ISSN 0012-9593

quatrième série - tome 44 *fascicule 4* *juillet-août 2011*

ANNALES SCIENTIFIQUES de L'ÉCOLE NORMALE SUPÉRIEURE

Ted CHINBURG & Robert GURALNICK & David HARBATER

The local lifting problem for actions of finite groups on curves

SOCIÉTÉ MATHÉMATIQUE DE FRANCE

Ann. Scient. Éc. Norm. Sup.
4 e série, t. 44, 2011, p. 537 à 605

THE LOCAL LIFTING PROBLEM FOR ACTIONS OF FINITE GROUPS ON CURVES

BY TED CHINBURG, ROBERT GURALNICK AND DAVID HARBATER

ABSTRACT. – Let k be an algebraically closed field of characteristic $p > 0$. We study obstructions to lifting to characteristic 0 the faithful continuous action ϕ of a finite group G on $k[[t]]$. To each such ϕ a theorem of Katz and Gabber associates an action of G on a smooth projective curve Y over k. We say that the KGB obstruction of ϕ vanishes if G acts on a smooth projective curve X in characteristic 0 in such a way that X/H and Y/H have the same genus for all subgroups $H \subset G$. We determine for which G the KGB obstruction of every ϕ vanishes. We also consider analogous problems in which one requires only that an obstruction to lifting ϕ due to Bertin vanishes for some ϕ, or for all sufficiently ramified ϕ. These results provide evidence for the strengthening of Oort's lifting conjecture which is discussed in [8, Conj. 1.2].

RÉSUMÉ. – Soit k un corps algébriquement clos de caractéristique $p > 0$. Nous étudions les obstructions au relèvement en caractéristique 0 d'une action fidèle et continue ϕ d'un groupe fini G sur $k[[t]]$. Le théorème de Katz-Gabber associe à ϕ une action du groupe G sur une courbe projective Y lisse sur k. La KGB-obstruction de ϕ est dite nulle si G agit sur une courbe projective lisse X de caractéristique 0 avec égalité des genres de X/H et Y/H pour tout sous-groupe $H \subset G$. Nous déterminons les groupes G pour lesquels la KGB-obstruction s'annule pour toute action ϕ. Nous considérons également des situations analogues pour lesquelles il suffit d'annuler l'obstruction de Bertin à relever une action ϕ ou toutes actions ϕ suffisamment ramifiées. Ces résultats renforcent les convictions en faveur de la conjecture de Oort généralisée aux relèvements d'une action fidèle sur une courbe projective lisse ([8], Conj. 1.2).

1. Introduction

This paper concerns the problem of lifting actions of finite groups on curves from positive characteristic to characteristic 0. Let k be an algebraically closed field of characteristic $p > 0$, and let Γ be a finite group acting faithfully on a smooth projective curve Y over k. We will say this action *lifts to characteristic* 0 if there is a complete discrete valuation ring R having

The authors were supported in part by NSF Grants DMS-0801030 and DMS-1100355, DMS-0653873 and DMS-1001962, DMS-0901164.

characteristic 0 and residue field k for which the following is true. There is an action of Γ on a smooth projective curve $\tilde{Y}$ over R for which there is a Γ-equivariant isomorphism between $k \otimes_R \tilde{Y}$ and Y.

We focus in this paper on the following local version of this problem. Let $\phi : G \to \mathrm{Aut}_k(k[[t]])$ be an injective homomorphism from a finite group G into the group of continuous automorphisms of the power series ring $k[[t]]$ over k. The existence of such a ϕ implies G is the semi-direct product of a cyclic group of order prime to p (the maximal tamely ramified quotient) by a normal p-subgroup (the wild inertia group). One says ϕ *lifts to characteristic* 0 if there is an R as above such that ϕ can be lifted to an embedding $\Phi : G \to \mathrm{Aut}_R(R[[t]])$ in the sense that $k \otimes_R \Phi = \phi$.

The local and global lifting problems are connected in the following way by a result of Bertin and Mézard [3]. For each wildly ramified closed point y of Y, fix an identification of the completion of the local ring of Y at y with $k[[t]]$, and let $\phi_y : \Gamma(y) \to \mathrm{Aut}_k(k[[t]])$ be the resulting action of the inertia group $\Gamma(y)$ of y on this completion. Then ϕ lifts to characteristic 0 if and only if each ϕ_y does.

In [8] we studied the global lifting problem. We defined Γ to be a (global) Oort group for k if every action of Γ on a smooth projective curve over k lifts to characteristic 0. This terminology arises from Oort's conjecture in [21, §I.7] that all cyclic groups Γ have this property, or equivalently that every connected cyclic cover lifts to characteristic 0. We showed in [8] that all groups Γ which are Oort groups for k must be on a certain list of finite groups that is recalled in Remark 1.4 below, and we conjectured this list was complete. Some results by various authors concerning Oort's conjecture and the generalization proposed in [8] are discussed after Remark 1.4 below.

In this paper we will focus on three local versions of the results in [8]. We will consider which finite groups G that are semi-direct products of a cyclic prime to p-group with a normal p-subgroup have the following properties for the field k.

1. If every local action $\phi : G \to \mathrm{Aut}_k(k[[t]])$ lifts to characteristic 0 we call G a *local Oort group for* k (as in [8]).
2. If every local action $\phi : G \to \mathrm{Aut}_k(k[[t]])$ that is sufficiently ramified lifts to characteristic 0, we will call G an *almost local Oort group for* k. More precisely, G is an almost local Oort group if there is an integer $N(G,k) \geq 0$ such that a local action ϕ lifts to characteristic 0 provided $t^{N(G,k)}$ divides $\phi(\sigma)(t) - t$ in $k[[t]]$ for all elements $\sigma \in G$ of p-power order.
3. If there is at least one local action $\phi : G \to \mathrm{Aut}_k(k[[t]])$ which lifts to characteristic 0 we will call G a *weak local Oort group for* k.

Our goal is to show that any G which has one of the three above properties must be on a certain list of groups associated to that property. In view of Oort's conjecture concerning cyclic groups we will ask to what extent these lists are complete.

The lists that we obtain will result from studying an obstruction to lifting ϕ that is due to Bertin [2], as well as from a refinement of this obstruction that we will call the KGB obstruction.

The *Bertin obstruction of* ϕ *vanishes* if there is a finite G-set S with non-trivial cyclic stabilizers such that the character χ_S of the action of G on S equals $-a_\phi$ on the non-trivial

elements of G, where a_ϕ is the Artin character associated to ϕ. (For the definition of a_ϕ see [28, Chap. VI].) The condition on χ_S is thus that

$$\chi_S = m \cdot \mathrm{reg}_G - a_\phi \tag{1.1}$$

for some integer m, where reg_G is the character of the regular representation of G.

We will say that *Katz-Gabber-Bertin obstruction of ϕ vanishes*, or simply that the *KGB obstruction of ϕ vanishes*, if the following is true. There is a field K of characteristic 0 and a G cover $X \to X/G = \mathbb{P}^1_K$ of smooth geometrically irreducible projective curves over K such that

$$\mathrm{genus}(X/H) = \mathrm{genus}(Y/H)$$

for all subgroups H of G, where $Y \to Y/G = \mathbb{P}^1_k$ is the G-cover of smooth projective curves associated to ϕ by a theorem of Katz and Gabber (see [16]). Up to isomorphism, the Katz-Gabber cover $Y \to Y/G = \mathbb{P}^1_k$ is characterized by the fact that this G-cover is totally ramified over one point $\infty \in \mathbb{P}^1_k$, at most tamely ramified over another point $0 \in \mathbb{P}^1_k$, unramified off of $\{\infty, 0\}$, and the action of G on the completion $\hat{\mathcal{O}}_{Y,x}$ of the local ring of Y at the unique point x over ∞ corresponds to ϕ via a continuous k-algebra isomorphism between $\hat{\mathcal{O}}_{Y,x}$ and $k[[t]]$.

We prove in Theorem 4.2 that the Bertin obstruction vanishes if the KGB obstruction vanishes. In Appendix 2 we show that the KGB obstruction for ϕ need not vanish when the Bertin obstruction of ϕ does.

DEFINITION 1.1. – Let G be a finite group which is the semi-direct product of a cyclic prime to p group by a normal p-subgroup. If the Bertin obstruction (resp. the KGB obstruction) vanishes for all ϕ then G will be called a *Bertin group* for k (resp. a *KGB group* for k). If this is true for all sufficiently ramified ϕ we call G an *almost Bertin group* for k (resp. an *almost KGB group* for k). Finally, if there is at least one ϕ for which the Bertin obstruction (resp. the KGB obstruction) vanishes, we will call G a *weak Bertin group* for k (resp. a *weak KGB group* for k).

Thus a local Oort group for k must be a KGB group for k, which must in turn be a Bertin group for k. One has a similar statement concerning almost local Oort groups and weak local Oort groups for k.

We can now state our main result concerning Bertin and KGB groups for k.

THEOREM 1.2. – *Suppose G is a finite group which is a semi-direct product of a normal p-subgroup with a cyclic group of order prime to p. Let k be an algebraically closed field of characteristic p. Then G is a KGB group for k if and only if it is a Bertin group for k, and this is true exactly when G is isomorphic to a group of one of the following kinds:*

1. *A cyclic group.*
2. *The dihedral group D_{2p^n} of order $2p^n$ for some $n \geq 1$.*
3. *A_4 when $p = 2$.*
4. *A generalized quaternion group Q_{2^m} of order 2^m for some $m \geq 4$ when $p = 2$.*

Note that if $p = 2$ and $n = 1$ in item (2), D_4 is simply $\mathbb{Z}/2 \times \mathbb{Z}/2$.

By considering particular covers we showed in [8, Thm. 3.3, 4.4] that if G is a local Oort group for k then it must either be on the list given in Theorem 1.2 or else $p = 2$ and G is a semi-dihedral group of order at least 16. Theorem 1.2 shows that in fact, semi-dihedral groups are not local Oort groups in characteristic 2. Note also that Theorem 1.2 provides a necessary and sufficient condition for a group to be a Bertin group, which is equivalent to being a KGB group. Theorem 3.3 of [8] concerns only necessary conditions which must be satisfied by local Oort groups.

There are examples of particular actions ϕ for which the Bertin obstruction to lifting vanishes but the KGB obstruction does not (see Example B.2). Thus the fact that the Bertin and KGB groups turn out to be the same has to do with the requirement that the associated obstructions vanish for *all* such ϕ.

Pagot has shown in [23, Thm. 3] (see also [18]) that there are ϕ which have vanishing Bertin and KGB obstructions but which nonetheless do not lift to characteristic 0. Thus the latter obstructions are not sufficient to determine whether ϕ has a lift.

In view of Theorem 1.2, we asked the following question:

QUESTION 1.3. – *Is the set of groups listed in items [1]–[4] of Theorem 1.2 the set of all local Oort groups for algebraically closed fields k of characteristic p?*

Brewis and Wewers [7] have announced a proof that the answer to this question is negative because the generalized quaternion group of order 16 is not a local Oort group in characteristic 2.

REMARK 1.4. – Suppose the groups of type (1), (2) and (3) in Theorem 1.2 are all local Oort groups. It would then follow from [8, Thm. 2.4, Cor. 3.4, Thm. 4.5] that a cyclic by p group Γ is a global Oort group for k if and only if Γ is either cyclic, dihedral of order $2p^n$ for some n or (if $p = 2$) the alternating group A_4. This implication is not dependent on determining which generalized quaternion groups are local Oort groups in characteristic 2.

Oort's conjecture in [26] that cyclic groups are local and global Oort groups was shown for cyclic groups having a p-Sylow subgroup of order p (resp. p^2) by Oort, Sekiguchi and Suwa [26] (resp. by Green and Matignon [12]). Pagot showed (see [23] and [18]) that when $p = 2$, the Klein four group D_4 is a local and global Oort group. Bouw and Wewers have shown [4] that for all odd p, the dihedral group D_{2p} is a local and global Oort group, and they have announced a proof that when $p = 2$, A_4 is a local and global Oort group. In [5], Bouw, Wewers and Zapponi establish necessary and sufficient conditions for a given ϕ to lift to characteristic 0 whenever the p-Sylow subgroup of G has order p, regardless of whether G is a local Oort group.

The following is our main result concerning almost KGB groups and almost Bertin groups for k.

THEOREM 1.5. – *Suppose G is a finite group which is the semi-direct product of a cyclic group of order prime to p by a normal p-subgroup. Then G is an almost KGB group for k if and only if it is an almost Bertin group for k. The list of these groups consists of those appearing in Theorem 1.2 together with the groups $\mathrm{SL}_2(\mathbb{Z}/3)$ and Q_8 when $p = 2$.*

In a similar vein to Question 1.3, we ask:

QUESTION 1.6. – *Is the set of groups described in Theorem 1.5 the set of almost local Oort groups for k?*

We now consider G which are weak Bertin groups, i.e. for which there is at least one injection $\phi : G \to \mathrm{Aut}_k(k[[t]])$ that has vanishing Bertin obstruction. We will give a purely group theoretic characterization of such G which requires no quantification over embeddings of G into $\mathrm{Aut}_k(k[[t]])$.

DEFINITION 1.7. – Let G be the semi-direct product of a normal p-group P by cyclic subgroup C of order prime to p. Let B be the maximal subgroup of C of order dividing $p-1$. We will call G a *Green-Matignon group for k*, or more briefly a *GM group for k*, if there is a faithful character $\Theta : B \to \mathbb{Z}_p^*$ for which the following is true:

a. If $1 \neq c \in C$, then $\mathrm{C}_P(c) = \mathrm{C}_P(C)$ and this group is cyclic.
b. Suppose T is a cyclic subgroup of P and that $\mathrm{C}_C(T)$ is trivial. Then

$$xyx^{-1} = y^{\Theta(x)}$$

for $y \in T$ and $x \in \mathrm{N}_B(T)$.

Note that if $|B| \leq 2$, Θ is unique and so condition (b) is vacuous. Clearly, cyclic groups and p-groups are GM-groups.

THEOREM 1.8. – *Let G be the semi-direct product of a normal p-group G by cyclic subgroup C of order prime to p. There is an injection $\phi : G \to \mathrm{Aut}_k(k[[t]])$ which has vanishing Bertin obstruction if and only if G is a GM group for k. Thus G is a weak Bertin group for k if and only if it is a GM group for k.*

This result generalizes a result of Green and Matignon in [12] which states that no ϕ can lift to characteristic 0 if G contains an abelian subgroup that is neither cyclic nor a p-group. In §10 we give some further examples and characterizations of GM groups. In particular, in Theorem 10.1(c)(ii-iv) we describe some groups which are not GM groups even though all of their abelian subgroups are either cyclic or p-groups.

Following Question 1.3, we ask:

QUESTION 1.9. – *Is the set of groups described in Theorem 1.8 the set of groups G for which some injection $\phi : G \to \mathrm{Aut}_k(k[[t]])$ lifts to characteristic 0, i.e. the set of weak local Oort groups for k?*

If the answer to this question is affirmative, then every p-group would be a weak local Oort group for k. Matignon has shown in [17] that every elementary abelian p-group is a weak local Oort group for k. Brewis has shown in [6] that when $p = 2$ the dihedral group of order 8 is a weak local Oort group for k. As one final instance of Question 1.3, it follows from work of Oort, Sekiguchi and Suwa and of Bouw, Wewers and Zapponi that the answer is affirmative if $\#G$ is exactly divisible by p; see Example 10.6.

We now discuss the organization of the paper.

In Proposition 2.1 of §2 we give a numerical reformulation of the Bertin obstruction of ϕ. We show this obstruction vanishes if and only if a constant $b_T(\phi) \in \mathbb{Q}$ associated

to each non-trivial cyclic subgroup T of G is non-negative and integral. The basis for this reformulation is Artin's Theorem that every character of G with rational values is a unique rational linear combination of the characters of G-sets of the form G/T as T ranges over a set of representatives for the conjugacy classes of cyclic subgroups of G. In §3 we compute the constants $b_T(\phi)$ when T contains a non-trivial element of order prime to p.

In §4 we give an alternate characterization of the vanishing of the KGB obstruction which shows that if it vanishes, then the Bertin obstruction vanishes.

In §5 we consider the functorial properties of the Bertin and KGB obstructions on passage to subgroups and quotient groups. We show that the vanishing of the Bertin (resp. KGB) obstruction for $\phi : G \to \mathrm{Aut}_k(k[[t]])$ implies that the corresponding obstruction vanishes for the injection $\phi^\Gamma : \Gamma \to \mathrm{Aut}_k(k[[t]]^N)$ associated to the quotient Γ of G by a normal subgroup N. The vanishing of the Bertin obstruction of ϕ implies that the Bertin obstruction of the restriction $\phi|_H$ of ϕ to any subgroup H of G also vanishes.

One consequence of §5 is that if the Bertin obstruction of ϕ vanishes, then that of the restriction $\phi|_P$ vanishes when P is the (normal) p-Sylow subgroup of G. In §6 we sharpen this statement by showing that the Bertin obstruction of ϕ vanishes if and only if that of $\phi|_P$ vanishes and G and a_ϕ satisfy some further conditions (see Theorem 6.6). The extra conditions are purely group theoretic except for one (condition c(ii) of Theorem 6.6) on the numerical size of the wild ramification associated to ϕ. This reduction to p-groups is central to the proof of Theorem 1.8. The proof of Theorem 6.6 is carried out in §8, using results from §3, §7 and §8. We prove Theorem 1.8 in §9. In §10 we give some examples and alternate group theoretic characterizations of GM groups.

To prove Theorems 1.2 and 1.5 we must introduce some further ideas. Our strategy is to exploit the fact that any quotient of a Bertin group must be a Bertin group (and similarly for almost Bertin groups). One can thus eliminate G from the list of Bertin groups by showing it has a quotient that is not Bertin. In §11 we recall from [8] some purely group theoretic results which show that if G is not on a small list of groups then it must have a quotient which is on a second list of groups. We then work to show that every element of the second list is not a Bertin group, while every element on the first list is a KGB group (and thus also a Bertin group).

The above strategy for proving Theorems 1.2 and 1.5 is carried out in the following way. In §12 various groups are shown not to be almost Bertin. To use local class field theory we show in §13 that we can allow k to be quasi-finite in the sense of [28, §XIII.2] rather than algebraically closed. In §14, §15 and §16 we analyze the case of dihedral groups for all p, quaternionic and semi-dihedral groups when $p = 2$ and the group $\mathrm{SL}_2(3)$ when $p = 2$. These results provide a new proof in Corollary 15.7 of a result of J-P. Serre [27, §5] and J.-M. Fontaine [9] concerning local Artin representations associated to generalized quaternion groups which are not realizable over $\mathbb{Q}$. The proofs of Theorems 1.2 and 1.5 are completed in §17 and §18 using results from Appendix 1. In Appendix 1 we prove a technical result which constructs solutions to certain embedding problems with p-group kernels such that the Artin character of the solution has large values on non-trivial elements of the kernel as well as further congruence properties. To keep the details of the construction from obscuring the arguments in the main theorems we put them in Appendix 1.

This is the second in a series of papers concerning lifting problems. In a later paper we will study the implications of Theorem 1.2 to the structure of the global Oort groups considered in [8].

Acknowledgments

We would like to thank J. Bertin, I. Bouw, O. Gabber, M. Matignon, A. Mézard, F. Oort, F. Pop and S. Wewers for useful conversations. We would also like to thank the referee for helpful suggestions.

2. The Bertin obstruction

Let k be an algebraically closed field of characteristic p. Suppose G is a finite group, and let $\phi : G \to \mathrm{Aut}_k(k[[t]])$ be an embedding. Let $\mathscr{C}$ be a set of representatives for the conjugacy classes of cyclic subgroups of G. For each subgroup H of G, let 1_H be the one-dimensional trivial character of H, and let $1_H^G = \mathrm{Ind}_H^G 1_H$ be the induction of 1_H from H to G.

PROPOSITION 2.1. – *Let a_ϕ be the Artin character of ϕ.*

i. *There are unique rational numbers $b_T = b_T(\phi)$ for $T \in \mathscr{C}$ such that*

$$-a_\phi = \sum_{T \in \mathscr{C}} b_T \, 1_T^G. \tag{2.1}$$

ii. *The following conditions are equivalent:*
   a. *The Bertin obstruction of ϕ vanishes.*
   b. *One has $0 \le b_T \in \mathbb{Z}$ for all $T \in \mathscr{C}$ such that $T \neq \{e\}$.*

iii *Suppose the conditions in part (ii) hold. Let S be the G-set whose character appears in the definition of the vanishing of the Bertin obstruction in (1.1). Then $m = -b_{\{e\}} \ge 0$ in (1.1), and there is an isomorphism of G-sets*

$$S \cong \coprod_{\{e\} \neq T \in \mathscr{C}} \coprod_{i=1}^{b_T} (G/T). \tag{2.2}$$

Proof. – We first prove (i). By Artin's Theorem [29, Thm. 13.30, Cor. 13.1], every character of G with rational values is a $\mathbb{Q}$-linear combination of the characters $\{1_T^G : T \in \mathscr{C}\}$, and the dimension over $\mathbb{Q}$ of the space of all $\mathbb{Q}$-valued characters is $\#\mathscr{C}$. Since the character $-a_\phi$ takes rational values, we conclude that (2.1) holds for a unique function $T \mapsto b_T$ from $\mathscr{C}$ to $\mathbb{Q}$.

We now prove (ii). Suppose statement (a) in part (ii) holds. By considering the G-orbits of elements of S, we see that there is a G-set isomorphism

$$S \cong \coprod_{\{e\} \neq T \in \mathscr{C}} \coprod_{i=1}^{n_T} G/T \tag{2.3}$$

for some integers $n_T \ge 0$. By (1.1) one has

$$m \, \mathrm{reg}_G - a_\phi = \chi_S = \sum_{\{e\} \neq T \in \mathscr{C}} n_T \, 1_T^G. \tag{2.4}$$

Hence

$$-a_\phi = -m\,\mathrm{reg}_G + \sum_{\{e\}\neq T\in\mathscr{C}} n_T\,1_T^G \tag{2.5}$$

where $\mathrm{reg}_G = 1_{\{e\}}^G$. So by the uniqueness of the rational numbers b_T in (2.1), we conclude that $m = -b_{\{e\}}$ and $n_T = b_T$ for $\{e\} \neq T \in \mathscr{C}$. Thus statement (b) in part (ii) holds since $0 \leq n_T \in \mathbb{Z}$ if $T \neq \{e\}$.

Suppose now that condition (b) of part (ii) holds. Define

$$S = \coprod_{\{e\}\neq T\in\mathscr{C}} \coprod_{i=1}^{b_T} (G/T) \tag{2.6}$$

where $b_T \geq 0$ for the T appearing in this coproduct. The stabilizers of elements of S are then conjugates of those T for which $b_T > 0$, so they are non-trivial cyclic subgroups. By (2.1) we have

$$\chi_S = \sum_{\{e\}\neq T\in\mathscr{C}} b_T\,1_T^G = -b_{\{e\}}\mathrm{reg}_G - a_\phi. \tag{2.7}$$

Therefore condition (a) of part (ii) holds.

It remains to show part (iii) of Proposition 2.1, so we assume that the conditions in part (ii) hold. The inner product $\langle a_\phi, \chi_0\rangle$ of a_ϕ with the one-dimensional trivial representation χ_0 of G is 0 by [28, §VI.2]. Hence (1.1) gives $m = \langle \chi_S, \chi_0\rangle / \langle \mathrm{reg}_G, \chi_0\rangle \geq 0$. It will now suffice to show that (2.6) defines up to isomorphism the unique G-set S with non-trivial cyclic stabilizers for which condition (a) of part (ii) holds. Since condition (a) of part (ii) determines the character of S up to an integral multiple of $1_{\{e\}}^G$, this is a consequence of the fact that the characters $\{1_T^G : T \in \mathscr{C}\}$ are linearly independent over $\mathbb{Q}$ by Artin's Theorem. □

We now develop some formulas for the constant b_T appearing in (2.1).

NOTATION 2.2. – Since k is algebraically closed, $G = G_0$ is the inertia group of G as an automorphism group of $k[[t]]$. Let G_i be the i^{th} ramification subgroup of G in the lower numbering. For all non-trivial subgroups Γ of G, let $\iota(\Gamma) = i + 1$ when i is the largest non-negative integer for which $\Gamma \subset G_i$. Let μ be the Möbius function, and let $\mathrm{N}_G(T)$ be the normalizer of a subgroup T in G. Let $S(T) = S_G(T)$ be the set of all non-trivial cyclic subgroups Γ of G which contain T. If T' is also a subgroup of G, let $\delta(T, T') = 1$ if $T = T'$ and let $\delta(T, T') = 0$ if $T \neq T'$.

THEOREM 2.3. – *For $T \in \mathscr{C}$ the constant b_T appearing in (2.1) is given by*

$$b_T = \frac{1}{[\mathrm{N}_G(T) : T]} \left(-\delta(T, \{e\})a_\phi(e) + \sum_{\Gamma\in S(T)} \mu([\Gamma : T])\iota(\Gamma) \right). \tag{2.8}$$

Proof. – If Γ is a non-trivial cyclic group with generator γ, then $\iota(\Gamma) = -a_\phi(\gamma)$. Since there are $[G : \mathrm{N}_G(T)]$ conjugates of a given cyclic group T, formula (2.8) results from applying the explicit Artin induction theorem proved by Snaith in [31, Thm. 2.1.3] to the rational valued character $-a_\phi$. □

3. Constants associated to cyclic subgroups which are not p-groups

In this section we analyze the constants $b_T = b_T(\phi)$ when T is not a p-group. This is needed to relate the KGB obstruction to the Bertin obstruction in the next section.

DEFINITION 3.1. – If H is a cyclic subgroup of a finite group J, define

$$\psi(H, J) = \sum_{H \subset \overline{\Gamma} \subset J,\ \overline{\Gamma} \text{ cyclic}} \mu([\overline{\Gamma} : H]).$$

PROPOSITION 3.2. – *Suppose T is a cyclic subgroup of G that contains a non-trivial element of order prime to p. Then b_T is integral if and only if one of the following alternatives occurs:*

a. $\mathrm{N}_G(T) = T$. *Then* $b_T = 1$.
b. *One has* $\psi(T, \mathrm{C}_G(T)) = 0$. *Then* $b_T = 0$.

If T has order prime to p, then (b) is equivalent to

b′. $\psi(\{e\}, \mathrm{C}_G(T)/T) = 0$.

Proof. – Let $\pi : \mathrm{C}_G(T) \to J = \mathrm{C}_G(T)/T$ be the quotient homomorphism. Recall from Notation 2.2 that $S_G(T)$ is the set of all non-trivial cyclic subgroups of G which contain T. We will first show that there is an injection

$$f : S_G(T) \to S_J(\{e\}) \cup \{\{e\}\} \quad \text{defined by} \quad f(\Gamma) = \pi(\Gamma). \tag{3.1}$$

which is a bijection if T has order prime to p. Clearly f is well defined, and since $\Gamma = \pi^{-1}(\pi(\Gamma))$, f is injective. Suppose T has order prime to p and $\overline{\Gamma}$ is a cyclic subgroup of J. It will suffice to show $\pi^{-1}(\overline{\Gamma})$ is cyclic, since then $\pi^{-1}(\overline{\Gamma}) \in S(T)$ because T is non-trivial. Since $\pi^{-1}(\overline{\Gamma})$ is an extension of the cyclic group $\overline{\Gamma}$ by the cyclic subgroup group T, $\pi^{-1}(\overline{\Gamma})$ is nilpotent. So it will suffice to show $\pi^{-1}(\overline{\Gamma})$ has cyclic Sylow subgroups. The Sylow subgroups of $\pi^{-1}(\overline{\Gamma})$ associated to primes $\ell \neq p$ are cyclic since G has cyclic Sylow subgroups at such ℓ. When $\ell = p$, the p-Sylow subgroup of $\pi^{-1}(\overline{\Gamma})$ maps isomorphically to that of $\overline{\Gamma}$ since T has order prime to p, so this group is cyclic because $\overline{\Gamma}$ is cyclic. This completes the proof that (3.1) is a bijection if T has order prime to p.

We now return to arbitrary cyclic T which contain a non-trivial element of order prime to p. Each $\Gamma \in S_G(T)$ contains a non-trivial element of order prime to p, so $\iota(\Gamma) = 1$. Theorem 2.3 gives

$$b_T = \frac{1}{[\mathrm{N}_G(T) : T]} \sum_{\Gamma \in S_G(T)} \mu([\Gamma : T])\iota(\Gamma) = \frac{1}{[\mathrm{N}_G(T) : T]} \sum_{\Gamma \in S_G(T)} \mu([\Gamma : T]). \tag{3.2}$$

Using the injection (3.1) we have

$$b_T = \frac{1}{[\mathrm{N}_G(T) : \mathrm{C}_G(T)]} \cdot \frac{1}{\#J} \sum_{\overline{\Gamma} \in f(S_G(T))} \mu(\#\overline{\Gamma}) \tag{3.3}$$

where $J = \mathrm{C}_G(T)/T$. Thus if $b_T \in \mathbb{Z}$, we have to have

$$\sum_{\overline{\Gamma} \in f(S_G(T))} \mu(\#\overline{\Gamma}) \equiv 0 \mod [\mathrm{N}_G(T) : \mathrm{C}_G(T)] \cdot \#J. \tag{3.4}$$

Let $\phi(z)$ be the value of the Euler phi function on an integer z. If $\overline{\Gamma}$ is a cyclic subgroup of J, there are exactly $\phi(\#\overline{\Gamma})$ generators for $\overline{\Gamma}$, each of which has order $\#\overline{\Gamma}$. This leads to the inequality

$$\sum_{\overline{\Gamma}\in f(S(T))} \mu(\#\overline{\Gamma}) \leq \sum_{\overline{\Gamma}\subset J,\ \overline{\Gamma}\ \text{cyclic}} 1 = \sum_{g\in J} \frac{1}{\phi(\mathrm{ord}(g))}. \tag{3.5}$$

The sum on the right is bounded by $\#J$, and is less than $\#J$ unless J is the trivial group. We conclude that the congruence (3.4) holds if and only if either $\mathrm{N}_G(T) = \mathrm{C}_G(T) = T$ and $b_T = 1$ or the sum on the left in (3.4) is 0, in which case $b_T = 0$. In the latter case, the elements Γ of $S_G(T)$ are exactly the cyclic subgroups $\Gamma \subset \mathrm{C}_G(T)$ containing T, which leads to condition (b) in Proposition 3.2 via (3.2). Conversely, if either condition (a) or (b) holds, then b_T is integral by (3.2). Finally, if T has order prime to p, then (b) is equivalent to (b') because we have shown that the map f in (3.1) is bijective. □

In view of Corollary 5.5 we have:

COROLLARY 3.3. – *Suppose J is a subquotient of G with the following property. There is a cyclic subgroup T of J which contains a non-trivial element of order prime to p such that $\mathrm{N}_J(T) \neq T$ and $\psi(T, \mathrm{C}_J(T)) \neq 0$. (If T has order prime to p, the second condition is equivalent to $\psi(\{e\}, \mathrm{C}_J(T)/T) \neq 0$.) Then $b_{T,J}$ is not integral. In particular, G is not a weak Bertin group in characteristic p, i.e. no local G-cover in characteristic p has vanishing Bertin obstruction. As a result, no such cover can be lifted to characteristic* 0.

COROLLARY 3.4 (Green [11, Prop. 3.3 and 3.4], Green–Matignon [12])
Suppose that the center $\mathrm{C}(G)$ of G is neither cyclic nor a p-group. Then there is a subquotient J of G and a non-trivial cyclic subgroup T of J of order prime to p such that $b_{T,J}$ is not integral. Thus G is not a weak Bertin group.

Proof. – If $\mathrm{C}(G)$ is neither cyclic nor a p-group, then there is a subquotient J of G which is the product of a non-trivial cyclic group T of order prime to p with an elementary abelian p-group $E = C_p^2$ of rank 2. Then $J = \mathrm{N}_J(T) = \mathrm{C}_J(T) \neq T$, and $\psi(T, \mathrm{C}_J(T)) = \psi(\{e\}, \mathrm{C}_J(T)/T) = \psi(\{e\}, E) = 1 + (p+1)\mu(p) = -p \neq 0$. Thus Corollary 3.3 shows that $b_{T,J}$ is not integral, which completes the proof. □

4. The Katz-Gabber-Bertin obstruction

As in §2 we suppose in this section that k is an algebraically closed field of characteristic p, that G is a finite group, and that $\phi : G \to \mathrm{Aut}_k(k[[t]])$ is an embedding. Let $\tilde{\phi} : G \to \mathrm{Aut}_k(Y)$ be the action of G on the Katz-Gabber cover $Y \to Y/G = \mathbb{P}^1_k$ associated to ϕ, whose properties were recalled in the introduction. Let a_ϕ be the Artin character of G associated to ϕ.

Recall from the introduction that the KGB obstruction of ϕ vanishes if there is a field K of characteristic 0 and a G cover $X \to X/G = \mathbb{P}^1_K$ of smooth geometrically irreducible projective curves over K such that $\mathrm{genus}(X/H) = \mathrm{genus}(Y/H)$ for all subgroups H of G.

THEOREM 4.1. – *If the embedding $\phi : G \to \mathrm{Aut}_k(k[[t]])$ lifts to characteristic* 0*, then the KGB obstruction vanishes.*

Proof. – By the local-global principle for lifting G-covers proved by Bertin and Mézard in [3, Cor. 3.3.5] (see also [8, Cor. 2.3]), there is a lifting of ϕ to characteristic 0 if and only if there is a lifting of $\tilde{\phi} : G \to \mathrm{Aut}_k(Y)$ to characteristic 0. Suppose such a lift exists. Thus there is a complete discrete valuation ring R having characteristic 0 and residue field k and an action of G on a smooth projective curve $\mathcal{X}$ over R with the following property. There is an isomorphism of the special fiber $k \otimes_R \mathcal{X}$ of $\mathcal{X}$ with Y which carries the action of G on $k \otimes_R \mathcal{X}$ to the action of G on Y specified by $\tilde{\phi}$.

Let K be the fraction field of R, and let $X = K \otimes_R \mathcal{X}$. Since $\mathcal{X}$ is smooth over R, flat base change implies $\mathrm{genus}(X/H) = \mathrm{genus}(Y/H)$ for all subgroups H of G. By formal smoothness (cf. [20, Remark I.3.22] and [14, 17.1.1, 17.5.1]), each of X and X/G has a point with residue field K because k is algebraically closed and $\mathcal{X}$ lifts Y. Therefore X is geometrically irreducible and X/G is isomorphic to $\mathbb{P}^1_K$, so the KGB obstruction of ϕ vanishes. □

THEOREM 4.2. – *The KGB obstruction vanishes if and only if there is a finite G-set S for which the following is true:*

a. *The stabilizer of each element of S is a non-trivial cyclic subgroup of G, and the character of the action of G on S is*

$$\chi_S = m \cdot \mathrm{reg}_G - a_\phi \tag{4.1}$$

for some integer m.

b. *There is a set of representatives Ω for the G-orbits in S and a subset $\{g_t\}_{t\in\Omega} \subset G$ such that g_t generates the stabilizer $G_t \neq \{e\}$ of t in G, $\{g_t\}_{t\in\Omega}$ generates G, and the order of $\prod_{t\in\Omega} g_t$ is the index $[G : G_1]$ in G of the wild inertia subgroup G_1.*

In particular, the vanishing of the KGB obstruction implies the vanishing of the Bertin obstruction, and both of these obstructions vanish if ϕ lifts to characteristic 0.

Proof. – Suppose first that the KGB obstruction vanishes, so that there is a G-cover $X \to X/G = \mathbb{P}^1_K$ of smooth geometrically irreducible curves over a field K of characteristic 0 such that

$$\mathrm{genus}(X/H) = \mathrm{genus}(Y/H) \tag{4.2}$$

for all subgroups H of G. By making a base change from K to an algebraic closure of K, we can assume that K is algebraically closed. For each point q of $X/G = \mathbb{P}^1_K$ let $x(q)$ be a point of X over q. The inertia group $I_{x(q)} \subset G$ is cyclic and equal to the decomposition group of q since K is algebraically closed of characteristic 0. Consider the character function

$$f_X = \sum_{q\in X/G} \mathrm{Ind}^G_{I_{x(q)}} a_{x(q)} = \sum_{q\in X/G} (1^G_{\{e\}} - 1^G_{I_{x(q)}}) \tag{4.3}$$

where $a_{x(q)} = 1^{I_{x(q)}}_{\{e\}} - 1_{I_{x(q)}}$ is the Artin character of the action of $I_{x(q)}$ on $\hat{O}_{X,x(q)}$. Let H be a subgroup of G. Then by the calculation of relative discriminants in [28, §3] we have

$$2 \cdot \mathrm{genus}(X) - 2 - \#H \cdot (2 \cdot \mathrm{genus}(X/H) - 2) = \langle f_X, 1^G_H \rangle \tag{4.4}$$

where $\langle\ ,\ \rangle$ is the usual inner product on characters. We now apply the same reasoning to the Katz-Gabber cover $Y \to Y/G = \mathbb{P}^1_k$ associated to ϕ, which is totally ramified over $\infty \in \mathbb{P}^1_k$,

tamely ramified with cyclic inertia groups isomorphic to C over $0 \in \mathbb{P}^1_k$ and unramified over all other points of $\mathbb{P}^1_k$. Define

$$f_Y = a_\phi + \delta_C \cdot (1^G_{\{e\}} - 1^G_C) \tag{4.5}$$

where the Artin character a_ϕ is the one associated to the action of G on the unique point of Y over ∞ and $\delta_C = 0$ (resp. $\delta = 1$) if C is trivial (resp. non-trivial). Then

$$2 \cdot \mathrm{genus}(Y) - 2 - \#H \cdot (2 \cdot \mathrm{genus}(X/H) - 2) = \langle f_Y, 1^G_H \rangle \tag{4.6}$$

for all subgroups H of G.

We conclude from (4.2), (4.4) and (4.6) that $\langle f_X, 1^G_H \rangle = \langle f_Y, 1^G_H \rangle$ for all H. Since f_X and f_Y take rational values and the characters of the form 1^G_H generate the $\mathbb{Q}$-vector space of rational valued characters, this implies that

$$\sum_{q \in X/G} (1^G_{\{e\}} - 1^G_{I_{x(q)}}) = f_X = f_Y = a_\phi + \delta_C \cdot (1^G_{\{e\}} - 1^G_C). \tag{4.7}$$

We now rewrite this equation using the formula for $-a_\phi$ in part (i) of Proposition 2.1. We can assume C is included in the set $\mathscr{C}$ of representatives for the cyclic subgroups of G. From (4.7) we have

$$\delta_C \cdot 1^G_C + \sum_{T \in \mathscr{C}} b_T 1^G_T = \delta_C \cdot 1^G_C - a_\phi = \sum_{q \in X/G} 1^G_{I_{x(q)}} - m \cdot 1^G_{\{e\}} = \chi_{S'} - m \cdot 1^G_{\{e\}} \tag{4.8}$$

for some integer m, where S' is the set of points of X which ramify over X/G, and the stabilizer in G of each element of S' is cyclic and non-trivial.

The uniqueness of the values of the b_T was proved in Proposition 2.1(i). Hence (4.8) shows that $\delta_C + b_C$ is the number of $q \in X/G$ such that $I_{x(q)}$ is a conjugate of C. This implies b_C is integral. Thus if C is non-trivial, Proposition 3.2 of §3 shows that $b_C \geq 0$. Since $\delta_C = 1$ if C is non-trivial, we conclude in this case that there is a point $q_0 \in X/G$ such that $I_{x(q_0)}$ is a conjugate of C. We now define S to be the complement of the G-orbit of $x(q_0)$ in S if C is non-trivial, and we let $S = S'$ if C is trivial. The uniqueness of the b_T in (4.8) now implies

$$-a_\phi = \chi_S - m \cdot r_G$$

where $r_G = 1^G_{\{e\}}$ is the regular representation of G. Since the elements of S have non-trivial cyclic stabilizers in G, S has the properties in part (a) of Theorem 4.2.

By the classical description of the fundamental group of $\mathbb{P}^1_K - Z$ (see [13, Chap. XIII, Thm. 2.12]), we can find a set Ω' of representatives for the G-orbits in S' and a generator g_t of the inertia group of each $t \in \Omega'$ such that $\prod_{t \in \Omega'} g_t = e$ is the identity of G and $\{g_t\}_{t \in \Omega'}$ generates G. Letting $\Omega = \Omega' \cap S$ shows $\prod_{t \in \Omega} g_t$ is either trivial if C is trivial or is a generator of a conjugate of the cyclic group $I_{x(q_0)}$ of order $\#C$ if C is non-trivial. This proves that S has all properties stated in Theorem 4.2.

Conversely, suppose that we have an S with the properties stated in Proposition 2.1. Let K be an algebraically closed field of characteristic 0. By reversing the above steps, we can construct a G-cover $X \to \mathbb{P}^1_K$ of smooth irreducible curves for which (4.7) holds. Now (4.3) and (4.5) establish (4.2) for all H.

The vanishing of the Bertin obstruction is equivalent, by definition, to condition (a) of Theorem 4.2. So the Bertin obstruction vanishes if the KGB obstruction does. Both obstructions vanish if ϕ lifts to characteristic 0 by Theorem 4.1. □

REMARK 4.3. – Using [28, §3], the vanishing KGB obstruction can also be formulated in the following way. There is a G-cover of smooth geometrically irreducible projective curves $X \to X/G$ such that for all primes ℓ different from the characteristic of k, the ℓ-adic Tate modules of X and of Y are G-isomorphic, where $Y \to Y/G$ is as before the Katz-Gabber cover associated to ϕ. We will not need this interpretation in what follows.

5. Functorality

Suppose $\phi : G \to \mathrm{Aut}_k(k[[t]])$ as in §4 is given. Let N be a normal subgroup of G, and let $\Gamma = G/N$. Define $\phi^\Gamma : \Gamma \to \mathrm{Aut}_k(k[[t]]^N)$ by $\phi^\Gamma(\gamma) = \phi(g)$ if $g \in G$ has image $\gamma \in \Gamma$. Since $k[[t]]^N$ is a complete discrete valuation ring with residue field k, it is isomorphic to $k[[z]]$ for some $z \in k[[t]]^N$ by [28, Prop. II.5]. If H is an arbitrary subgroup of G, define $\phi_H : H \to \mathrm{Aut}_k(k[[t]])$ to be the restriction of ϕ from G to H.

THEOREM 5.1. – *If the Bertin obstruction (resp. the KGB obstruction) vanishes for ϕ, then the same is true of ϕ^Γ. If the Bertin obstruction of ϕ vanishes, then it does for ϕ_H.*

To prove this result we need a lemma concerning characters χ of G. Define a character $\chi^\sharp$ of $\Gamma = G/N$ by

$$\chi^\sharp(\gamma) = \frac{1}{\#N} \sum_{g \in G,\ q(g)=\gamma} \chi(g) \tag{5.1}$$

where $q : G \to G/N$ is the quotient map. By [28, Prop. VI.3],

$$a_{\phi^\Gamma} = (a_\phi)^\sharp. \tag{5.2}$$

The next result follows directly from Frobenius reciprocity [29, Thm. 13, Chap. 7].

LEMMA 5.2. – *If S is a left G-set, let $N\backslash S$ be the G/N set formed by the orbits Ns of elements $s \in S$ under the left action of N. Let χ_S (resp. $\chi_{N\backslash S}$) be the character of the permutation representation of G (resp. G/N) defined by S (resp. $N\backslash S$). Then*

$$\chi_{N\backslash S} = \chi_S^\sharp. \tag{5.3}$$

Proof of Theorem 5.1. – Suppose that the Bertin obstruction vanishes for ϕ, and that S is as in Proposition 2.1(ii)(a). Let S'' be the G/N set $N\backslash S$. Let S''_0 be the set of the elements of S'' which have trivial stabilizer, and let S' be the complement $S'' - S''_0$. The stabilizers in G/N of the elements of S' are then non-trivial, and these are cyclic because they are the images in G/N of the cyclic stabilizers of elements of S. By hypothesis,

$$\chi_S = m \cdot \mathrm{reg}_G - a_\phi \tag{5.4}$$

for some integer m. By (5.3) and (5.2), one has

$$\chi_{S''} = \chi_S^\sharp = m \cdot (\mathrm{reg}_G)^\sharp - a_\phi^\sharp = m \cdot (\mathrm{reg}_{G/N}) - a_{\phi^\Gamma}.$$

Since $\chi_{S''}$ and $\chi_{S'}$ differ by an integer multiple of the character of the regular representation of G/N, we conclude that

$$\chi_{S'} = m' \cdot (\mathrm{reg}_{G/N}) - a_{\phi^\Gamma} \tag{5.5}$$

for some integer m', so S' satisfies condition (ii)(a) of Proposition 2.1 for ϕ^Γ.

Suppose now that the KGB obstruction vanishes for ϕ. Let S, Ω and $\{g_t : t \in \Omega\}$ be as in Theorem 4.2. By hypothesis, Ω is a set of representatives for the G orbits in S, $\{g_t\}_{t\in\Omega}$ is a subset of G such that g_t generates the stabilizer $G_t \neq \{e\}$ of t in G, $\{g_t\}_{t\in\Omega}$ generates G, and $\prod_{t\in\Omega} g_t$ has order $[G : G_1]$.

Let $t' = Nt$ be the image of $t \in \Omega$ in $S'' = N\backslash S$. One has $G_t \subset N$ if and only if the stabilizer $G_{t'}$ is trivial; this is true if and only if $t' \in S''_0$. Define

$$\Omega' = \{t' = Nt : t \in \Omega, t' \notin S''_0\}.$$

Now Ω' is a set of representatives for the G/N orbits in S', and for $t' \in \Omega'$ the image $g_{t'}$ of g_t in G/N is non-trivial and generates the stabilizer of t' in G/N. By hypothesis, $\{g_t : t \in \Omega\}$ generates G and $\prod\{g_t : t \in \Omega\}$ has order $[G : G_1]$. The image of g_t in G/N is non-trivial if and only if $t' = Nt \notin S''_0$, so we conclude that $\{g_{t'} : t' \in \Omega\}$ generates G/N, and the image of $\gamma = \prod\{g_t : t \in \Omega\}$ in G/N is $\gamma' = \prod\{g_{t'} : t' \in \Omega'\}$. Thus γ' has order $[G/N : G_1N/N]$. Here G_1N/N is the p-Sylow subgroup of G/N, so Ω' and $\{g_{t'} : t' \in \Omega'\}$ satisfy condition (b) of Theorem 4.2.

We now have to show that if the Bertin obstruction of ϕ vanishes, then it does for ϕ_H for all subgroups H of G. Since the residue field k is algebraically closed, [28, Prop. VI.4] shows

$$\operatorname{res}^H_G a_\phi = \lambda \cdot \operatorname{reg}_H + a_{\phi_H} \tag{5.6}$$

where λ is the valuation in $k((t))^H$ of the discriminant of $k((t))$ over $k((t))^H$. This implies that if S is a G-set satisfying condition (ii)(a) of Proposition 2.1 for ϕ, then the restriction of S to H satisfies this condition for ϕ_H. This completes the proof of Theorem 5.1. □

REMARK 5.3. – In a later paper we will show that the KGB obstruction for ϕ_H vanishes if that of ϕ vanishes; we will not need this result in this paper.

NOTATION 5.4. – Let J be a subquotient of G, i.e. a quotient of a subgroup H of G by a normal subgroup D of H. Suppose T is a cyclic subgroup of J. Define $b_{T,J} = b_{T,J}(\phi)$ to be the constant b_T appearing in Proposition 2.1 when G is replaced by J and ϕ is replaced by the induced injection $\phi_J : J \to \operatorname{Aut}_k(k[[t]]^D)$.

Combining Theorem 5.1 with Proposition 2.1 we obtain:

COROLLARY 5.5. – *Suppose the Bertin obstruction of ϕ vanishes. With the notations of Notation 5.4, one has $0 \leq b_{T,J} \in \mathbb{Z}$, for all non-trivial cyclic subgroups T of J.*

COROLLARY 5.6. – *Let G be a finite group, and suppose H is a quotient group of G.*

a. *If H is not a Bertin group (resp. almost Bertin group), then G is not a Bertin group (resp. almost Bertin group).*
b. *If G has a subquotient J which is not a weak Bertin group, then G is not a weak Bertin group.*

Proof. – In view of Theorem 5.1, part (a) is clear for Bertin groups, and to show part (a) for almost Bertin groups it will suffice to prove the following. Suppose that $\phi_H : H \to \operatorname{Aut}_k(k[[t]])$ is an injection with the property that the Artin character a_{ϕ_H} has the property that $-a_{\phi_H}(\tau) \geq M$ for some integer M and all non-trivial elements $\tau \in H$ of p-power order. It will be enough to show that there is an injection $\phi_G : G \to \operatorname{Aut}_k(k[[z]])$

inducing ϕ_H when we identify $k[[z]]^T$ with $k[[t]]$ when T is the kernel of the surjection $G \to H$, and for which $-\phi_G(\tau') \geq M$ for all non-trivial elements τ' of G of p-power order. This statement is a consequence of the parts (i) and (ii) of Proposition A.3(i) of Appendix 1. Part (b) of Corollary 5.6 follows directly from Theorem 5.1, which shows that if the Bertin obstruction of some injection $\phi : G \to \mathrm{Aut}_k(k[[t]])$ vanishes, then Bertin obstruction of the induced local J-cover would also have to vanish. □

REMARK 5.7. – Suppose H is a subgroup of G, and that H is not a Bertin group. In general this need not imply G is not a Bertin group, since it may not be possible to realize a local H-cover with non-zero Bertin obstruction as the restriction of a local G-cover. We will show later in Proposition 15.6 that this occurs, for example, when H is the quaternion group of order 8 and G is a generalized quaternion group of order at least 16.

6. The reduction to p-groups

Throughout this section we suppose given an injection $\phi : G \to \mathrm{Aut}_k(k[[t]])$ as in §4.

By Theorem 5.1, if the Bertin obstruction of ϕ vanishes, then so does the Bertin obstruction of the restriction ϕ_P of ϕ to a p-Sylow subgroup P of G. In this section we state our main result concerning exactly which further conditions G and ϕ must satisfy in order for the Bertin obstruction of ϕ to vanish provided that of ϕ_P vanishes. The proof of this result is given in §7–§8.

We begin with a well-known result about the structure of G which follows from a theorem of P. Hall [1, Thm. 18.5].

LEMMA 6.1. – *The group G is the semi-direct product of a normal p-group P and a cyclic group C of order prime to p. Let $z \in G$ be an element which is not of p-power order. Let m be the smallest positive integer such that $w = z^m$ has order prime to p. Let t be the unique element of C having the same image as w in G/P. Then w is conjugate to t in G. In particular, all subgroups of G having a given prime-to-p order are conjugate.*

NOTATION 6.2. – Let T be a non-trivial cyclic subgroup of G. Define

$$b'_T = b'_{T,G} = \sum_{P \not\supset \Gamma \in S(T)} \mu([\Gamma : T]) \tag{6.1}$$

where as before $S(T) = S_G(T)$ is the set of cyclic subgroups Γ of G which contain T.

Recall from Definition (3.1) that

$$\psi(T, G) = \sum_{\Gamma \in S(T)} \mu([\Gamma : T]). \tag{6.2}$$

DEFINITION 6.3. – Let u be a uniformizer in the discrete valuation ring $k[[t]]^{\phi(P)}$. The field $k((t))^{\phi(P)}$ is a cyclic $C = G/P$ extension of $k((t))^{\phi(G)}$ via ϕ. Let $\theta : C \to k^*$ be the faithful character defined by $\phi(\sigma)(u)/u \equiv \theta(\sigma) \bmod uk[[u]]$ for $\sigma \in C$. Suppose C_1 is a subgroup of C and that j is an integer such that the restriction $\theta^j|_{C_1}$ of θ^j to C_1 takes values in $(\mathbb{Z}/p)^*$. We define the *Teichmüller* lift of $\theta^j|_{C_1}$ to be the unique character $\psi : C_1 \to \mathbb{Z}_p^*$ whose reduction mod p is equal to $\theta^j|_{C_1}$.

REMARK 6.4. – The definition of θ does not depend on the choice of uniformizer u. In Lemma 8.7 below we consider the character $\theta_0 : C \to k^*$ defined by $\theta_0(\sigma) \equiv \sigma(t)/t \bmod tk[[t]]$. This also does not depend on the choice of the uniformizing parameter t. Hence on letting $u = \prod_{\gamma \in P} \gamma(t) = \mathrm{Norm}_P(t)$, we see that $\theta(\sigma) = \theta_0(\sigma)^{\#P}$. Since $\#P$ is a power of p, we conclude that $\theta(\sigma) = \theta_0(\sigma)$ if $\theta_0(\sigma) \in (\mathbb{Z}/p)^*$.

NOTATION 6.5. – Suppose T is a cyclic subgroup of P. The normalizer $\mathrm{N}_C(T)$ of T in C acts on T by conjugation. Since T is cyclic of order a power of p, say of order p^n, and $N_C(T)$ is of order prime to p, the order of the image of $N_C(T)$ in $Aut(T)$ divides $p-1$. Thus we can write $\chi_T : \mathrm{N}_C(T) \to \mathbb{Z}_p^*$ for the unique Teichmülller lift character such that $xyx^{-1} = y^{\chi_T(x)}$ for $x \in \mathrm{N}_C(T)$ and $y \in T$.

THEOREM 6.6. – *The Bertin obstruction of ϕ vanishes if and only if all the following conditions hold:*

a. *The Bertin obstruction of the restriction ϕ_P of ϕ to P vanishes.*
b. *If t is a non-trivial element of C, the centralizer $\mathrm{C}_G(t)$ of t in G is cyclic and equal to the product group $\mathrm{C}_P(t) \times C = \mathrm{C}_P(C) \times C$.*
c. *For each non-trivial cyclic subgroup T of P, both of the following statements are true:*
   i. $b'_{T,G} \equiv 0$ *mod* $[\mathrm{N}_P(T) : T]\mathbb{Z}$.
   ii. $[\mathrm{N}_P(T) : T] b_{T,P} \geq -b'_{T,G}$.
d. *For each non-trivial cyclic subgroup T of P, one of the following is true:*
   i. *The centralizer $\mathrm{C}_C(T)$ of T in C is non-trivial, and*
   $$\psi(T, G) \equiv 0 \mod \#\mathrm{N}_C(T)\mathbb{Z}.$$
   ii. *The centralizer $\mathrm{C}_C(T)$ is trivial. Then the restriction of θ to $\mathrm{N}_C(T)$ is faithful, takes values in $(\mathbb{Z}/p)^*$ and has Teichmüller lift χ_T^{-1}, and*
   $$b'_{T,G} \equiv 0 \mod \#\mathrm{N}_C(T)\mathbb{Z}.$$

The proof of this result is completed at the end of §8 using the results in §3, §7 and §8.

We should point out that conditions (b), (c)(i) and (d)(i) of the above theorem are purely group theoretic, in the sense that they do not depend on ϕ. Condition (c)(ii) should be interpreted as saying that the wild ramification groups of G are sufficiently large relative to the constant $-b_{T',G}$ which does not depend on the ramification filtration of G determined by ϕ. Condition (d)(ii) (when it applies) should be viewed as saying that the conjugation action of $\mathrm{N}_C(T)$ on T is the inverse of the Teichmüller lift of the restriction of the tame character $\theta : C \to k^*$ to $\mathrm{N}_C(T)$. Note that θ does not depend on T and is also independent of ϕ. Thus condition (d)(ii) does involve the arithmetic information contained in θ, but this information is connected only with tame ramification. The higher ramification filtration of G therefore enters into only condition (a) and condition (c)(ii) of Theorem 6.6.

7. Obstructions associated to cyclic subquotients which are not p-groups

Throughout this section we suppose that the finite group $G = P.C$ is a semi-direct product of a normal p-group P with a cyclic prime to p group C. Our goal is to prove the following proposition concerning the constants $b_{T,J} = b_{T,J}(\phi)$ in Corollary 5.5:

PROPOSITION 7.1. – *The following conditions are equivalent.*

a. *For each cyclic subgroup T of a subquotient J of G such that T is not a p-group, then the constant $b_{T,J} = b_{T,J}(\phi)$ in Corollary 5.5 has the property that $0 \leq b_{T,J} \in \mathbb{Z}$.*
b. *If t is a non-trivial element of a cyclic subgroup C_0 of G of maximal prime to p order, the centralizer $\mathrm{C}_G(t)$ is cyclic and equal to the product group $\mathrm{C}_P(t) \times C_0 = \mathrm{C}_P(C_0) \times C_0$.*

If one (and hence both) of these conditions holds, then all of the constants $b_{T,J}$ in part (a) are either 0 or 1. Both conditions hold if the Bertin obstruction of ϕ vanishes.

Proof that condition (a) of Proposition 7.1 implies condition (b).

We assume that condition (a) of the proposition holds. Condition (b) holds trivially if P is trivial, so we assume P is not trivial. All of the cyclic subgroups of G of maximal prime-to-p order are conjugate to C by Lemma 6.1. Hence to prove (b), we can reduce to the case $C_0 = C$. The fact that $\mathrm{C}_G(C) = \mathrm{C}_P(C) \times C$ is clear because G is the semi-direct product of the abelian group C with P.

We first show that $\mathrm{C}_P(t)$ is cyclic. Since condition (a) applies to all subquotients of G, to show $\mathrm{C}_P(t)$ is cyclic, we can replace G by $\mathrm{C}_P(t) \times \langle t \rangle$. We may thus temporarily assume that G is the product group $P \times \langle t \rangle$, with $\mathrm{C}_P(t) = P$. Let P_1 be the Frattini subgroup of G, so that $P_1 = [P,P] \cdot P^p$ is the normal subgroup of G generated by the commutator subgroup $[P,P]$ of P and the p^{th} powers of elements of P. Thus P/P_1 is an elementary abelian group of rank equal to that of P. By Corollary 3.4 and the fact that condition (a) applies to all subquotients, we may conclude that if H is a subquotient of G, then $\mathrm{C}(H)$ must be either a p-group or a cyclic group. But $G/P_1 = (P/P_1) \times \langle t \rangle$ is abelian and not a p-group, so this group must be cyclic. Hence the p-Frattini quotient P/P_1 is cyclic, so $P = \mathrm{C}_P(t)$ itself must be cyclic, as asserted.

We now drop the assumption that $G = P \times \langle t \rangle$. To show the last equality in part (b) of Proposition 7.1, it will suffice to prove

$$\mathrm{C}_P(t) = \mathrm{C}_P(C). \tag{7.1}$$

To prove (7.1), we can use induction on $\#C$ to reduce to the case in which the index of $\langle t \rangle$ in C is a prime number by replacing G by $P.\mathrm{C}_P(t)$. We have already shown that $\mathrm{C}_P(t)$ is cyclic, and clearly $\mathrm{C}_P(C) \subset \mathrm{C}_P(t)$. We now check that C normalizes $\mathrm{C}_P(t)$. Suppose $c \in C$ and $g \in \mathrm{C}_P(t)$. Then $cgc^{-1} = g' \in P$ since P is normal, and

$$g'tg'^{-1} = cgc^{-1}tcg^{-1}c^{-1} = cgtg^{-1}c^{-1} = ctc^{-1} = t$$

since c and t are in the abelian group C and $g \in \mathrm{C}_P(t)$. Thus the subgroup $\mathrm{C}_P(t).C$ generated by $\mathrm{C}_P(t)$ and C is a semi-direct product of these two groups. We now replace G by $\mathrm{C}_P(t).C$ to be able to assume that $P = \mathrm{C}_P(t)$ is cyclic and that $[C : \langle t \rangle] = \ell$ is prime (and prime to p). If C centralizes P, then (7.1) holds. So we will now assume that C does not centralize P and derive a contradiction.

Since t commutes with $P = \mathrm{C}_P(t)$ and with all of C, we find that the centralizer $\mathrm{C}_G(\langle t \rangle)$ is equal to all of G. We now apply Proposition 3.2 to the subgroup $T = \langle t \rangle$ of G. Since $\mathrm{N}_G(T) = \mathrm{C}_G(T) = G$ is not T, this proposition implies that

$$\psi(\{e\}, \mathrm{C}_G(T)/T) = \sum_{\text{cyclic } H \subset \mathrm{C}_G(T)/T} \mu(\#H) = 0 \tag{7.2}$$

where the sum is over the cyclic subgroups H of $\mathrm{C}_G(T)/T$, including the trivial subgroup, and μ is the Möbius function.

In our situation, $\mathrm{C}_G(T)/T = G/\langle t\rangle = P.(C/\langle t\rangle)$ is a non-trivial semi-direct product of the cyclic p-group P with the cyclic group $C/\langle t\rangle$ of prime order $\ell \neq p$. Then $C/\langle t\rangle$ acts non-trivially by conjugation on every element of P. It follows that any element $g \in \mathrm{C}_G(T)/T$ which does not lie in P must have order exactly ℓ, since otherwise conjugation by g would fix the non-trivial element g^ℓ of P. The number of elements of $\mathrm{C}_G(T)/T$ which do not lie in P is $(\ell-1)(\#P)$, and these generate the $\#P$ subgroups H of order ℓ in $\mathrm{C}_G(T)/T$. The other groups H appearing on the right hand side of (7.2) are subgroups of P, and the only groups H of this kind for which $\mu(\#H) \neq 0$ are the trivial group $\{e\}$ and the unique subgroup P_0 of order p in $\mathrm{C}_G(T)/T$. Thus

$$\psi(\{e\}, \mathrm{C}_G(T)/T) = \sum_{H \subset \mathrm{C}_G(T)/T} \mu(\#H) = \mu(1) + \mu(p) + \#P \cdot \mu(\ell) = -\#P \neq 0. \tag{7.3}$$

This contradicts (7.2), which completes the proof that part (a) of Proposition 7.1 implies part (b).

Conclusion of the proof of Proposition 7.1. – We first prove two lemmas.

LEMMA 7.2. – *Every subquotient J of G is the semi-direct product of a p-group with a cyclic prime to p-group. If condition (b) of Proposition 7.1 holds for G, then it also holds when G is replaced by J.*

Proof. – The first statement is a consequence of Hall's Theorem [1, Thm. 18.5] together with the fact that J is an extension of a cyclic group of order prime to p by a normal p-subgroup. Suppose now that G satisfies condition (b) of Proposition 7.1. It is clear that every subgroup of G then satisfies this condition. We are thus reduced to showing that $J = G/H$ satisfies this condition for all normal subgroups H of G. It is enough to prove this when H is either a p-group or a cyclic prime to p-group.

Suppose first that H is a p-group. Then $H \subset P$ and $J = (P/H).C$ is the semi-direct product of the p-group P/H with C. Let t be a non-trivial element of C. By hypothesis, $\mathrm{C}_G(t) = \mathrm{C}_P(t) \times C$ is cyclic. Hence to show $\mathrm{C}_J(t) = \mathrm{C}_{P/H}(t).C$ is cyclic, it will suffice to show that the quotient homomorphism $P \to P/H$ gives a surjection $\mathrm{C}_P(t) \to \mathrm{C}_{P/H}(t)$. Here t acts on P and P/H by conjugation, so we are to show that the invariants $P^{\langle t\rangle}$ surject onto $(P/H)^{\langle t\rangle}$. Since P is a p-group and t has order prime to p, this follows from taking the non-abelian cohomology with respect to $\langle t\rangle$ of the sequence of $1 \to H \to P \to P/H \to 1$ (see [28, Chap. VII, Annexe]).

Finally, suppose that H is cyclic of order prime to p. By Lemma 6.1, H is a subgroup of C since it is conjugate to such a subgroup and is normal. Then $P.H$ contains the normal subgroups P and H, so $P.H$ is isomorphic to $P \times H$, and H and P commute. Since $H \subset C$ commutes with C, we conclude H is in the center of G. Suppose $t' \in J = G/H = P.(C/H)$ has order prime to p. Since H is central, it is clear that condition (b) of Proposition 7.1 implies $\mathrm{C}_J(t') = \mathrm{C}_P(t') \times (C/H)$ is cyclic, so condition (b) holds for J. □

For $z \in G$, we will write $\mathrm{N}_G(z)$ for $\mathrm{N}_G(\langle z\rangle)$, where $\langle z\rangle$ is the subgroup generated by z.

LEMMA 7.3. – *Suppose that condition (b) of Proposition 7.1 holds. Let $z \in G$ be an element which is not of p-power order. Let m be the smallest positive integer such that $w = z^m$ is a (non-trivial) element of order prime to p.*

a. *The group $\mathrm{C}_G(z) = \mathrm{C}_G(w)$ is cyclic and conjugate to $\mathrm{C}_P(C) \times C$.*
b. *If $\mathrm{N}_G(z)$ properly contains $\langle z \rangle$, then so does $\mathrm{C}_G(z)$.*

Proof. – By Lemma 6.1, w is conjugate to an element t of C. By replacing z by a conjugate of itself, we can assume that $w = t \in C$. Since we assume that condition (b) of Proposition 7.1 holds, $\mathrm{C}_G(w) = \mathrm{C}_G(t) = \mathrm{C}_P(C) \times C$ is cyclic. We have $z \in \mathrm{C}_G(w) \supset \mathrm{C}_G(z)$ since w is a power of z. Because $\mathrm{C}_G(w)$ is abelian, this implies $\mathrm{C}_G(w) \subset \mathrm{C}_G(z)$, so $\mathrm{C}_G(z) = \mathrm{C}_G(w) = \mathrm{C}_P(C) \times C$. This proves part (a).

To show part (b), we assume to the contrary that

$$\mathrm{C}_G(z) = \mathrm{C}_P(C) \times C = \langle z \rangle. \tag{7.4}$$

Note that this forces $w = t$ above to be a generator of C. It will suffice to show

$$\mathrm{N}_G(z) \subset \mathrm{C}_G(z) \tag{7.5}$$

since then $\mathrm{C}_G(z) = \mathrm{N}_G(z)$ will equal $\langle z \rangle$.

The group $\langle z \rangle$ is obviously normal in $\mathrm{N}_G(z)$, and $\langle w \rangle = \langle t \rangle = C \subset \langle z \rangle$ is characteristic in $\langle z \rangle$. Hence C is a normal subgroup of $\mathrm{N}_G(z)$. The group $\mathrm{N}_G(z) \cap P$ is also normal in $\mathrm{N}_G(z)$ since P is normal in G. Since $\mathrm{N}_G(z) \cap P$ and C have coprime orders, and the product of these orders is $\#\mathrm{N}_G(z)$, we conclude that $\mathrm{N}_G(z)$ is isomorphic to the product group $(\mathrm{N}_G(z) \cap P) \times C$. This means that C commutes with $\mathrm{N}_G(z) \cap P$.

Thus $\mathrm{N}_G(z) \cap P$ is contained in the cyclic group $\mathrm{C}_G(C) = \mathrm{C}_P(C) \times C$. Hence $\mathrm{N}_G(z) \cap P$ is abelian. Since $\langle z \rangle \cap P$ is contained in $\mathrm{N}_G(z) \cap P$, this means that $\mathrm{N}_G(z) \cap P$ centralizes $\langle z \rangle \cap P$. However, we have already shown that C commutes with $\mathrm{N}_G(z) \cap P$. Thus $\mathrm{C}_G(\mathrm{N}_G(z) \cap P)$ contains both $\langle z \rangle \cap P$ and $C = \langle w \rangle$, and the latter two groups generate $\langle z \rangle$. Hence $\mathrm{C}_G(\mathrm{N}_G(z) \cap P)$ contains $\langle z \rangle$, so $\mathrm{N}_G(z) \cap P$ is contained in $\mathrm{C}_G(z)$.

We now use the fact that $\mathrm{N}_G(z)$ is generated by $\mathrm{N}_G(z) \cap P \subset \mathrm{C}_G(z)$ and $C = \langle w \rangle \subset \mathrm{C}_G(w)$, where we have shown $\mathrm{C}_G(w) = \mathrm{C}_G(z)$ already. This implies $\mathrm{N}_G(z) \subset \mathrm{C}_G(z)$ and proves (7.5). □

COROLLARY 7.4. – *Condition (b) of Proposition 7.1 implies that if T is a cyclic subgroup of a subquotient J of G such that T is not a p-group, then $b_{T,J}$ is equal to 0 or 1.*

Proof. – By Lemma 7.2, it will be enough to consider the case in which the subquotient J is G itself. By Proposition 3.2, $b_T = 1$ if $\mathrm{N}_G(T) = T$, and $b_T = 0$ provided

$$\psi(T, \mathrm{C}_G(T)) = \sum_{T \subset W \subset \mathrm{C}_G(T), W \text{ cyclic}} \mu([W : T]) = 0. \tag{7.6}$$

To prove that one or the other of these alternatives applies, let z be a generator of T, and suppose that $\mathrm{N}_G(T) \neq T$. By Lemma 7.3, $\mathrm{C}_G(T)$ is a cyclic group which strictly contains T. We conclude that $\psi(T, \mathrm{C}_G(T)) = \psi(\{e\}, \mathrm{C}_G(T)/T) = \sum_{d | [\mathrm{C}_G(T) : T]} \mu(d) = 0$ in (7.6), so the corollary holds. □

The last two assertions in Proposition 7.1 now follow from Corollaries 7.4 and 5.5, and this completes the proof. □

8. Obstructions associated to cyclic p-subgroups

We will fix the following hypotheses and notation throughout this section.

HYPOTHESIS 8.1. – *Let $\phi : G \to \mathrm{Aut}_k(k[[t]])$ be an injection, and write G as the semi-direct product $P.C$ of a normal p-group P and a cyclic group C of order prime to p. Let T be a non-trivial cyclic subgroup of G of p-power order. Define $b'_T = b'_{T,G}$ as in (6.1). We assume finally that if t is a non-trivial element of C, then $\mathrm{C}_G(t) = \mathrm{C}_P(t) \times C$ is cyclic.*

Note that by Proposition 7.1, the final assumption in this hypothesis holds if ϕ has vanishing Bertin obstruction.

The goal of this section is to compare the constants $b_T = b_{T,G}$ and $b_{T,P}$.

LEMMA 8.2. – *After replacing T by a conjugate subgroup, the centralizer $\mathrm{C}_G(T)$ is the semi-direct product $\mathrm{C}_P(T).\mathrm{C}_C(T)$ and the normalizer $\mathrm{N}_G(T)$ is $\mathrm{N}_P(T).\mathrm{N}_C(T)$.*

Proof. – The group $\mathrm{N}_P(T) = \mathrm{N}_G(T) \cap P$ is normal in $\mathrm{N}_G(T)$ since P is normal in G. The quotient group $\mathrm{N}_G(T)/\mathrm{N}_P(T)$ injects into the cyclic prime to p-group G/P, so $\mathrm{N}_G(T)$ is the semi-direct product of $\mathrm{N}_P(T)$ with a subgroup C' of order prime to p. By Lemma 6.1 we can replace T by a conjugate of itself to be able to assume that $C' \subset C$. After this replacement we have $C' = \mathrm{N}_C(T)$. Since $\mathrm{C}_G(T) \subset \mathrm{N}_G(T)$, we can write each element of $\mathrm{C}_G(T)$ in a unique way in the form $\alpha\beta$ with $\alpha \in \mathrm{N}_P(T)$ and $\beta \in C' = \mathrm{N}_C(T)$. Then the conjugation action of β on T must be the inverse of the conjugation action of α on T. Since β and α have co-prime orders, this implies that each of these actions are trivial, so $\alpha \in \mathrm{C}_P(T)$ and $\beta \in \mathrm{C}_C(T)$. Thus $\mathrm{C}_G(T) = \mathrm{C}_P(T).\mathrm{C}_C(T)$. □

COROLLARY 8.3. – *One has*

$$b_T = \frac{b_{T,\mathrm{C}_G(T)}}{[\mathrm{N}_G(T) : \mathrm{C}_G(T)]} = \frac{b_{T,P}}{\#\mathrm{N}_C(T)} + \frac{b'_{T,G}}{\#\mathrm{N}_C(T) \cdot [\mathrm{N}_P(T) : T]}. \tag{8.1}$$

Proof. – By Theorem 2.3, since T is non-trivial,

$$b_T = \frac{1}{[\mathrm{N}_G(T) : T]} \left(\sum_{\Gamma \in S(T)} \mu([\Gamma : T]) \iota(\Gamma) \right), \tag{8.2}$$

where $\iota(\Gamma) = \iota_G(\Gamma)$ is defined in Notation 2.2. Clearly if $\Gamma \in S(T)$ then $\Gamma \subset \mathrm{C}_G(T)$ since Γ is abelian and contains T. Thus $S_G(T) = S_{\mathrm{C}_G(T)}(T)$, and the compatibility of the lower numbering of ramification groups with passing from G to subgroups leads to the first equality in (8.1). To prove the second equality, note that the $\Gamma \in S_G(T)$ which are p-groups are exactly the elements of $S_P(T)$; the other $\Gamma \in S_G(T)$ have $\iota(\Gamma) = 1$ since no higher ramification group can contain a group which is not a p-group. This leads to

$$[\mathrm{N}_G(T) : T] b_T = \sum_{\Gamma \in S(T)} \mu([\Gamma : T]) \iota(\Gamma) = [\mathrm{N}_P(T) : T] b_{T,P} + b'_{T,G}.$$

The second equality in (8.1) follows from this and Lemma 8.2. □

COROLLARY 8.4. – *Suppose that* $0 \leq b_{T,P} \in \mathbb{Z}$. *Then* $0 \leq b_T \in \mathbb{Z}$ *if and only if all of the following are true:*

(a.) $b'_{T,G} \equiv 0$ *mod* $[\mathrm{N}_P(T) : T]\mathbb{Z}$.
(b.) $\sum_{\Gamma \in S(T)} \mu([\Gamma : T])\iota(\Gamma) \equiv 0$ *mod* $\#\mathrm{N}_C(T)\mathbb{Z}$.
(c.) $b_{T,P} \geq \frac{-b'_{T,G}}{[\mathrm{N}_P(T):T]}$.

Proof. – We have $b_T \in \mathbb{Z}$ if and only if $\#\mathrm{N}_C(T)b_T \in \mathbb{Z}$ and $[\mathrm{N}_P(T) : T]b_T \in \mathbb{Z}$, since $[\mathrm{N}_P(T) : T]$ is a power of p while $\#\mathrm{N}_C(T)$ is prime to p. From (8.1) we have

$$\#\mathrm{N}_C(T)b_T = b_{T,P} + \frac{b'_{T,G}}{[\mathrm{N}_P(T) : T]}.$$

So since we suppose $b_{T,P} \in \mathbb{Z}$, we see that this is in $\mathbb{Z}$ if and only if condition (a) of Corollary 8.4 holds. From (8.2) we have

$$[\mathrm{N}_P(T) : T]b_T = \frac{[\mathrm{N}_P(T) : T]}{[\mathrm{N}_G(T) : T]} \left(\sum_{\Gamma \in S(T)} \mu([\Gamma : T])\iota(\Gamma) \right).$$

Since $[\mathrm{N}_G(T) : T]/[\mathrm{N}_P(T) : T] = \#\mathrm{N}_C(T)$ by Lemma 8.2, condition (b) of Corollary 8.4 is equivalent to $[\mathrm{N}_P(T) : T]b_T \in \mathbb{Z}$. Finally, Corollary 8.3 shows condition (c) is equivalent to $b_T \geq 0$. □

REMARK 8.5. – The hypothesis that $0 \leq b_{T,P} \in \mathbb{Z}$ holds if the Bertin obstruction of the restriction $\phi|_P$ of ϕ to P vanishes by Proposition 2.1. Corollary 8.4 has to do with the further conditions which must hold if the Bertin obstruction of ϕ is to vanish. (Recall that if the Bertin obstruction of ϕ vanishes then so does that of ϕ_P by Theorem 5.1.) In condition (a) of the corollary, the constant $b'_{T,G}$ is a purely group theoretic invariant which does not depend on ϕ. Condition (c) can be thought of as a lower bound on the size of the wild ramification groups of G. The object of the rest of this section is to quantify the arithmetic information contained in condition (b).

LEMMA 8.6. – *Suppose* $\Gamma \in S_P(T)$. *Then* $\mathrm{N}_C(\Gamma) \subset \mathrm{N}_C(T)$ *and the restriction of the character* $\chi_T : \mathrm{N}_C(T) \to \mathbb{Z}_p^*$ *of Notation 6.5 to* $\mathrm{N}_C(\Gamma)$ *equals* χ_Γ.

Proof. – Recall that $\Gamma \in S_P(T)$ must be a cyclic p-group containing T. Hence T is characteristic in Γ, so $\mathrm{N}_C(\Gamma) \subset \mathrm{N}_C(T)$. By definition, $\chi_T : \mathrm{N}_C(T) \to \mathbb{Z}_p^*$ gives the conjugation action of $\mathrm{N}_C(T)$ on T, while $\chi_\Gamma : \mathrm{N}_C(\Gamma) \to \mathbb{Z}_p^*$ gives the conjugation action of $\mathrm{N}_C(\Gamma)$ on Γ. Since the kernel of the restriction homomorphism $\mathrm{Aut}(\Gamma) \to \mathrm{Aut}(T)$ is a p-group, and $\mathrm{N}_C(T)$ has order prime to p, this implies χ_T restricts to χ_Γ. □

The following result is Proposition 9 of §IV.2 of [28].

LEMMA 8.7 (Serre). – *Let* $\mathbf{p}$ *be the maximal ideal* $tk[[t]]$ *of* $k[[t]]$, *and recall that* G_j *is the* j^{th} *ramification subgroup of* G *in the lower numbering. Let* $\theta_0 : C = G_0/G_1 \to k^*$ *be the faithful character defined by*

$$\theta_0(\sigma) \equiv \frac{\phi(\sigma)(t)}{t} \mod \mathbf{p} \quad \text{for} \quad \sigma \in C.$$

For each $j \geq 1$ we have an injective group homomorphism $\theta_j : G_j/G_{j+1} \to \mathbf{p}^j/\mathbf{p}^{j+1}$ defined by $\phi(\sigma)(t)/t \equiv 1 + \theta_j(\sigma)$ mod $\mathbf{p}^{j+1}$. Then

$$\theta_j(sxs^{-1}) = \theta_0(s)^j \cdot \theta_j(x) \tag{8.3}$$

for $x \in G_j/G_{j+1}$ and $s \in C$.

COROLLARY 8.8. – *Let $\theta_0 : C \to k^*$ and $\theta : C \to k^*$ be the characters defined in Lemma 8.7 and Definition 6.3. Then $\theta = \theta_0^{\#P}$ where $\#P$ is a power of p. If $g \in C$ then $\theta(g) \in (\mathbb{Z}/p)^*$ if and only if $\theta_0(g) \in (\mathbb{Z}/p)^*$, and in this case $\theta(g) = \theta_0(g)$.*

Proof. – The equality $\theta = \theta_0^{\#P}$ is clear from the fact that if u is the uniformizer in $k[[t]]^{\phi(P)}$ used in Definition 6.3 then $u = t^{\#P}v$ for some unit v in $k[[t]]$. The second statement in the corollary follows from the fact that $\#P$ is a power of p. □

COROLLARY 8.9. – *Suppose $\Gamma \in S_P(T)$. Let $i = \iota(\Gamma) - 1$ as in Definition 2.2. Suppose $\mathrm{N}_C(\Gamma)$ is not trivial. The character $\theta_0^i : \mathrm{N}_C(\Gamma) \to k^*$ takes values in $(\mathbb{Z}/p)^*$ and is trivial if $p = 2$. The resulting Teichmüller lift of this character is the restriction of $\chi_T : \mathrm{N}_C(T) \to \mathbb{Z}_p^*$ to $\mathrm{N}_C(\Gamma)$.*

Proof. – Since Γ is a cyclic p-group and $\Gamma_i = \Gamma$ properly contains Γ_{i+1}, we have $i \geq 1$, and the group Γ_i/Γ_{i+1} is a non-trivial cyclic p-group. This group must in fact be of order p, since θ_i is an embedding of it into $\mathbf{p}^i/\mathbf{p}^{i+1}$. Thus $\theta_i(\Gamma_i/\Gamma_{i+1})$ is a one dimensional $\mathbb{Z}/p$ vector space inside $\mathbf{p}^i/\mathbf{p}^{i+1}$ which by Lemma 8.7 is stable by multiplication by the elements of $\theta_0^i(\mathrm{N}_C(\Gamma)) \subset k^*$. This implies $\theta_0^i(\mathrm{N}_C(\Gamma)) \subset (\mathbb{Z}/p)^*$. If $p = 2$, this shows θ_0^i restricts to the trivial character on $\mathrm{N}_C(\Gamma)$. In general, Lemma 8.7 shows that $\theta_0^i|_{\mathrm{N}_C(\Gamma)}$ gives the conjugation action of $\mathrm{N}_C(\Gamma)$ on Γ. By Lemma 8.6, this action is also given by the restriction of χ_T to $\mathrm{N}_C(\Gamma)$. □

LEMMA 8.10. – *Suppose that $\Gamma \in S_P(T)$, so that Γ is a cyclic p-group which contains T. The group $\mathrm{N}_C(T)$ acts by conjugation on $S_P(T)$. Let $S_P^T(\Gamma)$ be the orbit of Γ under this action. One has*

$$\sum_{\Gamma_1 \in S_P^T(\Gamma)} \mu([\Gamma_1 : T])\iota(\Gamma_1) \equiv \sum_{\Gamma_1 \in S_P^T(\Gamma)} \mu([\Gamma_1 : T])\iota(T) \mod \#\mathrm{N}_C(T)\mathbb{Z}. \tag{8.4}$$

Proof. – By Corollary 8.9, the restriction $\theta_0^{\iota(T)-1}|_{\mathrm{N}_C(T)}$ of $\theta_0^{\iota(T)-1} : C \to k^*$ to $\mathrm{N}_C(T)$ takes values in $(\mathbb{Z}/p)^*$ and has the Teichmüller lift of the character χ_T of Lemma 8.6. Since $\mathrm{N}_C(T)$ conjugates T to itself, it acts on $S_P(T)$, and elements in each orbit have the same order and value for ι. The stabilizer of Γ under this action is $\mathrm{N}_C(\Gamma)$, so

$$\sum_{\Gamma_1 \in S_P^T(\Gamma)} \mu([\Gamma_1 : T])\iota(\Gamma_1) = [\mathrm{N}_C(T) : \mathrm{N}_C(\Gamma)]\mu([\Gamma : T])\iota(\Gamma). \tag{8.5}$$

By Lemma 8.6, the action of $\mathrm{N}_C(\Gamma)$ on Γ by conjugation is given by the restriction of χ from C to $\mathrm{N}_C(\Gamma)$. As in Corollary 8.9, let i be the largest integer such that $\Gamma \subset G_i$, so that $\iota(\Gamma) = i+1$. By Corollary 8.9, $\theta_0^i|_{\mathrm{N}_C(\Gamma)}$ has Teichmüller lift $\chi|_{\mathrm{N}_C(\Gamma)}$. However, $\theta_0^{\iota(T)-1}|_{\mathrm{N}_C(\Gamma)}$ also has Teichmüller lift $\chi|_{\mathrm{N}_C(\Gamma)}$. Since θ_0 is a faithful character of C, this forces $i \equiv \iota(T) - 1$ mod $\#\mathrm{N}_C(\Gamma)$. Therefore $\iota(\Gamma) \equiv \iota(T)$ mod $\#\mathrm{N}_C(\Gamma)$. Substituting this into (8.5) proves (8.4) since $[\mathrm{N}_C(T) : \mathrm{N}_C(\Gamma)] \cdot \#\mathrm{N}_C(\Gamma) = \#\mathrm{N}_C(T)$. □

LEMMA 8.11. – *Suppose that χ_T in Lemma 8.6 has a non-trivial kernel. Then $\mathrm{N}_C(T) = \mathrm{C}_C(T) = C$ and χ_T is trivial. Condition (b) of Corollary 8.4 is equivalent to*

$$\sum_{\Gamma \in S(T)} \mu([\Gamma : T]) \equiv 0 \mod \#\mathrm{N}_C(T)\mathbb{Z} \tag{8.6}$$

which is independent of ϕ.

Proof. – Suppose that $t \in \mathrm{N}_C(T)$ is a non-trivial element of the kernel of χ_T. Then t acts trivially on the cyclic p-group T by conjugation. The final assumption of Hypothesis 8.1 now says that $\mathrm{C}_G(t) = \mathrm{C}_P(t) \times C$ is cyclic. Thus T is contained in $\mathrm{C}_G(t)$, and every element of $\mathrm{C}_G(t)$ commutes with T. In particular, C is contained in $\mathrm{C}_G(T)$, so we get that $\mathrm{N}_C(T) = \mathrm{C}_C(T) = C$ and that χ_T is trivial. Hence the residue class $\iota(T) - 1 \in \mathbb{Z}/\#\mathrm{N}_C(T)\mathbb{Z}$ is trivial by Corollary 8.9. Summing (8.4) over the $\mathrm{N}_C(T)$ orbits in $S_P(T)$ now gives

$$\sum_{\Gamma_1 \in S_P(T)} \mu([\Gamma_1 : T])\iota(\Gamma_1) \equiv \sum_{\Gamma_1 \in S_P(\Gamma)} \mu([\Gamma_1 : T]) \bmod \#\mathrm{N}_C(T)\mathbb{Z}. \tag{8.7}$$

If $\Gamma \in S(T)$ is not in $S_P(T)$ then $\iota(T) = 1$ since Γ is not a p-group. Hence summing $\mu([\Gamma : T])\iota(\Gamma) = \mu([\Gamma : T])$ as Γ runs over these groups to both sides of (8.7) leads to the reformulation of condition (b) stated in Lemma 8.11. □

LEMMA 8.12. – *Suppose that χ_T in Lemma 8.6 has trivial kernel, which is equivalent to $\mathrm{C}_C(T) = \{e\}$. Let D be the subgroup of G generated by T and by $\mathrm{N}_C(T)$. Then the constant $b_{T,D}$ equals $\iota(T)/\#\mathrm{N}_C(T)$.*

a. *One has $b_{T,D} \in \mathbb{Z}$ if and only if $\iota(T) \equiv 0$ mod $\#\mathrm{N}_C(T)\mathbb{Z}$.*
b. *Suppose $b_{T,D} \in \mathbb{Z}$. Then condition (b) of Corollary 8.4 is equivalent to the congruence*

$$b'_T = b'_{T,G} = \sum_{P \not\supset \Gamma \in S(T)} \mu([\Gamma : T]) \equiv 0 \mod \#\mathrm{N}_C(T)\mathbb{Z}. \tag{8.8}$$

Proof. – Since χ_T has trivial kernel, D is the semi-direct product of the normal p-group T with the cyclic prime to p group $\mathrm{N}_C(T)$, and the action of $\mathrm{N}_C(T)$ on T is faithful. If Γ is a cyclic subgroup of D containing T, then $\Gamma/T \subset D/T \cong \mathrm{N}_C(T)$ acts faithfully by conjugation on T. This forces $\Gamma = T$, so the set $S_D(T)$ of such Γ is simply $\{T\}$. Therefore $b_{T,D} = \iota(T)/\#\mathrm{N}_C(T)$ by Theorem 2.3. Replacing G by D in Lemma 8.10 shows $b_{T,D}$ is integral if and only if $\iota(T) \equiv 0 \bmod \#\mathrm{N}_C(T)$, which we will suppose is the case for the rest of the proof. We now return to G as before, so that G need not be D. Summing the formula in Lemma 8.10 over the $\mathrm{N}_C(T)$ orbits in $S_P(T)$ now gives

$$\sum_{\Gamma \in S_P(T)} \mu([\Gamma_1 : T])\iota(\Gamma_1) \equiv 0 \mod \#\mathrm{N}_C(T)\mathbb{Z}$$

since $\iota(T) \equiv 0 \bmod \#\mathrm{N}_C(T)\mathbb{Z}$. Hence condition (b) of Corollary 8.4 becomes the congruence

$$\begin{aligned} 0 &\equiv \sum_{\Gamma \in S(T)} \mu([\Gamma : T])\iota(\Gamma) \bmod \#\mathrm{N}_C(T)\mathbb{Z} \\ &\equiv \sum_{P \not\supset \Gamma \in S(T)} \mu([\Gamma : T])\iota(\Gamma) \bmod \#\mathrm{N}_C(T)\mathbb{Z} \\ &= b'_{T,G} \bmod \#\mathrm{N}_C(T)\mathbb{Z} \end{aligned} \tag{8.9}$$

since $\iota(\Gamma) = 1$ if $\Gamma \not\subset P$. □

REMARK 8.13. – In view of Lemma 8.10, the arithmetic condition in part (a) of Lemma 8.12 is that the conjugation action of $\mathrm{N}_C(T)$ on T is via the inverse of the Teichmüller lift of the character $\theta_0|_{\mathrm{N}_C(T)}$. Note that $\theta_0|_{\mathrm{N}_C(T)}$ takes values in $(\mathbb{Z}/p)^*$, so it agrees with the restriction $\theta|_{\mathrm{N}_C(T)}$ of the character $\theta : C \to k^*$ defined in Definition 6.3 because of Remark 6.4.

Completion of the proof of Theorem 6.6. – We split the proof into two parts:

Part 1. – *Suppose the Bertin obstruction of ϕ vanishes.*

The Bertin obstruction of ϕ_P then vanishes by Theorem 5.1, so condition (a) of Theorem 6.6 holds. Condition (b) of the theorem follows from Corollary 5.5 and Proposition 7.1. Condition (c) of Theorem 6.6 is a consequence of Corollary 5.5 and conditions (a) and (c) of Corollary 8.4 together with Proposition 2.1 and Theorem 5.1 .

We now suppose as in condition (d) of Theorem 6.6 that T is a non-trivial cyclic subgroup of P. Since we have supposed the Bertin obstruction of ϕ vanishes, we have $b_T \geq 0$ by Proposition 2.1(ii). Therefore conditions (a), (b) and (c) of Corollary 8.4 hold.

Suppose first that $\mathrm{C}_C(T)$ is non-trivial. By the definition of χ_T in Lemma 8.6, χ_T is trivial on $\mathrm{C}_C(T)$. Hence the hypothesis of Lemma 8.11 holds. This Lemma 8.11 now shows that $\mathrm{C}_C(T) = C$. This lemma also shows that since (b) of Corollary 8.4 holds, the congruence claimed in condition (d)(i) of Theorem 6.6 is true, since $\psi(T, G)$ is the constant on the left side of (8.6) by (6.2). This completes the proof of condition (d) of Theorem 6.6 if $\mathrm{C}_C(T)$ is not trivial.

Suppose now that $\mathrm{C}_C(T)$ is trivial. The hypotheses of Lemma 8.12 now hold, and the character χ_T in this lemma has trivial kernel. As in this lemma, let D be the subgroup generated by T and $\mathrm{N}_C(T)$. Since we supposed that the Bertin obstruction of ϕ vanishes, $b_{T,D}$ is an integer by Corollary 5.5. The character θ in Definition 6.3 and Theorem 6.6(d)(ii) now has the properties claimed because of Lemma 8.12(a), Lemma 8.10 and Remark 8.13. Finally, since we have already proved that (b) of Corollary 8.4 is true under the above hypotheses, the remaining congruence to be proved in Theorem 6.6(d)(ii) follows from Corollary 5.5 and Lemma 8.12(b). This completes the proof of condition (d) of Theorem 6.6. We have now shown that if the Bertin obstruction of ϕ vanishes, then (a)–(d) of Theorem 6.6 hold.

Part 2. – Suppose conditions (a)–(d) of Theorem 6.6 hold.

By Proposition 2.1(ii) it will suffice to show that $0 \leq b_T \in \mathbb{Z}$ for all non-trivial cyclic subgroups T of G, since then the Bertin obstruction of ϕ vanishes.

Suppose first that T is not a p-group. We have supposed that condition (b) of Theorem 6.6 holds. By Lemma 6.1, all cyclic subgroups C_0 of G of maximal prime-to-p order are conjugate to C. If now follows from condition (b) of Theorem 6.6 that condition (b) of Proposition 7.1 holds. Therefore by letting $J = G$ in Proposition 7.1(a) we see that $0 \leq b_T = b_{T,J} \in \mathbb{Z}$, as required.

Now suppose that T is a non-trivial cyclic p-subgroup of G. We have supposed in condition (a) of Theorem 6.6 that the Bertin obstruction of the restriction of ϕ to P vanishes. Thus $0 \leq b_{T,P} \in \mathbb{Z}$ by Notation 5.4 and Proposition 2.1. Thus to complete the proof, it will suffice to show that conditions (a), (b) and (c) of Corollary 8.4 hold. Hypothesis (c) of Theorem 6.6 is that (a) and (c) of Corollary 8.4 hold, so we are reduced to checking (b) of that corollary.

Suppose first that the centralizer $\mathrm{C}_C(T)$ of T in C is non-trivial. This is equivalent to supposing that the character χ_T in Lemma 8.6 has a non-trivial kernel. Lemma 8.11, Notation 6.2 and (6.2) now show that Hypothesis d(i) of Theorem 6.6 is equivalent to condition (b) of Corollary 8.4, so we are done in this case.

Finally, suppose that $\mathrm{C}_C(T)$ is trivial. In view of Remark 8.13, the hypothesis in part (d)(ii) of Theorem 6.6 concerning the character θ is equivalent to condition (a) of Lemma 8.12. Therefore part (b) of Lemma 8.12 shows that condition (b) of Corollary 8.4 is equivalent to the hypothesis on $b'_{T,G}$ in Theorem 6.6. Therefore condition (b) of Corollary 8.4 holds in all cases and the proof is complete. □

9. Proof of Theorem 1.8

We begin by proving that GM-groups have certain properties that we require.

THEOREM 9.1. – *Let G be a GM group with respect to the character Θ. Let P, B and C be as in the Definition 1.7. Set $D := \mathrm{C}_P(C)$. Suppose T is a non-trivial cyclic subgroup of P. Recall that $S_G(T)$ is the set of cyclic subgroups of G which contain T, and $\mu(x)$ is the Möbius μ function. Let $b'_{T,G}$ and $\psi(T,G)$ be as in Notation 6.2 and (6.2).*

a. *One has*

$$b'_{T,G} = \sum_{P \not\supset \Gamma \in S_G(T)} \mu([\Gamma : T]) \equiv 0 \mod [\mathrm{N}_P(T) : T]\mathbb{Z}. \tag{9.1}$$

b. *Suppose $\mathrm{C}_C(T)$ is not trivial. Then $T \subset D$ and*

$$\psi(T,G) = \sum_{\Gamma \in S_G(T)} \mu([\Gamma : T]) \equiv 0 \mod \#C\mathbb{Z}. \tag{9.2}$$

c. *Suppose $\mathrm{C}_C(T) = 1$. Then either $\mathrm{N}_C(T) = 1$ or every cyclic overgroup of T is contained in P.*

Proof. – The results are obvious if $C \neq 1$. So assume this is not the case. Set $H = D \times C$. Let $1 \neq W \leq C$. Then $\mathrm{C}_G(W) = DC = H$ (since $D = \mathrm{C}_P(W)$ and C is a complement to any Sylow p-subgroup of $\mathrm{C}_G(W)$). Similarly, $\mathrm{N}_G(W) = \mathrm{N}_P(W)C = \mathrm{C}_P(W)C = \mathrm{C}_G(W)$. It follows that $C \cap C' = 1$ for any conjugate C' of C other than C.

We first prove (c). Suppose that T is contained in some cyclic subgroup not contained in P. It follows that T centralizes some element $c' \neq 1$ of order prime to p. By Lemma 6.1, c' is conjugate to some element $c \in C$. Thus, T centralizes a conjugate C' of C. It follows that $[G : \mathrm{C}_G(T)]$ is a power of p and so $\mathrm{N}_G(T)/\mathrm{C}_G(T)$ is a p-group. Thus, $\mathrm{N}_C(T) \leq \mathrm{C}_G(T) \cap C = 1$, and (c) follows.

We next prove (a) and (b). By Lemma 8.2 we can replace T by a conjugate subgroup in order to have $\mathrm{C}_G(T) = \mathrm{C}_P(T).\mathrm{C}_C(T)$ and $\mathrm{N}_G(T) = \mathrm{N}_P(T).\mathrm{N}_C(T)$. We may assume that $\mathrm{C}_C(T) \neq 1$ (this is the assumption in (b); and in (a) if this is not the case, then we are summing over the empty set). Thus, $1 \neq T \leq D$ by Definition 1.7(a). So $\mathrm{N}_G(T) = \mathrm{N}_P(T)C$.

Since H is cyclic, it is clear that $b'_{T,H} = -1$ if $T = D$ and $b'_{T,H} = 0$ if $T < D$. Also, $\psi(T, H) = 0$.

We claim that every cyclic subgroup E of G that contains T and that is not contained in P is conjugate to a unique subgroup of H containing T via an element of $\mathrm{N}_G(T)$. Here uniqueness is clear because H is cyclic and so has a unique subgroup of each order. Existence follows by Lemma 7.3 since E contains a nontrivial p'-subgroup which is conjugate (in $\mathrm{N}_G(T)$) to a subgroup of C. So we may assume that $E \cap C \neq 1$, whence $E \leq H$.

Now let $E \leq H$ be such a subgroup. Then $\mathrm{N}_G(E)$ must normalize every subgroup of E, and so $\mathrm{N}_G(E) = H$. Thus, $b'_{T,G} = [\mathrm{N}_G(T) : H]b'_{T,H}$. If $T < D$, this implies that $b'_{T,G} = 0$ and (a) follows. If $T = D$, then $[\mathrm{N}_G(T) : H] = [\mathrm{N}_P(D) : D]$, and again (a) follows.

We now prove (b). Note that C acts on $S_G(T)$. Let $E \in S_G(T)$. Then C centralizes E if $E \subset H$. Suppose E is not contained in H and $1 \neq c \in C$ normalizes E. Since $T \subset D$, c centralizes T, so c centralizes the cyclic Sylow p-subgroup of E. Thus, the Sylow p-subgroup of E is contained in D. Thus, E must contain a nontrivial p'-subgroup C' not contained in C since we have assumed $E \not\subset H$. Then c normalizes C' and so c centralizes C' because it does so mod P. Therefore $C' \subset H$, so $C' \subset C$, which is a contradiction. Thus, C acts freely by conjugation on the elements of $S_G(T)$ not contained in H. Since $\mu([\Gamma : T])$ is constant on C-conjugates, it follows that:

$$\sum_{\Gamma \in S_H(T)} \mu([\Gamma : T]) \equiv \psi(T, G) \mod \#C\mathbb{Z}. \tag{9.3}$$

Since H is a cyclic group which properly contains T, the sum on the left in (9.3) is 0, which completes the proof. □

LEMMA 9.2. – *Let Q be a p-group and x an automorphism of Q of order dividing $p - 1$. Let $\phi : Q \to R$ be an x-equivariant surjection. If $r \in R$ with $x(r) = r^e$, then there exists $s \in Q$ with $\phi(s) = r$ and $x(s) = s^e$.*

Proof. – There is no loss in assuming that R is generated by r (replace R by this subgroup and Q by the inverse image). If ϕ factors equivariantly through an intermediate group, the result follows by induction. So we may assume that $K := \ker(\phi)$ is a minimal normal x-invariant subgroup of Q. Thus, we may assume that K is a central elementary abelian

p-subgroup of Q with x irreducible on Q. Since x has order dividing $p-1$, this forces K to have order p. So either Q is cyclic of order p^2, in which case the result is clear, or else Q is elementary abelian. In that case, Q is a completely reducible x-module and so the result is also clear. □

LEMMA 9.3. – *If G is a GM-group with respect to a character Θ, then so is every subquotient.*

Proof. – Keep the usual notation. We induct on the order of G. It is clear that subgroups of GM groups are GM groups. So it suffices to consider quotients by minimal normal non-trivial subgroups N. Since P is normal in G, either $N \cap P$ is trivial and N is of order prime to p or $N \subset P$. If N has order prime to P, then $N.P$ must be the product group $N \times P$, so N and P commute. Hence N is a subgroup of the cyclic group C since all subgroups of G of order prime to p are conjugate by an element of P to a subgroup of C. Definition 1.7(a) now implies P must be cyclic by choosing c to be a non-trivial element of N, and C must commute with P. Hence G is cyclic, and it follows that G/N is GM.

Suppose now that N is a minimal normal subgroup of G contained in P. On taking the intersection of N with the lower central series of P, we see that there is a non-trivial subgroup N_0 of N which is normal in G such that the commutator group $[P, \mathrm{N}_0]$ is trivial. Since N is a minimal normal subgroup of G, this implies $N = \mathrm{N}_0 \subset \mathrm{C}(P)$. Because C has order prime to p, we see that if $1 \neq c \in C$, then Lemma 9.2 implies that $\mathrm{C}_{P/N}(c) = \mathrm{C}_P(c)N/N = \mathrm{C}_P(C)N/N = \mathrm{C}_{P/N}(C)$ is cyclic. So condition (a) of Definition 1.7 holds in G/N. In a similar way, Lemma 9.2 implies that condition (b) of Definition 1.7 holds for G/N because it holds for G. □

Completion of the proof of Theorem 1.8. – Suppose first that there is an injection $\phi_G :\to \mathrm{Aut}_k(k[[t]])$ having vanishing Bertin obstruction. Let $W(k)$ be the ring of infinite Witt vectors of k. Define $\Theta_C : C \to W(k)^*$ to be the inverse of the Teichmüller lift of the character $\theta : C \to k^*$ appearing in Theorem 6.6. Parts (b) and (d) of Theorem 6.6 then show that G is a GM group for k with respect to the restriction Θ of Θ_C to the maximal subgroup B of order dividing $p-1$.

Suppose now that G is GM for k with respect to Θ. Pick a faithful extension $\Theta_C : C \to W(k)^*$ of Θ from B to C. Let M be a positive integer. By induction on the length of a composition series for G, we can use Lemma A.2 and Proposition A.3 of Appendix 1 to construct an injection $\phi_G : G \to \mathrm{Aut}_k(k[[z]])$ which is GM with respect to Θ_C and such that

$$\iota(T) \geq \iota(\Gamma) + M \quad \text{and} \quad \iota(T) \equiv 0 \bmod p^M \tag{9.4}$$

if T is a non-trivial proper subgroup of the cyclic p-subgroup Γ of G. We will show that if M is chosen to be sufficiently large, then ϕ_G will satisfy all the conditions of Theorem 6.6. This theorem will then imply that ϕ_G has vanishing Bertin obstruction, and this will complete the proof of Theorem 1.8.

Consider first condition (a) of Theorem 6.6. By Theorem 2.3,

$$b_{T,P} = \frac{1}{[\mathrm{N}_P(T) : T]} \sum_{\Gamma \in S_P(T)} \mu([\Gamma : T])\iota(\Gamma)$$

$$= \frac{1}{[\mathrm{N}_P(T) : T]} \left(\iota(T) + \sum_{T \neq \Gamma \in S_P(T)} \mu([\Gamma : T])\iota(\Gamma) \right) \tag{9.5}$$

where $S_P(T)$ is the set of cyclic subgroups $\Gamma \subset P$ which contain T. So by making M sufficiently large, (9.4) will insure that each such $b_{T,P}$ will be larger than any specified integer and will be integral. Thus the Bertin obstruction of the restriction of ϕ to P vanishes by Proposition 2.1(ii)(b), so hypothesis (a) of Theorem 6.6 holds. We see also from this that since the constant $b'_{T,G}$ in Notation 6.2 depends only on G, we can insure that the inequality in condition (c)(ii) of Theorem 6.6 holds by making M sufficiently large.

It remains to check conditions (b), (c)(i) and (d) of Theorem 6.6.

Concerning condition (b), let t be a non-trivial element of C. Then C commutes with t; so since $G = P.C$ we conclude that $\mathrm{C}_G(t) = \mathrm{C}_P(t).C$. However, $\mathrm{C}_P(c) = \mathrm{C}_P(C)$ is a cyclic p-group since G is a GM group (see Definition 1.7). Hence $\mathrm{C}_G(t) = \mathrm{C}_P(C) \times C$ is cyclic and condition (b) of Theorem 6.6 holds.

Suppose now that T is a non-trivial cyclic subgroup of P as in conditions (c) and (d) of Theorem 6.6. Condition (c)(i) of this theorem holds by part (a) of Theorem 9.1. If $\mathrm{C}_C(T)$ is not trivial, condition d(i) of Theorem 6.6 holds by part (b) of Theorem 9.1. Suppose now that $\mathrm{C}_C(T)$ is trivial. The statements about θ in condition d(ii) of Theorem 6.6 hold because we constructed $\phi_G : G \to \mathrm{Aut}_k(k[[z]])$ to be GM with respect to Θ in the sense of Proposition A.3 of Appendix 1. It remains to prove the congruence

$$b'_{T,G} = \sum_{P \not\supset \Gamma \in S(T)} \mu([\Gamma : T]) \equiv 0 \mod \#\mathrm{N}_C(T)\mathbb{Z}$$

required in part d(ii) of Theorem 6.6. Part (c) of Theorem 9.1 shows that either $\#\mathrm{N}_C(T) = 1$ or the sum defining $b'_{T,G}$ is empty; so this congruence holds and the proof is complete. □

10. Examples and characterizations of GM groups

We begin with some examples.

THEOREM 10.1. – *Let G be the semi-direct product of a normal p-group P by cyclic subgroup C of order prime to p. Let B be the maximal subgroup of C of order dividing $p-1$.*

a. *If G is cyclic or a p-group then G is a GM-group.*
b. *If $\#B \leq 2$, and C acts freely on the nontrivial elements of P, then G is a GM-group.*
c. *G is not a GM group if it has any of the following properties:*
   i. (Green-Matignon) *G contains an abelian subgroup that is neither cyclic nor a p-group;*
   ii. *P is elementary abelian of order p^2, C has order dividing $p-1$ and C acts with two distinct nontrivial eigenvalues on P.*
   iii. *P is cyclic of order p, and C neither acts faithfully or trivially on P.*

iv. *P is extraspecial of order p^3 and exponent p, C is cyclic, $\#C$ does not divide $p+1$, and $\mathrm{C}_P(C) = \mathrm{C}(P)$. (Recall that a p-group P is extraspecial if $\mathrm{C}(P)$ is cyclic of order p and $P/C(P)$ is a non-trivial elementary abelian p-group.)*

Proof. – Parts (a) and (b) follow directly from 1.7. If conditions (i) (resp. (ii), resp. (iii)) of part (c) hold, then condition (a) (resp. (b), resp. (a)) of Definition 1.7 does not hold. Suppose now that condition (iv) of part (c) holds but that G is a GM group.

Let us first show that C must act faithfully on $P/\mathrm{C}(P)$. Suppose to the contrary that $c \in C$ is non-trivial and acts trivially on $P/\mathrm{C}(P)$. Because c commutes with $\mathrm{C}_P(C) = \mathrm{C}(P)$ and has order prime to p, c must act trivially on P. Then $P = \mathrm{C}_P(c) = \mathrm{C}_P(C)$ by part (a) of Definition 1.7, which contradicts the assumption that $\mathrm{C}_P(C) = \mathrm{C}(P)$ in part (iv). Therefore C must act faithfully on $P/\mathrm{C}(P)$.

We have $\dim_{\mathbb{Z}/p} P/\mathrm{C}(P) = 2$, and $\mathrm{C}(P) \cong \wedge^2(P/\mathrm{C}(P))$ as a C-module. We have assumed in (iv) of part (c) that the action of C on $\mathrm{C}(P)$ is trivial, so the determinant of the action of C on $P/\mathrm{C}(P)$ is trivial. Let c_0 be a generator of C. The characteristic polynomial of the action of c_0 on the two-dimensional $\mathbb{Z}/p$-vector space $P/\mathrm{C}(P)$ thus has the form $X^2 - aX + 1$ for some $a \in \mathbb{Z}/p$. If this polynomial does not split over $\mathbb{Z}/p$, its roots have multiplicative order dividing $p+1$. Since the action of C on $P/\mathrm{C}(P)$ is semi-simple, this would force the order of C to divide $p+1$, contradicting one of the assumptions in (iv). Therefore $X^2 - aX + 1$ splits over $\mathbb{Z}/p$. We conclude that as a representation of C over $\mathbb{Z}/p$, $P/\mathrm{C}(P)$ must be isomorphic to the direct sum of two characters ϕ_1 and ϕ_2 over $\mathbb{Z}/p$. Thus $\#C$ divides $p-1$. Now Lemma 9.3 and part (ii) imply that either $\phi_2 = \phi_1$ or we can order ϕ_1 and ϕ_2 so that ϕ_2 is trivial. The action of C on $\mathrm{C}(P) \cong \wedge^2(P/\mathrm{C}(P))$ is given by the character $\phi_1 \cdot \phi_2$, and we assumed this action is trivial in part (iv). Thus $\phi_1 = \phi_2^{-1}$. If $\phi_1 = \phi_2$ then ϕ_1 and C have order 2. However, we assumed that $\#C$ does not divide $p+1$, so $\#C = 2$ would force $p = 2$, which is impossible since $\#C$ is prime to p. Thus $\phi_1 = \phi_2^{-1}$ and ϕ_2 are distinct characters of C. Part (ii) now shows that $G/\mathrm{C}(P)$ is not a GM group, so G is not a GM group by Lemma 9.3. □

In fact, we now show that GM groups can be characterized as those groups of the form PC which do not contain subgroups of the form in Theorem 10.1(c).

THEOREM 10.2. – *Let $G = PC$ be a group with P the normal Sylow p-subgroup of G with C cyclic of order prime to p. Then G is a GM group if and only if it has no subgroup of the following types:*

1. *$\mathbb{Z}/p \times \mathbb{Z}/p \times \mathbb{Z}/r$, with r a prime distinct from p;*
2. *QE where Q is of order p, E is cyclic of order prime to p and E acts neither faithfully nor trivially on Q;*
3. *QE where Q is elementary abelian of order p^2, E is cyclic of order dividing $p-1$, $\mathrm{C}_E(Q) = 1$ and E does not act like a scalar on Q; or*
4. *QE where Q is extraspecial of exponent p and order p^3, E is cyclic of order e with e not dividing $p+1$ and $\mathrm{C}_Q(E) = \mathrm{C}(Q)$.*

We require the following lemmas, the first of which is an exercise beginning with the definition $[x, y] = x^{-1}y^{-1}xy$.

LEMMA 10.3. – *If H is a group and $z = [x, y]$ commutes with x for some $x, y \in H$, then $z^e = [x^e, y]$. If z commutes with both x and y, then $[x^e, y^f] = z^{ef}$.*

LEMMA 10.4. – *Let Q be a p-group with $B = \langle b \rangle$ a group of order dividing $p-1$ acting on Q. There is a filtration:*

$$1 = Q_0 < Q_1 < \cdots < Q_m = Q,$$

such that:

a. *each Q_i is normal in Q and B-invariant;*
b. *each quotient Q_i/Q_{i-1} is cyclic of order p;*
c. *there is a unique root of unity e_i of order dividing $p-1$ in $\mathbb{Z}_p$ such that there is an element $x_i \in Q_i$ for which $x_i Q_{i-1}$ generates Q_i/Q_{i-1} and $bx_ib^{-1} = x_i^{e_i}$, where $x_i^{e_i}$ is well defined because x_i has non-trivial p-power order.*

Proof. – Using the Frattini subgroup of Q and induction on the order of Q we can reduce to the case in which Q is an elementary abelian p-group, in which case the lemma is obvious. □

Note that one can modify the proof so that the filtration will pass through any given normal subgroup of Q that is B-invariant.

Proof of Theorem 10.2. – Having no subgroup of the form (1) or (2) is equivalent to the condition that if $1 \neq c \in C$, then $\mathrm{C}_P(C) = \mathrm{C}_P(c)$ is cyclic. This is the condition (a) in the definition of GM groups (see Definition 1.7).

So it suffices to show that if G satisfies condition (a) of Definition 1.7, then it is a GM group if and only if it does not contain a subgroup as in (3) or (4). By condition (b) of Definition 1.7, a GM group has no subgroups as in (3) or (4). (For (4), see Theorem 10.1.c(iv) and Lemma 9.3.) Thus it remains to show that if G is not a GM group, it contains such a subgroup.

So assume that G is not a GM group but satisfies condition (a) of Definition 1.7. Therefore condition (b) of Definition 1.7 does not hold. By passing to counterexample of minimal order, we may assume that C has order at least 3 and dividing $p-1$. We will use in what follows that fact that since G is a minimal order counterexample, every subquotient of G which is not G itself must be a GM group because of Lemma 9.3. In particular condition (b) of Definition 1.7 holds for all proper subquotients of G but not for G itself.

Let Q be a C-stable subquotient of P, which may equal P. Let $B = C$ in Lemma 10.4, and let $1 = Q_0 < Q_1 < \cdots < Q_m = Q$, the x_i and the e_i be as in this lemma. If there are indices $i \neq j$ such that e_i, e_j and 1 are distinct, then C acts on x_i and x_j via distinct non-trivial characters, so that $C.Q$ cannot be a GM-group because this violates condition (b) of Definition 1.7. Thus if Q is a proper subquotient of P, there is at most one e_i different from 1; we let $e(Q)$ be this e_i if it exists, and we let $e(Q) = 1$ otherwise. We claim:

(10.6) If $Q = P$ then at least two distinct e_i are different from 1.

Suppose to the contrary that $Q = P$ and that there is at most one e_i which is different from 1. It will suffice to show that condition (b) of Definition 1.7 holds, since this will be a contradiction. If all the e_i equal 1, then C commutes with all the x_i and thus with $Q = P$,

so $\mathrm{C}_P(C) = P$ and condition (b) holds automatically. If all the e_i which are different from 1 are equal and there is at least one such e_i, we define $\Theta : B \to \mathbb{Z}_p^*$ by $\Theta(b) = b^{e_i}$ for any such e_i, where we have set $B = C$. If T is cyclic subgroup of P such that $\mathrm{C}_C(T)$ is trivial, then by considering the smallest i such that $T \subset Q_i$ and the image of T in Q_i/Q_{i-1} we see that condition (b) of Definition 1.7 holds for T. This contradiction proves the claim (10.6).

Let $P^p[P,P]$ be the Frattini subgroup of P, and let $P(p) = P/(P^p[P,P])$ be the p-Frattini quotient. If $P(p)$ is cyclic, then P is cyclic, and the action of C on P must be through a single character, contrary to the fact that we have shown there must be at least two distinct e_i different from 1 when $Q = P$. Thus $P(p)$ is a $\mathbb{Z}/p$-vector space of dimension at least 2, and the action of $C = B$ on $P(p)$ can be diagonalized over $\mathbb{Z}/p$ since $\#C$ divides $p-1$. By pulling back two C-eigenspaces, we conclude that there are C-stable normal subgroups P_1 and P_2 in P such that $P/(P_1 \cap P_2)$ is elementary abelian of order p^2 and isomorphic as a C-module to a sum of two characters ϕ_1 and ϕ_2 of P.

If $P_1 \cap P_2$ is trivial, so that $P = P/(P_1 \cap P_2)$, we have seen that ϕ_1 and ϕ_2 must be distinct and non-trivial (since there are at least two distinct e_i which are different from 1). In this case $G = PC$ satisfies the conditions in part (3) of Theorem 10.2.

Suppose now that $P_1 \cap P_2$ is non-trivial. If C acts non-trivially on $P_1 \cap P_2$, then we conclude that $e(P_1) = e(P_2) = e(P_1 \cap P_2)$ in the above notation, since P_1, P_2 and $P_1 \cap P_2$ are proper subquotients of P. We have a C-isomorphism $P_1/(P_1 \cap P_2) \to P/P_2$. Since $P_1 \cap P_2$ contains $P^p[P,P]$ we can now find a filtration

$$1 = Q_0 < Q_1 < \cdots < Q_{m-2} = P_1 \cap P_2 < Q_{m-1} = P_2 < Q_m = P$$

as in Lemma 10.4 such that at most one non-trivial character of C arises from a C-module quotient Q_i/Q_{i-1}. This contradicts that at least two distinct e_i different from 1 must arise when we set $Q = P$. We conclude that C acts trivially on $P_1 \cap P_2$, so $P_1 \cap P_2 \subset \mathrm{C}_P(C)$, where $\mathrm{C}_P(C)$ is cyclic because we have assumed condition (a) of Definition 1.7 holds. Thus P/P_1 and P/P_2 must define distinct non-trivial characters ϕ_1 and ϕ_2 of C in order for them to be two distinct non-trivial e_1 and e_2 associated to setting $Q = P$. We now use Lemma 10.4 to find $x_i \in P_i$ such that $bx_ib^{-1} = x_i^{e_i}$ if b is a generator of $B = C$ and for which $x_i(P_1 \cap P_2)$ generates the cyclic group $P_i/(P_1 \cap P_2)$ of order p. Then $x_i^p \in P_1 \cap P_2$ so C acts trivially on x_i^p. Thus

$$x_i^{pe_i} = (bx_ib^{-1})^p = bx_i^pb^{-1} = x_i^p$$

so $x_i^p = 1$ because e_i is a non-trivial $(p-1)^{st}$ root of 1 in $\mathbb{Z}_p$. Let us check that x_i must centralize each $\gamma \in P_1 \cap P_2$. Since $x_i\gamma x_i^{-1} \in P_1 \cap P_2 \subset \mathrm{C}_P(C)$ we have

$$x_i^{e_i}\gamma x_i^{-e_i} = (bx_ib^{-1})(b\gamma b^{-1})(bx_ib^{-1})^{-1} = b(x_i\gamma x_i^{-1})b^{-1} = x_i\gamma x_i^{-1}$$

so $x_i^{e_i-1}$ centralizes γ, from which it follows that x_i centralizes γ. This implies that $P_1 \cap P_2$ is central in G, since we have shown that C commutes with $P_1 \cap P_2$ and because G is generated by C, $P_1 \cap P_2$, x_1 and x_2. Thus $z = [x_1, x_2] \in P_1 \cap P_2$ is central in G, so Lemma 10.3 shows $z^p = [x_1^p, x_2] = 1$ because $x_1^p = 1$. The group generated by C, x_1, x_2 and z is now a subgroup of G of the kind in part (4) of Theorem 10.2, which completes the proof. □

If the subgroup B (in the notation above) has order bigger than 2, the structure of GM groups is quite limited, as we show in the next theorem.

THEOREM 10.5. – *Let $G = PC$ be a GM-group with $\#B > 2$, where B is the maximal subgroup of C order dividing $p-1$. Let $D = \mathrm{C}_P(C)$. Then the derived subgroup $H = [G,G]$ of G is abelian, C acts freely on the nonidentity elements of H, G is the semi-direct product $H.(C \times D)$ and B acts as a scalar on H. Conversely, any such group is a GM group.*

Proof. – We prove the first statement. By coprime action, we have that $P = D[C,P]$ and $[C,H] = [C,P]$ (see [10, 5.3.5]). Since D normalizes both C and P and since $G = [C,P]DC$, it follows that $[C,P]$ is normal in G. Clearly, $[C,P]$ is contained in the derived subgroup of G. On the other hand C and P commute modulo $[C,P]$, whence $G/[C,P]$ is abelian. Thus $[C,P] = H$.

We next claim that H is abelian. Suppose not. Then we can pass to the quotient $H/[H,[H,H]]$ and so assume that H is nilpotent of class 2. Let $T = H/\Phi(H)$, where $\Phi(H)$ is the Frattini subgroup of H. Let b be a generator for B. Then b is diagonalizable on T and we may choose a basis $y_1, \ldots, y_r$ of T with each y_i an eigenvector for b. We may lift y_i to an element $x_i \in H$ with b normalizing each $\langle x_i \rangle$. Since $H = [C,H]$, $T = [C,T]$ and so b centralizes none of the y_i. Since G is a GM-group, this implies that $bx_ib^{-1} = x_i^{\Theta(b)}$ for each i. Thus, by Lemma 10.3, $b[x_i,x_j]b^{-1} = [x_i,x_j]^{\Theta(b)^2}$ for each i,j. Since the order of b is greater than 2 and Θ is faithful, $\Theta(b)^2 \neq \Theta(b)$ and $\Theta(b) \neq 1$. By definition, this implies that $[x_i,x_j] = 1$, whence H is abelian.

Again by coprime action on abelian groups, we have (see [10, 5.2.3]) that $H = \mathrm{C}_H(C) \times [C,H]$ and so $\mathrm{C}_H(C) = 1$, using $H = [C,H]$. Thus C acts fixed point freely on the nontrivial elements of H. We have already noted that $G = HDC = H.(C \times D)$.

Now assume that G is as described. If $1 \neq c \in C$, then $\mathrm{C}_P(c) = D = \mathrm{C}_P(C)$ is cyclic. Moreover, we see that c normalizes a cyclic subgroup if and only if it centralizes it or acts via the character given by its action on H. Thus G is a GM-group. □

EXAMPLE 10.6. – Suppose P is cyclic. Since C is cyclic of order prime to p, it acts faithfully on P if and only if it acts faithfully on the cyclic subgroup Q of order p in P. We conclude from Theorem 10.2 that when P is cyclic, G is a GM group if and only if it is cyclic or C acts faithfully on Q; the latter condition is equivalent to the statement that the center of G is trivial. If $P = Q$ has order p, it follows from [26] (for cyclic G) and from [5, Theorem 2.1] (for non-cyclic G) that if G is a GM group then it is in fact a weak local Oort group.

11. Reducing the proofs of Theorems 1.2 and 1.5 to particular groups

In this section we recall Propositions 3.1 and 4.2 of [8], which limit the possible cyclic by p-groups which has no quotients of certain kinds. This will be used to limit the possible isomorphism classes of Bertin and KGB groups. We will assume that $G = P.C$ is a finite group which is the semi-direct product of a normal p-group P with a cyclic prime to p-group C. Let C_n be a cyclic group of order n.

THEOREM 11.1. – *Let p be an odd prime. Assume that G has no homomorphic image of the following types:*

1. *$C_p \times C_p$;*

2. *$E.C_m$, where E is an elementary abelian p group, $p \nmid m \geq 3$, and C_m acts faithfully and irreducibly on E;*
3. *$E.C_2$ where $E = C_p \times C_p$, and C_2 acts on E by inversion;*
4. *$D_{2p} \times C_\ell$ for some prime number $\ell > 2$ (including the possibility that $\ell = p$);*
5. *$E.C_4$ where $E = C_p$, and a generator of C_4 acts on E by inversion.*

Then G is either cyclic or dihedral of order $2p^a$ for some a.

We recall some notation and facts about 2-groups. A generalized quaternion group of order $2^a, a \geq 3$, is given by $Q_a = \langle x, y | x^{2^{a-1}} = 1, yxy^{-1} = x^{-1}, y^2 = x^{2^{a-2}} \rangle$. These are the only noncyclic 2-groups that contain a unique involution.

The semidihedral group of order $2^a, a > 3$ is denoted by SD_a and has presentation $\langle x, y | x^{2^{a-1}} = 1, y^2 = 1, yxy = x^{-1+2^{a-2}} \rangle$. Note that if G is dihedral, semidihedral or generalized quaternion then $G/[G,G]$ is elementary abelian of order 4.

THEOREM 11.2. – *Suppose $p = 2$. Assume that G has no homomorphic image of the following types:*

1. *$E.D$, where E is a non-trivial elementary abelian 2-group, D is cyclic of odd order at least 5 and D acts irreducibly on E;*
2. *$E.D$, where E is elementary abelian of order 16, D has order 3 and acts without fixed points on E;*
3. *$E.D$ where $E = \mathbb{Z}/4 \times \mathbb{Z}/4$, D has order 3 and acts faithfully on E;*
4. *$E.D$, where E is elementary abelian of order 8 and D acts faithfully on E with D of order 1 or 3 (note this is isomorphic to $A_4 \times \mathbb{Z}/2$ or E);*
5. *$E \times C$ where E is elementary abelian of order 4 and C has prime order;*
6. *$E.C$ where C is cyclic of order $3p$ with p an odd prime and E is elementary abelian of order 4 with C acting nontrivially on E; or*
7. *$\mathbb{Z}/4 \times \mathbb{Z}/2$.*

Then G is cyclic, A_4, or $SL_2(3)$, or $G = S$ is a dihedral, semidihedral or generalized quaternion 2-group.

12. Some groups which are not almost Bertin groups

We assume as before that k is an algebraically closed field of characteristic $p > 0$.

PROPOSITION 12.1. – *Let G be the semidirect product of an elementary abelian p-group E of order $q > 1$ with a cyclic group C_m of order m prime to p.*

a. *Suppose $q > p$. Then G is not an almost Bertin group for k unless $p = 2$ and $q = 4$. If $(p,q) = (2,4)$, then G is not a weak Bertin group for k and not an almost Bertin group for k unless $m \in \{1,3\}$ and C_m acts faithfully on E, in which case G is isomorphic to either C_2^2 or A_4.*
b. *Suppose $(p,q) = (2,4)$ and that G is isomorphic to A_4. Then for each integer $M \geq 0$, there is an integer $j \geq M - 1$ such that $j \equiv 1$ mod 4 and there is an injection $\phi : G \to \mathrm{Aut}_k(k[[t]])$ with the property that $G_1 = E = G_j \neq G_{j+1}$.*
c. *Suppose $q = p$, $m \geq 3$ and that C_m acts faithfully on E. Then G is not an almost Bertin group for k.*

Proof. – Let T be a subgroup of order p in E, and recall that $S(T)$ is the set of cyclic subgroups of G containing T. Since E is the unique p-Sylow subgroup of G, and E is elementary abelian, each $\Gamma \in S(T)$ which is different from T has order divisible by some prime different from p. Thus $\iota(\Gamma) = 1$ for such Γ. Therefore Theorem 2.3 gives

$$b_T = \frac{1}{[\mathrm{N}_G(T) : T]} \sum_{\Gamma \in S(T)} \mu([\Gamma : T])\iota(\Gamma) = \frac{\iota(T) + c(T)}{[\mathrm{N}_G(T) : T]} \tag{12.1}$$

where

$$c(T) = \sum_{T \neq \Gamma \in S(T)} \mu([\Gamma : T]) \tag{12.2}$$

is independent of the ramification filtration of G.

We now suppose $q > p$, so that $p^2|q$. Here $E \subset \mathrm{N}_G(T)$ since $T \subset E$ and E is elementary abelian of order q. Thus q/p is a positive power of p dividing $[\mathrm{N}_G(T) : T]$. It follows that to show G is not a Bertin group for k, it will suffice to show that for each integer $M \geq 1$, there is an embedding $\phi : G \to \mathrm{Aut}_k(k[[t]])$ such that $-a_\phi(\tau) \geq M$ for all non-trivial elements $\tau \in G$ of p-power order, and such that $\iota(T) \not\equiv -c(T) \bmod q/p$ for some subgroup T of order p in E.

The condition on $-a_\phi(\tau)$ is equivalent to requiring that if j is the first jump in the wild ramification filtration of G, so that $G_1 = G_j \neq G_{j+1}$, then $j \geq M - 1$. Suppose that in addition we arrange that T is not contained in G_{j+1}. Then $\iota(T) = j + 1$, so we will be done if we can also arrange that $j + 1 \not\equiv -c(T) \bmod q/p$. We may assume that k is the algebraic closure of $\mathbb{Z}/p$, since if we can construct an extension of the required kind in this case we can simply take its base change to an arbitrary algebraically closed field of characteristic p.

To construct a ϕ of the required kind, choose a power q' of p such that $\mathbb{F}_{q'}$ contains a primitive m^{th} root of unity, and let $L = \mathbb{F}_{q'}((y))$ for an indeterminate y. Letting $z = y^{1/m}$ we see that $N = L(z)$ is a cyclic totally and tamely ramified extension of L, and the integral closure of $O_L = \mathbb{F}_{q'}[[y]]$ in N is $O_N = \mathbb{F}_{q'}[[z]]$. We fix an identification of $H = \mathrm{Gal}(N/L)$ with C_m.

The group ring $(\mathbb{Z}/p)[C_m]$ is semi-simple and acts on $N^*/(N^*)^p$. For each integer $i \geq 1$ the natural map

$$W_i = \frac{1 + z^i O_N}{1 + z^{i+1} O_N} \to \frac{N^*}{(N^*)^p (1 + z^{i+1} O_N)} \tag{12.3}$$

is injective if $i \not\equiv 0 \bmod p$ and is the trivial homomorphism otherwise. The group $H = \mathrm{Gal}(N/L) \cong C_m$ acts on the one-dimensional $\mathbb{F}_{q'}$ vector space $\mathbb{F}_{q'} \cdot z$ via a faithful character $\chi : H \to \mathbb{F}_{q'}^*$. Thus H acts on the one-dimensional $\mathbb{F}_{q'}$ vector space

$$W_i = \frac{1 + z^i O_N}{1 + z^{i+1} O_N} \cong \frac{z^i O_N}{z^{i+1} O_N}$$

via the character χ^i. As a $(\mathbb{Z}/p)[C_m]$-module, W_i is the direct sum of finitely many copies of the unique simple $(\mathbb{Z}/p)[C_m]$-module V_i whose character is the sum of the conjugates of χ^i over $\mathbb{Z}/p$. Each simple $(\mathbb{Z}/p)[C_m]$-module is isomorphic to V_i for some $i \not\equiv 0 \bmod p$. Finally W_i and W_{i+m} are isomorphic, so V_i and V_{i+m} are isomorphic.

Suppose first that $q/p > 2$, and recall that we have assumed $p^2|q$. There is a direct sum decomposition $E = T_0 \oplus T_1$ of E as a $(\mathbb{Z}/p)[C_m]$-module in which T_0 is a simple

$(\mathbb{Z}/p)[C_m]$-module. Let T be an order p subgroup of T_0. We claim there is an integer j such that $j \not\equiv 0 \bmod p$, $1+j \not\equiv -c(T) \bmod q/p$, T_0 is isomorphic to V_j and $j \geq M-1$. The condition that $j \not\equiv 0 \bmod p$ removes q/p^2 residue classes mod q/p, while $1+j \not\equiv -c(T) \bmod q/p$ removes at most one more residue class mod q/p. Since $q/p > 2$ by assumption, we have $q/p - q/p^2 - 1 = (q/p)(1-1/p) - 1 > 0$ so both of these congruences may be satisfied. The condition that T_0 is isomorphic to V_j is a condition on j mod m. Since m is prime to p we can find arbitrarily large j satisfying all three congruences, as claimed.

The group $N^*/(N^*)^p$ is a semi-simple $(\mathbb{Z}/p)[C_m]$-module with a descending filtration whose terms are given by the image of $1+z^iO_N$ for $i \geq 1$ prime to p. The successive quotients in this filtration are the W_i above. Since V_j is by construction isomorphic to T_0, it follows from the semi-simplicity of $N^*/(N^*)^p$ and of E that we can find an H-stable subgroup U of N^* containing $1+z^hO_N$ for some $h \geq 1$ with the following properties. There is an H-equivariant isomorphism $N^*/(U \cdot (N^*)^p) \to E$ which gives rise to surjections $1+z^jO_N \to E = T_0 \oplus T_1$ and $1+z^{j+1}O_N \to T_1$. Let F be the extension of N corresponding to $U \cdot (N^*)^p$ by local class field theory. Then F/L is a Galois extension, and there is an isomorphism $\mathrm{Gal}(F/L) = G$ such that $G_1 = G_j$ and $G_{j+1} \neq G_j$ does not contain $T_0 \supset T$. The existence of this G-extension shows that G is not an almost Bertin group for k if $q/p > 2$.

Suppose now that $q/p = 2$, so that $p = 2$ and $q = 4$. Let $C_{m'} \subset C_m$ be the kernel of the action of C_m on $E = (C_2)^2$. Then $C_{m'}$ is in the center of G, and C_m/C'_m is a cyclic group of odd order acting faithfully on $E = (C_2)^2$. It follows that $G/C_{m'}$ is either isomorphic to $E = (C_2)^2$ or to A_4.

Suppose first that $m' = 1$ and $(p,q) = (2,4)$. In this case, G is isomorphic to either $E = (C_2)^2$ or to A_4. All that we must prove for such G is that part (b) of Proposition 12.1 holds when G is isomorphic to A_4. Thus we now assume $m = 3$. With the above notation, we can find an integer $j \geq M-1$ such that $j \equiv 1 \bmod 4$, and V_j is faithful as a module for $C_m = C_3 = H$. (The last condition is equivalent to $j \not\equiv 0 \bmod 3$.) The above construction now produces an example in which $E = G_1 = G_j \neq G_{j+1}$, which is all that is required when $m' = 1$.

We now suppose $m' > 1$, $(p,q) = (2,4)$ and that k is an arbitrary algebraically closed field of characteristic p. Then $\mathrm{C}_G(C_{m'}) = G \neq C_{m'}$. If $G/C_{m'}$ is isomorphic to $E = (C_2)^2$, then with the notation of Definition 3.1,

$$\psi(\{e\}, \mathrm{C}_G(C_{m'})/C_{m'}) = 1 + 3\mu(2) = -2.$$

Otherwise $G/C_{m'}$ is isomorphic to A_4 and

$$\psi(\{e\}, \mathrm{C}_G(C_{m'})/C_{m'}) = 1 + 3\mu(2) + 4\mu(3) = -6.$$

It now follows from Corollary 3.3 that there is no local G-cover for which the Bertin obstruction vanishes, so that G is not a weak Bertin group for k. We can construct examples of such covers in which the first jump in the wild ramification is arbitrarily large by the same arguments used earlier, so this completes the proof of case (a) of Proposition 12.1.

We now suppose that $q = p$, $m \geq 3$ and that C_m acts faithfully on $E = C_p$. Let $T = E$. Then $S(T) = \{T\}$, since the image of T in $G/E \cong C_m$ has to act trivially on $T = E$. We have $\mathrm{N}_G(T) = G$. So Theorem 2.3 gives

$$b_T = \frac{\iota(T)}{m}. \tag{12.4}$$

Therefore we just have to produce a $\phi : G \to \mathrm{Aut}_k(k[[t]])$ such that when j is the first (and only) jump in the wild ramification of G, j is arbitrarily large and $j+1 = \iota(T)$ is not congruent to 0 mod m. The action of C_m on $E = C_p$ is via some faithful character of C_m, and $\mathrm{Aut}(C_m)$ acts transitively on these faithful characters. Thus by varying the identification of $\mathrm{Gal}(N/L) = \mathrm{Gal}(\mathbb{F}((y^{1/m}))/\mathbb{F}(y))$ with C_m in our earlier construction of G extensions, we can produce an example in which j is any positive integer such that $j \not\equiv 0 \bmod p$ and j is relatively prime to m. Since m is prime to p, we can find arbitrarily large j such that $j \not\equiv 0 \bmod p$ and $j \equiv 1 \bmod m$. Since $m \geq 3$, such j will have $j+1 \not\equiv 0 \bmod m$, so we are done. □

EXAMPLE 12.2. – Suppose $p > 2$ and that $G = C_p \times C_p$, so that $q = p^2$ and $m = 1$ in Proposition 12.1. Thus G is not an almost Bertin group. Nevertheless, there exists a ϕ for which the Bertin obstruction vanishes. Namely, each non-trivial $T \in \mathscr{C}$ has order p, and (12.1) shows $b_T = (1 + \iota(T))/p$. For all positive integers $a \equiv -1 \bmod p$, we can construct an injection $\phi : G \to \mathrm{Aut}_k(k[[t]])$ such that $\iota(T) = a$ for all non-trivial subgroups T of G. Thus the Bertin obstruction for such a ϕ vanishes. Moreover, Pagot proves in [22] that when $a = p - 1$, one cannot lift ϕ to characteristic 0.

LEMMA 12.3. – *Suppose that p is odd and that G is the semidirect product of a normal cyclic subgroup E of order p with a cyclic group $C_{2\ell}$ of order 2ℓ, where ℓ is a prime different from p, with a generator of $C_{2\ell}$ acting on E by inversion. Then there is a non-trivial cyclic subgroup T of G such that the constant b_T in Proposition 2.1 is not integral. Therefore G is not a weak Bertin group for k, not an almost Bertin group for k, and not a local Oort group for k.*

Proof. – Suppose first that $\ell = 2$ and that σ is a generator for $C_{2\ell} = C_4$. Let $T = \{e, \sigma^2\}$, so that T is in the center of G and $\mathrm{N}_G(T) = \mathrm{C}_G(T) = G$. The group $\mathrm{C}_G(T)/T$ is isomorphic to the dihedral group D_{2p}, and $\psi(\{e\}, \mathrm{C}_G(T)/T) = 1 + \mu(p) + p\mu(2) = 1 - 1 - p = -p$. Therefore 3.3 implies no local G cover has vanishing Bertin obstruction. To show that G is not a local almost Bertin group for k, it will now be enough to prove that for each integer $M \geq 0$, there is an injection $\phi : G \to \mathrm{Aut}_k(k[[t]]))$ such that $-a_\phi(\tau) \geq M$ for all non-trivial elements $\tau \in G$ of p-power order. Let $q = p^2$ and let L/K be the cyclic quartic extension $\mathbb{F}_q((z))/\mathbb{F}_q((t))$ for which $z^4 = t$. One can construct a ϕ with the above properties by considering $L^*/(L^*)^p$ as a module for $(\mathbb{Z}/p)[\mathrm{Gal}(L/K)]$ and by applying the class field theory arguments used in the proof of Proposition 12.1; we will leave the details to the reader.

In the other case of Lemma 12.3, $G = (E.C_2) \times C_\ell$ where $\ell > 2$ is prime, $p \neq \ell$ and C_2 acts on $E = C_p$ by inversion. Let T be the cyclic subgroup $E \times C_\ell \cong C_{p\ell}$. Then T has index 2 in G, so $\mathrm{N}_G(T) = G$ while $\mathrm{C}_G(T) = T$. Hence $\psi(T, \mathrm{C}_G(T)) = 1$, so Corollary 3.3 shows that no local G cover has vanishing Bertin obstruction. We can construct injections $\phi : G \to \mathrm{Aut}_k(k[[t]])$ leading to such covers such that $-a_\phi(\tau)$ is arbitrarily large for all non-trivial elements $\tau \in G$ of p-power order by the same local class field theory arguments used in previous cases. This completes the proof. □

COROLLARY 12.4. – *Suppose that $p > 2$, that G is a semi-direct product of a non-trivial p-group with a cyclic prime-to-p group, and that G is an almost Bertin group for k. Then G must be either a cyclic p-group or a dihedral group D_{2p^a} of order $2p^a$ for some $a \geq 1$.*

Proof. – Suppose the corollary is false for some group G. By Theorem 11.1, G has a quotient H having one of the forms (1)-(5) there. Forms (1)-(3) are not almost Bertin groups by Proposition 12.1, and similarly for (4) and (5) by Lemma 12.3. So there is a quotient H of G that is not an almost Bertin group for k. Thus G is not an almost Bertin group by Corollary 5.6, and this is a contradiction. □

COROLLARY 12.5. – *Suppose that $p = 2$. Let G be a group which is not cyclic, and which is one of the groups described in items (1), (2), (4), (5) or (6) of Theorem 11.2. Then G is not an almost-Bertin group for k.*

Proof. – The only G described in items (1), (2), (4), (5) or (6) of Theorem 11.2 which are not covered by Proposition 12.1(a) are those described in item (1) of Theorem 11.2 for which the elementary abelian $p = 2$ group E is of order 2. However, these G are cyclic, so Corollary 12.5 follows. □

PROPOSITION 12.6. – *Suppose $p = 2$ and that as in item (3) of Theorem 11.2, G is isomorphic to the semi-direct product $E.C_3$ where the normal subgroup E is isomorphic to $(\mathbb{Z}/4)^2$ and the cyclic group C_3 of order 3 acts faithfully on E. Then G is not an almost Bertin group for k.*

Proof. – Since the ramification groups G_i are normal in G, there is an integer $r \geq 1$ such that $G = G_0 \supset G_1 = E = \cdots = G_r \neq G_{r+1}$ and $G_{r+1} \subset E^2 = (2\mathbb{Z}/4\mathbb{Z})^2$. Let T be a cyclic subgroup of order 4 in E. Then $\mathrm{N}_G(T) = E$ and there are no cyclic subgroups of G which properly contain T. Now Theorem 2.3 gives

$$b_T = \frac{1}{[\mathrm{N}_G(T) : T]}\iota(T) = \frac{r+1}{4}. \tag{12.5}$$

Following [28, §IV.3] we let G_u for $u \geq 0$ be G_i when i is the smallest integer $\geq u$, and we define

$$\varphi(u) = \int_0^u \frac{dt}{[G_0 : G_t]}.$$

The upper ramification group $G^{\varphi(u)}$ then equals G_u. Since G_0 contains E with index 3, we find that $\varphi(u) = u/3$ for $0 \leq u \leq r$. Thus $G^{r/3} = E$ and $G^{r/3+\epsilon}$ is contained in E^2 if $\epsilon > 0$. The group E^2 is normal in G, and $H = G/E^2$ is isomorphic to A_4. By [28, Prop. IV.14], the image of G^ν in H is H^ν for all $\nu \geq 0$. Thus $H^{r/3} = E/E^2$ and $H^{r/3+\epsilon} = \{e\}$ for $\epsilon > 0$. By comparing the lower and upper ramification groups of H, we find that $H_r = E/E^2$ while $H_{r+1} = \{e\}$.

Suppose now that $M \geq 0$ is given. To show that G is not an almost Bertin group for k, it will suffice to show that there is $\phi : G \to \mathrm{Aut}_k(k[[t]])$ such that when r is defined as above, $r \geq M - 1$ and $r + 1 \not\equiv 0 \bmod 4$. This is because (12.5) will then show b_T is not integral, so the Bertin obstruction of ϕ does not vanish by Proposition 2.1.

To construct such a ϕ, we apply Proposition A.3 of Appendix 1 to the surjection $G \to H = A_4$. This produces an integer M' depending on M for which we may use the following argument. Replace M by M' in Proposition 12.1 and let r be the integer j in part (b) of Proposition 12.1. Proposition 12.1 then produces an injection $\psi : H = A_4 \to \mathrm{Aut}_k(k[[z]])$ such that $H_1 = H_r \neq H_{r+1}$ for some integer $r \geq M' - 1$ such that $r + 1 \equiv 2 \bmod 4$. Proposition A.3 now produces an injection $\phi : G \to \mathrm{Aut}_k(k[[t]])$ as follows. The H-cover

associated to ψ is the quotient of the local G-cover associated to ϕ, and $-a_\phi(\tau) \geq M$ if τ is a $p = 2$-torsion element of G. We now see from the above computation of upper and lower ramification groups that r is the first jump in the wild lower ramification filtration of G, so we are done. □

PROPOSITION 12.7. – *Suppose $p = 2$ and that as in item (7) of Theorem 11.2, G is isomorphic to $(\mathbb{Z}/4) \times (\mathbb{Z}/2)$. Then G is not an almost Bertin group for k.*

Proof. – Suppose $M \geq 1$. Let $H = \mathbb{Z}/2$ be the second factor in G, so that there is a split surjection $\pi : G \to H$. Let M' be an integer having the properties for M and $G \to H$ described in Proposition A.3 of Appendix 1. We can construct an H-extension N/L of $L = k((y))$ such that the first (and only) jump in the lower numbering ramification filtration of H occurs at an integer $r \geq M' - 1$ such that $r \equiv 1 \bmod 4$. By Proposition A.3(i), there is an injection $\phi : G \to \mathrm{Aut}_k(k[[t]])$ which defines a local G-cover of $L = k((y))$ having N/L as the quotient cover associated to $\pi : G \to H$. By Proposition A.3(ii), we can furthermore require that $a_\phi(\tau) \geq r + 1$ for all non-trivial elements $\tau \in \ker(\pi)$, since all such τ have order a power of $p = 2$. This means that $\ker(\pi) \subset G_r$. Since $\pi(G^\nu) = H^\nu$ for all ν, we conclude that $\pi(G^r) = H$ while $\pi(G^{r+\epsilon}) = \{e\}$ for $\epsilon > 0$. Now $\ker(\pi) \subset G_r \subset G^r$, so we conclude that $G^r = G$, while $G^{r+\epsilon} \subset \ker(\pi)$ for $\epsilon > 0$. The first jumps in the lower and upper ramification filtrations of G are equal, so we deduce from this that $G_r = G$ while $G_{r+1} \subset \ker(\pi)$. When we now view $H = \mathbb{Z}/2$ as a subgroup of $G = (\mathbb{Z}/4) \times H$, we see that $\iota(H) = r + 1$. Furthermore, $\mathrm{N}_G(H) = G$, while there are no cyclic subgroups of G which property contain H. Thus

$$b_H = \frac{1}{[\mathrm{N}_G(H) : H]}\iota(H) = \frac{r+1}{4}.$$

Since we arranged that $r \equiv 1 \bmod 4$, this proves b_H is not integral, so the Bertin obstruction of $\phi : G \to \mathrm{Aut}_k(k[[t]])$ is non-trivial by Proposition 2.1. Because $G_r = G$ and $r \geq M - 1$, this completes the proof that G is not an almost Bertin group for k. □

COROLLARY 12.8. – *To complete the proof of Theorem 1.2, it will suffice to show the following:*

a. *The groups listed in items (1)–(4) of Theorem 1.2 are KGB groups for k.*
b. *When $p = 2$, neither the quaternion group Q_8 nor the group $\mathrm{SL}_2(3)$ is a Bertin group for k.*
c. *When $p = 2$, no semi-dihedral group of order at least 16 is a Bertin group for k.*

Proof. – If p is odd, this follows from Corollary 12.4, since KGB groups are Bertin and hence almost Bertin. Suppose now that $p = 2$. If we grant the results stated in parts (b) and (c) of Corollary 12.8, then Corollary 12.5 together with Propositions 12.6 and 12.7 show that none of the groups listed in items (1)–(7) of Theorem 11.2 are Bertin groups for k, and that Q_8, $\mathrm{SL}_2(3)$ and semi-dihedral groups of order ≥ 16 are not Bertin groups for k. By Corollary 5.6, no group G that has one of these groups as a quotient can be a Bertin group for k. Thus Theorem 11.2 shows that if G is a cyclic-by-p group which is a Bertin group for k for $p = 2$, it must be cyclic, dihedral, generalized quaternion of order at least 16, or A_4.

Thus a proof that all of these groups are in fact KGB groups for k will complete the proof of Theorem 1.2. □

13. Reduction to quasi-finite residue fields

To further apply classfield theory to study Artin characters, it is useful to be able to replace the algebraically closed field k by a quasi-finite field. We first recall the definition of such fields from [28, §XIII.2].

DEFINITION 13.1. – A field L of characteristic $p > 0$ is *quasi-finite* if it has the following properties:

a. L is perfect;
b. There is an automorphism $F \in \mathrm{Gal}(L^{\mathrm{sep}}/L)$ of the separable closure L^{sep} of L such that the map $\hat{\mathbb{Z}} \to \mathrm{Gal}(L^{\mathrm{sep}}/L)$ defined by $\nu \mapsto F^{\nu}$ is an isomorphism of profinite groups.

PROPOSITION 13.2. – *Suppose that G is a finite group, k is an algebraically closed field of characteristic p and that $\phi : G \to \mathrm{Aut}_k(k[[t]])$ is an injection. There is a subfield k' of k of finite type over the prime field $\mathbb{F}_p$ such that ϕ is the base change from k' to k of a unique injection $\phi' : G \to \mathrm{Aut}_{k'}(k'[[t]])$. There is a quasi-finite field L containing k' such that ϕ' induces an injection $\phi'_L : G \to \mathrm{Aut}_L(L[[t]])$ with the following properties. Let $\overline{L}$ be an algebraic closure of L. Then ϕ'_L induces an injection $\phi'_{\overline{L}} : G \to \mathrm{Aut}_{\overline{L}}(\overline{L}[[t]])$, and the Artin characters of ϕ, ϕ', ϕ'_L and $\phi'_{\overline{L}}$ are equal.*

Proof. – The existence of k' and ϕ' is clear from the fact that a Katz-Gabber G-cover associated to ϕ, together with the action of G on this cover, is defined over a field of finite type over the prime field $\mathbb{F}_p$. Since ϕ defines a totally ramified action of G, so does ϕ'. If k' is finite, we can therefore take L to be k'. Suppose now that k' has positive transcendence degree over $\mathbb{F}_p$. By the Noether normalization theorem, k' is a finite extension of a rational subfield $\mathbb{F}_p(t_1, \ldots, t_n)$ for some algebraically independent indeterminates $t_1, \ldots, t_n$, where $n \geq 1$. Let $k_1 = \overline{\mathbb{F}_p(t_1, \ldots, t_{n-1})}$ be an algebraic closure of the subfield $\mathbb{F}_p(t_1, \ldots, t_{n-1})$, and let N be the compositum of k' and k_1 in an extension field of k. Then N has transcendence degree 1 over k_1. Since k_1 is algebraically closed, N is the function field of a smooth projective curve V over k_1, and k_1 is the field of constants of V. By [15] and [24], $\mathrm{Gal}(\overline{N}/N) = \mathrm{Gal}(\overline{k_1(V)}/k_1(V))$ is a free profinite group of countable rank since k_1 is countable. Let F be one element of a set of topological generators for $\mathrm{Gal}(\overline{N}/N)$, and let $L = \overline{N}^{\langle F \rangle}$ be the fixed field of F acting on $\overline{N}$. Then L is a quasi-finite field, with algebraic closure $\overline{L} = \overline{N}$ and an isomorphism $\hat{\mathbb{Z}} \to \mathrm{Gal}(\overline{L}/L)$ defined by $\nu \mapsto F^{\nu}$. Since $k' \subset N \subset L$, we can let $\phi_L : G \to \mathrm{Aut}_L(L[[t]])$ be the base change of ϕ' from k' to L. Since ϕ, ϕ_L and $\phi_{\overline{L}}$ are base changes of ϕ', all of the associated Artin characters are equal. □

COROLLARY 13.3. – *Fix an algebraically closed field k of characteristic $p > 0$, and let a be a complex character of G. There is an injection $\phi : G \to \mathrm{Aut}_k(k[[t]])$ for which $a_\phi = a$ if and only if there is a quasi-finite field L of characteristic p together with an injection $\phi_L : G \to \mathrm{Aut}_L(L[[t]])$ such that $a_{\phi_L} = a$.*

Proof. – Given ϕ, we can take L and a_{ϕ_L} to be as in Proposition 13.2. Given L and ϕ_L, we take $k = \overline{L}$, and we let ϕ be the base change of ϕ_L from L to k. □

14. Dihedral, quaternion and semi-dihedral groups: Ramification filtrations

The object of this section is to begin the analysis of the Bertin obstruction for certain dihedral, generalized quaternion and semi-dihedral groups.

The following lemma is an example from the end of §IV.3 of [28]. Recall that a real number μ is a *jump* in the upper (resp. lower) ramification filtration of a subgroup $J \subset G$ if $J^\nu \neq J^{\nu+\epsilon}$ (resp. $J_\nu \neq J_{\nu+\epsilon}$) for all $\epsilon > 0$.

LEMMA 14.1 ([28]). – *Let k be a field of characteristic $p > 0$, let H be a cyclic group of order p^n, and assume we are given a Galois extension of $k((t))$ with group H. Then there are positive integers $i_0, i_1, \ldots, i_{n-1}$ such that the jumps in the upper numbering of the ramification filtration of H occur at $i_0, i_0 + i_1, \ldots, i_0 + i_1 + \cdots + i_{n-1}$. We have ramification groups*

$$\begin{aligned} H_0 &= \cdots = H_{i_0} = H = H^0 = \cdots = H^{i_0} \\ H_{i_0+1} &= \cdots = H_{i_0+pi_1} = pH = H^{i_0+1} = \cdots = H^{i_0+i_1} \\ H_{i_0+pi_1+1} &= \cdots = H_{i_0+pi_1+p^2i_2} = p^2H = H^{i_0+i_1+1} = \cdots = H^{i_0+i_1+i_2} \\ &\cdots \\ H_{i_0+pi_2+\cdots+p^{n-1}i_{n-1}+1} &= p^nH = \{e\} = H^{i_0+\cdots i_{n-1}+1}. \end{aligned} \tag{14.1}$$

Thus the jumps in the lower ramification filtration are at $\sum_{j=0}^{\ell} p^j i_j$ for $0 \leq \ell \leq n-1$.

For the remainder of this section we make the following standing hypothesis:

HYPOTHESIS 14.2. – *Let k be an algebraically closed field of characteristic $p > 0$ and let $n \geq 1$ be an integer. The group G is of order $2p^n$, is generated by a cyclic subgroup $H = \langle \tau \rangle$ of order p^n and an element σ. In addition to the relation $\tau^{p^n} = e$, G is specified by the following relations:*

a. *(Dihedral case) $\sigma^2 = e$ and $\sigma\tau\sigma^{-1} = \tau^{-1}$.*
b. *(Generalized quaternion case) $p = 2$, $n \geq 2$, $\sigma^2 = \tau^{p^{n-1}}$, $\sigma\tau\sigma^{-1} = \tau^{-1}$.*
c. *(Semi-dihedral case) $p = 2$, $n \geq 3$, $\sigma^2 = e$, $\sigma\tau\sigma^{-1} = \tau^{-1+p^{n-1}}$.*

Let $\phi : G \to \mathrm{Aut}_k(k[[t]])$ be an injection. For Γ a subgroup of G, let Γ_ν and Γ^ν be the lower and upper ramification subgroups of Γ associated to $\nu \in \mathbb{R}$.

Under Hypothesis 14.2, Lemma 14.1 yields:

COROLLARY 14.3. – *Suppose that $\Gamma = p^jH$ is a non-trivial subgroup of H, so that $0 \leq j \leq n-1$. Then*

$$\iota(\Gamma) = 1 + i_0 + pi_1 + \cdots + p^j i_j. \tag{14.2}$$

It is straightforward to verify the following lemma and corollary.

LEMMA 14.4. – *A set $\mathcal{C}$ of representatives for the cyclic subgroups T of G may be given as follows. For $0 \leq j \leq n$, let $p^jH = \langle \tau^{p^j} \rangle$ be the subgroup of index p^j in H, and let $\mathcal{H} = \{p^jH : 0 \leq j \leq n\}$. One has $\mathrm{N}_G(T) = T$ for $T \in \mathcal{H}$.*

a. *(Dihedral case when $p > 2$)* $\mathscr{C} = \mathscr{H} \cup \{D_1\}$, *where* $D_1 = \langle\sigma\rangle$ *has order* 2 *and* $\mathrm{N}_G(D_1) = D_1$.

a′. *(Dihedral case when $p = 2$)* $\mathscr{C} = \mathscr{H} \cup \{D_1, D_2\}$ *where* $D_1 = \langle\sigma\rangle$ *and* $D_2 = \langle\tau\sigma\rangle$ *have order* 2. *The group* $\mathrm{N}_G(D_i) = \langle D_i, 2^{n-1}H\rangle$ *contains* D_i *with index* 2.

b. *(Generalized quaternion case)* $\mathscr{C} = \mathscr{H} \cup \{D_1, D_2\}$ *where* $D_1 = \langle\sigma\rangle$ *and* $D_2 = \langle\tau\sigma\rangle$ *have order* 4. *The group* $\mathrm{N}_G(D_i) = \{2^{n-2}H, D_i\}$ *contains* D_i *with index* 2.

c. *(Semi-dihedral case)* $\mathscr{C} = \mathscr{H} \cup \{D_1, D_2\}$ *where* $D_1 = \langle\sigma\rangle$ *has order* 2 *and* $D_2 = \langle\sigma\tau\rangle$ *has order* 4. *One has* $\mathrm{N}_G(D_1) = \langle 2^{n-1}H, D_1\rangle$ *and* $\mathrm{N}_G(D_2) = \langle 2^{n-2}H, D_2\rangle$. *For* $i = 1, 2$, *the index* $[\mathrm{N}_G(D_i) : D_i]$ *equals* 2.

COROLLARY 14.5. – *Suppose* $T \in \mathscr{C}$ *is non-trivial. Recall that* $S(T)$ *is the set of non-trivial cyclic subgroups* $\Gamma \subset G$ *which contain* T. *Define* $S'(T)$ *to be the set of* $\Gamma \in S(T)$ *such that* $\mu([\Gamma : T])$ *is non-zero, i.e. for which* $[\Gamma : T]$ *is square-free. Then* $S'(T)$ *has the following description.*

a. *If* $T = D_i$ *for some* i *as in Lemma 14.4, then* $S'(T) = \{T\}$.

b. *Suppose* $T = p^j H$ *for some* $0 \le j \le n-1$ *and that either* G *is dihedral or* $j \ne n-1$. *Then* $S'(T) = \{T\}$ *if* $j = 0$ *and* $S'(T) = \{T, p^{j-1}T\}$ *if* $0 < j$.

c. *Suppose* G *is quaternionic and* $T = 2^{n-1}H$. *Then* $S'(T)$ *is the union of* $\{T, 2^{n-2}H\}$ *with the set of* $\#(G/\mathrm{N}_G(D_1)) = 2^{n-2}$ *distinct conjugates of* D_1 *and the set of* $\#(G/\mathrm{N}_G(D_2)) = 2^{n-2}$ *distinct conjugates of* D_2.

d. *Suppose* G *is semi-dihedral and* $T = 2^{n-1}H$. *Then* $S'(T)$ *is the union of* $\{T, 2^{n-2}H\}$ *with the set of* $\#(G/\mathrm{N}_G(D_2)) = 2^{n-2}$ *distinct conjugates of* D_2.

COROLLARY 14.6. – *Suppose that* $T = p^j H$ *is a non-trivial subgroup of* H *satisfying the conditions of part (b) of Corollary 14.5. Thus either* G *is dihedral or* $0 \le j < n-1$. *Then*

$$b_T = \frac{1 + i_0}{2} \quad \text{if} \quad j = 0 \quad \text{and} \quad b_T = \frac{i_j}{2} \quad \text{if} \quad j > 0. \tag{14.3}$$

Proof. – Recall from Theorem 2.3 that

$$b_T = \frac{1}{[\mathrm{N}_G(T) : T]} \sum_{\Gamma \in S(T)} \mu([\Gamma : T])\iota(\Gamma). \tag{14.4}$$

Since T is normal in G, $[\mathrm{N}_G(T) : T] = \#G/\#T = 2p^n/p^{n-j} = 2p^j$. The only Γ which contribute to the sum for b_T are those Γ in $S'(T)$. Hence Corollary 14.5 gives $b_T = \frac{1}{2}\iota(H)$ if $j = 0$ while $b_T = \frac{1}{2p^j}(\iota(p^j H) - \iota(p^{j-1}H))$ if $j > 0$. Corollary 14.3 now gives the stated formulas for b_T. □

COROLLARY 14.7. – *Suppose* $p > 2$, G *is dihedral, and that* $T = D_1$ *is as in Lemma 14.4(a). Then* $b_T = \iota(T) = 1$.

Proof. – This is clear from the general formula (14.4) for b_T and the fact that $S'(T) = \{T\}$, $\mathrm{N}_G(T) = T$ and T has order 2, which is prime to p. □

LEMMA 14.8. – *Suppose that G, D_1 and D_2 are as in parts (a′), (b) or (c) of Lemma 14.4. Let $\phi : G \to \mathrm{Aut}_k(k[[t]])$ be an injection. Define $D_0 = H$. Let $N = k((t))$, $K = N^G$, and $L_i = N^{\langle 2H, D_i\rangle}$ for $i = 0, 1, 2$, where $\langle 2H, D_i\rangle$ is the subgroup generated by $2H$ and D_i. Then L_i/K is quadratic for $i = 0, 1, 2$, with relative discriminant ideal $(m_K)^{d_i}$ for some even integer d_i, where m_K is the maximal ideal of the integers O_K of K. Moreover for $i = 0, 1, 2$,*

$$b_{D_i} = \frac{\left(\sum_{j\in\{0,1,2\}, j\neq i} d_j\right) - d_i}{2} \tag{14.5}$$

is a positive integer.

Proof. – Let ψ_i be the quadratic one-dimensional character of $G = \mathrm{Gal}(N/K)$ which is the inflation of the non-trivial one dimensional character of $\mathrm{Gal}(L_i/K)$. Then ψ_i is trivial on D_i. Write

$$-a_\phi = \sum_{T\in\mathcal{C}} b_T\, 1_T^G = \sum_{2H\supset T\in\mathcal{C}} b_T\, 1_T^G + \sum_{i=0}^{2} b_{D_i}\, 1_{D_i}^G. \tag{14.6}$$

Take the inner product of this expression with $\chi_0 - \psi_i$ when χ_0 is the one-dimensional trivial character of G. If $T \subset 2H$ then $\langle 1_T^G, \chi_0 - \psi_i\rangle = 0$, and

$$\langle -a_\phi, \chi_0 - \psi_i\rangle = -\langle a_\phi, \chi_0\rangle + \langle a_\phi, \psi_i\rangle = 0 + \langle a_\phi, \psi_i\rangle = d_i \tag{14.7}$$

by [28, §VI.2]. For $i, j \in \{0, 1, 2\}$, one has

$$\langle 1_{D_j}^G, \chi_0 - \psi_i\rangle = \langle 1_{D_j}^G, \chi_0\rangle - \langle 1_{D_j}^G, \psi_i\rangle = 1 - \delta(i, j) \tag{14.8}$$

since the restriction of ψ_i to D_j is trivial if $i = j$ and non-trivial otherwise. Combining (14.6), (14.7) and (14.8) gives the system of equations

$$\begin{aligned} d_0 &= b_{D_1} + b_{D_2} \\ d_1 &= b_{D_0} + b_{D_2} \\ d_2 &= b_{D_0} + b_{D_1}. \end{aligned} \tag{14.9}$$

The formula (14.5) is clear from this. The exponents d_0, d_1, d_2 are even and positive since $p = 2$, so that all the b_{D_i} are integral. The compositum of L_0, L_1 and L_2 over K is a biquadratic extension of K. Thus either all the d_i are equal, or two are equal and the third is smaller than these two. This implies that all the b_{D_i} are positive, which completes the proof. □

COROLLARY 14.9. – *Assume the hypotheses of Lemma 14.8. Then*

$$\iota(D_i) = 2b_{D_i} = \left(\sum_{j\in\{0,1,2\}, j\neq i} d_j\right) - d_i$$

for $i = 0, 1, 2$.

Proof. – By Lemma 14.4 and Corollary 14.5, $[\mathrm{N}_G(D_i) : D_i] = 2$ and $S'(D_i) = \{D_i\}$, so the result follows from (14.4) and Lemma 14.8. □

COROLLARY 14.10. – *With the hypotheses of Lemma 14.8, suppose G is quaternionic or semi-dihedral, and that $T = 2^{n-1}H$.*

a. *If G is quaternionic then*

$$b_T = \frac{i_{n-1}}{2} - \frac{d_0}{2}.$$

b. *If G is semi-dihedral then*

$$b_T = \frac{i_{n-1}}{2} - \frac{d_0 + d_1 - d_2}{4}.$$

Proof. – If G is quaternionic, then Corollaries 14.5, 14.3 and 14.9 give

$$\begin{aligned} b_T &= \frac{1}{[\mathrm{N}_G(T) : T]} \sum_{\Gamma \in S(T)} \mu([\Gamma : T])\iota(\Gamma) \\ &= \frac{1}{2^n}\left(\iota(2^{n-1}H) - \iota(2^{n-2}H) - 2^{n-2}(\iota(D_1) + \iota(D_2))\right) \qquad (14.10) \\ &= \frac{1}{2^n}\left(2^{n-1}i_{n-1} - 2^{n-1}(b_{D_1} + b_{D_2})\right) \\ &= \frac{i_{n-1}}{2} - \frac{d_0}{2}. \qquad (14.11) \end{aligned}$$

If G is semi-dihedral, the same arguments show

$$\begin{aligned} b_T &= \frac{1}{[\mathrm{N}_G(T) : T]} \sum_{\Gamma \in S(T)} \mu([\Gamma : T])\iota(\Gamma) \\ &= \frac{1}{2^n}\left(\iota(2^{n-1}H) - \iota(2^{n-2}H) - 2^{n-2}\iota(D_2))\right) \qquad (14.12) \\ &= \frac{1}{2^n}\left(2^{n-1}i_{n-1} - 2^{n-1}b_{D_2}\right) \\ &= \frac{i_{n-1}}{2} - \frac{d_0 + d_1 - d_2}{4}. \end{aligned}$$

□

COROLLARY 14.11. – *The Bertin obstruction of an injection $\phi : G \to \mathrm{Aut}_k(k[[t]])$ vanishes if and only if the following conditions hold:*

a. *i_0 is odd, and i_j is even for $0 < j < n-1$.*
b. *If G is dihedral, i_{n-1} is even.*
c. *If G is quaternionic, i_{n-1} is even and $i_{n-1} \geq d_0$.*
d. *If G is semidihedral, $\frac{i_{n-1}}{2} - \frac{d_0+d_1-d_2}{4}$ is a non-negative integer.*

Proof. – By Proposition 2.1, the Bertin obstruction of ϕ vanishes if and only if b_T is a non-negative integer for T a non-trivial subgroup contained in the set $\mathscr{C}$ described in Lemma 14.4. Those non-trivial $T \in \mathscr{C}$ contained in H are treated in Corollaries 14.6 and 14.10 since the d_i in Lemma 14.8 are even. The $T \in \mathscr{C}$ which are not contained in H are treated in Corollary 14.7 and Lemma 14.8. Conditions (a)–(d) are equivalent to the statement that the b_T in Corollaries 14.6, 14.10 and 14.7 and in Lemma 14.8 are non-negative integers. □

COROLLARY 14.12. – *Suppose that the Bertin obstruction of ϕ vanishes, so that (a)–(d) of Corollary 14.11 hold. Then the KGB obstruction of ϕ vanishes.*

Proof. – We claim that the KGB obstruction vanishes if we can find for each non-trivial $T \in \mathscr{C}$ a sequence of elements $\{g_{T,i}\}_{i=1}^{b_T}$ of G with the following properties:

i. Each $g_{T,i}$ is in a conjugate of T;
ii. There is an ordering $\{g_t\}_{t\in\Omega}$ of the doubly indexed set $\{g_{T,i}\}_{T,i}$, counting multiplicities, such that $\prod_{t\in\Omega} g_t$ has order $[G : G_1]$.

To prove this claim, suppose we can find $\{g_t\}_{t\in\Omega}$ as above. In Theorem 4.2(b) we can then take S to be $\coprod_{t\in\Omega} G/\langle g_t\rangle$ provided we show that $\{g_t\}_{t\in\Omega}$ generates G. Suppose first that $p > 2$, so $G = D_{2p^n}$. By Corollary 14.7, $b_{D_1} = 1$, so there is one g_t which has order 2. By Corollary 14.6, $b_H = \frac{1+i_0}{2} > 0$. Thus the subgroup of G generated by $\{g_t\}_{t\in\Omega}$ contains H and D_1, so must be all of G. Suppose now that $p = 2$. By Lemma 14.8, b_H, b_{D_1} and b_{D_2} are positive. Hence the subgroup of G generated by $\{g_t\}_{t\in\Omega}$ surjects onto the Klein four quotient $G/2H$ of G. This implies this subgroup must be all of G.

We now have to show that we can choose the $g_{T,i}$ so that (i) and (ii) hold.

We consider first the case $p > 2$. Then G is isomorphic to D_{2p^n} for some $n \geq 1$, and (14.13) holds vacuously. By Corollary 14.7, $b_{D_1} = 1$. It follows that if we pick the $g_{T,i}$ to be any generators of T, and pick any ordering $\{g_t\}_{t\in\Omega}$ of all these $g_{T,i}$, then the product $\prod_{t\in\Omega} g_t$ projects to the non-trivial element of G/H. Hence this product has order $2 = [G : G_1]$, since every element of $G = D_{2p^n}$ not in H has order 2. Hence (i) and (ii) hold.

Suppose now that $p = 2$ and that G is a 2-group and is either dihedral, quaternionic or semi-dihedral. The quotient $G/(2H)$ is then isomorphic to the Klein four group, and $G = G_1$. We claim that

$$b_H \equiv b_{D_1} \equiv b_{D_2} \bmod 2\mathbb{Z}. \tag{14.13}$$

Here $b_H = b_{D_0}$ in the terminology of Lemma 14.8, where it was shown that

$$b_{D_i} = \frac{\left(\sum_{j\in\{0,1,2\}, j\neq i} d_j\right) - d_i}{2} \tag{14.14}$$

for $i = 0, 1, 2$. Since all the d_i are even, we have $d_i \cong -d_i \bmod 4\mathbb{Z}$. Thus

$$2b_{D_i} \equiv \sum_{j\in\{0,1,2\}} d_j \mod 4\mathbb{Z}$$

from which (14.13) is clear. Let the $g_{T,i}$ be any choice of generators for T as T ranges over $\mathcal{C}$ and $i = 1, \ldots, b_T$. By Corollary 14.6, $b_H > 0$. Hence we can choose an ordering $\{g_t\}_{t\in\Omega}$ of these $g_{T,i}$ such that the first g_t is a generator of H. The congruence (14.13) implies that $\prod_{t\in\Omega} g_t$ lies in $2H$. We can now multiply the first g_t by an element of $2H$ to produce a new generator of H such that when we use this element as the first g_t we have $\prod_{t\in\Omega} g_t = e$. This shows that (i) and (ii) hold and completes the proof. □

COROLLARY 14.13. – *With G a finite group and k a field of characteristic $p > 0$, let $P(G, k)$ be the assertion that every injection $\phi : G \to \mathrm{Aut}_k(k[[t]])$ satisfies conditions (a)–(d) of Corollary 14.11. Then fixing G, the assertion $P(G, k)$ holds for all algebraically closed fields k of characteristic p if and only if $P(G, k)$ holds for all quasi-finite fields k of characteristic p. The same is true if we add condition (14.13) to $P(G, k)$.*

Proof. – This a consequence of Corollary 13.3. □

15. Dihedral, quaternion and semi-dihedral groups: Class field theory

In the section we will assume the hypotheses and notations of the previous section, with the following modifications:

HYPOTHESIS 15.1. – *The field k is quasi-finite (rather than algebraically closed) of characteristic p. Fix an injection $\phi : G \to \mathrm{Aut}_k(k[[t]])$. Let $N = k((t))$, $L = N^H$ and $K = N^G$. Define $\chi : L^* \to H = \mathrm{Gal}(N/L)$ to be the Artin isomorphism. Let $\overline{\sigma}$ be the image of $\sigma \in G$ in $G/H = \mathrm{Gal}(L/K)$, so that $\overline{\sigma}$ has order 2 and is a generator of G/H. We choose a uniformizer π_L in L such that if $p > 2$, $\overline{\sigma}(\pi_L) = -\pi_L$. Let $\mathrm{Norm}_{L/K} : L \to K$ be the norm. Define $D_0 = H$, so that $L = N^{D_0}$. If $p = 2$, we also have the quadratic extensions L_1 and L_2 of K defined in Lemma 14.8; in this case, $L_0 = L, L_1$ and L_2 are the three quadratic subfields of N containing K.*

DEFINITION 15.2. – Let $\chi : L^* \to \mathbb{C}^*$ be a character of order p^n, and let $\chi|_{K^*}$ be the restriction of χ to K^*.

a. Say χ is of *dihedral type* if $\chi|_{K^*}$ is trivial.
b. Say χ is of *quaternionic type* if $p = 2$ and $\chi|_{K^*}$ is the non-trivial quadratic character $\epsilon_0 : K^* \to \{\pm 1\}$ associated to L/K. This is the character with kernel $\mathrm{Norm}_{L/K}(L^*)$.
c. Say χ is of *semi-dihedral type* if $p = 2, n \geq 3$, $\chi|_{K^*}$ is the non-trivial quadratic character $\epsilon_1 : K^* \to \{\pm 1\}$ associated to L_1/K, and $\chi \circ \mathrm{Norm}_{L/K} = \chi^{2^{n-1}}$.

LEMMA 15.3. – *If G is a dihedral (resp. quaternion, resp. semi-dihedral) group then χ is of dihedral (resp. quaternion, resp. semi-dihedral) type. Conversely, suspend Hypothesis 15.1 for the moment, and suppose L/K is a specified quadratic extension of $K = k((z))$ for some indeterminate z. Let χ be a character of order p^n of L^*, and let N be the cyclic extension of L of degree p^n over L which corresponds to the kernel of χ by local classfield theory.*

i. *Suppose χ is of dihedral (resp. quaternionic) type, in the sense of parts (a) and (b) of Definition 15.2. Then N is a Galois extension of N and $\mathrm{Gal}(N/K)$ is a dihedral group (resp. generalized quaternion group) of order $2p^n$.*
ii. *Suppose that $\chi|_{K^*}$ is an order 2 character of K^* which corresponds to a quadratic extension L_1/K different from L/K, and that $\chi \circ \mathrm{N}_{L/K} = \chi^{2^{n-1}}$. Then N is a semi-dihedral extension of K of degree $2p^n$, with biquadratic subfield over K the compositum of L and L_1 over K. The character χ is of semi-dihedral type in the sense of Definition 15.2(c).*

Proof. – Suppose first that Hypothesis 15.1 holds and that G is dihedral, quaternionic or semi-dihedral. By local classfield theory, $\chi|_{K^*} : K^* \to \mathbb{C}^*$ corresponds to the character $G^{\mathrm{ab}} \to \mathbb{C}^*$ which is the composition of the transfer map $\mathrm{ver} : G^{\mathrm{ab}} \to H^{\mathrm{ab}} = H$ with $\chi : H \to \mathbb{C}^*$. The action of $\mathrm{Gal}(L/K) = G/H$ on L^* corresponds via $\xi : L^* \to \mathrm{Gal}(N/L) = H$ with the conjugation action of $\mathrm{Gal}(L/K)$ on H. The assertions in the lemma now follow from the properties of this conjugation action and of ver when G is a dihedral, quaternion or semi-dihedral group (see [28, §VII.8]). The converse implications of the lemma are proved similarly. □

LEMMA 15.4. – *Assume Hypothesis 15.1 holds. If* $0 \leq \ell \leq n-1$ *then*

$$c(\ell) = i_0 + \cdots + i_\ell \tag{15.1}$$

is a jump in the upper ramification filtration of H. *Let* $\chi : L^* \to \mathbb{C}^*$ *be a character having the properties in the converse direction of Lemma 15.3. Then the kernel of* $\chi^{p^{n-(\ell+1)}}$ *corresponds via class field theory to the extension* $N^{p^{\ell+1}H}/L$, *which has Galois group* $H/(p^{\ell+1}H)$. *The integer* $c(\ell)$ *is the largest positive integer such that* $\chi^{p^{n-(\ell+1)}}$ *is non-trivial on* $1 + \pi_L^{c(\ell)} O_L$.

Proof. – By [28, §XV.2], if $h \geq 1$ is integral then the image $\xi(1+\pi_L^h O_L)$ of the multiplicative subgroup $1+\pi_L^j O_L$ under the local Artin map $\xi : L^* \to H$ equals the upper ramification subgroup H^h of H. Since $\chi^{p^{n-(\ell+1)}}$ has kernel $p^{\ell+1}H$ when we view it as a character of H via the local Artin map, this leads to the interpretation $c(\ell)$ in the lemma. □

COROLLARY 15.5. – *The jump* i_0 *is odd. If* G *is dihedral, then* i_j *is even for* $0 < j \leq n-1$. *Suppose that* G *is quaternionic or semi-dihedral. Then* $c(\ell)$ *is odd for* $0 \leq \ell \leq n-2$, i_j *is even for* $0 < j < n-1$, *and* $i_{n-1} = c(n-1) - c(n-2)$ *is even if and only if* $c(n-1)$ *is odd.*

Proof. – By [28, §XV.2], the local Artin map ξ induces an isomorphism

$$\frac{1+\pi_L^{c(\ell)} O_L}{1+\pi_L^{c(\ell)+1} O_L} = H^{c(\ell)}/H^{c(\ell)+1} = p^\ell H/(p^{\ell+1}H) \cong \mathbb{Z}/p \quad \text{for} \quad 0 \leq \ell \leq n-1. \tag{15.2}$$

This isomorphism is equivariant with respect to the action of $\mathrm{Gal}(L/K)$. Recall that we chose the uniformizer π_L so that that $\gamma(\pi_L) = -\pi_L$ if $p > 2$, and there is an isomorphism of the left hand side of (15.2) with the one dimensional k-vector space $\pi_L^{c(\ell)} k$. Hence if $p > 2$, then γ acts on the left hand side of (15.2) by $(-1)^{c(\ell)}$. We conclude that $c(\ell)$ is odd because γ acts by inversion on the right hand side of (15.2). In view of (15.1), this shows that i_0 must be odd and i_j is even for $j > 0$, so we are done in case $p > 2$.

Suppose now that $p = 2$. To complete the proof, it will suffice by Lemma 15.4 to show that $c(\ell)$ is odd if either

i. $0 \leq \ell \leq n-1$ and G is dihedral, or
ii. $0 \leq \ell \leq n-2$ and G is either quaternionic or semi-dihedral.

By Lemma 15.4, $c(\ell)$ is the largest positive integer such that $\chi^{p^{n-(\ell+1)}}$ is non-trivial on $1 + \pi_L^{c(\ell)} O_L$. Therefore $\chi^{p^{n-(\ell+1)}}$ is trivial on $1 + \pi_L^{c(\ell)+1} O_L$. Suppose $c(\ell)$ is even. Then $\pi_L^{c(\ell)}$ is equal to $\pi_K^{c(\ell)/2} \cdot u$, where $\pi_K = \mathrm{Norm}_{L/K} \pi_L$ is a uniformizer in K and u is a unit in O_L^*. Since O_L and O_K have the same residue field k, we would then have

$$1 + \pi_L^{c(\ell)} O_L = (1 + \pi_K^{c(\ell)/2} O_K) \cdot (1 + \pi_L^{c(\ell)+1} O_L). \tag{15.3}$$

It follows that $\chi^{p^{n-(\ell+1)}}$ must be non-trivial on $1+\pi_K^{c(\ell)/2} O_K$. By Lemma 15.3, the restriction of χ to K^* is trivial if G is dihedral, so we have a contradiction in this case. Suppose now that G is quaternionic or semi-dihedral. By Lemma 15.3, the restriction of χ to K^* then has order 2. We have supposed $0 \leq \ell \leq n-2$ if G is quaternionic or semi-dihedral, so $n-(\ell+1) \geq 1$ and $\chi^{p^{n-(\ell+1)}}$ is an integral power of $\chi^p = \chi^2$. Thus $\chi^{p^{n-(\ell+1)}}$ is trivial on K^* in this case, and we again have a contradiction. This shows that $c(\ell)$ must have been odd, and completes the proof. □

PROPOSITION 15.6. – *Suppose* G *is quaternionic or semi-dihedral.*

i. *The integer i_{n-1} is even unless G is the quaternion group of order 8 and $G_4 = \{e\}$. In this case i_{n-1} is odd and the following is true:*
   a. *The lower ramification filtration of G is $G = G_0 = G_1 \neq G_2 = G_3 \neq G_4 = \{e\}$, where G_2 is the order 2 center of G.*
   b. *The Bertin obstruction of $\phi : G \to \mathrm{Aut}_k(k[[t]])$ does not vanish.*

ii. *Suppose G is a generalized quaternion group and i_{n-1} is even. Then the KGB obstruction (and hence the Bertin obstruction) associated to ϕ vanishes.*

iii. *Suppose G is semi-dihedral. The Bertin obstruction of ϕ does not vanish if $d_0 + d_1 + d_2$ is not divisible by 4, in the notation of Lemma 14.8.*

The proof is an argument by contradiction, and requires a series of lemmas. Before beginning this we note that this result gives a new proof of a result of Serre [27, §5] and Fontaine [9] concerning Artin representations which cannot be realized over $\mathbb{Q}$.

COROLLARY 15.7 (Serre, Fontaine). – *Suppose G is a generalized quaternion group. Then the Artin character $-a_\phi$ is not realizable over $\mathbb{Q}$ if and only if G has order 8 and the lower ramification filtration of G is as in Proposition 15.6.i.a.*

Proof. – If the Bertin obstruction vanishes, then $-a_\phi$ is the character of a permutation representation by Proposition 2.1 so it is realizable over $\mathbb{Q}$. Otherwise, G must have order 8 and must have the ramification filtration in part (i.a) of Proposition 15.6. Suppose now that G is as in part (i.a) of Proposition 15.6. Serre proved in [27, §5] that $-a_\phi$ is not realizable over $\mathbb{Q}$ by proving that the multiplicity of the two-dimensional irreducible representation of G in $-a_\phi$ is 5. □

LEMMA 15.8. – *Suppose G is quaternionic or semi-dihedral. Then i_{n-1} is odd if and only if $c(n-1)$ in (15.1) is even. Suppose i_{n-1} is odd, and let d_0 and d_1 be as in Lemma 14.8. Then*

$$\frac{c(n-1)}{2} = d_0 - 1 \text{ (resp. } d_1 - 1) \quad \text{if} \quad G \quad \text{is quaternionic (resp. semi} - \text{dihedral).} \tag{15.4}$$

Proof. – The first statement is clear from (15.1) and Corollary 15.5. Now suppose i_{n-1} is odd, so that $c(n-1)$ is even. By Lemma 15.4, $c(n-1)$ is the largest positive integer such that $\chi|(1+\pi_L^{c(n-1)}O_L)$ is non-trivial. Now $c(n-1)$ is even, $\pi_K O_L = \pi_L^2 O_L$, and the residue fields of L and K are both k; so we have

$$(1+\pi_L^{c(n-1)}O_L) = (1+\pi_K^{c(n-1)/2}O_K)\cdot(1+\pi_L^{c(n-1)+1}O_L).$$

This implies that $c(n-1)/2$ is the largest positive integer j such that $\chi|(1+\pi_K^j O_K)$ is non-trivial. By Lemma 15.3, the restriction $\chi|K^*$ is the non-trivial quadratic character associated to the quadratic extension L_i/K, where $i = 0$ and $L_0 = L$ if G is quaternionic, and $i = 1$ and L_1/K is described in Lemma 15.3 if G is semi-dihedral. The ramification groups $\mathrm{Gal}(L_i/K)^\nu = \mathrm{Gal}(L_i/K)_\nu$ equal $\mathrm{Gal}(L_i/K)$ if $\nu = 0, \ldots, d_i - 1$ and these groups are trivial for $\nu > d_i - 1$ since $[L_i : K] = 2$. Thus $c(n-1)/2 = d_i - 1$ as claimed. □

LEMMA 15.9. – *Recall that $\sigma \in G = \mathrm{Gal}(N/K)$ is an element not in $H = \mathrm{Gal}(N/L)$. One has*

$$\sigma(\pi_L) = \pi_L \cdot (1 + \beta\pi_L^{d_0-1} + \pi_L^{d_0}\gamma) \tag{15.5}$$

for some $\gamma \in O_L$ and some $\beta \in k^*$. We may define a uniformizer π_K in K by

$$\pi_K = \pi_L \sigma(\pi_L) = \pi_L^2 \cdot (1 + \beta \pi_L^{d_0 - 1} + \pi_L^{d_0} \gamma). \tag{15.6}$$

Proof. – The first and only jump in the lower ramification numbering of $\mathrm{Gal}(L/K)$ occurs at $d_0 - 1$. By the definition of the lower numbering, this gives (15.5), and (15.6) follows from the fact that L/K is quadratic and totally ramified. □

LEMMA 15.10. – *Let G be quaternionic or semi-dihedral. The integer $i_0 = c(0)$ is the largest integer for which there exists an element $\delta \in k^*$ such that $\chi(1 + \delta \pi_L^{i_0}) = \zeta$ is a primitive 2^n-th root of unity. The value of i_0 is odd and given by*

$$i_0 = d_1 + d_2 - d_0 - 1. \tag{15.7}$$

Proof. – The first statement follows from [28, Cor. 3, §XV.2] since χ has order 2^n. In the quaternionic or semi-dihedral case, $p = 2$. For $\gamma \in L^*$, the value $\chi(\gamma)$ is a primitive 2^n-th root of unity if and only if $\chi^{p^{n-1}}(\gamma)$ is non-trivial. Hence Lemma 15.4 shows the first statement about i_0, since i_0 is the largest integer such that $\chi^{2^{n-1}}$ is not trivial on $1 + \pi_L^{i_0} O_L$. The character $\chi^{2^{n-1}}$ corresponds to the order two character of the Galois group $\mathrm{Gal}(L'/L)$, where $L = L_0$ and L' is the compositum $L \cdot L_1 = L_1 \cdot L_2$ over K (with notation as in Hypothesis 15.1). Thus i_0 is the first (and only) jump in the upper (and lower) ramification filtration of $\mathrm{Gal}(L'/L)$. It follows that the relative discriminant $d_{L'/L}$ equals $\pi_L^{i_0+1} O_L$. The relative discriminant $d_{L'/K}$ is given by

$$d_{L/K}^2 \cdot \mathrm{Norm}_{L/K} d_{L'/L} = d_{L'/K} = d_{L/K} \cdot d_{L_1/K} \cdot d_{L_2/K}$$

where the second equality follows from the conductor discriminant formula. Since $L = L_0$ is totally and quadratically ramified over K, this gives

$$2d_0 + i_0 + 1 = d_0 + d_1 + d_2$$

which is equivalent to (15.7). Since all of d_0, d_1 and d_2 are even, i_0 is odd. □

LEMMA 15.11. – *Suppose β, π_L are as in Lemma 15.10 and that π_K is a uniformizer in K. For all $a \in k$, all odd integers $h \geq 1$, and all sufficiently large positive integers $M > 1$, we have*

$$(1 + a\pi_L^h)^{2^M - 2} \cdot (1 + a^2 \pi_K^h) = 1 + a^2 \beta \pi_L^{2h + d_0 - 1} + \pi_L^{2h + d_0} \eta \tag{15.8}$$

for some $\eta \in k[[\pi_L]] = O_L$.

Proof. – We will show by induction on the integer $\mu \geq 1$ that

$$(1 + a\pi_L^h)^{2^\mu - 2} \cdot (1 + a^2 \pi_K^h) = 1 + a^{2^\mu} \pi_L^{h 2^\mu} + a^2 \beta \pi_L^{2h + d_0 - 1} + \pi_L^{2h + d_0} \cdot \eta_\mu \tag{15.9}$$

for some $\eta_\mu \in k[[\pi_L]] = O_L$, using that the characteristic is 2. We then get (15.8) by setting $M = \mu$ and

$$\eta = a^{2^\mu} \pi_L^{h 2^\mu - (2h + d_0)} + \eta_\mu$$

when μ is large enough so that $h 2^\mu \geq 2h + d_0$.

To prove (15.9), first consider the case $\mu = 1$. We have from (15.6) that since h is odd and $d_0 \geq 2$,

$$\begin{aligned} 1 + a^2\pi_K^h &= 1 + a^2(\pi_L\sigma(\pi_L))^h \\ &= 1 + a^2(\pi_L^2 \cdot (1 + \beta\pi_L^{d_0-1} + \pi_L^{d_0}\gamma))^h \\ &= 1 + a^2\pi_L^{2h} + a^2\beta\pi_L^{2h+d_0-1} + \pi_L^{2h+d_0}\eta_1 \end{aligned} \tag{15.10}$$

for some $\eta_1 \in k[[\pi_L]] = O_L$. This is exactly the assertion in (15.9) when $\mu = 1$.

Now assume that (15.9) holds for some $\mu \geq 1$. We multiply both sides by

$$(1 + a\pi_L^h)^{2^\mu} = 1 + a^{2^\mu}\pi_L^{h2^\mu}.$$

The left side becomes

$$(1 + a\pi_L^h)^{2^\mu} \cdot (1 + a\pi_L^h)^{2^\mu-2} \cdot (1 + a^2\pi_K^h) = (1 + a\pi_L^h)^{2^{\mu+1}-2} \cdot (1 + a^2\pi_K^h). \tag{15.11}$$

The right hand side becomes

$$\begin{aligned} &\left(1 + a^{2^\mu}\pi_L^{h2^\mu}\right)\left(1 + a^{2^\mu}\pi_L^{h2^\mu} + a^2\beta\pi_L^{2h+d_0-1} + \pi_L^{2h+d_0} \cdot \eta_\mu\right) \\ &\qquad = 1 + a^{2^{\mu+1}}\pi_L^{h2^{\mu+1}} + a^2\beta\pi_L^{2h+d_0-1} + \pi_L^{2h+d_0} \cdot \eta_{\mu+1} \end{aligned} \tag{15.12}$$

where

$$\eta_{\mu+1} = (1 + a^{2^\mu}\pi_L^{h2^\mu})\eta_\mu + a^{2^\mu+2}\pi_L^{h2^\mu-1}\beta \in k[[\pi_L]] = O_L.$$

Equating the right hand sides of (15.11) and (15.12) shows (15.9) when μ is replaced by $\mu+1$, so the induction is complete. □

COROLLARY 15.12. – *With the notations of Lemma 15.11, let $a = \delta$, $h = i_0$ and*

$$z = 1 + \delta^2\beta\pi_L^{2i_0+d_0-1} + \pi_L^{2i_0+d_0}\eta. \tag{15.13}$$

Then $\chi(z)$ is a root of unity of order exactly 2^{n-1} unless $n = 2$, G is a quaternion group of order 8 and $\chi(1 + \delta^2\pi_K^{i_0}) = -1$; in this case, $\chi(z) = 1$.

Proof. – From (15.8), we have

$$\chi(z) = \chi(1 + \delta\pi_L^{i_0})^{2^M-2} \cdot \chi(1 + \delta^2\pi_K^{i_0}). \tag{15.14}$$

Now from Lemma 15.10, $\chi(1 + \delta\pi_L^{i_0}) = \zeta$ is a primitive root of unity of order 2^n, while $\chi(1+\delta^2\pi_K^{i_0}) = \pm 1$ by Lemma 15.3 since $1+\delta^2\pi_K^{i_0} \in K^*$. Thus $\chi(1+\delta\pi_L^{i_0})^{2^M-2} = \zeta^{2^M-2}$ is a root of unity of order 2^{n-1} since $M > 1$. If $n \geq 3$, the product of a root of unity of order 2^{n-1} with ± 1 is a root of unity of order 2^{n-1}, so (15.14) shows $\chi(z)$ has order 2^{n-1}. Since G is quaternionic or semi-dihedral of order 2^{n+1}, the only way in which one can have $n < 3$ is for $n = 2$ and for G to be a quaternion group of order 8. In this case, $\chi(1+\delta\pi_L^{i_0})^{2^M-2} = -1$, so $\chi(z) = -\chi(1+\delta^2\pi_K^{i_0})$ is a root of unity of order $2^{n-1} = 2$ if and only if $\chi(1+\delta^2\pi_K^{i_0}) = 1$. □

LEMMA 15.13. – *Suppose G is quaternionic or semi-dihedral. Then i_{n-1} is even unless all of the following hypotheses hold:*

i. *$n = 2$ and G is the quaternion group of order 8;*
ii. *The constants d_0, d_1 and d_2 are all equal to $i_0 + 1$ in the notation of Lemma 15.10;*
iii. *The largest integer $c(1) = c(n-1)$ such that χ is non-trivial on $1+\pi_L^{c(1)}O_L$ is $c(1) = 2i_0$.*

Proof. – We assume throughout the proof that i_{n-1} is odd, so that $c(n-1)$ is even by Lemma 15.8. Suppose first that $n > 2$. By Corollary 15.12, $\chi(z)$ is a root of unity of order exactly 2^{n-1}. Then since L has characteristic 2,

$$\chi(z^{2^{n-2}}) = \chi(1 + \delta^{2^{n-1}}\beta^{2^{n-2}}\pi_L^{(2i_0+d_0-1)2^{n-2}} + \pi_L^{(2i_0+d_0)2^{n-2}}\eta^{2^{n-2}}) \tag{15.15}$$

is a primitive root of unity of order 2, so it is equal to -1. Since

$$\delta^{2^{n-1}}\beta^{2^{n-2}} \neq 0$$

in k, this shows that

$$c(n-1) \geq (2i_0 + d_0 - 1)2^{n-2}. \tag{15.16}$$

On the other hand, Lemma 15.8 shows

$$d_i - 1 = \frac{c(n-1)}{2}, \tag{15.17}$$

where $i = 0$ if G is quaternionic and $i = 1$ if G is semi-dihedral. We conclude from (15.17) and (15.16) that

$$(2i_0 + d_0 - 1)2^{n-2} = 2^{n-2}(d_0 - 1) + 2^{n-1}i_0 \leq c(n-1) = 2(d_i - 1). \tag{15.18}$$

Now $i_0 \geq 1$ and $d_0 - 1 \geq 1$ because d_0 is an even positive integer. Since we have assumed $n \geq 3$ in deducing (15.18), we conclude from (15.18) that $d_i > d_0$. Then $i = 1$ and G must be semi-dihedral. In this case, $d_1 = d_2 > d_0$, since $\pi_K^{d_i}O_K$ is the relative discriminant of the quadratic extension L_i/K, and the compositum of L_0, L_1 and L_2 is the biquadratic extension L'/K. Here

$$d_2 \geq d_0 + 2 \tag{15.19}$$

since $d_2 = d_1 > d_0$ and each of d_0, d_1 and d_2 are even. By Lemma 15.10, $\chi(1 + \delta\pi_L^{i_0})$ is a root of unity of order 2^n for some $\delta \in k^*$ and $i_0 = d_1 + d_2 - d_0 - 1$ and some $\delta \in k^*$. Hence (15.19) gives

$$i_0 = d_1 + d_2 - d_0 - 1 \geq d_1 + 1. \tag{15.20}$$

Thus (15.17), (15.18) and (15.20) give

$$2^{n-1}(d_1 + 1) \leq 2^{n-1}i_0 < 2^{n-2}(d_0 - 1) + 2^{n-1}i_0 \leq c(n-1) = 2(d_1 - 1). \tag{15.21}$$

Since $n \geq 3$, this would imply $d_1 < 0$, which is impossible. Thus $d_i > d_0$ is impossible, and we conclude our assumption that $n \geq 3$ is also impossible.

What we have shown thus far is that if i_{n-1} is odd then $n < 3$. So $n = 2$ and G must be the quaternion group of order 8, which we will assume for the rest of the proof. In view of Lemma 15.8 we have $c(n-1) = c(1) = d_0 - 1$. Suppose that the discriminant exponents d_0, d_1 and d_2 are not all equal. Since G is the quaternion group of order 8, we can switch the roles of L_0, L_1 and L_2 to be able to assume that $d_0 < d_1 = d_2$. We now have the lower bound

$$i_0 = d_1 + d_2 - d_0 - 1 = 2d_1 - d_0 - 1 \geq 2(d_0 + 2) - d_0 - 1 = d_0 + 3 \tag{15.22}$$

provided that i_{n-1} is odd. Since $\chi(1 + \delta\pi_L^{i_0})$ is a root of unity of order $2^n = 4$, $\chi(1 + \delta^2\pi_L^{2i_0}) = \chi(1 + \delta\pi_L)^2 = -1$, so χ is non-trivial on $1 + \pi^{2(d_0+3)}O_L$ by (15.22). This implies $2(d_0 + 3) \leq c(1) = 2(d_0 - 1)$ which is impossible. Hence all of d_0, d_1 and d_2

must be equal, and we find from Lemma 15.10 that they equal i_0+1. This and (15.17) (in which $i=0$, since G is a quaternion group) complete the proof. □

LEMMA 15.14. – *Suppose G is quaternionic. Then $i_{n-1} \geq d_0$ unless conditions (i), (ii) and (iii) of Lemma 15.13 hold.*

Proof. – By Lemma 15.4,

$$i_{n-1} = c(n-1) - c(n-2) \tag{15.23}$$

where $j = c(n-1)$ (resp. $j = c(n-2)$) is the largest positive integer such that χ (resp. χ^2) is non-trivial on $1+\pi_L^j O_L$. Thus $c(n-2)$ is the largest positive integer such that there is a constant $a \in k^*$ such that $\chi(1+a\pi_L^{c(n-2)}) = \zeta$ is a primitive fourth root of unity. It follows from Corollary 15.5 and (15.1) that $c(n-2)$ is odd, so we can let $h = c(n-2)$ in Lemma 15.11. With the notations of Lemma 15.11,

$$(1+a\pi_L^{c(n-2)})^{2^M-2} \cdot (1+a^2\pi_K^{c(n-2)}) = 1 + a^2\beta\pi_L^{2c(n-2)+d_0-1} + \pi_L^{2c(n-2)+d_0}\eta \tag{15.24}$$

for some $\eta \in k[[\pi_L]] = O_L$. Since M is very large, $\chi(1+a\pi_L^{c(n-2)})^{2^M-2} = \zeta^{2^M-2} = -1$ because ζ is a root of unity of order 4. Hence (15.24) shows

$$\chi(1+a^2\beta\pi_L^{2c(n-2)+d_0-1} + \pi_L^{2c(n-2)+d_0}\eta) \neq 1 \quad \text{if} \quad \chi(1+a^2\pi_K^{c(n-2)}) = 1.$$

This shows that if $\chi(1+a^2\pi_K^{c(n-2)}) = 1$ then χ is non-trivial on $1+\pi_L^{2c(n-2)+d_0-1}O_L$, so (15.23) gives

$$i_{n-1} = c(n-1) - c(n-2) \geq 2c(n-2) + d_0 - 1 - c(n-2) \geq d_0$$

as required.

We now must consider the case in which $\chi(1+a^2\pi_K^{c(n-2)}) \neq 1$. For quaternionic G, $\chi|_{K^*}$ is the character associated to L/K. Hence if $\chi(1+a^2\pi_K^{c(n-2)}) \neq 1$ then $c(n-2) \leq d_0 - 1$ since the first jump in the ramification filtration of $\mathrm{Gal}(L/K)$ occurs at $d_0 - 1$. However, Lemmas 15.4 and 15.10 show that

$$c(n-2) = i_0 + i_1 + \cdots + i_{n-2} \geq i_0 = d_1 + d_2 - d_0 - 1 \tag{15.25}$$

where all of the i_j are positive. Since d_0, d_1 and d_2 are the exponents of the discriminants of quadratic subextensions of a Klein four extension of K, either all of these integers are the same or two of them are equal and larger than the third. Hence we see from (15.25) that $c(n-2) \geq d_0 - 1$, with strict inequality unless $n=2$, $d_0 = d_1 = d_2$ and $c(n-2) = i_0 = d_0 - 1$. Suppose now that all of these conditions hold. Then $\chi(1+\pi_L^{c(n-2)}O_L) = \chi(1+\pi_L^{i_0}O_L)$ contains a primitive fourth root of unity, so $\chi(1+\pi_L^{2c(n-2)}O_L) \neq \{1\}$. If follows that $c(1) = c(n-1) \geq 2c(n-2) = 2i_0$, and if $c(1) > 2i_0$ then (15.23) implies

$$i_{n-1} = c(n-1) - c(n-2) \geq 2i_0 + 1 - i_0 = i_0 + 1 = d_0.$$

Thus the only way in which we could have $i_{n-1} < d_0$ is for $c(1) = 2i_0$, which shows that all of the conditions of Lemma 15.13 hold. □

LEMMA 15.15. – *Suppose hypotheses (i), (ii) and (iii) of Lemma 15.13 hold and that $i_0 > 1$. There is an inclusion of multiplicative groups*

$$1 + \pi_L^{2i_0}O_L \subset (\mathrm{Norm}_{L/K}L^*) \cdot (L^*)^4 \cdot (1+\pi_L^{2i_0+1}O_L). \tag{15.26}$$

Proof. – By Lemma 14.8, d_0 is even. We have

$$i_0 = d_1 + d_2 - d_0 - 1 = d_0 - 1$$

by Lemma 15.10 and hypothesis (ii) of Lemma 15.13. By [19, Lemme 5.1.1] and the paragraph following that lemma, we can choose the uniformizer π_L of L such that

$$\sigma(\pi_L) = \frac{\pi_L}{(1+\pi_L^{i_0})^{1/i_0}} \tag{15.27}$$

where $\sigma \in G$ projects to the non-trivial element of $\mathrm{Gal}(L/K)$.

For $i \geq 1$ the binomial theorem for fractional exponents now gives

$$\sigma(\pi_L^i) \equiv \pi_L^i \text{ (resp. } \pi_L^i(1+\pi_L^{i_0})\text{) mod } \pi_L^{2i_0+1}O_L \quad \text{if} \quad 2 \,|\, i \text{ (resp. } 2 \not| \, i\text{)}. \tag{15.28}$$

Suppose now that $\zeta \in k$. Define

$$h(\zeta) = (1+\pi_L+\zeta^2\pi_L^{i_0-1}) \cdot \sigma(1+\pi_L+\zeta^2\pi_L^{i_0-1}) = \mathrm{Norm}_{L/K}(1+\pi_L+\zeta^2\pi_L^{i_0-1}). \tag{15.29}$$

Using $i_0 > 1$ and the fact that $i_0 - 1$ is even, we have from (15.28) the following congruences mod $\pi_L^{2i_0+1}O_L$:

$$\begin{aligned} h(\zeta) &\equiv (1+\pi_L+\zeta^2\pi_L^{i_0-1})(1+\pi_L+\pi_L^{i_0+1}+\zeta^2\pi_L^{i_0-1}) \\ &\equiv 1+\pi_L^2+\zeta^4\pi_L^{2(i_0-1)}+\pi_L^{i_0+1}+\pi_L^{i_0+2}+\zeta^2\pi_L^{2i_0} \\ &\equiv h(0)+\zeta^4\pi_L^{2(i_0-1)}+\zeta^2\pi_L^{2i_0}. \end{aligned} \tag{15.30}$$

Here

$$h(0)^{-1} = \left(1+\pi_L^2+\pi_L^{i_0+1}+\pi_L^{i_0+2}\right)^{-1} \equiv 1-\pi_L^2 \mod \pi_L^3 O_L \tag{15.31}$$

since $i_0 \geq 3$. Thus (15.30) gives congruences

$$\begin{aligned} h(0)^{-1}h(\zeta) &\equiv 1+h(0)^{-1}(\zeta^4\pi_L^{2(i_0-1)}+\zeta^2\pi_L^{2i_0}) \mod \pi_L^{2i_0+1}O_L \\ &\equiv 1+(1-\pi_L^2)(\zeta^4\pi_L^{2(i_0-1)}+\zeta^2\pi_L^{2i_0}) \mod \pi_L^{2i_0+1}O_L \\ &\equiv (1+\zeta^4\pi_L^{2(i_0-1)})\cdot(1+(\zeta^2-\zeta^4)\pi_L^{2i_0}) \mod \pi_L^{2i_0+1}O_L \end{aligned} \tag{15.32}$$

where the last congruence holds because

$$2(i_0-1)+2i_0 = 4i_0-2 \geq 2i_0+1$$

since $i_0 \geq 3$. Because $i_0 \geq 3$ is odd, $(i_0-1)/2 \geq 1$ is an integer. Hence (15.32) gives

$$(1+\zeta\pi_L^{(i_0-1)/2})^{-4} \cdot h(0)^{-1} \cdot h(\zeta) \equiv 1+(\zeta^2-\zeta^4)\pi_L^{2i_0} \mod \pi_L^{2i_0+1}O_L. \tag{15.33}$$

Now for each $\lambda \in k$, there is a $\zeta \in K$ such that $\zeta^2-\zeta^4 = \lambda$. By (15.29), $h(0)^{-1} \in \mathrm{Norm}_{L/K}(L^*)$. We conclude from (15.33) that

$$1+\pi_L^{2i_0}O_L \subset (L^*)^4 \cdot \mathrm{Norm}_{L/K}(L^*) \cdot (1+\pi_L^{2i_0+1}O_L)$$

which proves Lemma 15.15. □

COROLLARY 15.16. – *Hypotheses (i), (ii) and (iii) of Lemma 15.13 imply* $i_0 = 1$.

Proof. – Suppose $i_0 > 1$. By part (iii) of Lemma 15.13, χ is not trivial on $1 + \pi^{2i_0} O_L$ but trivial on $1 + \pi^{2i_0+1} O_L$. Since G is the quaternion group of order 8, the character χ has order $2^n = 4$. By Lemma 15.3, χ is trivial on $\mathrm{Norm}_{L/K}(L^*)$. Hence χ is trivial on $(\mathrm{Norm}_{L/K} L^*) \cdot (L^*)^4 \cdot (1 + \pi_L^{2i_0+1} O_L)$ so χ is trivial on $1 + \pi^{2i_0} O_L$ by Lemma 15.15, which is a contradiction. This proves that we must have $i_0 = 1$. □

Completion of the proof of Proposition 15.6. – We begin with statement (i) of the proposition.

Suppose first that i_{n-1} is odd. By Lemma 15.13, we can reduce the case in which G satisfies the hypotheses of Lemma 15.13. By Corollary 15.16, $i_0 = 1$. For $i = 0, 1, 2$, let $H_i = \mathrm{Gal}(N/L_i)$ where L_i is the quadratic extension of K described in Lemma 14.8, so that $H = H_0$. The first (and only) jump in the upper (and lower) ramification filtration on G/H_i occurs at $d_i - 1$. By Lemma 15.13, $d_0 = d_1 = d_2$. Therefore if $\nu \in \mathbb{R}$ is a jump in the ramification filtration of G/H_i for one i, it is a jump in this filtration for all i. The image of the higher ramification group G^ν in G/H_i is equal to the ramification group $(G/H_i)^\nu$. It follows that $G^\nu \cap H_i$ has order independent of $i \in \{0, 1, 2\}$. Hence G^ν is either G, $\{e\}$ or the center $\mathrm{C}(G) = \{e, \tau^2\}$ of G. By Lemma 15.13 and the definition of i_0 in Lemma 15.10, the jumps in the ramification filtration of $H_0 = H = \mathrm{Gal}(N/L)$ occur at the integers $i_0 = 1$ and at $2i_0 = 2$. Hence by the Hasse-Arf Theorem (see Lemma 14.1), the jumps in the lower numbering of the ramification filtration of H occur at 1 and at $1 + 2 = 3$. Since each ramification group is either G, $\{e\}$ or $\mathrm{C}(G)$, we conclude that the lower numbering of the ramification filtration of G is

$$G = G_0 = G_1 \supset \mathrm{C}(G) = G_2 = G_3 \supset G_4 = \{e\}. \tag{15.34}$$

Suppose now that G is the quaternion group of order 8 and $G_4 = \{e\}$. From $G_4 = \{e\}$ and Lemma 14.1 we must have $H = H_0 = H_1 \supset H_2 = 2H = H_3 \supset H_4 = \{e\}$. Since this holds true for each of the cyclic subgroups H of index 2 in G, the lower ramification filtration of G must be given by (15.34). Since $\#G = 8$, we have $n = 2$. Lemmas 15.4 and 14.1 give that $i_0 = i_1 = 1$, so that $i_{n-1} = i_1$ is odd.

We now check that if G has order 8 and ramification filtration (15.34) then the Bertin obstruction does not vanish. Let $T = \mathrm{C}(G)$. The set $S(T)$ of cyclic subgroups of G which contain T is $\{T, H_0, H_1, H_2\}$. The constant b_T appearing in Theorem 2.3 is thus

$$b_T = \frac{1}{[\mathrm{N}_G(T) : T]} \left(-\delta(T, \{e\}) a_\phi(1) + \sum_{\Gamma \in S(T)} \mu([\Gamma : T]) \iota(\Gamma) \right) = -\frac{1}{2}. \tag{15.35}$$

Proposition 2.1 now shows that the Bertin obstruction associated to the given action of G on N does not vanish. This completes the proof of part (i) of Proposition 15.6.

We now suppose that as in part (ii) of Proposition 15.6, G is a generalized quaternion group and i_{n-1} is even. We claim that not all of hypotheses (i), (ii) and (iii) of Lemma 15.13 can hold. Suppose to the contrary that all of these hypotheses do hold. Thus $n = 2$, $c(1) = 2i_0$, and by Corollary 15.16, $i_0 = 1$. Thus Lemma 15.4 gives $i_{n-1} = i_1 = c(1) - c(0) = c(1) - i_0 = i_0 = 1$. This contradicts our assumption that i_{n-1} is even, so not all of hypotheses (i), (ii) and (iii) of Lemma 15.13 hold. Therefore Lemma 15.14 proves

$i_{n-1} \geq d_0$. Hence Corollaries 14.11(c), 14.12 and 14.13 show that the KGB obstruction vanishes.

To prove the final statement (iii) in Proposition 15.6, we know by Lemma 15.13 that i_{n-1} is even if G is semi-dihedral. Since the d_i are all even, we conclude from Corollary 14.11(d) that the Bertin obstruction does not vanish if

$$d_0 + d_1 + d_2 \equiv d_0 + d_1 - d_2 \not\equiv 0 \mod 4\mathbb{Z}. \tag{15.36}$$

□

16. The group $\mathrm{SL}_2(3)$ when $p = 2$

PROPOSITION 16.1. – *Suppose $p = 2$ and that G is isomorphic to $\mathrm{SL}_2(3)$. A 2-Sylow subgroup P of G is normal and isomorphic to a quaternion group of order 8. The Bertin obstruction associated to an injection $\phi : G \to \mathrm{Aut}_k(k[[t]])$ vanishes if and only if the Bertin obstruction associated to the restriction ϕ_P of $\phi = \phi_G$ from G to P vanishes. These two equivalent conditions hold if and only if the KGB obstructions of both ϕ and ϕ_P vanish.*

Proof. – Because of Theorem 6.6, the Bertin obstruction of ϕ_P vanishes if that of ϕ does, and we now prove the converse. We suppose for the rest of the proof that Bertin obstruction of ϕ_P vanishes. To show that the Bertin obstruction of ϕ_G vanishes, it will be enough to show that conditions (b), (c) and (d) of Theorem 6.6 hold.

Let t be a non-trivial element of the cyclic group C of order 3. Then $\mathrm{C}_G(t) = \mathrm{C}_P(t) \times C$ where $\mathrm{C}_P(t)$ is the center $\mathrm{C}(G)$ of G, which has order 2. This shows condition (b) of Theorem 6.6.

The cyclic non-trivial subgroups T of P are $\mathrm{C}(G)$ together with the three cyclic subgroups $\Gamma(1)$, $\Gamma(2)$ and $\Gamma(3)$ of order 4 which are conjugate under the action of C. There are four conjugates $C(1) = C$, $C(2)$, $C(3)$ and $C(4)$ of C in G. Let $J(j) = \langle \mathrm{C}(G), C(j) \rangle$ be the cyclic group of order 6 generated by $C(j)$ and $\mathrm{C}(G)$. One has

$$S_G(\mathrm{C}(G)) = \{\mathrm{C}(G), \Gamma(1), \Gamma(2), \Gamma(3), J(1), J(2), J(3), J(4)\} \tag{16.1}$$

and

$$S_G(\Gamma(j)) = \{\Gamma(j)\}. \tag{16.2}$$

In the notation of Theorem 6.6, we have

$$b'_{\mathrm{C}(G),G} = \sum_{P \not\supset \Gamma \in S_G(\mathrm{C}(G))} \mu([\Gamma : \mathrm{C}(G)]) = \sum_{j=1}^{4} \mu([J(j) : \mathrm{C}(G)]) = -4. \tag{16.3}$$

Since every $\Gamma \in S_G(\Gamma(j))$ is contained in P, we have

$$b'_{\Gamma(j),G} = \sum_{P \not\supset \Gamma \in S_G(\Gamma(j))} \mu([\Gamma : \Gamma(j)]) = 0. \tag{16.4}$$

Condition (c.i) of Theorem 6.6 is that $b'_{T,G} \equiv 0 \bmod [\mathrm{N}_P(T) : T]\mathbb{Z}$, which we see follows from (16.3) and (16.4) since $[\mathrm{N}_P(\mathrm{C}(P)) : P] = 4$.

Since we have supposed that the Bertin obstruction of ϕ_P vanishes, we have $b_{T,P} \geq 0$ for $T = \mathrm{C}(G)$ and $T = \Gamma(j)$. Condition (c.ii) of Theorem 6.6 is that

$$[\mathrm{N}_G(P) : T] b_{T,P} = \sum_{\Gamma \in S_P(T)} \mu([\Gamma : T]) \iota(T) \geq -b_{T,G}. \tag{16.5}$$

When $T = \Gamma(j)$, this follows from $b_{\Gamma(j),P} \geq 0 = -b_{\Gamma(j),G}$. We now assume that $T = \mathrm{C}(G)$, so that $-b_{T,G} = -b_{\mathrm{C}(G),G} = 4$. It remains to prove the inequality (16.5) in this case.

Let $H = \Gamma(1)$ be one of the three cyclic subgroups of order 4 in P. Let i_0 and i_1 be the integers associated to ϕ_P and to H in Lemma 14.1. Let $\chi : H \to \mu_4$ be a faithful character of H. We let $L = N^H$ be the fixed field of H acting on N, where N/F is the G extension associated to ϕ_G. By classfield theory, we can view χ as a character of L^*, after reducing to the case of quasi-finite residue fields via Proposition 13.2. By Lemma 15.4, i_0 is the largest integer such that $\chi(1 + \pi_L^{i_0} O_L) = \mu_4$, while i_1 is the largest integer such that $\chi(1+\pi_L^{i_0+i_1} O_L) = \{\pm 1\}$. Since $(1+\pi_L^{i_0} O_L)^2 \subset 1+\pi_L^{2i_0} O_L$ we conclude that $i_0 + i_1 \geq 2i_0$, so $i_1 \geq i_0$. By Corollary 14.11, i_0 is odd and i_1 is even since the Bertin obstruction to ϕ_P is trivial. Hence $i_1 \geq i_0$ implies $i_1 = i_0 + 1 + 2h$ for some $h \geq 0$. By the definition of i_0 and i_1, the jumps in the upper ramification filtration of H occur at i_0 and $i_0 + i_1$. By Herbrand's theorem [28, Chap. IV.3, Lemma 5], the jumps in the lower ramification filtration occur at i_0 and $i_0 + 2i_1 = i_0 + 2(i_0 + 1 + 2h) = 3i_0 + 2 + 4h$. Now $\mathrm{C}(G)$ is the order 2 subgroup of H, so the jumps in the lower and the upper ramification filtration of $\mathrm{C}(G)$ both occur at $3i_0+2+4h$. Recall that $J(1)$ is a cyclic group of order 6 which contains $\mathrm{C}(G)$ (see (16.1)). By the Hasse-Arf Theorem, the jumps in the upper ramification of $J(1)$ occur at integers $j_0 = 0$ and $j_1 \geq 0$ since $J(1)$ is abelian and the wild ramification subgroup of $J(1)$ is $\mathrm{C}(G)$. Herbrand's theorem now shows that the jumps in the lower ramification of $J(1)$ occur at 0 and at $3j_1$. Therefore the (unique) jump in the lower ramification of $\mathrm{C}(G)$ occurs at $3j_1 = 3i_0 + 2 + 4h$. This and $h \geq 0$ force $h = 1 + 3h'$ for some $0 \leq h' \in \mathbb{Z}$. Thus

$$i_1 = i_0 + 1 + 2h = i_0 + 1 + 2(1 + 3h') = i_0 + 3 + 6h' \quad \text{with} \quad 0 \leq h' \in \mathbb{Z}. \tag{16.6}$$

Since $\Gamma(1)$ is conjugate to Γ_j for $j = 2, 3$, we have $\iota(\Gamma(1)) = \iota(\Gamma(j))$ for $j \in \{1, 2, 3\}$. Considering that the jumps in the lower numbering of $H = \Gamma(1)$ occur at i_0 and $i_0 + 2i_1$, we conclude that

$$\iota(\mathrm{C}(G)) = i_0 + 2i_1 + 1 = i_0 + 2(i_0 + 3 + 6h') + 1 = 3i_0 + 7 + 12h' \tag{16.7}$$

and

$$\iota(\Gamma(1)) = i_0 + 1. \tag{16.8}$$

Now

$$\begin{aligned} [\mathrm{N}_P(\mathrm{C}(G)) : \mathrm{C}(G)] b_{\mathrm{C}(G),P} &= \sum_{\mathrm{C}(G) \subset \Gamma \in S_P(\mathrm{C}(G))} \mu([\Gamma : \mathrm{C}(G)]) \iota(\Gamma) \\ &= \iota(\mathrm{C}(G)) - 3\iota(\Gamma(1)) \\ &= 3i_0 + 7 + 12h' - 3(i_0 + 1) \\ &= 4 + 12h' \geq 4 = -b'_{\mathrm{C}(G),G} \end{aligned} \tag{16.9}$$

because of (16.7), (16.8) and (16.3). This proves (16.5) for $T = \mathrm{C}(G)$, which completes the proof of condition (c.ii) of Theorem 6.6.

We finally consider condition (d) of Theorem 6.6. If $T = \mathrm{C}(G)$ then $\mathrm{C}_C(T) = C = \mathrm{N}_C(T)$ and

$$\psi(\mathrm{C}(G), G) = \sum_{\Gamma \in S_G(\mathrm{C}(G))} \mu([\Gamma : \mathrm{C}(G)]) = 1 - 3 - 4 = -6 \equiv 0 \mod \#\mathrm{N}_C(T)\mathbb{Z}$$

since $\#\mathrm{N}_C(T) = 3$. Thus condition (d.ii) of Theorem 6.6 holds for $T = \mathrm{C}(G)$. The other non-trivial cyclic subgroups T of p-power order in G are the $\Gamma(j)$ for $j = 1, 2, 3$. We have $\mathrm{N}_C(\Gamma(j)) = \{e\} = \mathrm{C}_C(\Gamma(j))$, so condition (d.ii) of Theorem 6.6 holds trivially for $T = \Gamma(j)$. This completes the proof that the Bertin obstruction of ϕ_G vanishes if and only if that of ϕ_P does.

It remains to prove the last assertion of the proposition. It follows from Proposition 15.6 that the Bertin obstruction of ϕ_P vanishes if and only if the KGB obstruction of ϕ_P vanishes. By Theorem 4.2, if the KGB obstruction of ϕ_G vanishes then the Bertin obstruction of ϕ_G does also. So to finish the proof of Proposition 16.1, it will suffice to show that if the Bertin obstructions of ϕ_G and ϕ_P vanish then the KGB obstruction of ϕ_G vanishes.

We can choose a set $\mathscr{C}_G$ of representatives for the conjugacy classes of non-trivial cyclic subgroups of G in the following way:

$$\mathscr{C}_G = \{\mathrm{C}(G), \Gamma(1), C(1), J(1)\}. \tag{16.10}$$

We have

$$b_{\Gamma(1),G} = \frac{1}{[\mathrm{N}_G(\Gamma(1)) : \Gamma(1)]} \sum_{\Gamma \in S_G(\Gamma(1))} \mu([\Gamma : \Gamma(1)])\iota_G(\Gamma) = \frac{\iota(\Gamma(1))}{2} = \frac{i_0 + 1}{2}. \tag{16.11}$$

Thus $b_{\Gamma(1),G} > 0$, and this is integral by Proposition 2.1 because the Bertin obstruction of ϕ_G vanishes. One has $\mathrm{N}_G(C(1)) = J(1) \neq C(1)$ and $\mathrm{N}_G(J(1)) = J(1)$, so Proposition 3.2 gives

$$b_{C(1),G} = 0 \quad \text{and} \quad b_{J(1),G} = 1. \tag{16.12}$$

From Theorem 4.2 and Proposition 2.1, to show that the KGB obstruction vanishes, it will be enough to construct for each $T \in \mathscr{C}_G$ a sequence B_T of $b_{T,B}$ elements of G such that each $b \in B_T$ generates a conjugate of T and $\prod_{T \in \mathscr{C}_G} \prod_{b \in B_T} b$ has order $[G : G_1] = \#C = 3$ after choosing some ordering for $\coprod_{T \in \mathscr{C}_G} B_T$. Here $b_{\Gamma(1),G} > 0$, so since we can choose the elements of $B_{\Gamma(1)}$ to be generators of any of the three (conjugate) order 4 subgroups of P, we can arrange that $\prod_{b \in B_{\Gamma(1)}} b$ has order 4. We know that $B_{C(1)} = \varnothing$ and that $B_{J(1)}$ has one element by (16.12). Now the product of an element of order 4 and an element of order 3 in $\mathrm{PSL}_2(3) = \mathrm{SL}_2(3)/\{\pm I\}$ is an element of order 3. Thus for any choice of $B_{\mathrm{C}(G)}$, the resulting product

$$\prod_{T \in \mathscr{C}_G} \prod_{b \in B_T} b$$

has order 3 image in $\mathrm{PSL}_2(3)$. We can make this element have order 3 in $\mathrm{SL}_2(3) = G$ by adjusting one of the elements of $B_{\Gamma(1)}$ by multiplying it by either the trivial or the non-trivial element of $\mathrm{C}(G)$. This completes the proof of Proposition 16.1. □

17. Proof of Theorem 1.2

By Corollary 12.8, the proof of Theorem 1.2 is reduced to showing the following results:

a. The groups listed in items (1)–(4) of Theorem 1.2 are KGB groups for k.
b. When $p = 2$, the quaternion group Q_8 and the group $\mathrm{SL}_2(3)$ are not Bertin groups for k.
c. When $p = 2$, no semi-dihedral group of order at least 16 is a Bertin group for k.

LEMMA 17.1. – *For all k, every cyclic group G is a KGB group for k.*

Proof. – Let G be a cyclic group with p-Sylow group H of order p^n. It was noted in Remark 1 of §4 of [2] that the Bertin obstruction of G vanishes. To show that the KGB obstruction vanishes, we first compute b_T when T is a non-trivial cyclic subgroup of G.

The lower numbering of the ramification groups of G has $G_0 = G$ and $G_i = H_i$ if $i > 0$. By Lemma 14.1, there are positive integers $i_0, i_1, \dots, i_{n-1}$ such that the jumps in the upper numbering of the ramification filtration of H occur at $i_0, i_0 + i_1, \dots, i_0 + i_1 + \cdots + i_{n-1}$. Write $\#G = mp^n$ for some integer m prime to p. By the Hasse-Arf Theorem, the jumps in the lower ramification filtration are at $q(-1) := 0$ if $m > 1$ together with the integers $q(\ell) := m \sum_{j=0}^{\ell} p^j i_j$ for $\ell = 0, \cdots, n-1$. We find by Corollary 14.3 that

$$\iota(p^\ell H) = 1 + q(\ell) \quad \text{for} \quad 0 \le \ell \le n-1 \quad ; \quad \iota(\Gamma) = 1 \quad \text{if} \quad \Gamma \not\subset H. \tag{17.1}$$

By Proposition 3.2,

$$b_T = 0 \text{ if } G \neq T \not\subset H \quad \text{and} \quad b_G = 1 \text{ if } G \neq H. \tag{17.2}$$

Otherwise, $T \subset H$ and we may write $T = p^\ell H$ for some $0 \le \ell \le n-1$. By Theorem 2.3,

$$\begin{aligned} b_T &= \frac{1}{[\mathrm{N}_G(T) : T]} \left(\sum_{\Gamma \in S(T)} \mu([\Gamma : T]) \iota(\Gamma) \right) \\ &= \frac{1}{mp^\ell} \left(\sum_{\Gamma \in S(T)} \mu([\Gamma : T]) + \sum_{\Gamma \in S(T), \Gamma \subset H} \mu([\Gamma : T])(\iota(\Gamma) - 1) \right) \\ &= \frac{1}{mp^\ell} \left(\delta(p^\ell H, G) + mp^\ell i_\ell \right) = \delta(p^\ell H, G) + i_\ell. \end{aligned} \tag{17.3}$$

(In the second sum in (17.3), only $\Gamma = H$ contributes if $\ell = 0$, while $\Gamma = p^\ell H$ and $\Gamma = p^{\ell-1} H$ contribute if $\ell > 0$. The last equality in (17.3) is a consequence of the fact that $p^\ell H = G$ if and only if $m = 1$ and $\ell = 0$.)

To show that the KGB obstruction vanishes, we start by picking an ordered set $\{g_t\}_{t \in \Omega}$ of elements of G such that each g_t is non-trivial, and the number of g_t which generate a given non-trivial $T \in \mathcal{C}$ is b_T. As in Theorem 4.2(b), we have to show that we can adjust these g_t so that they collectively generate G and so that $\prod_{t \in \Omega} g_t$ has order $[G : G_1] = m$.

Suppose first that $G = H$, so that $m = 1$. By (17.3), $b_H = 1 + i_0 \ge 2$. Hence there must be at least two distinct elements $u, v \in \Omega$ such that g_u and g_v generate $G = H$. Consider the product $g = \prod_{t \in \Omega - \{u,v\}} g_t$. It will suffice to show that there are generators g'_u and g'_v of G such that $g'_u g'_v = g^{-1}$, since then we can replace g_u by g'_u and g_v by g'_v to have a set with the required properties. We claim that for all primes p, the elements of a cyclic group $G = H$ of order p^n which are the product of two generators are exactly the set of squares in G (which equals G unless $p = 2$). This is clear for $n = 1$, and it follows by induction for all n. Thus to construct the required g'_u and g'_v, it will suffice to show that g above is a square if $p = 2$. So we now suppose $p = 2$. Then $1 + i_0$ is the valuation of the discriminant of the quadratic extension $k((t))^{2G}$ of $k((t))^G$ inside $k((t))$, and this must be even. Hence i_0 is odd so $b_G = 1 + i_0 > 0$ is even. Every $T \in \mathcal{C}$ except for $T = G$ is contained in $2G = 2H$. Hence

the product $g = \prod_{t\in\Omega-\{u,v\}} g_t$ lies in $2G = 2H$, and this completes the analysis of the case $G = H$.

We now suppose that $G \neq H$. By (17.2), the unique $T \in \mathscr{C}$ which is not a p-group and for which b_T is not 0 is $T = G$, and $b_G = 1$. We can therefore pick the first element g_u of $\{g_t : t \in \Omega\}$ to be a generator of G, and all the other elements will be in H. We are therefore done if H is trivial, so suppose from now on that H is non-trivial. Consider the product $\prod_{u\neq t\in\Omega} g_t \in H$. If $p = 2$ then all terms of this product are in $2H$ except for b_H terms in which g_t is a generator of H. Here $b_H = i_0 > 0$ by (17.3), and this is odd if $p = 2$. Thus we can pick an element $v \in \Omega - \{u\}$ such that g_v is a generator of H, and the number of $v' \in \Omega - \{u, v\}$ for which $g_{v'}$ generates H is even. Taking into account that g_u is a generator of G, we find that $g = \prod_{t\in\Omega} g_t$ lies in $2G$ if $p = 2$; and whether or not $p = 2$, this is the product of a generator g_u of G with an element of the p-Sylow subgroup H of G. This implies g has order divisible by m. It will suffice to show that we can pick elements $h_u, h_v \in H$ such that $g'_u = g_u h_u$ is a generator of G, $g'_v = g_v h_v$ is a generator of H, and

$$g'_u g'_v \prod_{t\in\Omega-\{u,v\}} g_t = h_u h_v g$$

has order m, since then we can simply replace g_u by g'_u and g_v by g'_v.

We first observe that $h_u h_v g$ always has order divisible by m since h_u and h_v are elements of p-power order and g has order divisible by m. Hence $h_u h_v g$ has order m if and only if $h_u^m h_v^m g^m = e$, where $g^m \in H$ and $g^m \in 2H$ if $p = 2$. Since $h_u \in H$ and g_u is a generator of G, the element $g'_u = g_u h_u$ will be a generator of G if and only if $g_u^m h_u^m$ is a generator of the p-Sylow subgroup H of G. This will be the case if h_u^m is not congruent mod pH to $g_u^{-m} \in H$. Similarly, $h_v g_v$ will be a generator of H if and only if $h_v^m g_v^m$ is such a generator, and this will be so if and only if h_v^m is not congruent mod pH to g_v^{-m}. We thus see that h_u^m and h_v^m are to be elements of H which each avoid a particular congruence class mod pH which generates H mod pH, and for which $h_u^m h_v^m$ is equal to g^m, where $g^m \in H$ and $g^m \in 2H$ if $p = 2$. Since H is cyclic of order p^n, one sees by induction on n that such h_u^m and h_v^m always exist. Since m is prime to p, we can then find h_u and h_v in H with the required properties, which completes the proof. □

PROPOSITION 17.2. – *For all primes p and integers $n \geq 1$, the dihedral group D_{2p^n} is a KGB group for k. If $p = 2$, then the following hold:*

i. *If G is a generalized quaternion group of order $2^n \geq 16$, then G is a KGB group for k.*
ii. *If G is the quaternion group of order 8, G is an almost KGB group for k.*
iii. *If G is a semi-dihedral group then G is not an almost Bertin group for k.*

Proof. – By Corollaries 14.11, 14.12, 14.13 and 15.5, D_{2p^n} is a KGB group for k, for all p. Now assume that $p = 2$. These corollaries together with Proposition 15.6(iii) imply statements (i) and (ii) concerning generalized quaternion groups. Suppose now that G is a semi-dihedral group. We can construct a Klein four extension L'/K such that the exponents d_0, d_1 and d_2 of the discriminants of the three quadratic subfields (as in Lemma 14.8) are larger than a specified number and for which $d_0 + d_1 + d_2$ is not divisible by 4. By parts (i) and (ii) of Proposition A.3 of Appendix 1, we can realize this L'/K as a subfield of a

G-extension of K such that the first jump in the ramification filtration of G occurs above a specified number. Proposition 15.6(iii) now shows G is not an almost Bertin group for k. □

COROLLARY 17.3. – *When $p = 2$, the group $\mathrm{SL}_2(3)$ is an almost KGB group for k.*

Proof. – This follows from Propositions 17.2 and 16.1. □

LEMMA 17.4. – *When $p = 2$, the alternating group A_4 is a KGB group for k.*

Proof. – We can take the set $\mathscr{C}$ to consist of a group H_2 of order 2 and a group H_3 of order 3. Since $\mathrm{N}_G(H_3) = H_3$, Proposition 3.2 shows $b_{H_3} = 1$. There is no cyclic subgroup of A_4 which properly contains H_2, and $\mathrm{N}_{A_4}(H_2)$ has order 4, so

$$b_{H_2} = \frac{1}{[\mathrm{N}_{A_4}(H_2) : H_2]}\iota(H_2) = \frac{\iota(H_2)}{2}.$$

Since H_2 has order $p = 2$, the first (and only) jump i_0 in the upper (and lower) ramification filtration of H_2 occurs at an odd integer, so $\iota(H_2) = 1 + i_0 \geq 2$ is even. Thus $b_{H_2} \geq 1$ is an integer. This shows that Bertin obstruction associated to local A_4 covers in characteristic 2 is trivial. Since $b_{H_3} = 1$ and the 2-Sylow of A_4 is normal, if we choose any set of generators for the stabilizers appearing in the product described in the KGB condition of Theorem 4.2(b), this product will not lie in the 2-Sylow of A_4. Therefore this product has to be an element of order $3 = [A_4 : (A_4)_1]$, so the KGB condition holds. □

In view of the remarks at the beginning of this section, the following result completes the proof of Theorem 1.2.

LEMMA 17.5. – *Suppose $p = 2$. The quaternion group Q_8 of order 8 and the group $\mathrm{SL}_2(3)$ are not Bertin groups for k.*

Proof. – By Proposition 16.1, it will be enough to construct an injection

$$\phi : G = \mathrm{SL}_2(3) \to \mathrm{Aut}_k(k[[t]])$$

such that the restriction of G to the (unique) 2-Sylow subgroup P of G has non-trivial Bertin obstruction, where P is isomorphic to Q_8. By Proposition 15.6(ii), it will be enough to construct an example of this kind in which the lower ramification filtration of P has the form $P = P_0 = P_1, \mathrm{C}(P) = P_2 = P_3$ and $P_4 = \{e\}$. By [30, Ex. A.1.b], there is an elliptic curve E over k whose automorphism group $G = \mathrm{Aut}(E)$ is isomorphic to $\mathrm{SL}_2(3)$. Every element of G fixes the origin $\underline{0}$ of E, so $\underline{0}$ is totally ramified over its image c in the quotient cover $E \to E/G$. Let $P_{\underline{0},i}$ be the i^{th} lower ramification subgroup of P acting on the completion of the local ring of $\underline{0}$ on E. Then $P_{\underline{0},0} = P_{\underline{0},1} = P$. By applying Lemma 14.1 to the action of a cyclic subgroup H of order 4 in P, we see that $P_{\underline{0},2}$ and $P_{\underline{0},3}$ must be non-trivial. The Hurwitz formula gives

$$\begin{aligned} 0 = 2g(E) - 2 &= 8 \cdot (2g(E/P) - 2) + \sum_{i=0}^{\infty}(\#P_{\underline{0},i} - 1) + r_{\neq 0} \\ &= 8 \cdot (2g(E/P) - 2) + 16 + \sum_{i=2}^{3}(\#P_{\underline{0},i} - 2) + \sum_{i=4}^{\infty}(\#P_{\underline{0},i} - 1) + r_{\neq 0} \end{aligned} \tag{17.4}$$

where $r_{\neq 0}$ is the contribution of ramification points of the cover $E \to E/P$ which are not equal to $\underline{0}$. This implies $g(E/P) = 0$, $r_{\neq 0} = 0$ and that the ramification filtration of $P = P_{\underline{0}}$ has the required form, in the sense that $P = P_0 = P_1$, $\mathrm{C}(P) = P_2 = P_3$ and $P_4 = \{e\}$. Hence the action of G on the completion of the local ring of E at $\underline{0}$ defines an injection $\phi : G = \mathrm{SL}_2(3) \to \mathrm{Aut}_k(k[[t]])$ for which the Bertin obstruction does not vanish. □

18. Proof of Theorem 1.5

By Corollary 5.6, if a quotient of a group G is not an almost Bertin group then G is not an almost Bertin group for k. The Bertin groups for k have been determined in Theorem 1.2, and each of these is a KGB group for k and hence an almost KGB group for k. Hence by Theorems 11.1 and 11.2, Theorem 1.5 follows from the following assertions, which have already been shown:

i. The groups listed in items (1)–(5) of Theorem 11.1 are not almost Bertin groups for k if $p = \mathrm{char}\, k \neq 2$. This follows from Corollary 12.4, since each of the groups (1)–(5) in Theorem 11.1 are cyclic-by-p.
ii. The groups listed in items (1)–(7) of Theorem 11.2 are not almost Bertin groups for k if $\mathrm{char}\, k = 2$. This follows from Corollary 12.5, Proposition 12.6 and Proposition 12.7.
iii. The groups H_8 and $\mathrm{SL}_2(3)$ are almost KGB groups k if $\mathrm{char}\, k = 2$. This was shown in Proposition 17.2 and Corollary 17.3.
iv. Semi-dihedral groups are not almost Bertin groups in characteristic 2. This was shown in Proposition 17.2.

Appendix A
Constructing extensions with prescribed ramification

In this section we suppose G is a finite group which is the semi-direct product of a normal p-group P with a finite cyclic group C of order prime to p.

Definition A.1. – Suppose that G is a GM group for k with respect to a faithful character $\Theta : B \to \mathbb{Z}_p^*$ as in Definition 1.7. Let $\Theta_C : C \to W(k)^*$ be an extension of Θ to a faithful character of C. An injection $\phi_G : G \to \mathrm{Aut}_k(k[[z]])$ will be said to be GM for Θ_C if

$$\phi_G(c)(u)/u \equiv \overline{\Theta}_C(c)^{-1} \mod uk[[u]] \tag{A.1}$$

for some uniformizer u in $k[[z]]^{\phi_G(P)}$, where $\overline{\Theta}_C : C \to k^*$ is the reduction of Θ_C mod $pW(k)$.

Lemma A.2. – *Suppose $G = C$. Then G is GM with respect to any given faithful character $\Theta : B \to \mathbb{Z}_p^*$. Let $\Theta_C : C \to W(k)^*$ be a faithful extension of Θ. There is an injection $\phi_G : G \to \mathrm{Aut}_k(k[[z]])$ which is GM with respect to Θ_C.*

Proof. – The first statement is clear from Definition 1.7. For the second statement, pick a root of unity $\zeta \in k^*$ of order $\#C$ and a generator c of $C = G$. Let $\phi'_G : G \to \mathrm{Aut}_k(k[[z]])$ be the injection for which $\phi'_G(c)(z) = \zeta c$. Since $\mathrm{Aut}(C)$ acts transitively on the faithful characters of C, there will be a unique $\alpha \in \mathrm{Aut}(C)$ such that $\phi_G = \phi'_G \circ \alpha$ will be GM with respect to Θ_C. □

The main result of this section is:

PROPOSITION A.3. – *Suppose H is a quotient group of G, and let $H(p)$ be the p-Sylow subgroup of H. Let M be a positive integer. There is an integer $M' \geq 1$, with $M' = 1$ if $M = 1$, for which the following is true. Suppose $\phi_H : H \to \mathrm{Aut}_k(k[[t]])$ is an injection such that the lower ramification group $H_{M'-1}$ contains $H(p)$. Let J be the kernel of the surjection $\pi : G \to H$. Then there is an injection $\phi_G : G \to \mathrm{Aut}_k(k[[z]])$ with the following properties:*

i. *There is a k-isomorphism between $k[[z]]^J$ and $k[[t]]$ such that the induced action of $G/J = H$ on $k[[t]]$ is given by ϕ_H.*
ii. *The lower ramification group G_{M-1} contains P.*
iii. *Suppose $J \subset P$, G is GM with respect to $\Theta : B \to \mathbb{Z}_p^*$, and $\Theta_C : C \to W(k)^*$ is a faithful extension of Θ to C. Suppose ϕ_H is GM with respect to Θ_C. Then ϕ_G is GM with respect to Θ_C.*
iv. *Suppose $J \subset P$ and T is a proper non-trivial cyclic subgroup of J. Then $\iota_G(T) \equiv 0$ mod p^{M-1}, where as before $\iota_G(T)$ is $i+1$ if i is the largest integer such that T lies in the ramification group G_i. Let Γ be cyclic subgroup of P containing T such that $J \not\supset \Gamma$. Then $\iota_G(T) > \iota_G(\Gamma) + M$.*
v. *Suppose $M > 1$, $J \subset P$ and $\iota_H(T') \equiv 0$ mod $p^{M'-1}$ for all non-trivial cyclic p-subgroups T' of H. Then $\iota_G(T) \equiv 0$ mod p^{M-1} for all non-trivial cyclic p-subgroups T of G.*

The remainder of this section is devoted to proving Proposition A.3. For a related result, see the work of Pries in [25, Prop. 2.7]. Since J is solvable we have the following result by induction on $\#J$.

LEMMA A.4. – *To prove Proposition A.3, it will suffice to consider the case in which J is abelian and the conjugation action of H on J makes J into a simple $\mathbb{Z}[H]$-module. We will assume J to be such a module for the rest of this section.*

LEMMA A.5. – *Given any $\phi_H : H \to \mathrm{Aut}_k(k[[t]])$ as in Proposition A.3, there is always an injection $\phi_G : G \to \mathrm{Aut}_k(k[[z]])$ for which condition (i) of the proposition holds. To complete the proof of the proposition, it will suffice to show that there is a ϕ_G for which (i) and (iv) hold.*

Proof. – It is shown in [8, Lemma 2.10] that there is always a ϕ_G as in part (i). We now show part (iii) of Proposition A.3. (See Lemma A.2 for the case $G = C$.) Let J, G, Θ_C and ϕ_H be as in part (iii), so that ϕ_H is GM for Θ_C. Then the identification of $k[[t]]$ with $k[[z]]^{\phi_G(J)}$ identifies $k[[z]]^{\phi_G(P)}$ with $k[[t]]^{\phi_H(P/J)} = k[[u]]$. We have identified C as a subgroup of both G and H, and the actions of $\phi_G(c)$ and $\phi_H(c)$ on $k[[u]]$ for $c \in C$ must be the same since ϕ_G induces ϕ_H. Since ϕ_H is GM with respect to Θ_C,

$$\phi_H(c)(u)/u \equiv \overline{\Theta}_C(c)^{-1} \mod uk[[u]].$$

Thus this congruence holds when ϕ_H is replaced by ϕ_G; so ϕ_G is GM with respect to Θ_C.

To complete the proof of Lemma A.5 now amounts to showing that if we can always construct an M' for which parts (i) and (iv) of Proposition A.3 hold, then we can construct an M' for which parts (ii) and (v) also hold. By increasing M', we can assume $M' \geq M$.

Let σ be a non-trivial element of G of p-power order, and define $\sigma' = \pi(\sigma) \in H$. To show G_{M-1} contains P as in part (ii), it will suffice to show

$$i_G(\sigma) \geq M. \tag{A.2}$$

To show part (v), it will be enough to prove

$$\iota_G(\langle\sigma\rangle) \equiv 0 \mod p^{M-1}\mathbb{Z}. \tag{A.3}$$

Suppose first J is a p-group. If $\sigma \in J$, then condition (iv) applied to the subgroup $\langle\sigma\rangle$ generated by σ shows $0 < i_G(\sigma) = \iota_G(\langle\sigma\rangle) \equiv 0 \bmod p^{M-1}$, which shows (A.3). We also have $i_G(\sigma) \geq p^{M-1} \geq M$ which proves (A.2). Suppose now that $\sigma \notin J$, so that $\sigma' = \pi(\sigma) \in H$ is not trivial. By [28, Chap. IV.1, Prop. 3],

$$i_H(\sigma') = \frac{1}{\#J} \sum_{\nu \in G, \pi(\nu) = t'} i_G(\nu) = \frac{1}{\#J} \sum_{j \in J} i_G(\sigma j). \tag{A.4}$$

From [28, Chap. IV.1] we have

$$i_G(\sigma j) \geq \mathrm{Inf}(i_G(\sigma), i_G(j)).$$

Since $\sigma \notin J$ and we have supposed that (iv) holds, we have $i_G(j) > i_G(\sigma)$ for all $j \in J$, where $i_G(e) = \infty$ by definition if e is the identity element of J. It follows that $i_G(\sigma j) \geq i_G(\sigma)$ for all $j \in J$, and similarly $i_G(\sigma) = i_G(\sigma j j^{-1}) \geq i_G(\sigma j^{-1})$, so $i_G(\sigma j) = i_G(\sigma)$ for $j \in J$. Thus (A.4) becomes $i_H(\sigma') = i_G(\sigma)$, so $\iota_G(\langle\sigma\rangle) = i_G(\sigma) = i_H(\sigma') = \iota_H(\langle\sigma'\rangle)$. Because we chose $M' \geq M$, part (iv) now gives $0 < i_G(\sigma) = \iota_H(\langle\sigma'\rangle) \equiv 0 \bmod p^{M-1}$, so $i_G(\sigma) \geq p^{M-1} \geq M$ as above, which completes the proof of (A.2) and (A.3) when J is a p-group.

Suppose now that J is not a p-group. We only need to show (A.2), since statement (v) of Proposition A.3 holds vacuously. Since J is a simple $\mathbb{Z}[H]$-module, it has order prime to p. Therefore $\sigma' = \pi(\sigma)$ has the same order as σ, and in particular is not trivial. The group $P.J$ generated by P and J has normal subgroups P and J, and these groups have coprime order and the product of their orders is $\#P.J$. Hence $P.J$ is isomorphic to $P \times J$ and we conclude that P and J commute. Thus if $e \neq j \in J$ then tj is not of p-power order and so $i_G(\sigma j) = 1$. In this way, (A.4) becomes

$$i_H(\sigma') = \frac{1}{\#J} \sum_{j \in J} i_G(\sigma j) = \frac{i_G(\sigma) + \#J - 1}{\#J}.$$

This shows

$$i_G(\sigma) - i_H(\sigma') = (\#J - 1)(i_H(\sigma') - 1) \geq 0.$$

Thus $M' \geq M$ and the assumption that $H_{M'-1}$ contains $H(p)$ in Proposition A.3 implies

$$i_G(\sigma) \geq i_H(\sigma') \geq M' \geq M.$$

This establishes (A.2) and completes the proof. □

The following corollary is now clear from Lemma A.5 because condition (iv) of Proposition A.3 holds vacuously if J has order prime to p.

COROLLARY A.6. – *Suppose J is abelian and is a simple $\mathbb{Z}[H]$-module of order prime to p. Then Proposition A.3 holds.*

For the rest of this section we assume the hypotheses of the following lemma.

LEMMA A.7. – *Suppose J is abelian and is a simple $\mathbb{Z}[H]$-module of p-power order. Let $c = \#C$ be the order of the prime to p-part of $\#G$ (and of $\#H$). There is a divisor c' of c such that J has the following description. There is an isomorphism of abelian groups between J and the additive group $\mathbb{F}_{p^d}^+$ of the finite field $\mathbb{F}_{p^d}$ of order p^d such that the action of H on J is given by the inflation to H of a multiplicative character $\chi : C \to \mathbb{F}_{p^d}^*$ of order c'. The field $\mathbb{F}_{p^d}$ is generated over $\mathbb{F}_p$ by a primitive c'^{th} root of unity. We can choose a uniformizer w in $k[[t]]^{H(p)}$ in such a way that there is a faithful character $\chi' : C \to k^*$ with the property that $\phi_H(\sigma)$ sends w to $\chi'(\sigma)w$ for all $\sigma \in C$ under the natural identification of $C = H/H(p)$ with $\mathrm{Gal}(k((w))/k((t))^H)$.*

Proof. – Recall that since J is a p-group, the surjection $G \to H$ is an isomorphism on C; so we can view C as a subgroup of H. Thus H is the semi-direct product $H(p).C$. All simple $(\mathbb{Z}/p)[H]$-modules must be inflated from simple $(\mathbb{Z}/p)[C]$-modules since the kernel of the natural surjection $(\mathbb{Z}/p)[H] \mapsto (\mathbb{Z}/p)[C]$ is the radical of $(\mathbb{Z}/p)[H]$. The description of J is now a consequence of the well-known description of the simple modules in characteristic p for a cyclic group C of order prime to p. The action of C on $k[[t]]^{H(p)}$ via ϕ_H makes $k((t))^{H(p)}$ into a tame Kummer extension of $k((t))^H$. From this we get the existence of a uniformizer w in $k[[t]]^{H(p)}$ and of a character χ' with the properties stated in the lemma. □

LEMMA A.8. – *With the notations and assumptions of Lemma A.7, let $q = p^d$. There are arbitrarily large integers $n > 0$ which are relatively prime to p such that $\chi = \chi'^n$ as characters from C to $\mathbb{F}_q$. By Lemma A.7, J as a $(\mathbb{Z}/p)[H]$-module is inflated from a $(\mathbb{Z}/p)[C]$-module $\tilde{J}$. The polynomial*

$$y^q - y - w^{-n} \tag{A.5}$$

is irreducible in $k((w))[y]$. Let L be the splitting field of this polynomial over $k((w)) = k((t))^{H(p)}$. Define $F = k((t))^H$. When we identify $\tilde{J}$ with $\mathbb{F}_q^+$, there is an isomorphism $\mathrm{Gal}(L/k((w))) \to \tilde{J}$ defined by $\sigma \mapsto \sigma(y) - y$. The group C embeds into $\mathrm{Aut}_k(L)$ via the map which sends $\tau \in C$ to the automorphism defined by $\tau(w) = \chi'(\tau)w$ and $\tau(y) = \chi'(\tau)^{-n}y$. This extends to an action of the semi-direct product $\tilde{J}.C$ on L which fixes F, and in this way $\mathrm{Gal}(L/F) = \tilde{J}.C$. The corresponding lower ramification group $\tilde{J}_n$ equals $\tilde{J}$ while $\tilde{J}_{n+1} = \{e\}$.

Proof. – All of the assertions are clear from Artin-Schreier theory except for the fact that $\tilde{J}_n = \tilde{J}$ and $\tilde{J}_{n+1} = \{e\}$. For this observe that if $a, b \in \mathbb{Z}$ are such that $aq - bn = 1$ then $w^a y^b$ is a uniformizer in L. If $e \neq \sigma \in \mathrm{Gal}(L/k((w)))$ then $0 \neq \sigma(y) - y = \zeta \in \mathbb{F}_q$, b is prime to p and

$$\mathrm{ord}_L\left(\frac{\sigma(w^a y^b)}{w^a y^b} - 1\right) = \mathrm{ord}_L\left(\frac{(y+\zeta)^b}{y^b} - 1\right) = \mathrm{ord}_L((1 + \zeta y^{-1})^b - 1) = n. \tag{A.6}$$

Thus σ lies in the ramification group $\tilde{J}_n$ but not in $\tilde{J}_{n+1}$. □

In view of Lemma A.5, part (v) of the following lemma completes the proof of Proposition A.3.

LEMMA A.9. – *Assume the hypothesis and notations of Lemmas A.7 and A.8. By Lemma A.5, there is an injection* $\phi_G : G \to \mathrm{Aut}_k(k[[z]])$ *inducing* ϕ_H. *Let* $F = k((t))^H = L^{\tilde{J}.C}$ *as in Lemma A.8, so that* $k((z))/F$ *is a Galois* $G = P.C$*-extension while* L/F *is a Galois* $\tilde{J}.C$ *extension. If* n *in Lemma A.8 is sufficiently large, then the following hold:*

i. *The fields* $k((z))$ *and* L *are linearly disjoint over their common subfield,* $k((w)) = k((t))^{H(p)} = k((z))^P = L^{\tilde{J}}$.

ii. *Let* $N = L \cdot k((z))$ *be the compositum of these two extensions of* $k((w))$. *Then*

$$\mathrm{Gal}(N/F) = (\tilde{J} \times P).C$$

where the action of C *on the product group* $\tilde{J} \times P$ *is via the conjugation action of* C *on both factors.*

iii. *Fix identifications of* $\tilde{J}$ *and* $J \subset P$ *with* $\mathbb{F}_q^+$ *as in Lemmas A.7 and A.8. This gives an isomorphism* $\psi : \tilde{J} \to J$, *with the property that*

$$\Delta = \{(\tilde{t}, \psi(\tilde{t})) : \tilde{t} \in \tilde{J}\} \tag{A.7}$$

is a subgroup of $\tilde{J} \times J \subset \tilde{J} \times P$ *that is normal in* $\mathrm{Gal}(N/F) = (\tilde{J} \times P).C$.

iv. *The fixed field* N^Δ *is Galois over* F, *with* $\mathrm{Gal}(N^\Delta/F)$ *isomorphic to* G. *We can choose a uniformizer* z' *in* N^Δ *and an injection* $\phi'_G : G \to \mathrm{Aut}_k(k[[z']])$ *having the following properties:*
   a. *There is an isomorphism of* $k[[z']]^{\phi'_G(J)}$ *with* $k[[t]]$ *such that* ϕ'_G *induces* $\phi_H : H \to \mathrm{Aut}_k(k[[t]])$.
   b. *The ramification group* $\phi'_G(G)_n$ *equals* $\phi'_G(J)$, *while* $\phi'_G(G)_{n+1} = \{e\}$.

v. *Suppose* $1 \leq M \in \mathbb{Z}$. *We can choose* n *to be arbitrarily large with* $n \equiv -1 \bmod p^{M-1}$. *For such* n, *the following will be true for each cyclic subgroup* T *of* J:
   a. $\iota_G(T) = n+1 \equiv 0 \bmod p^{M-1}\mathbb{Z}$,*s where* n *is the largest integer such that* $\phi'_G(G)_n$ *contains* T *and where we compute* ι_G *using* ϕ'_G.
   b. $\iota_G(T) > \iota_G(\Gamma) + M$ *for all cyclic groups* $\Gamma \subset P$ *that properly contain* T.

   For such n, ϕ'_G *will have properties (i) and (iv) in Proposition A.3.*

Proof. – Part (i) follows from the fact that if n in Lemma A.8 is sufficiently large, the valuation of the relative discriminant of every non-trivial extension of $k((w))$ inside L is larger than that of every non-trivial extension of $k((w))$ inside $k((z))$.

Parts (ii), (iii) and (iv)(a) are straightforward from Galois theory.

To prove (iv)(b), consider the j^{th} upper ramification subgroup of the p-group

$$\mathrm{Gal}(N/k((w))) = \tilde{J} \times P. \tag{A.8}$$

This must surject onto $\mathrm{Gal}(L/k((w)))^j$ as well as onto $\mathrm{Gal}(k((z))/k((w)))^j = P^j$. By Lemma A.8, $\mathrm{Gal}(L/k((w)))^n = \mathrm{Gal}(L/k((w)))_n = \mathrm{Gal}(L/k((w)))$, and this group is identified with

$$(\tilde{J} \times P)/(1 \times P) \cong \tilde{J}.$$

Furthermore, $\mathrm{Gal}(L/k((w)))^{n+\epsilon} = \{e\}$ if $\epsilon > 0$. If we choose n sufficiently large, then $\mathrm{Gal}(k((z))/k((w)))^n = P^n$ will be the trivial group, where $\mathrm{Gal}(k((z))/k((w)))$ is identified with the quotient group

$$(\tilde{J} \times P)/(\tilde{J} \times 1) \cong \tilde{P}.$$

It follows that if n is sufficiently large, then $\mathrm{Gal}(N/k((w)))^n$ must lie in $\tilde{J} \times 1$ and surject onto $\tilde{J}$, so in fact $\mathrm{Gal}(N/k((w)))^n = \tilde{J} \times 1$ relative to the description of $\mathrm{Gal}(N/k((w))$ in (A.8). Hence the image of $\mathrm{Gal}(N/k((w)))^n$ in $\mathrm{Gal}(N^{\Delta}/k((w))) = (\tilde{J} \times P)/\Delta$ is the image of $\tilde{J} \times 1$, and this group is identified with J when we identify G with $((\tilde{J} \times P).C)/\Delta$ as above. Thus the action of G on $k[[z']]$ specified by ϕ'_G leads to the ramification group J^n being equal to J and $J^{n+\epsilon}$ being $\{e\}$ if $\epsilon > 0$. Since J is a p-group, we conclude that $J_n = J$ and $J_{n+1} = \{e\}$, which completes the proof of part (iv).

For part (v), we observe that the condition on n in Lemma A.8 is that it be sufficiently large, relatively prime to p, and satisfy $\chi = \chi'^n$ as characters from C to $\mathbb{F}_q$. The last condition is one on n mod $\#C$; so since $\#C$ is prime to p, we can always find such n for which $n \equiv -1$ mod p^{M-1}. Since $\iota_G(T) = n + 1$ for T a non-trivial cyclic subgroup of J by part (iv.b), we conclude that $\iota_G(T) \equiv 0$ mod p^{M-1} as in (v.a). Suppose now that Γ is a cyclic subgroup of P which contains T but is not contained in J. Then $\Gamma(H) = \Gamma/(\Gamma \cap J)$ is identified with a non-trivial subgroup of $G/J = H = \mathrm{Gal}(k[[z']]^{\phi'_G(J)}/F)$, where $k[[z']]^{\phi'_G(J)}$ is identified with $k[[t]]$ as in part (iv.a). This last identification shows that there is an integer $c_0 \geq 0$ independent of the choice of n such that the upper ramification group $\Gamma(H)^c$ equals $\{e\}$ if $c \geq c_0$. Then $\Gamma^c \subset J$ for such c since Γ^c surjects onto $\Gamma(H)^c$. We have $\Gamma_{\#Gc} \subset \Gamma^c$ by the crudest estimates for the Herbrand function, so $\Gamma_{\#Gc_0} \subset J$. Thus $\Gamma_{\#Gc_0} \neq \Gamma$, so $\iota_G(\Gamma) \leq \#Gc_0$. We now choose n so that $n \geq \#Gc_0 + M$, to have $\iota_G(T) = n + 1 > \#Gc_0 + M \geq \iota_G(\Gamma) + M$ as required in part (v). Finally, we note that having chosen n so that all of parts (i)–(v) hold, ϕ'_G will satisfy conditions (i) and (iv) of Proposition A.3. □

Appendix B

Appendix 2: Distinguishing the Bertin and KGB obstructions

In this section we show the KGB obstruction to lifting an injection $\phi : G \to \mathrm{Aut}_k(k[[t]])$ can be non-zero when the Bertin obstruction vanishes, by proving the following result.

Recall that the first jump in the lower ramification filtration of G occurs at the largest integer i_0 such that $G = G_{i_0}$.

PROPOSITION B.1. – *Suppose G is isomorphic to $\mathbb{Z}/p \times \mathbb{Z}/p$.*

a. (Bertin) *The Bertin obstruction for lifting ϕ vanishes if and only if $p|(i_0 + 1)$.*
b. *When $p|(i_0 + 1)$, the KGB obstruction for lifting ϕ does not vanish if and only if $p = 3 = i_0 + 1$ and $G_{i_0+1} = \{e\}$.*

While this shows that the KGB obstruction is in general stronger than the Bertin obstruction for particular ϕ, our results in §1 show that every Bertin group for k is a KGB group for k and vice versa.

EXAMPLE B.2. – When $p = 3$, one obtains from statement (b) an explicit example of a ϕ with vanishing Bertin obstruction and non-vanishing KGB obstruction in the following way. Let $i_0 > 0$ be any integer such that $p|(i_0 + 1)$. Let u be an indeterminate, and let N be the extension $k((u))[X]/(X^9 - u^{-i_0})$ of $k((u))$. Then $G = \mathrm{Gal}(N/k((u)))$ is isomorphic to the finite field $\mathbb{F}_9 \cong \mathbb{Z}/p \times \mathbb{Z}/p$ via the map sending $\alpha \in \mathbb{F}_9$ to the automorphism σ_α for which $\sigma_\alpha(X) = X + \alpha$. One has $\mathrm{ord}_N(u) = 9$, $\mathrm{ord}_N(X) = -i_0$ and $\mathrm{ord}_N(t) = 1$ when $t = X^a u^b$ and $9b - ai_0 = 1$ for some integers a and b. Thus t is a uniformizer in N, and $(\sigma_\alpha(t)/t) - 1 = (1 + \alpha X^{-1})^a - 1$ has valuation $\mathrm{ord}_N(a\alpha X^{-1}) = i_0$ for $0 \neq \alpha \in \mathbb{F}_9$. It follows $G = G_{i_0} \supset G_{i_0+1} = \{e\}$.

Proof of Proposition B.1. – Statement (a) is a special case of Example 1 of §4 of [2]. As noted there, Green and Matignon proved earlier in [12] for $G = \mathbb{Z}/p \times \mathbb{Z}/p$ there is no lift of ϕ to characteristic 0 unless $p|(i_0 + 1)$.

We now focus on statement (b). The (unique) set $\mathcal{C}$ of representatives for the conjugacy classes of cyclic subgroups T of G consists of the trivial subgroup $\{e\}$ together with the $p + 1$ subgroups of G of order p. By Proposition 2.1 and Theorem 2.3, the set S appearing in Theorem 4.2 is the disjoint union over the non-trivial $T \in \mathcal{C}$ of $b_T = \iota(T)/p$ copies of the left G-set G/T. There are always $T \in \mathcal{C}$ not contained in G_{i_0+1}, and for these T one has $\iota(T) = i_0 + 1$. By the Hasse-Arf Theorem, if $T \subset G_{i_0+1}$ then $T = G_{i_0+1}$ and $\iota(T) = i_0 + pi_1 + 1$, where $i_1 \geq 1$ is an integer and the second jump in the upper numbering of the ramification groups of G is at $i_0 + i_1$. The KGB obstruction vanishes if and only if for each non-trivial $T \in \mathcal{C}$ and each integer j such that $1 \leq j \leq b_T$, we can choose a generator $g_{T,j}$ for T such that

$$\prod_{\{e\} \neq T \in \mathcal{C}} \prod_{j=1}^{b_T} g_{T,j} = e \quad \text{in} \quad G. \tag{B.1}$$

Note that $b_T = \iota(T)/p > 0$ for all $\{e\} \neq T \in \mathcal{C}$ so $\{g_{T,j}\}_{T,j}$ generates G.

Suppose first that $i_0 + 1 > p$. Then $b_T \geq (i_0 + 1)/p > 1$ for all $\{e\} \neq T \in \mathcal{C}$. For each such T, we can therefore choose the generators $g_{T,j}$ for $1 \leq j \leq b_T$ so that $\prod_{j=1}^{b_T} g_{T,j} = e$. This makes (B.1) hold, so the KGB obstruction vanishes.

We now suppose that $i_0 + 1 = p$, but that $G_{i_0+1} \neq \{e\}$. Then G_{i_0+1} has order p, and there are exactly p order p subgroups $T_0, \ldots, T_{p-1}$ of G different from G_{i_0+1}. We can choose the generators for $G = \mathbb{Z}/p \times \mathbb{Z}/p$ so that G_{i_0+1} corresponds to the subgroup $\{0\} \times \mathbb{Z}/p$. Then $g_{T_i,1} = (1, i)$ is a generator for T_i for $0 \leq i \leq p - 1$. We have

$$\prod_{i=0}^{p-1} g_{T_i,1} = (0, (p-1)p/2) \quad \text{in} \quad G = \mathbb{Z}/p \times \mathbb{Z}/p.$$

Thus this product is in the last cyclic order p subgroup G_{i_0+1}, and as noted above, $b_{G_{i_0+1}} = \frac{i_0+pi_1+1}{p} > 1$. Hence we can choose the final generators $g_{G_{i_0+1},j}$ for $1 \leq j \leq b_{G_{i_0+1}}$ in such a way that (B.1) holds, which shows that the KGB obstruction vanishes.

We are thus reduced to showing that if $p = i_0 + 1$ and $G_{i_0+1} = \{e\}$, then the KGB obstruction vanishes if and only if $p \neq 3$. Fix an isomorphism of G with $\mathbb{Z}/p \times \mathbb{Z}/p$, and define $h_i = (1, i)$ for $0 \leq i \leq p - 1$ and $h_p = (0, 1)$. Any generator for the subgroup T_i generated by h_i has the form $g_{i,1} = c_i \cdot h_i$ for some $c_i \in (\mathbb{Z}/p)^*$. The question of whether

we can choose generators of these groups for which (B.1) holds is the same as asking where there are $c_i \in (\mathbb{Z}/p)^*$ such that

$$\left(\sum_{i=0}^{p-1} c_i \cdot (1,i)\right) + c_p \cdot (0,1) = (0,0) \quad \text{in} \quad G = \mathbb{Z}/p \times \mathbb{Z}/p. \tag{B.2}$$

Such c_i exist if and only if the KGB obstruction vanishes.

We will leave it to the reader to check the following facts. If $p = 2$ then $c_0 = c_1 = c_2 = 1$ is a solution of (B.2). If $p = 3$ there is no solution with the $c_i \in (\mathbb{Z}/p)^*$. Finally, if $p > 2$ then a solution is given by $c_i = 1$ if $0 \leq i \leq p-3$, $c_{p-2} = -1$, $c_{p-1} = 3$ and $c_p = -2$. This completes the proof. □

REFERENCES

[1] M. Aschbacher, *Finite group theory*, second ed., Cambridge Studies in Advanced Math. **10**, Cambridge Univ. Press, 2000.

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

[3] J. Bertin, A. Mézard, Déformations formelles des revêtements sauvagement ramifiés de courbes algébriques, *Invent. Math.* **141** (2000), 195–238.

[4] I. I. Bouw, S. Wewers, The local lifting problem for dihedral groups, *Duke Math. J.* **134** (2006), 421–452.

[5] I. I. Bouw, S. Wewers, L. Zapponi, Deformation data, Belyi maps, and the local lifting problem, *Trans. Amer. Math. Soc.* **361** (2009), 6645–6659.

[6] L. H. Brewis, Liftable D_4-covers, *Manuscripta Math.* **126** (2008), 293–313.

[7] L. H. Brewis, S. Wewers, Artin characters, Hurwitz trees and the lifting problem, *Math. Ann.* **345** (2009), 711–730.

[8] T. Chinburg, R. Guralnick, D. Harbater, Oort groups and lifting problems, *Compos. Math.* **144** (2008), 849–866.

[9] J.-M. Fontaine, Groupes de ramification et représentations d'Artin, *Ann. Sci. École Norm. Sup.* **4** (1971), 337–392.

[10] D. Gorenstein, *Finite groups*, Harper & Row Publishers, 1968.

[11] B. Green, Automorphisms of formal power series rings over a valuation ring, in *Valuation theory and its applications, Vol. II (Saskatoon, SK, 1999)*, Fields Inst. Commun. **33**, Amer. Math. Soc., 2003, 79–87.

[12] B. Green, M. Matignon, Liftings of Galois covers of smooth curves, *Compositio Math.* **113** (1998), 237–272.

[13] A. Grothendieck (ed.), *Revêtements étales et groupe fondamental. Séminaire de Géométrie Algébrique du Bois Marie 1960–1961 (SGA 1)*, Lect. Notes in Math. **224**, Springer, 1971.

[14] A. Grothendieck, J. Dieudonné, Étude locale des schémas et des morphismes de schémas (EGA IV), *Publ. Math. IHÉS* **20** (1964), **24** (1965), **28** (1966), **32** (1967).

[15] D. Harbater, Fundamental groups and embedding problems in characteristic p, in *Recent developments in the inverse Galois problem (Seattle, WA, 1993)*, Contemp. Math. **186**, Amer. Math. Soc., 1995, 353–369.

[16] N. M. Katz, Local-to-global extensions of representations of fundamental groups, *Ann. Inst. Fourier (Grenoble)* **36** (1986), 69–106.

[17] M. Matignon, p-groupes abéliens de type $(p, \dots, p)$ et disques ouverts p-adiques, *Manuscripta Math.* **99** (1999), 93–109.

[18] M. Matignon, Lifting $(\mathbb{Z}/2\mathbb{Z})^2$ actions, preprint http://www.math.u-bordeaux.fr/~matignon/chap5.ps.

[19] A. Mézard, Quelques problèmes de déformations en caractéristique mixte, Thèse de doctorat, Université Joseph Fourier, Grenoble, 1998.

[20] J. S. Milne, *Étale cohomology*, Princeton Mathematical Series **33**, Princeton Univ. Press, 1980.

[21] F. Oort, Lifting algebraic curves, abelian varieties, and their endomorphisms to characteristic zero, in *Algebraic geometry, Bowdoin, 1985 (Brunswick, Maine, 1985)*, Proc. Sympos. Pure Math. **46**, Amer. Math. Soc., 1987, 165–195.

[22] G. Pagot, F_p-espaces vectoriels de formes différentielles logarithmiques sur la droite projective, *J. Number Theory* **97** (2002), 58–94.

[23] G. Pagot, Relèvement en caractéristique zéro d'actions de groupes abéliens de type $(p, \dots, p)$, Thèse de doctorat, Université Bordeaux I, 2002.

[24] F. Pop, Étale Galois covers of affine smooth curves. The geometric case of a conjecture of Shafarevich. On Abhyankar's conjecture, *Invent. Math.* **120** (1995), 555–578.

[25] R. J. Pries, Wildly ramified covers with large genus, *J. Number Theory* **119** (2006), 194–209.

[26] T. Sekiguchi, F. Oort, N. Suwa, On the deformation of Artin-Schreier to Kummer, *Ann. Sci. École Norm. Sup.* **22** (1989), 345–375.

[27] J-P. Serre, Sur la rationalité des représentations d'Artin, *Ann. of Math.* **72** (1960), 405–420.

[28] J-P. Serre, *Corps locaux*, Hermann, 1968, Deuxième édition, Publications de l'Université de Nancago, No. VIII.

[29] J-P. Serre, *Linear representations of finite groups*, Springer, 1977.

[30] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Math. **106**, Springer, 1986.

[31] V. P. SNAITH, *Explicit Brauer induction*, Cambridge Studies in Advanced Math. **40**, Cambridge Univ. Press, 1994.

(Manuscrit reçu le 6 octobre 2009 ;
accepté, après révision, le 22 novembre 2010.)

Ted CHINBURG
Department of Mathematics
University of Pennsylvania
Philadelphia, PA 19104-6395, USA
E-mail: ted@math.upenn.edu

Robert GURALNICK
Department of Mathematics
University of Southern California
3620 South Vermont Ave., KAP 108
Los Angeles, California 90089-2532, USA
E-mail: guralnic@usc.edu

David HARBATER
Department of Mathematics
University of Pennsylvania
Philadelphia, PA 19104-6395, USA
E-mail: harbater@math.upenn.edu