ISRAEL JOURNAL OF MATHEMATICS **157** (2007), 63–102
DOI: 10.1007/s11856-006-0003-5

PARAMETRIZATION OF CENTRAL FRATTINI EXTENSIONS AND ISOMORPHISMS OF SMALL GROUP RINGS

BY

Martin Hertweck*

Universität Stuttgart, Fachbereich Mathematik, Institut für Geometrie und Topologie
Pfaffenwaldring 57, 70550 Stuttgart, Germany
e-mail: hertweck@mathematik.uni-stuttgart.de

AND

Marcos Soriano

Universität Hannover, Institut für Mathematik, Lehrgebiet Algebra und Zahlentheorie
Welfengarten 1, 30167 Hannover, Germany
e-mail: soriano@math.uni-hannover.de

ABSTRACT

We solve the modular isomorphism problem for small group rings, i.e., we determine, for a given finite p-group H, precisely which central Frattini extensions of H give rise to isomorphic small group rings over the field with p elements.

1. Introduction

Let G be a finite p-group, where p is an arbitrary rational prime. Any descending central series

$$G = G_1 \geq G_2 \geq \cdots \geq G_l \gneq G_{l+1} = 1$$

with $G_2 = \Phi(G) = [G, G]G^p$, the Frattini subgroup of G, and elementary abelian sub-quotients G_i/G_{i+1}, allows us to describe G as being successively built from extensions $\mathbb{E}_1, \ldots, \mathbb{E}_{l-1}$:

$$\mathbb{E}_i \colon 1 \longrightarrow G_{i+1}/G_{i+2} \longrightarrow G/G_{i+2} \longrightarrow G/G_{i+1} \longrightarrow 1.$$

* The first author acknowledges support by the Deutsche Forschungsgemeinschaft.
Received March 2, 2005

Note that, by assumption, G_{i+1}/G_{i+2} is a central elementary abelian subgroup contained in the Frattini subgroup of G/G_{i+2}, which shall be expressed shortly by saying that $\mathbb{E}_i$ is a **central Frattini extension**.

An important example of such a central series is the Brauer–Jennings–Zassenhaus series $G = \mathrm{M}_1(G) \geq \mathrm{M}_2(G) \geq \cdots$ (see [13] and Section 3). It appears naturally in the context of modular group algebras, since $\mathrm{M}_n(G)$ is the so-called n-th dimension subgroup of G:

$$\mathrm{M}_n(G) = G \cap (1 + \mathrm{I}(kG)^n),$$

where $\mathrm{I}(kG)$ denotes the augmentation ideal of the modular group ring kG, with $k = \mathbb{F}_p$ being the field with p elements.

A **group basis** of kG is a subgroup of the group of units of kG which constitutes a basis of the vector space kG over k. The Modular Isomorphism Problem (usually abbreviated as MIP) asks whether, for a given p-group G, a group basis of kG must be necessarily isomorphic to G.

The results obtained by Passi and Sehgal in [14] and Ritter and Sehgal in [16] say — to be read as successive improvements — that the isomorphism classes of the sub-quotients

$$\mathrm{M}_n(\tilde{G})/\mathrm{M}_{n+1}(\tilde{G}), \quad \mathrm{M}_n(\tilde{G})/\mathrm{M}_{n+2}(\tilde{G}), \quad \mathrm{M}_n(\tilde{G})/\mathrm{M}_{2n+1}(\tilde{G})$$

are independent of the chosen group basis $\tilde{G}$ of kG.

They seem to suggest that an inductive approach to (MIP) should be possible, a point of view taken in the recent attack of Borge and Laudal on (MIP) (see [2, 3], as well as the discussion of this approach given by the authors in [8, §3]). Trying to substantiate the attempt of [2, 3] was the starting point of the investigation that led to the present paper.

It appears natural to consider for a *fixed* p-group H the class $\mathbb{F}(H)$ of all short exact sequences of groups

$$\mathbb{E}\colon 1 \longrightarrow V \longrightarrow E \longrightarrow H \longrightarrow 1,$$

where V is a central elementary abelian p-subgroup contained in the Frattini subgroup of E (see Definition 4.1). The **small group ring** of E with respect to V is the quotient

$$s(E, V) = \frac{kE}{\mathrm{I}(kV)\mathrm{I}(kE)}.$$

Associated to $\mathbb{E}$ there is a short exact sequence of k-algebras, the sequence for the small group ring (see Section 3):

$$\mathbb{S}\colon 0 \longrightarrow \{V - 1\} \longrightarrow s(E, V) \longrightarrow kH \longrightarrow 0.$$

We introduce two equivalence relations on $\mathbb{F}(H)$ — **isomorphism** and ***s*-equivalence** — which essentially describe isomorphisms between group sequences $\mathbb{E}$ or, rather, small group ring sequences $\mathbb{S}$ (see Definition 4.3).

The main result of the paper, Theorem 4.4, describes the *s-equivalence classes* of extensions in $\mathbb{F}(H)$ in terms of an action of the outer automorphism group $\mathrm{Out}(kH)$ on the kernel V of a certain 'universal' extension $\mathbb{E}$, given in (4.3). There is a natural inclusion $\mathrm{Out}(H) \subseteq \mathrm{Out}(kH)$, and restriction of the action to $\mathrm{Out}(H)$ yields precisely the *isomorphism classes* of extensions in $\mathbb{F}(H)$. This solves, in view of Corollary 3.7, the isomorphism problem for small group rings in an optimal way.

With the guide of Theorem 4.4, it is fairly easy to verify that for the dihedral group D_8 of order 8, the (non-isomorphic) central Frattini extensions in $\mathbb{F}(D_8)$ with middle terms isomorphic to the dihedral, semi-dihedral and generalized quaternion group of order 16 give rise to isomorphic small group rings, and to construct two pairs of central Frattini extensions in $\mathbb{F}(D_8)$ with non-isomorphic middle groups of order 32 which give rise to isomorphic small group rings (see Example 6.3). Although announced in the literature (see the (foot)note (e) contained in the remark following Theorem 6.25 in [21]), such examples do not seem to have been published until now.

For the orientation of the reader, we briefly describe the contents of each section.

Section 2 contains the fairly elementary group-theoretical Lemma 2.1 on the lifting of group homomorphisms in a special situation, which, as a consequence, allows the — completely cohomology-free — introduction of the key concept of **obstruction space** (see Proposition 2.2). The reader interested in an alternative approach to this concept may wish to consult [8].

Besides giving a short introduction into small group rings, the purpose of Section 3 is twofold: first, to transfer the concept of obstruction spaces to the setting of small group rings (see Corollary 3.2), and second, to show that s-equivalence of central Frattini extensions as introduced in Section 4 (see Definition 4.3) is nothing but isomorphism of small group rings (see Corollary 3.7).

In Section 4 we introduce central Frattini extensions (see Definition 4.1) and study the class $\mathbb{F}(H)$ of all such extensions with fixed finite factor p-group H with respect to two closely related equivalence relations: isomorphism and s-equivalence (see Definition 4.3). A key observation (see Lemma 4.2) relates obstruction spaces to sequences in $\mathbb{F}(H)$. The main Theorem 4.4 may be interpreted as the construction of all classes of sequences in $\mathbb{F}(H)$ as appropriate

quotients of a certain 'universal' central Frattini extension (4.3). Thereby, the action of the groups $\mathrm{Out}(H)$ and $\mathrm{Out}(kH)$ on the subspaces U of the kernel V of this extension, which is described in detail in Section 4, identifies isomorphic respectively s-equivalent sequences by interpreting the subspaces U as obstruction spaces in the group respectively small group ring setting.

Section 5 is mainly devoted to the formulation of a new proof of the result of Röhl [20] in our setting (see Theorem 5.8), thus relating it to small group rings. Roughly speaking, the theorem is about the modular isomorphism problem for p-groups allowing a certain type of presentation. En passant, we derive a couple of (hopefully) useful results, from which Lemma 5.7 and Corollary 5.9 might be highlighted.

It might be helpful to complement the reading of Sections 3 and 4 with looking at the examples from Section 6. Example 6.1 contains all of what can be said about the simple (and exceptional) case of cyclic groups, giving also an easy, explicit example of small group rings. Example 6.2 aims at describing $\mathbb{F}(H)$ for H elementary abelian. It turns out that in this case isomorphism and s-equivalence classes coincide, and their explicit description is reduced to a combinatorial problem related to certain $\mathrm{GL}(\mathbb{F}_p)$-modules. Finally, due to a 'strictly larger' action of $\mathrm{Out}(\mathbb{F}_2 D_8)$ when compared to the action of $\mathrm{Out}(D_8)$ (D_8 denoting the dihedral group of order 8), we are able to construct in Example 6.3 non-isomorphic groups having isomorphic modular small group rings with quotient algebra $\mathbb{F}_2 D_8$. The reader is invited to extend this family of examples by working with GAP [7], our favourite computer algebra system in this context.

2. A lemma about lifting of group homomorphisms

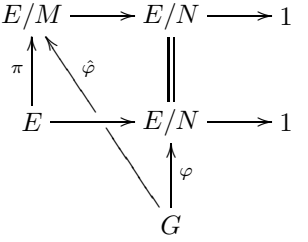
Let G be a finite group. We shall consider short exact sequences $\mathbb{E}$ of finite groups together with homomorphisms φ from G to the end term of the sequence:

$$\mathbb{E}_\varphi\colon 1 \longrightarrow N \longrightarrow E \longrightarrow E/N \longrightarrow 1, \quad \text{with } \varphi\colon G \to E/N \tag{2.1}$$

We shall refer to $\mathbb{E}_\varphi$ just as a diagram. We will say that φ lifts modulo M, where M is a normal subgroup of E contained in N, if there exists a homomorphism $\widehat{\varphi}\colon G \longrightarrow E/M$ such that the following diagram, where $\pi\colon E \longrightarrow E/M$ is the

natural map, is commutative:

(2.2)



Then, the homomorphism $\widehat{\varphi}$ will be called a lifting of φ.

Sometimes it is possible to make a statement about the collection of all normal subgroups modulo which φ lifts. We show:

LEMMA 2.1: *Suppose that a diagram $\mathbb{E}_\varphi$ is given, as shown in (2.1), and that N is a direct product of minimal normal subgroups of E. Then there exists a unique normal subgroup U of E contained in N which is minimal in the following sense: φ can be lifted modulo U, and any other normal subgroup modulo which φ lifts contains U.*

Proof: We begin with a preliminary remark about the normal subgroups of E which are contained in N: If M is such a subgroup, $M \neq 1$, and $N = N_1 \times \cdots \times N_r$ with minimal normal subgroups N_i of E, then we have, possibly after a renumbering of the N_i, that $N = M \times N_1 \times \cdots \times N_s$ for some $s < r$. This can be proved by induction on the order of M as follows. First of all, the projection of M onto some N_{i_0} is surjective. Let L be the kernel of this surjection. If $L = 1$, then N is the direct product of M and the N_i, $i \neq i_0$. Otherwise $L \neq 1$, and we may assume by induction on $|M|$ that $N = L \times K$ with $K = N_1 \times \cdots \times N_{s+1}$, some $s < r - 1$, after a suitable renumbering. Note that $M = L \times (M \cap K)$ and that $M \cap K$ is a minimal normal subgroup of E contained in K. As before (the case $L = 1$), we have $K = (M \cap K) \times N_1 \times \cdots \times N_s$ after renumbering, which proves the claim. In particular, any normal subgroup M of E contained in N has a direct complement in N which is normal in E.

Now let U be a normal subgroup of E contained in N such that φ lifts modulo U, but not modulo any normal subgroup which is properly contained in U (possibly $U = N$). By way of contradiction, suppose that V is a normal subgroup of E contained in N such that φ lifts modulo V, but that V does not contain U.

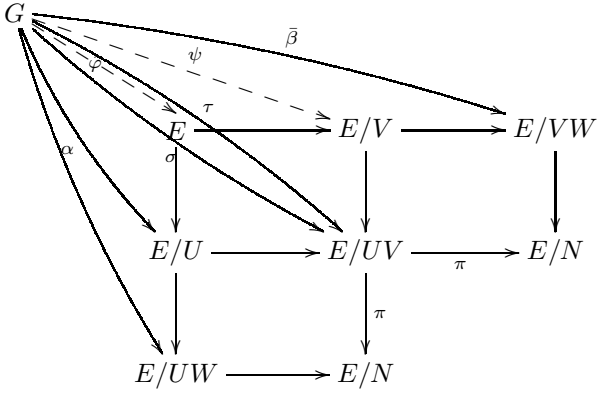
We assume without lost of generality that the injection $N \longrightarrow E$ is in fact inclusion.

If $U \cap V \neq 1$, we may consider the diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N/U \cap V & \longrightarrow & E/U \cap V & \longrightarrow & E/N & \longrightarrow & 1. \\ & & & & & & \uparrow{\scriptstyle \varphi} & & \\ & & & & & & G & & \end{array}$$

Then φ lifts modulo $U/U \cap V$ and modulo $V/U \cap V$. By induction on the order of E, we can assume that φ lifts modulo the intersection of these subgroups, i.e., that there exists a lifting $\widehat{\varphi}\colon G \longrightarrow E/U \cap V$ of φ, contradicting our choice of U since $U \cap V$ is a proper subgroup of U.

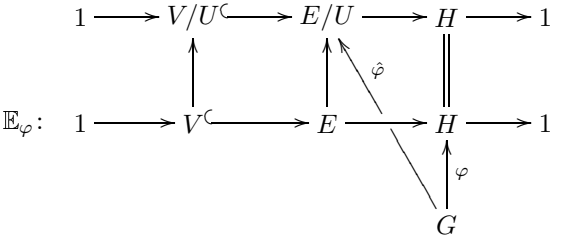
Hence we can assume that $U \cap V = 1$. Then there exists a normal subgroup W of E such that $N = U \times V \times W$. Let $\alpha\colon G \longrightarrow E/U$ and $\beta\colon G \longrightarrow E/V$ be liftings of φ. Let σ be the composite of α and the natural map $E/U \longrightarrow E/UV$, and let τ be the composite of β and the natural map $E/V \longrightarrow E/UV$. If $\pi\colon E/UV \longrightarrow E/N$ is the natural map, then $\sigma\pi = \tau\pi$ since both $\sigma\pi$ and $\tau\pi$ are the composite of φ and the inverse of the automorphism of E/N which the given surjection $E \longrightarrow E/N$ induces. At last, let $\bar{\beta}$ denote the composite of β and the natural map $E/V \longrightarrow E/VW$. Now consider the following commutative diagram, in which each square is a pullback diagram where the maps are the natural ones. Note that pullback diagrams have a universal mapping property (as described in [6, §3, Exercise 11] for pullback diagrams of modules).



As $\sigma\pi = \tau\pi$, we obtain a homomorphism $\psi\colon G \longrightarrow E/V$ such that the composite of ψ with the natural map $E/V \longrightarrow E/VW$ is $\bar{\beta}$, and the composite of ψ with the natural map $E/V \longrightarrow E/UV$ is σ. It follows that α and ψ induce a homomorphism $\widehat{\varphi}\colon G \longrightarrow E$, which is a lifting of φ. Consequently $U = 1$, contradicting our assumption that V does not contain U, and the lemma is proved. ∎

The hypothesis of Lemma 2.1 is naturally satisfied if N is an elementary abelian p-group (for some prime p) which is contained in the center of E. In this case, we shall write $\operatorname{obspace}\mathbb{E}_\varphi$ for the subgroup U described in Lemma 2.1 as we think of the vector space U as an "obstruction space." As we shall deal only with such extensions, we record this conclusion in a separate proposition:

PROPOSITION 2.2 (and Definition): *Let $\mathbb{E}_\varphi$ be a diagram as shown below, where V is an elementary abelian p-group contained in the center of E (and $V \hookrightarrow E$ denotes inclusion). Then among the subgroups U of V which admit a lifting, as shown below, there is a unique smallest one, called* $\operatorname{obspace}\mathbb{E}_\varphi$.



The concept of obstruction spaces for diagrams of p-groups was recently picked up by Borge and Laudal in their attack on the modular isomorphism problem (see [3]). In [8], the authors presented an elementary cohomological argument giving $\operatorname{obspace}\mathbb{E}_\varphi$ as the image of a certain homomorphism which is naturally assigned to a 2-cocycle associated with $\mathbb{E}_\varphi$, closely following the path marked in [3, Section 2].

3. A glance on algebras: The small group ring

The group-theoretical Proposition 2.2 has an analogue on the algebra-side. We do not go into details but present some ideas by means of the "small group ring". Originally, the small group ring was introduced to deal with problems for integral group rings, leading to Whitcomb's result [23]. See [18, 1.1.8] for more details.

Let E be a finite group which has, for some prime p, an elementary abelian normal p-subgroup V. Set $k = \mathbb{F}_p$, the field with p elements. We write $\mathrm{I}(kE)$ for the augmentation ideal of kE (the elements of kE with sum-of-coefficients equal to zero). Note that $\mathrm{I}(kV)kE$ is the kernel of the natural homomorphism $kE \longrightarrow kE/V$. There is an isomorphism of abelian groups

$$V \cong \frac{\mathrm{I}(kV)kE}{\mathrm{I}(kV)\mathrm{I}(kE)} \tag{3.1}$$

sending $v \in V$ to the coset of $v-1$. Indeed, this is a surjective homomorphism since $vw-1 = (v-1)+(w-1)+(v-1)(w-1)$ for all $v, w \in V$. Note that $\mathrm{I}(kV)kE$ has dimension $|E|-|E/V|$, so if T is a system of coset representatives to V in E then $\{(v-1)t|\ 1 \neq v \in V, t \in T\}$ is a k-basis of $\mathrm{I}(kV)kE$ and we obtain a homomorphism $\mathrm{I}(kV)kE \longrightarrow V$ of vector spaces by sending $(v-1)t$ to v. Since the kernel of this homomorphism contains $\mathrm{I}(kV)\mathrm{I}(kE)$, (3.1) follows.

For $U \leq V$, we suggestively write $\{U-1\}$ for the image of U under the isomorphism (3.1). The **small group ring** of E over k associated with V is the quotient

$$s(E,V) = \frac{kE}{\mathrm{I}(kV)\mathrm{I}(kE)}.$$

Thus we have an exact sequence

$$\mathbb{S}\colon 0 \longrightarrow \{V-1\} \longrightarrow s(E,V) \longrightarrow kE/V \longrightarrow 0.$$

Since $\{V-1\}$ is an ideal of square zero, we also have an exact sequence of multiplicative groups of units:

$$1 \longrightarrow V \longrightarrow s(E,V)^\times \longrightarrow (kE/V)^\times \longrightarrow 1.$$

Note that the pre-image of E/V in $s(E,V)^\times$ is precisely E.

Let $U \leq V$. Then U is a normal subgroup of E if and only if $\{U-1\}$ is an ideal of $s(E,V)$. Furthermore, if one of these conditions hold, we have a commutative diagram, in which the vertical maps are the natural isomorphisms:

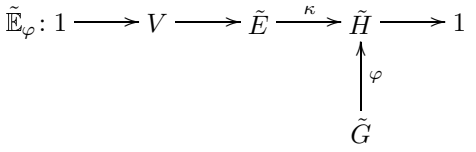
$$\begin{array}{ccccccccc} (3.2) & 0 & \longrightarrow & \{V/U-1\} & \longrightarrow & s(E/U,V/U) & \longrightarrow & kE/V & \longrightarrow 0 \\ & & & \uparrow & & \uparrow & & \| & \\ & 0 & \longrightarrow & \frac{\{V-1\}}{\{U-1\}} & \longrightarrow & \frac{s(E,V)}{\{U-1\}} & \longrightarrow & kE/V & \longrightarrow 0 \end{array}$$

Set $H = E/V$. For a finite group G, consider the exact sequence $\mathbb{S}$ for the small group ring together with a homomorphism φ from kG to the end term of the sequence:

$$\begin{array}{ccccccccc} \mathbb{S}_\varphi\colon 0 & \longrightarrow & \{V-1\} & \longrightarrow & s(E,V) & \xrightarrow{\kappa} & kH & \longrightarrow & 0 \\ & & & & & & \uparrow{\scriptstyle \varphi} & & \\ & & & & & & kG & & \end{array}$$

Assume that a group basis $\tilde{G}$ of kG is mapped under φ to a group basis $\tilde{H}$ of kH, and let $\tilde{E}$ be the pre-image $\kappa^{-1}(\tilde{H})$ of $\tilde{H}$ in $s(E,V)^\times$. Switching to units,

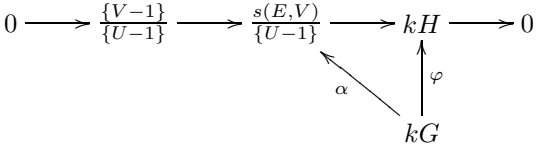
we get a diagram for groups:



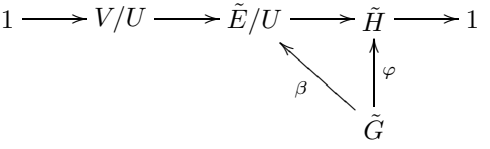
In the present case, the following simple lemma describes the transformation between lifting group and algebra homomorphisms.

LEMMA 3.1: *With the notation as above, let U be a normal subgroup of E contained in V. Then the following are equivalent:*

(i) *There exists an algebra homomorphism α making the following diagram commutative:*

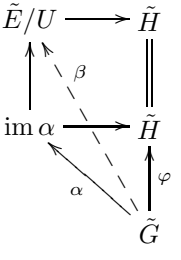


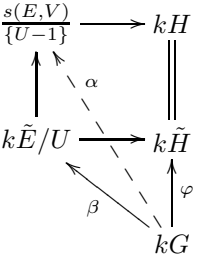
(ii) *There exists a group homomorphism β making the following diagram commutative:*



Proof: Note that $\tilde{E}/U$ embeds naturally into the group of units of $s(E,V)/\{U-1\}$.

(i)$\Longrightarrow$(ii): Let Q be the pre-image of $\tilde{G}\alpha$ in $s(E,V)$. By commutativity, $Q\kappa = \tilde{H}$, so $Q \leq \tilde{E}$, and we obtain β as a composite map, as shown in the left diagram below.





(ii)$\Longrightarrow$(i): Since $kG = k\tilde{G}$ and $kH = k\tilde{H}$, we obtain α as a composite map, as shown in the right diagram above. ∎

From Proposition 2.2 and Lemma 3.1 we immediately obtain the following two corollaries.

COROLLARY 3.2: *Suppose that V is central in E. Among the ideals I of $s(E,V)$ contained in $\{V-1\}$ for which there exists an algebra homomorphism α making the following diagram commutative:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \{V-1\}/I & \longrightarrow & s(E,V)/I & \longrightarrow & kH & \longrightarrow & 0, \\ & & & & & \nwarrow^{\alpha} & \uparrow{\scriptstyle \varphi} & & \\ & & & & & & kG & & \end{array}$$

there exists a unique minimal one (with respect to inclusion), namely $I = \{U-1\}$ with $U = \operatorname{obspace} \tilde{\mathbb{E}}_\varphi$. ∎

COROLLARY 3.3: *Suppose that V is central in E, and that $G\varphi = H$, so that we have another diagram*

$$\begin{array}{ccccccccc} \mathbb{E}_\varphi\colon 1 & \longrightarrow & V & \longrightarrow & E & \longrightarrow & H & \longrightarrow & 1 \\ & & & & & & \uparrow{\scriptstyle \varphi} & & \\ & & & & & & G & & \end{array}$$

Then $\operatorname{obspace} \mathbb{E}_\varphi = \operatorname{obspace} \tilde{\mathbb{E}}_\varphi$. ∎

Though the groups G and $\tilde{G}$ (a priori) might be assumed to be non-isomorphic, this should not come as a surprise since we may very well have $E \neq \tilde{E}$.

In the remaining part of this section we consider isomorphisms between small group rings $s(G,A)$ and $s(H,B)$ of p-groups G and H associated with central elementary abelian subgroups A and B, and address the question whether $\{A-1\}$ must be mapped to $\{B-1\}$. Apart from some minor exceptions, the answer will be in the affirmative. We begin with:

LEMMA 3.4: *Let G be a finite p-group, and let A be a central elementary abelian subgroup of G with $1 \neq A < G$. Let T be a set of coset representatives of A in G, and let τ be the image of $\sum_{t\in T} t$ in $s(G,A)$. Then the annihilator of the radical of $s(G,A)$ is $\{A-1\} + k\tau$ unless G contains an element of order $p|G/A|$, when the annihilator is $\{A-1\}$ (note that in the latter case, G/A is cyclic).*

Proof: Let π: $kG \longrightarrow s(G,A)$ be the natural map, let $m \in kG$, and suppose that $m\pi$ annihilates the radical $\mathrm{I}(kG)\pi$ of $s(G,A)$. Write $m = \sum_{t\in T} m_t t$ with all m_t in kA. We have $\sum_t m_t t \equiv \sum_t \varepsilon(m_t)(t-1) + \sum_t m_t \bmod \mathrm{I}(kA)\mathrm{I}(kG)$, where ε denotes the augmentation map. Since $\varepsilon(m) = 0$ (otherwise m would be a unit), $(\sum_t m_t)\pi \in \{A-1\}$. Note that $\{A-1\}$ annihilates the radical. Set $\tilde{m} = \sum_t \varepsilon(m_t)(t-1)$. Then $\tilde{m}\pi$ annihilates the radical, so if κ: $kG \longrightarrow kG/A$ denotes the natural map, then $\tilde{m}\kappa$ annihilates $\mathrm{I}(kG/A)$. It follows that $\tilde{m}\kappa \in k(\sum_{x\in G/A} x)$, and $\tilde{m}\pi \in \{A-1\}+k\tau$ where $\tau = (\sum_{t\in T} t)\pi$ as above. It remains to check when τ annihilates the radical. Let $g \in G$. Then $(\sum_t t)g = \sum_t a_t t$ with all $a_t \in A$. Using the formula $xy - 1 = (x-1) + (y-1) + (x-1)(y-1)$, we obtain modulo $\mathrm{I}(kA)\mathrm{I}(kG)$

$$\sum_t a_t t = \sum_t (a_t t - 1) \equiv \sum_t (a_t - 1) + \sum_t (t-1) \equiv \left(\prod_t a_t\right) - 1 + \sum_t t. \tag{3.3}$$

The product $\prod_t a_t$ is the image of g under the transfer homomorphism $G \longrightarrow A$ (see [17, 10.1]), and it follows that $\prod_t a_t \neq 1$, i.e., $\tau(g\pi) \neq \tau$, if and only if g has order $p|G/A|$ (cf. [17, 10.1.2]), and the lemma is proved. ∎

We briefly introduce the notion of "Zassenhaus ideals", which will be needed in the proof of the next lemma. Let G be an arbitrary group. The **Lie powers of the augmentation ideal** $\mathrm{I}(kG)$ are the (two-sided) ideals $\Delta^{(i)}(kG)$ defined inductively by

$$\Delta^{(1)}(kG) = \mathrm{I}(kG), \quad \Delta^{(i+1)}(kG) = [\mathrm{I}(kG), \Delta^{(i)}(kG)]kG,$$

where $[M,N]$ denotes the k-submodule generated by all elements $mn - nm$ with $m \in M$ and $n \in N$. Following [14, 24] we define the **Zassenhaus ideals** $\mathrm{H}_n(kG)$ of kG for $n \geq 1$ by setting

$$\mathrm{H}_n(kG) = \sum_{ip^j \geq n} \Delta^{(i)}(kG)^{p^j} + \mathrm{I}(kG)^{n+1}. \tag{3.4}$$

These ideals have an alternative description in terms of the **Brauer–Jennings–Zassenhaus series** for G, called M-series by Jennings (see [13], or [15, p. 481]): $\mathrm{M}_1(G) = G$, and for $n \geq 2$

$$\mathrm{M}_n(G) = \langle [G, \mathrm{M}_{n-1}(G)], \mathrm{M}_{\lceil n/p\rceil}(G)^p \rangle \tag{3.5}$$

where $\lceil n/p\rceil$ is the smallest integer $\geq n/p$. Jennings' result is that

$$\mathrm{M}_n(G) = \mathrm{D}_n(G), \tag{3.6}$$

where the n**-th dimension subgroup** $\mathrm{D}_n(G)$ is defined by

$$\mathrm{D}_n(G) = G \cap (1 + \mathrm{I}(kG)^n).$$

Passi and Sehgal [14] showed that

$$\begin{aligned} \mathrm{H}_n(kG) &= \mathrm{I}(k\mathrm{M}_n(G))kG + \mathrm{I}(kG)^{n+1} \\ &= (\mathrm{M}_n(G) - 1) + \mathrm{I}(kG)^{n+1}. \end{aligned} \tag{3.7}$$

Now we are in a position to prove:

LEMMA 3.5: *Let G be a finite p-group with a proper normal subgroup A of order p. If G is not a Klein's four-group, and J is a 1-dimensional ideal in $s(G,A)$ such that $s(G,A)/J$ is the group algebra of a finite group, then $J = \{A-1\}$.*

Proof: Let J be a 1-dimensional ideal in $s(G,A)$ such that $s(G,A)/J$ is the group algebra of a finite group. As $s(G,A)$ modulo its radical is isomorphic to k, it follows that $s(G,A)/J$ is isomorphic to kP for a p-group P. Let J_0 be the kernel of the natural homomorphism $kG \longrightarrow s(G,A)/J$, let π: $kG \longrightarrow kG/J_0$ be the natural map, and fix an isomorphism θ: $kG/J_0 \longrightarrow kP$. Suppose that $J \neq \{A-1\}$. Then $(A-1)\pi \neq 0$. As $\{A-1\}$ annihilates the radical of $s(G,A)$, the image $(A-1)\pi\theta$ annihilates the radical of kP, and it follows that $k(A-1)\pi\theta = k\widehat{P}$, where $\widehat{P}$ denotes the sum of the elements of P. We have $A \subseteq \mathrm{M}_n(G) \setminus \mathrm{M}_{n+1}(G)$ for some integer n; by (3.6), equivalently $A - 1 \in \mathrm{I}(kG)^n \setminus \mathrm{I}(kG)^{n+1}$.

Suppose that $\mathrm{I}(kP)^{n+1} \neq 0$, so that $\widehat{P} \in \mathrm{I}(kP)^{n+1}$. Then $A - 1 \subseteq \mathrm{I}(kG)^{n+1} + J_0$. Note that J, as a 1-dimensional ideal in $s(G,A)$, is contained in the annihilator of the radical of $s(G,A)$, so by Lemma 3.4 and (3.3), $J_0 = \mathrm{I}(kA)\mathrm{I}(kG) + k\sigma$ where σ denotes the sum of a system of coset representatives of A in G. It follows that $A - 1 \subseteq \mathrm{I}(kG)^{n+1} + k\sigma$. Consequently $\sigma \in \mathrm{I}(kG)^n \setminus \mathrm{I}(kG)^{n+1}$ and

$$k\sigma + \mathrm{I}(kG)^{n+1} = (A-1) + \mathrm{I}(kG)^{n+1}. \tag{3.8}$$

However, we can choose a Jennings basis of $\mathrm{I}(kG)$ (see [13], or [15, Chapter 3,§3]) which, by [9, Theorem 7], contains the sum $\tilde{\sigma}$ of a system of coset representatives of A in G, and by (3.3), $\tilde{\sigma} \in \sigma + (A-1) + \mathrm{I}(kG)^{n+1}$. We can also assume that the Jennings basis contains $a - 1$ for some $1 \neq a \in A$. Then $\tilde{\sigma}$ and $a - 1$ are linearly independent over $\mathrm{I}(kG)^{n+1}$ (see [15, Chapter 3, Lemma 3.5]), which contradicts (3.8). Hence $\mathrm{I}(kP)^{n+1} = 0$, and $\mathrm{I}(kP)^n = k\widehat{P}$.

We have shown that $\mathrm{I}(kG)^{n+1}$ is contained in J_0, and that $\mathrm{I}(kG)^n$ maps to a 1-dimensional ideal in kG/J_0. Together with (3.7), it follows that the Zassenhaus ideal $\mathrm{H}_n(kG)$ maps under π onto $(A-1)\pi$, so $\mathrm{H}_n(kG)\pi\theta = k\widehat{P}$. Furthermore, $\mathrm{H}_n(kG)\pi\theta = \mathrm{H}_n(kP)$ by (3.4) since $\mathrm{I}(kG)\pi\theta = \mathrm{I}(kP)$. By (3.7), $\mathrm{H}_n(kP) = \mathrm{M}_n(P) - 1$. Hence $k\widehat{P} = \mathrm{M}_n(P) - 1$ and it follows that $n = 1$, $\mathrm{I}(kP)^2 = 0$, $kP = \mathbb{F}_2 C_2$ (=group ring of a cyclic group of order 2), and $|G| = 4$. Thus G is cyclic (by assumption), and $J = \{A-1\}$ since $s(G,A) = \mathbb{F}_2 C_4/\mathrm{I}(\mathbb{F}_2 C_4)^3$ has only one ideal of dimension 1. This final contradiction proves the lemma. ∎

We note that the case of G being a Klein's four-group must be excluded. We also note that if G is a Klein's four-group, then with $A = G$ and B a subgroup of order 2, we have $s(G,A) \cong s(G,B)$ as $\mathrm{I}(\mathbb{F}_2 A)\mathrm{I}(\mathbb{F}_2 G) = \mathrm{I}(\mathbb{F}_2 G)^2 = \mathrm{I}(\mathbb{F}_2 B)\mathrm{I}(\mathbb{F}_2 G)$.

We finally record:

PROPOSITION 3.6: *Let G and H be finite non-cyclic p-groups, with central elementary abelian proper subgroups A and B, respectively. Suppose that H/B is not of order two. Then an isomorphism between $s(G,A)$ and $s(H,B)$, if existing, maps $\{A-1\}$ onto $\{B-1\}$.*

Proof: Assume that we are given an isomorphism θ: $s(G,A) \longrightarrow s(H,B)$. For some set T of coset representatives of A in G, let τ_A be the image of $\sum_{t\in T} t$ in $s(G,A)$, and define similarly $\tau_B \in s(G,B)$.

Suppose that $A = 1$ and $B \neq 1$. Then the annihilator of the radical of $s(G,A)$ $(= kG)$ is 1-dimensional. Consequently $\{B-1\}$ is 1-dimensional and τ_B does not annihilate the radical of $s(H,B)$, since otherwise the annihilator of the radical of $s(H,B)$ would be at least 2-dimensional. By Lemma 3.4, it follows that H is cyclic, contrary to our assumption. Thus we can assume that $A, B \neq 1$.

Suppose that τ_A annihilates the radical of $s(G,A)$ but τ_B does not annihilate the radical of $s(H,B)$. Then by Lemma 3.4, $\{A-1\}\theta = \{\tilde{B}-1\}$ for some subgroup $\tilde{B}$ of B of index p. By (3.2), it follows that $kG/A \cong s(H/\tilde{B}, B/\tilde{B})$. But kG/A has dimension $|G/A|$ whereas $s(H/\tilde{B}, B/\tilde{B})$ has dimension $1+|H/B|$, which is impossible since p divides the first, but not the second number. Hence we can assume, by Lemma 3.4, that both τ_A and τ_B annihilate the radicals.

By Lemma 3.4, θ maps $\{A-1\}+k\tau_A$ onto $\{B-1\}+k\tau_B$. In particular, A and B have the same order. There are subgroups $\tilde{A}$ and $\tilde{B}$ of index p in A and B, respectively, such that θ maps $\{\tilde{A}-1\}$ onto $\{\tilde{B}-1\}$. By (3.2), θ induces an iso-

morphism between the small group rings $s(G/\tilde{A}, A/\tilde{A})$ and $s(H/\tilde{B}, B/\tilde{B})$. The image J of $\{A/\tilde{A}-1\}$ in $s(H/\tilde{B}, B/\tilde{B})$ is a 1-dimensional ideal, with quotient isomorphic to the group algebra kG/A. By assumption, $H/\tilde{B}$ is not a Klein's four-group, so $J = \{B/\tilde{B}-1\}$ by Lemma 3.5, and it follows that θ maps $\{A-1\}$ onto $\{B-1\}$. ∎

COROLLARY 3.7: *Let G and H be finite p-groups, with central elementary abelian subgroups A and B contained in the Frattini subgroups $\Phi(G)$ and $\Phi(H)$, respectively. If G is cyclic, suppose that G and H have the same order. Then an isomorphism between $s(G,A)$ and $s(H,B)$, if existing, maps $\{A-1\}$ onto $\{B-1\}$.*

Proof: The radical of $s(G,A)$ modulo its square is isomorphic to $\mathrm{I}(kG)/\mathrm{I}(kG)^2$, a quotient which is known to be isomorphic to $G/\Phi(G)$ (cf. [10, VI, Lemma 4.1]). It follows that G and H are either both cyclic or non-cyclic. If H is non-cyclic, then H/B is not of order two, and the statement follows from Proposition 3.6. Otherwise G and H are cyclic of the same order, and the small group rings are uniserial (see [9, Corollary 14] or [1, p. 26]), so the statement follows also in this case.

4. Central Frattini extensions and the small group ring

Let H be a (fixed) finite p-group, and let

$$1 \longrightarrow R \longrightarrow F \longrightarrow H \longrightarrow 1 \tag{4.1}$$

be any presentation with F free. Additionally, we assume that

$$R \leq [F,F]F^p \tag{4.2}$$

(this holds, for example, if F is free on a minimal generating set of H). We set

$$L = [F,R]R^p$$

and $E = F/L$, $V = R/L$, so that

$$\begin{array}{cccccccccc} & & 1 & \longrightarrow & R/L & \longrightarrow & F/L & \longrightarrow & H & \longrightarrow 1 \\ & & & & \| & & \| & & \| & \\ \mathbb{E}: & & 1 & \longrightarrow & V & \longrightarrow & E & \longrightarrow & H & \longrightarrow 1 \end{array} \tag{4.3}$$

is a central extension of H by the elementary abelian p-group V, and by (4.2), V is contained in the Frattini subgroup $\Phi(E)$. We shall see (in Lemma 4.2) that $\mathbb{E}$ is the 'universal one' among all extensions of H having these properties.

Definition 4.1: We denote by $\mathbb{F}(H)$ the collection of all central extensions

$$1 \longrightarrow A \longrightarrow G \longrightarrow H \longrightarrow 1$$

with A an elementary abelian p-group whose image in G is contained in the Frattini subgroup of G. (Such an extension might be called a **central Frattini extension**.)

In this section, we give a description of the isomorphism classes of the extensions in $\mathbb{F}(H)$ in terms of an $\mathrm{Out}(H)$-action on V, as well as a description of a coarser equivalence relation related to the small group ring in terms of an $\mathrm{Out}(kH)$-action on V. (As before, k denotes the field with p elements.) We begin with the following basic lemma.

LEMMA 4.2: *Suppose that an exact sequence in $\mathbb{F}(H)$ is given:*

$$1 \longrightarrow A \xrightarrow{\iota} G \xrightarrow{\varphi} H \longrightarrow 1. \tag{4.4}$$

Then $G \cong E/\operatorname{obspace}\mathbb{E}_\varphi$, where

$$\mathbb{E}_\varphi\colon\ 1 \longrightarrow V \longrightarrow E \longrightarrow H \longrightarrow 1, \quad \text{with } G \xrightarrow{\varphi} H \tag{4.5}$$

More precisely, we have a commutative diagram in which all vertical maps are isomorphisms:

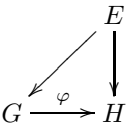
$$\begin{array}{ccccccccc}
1 & \longrightarrow & A & \xrightarrow{\iota} & G & \xrightarrow{\varphi} & H & \longrightarrow & 1 \\
 & & \uparrow & & \uparrow & & \| & & \\
1 & \longrightarrow & V/\operatorname{obspace}\mathbb{E}_\varphi & \longrightarrow & E/\operatorname{obspace}\mathbb{E}_\varphi & \longrightarrow & H & \longrightarrow & 1.
\end{array}$$

Proof: By the universal property of F, we have a commutative diagram

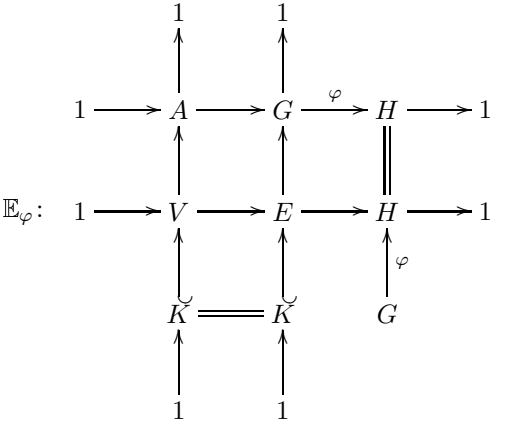
$$\begin{array}{ccccccccc}
 & & & & & & F & & \\
 & & & & & \swarrow^{\psi} & \downarrow & & \\
1 & \longrightarrow & A & \xrightarrow{\iota} & G & \xrightarrow{\varphi} & H & \longrightarrow & 1 \\
 & & & & & & \downarrow & & \\
 & & & & & & 1 & &
\end{array}$$

Note that G is generated by $A\iota$ and $F\psi$. Since $A\iota \leq \Phi(G)$, and elements of the Frattini subgroup are non-generators (see [17, 5.2.12]), it follows that ψ is

surjective. Moreover, $R\psi \leq A\iota$ implies that $L\psi = [F,R]R^p\psi = 1$, so that we have a factorization



Now consider the commutative diagram



Set $U = \operatorname{obspace}\mathbb{E}_\varphi$. By Proposition 2.2, $U \leq K$. In particular, $|G| = |E/K| \leq |E/U|$. The same argument as in the beginning of the proof shows that a lifting $G \longrightarrow E/U$ of φ is surjective, so $|G| \geq |E/U|$. Thus $U = K$ as desired, and the final statement follows from the above diagram. ∎

Next, we define two equivalence relations on $\mathbb{F}(H)$.

Definition 4.3: Two extensions

$$1 \longrightarrow \tilde{A} \xrightarrow{\tilde{\iota}} \tilde{G} \xrightarrow{\tilde{\varphi}} H \longrightarrow 1, \tag{4.6}$$

$$1 \longrightarrow A \xrightarrow{\iota} G \xrightarrow{\varphi} H \longrightarrow 1$$

from $\mathbb{F}(H)$ are **isomorphic** if there exists a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \tilde{A} & \xrightarrow{\tilde{\iota}} & \tilde{G} & \xrightarrow{\tilde{\varphi}} & H & \longrightarrow & 1 \\ & & \uparrow & & \uparrow & & \uparrow{\scriptstyle \alpha} & & \\ 1 & \longrightarrow & A & \xrightarrow{\iota} & G & \xrightarrow{\varphi} & H & \longrightarrow & 1 \end{array} \tag{4.7}$$

where the vertical maps are isomorphisms. Furthermore, we shall say that the two extensions (4.6) are **s-equivalent** if we have a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \{\tilde{A}-1\} & \longrightarrow & s(\tilde{G},\tilde{A}\tilde{\iota}) & \xrightarrow{\tilde{\varphi}} & kH & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \uparrow{\scriptstyle \alpha} & & \\ 0 & \longrightarrow & \{A-1\} & \longrightarrow & s(G,A\iota) & \xrightarrow{\varphi} & kH & \longrightarrow & 0 \end{array} \tag{4.8}$$

where the vertical maps are isomorphisms.

Certainly, isomorphic extensions are s-equivalent. If we consider short exact sequences (4.6) from $\mathbb{F}(H)$ up to one of these equivalence relations, we can assume (and will do) that the injections ι and $\tilde{\iota}$ are in fact inclusions.

By Corollary 3.7, two extensions (4.6) from $\mathbb{F}(H)$ are s-equivalent if and only if the associated small group rings $s(G,A)$ and $s(\tilde{G},\tilde{A})$ are isomorphic.

We shall define an action of $\mathrm{Out}(kH)$ on $V = R/L = R/[F,R]R^p$. As H is a p-group, $\mathrm{Out}(H)$ naturally embeds into $\mathrm{Out}(kH)$, a fact which was observed independently by Coleman [5] and Ward [22]. Then we will have the following straightforward result.

THEOREM 4.4: *The isomorphism classes of extensions in $\mathbb{F}(H)$ are in bijection with the $\mathrm{Out}(H)$-orbits of subspaces of V, and the s-equivalence classes of extensions in $\mathbb{F}(H)$ are in bijection with the $\mathrm{Out}(kH)$-orbits of subspaces of V. Both correspondences are given as follows: The class of the extension (4.4) in $\mathbb{F}(H)$ corresponds to the orbit of* $\mathrm{obspace}\,\mathbb{E}_\varphi$*, where the diagram $\mathbb{E}_\varphi$ is given by (4.5). Conversely, the orbit of $U \leq V$ corresponds to the class of*

$$1 \longrightarrow V/U \longrightarrow E/U \longrightarrow H \longrightarrow 1.$$

THE ACTION OF $\mathrm{Out}(kH)$: We shall first define the action of $\mathrm{Out}(H)$ on V, which can be done more easily. Let $\alpha \in \mathrm{Aut}(H)$. By the universal property of F, we have a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & R/L & \longrightarrow & F/L & \longrightarrow & H & \longrightarrow & 1 \\ & & \uparrow & & \uparrow{\scriptstyle \beta} & & \uparrow{\scriptstyle \alpha} & & \\ 1 & \longrightarrow & R & \longrightarrow & F & \longrightarrow & H & \longrightarrow & 1 \end{array}$$

From $R\beta \subseteq R/L$ it is immediate that $L\beta = [F,R]R^p\beta = 1$, and we obtain a

'lift' $\hat{\alpha}$, i.e., a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & V & \longrightarrow & E & \longrightarrow & H & \longrightarrow & 1 \\ & & \uparrow & & \uparrow{\scriptstyle \hat{\alpha}} & & \uparrow{\scriptstyle \alpha} & & \\ 1 & \longrightarrow & V & \longrightarrow & E & \longrightarrow & H & \longrightarrow & 1 \end{array}$$

Note that $\hat{\alpha} \in \mathrm{Aut}(E)$ since $V \leq \Phi(E)$. Assume that for some $\gamma \in \mathrm{Aut}(E)$, we have a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & V & \longrightarrow & E & \longrightarrow & H & \longrightarrow & 1 \\ & & \uparrow & & \uparrow{\scriptstyle \gamma} & & \| & & \\ 1 & \longrightarrow & V & \longrightarrow & E & \longrightarrow & H & \longrightarrow & 1 \end{array}$$

This means that γ induces the identity on E/V. A simple computation using that V is central of exponent p shows that γ fixes $\Phi(E) = [E,E]E^p$, so in particular V, element-wise. Thus we get a well-defined action of $\mathrm{Aut}(H)$ on V by letting α act via a lift $\hat{\alpha}$. Inner automorphisms lift to inner automorphisms which act trivially on V, so we really have an action of $\mathrm{Out}(H)$ on V.

Similarly, the action of $\mathrm{Out}(kH)$ on V is defined. Let $\alpha \in \mathrm{Aut}(kH)$. By the universal property of F, we have a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & V & \longrightarrow & s(E,V)^\times & \longrightarrow & (kH)^\times & \longrightarrow & 1 \\ & & \uparrow & & \uparrow{\scriptstyle \pi} & & \| & & \\ 1 & \longrightarrow & 1+\mathrm{I}(kV)kE & \longrightarrow & (kE)^\times & \longrightarrow & (kH)^\times & \longrightarrow & 1 \\ & & \uparrow & & \uparrow{\scriptstyle \beta} & & \uparrow{\scriptstyle \alpha} & & \\ 1 & \longrightarrow & R & \longrightarrow & F & \longrightarrow & H & \longrightarrow & 1 \end{array}$$

The k-linear extension $\beta\colon kF \longrightarrow kE$ maps $\mathrm{I}(kR)kF$ into $\mathrm{I}(kV)kE$ and $\mathrm{I}(kF)$ into $\mathrm{I}(kE)$. Also note that V is a central elementary abelian p-subgroup of $s(E,V)^\times$, so $L\beta\pi = 1$. Hence we get a lift $\hat{\alpha}$ such that

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \{V-1\} & \longrightarrow & s(E,V) & \longrightarrow & kH & \longrightarrow & 0 \\ & & \uparrow & & \uparrow{\scriptstyle \hat{\alpha}} & & \uparrow{\scriptstyle \alpha} & & \\ 0 & \longrightarrow & \{V-1\} & \longrightarrow & s(E,V) & \longrightarrow & kH & \longrightarrow & 0 \end{array} \tag{4.9}$$

is commutative. Let $\widehat{\alpha^{-1}}$ be a lift of α^{-1}. Then $E\hat{\alpha}\widehat{\alpha^{-1}}$ maps onto H under the map $s(E,V) \longrightarrow kH$, whence is a subgroup of E. Since $V \leq \Phi(E)$, it follows that $E\hat{\alpha}\widehat{\alpha^{-1}} = E$, and consequently $\hat{\alpha} \in \mathrm{Aut}(s(E,V))$.

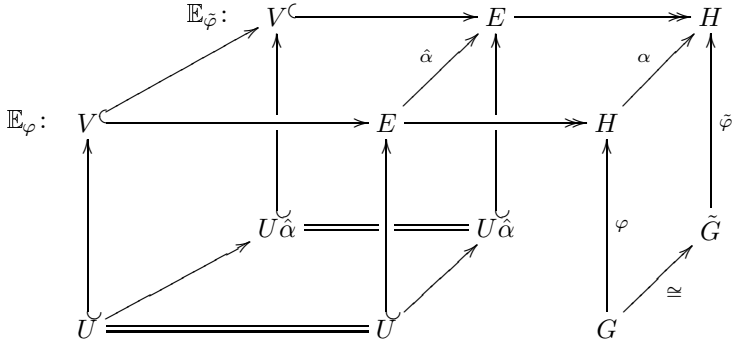
Assume that for some $\gamma \in \mathrm{Aut}(s(E,V))$, we have a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \{V-1\} & \longrightarrow & s(E,V) & \longrightarrow & kH & \longrightarrow & 0 \\ & & \uparrow & & \uparrow{\scriptstyle \gamma} & & \| & & \\ 0 & \longrightarrow & \{V-1\} & \longrightarrow & s(E,V) & \longrightarrow & kH & \longrightarrow & 0 \end{array}$$

Then γ fixes $[E,E]E^p$, so in particular V, element-wise. Using the natural isomorphism $V \cong \{V-1\}$, we obtain a well-defined action of $\mathrm{Aut}(kH)$ on V by letting α act via a lift $\hat{\alpha}$. Inner automorphisms lift to inner automorphisms which act trivially on $\{V-1\}$, so we have indeed an action of $\mathrm{Out}(kH)$ on V.

It is immediate that this action, when restricted to $\mathrm{Out}(H)$, coincides with the action of $\mathrm{Out}(H)$ defined before.

Proof of Theorem 4.4: We first treat the parametrization of the isomorphism classes of extensions. Given two isomorphic extensions in $\mathbb{F}(H)$, as shown in (4.7), and any subspace U of V, we have a commutative diagram



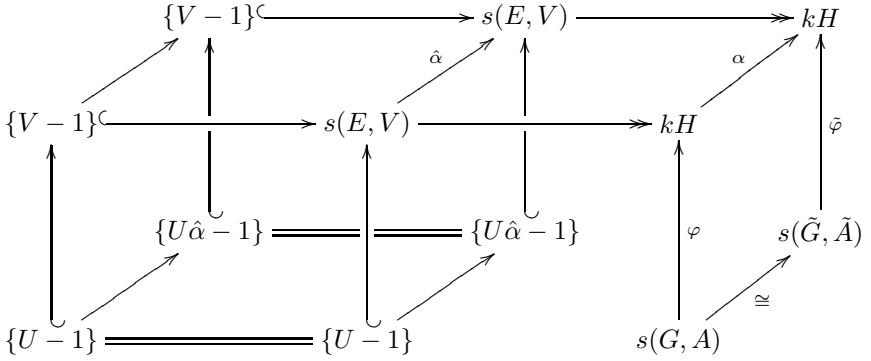
showing that φ factors over E/U if and only if $\tilde{\varphi}$ factors over $E/U\hat{\alpha}$. Thus $\hat{\alpha}$ maps obspace $\mathbb{E}_{\varphi}$ to obspace $\mathbb{E}_{\tilde{\varphi}}$ by Proposition 2.2, and both extensions define the same $\mathrm{Out}(H)$-orbit of subspaces of V.

Conversely, let U be a subspace of V, and let $\alpha \in \mathrm{Aut}(H)$, with lift $\hat{\alpha} \in \mathrm{Aut}(E)$. Then we have a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & V/U\hat{\alpha} & \longrightarrow & E/U\hat{\alpha} & \longrightarrow & H & \longrightarrow & 1 \\ & & \uparrow & & \uparrow & & \uparrow{\scriptstyle \alpha} & & \\ 1 & \longrightarrow & V/U & \longrightarrow & E/U & \longrightarrow & H & \longrightarrow & 1 \end{array}$$

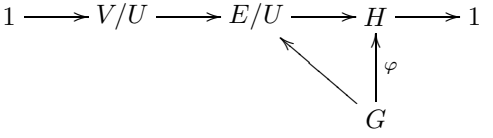
where the vertical map in the middle is induced by $\hat{\alpha}$. This shows that U and $U\hat{\alpha}$ define isomorphic extensions. Thus we have well-defined maps, and it follows from Lemma 4.2 that they are mutually inverse.

Next, assume that we are given two extensions in $\mathbb{F}(H)$, as shown in (4.6), which are s-equivalent, as shown in (4.8). Then for any subspace U of V, we have a commutative diagram

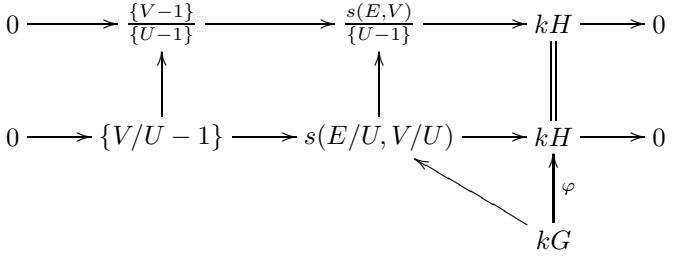


Hence φ factors over $s(E,V)/\{U-1\}$ if and only if $\tilde{\varphi}$ factors over $s(E,V)/\{U\hat{\alpha}-1\}$.

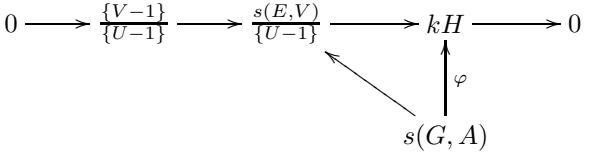
Note that a commutative diagram



affords by (3.2) a commutative diagram



Since $\mathrm{I}(kA)$ is mapped into $\{V/U-1\}$ under the diagonal map, $\mathrm{I}(kA)\mathrm{I}(kG)$ is contained in the kernel of the diagonal map, and there is an induced commutative diagram



The same applies to the homomorphism $\tilde{\varphi}\colon \tilde{G} \longrightarrow H$.

Thus $\hat{\alpha}$ maps $\{\mathrm{obspace}\,\mathbb{E}_{\varphi} - 1\}$ to $\{\mathrm{obspace}\,\mathbb{E}_{\tilde{\varphi}} - 1\}$ by Corollary 3.2 (where $\mathbb{E}_{\varphi}$ is the diagram (4.5), and $\mathbb{E}_{\tilde{\varphi}}$ is defined analogously), and both extensions define the same $\mathrm{Out}(kH)$-orbit of subspaces of V.

Conversely, let U be a subspace of V, and let $\alpha \in \mathrm{Aut}(kH)$, with lift $\hat{\alpha} \in \mathrm{Aut}(s(E,V))$. By (3.2), we have a commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \{V/U\hat{\alpha} - 1\} & \longrightarrow & s(E/U\hat{\alpha}, V/U\hat{\alpha}) & \longrightarrow & kH & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \| & & \\
0 & \longrightarrow & \frac{\{V-1\}}{\{U\hat{\alpha}-1\}} & \longrightarrow & \frac{s(E,V)}{\{U\hat{\alpha}-1\}} & \longrightarrow & kH & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow{\scriptstyle \alpha} & & \\
0 & \longrightarrow & \frac{\{V-1\}}{\{U-1\}} & \longrightarrow & \frac{s(E,V)}{\{U-1\}} & \longrightarrow & kH & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \| & & \\
0 & \longrightarrow & \{V/U - 1\} & \longrightarrow & s(E/U, V/U) & \longrightarrow & kH & \longrightarrow & 0
\end{array}$$

where the vertical map in the middle is induced by $\hat{\alpha}$, and all vertical maps are isomorphisms. Hence the canonical sequences

$$1 \longrightarrow V/U\hat{\alpha} \longrightarrow E/U\hat{\alpha} \longrightarrow H \longrightarrow 1,$$

$$1 \longrightarrow V/U \longrightarrow E/U \longrightarrow H \longrightarrow 1$$

are s-equivalent. Again we have well-defined maps, which are mutually inverse by Lemma 4.2, and the proof of Theorem 4.4 is complete. ∎

We conclude this section with a couple of remarks.

Remark 4.5: We have shown that any automorphism of kH can be lifted to an automorphism of $s(E,V)$. Conversely, any automorphism of $s(E,V)$ induces an automorphism of kH by Corollary 3.7. An automorphism of $s(E,V)$ which induces the identity of kH is really an automorphism of E which induces the identity on E/V. For the moment, let X denote the group of all these automorphisms. Any σ in X fixes $\Phi(E)$ element-wise (this we noticed already when proving that the $\mathrm{Aut}(H)$-action on V is well-defined), and gives rise to a homomorphism $E \longrightarrow V$, $x \mapsto x^{-1}(x\sigma)$. In this way, we obtain a homomorphism $X \longrightarrow \mathrm{Hom}(E/\Phi(E), V)$, and since conversely any map from $\mathrm{Hom}(E/\Phi(E), V)$ gives rise to an automorphism in X, this is an isomorphism (of abelian groups).

Thus we have an exact sequence

$$1 \longrightarrow \mathrm{Hom}(H/\Phi(H), V) \longrightarrow \mathrm{Aut}(s(E,V)) \longrightarrow \mathrm{Aut}(kH) \longrightarrow 1.$$

Remark 4.6: Let $U \leq V$. The extensions from $\mathbb{F}(H)$ which are s-equivalent to

$$1 \longrightarrow V/U \longrightarrow E/U \longrightarrow H \longrightarrow 1$$

can also be described as follows. We may start from the exact sequence for the small group ring $s(E/U, V/U)$, with associated exact sequence of unit groups

$$1 \longrightarrow V/U \longrightarrow s(E/U, V/U)^\times \xrightarrow{\kappa} (kH)^\times \longrightarrow 1.$$

Then the extensions

$$1 \longrightarrow V/U \longrightarrow \kappa^{-1}(H\alpha) \xrightarrow{\kappa} H\alpha \longrightarrow 1,$$

$\alpha \in \mathrm{Aut}(kH)$, yield all isomorphism classes of extensions from $\mathbb{F}(H)$ which are s-equivalent to the above extension.

We shall see in the next section that the middle terms $\kappa^{-1}(H\alpha)$ need not be isomorphic to E/U, which shows that automorphisms of kH in general cannot be lifted to automorphisms of $s(E/U, V/U)$.

To verify the claim, let $\alpha \in \mathrm{Aut}(kH)$, with lift $\hat{\alpha} \in \mathrm{Aut}(s(E,V))$. Then we have an isomorphism

$$\begin{array}{ccccccccc}
1 & \longrightarrow & V & \longrightarrow & E\hat{\alpha} & \longrightarrow & H\alpha & \longrightarrow & 1 \\
 & & \uparrow & & \uparrow{\scriptstyle \hat{\alpha}} & & \uparrow{\scriptstyle \alpha} & & \\
1 & \longrightarrow & V & \longrightarrow & E & \longrightarrow & H & \longrightarrow & 1
\end{array}$$

which together with (3.2) shows that we have isomorphisms

$$\begin{array}{ccccccccc}
1 & \longrightarrow & V/U & \longrightarrow & \kappa^{-1}(H\alpha) & \xrightarrow{\kappa} & H\alpha & \longrightarrow & 1 \\
 & & \| & & \uparrow & & \| & & \\
1 & \longrightarrow & V/U & \longrightarrow & E\hat{\alpha}/U & \longrightarrow & H\alpha & \longrightarrow & 1 \\
 & & \uparrow & & \uparrow{\scriptstyle \hat{\alpha}} & & \uparrow{\scriptstyle \alpha} & & \\
1 & \longrightarrow & V/U\hat{\alpha}^{-1} & \longrightarrow & E/U\hat{\alpha}^{-1} & \longrightarrow & H & \longrightarrow & 1
\end{array}$$

For computational purposes, however, the description of an s-equivalence class given by Theorem 4.4 is more convenient.

Remark 4.7: We found Theorem 4.4 while thinking about how the attempt from [2, 3] might be substantiated, as we will briefly set out. Assume that we are given an exact sequence in $\mathbb{F}(H)$:

$$1 \longrightarrow A \hookrightarrow G \xrightarrow{\varphi} H \longrightarrow 1.$$

Then we have a diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \{V-1\} & \longrightarrow & s(E,V) & \longrightarrow & kH & \longrightarrow & 0 \\ & & & & & & \uparrow{\scriptstyle \varphi} & & \\ & & & & & & kG & & \end{array}$$

By Corollary 3.2 and Lemma 4.2, there is a unique minimal ideal $I = \{U-1\}$ of $s(E,V)$ contained in $\{V-1\}$ such that φ factors over $s(E,V)/I$, and $\varphi\colon G \longrightarrow H$ does not only factor over E/U (the pre-image of H), but in fact $G \cong E/U$.

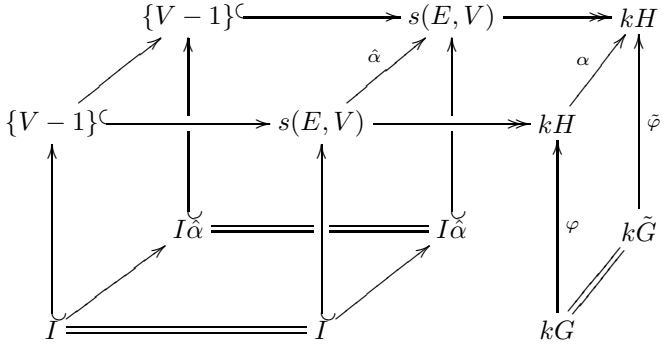
Assume that we are given another exact sequence in $\mathbb{F}(H)$:

$$1 \longrightarrow \tilde{A} \hookrightarrow \tilde{G} \xrightarrow{\tilde{\varphi}} H \longrightarrow 1,$$

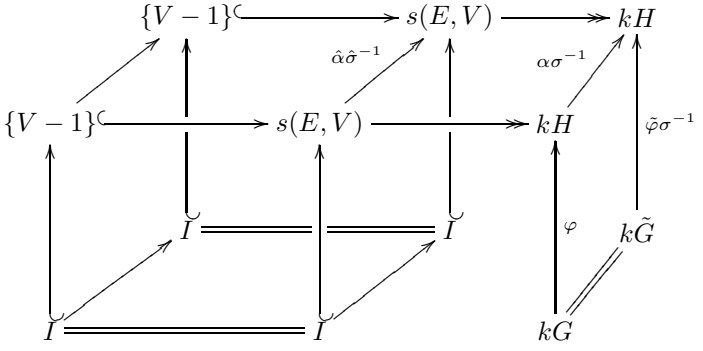
and that $\tilde{G}$ is a group basis of kG. Then, of course, similar remarks hold for the homomorphism $\tilde{\varphi}\colon k\tilde{G} = kG \longrightarrow kH$. Suppose that $G\tilde{\varphi}$ is a group basis of kH, isomorphic to H. Then there is an automorphism α of kH making the following diagram commutative:

(4.10)
$$\begin{array}{ccc} kH & \xrightarrow{\alpha} & kH \\ \uparrow{\scriptstyle \varphi} & & \uparrow{\scriptstyle \tilde{\varphi}} \\ kG & = & k\tilde{G} \end{array}$$

We have seen that α lifts to an automorphism $\hat{\alpha}$ of $s(E,V)$, so that we have a commutative diagram



It follows that $\tilde{\varphi}$ factors over $s(E,V)/I\hat{\alpha}$ with $I\hat{\alpha} = \{U-1\}\hat{\alpha} = \{U\hat{\alpha}-1\}$, and that $\tilde{G} \cong E/U\hat{\alpha}$. Since we wish to conclude that $G \cong \tilde{G}$, we would like to have the subspace I to be fixed under $\hat{\alpha}$. One might hope that the action of $\hat{\alpha}$ can be compensated by a group automorphism σ of H (which lifts to an automorphism $\hat{\sigma}$ of E, as we have seen): Assuming that $I\hat{\alpha}\hat{\sigma}^{-1} = I$, we have a commutative diagram



and can conclude that $\tilde{\varphi}\sigma^{-1}$ factors over $s(E,V)/I$, so that $\tilde{G} \cong E/U \cong G$ (note that E is still the pre-image of $\tilde{G}\tilde{\varphi}\sigma^{-1}$). But it appears that all this is asked for too much.

5. Röhl's observation revisited

In this section, we discuss an observation of Röhl [19, 20], thus relating it to the small group ring, and give, in our setting, a detailed exposition of the main result in [20]. We keep the notation introduced in Section 4.

Let G denote an arbitrary group.

Definition 5.1: A **unipotent automorphism** of kG is an augmentation-preserving automorphism of kG which induces the identity on $\mathrm{I}(kG)/\mathrm{I}(kG)^2$. The unipotent automorphisms of kG form a normal subgroup $\mathrm{UAut}(kG)$ of $\mathrm{Aut}(kG)$.

The notion of unipotent automorphism is also meaningful for quotients of kG. Note that a unipotent automorphism of kG induces the identity on all quotients $\mathrm{I}(kG)^l/\mathrm{I}(kG)^{l+1}$ of successive powers of the augmentation ideal.

It is a well-known result in low degree cohomology that $\mathrm{I}(\mathbb{Z}G)/\mathrm{I}(\mathbb{Z}G)^2 \cong G/[G,G]$ (cf. [10, VI, Lemma 4.1]; the isomorphism maps the coset of $g-1$ to the coset of g, for any $g \in G$). Tensoring with $k = \mathbb{F}_p$ over $\mathbb{Z}$ yields

$$\mathrm{I}(kG)/\mathrm{I}(kG)^2 \cong G/[G,G]G^p. \tag{5.1}$$

Recall that we are given a finite p-group H together with a presentation (4.1) and a 'universal' extension (4.3). We assume that F is free on a minimal generating set of H, so that $E/[E,E]E^p \cong F/[F,F]F^p \cong H/[H,H]H^p$. Combined with (5.1), this yields

$$\mathrm{I}(kE)/\mathrm{I}(kE)^2 \cong \mathrm{I}(kF)/\mathrm{I}(kF)^2 \cong \mathrm{I}(kH)/\mathrm{I}(kH)^2. \tag{5.2}$$

Let $\mathcal{I}$ denote the image of $\mathrm{I}(kE)$ in the small group ring $s(E,V)$ associated with the sequence (4.3). We obtain immediately:

LEMMA 5.2: *Let $\alpha \in \mathrm{UAut}(kH)$, and let $\hat{\alpha} \in \mathrm{Aut}(s(E,V))$ be a lift as shown in (4.9). Then $\hat{\alpha}$ induces the identity on all sections $\mathcal{I}^l/\mathcal{I}^{l+1}$ (i.e., $\hat{\alpha}$ is a unipotent automorphism).*

Proof: We have $\mathcal{I}\hat{\alpha} = \mathcal{I}$ since α is augmentation-preserving, and obtain from (4.9) an induced commutative diagram

$$\begin{array}{ccc} \mathcal{I}/\mathcal{I}^2 & \longrightarrow & \mathrm{I}(kH)/\mathrm{I}(kH)^2 \\ \uparrow{\scriptstyle \hat{\alpha}} & & \| \\ \mathcal{I}/\mathcal{I}^2 & \longrightarrow & \mathrm{I}(kH)/\mathrm{I}(kH)^2 \end{array}$$

The horizontal maps are the isomorphism arising from (5.2) since $\mathrm{I}(kV)\mathrm{I}(kE) \subseteq \mathrm{I}(kE)^2$ implies that $\mathcal{I}/\mathcal{I}^2 \cong \mathrm{I}(kE)/\mathrm{I}(kE)^2$. Hence $\hat{\alpha}$ is a unipotent automorphism. ∎

Recall the definition of the Brauer–Jennings–Zassenhaus series for the group G (and the fixed prime p) from (3.5) and (3.6). We shall write $G^{[n]} = G/\mathrm{M}_{n+1}(G)$ for $n \geq 1$.

We record two simple lemmas.

LEMMA 5.3: *Suppose that $H = F^{[n]}$ for some $n \geq 1$. Then $V = \mathrm{M}_{n+1}(E)$, so $\{V-1\}$ is contained in $\mathcal{I}^{n+1}$ and $\{V-1\} \cap \mathcal{I}^{n+2} = \{\mathrm{M}_{n+2}(E)-1\}$.*

Proof: By assumption, $R = \mathrm{M}_{n+1}(F)$, so $\mathrm{M}_{n+1}(E) = \mathrm{M}_{n+1}(F)L/L = R/L = V$ and the first statement follows. Let $U \leq E$ be such that $\{V-1\} \cap \mathcal{I}^{n+2} = \{U-1\}$. By (3.6), we have $U = E \cap (1 + \mathrm{I}(kE)^{n+2} + \mathrm{I}(kV)\mathrm{I}(kE)) = E \cap (1 + \mathrm{I}(kE)^{n+2}) = \mathrm{M}_{n+2}(E)$, whence the second statement. ∎

Next, we have (cf. [20, Theorem 3.2.1]):

LEMMA 5.4: *Suppose that $H = F^{[n]}$ for some $n \geq 1$. Then for every $m > n$,*

$$\mathrm{Aut}(kH/\mathrm{I}(kH)^m) = \mathrm{Aut}(H) \cdot \mathrm{UAut}(kH/\mathrm{I}(kH)^m).$$

Proof: First, note that the statement makes sense since by (3.6), H embeds into $kH/\mathrm{I}(kH)^m$, and therefore $\mathrm{Aut}(H)$ embeds into $\mathrm{Aut}(kH/\mathrm{I}(kH)^m)$.

Let $\alpha \in \mathrm{Aut}(kH/\mathrm{I}(kH)^m)$. Taking augmentation is a homomorphism, so α is augmentation-preserving since H is a p-group. Hence α induces an automorphism of the abelian group $\mathrm{I}(kH)/\mathrm{I}(kH)^2$, which by (5.1) is canonically isomorphic to $H/\mathrm{M}_2(H)$. Thus, it suffices to show that any automorphism β of $H/\mathrm{M}_2(H)$ can be lifted to an automorphism of H. By the universal property of F, we obtain a homomorphism $\varphi\colon F \longrightarrow H$ making the following diagram commute:

$$\begin{array}{ccc} F & \overset{\varphi}{\dashrightarrow} & H \\ \downarrow & & \downarrow \\ H/\mathrm{M}_2(H) & \xrightarrow{\beta} & H/\mathrm{M}_2(H) \end{array}$$

Then $H = \langle F\varphi, \mathrm{M}_2(H)\rangle = \langle F\varphi, \Phi(H)\rangle = F\varphi$ (see [17, 5.2.12]). Since $\mathrm{M}_{n+1}(F)$ is the kernel of any surjection $F \longrightarrow H = F^{[n]}$, we are done. ∎

COROLLARY 5.5: *Suppose that $H = F^{[n]}$ for some $n \geq 1$. Let $\alpha \in \mathrm{Aut}(kH)$, and let $\hat{\alpha} \in \mathrm{Aut}(s(E,V))$ be a lift as shown in (4.9). Then $\hat{\alpha}$ fixes $\{\mathrm{M}_{n+2}(E)-1\}$, and acts on $\{V-1\}/\{\mathrm{M}_{n+2}(E)-1\}$ just like an automorphism of E.*

Proof: By Lemma 5.4, $\mathrm{Aut}(kH) = \mathrm{Aut}(H) \cdot \mathrm{UAut}(kH)$. From the description of $\{\mathrm{M}_{n+2}(E)-1\}$ given in Lemma 5.3 it follows that $\hat{\alpha}$ fixes $\{\mathrm{M}_{n+2}(E)-1\}$.

Recall from the definition of the action of $\mathrm{Out}(kH)$ on V in Section 4 that if $\alpha \in \mathrm{Aut}(H)$, then α actually can be lifted to an automorphism of E which acts on V just like the given lift $\hat{\alpha}$.

Thus we can assume that α is a unipotent automorphism. Then $\hat{\alpha}$ is a unipotent automorphism by Lemma 5.2, whence acts trivially on $\{V-1\}/\{\mathrm{M}_{n+2}(E)-1\}$ by Lemma 5.3. The corollary is proved. ∎

From now on, we let $H = F^{[n]}$ for some $n \geq 1$. Writing $F_i = \mathrm{M}_i(F)$, we then have $R = F_{n+1}$, so $L = [F,R]R^p \leq F_{n+2}$ by (3.5) and $\mathrm{M}_{n+2}(E) = F_{n+2}/L$. Setting $\bar{E} = E/\mathrm{M}_{n+2}(E)$, we have a central extension in $\mathbb{F}(H)$:

$$\begin{array}{cccccccccc} & 1 & \longrightarrow & F_{n+1}/F_{n+2} & \longrightarrow & F^{[n+1]} & \longrightarrow & F^{[n]} & \longrightarrow & 1 \\ & & & \| & & \| & & \| & & \\ \bar{\mathbb{E}}\colon & 1 & \longrightarrow & \bar{V} & \longrightarrow & \bar{E} & \longrightarrow & H & \longrightarrow & 1 \end{array}$$

For the moment, let us denote by $\mathbb{F}^{[n]}$ the collection of all exact sequences (4.4) in $\mathbb{F}(H)$ such that $\mathrm{M}_{n+2}(G) = 1$.

If (4.4) is a sequence in $\mathbb{F}^{[n]}$, with associated diagram $\mathbb{E}_\varphi$ as shown in (4.5), then $\mathrm{M}_{n+2}(E) \leq \mathrm{obspace}\,\mathbb{E}_\varphi$ by Lemma 4.2, and we may replace in the formulation of Lemma 4.2 the diagram $\mathbb{E}_\varphi$ by the diagram $\bar{\mathbb{E}}_\varphi$. Moreover, the action of $\mathrm{Out}(kH)$ on V gives rise to an action of $\mathrm{Out}(kH)$ on $\bar{V}$ which is really an $\mathrm{Out}(H)$-action, as we have seen in Corollary 5.5. Following the proof of Theorem 4.4, we obtain mutatis mutandis:

PROPOSITION 5.6: *With the notation as above, the following classes are in natural bijection:*

- *the isomorphism classes of extensions in* $\mathbb{F}^{[n]}$*;*
- *the* $\mathrm{Out}(H)$*-orbits of subspaces of* $\bar{V}$*;*
- *the s-equivalence classes of extensions in* $\mathbb{F}^{[n]}$*.*

Assume that we are given two exact sequences (4.6) in $\mathbb{F}^{[n]}$. These sequences are isomorphic if and only if the middle terms G and $\tilde{G}$ are isomorphic since $A = \mathrm{M}_{n+1}(G)$ and $\tilde{A} = \mathrm{M}_{n+1}(\tilde{G})$. Recall from Corollary 3.7 that s-equivalence means isomorphism of small group rings. Thus we have shown that if the small group rings $s(G, \mathrm{M}_{n+1}(G))$ and $s(\tilde{G}, \mathrm{M}_{n+1}(\tilde{G}))$ are isomorphic, then the groups G and $\tilde{G}$ are isomorphic. However, as yet we do not know whether the small group rings are isomorphic provided that the group algebras kG and $k\tilde{G}$ are isomorphic.

If $kG = k\tilde{G}$, we also do not know whether we have a commutative diagram (4.10) at our disposal, so we cannot compare "obstructions" using the small group ring, but in the present case one can use the following simple observation.

LEMMA 5.7: *Suppose that* G *and* $\tilde{G}$ *are two finite groups such that* $G^{[n]} \cong \tilde{G}^{[n]}$ *for some* $n \geq 1$*, and that there is an isomorphism* $\theta\colon kG/\mathrm{I}(kG)^m \longrightarrow k\tilde{G}/\mathrm{I}(k\tilde{G})^m$ *for some* $m > n+1$ *which maps* $\mathrm{I}(kG)/\mathrm{I}(kG)^m$ *onto* $\mathrm{I}(k\tilde{G})/\mathrm{I}(k\tilde{G})^m$*. Set* $Q = G^{[n]}$*, and identify* Q *with its isomorphic image in* $kQ/\mathrm{I}(kQ)^{n+1}$*. Then there is a commutative diagram*

$$\begin{array}{ccc} kQ/\mathrm{I}(kQ)^{n+1} & \xrightarrow{\alpha} & kQ/\mathrm{I}(kQ)^{n+1} \\ \uparrow{\scriptstyle \varphi} & & \uparrow{\scriptstyle \tilde{\varphi}} \\ kG/\mathrm{I}(kG)^m & \xrightarrow{\theta} & k\tilde{G}/\mathrm{I}(k\tilde{G})^m \end{array}$$

such that $G\varphi = Q = \tilde{G}\tilde{\varphi}$*, and* α *is an isomorphism.*

Suppose further that $m = n + 2$, and that α is induced by an automorphism of Q. Then there exists an isomorphism $G^{[n+1]} \longrightarrow \tilde{G}^{[n+1]}$ which induces α.

Proof: Note that for any group X, we have a canonical isomorphism

$$kX/\mathrm{I}(kX)^{n+1} \cong kX^{[n]}/\mathrm{I}(kX^{[n]})^{n+1}.$$

Indeed, the kernel of the composition $kX \longrightarrow kX^{[n]} \longrightarrow kX^{[n]}/\mathrm{I}(kX^{[n]})^{n+1}$ is $\mathrm{I}(kX)^{n+1}+\mathrm{I}(k\mathrm{M}_{n+1}(X))kX$, and by (3.6), $\mathrm{I}(k\mathrm{M}_{n+1}(X)) \subseteq \mathrm{I}(kX)^{n+1}$. The map φ above is the composition of the quotient map $kG/\mathrm{I}(kG)^m \longrightarrow kG/\mathrm{I}(kG)^{n+1}$ and this canonical isomorphism, and $\tilde{\varphi}$ is the composition of the similarly defined map $k\tilde{G}/\mathrm{I}(k\tilde{G})^m \longrightarrow k\tilde{G}^{[n]}/\mathrm{I}(k\tilde{G}^{[n]})^{n+1}$ and an isomorphism arising from an isomorphism $\tilde{G}^{[n]} \cong Q$.

The kernel of both φ and $\theta\tilde{\varphi}$ is $\mathrm{I}(kG)^{n+1}/\mathrm{I}(kG)^m$, so that there is an isomorphism α making the above diagram commutative.

Now suppose further that $m = n + 2$ and $Q\alpha = Q$. By definition (3.4) of the Zassenhaus ideals, θ maps $\mathrm{H}_{n+1}(kG)/\mathrm{I}(kG)^{n+2}$ onto $\mathrm{H}_{n+1}(k\tilde{G})/\mathrm{I}(k\tilde{G})^{n+2}$. By (3.7) and (3.6), these quotients are naturally isomorphic to $\mathrm{M}_{n+1}(G)/\mathrm{M}_{n+2}(G)$ and $\mathrm{M}_{n+1}(\tilde{G})/\mathrm{M}_{n+2}(\tilde{G})$, respectively. In particular, $G^{[n+1]}$ and $\tilde{G}^{[n+1]}$ have the same order. Choose a subspace C of $k\tilde{G}$ with $\mathrm{I}(k\tilde{G})^{n+2} \leq C \leq \mathrm{I}(k\tilde{G})^{n+1}$ such that $C/\mathrm{I}(k\tilde{G})^{n+2}$ is a complement to $\mathrm{H}_{n+1}(k\tilde{G})/\mathrm{I}(k\tilde{G})^{n+2}$ in $\mathrm{I}(k\tilde{G})^{n+1}/\mathrm{I}(k\tilde{G})^{n+2}$. Note that C is an ideal of $k\tilde{G}$, and that $\tilde{\varphi}$ factors over $k\tilde{G}/C$. Identify the image of G in $kG/\mathrm{I}(kG)^{n+2}$ with $G^{[n+1]}$, and the image of $\tilde{G}$ in $k\tilde{G}/\mathrm{I}(k\tilde{G})^{n+2}$ or $k\tilde{G}/C$ with $\tilde{G}^{[n+1]}$. Then $G^{[n+1]}\theta$ embeds into $k\tilde{G}/C$ since

$$(G^{[n+1]}\theta - 1) \cap \mathrm{I}(k\tilde{G})^{n+1}/\mathrm{I}(k\tilde{G})^{n+2} = \mathrm{H}_{n+1}(k\tilde{G})/\mathrm{I}(k\tilde{G})^{n+2}.$$

Also $G^{[n+1]}\theta\tilde{\varphi} = Q$ by assumption, and the pre-image of Q in $(k\tilde{G}/C)^\times$ is $\tilde{G}^{[n+1]}$. It follows that $G^{[n+1]}$ maps onto $\tilde{G}^{[n+1]}$ in $k\tilde{G}/C$, which yields the desired isomorphism. ∎

Röhl's result is slightly stronger than the above proposition. In the end, we shall give another proof thereof, which in particular avoids induction on n, and shows that there is no need for replacing kF by a (completed) inverse limit of its quotients by powers of the augmentation ideal.

Note that by (3.7), the assumption $\mathrm{M}_{n+2}(\tilde{G}) = 1$ in the following theorem is automatically fullfilled if $kG \cong k\tilde{G}$.

THEOREM 5.8 ([20, Theorem 3.1.2]): *Let $\mathrm{M}_{n+2}(F) \leq U \leq \mathrm{M}_{n+1}(F)$ for some $n \geq 1$, and set $G = F/U$. Then $kG/\mathrm{I}(kG)^{n+2} \cong k\tilde{G}/\mathrm{I}(k\tilde{G})^{n+2}$ for a group $\tilde{G}$ with $\mathrm{M}_{n+2}(\tilde{G}) = 1$ implies $G \cong \tilde{G}$.*

Proof: Our assumption on G is that $G^{[n]} = F^{[n]} = H$ and $\mathrm{M}_{n+2}(G) = 1$.

Let $\theta\colon kG/\mathrm{I}(kG)^{n+2} \longrightarrow k\tilde{G}/\mathrm{I}(k\tilde{G})^{n+2}$ be an isomorphism, and let X denote either G or $\tilde{G}$. Note that since X is a p-group, $\mathrm{I}(kX)/\mathrm{I}(kX)^{n+2}$ is the radical of $kX/\mathrm{I}(kX)^{n+2}$.

By (3.7) and (3.6), the elementary abelian quotient $\mathrm{M}_i(X)/\mathrm{M}_{i+1}(X)$ is isomorphic to the image of the Zassenhaus ideal $\mathrm{H}_i(kX)$ in $kX/\mathrm{I}(kX)^{i+1}$, and by the definition (3.4) of the Zassenhaus ideals, these images are determined by the ring $kX/\mathrm{I}(kX)^{n+2}$ as long as $i \leq n+1$. Therefore $\mathrm{M}_i(G)/\mathrm{M}_{i+1}(G)$ and $\mathrm{M}_i(\tilde{G})/\mathrm{M}_{i+1}(\tilde{G})$ are isomorphic for $i \leq n+1$. In particular, $|G| = |\tilde{G}|$. Moreover, $\tilde{G}^{[n]} \cong H$ as any group X with $\mathrm{M}_{n+1}(X) = 1$ and $X/\mathrm{M}_2(X) \cong G/\mathrm{M}_2(G)$ is a homomorphic image of H.

Thus by Lemma 5.7, we have a commutative diagram

$$\begin{array}{ccc} kH/\mathrm{I}(kH)^{n+1} & \xrightarrow{\alpha} & kH/\mathrm{I}(kH)^{n+1} \\ \uparrow{\scriptstyle\varphi} & & \uparrow{\scriptstyle\tilde{\varphi}} \\ kG/\mathrm{I}(kG)^{n+2} & \xrightarrow{\theta} & k\tilde{G}/\mathrm{I}(k\tilde{G})^{n+2} \end{array}$$

with $G\varphi = H = \tilde{G}\tilde{\varphi}$. By Lemma 5.4, we may assume, possibly after modifying $\tilde{\varphi}$ with an automorphism induced by an automorphism of H, that α is unipotent.

The kernel of the natural map $kE \longrightarrow kH/\mathrm{I}(kH)^{n+1}$ is $\mathrm{I}(kE)^{n+1} + \mathrm{I}(kV)kE$, and by Lemma 5.3, we have $V = \mathrm{M}_{n+1}(E)$ and $\mathrm{I}(kV)kE \subseteq \mathrm{I}(kE)^{n+1}$. Thus we have an exact sequence $0 \longrightarrow \mathrm{I}(kE)^{n+1} \longrightarrow kE \longrightarrow kH/\mathrm{I}(kH)^{n+1} \longrightarrow 0$ from which we obtain the exact sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{I}(kE)^{n+1}/\mathrm{I}(kE)^{n+2} & \longrightarrow & kE/\mathrm{I}(kE)^{n+2} & \xrightarrow{\tau} & kH/\mathrm{I}(kH)^{n+1} & \longrightarrow & 0 \\ & & \| & & \| & & \| & & \\ 0 & \longrightarrow & J & \longrightarrow & A & \xrightarrow{\tau} & A/J & \longrightarrow & 0 \end{array}$$

Let $\sigma\colon kF/\mathrm{I}(kF)^{n+2} \longrightarrow kE/\mathrm{I}(kE)^{n+2}$ be the map induced by the natural map $kF \longrightarrow kE = kF/L$, and note that the kernel of σ is $\mathrm{I}(kL)kF + \mathrm{I}(kF)^{n+2}/\mathrm{I}(kF)^{n+2}$. As σ is surjective on units, the universal property of F provides us with a commutative diagram

$$\begin{array}{ccccc} kF/\mathrm{I}(kF)^{n+2} & \xrightarrow{\sigma} & kE/\mathrm{I}(kE)^{n+2} & \xrightarrow{\tau} & kH/\mathrm{I}(kH)^{n+1} \\ \uparrow{\scriptstyle\beta} & & & & \uparrow{\scriptstyle\alpha} \\ kF/\mathrm{I}(kF)^{n+2} & \xrightarrow{\sigma} & kE/\mathrm{I}(kE)^{n+2} & \xrightarrow{\tau} & kH/\mathrm{I}(kH)^{n+1} \end{array}$$

where β is unipotent by (5.2). Let $\pi\colon kF \longrightarrow kF/\mathrm{I}(kF)^{n+2}$ be the natural map. By commutativity, $R\pi\beta\sigma$ maps to 1 under τ, so $R\pi\beta\sigma$ is contained in $1+\mathrm{I}(kE)^{n+1}/\mathrm{I}(kE)^{n+2}$, an elementary abelian central p-group in the units of $kE/\mathrm{I}(kE)^{n+2}$. As $L=[F,R]R^p$, it follows that $L\pi\beta\sigma=1$, which means that β stabilizes the kernel of σ. Hence there is an induced commutative diagram

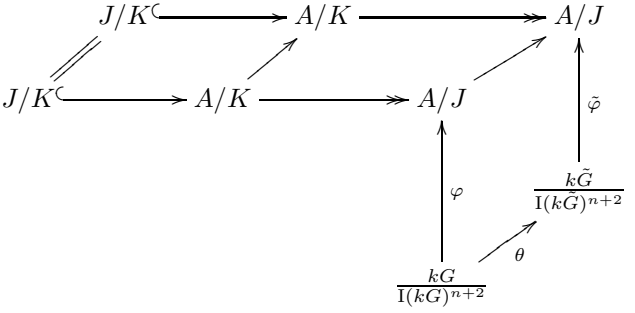
$$\begin{array}{ccccccccc} 0 & \longrightarrow & J & \longrightarrow & A & \longrightarrow & A/J & \longrightarrow & 0 \\ & & \| & & \uparrow{\scriptstyle\hat{\alpha}} & & \uparrow{\scriptstyle\alpha} & & \\ 0 & \longrightarrow & J & \longrightarrow & A & \longrightarrow & A/J & \longrightarrow & 0 \end{array}$$

($\hat{\alpha}$ induces the identity on $J=\mathrm{I}(kE)^{n+1}/\mathrm{I}(kE)^{n+2}$ since $\hat{\alpha}$ is unipotent, too).

Choose a subspace K of J which is a complement to the image of $\mathrm{I}(k\mathrm{M}_{n+1}(E))$ in J. Then K is an ideal of A, and the image of E in A/K is $\bar{E}=E/\mathrm{M}_{n+2}(E)$. Moreover, $J/K\cong\{\mathrm{M}_{n+1}(E)/\mathrm{M}_{n+2}(E)-1\}=\{\bar{V}-1\}$ by Lemma 5.3, so that

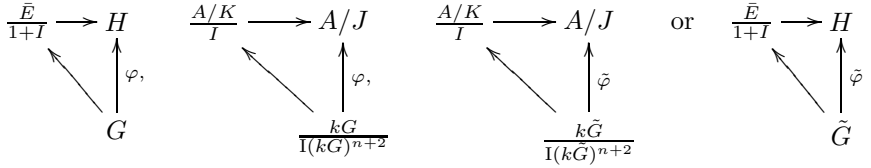
$$\begin{array}{ccccccccc} 1 & \longrightarrow & 1+J/K & \longrightarrow & \tau^{-1}(H)/K & \longrightarrow & H & \longrightarrow & 1 \\ & & \| & & \| & & \| & & \\ 1 & \longrightarrow & \bar{V} & \longrightarrow & \bar{E} & \longrightarrow & H & \longrightarrow & 1 \end{array}$$

Altogether, we obtain a commutative diagram of the form

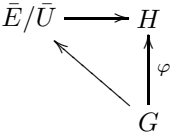


The ideals of A/K contained in J/K are in one-to-one correspondence with the subgroups of $\bar{E}$ contained in $\bar{V}$, with an ideal I corresponding to the subgroup $1+I$. Let I be an ideal of A/K contained in J/K. The commutative diagram above shows that the existence of *one* commutative diagram of the

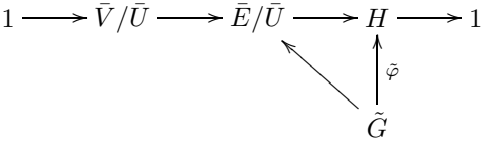
form



implies the existence of all of them. By assumption, $G \cong \bar{E}/\bar{U}$, and there is a commutative diagram



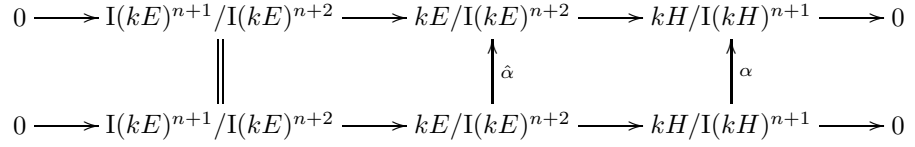
As we have seen, this implies the existence of a commutative diagram



Since $\bar{V}/\bar{U} \leq \Phi(\bar{E}/\bar{U})$, and $\tilde{\varphi}$ is surjective, the diagonal map is surjective, too, and as $|G| = |\tilde{G}|$, it follows that $G \cong \bar{E}/\bar{U} \cong \tilde{G}$, and the theorem is proved. ∎

COROLLARY 5.9: *Let* $\mathrm{M}_{n+2}(F) \leq U \leq \mathrm{M}_{n+1}(F)$ *for some* $n \geq 1$, *and set* $G = F/U$. *Then* $\mathrm{Aut}(kG) = \mathrm{Aut}(G) \cdot \mathrm{UAut}(kG)$.

Proof: We have $G^{[n]} = F^{[n]} = H$ and $\mathrm{M}_{n+2}(G) = 1$. Suppose that α is a unipotent automorphism of $kH/\mathrm{I}(kH)^{n+1}$. As in the proof of Theorem 5.8, we then obtain a unipotent lift $\hat{\alpha}$, as shown below.



Note that $G = F/U = (F/L)/(U/L) = E/(U/L)$. The kernel of the natural map $kE \longrightarrow kG/\mathrm{I}(kG)^{n+2}$ is $\mathrm{I}(kE)^{n+2} + \mathrm{I}(kU/L)kE$, and as $U \leq \mathrm{M}_{n+1}(F)$, the kernel of the natural map $kE/\mathrm{I}(kE)^{n+2} \longrightarrow kG/\mathrm{I}(kG)^{n+2}$ is contained in

$\mathrm{I}(kE)^{n+1}/\mathrm{I}(kE)^{n+2}$. It follows that α can be lifted to a unipotent automorphism of $kG/\mathrm{I}(kG)^{n+2}$.

Now let $\theta \in \mathrm{Aut}(kG)$, and denote the induced automorphism of $kG/\mathrm{I}(kG)^{n+2}$ also by θ. By Lemma 5.7, we have a commutative diagram

$$\begin{array}{ccc} kH/\mathrm{I}(kH)^{n+1} & \xrightarrow{\alpha} & kH/\mathrm{I}(kH)^{n+1} \\ \uparrow & & \uparrow \\ kG/\mathrm{I}(kG)^{n+2} & \xrightarrow{\theta} & kG/\mathrm{I}(kG)^{n+2} \end{array}$$

where α is an isomorphism, and the vertical maps are the natural ones. By Lemma 5.4, α is the product of a unipotent automorphism and a group automorphism of H. We have just seen that the unipotent automorphism can be lifted to a unipotent automorphism of $kG/\mathrm{I}(kG)^{n+2}$, and therefore the group automorphism of H can be lifted to a group automorphism σ of G, by Lemma 5.7. It follows that $\theta\sigma^{-1}$ is a unipotent automorphism of kG, and the proof is complete. ∎

6. First examples

Throughout this section we stick to the notation introduced in Section 4. Moreover, the reader should be aware of the notion of unipotent automorphisms (cf. Definition 5.1).

Still, p denotes a (fixed) prime number and k the field with p elements.

Example 6.1 (Cyclic groups)*:* It is certainly instructive to start by considering cyclic groups, so let $H = C_{p^n} = \langle x_n \rangle$ be a cyclic group of order p^n for some $n \in \mathbb{N}$. The obvious presentation with $F = \langle x \rangle$, $R = \langle x^{p^n} \rangle$ and surjection $F \longrightarrow H$ defined by $x \mapsto x_n$ gives rise to the following 'universal' central Frattini extension where $L = R^p = \langle x^{p^{n+1}} \rangle$, $E = F/L = \langle x_{n+1} \rangle$, $V = R/L = \langle x_{n+1}^{p^n} \rangle$ and π is defined by $x_{n+1} \mapsto x_n$:

$$\begin{array}{lccccccccc} \mathbb{E}: & 1 & \longrightarrow & V & \hookrightarrow & E & \xrightarrow{\pi} & H & \longrightarrow & 1 \\ & & & \uparrow{\scriptstyle \cong} & & \| & & \| & & \\ & 1 & \longrightarrow & C_p & \hookrightarrow & C_{p^{n+1}} & \longrightarrow & C_{p^n} & \longrightarrow & 1 \end{array}$$

The substitution $X \mapsto x_n - 1$ induces a k-algebra isomorphism between kH and the truncated polynomial ring $k[\bar{X}] = k[X]/(X^{p^n})$, which identifies the radical $\mathrm{I}(kH)$ with the ideal generated by $\bar{X} = \bar{X}_n = X + (X^{p^n})$. Therewith,

the ideal $\mathrm{I}(kV) = \langle x_{n+1}^{p^n} - 1\rangle = \langle (x_{n+1}-1)^{p^n}\rangle$ within kE is identified with $(\bar{X}_{n+1}^{p^n})$ and the small group ring is nothing but a truncated polynomial ring again,

$$s(E,V) = \frac{kE}{\mathrm{I}(kV)\mathrm{I}(kE)} \cong \frac{k[X]}{(X^{p^n+1})}.$$

Note that $\{V-1\}$ corresponds to the ideal $(\bar{X}^{p^n})$.

Any automorphism of the group algebra $k[\bar{X}_n]$ is induced from a substitution $\bar{X}_n \mapsto \lambda\bar{X}_n + \mathfrak{r}$ with $\lambda \in k^\times$ and $\mathfrak{r} \in (\bar{X}_n^2)$. The unipotent automorphisms are precisely the maps arising from substitutions with $\lambda = 1$, whereas the maps arising from substitutions with $\mathfrak{r} = 0$ constitute a subgroup $\mathcal{S}$ isomorphic to $k^\times$ which complements the group $\mathrm{UAut}(k[\bar{X}_n])$ of unipotent automorphisms. Thus, $\mathrm{Aut}(k[\bar{X}_n]) \cong \mathrm{UAut}(k[\bar{X}_n]) \rtimes k^\times$. Any automorphism of H can be described by $x_n \mapsto x_n^\beta$ for some $\beta \in \mathbb{N}$ relatively prime to p, and gives rise to the substitution

$$\bar{X}_n = (\bar{X}_n+1) - 1 \longmapsto (\bar{X}_n+1)^\beta - 1 = \sum_{i=1}^{\beta} \binom{\beta}{i} \bar{X}_n^i \in \beta\bar{X}_n + (\bar{X}_n^2)$$

which can always be compensated by a map from $\mathcal{S}$ to obtain a unipotent automorphism. Thus, we see directly that $\mathrm{Aut}(kH) = \mathrm{Aut}(H) \cdot \mathrm{UAut}(kH)$.

Unipotent automorphisms of $s(E,V)$, arising from substitutions $X \mapsto X + \mathfrak{r}$ with $\mathfrak{r} \in (X^2)$, induce the identity on $\{V-1\}$:

$$X^{p^n} \longmapsto (X+\mathfrak{r})^{p^n} = X^{p^n} + \mathfrak{r}^{p^n} \in X^{p^n} + (X^{p^n+1}).$$

On the other hand, decomposing any group automorphism along $\mathcal{S}\cdot\mathrm{UAut}(k[\bar{X}])$ shows that $\mathrm{Aut}(H)$ acts just as $k^\times$ on $\{V-1\}$:

$$X^{p^n} \longmapsto (\lambda X)^{p^n} = \lambda^{p^n} X^{p^n} = \lambda \cdot X^{p^n} \quad \text{for } \lambda \in k^\times.$$

Note that $\mathrm{Out}(kH) = \mathrm{Aut}(kH)$ and $\mathrm{Out}(H) = \mathrm{Aut}(H)$ since H is abelian. Thus the actions of $\mathrm{Out}(kH)$ and $\mathrm{Out}(H)$ coincide, and correspond to multiplication with field elements from $k^\times$ on the 1-dimensional space $\{V-1\}$. This observation (with $n=1$) will be useful in the following example when considering diagonal matrices.

Example 6.2 (Elementary abelian groups)*:* Let $H \cong C_p^r$ be an elementary abelian p-group of rank $r \geq 2$ (the case $r = 1$ is included in Example 6.1). We choose the obvious presentation for H with free group $F = \langle x_1, \ldots, x_r\rangle$ and relations

$$R = \langle x_i^p, [x_i, x_j] \mid 1 \leq i, j \leq r, i < j\rangle.$$

The 'universal' central Frattini extension with quotient group H is given by $E = F/L$ where $L = [F,R]R^p$. We set $\bar{x}_i := x_iR \in H$ and $\hat{x}_i := x_iL \in E$. Observe that the rank of V is precisely $r + \binom{r}{2}$, with a minimal set of generators given by $\{\hat{x}_i^p, [\hat{x}_i, \hat{x}_j] |\ 1 \le i,j \le r, i < j\}$.

If we want to parametrize the isomorphism and s-equivalence classes of extensions in $\mathbb{F}(H)$ then, by Theorem 4.4, we have to understand the action of $\mathrm{Out}(kH)$ on V. Note that $R = [F,F]F^p = \mathrm{M}_2(F)$, so $H = F^{[1]}$ in the notation from Section 5, and we have a factorization $\mathrm{Aut}(kH) = \mathrm{Aut}(H) \cdot \mathrm{UAut}(kH)$, by Lemma 5.4.

First we are going to show that the group of unipotent automorphisms $\mathrm{UAut}(kH)$ acts trivially on V. Therefore, the actions of $\mathrm{Out}(kH)$ and $\mathrm{Out}(H)$ on V coincide, implying that isomorphism classes in $\mathbb{F}(H)$ are in fact s-equivalence classes. Note that only for the prime $p = 2$ we have $L = \mathrm{M}_3(F)$ and, thus, $\mathrm{M}_3(E) = 1$, so we cannot deduce from Corollary 5.5 the trivial action of unipotent automorphisms.

The key equation implying the trivial action of unipotent automorphisms is the following:

$$\begin{aligned} \hat{x}_i(\hat{x}_j - 1) - (\hat{x}_j - 1)\hat{x}_i &= (\hat{x}_i - 1)(\hat{x}_j - 1) - (\hat{x}_j - 1)(\hat{x}_i - 1) \\ &= \hat{x}_i\hat{x}_j - \hat{x}_j\hat{x}_i \\ &= -\hat{x}_i\hat{x}_j([\hat{x}_j, \hat{x}_i] - 1) \in \mathrm{I}(kV)kE. \end{aligned} \tag{6.1}$$

Therefore, we have modulo $\mathrm{I}(kV)\mathrm{I}(kE)$ that

$$\begin{aligned} \hat{x}_i(\hat{x}_l - 1)\cdots(\hat{x}_m - 1) &\equiv (\hat{x}_l - 1)\hat{x}_i\cdots(\hat{x}_m - 1) \\ &\equiv \cdots \equiv (\hat{x}_l - 1)\cdots(\hat{x}_m - 1)\hat{x}_i, \end{aligned} \tag{6.2}$$

showing that the image of $\hat{x}_i$ in the small group ring $s(E,V)$ commutes with all monomials of degree ≥ 2 in the images of the $\hat{x}_j - 1$ (which generate the square of the radical). This immediately implies that modulo $\mathrm{I}(kV)\mathrm{I}(kE)$, we have

$$((\hat{x}_i - 1)(\hat{x}_j - 1))^p \equiv (\hat{x}_i - 1)^p(\hat{x}_j - 1)^p = (\hat{x}_i^p - 1)(\hat{x}_j - 1)^p \equiv 0. \tag{6.3}$$

By slight abuse of notation, we denote the image of $\hat{x}_i$ in $s(E,V)$ again by $\hat{x}_i$. Let $\alpha \in \mathrm{UAut}(kH)$, and consider a lift $\hat{\alpha} \in \mathrm{Aut}(s(E,V))$, which can be described by

$$\hat{x}_i\hat{\alpha} = \hat{x}_i + \mathfrak{r}_i,$$

where $\mathfrak{r}_i \in \mathrm{I}(kE)^2/\mathrm{I}(kV)\mathrm{I}(kE)$. Combining Equations (6.2) and (6.3) we obtain

$$\hat{x}_i^p\hat{\alpha} = (\hat{x}_i + \mathfrak{r}_i)^p = \hat{x}_i^p + \mathfrak{r}_i^p = \hat{x}_i^p.$$

Using again the commutation relation (6.2), we can check directly that $\hat{\alpha}$ fixes the element $(\hat{x}_i - 1)(\hat{x}_j - 1) - (\hat{x}_j - 1)(\hat{x}_i - 1)$. Since by (6.1), the additive commutator $(\hat{x}_i - 1)(\hat{x}_j - 1) - (\hat{x}_j - 1)(\hat{x}_i - 1)$ and $[\hat{x}_i, \hat{x}_j] - 1$ represent the same element in $s(E, V)$, we see that $\hat{\alpha}$ fixes the elements of a minimal generating set of V. Thus α acts trivially, as we wished to show.

Note that $\mathrm{Out}(H) = \mathrm{Aut}(H) \cong \mathrm{GL}_r(k)$: A matrix $A = (a_{ij})_{i,j=1}^r \in \mathrm{GL}_r(k)$ corresponds to the automorphism α_A of H given by $\bar{x}_i \mapsto \prod_{j=1}^r \bar{x}_j^{a_{ij}}$. The obvious lift $x_i \mapsto \prod_{j=1}^r x_j^{a_{ij}}$ of α_A to F induces a lift $\hat{\alpha}_A \in \mathrm{Aut}(E)$ leaving V invariant, thus giving rise to the $\mathrm{GL}_r(k)$-action under consideration. Next, we determine the action of $\mathrm{Aut}(H)$ on V, i.e., the structure of V as $\mathrm{GL}_r(k)$-module. Let $W = k^r$ be the natural $\mathrm{GL}_r(k)$-module with canonical basis $\{w_i |\ 1 \le i \le r\}$.

First, we note that the subgroup T of V generated by the commutators $[\hat{x}_i, \hat{x}_j]$ for $i < j$ is a $\mathrm{GL}_r(k)$-submodule. Since the group $\mathrm{GL}_r(k)$ is generated by elementary and diagonal matrices, it is enough to consider $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(k)$. Using basic commutator relations (see [11, Chapter III, (1.2)]), and the definition of L, we obtain

$$\begin{aligned}
[\hat{x}_i, \hat{x}_j]\hat{\alpha}_A &= [\hat{x}_i^a \hat{x}_j^b, \hat{x}_i^c \hat{x}_j^d] = [\hat{x}_i^a \hat{x}_j^b, \hat{x}_j^d] \cdot [\hat{x}_i^a \hat{x}_j^b, \hat{x}_i^c] \\
&= [\hat{x}_i^a, \hat{x}_j^d] \cdot [\hat{x}_j^b, \hat{x}_i^c] = [\hat{x}_i, \hat{x}_j]^{ad} \cdot [\hat{x}_j, \hat{x}_i]^{bc} \\
&= [\hat{x}_i, \hat{x}_j]^{ad-bc} = [\hat{x}_i, \hat{x}_j]^{\det(A)}.
\end{aligned}$$

This shows, in addition, that $w_i \wedge w_j \mapsto [\hat{x}_i, \hat{x}_j]$ $(i < j)$ defines a $\mathrm{GL}_r(k)$-isomorphism between $\bigwedge^2 W$ and T. Observing that E is a nilpotent group of class 2 and making use of [11, Chapter III, (1.3)], we obtain the action of the matrix A on the missing generators $\hat{x}_i^p$ $(1 \le i \le r)$ of V:

$$\begin{aligned}
\hat{x}_i^p \hat{\alpha}_A &= (\hat{x}_i^a \hat{x}_j^b)^p \\
&= (\hat{x}_i^a)^p (\hat{x}_j^b)^p [\hat{x}_j^b, \hat{x}_i^a]^{\binom{p}{2}} \\
&= \begin{cases} (\hat{x}_i^p)^a (\hat{x}_j^p)^b & \text{for } p \text{ odd}, \\ (\hat{x}_i^p)^a (\hat{x}_j^p)^b \cdot [\hat{x}_i, \hat{x}_j]^{ab} & \text{for } p = 2. \end{cases}
\end{aligned}$$

Thus, in any case, V/T is isomorphic to W as $\mathrm{GL}_r(k)$-module, an isomorphism being given by $w_i \mapsto \hat{x}_i^p T$. So we have a short exact sequence of $\mathrm{GL}_r(k)$-modules

$$\mathbb{E}_r \colon 0 \longrightarrow \bigwedge^2 W \longrightarrow V \longrightarrow W \longrightarrow 0,$$

the sequence being split for odd primes p.

Let $p = 2$, and write more clearly $V_r = V$. The sequence $\mathbb{E}_2$ turns out to be split by sort of an accident: generators of $\mathrm{GL}_2(\mathbb{F}_2)$ (isomorphic to the symmetric

group on 3 letters) act on V_2 via the matrices $\left(\begin{smallmatrix}1&1&1\\0&1&0\\0&0&1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}0&1&0\\1&0&0\\0&0&1\end{smallmatrix}\right)$, which can be conjugated into block diagonal form by $\left(\begin{smallmatrix}1&0&1\\0&1&1\\0&0&1\end{smallmatrix}\right)$. But $\mathbb{E}_r$ for $r \geq 3$ is a non-split extension of $\mathrm{GL}_r(k)$-modules: For $r = 3$, this can be shown by direct inspection, and for $r > 3$, this can be deduced inductively, just noting that the restriction of the $\mathrm{GL}_r(k)$-module V_r to $\mathrm{GL}_{r-1}(k) = \mathrm{Stab}_{\mathrm{GL}_r(k)}(w_r)$ splits according to (in suggestive notation)

$$V_r|_{\mathrm{GL}_{r-1}(k)} = V_{r-1} \oplus (V_{r-1} \wedge w_r) \oplus kw_r.$$

Therefore, a splitting of $\mathbb{E}_r$ would induce a splitting of $\mathbb{E}_{r-1}$, which is impossible by the induction hypothesis.

Summarizing, we have reduced the parametrization of s-equivalence (=isomorphism) classes of central Frattini extensions with elementary abelian factor p-group of rank r and middle group of order $p^{2r+\binom{r}{2}-d}$ to the combinatorial determination of $\mathrm{GL}_r(k)$-orbits of d-dimensional subspaces of the $(r + \binom{r}{2})$-dimensional $\mathrm{GL}_r(k)$-module V_r from the sequence $\mathbb{E}_r$.

Example 6.3 (Non-isomorphic groups with isomorphic small group rings)*:* In the last example we consider a case where the action of $\mathrm{Out}(kH)$ on V is strictly larger than the action of $\mathrm{Out}(H)$. Let $H = D_8$ be the dihedral group of order 8 as given by the Coxeter presentation, i.e.,

$$H \cong F/R = \langle a, b \mid a^2, b^2, (ab)^4 \rangle.$$

Thus, $\bar{a} = aR$ and $\bar{b} = bR$ can be interpreted as (simple) reflections in Euclidean space $\mathbb{R}^2$ generating the group of symmetries of a square.

We will omit most of the calculations, which anyway can easily be reproduced — if not by hand, then at least with the aid of a computing system like GAP (cf. [7]). For convenience, we shall use the numbering of isomorphism classes of groups of small order as established in the *Small Groups library* embedded in GAP.

Let $L = [F, R]R^2$ and set $E = F/L$ and $V = R/L$. The three relators from R give rise to a minimal generating set for V, i.e., setting $\hat{a} = aL$ and $\hat{b} = bL$, we can identify the canonical basis of $\mathbb{F}_2^3$ with the (ordered) set $\{\hat{a}^2, \hat{b}^2, (\hat{a}\hat{b})^4\} \subset V \cong C_2^3$. We shall make explicit use of this identification when representing group actions on V by matrices in $\mathrm{GL}_3(\mathbb{F}_2)$.

We want to parametrize the isomorphism and s-equivalence classes of extensions in $\mathbb{F}(H)$. By Theorem 4.4, this amounts to computing the homomorphism $\mathrm{Out}(\mathbb{F}_2 H) \longrightarrow \mathrm{GL}(V)$ and its restriction to $\mathrm{Out}(H)$ (as outlined in the proof

of Theorem 4.4) and studying the induced action on the set of subspaces of V. Note that $\mathrm{M}_3(H) = 1$, i.e., H has M-length ≤ 2. Finite p-groups G with M-length ≤ 2 have a normal complement in the normalized unit group of kG (see [14, Corollary 7]), a fact that readily implies that group ring automorphisms of kG can be written as the product of a group automorphism and a unipotent automorphism. Thus $\mathrm{Aut}(\mathbb{F}_2 H) = \mathrm{Aut}(H) \cdot \mathrm{UAut}(\mathbb{F}_2 H)$, and we compute both factors separately.

The symmetry of the Coxeter presentation shows that switching the two generators $\bar{a}$ and $\bar{b}$ induces an automorphism σ of H. In fact, this automorphism provides a generator of $\mathrm{Out}(H)$, which is a cyclic group of order two. To describe its action on V, we lift σ to the automorphism of F which switches the free generators a and b. Then, σ induces a lifting automorphism $\hat{\sigma}$ of E which acts on V by $\hat{a}^2\hat{\sigma} = \hat{b}^2$, $\hat{b}^2\hat{\sigma} = \hat{a}^2$ and

$$\begin{aligned}(\hat{a}\hat{b})^4\hat{\sigma} = (\hat{b}\hat{a})^4 &= \hat{a}^3 \cdot \hat{a} \cdot (\hat{b}\hat{a})^4 = \hat{a}^3(\hat{a}\hat{b})^4\hat{a} \\ &= \hat{a}^3 \cdot \hat{a} \cdot (\hat{a}\hat{b})^4 \cdot [(\hat{a}\hat{b})^4, \hat{a}] = \hat{a}^4 \cdot (\hat{a}\hat{b})^4 \\ &= (\hat{a}\hat{b})^4.\end{aligned}$$

Thus, the action of a generator of $\mathrm{Out}(H)$ on V is determined by the permutation matrix $X = \left(\begin{smallmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)$.

We set $\bar{A} = \bar{a} - 1$ and $\bar{B} = \bar{b} - 1$. These elements generate the radical $\mathrm{I}(\mathbb{F}_2 H)$ of the group ring $\mathbb{F}_2 H$. The elements of the group $\mathrm{UAut}(\mathbb{F}_2 H)$ can be compactly described by

$$\bar{a} \mapsto \bar{a} + s_a + t_a, \quad \bar{b} \mapsto \bar{b} + s_b + t_b,$$

where $s_a, s_b \in \{0, \bar{A}\bar{B} + \bar{B}\bar{A}\}$, and t_a and t_b are arbitrary elements of $\mathrm{I}(\mathbb{F}_2 G)^3$. This gives a total of 2^8 unipotent automorphisms. The automorphisms τ and υ determined by letting

$$\begin{aligned}\tau&\colon s_a = \bar{A}\bar{B} + \bar{B}\bar{A}, s_b = t_a = t_b = 0, \\ \upsilon&\colon s_b = \bar{A}\bar{B} + \bar{B}\bar{A}, s_a = t_a = t_b = 0,\end{aligned}$$

act on V — via liftings to automorphisms of $\mathrm{Aut}(s(E, V))$ — by multiplication with the matrices $Y = \left(\begin{smallmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)$ and $Z = \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{smallmatrix}\right)$, respectively. The action of $\langle Y, Z\rangle$ already gives the full action of $\mathrm{UAut}(\mathbb{F}_2 H)$ on V. Thus, the action of $\mathrm{Out}(\mathbb{F}_2 H)$ on V is determined by the matrix group

$$\langle X, Y, Z\rangle = \langle Y, Z\rangle \rtimes \langle X\rangle \cong (C_2 \times C_2) \rtimes C_2 \cong D_8,$$

with $\mathrm{Out}(H)$ corresponding to the subgroup $\langle X\rangle$.

The 2-dimensional subspaces of $\mathbb{F}_2^3$ can be parametrized by all 2×3 matrices over $\mathbb{F}_2$ in reduced row-echelon form (cf. [12, p. 14]). There are seven of these:

$$M_1 = \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{smallmatrix}\right), M_{2\mathrm{a}} = \left(\begin{smallmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{smallmatrix}\right), M_{2\mathrm{b}} = \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \end{smallmatrix}\right), M_3 = \left(\begin{smallmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{smallmatrix}\right),$$
$$M_{4\mathrm{a}} = \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right), M_5 = \left(\begin{smallmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right), M_{4\mathrm{b}} = \left(\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right).$$

To each of these matrices M_i one associates an elementary abelian subgroup U_i of V of rank 2: For example, $U_{2\mathrm{b}} = \langle \hat{a}^2, \hat{b}^2 \cdot (\hat{a}\hat{b})^4 \rangle$. The action of $\mathrm{Out}(H)$ on the 2-dimensional subspaces can be computed by calculating the reduced row-echelon form of $M_i \cdot X$. It turns out that there are five orbits,

$$O_1 = \{M_1\}, \quad O_2 = \{M_{2\mathrm{a}}, M_{2\mathrm{b}}\}, \quad O_3 = \{M_3\},$$
$$O_4 = \{M_{4\mathrm{a}}, M_{4\mathrm{b}}\} \quad \text{and} \quad O_5 = \{M_5\},$$

which correspond to the isomorphism classes of central Frattini extensions in $\mathbb{F}(H)$ with middle group of order 16, with representatives given by

$$\mathbb{E}_i \colon 1 \longrightarrow V/U_i \longrightarrow E/U_i \longrightarrow H \longrightarrow 1.$$

Set $E_i = E/U_i$. The groups $E_1, \ldots, E_5$ are pairwise non-isomorphic, with E_1 of dihedral, E_2 of semi-dihedral and E_3 of quaternion type. But the sequences $\mathbb{E}_1, \mathbb{E}_2$ and $\mathbb{E}_3$ are s-equivalent, and therefore their small group rings $s(E/U_i, V/U_i)$ are isomorphic, as one easily sees from the action of Y: we have $M_1 \overset{Y}{\longleftrightarrow} M_{2\mathrm{a}}$ and $M_{2\mathrm{b}} \overset{Y}{\longleftrightarrow} M_3$. (It should be remarked that the series of dihedral, semi-dihedral and generalized quaternion groups are nevertheless determined by their modular group rings (cf. [4, §2]).) It turns out that the $\mathrm{Out}(H)$-orbits O_4 and O_5 are already $\mathrm{Out}(\mathbb{F}_2 H)$-orbits.

The same kind of reasoning applied to vectors from $\mathbb{F}_2^3 \setminus \{0\}$ yields the isomorphism and s-equivalence classes in $\mathbb{F}(H)$ with middle group of order 32. There are again 5 isomorphism classes of such extensions (due to the fact that $X = X^{-\mathrm{t}}$), with representing vectors

$$v_9 = (1\ 0\ 0), v_{10} = (1\ 0\ 1), v_2 = (0\ 0\ 1), v_{14} = (1\ 1\ 0), v_{13} = (1\ 1\ 1).$$

Here, the index $i \in \{2, 9, 10, 13, 14\}$ corresponds to the number of the isomorphism class of the middle group G_i provided by the *Small Groups library* in GAP (cf. [7]). For example, we have an extension

$$\mathbb{G}_9 \colon 1 \longrightarrow V/\langle \hat{a}^2 \rangle \longrightarrow E/\langle \hat{a}^2 \rangle \longrightarrow H \longrightarrow 1$$

with middle group $G_9 = E/\langle \hat{a}^2 \rangle$. Again, all middle groups of the sequences $\mathbb{G}_i$ are pairwise non-isomorphic. None of these is of dihedral, semi-dihedral or

quaternion type. This time the classes of $\mathbb{G}_9$ and $\mathbb{G}_{10}$ as well as the classes of $\mathbb{G}_{13}$ and $\mathbb{G}_{14}$ are merged into one s-equivalence class, giving rise to two pairs of non-isomorphic central Frattini extensions with isomorphic corresponding small group ring sequences.

References

[1] J. L. Alperin, *Local Representation Theory,* Cambridge Studies in Advanced Mathematics, Vol. 11, Cambridge University Press, Cambridge, 1986, Modular representations as an introduction to the local representation theory of finite groups.

[2] I. C. Borge and O. A. Laudal, *The modular isomorphism problem,* University of Oslo, Department of Mathematics, Preprint series in Pure Mathematics 2002, no. 19, ISBN 82-553-1357-5, (`http://www.math.uio.no/eprint/`).

[3] I. C. Borge and O. A. Laudal, *The modular isomorphism problem,* University of Oslo, Department of Mathematics, Preprint series in Pure Mathematics 2003, no. 25, ISBN 82-553-1393-1, (`http://www.math.uio.no/eprint/`).

[4] J. F. Carlson, *Periodic modules over modular group algebras,* Journal of the London Mathematical Society (2) **15** (1977), 431–436.

[5] D. B. Coleman, *On the modular group ring of a p-group,* Proceedings of the American Mathematical Society **15** (1964), 511–514.

[6] C. W. Curtis and I. Reiner, *Methods of Representation Theory. Vol. I,* Wiley Classics Library, John Wiley & Sons Inc., New York, 1990, With applications to finite groups and orders, Reprint of the 1981 original, A Wiley-Interscience Publication.

[7] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.3, package SmallGroups,* 2002, (`http://www.gap-system.org`).

[8] M. Hertweck and M. Soriano, *Central p-group extensions: Laudal obstruction spaces revisited,* submitted, 2005.

[9] E. T. Hill, *The annihilator of radical powers in the modular group ring of a p-group,* Proceedings of the American Mathematical Society **25** (1970), 811–815.

[10] P. J. Hilton and U. Stammbach, *A Course in Homological Algebra,* Graduate Texts in Mathematics, Vol. 4, Springer-Verlag, New York, 1971.

[11] B. Huppert, *Endliche Gruppen. I,* Die Grundlehren der Mathematischen Wissenschaften, Band 134, Springer-Verlag, Berlin, 1967.

[12] G. D. James, *Representations of general linear groups,* London Mathematical Society Lecture Note Series, Vol. 94, Cambridge University Press, Cambridge, 1984.

[13] S. A. Jennings, *The structure of the group ring of a p-group over a modular field,* Transactions of the American Mathematical Society **50** (1941), 175–185.

[14] I. B. S. Passi and S. K. Sehgal, *Isomorphism of modular group algebras,* Mathematische Zeitschrift **129** (1972), 65–73.

[15] D. S. Passman, *The Algebraic Structure of Group Rings,* Pure and Applied Mathematics, Wiley-Interscience, New York, 1977.

[16] J. Ritter and S. Sehgal, *Isomorphism of group rings,* Archiv der Mathematik (Basel) **40** (1983), 32–39.

[17] D. J. S. Robinson, *A Course in the Theory of Groups,* second ed., Graduate Texts in Mathematics, Vol. 80, Springer-Verlag, New York, 1996.

[18] K. Roggenkamp and L. Scott, *Isomorphisms of p-adic group rings,* Annals of Mathematics (2) **126** (1987), 593–647.

[19] F. Röhl, *On the isomorphism problem for group rings and completed augmentation ideals,* Rocky Mountain Journal of Mathematics **17** (1987), 853–863.

[20] F. Röhl, *On automorphisms of complete algebras and the isomorphism problem for modular group rings,* Canadian Journal of Mathematics **42** (1990), 383–394.

[21] R. Sandling, *The isomorphism problem for group rings: a survey,* in *Orders and their Applications (Oberwolfach, 1984)*, Lecture Notes in Mathematics, Vol. 1142, Springer, Berlin, 1985, pp. 256–288.

[22] H. N. Ward, *Some results on the group algebra of a group over a prime field,* Seminar in Group Theory, Harvard University, Cambridge, MA, 1960–61, Mimeographed Notes, pp. 13–19.

[23] A. Whitcomb, *The group ring problem,* Ph.D. thesis, University of Chicago, 1968.

[24] H. Zassenhaus, *Ein Verfahren, jeder endlichen p-Gruppe einen Lie-Ring mit der Charakteristik p zuzuordnen,* Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg **13** (1939), 200–207.