Non-Abelian Groups of Order Eight and the Local Lifting Problem

Bradley Richard Weaver
Lebanon, Pennsylvania

Master of Science, University of Virginia, 2014
Bachelor of Science, Grove City College, 2012

A Dissertation presented to the Graduate Faculty
of the University of Virginia in Candidacy for the Degree of
Doctor of Philosophy

Department of Mathematics

University of Virginia
May, 2018

Abstract

For a prime p, a cyclic-by-p group G and a G-extension $L|K$ of complete discrete valuation fields of characteristic p with algebraically closed residue field, the local lifting problem asks whether the extension $L|K$ lifts to characteristic zero. In this thesis, we characterize D_4-extensions of fields of characteristic two, determine the ramification breaks of (suitable) D_4-extensions of complete discrete valuation fields of characteristic two, and solve the local lifting problem in the affirmative for every D_4-extension of complete discrete valuation fields of characteristic two with algebraically closed residue field; that is, we show that D_4 is a local Oort group for the prime 2. Furthermore, we characterize Q_8-extensions of fields of characteristic two, determine the ramification breaks of (suitable) Q_8-extensions of complete discrete valuation fields of characteristic two, and, by solving the local lifting problem in the negative for a family of Q_8-extensions of complete discrete valuation fields of characteristic two with algebraically closed residue field, show that neither Q_8 nor $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ is an almost local Oort group for the prime 2.

Contents

Chapter 1

Introduction

For a prime p, a cyclic-by-p group G and a G-extension $L|K$ of complete discrete valuation fields of characteristic p with algebraically closed residue field, the *local lifting problem* (see Problem 1.2.4) asks whether the extension $L|K$ *lifts to characteristic zero* (a notion whose precise definition we shall provide in Section 1.2). In this thesis, we consider the local lifting problem for cases in which the prime $p = 2$ and the group G is a non-abelian group of order eight. For the case $G = D_4$, the dihedral group of order eight, we answer the local lifting problem in the affirmative in all cases; that is, we show that D_4 is a *local Oort group* for $p = 2$. For the case $G = Q_8$, the quaternion group of order eight, we exhibit a family of extensions that do not lift to characteristic zero; the existence of this family suffices to show that neither Q_8 nor the special linear group $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ is an *almost local Oort group* for $p = 2$, a notion we shall define in Section 1.2.

1.1 The Global Lifting Problem

The local lifting problem, as stated above, is (upon reformulation) a natural local correlate to the global lifting problem, which may be stated as follows:

Problem 1.1.1 (Global Lifting Problem). Suppose that Y is a smooth proper curve over an algebraically closed field k of positive characteristic p, and that $\iota : G \to \mathrm{Aut}_k(Y)$ is a faithful action of a finite group G on Y by k-automorphisms. Do there exist a finite integral extension R of the Witt ring $W(k)$, a flat relative curve $\widetilde{Y} \to \mathrm{Spec}\ R$ and a faithful action $\tilde{\iota} : G \to \mathrm{Aut}_R(\widetilde{Y})$ such that

1. $\widetilde{Y} \times_R k \cong Y$, and
2. the action $\tilde{\iota}$ on $\widetilde{Y}$ reduces to the action ι on Y?

Remark 1.1.2. The *Witt ring*, or *ring of Witt vectors*, $W(k)$ of k is the unique complete discrete valuation ring, necessarily of characteristic zero, with uniformizer p and residue field k [Ser79].

2010 Mathematics Subject Classification: 14H37, 12F10 Primary; 13B05, 14B12 Secondary.

Remark 1.1.3. If R is a finite integral extension of $W(k)$, then, since $W(k)$ is a complete discrete valuation ring, the valuation of $W(k)$ extends uniquely to R. Thus R is itself a complete discrete valuation ring; moreover, since k is algebraically closed, the residue field of R is k. The projection map $R \to k$ thus provides k with the structure of an R-module, and gives meaning to the expression $\widetilde{Y} \times_R k$ in Problem 1.1.1.

If, for a particular Y and ι, the global lifting problem for that curve and action is answered in the affirmative, then we say both that ι *lifts to characteristic zero* and that Y (with G-action ι) *lifts to characteristic zero.* Moreover, we say that $\tilde{\iota}$ and $\widetilde{Y}$ (with G-action $\tilde{\iota}$) are, respectively, *lifts* of ι and of Y (with G-action ι) over R.

Definition 1.1.4. A finite group G is an *Oort group* for an algebraically closed field k of characteristic p if every faithful G-action on every smooth proper curve over k by k-automorphisms lifts to characteristic zero. If G is an Oort group for every algebraically closed field of characteristic p, then G is an *Oort group* for the prime p.

The following theorem is a consequence of Grothendieck's results on tame lifting, to wit, of Exposé XIII, Corollaire 2.12 in [GR71], and implies that there is no obstruction to lifting in the tame case. For an exposition, see [Wew99].

Theorem 1.1.5 (Grothendieck)**.** *Suppose that G is a finite group with order prime to p. Then G is an Oort group for p.*

Furthermore, in [SOS89], Oort, Sekiguchi and Suwa proved the following:

Theorem 1.1.6. *For all m such that $p \nmid m$, the group $\mathbb{Z}/pm\mathbb{Z}$ is an Oort group for p.*

1.2 The Local Lifting Problem

Let k be an algebraically closed field of positive characteristic p, let Y be a smooth proper curve over k, and let $\iota : G \to \mathrm{Aut}_k(Y)$ be a faithful action of a finite group G on Y by k-automorphisms. For every point P of Y, the action ι induces a faithful action ι_P by k-automorphisms of the inertia group I_P of G at P on the complete local ring of Y at P. Since this complete local ring is necessarily isomorphic to a power series ring over k in one variable, the induced action ι_P prompts the local lifting problem.

Problem 1.2.1 (Local Lifting Problem). Suppose that a finite group G has a faithful action $\iota : G \to \mathrm{Aut}_k(k[[t]])$ on the power series ring $k[[t]]$ by k-automorphisms. Do there exist a finite integral extension R of the Witt ring $W(k)$ and a faithful action $\tilde{\iota} : G \to \mathrm{Aut}_R(R[[T]])$ on the power series ring $R[[T]]$ such that

1. T reduces to t under the canonical map $R \to k$, and
2. the action $\tilde{\iota}$ reduces to the action ι?

Analogously to the global setting, we say that ι *lifts to characteristic zero* if such an action $\tilde{\iota}$ exists, and that $\tilde{\iota}$ is a lift of ι.

Definition 1.2.2. Let G be a finite group. If every faithful G-action on the power series ring $k[[t]]$ by k-automorphisms lifts to characteristic zero, then G is a *local Oort group* for k. If G is a local Oort group for all algebraically closed fields of characteristic p, then G is a *local Oort group* for the prime p.

Remark 1.2.3. Any faithful G-action by k-automorphisms on a power series ring $k[[t]]$ over k induces a Galois extension $k[[t]]^G \to k[[t]]$ of complete discrete valuation rings with Galois group G. As shown, *e.g.*, in Chapter IV of [Ser79], the Galois group of any finite Galois extension of complete discrete valuation rings with algebraically closed residue field is a cyclic-by-p group, that is, a group isomorphic to $P \rtimes \mathbb{Z}/m\mathbb{Z}$, where P is a p-group and m is prime to p. We shall thus, in discussing local Oort groups for p, consider only cyclic-by-p groups.

If $G = \langle \sigma \rangle$ is a cyclic group of order m, where $p \nmid m$, then it is relatively simple both to describe and to lift faithful actions $\phi : G \to \mathrm{Aut}_k(k[[t]])$. By Kummer theory, for any such action ϕ, there exists a uniformizer t' of $k[[t]] = k[[t']]$ such that $\phi(\sigma)(t') = \zeta_m t'$, where ζ_m is a primitive mth root of unity. Moreover, if $R = W(k)[\zeta_m]$, then the action $\tilde{\phi} : G \to \mathrm{Aut}_R(R[[T']])$ given by $\tilde{\phi}(\sigma)(T') = \zeta_m T'$ does define a lift to ϕ.

In most cases, especially those in which $p \mid |G|$, both describing and lifting faithful actions is rather more difficult. If G is a cyclic group of order p, then the assignment

$$t \mapsto \frac{t}{1-t} = \sum_{n=1}^{\infty} t^n$$

does induce an automorphism of $k[[t]]$ of order p, and hence a faithful action ϕ of $|G|$. While Theorem 1.1.6 implies that this action ϕ does lift to characteristic zero, attempting to lift ϕ via the automorphism of $R[[T']]$ induced by the assignment $T \mapsto T/(1-T)$ fails, for this automorphism is not of order p. If $p \mid |G|$, and G is not a cyclic group of order p, then it is difficult even to give explicit examples of actions ϕ in terms of power series.

To obviate this problem, we use the Galois extension of complete discrete valuation rings induced by a faithful G-action by k-automorphisms on $k[[t]]$ to reformulate the local lifting problem as follows.

Problem 1.2.4 (Local Lifting Problem, Galois Theory Reformulation). Let A be a finite Galois extension of $k[[t]]$ with Galois group G. Do there exist a finite integral extension R of the Witt ring $W(k)$ and a G-Galois extension $\widetilde{A}$ of $R[[T]]$ such that

1. $\widetilde{A} \otimes_R k \cong A$, and
2. the Galois action on $\widetilde{A}$ over $R[[T]]$ reduces to the Galois action on A over $k[[t]]$?

If such an $\widetilde{A}$ exists, we say that the extension $A|k[[t]]$ *lifts to characteristic zero*, and, by analogy, that the corresponding extension $\mathrm{Frac}(A)|k((t))$ of complete discrete valuation fields *lifts to characteristic zero*, as well.

The close connection between the global and local lifting problems is manifest in the presence, in this setting, of a local-to-global principle, proven by Garuti in [Gar96].

Theorem 1.2.5 (Local-to-Global Principle)**.** *Let Y be a smooth proper curve over k, let ι be a faithful action of a finite group G on Y by k-automorphisms, and let $P_i, 1 \leq i \leq N$, denote the points of Y ramified under ι. Then ι lifts to characteristic zero if and only if, for each point P_i of Y, the induced action ι_{P_i} on the complete local ring of Y at P_i lifts to characteristic zero.*

Remark 1.2.6. If P is not a ramification point of ι, that is, if the inertia group of G at P is trivial, then the induced action ι_P lifts to characteristic zero trivially.

In [CGH08], Chinburg, Guralnick and Harbater proved a close relation between Oort groups and local Oort groups.

Theorem 1.2.7 (Theorem 2.4 in [CGH08])**.** *Let G be a finite group. Then G is an Oort group for k if and only if every cyclic-by-p subgroup of G is a local Oort group for k.*

Moreover, for cyclic-by-p groups, Oort groups for k and local Oort groups for k coincide.

Theorem 1.2.8 (Theorem 2.1 in [CGH17])**.** *Let G be a cyclic-by-p group. Then G is an Oort group for k if and only if G is a local Oort group for k.*

1.3 Known Local Lifting Results

We now rehearse several of the more significant and salient known results concerning the local lifting problem. Let k be an algebraically closed field of characteristic p, let $K = k((t))$ be the field of Laurent series over k, and let v_K denote the discrete valuation of K corresponding to $k[[t]]$. Moreover, let G be a cyclic-by-p group (so that $G \cong P \rtimes \mathbb{Z}/m\mathbb{Z}$, where P is the unique p-Sylow subgroup of G, and $m \nmid p$).

Definition 1.3.1. As in Definition 1.2.2, we define G to be a *local Oort group* for k if every faithful G-action by k-automorphisms on the power series ring $k[[t]]$ lifts to characteristic zero. Moreover, we define G to be

(1) a *weak local Oort group* for k if at least one faithful G-action on $k[[t]]$ by k-automorphisms lifts to characteristic zero, and

(2) an *almost local Oort group* for k if every sufficiently ramified faithful G-action by k-automorphisms on $k[[t]]$ lifts to characteristic zero; *i.e*, if there exists an integer N such that every faithful G-action ϕ on $k[[t]]$ for which $v_K(\phi(\sigma)(t) - t) \geq N$ for all $\sigma \in P$ lifts to characteristic zero.

From Theorems 1.1.5 and 1.1.6, any cyclic group of order not divisible by p^2 is a local Oort group for p. Moreover, Green and Matignon proved in [GM98] that, for m such that $p \nmid m$, the group $\mathbb{Z}/p^2m\mathbb{Z}$ is local Oort for p, Bouw and Wewers in [BW06] proved for odd p that the dihedral group D_p is local Oort for p, and Pagot in [Pag02] proved that $D_2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is local Oort for 2.

In 2014, Obus and Wewers in [OW14] and Pop in [Pop14] jointly resolved the *Oort conjecture*, that is, they proved that every finite cyclic group is local Oort for p. Finally, Obus has proven, in [Obu15] and [Obu16], respectively, that D_9 is local Oort for 3, and that A_4 is local Oort for 2.

On the other hand, in [CGH11], Chinburg, Guralnick and Harbater used two obstructions to local lifting, the *Bertin obstruction*, introduced by Bertin in [Ber98], and the *Katz–Gabber–Bertin obstruction*, or more succinctly, the *KGB obstruction*), introduced in [CGH11], and showed that these obstructions prevent all but a few classes of cyclic-by-p groups from being either local Oort or almost local Oort. To state their results, we need the following definitions.

Definition 1.3.2. The group G is a *Bertin group* (resp. *KGB group*) for k if the Bertin (resp. KGB) obstruction vanishes for every faithful G-action on $k[[t]]$ by k-automorphisms. Moreover, G is an *almost Bertin group* (resp. *KGB group*) for k if the Bertin (resp. KGB) obstruction vanishes for every faithful G-action on $k[[t]]$ by k-automorphisms that is sufficiently ramified (in the sense of Definition 1.3.1).

Theorem 1.3.3 (Chinburg, Guralnick, Harbater)**.** *The group G is a Bertin group for k if and only if G is a KGB group for k, which holds if and only if G is isomorphic either to a cyclic group (of any order) or to a dihedral group of order $2p^n$, or (for $p = 2$) isomorphic either to A_4 or to the generalized quaternion group Q_{2^m} of order 2^m for some $m \geq 4$.*

Theorem 1.3.4 (Chinburg, Guralnick, Harbater)**.** *The group G is an almost Bertin group for k if and only if G is an almost KGB group for k. Moreover, if G is an almost Bertin group for k, then G is either a Bertin group for k, or $p = 2$, and G is isomorphic either to the quaternion group Q_8 or the special linear group $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$.*

Since every local Oort group for k is an Bertin group for k, and every almost local Oort group for k is an almost Bertin group for k, Theorems 1.3.3 and 1.3.4 imply the following corollary.

Corollary 1.3.5 (Chinburg, Guralnick, Harbater)**.** *If G is a local Oort group for k, then G is isomorphic either to a cyclic group (of any order) or to a dihedral group of order $2p^n$, or (for $p = 2$) isomorphic either to A_4 or to the generalized quaternion group Q_{2^m} of order 2^m for some $m \geq 4$. If G is an almost local Oort group for k, then G is isomorphic either to a cyclic group (of any order) or to a dihedral group of order $2p^n$, or (for $p = 2$) isomorphic either to one of the groups A_4, Q_8 and $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$, or to the generalized quaternion group Q_{2^m} of order 2^m for some $m \geq 4$.*

In [BW09], Brewis and Wewers introduced a further obsruction, the *Hurwitz tree obstruction*, and showed that this obstruction prevents the generalized quaternion groups from being local Oort groups for k when $p = 2$.

Combining all of the foregoing results together, we see that the groups whose status as local Oort groups is open are, save the known local Oort group D_9, precisely the dihedral groups of order $2p^n$ for $n > 1$. Moreover, the groups whose status as almost local Oort groups is open are, save the known local (and hence almost local) Oort group D_9, precisely the dihedral groups of order $2p^n$ for $n > 1$, and (for $p = 2$), the groups Q_8 and $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$, As noted above, in this thesis we shall prove (for $p = 2$) that D_4 is a local Oort group for k, and that neither Q_8 nor $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ is an almost local Oort group for k.

It should be noted that D_4 differs from D_9 in having no tame subextension and from D_2 in being non-abelian. To prove that D_4 is indeed local Oort, we shall employ the 'method of equicharacteristic deformation' used both by Pop in [Pop14] and by Obus in [Obu15] and [Obu16]; that is, we shall make equicharacteristic deformations such that the ramification breaks of the local extensions on the generic fiber of the deformation are, in a suitable way, smaller than those of the original extension. Using induction, we shall thus be able to reduce the problem to a particular class of extensions with small ramification breaks, defined by Brewis in [Bre08] as the *supersimple* D_4-extensions. Since, in the same paper, Brewis proves that all supersimple D_4-extensions in characteristic two lift to characteristic zero, we shall accordingly have completed the desired proof.

To show that neither Q_8 nor $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ is an almost local Oort group for k, we shall exhibit a family of Q_8-extensions whose Bertin obstructions all fail to vanish. As this family will contain arbitrarily highly ramified extensions, we shall conclude that Q_8 is not an almost Bertin group, and hence not an almost Oort group, for k. To extend this result to $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$, we then extend a subfamily of this family of extensions to exhibit a family of $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$-extensions whose Bertin obstructions all fail to vanish.

Remark 1.3.6. The field k, which in this chapter has consistently denoted an algebraically closed field of positive characteristic, will denote a field throughout this thesis, but we shall not always assume that k is algebraically closed. For the convenience of the reader, we here note that the sections and subsections in which we do not require k to be algebraically closed are Sections 2.1, 2.2, 4.2 and 5.1, and Subsection 4.1.1. We do, however, insist that k be algebraically closed in Subsections 4.2.1 and 5.1.1. In Section 2.1, k need not have positive characteristic; in Section 2.3 and Chapter 3, the notation does not occur at all.

Chapter 2

Preliminary Definitions and Background

In this chapter, we shall introduce a few definitions and provide some necessary background information. All of the results in this section are well known; nevertheless, we provide proofs of a few results, as their proofs are somewhat difficult to find in the literature.

2.1 Higher Ramification Groups

Let k be a field, either of characteristic zero, or of positive characteristic p. We do not insist in this section that k be algebraically closed. Moreover, we let A be a complete discrete valuation ring with residue field k, let $K = \mathrm{Frac}(A)$ be the corresponding complete discrete valuation field, let L be a finite Galois extension of K such that the residue field of L is separable over k, let B be the integral closure of A in L, and let G be the Galois group of L over K. Since A is a complete discrete valuation ring, and $B|A$ is finite, the ring B is also a complete discrete valuation ring. By Proposition III.12 in [Ser79], there exists an element $x \in B$ such that $B = A[x]$. Moreover, if L is a totally ramified extension of K, that is, if the residue field of L is equal to k, then we may and do assume that x is a uniformizer of B. We now define a function $i_G : G \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$ such that $i_G(\sigma) = v_L(\sigma(x) - x)$, where v_L denotes the discrete valuation of L corresponding to B.

Definition 2.1.1. For all real numbers $j \geq -1$, the jth lower ramification group of $L|K$ is

$$G_j = \{\sigma \in G \mid i_G(\sigma) \geq j + 1\}.$$

The filtration of G given by the lower ramification groups has the following properties, given in Proposition IV.1 and Corollary 4 to Proposition IV.7 in [Ser79].

Proposition 2.1.2. *The ramification group $G_{-1} = G$, and G_0 is equal to the inertia group of $L|K$. If* char $k = 0$*, then G_0 is a cyclic group, and $G_1 = \{\mathrm{Id}_L\}$. Moreover, if* char $k = p$*, the following statements all hold.*

(1) G_0 *is a cyclic-by-p group;* i.e., $G_0 \cong P \rtimes \mathbb{Z}/m\mathbb{Z}$, *where* P *is the unique* p*-Sylow subgroup of* G_0, *and* m *is prime to* p.

(2) $G_1 = P$.

(3) $G_n = \{\mathrm{Id}_L\}$ *for sufficiently large* n.

Remark 2.1.3. The fixed field L^{G_0} is the maximal unramified extension of K in L, and the fixed field L^{G_1} is the maximal tamely ramified extensions of K in L. The higher ramification groups G_j (for $j \geq 2$) provide some indication as to how badly ramified the wildly ramified extension $L|L^{G_1}$ is.

Remark 2.1.4. Suppose that K has characteristic p, and that $L|K$ is a totally ramified extension. Then k has characteristic p as well, $B = k[[x]]$, and $G_1 = P$, where P is the unique p-Sylow subgroup G. If $\phi : G \to B = k[[x]]$ denotes the Galois action of G on B, then, for any positive integer n, the statement that $v_K(\phi(\sigma)(x) - x) \geq n$ for all $\sigma \in P$, as used in Definitions 1.3.1 and 1.3.2, is equivalent to the statement that $G_n = P$.

Now let $N \subseteq L$ be a subextension of K inside L, and let $H = \mathrm{Gal}(L|N)$. The following proposition relates the ramification groups of $L|N$ to those of $L|K$.

Proposition 2.1.5 (Proposition IV.2 in [Ser79])**.** *For all real numbers* $j \geq -1$, $H_j = G_j \cap H$.

If N is a normal extension of L, we must introduce the *upper ramification groups* to give an analogous result for the ramification groups of $N|K$. We may define the upper ramification groups by re-indexing the lower ramification groups using the Herbrand function $\phi : [-1, \infty) \to [-1, \infty)$, which we define such that

$$\phi(x) = \begin{cases} y & \text{if } y < 0 \\ \int_0^y \frac{1}{[G_0 : G_z]}\, dz & \text{if } y \geq 0 \end{cases}.$$

We observe that $f(u) = 1/[G_0 : G_u]$ is a positive decreasing left-continuous piecewise linear function on $[0, \infty)$, and that thus ϕ is itself an invertible (increasing) left-continuous piecewise linear function on $[-1, \infty)$. The Herbrand function converts the 'lower numbering' of the lower ramification groups into the 'upper numbering' of the upper ramification groups.

Definition 2.1.6. Let $\psi = \phi^{-1}$. For all real numbers $j \geq -1$, the jth upper ramification group of $L|K$ is

$$G^j = G_{\psi(j)}.$$

Proposition 2.1.7 (Proposition IV.14 in [Ser79])**.** *Suppose that* N *is a normal extension of* K, *so that* H *is a normal subgroup of* G. *For all real numbers* $j \geq -1$, $(G/H)_j = (G_j H)/H$.

We suppose henceforth that $L|K$ is totally ramified, that k has positive characteristic p, and that G is a group of order p^n; *i.e.*, suppose that $G_1 = G$. In this context, we make the following definitions.

Definition 2.1.8. For all $1 \leq i \leq n$, the *ith lower ramification break* ℓ_i of G is

$$\max\{\nu \mid |G_\nu| \geq p^{n+1-i}\}$$

and, similarly, the *ith upper ramification break* u_i of G is

$$\max\{\nu \mid |G^\nu| \geq p^{n+1-i}\}.$$

Definition 2.1.9. The *sequence of ramification groups* of L over K is the finite sequence $(G^{u_i})_{i=1}^n$.

Remark 2.1.10. Since $G_{\ell_i} = G^{u_i}$ for all i, the sequence of ramification groups of L over K can also be written as $(G_{\ell_i})_{i=1}^n$.

Proposition 2.1.11. *The first lower and upper ramification breaks of $L|K$ are equal;* i.e., $u_1 = \ell_1$. *Moreover, for all $2 \leq i \leq n$,*

(1) $u_i - u_{i-1} = p^{-(i-1)}(\ell_i - \ell_{i-1})$,

(2) $u_i = p^{-(i-1)}\ell_i + (p-1)\sum_{j=1}^{i-1} p^{-j}\ell_j$, *and*

(3) $\ell_i = p^{i-1}u_i - (p-1)\sum_{j=1}^{i-1} p^{j-1}u_j$.

Proof. Since $G = G_z$ for all $z \leq \ell_1$, the equation $u_1 = \ell_1$ holds. Moroever, for all $2 \leq i \leq n$, the index $[G : G_z]$ is equal to p^{i-1} for all $\ell_{i-1} < z \leq \ell_i$; hence $u_i - u_{i-1} = \phi(\ell_i) - \phi(\ell_{i-1}) = p^{-(i-1)}(\ell_i - \ell_{i-1})$ for all $2 \leq i \leq n$. Therefore,

$$\begin{aligned} u_i &= \sum_{j=2}^{i}(u_j - u_{j-1}) + u_1 = \sum_{j=2}^{i} p^{-(j-1)}(\ell_j - \ell_{j-1}) + \ell_1 \\ &= p^{-(i-1)}\ell_1 + \sum_{j=1}^{i-1}(p^{-(j-1)} - p^{-j})\ell_j = p^{-(i-1)}\ell_1 + (p-1)\sum_{j=1}^{i-1} p^{-j}\ell_j \end{aligned}$$

and

$$\begin{aligned} \ell_i &= \sum_{j=2}^{i}(\ell_j - \ell_{j-1}) + \ell_1 = \sum_{j=2}^{i} p^{j-1}(u_j - u_{j-1}) + u_1 \\ &= p^{i-1}u_i + \sum_{j=1}^{i-1}(p^{j-1} - p^j)u_j = p^{i-1}u_i - (p-1)\sum_{j=1}^{i-1} p^{j-1}u_j. \end{aligned}$$ □

Remark 2.1.12. Though Definition 2.1.1 implies that each lower ramification break ℓ_i must be an integer, the upper ramification breaks u_i need not all be integers.

For convenience, if $L|K$ is totally ramified, and G has order p, we shall use the term *conductor* to denote the unique ramification break of G. This agrees with the usage of, *e.g.*, Bouw and Wewers in [BW06]; others, such as Garuti in [Gar02] define the conductor to be the unique ramification break of G plus one.

2.2 Artin–Schreier Theory

Let K be a field of characteristic two, fix an algebraic closure K^{alg} of K, and let $\wp : K^{\mathrm{alg}} \to K^{\mathrm{alg}}$ denote the Artin–Schreier additive group homomorphism, which is given by the assignment

$$F \mapsto F^2 + F$$

on K^{alg}. For the moment we do not insist that K be a complete discrete valuation field. For any element F in K, we denote by $[F]$ the image of F in $K/\wp(K)$, and define two elements F_1 and F_2 of K to be *Artin–Schreier-equivalent* over K if $[F_1] = [F_2]$. By Artin–Schreier theory, $\wp$ induces a map

$$\Phi : K \to \{L|K \text{ separable} \mid \deg_K(L) = 2\} \cup \{K\}$$

given by the assignment $\Phi(F) = K[\wp^{-1}(F)]$ for all $F \in K$.

Proposition 2.2.1. *Let $F_1, F_2 \in K$. Then $[F_1] = [F_2]$ if and only $\Phi(F_1) = \Phi(F_2)$.*

Proof. Suppose $[F_1] = [F_2]$. Then there exists $\alpha \in K$ such that $\alpha^2 + \alpha = F_1 + F_2$. Thus $\wp^{-1}(F_1 + \alpha) = \wp^{-1}(F_2)$, and hence $\Phi(F_1) = \Phi(F_2)$.

Now suppose $\Phi(F_1) = \Phi(F_2) \neq K$. (If $\Phi(F_1) = K$, then $[F_1] = [F_2] = 0$.) Let $\alpha_1, \alpha_2 \in \Phi(F_1)$ such that $\wp(\alpha_1) = F_1$ and $\wp(\alpha_2) = F_2$, and let σ be the unique non-trivial element of $\mathrm{Gal}(\Phi(F_1)|K)$. Then $\wp(\alpha_1 + \alpha_2) = F_1 + F_2$, and

$$\sigma(\alpha_1 + \alpha_2) = \sigma(\alpha_1) + \sigma(\alpha_2) = (\alpha_1 + 1) + (\alpha_2 + 1) = \alpha_1 + \alpha_2.$$

Hence $\alpha_1 + \alpha_2 \in K$, and $[F_1] = [F_2]$. □

For our purposes it will suffice to consider the case in which K is a complete discrete valuation field, *i.e.*, in which $K = k((t))$ for some field k of characteristic two. Accordingly, we suppose for the remainder of this subsection that K is such a field.

Lemma 2.2.2. *Every Artin–Schreier class of K contains an element in the polynomial ring $k[t^{-1}]$. In particular, for any element $F = \sum_{n \geq -N} a_n t^n$ of K,*

$$[F] = \left[\sum_{-N \leq n \leq 0} a_n t^n \right].$$

Proof. Note that, for all $n \geq 1$, the equation

$$a_n t^n = \left(\sum_{j \geq 0} a_n^{2^j} t^{2^j n} \right)^2 + \sum_{j \geq 0} a_n^{2^j} t^{2^j n}$$

implies that $[a_n t^n] = 0$. Thus

$$[F] = \left[\sum_{N \leq n \leq 0} a_n t^n \right].$$

□

Definition 2.2.3. An element $\sum_{n\geq -N} a_n t^n$ of K is in *standard form over K with respect to t* if each coefficient a_n is zero unless n is both negative and odd.

Proposition 2.2.4. *Suppose that F_1 and F_2 are distinct standard form elements of K. Then $[F_1] \neq [F_2]$.*

Proof. Since F_1 and F_2 are distinct, F_1+F_2 is a non-zero standard form element of K. Thus the valuation $v_K(F_1+F_2) = -\deg_{t^{-1}}(F_1+F_2)$ is odd and negative. Since, for all $\alpha \in K$, the valuation $v_K(\alpha^2+\alpha) = 2v_K(\alpha)$ if $v_K(\alpha) < 0$, no element of $\wp^{-1}(F_1+F_2)$ is in K. Thus $[F_1+F_2] \neq 0$; *i.e.*, $[F_1] \neq [F_2]$. □

If the residue field k of K is algebraically closed, then Definition 2.2.3 obviates one difficulty associated with the equivalence relation defined above — that, in general, it may not be possible readily to select a canonical element from each Artin–Schreier equivalence class of K. In particular, the following proposition holds.

Proposition 2.2.5. *Suppose k is algebraically closed. Then every Artin–Schreier equivalence class of K contains precisely one standard form element of K.*

Proof. By Proposition 2.2.4, it suffices to show that every element of K is Artin–Schreier-equivalent over K to a standard form element of K. Let $F = \sum_{n\geq -N} a_n t^n \in K$. Lemma 2.2.2 implies that

$$[F] = \left[\sum_{-N\leq n\leq 0} a_n t^n\right].$$

Moreover, $[a_0] = 0$ since k is algebraically closed. Finally, if $1 \leq 2^\ell m \leq N$, and m is odd, then

$$\left[a_{-2^\ell m} t^{-2^\ell m}\right] = \left[(a_{-2^\ell m})^{2^{-\ell}} t^{-m}\right].$$

Thus F is Artin–Schreier-equivalent over K to a standard form element of K. □

Remark 2.2.6. If k is not algebraically closed, not every Artin–Schreier equivalence class need contain a standard form element. For example, if $k = \mathbb{F}_2$, then $[1] \neq [0]$ over K; hence the class $[1]$ contains no standard form element in K.

The conductor of a non-trivial extension associated to an element whose degree in t^{-1} is both positive and odd may be computed from this element as indicated in the following proposition. In particular, the conductor may be computed from any associated non-zero standard form element of K.

Proposition 2.2.7. *Let $F \in K$, and let $f = \deg_{t^{-1}} F$. Suppose that f is both positive and odd. Then $\Phi(F) = K[\wp^{-1}(F)]$ is a totally ramified degree two extension of K whose conductor is f.*

Proof. Let $\alpha \in \Phi(F)$ such that $\alpha^2+\alpha = F$. Note that then $v_{\Phi(F)}(F) < 0$ since $v_K(F) = -f < 0$. Since

$$v_{\Phi(F)}(F) = \min\{2v_{\Phi(F)}(\alpha), v_{\Phi(F)}(\alpha)\},$$

it follows that $v_{\Phi(F)}(F) = 2v_{\Phi(F)}(\alpha)$. Thus $v_{\Phi(F)}(F)$ is even. Since $v_K(F) = -f$ is odd, the ramification index of $\Phi(F)$ over K is 2; thus, $\Phi(F)$ is totally ramified over K.

To determine the conductor of $\Phi(F)$ over F, let $\pi = \alpha t^{(f+1)/2}$, and observe that $v_{\Phi(F)}(\pi) = 1$; *i.e.*, that π is a uniformizer of $\Phi(F)$. Let $g(T)$ be the characteristic polynomial of π over K. Since $\Phi(F)$ is totally ramified over K, the different $\mathfrak{D}_{\Phi(F)|K}$ of $\Phi(F)$ over K is generated by $g'(\pi)$ by Lemma III.3 and Corollary 2 of Lemma III.2 in [Ser79]. Since $\alpha^2 + \alpha = F$, the relation $\pi^2 + t^{(f+1)/2}\pi = Ft^{f+1}$ holds. Thus

$$g(T) = T^2 + t^{(f+1)/2}T + Ft^{f+1},$$

and $g'(T) = t^{(f+1)/2}$. Hence $\mathfrak{D}_{\Phi(F)|K} = (g'(\pi)) = (t)^{(f+1)/2}$. Since $v_{\Phi(F)}(t) = 2$, the valuation $v_{\Phi(F)}(\mathfrak{D}_{\Phi(F)|K}) = f+1$. By Hilbert's different formula (see Proposition 2.3.3 in Section 2.3), it follows that the conductor of $\Phi(F)$ over K is f. □

To determine the ramification behavior of Artin–Schreier extensions not associated to any element whose degree in t^{-1} is both positive and odd, we introduce the following definition.

Definition 2.2.8. An element $F \in K$ is in *minimal-degree form* over K with respect to t if the degree in t^{-1} of F is minimal among the degrees in t^{-1} of elements in $[F]$.

Remark 2.2.9. Lemma 2.2.2 implies that every Artin–Schreier class of K contains an element in minimal-degree form over K with respect to t, and that no element in minimal-degree form has negative, finite degree in t^{-1}.

Proposition 2.2.10. *Let F be an element in minimal-degree form over K with respect to t, let $f = \deg_{t^{-1}} F$, and let κ_F denote the residue field of $\Phi(F) = K[\wp^{-1}(F)]$ The following statements all hold.*

(1) *If $f = -\infty$, then $\Phi(F) = K$.*

(2) *If $f = 0$, then κ_F is a degree two separable extension of k.*

(3) *If f is positive and odd, then $\Phi(F)$ is a totally ramified degree two extension of K whose conductor is f.*

(4) *If f is positive and even, then κ_F is a degree two inseparable extension of k.*

Proof. Note that Proposition 2.2.7 directly implies statement (3), and that statement (1) is clear.

To prove statements (2) and (4), we suppose henceforth that f is a non-negative even number, let $F = \sum_{n\geq -f} a_n t^n$, and let $\alpha \in \Phi(F)$ such that $\alpha^2 + \alpha = F$.

First suppose $f = 0$. Then $F \in k[[t]]$. Hence α is an integer in $\Phi(F)$, and $\bar{\alpha}^2 + \bar{\alpha} = a_0$, where $\bar{\alpha} \in \kappa_F$ is the image of α under the canonical projection map to κ_F. Since F is in minimal-degree form with respect to t, it follows that $\bar{\alpha} \notin k$. Thus $\kappa_F = k[\bar{\alpha}]$ is a degree two separable extension of k; *i.e.*, statement (2) holds.

Now suppose $f > 0$, and let $\alpha' = t^{f/2}\alpha$. Then

$$(\alpha')^2 + t^{f/2}\alpha' = t^f\alpha^2 + t^f\alpha = t^f F = \sum_{n\geq 0} t_{n-f}t^n \in k[[t]];$$

as such, α' is an integer in $\Phi(F)$, and $(\bar{\alpha}')^2 = a_{-f}$, where $\bar{\alpha}' \in \kappa_F$ is the image of α' under the canonical projection map to κ_F. Since F is in minimal-degree form over K with respect to t, it follows that $\bar{\alpha}' \notin k$, for, if $\bar{\alpha}'$ were in k, then $[a_{-f}t^{-f}] = [\bar{\alpha}'t^{-f/2}]$ over K, and F would not be in minimal-degree form. Thus $\kappa_F = k[\bar{\alpha}']$ is a degree two inseparable extension of k; *i.e.*, statement (4) holds. □

Propositions 2.2.7 and 2.2.10 together imply the following corollary.

Corollary 2.2.11. *Any element of K whose degree in t^{-1} is positive and odd is in minimal-degree form over K with respect to t. In particular, any element of K in standard form is also in minimal-degree form.*

2.3 Degree of the Different

Let K be the field of fractions of a discrete valuation ring A with maximal ideal $\mathfrak{m}$, let L be a finite étale algebra over K, *i.e.*, a finite product of finite separable field extensions of K, and let B be the integral closure of A in L.

Definition 2.3.1. Let $\mathfrak{D}_{B|A} = \prod_{i=1}^m \mathfrak{P}_i^{n_i}$ denote the different of B over A. Then the *degree of the different* $\delta_{B|A}$ of B over A is the length of $B/\mathfrak{D}_{B|A}$ as an $A/\mathfrak{m}$-module.

Remark 2.3.2. This definition agrees with that used in [GM98], [Bre08] and [Obu17]. Note that the sum $\sum_{i=1}^m n_i$ does not always give $\delta_{B|A}$, though this is the case if, for all $1 \leq i \leq n$, the residue field $B/\mathfrak{P}_i B$ is equal to $A/\mathfrak{m}A$.

Suppose that A is an equal characteristic complete discrete valuation ring of characteristic p, that L is a Galois field extension of K, and that the extension $B/\mathfrak{P}B$ over $A/\mathfrak{m}A$ of residue fields is separable (where $\mathfrak{P}$ is the maximal ideal of the complete discrete valuation ring B). In this case, the degree of the different $\delta_{B|A}$ is given by $v_L(\mathfrak{D}_{B|A})$, where v_L is the discrete valuation on L defined by B. The following proposition, a restatement of Proposition IV.4 in [Ser79], thus gives a formula for the degree of the different in terms of the lower ramification groups of $G = \mathrm{Gal}(L|K)$.

Proposition 2.3.3 (Hilbert's Different Formula)**.** *The equation*

$$v_L\left(\mathfrak{D}_{B|A}\right) = \sum_{j=0}^{\infty} \left(|G_j| - 1\right)$$

holds

Proposition 2.3.3 has the following corollary.

Corollary 2.3.4. *Suppose that $L|K$ is totally ramified, and that G is a group of order p^n. For all $1 \leq i \leq n$, let ℓ_i denote the ith lower ramification break of $L|K$. Then*

$$\delta_{B|A} = (p-1)\sum_{i=1}^{n} p^{n-i}\ell_i + p^n - 1.$$

Proof. By Proposition 2.3.3, $\delta_{B|A} = \sum_{j=0}^{\infty} (|G_j| - 1)$. Thus

$$\begin{aligned}
\delta_{B|A} &= \sum_{j=0}^{\ell_1} (|G_j| - 1) + \sum_{i=1}^{n-1} \sum_{j=\ell_i+1}^{\ell_{i+1}} (|G_j| - 1) \\
&= (p^n - 1)(\ell_1 + 1) + \sum_{i=1}^{n-1} (p^{n-i} - 1)(\ell_{i+1} - \ell_i) \\
&= p^n - 1 + \sum_{i=1}^{n-1} (p^{n-i+1} - p^{n-i})\ell_i + (p-1)\ell_n \\
&= (p-1)\sum_{i=1}^{n} p^{n-i}\ell_i + p^n - 1
\end{aligned}$$

□

Chapter 3

Non-Cyclic Galois Extensions of Degree Eight of Fields of Characteristic Two

3.1 D_4-Extensions as Galois Closures of Non-Galois Extensions

In this section we shall realize D_4-extensions of fields of characteristic two as the Galois closures of (two-level) towers of $\mathbb{Z}/2\mathbb{Z}$-extensions. Throughout the section, let K be a field of characteristic two, let K^{alg} be a fixed algebraic closure of K, let $M \subset K^{\text{alg}}$ be a separable extension of K of degree two, and let $N \subset K^{\text{alg}}$ be a separable extension of M of degree not exceeding two. Note that then there exist $F, G, H \in K$ and $q, r, s \in K^{\text{alg}}$ such that

$$q^2 + q = F, \quad r^2 + r = Gq + H \quad \text{and} \quad s^2 + s = G,$$

and such that $M = K[q]$ and $N = M[r]$. Moreover, there exists $\sigma \in \text{Gal}(K^{\text{alg}}|K)$ such that $\sigma|_M$ is the unique non-trivial element of $\text{Gal}(M|K)$.

Lemma 3.1.1. *The equation*

$$(qs)^2 + qs = Gq + Fs^2 = Gq + Fs + FG$$

holds.

Proof. Note that

$$(qs)^2 + qs = q^2s^2 + qs^2 + qs^2 + qs = q(s^2 + s) + (q^2 + q)s^2 = Gq + Fs^2 = Gq + Fs + FG.$$

□

Lemma 3.1.2. $[G] = 0$ *over* M *if and only if either* $[G] = 0$ *over* K *or* $[G] = [F]$ *over* K.

Proof. Suppose $[G] = 0$ over M. Then there exist $\alpha, \beta \in K$ such that

$$G = (\alpha q + \beta)^2 + \alpha q + \beta = \alpha^2 q^2 + \beta^2 + \alpha q + \beta$$
$$= \alpha^2(q + F) + \alpha q + \beta^2 + \beta = (\alpha^2 + \alpha)q + \alpha^2 F + \beta^2 + \beta.$$

Since $G \in K$ and $M = K[q]$, it follows that $\alpha^2 + \alpha = 0$. Thus either $\alpha = 0$, in which case $[G] = 0$ over K, or $\alpha = 1$, in which case $[G] = [F]$ over K.

Now suppose either that $[G] = 0$ over K, or that $[G] = [F]$ over K. If $[G] = 0$ over K, then $[G] = 0$ over M. If $[G] = [F]$ over K, then $[G] = [F] = 0$ over M since $q^2 + q = F$ and $q \in M$. □

Lemma 3.1.3. *The following three conditions are equivalent:*

(1) $[Gq + H] = 0$ *over* M.

(2) $[G] = 0$ *over* K *and* $[H] = [Fs^2]$ *over* M.

(3) $[G] = 0$ *over* M *and* $[H] = [Fs^2]$ *over* M.

Proof. ((1) $\Longrightarrow$ (2)) Suppose $[Gq + H] = 0$ over M. Then there exist $\alpha, \beta \in K$ such that

$$Gq + H = (\alpha q + \beta)^2 + \alpha q + \beta = (\alpha^2 + \alpha)q + \alpha^2 F + \beta^2 + \beta,$$

as above. Hence, since $G, H \in K$, it follows that $G = \alpha^2 + \alpha$ and $H = \alpha^2 F + \beta^2 + \beta$. Therefore, $[G] = 0$ over K, and either $\alpha = s$ or $\alpha = s + 1$.

First suppose $\alpha = s$. Then $H = Fs^2 + \beta^2 + \beta$, and hence $[H] = [Fs^2]$ over K. Thus $[H] = [Fs^2]$ over M as well.

Now suppose $\alpha = s + 1$. Then

$$H = (s + 1)^2 F + \beta^2 + \beta = Fs^2 + F + \beta^2 + \beta,$$

and hence $[H] = [Fs^2 + F]$ over K. Thus, over M, $[H] = [Fs^2 + F] = [Fs^2] + [F] = [Fs^2]$.

Therefore, in both cases, $[H] = [Fs^2]$ over M. Thus $[H] = [Fs^2]$ over M.

((2) $\Longrightarrow$ (3)) Since $K \subseteq M$, this implication holds *a fortiori*.

((3) $\Longrightarrow$ (1)) Finally, suppose that $[G] = 0$ over M and that $[H] = [Fs^2]$ over M. By Lemma 3.1.1, $(qs)^2 + qs = Gq + Fs^2$. Since $[G] = 0$ over M, it follows that $s \in M$ and that $qs \in M = K[q]$. Thus, over M,

$$0 = [(qs)^2 + qs] = [Gq + Fs^2] = [Gq] + [Fs^2] = [Gq] + [H] = [Gq + H]. \quad \square$$

Lemma 3.1.4. *Suppose that* N *is a degree four extension of* K. *The following four conditions are equivalent:*

(1) N *is a Galois extension of* K.

(2) $\sigma(N) = N$.

(3) $[\sigma(Gq + H)] = [Gq + H]$ *over* M.

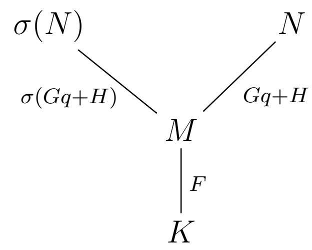

Figure 3.1

(4) $[G] = 0$ *over* M.

Remark 3.1.5. The situation described in Lemma 3.1.4 may be visualized as in Figure 3.1.

Proof. Recall that $\sigma|_M$ is the unique non-trivial element of M.

Suppose that $\sigma(N) = N$. Since $\sigma|_M$ is non-trivial, $\sigma|_N$ is non-trivial. Let τ be the unique non-trivial element of $\mathrm{Gal}(N|M)$. Then $\tau(N) = N$, and $\tau|_M$ is trivial. Thus $\sigma|_M \neq \tau|_M$; as such, $\sigma|_N$ and τ are distinct non-trivial K-automorphisms of N. Hence N is Galois over K, and conditions (1) and (2) are equivalent.

Moreover, since $\sigma|_M$ is non-trivial, $\sigma(q) = q + 1$. Thus $\sigma(Gq + H) = G(q + 1) + H = Gq + G + H$. Therefore, $[\sigma(Gq + H)] = [Gq + H]$ over M if and only if $[Gq + G + H] = [Gq + H]$ over M, which holds if and only if $[G] = 0$ over M. Thus (3) and (4) are equivalent.

Note now that $(\sigma(r))^2 + \sigma(r) = \sigma(r^2 + r) = \sigma(Gq + H)$. Thus $[\sigma(Gq + H)] = [Gq + H]$ over M if and only if $M[\sigma(r)] = M[r] = N$, which holds if and only if $\sigma(N) = N$. Hence (2) and (3) are equivalent.

Therefore, conditions (1) through (4) are equivalent, as claimed. □

Proposition 3.1.6. *The following statements, exactly one of which applies, all hold:*

(1) *If* $[G] = 0$ *over* K *and* $[H] = [Fs^2]$ *over* M, *then* $N = M$.

(2) *If* $[G] = 0$ *over* K *and* $[H] \neq [Fs^2]$ *over* M, *then* N *is a Galois extension of* K, *and* $\mathrm{Gal}(N|K) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(3) *If* $[G] = [F]$ *over* K, *then* N *is a Galois extension of* K, *and* $\mathrm{Gal}(N|K) \cong \mathbb{Z}/4\mathbb{Z}$.

(4) *If* $[G] \neq 0$ *over* M, *then* N *is not a Galois extension of* K, *and* $\mathrm{Gal}(\widetilde{N}|K) \cong D_4$, *where* $\widetilde{N}$ *denotes the Galois closure of* N *over* K.

Proof. To prove (1), suppose that $[G] = 0$ over K and that $[H] = [Fs^2]$ over M. Then, by Lemma 3.1.3, $[Gq + H] = 0$ over M. Thus $r \in M$, and hence $N = M[r] = M$.

To prove (2), suppose that $[G] = 0$ over K and that $[H] \neq [Fs^2]$ over M. By Lemma 3.1.3, $[Gq + H] \neq 0$ over M; as such, $N \neq M$. Thus N is a degree four extension of K. Since $[G] = 0$ over M, Lemma 3.1.4 implies that N is a Galois extension of K. Moreover, since $[G] = 0$ over K, it follows that $s \in K$. Thus

$$(r+qs)^2 + (r+qs) = r^2 + r + (qs)^2 + qs = Gq + H + Gq + Fs^2 = H + Fs^2 \in K,$$

where the second equality follows by Lemma 3.1.1. Since $[H] \neq [Fs^2]$ over M, $[H + Fs^2] \neq 0$ over M. By Lemma 3.1.2, it follows that $[H + Fs^2] \neq 0$ over K and that $[H + Fs^2] \neq [F]$ over K. Hence $K[r + qs]$ is a degree two subfield of N that is not equal to $M = K[q]$. Thus $\mathrm{Gal}(N|K) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

To prove (3), suppose that $[G] = [F]$ over K. Then $[G] \neq 0$ over K, and so $[Gq + H] \neq 0$ over M by Lemma 3.1.3. Thus N is a degree four extension of K. Since $[G] = [F] = 0$ over M, Lemma 3.1.4 implies that N is a Galois extension of K. Moreover, since $[G] = [F] \neq 0$ over K, it follows that $s \in M \backslash K$, and hence that $\sigma(s) = s + 1$. Furthermore, since

$$(\sigma(r))^2 + (\sigma(r)) = \sigma(Gq + H) = Gq + H + G = (r+s)^2 + (r+s),$$

either $\sigma(r) = r + s$, or $\sigma(r) = r + s + 1$. In either case, one easily verifies that $\sigma^2(r) = r + 1$. Therefore $\sigma^2|_N$ is not trivial, and $\mathrm{Gal}(N|K) \cong \mathbb{Z}/4\mathbb{Z}$.

To prove (4), suppose that $[G] \neq 0$ over M. Then $[G] \neq 0$ over K, and hence $N \neq M$ by Lemma 3.1.3. Thus N is a degree four extension of K; hence, by Lemma 3.1.4, N is not a Galois extension of K. Moreover, $\mathrm{Gal}(\widetilde{N}|K)$ is isomorphic to a subgroup of S_4 and contains an index two (normal) subgroup, *viz.* $\mathrm{Gal}(\widetilde{N}|M)$, which itself contains a subgroup of index four in $\mathrm{Gal}(\widetilde{N}|K)$ that is not normal in $\mathrm{Gal}(\widetilde{N}|K)$. The only group satisfying all these conditions is D_4, so $\mathrm{Gal}(\widetilde{N}|K) \cong D_4$. □

Lemma 3.1.7. *Let $F', G', H' \in K$, and let $q', r', s' \in K^{\mathrm{alg}}$ such that $(q')^2 + q' = F'$, $(r')^2 + r' = G'q' + H'$, and $(s')^2 + s' = G'$. Also, let $M' = K[q']$. Suppose that $[F] = [F']$ over K,* i.e., *that $M' = M$. Then $[Gq + H] = [G'q' + H']$ over M if and only if $[G] = [G']$ over K, and $[H] = [H' + G'(q + q') + F(s + s')^2]$ over M.*

Proof. Note that $[Gq + H] = [G'q' + H']$ over M if and only if

$$[Gq + H + G'q' + H'] = [(G + G')q + G'(q + q') + H + H'] = 0$$

over M. Since $[F] = [F']$ over K, the element $q + q'$ is in K. Thus, by Lemma 3.1.3, $N' = N$ if and only if both $[G+G'] = 0$ over K, and $[G'(q+q')+H+H'] = [F(s+s')^2]$ over M; *i.e.*, if and only if both $[G] = [G']$ over K, and $[H] = [H'+G'(q+q')+F(s+s')^2]$ over M. □

Proposition 3.1.8. *Let $F', G', H' \in K$, and let $q', r', s' \in K^{\mathrm{alg}}$ such that $(q')^2 + q' = F'$, $(r')^2 + r' = G'q' + H'$, and $(s')^2 + s' = G'$. Also, let $M' = K[q']$ and $N' = M'[r']$. Then*

(1) *$M' = M$ and $N' = N$ if and only if $[F] = [F']$ over K, $[G] = [G']$ over K, and $[H] = [H' + G'(q + q') + F(s + s')^2]$ over M.*

(2) *$M' = M$ and $N' = \sigma(N)$ if and only if $[F] = [F']$ over K, $[G] = [G']$ over K, and $[H] = [H' + G'(q + q') + F(s + s')^2 + G]$ over M.*

Proof. As noted in Lemma 3.1.7, $M' = M$ if and only if $[F] = [F']$ over K. This statement will be used without citation henceforth.

To prove (1), suppose that $M' = M$. Then $N' = N$ if and only if $[Gq + H] = [G'q' + H']$ over M. By Lemma 3.1.7, this holds if and only if $[G] = [G']$ over K and $[H] = [H' + G'(q + q') + F(s + s')^2]$ over M. Statement (1) now follows.

To prove (2), suppose that $M' = M$, and note both that $\sigma(N) = M[\sigma(r)]$, and that $(\sigma(r))^2 + \sigma(r) = \sigma(Gq + H) = Gq + H + G$. Then $N' = \sigma(N)$ if and only if $[Gq + H + G] = [G'q' + H']$ over M. By Lemma 3.1.7, this holds if and only if $[G] = [G']$ over K and $[H] = [H' + G'(q + q') + F(s + s')^2 + G]$ over M. Statement (2) now follows. □

3.2 D_4-Extensions of Fields of Characteristic Two

Let K be a field of characteristic two, let K^{alg} be a fixed algebraic closure of K, and let $L \subseteq K^{\text{alg}}$ be a Galois extension of K such that $\text{Gal}(L|K) \cong D_4$.

Proposition 3.2.1. *There exist $F, G, H \in K$, and $q, r \in K^{\text{alg}}$ such that $q^2 + q = F$, $r^2 + r = Gq + H$, and L is the Galois closure over K of $K[q, r]$.*

Proof. Note that D_4 contains a subgroup of index two containing a non-normal subgroup of index four. Thus there exists a non-normal degree four subfield L' of L over K containing a degree two subfield K' of L. Then there exist $F \in K$ and $q \in K^{\text{alg}}$ such that $q^2 + q = F$ and $K[q] = K'$. Hence there exist $G, H \in K$ and $r \in K^{\text{alg}}$ such that $r^2 + r = Gq + H$ and $L' = K'[r] = K[q, r]$. Since $L' \subset L$ is not Galois over K, it follows that L is the Galois closure of $L' = K[q, r]$ over K, as desired. □

Proposition 3.2.2. *Suppose that $F, G, H \in K$, and $q, r, s \in K^{\text{alg}}$ such that $q^2 + q = F$, $r^2 + r = Gq + H$ and $s^2 + s = G$, and L is the Galois closure over K of $K[q, r]$. Then*

(1) *the degree two subfields of L are $K[q], K[s]$ and $K[q + s]$,*

(2) *the unique degree four normal subfield of L is $K[q, s]$,*

(3) *the two non-normal degree four subfields of L containing $K[q]$ are $K[q, r]$ and $K[q, r + s]$,*

(4) *the two non-normal degree four subfields of L containing $K[s]$ are $K[s, r + qs]$ and $K[s, r + qs + q]$, and*

(5) *$L = K[q, r, s]$.*

Remark 3.2.3. The situation described in Proposition 3.2.2 may be visualized as in Figure 3.2.

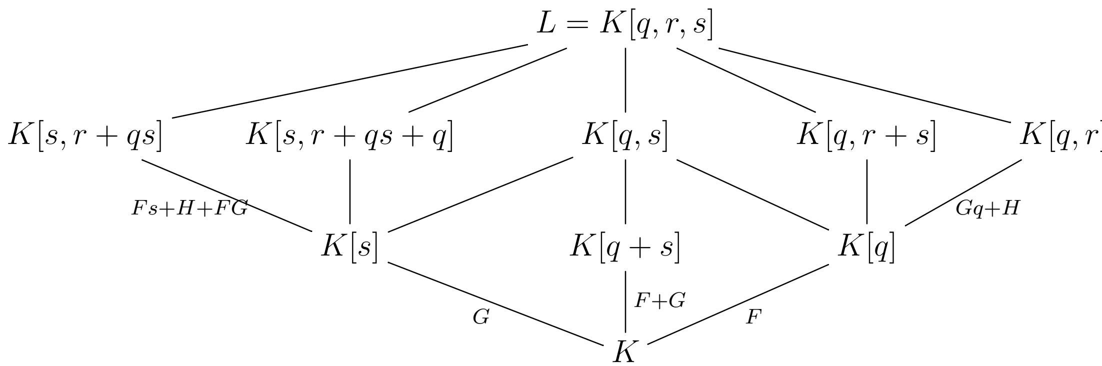

Figure 3.2: Subfields of L over K

Proof. Let $\sigma \in \mathrm{Gal}(L|K)$ such that $\sigma|_{K[q]}$ is non-trivial. Then the non-normal degree four subfields of L containing $K[q]$ are $K[q, r]$ and $\sigma(K[q, r])$. Since $(r+s)^2+(r+s) = Gq+H+G = \sigma(Gq+H)$, it follows that $\sigma(K[q, r]) = K[q, r+s]$. Statement (3) now follows immediately.

To prove (1), (2) and (5), note that, since $K[q, r]$ and $K[q, r+s]$ are both subfields of L, it follows that $s = r + (r + s) \in L$. Moreover, since $K[q, r]$ is not Galois over K, $[G] \neq 0$ over $K[q]$ by Lemma 3.1.4. Hence $K[q, s] = K[q][s]$ is a degree four extension of K. Since $\sigma(G) = G$, it follows by Lemma 3.1.4 that $K[q, s]$ is a Galois extension of K. Statement (2) now follows, and, since $K[q]$, $K[s]$, and $K[q + s]$ are the three degree two subfields of $K[q, s]$, so does (1). Finally, since $K[q, s]$ and $K[q, r]$ are distinct degree four subfields of L, $L = K[q, r, s]$; *i.e.*, (5) holds.

To prove (4), recall that $(qs)^2 + qs = Gq + Fs + FG$ by Lemma 3.1.1. Thus $[Gq + H] = [Fs + H + FG]$ over $K[q, s]$. Since $[G] \neq 0$ over $K[q]$, $[F] \neq 0$ over $K[s]$. As such, since $Fs + H + FG = (r + qs)^2 + (r + qs)$, it follows that $K[s, r + qs]$ is a non-Galois degree four subfield of L by Proposition 3.1.6. Hence the non-normal degree four subfields of L containing $K[s]$ are $K[s, r + qs]$ and $\tau(K[s, r + qs])$, where $\tau \in \mathrm{Gal}(L|K)$ such that $\tau|_{K[s]}$ is non-trivial. Since

$$(r + qs + q)^2 + (r + qs + q) = Fs + H + FG + F = \tau(Fs + H + FG),$$

it follows that $\tau(K[s, r+qs]) = K[s, r+qs+q]$. Statement (4) now follows immediately. □

3.3 Non-Cyclic Galois Extensions of Degree Eight over $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$-Extensions

Let K be a field of characteristic two, let K^{alg} be a fixed algebraic closure of K, and let $N \subseteq K^{\mathrm{alg}}$ be a Galois extension of K such that $\mathrm{Gal}(N|K) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Note that then there exist $F_0, F_1 \in K$, and $q_0, q_1 \in K^{\mathrm{alg}}$ such that $q_0^2+q_0 = F_0$, $q_1^2+q_1 = F_1$, and $N = K[q_0, q_1]$. Finally, let $q_2 = q_0 + q_1$, and let $F_2 = F_0 + F_1$.

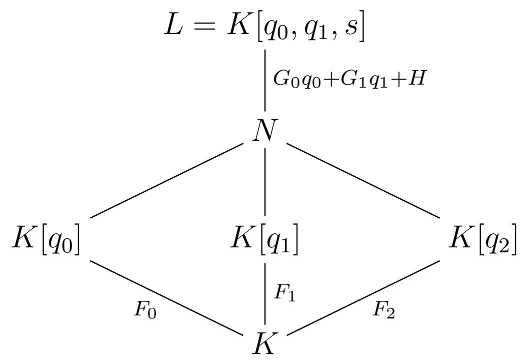

Figure 3.3: Subfields of L over K

Lemma 3.3.1. *The three degree two subfields of N over K are $K[q_0]$, $K[q_1]$ and $K[q_2]$.*

Proof. Since $N = K[q_0, q_1]$, it follows that $K[q_0]$ and $K[q_1]$ are distinct degree two subfields of N. Moreover, $q_2 = q_0 + q_1 \in N$, and $q_2^2 + q_2 = q_0^2 + q_0 + q_1^2 + q_1 = F_0 + F_1 = F_2 \in K$. Hence $K[q_2]$ is a degree two subfield of N. Since $K[q_0]$ and $K[q_1]$ are distinct degree two subfields, $K[q_2]$ is distinct from both. $\square$

Lemma 3.3.2. *Let $L \subseteq K^{\text{alg}}$ be a degree two Galois extension of N such that $L|K$ is a Galois extension. Then there exist $G_0, G_1, H \in K$ such that $L = N[s]$, where $s \in K^{\text{alg}}$ such that $s^2 + s = G_0q_0 + G_1q_1 + H$.*

Proof. Since $N = K[q_0, q_1]$, there exist $A, B, C, D \in K$ and $a \in K^{\text{alg}}$ such that

$$a^2 + a = Aq_0q_1 + Bq_0 + Cq_1 + D = (Aq_0 + C)q_1 + Bq_0 + D$$

and $L = N[a]$. Moreover, since $L|K$ is Galois, $L|K[q_0]$ is Galois; hence $[Aq_0 + C] = 0$ over $N = K[q_0][q_1]$ by Lemma 3.1.4. Applying Lemma 3.1.3 to the tower of fields $N \supseteq K[q_0] \supseteq K$, it follows that $[A] = 0$ over K. Hence there exists $\alpha \in K$ such that $\alpha^2 + \alpha = A$. Therefore, over N,

$$\begin{aligned}[Aq_0q_1] &= [\alpha^2 q_0q_1 + \alpha q_0q_1] = [\alpha^2(q_0^2 + F_0)(q_1^2 + F_1) + \alpha q_0q_1] \\ &= [\alpha^2 q_0^2q_1^2 + \alpha q_0q_1 + \alpha^2(q_0^2F_1 + q_1^2F_0 + F_0F_1)] \\ &= [\alpha^2\left((q_0 + F_0)F_1 + (q_1 + F_1)F_0 + F_0F_1\right)] \\ &= [\alpha^2F_1q_0 + \alpha^2F_0q_1 + \alpha^2F_0F_1].\end{aligned}$$

Let now $G_0 = B+\alpha^2F_1$, $G_1 = C+\alpha^2F_0$ and $H = D+\alpha^2F_0F_1$, and let $s \in K^{\text{alg}}$ such that $s^2+s = G_0q_0+G_1q_1+H$. Since $\alpha \in K$, it follows that $[Aq_0q_1+Bq_0+Cq_1+D] = [G_0q_0 + G_1q_1 + H]$ over N. Thus $L = N[s]$ by Proposition 2.2.1. $\square$

Remark 3.3.3. The situation described in Lemma 3.3.2 may be visualized as in Figure 3.3.

Proposition 3.3.4. *Let G_0, G_1, $H \in K$, let $s \in K^{\mathrm{alg}}$ such that $s^2 + s = G_0q_0 + G_1q_1 + H$, and let $L = N[s]$. Then $L|K$ is Galois if and only if $[G_0] = 0$ over N and $[G_1] = 0$ over N.*

Proof. Suppose first that $N = L$; *i.e.*, that $[G_0q_0 + G_1q_1 + H] = 0$ over N. Then $L|K$ is Galois. Moreover, $[G_0] = 0$ over N by Lemma 3.1.3 applied to $N|K[q_0]$, and $[G_1] = 0$ over N by Lemma 3.1.3 applied to $N|K[q_1]$. Hence the statement holds in this case.

Now suppose that $N \neq L$. Note that then $L|K$ is Galois if and only if $L|K[q_i]$ is Galois for all $i \in \{0, 1\}$. For each $i \in \{0, 1\}$, Lemma 3.1.4 implies that $L|K[q_i]$ is Galois if and only if $[G_{1-i}] = 0$ over N. Thus $L|K$ is Galois if and only if both $[G_0]$ and $[G_1]$ are trivial over N. □

Proposition 3.3.5. *Let $L \subseteq K^{\mathrm{alg}}$ be an extension of N of degree at most two such that L is Galois over K. Then there exist $G_0 \in \{0, F_0, F_1, F_2\}$, $G_1 \in \{0, F_1\}$, $H \in K$, and $s \in K^{\mathrm{alg}}$ such that $s^2 + s = G_0q_0 + G_1q_1 + H$, and $L = N[s]$.*

Proof. Observe that, by Lemma 3.3.2, there exist G_0', G_1' and $H' \in K$, and $s' \in K^{\mathrm{alg}}$ such that $(s')^2 + s' = G_0'q_0 + G_1'q_1 + H'$, and $N = L[s']$. By Proposition 3.3.4, $[G_0'] = [G_1'] = 0$ over N.

Let $X = \{0, F_0, F_1, F_2\}$, and let $i \in \{0, 1\}$. Applying Lemma 3.1.2 to $N|K[q_i]$ and then (twice) to $K[q_i]||K$ implies that there exists $C_i \in X$ such that $[G_i'] = [C_i]$ over K. Thus there exists $\alpha_i \in K$ such that $\alpha_i^2 + \alpha_i = C_i + G_i'$. By Lemma 3.1.3 applied to $K[q_i]||K$, it follows that $[(G_i'+C_i)q_i+\alpha_i^2F_i] = 0$ over $K[q_i]$. Therefore, over $N = K[q_0, q_1]$,

$$[G_0'q_0 + G_1'q_1 + H'] = [C_0q_0 + C_1q_1 + \alpha_0^2F_0 + \alpha_1^2F_1 + H'].$$

Note that either $C_1 \in \{0, F_1\}$, or that $C_1 \in \{F_0, F_2\}$. First suppose that $C_1 \in \{0, F_1\}$, and let $G_0 = C_0$, $G_1 = C_1$, and $H = \alpha_0^2F_0 + \alpha_1^2F_1 + H'$. Then $L = N[s'] = N[s]$, where $s \in K^{\mathrm{alg}}$ such that $s^2 + s = G_0q_0 + G_1q_1 + H$.

Now suppose that $C_1 \in \{F_0, F_2\}$, and let $G_0 = C_0 + F_1$, $G_1 = C_1 + F_0$, and $H = \alpha_0^2F_0 + \alpha_1^2F_1 + H' + F_0F_1$. By Lemma 3.1.1, $(q_0q_1)^2 + q_0q_1 = F_1q_0 + F_0q_1 + F_0F_1$. Thus, over N,

$$\begin{aligned}[C_0q_0 + C_1q_1 + \alpha_0^2F_0 + \alpha_1^2F_1 + H'] &= [G_0q_0 + F_1q_0 + G_1q_1 + F_0q_1 + H + F_0F_1] \\ &= [G_0q_0 + G_1q_1 + H].\end{aligned}$$

Hence $L = N[s'] = N[s]$, where $s \in K^{\mathrm{alg}}$ such that $s^2 + s = G_0q_0 + G_1q_1 + H$. □

Lemma 3.3.6. *Let L, G_0, G_1, H and s be as in Proposition 3.3.5. Then $L = N$ if and only if $G_0 = 0$, $G_1 = 0$, and $[H] = 0$ over N.*

Proof. Note that, by Proposition 2.2.1, $L = N$ if and only if $[G_0q_0+G_1q_1+H] = 0$ over N. Moreover, if $G_0 = 0$, $G_1 = 0$, and $[H] = 0$ over N, then $[G_0q_0+G_1q_1+H] = [H] = 0$ over N.

Suppose that $[G_0q_0+G_1q_1+H] = 0$ over N. Lemma 3.1.3 applied to the extension $N = K[q_0][q_1]$ over $K[q_0]$ implies that $[G_1] = 0$ over $K[q_0]$. Thus either $[G_1] = 0$ over

K, or $[G_1] = [F_0]$ over K by Lemma 3.1.2. Since $G_1 \in \{0, F_1\}$ by hypothesis, it follows that $G_1 = 0$, and that $[G_0q_0 + G_1q_1 + H] = [G_0q_0 + H]$.

To show that $G_0 = 0$, we now apply Lemma 3.1.3 to the extensions $N|K[q_1]$ and $N|K[q_2]$. The former application implies that $[G_0] = 0$ over $K[q_1]$; the latter implies that $[G_0] = 0$ over $K[q_2]$. Thus $[G_0] = 0$ over $K[q_1] \cap K[q_2] = K$. Since $G_0 \in \{0, F_0, F_1, F_2\}$, it follows that $G_0 = 0$, and hence that $0 = [G_0q_0 + H] = [H]$ over N. □

Proposition 3.3.7. *Let L, G_0, G_1, H and s be as in Proposition 3.3.5. Then the following statements, exactly one of which applies, all hold:*

(1) *If $G_0 = 0$, $G_1 = 0$, and $[H] = 0$ over N, then* $\mathrm{Gal}(L|K) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(2) *If $G_0 = 0$, $G_1 = 0$, and $[H] \neq 0$ over N, then* $\mathrm{Gal}(L|K) \cong (\mathbb{Z}/2\mathbb{Z})^3$.

(3) *If $G_0 = F_0$, and $G_1 = 0$, then* $\mathrm{Gal}(L|K) \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, *and* $\mathrm{Gal}(L|K[q_0]) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(4) *If $G_0 = 0$, and $G_1 = F_1$, then* $\mathrm{Gal}(L|K) \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, *and* $\mathrm{Gal}(L|K[q_1]) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(5) *If $G_0 = F_0$, and $G_1 = F_1$, then* $\mathrm{Gal}(L|K) \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, *and* $\mathrm{Gal}(L|K[q_2]) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(6) *If $G_0 = F_1$, and $G_1 = 0$, then* $\mathrm{Gal}(L|K) \cong D_4$, *and* $\mathrm{Gal}(L|K[q_2]) \cong \mathbb{Z}/4\mathbb{Z}$.

(7) *If $G_0 = F_2$, and $G_1 = 0$, then* $\mathrm{Gal}(L|K) \cong D_4$, *and* $\mathrm{Gal}(L|K[q_1]) \cong \mathbb{Z}/4\mathbb{Z}$.

(8) *If $G_0 = F_1$, and $G_1 = F_1$, then* $\mathrm{Gal}(L|K) \cong D_4$, *and* $\mathrm{Gal}(L|K[q_0]) \cong \mathbb{Z}/4\mathbb{Z}$.

(9) *If $G_0 = F_2$, and $G_1 = F_1$, then* $\mathrm{Gal}(L|K) \cong Q_8$.

Proof. Statement (1) follows directly from Lemma 3.3.6. Moreover, if the conditions of any one of the statements (2) through (9) applies, then Lemma 3.3.6 implies that L is a degree eight extension of K. Accordingly, to prove these statements, we suppose henceforth that L is a degree eight extension of K.

Note that, since $L|K$ has degree eight, for each $i \in \{0, 1, 2\}$, the extension $L|K[q_i]$ of degree four has Galois group isomorphic either to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or to $\mathbb{Z}/4\mathbb{Z}$. Furthermore, to determine the isomorphism class of $\mathrm{Gal}(L|K)$, it suffices to determine the number N of elements $i \in \{0, 1, 2\}$ for which $\mathrm{Gal}(L|K[q_i]) \cong \mathbb{Z}/4\mathbb{Z}$:

if $N = 0$, then $\mathrm{Gal}(L|K) \cong (\mathbb{Z}/2\mathbb{Z})^3$;

if $N = 1$, then $\mathrm{Gal}(L|K) \cong D_4$;

if $N = 2$, then $\mathrm{Gal}(L|K) \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$;

if $N = 3$, then $\mathrm{Gal}(L|K) \cong Q_8$.

Proposition 3.1.6 applied to $L|K[q_0]$ implies that

$$\mathrm{Gal}(L|K[q_0]) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{if } [G_1] = 0 \text{ over } K[q_0] \\ \mathbb{Z}/4\mathbb{Z} & \text{if } [G_1] = [F_1] \text{ over } K[q_0] \end{cases}. \tag{3.1}$$

Similarly, Proposition 3.1.6 applied to $L|K[q_1]$ implies that

$$\mathrm{Gal}(L|K[q_1]) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{if } [G_0] = 0 \text{ over } K[q_1] \\ \mathbb{Z}/4\mathbb{Z} & \text{if } [G_0] = [F_0] \text{ over } K[q_1] \end{cases}. \tag{3.2}$$

Moreover, since $G_0q_0 + G_1q_1 + H = (G_0 + G_1)q_0 + G_1q_2 + H$, Proposition 3.1.6 applied to $L|K[q_2]$ implies that

$$\mathrm{Gal}(L|K[q_2]) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{if } [G_0 + G_1] = 0 \text{ over } K[q_2] \\ \mathbb{Z}/4\mathbb{Z} & \text{if } [G_0 + G_1] = [F_0] \text{ over } K[q_2] \end{cases}. \tag{3.3}$$

The proposition now follows by applying, for each case, the isomorphisms (3.1), (3.2) and (3.3) to determine $\mathrm{Gal}(L|K)$ in that case. For example, if $G_0 = F_2$, and $G_1 = F_1$, then $[G_1] = [F_1]$ over $K[q_0]$, $[G_0] = [F_2] = [F_0]$ over $K[q_1]$, and $[G_0 + G_1] = [F_2 + F_1] = [F_0]$ over $K[q_2]$. Isomorphisms (3.1), (3.2) and (3.3) then imply that $\mathrm{Gal}(L|K[q_i]) \cong \mathbb{Z}/4\mathbb{Z}$ for all $i \in \{0, 1, 2\}$. Thus $\mathrm{Gal}(L|K) \cong Q_8$; *i.e.*, statement (9) holds. The seven statements remaining follow similarly. □

3.4 Q_8-Extensions of Fields of Characteristic Two

Let K be a field of characteristic two, let K^{alg} be a fixed algebraic closure of K, and let $L \subseteq K^{\mathrm{alg}}$ be a Galois extension of K such that $\mathrm{Gal}(L|K) \cong Q_8$.

Proposition 3.4.1. *There exist F_0, F_1, F_2, $H \in K$ and q_0, q_1, q_2, $s \in K^{\mathrm{alg}}$ such that $q_2 = q_0 + q_1$, $q_i^2 + q_i = F_i$ for all $i \in \{0, 1, 2\}$, $s^2 + s = F_1q_0 + F_2q_1 + F_0q_2 + H$, and $L = K[q_0, q_1, s]$.*

Proof. Let $N \subseteq L$ be the unique degree four subextension of $L|K$. Then $\mathrm{Gal}(N|K) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Hence there exist F_0, $F_1 \in K$, and q_0, $q_1 \in K^{\mathrm{alg}}$ such that $q_0^2 + q_0 = F_0$, $q_1^2 + q_1 = F_1$, and $N = K[q_0, q_1]$.

Now let $q_2 = q_0 + q_1$, and let $F_2 = F_0 + F_1$. Then $q_2^2 + q_2 = F_2$, as well. Moreover, by Propositions 3.3.5 and 3.3.7, there exist $H \in K$ and $s \in K^{\mathrm{alg}}$ such that $s^2 + s = F_2q_0 + F_1q_1 + H$, and $L = N[s] = K[q_0, q_1, s]$. Since

$$\begin{aligned} F_2q_0 + F_1q_1 + H &= F_2q_1 + F_2q_2 + F_1q_2 + F_1q_0 + H \\ &= F_1q_0 + F_2q_1 + F_0q_2 + H, \end{aligned}$$

the proposition follows immediately. □

Proposition 3.4.2. *Suppose that F_0, F_1, F_2, $H \in K$ and q_0, q_1, q_2, $s \in K^{\mathrm{alg}}$ such that $q_2 = q_0 + q_1$, $q_i^2 + q_i = F_i$ for all $i \in \{0, 1, 2\}$, $s^2 + s = F_1q_0 + F_2q_1 + F_0q_2 + H$, and $L = K[q_0, q_1, s]$. Then*

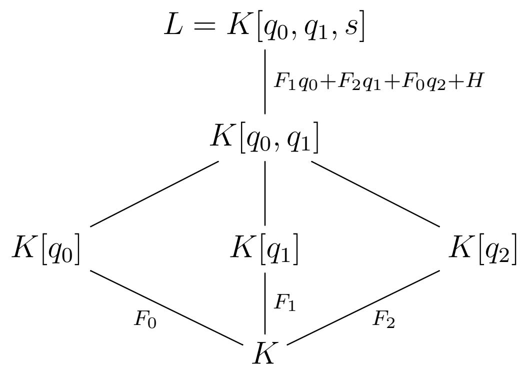

Figure 3.4: Subfields of L over K

(1) *the degree two subfields of* L *are* $K[q_0]$, $K[q_1]$ *and* $K[q_2]$,

(2) *the unique degree four subfield of* L *is* $K[q_0, q_1]$.

Remark 3.4.3. The situation described in Proposition 3.4.2 may be visualized as in Figure 3.4.

Proof. Since $L = K[q_0, q_1, s]$, and L is a degree eight extension of K, the field $L = K[q_0, q_1]$ is a degree four extension of K. It follows that (2) holds, and that $K[q_0]$ and $K[q_1]$ are distinct degree two extension of K. Thus $K[q_2] = K[q_0 + q_1]$ is a degree two extension of K that is both distinct from $K[q_0]$ and $K[q_1]$, and contained in $K[q_0, q_1]$. Statement (1) now follows. □

Chapter 4

D_4-Extensions of Complete Discrete Valuation Fields of Characteristic Two

4.1 Preliminary Results

4.1.1 Passage to Algebraically Closed Residue Field

Let k be a (not necessarily algebraically closed) field of characteristic two, let $K = k((t))$ be the field of Laurent series over k, and let k^{alg} denote a fixed algebraic closure of k, and let K^{alg} denote a fixed algebraic closure of k. The following proposition, adapted from exercises in Serre [Ser79], allows us to reduce computations of ramification breaks of totally ramified Galois extensions of complete discretely valued fields to the case in which the fields have algebraically closed residue field.

Proposition 4.1.1. *Let $k((s)) \subseteq K^{\mathrm{alg}}$ be a finite totally ramified Galois extension of $k((t))$, let $\Gamma = \mathrm{Gal}(k((s))|k((t)))$, and let L be the compositum of $k((s))$ and $k^{\mathrm{alg}}((t))$. Then*

(1) *L is a Galois extension of $k^{\mathrm{alg}}((t))$,*

(2) *$L = k^{\mathrm{alg}}((s))$,*

(3) *the canonical homomorphism*

$$\Phi : \mathrm{Gal}(L|k^{\mathrm{alg}}((t))) \to \mathrm{Gal}(k((s))|k((t)))$$

given by restriction is an isomorphism, and

(4) *$\Phi((\Gamma')^i) = \Gamma^i$, and $\Phi(\Gamma'_i) = \Gamma_i$ for all $i \geq -1$,*

where $\Gamma' = \mathrm{Gal}(L|k^{\mathrm{alg}}((t)))$.

Proof. Let $n = [k((s)) : k((t))]$. We observe that, since $k((s))$ is a totally ramified extension of $k((t))$, the degree of the characteristic polynomial of s over $k((t))$ is n. Thus $k((s)) = k((t))[s]$, and hence $L = k^{\mathrm{alg}}((t))[s]$. Since $k((t))[s]$ is a Galois extension of $k((t))$, it follows that L is a Galois extension of $k^{\mathrm{alg}}((t))$, and that the restriction homomorphism $\Phi : \mathrm{Gal}(L|k^{\mathrm{alg}}((t))) \to \mathrm{Gal}(k((s))|k((t)))$ is indeed defined.

To prove statement (3), we note that Φ is injective since L is the compositum of $k((s))$ and $\mathrm{Gal}(k((s))|k((t)))$, and that the fixed field $k((s))^{\mathrm{Im}\Phi}$ is equal to $E = k((s)) \cap k^{\mathrm{alg}}((t))$. Since $k((t))|k((s))$ is totally ramified, $E|k((s))$ is totally ramified, and so $v_E(t) = [E : k((s))]$. Moreover, $v_E(t) = 1$ since t is a uniformizer both in $k((t))$ and in $k^{\mathrm{alg}}((t))$. Hence $[E : k((s))] = 1$. Therefore, $k((s))^{\mathrm{Im}\Phi} = k((t))$, and Φ is surjective. Statement (3) now follows.

To prove statements (2) and (4), we observe that statement (3) implies that $v_L(t) = [L : k^{\mathrm{alg}}((t))] = n = v_{k((s))}(t)$. It follows that the restriction of the discrete valuation v_L on L to $k((s))$ is precisely the discrete valuation $v_{k((s))}$ on $k((s))$. Thus $v_L(s) = 1$, and $L = k((s))$. Moreover, since Φ is given by restriction, it follows that $\Phi(\sigma)(s) - s = \sigma(s) - s$ for all $\sigma \in \Gamma'$. Hence $v_L(\sigma(s) - s) = v_{k((s))}(\Phi(\sigma(s)) - s)$ for all $\sigma \in \Gamma'$. Statement (4) now follows by Definition 2.1.1. □

Corollary 4.1.2. *The sequences of the lower and of the upper ramification breaks of the extension $k^{\mathrm{alg}}((s))|k^{\mathrm{alg}}((t))$ are equal, respectively, to the sequences of the lower and of the upper ramification breaks of the extension $k((s))|k((t))$.*

4.1.2 Ramification Breaks and Conductors of Degree Four Extensions

In this subsection, we maintain the notation of the previous subsection, and insist moreover that the residue field k of $K = k((t))$ be algebraically closed. This guarantees that every finite extension of K is totally ramified over K. We begin with two lemmas, both adapted from Lemme 1.1.4 in [Ray99], for $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ extensions.

Lemma 4.1.3. *Let K_1 and K_2 be distinct Artin–Schreier extensions of K, and let K_3 be the unique degree two subfield of K_1K_2 distinct from both K_1 and K_2. Moreover, let c_1, c_2 and c_3 denote the conductors over K of K_1, K_2 and K_3, respectively. Suppose that $c_1 < c_2$. Then*

(1) $c_3 = c_2$,

(2) *the conductor of K_1K_2 over K_1 is $2c_2 - c_1$.*

(3) *the conductors both of K_1K_2 over K_2 and of K_1K_2 over K_3 are c_1,*

(4) *the sequence of lower ramification breaks of K_1K_2 over K is $(c_1, 2c_2 - c_1)$, and*

(5) *the sequence of upper ramification breaks of K_1K_2 over K is (c_1, c_2).*

Remark 4.1.4. The situation described in Lemma 4.1.3 may be visualized as in Figure 4.1.

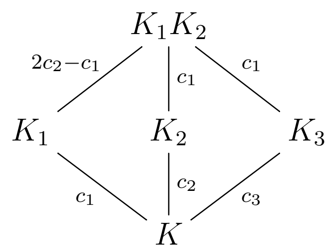

Figure 4.1: Conductors in Lemma 4.1.3 ($c_1 < c_2$)

Proof. Note that, since K_1 and K_2 are distinct, K_1K_2 is an Artin–Schreier extension both of K_1 and of K_2.

Let Γ denote the Galois group of K_1K_2 over K, and let H_1, H_2 and H_3 denote the subgroups of Γ consisting of those elements of Γ fixing K_1, K_2 and K_3, respectively. To prove statements (5) and (1), we observe that, by Proposition 2.1.7, $(\Gamma/H_j)^i = \Gamma^i H_j/H_j$ for all $i \geq -1, j \in \{1,2,3\}$. Thus each of the conductors c_j of Γ/H_j is an upper ramification break of K_1K_2 over K. Since $c_1 < c_2$, the sequence of upper ramification breaks of K_1K_2 over K is (c_1, c_2); *i.e.*, statement (5) holds. Hence $\Gamma^i H_1/H_1 = (\Gamma/H_1)^i = 1$ for all $i > c_1$, and $\Gamma^i = H_1$ for all $c_1 < i \leq c_2$. Thus $(\Gamma/H_3)^i = \Gamma^i H_3/H_3 = \Gamma/H_3$ for all $i \leq c_2$; as such, $c_3 = c_2$.

To prove statements (2) and (3), we consider the sequence of lower ramification breaks of K_1K_2 over K. The application of Proposition 2.1.11 to the corresponding sequence (c_1, c_2) of upper ramification breaks of K_1K_2 over K implies that this sequence is $(c_1, 2c_2 - c_1)$, *i.e.*, that statement (4) holds. Thus $\Gamma_i = H_1$ for all $c_1 < i \leq 2c_2 - c_1$. Since, by Proposition 2.1.5, $(H_j)_i = \Gamma_i \cap H_j$ for all $i \geq -1, j \in \{1,2,3\}$, it follows that

$$(H_1)_i = \Gamma_i \cap H_1 = \begin{cases} H_1 & \text{if } i \leq 2c_2 - c_1 \\ 1 & \text{if } i > 2c_2 - c_1 \end{cases}, \quad \text{and} \quad (H_j)_i = \Gamma_i \cap H_j = \begin{cases} H_j & \text{if } i \leq c_1 \\ 1 & \text{if } i > c_1 \end{cases}$$

for $j \in \{2,3\}$; *i.e.*, that the conductor of K_1K_2 over K_1 is $2c_2 - c_1$, and the conductors both of K_1K_2 over K_2 and of K_1K_2 over K_3 are c_1. □

Lemma 4.1.5. *Let K_1 and K_2 be distinct Artin–Schreier extensions of K, and let c_1 and c_2 denote the conductors over K of K_1 and K_2, respectively. Moreover, let K_3 be the unique degree two subfield of K_1K_2 distinct from both K_1 and K_2, and let c_3 be the conductor of K_3 over K. Suppose that $c_1 = c_2$. Then*

(1) $c_3 \leq c_1$,

(2) *the conductors both of K_1K_2 over K_1 and of K_1K_2 over K_2 are c_3.*

(3) *the conductor of K_1K_2 over K_3 is $2c_3 - c_1$,*

(4) *the sequence of lower ramification breaks of K_1K_2 over K is $(c_3, 2c_1 - c_3)$, and*

(5) *the sequence of upper ramification breaks of K_1K_2 over K is (c_3, c_1).*

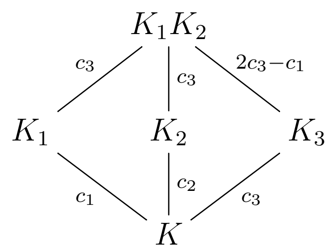

Figure 4.2: Conductors in Lemma 4.1.3 ($c_1 = c_2$)

Remark 4.1.6. The situation described in Lemma 4.1.5 may be visualized as in Figure 4.2.

Proof. Let Γ be the Galois group of K_1K_2 over K, and let H_1, H_2 and H_3 denote the subgroups of Γ consisting of those elements of Γ fixing K_1, K_2 and K_3, respectively.

Suppose that $c_3 > c_1 = c_2$. Then, as in Lemma 4.1.3, $\Gamma^i = H_1$ and $\Gamma^i = H_2$ for all $c_1 = c_2 < i \leq c_3$. Since $H_1 \neq H_2$, it follows that $c_3 \leq c_1$; *i.e.*, that (1) holds. Moreover, if $c_3 < c_1$, then statements (2) through (5) follow directly by the application of Lemma 4.1.3 to the extensions $K_3|K$ and $K_1|K$.

Now suppose that $c_3 = c_1$. Since, for each $j \in \{1, 2, 3\}$, the upper ramification group $(\Gamma/H_j)^i = \Gamma^i H_j/H_j$ is non-trivial for all $-1 \leq i \leq c_j = c_1$, and trivial for all $i > c_j = c_1$. Hence, for all $i \geq -1$,

$$\Gamma^i = \begin{cases} \Gamma & \text{if } i \leq c_1 \\ 1 & \text{if } i > c_1 \end{cases}.$$

Since $c_3 = 2c_3 - c_1 = c_1$, statements (2) through (5) now follow. $\square$

Lemmas 4.1.3 and 4.1.5 together imply the following proposition.

Proposition 4.1.7. *Let K_1 and K_2 be distinct Artin–Schreier extensions of K, and let c_1 and c_2 denote the conductors over K of K_1 and K_2, respectively. Moreover, let K_3 be the unique degree two subfield of K_1K_2 distinct from both K_1 and K_2, let c_3 be the conductor of K_3 over K, and let $X = \{c_1, c_2, c_3\}$. Then*

(1) *for all $i \in \{1, 2, 3\}$, the conductor of K_1K_2 over K_i is $2\max X + \min X - 2c_i$.*

(2) *the sequence of lower ramification breaks of K_1K_2 over K is $(\min X, 2\max X - \min X)$, and*

(3) *the sequence of upper ramification breaks of K_1K_2 over K is $(\min X, \max X)$.*

Proof. Note that statement (2) follows directly from the fourth statements of both Lemma 4.1.3 and Lemma 4.1.5, while statement (3) follows directly from the fifth statements of both Lemma 4.1.3 and Lemma 4.1.5.

To show statement (1), let i and j be distinct elements of $\{1, 2, 3\}$. If $c_i > c_j$, then $c_i = \max X$, and the conductor of K_1K_2 over K_i is $c_j = \min X = 2\max X +$

$\min X - 2c_i$ by Lemma 4.1.3 applied to the extensions $K_j|K$ and $K_i|K$. Similarly, if $c_i = c_j$, then $c_i = \max X$, and the conductor of K_1K_2 over K_i is $c_j = \min X = 2\max X + \min X - 2c_i$ by Lemma 4.1.5 applied to the extensions $K_j|K$ and $K_i|K$. Finally, if $c_i < c_j$, then $c_i = \min X$, and the conductor of K_1K_2 over K_i is $2c_j - c_i = 2\max X - \min X = 2\max X + \min X - 2c_i$ by Lemma 4.1.3 applied to the extensions $K_i|K$ and $K_j|K$. □

Now let $F, G, H \in K$ and $q, r, u \in K^{\mathrm{alg}}$ such that

$$q^2 + q = F, \quad r^2 + r = Gq + H \quad \text{and} \quad u^2 + u = H;$$

and let $f = \deg_{t^{-1}}(F)$, $g = \deg_{t^{-1}}(G)$ and $h = \deg_{t^{-1}}(H)$.

Proposition 4.1.8. *Suppose that f and g are both positive and odd, and that h is not both positive and even. The conductor of $K[q]$ over K is f. Moreover, the conductor of $K[q,r]$ over $K[q]$ is $2\max\{f+g, h\} - f$.*

Proof. Since the degree in t^{-1} of F is both odd and positive by hypothesis, the first claim follows immediately by Proposition 2.2.7. For the second claim, note that $v_{K[q]}(F) = -2f$, where $v_{K[q]}$ denotes the discrete valuation of the field $K[q]$, since $K[q]$ is a totally ramified extension of K. Thus $v_{K[q]}(q) = -f$, and $v_{K[q]}(Gq) = -(2g+f)$.

Let c_u denote the conductor of $K[q,u]$ over $K[q]$, and let C_u denote the conductor of $K[q, r+u]$ over $K[q]$. Since $v_q(Gq) = -(2g+f)$, and $2g+f$ is odd, $C_u = 2g+f$ by Proposition 2.2.7. Similarly, the conductor of $K[u]$ over K is h.

First, suppose that $h \leq 0$. Then $v_{K[q]}(H) \geq 0 > -(2g+f) = v_{K[q]}(Gq)$. Hence $v_{K[q]}(Gq+H) = -(2g+f)$; since $2g+f$ is odd, it follows by Proposition 2.2.7 that the conductor of $K[q,r]$ over $K[q]$ is $2g+f = 2\max\{f+g, h\} - f$.

Second, suppose that $0 < h \leq f$. If $h < f$, then $c_u = h$ by Lemma 4.1.3 applied to the extensions $K[u]|K$ and $K[q]|K$. If $h = f$, then $c_u \leq h$ by Lemma 4.1.5 applied to the extensions $K[u]|K$ and $K[q]|K$. In either case, $c_u \leq h \leq f < 2g+f = C_u$. Hence the conductor of $K[q,r]$ over $K[q]$ is $2g+f = 2(f+g) - f = 2\max\{f+g, h\} - f$ by Lemma 4.1.3 applied to the extensions $K[q, r+u]|K[q]$ and $K[q,r]|K[q]$.

Finally, suppose that $f < h$. Then $c_u = 2h - f$ by Lemma 4.1.3 applied to the extensions $K[q]|K$ and $K[u]|K$. Since f, g and h are all odd, $2g+f-(2h-f) = 2(f+g-h) \neq 0$; hence $C_u = 2g+f \neq 2h-f = c_u$. Thus the conductor of $K[q,r]$ over $K[q]$ is $\max\{2g+f, 2h-f\} = 2\max\{f+g, h\} - f$ by Lemma 4.1.3 applied to the extensions $K[q, r+u]|K[q]$ and $K[q,r]|K[q]$. □

Remark 4.1.9. The situation described in the proof of Proposition 4.1.8 may be visualized as in Figure 4.3.

Remark 4.1.10. Proposition 4.1.8 has the following corollary, which also (essentially) follows from a known result (see, *e.g.*, [Gar02]) on ramification breaks of Witt vectors.

Corollary 4.1.11. *Suppose that $F = G$ (so that $K[q,r]$ is a $\mathbb{Z}/4\mathbb{Z}$-extension of K by Proposition 3.1.6). Then the conductor of $K[q,r]$ over $K[q]$ is $2\max\{2f, h\} - f$. Moreover,*

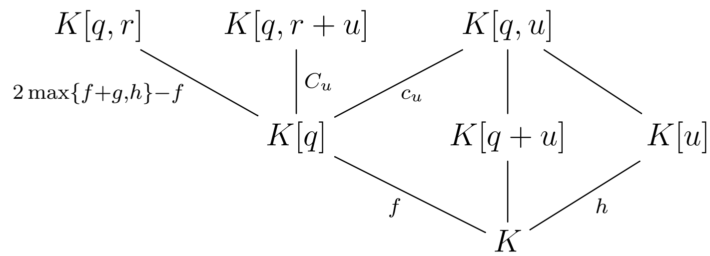

Figure 4.3

(1) *the sequence of lower ramification breaks of* $K[q,r]$ *over* K *is* $(f, 2\max\{2f,h\} - f)$*, and*

(2) *the sequence of upper ramification breaks of* $K[q,r]$ *over* K *is* $(f, \max\{2f,h\})$*.*

4.2 Standard and Odd Form D_4-Extensions

Having described the structure of D_4-extensions over all fields of characteristic two, in this section we restrict our attention to complete discrete valuation fields of characteristic two, and parametrize and classify D_4-extensions of complete discrete valuation fields of characteristic two with algebraically closed residue field. To this end, let k be a (not necessarily algebraically closed) field of characteristic two, let $K = k((t))$ be the field of Laurent series over k, and let K^{alg} denote a fixed algebraic closure of K.

Definition 4.2.1. A triple (F, G, H) of elements of K is a *standard form triple* if each of F, G and H is a standard form element of K with respect to t.

Definition 4.2.2. Let $L \subseteq K^{\text{alg}}$ be a Galois extension of K such that $\text{Gal}(L|K) \leq D_4$. The extension L over K is *generated by standard form elements* if there exists a standard form triple (F, G, H) such that L is the Galois closure of $K[q,r]$, where $q, r \in K^{\text{alg}}$ such that $q^2 + q = F$ and $r^2 + r = Gq + H$.

Remark 4.2.3. By Proposition 3.1.6, $\text{Gal}(L|K) \cong D_4$ unless $F = 0$, $G = 0$, or $F = G$. If $\text{Gal}(L|K) \cong D_4$, we say that L is a D_4*-standard form* extension of K.

The standard form triple (F, G, H) may be considered a sort of ‘canonical form’ for a D_4-standard form extension of K, though any given D_4-standard form extension is associated not to one triple, but to several.

Definition 4.2.4. A triple (F, G, H) of elements of K is a D_4*-odd form triple* if

(1) each of $\deg_{t^{-1}} F$, $\deg_{t^{-1}} G$ and $\deg_{t^{-1}}(F + G)$ is both positive and odd, and

(2) $\deg_{t^{-1}} H$ is not both positive and even.

Definition 4.2.5. Suppose that L is a D_4-Galois extension of K. The extension L over K is a D_4*-odd form* extension of K if there exists a D_4-odd form triple (F, G, H) such that $L = K[q, r, s]$, where $q, r, s \in K^{\text{alg}}$ such that $q^2 + q = F$, that $r^2 + r = Gq + H$, and that $s^2 + s = G$.

4.2.1 Parametrization of D_4-Extensions via Standard Form Elements

Suppose now that k is algebraically closed, and that L is an extension of K such that $\mathrm{Gal}(L|K) \cong D_4$.

Proposition 4.2.6. *There exist $F, G, H \in K = k((t))$ in standard form with respect to t, and $q, r \in K^{\mathrm{alg}}$ such that $q^2 + q = F, r^2 + r = Gq + H$, and L is the Galois closure over K of $K[q, r]$.*

Proof. By Proposition 3.2.1, there exist $F', G', H' \in K$, not necessarily in standard form, and $q', r', s' \in K^{\mathrm{alg}}$ such that $(q')^2 + q' = F'$, $(r')^2 + r' = G'q' + H'$, and $(s')^2 + s' = G'$, and such that L is the Galois closure over K of $K[q', r']$. Since k is algebraically closed, by Proposition 2.2.5 there exist unique elements $F, G \in K = k((t))$ in standard form such that $[F] = [F']$ and $[G] = [G']$, respectively, over K. Let $q, s \in K^{\mathrm{alg}}$ such that $q^2 + q = F$ and $s^2 + s = G$. Since

$$(q + q')^2 + (q + q') = \big(q^2 + q\big) + \big((q')^2 + q'\big) = F + F',$$

and since $[F] = [F']$ over K, it follows that $q + q' \in K$. Similarly, $s + s' \in K$, and thus $H' + G'(q + q') + F(s + s')^2 + G \in K$ as well. Therefore, there exists $H \in K$ in standard form such that $[H] = [H' + G'(q + q') + F(s + s')^2]$ over $K[q] = K[q']$. Let $r \in K^{\mathrm{alg}}$ such that $r^2 + r = Gq + H$. Then $K[q, r] = K[q', r']$ by Proposition 3.1.8. $\square$

Note that, by Proposition 3.2.2, $L = K[q, r, s]$. Proposition 3.2.1 thus has the following corollary:

Corollary 4.2.7. *The extension L is a D_4-standard form extension of K.*

As noted above, the standard form triple (F, G, H) is not unique; indeed, in this case any given D_4-extension of K is associated to eight distinct standard form triples, which are enumerated in the following proposition.

Proposition 4.2.8. *Let $L' \subseteq K^{\mathrm{alg}}$ be another Galois extension of K such that $\mathrm{Gal}(L'|K) \cong D_4$, and let F', G', H' be standard form elements of K (with respect to t) such that L' is the Galois closure of $K[q', r']$, where $q', r' \in K^{\mathrm{alg}}$ such that $(q')^2 + q' = F'$ and $(r')^2 + r' = Gq' + H'$. Then the fields L' and L are equal if and only if one of the four following conditions holds.*

(1) *$F' = F$, $G' = G$, and $[H'] = [H]$ over $K[q']$.*

(2) *$F' = F$, $G' = G$, and $[H'] = [H + G]$ over $K[q']$*

(3) *$F' = G$, $G' = F$, and $[H'] = [H + FG]$ over $K[q']$.*

(4) *$F' = G$, $G' = F$, and $[H'] = [H + FG + F]$ over $K[q']$.*

Proof. Note from Proposition 3.2.2 that L' and L are equal if and only if $K[q', r']$ is equal to one of the four non-normal degree four subfields $K[q, r], K[q, r + s], K[s, r + qs], K[s, r + qs + q]$ of L.

By Proposition 3.1.8, $K[q', r'] = K[q, r]$ if and only if condition (1) holds, and $K[q', r'] = K[q, r + s]$ if and only if condition (2) holds. Similarly, since $(r + qs)^2 = Fs + H + FG$ by Lemma 3.1.1, $K[q', r'] = K[s, r + qs]$ if and only if condition (3) holds, and $K[q', r'] = K[s, r + qs + q]$ if and only if condition (4) holds. □

Corollary 4.2.9. *Let $\mathcal{K}$ be the set of standard form elements of K, and let $\mathcal{G}$ be the set of Galois extensions of K contained in K^{alg} whose Galois group over K is isomorphic to D_4. Furthermore, let $\mathcal{D} = \{(\phi, \gamma, \eta) \in \mathcal{K}^3 \mid \phi = 0$ or $\gamma = 0$ or $\gamma = \phi\}$, and define $\Phi : \mathcal{K}^3 \backslash \mathcal{D} \to \mathcal{G}$ such that, for all $(\phi, \gamma, \eta) \in \mathcal{K}^3 \backslash \mathcal{D}$, $\Phi(\phi, \gamma, \eta)$ is the Galois closure of $K[\kappa, \rho]$, where $\kappa, \rho \in K^{\text{alg}}$ such that $\kappa^2 + \kappa = \phi$ and $\rho^2 + \rho = \gamma\kappa + \eta$. Then Φ is surjective.*

Remark 4.2.10. By Lemma 3.1.2, each condition in Proposition 4.2.8 corresponds to two pre-images under Φ of any given element of $\mathcal{G}$. Thus the surjection Φ is, in fact, eight-to-one.

4.3 Computation of Ramification Breaks

Let L be a D_4-extension of K. In this section, we shall, under the continued supposition that the residue field k of K is algebraically closed (so that $L|K$ is totally ramified), compute the ramification breaks of L over K. By Corollary 4.2.7, L is a D_4-standard form, and hence a D_4-odd form, extension of K.

Accordingly, we let (F, G, H) be a D_4-odd form triple corresponding to $L|K$; let $f = \deg_{t^{-1}}(F)$, $g = \deg_{t^{-1}}(G)$, $h = \deg_{t^{-1}}(H)$, and $d = \deg_{t^{-1}}(F + G)$; and let $q, r, s \in K^{\text{alg}}$ such that $q^2 + q = F$, that $r^2 + r = Gq + H$, that $s^2 + s = G$. By Definitions 4.2.4 and 4.2.5, the degrees f, g and d are all both positive and odd, the degree h is not both positive and even, and $L = K[q, r, s]$. We do not insist that the triple (F, G, H) be a standard form triple.

The degrees d, f, g and h suffice to determine the lower and upper ramification breaks of the extension L of K.

Lemma 4.3.1. *Let c_q and c_s denote the conductors over K of $K[q]$ and $K[s]$, respectively, and let c_r denote the conductor of $K[q, r]$ over $K[q]$. Then $c_r \geq 2c_s + c_q$.*

Proof. Observe that, by Proposition 2.2.7, $c_q = f$, and $c_q = g$. Moreover, $c_r = 2\max\{f + g, h\} - f$ by Lemma 4.1.8. Thus

$$c_r = 2\max\{f + g, h\} - f \geq 2(f + g) - f = 2g + f = 2c_s + c_q.$$ □

Proposition 4.3.2. *Let c_q, c_s and c_{q+s} denote the conductors over K of $K[q], K[s]$ and $K[q + s]$, respectively, and let c_r denote the conductor of $K[q, r]$ over $K[q]$. Then the lower ramification breaks of L over K are $\ell_1 = \min\{c_{q+s}, c_q, c_s\}$, $\ell_2 = 2\max\{c_{q+s}, c_q, c_s\} - \min\{c_{q+s}, c_q, c_s\}$ and*

$$\ell_3 = 2c_q + 2c_r - 2\max\{c_{q+s}, c_q, c_s\} - \min\{c_{q+s}, c_q, c_s\},$$

and the upper ramification breaks of L over K are $u_1 = \min\{c_{q+s}, c_q, c_s\}, u_2 = \max\{c_{q+s}, c_q, c_s\}$ *and* $u_3 = (c_q + c_r)/2$.

Proof. Let c_L denote the conductor of L over $K[q, s]$, let C_q denote the conductor of $K[q, s]$ over $K[q]$, and let $\Gamma = \mathrm{Gal}(L|K)$. By Proposition 3.2.2, $K[q, s]$ is the unique normal degree four subfield of L; thus, $\mathrm{Gal}(L|K[q, s])$ is the only normal subgroup of Γ of order two. By Proposition IV.1 in [Ser79], Γ_i is a normal subgroup of Γ for all i. In light of Proposition 2.1.5, it follows that $\ell_3 = c_L$. Similarly, by Proposition 2.1.7, u_1 and u_2 equal the first and second upper ramification breaks of $K[q, s]$ over K, respectively.

To determine u_1 and u_2, we observe that, since $K[q, s]$ is a $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$-extension of K, the sequence of upper ramification breaks of $K[q, s]$ over K is

$$(\min\{c_{q+s}, c_q, c_s\}, \max\{c_{q+s}, c_q, c_s\})$$

by Proposition 4.1.7. Thus $u_1 = \min\{c_{q+s}, c_q, c_s\}$, and $u_2 = \max\{c_{q+s}, c_q, c_s\}$. By Proposition 2.1.11, it follows that $\ell_1 = u_1 = \min\{c_{q+s}, c_q, c_s\}$, and that $\ell_2 = 2u_2 - u_1 = 2\max\{c_{q+s}, c_q, c_s\} - \min\{c_{q+s}, c_q, c_s\}$.

To compute ℓ_3 (and u_3), we note that either c_q or c_s is equal to $\max\{c_{q+s}, c_q, c_s\}$, and that thus

$$\max\{c_{q+s}, c_q, c_s\} + \min\{c_{q+s}, c_q, c_s\} \leq c_q + c_s$$

Therefore, by Proposition 4.1.7,

$$\begin{aligned} C_q &= 2\max\{c_{q+s}, c_q, c_s\} + \min\{c_{q+s}, c_q, c_s\} - 2c_q \\ &< 2(\max\{c_{q+s}, c_q, c_s\} + \min\{c_{q+s}, c_q, c_s\}) - 2c_q \\ &\leq 2(c_q + c_s) - 2c_q = 2c_s. \end{aligned}$$

Moreover, by Lemma 4.3.1, $c_r \geq 2c_s + c_q$. Thus $c_r > C_q$; hence

$$\ell_3 = c_L = 2c_r - C_q = 2c_q + 2c_r - 2\max\{c_{q+s}, c_q, c_s\} - \min\{c_{q+s}, c_q, c_s\}$$

by Lemma 4.1.3. Therefore,

$$\begin{aligned} u_3 &= \ell_1 + (\ell_2 - \ell_1)/2 + (\ell_3 - \ell_2)/4 = \ell_3/4 + \ell_2/4 + \ell_1/2 \\ &= (2c_q + 2c_r - 2\max\{c_{q+s}, c_q, c_s\} - \min\{c_{q+s}, c_q, c_s\})/4 \\ &+ (2\max\{c_{q+s}, c_q, c_s\} - \min\{c_{q+s}, c_q, c_s\})/4 + \min\{c_{q+s}, c_q, c_s\}/2 \\ &= (c_q + c_r)/2, \end{aligned}$$

the first equality holding by Proposition 2.1.11. □

Applying Proposition 4.1.8 to Proposition 4.3.2 yields the following corollary.

Corollary 4.3.3. *The lower ramification breaks of L over K are* $\ell_1 = \min\{d, f, g\}$, $\ell_2 = 2\max\{d, f, g\} - \min\{d, f, g\}$ *and*

$$\ell_3 = 4\max\{f + g, h\} - 2\max\{d, f, g\} - \min\{d, f, g\},$$

and the upper ramification breaks of L over K are $u_1 = \min\{d, f, g\}, u_2 = \max\{d, f, g\}$ *and* $u_3 = \max\{f + g, h\}$.

4.4 Characterization of Sequences of Ramification Breaks

In this subsection, we once again suppose that k is algebraically closed. By Corollary 4.2.7 it follows that every D_4-extension of K is a D_4-standard form extension of K. Moreover, by Proposition 4.2.8, every D_4-extension of K has a standard form triple (F', G', H') satisfying the additional condition $\deg_{t^{-1}} F' \leq \deg_{t^{-1}} G'$.

Suppose $\mathrm{Gal}(L|K) \cong D_4$. Recall that we have defined (in Defintion 2.1.9) the nth element of the sequence of ramification groups of L over K to be $\mathrm{Gal}(L|K)^{u_i}$, where u_i denotes the ith upper ramification break of $L|K$. We now define the sequence of ramification groups of L over K to be a *Type I* sequence if the sequence's second element is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, to be a *Type II* sequence if the sequence's second element is isomorphic to $\mathbb{Z}/4\mathbb{Z}$, and to be a *Type III* sequence if the sequence's second element is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Note that in all cases, the second ramification break is strictly smaller than the third; thus the sequence's third element is always isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

The type of the sequence of ramification groups of the extension L over K informs, to a large extent, which of the equicharacteristic deformations in Section 6.1 may and will be applied to the extension L. Moreover, the type of an extension's sequence of ramification groups affects the possible sequences of lower and of upper ramification breaks of that extension significantly. In this subsection, we consider (in the case where k is algebraically closed) the relation between the type of an extension's sequence of ramification groups and the sequences of lower and of upper ramification breaks of that sequence exhaustively.

Let $\mathcal{C}$ denote the set of triples (F', G', H') of standard form elements of K such that F', G' and 0 are pairwise distinct, and let Φ denote the surjection from $\mathcal{C}$ to the set of D_4-extensions of K defined in Corollary 4.2.9.

Lemma 4.4.1. *Let $(\alpha, \beta, \gamma) \in (\mathbb{Z}^+)^3$ such that α is odd, $\alpha \leq \beta$, β is odd, $\gamma \geq \alpha + \beta$, and γ is odd if $\gamma \notin \{\alpha + \beta, 2\beta\}$. Also, let $G = t^{-\beta}$, let*

$$F = \begin{cases} \zeta_3 t^{-\alpha} & \text{if } \alpha = \beta \\ t^{-\beta} + t^{-\alpha} & \text{if } \alpha < \beta \text{ and } \gamma = 2\beta \\ t^{-\alpha} & \text{if } \alpha < \beta \text{ and } \gamma \neq 2\beta \end{cases}, \quad \text{and let} \quad H = \begin{cases} t^{-\gamma} & \text{if } \gamma \text{ is odd} \\ 0 & \text{if } \gamma \text{ is even} \end{cases},$$

where $\zeta_3 \in k$ is a primitive cube root of unity. Then $(F, G, H) \in \mathcal{C}$, and the sequence of upper ramification breaks of the D_4-extension $\Phi((F, G, H))$ of K is (α, β, γ).

Proof. Since α and β are both odd, F, G and H are all standard form elements of K. Since F, G and 0 are pairwise distinct, it follows that $(F, G, H) \in \mathcal{C}$.

Let $f = \deg_{t^{-1}}(F)$, $g = \deg_{t^{-1}}(G)$, $h = \deg_{t^{-1}}(H)$, and $d = \deg_{t^{-1}}(F + G)$. Then $f \leq \beta = g$. Hence the sequence of upper ramification breaks of $L = \Phi((F, G, H))$ is $(u_1, u_2, u_3) = (\min\{d, f\}, g, \max\{f + g, h\})$ by Corollary 4.3.3. Thus $u_2 = g = \beta$.

Suppose $\alpha = \beta$. Then $F + G = (\zeta_3 + 1)t^{-\alpha} = \zeta_3^2 t^{-\alpha}$, and $d = f = g = \alpha$. Hence $u_1 = \alpha$, and $u_3 = \max\{\alpha + \beta, h\}$. Moreover, $\alpha = \beta$ implies that γ is odd if and only if $\gamma > \alpha + \beta$. Thus $u_3 = \gamma$.

Now suppose that $\alpha < \beta$, and that $\gamma = 2\beta$. Then $F + G = t^{-\alpha}$. Hence $d = \alpha$, $f = g = \beta$, and $h = 0$. Thus $u_1 = \min\{\alpha, \beta\} = \alpha$, and $u_3 = \max\{2\beta, 0\} = 2\beta = \gamma$.

Finally, suppose that $\alpha < \beta$, and that $\gamma \neq 2\beta$. Then $F + G = t^{-\beta} + t^{-\alpha}$. Hence $f = \alpha$, and $d = g = \beta$. Thus $u_1 = \min\{\alpha, \beta\} = \alpha$, and $u_3 = \max\{\alpha + \beta, h\}$. Moreover, $\gamma \neq 2\beta$ implies that γ is odd if and only if $\gamma > \alpha + \beta$. Thus $u_3 = \gamma$. □

Proposition 4.4.2. *Let $(\alpha, \beta, \gamma) \in (\mathbb{Z}^+)^3$. Then (α, β, γ) is the sequence of upper ramification breaks for a D_4-extension of K if and only if α is odd, $\alpha \leq \beta$, β is odd, $\gamma \geq \alpha + \beta$, and γ is odd if $\gamma \notin \{\alpha + \beta, 2\beta\}$. Moreover, if M is a D_4-extension of K with sequence of upper ramification breaks (α, β, γ), then*

(1) *M has a Type I sequence of ramification groups if $\gamma < 2\beta$;*

(2) *M has a Type II sequence of ramification groups if $\alpha < \beta$ and $\gamma = 2\beta$;*

(3) *M has a Type I or a Type II sequence of ramification groups if $\alpha < \beta$ and $\gamma > 2\beta$;*

(4) *M has a Type III sequence of ramification groups if and only if $\alpha = \beta$.*

Proof. Since Φ is surjective, the triple (α, β, γ) is the sequence of upper ramification breaks for a D_4-extension of K if and only if there is a triple in $\mathcal{C}$ whose image under Φ has (α, β, γ) as its sequence of upper ramification breaks. Lemma 4.4.1 provides such a triple in $\mathcal{C}$ if (α, β, γ) satisfies the conditions of the unnumbered claim of the proposition.

To prove the converse, let $(F, G, H) \in \mathcal{C}$, and let $f = \deg_{t^{-1}}(F)$, $g = \deg_{t^{-1}}(G)$, $h = \deg_{t^{-1}}(H)$, and $d = \deg_{t^{-1}}(F+G)$. By Proposition 4.2.8, we may and do assume, without loss of generality, that $f \leq g$. Then the sequence of upper ramification breaks of $L = \Phi((F, G, H))$ is $(u_1, u_2, u_3) = (\min\{d, f\}, g, \max\{f + g, h\})$ by Corollary 4.3.3. Moreover, it follows that f, d and g are all both odd and positive, that h is either both odd and positive or equal to $-\infty$, that $d = g$ if $f < g$, and that $d \leq f$ if $f = g$. These conditions imply that u_1 is odd, that $u_1 \leq u_2$, that u_2 is odd, and that $u_3 \geq u_1 + u_2$.

Suppose first that $f < g = d$. Then $u_1 = f < g = u_2$. Hence the second element of the sequence of ramification groups of L over K is $\mathrm{Gal}(L|K[q]) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$; *i.e.*, L has a Type I sequence of ramification groups. Moreover, $u_3 = \max\{u_1 + u_2, h\}$. Thus u_3 is odd if $u_3 \neq u_1 + u_2$.

Suppose second that $d < f = g$. Then $u_1 = d < g = u_2$. Hence the second element of the sequence of ramification groups of L over K is $\mathrm{Gal}(L|K[q + s]) \cong \mathbb{Z}/4\mathbb{Z}$; *i.e.*, L has a Type II sequence of ramification groups. Moreover, $u_3 = \max\{2u_2, h\}$. Thus $u_3 \geq 2u_2$, and u_3 is odd if $u_3 \neq 2u_2$.

Suppose third that $d = f = g$. Then $u_1 = g = u_2$. Hence the second element of the sequence of ramification groups of L over K is $\mathrm{Gal}(L|K[q, s]) \cong \mathbb{Z}/2\mathbb{Z}$; *i.e.*, L has a Type III sequence of ramification groups. Moreover, $u_3 = \max\{2u_2, h\}$. Thus $u_3 \geq 2u_2$, and u_3 is odd if $u_3 \neq 2u_2$.

Note that in all cases, u_3 is odd if $u_3 \notin \{u_1 + u_2, 2u_2\}$. The unnumbered claim of the proposition now follows. Moreover, statement (4) holds since $u_1 < u_2$ in the first and second cases and $u_1 = u_2$ in the third case. Since $u_3 \geq 2u_2$ in the second case and $2u_2 > u_3 \geq u_1 + u_2$ implies that $u_1 < u_2$, statement (1) holds as well. Finally, statements (2) and (3) both hold since u_3 is odd in the first case if $u_3 > u_1 + u_2$, and since there is no restriction in either the first or the second case on u_3 if $u_3 > 2u_2 > u_1 + u_2$, save that in both cases u_3 must be odd. □

The following proposition is the precise analogue to Proposition 4.4.2 concerning the lower ramification breaks of D_4; accordingly, we omit its proof.

Proposition 4.4.3. *Let* $(a, b, c) \in (\mathbb{Z}^+)^3$. *Then* (a, b, c) *is the sequence of lower ramification breaks for a* D_4*-extension of* K *if and only if* a *is odd,* $a \leq b$, $a \equiv b \pmod 4$, $c \geq 4a + b$, *and* $b \equiv c \pmod 8$ *if* $c \notin \{4a + b, 2a + 3b\}$. *Moreover, if* M *is a* D_4*-extension of* K *with sequence of lower ramification breaks* (a, b, c), *then*

(1) *M has a Type I sequence of ramification groups if* $c < 2a + 3b$.

(2) *M has a Type II sequence of ramification groups if* $a < b$ *and* $c = 2a + 3b$.

(3) *M has a Type I or a Type II sequence of ramification groups if* $a < b$ *and* $c > 2a + 3b$.

(4) *M has a Type III sequence of ramification groups if and only if* $a = b$.

Chapter 5

Q_8-Extensions of Complete Discrete Valuation Fields of Characteristic Two

5.1 Standard and Odd Form Q_8-Extensions

Let k be a (not necessarily algebraically closed) field of characteristic two, let $K = k((t))$ be the field of Laurent series over k, let K^{alg} denote a fixed algebraic closure of K.

Definition 5.1.1. Let $L \subseteq K^{\text{alg}}$ be a Galois extension of K such that $\text{Gal}(L|K) \leq Q_8$. The extension L over K is *generated by standard form elements* if there exists a standard form triple (F_0, F_1, H) such that $L = K[q_0, q_1, s]$, where $F_2 \in K$ and $q_0, q_1, q_2, s \in K^{\text{alg}}$ such that

(1) $q_2 = q_0 + q_1$,

(2) $q_i^2 + q_i = F_i$ for all $i \in \{0, 1, 2\}$ (so that $F_2 = F_0 + F_1$), and

(3) $s^2 + s = F_1 q_0 + F_2 q_1 + F_0 q_2 + H$.

Remark 5.1.2. By Proposition 3.3.7, $\text{Gal}(L|K) \cong Q_8$ unless $F_i = 0$ for some $i \in \{0, 1, 2\}$. If $\text{Gal}(L|K) \cong Q_8$, we say that L is a Q_8*-standard form* extension of K.

The standard form triple (F_0, F_1, H) may be considered a sort of 'canonical form' for a Q_8-standard form extension of K, though, as in the D_4 case, any given Q_8-standard form extension is associated not to one triple, but to several.

Definition 5.1.3. A triple (F_0, F_1, H) of elements of K is an Q_8*-odd form triple* if

(1) each of $\deg_{t^{-1}} F_0$, $\deg_{t^{-1}} F_1$ and $\deg_{t^{-1}} F_2$ is both positive and odd, and

(2) $\deg_{t^{-1}} H$ is not both positive and even,

where $F_2 = F_0 + F_1$.

Definition 5.1.4. The Galois extension L over K is a Q_8-*odd form* extension of K if, firstly, $\mathrm{Gal}(L|K) \cong Q_8$ and, secondly, there exists a Q_8-odd form triple (F_0, F_1, H) such that $L = K[q_0, q_1, s]$, where $F_2 \in K$ and $q_0, q_1, q_2, s \in K^{\mathrm{alg}}$ such that

(1) $q_2 = q_0 + q_1$,

(2) $q_i^2 + q_i = F_i$ for all $i \in \{0, 1, 2\}$ (so that $F_2 = F_0 + F_1$), and

(3) $s^2 + s = F_1 q_0 + F_2 q_1 + F_0 q_2 + H$.

5.1.1 Parametrization of Q_8-Extensions via Standard Form Elements

Suppose now that k is algebraically closed and that L is an extension of K such that $\mathrm{Gal}(L|K) \cong Q_8$.

Proposition 5.1.5. *The extension L is a Q_8-standard form extension of K; that is, there exist $F_0, F_1, F_2, H \in K = k((t))$ in standard form with respect to t, and $q_0, q_1, q_2, s \in K^{\mathrm{alg}}$ such that $q_2 = q_0 + q_1$, that $(q_i)^2 + q_i = F_i$ for all $i \in \{0, 1, 2\}$ (so that $F_2 = F_0 + F_1$), that $s^2 + s = F_1 q_0 + F_2 q_1 + F_0 q_2 + H$, and that $L = K[q_0, q_1, s]$.*

Proof. By Proposition 3.4.1, there exist F_0', F_1', F_2', $H' \in K$, not necessarily in standard form, and q_0', q_1', q_2', $s' \in K^{\mathrm{alg}}$ such that $q_2' = q_0' + q_1'$, that $(q_i')^2 + q_i' = F_i'$ for all $i \in \{0, 1, 2\}$, that

$$\begin{aligned}(s')^2 + s' &= F_1' q_0' + F_2' q_1' + F_0' q_2' + H' = F_1' q_0' + F_2' q_1' + F_0'(q_0' + q_1') + H' \\ &= F_2' q_0' + F_1' q_1' H',\end{aligned}$$

and that $L = K[q_0', q_1', s']$. Since k is algebraically closed, by Proposition 2.2.5 there exist unique elements $F_0, F_1 \in K = k((t))$ in standard form such that $[F_0] = [F_0']$ and $[F_1] = [F_1']$, respectively, over K. Let $F_2 = F_0 + F_1$, and note that then F_2 is the unique element in standard form such that $[F_2] = [F_2']$ over K. Moreover, let $q_0, q_1, q_2 \in K^{\mathrm{alg}}$ such that $q_2 = q_0 + q_1$, and $q_i^2 + q_i = F_i$ for all $i \in \{0, 1, 2\}$.

Let $i \in \{0, 1, 2\}$. Then, since

$$(q_i + q_i')^2 + (q_i + q_i') = \left(q_i^2 + q_i\right) + \left((q_i')^2 + q_i'\right) = F_i + F_i',$$

and $[F_i] = [F_i']$ over K, it follows that $q_i + q_i' \in K$. Therefore,

$$H' + F_1'(q_1 + q_1') + F_1(q_1 + q_1')^2 + F_2'(q_0 + q_0') + F_0(q_2 + q_2')^2 \in K.$$

Thus there exists $H \in K$ in standard form with respect to t such that

$$[H] = [H' + F_1'(q_1 + q_1') + F_1(q_1 + q_1')^2 + F_2'(q_0 + q_0') + F_0(q_2 + q_2')^2]$$

over K.

Let $s \in K^{\mathrm{alg}}$ such that

$$s^2 + s = F_1 q_0 + F_2 q_1 + F_0 q_2 + H = F_2 q_0 + F_1 q_1 + H.$$

Note that $K[q_1'] = K[q_1]$ since $[F_1] = [F_1']$ over K. Therefore, by Proposition 3.1.8, $L = K[q_1'][q_0', s'] = K[q_1][q_0, s] = K[q_0, q_1, s]$ if and only $[F_2] = [F_2']$ over $K[q_1]$, and

$$[F_1q_1 + H] = [F_1'q_1' + H' + F_2'(q_0 + q_0') + F_0(q_2 + q_2')^2]$$

over $K[q_0, q_1]$.

Since $[F_2] = [F_2']$ over K, it follows *a fortiori* that $[F_2] = [F_2']$ over $K[q_1]$. Moreover, by Lemma 3.1.7 applied to the tower $K[q_0, q_1] \supseteq K[q_1] \supseteq K$ of fields,

$$[F_1q_1] = [F_1'q_1' + F_1'(q_1 + q_1') + F_1(q_1 + q_1')^2]$$

over $K[q_1]$. Hence

$$\begin{aligned}[F_1q_1 + H] &= [F_1q_1 + H' + F_1'(q_1 + q_1') + F_1(q_1 + q_1')^2 + F_2'(q_0 + q_0') + F_0(q_2 + q_2')^2] \\ &= [F_1'q_1' + H' + F_2'(q_0 + q_0') + F_0(q_2 + q_2')^2]\end{aligned}$$

over $K[q_1]$. Therefore, $L = K[q_0, q_1, s]$ by Proposition 3.1.8. □

As noted above, the standard form triple (F_0, F_1, H) is not unique; indeed, in this case any given Q_8-extension of K is associated to twenty-four distinct standard form triples, which are enumerated in the following proposition.

Proposition 5.1.6. *Let $L' \subseteq K^{\text{alg}}$ be another Galois extension of K such that $\text{Gal}(L'|K) \cong Q_8$, and let F_0', F_1', F_2', H' be standard form elements of K (with respect to t) such that $L' = K[q_0', q_1', s']$, where $q_0', q_1', q_2', s' \in K^{\text{alg}}$ such that $q_2' = q_0' + q_1'$, that $(q_i')^2 + q_i = F_i$ for all $i \in \{0, 1, 2\}$ (so that $F_2' = F_0' + F_1'$), and that $(s')^2 + s' = F_1'q_0' + F_2'q_1' + F_0'q_2' + H'$. Then the fields L' and L are equal if and only if one of the six following conditions holds.*

(1) *$F_0' = F_0$, $F_1' = F_1$, and $[H'] = [H]$ over $K[q_0', q_1']$.*

(2) *$F_0' = F_1$, $F_1' = F_2$, and $[H'] = [H]$ over $K[q_0', q_1']$.*

(3) *$F_0' = F_2$, $F_1' = F_0$, and $[H'] = [H]$ over $K[q_0', q_1']$.*

(4) *$F_0' = F_0$, $F_1' = F_2$, and $[H'] = [H + F_0F_1]$ over $K[q_0', q_1']$.*

(5) *$F_0' = F_1$, $F_1' = F_0$, and $[H'] = [H + F_0F_1]$ over $K[q_0', q_1']$.*

(6) *$F_0' = F_2$, $F_1' = F_1$, and $[H'] = [H + F_0F_1]$ over $K[q_0', q_1']$.*

Proof. Observe that, by Proposition 3.4.2, L' and L are equal if and only if both $K[q_0, q_1] = K[q_0', q_1']$, and $[F_1q_0 + F_2q_1 + F_0q_2 + H] = [F_1'q_0' + F_2'q_1' + F_0'q_2' + H']$ over $K[q_0, q_1]$. Moreover, since $K[q_0, q_1]$ and $K[q_0', q_1']$ are both $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$-extensions of K, the two extensions are equal if and only if both extensions contain the same set of degree two subextensions of K, *i.e.*, if and only if $\{K[q_0], K[q_1], K[q_2]\} = \{K[q_0'], K[q_1'], K[q_2']\}$. Since, for all $i \in \{0, 1, 2\}$, both F_i and F_i' are standard form elements of K, it follows by Proposition 2.2.5 that $K[q_0, q_1] = K[q_0', q_1']$ if and only if $\{F_0, F_1, F_2\} = \{F_0', F_1', F_2'\}$.

Suppose henceforth that $K[q_0, q_1] = K[q_0', q_1']$. It suffices to show that $[F_1q_0 + F_2q_1 + F_0q_2 + H] = [F_1'q_0' + F_2'q_1' + F_0'q_2' + H']$ over $K[q_0, q_1]$ if and only if one of the six conditions listed in the proposition holds. To show this, it is convenient to let $i, j \in \{0, 1, 2\}$ such that $F_0' = F_i$ and $F_1' = F_j$. Then either $j \equiv i + 1 \pmod 3$ or $j \equiv i - 1 \pmod 3$.

First suppose that $j \equiv i+1 \pmod 3$. Then $F_1'q_0'+F_2'q_1'+F_0'q_2' = F_1q_0+F_2q_1+F_0q_2$. As such, in this case, $[F_1'q_0'+F_2'q_1'+F_0'q_2'+H'] = [F_1q_0+F_2q_1+F_0q_2+H]$ over $K[q_0, q_1]$ if and only if $[H'] = [H]$ over $K[q_0, q_1]$, *i.e.*, if and only if one of conditions (1) through (3) holds.

Now suppose that $j \equiv i - 1 \pmod 3$. Then

$$\begin{aligned} F_1'q_0' + F_2'q_1' + F_0'q_2' &= F_1q_2 + F_0q_1 + F_2q_0 \\ &= F_1q_2 + F_1q_1 + F_2q_1 + F_0q_0 + F_1q_0 \\ &= F_1q_0 + F_2q_1 + F_0q_2 + F_0q_1 + F_1q_0. \end{aligned}$$

By Lemma 3.1.1, $[F_0q_1 + F_1q_0] = [F_0F_1]$ over $K[q_0, q_1]$. Hence

$$[F_1'q_0' + F_2'q_1' + F_0'q_2' + H'] = [F_1q_0 + F_2q_1 + F_0q_2 + F_0F_1 + H'].$$

Therefore, in this case, $[F_1'q_0' + F_2'q_1' + F_0'q_2' + H'] = [F_1q_0 + F_2q_1 + F_0q_2 + H]$ over $K[q_0, q_1]$ if and only if $[H'] = [H + F_0F_1]$ over $K[q_0, q_1]$, *i.e.*, if and only if one of conditions (4) through (6) holds. □

Corollary 5.1.7. *Let $\mathcal{K}$ be the set of standard form elements of K, and let $\mathcal{G}$ be the set of Galois extensions of K contained in K^{alg} whose Galois group over K is isomorphic to Q_8. Furthermore, let $\mathcal{D} = \{(\phi_0, \phi_1, \eta) \in \mathcal{K}^3 \mid \phi_0 = 0$ or $\phi_1 = 0$ or $\phi_0 = \phi_1\}$, and define $\Phi : \mathcal{K}^3 \backslash \mathcal{D} \to \mathcal{G}$ such that, for all $(\phi_0, \phi_1, \eta) \in \mathcal{K}^3 \backslash \mathcal{D}$,*

$$\Phi(\phi, \gamma, \eta) = K[\kappa_0, \kappa_1, \sigma],$$

where $\kappa_0, \kappa_1, \sigma \in K^{\text{alg}}$ such that $\kappa_0^2 + \kappa_0 = \phi_0$, $\kappa_1^2 + \kappa_1 = \phi_1$, and

$$\sigma^2 + \sigma = \phi_1\kappa_0 + (\phi_0 + \phi_1)\kappa_1 + \phi_0(\kappa_0 + \kappa_1) + \eta.$$

Then Φ is surjective.

Remark 5.1.8. By Lemma 3.1.2 (applied twice), each condition in Proposition 5.1.6 corresponds to four pre-images under Φ of any given element of $\mathcal{G}$. Thus the surjection Φ is, in fact, twenty-four-to-one.

5.2 Computation of Ramification Breaks

Let L be a Q_8-extension of K. In this section, we shall, under the continued supposition that the residue field k of K is algebraically closed, compute the ramification breaks of L over K. By Proposition 5.1.5, L is a Q_8-standard form, and hence a Q_8-odd form, extension of K.

Accordingly, we let (F_0, F_1, H) be a Q_8-odd form triple corresponding to $L|K$; let $f_0 = \deg_{t^{-1}}(F_0)$, $f_1 = \deg_{t^{-1}}(F_1)$, $f_2 = \deg_{t^{-1}}(F_0 + F_1)$, $h = \deg_{t^{-1}}(H)$, and $d = \deg_{t^{-1}}(F_0F_1 + F_1F_2 + F_2F_0)$; and let $F_2 \in K$, and $q_0, q_1, q_2, s \in K^{\text{alg}}$ such that $q_2 = q_0 + q_1$, that $q_i^2 + q_i = F_i$ for all $i \in \{0, 1, 2\}$ (so that $F_2 = F_0 + F_1$), and that $s^2 + s = F_1q_0 + F_2q_1 + F_0q_2 + H$. Finally, we let $N = K[q_0, q_1]$, and, for all $\ell \in \mathbb{Z}$, we let ℓ' denote the unique element of $\{0, 1, 2\}$ such that $\ell \cong \ell' \pmod 3$.

By Definitions 5.1.3 and 5.1.4, the degrees f_0, f_1 and f_2 are all both positive and odd, the degree h is not both positive and even, the degree d is either equal to zero or congruent to 2 (mod 4), and $L = K[q_0, q_1, s]$. Moreover, we can and do assume, without loss of generality, that $f_0 = \min\{f_0, f_1, f_2\}$. Then $f_1 = f_2$ by Lemma 4.1.3.

The degrees f_0, f_1 and h suffice to determine the lower and upper ramification breaks of the extension L of K if $f_0 < f_1$, but not do suffice if $f_0 = f_1$. In determining these ramification breaks, it is convenient to let c_L denote the conductor of the extension L over $K[q_0, q_1]$.

Lemma 5.2.1. *The lower ramification breaks of L over K are $\ell_1 = f_0$, $\ell_2 = 2f_1 - f_0$, and $\ell_3 = c_L$, and the upper ramification breaks of L over K are $u_1 = f_0$, $u_2 = f_1$, and $u_3 = (c_L + f_0)/4 + f_1/2$.*

Proof. Let $\Gamma = \text{Gal}(L|K)$. By Proposition 3.4.2, $N = K[q_0, q_1]$ is the unique degree four subfield of L; thus, $\text{Gal}(L|N)$ is the unique subgroup of Γ of order two. By Proposition IV.1 in [Ser79], Γ_i is a (normal) subgroup of Γ for all i. In light of Proposition 2.1.5, it follows that $\ell_3 = c_L$. Similarly, by Proposition 2.1.7, u_1 and u_2 equal the first and second upper ramification breaks of $K[q_0, q_1]$ over K, respectively.

To determine u_1 and u_2, we note that, since N is a $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$-extension of K, the sequence of upper ramification breaks of N over K is $(\min\{f_0, f_1, f_2\}, \max\{f_0, f_1, f_2\})$ by Proposition 4.1.7. Thus $u_1 = \min\{f_0, f_1, f_2\} = f_0$, and $u_2 = \min\{f_0, f_1, f_2\} = f_1$. By Proposition 2.1.11, it follows that $\ell_1 = u_1 = f_0$, that $\ell_2 = 2u_2 - u_1 = 2f_1 - f_0$, and that $u_3 = u_2 + (\ell_3 - \ell_2)/4$. Hence

$$u_3 = u_2 + (\ell_3 - \ell_2)/4 = f_1 + (c_L - 2f_1 + f_0)/4 = (c_L + f_0)/4 + f_1/2. \qquad \square$$

For each $i \in \{0, 1, 2\}$, let $s_i \in K^{\text{alg}}$ such that $s_i^2 + s_i = F_{(i+1)'}q_i$, and let c_i denote the conductor of $K[q_0, q_1, s_i] = N[s_i]$ over N. Moreover let $w = s_0 + s_1 + s_2$ (so that $w^2 + w = F_1q_0 + F_2q_1 + F_0q_2$), and let c_w denote the conductor of $N[w]$ over N. Finally, let $u \in K^{\text{alg}}$ such that $u^2 + u = H$, and, if $[H] \neq 0$ over N, let c_u denote the conductor of $K[q_0, q_1, u] = N[u]$ over N.

Lemma 5.2.2. *Suppose $[H] \neq 0$ over N. If $h \leq f_1$, then $c_u \leq 2h - \min\{h, f_0\}$. Moreover, if $h > f_1$, then $c_u = 4h - 2f_1 - f_0$.*

Proof. Let C_u denote the conductor of $K[q_1, u]$ over $K[q_1]$, and let C_1 denote the conductor of N over $K[q_1]$. Since $f_0 \leq f_1 = f_2$, Proposition 4.1.7 implies that $C_1 = 2f_1 + f_0 - 2f_1 = f_0$.

First, suppose $h \leq f_1$. Let C_2 denote the conductor of $K[q_1 + u]$ over K, and let C_3 denote the conductor of $K[q_1, q_0 + u]$ over $K[q_1]$. Then

$$C_u = 2\max\{h, f_1, C_2\} + \min\{h, f_1, C_2\} - 2f_1 = 2f_1 + \min\{h, f_1, C_2\} - 2f_1 \leq h$$

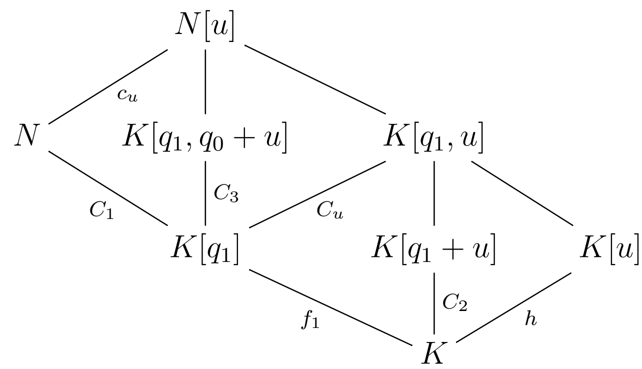

Figure 5.1

by Proposition 4.1.7 applied to the tower of extensions $K[q_1, u] \supseteq K[q_1] \supseteq K$. Futhermore, applying Proposition 4.1.7 to the tower of extensions $K[q_0, q_1, u] \supseteq N \supseteq K[q_1]$ implies that

$$\begin{aligned} c_u &= 2\max\{C_u, C_1, C_3\} + \min\{C_u, C_1, C_3\} - 2C_1 \\ &= 2\max\{C_u, C_1\} + \min\{C_u, C_1, C_3\} - 2C_1 \\ &\leq 2\max\{C_u, C_1\} + \min\{C_u, C_1\} - 2C_1 \\ &\leq 2\max\{h, f_0\} + \min\{h, f_0\} - 2f_0 \\ &= 2(\max\{h, f_0\} + \min\{h, f_0\}) - \min\{h, f_0\} - 2f_0 \\ &= 2(h + f_0) - \min\{h, f_0\} - 2f_0 = 2h - \min\{h, f_0\}. \end{aligned}$$

Second, suppose $h > f_1$. Then $C_u = 2h - f_1$ by Lemma 4.1.3. Hence

$$C_u > 2f_1 - f_1 = f_1 \geq f_0 = C_1.$$

Therefore, $c_u = 2C_u - C_1 = 4h - 2f_1 - f_0$ by Lemma 4.1.3. □

Remark 5.2.3. The situation described in the proof of Lemma 5.2.2 may be visualized as in Figure 5.1.

Lemma 5.2.4. *The conductor* $c_1 = 6f_1 - f_0$*, and* $c_0 = c_2 = 3f_0 + 2f_1$*.*

Proof. Let $i \in \{0, 1, 2\}$. By Proposition 3.1.6, the Galois closure of $K[q_i, s_i]$ over K is a D_4-extension of K. Moreover, by Proposition 3.2.2, $K[q_i, q_{(i+1)'}, s_i] = N[s_i]$ is the Galois closure of $K[q_i, s_i]$ over K. Therefore, since N is the unique normal degree four subfield of $N[s_i]$ over K, the conductor c_i is, as in Proposition 4.3.2, equal to the third lower ramification break of $N[s_i]$ over K. By Corollary 4.3.3, this break is

$$4\max\{f_i + f_{(i+1)'}, 0\} - 2\max\{f_0, f_1, f_2\} - \min\{f_0, f_1, f_2\} = 4(f_i + f_{(i+1)'}) - 2f_1 - f_0.$$

Hence

$$\begin{aligned} c_0 &= 4(f_0 + f_1) - 2f_1 - f_0 = 3f_0 + 2f_1, \\ c_1 &= 4(f_1 + f_2) - 2f_1 - f_0 = 6f_1 - f_0, \text{ and} \\ c_2 &= 4(f_2 + f_0) - 2f_1 - f_0 = 3f_0 + 2f_1. \end{aligned}$$

□

Corollary 5.2.5. *The conductor* $c_w \leq 6f_1 - f_0$. *If* $f_0 < f_1$, *then* $c_w = 6f_1 - f_0$.

Proof. Let $i \in \{0,1,2\}$. By Propositions 2.2.5 and 2.2.7, there exists a element ϕ_i of N in standard form over N (with respect to some uniformizer π of N) such that $c_i = -v_N(\phi_i)$, and $[F_{(i+1)'}q_i] = [\phi_i]$ over N. Then $\phi_0 + \phi_1 + \phi_2$ is also in standard form, and

$$[F_1q_0 + F_2q_1 + F_0q_2] = [\phi_0 + \phi_1 + \phi_2]$$

over N. Hence

$$c_w = -v_N(\phi_0 + \phi_1 + \phi_2) \leq -\min\{v_N(\phi_0), v_N(\phi_1), v_N(\phi_2)\} = \max\{c_0, c_1, c_2\}.$$

By Lemma 5.2.4, $c_0 = c_2 = 3f_0 + 2f_1 = 6f_1 - f_0 - 4(f_1 - f_0) = c_1 - 4(f_1 - f_0)$. Since $f_0 \leq f_1$, it follows that $c_w \leq c_1 = 6f_1 - f_0$.

Now suppose that $f_0 < f_1$. Then $c_1 > c_0 = c_2$, and so $v_N(\phi_1) < v_N(\phi_0) = v_N(\phi_2)$. Thus

$$c_w = -v_N(\phi_0 + \phi_1 + \phi_2) = -v_N(\phi_1) = c_1 = 6f_1 - f_0. \qquad \square$$

Proposition 5.2.6. *Suppose that* $f_0 < f_1$. *Then* $c_L = 4\max\{2f_1, h\} - 2f_1 - f_0$.

Proof. Suppose $[H] = 0$ over N. Then $L = N[s] = N[w]$ by Proposition 2.2.1. Moreover, it follows via Lemma 3.1.2 that $h \leq f_1$, Thus $c_L = c_w = 6f_1 - f_0 = 4\max\{2f_1, h\} - 2f_1 - f_0$.

Now suppose that $[H] \neq 0$ over N. Note then that h is both odd and positive, and that, since $[F_1q_0 + F_2q_1 + F_0q_2 + H] = [F_1q_0 + F_2q_1 + F_0q_2] + [H]$, it follows that $c_L \leq \max\{c_w, c_u\}$, and that $c_L = \max\{c_w, c_u\}$ if c_w and c_u differ. Moreover, $c_w = 6f_1 - f_0$ by Lemma 5.2.4 since $f_0 < f_1$.

First, suppose that $h \leq f_1$. Then $c_u \leq 2h - \min\{h, f_0\}$ by Lemma 5.2.2. Hence

$$c_u \leq 2h - \min\{h, f_0\} < 2h \leq 2f_1 < 6f_1 - f_0 = c_w.$$

Thus $c_L = 6f_1 - f_0 = 4\max\{2f_1, h\} - 2f_1 - f_0$.

Second, suppose that $h > f_1$. Then $c_u = 4h - 2f_1 - f_0$ by Lemma 5.2.2. Therefore,

$$c_w - c_u = (6f_1 - f_0) - (4h - 2f_1 - f_0) = 8f_1 - 4h = 4(2f_1 - h) \neq 0$$

since h is odd. Thus

$$c_L = \max\{c_w, c_u\} = \max\{6f_1 - f_0, 4h - 2f_1 - f_0\} = 4\max\{2f_1, h\} - 2f_1 - f_0. \qquad \square$$

Applying Lemma 5.2.1 to Proposition 5.2.6 yields the following corollary.

Corollary 5.2.7. *Suppose* $f_0 < f_1$. *The lower ramification breaks of* L *over* K *are* $\ell_1 = f_0$, $\ell_2 = 2f_1 - f_0$, *and* $\ell_3 = 4\max\{2f_1, h\} - 2f_1 - f_0$, *and the upper ramification breaks of* L *over* K *are* $u_1 = f_0$, $u_2 = f_1$, *and* $u_3 = \max\{2f_1, h\}$.

5.2.1 Computation of Ramification Breaks in $f_0 = f_1$ Case

Having computed the ramification breaks of L over K in the case in which $f_0 < f_1$, we now compute the ramification breaks of L over K in the case in which $f_0 = f_1$. These computations require that the triple (F_0, F_1, H) be a standard form triple, not merely, as we have so far assumed, a Q_8-odd form triple. Accordingly, we assume henceforth that (F_0, F_1, H) is indeed a standard form triple corresponding to the extension $L|K$. By Proposition 5.1.5, such a triple must exist.

As we mentioned in the introduction to Section 5.2, the degrees f_0, f_1 and h do not, in this case, invariably suffice to determine the ramification breaks of L over K; rather, we must consider the degrees (in t^{-1}) of $F_1+\zeta_3 F_0$ and of $F_1+\zeta_3^2 F_0$ as well, where $\zeta_3 \in k$ is a fixed primitive cube root of 1. Let $m = \min\{\deg_{t^{-1}}(F_1+\zeta_3 F_0), \deg_{t^{-1}}(F_1+\zeta_3^2 F_0)\}$, and, for convenience, let $n = f_0 (= f_1)$. We seek a formula for the ramification breaks of L over K in terms of m, n, and h.

By Lemma 5.2.1, to find such a formula, it suffices to compute c_L in terms of m, n and h. The chief difficulty in the computation of c_L is the computation of the conductor c_w of $N[w]$ over N. Since $f_0 = f_1$, Corollary 5.2.5 provides only an upper bound, not a precise value, for c_w. Therefore, instead of considering, as above, the conductors c_0 c_1, and c_2 to determine c_w, we shall determine c_w more directly. In particular, we shall exhibit an element of N that is both Artin–Schreier equivalent over N to $w^2+w = F_1q_0+F_2q_1+F_0q_2$ and of odd valuation over N. By Proposition 2.2.7, $-c_w$ is equal to the valuation of this element, which valuation is, as desired, a function of m, n and h. Having determined c_w, we shall, as in Proposition 5.2.6, compare c_w and c_u to determine c_L.

To find this desired element of N, we shall first define a particular element r of odd valuation over N as a K-linear (not necessarily as a k-linear) combination of q_0 and q_1. The element r is an Artin–Schreier root of a K-multiple of q_0; we shall exploit this property of r to write $F_1q_0 + F_2q_1 + F_0q_2$ as a polynomial of degree six in r (with coefficients in $k[[t]]$). We shall then split the sixth-degree term of this polynomial into two separate terms. One of these terms will have a valuation of smaller magnitude than that of the original term; the other will be a square over N. Finally, we shall replace the square term with its square root, show that the resulting element of N, which is necessarily Artin–Schreier equivalent over N to $F_1q_0 + F_2q_1 + F_0q_2$, has odd valuation over N, and give this valuation in terms of m, n and h.

Lemma 5.2.8. *The degree m either is an odd positive integer no greater than n, or is equal to $-\infty$. Moreover,*

(1) *either* $\deg_{t^{-1}}(F_1 + \zeta_3 F_0) = n$, *or* $\deg_{t^{-1}}(F_1 + \zeta_3^2 F_0) = n$, *and*

(2) $\deg_{t^{-1}}(F_0F_1 + F_1F_2 + F_2F_0) = n + m$.

Proof. Note that, since $\deg_{t^{-1}} F_0 = \deg_{t^{-1}} F_1 = n$, the degrees both of $F_1 + \zeta_3 F_0$ and of $F_1+\zeta_3^2 F_0$ are no greater than n. Hence $m \leq n$. Moreover, since F_0 and F_1 are both standard form elements of K with respect to t, the elements $F_1 + \zeta_3 F_0$ and $F_1 + \zeta_3^2 F_0$ are as well. The unnumbered statement of the proposition now follows.

To show statement (1), we observe that $(F_1+\zeta_3 F_0)+(F_1+\zeta_3^2 F_0) = F_1+F_0 = F_2$. Thus $\max\{\deg_{t^{-1}}(F_1+\zeta_3 F_0), \deg_{t^{-1}}(F_1+\zeta_3^2 F_0)\} \geq \deg_{t^{-1}} F_2 = n$. Since $\deg_{t^{-1}}(F_1 + \zeta_3^i F_0) \leq n$ for each $i \in \{1,2\}$, statement (1) now follows.

To show statement (2), we note that

$$\begin{aligned}(F_1+\zeta_3 F_0)(F_1+\zeta_3^2 F_0) &= F_1^2 + (\zeta_3+\zeta_3^2)F_0F_1 + F_0^2 \\ &= F_1F_2 + F_0F_1 + F_0F_1 + F_0F_1 + F_2F_0 \\ &= F_0F_1 + F_1F_2 + F_2F_0.\end{aligned}$$

Hence $\deg_{t^{-1}}(F_0F_1+F_1F_2+F_2F_0) = \deg_{t^{-1}}(F_1+\zeta_3F_0) + \deg_{t^{-1}}(F_1+\zeta_3^2F_0) = n+m$ by statement (1). □

Lemma 5.2.9. *The inequality $3n \leq c_w \leq 5n$ holds.*

Proof. To prove the upper bound on c_w, we note that $c_w \leq 6f_1 - f_0 = 5n$ by Lemma 5.2.5.

To prove the lower bound, we note that $N[w]$ is a Q_8-extension of K by Proposition 3.3.7. Hence $N[w]$ is a $\mathbb{Z}/4\mathbb{Z}$-extension of $K[q_1]$. Moreover, the conductor of N over $K[q_1]$ is n by Lemma 4.1.5. It follows by Proposition 2.1.7 and by Corollary 4.1.11 that the sequence of lower ramification breaks of $N[w]|K[q_1]$ is $(n, 2\max\{2n,h\}-n)$. Moreover, by Proposition 2.1.5, c_w is equal to the second lower ramification break of $N[w]|K[q_1]$. Thus $c_w = 2\max\{2n,h\}-n \geq 4n-n = 3n$. □

We now introduce further notation. For each $i \in \{0,1,2\}$, let $A_i = t^nF_i$. Note that, for each $i \in \{0,1,2\}$, the element F_i is a standard form element of K with respect to t of degree $-n$, and hence A_i is a degree zero element of $k[[t^2]] \subseteq K$. Therefore, for each $i \in \{0,1,2\}$, the element $B_i = \sqrt{A_i}$ is a degree zero element of $k[[t]]$.

Lemma 5.2.10. *Let $r = q_1 + \dfrac{B_1}{B_0}q_0$. Then $r^2 + r = \dfrac{B_1B_2}{A_0}q_0$, and $v_N(r) = -n$.*

Proof. Note that

$$\begin{aligned} q_1^2 + q_1 = A_1t^{-n} &= \frac{A_1}{A_0}(A_0t^{-n}) \\ &= \frac{A_1}{A_0}(q_0^2+q_0) = \left(\frac{B_1}{B_0}q_0\right)^2 + \frac{A_1}{A_0}q_0 \\ &= \left(\frac{B_1}{B_0}q_0\right)^2 + \frac{B_1}{B_0}q_0 + \left(\frac{B_1}{B_0}+\frac{A_1}{A_0}\right)q_0.\end{aligned}$$

Moreover,

$$\frac{B_1}{B_0}+\frac{A_1}{A_0} = \frac{B_1B_0+A_1}{A_0} = \frac{B_1(B_0+B_1)}{A_0} = \frac{B_1B_2}{A_0}.$$

Thus

$$r^2 + r = \left(\frac{B_1}{B_0}+\frac{A_1}{A_0}\right)q_0 = \frac{B_1B_2}{A_0}q_0.$$

To show that $v_N(r) = -n$, we observe that $N|K$ is a totally ramified Galois extension of degree four. Hence $v_N(F_0) = 4v_K(F_0) = -4n$. Since $n > 0$ and $q_0^2 + q_0 = F_0$, it follows that $2v_N(q_0) = v_N(F_0)$, and that $v_N(q_0) = -2n$. Moreover, B_1, B_2 and A_0 all have valuation 0 over K, and hence over N. Thus $v_N\left(\frac{B_1B_2}{A_0}q_0\right) = -2n$ as well; since $r^2 + r = \frac{B_1B_2}{A_0}q_0$, it follows that $2v_N(r) = -2n$, and that $v_N(r) = -n$. □

Observing that r is an element of N with odd valuation, we shall now write $F_1q_0 + F_2q_1 + F_0q_2 = t^{-n}(A_1q_0 + A_2q_1 + A_0q_2)$ as a polynomial in r. We begin with two lemmas.

Lemma 5.2.11. *The equation*

$$t^{-n} = \frac{A_0}{A_1A_2}r^4 + \frac{B_0B_1 + B_1B_2 + B_2B_0}{A_1A_2}r^2 + \frac{1}{B_1B_2}r$$

holds.

Proof. Note that

$$q_0 = \frac{A_0}{B_1B_2}(r^2 + r)$$

by Lemma 5.2.10. Thus

$$\begin{aligned} A_0t^{-n} = F_0 = q_0^2 + q_0 &= \frac{A_0^2}{A_1A_2}(r^4 + r^2) + \frac{A_0}{B_1B_2}(r^2 + r) \\ &= \frac{A_0^2}{A_1A_2}r^4 + \left(\frac{A_0B_0^2}{A_1A_2} + \frac{A_0B_1B_2}{A_1A_2}\right)r^2 + \frac{A_0}{B_1B_2}r \\ &= \frac{A_0^2}{A_1A_2}r^4 + \frac{A_0}{A_1A_2}\left(B_0^2 + B_1B_2\right)r^2 + \frac{A_0}{B_1B_2}r \\ &= \frac{A_0^2}{A_1A_2}r^4 + \frac{A_0}{A_1A_2}\left(B_0(B_1 + B_2) + B_1B_2\right)r^2 + \frac{A_0}{B_1B_2}r. \end{aligned}$$

Hence

$$t^{-n} = \frac{A_0}{A_1A_2}r^4 + \frac{B_0B_1 + B_1B_2 + B_2B_0}{A_1A_2}r^2 + \frac{1}{B_1B_2}r.$$

□

Lemma 5.2.12. *The equation*

$$A_1q_0 + A_2q_1 + A_0q_2 = \frac{B_0(B_0A_1 + B_1A_2 + B_2A_0)}{B_1B_2}r^2 + \frac{A_0A_1 + A_1A_2 + A_2A_0}{B_1B_2}r$$

holds.

Proof. By Lemma 5.2.10, $q_0 = \dfrac{A_0}{B_1B_2}(r^2 + r)$, and $q_1 = \dfrac{B_1}{B_0}q_0 + r$. Thus

$$q_1 = \frac{B_1}{B_0}\left(\frac{A_0}{B_1B_2}\right)(r^2 + r) + r = \frac{B_0}{B_2}r^2 + \left(\frac{B_0}{B_2} + \frac{B_2}{B_2}\right)r = \frac{B_0}{B_2}r^2 + \frac{B_1}{B_2}r.$$

Moreover, $q_2 = q_0 + q_1 = \left(\frac{B_1}{B_0} + 1\right) q_0 + r = \frac{B_2}{B_0} q_0 + r$, and so

$$q_2 = \frac{B_2}{B_0}\left(\frac{A_0}{B_1 B_2}\right)(r^2 + r) + r = \frac{B_0}{B_1} r^2 + \left(\frac{B_0}{B_1} + \frac{B_1}{B_1}\right) r = \frac{B_0}{B_1} r^2 + \frac{B_2}{B_1} r.$$

Therefore,

$$A_1 q_0 = A_1\left(\frac{A_0}{B_1 B_2}\right)(r^2 + r) = \frac{A_0 B_1}{B_2} r^2 + \frac{A_0 B_1}{B_2} r,$$

$$A_2 q_1 = A_2\left(\frac{B_0}{B_2} r^2 + \frac{B_1}{B_2} r\right) = B_2 B_0 r^2 + B_1 B_2 r, \text{ and}$$

$$A_0 q_2 = A_0\left(\frac{B_0}{B_1} r^2 + \frac{B_2}{B_1} r\right) = \frac{A_0 B_0}{B_1} r^2 + \frac{B_2 A_0}{B_1} r.$$

Hence

$$\begin{aligned} A_1 q_0 + A_2 q_1 + A_0 q_2 &= \left(\frac{A_0 B_1}{B_2} + B_2 B_0 + \frac{A_0 B_0}{B_1}\right) r^2 + \left(\frac{A_0 B_1}{B_2} + B_1 B_2 + \frac{B_2 A_0}{B_1}\right) r \\ &= \frac{A_0 A_1 + B_0 B_1 A_2 + B_2 A_0 B_0}{B_1 B_2} r^2 + \frac{A_0 A_1 + A_1 A_2 + A_2 A_0}{B_1 B_2} r \\ &= \frac{B_0(B_0 A_1 + B_1 A_2 + B_2 A_0)}{B_1 B_2} r^2 + \frac{A_0 A_1 + A_1 A_2 + A_2 A_0}{B_1 B_2} r. \end{aligned}$$ □

Proposition 5.2.13. *The equation*

$$F_1 q_0 + F_2 q_1 + F_0 q_2 = (ar^4 + br^2 + cr)(dr^2 + er) = adr^6 + aer^5 + bdr^4 + (be + cd)r^3 + cer^2$$

holds, where

$$a = \frac{A_0}{A_1 A_2}, \quad b = \frac{B_0 B_1 + B_1 B_2 + B_2 B_0}{A_1 A_2}, \quad c = \frac{1}{B_1 B_2},$$

$$d = \frac{B_0(B_0 A_1 + B_1 A_2 + B_2 A_0)}{B_1 B_2}, \quad e = \frac{A_0 A_1 + A_1 A_2 + A_2 A_0}{B_1 B_2}.$$

Proof. Observe that $F_1 q_0 + F_2 q_1 + F_0 q_2 = t^{-n}(A_1 q_0 + A_2 q_1 + A_0 q_2)$. By Lemma 5.2.11, $t^{-n} = ar^4 + br^2 + cr$. By Lemma 5.2.12, $A_1 q_0 + A_2 q_1 + A_0 q_2 = dr^2 + er$. The proposition now follows. □

Lemma 5.2.14. *The statements*

$$v_N(a) = 0, \qquad v_N(b) = 2n - 2m, \qquad v_N(c) = 0, \qquad v_N(d) \geq 0$$

$$v_N(e) = 4n - 4m, \qquad v_N(aer^5) = -n - 4m, \qquad v_N(bdr^4) \geq -2n - 2m$$

all hold.

Proof. Recall that A_i and B_i are degree zero elements of K for all $i \in \{0,1,2\}$. Thus $v_N(A_i) = v_N(B_i) = 0$ for all $i \in \{0,1,2\}$; hence $v_N(a) = v_N(A_0) - v_N(A_1) = v_N(A_2) = 0$, $v_N(c) = -v_N(B_1) - v_N(B_2) = 0$, and

$$\begin{aligned} v_N(d) &= v_N(B_0) + v_N(B_0A_1 + B_1A_2 + B_2A_0) - v_N(B_1) - v_N(B_2) \\ &= v_N(B_0A_1 + B_1A_2 + B_2A_0) \geq 0. \end{aligned}$$

Moreover, note that, since $A_0A_1 + A_1A_2 + A_2A_0 = t^{2n}(F_0F_1 + F_1F_2 + F_2F_0)$,

$$\begin{aligned} v_K(A_0A_1 + A_1A_2 + A_2A_0) &= v_K(t^{2n}(F_0F_1 + F_1F_2 + F_2F_0)) \\ &= 2n - \deg_{t^{-1}}(F_0F_1 + F_1F_2 + F_2F_0) \\ &= 2n - (n+m) = n - m \end{aligned}$$

by Lemma 5.2.8. Thus

$$v_N(e) = v_N(A_0A_1 + A_1A_2 + A_2A_0) - v_N(B_1) - v_N(B_2) = 4n - 4m,$$

and

$$\begin{aligned} v_N(b) &= v_N(B_0B_1 + B_1B_2 + B_2B_0) - v_N(A_1) - v_N(A_2) \\ &= v_N\left(\sqrt{A_0A_1 + A_1A_2 + A_2A_0}\right) = (4n-4m)/2 = 2n - 2m. \end{aligned}$$

The last two statements of the lemma now follow by Lemma 5.2.10. □

Lemma 5.2.15. *Define a, b, c, d and e as in Propostion 5.2.13 and Lemma 5.2.14. There exist D_1, $D_2 \in k[[t]]$ such that $d = D_1 + D_2$, that D_1 is a square in $k[[t]]$, and that $v_N(D_2) \geq 4n - \max\{2m, n\} + 4$.*

Proof. We observe that

$$t = t^{n+1}t^{-n} = t^{n+1}(ar^4 + br^2 + cr) = at^{n+1}r^4 + bt^{n+1}r^2 + ct^{n+1}r$$

by Lemma 5.2.11, and that $v_N(t) = 4v_K(t) = 4$ since $N|K$ is a totally ramified Galois extension of degree four. Therefore, by Lemma 5.2.14,

$$v_N(at^{n+1}r^4) = v_N(a) + (n+1)v_N(t) + 4v_N(r) = 4(n+1) - 4n = 4,$$

and

$$\begin{aligned} v_N(t - at^{n+1}r^4) &\geq \min\{v_N(b) + v_N(t^{n+1}) + v_N(r^2), v_N(c) + v_N(t^{n+1}) + v_N(r)\} \\ &= \min\{2n - 2m + 4(n+1) - 2n, 4(n+1) - n\} \\ &= 4n - \max\{2m, n\} + 4. \end{aligned}$$

Furthermore, since $v_N(d) \geq 0$, there exist $d_i \in k$ (for $i \geq 0$) such that $d = \sum_{i=0}^{\infty} d_i t^i$. Thus

$$\begin{aligned} d &= \sum_{i=0}^{\infty} d_i t^i = \sum_{i=0}^{\infty} d_i \left(at^{n+1}r^4 + (t - at^{n+1}r^4)\right)^i \\ &= \sum_{i=0}^{\infty} \sum_{\ell=0}^{i} d_i \binom{i}{\ell} (at^{n+1}r^4)^{i-\ell}(t - at^{n+1}r^4)^{\ell} \\ &= \sum_{i=0}^{\infty} d_i (at^{n+1}r^4)^i + (t - at^{n+1}r^4) \sum_{i=1}^{\infty} \sum_{\ell=1}^{i} d_i \binom{i}{\ell} (at^{n+1}r^4)^{i-\ell}(t - at^{n+1}r^4)^{\ell-1}. \end{aligned}$$

Let $D_1 = \sum_{i=0}^{\infty} d_i(at^{n+1}r^4)^i$, and let $D_2 = d - D_1$. We note that $v_N(at^{n+1}r^4) = 4 \geq 0$, and that

$$v_N(t - at^{n+1}r^4) \geq 4n - \max\{2m, n\} + 4 \geq 2n + 4 \geq 0,$$

the second inequality holding by Lemma 5.2.8. Therefore, $v_N((t - at^{n+1}r^4)^{-1}D_2) \geq 0$, and

$$v_N(D_2) \geq v_N(t - at^{n+1}r^4) \geq 4n - \max\{2m, n\} + 4.$$

To show that D_1 is a square in $k[[t]]$, we observe that $t^{(n+1)/2} \in K$ since n is odd, and that $v_N(t^{(n+1)/2}r^2) = 2 \geq 0$. Therefore, since k is algebraically closed, and $d_i \in k$ for all $i \geq 0$, the formal series

$$\sum_{i=0}^{\infty} \sqrt{d_i} \left(\frac{B_0}{B_1 B_2} t^{(n+1)/2} r^2 \right)^i$$

is an element of $k[[t]]$. Moreover, since $a = \dfrac{A_0}{A_1 A_2}$ by definition,

$$\begin{aligned} \left(\sum_{i=0}^{\infty} \sqrt{d_i} \left(\frac{B_0}{B_1 B_2} t^{(n+1)/2} r^2 \right)^i \right)^2 &= \sum_{i=0}^{\infty} \left(\sqrt{d_i} \left(\frac{B_0}{B_1 B_2} t^{(n+1)/2} r^2 \right)^i \right)^2 \\ &= \sum_{i=0}^{\infty} d_i \left(\frac{A_0}{A_1 A_2} t^{n+1} r^4 \right)^i = \sum_{i=0}^{\infty} d_i (at^{n+1}r^4)^i = D_1. \square \end{aligned}$$

Proposition 5.2.16. *The conductor* $c_w = n + 2\max\{2m, n\}$.

Proof. Recall that $F_1q_0 + F_2q_1 + F_0q_2 = adr^6 + aer^5 + bdr^4 + (be + cd)r^3 + cer^2$, and let $D_1, D_2 \in k[[t]]$ as in Lemma 5.2.15. Since $a = \left(\frac{B_0}{B_1B_2}\right)^2$ and D_1 is a square in $k[[t]]$, it follows that $[adr^6] = [a(D_1 + D_2)r^6] = [aD_2r^6 + \sqrt{aD_1}r^3]$ over N. Therefore,

$$[F_1q_0 + F_2q_1 + F_0q_2] = \left[aD_2r^6 + aer^5 + bdr^4 + \left(be + cd + \sqrt{aD_1}\right) r^3 + cer^2\right]$$

over N, and $c_w \leq -v_N\left(aD_2r^6 + aer^5 + bdr^4 + \left(be + cd + \sqrt{aD_1}\right) r^3 + cer^2\right)$. By Lemma 5.2.14, $v_N(aer^5) = -n - 4m$, and $v_N(bdr^4) \geq -2n - 2m$. Moreover, since $\sqrt{D_1} \in k[[t]]$ by Lemma 5.2.15,

$$v_N\left(\left(be + cd + \sqrt{aD_1}\right) r^3 + cer^2\right) \geq -3n$$

by Lemma 5.2.14. Finally, $v_N(aD_2r^6) \geq -2n - \max\{2m, n\} + 4$ since $v_N(D_2) \geq 4n - \max\{2m, n\} + 4$ by Lemma 5.2.15.

First suppose that $2m > n$. Then

$$v_N(aer^5) = -n - 4m < -3n \leq v_N\left(\left(be + cd + \sqrt{aD_1}\right) r^3 + cer^2\right),$$

$$v_N(aD_2r^6) \geq -2n - 2m + 4 > -n - 4m + 4 > v_N(aer^5), \text{ and}$$

$$v_N(bdr^4) \geq -2n - 2m > -n - 4m = v_N(aer^5).$$

Hence $c_w = -v_N(aer^5) = n + 4m = n + 2\max\{2m, n\}$.

Now suppose that $2m < n$. (Note that $2m \neq n$ since n is odd.) Then $v_N(aer^5) = -n - 4m > -3n$, and $v_N(aD_2r^6) \geq -3n + 4 > -3n$, and $v_N(bdr^4) \geq -2n - 2m > -3n$. Thus $c_w \leq 3n$. By Lemma 5.2.9, $c_w \geq 3n$ as well. Hence $c_w = 3n = n + 2\max\{2m, n\}$. □

Proposition 5.2.17. *The conductor $c_L = 4\max\{3/2n, n + m, h\} - 3n$.*

Proof. Note that, by proposition 5.2.16

$$c_w = n + 2\max\{2m, n\} = \max\{n + 4m, 3n\} = 4\max\{3n/2, n + m\} - 3n.$$

First, suppose that $[H] = 0$ over N. By Lemma 4.1.3 (applied twice), it follows that $h \leq n$. Moreover, $N[s] = N[w]$, and hence

$$c_L = c_w = 4\max\{3n/2, n + m\} - 3n = 4\max\{3/2n, n + m, h\} - 3n.$$

Second, suppose that $[H] \neq 0$, and that $h \leq n$. Then $c_u \leq 2h - \min\{h, n\} < 2h$ by Lemma 5.2.2, and so $c_w = 4\max\{3n/2, n + m\} - 3n \geq 3n \geq 3h > c_u$. Thus $c_L = c_w = 4\max\{3n/2, n + m\} - 3n = 4\max\{3n/2, n + m, h\} - 3n$.

Third, suppose that $h > n$. Then $c_u = 4h - 3n$ by Lemma 5.2.2. Thus

$$\begin{aligned} c_L &= \max\{c_w, c_u\} = \max\{4\max\{3n/2, n + m\} - 3n, 4h - 3n\} \\ &= 4\max\{3n/2, n + m, h\} - 3n \end{aligned}$$

if $c_w \neq c_u$; *i.e.*, if $h \neq \max\{3n/2, n + m\}$. Since both h and n are odd integers, $h \neq 3n/2$. Moreover, since m is odd by Lemma 5.2.8, $h \neq n + m$. The proposition now follows. □

Applying Lemma 5.2.1 to Proposition 5.2.17 yields the following corollary.

Corollary 5.2.18. *The lower ramification breaks of L over K are $\ell_1 = n$, $\ell_2 = n$, and $\ell_3 = 4\max\{3n/2, n + m, h\} - 3n$, and the upper ramification breaks of L over K are $u_1 = n$, $u_2 = n$, and $u_3 = \max\{3n/2, n + m, h\}$.*

We now combine the results of Corollaries 5.2.7 and 5.2.18 into a general proposition giving the ramification breaks of L over K in all cases. In this proposition, we remove the assumption that $f_0 = f_1$, but continue to insist the (F_0, F_1, H) is a standard form Q_8-triple.

Lemma 5.2.19. *Suppose $f_0 < f_1$. Then $m = f_1$.*

Proof. For each $i \in \{1, 2\}$, $\deg_{t^{-1}}(\zeta_3^i F_0) = f_0 < f_1 = \deg_{t^{-1}} F_1$. Thus $\deg_{t^{-1}}(F_1 + \zeta_3^i F_0) = f_1$ for each $i \in \{1, 2\}$. Hence $m = f_1$. □

Proposition 5.2.20. *The lower ramification breaks of L over K are $\ell_1 = f_0$, $\ell_2 = 2f_1 - f_0$, and $\ell_3 = 4\max\{3f_1/2, f_1 + m, h\} - 2f_1 - f_0$, and the upper ramification breaks of L over K are $u_1 = f_0$, $u_2 = f_1$, and $u_3 = \max\{3f_1/2, f_1 + m, h\}$.*

Proof. Suppose $f_0 < f_1$. Then Lemma 5.2.19 implies that $f_1 + m = 2f_1 > 3f_1/2$. Moreover, by Corollary 5.2.7, the upper ramification breaks of L over K are $u_1 = f_0$, $u_2 = f_1$, and $u_3 = \max\{2f_1, h\} = \max\{3f_1/2, f_1 + m, h\}$.

Now suppose $f_0 = f_1$. Then the upper ramification breaks of L over K are $u_1 = f_0$, $u_2 = f_1$, and $u_3 = \max\{3f_1/2, f_1 + m, h\}$ by Corollary 5.2.18. The proposition now follows. □

5.3 Characterization of Sequences of Ramification Breaks

In this subsection, we continue to suppose that k is algebraically closed. By Proposition 5.1.5 it follows that every Q_8-extension of K is a Q_8-standard form extension of K. Moreover, by Proposition 5.1.6, every Q_8-extension of K has a standard form triple (F_0', F_1', H') satisfying the additional condition $\deg_{t^{-1}} F_0' \leq \deg_{t^{-1}} F_1'$.

Suppose $\mathrm{Gal}(L|K) \cong Q_8$. Recall that we have defined (in Defintion 2.1.9) the nth element of the sequence of ramification groups of L over K to be $\mathrm{Gal}(L|K)^{u_i}$, where u_i denotes the ith upper ramification break of $L|K$. We now define the sequence of ramification groups of L over K to be a *Type I* sequence if the sequence's second element is isomorphic to $\mathbb{Z}/4\mathbb{Z}$, and to be a *Type II* sequence if the sequence's second element is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Note that in all cases, the second ramification break is strictly smaller than the third; thus the sequence's third element is always isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

As in the D_4 case, the type of an extension's sequence of ramification groups affects the possible sequences of lower and of upper ramification breaks of that extension. In this subsection, we consider (in the case where k is algebraically closed) the relation between the type of an extension's sequence of ramification groups and the sequences of lower and of upper ramification breaks of that sequence exhaustively.

Let $\mathcal{C}$ denote the set of triples (F_0', F_1', H') of standard form elements of K such that F_0', F_1' and 0 are pairwise distinct, and let Φ denote the surjection from $\mathcal{C}$ to the set of Q_8-extensions of K defined in Corollary 5.1.7.

Lemma 5.3.1. *Let $(\alpha, \beta, \gamma) \in (\mathbb{Z}^+)^2 \times (1/2)\mathbb{Z}^+$ such that α is odd, $\alpha \leq \beta$, β is odd, $\gamma \geq 3\beta/2$, $\gamma \geq 2\beta$ if $\alpha < \beta$, $\gamma \in \mathbb{Z}$ if $\gamma > 3\beta/2$, and γ is odd if $\gamma > 2\beta$. Also, let $F_0 = t^{-\alpha}$, let*

$$F_1 = \begin{cases} \lambda t^{-\beta} & \text{if } \gamma = 2\beta \\ \zeta_3 t^{-\beta} + t^{-\gamma+\beta} & \text{if } \gamma \neq 2\beta \text{ and } \gamma \text{ is even} \\ \zeta_3 t^{-\beta} & \text{if } \gamma \text{ is odd or } \gamma \notin \mathbb{Z} \end{cases},$$

where $\zeta_3 \in k$ is a primitive cube root of unity, and λ is an element of $k \backslash \mathbb{F}_4$, and let

$$H = \begin{cases} t^{-\gamma} & \text{if } \gamma \text{ is odd} \\ 0 & \text{if } \gamma \text{ is even or } \gamma \notin \mathbb{Z} \end{cases}.$$

Then $(F_0, F_1, H) \in \mathcal{C}$, and the sequence of upper ramification breaks of the Q_8-extension $\Phi((F_0, F_1, H))$ of K is (α, β, γ).

Proof. Since α and β are both odd, F_0, F_1 and H are all standard form elements of K. Since $\lambda \notin \mathbb{F}_4$, the elements F_0, F_1 and 0 are pairwise distinct; as such, $(F_0, F_1, H) \in \mathcal{C}$.

Now let $f_0 = \deg_{t^{-1}}(F_0)$, $f_1 = \deg_{t^{-1}}(F_1)$, $h = \deg_{t^{-1}}(H)$, and let

$$m = \min\{\deg_{t^{-1}}(F_1 + \zeta_3 F_0), \deg_{t^{-1}}(F_1 + \zeta_3^2 F_0)\}.$$

Then $f_0 = \alpha$, and $f_1 = \beta$ unless γ is even and not equal to 2β. Moreover, if γ is even and not equal to 2β, then $\gamma < 2\beta$; hence $-\gamma + \beta > -\beta$, and $f_1 = \beta$. Thus $f_0 = \alpha \leq \beta = f_1$ in all cases; therefore, the sequence of upper ramification breaks of $L = \Phi((F_0, F_1, H))$ is $(u_1, u_2, u_3) = (f_0, f_1, \max\{3f_1/2, f_1 + m, h\})$ by Proposition 5.2.20. Hence $u_1 = f_0 = \alpha$, and $u_2 = f_1 = \beta$.

First, suppose $\alpha < \beta$. Then $\deg_{t^{-1}}(F_1 + \zeta_3^i F_0) = \max\{\alpha, \beta\} = \beta$ for each $i \in \{1, 2\}$. Hence $m = \beta$, and $f_1 + m = 2\beta$. Thus $u_3 = \max\{2\beta, h\}$. Moreover, in this case $\gamma \geq 2\beta$, and γ is odd if and only $\gamma > 2\beta$. Hence $u_3 = \gamma$.

Second, suppose that $\alpha = \beta$, and that γ is odd. Then $F_1 + \zeta_3 F_0 = 0$, and $H = t^{-\gamma}$. Since $\gamma \geq 3\beta/2$, it follows that $u_3 = \max\{3\beta/2, \gamma\} = \gamma$.

Third, suppose that $\alpha = \beta$, and that γ is not odd. Then $H = 0$, and $u_3 = \max\{3\beta/2, \beta + m\}$.

If $\gamma = 2\beta$, then $F_1 + \zeta_3^i F_0 = (\lambda + \zeta_3^i)t^{-\beta}$ for each $i \in \{1, 2\}$. Since $\lambda \notin \mathbb{F}_4$, it follows that $m = \beta$, and that $u_3 = \max\{3\beta/2, 2\beta\} = 2\beta = \gamma$.

If $\gamma \neq 2\beta$, and γ is even, then $\gamma < 2\beta$, and $F_1 + \zeta_3 F_0 = t^{-\gamma+\beta}$. Hence $m = \gamma - \beta$, and $u_3 = \max\{3\beta/2, \gamma\} = \gamma$.

If $\gamma \notin \mathbb{Z}$, *i.e.*, if $\gamma = 3\beta/2$, then $F_1 + \zeta_3 F_0 = 0$. Hence $m = -\infty$, and $u_3 = 3\beta/2 = \gamma$. □

Proposition 5.3.2. *Let $(\alpha, \beta, \gamma) \in (\mathbb{Z}^+)^2 \times (1/2)\mathbb{Z}^+$. Then (α, β, γ) is the sequence of upper ramification breaks for a Q_8-extension of K if and only if α is odd, $\alpha \leq \beta$, β is odd, $\gamma \geq 3\beta/2$, $\gamma \geq 2\beta$ if $\alpha < \beta$, $\gamma \in \mathbb{Z}$ if $\gamma > 3\beta/2$, and γ is odd if $\gamma > 2\beta$. Moreover, if M is a Q_8-extension of K with sequence of upper ramification breaks (α, β, γ), then*

(1) *M has a Type I sequence of ramification groups if $\alpha < \beta$, and*

(2) *M has a Type II sequence of ramification groups if $\alpha = \beta$.*

Proof. Since Φ is surjective, the triple (α, β, γ) is the sequence of upper ramification breaks for a D_4-extension of K if and only if there is a triple in $\mathcal{C}$ whose image under Φ has (α, β, γ) as its sequence of upper ramification breaks. Lemma 4.4.1 provides such a triple in $\mathcal{C}$ if (α, β, γ) satisfies the conditions of the unnumbered claim of the proposition.

To prove the converse, let $(F_0, F_1, H) \in \mathcal{C}$, and let $f = \deg_{t^{-1}}(F_0)$, $g = \deg_{t^{-1}}(F_1)$, $h = \deg_{t^{-1}}(H)$, and $m = \min\{\deg_{t^{-1}}(F_1 + \zeta_3 F_0), \deg_{t^{-1}} F_1 + \zeta_3 F_0\}$. By Proposition 5.1.6, we may and do assume, without loss of generality, that $f_0 \leq f_1$. Then the sequence of upper ramification breaks of $L = \Phi((F_0, F_1, H))$ is $(u_1, u_2, u_3) = (f_0, f_1, \max\{3f_1/2, f_1 + m, h\})$ by Proposition 5.2.20.

Since F_0, F_1 and H are all in standard form over K, and neither F_0 nor F_1 is equal to zero, f_0 and f_1 and both odd and positive, and h either is either both odd and positive, or is equal to $-\infty$. It follows that u_1 is odd, that $u_1 \leq u_2$, that u_2 is odd, that $u_3 \geq 3u_2/2$. Moreover, m either is an odd positive integer no greater than f_1, or is equal to $-\infty$ by Lemma 5.2.8. Thus $u_3 \in \mathbb{Z}$ if $u_3 > 3u_2/2$, and u_3 is odd if $u_3 > 2u_2$.

Suppose that $f_0 < f_1$. Then $u_1 = f_0 < f_1 = u_2$. Hence the second element of the sequence of ramification groups of L over K is $\mathrm{Gal}(L|K[q_0]) \cong \mathbb{Z}/4\mathbb{Z}$; *i.e.*, L has a Type I sequence of ramification groups. Moreover, $m = f_1$ by Lemma 5.2.19. Hence $u_3 \geq 2u_2$. This completes the proof of the unnumbered claim of the proposition.

Now suppose that $f_0 = f_1$. Then $u_1 = f_0 = f_1 = u_2$. Hence the second element of the sequence of ramification groups of L over K is $\mathrm{Gal}(L|K[q_0, q_1]) \cong \mathbb{Z}/2\mathbb{Z}$; *i.e.*, L has a Type II sequence of ramification groups. □

The following proposition is the precise analogue to Proposition 4.4.2 concerning the lower ramification breaks of D_4; accordingly, we omit its proof.

Proposition 5.3.3. *Let $(a, b, c) \in (\mathbb{Z}^+)^2 \times (1/2)\mathbb{Z}^+$. Then (a, b, c) is the sequence of lower ramification breaks for a Q_8-extension of K if and only if a is odd, $a \leq b$, $a \equiv b \pmod 4$, $c \geq a + 2b$, $c \geq 2a + 3b$ if $a < b$, $b \equiv c \pmod 8$ if $c > a + 2b$, and $b \equiv c \pmod 8$ if $c > 2a + 3b$. Moreover, if M is a Q_8-extension of K with sequence of lower ramification breaks (a, b, c), then*

(1) *M has a Type I sequence of ramification groups if $a < b$, and*

(2) *M has a Type II sequence of ramification groups if $a = b$.*

Chapter 6

Local Lifting of D_4-Extensions

6.1 Deformations in Characteristic Two

Having determined the ramification breaks of a D_4-extension corresponding to an odd-form triple of elements, we are now ready to define the equicharacteristic deformations needed to prove that D_4 is indeed a local Oort group. Let k be an algebraically closed field of characteristic $p > 0$, let $K = k((t))$ be the field of Laurent series over k, fix an algebraic closure K^{alg} of K, and let $L \subseteq K^{\text{alg}}$ be a Galois extension of K with cyclic-by-p Galois group Γ. Furthermore, let $A = k[[t]]$, and let $B \cong k[[z]]$ be the integral closure of A in L. Finally, let $\mathcal{A} = k[[\varpi, t]]$, let $\mathcal{K} = \text{Frac}(\mathcal{A})$, and let $\mathcal{S} = \mathcal{A}[\varpi^{-1}]$, where ϖ is an element transcendental over A.

Definition 6.1.1. An *equicharacteristic deformation* of the Γ-extension B over A is a Γ-extension $k[[\varpi, z]]$ over $\mathcal{A}$ such that the Galois action of Γ on $k[[\varpi, z]]$ over $\mathcal{A}$ restricts to the Galois action of Γ on the extension B over A.

Remark 6.1.2. The original extension B over A is the special fiber of the deformation, while the extension $k[[\varpi, z]][\varpi^{-1}]$ over $\mathcal{S}$ is the generic fiber. One can think of $\mathcal{S}$ as the ring of functions on the open unit disc of $k((\varpi))$ about t.

Since we shall only be concerned with the case in which $p = 2$ and $\Gamma \cong D_4$, we assume that $p = 2$ and that $\Gamma \cong D_4$ henceforth. We shall define the needed equicharacteristic deformations by deforming, in a few particular ways, a triple of standard form elements that generates the D_4-extension L of K. Accordingly, let F, G and H be elements of $K = k((t))$ in standard form with respect to t, and let q, r, and s be elements of K^{alg} such that, firstly, $q^2 + q = F$, $r^2 + r = Gq + H$ and $s^2 + s = G$, and, secondly, L is the Galois closure over K of $K[q, r]$. The existence of these elements in guaranteed by Proposition 4.2.6. Let f, g, h and d denote the degrees in t^{-1} of F, G, H and $F + G$, respectively. Moreover, for $1 \le i \le 3$, let u_i denote the ith upper ramification break of L over K, and let ℓ_i denote the ith lower ramification break of L over K.

6.1.1 Preparatory Lemmas

Let $\widetilde{F}, \widetilde{G}$, and $\widetilde{H} \in \mathcal{K}$, and let $\tilde{q}, \tilde{r}, \tilde{s} \in \mathcal{K}^{\mathrm{alg}}$ such that $\tilde{q}^2 + \tilde{q} = \widetilde{F}$, $\tilde{r}^2 + \tilde{r} = \widetilde{G}\tilde{q} + \widetilde{H}$. Also, let $\varrho \in k[[\varpi]]$. Then $\widehat{\mathcal{S}}_{(t-\varrho)} \cong k((\varpi))[[t-\varrho]]$, and $\widehat{\mathcal{K}}_{(t-\varrho)} = \mathrm{Frac}(\widehat{\mathcal{S}}_{(t-\varrho)}) \cong k((\varpi))((t-\varrho))$.

Lemma 6.1.3. *There exist a finite extension $k((\alpha)) \subseteq k((\varpi))^{\mathrm{alg}}$ of $k((\varpi))$ and elements $F', G' \in k((\alpha))((t-\varrho))$ in standard form with respect to $t-\varrho$ such that $[\widetilde{F}] = [F']$ and $[\widetilde{G}] = [G']$ over $k((\alpha))((t-\varrho))$.*

Proof. Let $\widetilde{F} = \sum_{n \geq -N} \phi_n (t-\varrho)^n$, and let $\widetilde{G} = \sum_{n \geq -N} \gamma_n (t-\varrho)^n$, where each coefficient ϕ_n and each coefficient γ_n is in $k((\varpi))$. Define $\alpha \in k((\varpi))^{\mathrm{alg}}$ such that $k((\alpha))((t-\varrho))$ is the finite extension of $k((\varpi))((t-\varrho))$ given by appending Artin–Schreier roots of ϕ_0 and γ_0, and, for all $d = 2^\ell m$, m being odd, the 2^ℓ-th root of ϕ_{-d} and of γ_{-d}. Then $[\phi_0] = [\gamma_0] = 0$ over $k((\alpha))((t-\varrho))$, and, for all $d = 2^\ell m$, m being odd,

$$[\phi_{-d}(t-\varrho)^{-d}] = [\phi_{-d}^{2^{-\ell}}(t-\varrho)^{-m}], \quad \text{and} \quad [\gamma_{-d}(t-\varrho)^{-d}] = [\gamma_{-d}^{2^{-\ell}}(t-\varrho)^{-m}]$$

Hence, as in the proof of Proposition 2.2.5, each of $\widetilde{F}$ and $\widetilde{G}$ is Artin–Schreier-equivalent over $k((\alpha))((t-\varrho))$ to an element in standard form with respect to $t-\varrho$. □

Let $q' \in k((\alpha))((t-\varrho))^{\mathrm{alg}}$ such that $(q')^2 + (q') = F'$, let $s' \in k((\alpha))((t-\varrho))^{\mathrm{alg}}$ such that $(s')^2 + (s') = G'$, and let $\widetilde{J} = G'(q' + \tilde{q}) + \widetilde{F}(s' + \tilde{s})^2 + \widetilde{H}$.

Lemma 6.1.4. *There exist a finite extension $k((\alpha')) \subseteq k((\varpi))^{\mathrm{alg}}$ of $k((\alpha))$ and $J \in k((\alpha'))((t-\varrho))$ in standard form with respect to $t-\varrho$ such that $[\widetilde{J}] = [J]$ over $k((\alpha'))((t-\varrho))$.*

Proof. The proof of this lemma is entirely analogous to that of Lemma 6.1.3. □

Lemma 6.1.5. *There exists a finite extension $k((\beta)) \subseteq k((\varpi))^{\mathrm{alg}}$ of $k((\alpha'))$ such that each degree two extension $K_2|K_1$ of fields satisfying*

$$\widehat{\mathcal{L}}_{(t-\varrho)} \supseteq K_2 \supseteq K_1 \supseteq \widehat{\mathcal{K}'}_{(t-\varrho)} \cong k((\beta))((t-\varrho)),$$

where $\mathcal{K}'$ denotes the fraction field of $k[[\beta, t]]$, and $\mathcal{L}$ denotes the Galois closure of $\mathcal{K}'[\tilde{q}, \tilde{r}]$, is totally ramified.

Proof. By appending elements to $k((\alpha'))$ as in Lemma 6.1.3, we generate a finite extension $k((\beta))$ of $k((\alpha'))$ such that each degree two extension $K_2|K_1$ of fields satisfying $\widehat{\mathcal{L}}_{(t-\varrho)} \supseteq K_2 \supseteq K_1 \supseteq \widehat{\mathcal{K}'}_{(t-\varrho)}$ is generated by an Artin–Schreier root of an element in K_1 with odd valuation. Proposition 2.2.7 then implies that each such extension is a totally ramified extension of fields. □

Now let $\mathcal{A}' = k[[\beta, t]]$, let $\mathcal{K}' = \mathrm{Frac}(\mathcal{A}')$ (as in Lemma 6.1.5), and let $\mathcal{S}' = \mathcal{A}'[\beta^{-1}]$. Moreover, let $\mathcal{L}$ be the Galois closure of $\mathcal{K}'[\tilde{q}, \tilde{r}]$ (as in Lemma 6.1.5), let $\mathcal{B}$ be the integral closure of $\mathcal{A}'$ in $\mathcal{L}$, and let $\mathcal{T} = \mathcal{B}[\varpi^{-1}]$.

Corollary 6.1.6. *Each of the factors of the degree eight* $\widehat{\mathcal{K}'}_{(t-\varrho)}$*-algebra* $\widehat{\mathcal{L}}_{(t-\varrho)}$ *is both totally ramified over and generated by standard form elements over* $\widehat{\mathcal{K}'}_{(t-\varrho)} \cong k((\beta))((t-\varrho))$.

Proof. The first claim of the corollary follows immediately from Lemma 6.1.5. For the second claim, let $r' \in k((\beta))((t-\varrho))$ such that $(r')^2 + r' = G'q' + J$. By Proposition 3.1.8, $\mathcal{K}'[\tilde{q}, \tilde{r}] = \mathcal{K}'[q', r']$. The second claim of the corollary now follows. □

Lemma 6.1.7. *Suppose that* $\widetilde{F}, \widetilde{G} \in \mathcal{A}'_{(\beta)} \cap \mathcal{K} = \mathcal{A}_{(\varpi)}$*, that* $\widetilde{F} \equiv F \pmod{\varpi}$ *and that* $\widetilde{G} \equiv G \pmod{\varpi}$*. Then* $\mathrm{Gal}(\mathcal{L}|\mathcal{K}') \cong D_4$.

Proof. Since $\mathrm{Gal}(\mathcal{L}|\mathcal{K}') \cong D_4$, it follows that $[F] \neq 0$ over K, that $[G] \neq 0$ over K, and that $[G] \neq [F]$ over K by Proposition 3.1.8. Since $\widetilde{F} \equiv F \pmod{\varpi}$ and $\widetilde{G} \equiv G \pmod{\varpi}$, it follows that $\widetilde{F} \equiv F \pmod{\beta}$ and $\widetilde{G} \equiv G \pmod{\beta}$. Hence $[\widetilde{F}] \neq 0$ over $\mathcal{A}'_{(\beta)}$, $[\widetilde{G}] \neq 0$ over $\mathcal{A}'_{(\beta)}$ and $[\widetilde{G}] \neq [\widetilde{F}]$ over $\mathcal{A}'_{(\beta)}$. Moreover, Since $\mathcal{A}'_{(\beta)}$ is a discrete valuation ring (and hence is integrally closed), it follows that $[\widetilde{F}] \neq 0$ over $\mathcal{K}'$, $[\widetilde{G}] \neq 0$ over $\mathcal{K}'$ and $[\widetilde{G}] \neq [\widetilde{F}]$ over $\mathcal{K}'$. Therefore, $\mathrm{Gal}(\mathcal{L}|\mathcal{K}') \cong D_4$ by Proposition 3.1.6 and by Lemma 3.1.2. □

6.1.2 First Deformation

For the first equicharacteristic deformation, suppose that the sequence of ramification groups of L over K is of Type I, *i.e.*, that $f < d = g$. Let $\widetilde{F} = F$, $\widetilde{G} = Gt^2(t-\varpi)^{-2}$, and $\widetilde{H} = Ht^2(t-\varpi)^{-2}$. By Corollary 6.1.6, there exists a finite extension $k((\beta))$ of $k((\varpi))$ such that each of the factors of the degree eight $\widehat{\mathcal{K}'}_{(t-\varpi)}$-algebra $\widehat{\mathcal{L}}_{(t-\varpi)}$ is both totally ramified over and generated by standard form elements over $\widehat{\mathcal{K}'}_{(t-\varpi)} \cong k((\beta))((t-\varpi))$, where $\mathcal{A}'$, $\mathcal{K}'$, $\mathcal{S}'$, $\mathcal{L}$, $\mathcal{B}$ and $\mathcal{T}$ are defined as in Subsection 6.1.1.

Proposition 6.1.8 (First Deformation)**.** *The following statements all hold.*

(1) $\mathrm{Gal}(\mathcal{L}|\mathcal{K}') \cong D_4$.

(2) *As a* D_4*-extension of Dedekind domains,* $\mathcal{B}/(\beta)$ *over* $\mathcal{A}'/(\beta)$ *is isomorphic to* B *over* A.

(3) *The* D_4*-extension of Dedekind domains* $\mathcal{T}$ *over* $\mathcal{S}'$ *is branched at precisely two maximal ideals,* viz. (t) *and* $(t-\varpi)$*. Above* (t)*, the inertia group is* D_4*, the sequence of lower ramification breaks is* $(\ell_1, \ell_2 - 4, \ell_3 - 4)$*, and the sequence of upper ramification breaks is* $(u_1, u_2 - 2, u_3 - 2)$*. Above* $(t-\varpi)$*, the inertia group is* $\mathrm{Gal}(\mathcal{L}|\mathcal{K}'[\tilde{q}]) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$*, and the sequence of lower ramification breaks is* $(1, 1)$.

Proof. To prove statement (1), note that $\widetilde{F}, \widetilde{G} \in \mathcal{A}_{(\varpi)} = \mathcal{A}'_{(\beta)} \cap \mathcal{K}$ since $(t-\varpi)^{-2} = t^{-2}\sum_{n=0}^{\infty}(t^{-1}\varpi)^{2n}$. Note also that $\widetilde{F} \equiv F \pmod{\varpi}$, and that $\widetilde{G} \equiv G \pmod{\varpi}$. Thus (1) holds by Lemma 6.1.7.

To prove (3) for the ideal (t), consider the completion $\widehat{\mathcal{S}'}_{(t)} \cong k((\beta))[[t]]$ of the localization $\mathcal{S}'_{(t)}$ of $\mathcal{S}'$, and note that, over $k((\beta))[[t]]$, $(t-\varpi)^{-2}$ is a unit. Thus $-v_{(t)}(\widetilde{F}) = f$, $-v_{(t)}(\widetilde{G}) = g-2$ and $-v_{(t)}(\widetilde{H}) = h-2$ (unless $H=0$). Since f is odd, $\widehat{\mathcal{K}'}_{(t)}[\tilde{q}]$ is a totally ramified extension of $\widehat{\mathcal{K}'}_{(t)} \cong k((\beta))((t))$ with conductor f by Proposition 2.2.7. Similarly, $\widehat{\mathcal{K}'}_{(t)}[\tilde{s}]$ is a totally ramified extensions of $\widehat{\mathcal{K}'}_{(t)}$ with conductor $g-2$. Moreover, if $f < g-2$, $-v_{(t)}(\widetilde{F}+\widetilde{G}) = g-2$. Since $(t-\varpi)^{-2} = \varpi^{-2}\sum_{n=0}^{\infty}(t\varpi^{-1})^{2n}$, the coefficient of t^{-g+2} in the Laurent series expansion of $\widetilde{G}$ is not contained in k, whereas the coefficient of t^{-f} in the Laurent series expansion of $\widetilde{F}$ is contained in k. Thus, if $f = g-2$, $-v_{(t)}(\widetilde{F}+\widetilde{G}) = g-2$ as well. Therefore, by Proposition 2.2.7, $\widehat{\mathcal{K}'}_{(t)}[\tilde{q}+\tilde{s}]$ is ramified over $\widehat{\mathcal{K}'}_{(t)}$ with conductor $g-2$. Hence, by Corollaries 4.1.2 and 4.3.3, the first, second and third terms in the sequence of upper ramification breaks over (t) are $\min\{g-2, f\} = f = u_1$, $g-2 = u_2-2$ and $\min\{f+g-2, h-2\} = \max\{f+g, h\} - 2 = u_3 - 2$, respectively. Statement (3) for (t) now follows by Proposition 2.1.11.

To prove (3) for the ideal $(t-\varpi)$, note that, over the completion $\widehat{\mathcal{S}'}_{(t-\varpi)} \cong k((\beta))[[t-\varpi]]$ of the localization $\mathcal{S}'_{(t-\varpi)}$ of $\mathcal{S}'$, t is a unit. Thus $-v_{(t-\varpi)}(\widetilde{F}) = 0$, $-v_{(t-\varpi)}(\widetilde{G}) = -v_{(t-\varpi)}(\widetilde{F}+\widetilde{G}) = 2$, and $-v_{(t-\varpi)}(\widetilde{H}) \le 2$. Since each factor of $\widehat{\mathcal{L}}_{(t-\varpi)}$ is generated by standard form elements over $\widehat{\mathcal{K}'}_{(t-\varpi)}$, it follows that $[\widetilde{F}] = 0$ over $\widehat{\mathcal{K}'}_{(t-\varpi)}$ and that thus $\widehat{\mathcal{K}'}_{(t-\varpi)}[\tilde{q}] = \widehat{\mathcal{K}'}_{(t-\varpi)}$. Furthermore, the conductor of $\widehat{\mathcal{K}'}_{(t-\varpi)}[\tilde{q}, \tilde{s}]$ over $\widehat{\mathcal{K}}_{(t-\varpi)}[\tilde{q}]$ is 1.

Since $[\widetilde{F}] = 0$ over $\widehat{\mathcal{K}'}_{(t-\varpi)}$, the fact that each factor of $\widehat{\mathcal{L}}_{(t-\varpi)}$ is generated by standard form elements over $\widehat{\mathcal{K}'}_{(t-\varpi)}$ implies that $\widetilde{G}\tilde{q}+\widetilde{H}$ is Artin–Schreier-equivalent over $\widehat{\mathcal{K}'}_{(t-\varpi)}$ to an element J in standard form with respect to $t-\varpi$. Moreover, since $\tilde{q} \notin k((\beta))$, $-v_{(t-\varpi)}(\widetilde{G}\tilde{q}+\widetilde{H}) = 2$. Thus $-v_{(t-\varpi)}(J) = 1$, and the conductor of $\widehat{\mathcal{K}'}_{(t-\varpi)}[\tilde{q}, \tilde{r}]$ over $\widehat{\mathcal{K}'}_{(t-\varpi)}[\tilde{q}]$ is 1. Similarly, $-v_{(t-\varpi)}(\widetilde{G}\tilde{q}+\widetilde{G}+\widetilde{H}) = 2$, and the conductor of $\widehat{\mathcal{K}'}_{(t-\varpi)}[\tilde{q}, \tilde{r}+\tilde{s}]$ over $\widehat{\mathcal{K}'}_{(t-\varpi)}[\tilde{q}]$ is 1. Statement (3) for $(t-\varpi)$ now follows by Lemma 4.1.5 (and Corollary 4.1.2).

Finally, to prove (2), note that the degree $\delta_{L|K}$ of the different of L over K is $4\ell_1 + 2\ell_2 + \ell_3 + 7$ by Corollary 2.3.4 (Hilbert's different formula). Similarly, by (3), the contribution of (t) to the degree $\delta_{\mathcal{T}'|\mathcal{S}'}$ of the different of $\mathcal{T}'$ over $\mathcal{S}'$ is $4\ell_1 + 2(\ell_2-4) + (\ell_3-4) + 7 = \delta_{L|K} - 12$, and the contribution of $(t-\varpi)$ is $\delta_{\mathcal{T}'|\mathcal{S}'}$ is $2\cdot(2(1)+1+3) = 12$. Thus $\delta_{\mathcal{T}'|\mathcal{S}'} = \delta_{L|K} - 12 + 12 = \delta_{L|K}$. Therefore (2) holds by Theorem 3.4 in [GM98]. □

6.1.3 Second Deformation

For the second equicharacteristic deformation, suppose that the sequence of ramification groups of L over K is of Type II, *i.e.*, that $d < f = g$. Let a_f denote the coefficient of t^{-f} in the Laurent series expansion of F, and let a_g denote the coefficient of t^{-g} in the Laurent series expansion of G. Let also $\widetilde{F} = F + a_f t^{-f} + a_f t^{-f+2}(t-\varpi)^{-2}$, $\widetilde{G} = G + a_g t^{-g} + a_g t^{-g+2}(t-\varpi)^{-2}$, and $\widetilde{H} = Ht^4(t-\varpi)^{-4}$. By Corollary 6.1.6, there exists a finite extension $k((\beta))$ of $k((\varpi))$ such that each of the factors of the degree eight $\widehat{\mathcal{K}'}_{(t-\varpi)}$-algebra $\widehat{\mathcal{L}}_{(t-\varpi)}$ is both totally ramified over and generated by standard form elements over $\widehat{\mathcal{K}'}_{(t-\varpi)} \cong k((\beta))((t-\varpi))$, where $\mathcal{A}'$, $\mathcal{K}'$, $\mathcal{S}'$, $\mathcal{L}$, $\mathcal{B}$ and $\mathcal{T}$ are defined as in Subsection 6.1.1.

Proposition 6.1.9 (Second Deformation)**.** *The following statements all hold.*

(1) $\mathrm{Gal}(\mathcal{L}|\mathcal{K}') \cong D_4$.

(2) *As a D_4-extension of Dedekind domains, $\mathcal{B}/(\beta)$ over $\mathcal{A}'/(\beta)$, is isomorphic to B over A.*

(3) *The D_4-extension of Dedekind domains $\mathcal{T}$ over $\mathcal{S}'$ is branched at precisely two maximal ideals,* viz. *(t) and $(t-\varpi)$. Above (t), the inertia group is D_4, the sequence of lower ramification breaks is $(\ell_1, \ell_2 - 4, \ell_3 - 12)$, and the sequence of upper ramification breaks is $(u_1, u_2 - 2, u_3 - 4)$. Above $(t-\varpi)$, the inertia group is $\mathrm{Gal}(\mathcal{L}|\mathcal{K}'[\tilde{q}+\tilde{s}]) \cong \mathbb{Z}/4\mathbb{Z}$, and the sequence of lower ramification breaks is $(1,5)$.*

Proof. To prove statement (1), note that $\widetilde{F}, \widetilde{G} \in \mathcal{A}_{(\varpi)} = \mathcal{A}'_{(\beta)} \cap \mathcal{K}$ since $(t-\varpi)^{-2} = t^{-2}\sum_{n=0}^{\infty}(t^{-1}\varpi)^{2n}$. Note also that $\widetilde{F} \equiv F \pmod{\varpi}$, and that $\widetilde{G} \equiv G \pmod{\varpi}$. Thus (1) holds by Lemma 6.1.7.

To prove (3) for the ideal (t), note that, over the completion $\widehat{\mathcal{S}'}_{(t)} \cong k((\beta))[[t]]$ of the localization $\mathcal{S}'_{(t)}$ of $\mathcal{S}'$, $(t-\varpi)^{-2}$ is a unit. Thus $-v_{(t)}(\widetilde{F}) = f-2$ and $-v_{(t)}(\widetilde{G}) = g-2$, and $-v_{(t)}(\widetilde{H}) = h-4$ (unless $H=0$). Since $f-2$ is odd, $\widehat{\mathcal{K}'}_{(t)}[\tilde{q}]$ is a totally ramified extension of $\widehat{\mathcal{K}'}_{(t)} \cong k((\beta))((t))$ with conductor $f-2$ by Proposition 2.2.7. Similarly, $\widehat{\mathcal{K}'}_{(t)}[\tilde{s}]$ is totally ramified over $\widehat{\mathcal{K}'}_{(t)}$ with conductor $g-2$. Moreover, since $d < f = g$, it follows that $a_f = a_g$ and that $\widetilde{F}+\widetilde{G} = F+G$. Thus $-v_{(t)}(\widetilde{F}+\widetilde{G}) = d$. Therefore, since $f-2$, $g-2$ and d are all both positive and odd, it follows by Corollary 4.3.3 (and Corollary 4.1.2) that $\widehat{\mathcal{L}}_{(t)}$ is a field extension of $\widehat{\mathcal{K}'}_{(t)}$, and that the first, second and third terms of the sequence of upper ramification breaks over (t) are $\min\{d, f-2\} = d = u_1$, $g-2 = u_2-2$ and $\max\{f-2+g-2, h-4\} = \max\{f+g, h\} - 4 = u_3 - 4$, respectively. Statement (3) for (t) now follows by Proposition 2.1.11.

To prove (3) for the ideal $(t-\varpi)$, note that, over the completion $\widehat{\mathcal{S}'}_{(t-\varpi)} \cong k((\beta))[[t-\varpi]]$ of the localization $\mathcal{S}'_{(t-\varpi)}$ of $\mathcal{S}'$, t is a unit. Thus $-v_{(t-\varpi)}(\widetilde{F}) = -v_{(t-\varpi)}(\widetilde{G}) = 2$, $-v_{(t-\varpi)}(\widetilde{F}+\widetilde{G}) = -v_{(t-\varpi)}(F+G) = 0$, and $-v_{(t-\varpi)}(\widetilde{H}) \leq 4$. Since each factor of $\widehat{\mathcal{L}}_{(t-\varpi)}$ is generated by standard form elements over $\widehat{\mathcal{K}'}_{(t-\varpi)}$, it follows that $[\widetilde{F}+\widetilde{G}] = 0$ over $\widehat{\mathcal{K}'}_{(t-\varpi)}$ and that thus $\widehat{\mathcal{K}'}_{(t-\varpi)}[\tilde{q}+\tilde{s}] = \widehat{\mathcal{K}'}_{(t-\varpi)}$. Furthermore, the conductor of $\widehat{\mathcal{K}'}_{(t-\varpi)}[\tilde{q}] = \widehat{\mathcal{K}'}_{(t-\varpi)}[\tilde{s}]$ over $\widehat{\mathcal{K}'}_{(t-\varpi)}$ is 1.

Let F' and G' denote the elements of $\widehat{\mathcal{K}'}_{(t-\varpi)}$ in standard form that are Artin–Schreier-equivalent to $\widetilde{F}$ and $\widetilde{G}$, respectively, and let $q', s' \in \widehat{\mathcal{K}'}^{\mathrm{alg}}_{(t-\varpi)}$ such that $(q')^2 + q' = F'$ and $(s')^2 + s' = G'$. Let also $\widetilde{J} = G'(q'+\tilde{q}) + \widetilde{F}(s'+\tilde{s})^2 + \widetilde{H} \in \widehat{\mathcal{K}'}_{(t-\varpi)}$. Then

$[\widetilde{G}\tilde{q} + \widetilde{H}] = [G'q' + \widetilde{J}]$ by Proposition 3.1.8. Since $\widehat{\mathcal{L}}_{(t-\varpi)}$ is generated by standard form elements over $\widehat{\mathcal{K}'}_{(t-\varpi)}$, it follows that $\widetilde{J}$ is Artin–Schreier-equivalent over $\widehat{\mathcal{K}'}_{(t-\varpi)}$ to an element J in standard form with respect to $t - \varpi$.

Let b denote the conductor of $\widehat{\mathcal{K}'}_{(t-\varpi)}[\tilde{q}, \tilde{r}, \tilde{s}] = \widehat{\mathcal{K}'}_{(t-\varpi)}[\tilde{q}, \tilde{r}]$ over $\widehat{\mathcal{K}'}_{(t-\varpi)}[\tilde{q}]$. It follows from Proposition 2.1.5 that the sequence of lower ramification breaks of $\widehat{\mathcal{K}'}_{(t-\varpi)}[\tilde{q}, \tilde{r}]$ over $\widehat{\mathcal{K}'}_{(t-\varpi)}[\tilde{q}]$ is $(1, b)$. Since $-v_{(t-\varpi)}(F' + \widetilde{F}) = 2$, $-v_{(t-\varpi)}(q' + \tilde{q}) = 1$. Similarly, $-v_{(t-\varpi)}(s' + \tilde{s}) = 1$. Thus

$$-v_{(t-\varpi)}(\widetilde{J}) = G'(q' + \tilde{q}) + \widetilde{F}(s' + \tilde{s})^2 + \widetilde{H} \leq 4,$$

and hence $-v_{(t-\varpi)}(J) \leq 3$. Since $\widehat{\mathcal{K}'}_{(t-\varpi)}[\tilde{q}] = \widehat{\mathcal{K}'}_{(t-\varpi)}[\tilde{s}]$, Proposition 2.2.1 implies that $F' = G'$. Therefore, $b = 2\max\{1 + 1, -v_{(t-\varpi)}(J)\} - 1 \leq 5$ by Corollary 4.1.11. Thus the contribution of $(t - \varpi)$ to the degree $\delta_{\mathcal{T}'|\mathcal{S}'}$ of the different of $\mathcal{T}'$ over $\mathcal{S}'$ is $2 \cdot (2(1) + b + 3) = 2b + 10 \leq 20$ by Corollary 2.3.4 (Hilbert's different formula). Moreover, the contribution of (t) to the degree $\delta_{\mathcal{T}'|\mathcal{S}'}$ is $4\ell_1 + 2(\ell_2 - 4) + (\ell_3 - 12) + 7 = \delta_{L|K} - 20$ by statement (3) for (t). Hence $\delta_{\mathcal{T}'|\mathcal{S}'} \leq \delta_{L|K}$. By Theorem 3.4 in [GM98], $\delta_{\mathcal{T}'|\mathcal{S}'} \geq \delta_{L|K}$. Thus $\delta_{\mathcal{T}'|\mathcal{S}'} = \delta_{L|K}$, $2b + 10 = 20$, and $b = 5$. Statement (3) for $(t - \varpi)$ now follows immediately, and statement (2) follows by Theorem 3.4 in [GM98]. □

6.1.4 Third Deformation

For the third equicharacteristic deformation, suppose that $u_1 = \min\{d, f\} > 1$. Let $\widetilde{F} = Ft^2(t - \varpi)^{-2}$, $\widetilde{G} = Gt^2(t - \varpi)^{-2}$, and $\widetilde{H} = Ht^4(t - \varpi)^{-4}$. By Corollary 6.1.6, there exists a finite extension $k((\beta))$ of $k((\varpi))$ such that each of the factors of the degree eight $\widehat{\mathcal{K}'}_{(t-\varpi)}$-algebra $\widehat{\mathcal{L}}_{(t-\varpi)}$ is both totally ramified over and generated by standard form elements over $\widehat{\mathcal{K}'}_{(t-\varpi)} \cong k((\beta))((t - \varpi))$, where $\mathcal{A}'$, $\mathcal{K}'$, $\mathcal{S}'$, $\mathcal{L}$, $\mathcal{B}$ and $\mathcal{T}$ are defined as in Subsection 6.1.1.

Proposition 6.1.10 (Third Deformation)**.** *The following statements all hold.*

(1) $\mathrm{Gal}(\mathcal{L}|\mathcal{K}') \cong D_4$.

(2) *As a D_4-extension of Dedekind domains, $\mathcal{B}/(\beta)$ over $\mathcal{A}'/(\beta)$ is isomorphic to B over A.*

(3) *The D_4-extension of Dedekind domains $\mathcal{T}$ over $\mathcal{S}'$ is branched at precisely two maximal ideals,* viz. *(t) and $(t - \varpi)$. Above (t), the inertia group is D_4, the sequence of lower ramification breaks is $(\ell_1 - 2, \ell_2 - 2, \ell_3 - 10)$, and the sequence of upper ramification breaks is $(u_1 - 2, u_2 - 2, u_3 - 4)$. Above $(t - \varpi)$, the inertia group is D_4, and the sequence of lower ramification breaks is $(1, 1, 9)$.*

Proof. To prove statement (1), note that $\widetilde{F}, \widetilde{G} \in \mathcal{A}_{(\varpi)} = \mathcal{A}'_{(\beta)} \cap \mathcal{K}$ since $(t - \varpi)^{-2} = t^{-2}\sum_{n=0}^{\infty}(t^{-1}\varpi)^{2n}$. Note also that $\widetilde{F} \equiv F \pmod{\varpi}$, and that $\widetilde{G} \equiv G \pmod{\varpi}$. Thus (1) holds by Lemma 6.1.7.

To prove (3) for the ideal (t), note that, over the completion $\widehat{\mathcal{S}'}_{(t)} \cong k((\beta))[[t]]$ of the localization $\mathcal{S}'_{(t)}$ of $\mathcal{S}'$, $(t - \varpi)^{-2}$ is a unit. Thus $-v_{(t)}(\widetilde{F}) = f - 2$, $-v_{(t)}(\widetilde{G}) =$

$g-2$, and $-v_{(t)}(\widetilde{H}) = h-4$ (unless $H=0$). Since $f-2$ is both positive and odd, $\widehat{\mathcal{K}'}_{(t)}[\tilde{q}]$ is a totally ramified extension of $\widehat{\mathcal{K}'}_{(t)} \cong k((\beta))((t))$ with conductor $f-2$ by Proposition 2.2.7. Similarly, $\widehat{\mathcal{K}'}_{(t)}[\tilde{s}]$ is totally ramified over $\widehat{\mathcal{K}'}_{(t)} \cong k((\beta))((t))$ with conductor $g-2$. Moreover, since $\widetilde{F}+\widetilde{G} = (F+G)t^2(t-\varpi)^{-2}$, it follows that $\widehat{\mathcal{K}'}_{(t)}[\tilde{q}+\tilde{s}]$ is totally ramified over $\widehat{\mathcal{K}'}_{(t)}$ with conductor $d-2$. Since $f-2$, $g-2$ and $d-2$ are all both positive and odd, and $h-4$ is not both positive and even, Corollaries 4.1.2 and 4.3.3 together imply that $\widehat{\mathcal{L}}_{(t)}$ is a field extension of $\widehat{\mathcal{K}'}_{(t)}$, and that the first, second and third terms of the sequence of upper ramification breaks over (t) are $\min\{d-2, f-2\} = \min\{d,f\}-2 = u_1-2$, $g-2 = u_2-2$ and $\max\{f-2+g-2, h-4\} = \max\{f+g,h\}-4 = u_3-4$, respectively. Statement (3) for (t) now follows by Proposition 2.1.11.

To prove (3) for the ideal $(t-\varpi)$, note that, over the completion $\widehat{\mathcal{S}'}_{(t-\varpi)} \cong k((\beta))[[t-\varpi]]$ of the localization $\mathcal{S}'_{(t-\varpi)}$ of $\mathcal{S}'$, t is a unit. Thus $-v_{(t-\varpi)}(\widetilde{F}) = 2 = -v_{(t-\varpi)}(\widetilde{G}) = -v_{(t-\varpi)}(\widetilde{F}+\widetilde{G}) = 2$, and $-v_{(t-\varpi)}(\widetilde{H}) \le 4$. Since each factor of $\widehat{\mathcal{L}}_{(t-\varpi)}$ is generated by standard form elements over $\widehat{\mathcal{K}'}_{(t-\varpi)}$, it follows that each of the conductors of $\widehat{\mathcal{K}'}_{(t-\varpi)}[\tilde{q}]$, $\widehat{\mathcal{K}'}_{(t-\varpi)}[\tilde{s}]$, and $\widehat{\mathcal{K}'}_{(t-\varpi)}[\tilde{q}+\tilde{s}]$ over $\widehat{\mathcal{K}'}_{(t-\varpi)}$ is 1. Thus (*cf.* Remark 4.2.3) $\widehat{\mathcal{L}}_{(t-\varpi)}$ is itself a (totally ramified) field extension of $\widehat{\mathcal{K}'}_{(t-\varpi)}$.

As in the second deformation, let F' and G' denote the elements of $\widehat{\mathcal{K}'}_{(t-\varpi)}$ in standard form that are Artin–Schreier-equivalent to $\widetilde{F}$ and $\widetilde{G}$, respectively, and let $q', s' \in \widehat{\mathcal{K}'}^{\mathrm{alg}}_{(t-\varpi)}$ such that $(q')^2+q' = F'$ and $(s')^2+s' = G'$. Let also $\widetilde{J} = G'(q'+\tilde{q}) + \widetilde{F}(s'+\tilde{s})^2 + \widetilde{H} \in \widehat{\mathcal{K}'}_{(t-\varpi)}$. Then $[\widetilde{G}\tilde{q}+\widetilde{H}] = [G'q'+\widetilde{J}]$ by Proposition 3.1.8. Since $\widehat{\mathcal{L}}_{(t-\varpi)}$ is a D_4-standard form extension of $\widehat{\mathcal{K}'}_{(t-\varpi)}$, it follows that $\widetilde{J}$ is Artin–Schreier-equivalent over $\widehat{\mathcal{K}'}_{(t-\varpi)}$ to an element J in standard form with respect to $t-\varpi$.

Let b denote the conductor of $\widehat{\mathcal{K}'}_{(t-\varpi)}[\tilde{q},\tilde{r}]$ over $\widehat{\mathcal{K}'}_{(t-\varpi)}[\tilde{q}]$. By Proposition 4.3.2 (and Corollary 4.1.2), it follows that the sequence of lower ramification breaks of $\widehat{\mathcal{L}}_{(t-\varpi)}$ over $\widehat{\mathcal{K}'}_{(t-\varpi)}$ is $(1,1,2b-1)$. Since $-v_{(t-\varpi)}(F'+\widetilde{F}) = 2$, $-v_{(t-\varpi)}(q'+\tilde{q}) = 1$. Similarly, $-v_{(t-\varpi)}(s'+\tilde{s}) = 1$. Thus

$$-v_{(t-\varpi)}(\widetilde{J}) = G'(q'+\tilde{q}) + \widetilde{F}(s'+\tilde{s})^2 + \widetilde{H} \le 4,$$

and hence $-v_{(t-\varpi)}(J) \le 3$. Therefore, $b = 2\max\{1+1, -v_{(t-\varpi)}(J)\} - 1 \le 5$ by Proposition 4.1.8. Thus the contribution of $(t-\varpi)$ to the degree $\delta_{\mathcal{T}'|\mathcal{S}'}$ of the different of $\mathcal{T}'$ over $\mathcal{S}'$ is $4(1)+2(1)+(2b-1)+7 = 2b+12 \le 22$ by Corollary 2.3.4 (Hilbert's different formula). Moreover, the contribution of (t) to the degree $\delta_{\mathcal{T}'|\mathcal{S}'}$ is $4(\ell_1-2)+2(\ell_2-2)+(\ell_3-10)+7 = \delta_{L|K}-22$ by statement (3) for (t). Hence $\delta_{\mathcal{T}'|\mathcal{S}'} \le \delta_{L|K}$. By Theorem 3.4 in [GM98], $\delta_{\mathcal{T}'|\mathcal{S}'} \ge \delta_{L|K}$. Thus $\delta_{\mathcal{T}'|\mathcal{S}'} = \delta_{L|K}$, $2b+12 = 22$ and $b=5$. Statement (3) for $(t-\varpi)$ now follows immediately, and statement (2) follows by Theorem 3.4 in [GM98]. □

6.2 Main Theorem

Having now found various equicharacteristic deformations of D_4-Galois extensions of complete discrete valuation fields of characteristic two with algebraically closed residue field, we use the 'method of equicharacteristic deformation', as used in [Pop14], in [Obu15], and in [Obu16] to prove that all such extensions lift to characteristic zero, *i.e.*, that D_4 is a local Oort group for the prime two. We begin by using the deformations of Section 6.1 to reduce to the case of extensions with, in some sense, small ramification breaks.

6.2.1 Deformation Reductions

In order to use the deformations of Section 6.1 effectively to reduce the cases under consideration, we shall need to use Theorem 6.20 in [Obu17], which is reproduced below as Theorem 6.2.1 for convenience. The argument for this theorem was communicated orally by Pop, who presented an earlier version of this theorem, peculiar to the cyclic case, in [Pop14].

Let k be an algebraically closed residue field of characteristic $p > 0$, let $K = k((t))$, and let G be a cyclic-by-p group.

Theorem 6.2.1. *Suppose that $k[[z]]/k[[t]]$ is a local G-extension that admits an equicharacteristic deformation whose generic fiber lifts to characteristic zero after base change to the algebraic closure. Then $k[[z]]/k[[t]]$ lifts to characteristic zero.*

As we shall only require the case in which $p = 2$, we shall assume that $p = 2$ henceforth.

Proposition 6.2.2. *Let (u_1, u_2, u_3) be a triple of positive integers such that there exists a D_4-extension of K whose sequence of ramification breaks (u_1, u_2, u_3). Suppose that $u_2 > 1$, and that every D_4-Galois extension of K with second ramification break over K less than or equal to $u_2 - 2$ lifts to characteristic zero. Then every D_4-Galois extension of K whose sequence of ramification breaks is (u_1, u_2, u_3) lifts to characteristic zero.*

Proof. Let L be a D_4-extension of K whose sequence of upper ramification breaks is (u_1, u_2, u_3). The sequence of ramification groups must be of one of the three types enumerated in Subection 4.4.

Suppose firstly that the sequence of ramification groups of L is of Type I. By Proposition 6.1.8, L admits an equicharacteristic deformation whose generic fiber has second ramification break $u_2 - 2$ over the ideal (t) and inertia group congruent to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ over the ideal $(t - \varpi)$. By the hypothesis above and [Pag02], the base change of this generic fiber to the algebraic closure lifts to characteristic zero. Thus $L|K$ lifts to characteristic zero by Theorem 6.2.1.

Suppose secondly that the sequence of ramification groups of L is of Type II. By Propostition 6.1.9, L admits an equicharacteristic deformation whose generic fiber has second ramification break $u_2 - 2$ over the ideal (t) and inertia group congruent to

$\mathbb{Z}/4\mathbb{Z}$ over the ideal $(t-\varpi)$. By the hypothesis above and [GM98], the base change of this generic fiber to the algebraic closure lifts to characteristic zero. Thus $L|K$ lifts to characteristic zero by Theorem 6.2.1.

Suppose finally that the sequence of ramification groups of L is of Type III. By Proposition 4.4.2, $u_1 = u_2$. Since $u_2 > 1$ by supposition, $u_1 > 1$ as well. Therefore, L admits an equicharacteristic deformation whose generic fiber has second ramification break $u_2 - 2$ over the ideal (t) and second ramification break 1 over the ideal $(t-\varpi)$ by Proposition 6.1.10. Thus the base change of this generic fiber to the algebraic closure lifts to characteristic zero by hypothesis. Hence $L|K$ lifts to characteristic zero by Theorem 6.2.1. □

6.2.2 Supersimple Extensions

The propositions of the previous subsection have effectively reduced the proof that D_4 is a local Oort group to showing that every D_4-extension of a complete discrete valuation field of characteristic two with algebraically closed residue field whose second upper ramification break is 1 lifts to characteristic zero. That all such extensions do, in fact, lift to characteristic zero, is a result of Brewis in [Bre08], phrased there in somewhat different language.

Let K be a complete discrete valuation field of characteristic two with algebraically closed residue field, and let L be a Galois extension of K such that $\mathrm{Gal}(L|K) \cong D_4$. Following Brewis, we fix $a, b \in D_4$ such that $D_4 = \langle a, b \mid a^4 = b^2 = e, bab^{-1} = a^3 \rangle$.

Definition 6.2.3 (Brewis)**.** The extension L over K is *supersimple* if both of the following two conditions hold:

1. The degree of different of $L^{\langle a^2 \rangle}$ over $L^{\langle a^2, b \rangle}$ is 2.
2. The degree of different of $L^{\langle a^2, b \rangle}$ over K is 2.

The main result of [Bre08], denoted therein as Theorem 4, is as follows:

Theorem 6.2.4 (Brewis)**.** *If $L|K$ is supersimple, then $L|K$ lifts to characteristic zero.*

To rephrase Theorem 6.2.4 in terms of the ramification breaks of L over K, we shall need the following proposition.

Proposition 6.2.5. *The extension $L|K$ is supersimple if and only if the second ramification break of $L|K$ is 1.*

Proof. By Hilbert's different formula (Corollary 2.3.4), $L|K$ is supersimple if and only if both the conductor of $L^{\langle a^2 \rangle}$ over $L^{\langle a^2, b \rangle}$ and the conductor of $L^{\langle a^2, b \rangle}$ over K are equal to 1. By Lemma 4.1.3 and Lemma 4.1.5, this occurs if and only if all three of the conductors over K of the degree two subextensions $L^{\langle a^2, b \rangle}$, $L^{\langle a^2, ab \rangle}$ and $L^{\langle a \rangle}$ are equal to 1. By Proposition 4.3.2, this occurs if and only if the second ramification break of $L|K$ is 1. □

Corollary 6.2.6. *Suppose that the second upper ramification break of L over K is 1. Then $L|K$ lifts to characteristic zero.*

6.2.3 Proof of Main Theorem

We conclude by proving the main theorem of the thesis concerning D_4, and by observing an immediate corollary.

Theorem 6.2.7. *The group D_4 is a local Oort group for the prime 2. That is, the following statement holds:*

Let K be a complete discrete valuation field of characteristic two with algebraically closed residue field, and let L be a Galois extension of K such that $\mathrm{Gal}(L|K) \cong D_4$. *Then $L|K$ lifts to characteristic zero.*

Proof. Let u_2 denote the second upper ramification break of L over K. We shall proceed by strong induction on u_2. By Corollary 4.3.3, u_2 is odd. The base case ($u_2 = 1$) is given by Corollary 6.2.6. Since u_2 is odd, the induction step is given by Proposition 6.2.2. Thus $L|K$ lifts to characteristic zero, as claimed. □

By Theorem 1.2.7 (or by Theorem 1.2.8), Theorem 6.2.7 implies the following corollary.

Corollary 6.2.8. *The group D_4 is an Oort group for the prime 2.*

Remark 6.2.9. One might hope to use the methods used in this paper to prove that D_8, or more ambitiously, D_{2^n} for some $n \geq 4$, is also a local Oort group for $p = 2$. However, there are at present at least two substantial obstacles to such a proof.

Firstly, the calculation of the ramification breaks (and hence the differents) of D_4-extensions of complete discrete valuation fields presented in Subsection 4.3 depends essentially on the fact that the Galois closure of any non-Galois two-level tower of $\mathbb{Z}/2\mathbb{Z}$-extensions of a field is a D_4-extension of that field. While D_8-extensions do occur as the Galois closures of smaller field extensions, there is no similarly simple class of extensions whose Galois closures are invariably D_8-extensions. The situation for higher dihedral extensions is similar to that for D_8-extensions.

Secondly, the effective use of the 'method of equicharacteristic deformation' requires a base case of extensions known to lift to characteristic zero. In the D_4 case, the work of Brewis in [Bre08] provided this base. However, neither in the D_8 case nor in any higher dihedral case is any extension in characteristic two known to lift to characteristic zero.

Chapter 7

Local Lifting of Q_8-Extensions and $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$-Extensions

Let k be an algebraically closed field of characteristic two. In this chapter, we shall show that neither Q_8 nor $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ is an almost local Oort group (or even an almost local Bertin group) for k, and shall rehearse open problems concerning the local lifting of Q_8-extensions and of $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$-extensions.

7.1 The Bertin Obstruction

Let $K = k((t))$ be the field of Laurent series over k let $L = k((s))$ be a finite Galois extension of K. Moreover, let $\Gamma = \mathrm{Gal}(L|K)$, and let $\phi : \Gamma \to \mathrm{Aut}_k(k[[s]])$ denote the canonical Galois action of Γ on $k[[s]]$. As in Subsection 2.1, we define a function $i_\Gamma : \Gamma \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$ such that

$$i_\Gamma(\sigma) = v_L\left(\sigma(s) - s\right)$$

for all $\sigma \in \Gamma$, where v_L is the discrete valuation of L.

Definition 7.1.1. The *Artin character* $a_\phi : G \to \mathbb{Z}$ of ϕ is defined such that

$$a_\phi(\sigma) = \begin{cases} -i_\Gamma(\sigma) & \text{if } \sigma \neq \mathrm{Id}_L \\ \sum_{\sigma \neq \mathrm{Id}_L} i_\Gamma(\sigma) & \text{if } \sigma = \mathrm{Id}_L \end{cases}.$$

In [Ber98], Bertin proved a more general, global version of the following local theorem, which follows the rephrasing in [CGH11].

Theorem 7.1.2 (Théoréme in [Ber98])**.** *Suppose $L|K$ lifts to characteristic zero. Then there exists a positive integer m and a finite G-set S with non-cyclic trivial stabilizers such that $a_\phi = m \cdot \mathrm{reg}_\Gamma - \chi_S$, where reg_Γ is the character of the regular representation of G, and χ_S is the character defined by the action of G on S.*

In light of Theorem 7.1.2, we say that the *Bertin obstruction of ϕ vanishes* if such an m and an S do exist.

We now let $\mathcal{C}$ be a set of representatives of the conjugacy classes of the cyclic subgroups of G, and, for all subgroups H of G, let 1_H denote the trivial one-dimensional character of H.

Proposition 7.1.3 (Proposition 2.1 in [CGH11]). *The following statements both hold.*

(1) *There exist unique rational numbers b_T for $T \in \mathcal{C}$ such that*

$$-a_\phi = \sum_{T \in \mathcal{C}} b_T \mathrm{Ind}_T^H 1_T.$$

(2) *The Bertin obstruction of ϕ vanishes if and only if b_T is a non-negative integer for all $T \neq \{\mathrm{Id}_{k[[s]]}\}$.*

In the case in which Γ is either a dihedral group of order $2p^n$, or (if $p = 2$) a semi-dihedral or quaternion group of order $2p^n$, Chinburg, Guralnick and Harbater used the characterization of the Bertin obstruction given in 7.1.3 to prove necessary and sufficient conditions for the Bertin obstruction of ϕ to vanish in terms of the ramification breaks of extensions $L'|K'$ such that $K \subseteq K' \subseteq L' \subseteq L$. We provide the result for $\Gamma = \mathrm{Gal}(L|K) \cong Q_8$ below.

Proposition 7.1.4 (Corollary 14.11.c in [CGH11]). *Suppose that $\Gamma \cong Q_8$, and let $L_0 \subseteq L$ denote a degree two subextension of K. Moreover, let d_0 denote the degree of the different of $L_0|K$ (so that $d_0 - 1$ is the conductor of $L_0|K$), and define i_0 and i_1 such that the sequence of upper ramification breaks of $N|L_0$ is $(i_0, i_0 + i_1)$. Then the Bertin obstruction of ϕ vanishes if and only if i_1 is even, and $i_1 \geq d_0$.*

7.2 Q_8-Extensions and $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$-Extensions with Non-Vanishing Bertin Obstruction

Let k be an algebraically closed field of characteristic two, let $K = k((t))$, let $K' = k((t^3))$and fix an algebraic closure K^{alg} of K. In this section we exhibit, for each odd positive integer n, a Q_8-extension $N|K$ whose sequence of lower ramification breaks is $(n, n, 3n)$. Moreover, if $3 \nmid n$, the extension $N|K'$ is a $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$-extension. We observe that it follows that both the local Q_8-action corresponding to $N|K$ and the local $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$-action corresponding to $N|K'$ if $3 \nmid n$ have non-vanishing Bertin obstruction. Hence neither Q_8 nor $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ is, in the sense of [CGH11], an almost Bertin group for k.

7.2.1 Q_8-Extensions

Let n be an odd positive integer. Moreover, for all $i \in \{0, 1, 2\}$, let $F_i = \zeta_3^i t^{-n}$, where $\zeta_3 \in k$ is a fixed non-trivial cube root of unity, and let $q_i \in K^{\mathrm{alg}}$ such that $q_i^2 + q_i = F_i$. Finally, let $L_i = K[q_i]$ for all $i \in \{0, 1, 2\}$, let M be the compositum of L_0, L_1 and L_2, and let $N = M[s]$, where $s \in K^{\mathrm{alg}}$ such that

$$s^2 + s = F_1 q_0 + F_2 q_1 + F_0 q_2 = \zeta_3 t^{-n} q_0 + \zeta_3^2 t^{-n} q_1 + t^{-n} q_2.$$

Lemma 7.2.1. *The field N is a Q_8-extension of K. Moreover, the sequence of lower ramification breaks of $N|K$ is $(n, n, 3n)$.*

Proof. Note that

$$s^2 + s = F_1 q_0 + F_2 q_1 + F_0 q_2 = (F_1 + F_0)q_0 + (F_2 + F_0)q_1 = F_2 q_0 + F_1 q_1.$$

Thus N is a Q_8-extension of K by Proposition 3.3.7. Furthermore, by Corollary 5.2.18, the sequence of lower ramification breaks of $N|K$ is $(n, n, 4\max\{3n/2, n+m\} - 3n)$, where $m = \min\{\deg_{t^{-1}}(F_1 + \zeta_3 F_0), \deg_{t^{-1}}(F_1 + \zeta_3^2 F_0)\}$. Since $F_1 = \zeta_3 t^{-n} = \zeta_3 F_0$, it follows that $m = -\infty$, and that the sequence of lower ramification breaks of $N|K$ is $(n, n, 3n)$. □

Lemma 7.2.2. *Let $i \in \{0, 1, 2\}$ The sequence of upper ramification breaks of $N|L_i$ is $(n, 2n)$.*

Proof. Let $\Gamma = \mathrm{Gal}(N|K)$. Since $\mathrm{Gal}(N|L_i)$ is a subgroup of $\mathrm{Gal}(N|K)$, it follows by Proposition 2.1.5 that $\Gamma_\ell \cap \mathrm{Gal}(N|M) = \mathrm{Gal}(N|M)_\ell$ for all $\ell \geq -1$. Therefore, by Lemma 7.2.1, the sequence of lower ramification breaks of $N|L_i$ is $(n, 3n)$. By Proposition 2.1.11, the sequence of upper ramification breaks of $N|L_i$ is thus $(n, 2n)$. □

Proposition 7.2.3. *Let u be a uniformizer of N, and let $\phi : Q_8 \to \mathrm{Aut}_k(k[[u]])$ be the local Q_8-action corresponding to $N|K$. Then the Bertin obstruction of ϕ does not vanish.*

Proof. Let $H = \mathrm{Gal}(N|L_0)$, and define i_0 and i_1 such that the sequence of upper ramification breaks of $N|L_0$ is $(i_0, i_0 + i_1)$. By Lemma 7.2.2, $i_0 = i_1 = n$. Thus i_1 is odd. Therefore, by Propostion 7.1.4, the Bertin obstruction of ϕ does not vanish. □

Corollary 7.2.4. *The group Q_8 is not an almost Bertin group for k.*

Proof. Let m be an odd positive integer. By Lemma 7.2.1 and Proposition 7.2.3, there is a Q_8-extension $\widetilde{K}$ of K such that

1. the first ramification break of $\widetilde{K}$ over K is m, and
2. the local Q_8-action corresponding to $\widetilde{K}$ over K has non-vanishing Bertin obstruction.

By Remark 2.1.4, the first enumerated statement is equivalent to the statement that $v_{\widetilde{K}}(\sigma(u) - u) \geq m$ for all $\sigma \in \mathrm{Gal}(\widetilde{K}|K)$, where u is a uniformizer of $\widetilde{K}$. Therefore, it is not the case that every sufficiently ramified local Q_8-action has vanishing Bertin obstruction. Thus Q_8 is not an almost Bertin group. □

7.2.2 $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$-Extensions

In this section, we shall use the Q_8-extensions from the previous section to construct local $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$-extensions that correspond to local $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$-actions with non-vanishing Bertin obstruction. To this end, let K, n, L_i, M, N, q_i, s be defined as in the previous section, let $w = t^3$, and let $K' = k((w))$. Then $K|K'$ is a Galois extension, and $\mathrm{Gal}(K|K') \cong \mathbb{Z}/3\mathbb{Z}$. Moreover, let $\sigma : N \to K^{\mathrm{alg}}$ be a k-linear embedding such that $\sigma|_K$ is the generator of $\mathrm{Gal}(K|K')$ mapping t to $\zeta_3 t$. Finally, for all $\ell \in \mathbb{Z}$, let ℓ' be the unique element of $\{0, 1, 2\}$ such that $\ell \equiv \ell' \pmod 3$.

Lemma 7.2.5. *Let $i \in \{0, 1, 2\}$. Then either $\sigma(q_i) = q_{(i-n)'}$ or $\sigma(q_i) = q_{(i-n)'} + 1$. In particular, the following statements both hold.*

(1) $\sigma(L_i) = L_{(i-n)'}$.

(2) *The extension $L_i|K'$ is Galois if and only if $3 \mid n$.*

Proof. Let $i \in \{0, 1, 2\}$. Since $\sigma(t) = \zeta_3 t$, it follows that

$$(\sigma(q_i))^2 + \sigma(q_i) = \sigma(\zeta_3^i t^{-n}) = \zeta_3^{i-n} t^{-n} = \zeta_3^{(i-n)'} t^{-n} = q_{(i-n)'}^2 + q_{(i-n)'}.$$

Therefore, either $\sigma(q_i) = q_{(i-n)'}$, or $\sigma(q_i) = q_{(i-n)'} + 1$. Hence $\sigma(L_i) = L_{(i-n)'}$.

To prove (2), note that, since $L_i|K$ is Galois, $L_i|K'$ is Galois if and only if $\sigma(L_i) = L_i$, which occurs if and only if $n' = 0$, *i.e.*, if and only if $3 \mid n$. □

Remark 7.2.6. Since $M|K$ has degree four, there are four extensions of $\sigma|_K$ to embeddings of M in K^{alg}. Since any such extension is completely determined by its action on q_0 and q_1, we may and do pick σ such that $\sigma(q_0) = q_{(-n)'}$, and $\sigma(q_1) = q_{(1-n)'}$. In this case, $\sigma(q_2) = q_{(2-n)'}$, as well.

Proposition 7.2.7. *The field N is a Galois extension of K'. Moreover, the following statements both hold.*

(1) *If $3 \mid n$, then* $\mathrm{Gal}(N|K') \cong Q_8 \times \mathbb{Z}/3\mathbb{Z}$.

(2) *If $3 \nmid n$, then* $\mathrm{Gal}(N|K') \cong \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$.

Proof. Note that $\sigma|_K$ generates $\mathrm{Gal}(K|K')$, and that $N|K$ is a Galois extension by Lemma 7.2.1. Therefore, to show that $N|K'$ is Galois, it suffices to show that $\sigma(N) = N$.

Recall that M is the compositum of L_0, L_1 and L_2. By Lemma 7.2.5, $\sigma(L_i) = L_{(i-n)'}$ for all $i \in \{0, 1, 2\}$. Hence

$$\sigma(M) = \sigma(L_0)\sigma(L_1)\sigma(L_2) = L_{(-n)'} L_{(1-n)'} L_{(2-n)'} = M.$$

Furthermore, since

$$s^2 + s = \zeta_3 t^{-n} q_0 + \zeta_3^2 t^{-n} q_1 + t^{-n} q_2 = \zeta_3 t^{-n} q_0 + \zeta_3^2 t^{-n} q_1 + \zeta_3^3 t^{-n} q_2,$$

it follows that

$$\begin{aligned}\sigma(s)^2+\sigma(s) &= \sigma(\zeta_3 t^{-n} q_0 + \zeta_3^2 t^{-n} q_1 + \zeta_3^3 t^{-n} q_2)\\ &= \zeta_3^{1-n} t^{-n} q_{(-n)'} + \zeta_3^{2-n} t^{-n} q_{(1-n)'} + \zeta_3^{3-n} t^{-n} q_{(2-n)'}\\ &= \zeta_3^{1+(-n)'} t^{-n} q_{(-n)'} + \zeta_3^{1+(1-n)'} t^{-n} q_{(1-n)'} + \zeta_3^{1+(2-n)'} t^{-n} q_{(2-n)'}\\ &= s^2+s,\end{aligned}$$

the second equality holding by Remark 7.2.6. Thus $\sigma(N)=N$, and $N|K'$ is Galois.

To prove statements (1) and (2), note that $\mathrm{Gal}(N|K)$ is a 2-Sylow subgroup of $\mathrm{Gal}(N|K')$, and recall that $K|K'$ is Galois. Thus $\mathrm{Gal}(N|K)$ is normal in $\mathrm{Gal}(N|K')$. Moreover, by Lemma 7.2.1, $\mathrm{Gal}(N|K)\cong Q_8$. Therefore, $\mathrm{Gal}(N|K')$ is a group of order twenty-four that contains a normal (and hence unique) 2-Sylow subgroup isomorphic to Q_8. Up to isomorphism, the only such groups are $Q_8\times\mathbb{Z}/3\mathbb{Z}$ and $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$.

To distinguish between the groups $Q_8\times\mathbb{Z}/3\mathbb{Z}$ and $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$, we consider the three order four subgroups of the 2-Sylow subgroup of $\mathrm{Gal}(N|K')$, that is, the subgroups $\mathrm{Gal}(N|L_i)$ for $i\in\{0,1,2\}$. If $\mathrm{Gal}(N|K')\cong Q_8\times\mathbb{Z}/3\mathbb{Z}$, then each of these subgroups will be normal in $\mathrm{Gal}(N|K')$, while if $\mathrm{Gal}(N|K')\cong\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$, then each of these subgroups will not be normal in $\mathrm{Gal}(N|K')$.

Let $i\in\{0,1,2\}$. By Lemma 7.2.5, $L_i|K'$ is a Galois extension if and only if $3\mid n$. Hence $\mathrm{Gal}(N|L_i)$ is normal in $\mathrm{Gal}(N|K')$ if and only if $3\mid n$. Statements (1) and (2) both now follow. □

Proposition 7.2.8. *Suppose that $3\nmid n$. Let u be a uniformizer of N, and let $\phi:\mathrm{Gal}(N|K')\to\mathrm{Aut}_k(k[[u]])$ be the local $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$-action corresponding to $N|K$. Then the Bertin obstruction of ϕ does not vanish.*

Proof. Note that, since $3\nmid n$, ϕ is indeed a local $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$-action by Proposition 7.2.7. Let $\phi_K:\mathrm{Gal}(N|K)\to\mathrm{Aut}_k(k[[u]])$ be the restriction of ϕ from $\mathrm{Gal}(N|K')$ to $\mathrm{Gal}(N|K)$. By 7.2.3, the Bertin obstruction of ϕ_K does not vanish. Therefore, by Theorem 5.1 in [CGH11], the Bertin obstruction of ϕ does not vanish. □

Corollary 7.2.9. *The group $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ is not an almost Bertin group for k.*

Proof. Let m be an odd positive integer. By Lemma 7.2.1 and Proposition 7.2.3, there is a $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$-extension $\widetilde{K}$ of K' such that

1. the first ramification break of the Q_8-extension $\widetilde{K}|K$ is m, and

2. the local $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$-action corresponding to $\widetilde{K}$ over K has non-vanishing Bertin obstruction.

By Remark 2.1.4, the first enumerated statement is equivalent to the statement that $v_{\widetilde{K}}(\sigma(u)-u)\geq m$ for all $\sigma\in\mathrm{Gal}(\widetilde{K}|K)$, where u is a uniformizer of $\widetilde{K}$. Since $\mathrm{Gal}(\widetilde{K}|K)$ is the unique 2-Sylow subgroup of $\mathrm{Gal}(\widetilde{K}|K')$, it follows that not every sufficiently ramified local $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$-action has vanishing Bertin obstruction. Therefore, $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ is not an almost Bertin group. □

Remark 7.2.10. The removal of $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ and Q_8 from the list of almost Bertin groups implies the following proposition.

Proposition 7.2.11. *Let G be a cyclic-by-p group, and let k be an algebraically closed field of characteristic p. Then the following statements are equivalent.*

(1) *G is a KGB group for k.*

(2) *G is a Bertin group for k.*

(3) *G is an almost KGB group for k.*

(4) *G is an almost Bertin group for k.*

Acknowledgement

The author thanks Andrew Obus, his doctoral advisor, for the latter's considerable assistance in guiding, at a multitude of points, both the direction of the work presented in this thesis, and the writing of the thesis itself.

Bibliography

[Ber98] José Bertin. Obstructions locales au relèvement de revêtements galoisiens de courbes lisses. *C. R. Acad. Sci. Paris Sér. I Math.*, 326(1):55–58, 1998.

[Bre08] Louis Hugo Brewis. Liftable D_4-covers. *Manuscripta Math.*, 126(3):293–313, 2008.

[BW06] Irene I. Bouw and Stefan Wewers. The local lifting problem for dihedral groups. *Duke Math. J.*, 134(3):421–452, 2006.

[BW09] Louis Hugo Brewis and Stefan Wewers. Artin characters, Hurwitz trees and the lifting problem. *Math. Ann.*, 345(3):711–730, 2009.

[CGH08] Ted Chinburg, Robert Guralnick, and David Harbater. Oort groups and lifting problems. *Compositio Math.*, 144(4):849–866, 2008.

[CGH11] Ted Chinburg, Robert Guralnick, and David Harbater. The local lifting problem for actions of finite groups on curves. *Ann. Sci. Éc. Norm. Supér. (4)*, 44(4):537–605, 2011.

[CGH17] Ted Chinburg, Robert Guralnick, and David Harbater. Global Oort groups. *J. Algebra*, 473:374–396, 2017.

[Gar96] Marco A. Garuti. Prolongement de revêtements galoisiens en géométrie rigide. *Compositio Math.*, 104(3):305–331, 1996.

[Gar02] Marco A. Garuti. Linear systems attached to cyclic inertia. In *Arithmetic fundamental groups and noncommutative algebra (Berkeley, CA, 1999)*, volume 70 of *Proc. Sympos. Pure Math.*, pages 377–386. Amer. Math. Soc., Providence, RI, 2002.

[GM98] Barry Green and Michel Matignon. Liftings of Galois covers of smooth curves. *Compositio Math.*, 113(3):237–272, 1998.

[GR71] Alexander Grothendieck and Michel Raynaud. *Revêtements étales et groupe fondamental*, volume 224 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, New York, 1971.

[Obu15] Andrew Obus. A generalization of the Oort Conjecture. *ArXiv e-prints*, February 2015. arxiv:1502.07623.

[Obu16] Andrew Obus. The local lifting problem for A_4. *Algebra Number Theory*, 10(8):1683–1693, 2016.

[Obu17] Andrew Obus. Lifting of curves with automorphisms. *ArXiv e-prints*, March 2017. arxiv:1703.01191.

[OW14] Andrew Obus and Stefan Wewers. Cyclic extensions and the local lifting problem. *Ann. of Math. (2)*, 180(1):233–284, 2014.

[Pag02] Guillaume Pagot. *Relèvement en caractéristique zèro d'actions de groupes abéliens de type* $(p, ..., p)$. PhD thesis, Université Bordeaux I, 2002.

[Pop14] Florian Pop. The Oort conjecture on lifting covers of curves. *Ann. of Math. (2)*, 180(1):285–322, 2014.

[Ray99] Michel Raynaud. Spécialisation des revêtements en caractéristique $p > 0$. *Ann. Sci. École Norm. Sup. (4)*, 32(1):87–126, 1999.

[Ser79] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1979. Translated from the French by Marvin Jay Greenberg.

[SOS89] Tsutomu Sekiguchi, Frans Oort, and Noriyuki Suwa. On the deformation of Artin-Schreier to Kummer. *Ann. Sci. École Norm. Sup. (4)*, 22(3):345–375, 1989.

[Wew99] Stefan Wewers. Deformation of tame admissible covers of curves. In *Aspects of Galois theory (Gainesville, FL, 1996)*, volume 256 of *London Math. Soc. Lecture Note Ser.*, pages 239–282. Cambridge Univ. Press, Cambridge, 1999.