Automorphisms and Nonabelian Cohomology: An Algorithm

K. W. Roggenkamp*
Mathematisches Institut B
Universität Stuttgart
7000 Stuttgart, Germany

and

L. L. Scott†
Department of Mathematics
University of Virginia
Charlottesville, Virginia

Submitted by Gerhard O. Michler

ABSTRACT

We give an algorithm to compute the group of outer automorphisms of $\mathbb{Z}/p\mathbb{Z}$-group rings of p-groups; this can also be used to test whether two p-groups have isomorphic group rings over $\mathbb{Z}/p\mathbb{Z}$ (our original motivation). We work our way down the powers of the augmentation ideal, using homological methods. Careful attention is given to which calculations can be done with linear methods and which cannot, with computer implementation in mind.

1. THE IDEA OF THE ALGORITHM

Let us first explain the strategy: G and H are finite p-groups, and $\mathbb{F} = \mathbb{Z}/p\mathbb{Z}$ is the field with p elements. We would like to test whether

$$\mathbb{F}G \overset{\phi}{\simeq} \mathbb{F}H \qquad \text{as augmented algebras.}^{1}$$

*This research was partially supported by the NSF and the DFG.
†This research was partially supported by the NSF and the DFG.

655 Avenue of the Americas, New York, NY 10010 0024-3795/93/$6.00

This means that we would like to construct a group homomorphism

$$\varrho : G \to V(\mathbb{F}H),$$

where $V(\mathbb{F}H) = 1 + \mathrm{rad}(\mathbb{F}H)$ are the units of augmentation one in $\mathbb{F}H$, in such a way that

(1) ϱ is injective,
(2) $\mathrm{Im}(\varrho) \subset \mathbb{F}H$ consists of $\mathbb{F}$-linearly independent elements.

The second condition is not a serious problem (cf. Remark 3).

As for the construction of ϱ, we observe that a direct approach, by trying to find the generators and relations of G in $\mathbb{F}H$, is impossible even with the largest available computers, since $|V(\mathbb{F}H| = p^{p^n - 1}$ if $|H| = p^n$. Moreover, constructing homomorphisms is a highly nonlinear process, and hence is against the "nature" of computers. We thus try to linearize the problem by using the filtration $1 + \mathrm{rad}^i(\mathbb{F}H)$ of $V(\mathbb{F}H)$ and play nonabelian cohomology versus abelian cohomology.

The inductive procedure is as follows:

1. Assume that we have constructed a homomorphism

$$\varrho_i : G \to 1 + \mathrm{rad}(\mathbb{F}H)/\left[1 + \mathrm{rad}^i(\mathbb{F}H)\right].$$

2. Then we would like to know whether ϱ_i can be extended to a homomorphism

$$\hat{\varrho}_i : G \to 1 + \mathrm{rad}(\mathbb{F}H)/\left[1 + \mathrm{rad}^{i+1}(\mathbb{F}H)\right].$$

This question we have to answer for each of the above maps ρ_i.

3. Once we have answered the question of whether ϱ_i extends to $\hat{\varrho}_i$, we have to find all extensions

$$\hat{\varrho}_{ij} : G \to 1 + \mathrm{rad}(\mathbb{F}H)/\left[1 + \mathrm{rad}^{i+1}(\mathbb{F}H)\right]$$

of ϱ_i.

However, the situation is not quite as complicated as it looks, since the question of extendibility of a homomorphism ϱ_i depends only on the conjugacy class of ϱ_i under conjugation with elements in $V(\mathbb{F}H)$, and for a

[1] That is, the above isomorphism ϕ commutes with the augmentations of both $\mathbb{F}G$ and $\mathbb{F}H$.

fixed ϱ_i which extends, we only have to find representatives of the $V(\mathbb{F}H)$-conjugacy classes of the various extensions. To take this into account is a necessity because of limited storage space. This is now a situation where cohomology comes in quite handy; it enters because cohomology classifies "things up to conjugacy": Every homomorphism

$$\varrho_i : G \to 1 + \operatorname{rad}(\mathbb{F}H)/\left[1 + \operatorname{rad}^i(\mathbb{F}H)\right]$$

gives rise to a multiplicative 1-cocycle (cf. Section 2) $\mu_i(g) = \varrho_0(g) \cdot \rho_i(g^{-1})$, where

$$\varrho_0 : G \to 1 + \operatorname{rad}(\mathbb{F}H)/\left[1 + \operatorname{rad}^i(\mathbb{F}H)\right]$$

is a fixed homomorphism, and conversely. Moreover, modulo 1-coboundaries, we get exactly the homomorphisms ϱ_i up to conjugacy with elements in $V(\mathbb{F}H)$. Abelian - even central - cohomology enters in the question of whether or not ϱ_i extends to some $\hat{\varrho}_i$. The obstruction is an element in $H^2(G, \operatorname{rad}^i(\mathbb{F}H)/\operatorname{rad}^{i+1}(\mathbb{F}H))$ (cf. Lemma 3). Computing this cohomology group is a linear problem if one uses relation modules. Once we know that ϱ_i extends, we want to find all extensions to $\hat{\varrho}_{ij}$ of ϱ_i up to conjugacy with elements in $V(\mathbb{F}H)$. It is easy to find the extensions up to conjugacy in the H-trivial group $1 + \operatorname{rad}^i(\mathbb{F}H)/[1 + \operatorname{rad}^{i+1}(\mathbb{F}H)]$; the orbits are then parametrized by $H^1(G, 1 + \operatorname{rad}^i(\mathbb{F}H)/[1 + \operatorname{rad}^{i+1}(\mathbb{F}H)])$. However, in order to classify the extensions up to conjugacy with elements in $V(\mathbb{F}H)$ - a highly nonlinear problem - we invoke Serre's exact sequence of nonabelian cohomology sets, and eventually will be able to even linearize this problem.

The induction is - because of the limited storage space - not quite as simple as explained above: The inductive step goes first from homomorphisms

$$\varrho : G \to 1 + \operatorname{rad}(\mathbb{F}H)/\left[1 + \operatorname{rad}^i(\mathbb{F}H)\right]$$

to homomorphisms

$$\hat{\varrho} : G \to 1 + \operatorname{rad}(\mathbb{F}H)/\left[1 + \operatorname{rad}^{2i}(\mathbb{F}H)\right],$$

which means that we have to compute second cohomology groups with nontrivial but still abelian coefficients—however, this is also a linear problem using relation modules. We then have the extensions $\hat{\varrho}$ classified up to conjugacy with elements in the abelian group $1 + \operatorname{rad}^i(\mathbb{F}H)/[1 + \operatorname{rad}^{2i}(\mathbb{F}H)]$. Now we can use Serre's exact sequence of nonabelian cohomology sets in order to get the homomorphisms $\varrho : G \to 1 + \operatorname{rad}(\mathbb{F}H)/[1 + \operatorname{rad}^{i+1}(\mathbb{F}H)]$ classified up to conjugation with elements in $V(\mathbb{F}H)$.

To make the paper available to a larger audience we have filled in most of the details on nonabelian cohomology and explained the connection between automorphisms and cohomology in detail.

We would like to point out that the algorithm developed here can also be used to

(1) compute $\mathrm{Out}(\mathbb{F}H)$,
(2) compute $\mathrm{Out}(G)$, where G is a p-group of pretty large order (cf. [5]).

M. Wursthorn in his Diplom thesis in Stuttgart has implemented the algorithms developed here in a modified form in his program package SISYPHOS[2] and used them to show all 2-groups of order 64 are determined by their $\mathbb{Z}/2 \cdot \mathbb{Z}$ group rings.

2. NONABELIAN COHOMOLOGY

The material in this section is well known, but we review it for the convenience of the reader and to set notation. Let G and W be groups, and assume that we have a group homomorphism $\varrho : G \to \mathrm{Aut}(W)$. That is, we have an action of G on W, which we shall also denote by ϱ, writing ${}^{\varrho(g)}w$ for its action on w, for $g \in G$ and $w \in W$. Sometimes we write ${}^{g}w$ if ϱ is to be understood from the context. If we are given a homomorphism $\varrho : G \to W$ or, more generally, $\varrho : G \to W/C$, where C is a central subgroup of W, then we also write ϱ for the induced homomorphism $G \to \mathrm{Aut}(W)$ given by the induced conjugation action.

DEFINITION 1.

(1) A *multiplicative* 1-*cocycle* of G with coefficients in W is a map $\mu : G \to W$ with $\mu(gh) = \mu(g) \cdot [{}^{g}\mu(h)]$, $g, h \in G$.

(2) A *multiplicative* 1-*coboundary* is a map of the form $\mu(g) = w \cdot {}^{g}(w^{-1})$ for some $w \in W$.

(3) Two cocycles ν and μ are said to be *equivalent* if there exists $w \in W$ such that $\nu(g) = w \cdot \mu(g) \cdot {}^{g}(w^{-1})$ for all $g \in G$.

[2] This program can be obtained upon request from the first author. Besides ordinary calculations in modular group rings, it allows calculations with ideals and Lie series and the computation of cohomology groups of low degree. The program is written in (ANSI) C, and it is implemented for Sun 3/60, IBM RS6000, HP 9000/7xx, ATARI TT, and PC 386/486 under OS/2. In this implemented version it also can be used to compute the group of outer automorphisms of finite p-groups. A detailed description of the program will be published by M. Wursthorn in [5].

The next result is straightforward.

LEMMA 1. *Every coboundary is a cocycle, and being equivalent is an equivalence relation.*

DEFINITION 2. By $H_{\varrho}^{1}(G, W)$ we denote the set of equivalence classes, viewed as pointed set, where the point consists of the class of coboundaries. [Sometimes we shall omit ϱ; note, however, that $H_{\varrho}^{1}(G, W)$ depends strongly on the action ϱ.]

It should be noted though that $H_{\varrho}^{1}(G, W)$ is in general not a group; it is a group if W is an abelian group. In this case the multiplication is given as $(\mu \cdot \nu)(g) = \mu(g) \cdot \nu(g)$, induced by the group multiplication. We shall need 2-cocycles only in case of W abelian; for nonabelian 2-cohomology we refer the interested reader to Serre's book [4]. So we assume now that W is an abelian group.

DEFINITION 3.

(1) A *multiplicative* 2*-cocycle* is a map $\mu : G \times G \to W$ satisfying

$$\mu(xy, z)^{-1} \cdot \mu(x, y)^{-1} \cdot {}^{x}(y, z) \cdot \mu(x, yz) = 1.$$

(2) A *multiplicative* 2*-coboundary* is a map of the form

$$\mu(x, y) = [f(x) \cdot {}^{x}f(y)]^{-1} \cdot f(xy)$$

for some function $f : G \to W$.

It turns out that a 2-coboundary is a 2-cocycle, and the 2-coboundaries form a subgroup inside the group of 2-cocycles, where the multiplication is induced from the multiplication in W, and the quotient is $H_{\varrho}^{2}(G, U)$, the 2-cohomology group. In this case two cocycles μ_1 and μ are equivalent if $\mu_1(g, h) = [f(g) \cdot {}^{g}f(h)]^{-1} \cdot \mu(g, h) \cdot f(gh)$. Assume that we are given an exact sequence

$$1 \to W' \xrightarrow{\alpha} W \xrightarrow{\beta} W'' \to 1$$

of groups (not necessarily abelian) on each of which G acts compatibly, say as ϱ', ϱ, and ϱ'' on W', W and W'' respectively, i.e. such that the maps α and

β are G-equivariant. By $H^0_\varrho(G, W)$ we denote the group of fixed points in W under the G-action via ϱ. Then we get a long exact sequence of pointed sets (cf. [4]) (a group is in a natural way a pointed set):

$$\begin{aligned} 1 &\to H^0_{\varrho'}(G, W') \overset{\alpha^0}{\to} H^0_\varrho(G, W) \overset{\beta^0}{\to} H^0_{\varrho''}(G, W'') \\ &\overset{\partial^0}{\to} H^1_{\varrho'}(G, W') \overset{\alpha^1}{\to} H^1_\varrho(G, W) \overset{\beta^1}{\to} H^1_{\varrho''}(G, W''). \end{aligned} \tag{1}$$

The maps α^i and β^i for $i = 0, 1$ are self-explanatory, so we just give the definition of the connecting map $H^0_{\varrho''}(G, W'') \overset{\partial^0}{\to} H^1_{\varrho'}(G, W')$. For a fixed point $w'' \in W''$ we pick a coset representative under β, say $w \in W$, and define the 1-cocycle $\partial^0(w'')$ by $g \to w \cdot {}^{\varrho(g)}(w^{-1})$.

Assume now that W' is central in W. Then we have a further map

$$H^1_{\varrho''}(G, W'') \overset{\partial^1}{\to} H^2_{\varrho'}(G, W'). \tag{2}$$

which is described as follows: For a 1-cocycle $\mu : G \to W''$ with respect to ϱ'', we choose a coset representative under β, say $\tilde{\mu}(g)$ in W, for each $\mu(g)$, $g \in G$. Then $\partial^1(\mu) : G \times G \to W'$, defined by $\tilde{\mu}(g \cdot h) = \partial^1(g, h) \cdot \tilde{\mu}(g) \cdot {}^{\varrho(g)}\tilde{\mu}(h)$, is a 2-cocycle.

For later applications we have to compute the image of

$$\alpha^1 : H^1_{\varrho'}(G, W') \to H^1_\varrho(G, W). \tag{3}$$

Note that α^1 is just a map of pointed sets. However, $H^0_{\varrho''}(G, W'')$ acts via ∂^0 on $H^1_{\varrho''}(G, W')$, and the orbits under this action are precisely the fibers of the above map α^1 into $H^1_\varrho(G, W)$. More precisely, the inverse image under β^0 of $H^0_{\varrho'}(G, W'')$ in W is the centralizer modulo W' in W of G, $C_W(G, W') = \{w \in W \mid w \cdot {}^{\varrho(g)}(w^{-1}) \in W'\}$. This centralizer acts on $H^1_{\varrho'}(G, W')$ - cf. the definition of ∂^0 - as follows:

$$\begin{aligned} {}^c\mu(g) &= c \cdot \mu(g) \cdot {}^{\varrho(g)}(c^{-1}), \qquad \mu \in H^1_{\rho'}(G, W'), \quad c \in C_G(W, W') \\ &= c \cdot {}^{\varrho(g)}(c^{-1}) \cdot \left[{}^{\varrho(g)}c \cdot \mu(g) \cdot {}^{\varrho(g)}(c^{-1})\right]. \end{aligned} \tag{4}$$

This formula also shows that ${}^c\mu$ has indeed values in W'. Also ${}^c\mu$ is a cocycle, and is equivalent to μ if c belongs to W'.

To ease our notational burden, we will henceforth sometimes use the same notation for a 1-cocycle class and its representing cocycle.

The image of α^1 is thus parametrized by the orbits under $C_W(G, W')$. For computational purposes, the orbits under conjugation action are difficult to handle. Therefore we shall only apply the formula in Equation (4) in a situation where the orbits are "linear." We summarize this as

LEMMA 2. *Assume that W' is abelian and that W acts trivially on W'. Then the set of orbits of $H^1_{\varrho'}(G, W')$ under $C_W(G, W')$, i.e. the image of α^1, is given by the "linear cosets"*

$$\left\{ {}^{c}\mu \,\middle|\, c \in C_W(G, W'),\ \mu \in H^1_{\varrho'}(G, W') \textit{ with } {}^{c}\mu(g) = c \cdot {}^{\varrho(g)}(c^{-1}) \cdot \mu(g) \right\}.$$

3. HOMOMORPHISMS AND COHOMOLOGY

Let G and U be groups. Given a homomorphism $\varrho : G \to U$, then all other homomorphisms $\sigma : G \to U$ are, up to conjugation by elements in U, parametrized by $H^1(G, U)$. To see this, assume that a homomorphism σ is given; then $\mu(g) = \sigma(g) \cdot \varrho(g)^{-1}$ satisfies

$$\begin{aligned} \mu(gh) &= \sigma(g) \cdot \sigma(h) \cdot \varrho(h)^{-1} \cdot \varrho(g)^{-1} \\ &= \sigma(g) \cdot \varrho(g)^{-1} \cdot {}^{\varrho(g)}\!\left[\sigma(h) \cdot \varrho(h)^{-1}\right], \end{aligned}$$

and so μ is a 1-cocycle relative to ϱ. Conversely, the same calculations show that if μ is a 1-cocycle, then $\sigma(g) = \mu(g) \cdot \varrho(g)$ is a homomorphism. So, modifying ϱ by 1-cocycles (with respect to ϱ), we get all possible homomorphisms from G to U.

Assume that $\sigma(g) = {}^{u}\tau(g)$ for some fixed $u \in U$ - i.e., σ and τ are conjugate. Then $\mu_\sigma(g) = \sigma(g) \cdot \varrho(g)^{-1} = {}^{u}\tau(g) \cdot \varrho(g)^{-1} = u \cdot \mu_\tau(g) \cdot {}^{\varrho(g)}u^{-1}$, and so μ_σ and μ_τ are equivalent 1-cocycles, and conversely. Thus σ and τ differ by conjugation with a unit if and only if the associated cocycles are equivalent. Thus we have shown:

LEMMA 3. *Given a fixed homomorphism $\varrho : G \to U$, then every homomorphism $\sigma : G \to U$ is of the form $\sigma(g) = \mu(g) \cdot \varrho(g)$ for some 1-cocycle μ with respect to ϱ. Moreover, two homomorphisms σ and τ are conjugate if, and only if, the associated cocycles are equivalent.*

We next turn to the question of liftings of homomorphisms. Let V be a normal subgroup in U, and assume that we have a homomorphism

$\varrho : G \to U/V$. There are two parts to the obstruction to lifting ϱ to a homomorphism $\hat{\varrho} : G \to U$.

PROBLEM 1.

(1) Conjugation by $\varrho(g)$ gives a homomorphism, also denoted by ϱ, from G to $\mathrm{Aut}(U/V)$. Can we find an action $\tilde{\varrho}$ of G on U which is compatible with ϱ?

(2) If $\tilde{\varrho}$ can be found, when does it arise from a homomorphism $\hat{\varrho} : G \to U$; i.e., can we lift ϱ to a homomorphism from G to U?

For the sake of simplicity, and also because the nonabelian situation does not give any new insight, we shall assume from now on that V is abelian. In that situation $\tilde{\varrho}$ always exists: Let $\tilde{\varrho}(g)$ be any coset representative of $\varrho(g)$ in U; then conjugation by $\tilde{\varrho}(g)$ induces a well-defined action of G on U.

This induces a unique homomorphism, also denoted by $\varrho : G \to \mathrm{Aut}(V)$, compatible with the action ϱ of G on U/V. Note that for this construction we do need a homomorphism $\varrho : G \to U/V$ and not just an action of G on U/V.

Let $\varrho_1(g)$ be any coset representative of $\varrho(g)$ in U, $g \in G$, and define $\mu(g, h)$ by

$$\varrho_1(g) \cdot \varrho_1(h) = \mu(g, h) \cdot \varrho_1(gh); \tag{5}$$

i.e., μ is the obstruction for ϱ_1 to be a homomorphism. Then μ is a 2-cocycle of G with values in V with respect to the action ϱ (cf. Definition 3). In fact, the associativity of the multiplication implies

$$\begin{aligned}
[\varrho_1(x) \cdot \varrho_1(y)] \cdot \varrho_1(z) &= \mu(x, y) \cdot \mu(xy, z) \cdot \varrho_1(xyz), \\
\varrho_1(x) \cdot (\varrho_1(y) \cdot \varrho_1(z)) &= \varrho_1(x) \cdot \mu(y, z) \cdot \varrho_1(yz) \\
&= {}^{\varrho_1(x)}\mu(y, z) \cdot \mu(x, yz) \cdot \varrho_1(xyz).
\end{aligned}$$

However, the actions of ϱ_1 and ϱ coincide on V, and thus μ is a cocycle on V with respect to ϱ.

DEFINITION 4. The cocycle μ from (15), and also its equivalence class in $H_\varrho^2(G, V)$, will be denoted by $\Delta(\varrho)$.

Note that the class of $\Delta(\varrho)$ in $H_\varrho^2(G, V)$ does indeed depend only on ρ.

LEMMA 4. *ϱ can be lifted to a homomorphism $\hat{\varrho} : G \to U$ if, and only if, $\Delta(\varrho)$ is a 2-coboundary.*

Proof. Assume that $\Delta(\varrho) = \mu \in H_{\varrho}^2(G, V)$ is a coboundary (cf. Definition 3), say $\Delta(\varrho)(g, h) = \mu(g, h) = [f(g) \cdot {}^{\varrho(g)}f(h)]^{-1} \cdot f(gh)$ for some function $f : G \to V$. Then

$$\hat{\varrho}(g) = f(g) \cdot \varrho_1(g) \tag{6}$$

is a homomoprhism; in fact,

$$f(g) \cdot \varrho_1(g) \cdot f(h) \cdot \varrho_1(h) = f(g) \cdot {}^{\varrho_1(g)}f(h) \cdot \left[f(g) \cdot {}^{\varrho_1(g)}f(h)\right]^{-1},$$

$$f(gh) \cdot \varrho_1(gh) = f(gh) \cdot \varrho_1(gh).$$

(Note that ϱ_1 acts as ϱ on V.) ■

We now turn to the problem of finding all liftings of $\varrho : G \to U/V$ to $\sigma : G \to U$, provided we already have constructed one lifting $\hat{\varrho}$ as in Equation (6); i.e., $\Delta(\varrho)$ (cf. Definition 4) is a coboundary.

LEMMA 5. *All other liftings σ are of the form $\mu \cdot \hat{\varrho}$, where $\mu : G \to V$ is a 1-cocycle with respect to the conjugation action induced by $\hat{\varrho}$ on V, and conversely. Two liftings σ and σ' are conjugate by some $v \in V$ if and only if the corresponding 1-cocycles μ and μ' represent the same element in $H_{\hat{\varrho}}^1(G, V)$.*

REMARK 1. The above lemma gives the liftings up to conjugacy with elements in V; however, we are really interested in the liftings up to conjugacy with elements in U. It should be noted, though, that different elements in $H_{\hat{\varrho}}^1(G, V)$ might give rise to conjugate (in U) homomorphisms. This is where the exact sequence (1) of nonabelian cohomology sets comes into the picture. In general U and U/V will not be abelian. According to Equation (5), the image of $H_{\hat{\varrho}}^1(G, V)$ in $H_{\hat{\varrho}}^1(G, U)$ [cf. the exact sequence (1)], induced from the exact sequence

$$1 \to V \to U \to U/V \to 1, \tag{7}$$

parametrizes the liftings exactly up to conjugacy with elements in U.

Before we turn to the proof of Lemma 5, let us make some comments: Let us elaborate on the part of the exact cohomology sequence (1), which is relevant in the above application. We have the exact sequence

$$H_{\hat{\varrho}}^{0}(G, U/V) \overset{\partial^0}{\to} H_{\hat{\varrho}}^{1}(G, V) \overset{\alpha_1}{\to} H_{\hat{\varrho}}^{1}(G, U), \tag{8}$$

where $H_{\hat{\varrho}}^{0}(G, U/V) := \{u \cdot V : {}^{\varrho(g)}u \cdot V = u \cdot V\}$ is the set of fixed points. Note that $H_{\hat{\varrho}}^{0}(G, U/V)$ is a subgroup of U/V. the proof of the exactness can be found in [4].

It should be noted however that though $H_{\hat{\varrho}}^{0}(\mathrm{G, U/V})$ *and* $\mathrm{H}_{\hat{\varrho}}^{1}(\mathrm{G, V})$ *are abelian groups,* ∂^0 *need not be a group homomorphism.*

Proof. If we put $\mu(g) = \sigma(g) \cdot \hat{\varrho}(g)^{-1}$, then (cf. Lemma 4)

$$\mu(gh) = \sigma(gh) \cdot \hat{\varrho}(gh)^{-1} = \sigma(g) \cdot \hat{\varrho}(g)^{-1} \cdot {}^{\hat{\varrho}(g)}\left[\sigma(h) \cdot \hat{\varrho}(h)^{-1}\right],$$

and μ is a 1-cocycle with respect to $\hat{\varrho}$. The same equation shows that for every 1-cocycle μ, the map $\sigma(g) = \mu(g) \cdot \hat{\varrho}(g)$ is a homomorphism.

Assume now that for $\sigma_i(g) = \mu_i(g) \cdot \hat{\varrho}(g)$, $i = 1, 2$, we have $\sigma_1(g) = {}^{v}\sigma_2(g)$ for some fixed $v \in V$. Then

$$\mu_1(g) \cdot \hat{\varrho}(g) = {}^{v}[\mu_2(g) \cdot \hat{\varrho}(g)] = {}^{v}\mu_2(g) \cdot {}^{\hat{\varrho}(g)}v^{-1} \cdot \hat{\varrho}(g),$$

and so μ_1 and μ_2 are equivalent (cf. Definition 3). The same equation shows that if μ_1 and μ_2 are equivalent, then the corresponding homomorphisms are conjugate by an element in V. ■

4. UNIT GROUPS OF RINGS

We assume from now on that A is a ring, and we denote by $A^{\times}$ its multiplicative group of units. I will be a two-sided nilpotent ideal in A. Thus $1 + I$ is a normal subgroup in $A^{\times}$. We note that if $I^2 = 0$, then we have a natural isomorphism

$$(1 + I, \cdot) \simeq (I, +) \qquad \text{defined by} \quad 1 + x \mapsto x, \tag{9}$$

since $(1 + x) \cdot (1 + y) = 1 + x + y$; in particular, $1 + I$ is an abelian group. We assume from now on that $I^2 = 0$.

Let $\varrho : G \to A^{\times}/(1 + I)$ be a homomorphism. Since $I^2 = 0$, the conjugation action with a coset representative of $\varrho(g)$ in $A^{\times}$ induces an action on $1 + I$, also denoted by ϱ, which makes $1 + I$ and I into G-modules.

We shall now apply the results of the previous section to the present situation: Because of Remark 1 we have an induced natural isomorphism:

$$H_{\varrho}^{i}(G, (1 + I, \cdot)) \simeq H_{\varrho}^{i}(G, (I +)), \qquad i = 1, 2, \tag{10a}$$

via

$$\mu(g) \mapsto \mu(g) - 1 \quad \text{and} \quad \mu(g, h) \mapsto \mu(g, h) - 1. \tag{10b}$$

REMARK 2. In order to find all liftings of ϱ to a homomorphism $\hat{\varrho}$ from G to $A^{\times}$, we have to follow these two steps:

(1) Compute whether the 2-cocycle $\Delta(\varrho)$ associated to ϱ (Definition 4) is represented by zero in $H_{\varrho}^{2}(G, I)$ under the isomorphism in (10). Note that this involves the natural isomorphism in (9). If this is so, then Lemma 4 gives a natural construction for one lifting $\hat{\varrho}$, provided we can find the 2-coboundary associated to $\Delta(\varrho)$; but this is given by the formula in Equation (5).

(2) All other liftings, up to conjugation with elements in $1 + I$, are obtained as $\sigma = \nu \cdot \hat{\varrho}$, where ν runs over representatives of 1-cocycles in $H_{\varrho}^{1}(G, I)$ (cf. Lemma 4). Again we have invoked the natural isomorphism in (10).

Let us recall that we actually want the liftings only up to conjugation with the units in $A^{\times}$. We shall come back to this problem later. Note that all these constructions depend only on the homomorphism $\varrho : G \to A^{\times}/(1 + I)$. We now turn to the special situation of group rings.

DEFINITION 5. G and H are finite p-groups; $\mathbb{F}$ is the field with p elements; $\mathbb{F}H$ is the group ring of H over $\mathbb{F}$; $I = I(\mathbb{F}H)$ is the augmentation ideal of $\mathbb{F}H$, which is at the same time the radical of $\mathbb{F}H$; and n_0 is defined as the index of nilpotency of I ($I^{n_0} \neq 0$, but $I^{n_0+1} = 0$), where $I(G)$ is the augmentation ideal of $\mathbb{F}G$.

The aim is to develop a test as to when $\mathbb{F}G \simeq \mathbb{F}H$ as augmented algebras. This will be achieved by finding all homomorphisms, up to conjugation, from G to $\mathbb{F}H/I^n$ for "large" n, depending on the computer power available. If $2 \cdot n \geqslant n_0$, then Lemmata 4 and 5, together with the exact sequence (1) of cohomology sets, will give all augmented homomorphisms $G \to \mathbb{F}H$ up to conjugation.

Our program will test whether or not $\mathbb{F}G/I(G)^n \simeq \mathbb{F}H/I^n$, and in this process we compute all possible isomorphisms up to inner isomorphisms. [In many situations, even this might be too coarse, since the algorithms are very time consuming, and therefore one should also invoke the automorphisms of the group G. Note that $\mathrm{Aut}(G)$ acts on the set of these isomorphisms $\mathbb{F}G/I(G)^n \to \mathbb{F}H/I(H)^n$, and one does consider only one representative from each orbit under this action in passing from n to $n+1$.]

This construction will be done in small steps according to the filtration induced by the ideals I^n. The algorithms from Lemmata 4, 5 will give only homomorphisms from G to $\mathbb{F}H/I^n$; however, we are interested in epimorphisms.

This is remedied by

REMARK 3. Let $\varrho : G \to \mathbb{F}H^\times/(1 + I^n)$, $n \geqslant 2$, be a homomorphism such that $\varrho(G)$ generates $\mathbb{F}H/I^2$ as a ring. Then $\varrho(G)$ generates $\mathbb{F}H/I^n$ as a ring. In fact, the graded version with respect to the powers of the radical of $\mathbb{F}H/I^n$ is an epimorphic image of the tensor algebra of I/I^2; whence the statement.

Assume that we have already constructed one homomorphism

$$\varrho : G \to \left(\mathbb{F}H/I^{n-1}\right)^\times = \mathbb{F}H^\times/(1+I)^{n-1}.$$

We recall that then all homomorphisms, up to conjugation, are obtained by modifying ϱ with 1-cocycles from classes in $H^1_\varrho(G, \mathbb{F}H^\times/(1+I)^{n-1})$ (cf. Lemma 3). Now $H^1_\varrho(G, \mathbb{F}H^\times/(1+I)^{n-1})$ is not so easily computed as a nonabelian cohomology set, and so we shall filter it by abelian cohomology. For an integer n, let $[n/2]$ be the largest integer $\leqslant n/2$. We have the exact sequence

$$0 \to 1 + I^{[(n+1)/2]}/I^{n-1} \to \mathbb{F}H^\times/(1 + I^{n-1}) \to \mathbb{F}H^\times/(1 + I^{[(n+1)/2]}) \to 0.$$

Since $I^{[(n+1)/2]} \cdot I^{[(n+1)/2]} \subset I^n \subset I^{n-1}$, the group $1 + I^{[(n+1)/2]}/I^{n-1}$ is abelian, and so any homomorphism $\tilde{\varrho} : G \to \mathbb{F}H^\times/(1 + I^{[(n+1)/2]})$ induces an action on $1 + I^{[(n+1)/2]}/I^{n-1}$, and hence, if

$$\{\tilde{\varrho}_1, \ldots, \tilde{\varrho}_t\}, \qquad \tilde{\varrho}_i : G \to \mathbb{F}H^\times/(1 + I^{[(n+1)/2]})$$

are the homomorphisms, up to conjugation in $\mathbb{F}H^{\times}/(1 + I^{[(n+1)/2]})$, which lift to homomorphisms

$$\{\varrho_1, \dots, \varrho_t\}, \qquad \varrho_i : G \to \mathbb{F}H^{\times}/(1 + I^{n-1}), \tag{11}$$

then all homomorphisms $G \to \mathbb{F}H^{\times}/(1 + I^{n-1})$ - up to conjugation by elements in the group $(1 + I^{[(n+1)/2]})/(1 + I^{n-1})$ in some sense - are given by

$$\mu_{\varrho^i} \cdot \varrho_i, \tag{12a}$$

where

$$\mu_{\varrho_i} \in H^1_{\varrho_i}\big(G, 1 + I^{[(n+1)/2]}/I^{n-1}\big) \simeq H^1_{\varrho_i}\big(G, I^{[(n+1)/2]}/I^{n-1}\big). \tag{12b}$$

We abbreviate this set by

$$H^1_{\varrho_i}\big(G, I^{[(n+1)/2]}/I^{n-1}\big) \cdot \varrho_i, \qquad 1 \leqslant i \leqslant t. \tag{13}$$

Note however that we have not yet achieved our initial goal of parametrizing the set of homomorphisms $G \to \mathbb{F}H^{\times}/(1 + I^{n-1})$ up to conjugation in $\mathbb{F}H^{\times}/(1 + I^{n-1})$; cf. Lemma 5. (We have described them all, but there may be repetitions under conjugation.)

At this stage of the algorithm the above set is the image of our set in $H^1_{\varrho_i}(G, \mathbb{F}H^{\times}/(1 + I^{n-1}))$, which by the exact sequence (1) of cohomology sets is just the image of

$$H^1_{\varrho_i}\big(G, 1 + I^{[(n+1)/2]}/I^{n-1}\big)/\partial^0\Big(H^0_{\varrho_i}\big(G, \mathbb{F}H^{\times}/(1 + I^{[(n+1)/2]})\big)\Big)$$

under α_1 [cf. (3) and Lemma 2]. We shall invoke this at a later stage, where we can use "linear methods."

So the set in Equation (13) is a parametrization of *all* homomorphisms $G \to \mathbb{F}H^{\times}/(1 + I^{n-1})$, which we have obtained inductively. We now want to find all homomorphisms $G \to \mathbb{F}H^{\times}/(1 + I^{n})$ "up to conjugation." This process has to be done for each ϱ_i separately. Note that we do not have to test each homomorphism $G \to \mathbb{F}H^{\times}/(1 + I^{n-1})$ but only the maps ϱ_i, $1 \leqslant i \leqslant t$.

In order to see this, let ϱ be one of the ϱ_i's, which is a lifting of $\tilde{\varrho}_i : G \to \mathbb{F}H^{\times}/(1 + I^{[(n+1)/2]})$. Let us recall that we have exact sequences

$$0 \to 1 + I^{n-1}/I^{n} \to \mathbb{F}H^{\times}/(1 + I^{n}) \to \mathbb{F}H^{\times}/(1 + I^{n-1}) \to 0$$

and

$$0 \to 1 + I^{n-1}/I^{n} \to 1 + I^{[(n+1)/2]}/I^{n} \to 1 + I^{[(n+1)/2]}/I^{n-1} \to 0, \quad (14)$$

where the G-action is induced from $\varrho : G \to \mathbb{F}H^{\times}/(1 + I^{n-1})$.

Let $\varrho_1 : G \to \mathbb{F}H^{\times}/(1 + I^{n})$ be a set theoretical lifting of the homomorphism ϱ.

The 2-cocycle $\Delta(\varrho)(g, h)$, in $H_{\varrho}^{2}(G, 1 + I^{n-1}/I^{n})$, was defined in Definition 4. This is the "connecting homomorphism" associated to the sequence (1)—note that $1 + I^{n-1}/I^{n}$ is a trivial G-module. On the other hand, the exact sequence (14) also gives rise to the connecting homomorphism ∂^{1}; note that here we have abelian cohomology. We recall the definition of ∂^{1} [cf. Equation (2)]: Let α be a 1-cocycle from G to $1 + I^{[(n+1)/2]}/I^{n-1}$ with respect to ϱ. Then $\partial^{1}(\alpha)(g, h) = \alpha(gh)^{-1} \cdot \alpha(g) \cdot {}^{\varrho(g)}\alpha(h)$.

We have seen above in Lemma 4 that $\mu \cdot \rho$ [cf. Equation (12)] can be lifted if, and only if, $\Delta(\mu \cdot \varrho)$ is a 2-coboundary, i.e. is equal to 1 in $H_{\varrho}^{2}(G, 1 + I^{n-1}/I^{n})$. So it remains to show that $\Delta(\mu \cdot \varrho) = 1$ is equivalent to $\Delta^{1}(\varrho) \cdot \partial^{1}(\mu) = 1$. Using the above definition of ∂^{1}, we obtain

$$\begin{aligned}
\mu\varrho(g) \cdot \mu\varrho(h) &= \mu(g) \cdot \varrho(g) \cdot \varrho(h) \cdot \\
&= \mu(g) \cdot {}^{\varrho(g)}\mu(h) \cdot \varrho(g) \cdot \varrho(h) \\
&= \mu(g) \cdot {}^{\varrho(g)}\mu(h) \cdot \Delta(\varrho)(g, h) \cdot \varrho(gh) \\
&= \mu(g) \cdot {}^{\varrho(g)}\mu(h) \cdot \Delta(\varrho)(g, h) \\
&\quad \cdot \mu(gh)^{-1} \cdot \mu(g, h)\varrho(g \cdot h) \\
&= \partial^{1}(\mu) \cdot \Delta(\varrho)(g, h) \cdot \mu(g \cdot h) \cdot \varrho(g \cdot h).
\end{aligned}$$

Again using the fact that $1 + I^{[(n+1)/2]}/I^{n-1}$ is commutative, we conclude that $\Delta(\mu\varrho) = \partial^{1}(\mu) \cdot \Delta(\varrho)$, as claimed.

Recall that the exact Sequence 14 gives rise to the exact sequence—all groups are commutative—

$$1 \to H_{\varrho}^{1}(G, 1 + I^{n-1}/I^{n}) \to H_{\varrho}^{1}(G, 1 + I^{[(n+1)/2]}/I^{n})$$
$$\xrightarrow{\varphi} H_{\varrho}^{1}(G, 1 + I^{[(n+1)/2]}/I^{n-1}) \to H_{\varrho}^{2}(G, 1 + I^{n-1}/I^{n}).$$

Hence if $\mu \cdot \varrho$ does lift, so does $\operatorname{Im}(\varphi) \cdot \mu \cdot \varrho$. Thus we have proved:

LEMMA 6. *Some element in the "affine space" $H_{\varrho}^{1}(G, I^{[(n+1)/2]}/I^{n-1}) \cdot \varrho$ - here ϱ is one of the maps ϱ_i in Equation (11) - can be lifted to a homomorphism $\sigma : G \to \mathbb{F}H^{\times}/(1 + I^{n})$ if, and only if, $\Delta(\varrho) \in H_{\varrho}^{2}(G, 1 + I^{n-1}/I^{n})$ lies in the image of the map*

$$\partial^{1} : H_{\varrho}^{1}(G, 1 + I^{[(n+1)/2]}/I^{n-1}) \to H_{\varrho}^{2}(G, 1 + I^{n-1}/I^{n}).$$

In that case the elements $\mu \cdot \rho$ which can be lifted are those satisfying the condition $\Delta(\varrho) = \partial^{1}(\mu^{-1})$.

For computational purposes we note that $H_{\varrho}^{2}(G, 1 + I^{n-1}/I^{n})$ is independent of ϱ, since I^{n-1}/I^{n} is a trivial G-module.

Let us summarize: Starting out from the parametrization in Equation (12), where $\{\varrho_i\}$ is a set of representatives for liftings to $\mathbb{F}H^{\times}/(1 + I^{n-1})$ up to conjugacy in $\mathbb{F}H^{\times}/(1 + I^{[(n+1)/2]})$ of the homomorphisms $\tilde{\varrho}_i : G \to \mathbb{F}H^{\times}/(1 + I^{[(n+1)/2]})$, and μ is determined up to conjugacy with $1 + I^{[(n+1)/2]}/I^{n-1}$, we have now constructed all possible liftings $G \to \mathbb{F}H^{\times}/(1 + I^{n})$, up to modifications by $H^{1}(G, I^{n-1}/I^{n})$, as follows:

LEMMA 7. *After renumbering, if necessary, let $\mu_i \in H_{\varrho_i}^{1}(G, I^{[(n+1)/2]}/I^{n-1})$ be chosen such that $\mu_i \cdot \varrho_i$, $1 \leqslant i \leqslant \tau$, lift to $\mathbb{F}H^{\times}/(1 + I^{n})$ according to Lemma 4. Then all the liftable maps are given by $Im \cdot \mu_i \cdot \varrho_i$, $1 \leqslant i \leqslant \tau$, where*

$$\operatorname{Im} = \operatorname{Im}\Big(H_{\varrho_i}^{1}(G, 1 + I^{[(n+1)/2]}/I^{n}) \xrightarrow{\varphi} H_{\varrho_i}^{1}(G, 1 + I^{[(n+1)/2]}/I^{n-1})\Big).$$

Proof. This follows directly from Lemma 4. ∎

If we pass from n to $n + 1$, we have - in case $[(n + 1)/2] \neq [(n + 2)/2]$ - to invoke a process of reparametrization: The natural map

$$\gamma_i : H_{\varrho_i}^{1}(G, 1 + I^{[(n+1)/2]}/I^{n-1}) \to H_{\varrho_i}^{1}(G, 1 + I^{[(n+1)/2]}/I^{[(n+2)/2]})$$

sends Im to $\gamma_i(\mathrm{Im}) \subset H_{\varrho_i}^{1}(G, 1 + I^{[(n+1)/2]}/I^{[(n+2)/2]})$. The maps in the set $\gamma_i(\mathrm{Im}) \cdot \mu_i \cdot \varrho_i$ from G to $\mathbb{F}H^{\times}/(1 + I^{[(n+2)/2]})$ are precisely the homomorphisms which lift to $\mathbb{F}H^{\times}/(1+I^{n})$; however, they are not yet partitioned according to conjugation in $\mathbb{F}H^{\times}/(1+I^{[(n+2)/2]})$. But luckily enough, $1+I^{[(n+1)/2]}/I^{[(n+2)/2]}$ is a quotient of $\mathbb{F}H^{\times}/(1+I^{[(n+2)/2]})$ on which $\mathbb{F}H^{\times}/(1+I^{[(n+2)/2]})$ acts trivially. Thus we can use Equation (4) to compute the orbits of $H^{1}(G, 1+I^{[(n+1)/2]}/I^{[(n+2)/2]})$ under the action of the centralizer of G in $\mathbb{F}H^{\times}/(1+I^{[(n+2)/2]})$ modulo $\mathbb{F}H^{\times}/(1+I^{[(n+1)/2]})$ in a linear fashion.[3] Let now $\tilde{\sigma}_1, \ldots, \tilde{\sigma}_s$ be representatives of the orbits generated by $\gamma_i(\mathrm{Im}) \cdot \mu_i \cdot \varrho_i$, for $1 \leqslant i \leqslant \tau$ under the above action. Then $\tilde{\sigma}_1, \ldots, \tilde{\sigma}_s$ takes the rôle of $\tilde{\varrho}_1, \ldots, \tilde{\varrho}_t$ in the inductive process.

Thus we have reached the point where we can apply induction.

This is a theoretical construction to obtain all possible homomorphisms $G \to \mathbb{F}H^{\times}/(1+I^{n})$ "up to conjugation," once the homomorphisms $G \to \mathbb{F}H^{\times}/(1+I^{n-1})$ are known "up to conjugation." We now come to the practical computations.

5. COHOMOLOGY OF IDEALS AND BIMODULES.

5.1. *Generalities*

Let A be a ring as above, and G a group which acts via ϱ on $A^{\times}$ or on an ideal I. We could also replace I by a subquotient I^{n}/I^{m}, or more generally by any $\mathbb{F}G$-bimodule.

T compute $H_{\varrho}^{0}(G, A^{\times})$ amounts to computing fixed points, which is just the solution of a set of linear equations, depending on the number of generators of G.

We next turn to the computation of $H_{\varrho}^{1}(G, I)$. For a two-sided ideal I in A we have a natural isomorphism $H_{\varrho}^{1}(G, I) \simeq H_{\varrho}^{1}(\mathbb{F}G, I)$, where the latter are algebra derivations modulo inner derivations. The natural map from 1-cocycles to derivations, $\mu(g) \to \delta(g) = \mu(g) \cdot \varrho(g)$ induces the above isomorphism. It should be observed that for this isomorphism we do not need a homomorphism $G \to A^{\times}$, but only an action ϱ of G on A or even only on I. One advantage of $H_{\varrho}^{1}(\mathbb{F}G, I)$ over $H_{\varrho}^{1}(G, I)$ is that a computer likes multiplication better than conjugation.

5.2. *Computation of $H_{\varrho}^{1}(\mathbb{F}G, I)$*

For the rest of this section our group G is now finitely presented. So G is given by generators and relations:

$$G = \langle g_1, \ldots, g_{\nu}; R_1, \ldots, R_{\nu_0} \rangle. \tag{15}$$

[3] The point here is that we want to reduce as many operations as possible to linear operations in order to speed up the calculation.

In a specific example we have a group of order 3^5 given as

$$G = \langle a, b, c : a^9 = 1, b^9 = 1, c^3 = 1, ab = ba, {}^c a = ab^3, {}^c b = a^2 b \rangle.$$

The derivations are now determined by

$$\delta(g_i) = x_i \in I, \qquad 1 \leqslant i \leqslant \nu,$$

and these elements $\{x_i\}_{1 \leqslant i \leqslant \nu}$ have to satisfy $\delta(R_j) = 0$. Using the derivation rule and the G-action on I, the element $\delta(R_j)$ is expressed in terms of the $\{x_i\}_{1 \leqslant i \leqslant \nu}$. For example

$$\delta(g^i) = \varrho(g) \cdot \delta(g^{i-1}) + \delta(g) \cdot \varrho(g^{i-1})$$

by induction. Hence in the above example we get the relations

$$0 = \delta(c^3) = \varrho(c^2) \cdot \delta(c) + \varrho(c) \cdot \delta(c) \cdot \varrho(c) + \delta(c) \cdot \varrho(c^2),$$

and the relation $ab = ba$ gives

$$\begin{aligned} \delta(a \cdot b) &= \varrho(a) \cdot \delta(b) + \delta(a) \cdot \varrho(b) \\ = \delta(b \cdot a) &= \varrho(b) \cdot \delta(a) + \delta(b) \cdot \varrho(a), \end{aligned}$$

and so we must have

$$\varrho(a) \cdot \delta(b) + \delta(a) \cdot \varrho(b) - \varrho(b) \cdot \delta(a) - \delta(b) \cdot \varrho(a) = 0.$$

Each $\delta(R_j)$ is to be interpreted as an $\mathbb{F}$-linear map $D_j : I^{(\nu)} \to I$, associating with each ν-tuple $(x_i)_{1 \leqslant i \leqslant \nu}$ the value $\delta(R_j)$. We thus obtain an $\mathbb{F}$-linear mapping $D : I^{(\nu)} \to I^{(\nu_0)}$, if we take all relations into account. The kernel of D is the space of the $\mathbb{F}$-linear derivations with values in I. This is computed as solutions of a system of linear equations.

We next have to compute the subspace of the inner derivations. Above we have interpreted a derivation as a ν-tuple $(x_i)_{1 \leqslant i \leqslant \nu}$, where x_i is the value of the generator g_i under the derivation, $1 \leqslant i \leqslant \nu$. For the inner derivations we choose an $\mathbb{F}$-basis $\{v_j\}$ of I, and consider the subspace of the derivations generated by $\{(x_{ij})_{1 \leqslant i \leqslant \nu}\}$ with $x_{ij} = g_i \cdot v_j - v_j \cdot g_i$. This is the space of inner derivations, and now it is easy to find coset representatives, $\{\delta_k\}_{1 \leqslant k \leqslant d}$, which form an $\mathbb{F}$-basis for $H^1_\varrho(\mathbb{F}G, I)$. In order to obtain a basis of $H^1_\varrho(G, I)$, we form $\mu_k(g_i) = \delta_k(g_i) \cdot \varrho(g_i)^{-1}$. This completes the computations of abelian 1-cohomology of ideals.

We point out that we have computed $H_\varrho^1(G, I)$ by listing genuine 1-cocycles which form an $\mathbb{F}$-basis when reduced modulo 1-coboundaries. In general the ideal I will be a power of the augmentation ideal $I(H)$ of $\mathbb{F}H$, which has an $\mathbb{F}$-basis $\{h - 1, h \in H \setminus \{1\}\}$.

If G is a p-group and the presentation (15) is a minimal presentation of G, then $\{G_i = g_i - 1\}_{1 \leqslant i \leqslant \nu}$ is a minimal system of generators of $I(G)$, since $\{G_i\}_{1 \leqslant i \leqslant \nu}$ is an $\mathbb{F}$-basis for $I(G)/I(G)^2$. More generally, the elements

$$G_1^{n_1} \cdot \cdots \cdot G_\nu^{n_\nu}, n_1 + \cdots + n_\nu = n, \qquad G_i^{n_i} \neq 0$$

form a set of generators for $I(G)^n$, and they form an $\mathbb{F}$-basis for $I(G)^n/I(G)^{n+1}$. This basis is adjusted to our filtration of the augmentation ideal. With respect to this basis the multiplication is quite easy, since one only needs to store the additive commutators $[G_i, G_j] = G_i \cdot G_j - G_j \cdot G_i$.

5.3. *Computation of H^2 with Trivial Coefficients*

Now G and H are finite p-groups, $I := I(H)$ is the augmentation ideal of $\mathbb{F}H$, and char($\mathbb{F}$) $= p$. We know that I^{n-1}/I^n is a trivial G-module both under conjugation and under left multiplication. Then the homomorphism ϱ does not matter, and we just have to compute $H^2(G, T)$, where T is a trivial G-module.

The definition of $H^2(G, T)$, which we have given previously, is not at all suited for computation, but one strength of the cohomological interpretation of our problem lies in the fact that, using another interpretation of $H^2(G, T)$, we can compute the latter very easily. In order to give this interpretation, we have to construct projective resolutions. The following constructions are very explicit and suited for the computer.

We have augmentation sequence of 2-sided $\mathbb{F}G$-modules

$$0 \to I(G) \to \mathbb{F}G \xrightarrow{\varepsilon} \mathbb{F} \to 0,$$

where the augmentation map ε sends $g \in G$ to 1. $I(G)$ has an $\mathbb{F}$-basis $\{g - 1\}_{g \in G \setminus \{1\}}$. Moreover, a set of generators of $I(G)$ as left $\mathbb{F}G$-module is given by $\{g_i - 1\}_{1 \leqslant i \leqslant \nu}$, where $\{g_i\}_{1 \leqslant i \leqslant \nu}$ is a minimal set of generators of G. Hence we obtain an exact sequence of left $\mathbb{F}G$-modules

$$0 \to \Omega^2 \to \bigoplus_{i=1}^{\nu} \mathbb{F}Ge_i \xrightarrow{\phi} I(G) \to 0, \tag{16}$$

where ϕ is induced from $e_i \to g_i - 1$. Then ϕ is surely an epimorphism. Note again for computational purposes that Ω^2 as kernel of ϕ can be computed via a system of linear equations as a subspace of $\oplus_{i=1}^{\nu} \mathbb{F}Ge_i$. We can in fact list a natural set of generators for Ω^2 via the Fox derivative: The presentation (15) of G is tantamount to an exact sequence of groups

$$1 \to R \to F \overset{\phi'}{\to} G \to 1,$$

where F is free on the elements $\{f_i\}_{1 \leqslant i \leqslant n}$ and ϕ' is induced from $f_i \to g_i$, $1 \leqslant i \leqslant n$. The augmentation ideal $I(F)$ of $\mathbb{F}F$ is $\mathbb{F}F$-free on the elements $\{f_i - 1\}_{1 \leqslant i \leqslant n}$. We interpret the relations R_j as elements in F. Then we have a unique expression

$$R_j - 1 = \sum_i \hat{x}_{ij} \cdot (f_i - 1) \qquad \text{with} \quad \hat{x}_{ij} \in \mathbb{F}F. \tag{17}$$

Let x_{ij} be the image of $\hat{x}_{ij}$ under the natural map $\mathbb{F}F \to \mathbb{F}G$. Then the element

$$\omega_j = \sum x_{ij} e_i \in \bigoplus_{i=1}^{\mu} \mathbb{F}Ge_i$$

lies in Ω^2, $1 \leqslant j \leqslant \nu_0$, and in fact, these elements generate Ω^2 as left module. We now have to quote some more or less well-known facts:

THEOREM 1.

(1) *Ω^2 does not have a projective direct summand, since G is a p-group. And so Ω^2 above is indeed the second syzygy of the trivial module, and hence $\oplus_{i=1}^{\nu} \mathbb{F}Ge_i$ is the projective cover of $I(G)$.*[4]

(2) *One has*

$$H^2(G, \mathbb{F}) \simeq \mathrm{Hom}_{\mathbb{F}G}(\Omega^2, \mathbb{F}) \simeq \Omega^2 / I(G) \cdot \Omega^2,$$

taking into account that $\mathbb{F}$ is a trivial G-module.[5]

Note that above we have computed Ω^2 inside $\oplus_{i=1}^{\nu} \mathbb{F}Ge_i$, and thus we can easily compute $\Omega^2 / I(G) \cdot \Omega^2$, and hence also $H^2(G, \mathbb{F}) \simeq \mathrm{Hom}_{\mathbb{F}}(\Omega^2 / I(G) \cdot \Omega^2, \mathbb{F})$.

[4] It was shown in [1] that $\{g_i - 1\}_{1 \leqslant i \leqslant \nu}$ is indeed a minimal set of generators of $I(G)$, provided G is a p-group.

[5] We refer to [1, 3].

5.4. *Various Descriptions of H^2*

Let U be a group, and V an abelian normal p-subgroup of exponent p, which lies in the center of U. Assume that we have a homomorphism $\varrho : G \to U/V$.

LEMMA 8. *The conjugation action of G on U/V induced from ϱ can be lifted to an action of G on all of U.*

Proof. We have to construct a well-defined homomorphism $\hat{\varrho} : G \to \mathrm{Aut}(U)$. Let $\hat{\varrho}(g)$ and $\varrho'(g)$ be two coset representatives of $\varrho(g)$ in U. Then $\hat{\varrho}(g) \cdot v(g) = \varrho'(g)$ for some $v(g) \in V$. Thus $\hat{\varrho}(g) \cdot v(g) \cdot u \cdot v(g)^{-1} \cdot \hat{\varrho}(g)^{-1} = \hat{\varrho}(g) \cdot u \cdot \hat{\varrho}(g)^{-1}$, V being central. Hence the action can be lifted. Note that in order to give an action on V we only needed V to be abelian; however, to extent it generally to all of U, V had to be central. ■

We recall the various equivalent definitions of $H^2(G, V)$ for G acting trivially on V.

DEFINITION 6[6]

(1) The definition via factor sets: A *factor set* f is a function $f : G \times G \to V$ with

$$f(xy, z) \cdot f(x, y) = f(x, yz) \cdot f(y, z), \qquad x, y, z \in V.$$

A factor set is said to be *principal* if it is of the form

$$f(x, y) = \varphi(x)^{-1} \cdot \varphi(y)^{-1} \cdot \varphi(xy)$$

for some function $\varphi : G \to V$. $H^2_{\mathrm{fac}}(G, V)$ is the quotient of the factor sets modulo principal factor sets. $H^2_{\mathrm{fac}}(G, V)$ can then be identified with equivalence classes of group extensions

$$1 \to V \to X \to G \to 1,$$

where the factor set is given by choosing coset representatives x_g of g in X, and then defining $f(g, h)$ via

$$x_g \cdot x_h = f(g, h) \cdot x_{gh}. \tag{18}$$

[6] This definition has an analog also for nontrivial modules.

(2) The definition via the relation module: Now G has to be a p-group (cf. [1]). Choose a minimal free presentation of G:

$$1 \to R \to F \overset{\phi'}{\to} G \to 1, \tag{19}$$

where F is a free group on ν elements $\{f_i\}_{1 \leqslant i \leqslant \nu}$ and $g_i = \phi'(f_i)$, $1 \leqslant i \leqslant \nu$, for a minimal set of generators of G. R is then the normal subgroup generated by the relations. Let R' be the commutator subgroup of R. Then R/R' is an abelian group, which we write additively, and G acts on it by conjugation via coset representatives in F/R'. We make this into an $\mathbb{F}G$-module by tensoring with $\mathbb{Z}/p\mathbb{Z}$: $\overline{R} = \mathbb{F} \otimes_{\mathbb{Z}} R/R'$. Then $\overline{R}$ is called the *relation module* modulo p with respect to the exact sequence (19). It should be noted that under the above assumptions on G, $\overline{R}$ is the second syzygy for $\mathbb{F}$ as $\mathbb{F}G$-module (cf. [1]), which we have denoted earlier by Ω^2 [cf. (16)], and so it is unique up to natural isomorphism (we shall come back to this later). Equivalently, the second cohomology group is

$$H^2_\Omega(G,V) = \operatorname{Hom}_{\mathbb{F}G}(\overline{R},V), \tag{20}$$

where V is viewed as a trivial G-module.[7]

We shall now indicate the isomorphism between $H^2_{\text{fac}}(G,V)$ and $H^2_\Omega(G,V)$: Given an exact sequence

$$1 \to V \to X \to G \to 1,$$

where V is an $\mathbb{F}G$-module under conjugation (not necessarily trivial),we can complete the following diagram commutatively, F being a free group:

$$\begin{tikzcd}
1 \arrow[r] & R \arrow[r] \arrow[d, "\sigma'"'] & F \arrow[r, "\phi'"] \arrow[d, "\tau'"'] & G \arrow[r] \arrow[d, "\mathrm{id}"'] & 1 \\
1 \arrow[r] & V \arrow[r] & X \arrow[r] & G \arrow[r] & 1.
\end{tikzcd} \tag{21}$$

Since V is an $\mathbb{F}G$-module, σ' factorizes via $\overline{R}$, and thus we obtain an induced $\mathbb{F}G$-homomorphism $\sigma : \overline{R} \to V$.

[7] This isomorphism is again obtained from a dimension shift, using the fact that $\overline{R}$ has no projective summands and V is trivial.

We now return to the situation above: We are given the homomorphism $\varrho : G \to U/V$, and we want to interpret the associated 2-cocycle $\mu = \Delta(\varrho)$ (cf. Lemma 5) with values in V as a homomorphism from $\bar{R}$ to V. For this we form the pullback along ϱ:

$$\begin{tikzcd}
1 \arrow[r] & V \arrow[r] \arrow[d, "\mathrm{id}"'] & X \arrow[r] \arrow[d, "\hat{\varrho}"'] & G \arrow[r] \arrow[d, "\varrho"'] & 1 \\
1 \arrow[r] & V \arrow[r] & U \arrow[r] & U/V \arrow[r] & 1.
\end{tikzcd} \qquad (22)$$

We thus have constructed an exact sequence, giving rise to a factor set in Equation (18), and we claim that this factor set is, modulo principal factor sets, exactly the 2-cocycle associated to ϱ. Let the factor set as above be defined by $x_g \cdot x_h = f(g,h) \cdot x_{gh}$. Then $\hat{\varrho}(x_g)$ lies in the fiber of $\varrho(g)$. Thus applying $\hat{\varrho}$ and noting that $\hat{\varrho}$ is the identity on V, we have, identifying $\hat{\varrho}(g)$ with $\tilde{\varrho}(g)$ in the notation introduced in Lemma 3,

$$\tilde{\varrho}(g) \cdot \tilde{\varrho}(h) = \hat{\varrho}(x_g) \cdot \hat{\varrho}(x_h) = f(g,h) \cdot \hat{\varrho}(x_{gh}) = f(g,h) \cdot \tilde{\varrho}(gh).$$

Thus the associated cocycle to ϱ is exactly represented by the factor set of the exact sequence of the above pullback modulo 2-coboundaries.

Using the above commutative diagrams (21) and (22), we can now construct the homomorphism $\sigma : \bar{R} \simeq \Omega^2 \to V$, giving a 2-cocycle in the sense of Equation (20). This will be $\Delta(\varrho)$ in Definition 4.

Let us recall that we want to have a technique suited for the computer to check whether (ϱ_i) lies in $\mathrm{Im}(\partial_{\varrho_i})$ (Lemma 6 and Lemma 7). We shall write ϱ for one of the ϱ_i and ∂ for the corresponding ∂_{ϱ_i}.

Now recall that

$$\partial^1 : H^1_\varrho(G, 1 + I^{[(n+1)/2]}/I^{n-1}) \to H^2(G, 1 + I^{n-1}/I^n)$$

is the connecting homomorphisms in the exact sequence (1). Note that $H^2(G, 1 + I^{n-1}/I^n)$ is independent of ϱ, since I^{n-1}/I^n is a trivial module. hence $H^2(G, 1 + I^{n-1}/I^n)$ can be computed according to the description in Equation (20).

Let $[\beta_1], \dots, [\beta_s]$ be an $\mathbb{F}$-basis of $H^1_\varrho(G, I^{[(n+1)/2]}/I^{n-1})$, where the β_i are given as genuine cocycles, and recall that we have stored the elements $\beta_i(g_j)$, where g_j is a minimal system of generators for G. We now interpret the 1-cocycles β_i as homomorphisms

$$\hat{\beta}_i : I(G) \to I^{[(n+1)/2]}/I^{n-1}$$

via

$$g_j - 1 \to \beta_i(g_j).$$

Indeed, there is a natural isomorphism from 1-cocycles:

$$Z^1_\varrho(G, I^{[(n+1)/2]}/I^{n-1}) \to \operatorname{Hom}_{\mathbb{F}G}(I(G), I^{[(n+1)/2]}/I^{n-1}),$$

where $I(G)$ is to be considered as left G-module. In fact, let μ be a 1-cocycle, then

$$\hat{\mu}(g-1) = \mu(g)$$

is a homomorphism:

$$\begin{aligned}\hat{\mu}(g\cdot(h-1)) &= \hat{\mu}((gh-1)-(g-1)) = \hat{\mu}(gh-1) - \hat{\mu}(g-1) \\ &= \mu(gh) - \mu(g) = \mu(g) + {}^{\varrho(g)}\mu(h) - \mu(g) = {}^{\varrho(g)}\hat{\mu}(h).\end{aligned}$$

The same argument shows that any homomorphism gives rise to a 1-cocycle. Moreover, the 1-coboundaries give homomorphisms that factor via $\mathbb{F}G$ and conversely. Hence we have a natural isomorphism with the notation introduced in Theorem 1:

$$H^1_\varrho(G, I^{[(n+1)/2]}/I^{n-1}) \to \underline{\operatorname{Hom}_{\mathbb{F}G}(I(G), I^{[(n+1)/2]}/I^{n-1})} \times \operatorname{proj}(I/I^{n-1}),$$

where the right hand side are homomorphism modulo projectives. Note that $I(G)$ is the augmentation ideal of $\mathbb{F}G$, and that if $\mathbb{F}G = \mathbb{F}H$, then $I(G) = I(H) = I$. By the above formula (20), we have a natural isomorphism

$$H^2(G, 1 + I^{n-1}/I^n) \simeq \operatorname{Hom}_{\mathbb{F}G}(\Omega^2, I^{n-1}/I^n),$$

and we shall interpret $\operatorname{Im}(\partial^1)$ as a subgroup of $\operatorname{Hom}_{\mathbb{F}G}(\Omega^2, I^{n-1}/I^n)$. By the above Lemma 8 we can extend the action of G via ϱ to an action on $I^{[(n+1)/2]}/I^n$, also denoted by ϱ. We then construct the following commutative diagram with exact rows:

$$\begin{tikzcd}
0 \arrow[r] & \Omega^2 \arrow[r] \arrow[d, "\partial^1(\beta_j)"] & \bigoplus_{i=1}^{\nu} \mathbb{F}Ge_i \arrow[r, "\phi"] \arrow[d, "\tilde{\beta}_j"] & I(G) \arrow[r] \arrow[d, "\hat{\beta}_j"] & 0 \\
0 \arrow[r] & I^{n-1}/I^n \arrow[r] & I^{[(n+1)/2]}/I^n \arrow[r] & I^{[(n+1)/2]}/I^{n-1} \arrow[r] & 0.
\end{tikzcd}$$

We do this by choosing coset representatives y_i of $\hat{\beta}_j(g_i - 1) = \beta_j(g_i)$ in $I^{[(n+1)/2]}/I^n$. Note that in practice the basis of $I^{[(n+1)/2]}/I^n$ is given as an extension of the basis of $I^{[(n+1)/2]}/I^{n-1}$, and so it is easy to find the coset representatives. Then $\tilde{\beta}_j$ are defined by $e_i \to y_i$, and $\delta(\beta_j)$ is just the restriction to Ω^2. Then $\operatorname{Im}(\partial^1)$ is the $\mathbb{F}$-space spanned by $\partial^1(\beta_j)$ inside $\operatorname{Hom}_{\mathbb{F}G}(\Omega^2, I^{n-1}/I^n)$. Note that in general the $\partial^1(\beta_j)$ will not be linearly independent. However, we now have a concrete realization of $\operatorname{Im}(\partial^1)$.

Now we want to compute $\Delta(\varrho)$ as a homomorphism from Ω^2 to I^{n-1}/I^n, where we are given a homomorphism $\varrho : G \to \mathbb{F}H^{\times}/(1 + I^{n-1})$. We first describe the algorithm and then justify it.

Lemma 9. *As above, $\{g_i\}_{1 \leqslant i \leqslant \nu}$ is a minimal set of generators of G. This gives rise to the projective cover sequence* (16).

(1) *A set of generators $\{\omega_j,\ 1 \leqslant j \leqslant \nu_0\}$ of Ω^2 can easily be computed as inverse images of a basis of $\Omega^2/I(G)\Omega^2$. (Alternatively one could use the Fox derivative.) These elements ω_j are represented in side $\bigoplus_{i=1}^{\nu} \mathbb{F}Ge_i$, and so we have unique representations*

$$\omega_j = \sum_{i=1}^{\nu} x_{ij} \cdot e_i x_{ij} \in \mathbb{F}G.$$

(2) *If $\tilde{\varrho} : G \to \mathbb{F}H^{\times}/I^n$ is a lifting of ϱ as a map of sets, then we can form abstractly the 2-cocycle μ as $\tilde{\varrho}(g) \cdot \tilde{\varrho}(h) = \mu(g, h) \cdot \tilde{\varrho}(gh)$, which has values in I^{n-1}/I^n; note that μ depends on ϱ.*

(3) *We can extend μ to an $\mathbb{F}$-linear map and compute $\mu(x_{ij}, g_i)$ for all i, j.*

(4) *$\Delta(\varrho)$, interpreted as $\mathbb{F}G$-linear map from Ω^2 to $1 + I^{n-1}/1 + I^n$, is then given by*

$$\Delta(\varrho) : \omega_j \to \sum_{i=1}^{\nu} \mu(x_{ij}, g_i),\ 1 \leqslant j \leqslant \nu_0.$$

We postpone the proof until later.

Now we have to test, whether the map $\Delta(\varrho)$ lies in the $\mathbb{F}$-span of $\{\partial^1(\beta_j)\}$. Note that the elements $\{\partial^1(\beta_j)\}$ are in general not linearly independent. In computing the image of ∂^1, we have at the same time computed the kernel $\operatorname{Ker}(\partial^1)$. Assume that $\Delta(\varrho) \in \operatorname{Im}(\partial^1)$, and choose any representation $\Delta(\varrho) = \sum_{j=1}^{\nu_0} f_j \partial^1(\beta_j)$ - note that the $f_j \in \mathbb{F}$ are not unique. Then for this particular ϱ the possible homomorphisms $G \to \mathbb{F}H^\times/(1 + I^{n-1})$ that can be lifted are precisely the maps $\{\operatorname{Ker}(\partial^1) \cdot (1 + \sum f_j \beta_j)^{-1} \cdot \varrho\}$; note that this is an affine space!

The problem remains, to find all the liftings explicitly. We first have to find one lifting - note that we have not computed the 2-coboundaries from G to $1 + I^{n-1}/I^n$ yet; we have only given an abstract description of $H^2(G, I^{n-1}/I^n)$. However, this task is easier than one would expect, since we have:

LEMMA 10. *Assume that $\beta \cdot \varrho : G \to \mathbb{F}H^\times/(1 + I^{n-1})$ can be lifted. Choose any coset representative $\tilde{\varrho}(g_i)$ for $\beta \cdot \varrho(g_i)$ in $\mathbb{F}H^\times/(1 + I^n)$, where $\{g_i\}$ is a minimal set of generators for G. Then $\tilde{\varrho}(g_i)$ can be extended - in the obvious way - to a unique homomorphism $\tilde{\varrho} : G \to \mathbb{F}H^\times/(1 + I^n)$.*

Proof. We know that there exists a homomorphism $\varrho' : G \to \mathbb{F}H^\times/(1 + I^n)$, which reduces to $\beta \cdot \varrho$. Now $\tilde{\varrho}(g_i) \cdot \varrho'(g_i)^{-1} = 1 + \psi(g_i)$, where $\psi(g_i) \in I^{n-1}/I^n$. However,

$$\operatorname{Hom}\big(G, I^{n-1}/I^n\big) = \operatorname{Hom}\big(G/G', I^{n-1}/I^n\big) = \operatorname{Hom}\big(\mathbb{F} \otimes_{\mathbb{Z}} G/G', I^{n-1}/I^n\big)$$

is a space of homomorphisms of $\mathbb{F}$-vector spaces - note that I^{n-1}/I^n is a trivial G-module - and so every homomorphism is uniquely determined by the image on a basis. The cosets of $\{g_i\}$ form such a basis. Thus there exists a unique homomorphism $\psi : G \to I^{n-1}/I^n$, extending $\psi(g_i)$. But

$$\operatorname{Hom}\big(G, I^{n-1}/I^n\big) \simeq H^1\big(G, I^{n-1}/I^n\big) \simeq H^1\big(G, 1 + I^{n-1}/I^n\big),$$

i.e., ψ gives rise to a 1-cocycle $1 + \psi$, and thus by Lemma 5 $(1 + \psi) \cdot \varrho'$ is a homomorphism. However, $(1 + \psi) \cdot \varrho'$ is uniquely determined by its values on $\{g_i\}$, and $(1 + \psi) \cdot \varrho'(g_i) = \hat{\varrho}(g_i)$, whence $\{\hat{\varrho}(g_i)\}$ extends to a unique homomorphism $\hat{\varrho} : G \to \mathbb{F}H^\times/(1 + I^n)$ as claimed. ■

We can now summarize how to find all homomorphisms $G \to \mathbb{F}H^\times/(1 + I^n)$: According to the above, we have found a test to decide which $\beta \cdot \varrho_i$ do extend. For each i, if there is an extension, choose one β_i such that $\beta_i \cdot \varrho_i$

extends. Let $\hat{\varrho}_i$ be the extended homomorphism, according to Lemma 3, stored as $\{\hat{\varrho}_i(g_j)\}$. By Lemma 5 all other homomorphisms are then given by $H^1_{\hat{\varrho} i}(G, 1 + I^m/I^n) \cdot \hat{\varrho}_i$.

We now turn to the proof of Lemma 9. We only have to verify the last statement. For this we have to analyze carefully the isomorphism $H^2_{fac}(G, I^{n-1}/I^n) \simeq \mathrm{Hom}_{FG}(\Omega^2, I^{n-1}/I^n)$ [cf. the exact sequences (20), (21), (22)]. We have the exact sequence

$$1 \to 1 + I^{n-1}/I^n \to \mathbb{F}H^\times/(1 + I^n) \to \mathbb{F}H^\times/(1 + I^{n-1}) \to 1, \quad (23)$$

and our given homomorphism $\varrho : G \to \mathbb{F}H^\times/(1 + I^{n-1})$ allows us to construct the pullback diagram with exact rows

$$\begin{tikzcd}
1 \arrow[r] & 1 + \mathrm{I}^{n-1}/\mathrm{I}^n \arrow[r] & \mathbb{F}\mathrm{H}^\times/(1 + \mathrm{I}_n) \arrow[r] & \mathbb{F}\mathrm{H}^\times/(1 + \mathrm{I}^{n-1}) \arrow[r] & 1 \\
1 \arrow[r] & 1 + \mathrm{I}^{n-1}/\mathrm{i}^n \arrow[r] \arrow[u, "\mathrm{id}"] & \mathrm{X} \arrow[r] \arrow[u, "\varrho_1"] & \mathrm{G} \arrow[r] \arrow[u, "\varrho"] & 1.
\end{tikzcd}$$

It was shown, in the construction (22) ff., that the 2-cocycle μ associated to ϱ is (modulo 2-coboundaries) exactly the factor set corresponding to the sequence (23). We also have the free resolution defined in (19),

$$1 \to R \to F \overset{\phi'}{\to} G \to 1,$$

where $\phi' : F \to G$ sends the free generators of F, say, f_i to the generators g_i of G. Since F is a free group, we obtain a commutative diagram with exact rows:

$$\begin{tikzcd}
1 \arrow[r] & R \arrow[r] \arrow[d, "\sigma'"] & F \arrow[r, "\phi'"] \arrow[d, "\tau'"] & G \arrow[r] \arrow[d, "\mathrm{id}"] & 1, \\
1 \arrow[r] & 1 + I^{n-1}/I^n \arrow[r] & X \arrow[r] & G \arrow[r] & 1.
\end{tikzcd}$$

Since $1 + I^{n-1}/I^n$ is an $F -$ module, the map σ' factors via $\overline{R}$, the relation module. Thus we get the commutative diagram with exact rows, where $\overline{F} = F/\ker(R \to \overline{R})$:

$$\begin{tikzcd}
1 \arrow[r] & \overline{R} \arrow[r] \arrow[d, "\sigma"] & \overline{F} \arrow[r, "\phi'"] \arrow[d, "\tau"] & G \arrow[r] \arrow[d, "\mathrm{id}"] & 1, \\
1 \arrow[r] & 1 + I^{n-1}/I^{n} \arrow[r] & X \arrow[r] & G \arrow[r] & 1.
\end{tikzcd}$$

LEMMA 11. *If we identify $\overline{R}$ with Ω^2 (cf. the discussion following the exact sequence* (19)*), then σ gets identified with $\Delta(\varrho)$.*

Proof. As in the exact sequence (16), $x_g \in X$ are coset representatives of $g \in G$. Then τ is defined by sending the cosets of f_i to x_i. The natural isomorphism

$$H^2_{\mathrm{fac}}(G, -) \simeq \mathrm{Ext}^2_{FG}(I(G), -)\,[GR],$$

where the second variable is an FG-module, transforms the diagram (21) to the commutative diagram with exact rows:

$$\begin{tikzcd}
1 \arrow[r] & \overline{R} \arrow[r] \arrow[d, "\sigma"] & \oplus_{i=1}^{\nu} \mathbb{F}Ge_i \arrow[r, "\phi"] \arrow[d, "\tau"] & I(G) \arrow[r] \arrow[d, "\mathrm{id}"] & 1, \\
1 \arrow[r] & 1 + I^{n-1}/I^{n} \arrow[r] & M_X \arrow[r] & I(G) \arrow[r] & 1.
\end{tikzcd}$$

Recall from (16) that ϕ sends e_i to $g_i - 1$. The exact sequence (16) then shows that we may identify $\overline{R}$ in a canonical way with Ω^2. In the above diagram M_X is the extension corresponding to the factor set μ. Thus as an F-vector space we can identify

$$M_X \quad \text{with} \quad 1 + I^{n-1}/I^{n} \oplus I(G),$$

where $1 + I^{n-1}/I^{n}$ is the old FG-module, and the G-action on M_X is as follows:

$$h \cdot (1, g - 1) = (\mu(g, h), h \cdot (g - 1)) \qquad \text{with our old 2-cocycle } \mu.$$

The map τ_1 is induced from $\tau_1 : e_i \to (1, g_i - 1)$. Then σ is the restriction of τ_1 to Ω^2. Thus we have to compute τ_1 on the generating set

$$\omega_j = \sum_{i=1}^{\nu} x_{ij} \cdot e_i, \tag{24}$$

where

$$x_{ij} = \sum_{g \in G} f_{ijg} g \in FG. \tag{25}$$

However,

$$\tau_1(\omega_j) = \sum_{i=1}^{\nu} \sum_{g \in G} f_{ijg}(g \cdot (1, g_i - 1)) = \sum_{i=1}^{\nu} \sum_{g \in G} f_{ijg}(\mu(g, g_i), g_i - 1).$$

Since the image of ω_j lies in $1 + I^{n-1}/I^n$, we conclude

$$\sigma(\omega_j) = \sum_{i=1}^{\nu} \mu(x_{ij}, g_i),$$

if we extend μ linearly. But this is exactly the formula of Lemma 8, and thus proves Lemma 10. ■

It should be noted that (24) and (25) have to be computed only once, independently of n and ϱ. For each n and ϱ one does have to compute $\mu(g,g_i)$, but only for those $g \in G$ where f_{ijg} is different from zero.

This completes the description of our algorithm, which gives, up to conjugation, all homomorphisms from G to $\mathbb{F}H^{\times}$. We conclude by noting that the reader interested only in isomorphisms from $\mathbb{F}G$ to $\mathbb{F}H$ can use Remark 2 above. Also, the algorithm allows one to start with any given homomorphism $G \to (\mathbb{F}H/I^n)^{\times}$ and determine all possible liftings $G \to \mathbb{F}H^{\times}$.

REFERENCES

1 K. W. Gruenberg and K. W. Roggenkamp, Decomposition of the augmentation ideal and of the relation modules of a finite group, *Proc. London Math. Soc.* 31:146–166 (1975); Decomposition of the relation modules of a finite group, *J. London Math .Soc.* 12:262–266 (1976).

2 M. Hall, Jr., *The Theory of Groups*, MacMillan, New York, 1959.

3 K. W. Roggenkamp, Integral representations and presentations of finite groups, in *Integral Representations* (Reiner and K. W. Roggenkamp, Eds.), Lecture Notes in Math. 744, Springer-Verlag, 1979.

4 J.-P. Serre, *Corps Locaux*, Hermann, Paris, 1968.

5 M. Wursthorn, Isomorphisms of modular group algebras: An algorithm and its application to groups of order 2^6, *J. Symbolic Comput.*, to appear.

Received 2 September 1992; final manuscript accepted 4 February 1993