PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 131, Number 12, Pages 3657–3664
S 0002-9939(03)06974-0
Article electronically published on February 28, 2003

# $n$-INNER AUTOMORPHISMS OF FINITE GROUPS

FERNANDO SZECHTMAN

(Communicated by Stephen D. Smith)

Abstract. We refer to an automorphism $g$ of a group $G$ as $n$-inner if given any subset $S$ of $G$ with cardinality less than $n$, there exists an inner automorphism of $G$ agreeing with $g$ on $S$. Hence $g$ is 2-inner if it sends every element of $G$ to a conjugate. New examples are given of outer $n$-inner automorphisms of finite groups for all natural numbers $n \geq 2$.

## 1. Introduction

We refer to an automorphism $g$ of a group $G$ as $n$-inner if given any subset $S$ of $G$ with cardinality less than $n$, there exists an inner automorphism of $G$ agreeing with $g$ on $S$. Accordingly, $g$ is 2-inner if it is class-preserving. Examples of finite groups possessing class-preserving outer automorphisms were given by W. Burnside [Bur13], G. E. Wall [Wal47], C. H. Sah [Sah68], and M. Hertweck [Her01a], among others. B. H. Neumann [Neu81] produced outer $n$-inner automorphisms of finite groups for all natural numbers $n \geq 2$.

We present a generic construction to produce outer $n$-inner automorphisms. Concrete examples—arising from Linear Algebra—are exhibited.

One motivation is the recent use of class-preserving automorphisms in the area of group rings. For the benefit of the reader we briefly outline some of these applications. Let $G$ be a finite group, and let $R$ be an integral domain of characteristic 0 such that no divisor of $|G|$ is invertible. Given an automorphism $\tau$ of $G$, consider the polycyclic group $G_\tau = G \rtimes_\tau \langle c \rangle$, where $c$ has infinite order and acts on $G$ via $\tau$. M. Mazur [Maz95] proved that $G_\tau \cong G_{\mathrm{id}}$ if and only if $\tau$ is inner, and $RG_\tau \cong RG_{\mathrm{id}}$ if and only if $\tau$ becomes inner in $RG$. (Note that the later condition implies $\tau$ is class-preserving.) By exploiting this idea and suitably choosing a class-preserving outer automorphism, K. W. Roggenkamp and A. Zimmermann [RZ95] found a semilocal counterexample for the isomorphism problem of infinite polycyclic groups. M. Hertweck [Her01b] finally constructed a global counterexample to the normalizer and isomorphism problem for integral group rings of finite groups. Class-preserving automorphisms are also relevant in connection with a conjecture of Zassenhaus about the structure of automorphisms of integral group rings of finite groups; cf. [KR93].

Received by the editors March 6, 2002 and, in revised form, July 10, 2002.
2000 *Mathematics Subject Classification.* Primary 20D45, 20E36.

## 2. The construction

Let $\mathcal{X} \subseteq \mathcal{Y}$ be families of functions, all of which have common domain $D$. Given a natural (or cardinal) number $n$, the $n$-envelope $\mathcal{X}_n$ of $\mathcal{X}$ in $\mathcal{Y}$ consists of all $g \in \mathcal{Y}$ satisfying: given any subset $S$ of $D$ with cardinality less than $n$, there exists $f \in \mathcal{X}$ agreeing with $g$ on $S$. The interesting case occurs when $\mathcal{X}$ is properly contained in $\mathcal{X}_n$.

What concerns us here is the following group theoretical setting: $D = G$ (an arbitrary group), $\mathcal{X} = I(G)$ (the group of inner automorphisms of $G$) and $\mathcal{Y} = A(G)$ (the group of automorphisms of $G$). Observe that $I(G)_n$ is comprised of all $n$-inner automorphisms. In particular, $I(G)_2$ consists of all class-preserving automorphisms. It is readily verified that every $I(G)_n$ is a normal subgroup of $A(G)$. Thus $A(G)$ contains a descending chain of normal subgroups $A(G) = I(G)_1 \supseteq I(G)_2 \supseteq \cdots$, all of which contain $I(G)$. Let us write $O(G)_n$ for the quotient group $I(G)_n/I(G)$. Our aim is to construct, for all natural numbers $n \geq 2$, finite groups $G$ satisfying $O(G)_n \neq 1$. When $n = 2$ this means that $G$ has class-preserving automorphisms that are not inner.

Let $M$ be an abelian group. We have an action of $End(M)$ on $M^2$, given by

$$^f(x, y) = (x, f(x) + y), \quad f \in End(M),\ x, y \in M.$$

This action defines the semidirect product group $M^2 \rtimes End(M)$. Let $E$ be a subgroup of $End(M)$. Associated to $E$ we have the following normal subgroup of $M^2 \rtimes End(M)$:

$$G(E) = M^2 \rtimes E.$$

Given $g \in End(M)$, consider the automorphism $\Delta(g)$ of $G(E)$ obtained via conjugation by $(0, 0, g) \in M^2 \rtimes End(M)$. This yields a group embedding $\Delta : End(M) \to A(G(E))$ defined by

$$\begin{aligned}\Delta(g)(x, y, f) &= {}^{(0,0,g)}(x, y, f)\\ &= (x, y, f)(0, g(x), 0), \quad g \in End(M),\ f \in E,\ x, y \in M.\end{aligned}$$

It is readily verified that $\Delta(g) \in I(G(E))$ if and only if $g \in E$, and $\Delta(g) \in I(G(E))_n$ if and only if $g \in E_n$, the $n$-envelope of $E$ in $End(M)$. Hence for each $n$ there is a group embedding $\Delta_n : E_n/E \to O(G(E))_n$, given by

$$\Delta_n([g]) = [\Delta(g)], \quad g \in E_n.$$

We have proven

2.1. **Theorem.** *If $E_n/E \neq 0$, then $O(G(E))_n \neq 1$.*

In what follows $M$ is an $R$-module for a suitable ring $R$, and $End(M)$ is the set of all $R$-endomorphisms of $M$.

### The special linear Lie algebra.

2.2. **Example.** Let $V$ be a vector space of dimension $n > 1$ over a finite field $F_q$. Denote by $\mathfrak{sl}(V)$ the set of $F_q$-endomorphisms of $V$ having trace 0. Then $G(\mathfrak{sl}(V))$ is a finite group of order $q^{n^2+2n-1}$ satisfying $O(G(\mathfrak{sl}(V)))_n \neq 1$.

*Proof.* $\mathfrak{sl}(V)$ is properly contained in $\mathfrak{sl}(V)_n = End(V)$. Now apply Theorem 2.1. □

For instance if $q = 2$ and $n = 2$, then the group $G(\mathfrak{sl}(F_2 \times F_2))$ of order 128 has class-preserving outer automorphisms.

2.3. **Example.** Let $R$ be a discrete valuation ring with maximal ideal $(\pi)$ and finite residue class field $F_q$. Let $m \in \mathbf{N}$, and let $M$ be a free module of rank $n > 1$ over $R/(\pi^m)$. Denote by $\mathfrak{sl}(M)$ the set of $R/(\pi^m)$-endomorphisms of $M$ having trace 0. Then $G(\mathfrak{sl}(M))$ is a finite group of order $q^{m(n^2+2n-1)}$ satisfying $O(G(\mathfrak{sl}(M)))_n \neq 1$.

*Proof.* It is readily verified that any subset of $M$ of cardinality less than $n$ is contained in a hyperplane. This implies that $\mathfrak{sl}(M)$ is properly contained in $\mathfrak{sl}(M)_n = End(M)$. Now apply Theorem 2.1. □

For instance if $R = \mathbf{Z}_2$, the ring of 2-adic integers, and $n = m = 2$, then the group $G(\mathfrak{sl}(\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}))$ of order $2^{14}$ has class-preserving outer automorphisms.

2.4. **Example.** Let $R$ be a discrete valuation ring with maximal ideal $(\pi)$ and finite residue class field $F_q$. Let $M$ be a non-cyclic finite $R$-module. Let $(\pi^{m_1}) \supseteq (\pi^{m_2}) \supseteq \cdots \supseteq (\pi^{m_n})$ be the invariant factors of $M$, where $n > 1$ and $m_1 \leq m_2 \leq \cdots \leq m_n$ are natural numbers. Denote by $\mathfrak{sl}(M)$ the set of $R$-endomorphisms of $M$ having trace 0 modulo $(\pi)$. Assume that $m_n - m_1 \leq 1$. Then $G(\mathfrak{sl}(M))$ is a finite group of order $q^{2(m_1+\cdots+m_n)-1} \prod_{i=1}^n q^{m_i(2(n-i)+1)}$ satisfying $O(G(\mathfrak{sl}(M)))_n \neq 1$.

*Proof.* By a basis of $M$ we mean a set $\{x_1, ..., x_n\}$ that generates $M$ as an $R$-module and satisfies $ann\ x_i = (\pi^{m_i})$. Given such a basis, to each $g \in End(M)$ we may associate a matrix $A \in M_n(R)$ satisfying $g(x_j) = \sum_{i=1}^n A_{ij}x_i$. The matrix $A$ is not uniquely determined by $g$. Nonetheless, one verifies that the quantity $tr(g) = \sum_{i=1}^n A_{ii} + (\pi) \in F_q$ is well-defined, thus yielding a surjective homomorphism of $R$-modules $tr : End(M) \to F_q$. By $\mathfrak{sl}(M)$ we understand the kernel of this map.

By a hyperplane $H$ of $M$ we understand an $R$-submodule of the form $H = \bigoplus_{j \neq i} Ry_j$ for some basis $\{y_1, ..., y_n\}$ of $M$ and some index $i$. The hypothesis $m_n - m_1 \leq 1$ readily implies that any subset of $M$ of cardinality less than $n$ is contained in a hyperplane. This in turn yields that $\mathfrak{sl}(M)$ is properly contained in $\mathfrak{sl}(M)_n = End(M)$. Applying Theorem 2.1 we obtain $O(G(\mathfrak{sl}(V)))_n \neq 1$. Since the trace map is surjective, $\mathfrak{sl}(M)$ has index $q$ in $End(M)$. The order of $End(M)$ is known to be $\prod_{i=1}^n q^{m_i(2(n-i)+1)}$, while $|M^2| = q^{2(m_1+\cdots+m_n)}$. In this way we arrive at the correct order for $G(\mathfrak{sl}(M))$. □

For instance if $R = \mathbf{Z}_2$, $n = 2$ and $(m_1, m_2) = (1, 2)$, then $G(\mathfrak{sl}(\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}))$ is a group of order $2^{10}$ possessing class-preserving outer automorphisms. In general, it may be shown that $\mathfrak{sl}(M)$ is properly contained in $\mathfrak{sl}(M)_n$ if and only if $m_n - m_1 \leq 1$.

**The symplectic Lie algebra.** Let $R$ be a discrete valuation ring with maximal ideal $(\pi)$ and finite residue class field $F_q$. Let $m \in \mathbf{N}$, and suppose that $M$ is a free $R/(\pi^m)$-module of even rank $2\ell$. Let $\langle\ ,\ \rangle$ be a non-degenerate alternating $R/(\pi^m)$-bilinear form on $M$. Denote by $\mathfrak{sp}(M)$ the set of all endomorphisms $f$ of $V$ satisfying $\langle f(x), y\rangle = -\langle x, f(y)\rangle$ for all $x, y \in M$.

2.5. **Example.** The group $G(\mathfrak{sp}(M))$ is finite of order $q^{m(2\ell^2+5\ell)}$ and has class-preserving outer automorphisms.

*Proof.* We claim that $\mathfrak{sp}(M)_2 = End(M)$. Indeed, take any $g \in End(M)$, and let $x \in M$ be arbitrary. Refer to a vector $z \in M$ as primitive if, when written as a linear combination of basis vectors, at least one of its coordinates is a unit.

Write $x = \pi^k z$, where $z$ is primitive and $k \geq 0$. We readily see that $M$ admits a symplectic basis $\{x_1, ..., x_n, y_1, ..., y_n\}$ whose first vector is equal to $z$. Let $A$ be the matrix of $g$ relative to this basis. Construct a block matrix $B = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ such that $a^t = -d$, $b^t = b$, $c^t = c$ and the first column of $B$ is equal to the first column of $A$. Then $B$ represents an endomorphism $f$ in $\mathfrak{sp}(M)$ satisfying $g(z) = f(z)$. Since $x$ is a multiple of $z$, the claim follows. Now apply Theorem 2.1. $\square$

It may be shown that $\mathfrak{sp}(M)_i = \mathfrak{sp}(M)$ for all $i > 2$. Taking $m = 1$ above yields

2.6. **Corollary.** *Let $V$ be a vector space of even rank $2\ell$ over a finite field $F_q$. Denote by $\mathfrak{sp}(V)$ the symplectic Lie algebra. Then the group $G(\mathfrak{sp}(V))$ is finite of order $q^{2\ell^2+5\ell}$ and has class-preserving outer automorphisms.*

**Other Lie algebras.** In contrast to the case of special linear and symplectic Lie algebras, some Lie algebras do not fare as well in regards to being properly contained in their envelopes. Indeed, borrowing notation from [Hum87], for an arbitrary field $F$ one has $\mathfrak{o}(2\ell, F)_2 = \mathfrak{o}(2\ell, F)$ and $\mathfrak{o}(2\ell+1, F)_2 = \mathfrak{o}(2\ell+1, F)$ provided $charF \neq 2$. The case $charF = 2$ can be reduced to the symplectic case. We also have $\mathfrak{t}(n, F)_2 = \mathfrak{t}(n, F)$, $\mathfrak{n}(n, F)_2 = \mathfrak{n}(n, F)$, and $\mathfrak{d}(n, F)_2 = \mathfrak{d}(n, F)$, $n \geq 2$. On the other the Lie algebra $\mathfrak{t}(n, q)^0 = \mathfrak{t}(n, q) \cap \mathfrak{sl}(n, F)$ is both relatively small and properly contained in its $n$-envelope.

2.7. **Example.** Let $n > 1$ and let $q$ be a prime power. Denote by $\mathfrak{t}(n, q)$ the set of all $n \times n$ upper triangular matrices over $F_q$. Let $\mathfrak{t}(n, q)^0$ be the set of all matrices in $\mathfrak{t}(n, q)$ having trace 0. Then $G(\mathfrak{t}(n, q)^0)$ is a finite group of order $q^{n(n+5)/2-1}$ satisfying $O(G(\mathfrak{t}(n, q)^0))_n \neq 1$.

*Proof.* It is readily verified that $(\mathfrak{t}(n, q)^0)_n$ is a subspace of $\mathfrak{t}(n, q)$ that contains $\mathfrak{t}(n, q)^0$. Since $\mathfrak{t}(n, q)^0$ is a hyperplane of $\mathfrak{t}(n, q)$, it suffices to verify that the $n \times n$ matrix $A = \begin{pmatrix} 0 & ... & 0 & 0 \\ 0 & ... & 0 & 0 \\ \vdots & & \vdots & \vdots \\ 0 & ... & 0 & 1 \end{pmatrix}$ belongs to $(\mathfrak{t}(n, q)^0)_n$. To see this, let $B = \begin{pmatrix} b_{11} & ... & b_{1n-1} \\ b_{21} & ... & b_{2n-1} \\ \vdots & & \vdots \\ b_{n1} & ... & b_{nn-1} \end{pmatrix}$ be an $n \times n-1$ matrix whose columns represent $n-1$ arbitrary vectors in $F_q^n$. We need to find $X = \begin{pmatrix} x_{11} & x_{12} & ... & x_{1n} \\ 0 & x_{21} & ... & x_{2n} \\ \vdots & & & \vdots \\ 0 & 0 & ... & x_{nn} \end{pmatrix} \in \mathfrak{t}(n, q)^0$ such that $AB = XB$. Write $R_i(Y)$ for the $i$-th row of a given matrix $Y$. We consider three cases.

*Case* 1. $R_n(B) = (0, ..., 0)$. In this case we take $X$ to be the zero matrix.

*Case* 2. For some $i$, $2 \leq i < n$, $R_i(B)$ is a linear combination of $R_{i+1}(B), ...,$ $R_n(B)$. In this case we let

$$R_{i+1}(X) = \cdots = R_{n-1}(X) = (0, ..., 0, 0), \quad R_n(X) = (0, ..., 0, 1).$$

By hypothesis there exist $a_{i+1}, ..., a_n \in F_q$ such that $R_i(B) = a_{i+1}R_{i+1}(B) + \cdots + a_nR_n(B)$. Accordingly, we let

$$R_1(X) = \cdots = R_{i-1} = (0, ..., 0), \quad R_i(X) = (\underbrace{0, ..., 0}_{i-1}, -1, a_{i+1}, ..., a_n).$$

The chosen rows of $X$ ensure that $AB = XB$, $tr(X) = 0$ and $X$ is upper triangular.

*Case* 3. $R_2(B), ..., R_n(B)$ are linearly independent. In this case we let

$$R_2(X) = \cdots = R_{n-1}(B) = (0, ..., 0), \quad R_n(B) = (0, ..., 0, 1).$$

It remains to choose $R_1(X)$ so that $x_{11}+x_{22}+\cdots+x_{nn}=0$ and $R_1(X)B=(0,...,0)$. These conditions translate into $x_{11}=-1$ and $(x_{12},...,x_{1n})C=(b_{11},...,b_{1n-1})$, where $C$ is the $(n-1)\times(n-1)$ matrix $\begin{pmatrix} b_{21} & \dots & b_{2n-1} \\ \vdots & & \vdots \\ b_{n1} & \dots & b_{nn-1} \end{pmatrix}$. By hypothesis $C$ is invertible, so we can take $(x_{12},...,x_{1n})=(b_{11},...,b_{1n-1})C^{-1}$. This completes the proof. □

In regards to the problem of constructing, for a given $n>1$, a small group $G$ satisfying $O(G)_n \neq 1$, the following question is relevant:

2.8. **Question.** Let $V$ be a vector space of dimension $n>1$ over a finite field $F_q$. Set $d(n)=min\{\, dimE \,|\, E\leq End(V),\ E_n/E\neq 0\}$. What is $d(n)$?

Example 2.7 shows that $d(n)\leq n(n+1)/2-1$. A crude lower bound can be shown to be $n$. In particular, $d(2)=2$. We used GAP to see that $d(3)=5$ when $q=2$. The question, of course, makes sense for arbitrary fields.

**The regular representation of a field.**

2.9. **Example.** Let $m>1$ and let $p$ be an arbitrary prime. Let $L: F_{p^m}\to End(F_{p^m})$ be the regular representation of $F_{p^m}$, that is, $L(x)(y)=xy$ for all $x,y\in F_{p^m}$. Then $G(p^m)=G(L(F_{p^m}))$ is a finite group of order $p^{3m}$ having class-preserving outer automorphisms.

*Proof.* $L(F_{p^m})$ is properly contained in $L(F_{p^m})_2=End(F_{p^m})$. Now apply Theorem 2.1. □

More generally, let $R$ be any ring, and let $L$ be the left regular representation of $R$. By Theorem 2.1 $G(L(R))$ has class-preserving outer automorphisms, provided $R^+$ has endomorphisms which are not left multiplication but send every element $r$ of $R$ to $Rr$. This holds automatically for division rings which are not prime-fields. Sah [Sah68] shows that the desired property also holds for rings of the form $R=F_{p^m}[t]/(t^n)$, where $mn>1$.

**The example of Burnside.** Here we use our construction to view Burnside's example [Bur13] from a different angle.

2.10. **Example.** Let $p$ be a prime congruent to $\pm 3 \mod 8$. Let $G$ be the group constructed by Burnside in [Bur13], that is, the group defined by generators $A_1,A_2,A_3,A_4,P,Q$ subject to the relations

$$A_1^p=A_2^p=A_3^p=A_4^p=P^p=Q^p=1,\quad [A_1,A_2]=[A_3,A_4]=1,$$

$$[A_3,A_1]=P,\quad [A_4,A_1]=Q,\quad [A_3,A_2]=PQ,\quad [A_4,A_2]=PQ^{-1},$$

and relations expressing that both $P$ and $Q$ are permutable with $A_1,A_2,A_3,A_4$. Then $G\cong G(p^2)$.

*Proof.* If we replace the original generators by $A_1,A_2,A_3,A_4'=A_3A_4,P,Q'=PQ$, then we obtain the following defining relations for $G$:

$$A_1^p=A_2^p=A_3^p=(A_4')^p=P^p=(Q')^p=1,\quad [A_1,A_2]=[A_3,A_4']=1,$$

$$[A_3,A_1]=P,\quad [A_4',A_1]=Q',\quad [A_3,A_2]=Q',\quad [A_4',A_2]=P^2,$$

and relations expressing that both $P$ and $Q'$ are permutable with $A_1,A_2,A_3,A_4'$.

View $F_{p^2}$ as a vector space over $F_p$ of dimension 2. Since 2 is not a square modulo $p$, we can choose a basis $\{1, \theta\}$ of $F_{p^2}$ over $F_p$, such that $\theta^2 = 2$. Using this basis, the regular representation of $F_{p^2}$ adopts the form $L(1) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $L(\theta) = \left(\begin{smallmatrix} 0 & 2 \\ 1 & 0 \end{smallmatrix}\right)$. It readily follows that, as an abstract group, $G(p^2)$ is defined by the above generators and relations, as required. $\square$

Burnside's group, and more generally the groups $G(p^2)$ for an arbitrary prime $p$ have order $p^6$. The groups $G(\mathfrak{t}(2,p)^0)$ constructed in section 2 also have order $p^6$. Both have class-preserving outer automorphisms. However, they are not isomorphic. Indeed, every element of $G(p^2)$ that is not central has $p^4$ conjugates, whereas $G(\mathfrak{t}(2,p)^0)$ has non-central elements with $p^5$ conjugates.

**The example of Neumann.** We may also interpret Neumann's example [Neu81] in terms of our construction. For this purpose we require the following generalization of our method. Consider a second abelian group $N$. Replace $M \times M$ by $M \times N$, $End(M)$ by $Hom(M,N)$, and $E$ by a subgroup $H$ of $Hom(M,N)$. This yields the group $G(H) = (M \times N) \rtimes H$. Write $H_n$ for the $n$-envelope of $H$ in $Hom(M,N)$. Much as above, we see that $O(G(H))_n \neq 1$ provided $H_n/H \neq (0)$.

Given $n > 1$ and a prime power $q$, set $V = F_q^n$ and $W = V \oplus F_q c \cong F_q^{n+1}$. Associated to each $A \in M_n(F_q)$ we have the $F_q$-linear map $\tilde{A} : V \to W$, defined by

$$\tilde{A}x = Ax + (\sum_{i=1}^{n} A_{ii})(\sum_{i=1}^{n} x_i)c, \quad x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in V. \tag{1}$$

The correspondence $A \mapsto \tilde{A}$ defines an embedding of vector spaces $M_n(F_q) \to Hom(V,W)$. Let us denote by $T(n,q)$ the image of $\mathfrak{t}(n,q)$ under this map. With this notation the group of order $q^{n(n+5)/2+1}$ constructed by Neumann in [Neu81] is nothing but $G(T(n,q))$. Furthermore, $G(\mathfrak{t}(n,q)^0)$ is clearly a subgroup of $G(T(n,q))$, as the second summand of (1) vanishes when $tr(A) = 0$. The index of $G(\mathfrak{t}(n,q)^0)$ in $G(T(n,q))$ is $q^2$. Observe also that since $(\mathfrak{t}(n,q)^0)_n/\mathfrak{t}(n,q)^0 \neq (0)$, the embedding $M_n(F_q) \to Hom(V,W)$ yields $T(n,q)_n/T(n,q) \neq 1$, whence $O(G(T(n,q)))_n \neq 1$ by Theorem 2.1. This was first proved by Neumann using a different method.

## 3. Concluding remarks

Our construction can be some somewhat generalized as follows. Replace $M \times M$ by $X \times Y$, where $X$ and $Y$ are arbitrary groups. Substitute $End(M)$ by the abelian group $Hom(X, Z(Y))$, and $E$ by a subgroup $H$ of $Hom(X, Z(Y))$. This leads to the group $G(H) = (X \times Y) \rtimes H$. For each $n$ denote by $H_n$ the $n$-envelope of $H$ in $Hom(X, Z(Y))$. The group embedding $\Delta : Hom(X, Z(Y)) \to A(G(H))$ is defined much as before.

For $H^* = Hom(H, Z(Y))$ we have the group embedding $\Delta^* : H^* \to A(G(H))$, given by

$$\Delta^*(\tau)(x,y,f) = (x,y,f)(1,\tau(f),1), \quad \tau \in H^*, x \in X, y \in Y, f \in H.$$

Consider also the evaluation homomorphism $ev : X \to H^*$ defined by

$$ev(x)(\tau) = \tau(x), \quad x \in X, \tau \in H^*.$$

Write $ev(X)_n$ for the $n$-envelope of $ev(X)$ in $H^*$. The following properties are readily verified: $\Delta(g) \in I(G(H)) \Leftrightarrow g \in H$; $\Delta(g) \in I(G(H))_n \Leftrightarrow g \in H_n$;

$\Delta^*(\tau) \in I(G(H)) \Leftrightarrow \tau \in ev(X)$; $\Delta^*(\tau) \in I(G(H))_n \Leftrightarrow g \in ev(X)_n$; $\Delta(g)\Delta^*(\tau) = \Delta^*(\tau)\Delta(g)$; $\Delta(g)\Delta^*(\tau) \in I(G(H)) \Leftrightarrow \Delta(g)$, $\Delta^*(\tau) \in I(G(H))$. Thus for each $n$ we have a group embedding $(\Delta_n, \Delta_n^*) : (H_n/H) \times (H_n^*/ev(X)) \to O(G(H))_n$, defined by

$$(\Delta_n, \Delta_n^*)([g], [\tau]) = [\Delta(g)\Delta^*(\tau)], \quad g \in Hom(X, Z(Y)), \tau \in H^*.$$

This yields

3.1. **Theorem.** *If $H_n/H \neq 0$ or $ev(X)_n/ev(X) \neq 0$, then $O(G(H))_n \neq 1$.*

For instance, $(\Delta_2, \Delta_2^*)$ is readily seen to be an isomorphism for $G(p^m)$, $m > 1$, whence $O(G(p^m))_2 \cong (\mathbf{Z}/p\mathbf{Z})^{2(m^2-m)}$. This is an agreement with Burnside's result to the effect that the group of class-preserving outer automorphisms of his group is isomorphic to $(\mathbf{Z}/p\mathbf{Z})^4$.

All groups considered so far have been nilpotent of class 2. We may use the above procedure to construct a non-solvable group $G(H)$ satisfying $O(G(H))_n \neq 1$. Indeed, let $p$ be a prime and let $n \geq 2$. Consider the ring

$$R = F_p[t_1, ..., t_n]/(t_1^p, ..., t_n^p, t_1t_2, ..., t_{n-1}t_n),$$

which is finite and local. Set $X = Y = GL_2(R)$. From the facts $X' = SL_2(R)$ and $Z(Y) = \{rI \mid r \in R^*\}$ we deduce

$$X/X' \cong Z(Y) \cong R^* \cong F_p^* \times (F_p^+)^n.$$

Hence $End(F_p^n)$ can be canonically embedded in

$$Hom(X, Z(Y)) \cong Hom(X/X', Z(Y)).$$

Denote by $H$ the image of $\mathfrak{sl}(F_p^n)$ under this embedding. From Theorem 2.2 we infer that $H$ is properly contained in $H_n$. Note also that $GL_2(p)$ is a quotient of $GL_2(R)$, whence $GL_2(R)$ is non-solvable if $p > 3$ and non-nilpotent for all $p$. We have proven

3.2. **Example.** The finite group $G(H)$ satisfies $O(G(H))_n \neq 1$, is non-solvable if $p > 3$, and non-nilpotent for all $p$.

## Acknowledgements

I thank the referees for very useful suggestions. I also thank A. Herman and L. Creedon for helpful discussions.

## References

[Bur13] W. Burnside, *On the outer automorphisms of a group*, Proc. London Math. Soc. (2) **11** (1913), 40–42.

[Her01a] M. Hertweck, *Class-preserving automorphisms of finite groups*, J. Algebra **241** (2001), 1–26. MR **2002e:**20047

[Her01b] M. Hertweck, *A counterexample to the isomorphism problem for integral group rings*, Ann. of Math. (2) **154** (2001), 115–138. MR **2002e:**20010

[Hum87] J.E. Humphreys, *Introduction to Lie Algebras and Representation Theory*, Fifth ed., Springer-Verlag, New York, 1987.

[KR93] W. Kimmerle and K.W. Roggenkamp, *Projective limits of group rings*, J. Pure Appl. Algebra **88** (1993), 119–142. MR **94f:**20008

[Maz95] M. Mazur, *On the isomorphism problem for integral group rings*, Exposition. Math. **13** (1995), 433–445. MR **96k:**20007

[Neu81] B. Neumann, *Not quite inner automorphisms*, Bull. Austral. Math. Soc. **23** (1981), 461–469. MR **82i:**20039

[RZ95] K.W. Roggenkamp and A. Zimmermann, *Outer group automorphisms may become inner in the integral group ring*, J. Pure Appl. Algebra **103** (1995), 91–99. MR **97b:**20004

[Sah68] C.H. Sah, *Automorphisms of finite groups*, J. Algebra **10** (1968), 47–68. MR **55:**8172

[Wal47] G.E. Wall, *Finite groups with class-preserving outer automorphisms*, J. London Math. Soc. **22** (1947), 315–320. MR **10:**8g

Department of Pure Mathematics, University of Waterloo, Ontario, Canada N2L 3G1

*E-mail address*: fszechtm@herod.uwaterloo.ca