Can. J. Math., Vol. XLII, No. 3, 1990, pp. 383–394

ON AUTOMORPHISMS OF COMPLETE ALGEBRAS AND THE ISOMORPHISM PROBLEM FOR MODULAR GROUP RINGS

FRANK RÖHL

1. Introduction. In [**5**], Roggenkamp and Scott gave an affirmative answer to the isomorphism problem for integral group rings of finite p-groups G and H, i.e. to the question whether $\mathbf{Z}G \xrightarrow{\sim} \mathbf{Z}H$ implies $G \xrightarrow{\sim} H$ (in this case, G is said to be characterized by its integral group ring). Progress on the analogous question with $\mathbf{Z}$ replaced by the field $\mathbf{F}_p$ of p elements has been very little during the last couple of years; and the most far reaching result in this area in a certain sense – due to Passi and Sehgal, see [**8**] – may be compared to the integral case, where the group G is of nilpotency class 2.

Based on ideas developed in [**6**], we will generalize this last result to: Let F be a free group, $M_i(F)$ the i-th dimension subgroup of F with respect to $\mathbf{F}_p$ and R a normal subgroup with $M_{n+1}(F) \subset R \subset M_n(F)$ for some n. Then F/R is characterized by $\mathbf{F}_p(F/R)$ (Actually, a slightly sharper version of this is true: see 3.1.2 for the precise statement). Passi and Sehgal's result is included as the case $n = 2$. Note further that $M_i(F) = \Pi F_{jp^k}$, where F_j is the j-th term of the lower central series of F and the product is taken over all pairs (j, k) with $jp^k \geqq i$. In particular, $F/\Pi F_{jp^k}$ is characterized by its modular group ring.

It may be worthwhile mentioning a concrete class of groups G satisfying the above criterion (the author is indebted to C. Hobby for having this pointed out to him): Let $G := \langle a_0\rangle \alpha(\langle a_1\rangle \times \langle a_2\rangle \times \langle a_3\rangle)$, all groups $\langle a_i\rangle$ of order $p \geqq 5$ and $a_i^{-1}a_0^{-1}a_ia_0 = a_{i+1}$ for $i \geqq 1$, $a_4 := 1$.

To round off our above result from a methodical point of view, we then discuss a problem raised by Sehgal, and Roggenkamp and Scott's splitting of the automorphism group of $\mathbf{Z}_pG$, $\mathbf{Z}_p$ denoting the ring of p-adic integers.

In [**8**], Problem 24 on p. 229, Sehgal asks, whether $\mathbf{F}_pG \xrightarrow{\sim} \mathbf{F}_pH$ implies $\mathbf{Z}_pG \xrightarrow{\sim} \mathbf{Z}_pH$. In view of [**5**], this would imply $G \xrightarrow{\sim} H$, and we will show here that such a p-adic isomorphism will in general not induce the original isomorphism between $\mathbf{F}_pG$ and $\mathbf{F}_pH$, demonstrating thereby that there is no "natural way" to pass from the modular to the p-adic situation.

Furthermore, although a moments reflection already reveals that decisive parts of the methods of [**5**] are not available in the modular case, one might ask, whether at least the result from which Roggenkamp and Scott derived their solution of the integral isomorphism problem, carries over resp. how it could be modified: For finite p-groups G, every automorphism of $\mathbf{Z}_pG$ is a product of an

Received April 6, 1988.

AMS (1980) subject classification: 16A27, 20C07.

inner automorphism of $\mathbf{Z}_pG$ by an automorphism of G extended to the whole of $\mathbf{Z}_pG$ (see [**5**], Ch. 2, Cor. 1).

We will show that in the modular case this is no longer true; but that a promising modification might look as follows:

Note that the decisive properties (for our purposes) of inner automorphisms are

(i) Ideals are left invariant

(ii) They induce identity on all augmentation quotients $\Delta G^n/\Delta G^{n+1}$.

Due to a counterexample given by Sandling, it does not seem to be possible to save the first property. However, the second one is still rather useful. For the sake of brevity and in view of finite dimensional algebras, let us call UAut $J :=\{\psi \in \text{Aut } J | \text{gr}\psi = Id\}$ the group of "unipotent automorphisms" of an algebra J. Our second main result (3.2.1) then reads as follows: Let J be the Magnus algebra over $\mathbf{F}_p$ of either a free group G or a finite p-group G, which is relatively-free in some variety of groups. Then

$$\text{Aut } J = \text{Aut } G \cdot \text{UAut } J.$$

This holds, in particular, for F a free group and R any product of p^k-th powers of lower central series terms such that $G := F/R$ is a finite p-group.

2. Remarks on complete algebras. For the reader's convenience, we provide a couple of facts on completions and graded algebras. Since some of them are new and of interest in their own right, they will be formulated slightly more general than necessary for use later on. Furthermore, some terminology will be introduced.

2.1 Let K be a field of arbitrary characteristic and A a K-algebra. A is filtered by its powers A^i, $i \in \mathbf{N}$, and becomes in the usual way a topological algebra. In this paper, we will be concerned only with algebras A, which are hausdorff in this A-adic topology. This amounts to the same as to say $\cap_i A^i = 0$.

The A-adic completion of A is defined by $\overline{A} := \lim_{\leftarrow} A/A^{n+1}$.

From now on, "—" denotes always the completion functor, which is exact in the following sense: For a short exact sequence

$$0 \longrightarrow I \longrightarrow A \xrightarrow{f} B \longrightarrow 0$$

of K-algebras A, B and I a (two sided) ideal of A equipped with the filtration induced from A, i.e., $I_i := I \cap A^i$, the sequence

$$\text{(2.1.1)} \quad 0 \longrightarrow \overline{I} \longrightarrow \overline{A} \xrightarrow{\overline{f}} \overline{B} \longrightarrow 0$$

is exact (see for example [**2**], p. 291); in particular, $\ker\overline{f} = \overline{\ker f}$, and if J_2 is an ideal of B, $J_1 := f^{-1}(J_2)$, one has

$$\text{(2.1.2)} \quad \overline{f}^{-1}(\overline{J}_2) = \overline{J}_1.$$

https://doi.org/10.4153/CJM-1990-021-9 Published online by Cambridge University Press

By construction of inverse limits, there exist projections $\overline{A} \longrightarrow A/A^n$ for all $n \in \mathbf{N}$, whose kernel turns out to be $\overline{A}^n$. Thus, we may identify A/A^n with $\overline{A}/\overline{A}^n$. For the associated graded algebra

$$\mathrm{gr}\overline{A} := \bigoplus_{i \geqq 1} \overline{A}^i/\overline{A}^{i+1}$$

this identification implies $\mathrm{gr}_n\overline{A} := A^n/A^{n+1} = \mathrm{gr}_n A$, hence $\mathrm{gr}\overline{A} = \mathrm{gr}A$.

Furthermore, the $\overline{A}$-adic topology on $\overline{A}$ coincides with the completion topology, i.e. the topology inherited from $\Pi_i A/A^i \supset \overline{A}$. Hence, completions are complete. Since for a finite p-group G the augmentation ideal ΔG of $\mathbf{F}_p G$ is nilpotent, one has $\Delta G = \overline{\Delta G}$.

2.2. Is there a less trivial way to consider $\overline{A}$ as a completion of some other algebra than $\overline{A}$ itself? To answer this question (and for later applications), let us introduce "Burnside systems" of $\overline{A}$: Let $a_i \in \overline{A}$, $i \in I$, be such that $(a_i + \overline{A}^2)_{i \in I}$ forms a K-vectorspace base of $\overline{A}/\overline{A}^2$. Then $(a_i)_{i \in I}$ is called a Burnside system of $\overline{A}$ (because of the Burnside Basis Theorem for groups).

Since each Burnside system of $\overline{A}$ yields one of $\overline{A}/\overline{A}^n$, an easy limit argument gives

LEMMA 2.2.1. *As a complete algebra, $\overline{A}$ is generated by each of its Burnside systems.*

Thus, we may interpret a given complete algebra $\overline{A}$ as the completion of a subalgebra generated by a Burnside system.

It is well-known that $\overline{A}$ is a Jacobson-radical algebra and that therefore $\overline{A}$ forms a group $(\overline{A}, \circ)$ under the circle composition

$$x \circ y := x + y + xy.$$

Let G be a subgroup of $(\overline{A}, \circ)$ generated by a Burnside system $(a_i)_{i \in I}$ of $\overline{A}$. Denote by $M_2(G)$ the second dimension subgroup of G with respect to K and by ΔG the augmentation ideal of the group ring KG. One then has

PROPOSITION 2.2.2.

(i) $G \cap \overline{A}^2 = M_2(G)$

(ii) $G/M_2(G) \otimes_{\mathbf{Z}} K \xrightarrow{\sim} \overline{A}/\overline{A}^2$.

Proof. The inclusion "$\supset$" in (i) holds always for subgroups of circle groups. We are going to establish the reverse inclusion.

Let F be a group freely generated by $(f_i)_{i \in I}$. The map $f_i \longmapsto a_i$ for all $i \in I$ extends to a surjective homomorphism $\pi : F \longrightarrow G$ and still further to a homomorphism of the group rings of F and G over K. This gives

https://doi.org/10.4153/CJM-1990-021-9 Published online by Cambridge University Press

$$
(2.2.3)\qquad
\begin{array}{ccccc}
F & \longrightarrow & G & \xhookrightarrow{\text{incl.}} & A \\
\delta\downarrow & /\!/\!/ & \delta\downarrow & /\!/\!/ \;\nearrow & \\
\Delta F & \longrightarrow & \Delta G & &
\end{array}
$$

where the maps δ are given by $\delta(x) := x - 1$.

For char $K = p$, one has $M_2(F) = F_2 \cdot F^p$, where F_2 is the commutator subgroup of F. Since the second dimension subgroup of F with respect to $\mathbf{Z}$ is F_2, and F/F_2 is an abelian group free on $(f_iF_2)_{i\in I}$, one obtains for char $K = 0$

$$M_2(F) = \{f \in F \mid \exists\, n \in \mathbf{N} : f^n \in F_2\} = F_2.$$

In both cases, $(f_iM_2(F))_{i\in I}$ forms a base of the $\mathbf{F}_p$-resp. $\mathbf{Z}$-module $F/M_2(F)$.

By the definition of dimension subgroups, the map $F/M_2(F) \longrightarrow \Delta F/\Delta F^2$ (resp. $G/M^2(G) \longrightarrow \Delta G/\Delta G^2$) induced by δ is injective. (2.2.3) now induces

$$
(2.2.4)\qquad
\begin{array}{ccccccc}
 & & F/M_2(F) & \longrightarrow & G/M_2(G) & \longrightarrow & \overline{A}/\overline{A}^2 \\
 & \swarrow\; /\!/\!/ & \hookdownarrow & /\!/\!/ & \hookdownarrow & /\!/\!/\;\nearrow & \\
F/M_2(F)\otimes_{\mathbf{Z}} K & \xrightarrow{\sim} & \Delta F/\Delta F^2 & \longrightarrow & \Delta G/\Delta G^2 & &
\end{array}
$$

As we have seen above, $F/M_2(F) \otimes_{\mathbf{Z}} K$ is a K-vector space with base $(f_iM_2(F) \otimes 1)_{i\in I}$, and the resulting isomorphism

$$F/M_2(F) \otimes_{\mathbf{Z}} K \xrightarrow{\sim} \overline{A}/\overline{A}^2$$

makes all the maps of the bottom row of (2.2.4) ending at $\overline{A}/\overline{A}^2$ isomorphisms. In particular, the maps of the top row are injective. This gives $\overline{A}^2 \cap G \subset M_2(G)$, and (ii) is also clear by now. □

The significance of (2.2.2) lies in the fact that for these groups G the rank of G, i.e. the number of elements in a minimal generating system, equals the rank of $G/M_2(G)$ – a condition, which will be of importance for the following investigations.

The examples of complete algebras, which will concern us most in the sequel, are obtained by completing the augmentation ideal ΔG of a modular group ring KG: G is residually nilpotent – hausdorff in our terminology – if and only if

G is residually a "nilpotent p-group of bounded exponent" (see [**4**], 2.26 Thm. on p. 90). These are precisely the groups of residually "finite M-length": Let $M_i(G)$ be the i-th dimension subgroup of G with respect to K, then G is said to be of M-length n, if $M_n(G) \neq 1 = M_{n+1}(G)$. By (2.2.2) (ii), in this situation G is – as a group – generated by a Burnside system of $\overline{\Delta G}$, and this is already a minimal generating system of G. Conversely, every minimal generating system of G is a Burnside system of $\overline{\Delta G}$, because G is of finite M-length.

3. Automorphisms of complete algebras and applications. In this section, we generalize the automorphism lifting principle of [**6**] and discuss the automorphism groups of certain group rings with respect to questions related to the modular isomorphism problem.

3.1. We start by lifting automorphisms.

PROPOSITION 3.1.1. *Let K be an arbitrary field, $\overline{A}$ a K-algebra, which is complete and hausdorff in its $\overline{A}$-adic topology. Let $(a_i)_{i\in I}$ be a Burnside system of $\overline{A}$ and F the free group on $(f_i)_{i\in I}$. Then the following hold:*

(i) Every endomorphism of $\overline{A}$ is induced by an endomorphism of $\overline{\Delta F}$, i.e., for $\gamma \in \mathrm{End}\ \overline{A}$ there exists $\Gamma \in \mathrm{End}\ \overline{\Delta F}$ such that

$$\begin{array}{ccc} \overline{\Delta F} & \xrightarrow{\ \Gamma\ } & \overline{\Delta F} \\ {\scriptstyle\delta}\downarrow & /\!/\!/ & {\scriptstyle\delta}\downarrow \\ \overline{A} & \xrightarrow[\ \gamma\ ]{} & \overline{A}, \end{array}$$

where $\overline{\Delta F} \longrightarrow \overline{A}$ is obtained by extension of $f_i \longmapsto a_i$ for all $i \in I$.

(ii) The automorphisms of $\overline{A}$ are induced by automorphisms of $\overline{\Delta F}$, and the analogue applies to unipotent automorphisms.

Proof. Let G be the subgroup of $(\overline{A}, \circ)$ generated by $(a_i)_{i\in I}$ and A the subalgebra generated by the same elements. The map $f_i \longmapsto a_i$ extends to a homomorphism $F \xrightarrow{\pi} G \subset A$, giving thus a short exact sequence

$$0 \longrightarrow J \longrightarrow \Delta F \xrightarrow{\pi} A \longrightarrow 0,$$

(J being just the kernel of $\Delta F \longrightarrow A$). This sequence remains exact under completions, and by (2.2.1), we are allowed to identify the completion of A with our original $\overline{A}$. Thus

$$0 \longrightarrow \overline{J} \longrightarrow \overline{\Delta F} \xrightarrow{\overline{\pi}} \overline{A} \longrightarrow 0$$

https://doi.org/10.4153/CJM-1990-021-9 Published online by Cambridge University Press

is exact, and we may assume $\overline{A} = \overline{\Delta F}/\overline{J}$.

Let γ be an endomorphism of $\overline{A}$ with $\gamma(a_i) = y_i$ for $i \in I$. If $x_i \in \overline{\Delta F}$ is such that $\overline{\pi}(x_i) = y_i$, let

$$\Gamma\overline{\delta}(fi) : = x_i.$$

Γ then extends in the usual way to an endomorphism of $\overline{\Delta F}$.

By construction of Γ, the diagram in (3.1.1) is clearly commutative, once we have shown that Γ leaves $\overline{J}$ invariant. Since Γ is continuous, it is sufficient to check $\Gamma(J) \subset \overline{J}$. So let $x \in J$. Then $\gamma(x + \overline{J}) = \overline{J}$, and since Γ is an endomorphism of algebras,

$$\Gamma(x) + \overline{J} = \gamma(x + \overline{J}).$$

(As an element of ΔF, x can be written as a finite sum of products of finitely many f_i's!) This establishes (i).

The considerations following (2.2.4) have already shown $\overline{\Delta F}/\overline{\Delta F}^2 \xrightarrow{\sim} \overline{A}/\overline{A}^2$, and this isomorphism was induced by $\overline{\pi}$. Because of $\mathrm{gr}_1\gamma \in \mathrm{Aut}\ \overline{A}/\overline{A}^2$, we thus obtain $\mathrm{gr}_1\Gamma \in \mathrm{Aut}\ \overline{\Delta F}/\overline{\Delta F}^2$. We are going to show that this implies $\mathrm{gr}\Gamma \in \mathrm{Aut}\ \mathrm{gr}\overline{\Delta F}$.

Let Γ' be a lifting of γ^{-1}. Since $\overline{\Delta F}/\overline{\Delta F}^2 \xrightarrow{\sim} \overline{A}/\overline{A}^2$, one has $\mathrm{gr}_1\Gamma' = (\mathrm{gr}_1\Gamma)^{-1}$. Multiplication in $\overline{\Delta F}$ provides a mapping ($\otimes^n$ denoting the n-fold tensor product over K)

$$\otimes^n \overline{\Delta F}/\overline{\Delta F}^2 \twoheadrightarrow \overline{\Delta F}^n/\overline{\Delta F}^{n+1},$$

and we obtain

$$\begin{array}{ccccc}
\otimes^n \overline{\Delta F}/\overline{\Delta F}^2 & \xrightarrow{\otimes^n \mathrm{gr}_1\Gamma} & \otimes^n \overline{\Delta F}/\overline{\Delta F}^2 & \xrightarrow{\otimes^n \mathrm{gr}_1\Gamma'} & \otimes^n \overline{\Delta F}/\overline{\Delta F}^2 \\
\downarrow & /\!/ & \downarrow & /\!/ & \downarrow \\
\overline{\Delta F}^n/\overline{\Delta F}^{n+1} & \xrightarrow[\mathrm{gr}_n\Gamma]{} & \overline{\Delta F}^n/\overline{\Delta F}^{n+1} & \xrightarrow[\mathrm{gr}_n\Gamma']{} & \overline{\Delta F}^n/\overline{\Delta F}^{n+1}
\end{array}$$

Since the maps of the top row compose to give the identity, the same applies to the maps of the bottom row. Hence, $\mathrm{gr}_n\Gamma' \cdot \mathrm{gr}_n\Gamma = Id$, and – by symmetry – the same holds the other way round so that $\mathrm{gr}\Gamma \in \mathrm{Aut}\ \mathrm{gr}\overline{\Delta F}$. If one starts already with $\mathrm{gr}_1\Gamma = Id$, then the left half of the above diagram shows that $\mathrm{gr}\Gamma = Id$. Thus, Γ is unipotent, if γ is.

Now, $\mathrm{gr}\Gamma \in \mathrm{Aut}\ \mathrm{gr}\overline{\Delta F}$ implies inductively that Γ induces an automorphism on each quotient $\overline{\Delta F}/\overline{\Delta F}^n$. Since $\overline{\Delta F}$ is hausdorff, Γ is injective. But Γ is also surjective: Let $x = \sum x_j + \Delta F^{j+1} \in \overline{\Delta F}$, the $x_j \in \Delta F^j$. Then there exists $y_j \in \Delta F^j$ with

$$x_j + \Delta F^{j+1} = \mathrm{gr}_j \Gamma(y_j + \Delta F^{j+1}) \text{ and}$$

$$x = \sum \mathrm{gr}_j \Gamma(y_j + \Delta F^{j+1}) = \Gamma(\sum y_j + \Delta F^{j+1}).$$

Obviously, $\sum y_j + \Delta F^{j+1}$ converges and is therefore contained in $\overline{\Delta F}$. □

Note that the proof shows: An endomorphism Γ of $\overline{\Delta F}$ with $\mathrm{gr}_1 \Gamma = Id$ is unipotent. And clearly the same holds true for endomorphisms of $\overline{A}$ instead of $\overline{\Delta F}$.

Before we can give our main application of this theorem to the isomorphism problem for modular group rings, we have to say, what is meant by "a group G is characterized by $\mathbf{F}_p G/\Delta G^{n+1}$": Let H be any group of the same (finite) M-length as of G. If the M-length of G does not exceed n, and if $\mathbf{F}_p G/\Delta G^{n+1} \xrightarrow{\sim} \mathbf{F}_p H/\Delta H^{n+1}$ implies $G \xrightarrow{\sim} H$, we say that G is characterized by $\mathbf{F}_p G/\Delta G^{n+1}$. Clearly, that this implies G to be characterized by $\mathbf{F}_p G$, because $\mathrm{gr} G \xrightarrow{\sim} \mathrm{gr} H$.

THEOREM 3.1.2. *Let F be a free group, R a normal subgroup with $M_{n+1}(F) \subset R \subsetneqq M_n(F)$, where $M_i(F)$ is the i-th dimension subgroup of F with respect to F_p. Then F/R is characterized by $\mathbf{F}_p(F/R)/\Delta(F/R)^{n+1}$.*

Remark. In general it is a rather difficult task to decide, whether a given "concrete" group has a system of generators and relators satisfying the conditions of 3.1.2. Hence it might not be such a good idea to use 3.1.2. as a criterion; but rather it provides a class of "concrete" – in a different way – examples: Taking $R = M_n(F)$, 3.1.2 says that the free groups of those varieties of all groups of M-length n are characterized by their modular group algebra; and the same holds for groups of such varieties, which are "sufficiently close" to being free in this variety.

Before we turn to the proof, we look at a special case and a class of examples of groups G, which – by means of the Theorem – are characterized by their modular group ring:

(1) let G be a group with $M_3(G) = 1$, and let $(g_i)_{i \in I}$ be such that $(g_i M_2(G))_{i \in I}$ forms a vectorspace base of $G/M_2(G)$. Then G is generated by $(g_i)_{i \in I}$, and if F is free on $(f_i)_{i \in I}$, then $f_i \longmapsto g_i$ extends to a surjective homomorphism $\pi : F \longrightarrow G$. Moreover, $\ker \pi \subset M_2(F)$, because of the isomorphism $F/M_2(F) \xrightarrow{\sim} G/M_2(G)$ induced by π. Since $M_3(G) = 1$, we have $M_3(F) \subset \ker \pi$. (3.1.2) implies that $F/\ker \pi$ resp. G is characterized by $\mathbf{F}_p G$, which is precisely the content of Cor. 6.25 (see [**8**], p. 117).

(2) let $G := \langle a_0 \rangle \alpha(\langle a_1 \rangle \times \langle a_2 \rangle \times \langle a_3 \rangle)$, all groups $\langle a_i \rangle$ of prime order $p \geqq 5$, $(a_i, a_0) := a_i^{-1} a_0^{-1} a_i a_0 = a_{i+1}$ for $i \geqq 1$ and $a_4 := 1$. G then has order p^4, thus

$G_4 = 1$. Furthermore, since $(a_2, a_0) = a_3, G_3 \neq 1$. With $a := a_0$ and $b := a_1$, it is easy to see that $G = \langle a, b | a^p = b^p = (a, ((b, a), a)) = (b, ((b, a), a)) = (b, (b, a)) = 1\rangle$. Let F be free on a and b and $\pi : F \longrightarrow G$ the obvious map. Then $\ker \pi \subsetneq M_3(F)$, since $M_3(G) = G_3 G^p \neq 1$; and $p \geqq 5$ implies $G^p = 1$; hence, $\ker \pi \supset M_4(F) = F_4 F^p$.

The basic idea of the following proof is the same as in the integral case: Let $G := F/R$ and H a group with $\Delta G/\Delta G^{n+1} = \Delta H/\Delta H^{n+1}$ (since $\mathbf{F}_p G/\Delta G^{n+1}$ is an augmented K-algebra, we may assume that the isomorphism $\mathbf{F}_p G/\Delta G^{n+1} \xrightarrow{\sim} \mathbf{F}_p H/\Delta H^{n+1}$ is augmented so that we are allowed to identify the above mentioned augmentation ideal quotients). We proceed by induction on n: An automorphism of $\Delta G/\Delta G^n$ carrying the image of G onto the image of H in $\Delta H/\Delta H^n$ will then be lifted to an automorphism of $\overline{\Delta F}$, which finally induces the desired automorphism on $\Delta G/\Delta G^{n+1}$.

But the technicalities are harder, as is already apparent from the sketch of the basic idea. In order to survive among too many maps, we are forced to identify naturally isomorphic objects as often as possible. The verification that we are indeed allowed to do so are straightforward and left to the reader. Furthermore, there are several maps, which won't be given a name. For example, we will talk very often about "the image of G in some homomorphic image B of ΔG". It is to be understood that we mean a homomorphism of G into B induced by $\delta : G \longrightarrow \Delta G$ with $\delta(g) := g - 1$.

Proof. With the above notations, let $\Delta G/\Delta G^{n+1} = \Delta H/\Delta H^{n+1}$. By induction on n, we will show the existence of a unipotent automorphism carrying the iamge of G onto the image of H. Note that since $M_{n+1}(F) \subset R$, G embeds into $\Delta G/\Delta G^{n+1}$, and since G and H have the same M-length, they will be isomorphic.

Let $n = 1$. Then everything is clear because of

$$G \xrightarrow{\sim} \Delta G/\Delta G^2 = \Delta H/\Delta H^2 \xleftarrow{\sim} H.$$

So let us assume that $F/M_n(F)$ for $n \geqq 2$ is characterized by $\mathbf{F}_p(F/M_n(F))/\Delta(F/M_n(F))^n$ by means of unipotent automorphisms. $\Delta G/\Delta G^{n+1} = \Delta H/\Delta H^{n+1}$ implies $\Delta G/\Delta G^n = \Delta H/\Delta H^n$, and because of $M_n(F/R) = M_n(F)R/R = M_n(F)/R$, one has

$$G/M_n(G) = (F/R)/M_n(F/R) = F/M_n(F).$$

Hence.

$$\Delta(F/M_n(F))/\Delta(F/M_n(F))^n = \Delta H/\Delta H^n,$$

and by inductive hypothesis, there exists a unipotent automorphism γ'' carrying the images of the groups onto each other.

Let Γ be a unipotent lifting of γ'' to $\overline{\Delta F}$. With the extension $\overline{\pi} : \overline{\Delta F} \longrightarrow \overline{\Delta G}$ of the natural map $\pi : F \longrightarrow G$, one obtains according to (2.1.2)

$$\overline{\pi}^{-1}(\overline{\Delta G}^{n+1}) = \overline{\Delta F^{n+1} + \Delta(F,R)},$$

$\Delta(F,R)$ denoting the kernel of $\pi : \Delta F \longrightarrow \Delta G$. Because of $R \subset M_n(F)$, one has

$$\overline{\Delta F}^{n+1} \subset \overline{\Delta F^{n+1} + \Delta(F,R)} \subset \overline{\Delta F}^{n},$$

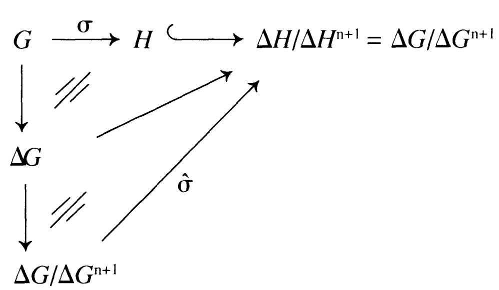
and since Γ is unipotent, $\overline{\Delta F^{n+1} + \Delta(F,R)}$ remains invariant under Γ. Thus, Γ induces a unipotent automorphism γ' on $\Delta G/\Delta G^{n+1}$.

The image of $M_n(G)$ in $\Delta G/\Delta G^{n+1}$ is a vectorsubspace of $\Delta G^n/\Delta G^{n+1}$, and as such, it admits a vectorspace complement C. Since the images of gr G and gr H in gr $\Delta G/\Delta G^{n+1}$ coincide (same proof as for ΔG), C is a complement of the image of $M_n(H)$ in $\Delta H^n/\Delta H^{n+1}$, too. Moreover, being annihilated by $\Delta G/\Delta G^{n+1}$, C is already an ideal. Thus, in $A := (\Delta G/\Delta G^{n+1})/C$, the images of $M_n(G)$ and $M_n(H)$ coincide; by the choice of C, one still has embeddings $G \hookrightarrow (A, \circ)$ and $H \hookrightarrow (A, \circ)$; and thus

(3.1.3) $A^n = M_n(G) = M_n(H)$.

As a unipotent automorphism of $\Delta G/\Delta G^{n+1}$, γ' leaves C invariant and induces therefore an automorphism γ on A. The natural isomorphism $A/A^n \xrightarrow{\sim} \Delta G/\Delta^n$ shows that the automorphism induced by γ on $\Delta G/\Delta G^n$ is the same as our original γ''. (3.1.3) makes it then clear that γ sends the image of G in A isomorphically onto the image of H in A, and by restricting γ, we have constructed an isomorphism $\sigma : G \xrightarrow{\sim} H$.

σ can now be extended via



to an endomorphism $\hat{\sigma}$ of $\Delta G/\Delta G^{n+1}$.

Because of $\mathrm{gr}_1 G \xrightarrow{\sim} \mathrm{gr}_1 \Delta \xrightarrow{\sim} \mathrm{gr}_1 A$ and since σ is a restriction of γ, one obtains $\mathrm{gr}_1\hat{\sigma} = \mathrm{gr}_1\gamma = Id$, and this implies that $\hat{\sigma}$ is a unipotent automorphism of $\Delta G/\Delta G^{n+1}$. $\square$

3.2. We now turn to the structure of the automorphism group of certain completed group rings.

Let G be a relatively-free group of finite M-length with respect to some prime p, or a free group. Then G possesses a system of free generators $(g_i)_{i\in I}$ in the sense that every map $(g_i)_{i\in I} \longrightarrow G$ can be extended to an endomorphism of G (see [**3**] Ch. I.3, p. 9), and this system forms already a Burnside system of $\overline{\Delta G}$.

THEOREM 3.2.1. *Under the above conditions, with* ΔG *the augmentation ideal of* $\mathbf{F}_pG$,

$$\text{Aut } \overline{\Delta G} = \text{Aut } G \cdot \text{UAut } \overline{\Delta G}.$$

Proof. $\psi \in \text{Aut } \overline{\Delta G}$ induces an automorphism of $\overline{\Delta G}/\overline{\Delta G}^2$, and since this quotient is isomorphic to $G/M_2(G)$, we obtain an automorphism of $G/M_2(G)$ from ψ. Since G is realtively-free, and a lifting of a base of $G/M_2(G)$ to G is a set of free generators, this automorphism lifts to an endomorphism τ of G, which can be extended to an endomorphism $\bar{\tau}$ of $\overline{\Delta G}$. Note that $\text{gr}_1\bar{\tau} = \text{gr}_1\psi$.

Since ψ is an automorphism, ψ^{-1} exists, and it is easily seen that $\text{gr}_1(\psi^{-1}\cdot\bar{\tau}) = Id$. But then $gr(\psi^{-1}\cdot\bar{\tau}) = Id$, and for $\varphi := \psi^{-1}\cdot\bar{\tau}$, one has $\varphi \in \text{UAut } \overline{\Delta G}$. Obviously, $\bar{\tau}$, too, has to be an automorphism. □

Remarks. 1. Inducing automorphisms on $\overline{\Delta G}/\overline{\Delta G}^2$ defines a homomorphism $\text{Aut } \overline{\Delta G} \longrightarrow \text{Aut } \overline{\Delta G}/\overline{\Delta G}^2$, whose kernel is precisely $\text{UAut } \overline{\Delta G}$, showing thereby the normality of $\text{UAut } \overline{\Delta G}$ in $\text{Aut } \overline{\Delta G}$. Furthermore, since every automorphism of $\overline{\Delta G}/\overline{\Delta G}^2$ can be lifted to an automorphism of $\overline{\Delta G}$ by the relative-freeness of G, the above homomorphism is surjective.

2. Since every automorphism of the Magnus algebra $\mathbf{F}_p \oplus \overline{\Delta G}$ is augmented, the splitting given in (3.2.1) applies to $\text{Aut } (\mathbf{F}_p \oplus \overline{\Delta G})$, too.

3. Since quotients of a free group by a verbal subgroup are relatively-free, this splitting holds in particular for $G := F/\Pi F_{ip^{k_i}}$, $k_1 \geqq 1$, all other $k_i \geqq 0$, and thus for elementary abelian p-groups (but see the following "counterexample").

Stronger than in (3.2.1), Roggenkamp and Scott have shown

$$\text{Aut } \mathbf{Z}_pG = \text{Aut } G \cdot \text{Inn}\, \mathbf{Z}_pG$$

for finite p-group G (see [**5**]). The question arises, whether this holds also in the modular case.

Counterexample. Let F be a group freely generated by $(f_i)_{i\in I}$ and $p > 2$ a prime. Then $G := F/M_2(F)$, where $M_2(F)$ is taken with respect to p, is an $\mathbf{F}_p$-vectorspace and certainly relatively-free such that (3.2.1) holds for $\text{Aut } \overline{\Delta G}$, $\Delta G \subset \mathbf{F}_pG$. For $g_i := f_iM_2(F)$ for $i \in I$, choose any elements $x_i \in \Delta G^2$, not all equal to 0, and let H be the subgroup of $(\overline{\Delta G}, \circ)$ generated by the $\delta(g_i)\circ x_i$, $i \in I$.

Then H forms a base of ΔG: Since linear combinations of the $\delta(g_i)\circ x_i$'s involve only finitely many (g_j)'s ($x_i \in \Delta G$!), it is sufficient to check this for G finitely generated. But $x^p = 0$ for all $x \in \Delta G$ implies that H, too, is an elementary abelian p-group, and as $\mathbf{F}_p$-vectorspaces $\dim H = \dim G$. Since $H \xrightarrow{\sim} \Delta G/\Delta G^2$, H generates ΔG; hence the result. Moreover, $H \neq \delta G$, because $\delta G \cap \Delta G^2 = 0$ by $M_2(G) = 1$ and (2.2.2), and certainly, $G \xrightarrow{\sim} H$.

The automorphism of $\overline{\Delta G}$ defined by $G \xrightarrow{\sim} H$ cannot split into a product of an extended automorphism of G by an inner automorphism of $\overline{\Delta G}$ (which in our situation are all equal to the identity), because $\delta G \neq H$.

A special case of the above example was pointed out to the author by R. Sandling in a private communication, where it was used as an example for the lack of ideal correspondence in the modular case (the interested reader may consider the ideal J generated by $\delta(g_1)$, choose any $x_1 \neq 0$ from ΔG^2 and put all other $x_i = 0$. Then $J \cap H = 0$, because $H \cap \Delta G^2 = 0$).

The reason why we were not satisfied with a cyclic group in the above example is the following

COROLLARY 3.2.2. *For all free groups F* $\mathrm{Aut}\ \overline{\Delta F} \supsetneq \mathrm{Aut}\ F \cdot \mathrm{Inn}\,\overline{\Delta F}$.

Proof. Let F be free and G and H as in the above example. Then the automorphism of $\overline{\Delta G}$ coming from the isomorphism $G \xrightarrow{\sim} H$ can be lifted to an automorphism Γ of $\overline{\Delta F}$.

Suppose, $\Gamma = \Gamma_1 \cdot \Gamma_2$ with $\Gamma_1 \in \mathrm{Aut}\ F$ and $\Gamma_2 \in \mathrm{Inn}\,\overline{\Delta F}$. As an inner automorphism, Γ_2 leaves the kernel of the natural map $\Delta F \longrightarrow \Delta G$ invariant. Because this holds trivially for Γ, the same must be true for Γ_i. But then $\Gamma_i \in \mathrm{Aut}\ F$ induces already an automorphism of G, and the splitting $\Gamma = \Gamma_1 \cdot \Gamma_2$ boils down to a splitting of the automorphism induced on ΔG by $G \xrightarrow{\sim} H$, which cannot hold, as we have just seen. □

In the same spirit, we are now going to show that in general not every isomorphism $\mathbf{F}_pG \xrightarrow{\sim} \mathbf{F}_pH$ is induced by an isomorphism $\mathbf{Z}_pG \xrightarrow{\sim} \mathbf{Z}_pH$ (this contributes to a problem raised by Sehgal; see [**8**], Problem 24 on p. 229).

Assume the contrary. We may identify $\mathbf{F}_pG = \mathbf{F}_pH$ and also $\mathbf{Z}_pG = \mathbf{Z}_pH$, and the assertion now becomes: Every automorphism of $\mathbf{F}_pG$ lifts to an automorphism of $\mathbf{Z}_pG$. Because of

$$\mathrm{Aut}\ \mathbf{Z}_pG = \mathrm{Aut}\ G \cdot \mathrm{Inn}\,\mathbf{Z}_pG$$

for finite p-groups G, this splitting would induce

$$\mathrm{Aut}\ \mathbf{F}_pG = \mathrm{Aut}\ G \cdot \mathrm{Inn}\,\mathbf{F}_pG,$$

since $p \cdot \mathbf{Z}_pG$ is a fully invariant ideal of $\mathbf{Z}_pG$. But our example shows that this is not true.

References

1. B. Huppert and N. Blackburn, *Finite groups II*, Springer 1982

2. C. Năstăsescu and F. van Oystayen, *Graded ring theory*, North-Holland 1982

3. H. Neumann, *Varieties of groups*, Springer 1967

4. I. B. S. Passi, *Group rings and their augmentation ideals*, Springer LNM 715, 1979

5. K. W. Roggenkamp and L. Scott, *Isomorphisms of p-adic group rings*, Ann. Math. *126* (1987), 593–647

6. F. Röhl, *On the isomorphism problem for group rings and completed augmentation ideals*, Rocky Mountain J. Math. *17*, No 4 (1987), 853–863

7. R. Sandling, *The isomorphism problem for group rings: a survey* in *Orders and their applications*, Springer LNM 1142, 1985

8. S. K. Sehgal, *Topics in group rings*, Marcel Dekker 1978

Department of Mathematics
The University of Alabama
Tuscaloosa, Al 35487, USA

https://doi.org/10.4153/CJM-1990-021-9 Published online by Cambridge University Press