element of order 2 in $\mathrm{Gal}(F/F_0^{\langle ba\rangle})$ and in the second there are more elements of order 2 in $G_{\pi}(P)$. Recall that

$$G_{\pi}(P) = \{\sigma \in G \mid \pi(\sigma)P = P\} = \{RST^k, T^k \mid k = 0,\dots,n-1\}.$$

Because n is even, one element of order 2 is $T^{n/2}$. If RST^k is of order 2 then

$$1 = (RST^k)^2 = T^{k(\beta(b)\beta(a)+1)+\lambda+\mu\beta(a)}, \tag{24}$$

so for some $k \in \{0, \ldots, n-1\}$,

$$k(\beta(b)\beta(a) + 1) + \lambda + \mu\beta(a) \equiv 0 \bmod n. \tag{25}$$

But Eq. (25) has solutions in k if and only if $(n, \beta(b)\beta(a) + 1) \mid (\lambda + \mu\beta(a))$.

If $(n, 2) = 1$, then the unique element of order 2 in $\mathrm{Gal}(F/F^{\langle ba \rangle})$ is of the form RST^k so (24) has a solution, which gives us the desired result as in the case that n is even. ∎

We consider now the three last cases of Theorem 15:

3. $A_R = \{P_{1,i}\}_{0 \le i < m} \cup \{P_{2,i}\}_{i=1,\ldots,m}$. All places $P_{i,j}$ are ramified in the extension F/F_0. Suppose as in Remark 6 that $D_m(P_{1,0}) = \langle b \rangle$. In view of Corollary 10 we may select a $R \in \pi^{-1}(b)$ such that $R^2 = T$, i.e., $\mu = 1$. Moreover the extension is central in this case, i.e.,

$$\beta(a) \equiv \beta(b) \equiv 1 \bmod n.$$

We consider two more subcases

- $(n, 2) = 1$. Because the extension is central we have $H^2(D_m, C_n) = 1$, so there is only one extension of D_m by C_n, namely,

$$G \cong C_n \times D_m.$$

- $(n, 2) = 2$. In this case Eq. (22) becomes

$$RS_1R^{-1} = T^{2x+\lambda}S_1^{-1}. \tag{26}$$

By Lemma 16 we have that $(n, \beta(a)\beta(b) + 1) = 2 \nmid \lambda + 1$, therefore $2|\lambda$ and the equation

$$2x + \lambda \equiv 0 \bmod n$$

has a solution x. Relation (26) for this solution x can be written as

$$RS_1R^{-1} = S_1^{-1}.$$

Let t be the order of S_1. The group G in this case is a metacyclic group given by the relations,

$$\langle R, S_1 \mid R^{2n} = 1, S_1^t = 1, RS_1R^{-1} = S_1^{-1} \rangle,$$

but then $|G| = 2nt$, so $t = m$.

4. $A_R = \varnothing$. All places $P_{i,j}$ are decomposed in the extension F/F_0. Suppose that $D_m(P_{1,0}) = \langle b \rangle$. By Corollary 10 we may select $R \in \pi^{-1}(b)$ such that $R^2 = 1$, and $\mu = 0$. Because all places of F_0 which are above

p_1, p_2 are decomposed in F/F_0, Lemma 16 gives us $(n, \beta(b)\beta(a)+1) | \lambda$. But $(\beta(b), n) = 1$, so $(n, \beta(ba)+1) = (n, \beta(b)\beta(b)\beta(a) + \beta(b)) = (n, \beta(a) + \beta(b)) | \lambda$. Therefore there is an x such that

$$x(\beta(a) + \beta(b)) + \lambda \equiv 0 \bmod n,$$

and for this x, (22) becomes

$$RS_1R^{-1} = T^{x(\beta(a)+\beta(b))+\lambda}S_1^{-1} = S_1^{-1}.$$

Denote by t the order of $S_1 = T^xS$. The group is given by the generators and relations

$$\langle R, T, S_1 \mid R^2 = 1, RTR^{-1} = T^{\beta(b)}, S_1TS_1^{-1} = T^{\beta(a)}, RS_1R^{-1} = S_1^{-1},$$
$$S_1^t = 1, T^n = 1 \rangle.$$

The group defined by the above generators and relations is a group of order $2nt$, therefore $t = m$ and the group G is isomorphic to the semidirect product

$$C_n \rtimes D_m,$$

where the action of D_m on C_n is determined by the function β.

5. $A_R = \{P_{1,i}\}_{0 \le i < m}$. In this case the set of places $P_{1,i}$, above p_1 are ramified in F/F_0 and the set of places $P_{2,i}$ above p_2 are decomposed. We may select an $R \in \pi^{-1}(b)$ such that $R^2 = T$ so $\mu = 1$. Moreover $\beta(b) \equiv 1 \bmod n$.

From Lemma 16 we have that $(\beta(b)\beta(a) + 1, n) = (\beta(a) + 1, n) | (\lambda + \beta(a))$. So there is an x such that

$$x(\beta(a) + 1) + \lambda \equiv -\beta(a) \bmod n,$$

and for this x Eq. (22) becomes

$$RS_1R^{-1} = T^{x(\beta(a)+\beta(b))+\lambda}S_1^{-1} = T^{-\beta(a)}S_1^{-1} = S_1^{-1}T^{-1}.$$

Because $T = R^2$, this relation is equivalent to

$$(RS_1)^2 = 1.$$

Denote by t the order of S_1. The group G admits the presentation:

$$G = \langle R, S_1 \mid R^{2n} = 1, S_1^t = 1, (RS_1)^2 = 1 \rangle.$$

Observe that the group generated by R^2 is the Galois group $\mathrm{Gal}(F/F_0)$ which is a normal subgroup of G. The quotient

$$\overline{G} := \frac{G}{\langle R^2 \rangle} = \langle \overline{R}, \overline{S}_1 \mid \overline{R}^2 = 1, \overline{S}_1^t = 1, \left(\overline{RS}_1\right)^2 = 1\rangle$$

is clearly isomorphic to a dihedral group of order $2t$. Hence the group G has order $2nt$ and $t = m$. ▮

We now show that those cases are realizable; i.e., we can select the divisor $D \in \mathscr{D}_n(G_0, A_R \subset A, \beta)$ to have degree 0 mod n. We will consider the cases:

1. We distinguish the subcases

- $n \equiv 2 \bmod 4$, $m \equiv 0 \bmod 2$. In this case, we must have the set A_R of fixed places of D_m in the support of D

$$A_R = \{P_{3,1}, P_{3,2}, P_{1,0}, P_{1,1}, \ldots, P_{1,i-1}, (P_{2,0}, P_{2,1}, \ldots, P_{2,i-1})\},$$

and of course s orbits $O(P_j, D_m)$ where P_j are not fixed by D_m. Recall that the action function β is trivial, so by taking $\lambda(Q) = 1$ for all $Q \in \mathrm{supp}(D)$, we have

$$\deg(D) = 2 + m + 2ms(+m).$$

Because $(2m, n) = 2$ which divides $2 + m(+m)$, we can choose s so that $\deg(D) \equiv 0 \bmod n$.

- $n \equiv 0 \bmod 4$, $m \equiv 0 \bmod 2$. In this case, we have the set A_R of fixed places of D_m in the support of D

$$A_R = \{P_{3,1}, P_{3,2}, P_{1,0}, P_{1,1}, \ldots, P_{1,i-1}\},$$

and s orbits $O(P_j, D_m)$ where P_j are not fixed by D_m. We take again $\lambda(Q) = 1$ for all Q in $\mathrm{supp}(D)$, so

$$\deg(D) = 2 + m + 2ms.$$

In this case $(2m, n) = 4$ which divides $2 + m$ (recall that because $(n, m) = 2$, $m \equiv 2 \bmod 4$), so we can choose s so that $\deg(D) \equiv 0 \bmod n$.

We can show similarly that we can choose $\deg(D) \equiv 0 \bmod n$ in the case $(n, m) = 1$.

2. In this case we have $A_R = \{P_{3,1}, P_{3,2}\}$. Decompose n into prime factors $n = p_1^{a_1} \cdots p_t^{a_t}$. According to Lemma 14 we write $n = n^+(\beta(b)) \cdot n^-(\beta(b))$, and $(n^+(\beta(b)), n^-(\beta(b))) = 1$ or 2. Equation (4), gives us $\deg(D) \equiv 0 \bmod p_i^{a_i}$ for every prime divisor p_i of $n^-(\beta(b))$, $p_i \neq 2$. If $2|n$,

and $p_{i_0} = 2$, then $\deg(D) \equiv 0 \mod p_{i_0}^{a'_{i_0}}$, where $a'_{i_0} = v_2(n^- \beta(b)) < a_{i_0}$. The arbitrary divisor $D \in \mathscr{D}_n(G_0, A_R \subset A, \beta)$ can be written in the form

$$D = \lambda(P_{3,1} + P_{3,2}) + \sum_{i=1}^{s} \lambda(P_i) \sum_{P \in O(P_i, D_m)} P.$$

We have to choose a D such that $\deg(D) \equiv 0 \mod n^+(\beta)$. We set $\lambda = \lambda(P_i) \equiv 1 \mod n$. We can choose the number s and the divisor $D \in \mathscr{D}_n(G_0, A_R \subset A, \beta)$, so that

$$\deg(D) = 2 + ms \equiv 0 \mod n^+(\beta),$$

because $(n^+(\beta), m) \mid 2$ (recall that $(n, m) \mid \beta(b) + 1$).

3. We have $A_R = \{P_{i,j} \mid i = 1, 2,\ j = 0, \dots, m-1\}$. In view of this we choose D to have s orbits $O(P_i, D_m)$ where P_i is not fixed by D_m, and, by taking $\lambda(Q_i) \equiv 1 \mod n$, we compute

$$\deg(D) = 2m + s2m.$$

We can choose an appropriate s so that the above degree is 0 mod n.

4. In this case, $A_R = \emptyset$ and the realization follows by Lemma 6.

5. In this case, $A_R = \{P_{1,0}, \dots, P_{1,m-1}\}$. Notice first that $\beta(b) \equiv 1 \mod n$. We decompose n into $n^+(\beta(a)), n^-(\beta(a))$ as in Lemma 14. By Eq. (4), we have $\deg(D) \equiv 0 \mod p_i^{a_i}$ for $p_i | n^-(\beta(a))$ and all divisors $D \in \mathscr{D}_n(G_0, A_R \subset A, \beta)$. So, we have to choose a D such that

$$\deg D \equiv 0 \mod n^+(\beta(a)) \text{ as well.}$$

By computation,

$$\deg D = m + 2ms \mod n^+(\beta(a)). \tag{27}$$

From Eq. (27) we obtain the necessary condition $(n^+(\beta(a)), 2m) \mid m$, for case 5 to be realizable. ▮

Case B. In this case, the characteristic of the field k is 2. We have that $G/C_n = D_m$, $(2, m) = 1$. By the characterization of the finite automorphism groups of the rational function field in Theorem 7, we deduce that two places p_1, p_2 of $F^G = F_0^{D_m}$ are ramified in $F_0/F_0^{D_m}$, with ramification indices 2 and m, respectively. Let $P_{1,i}$, $i = 1, \dots, m$ ($P_{2,j}$, $j = 1, 2$, resp.) be the set of places of F_0 above p (p_2, resp.).

THEOREM 17. *Let $G_0 = G/C_n$ be isomorphic to the dihedral group D_m, $p \nmid m$, $p = 2$. There are the following cases for the structure of G:*

1. $A_R \supset \{P_{1,i}\}_{0 \le i < m}$. *Then β is trivial and $G \cong C_n \times D_m$.*
2. $A_R = \{P_{2,j}\}_{j=1,2}$. *Then $G \cong C_{nm} \rtimes C_2$.*
3. $A_R = \emptyset$. *Then $G \cong C_n \rtimes D_m$.*

Proof. 1. $A_R \supset \{P_{1,i}\}_{0\le i<m}$, so the places $P_{1,i}$ $i=1,\dots,m$ above p_1 are ramified in the extension F/F_0. Observe also that the Galois group $\mathrm{Gal}(F/F_0^{\langle ba^i\rangle})$ of the extension $F/F_0^{\langle ba^i\rangle}$ is a group extension of the group $\langle ba^i\rangle \cong C_2$. By the study of extensions of elementary Abelian groups, we have that $\beta(ba^i)\equiv 1 \bmod n$, for all $i=0,\dots,m-1$ because the unique fixed point of ba^i is ramified in F/F_0. This holds for all i so the group G is a central extension of D_m by C_m. Because $n\equiv 1 \bmod 2$, we have that $H^2(D_m,C_n)=1$, therefore

$$G\cong C_n\times D_m.$$

2. $A_R=\{P_{2,j}\}_{j=1,2}$. In this case the places $P_{1,i}$ above p_1 are all decomposed in F/F_0, and the two places $P_{2,j}$ of F_0 above p_2 are ramified completely in F/F_0. $D_m(P_{2,j})=\langle a\rangle$, so by Corollary (10) we may find $S\in\pi^{-1}(a)$, which has order nm. The action of a on $\mathrm{Gal}(F/F_0)\cong\langle S^m\rangle$ is trivial, i.e., $\beta(a)\equiv 1 \bmod n$. Let $R\in\pi^{-1}(b)$. Observe that $|G:\langle S\rangle|=2$ so $\langle S\rangle\lhd G$. Therefore there is an r such that,

$$RSR^{-1}=S^r.$$

Observe that S^m generates the group $\mathrm{Gal}(F/F_0)\cong C_n$, so

$$S^{\beta(b)m}=RS^mR^{-1}=S^{mr},$$

therefore

$$\beta(b)=r \bmod n. \tag{28}$$

On the other hand we have

$$RSR^{-1}S=S^{r+1} \quad\Rightarrow\quad 1=\pi(RSR^{-1}S)=\pi(S^{r+1}),$$

so

$$r\equiv -1 \bmod m. \tag{29}$$

The system of (28), (29) has a solution r if and only if $(n,m)\mid(\beta(b)+1)$ and the group is given by the relations:

$$\langle R,S\mid R^2=1,\ S^{nm}=1,\ RSR^{-1}=S^r\rangle.$$

Notice that G is isomorphic to

$$G\cong C_{nm}\rtimes C_2.$$

3. In this case, all places, $P_{1,i}$, $P_{2,j}$ of F_0 above p_1 and p_2, respectively, are decomposed in F/F_0. Observe that $(n,2)=(m,2)=1$. We will use

the injection map of Proposition 8, namely, the map

$$H^2(D_m, C_n) = \bigoplus_{p|2m} H^2(D_m, C_n)_p \to \bigoplus_{p|2m} H^2(H_p, C_n)$$

$$\alpha = \sum \alpha_p \mapsto \sum \mathrm{res}_{D_m \to H_p}(\alpha_p).$$

Because $(n, 2) = 1$ we have $H^2(H_2, C_n) = 1$ by Zassenhaus theorem. If $p \neq 2$, $p|m$ then the p-Sylow subgroup is a subgroup of the cyclic subgroup $\langle a \rangle \cong C_m$ of D_m. Because $\langle a \rangle$ fixes $P_{2,j}$, which decomposes in F/F_0, the subextension

$$1 \to C_n \to \pi^{-1}(\langle a \rangle) \to \langle a \rangle \to 1,$$

splits. All subextensions corresponding to the p-Sylow subgroups of $\langle a \rangle$ split as well, so $H^2(H_p, C_n) = 1$ for $p \neq 2$. This implies that $H^2(D_m, C_n) = 1$ and finally

$$G \cong C_n \rtimes D_m,$$

where the semidirect action of D_m onto C_n is determined by the function β. ▮

To prove that the above three ramification types are realizable we have to select a $D \in \mathscr{D}_n(G_0, A_R \subset A, \beta)$ of degree 0 mod n. We will distinguish the cases:

1. We take s orbits $O(P_i, D_m)$, such that P_i are not fixed by D_m and $\lambda(P_i) \equiv 1 \bmod n$. We have $A_R = \{P_{1,1}, \dots, P_{1,m}, (P_{2,1}, P_{2,2})\}$ so the degree of D is

$$\deg D = m + (+2) + 2ms.$$

Obviously, because $(2m, n) = (n, m)$ we can find an s such that $\deg D \equiv 0 \bmod n$ in the case $A_R = \{P_{1,1}, \dots, P_{1,m}\}$. If $A_R = \{P_{1,1}, \dots, P_{1,m}, P_{2,1}, P_{2,2}\}$, we arrive at $(n, m) \mid 2$ as a necessary condition for this type to be realizable. Notice that the condition $(n, m) \mid 2$ is equivalent to $(n, m) = 1$ because $(n, 2) = (m, 2) = 1$.

2. By Lemma 5, it is enough to construct a D of degree 0 mod $n^+(\beta(b))$. We take s orbits $O(P_i, D_m)$, where P_i are not fixed by D_m and we set $\lambda(P) \equiv 1 \bmod n$ for all P in $\mathrm{supp}(D)$. We have then

$$\deg(D) = 2 + 2ms \bmod n^+(b).$$

We can take s such that $\deg(D) \equiv 0 \bmod n^+(b)$, because $(n, 2) = (n^+(b), 2) = 1$.

3. The ramification type of this case is realizable by Lemma 6, because $A_R = \emptyset$.

4.6. *The Group A_4 as Quotient Group*

In this section suppose that $G/C_n \cong A_4$. From the classification theorem 7 we have that three places of $F_1 := F^G = F_0^{A_4}$ are ramified in F_0/F_1, namely, p_1, p_2, p_3 with ramification indices $e_1 = 2$, $e_2 = e_3 = 3$, respectively. Moreover the characteristic is not 2 or 3. Denote by $P_{1,i}$, $i = 1, \ldots, 6$, $P_{2,j}$, $P_{3,j}$, $j = 1, \ldots, 4$ the set of places of F_0 lying over p_1, p_2, p_3, respectively.

The group A_4 admits the presentation in terms of generators and relations:

$$A_4 = \langle a, b \mid a^2 = b^3 = 1, (ab)^3 = 1 \rangle.$$

Notice also that the group A_4 has a normal 2-Sylow subgroup isomorphic to the Klein group V_4, which, as a subgroup of A_4, can be expressed in terms of the generators of A_4 as

$$V_4 = \{1, a, bab^{-1}, b^2ab^{-2}\}.$$

The group A_4 can be written as a semidirect product $A_4 \cong V_4 \rtimes \langle b \rangle$. The action map

$$\beta \colon A_4 \to \mathbb{Z}_n^*$$

cannot be injective, because A_4 is not Abelian. We have two possibilities for $\ker \beta$:

$$\ker \beta = V_4, \quad \text{or} \quad \ker \beta = A_4 \text{ (central extension)}.$$

In any case, because $A_4/V_4 \cong \mathbb{Z}_3$ and a has order 2 in A_4, we have that $\beta(a) \equiv 1 \bmod n$.

THEOREM 18. *If $G_0 = G/C_n \cong A_4$ then the group of automorphisms G is isomorphic to*:

(a) $G \cong C_n \rtimes A_4$ *if* $A_R = \emptyset$.

(b) $G \cong V_4 \rtimes C_{3n}$ *if* $A_R = \{P_{2,j}\}_{1 \le j \le 4}$

(c) $G \cong G' \rtimes C_3$ *if* $A_R = \{P_{1,i}\}_{1 \le i \le 6}$. *Here G' is defined in terms of generators and relations*

$$G' := \langle R, S \mid R^2 = S^2, S^{2n} = 1, RSR^{-1} = S^\tau \rangle.$$

(d) *G admits the following representation in terms of generators and relations*:

$$G = \langle R, S \mid R^{2n} = 1, R^2 = S^3, (RS)^3 = R^{2k} \rangle,$$

for some integer $k \in \{1, \ldots, n\}$, if $\{P_{1,i}\}_{i=1,\ldots,6} \not\subseteq A_R$.

(a) $A_R = \emptyset$; i.e., all places of F_0 above p_1, p_2, p_3 are decomposed in F/F_0. We claim that in this case

$$G \cong C_n \rtimes A_4,$$

where the action of A_4 on C_n is determined by β. To prove this we observe that A_4 is the semidirect product of $V_4 \rtimes \langle b \rangle$ and obviously V_4 is an elementary Abelian group of the form $\mathscr{E}_2(2)$. Now according to the study of the dihedral case, because the fixed places of $V_4 = D_2$ are decomposed, we have that the subextension

$$1 \to C_n \to \pi^{-1}(V_4) \to V_4 \to 1 \tag{30}$$

splits, so by Lemma 13 $G \cong C_n \rtimes A_4$.

(b) $A_R = \{P_{2,j}\}_{1 \le j \le 4}$ or $A_R = \{P_{3,j}\}_{1 \le j \le 4}$, hence the set of six places $P_{1,i}$, $i = 1, \ldots, 6$ are decomposed and at least one of the set of the places $P_{2,j}, P_{3,j}$, say $P_{2,j}$, $j = 1, \ldots, 4$ is ramified in F/F_0. According to Corollary 10, because the fixed places of b are ramified, we have that $\beta(b) \equiv 1 \bmod n$ so the extension is central. A_4 is a semidirect product of $V_4 \rtimes \langle b \rangle$ and as in case (a) we have that the short exact sequence (30) splits. Using Lemma 13 we have that

$$G \cong V_4 \rtimes C_{3n}.$$

Let R be the generator of the cyclic group C_{3n}. The conjugation action of R on V_4 induces a homomorphism ρ: $C_{3n} \to S_3$. Because $R^n = b$, and $\rho(b)$ is cycle of order 3 in S_3, we have that $\rho(R)$ must be also a cycle of order 3, therefore $(n, 3) = 1$.

(c) $A_R = \{P_{1,i}\}_{1 \le i \le 6}$, hence the set of places $P_{1,i}$, $i = 1, \ldots, 6$ are ramified and the set of places $P_{i,j}$, $i = 1, 2$, $j = 1, \ldots, 4$ are decomposed. Then by the study of dihedral extensions we have that the group $G' := \pi^{-1}(V_4)$ is given in terms of generators and relations by

$$G' = \langle R, S \mid R^2 = S^2, S^{2n} = 1, RSR^{-1} = S^r \rangle.$$

Here r is the unique solution of the system $r \equiv 1 \bmod n$, $r \equiv -1 \bmod 2$ if $(n, 2) = 1$, and the unique solution of the system $r \equiv 1 \bmod n$, $r \equiv -1 \bmod 2$ such that $(r + 1)/2$ is even, otherwise. Notice also that in the case $(n, 2) = 2$ this ramification type appears only if $n \equiv 2 \bmod 4$. We claim that $G \cong G' \rtimes \langle b \rangle \cong G' \rtimes C_3$. Observe that $G' \lhd G$ because $V_4 \lhd A_4$. On the other hand, by Corollary 10 the subextension

$$1 \to C_n \to \pi^{-1}(\langle b \rangle) \to \langle b \rangle \to 1 \tag{31}$$

splits, therefore there is a homomorphism

$$j \colon \langle b \rangle \hookrightarrow C_n \rtimes \langle b \rangle \hookrightarrow G,$$

such that $j(\langle b \rangle) \cap C_n = \{1\}$. To prove our claim we have to show that $j(\langle b \rangle) \cap G' = 1$. Let $x \in j(\langle b \rangle) \cap G'$. If $x \neq 1$ then $x \in j(\langle b \rangle)$ has order 3. On the other hand notice that the square of every element in G' is in $\langle S \rangle$. This implies that for x, which is written in the form $R^i S^j$, we have $x^3 = xx^2 = R^i S^j S^k$ so $x \in \langle S \rangle$ and $x^2 \in C_n$. Because $j(\langle b \rangle) \cap C_n = \{1\}$ we have $x^2 = 1$ and $x = 1$ because $(2, 3) = 1$.

(d) $\{P_{1,i}\}_{i=1,\dots,6} \not\subseteq A_R$, hence all places $P_{1,i}$, $i = 1, \dots, 6$ and at least one set of places among the $P_{2,j}$ and $P_{3,j}$, $j = 1, \dots, 4$ are ramified in the extension F/F_0. (Recall that the set of places $P_{2,j}$ and $P_{3,j}$ have different ramification type if and only if $(3, n) = 1$.) Moreover from the study of dihedral extensions, if $(n, 2) = 2$ then $n \equiv 2 \bmod 4$. Assume that $P_{1,1}$ is fixed by a and that $P_{2,1}$ is fixed by b. Using Corollary 10, we deduce that the function β is trivial, so the extension is central, and moreover there are elements $R \in \pi^{-1}(a)$ and $S \in \pi^{-1}(b)$ such that

$$\langle R \rangle \cong C_{2n}, \qquad \langle S \rangle \cong C_{3n}.$$

The group $\mathrm{Gal}(F/F_0) \cong C_n$ is a common subgroup of $\langle R \rangle, \langle S \rangle$ so by choosing suitable generators R, S we have the relations between R, S

$$R^{2n} = 1, \qquad R^2 = S^3.$$

Denote by π the projection $G \to G/C_n$. Because $\pi(RS) = ab$ has order 3 in A_4 we have the additional relation $(RS)^3 = R^{2k}$ between R, S. Let G_1 be the group

$$G_1 := \langle R, S \mid R^{2n} = 1,\, R^2 = S^3,\, (RS)^3 = R^{2k} \rangle. \tag{32}$$

Obviously $\langle R^2 \rangle$ is a normal subgroup of G_1 and $G_1/\langle R^2 \rangle \cong A_4$ so $G_1 \cong G$. We prove that there is only one solution to the extension problem with the ramification type of case (d), so there is only one group defined by the relations of (32). Unfortunately we could not find a neat formula for k. However, using the computer algebra package MAGMA [Ma] we can then compute k for several values of n. Thus,

n	2	3	5	6	7	9	10	11	13	14	15	17	18	19
k	1	1	5	1	6	7	5	8	9	6	10	11	7	12

.

In order to prove that there is only one solution to the extension problem in case (d), we count the number $i(A_4, C_n)$ of nonisomorphic groups G, obtained by extending the group A_4 by C_n. Because the extension in case (d) is central we have

$$H^2(A_4, C_4) \cong \mathbb{Z}_{(n,2)} \times \mathbb{Z}_{(n,3)}.$$

In case $(n,3) = (n,2) = 1$, the above formula implies that the extension splits and the group G is isomorphic to $C_n \times A_4$. In case $(n,2) = 1$, $(n,3) = 3$, the subextension

$$1 \to C_n \to \pi^{-1}(V_4) \to V_4 \to 1$$

splits by Zassenhaus theorem, so according Lemma 13, we have two possibilities for G, namely,

$$G \cong C_n \rtimes A_4 \quad \text{or} \quad G \cong V_4 \rtimes C_{3n}.$$

In case that $(n,2) = 2$, $(n,3) = 1$, we have $H^2(A_4, C_n) \cong \mathbb{Z}_2$. The two groups appearing here are isomorphic to the two groups of case (c).

Suppose now that $(n,2) = 2$, $(n,3) = 3$. We prove that the number of nonisomorphic central extensions of A_4 by C_4 is $i(A_4, C_4) = 4$. Let us write $n = 2^a 3^b m$ with $(m,2) = (m,3) = 1$. There are only two nonisomorphic extensions G_i', $i = 1,2$ of the form

$$1 \to C_{3^b m} \to G_i' \to A_4 \to 1,$$

as we have seen in the case that $(n,2) = 1$, $(n,3) = 3$. The group G is given by an extension of G_i', namely,

$$1 \to C_{2^a} \to G \to G_i' \to 1.$$

We claim that G has two possibilities for each selection of G_i', $i = 1,2$. Indeed,

$$H^1(C_{3^b m}, C_{2^a}) = \operatorname{Hom}(C_{3^b m}, C_{2^a}) \cong 0,$$

so the sequence (restriction-inflation) is exact

$$0 \to H^2\left(\frac{G_i'}{C_{3^b m}}, C_{2^a}\right) \to H^2(G_i', C_{2^a}) \to H^2(C_{3^b m}, C_{2^a}) \cong 0,$$

which implies that $H^2(G_i', C_{2^a}) \cong \mathbb{Z}_2$ because

$$H^2\left(\frac{G_i'}{C_{3^b m}}, C_{2^a}\right) = H^2(A_4, C_{2^a}) \cong \mathbb{Z}_2.$$

In order to prove that the ramification type of case (b) is realizable we have to find a divisor $D \in \mathcal{D}_n(A_4, A_R \subset A, \beta)$ of degree 0 mod n. We consider the cases:

(a) $A_R = \emptyset$. The ramification type of this case is realizable by Lemma 6.

(b) If $A_R = \{P_{2,1}, \dots, P_{2,4}, P_{3,1}, \dots, P_{3,4}\}$ we take s orbits $O(P_i, A_4)$ where P_i is not fixed by A_4 and we set $\lambda(P_i) \equiv 1 \bmod n$, $\lambda(P_{2,j}) \equiv -\lambda(P_{3,j}) \bmod n$. So, $\deg(D) = 12s$ and we can select an s such that $\deg(D) \equiv 0 \bmod n$. If $A_R = \{P_{2,1}, \dots, P_{2,4}\}$ we take s orbits $O(P_i, A_4)$ where P_i is not fixed by A_4 and we set $\lambda(P) \equiv 1 \bmod n$ for all $P \in \mathrm{supp}(D)$. The degree of D is

$$\deg(D) = 4 + 12s.$$

Therefore, because $(n, 3) = 1$ we have that $(n, 12) \mid 4$, so we can find an s such that $D \equiv 0 \bmod n$.

(c) In this case $A_R = \{P_{1,1}, \dots, P_{1,6}\}$. Let n_0 be the part of n such that

$$\beta(b) \equiv 1 \bmod n_0.$$

By Lemma 5 it is enough to prove that $\deg(D) \equiv 0 \bmod n_0$. Take s orbits $O(P_i, A_4)$ where P_i is not fixed by A_4 and put $\lambda(P) \equiv 1 \bmod n$ for all $P \in \mathrm{supp}(D)$. By computation

$$\deg(D) = 6 + 12s.$$

Because $n \equiv 2 \bmod 4$ or $n \equiv 1 \bmod 2$ we have that $(n_0, 12) \mid 6$, so we can find an s such that $\deg(D) \equiv 0 \bmod n_0$.

(d) We take s orbits $O(P_i, A_4)$ where P_i are not fixed by D_m. If $A_R = \{P_{1,1}, \dots, P_{1,6}, P_{2,1}, \dots, P_{2,4}\}$ then we set $\lambda(P_{1,i}) \equiv 1 \bmod n$ for $i = 1, \dots, 6$, and $\lambda(P_{2,j}) \equiv -1 \bmod n$ for $j = 1, \dots, 4$. If

$$A_R = \{P_{1,1}, \dots, P_{1,6}, P_{2,1}, \dots, P_{2,4}, P_{3,1}, \dots, P_{3,4}\},$$

then we set $\lambda(P_{1,i}) \equiv 1 \bmod n$ and $\lambda(P_{2,i}) \equiv -\lambda(P_{3,i}) \bmod n$, $i = 1, \dots, 6$, $j = 1, \dots, 4$. The degrees of the above divisors are

$$\deg(D) = 2 + 12s \quad \text{and} \quad \deg(D) = 6 + 12s.$$

We can select an s such that $\deg(D) \equiv 0 \bmod n$. Indeed, as in cases (b) and (c) we notice that $n \equiv 2 \bmod 4$ or $n \equiv 1 \bmod 2$ and, if the places $P_{3,1}, \dots, P_{3,4}$ are not ramified in F/F_0 then $(n, 3) = 1$ by Remark 2.

4.7. *The Group A_5 as a Quotient Group*

The group A_5 appears as a group of automorphisms of the rational function field with the following ramification types, which we handle together:

(a) In $F_0/F_0^{A_5}$ three places p_1, p_2, p_3 of $F_0^{A_5}$ are ramified, with ramification indices $e_1 = 2$, $e_2 = 3$, $e_3 = 5$, respectively. The characteristic is $p \neq 2, 3, 5$.

(b) In $F_0/F_0^{A_5}$ two places p_1, p_2 are ramified with ramification indices $e_1 = 6$, $e_2 = 5$, respectively. In this case the characteristic $p = 3$.

In this section we will prove:

THEOREM 19. *Let $G_0 = G/C_n$ be isomorphic to A_5. The cohomological class $\alpha \in H^2(A_5, C_n)$ describing G can be determined by the cohomology class corresponding to the subextension of a 2-Sylow subgroup H_2.*

If $(n, 2) = 1$ or all places of F_0 above p_1 are decomposed in F/F_0 then $G \cong C_n \times A_5$. Otherwise G admits a presentation in terms of generators and relations as:

$$\Big\langle X, Y, Z, T \mid T^n = X^3 = 1, Y^2 = T, Z^2 = T, (XY)^3 = T^l, (YZ)^3 = T^o,$$
$$(XZ)^2 = T^m, XTX^{-1} = T, ZTZ^{-1} = T, YTY^{-1} = T \Big\rangle,$$

for some integers $m, l, o \in \{1, \dots, n\}$.

Proof. A_5 is a simple non-Abelian group so the action homomorphism

$$\beta \colon A_5 \to \mathbb{Z}_n^*$$

is trivial and the extension

$$1 \to C_n \to G \overset{\pi}{\to} A_5 \to 1 \tag{33}$$

central. We have computed that $H^2(A_5, C_n) \cong \mathbb{Z}_{(n,2)}$. If n is odd then

$$G \cong C_n \times A_5.$$

Suppose now that n is even. By Proposition 8 the restriction map

$$\mathbb{Z}_2 \cong H^2(A_5, C_n) = H^2(A_5, C_n)_{(2)} \overset{1-1}{\to} H^2(H_2, C_n) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2,$$
$$\alpha \mapsto \operatorname{res}_{A_5 \to H_2}(\alpha) \tag{34}$$

is injective, where $H_2 \cong V_4$ is the 2-Sylow subgroup of A_5. This proves that we can determine the structure of the extension of A_5, by computing the structure of the subextension of a 2-Sylow subgroup. The 2-Sylow subgroup of A_5 is isomorphic to V_4. We consider the two cases:

1. All places above p_1 are decomposed in the extension F/F_0. By the study of extensions of dihedral groups we have that, $\pi^{-1} \cong C_n \times V_4$, hence $G \cong C_n \times A_5$.

2. All places above p_1 are ramified in extension F/F_0. By the study of dihedral extensions, this is possible only if $n \equiv 2 \bmod 4$. We would like to write a presentation for G in terms of generators and relations. The group A_5 admits the presentation [Hu, p. 138]:

$$A_5 = \langle x, y, z \mid x^3 = y^2 = z^2 = (xy)^3 = (yz)^3 = (xz)^2 \rangle. \tag{35}$$

Let T be a generator of the cyclic group C_n. The decomposition group of all places of F which extend p_1 have a cyclic subgroup of order $2n$. Let X,Y be elements of order $2n$, such that $\pi(X) = x$, $\pi(Y) = y$. We can select X, Y such that $Y^2 = X^2 = T$. By applying π to products of X, Y and using the relations of A_5 given in (35) we arrive at the presentation of G:

$$\Big\langle X, Y, Z, T \mid T^n = X^3 = 1, Y^2 = T, Z^2 = T, (XY)^3 = T^l, (YZ)^3 = T^o,$$
$$(XZ)^2 = T^m, XTX^{-1} = T, ZTZ^{-1} = T, YTY^{-1} = T\Big\rangle,$$

where $m, l, o \in \{1, \ldots, n\}$. One can compute m, l, o using the presentation of $\pi^{-1}(V_4)$ in terms of generations and relations. It is difficult to do this sort of computation generically. However, using MAGMA [Ma] symbolic algebra package we can calculate the values of m, l, o for certain n: For all values of n we have tried it turns out that we can take $m = 1 = l = 1$ for $n = 2$ and $m = 1$, $o = 3$, $l = 2 + (n - 2)/4$ for $n > 2$, $n \equiv 2 \bmod 4$. ▮

Let D be an arbitrary divisor in $\mathscr{D}_n(A_5, A_R \subset A, \beta)$

$$D = \sum_{i=1}^{3} a_i \sum_{P \mid p_i} P + \sum_{i=1}^{s} \lambda(P_i) \sum_{P \in O(P_i, A_5)} P,$$

where $a_i = 0$ if the places above p_i are not in A_R and $0 < a_i = \lambda(P_{i,j}) < n$ if the places of F_0 above p_i are in A_R, $P_{i,j}$ is an arbitrary place over p_i. The degree of D in case (a) is

$$\deg(D) = a_1 30 + a_2 20 + a_3 12 + 60 \sum_{i=1}^{s} \lambda_i(P_i).$$

This gives us

$$(60, n) \mid (a_1 30 + a_2 20 + a_3 12),$$

as a necessary and sufficient condition for the ramification type A_R to be realizable. Similarly in case (b) we have the condition

$$(60, n) \mid (a_1 10 + a_2 12),$$

as a necessary and sufficient condition for the ramification type A_R to be realizable.

4.8. *The Group S_4 as a Quotient Group*

In this section suppose that $G/C_n \cong S_4$. This case appears in characteristics $p \neq 2, 3$. In the extension $F_0/F_0^{S_4}$ three places q_1, q_2, q_3 of F_0 are ramified, with ramification indices $e_1 = 2$, $e_2 = 3$, $e_3 = 4$. Let $\{P_{1,i}\}_{1 \leq i \leq 12}$, $\{P_{2,j}\}_{1 \leq j \leq 8}$, $\{P_{3,k}\}_{1 \leq k \leq 6}$ be the sets of places of F_0 which are above q_1, q_2, q_3, respectively. S_4 admits the presentation in terms of generators and relations,

$$S_4 = \langle x, y \mid y^2, x^4, \left(x^{-1}y\right)^3 = 1\rangle, \tag{36}$$

and as one checks A_4 is the subgroup of S_4 generated by x^2, yx.

The ramification of S_4 compared to the ramification of A_4 is given in the diagram:

$$\begin{array}{ccccc}
F_0 & P_{1,1}, \ldots, P_{1,12} & P_{2,1}, \ldots, P_{2,8} & P_{3,1}, \ldots, P_{3,6} \\
| & \backslash/ & {}^3\backslash/ \quad \backslash/^3 & \backslash/^2 \\
F_0^{A_4} & * & p_2 \quad p_3 & p_1 \\
| & |^2 & \backslash/ & |^2 \\
F_0^{S_4} & q_1 & q_2 & q_3
\end{array}$$

THEOREM 20. *Let $G/C_n = G_0$ be isomorphic to the symmetric group S_4. Then there are the cases for the group of automorphisms of G.*

(a) $\{P_{1,i}\}_{1 \leq i \leq 12} \cup \{P_{3,k}\}_{1 \leq k \leq 6} \subset A_R$. *The action of S_4 on C_n is trivial. If $(n, 2) = 1$ then $G \cong C_n \times S_4$ and if $(n, 2) = 2$, $n \equiv 2 \bmod 4$ then G admits the presentation in terms of generators and relations*

$$G = \langle X, Y, T \mid T^n = 1, Y^2 = X^4 = XTX^{-1} = YTY^{-1} = T, \\ \left(X^{-1}Y\right)^3 = T^k\rangle,$$

for some $k \in \{1, \ldots, n\}$.

(b) *$G \cong C_n \rtimes S_4$ in all other cases.*

Proof. The map Φ of Proposition 8:

$$H^2(S_4, C_n) = \bigoplus_{p=2,3} H^2(S_4, C_n) \overset{\Phi}{\to} H^2(H_2, C_n) \oplus H^2(H_3, C_n)$$

$$\alpha = \alpha_2 + \alpha_3 \mapsto \mathrm{res}_{S_4 \to H_2}(\alpha_2) + \mathrm{res}_{S_4 \to H_3}(\alpha_3)$$

is injective, where H_2 (resp., H_3) is any 2-Sylow subgroup (resp., 3-Sylow). We will prove

LEMMA 21. *If $G/C_n \cong S_4$, then the map,*

$$H^2(S_4, C_n) \to H^2(H_2, C_n)$$

$$\alpha = \alpha_2 + \alpha_3 \mapsto \mathrm{res}_{S_4 \to H_2}(\alpha_2)$$

is injective.

Proof. If $A_R \supset \{P_{2,j}\}_{1 \le j \le 8} \cup \{P_{3,k}\}_{1 \le k \le 6}$ or $A_R \supset \{P_{1,i}\}_{1 \le i \le 12}$ then the action of S_4 on C_n is trivial, so $H^2(S_4, C_n) = \mathbb{Z}_{(2,n)} \times \mathbb{Z}_{(2,n)}$. If $A_R \cap \{P_{2,j}\}_{1 \le j \le 8} = \emptyset$ then by the study of extensions of cyclic groups, we have $\mathrm{res}_{S_4 \to H_3}(\alpha) = 0$. Finally if $A_R \supset \{P_{2,j}\}_{1 \le j \le 8}$ and $A_R \cap \{P_{3,k}\}_{1 \le k \le 6} = \emptyset$, then by the study of case (b) of extension of A_4 we have that $(n, 3) = 1$, so $H^2(H_3, C_n) = 0$. ∎

This proves that the structure of G is determined by the structure of the subextension

$$1 \to C_n \to \pi^{-1}(D_4) \to D_4 \to 1.$$

We have the tower of field extensions:

$$\begin{tikzcd}
F_0 \arrow[d, dash] & & P_{1,1}, \dots, P_{1,12} \arrow[dl, dash, "2"'] \arrow[dr, dash] & & P_{2,1}, \dots, P_{2,8} \arrow[d, dash] & & P_{3,1}, \dots, P_{3,6} \arrow[dl, dash, "2"'] \arrow[dr, dash, "4"] & \\
F_0^{D_4} \arrow[d, dash, "3"'] & p'_1 \arrow[dr, dash, "1"'] & & * \arrow[dl, dash, "2"] & * \arrow[d, dash, "3"'] & p'_2 \arrow[dr, dash, "2"'] & & p'_3 \arrow[dl, dash, "1"] . \\
F_0^{S_4} & & q_1 & & q_2 & & q_3 &
\end{tikzcd}$$

The ramification of q_2 of the extension $F_0/F_0^{S_4}$ does not affect the ramification type in the extension $F_0/F_0^{D_4}$. We have to consider the cases:

(1) $A_R \cap \{P_{1,i}\}_{1 \le i \le 12} = \emptyset$ and $\{P_{3,k}\}_{1 \le k \le 6} \subset A_R$ or $A_R \cap \{P_{3,k}\}_{1 \le k \le 6} = \emptyset$ and $\{P_{1,i}\}_{1 \le i \le 12} \subset A_R$.

In both of the above cases, the action of S_4 on C_n is trivial. Moreover $y \in S_4$ fixes a place of F_0 above q_1 and a place of F_0 above q_3. Hence by Remark 4 we have that $(n,2) = 1$. Therefore, $H^2(S_4, C_n) = 0$, so $G \cong C_n \times S_4$.

(2) $A_R \cap \{P_{1,i}\}_{1 \le i \le 12} = A_R \cap \{P_{3,k}\}_{1 \le k \le 6} = \emptyset$. In this case by the study of dihedral extensions we have $\operatorname{res}_{S_4 \to D_4}(\alpha) = 0$, hence $\alpha = 0$ and $G \cong C_n \rtimes S_4$.

(3) $\{P_{1,i}\}_{1 \le i \le 12} \cup \{P_{3,k}\}_{1 \le k \le 6} \subset A_R$. In this case the action of S_4 on C_n is trivial. Hence if $(n,2) = 1$ then $G \cong C_n \times S_4$. If $(n,2) = 2$ then by the study of dihedral extensions, this case appears only if $n \equiv 2 \bmod 4$. Let T be a generator of the cyclic group C_n. Consider elements X, Y in G of orders $4n$ and $2n$, respectively, such that $\pi(X) = x$ and $\pi(Y) = y$. We can choose X, Y such that $X^4 = T$ and $Y^2 = T$. Moreover we have the relations $XTX^{-1} = T$ and $YTY^{-1} = T$. Applying π to the products of X, Y and using the presentation (36) we arrive at the presentation of G,

$$G = \langle X, Y, T \mid T^n = 1, Y^2 = X^4 = XTX^{-1} = YTY^{-1} = T,$$
$$(X^{-1}Y)^3 = T^k \rangle,$$

for some $k \in \{1, \dots, n\}$. Although the structure of G can be determined by the structure of $\pi^{-1}(V_4)$ it is very difficult to compute k generically. Using MAGMA [Ma] we can compute k for several n, $n \equiv 2 \bmod 4$. It turns out that $k = 2 + (n-2)/4$. ∎

In order to prove that the above ramification types are realizable we have to find a divisor $D \in \mathscr{D}_n(S_4, A_R \subset A, \beta)$ with $\deg D \equiv 0 \bmod n$. As in the A_5 case we have that the condition

$$(n_0, 24) \mid (a_1 12 + a_2 8 + a_3 6)$$

is sufficient and necessary for $\deg(D) \equiv 0 \bmod n_0$, where $a_i = 0$ if the places $P_{i,j}$ of F_0 which are above p_i do not ramify in extension F/F_0 and $a_i = \lambda(P_{i,j}) \neq 0$, otherwise.

4.9. *The Matrix Groups $PSL(2,q)$ and $PGL(2,q)$ as a Quotient Group*

In this case $G_0 = G/C_n$ is isomorphic to $PSL(2,q)$ or to $PGL(2,q)$. In extension $F_0/F_0^{G_0}$ only two places p_1, p_2 are ramified. It is very complicated to give a presentation of G in terms of generators and relations because as far as the author knows, there is no general presentation of the matrix groups $PSL(2,q)$ and $PGL(2,q)$ in terms of generators and relations. However, we can prove:

THEOREM 22. *Let $G_0 = G/C_n$ be isomorphic to $PSL(2,q)$ or $PGL(2,q)$, where q is a power of the characteristic. The cohomology class $\alpha \in H^2(G_0, C_n)$ is determined by the restriction* $\mathrm{res}_{G_0 \to H_2}(\alpha)$ *to a 2-Sylow subgroup H_2. In particular, when $(n,2) = 1$, or when the places of F_0 which extend p_1, p_2 are decomposed in extension F/F_0 then $G \cong C_n \rtimes G_0$.*

Proof. We need:

LEMMA 23. *For $G_0 = PSL(2,q)$, $PGL(2,q)$, $H^2(G_0, C_n)$ is a 2-group.*

Proof. We have the two cases:

Case 1. $G_0 = PSL(2,q)$, $(q,2) = 1$ or $G_0 = PGL(2,2^f) = PSL(2,2^f)$. Because $PSL(2,q)$, where $q = p^f$ is a power of the characteristic, is simple, the action of G_0 on C_n is trivial. We have

$$H^2\big(PSL(2,q), C_n\big) \cong \begin{cases} \mathbb{Z}_{(2,n)} & \text{if } p^f \neq 9 \\ \mathbb{Z}_{(6,n)} & \text{if } p^f = 9. \end{cases}$$

Observe that if $p^f = 9$ then $(n,6) = (n,2)$ because we have assumed that the characteristic p does not divide n, so $H^2(PSL(2,q), C_n) = \mathbb{Z}_{(2,n)}$.

Case 2. $G_0 = PGL(2,q)$, $(q,2) = 1$. The kernel of the action homomorphism

$$\beta \colon PGL(2,q) \to \mathbb{Z}_n^*$$

is either $\ker\beta = PGL(2,q)$ or $\ker\beta = PSL(2,q)$. In the first case the extension is central and $H^2(PGL(2,q), C_n) = \mathbb{Z}_{(n,2)} \times \mathbb{Z}_{(n,2)}$. Observe that

$$H^1\big(PSL(2,q), C_n\big) \cong \mathrm{Hom}\big(PSL(2,q), C_n\big) = 0,$$

because $PSL(2,q)$ is simple and non-Abelian. We write the inflation-restriction sequence

$$0 \to H^2\left(\frac{PGL(2,q)}{PSL(2,q)}, C_n\right) \to H^2\big(PGL(2,q), C_n\big)$$
$$\to H^2\big(PSL(2,q), C_n\big) \cong \mathbb{Z}_{(2,n)},$$

and because $PGL(2, q)/PSL(2, q) \cong \mathbb{Z}_2$ we deduce that $H^2(PGL(2,q), C_n)$ is a 2-group. ▮

We return now to the proof of Theorem 22. The monomorphism Φ of Proposition 8:

$$H^2(G_0, C_n) = \bigoplus_{t|q(q^2-1)} H^2\big(PGL(2,q), C_n\big)_{(t)} \xrightarrow{\Phi} \bigoplus_{t\text{-Sylow}} H^2(H_t, C_n),$$

where H_t runs over the t-Sylow subgroups of G_0 is injective so the restriction map

$$H^2(G_0, C_n) \to H^2(H_2, C_n)$$
$$\alpha \mapsto \beta = \mathrm{res}_{G_0 \to H_2}(\alpha)$$

is injective as well. The 2-Sylow subgroup H_2 is isomorphic to a dihedral group D_{2^K}, of order 2^{K+1}, where $K = \max\{v_2(e_1), v_2(e_2)\}$.

Moreover, if $(n, 2) = 2$ then the cohomology group vanishes, so $G \cong C_n \rtimes G_0$, and by the study of dihedral extensions we have that if all places of F_0 above p_1, p_2 are decomposed in the extension F/F_0, then $\beta = \mathrm{res}_{G_0 \to H_2}(\alpha) = 1$, so $G \cong C_n \rtimes G_0$ as well. ▮

Let D be a divisor in $\mathscr{D}_n(G_0, A_R \subset A, \beta)$, and n_0 the greatest divisor of n, such that $\beta(\sigma) \equiv 1 \bmod n_0$. According to Lemma 6 we have that $\deg(D) \equiv 0 \bmod n \Leftrightarrow \deg(D) \equiv 0 \bmod n_0$. Therefore the condition

$$\big(n_0, q(q-1)(q+1)\big) \mid \big(a_1 q(q-1) + a_2(q+1)\big)$$

is necessary and sufficient for $\deg(D)$ to be congruent to 0 mod n_0, where $a_i = 0$ if the places of F_0 above p_i are in A_R and $a_i = \lambda(P)$, $P|p_i$ otherwise.

ACKNOWLEDGMENTS

I express my gratitude to my advisor, Jannis A. Antoniadis, for his continued support guidance and encouragement. I also thank the Greek National Scholarship Foundation (I.K.Y.) for their financial support.

REFERENCES

[Ac] R. D. M. Accola, Strongly branched coverings of closed Riemann surfaces, *Proc. Amer. Math. Soc.* **26** (1970), 315–322.

[A-C] E. Arbarello and M. Cornalba, Footnotes to a paper of Beniamino Segre, *Math. Ann.* (1981), 341–362.

[Br] R. Brandt, ‘‘Über die Automorphismengruppen von Algebraischen Funktionenkörpern,’’ Ph.D. dissertation, Universität-Gesamthochschule Essen, 1988.

[B-S] R. Brandt and H. Stichtenoth, Die Automorphismen hyperelliptischer Kurven, *Manuscripta Math*. **55** (1986), 83–92.

[B-R] V. Gonzalez and R. Rodriguez, On automorphism of curves and linear series, *in* ‘‘Complex Geometry Seminar,’’ Vol. III, Chile, 1994.

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

[Hu] B. Huppert, Endliche Gruppen, I, *in* ‘‘Die Grundlehren der Mathematischen Wissenschaften,’’ Vol. 134, Springer-Verlag, Berlin, 1967.

[Ko] A. Kontogeorgis, The group of automorphisms of function fields of the curves $x^n + y^m + 1 = 0$, *J. Number Theory* **72**, Sept. 1998.

[Ma] Magma Algebra System, Computational Algebra Group, University of Sydney, http://www.maths.usyd.edu.au:8000/u/magma/.

[Na] M. Namba, Equivalence problem and automorphism groups of certain compact Riemann surfaces, *Tsukuba J. Math*. **5**, No. 2 (1981), 319–338.

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

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

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

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