

INTEGRAL GROUP RING AUTOMORPHISMS WITHOUT ZASSENHAUS FACTORIZATION

MARTIN HERTWECK

ABSTRACT. An automorphism α of an integral group ring $\mathbb{Z}G$, where G is a finite group, is said to have a Zassenhaus factorization if it is the composition of an automorphism of G (extended to a ring automorphism) and a central automorphism. In 1988, Roggenkamp and Scott constructed a group G (of order 2880) such that $\mathbb{Z}G$ has a normalized (i.e., augmentation preserving) automorphism α which has no Zassenhaus factorization. In this paper, short proofs of the following two results are given. (1) For a group G of order 144, there is a normalized automorphism α of $\mathbb{Z}G$ which has no Zassenhaus factorization. Moreover, α can be chosen to have finite order. (2) There is a group G of order 1200, with abelian Sylow subgroups and Sylow tower, such that $\mathbb{Z}G$ has a normalized automorphism which has no Zassenhaus factorization.

1. Introduction

Automorphisms of group rings $\mathcal{O}G$, where \mathcal{O} is the ring of integers in a local or global field and G is a finite group, have been studied by various authors, mostly in their own right, but also for other reasons (such as applications to the isomorphism problem; see [7] and [10]). Of course, group ring automorphisms can also act on objects associated to the ring (see [2]). For example, the group of normalized (i.e., augmentation preserving) automorphisms of the integral group ring $\mathbb{Z}G$ acts on the character ring, and a conjecture of H. Zassenhaus asserts that this action coincides with the action of $\text{Aut}(G)$. Following [10, p. 327], we shall say that an automorphism α of $\mathbb{Z}G$ has a *Zassenhaus factorization* if it is the composition of a group automorphism of G (extended to a ring automorphism) and a *central* automorphism (an automorphism fixing the center element-wise). Then, the actions coincide

Received March 19, 2001; received in final form September 12, 2001.

2000 *Mathematics Subject Classification*. Primary 20C10, 20C05. Secondary 16U60, 16W20.

The research was supported by the Deutsche Forschungsgemeinschaft.

©2002 University of Illinois

if and only if each normalized automorphism of $\mathbb{Z}G$ has a Zassenhaus factorization. (It should be remarked that whether or not an automorphism has a Zassenhaus factorization depends on the distinguished basis G .)

Roggenkamp and Scott [9] constructed a metabelian group G of order 2880 such that $\mathbb{Z}G$ has a normalized automorphism α which has no Zassenhaus factorization. Their construction of α is explicit in the semilocal situation. To show that their example is also a global counterexample to the Zassenhaus conjecture, they developed a general theory, using Picard groups and Milnor's Mayer Vietoris sequence. An excellent outline of this work is given in [10].

Subsequently, Klingler [8] constructed explicitly a global automorphism. Certain quotients of $\mathbb{Z}G$ naturally show up in the presence of two normal subgroups of G of coprime order. Klingler made essential use of the fact that, in some situations, certain units of such a quotient, which, roughly speaking, correspond to elementary matrices, can be "lifted". This observation is formalized in Lemma 2.2 below.

Scott found a way to approach the construction of group ring automorphisms and isomorphisms in the semilocal case that avoids any explicit use of the theory of orders (see [10]). Using this idea, Blanchard [1] constructed further counterexamples in the semilocal case.

In [4, 2.2.1], a group G of order 144 was given which provides a semilocal counterexample. In this paper, it is shown that this group is also a global counterexample (Theorem A). The computations are done explicitly in order to show that there is a normalized automorphism of *finite* order of $\mathbb{Z}G$ which has no Zassenhaus factorization, thus answering a question of Klingler [8, p. 2329]. It should be remarked that the group G is different from the three groups of order 144 given by Blanchard [1, II.1.1], and that it is not yet known whether his examples are global counterexamples.

Zassenhaus [11] believed that his conjecture is true at least for groups with abelian Sylow subgroups and Sylow tower. Unfortunately, this is not the case, as our second example (Theorem B) shows.

Both counterexamples have the same structure which we will explain first.

Structure of the counterexamples. For a group X , write \hat{X} for the sum of its elements. The (two-sided) ideal generated by group ring elements s, t, \dots will be denoted by (s, t, \dots) .

Both counterexamples have the same structure. The underlying group G has normal subgroups M and N of coprime order. The quotient

$$\Lambda = \mathbb{Z}G/(\hat{M}, \hat{N})$$

is the projection on a factor of $\mathbb{Q}G$ (to which all blocks having neither M nor N in their kernel belong). The projection of $\mathbb{Z}G$ on the complementary factor is the image Γ of $\mathbb{Z}G$ under the natural map $\mathbb{Z}G \rightarrow \mathbb{Z}G/M \oplus \mathbb{Z}G/N$. Hence

there are pull-back diagrams

$$\begin{array}{ccc}
 \Gamma & \longrightarrow & \mathbb{Z}G/M \\
 \downarrow & & \downarrow \\
 \mathbb{Z}G/N & \longrightarrow & \mathbb{Z}G/MN
 \end{array}
 \quad \text{and} \quad
 \begin{array}{ccc}
 \mathbb{Z}G & \longrightarrow & \Gamma \\
 \downarrow & & \downarrow \\
 \Lambda & \longrightarrow & \bar{\Lambda}
 \end{array}
 .$$

Roggenkamp and Scott [9, Section 2] proved that the ring $\bar{\Lambda}$ over which the pull-back for $\mathbb{Z}G$ is taken has the form

$$(\mathbb{Z}G/M)/(|M|, \hat{N}) \oplus (\mathbb{Z}G/N)/(|N|, \hat{M}).$$

A group automorphism φ of G plays an important rôle. It fixes the normal subgroups M and N , and so, in particular, induces automorphisms of Γ , Λ and $\bar{\Lambda}$. Though the automorphism induced on Γ is not a central automorphism, φ will induce central automorphisms on the quotients $(\mathbb{Z}G/M)/(\hat{N})$ and $(\mathbb{Z}G/N)/(\hat{M})$, and even an inner automorphism on $\bar{\Lambda}$. We will show that there is an inner automorphism β of Γ which agrees with φ on $\bar{\Lambda}$. Thus there is an automorphism α of $\mathbb{Z}G$ which induces β on Γ and φ on Λ . Note that α is normalized; this is because Γ inherits the structure of an augmented algebra, and α induces on Γ an augmentation preserving automorphism. In order to show that α has no Zassenhaus factorization, it remains to show that there is no $\rho \in \text{Aut}(G)$ which differs on Λ from φ by a central automorphism and induces on Γ a central automorphism (this will be called the “group-theoretical obstruction”).

It should be remarked that the counterexample given by Roggenkamp and Scott has the property that there is a group ring automorphism which has no Zassenhaus factorization on “the level of Γ ”.

2. Preliminary results

Let H be a finite group, and N a normal subgroup of H . At the end of the Introduction, the following question arose: Given a central ring automorphism φ of $\mathbb{Z}H/(\hat{N})$, and a natural number $m \neq 1$ with $(m, |N|) = 1$, is there a central ring automorphism β of $\mathbb{Z}H$ which agrees with φ on $\mathbb{Z}H/(\hat{N}, m)$?

We first present a negative example. This example emerged as the author tried to obtain a global version of a semilocal counterexample to the conjecture of Zassenhaus for a group of order 180. (The semilocal version was announced in [6].)

EXAMPLE 2.1. Let $H = \langle n, a : n^5 = a^4 = n^a n = 1 \rangle \cong C_5 \rtimes C_4$ and $N = \langle n \rangle \cong C_5$. An automorphism φ of H is defined by $n\varphi = n$ and $a\varphi = a^3$. This automorphism fixes all irreducible characters which do not have N in their kernel, and therefore induces a central automorphism of $\mathbb{Z}H/(\hat{N})$. However, we will show that for any natural number m , there is no central automorphism β of $\mathbb{Z}H$ which agrees with φ on $\mathbb{Z}H/(\hat{N}, m)$ (although the

latter quotient could very well be semisimple, in which case φ induces an inner automorphism on it).

There is a surjective ring homomorphism θ from $\mathbb{Q}H$ onto the skew field $D = \{[\begin{smallmatrix} r & s \\ -\bar{s} & \bar{r} \end{smallmatrix}] : r, s \in \mathbb{Q}(\zeta)\}$ (where ζ is a primitive 5-th root of unity), mapping n to $[\begin{smallmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{smallmatrix}]$ and a to $[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}]$. Assume that some $d \in (\mathbb{Z}H)\theta$ is a unit of order 4. Clearly $\bar{d} = [\begin{smallmatrix} r & s \\ -\bar{s} & \bar{r} \end{smallmatrix}]$ for some $r, s \in \mathbb{Z}[\zeta]$, and $s \neq 0$. Furthermore, $\det(d)$ is a 4-th root of unity, so $\det(d) = r\bar{r} + s\bar{s} = 1$. It follows that $r\bar{r} = 1 - s\bar{s} < 1$, and the same is true for all algebraic conjugates of r . By a well-known theorem of Kronecker, it follows that $r = 0$ and $s = \pm\zeta^n$ for some $n \in \mathbb{Z}$. Hence the units of D of order 4 which are contained in $(\mathbb{Z}H)\theta$ are precisely the elements $h\theta$ with $h \in H$ of order 4. In particular, if such units are congruent modulo m , they are equal.

Let e be the central idempotent $\frac{1}{2}(1 - a^2)(1 - \frac{1}{5}\hat{N})$ of $\mathbb{Q}H$. The kernel of θ is $(1 - e)\mathbb{Q}H$, so $\mathbb{Z}H/(1 + a^2, \hat{N})$, which is the projection of $\mathbb{Z}H$ on $e\mathbb{Q}H$, is isomorphic to $(\mathbb{Z}H)\theta$.

Now assume that there is a central automorphism β of $\mathbb{Z}H$ which agrees with φ on $\mathbb{Z}H/(\hat{N}, m)$. Then $a\beta$ and a^3 have the same image in $\mathbb{Z}H/(\hat{N}, m)$, and from the commutativity of the diagram

$$\begin{array}{ccc} \mathbb{Z}H & \longrightarrow & \mathbb{Z}H/(1 + a^2, \hat{N}) \\ \downarrow & & \downarrow \text{mod } m \\ \mathbb{Z}H/(\hat{N}, m) & \longrightarrow & \mathbb{Z}H/(1 + a^2, \hat{N}, m) \end{array}$$

and the above considerations it follows that $a\beta$ and a^3 have the same image in $\mathbb{Z}H/(1 + a^2, \hat{N})$. The automorphism β induces on the commutative ring $\frac{1}{5}\hat{N} \cdot \mathbb{Z}H \cong \mathbb{Z}\langle a \rangle$ a central automorphism, i.e., the identity mapping. Altogether, it follows that

$$\begin{aligned} (1 - a^2)(a\beta) &= 2e(a\beta) + (1 - a^2)\frac{1}{5}\hat{N}(a\beta) \\ &= 2ea^3 + (1 - a^2)\frac{1}{5}\hat{N}a \\ &= (a^3 - a) + \frac{1}{5}\hat{N} \cdot 2(a - a^3). \end{aligned}$$

Since the element on the right-hand side does not lie in $\mathbb{Z}H$, we have reached a contradiction.

In [8], Klingler repeatedly lifted certain units of a ring $\mathbb{Z}H/(\hat{N}, m)$, which, roughly speaking, corresponded to elementary matrices, to units of $\mathbb{Z}H$. (Recall that a matrix is called elementary if it differs from the unit matrix in only one off-diagonal entry.) This idea is formalized in the next lemma.

For a natural number m , let $\mathbb{Z}_{\pi(m)}$ denote the intersection of all localizations $\mathbb{Z}_{(p)}$, with p a prime divisor of m . For a group G , write $\varepsilon_G = \hat{G}/|G|$ (the trivial idempotent) and $\eta_G = 1 - \varepsilon_G$.

LEMMA 2.2. *Let H be a finite group, N a normal subgroup of H and m a natural number with $(m, |N|) = 1$. Let φ be a central ring automorphism of $\mathbb{Z}H/(\hat{N})$. Assume that for each irreducible character χ of H which does not contain N in its kernel the following conditions hold:*

- (i) $(m, |H|/\chi(1)) = 1$, that is, χ is of p -defect zero for every prime p dividing m .
- (ii) χ can be realized over the rationals, i.e., there is a representation $\theta : H \rightarrow \text{GL}_d(\mathbb{Q})$ of H which affords the character χ .
- (iii) There is a matrix $A \in \text{GL}_d(\mathbb{Q})$ such that $(h\varphi)\theta = A^{-1}(h\theta)A$ for all $h \in H$ (this holds since φ is a central automorphism), and $\det(A) \in 1 + m\mathbb{Z}_{\pi(m)}$.

Then there is an inner automorphism of $\mathbb{Z}H$ which agrees on $\mathbb{Z}H/(\hat{N}, m)$ with φ . Given a natural number l with $(l, m) = 1$, this automorphism can be chosen to be the conjugation with a unit $u \in V(\mathbb{Z}H)$ which satisfies $u\varepsilon_N = \varepsilon_N$ and $u \in 1 + l \cdot \mathbb{Z}H$.

Proof. Note that $\mathbb{Z}H/(\hat{N})$ can be identified with the projection of $\mathbb{Z}H$ on $\mathbb{Q}H\eta_N$. In this way, φ induces an automorphism of $\mathbb{Q}H\eta_N$, which, for simplicity, will also be denoted by φ . Let χ and θ (viewed as a function $\mathbb{Q}H \rightarrow \text{Mat}_d(\mathbb{Q})$) be as above, and let e be the central idempotent which corresponds to χ . Without loss of generality, we may assume that $H\theta \subseteq \text{GL}_d(\mathbb{Z})$ (see [5, V.12.2]).

For $h \in H$, let $\theta_{ij}(h)$ be the (i, j) -th entry of the matrix $h\theta$, and let

$$e_{ij} = \frac{d}{|H|} \sum_{h \in H} \theta_{ij}(h^{-1})h, \quad 1 \leq i, j \leq d.$$

By Schur's relations (cf. [5, V.5.7]), we have $e_{ij}(1-e) = 0$, and $e_{ij}\theta$ is obtained from the zero matrix by replacing the (i, j) -th entry by 1. Thus if $R = \mathbb{Z}_{\pi(m)}$, then it follows from (i) and (ii) that the restriction $eRH \xrightarrow{\theta} \text{Mat}_d(R)$ is an isomorphism which takes $emRH$ to $\text{Mat}_d(mR)$. Altogether, if we let bars denote reduction mod m and note that $R/mR \cong \mathbb{Z}/m\mathbb{Z}$, then we have the following commutative diagram, where the horizontal maps are isomorphisms:

$$\begin{array}{ccc} eRH & \xrightarrow{\theta} & \text{Mat}_d(R) \\ \downarrow - & & \downarrow - \\ \bar{e}(\mathbb{Z}/m\mathbb{Z})H & \xrightarrow{\bar{\theta}} & \text{Mat}_d(\mathbb{Z}/m\mathbb{Z}) \end{array}$$

It is well-known that central automorphisms of $\text{Mat}_d(R)$ are inner automorphisms (see [3, (55.40) and (55.16)]). Thus φ induces an inner automorphism of $\text{Mat}_d(R)$, i.e., there is $U \in \text{GL}_d(R)$ with $(eh\varphi)\theta = U^{-1}(eh\theta)U$ for all $h \in H$. Note that $\text{rad}(R) = \pi R$, where π is the product of the primes dividing m , so $1 + mR \subseteq 1 + \text{rad}(R) \subseteq R^\times$ (the group of units of R). By (ii), there is $a \in \mathbb{Q}$

such that $\det(U)a^d \in 1 + mR$. It follows that $a \in R^\times$, and we may assume that $\det(U) \in 1 + mR$.

Then there are elementary matrices $E_j \in \mathrm{GL}_d(R)$ such that $\bar{U} = \bar{E}_1 \cdot \bar{E}_2 \cdot \dots \cdot \bar{E}_k$ in $\mathrm{GL}_d(\mathbb{Z}/m\mathbb{Z})$. Choose $a_j \in RH$ with $a_j\theta = E_j$. There is $r \in \mathbb{Z}$ with $(r, m) = 1$ and $ra_j \in \mathbb{Z}H$ for all j . Let l be a natural number with $(l, m) = 1$. There are $s, t \in \mathbb{Z}$ with $sm + trl(|H|/d) = 1$. Put

$$b_j^+ = 1 + (1 - sm)(a_j - 1) \quad \text{and} \quad b_j^- = 1 - (1 - sm)(a_j - 1).$$

Note that $b_j^+, b_j^- \in 1 + l(|H|/d)\mathbb{Z}H$, $\overline{b_j^+\theta} = \bar{E}_j$, and that $eb_j^-b_j^+ = e$. (Consider the image under θ , and recall that $(E - 1)^2 = 0$ for an elementary matrix E .) Put

$$u_* = b_1^+ b_2^+ \dots b_k^+ \quad \text{and} \quad v_* = b_k^- b_{k-1}^- \dots b_1^-.$$

Then $ev_*u_* = e$ and $\overline{u_*\theta} = \bar{U}$, which implies that $\overline{v_*\theta} = \bar{U}^{-1}$. Thus

$$\overline{(ev_*xu_*)\theta} = \bar{U}^{-1}(\overline{ex\theta})\bar{U} = \overline{(ex)\varphi\theta} \quad \text{for all } x \in \mathbb{Z}H.$$

Since the horizontal maps in the commutative diagram above are isomorphisms, it follows that

$$ev_*xu_* - (ex)\varphi \in m \cdot eRH \quad \text{for all } x \in \mathbb{Z}H.$$

Expanding the product u_* , we see that $u_* \in 1 + l(|H|/d)\mathbb{Z}H$, so $eu_* - e \in l \cdot \mathbb{Z}H$ since $e \in (d/|H|) \cdot \mathbb{Z}H$.

Now let e_1, \dots, e_n be the primitive central idempotents of $\mathbb{C}H$ such that $\eta_N = e_1 + \dots + e_n$. We have shown that there are $u_i, v_i \in \mathbb{Z}H$ with $e_i u_i - e_i \in l \cdot \mathbb{Z}H$ and $e_i v_i u_i = e_i$ such that, for some $y_i \in RH$,

$$e_i v_i x u_i - (e_i x)\varphi = m \cdot e_i y_i \quad \text{for all } x \in \mathbb{Z}H.$$

Let $u = \varepsilon_N + \sum_{i=1}^n e_i u_i$ and $v = \varepsilon_N + \sum_{i=1}^n e_i v_i$. Then $u \in 1 + l \cdot \mathbb{Z}H$ and $vu = 1$. Let β be the conjugation with u , and $x \in \mathbb{Z}H$. Then

$$x\beta = vxu = \varepsilon_N x + \sum_{i=1}^n (e_i x)\varphi + m \sum_{i=1}^n e_i y_i.$$

Multiplying with η_N , we obtain

$$\eta_N x \beta = \eta_N x \varphi + m \eta_N \sum_{i=1}^n e_i y_i.$$

Put $z = \eta_N x \beta - \eta_N x \varphi \in \eta_N \mathbb{Z}H$. By (i) and (ii), there is $c \in \mathbb{Z}$ with $(m, c) = 1$ such that $c \sum_{i=1}^n e_i y_i \in \mathbb{Z}H$. Take $s, t \in \mathbb{Z}$ with $sm + tc = 1$. Then

$$z = smz + tc m \eta_N \sum_{i=1}^n e_i y_i \in m \eta_N \mathbb{Z}H.$$

It follows that β agrees with φ on $\eta_N \mathbb{Z}H / m \eta_N \mathbb{Z}H = \mathbb{Z}H / (\hat{N}, m)$, and the lemma is proved. \square

The lemma will be applied in the following form. Note that if φ is an automorphism of a group H , we can form the semidirect product $H \rtimes \langle \varphi \rangle$, where the action of φ on H is defined by $[h, \phi] = h^{-1}(h\varphi)$ for all $h \in H$.

COROLLARY 2.3. *Let H be a finite group, N a normal subgroup of H and m a natural number with $(m, |N|) = 1$. Let φ be an automorphism of H . Assume that every irreducible complex representation of H which does not contain N in its kernel is the restriction of a rational representation Θ of $H \rtimes \langle \varphi \rangle$ with $\det(\varphi\Theta) = 1$, and that $(m, |H|/d) = 1$, where d is the degree of Θ . Then there is an inner automorphism of $\mathbb{Z}H$ which agrees with φ on $\mathbb{Z}H/(\hat{N}, m)$. Given a natural number l with $(l, m) = 1$, this automorphism can be chosen to be the conjugation with a unit $u \in V(\mathbb{Z}H)$ which satisfies $u\varepsilon_N = \varepsilon_N$ and $u \in 1 + l \cdot \mathbb{Z}H$. \square*

Though the following observation will not be needed, it seems appropriate to state it here, since it shows how the “group-theoretical obstruction” mentioned in the Introduction can be established.

For an element $g \in G$, denote its class sum, i.e., the sum of the conjugates of g in G , by \mathcal{K}_g .

LEMMA 2.4. *Let G be a finite group with normal subgroups $M, N \neq 1$ of coprime order. Let $x, y \in MN$ be two elements of the same order which are not conjugate within G . Then the class sums \mathcal{K}_x and \mathcal{K}_y have different images in $\mathbb{Z}G/(\hat{M}, \hat{N})$.*

Proof. Let $x = m_1n_1$ and $y = m_2n_2$ with $m_i \in M$ and $n_i \in N$. Choose $1 \neq m \in M$ and $1 \neq n \in N$ such that $m = m_1$, and also $n = n_1$, if possible.

Note that $M \cap N = 1$ since M and N are of coprime order, so $[M, N] = 1$. Further, x and y have the same order, so $m_1 = 1$ if and only if $m_2 = 1$ and $n_1 = 1$ if and only if $n_2 = 1$.

We show that there do not exist elements $g \in G$ and $\epsilon_1, \epsilon_2 \in \{0, 1\}$ such that $x = y^g m^{\epsilon_1} n^{\epsilon_2}$. By way of contradiction, assume the contrary. Then $m_1n_1 = x = y^g m^{\epsilon_1} n^{\epsilon_2} = (m_2^g m^{\epsilon_1})(n_2^g n^{\epsilon_2})$, that is, $m_1 = m_2^g m^{\epsilon_1}$ and $n_1 = n_2^g n^{\epsilon_2}$. Assume that $m_1 = 1$. Then $n_1 \neq 1$, and $m_2 = 1$. If $\epsilon_2 = 0$, then $x = n_1 = n_2^g = y^g$, which is a contradiction. But if $\epsilon_2 = 1$, then $n = n_1 = n_2^g n$, so $n_2 = 1$ and $y = 1$, which again is a contradiction. Hence we may assume that $m_1 \neq 1$. If $\epsilon_1 = 1$, then $m = m_1 = m_2^g m$, so $m_2 = 1$, which is a contradiction. Thus, $\epsilon_1 = 0$, that is, $m_1 = m_2^g$. By the assumption on x and y , it follows that $\epsilon_2 = 1$, and $n_1 \neq 1, n_2 \neq 1$. But then $n = n_1 = n_2^g n$, which leads to the final contradiction $1 = n_2 \neq 1$.

Now assume that there is an element $g \in G$ and numbers $\epsilon_1, \epsilon_2 \in \{0, 1\}$ such that $x = x^g m^{\epsilon_1} n^{\epsilon_2}$, that is, $m_1 = m_1^g m^{\epsilon_1}$ and $n_1 = n_1^g n^{\epsilon_2}$. If $m_1 = 1$, then $\epsilon_1 = 0$, while if $m_1 \neq 1$, then $m = m_1 = m_1^g m^{\epsilon_1}$, which again implies that $\epsilon_1 = 0$. Thus $\epsilon_1 = 0$, and $\epsilon_2 = 0$ by symmetry, so $x = x^g$.

Altogether, it follows that in $(\mathcal{K}_x - \mathcal{K}_y)(1 - m)(1 - n)$, viewed as a \mathbb{Z} -linear combination of elements of G , the coefficient of x is 1. In particular, $(1 - m)(1 - n)$ does not annihilate $\mathcal{K}_x - \mathcal{K}_y$, so $\mathcal{K}_x - \mathcal{K}_y$ is not contained in (\hat{M}, \hat{N}) , and the lemma is proved. \square

3. The examples

THEOREM A. *There is a group G of order 144 ($= 2^4 \cdot 3^2$) such that $\mathbb{Z}G$ has a normalized automorphism α which has no Zassenhaus factorization. Moreover, α can be chosen to have finite order.*

The group G is a semidirect product $(L \times N) \rtimes \langle a \rangle$, where $L = \langle y, z \rangle \cong C_2 \times C_2$ and $N = \langle v, w \rangle \cong C_3 \times C_3$ are elementary abelian groups of order 4 and 9, respectively, and the element a is of order 4, acting non-trivially on L and fixed-point free on N . More precisely, if L and N are considered as vector spaces over the prime fields \mathbb{F}_2 and \mathbb{F}_3 , respectively, then a acts on L by multiplication with $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in \text{GL}_2(\mathbb{F}_2)$, and on N by multiplication with $\begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix} \in \text{GL}_2(\mathbb{F}_3)$ (that is, $y^a = zy$, $z^a = z$, $v^a = w$ and $w^a = v^2$). Note that $[a^2, L] = 1$.

The center of G is given by $M = \langle z \rangle$. Note that L , M and N are characteristic subgroups of G . The Sylow 2-subgroup $S = \langle y, z, a \rangle$ of G is a complement to N in G , and we shall identify G/N with S . The quotient G/M will be identified with the direct product of the Frobenius group $F = \langle v, w, a \rangle$ and the group $\langle \bar{y} \rangle$ of order 2.

Let $\Lambda = \mathbb{Z}G/(\hat{M}, \hat{N})$, and let Γ be the image of $\mathbb{Z}G$ under the natural map $\mathbb{Z}G \rightarrow \mathbb{Z}G/M \oplus \mathbb{Z}G/N$. Then $\mathbb{Z}G$ can be described by pull-back diagrams, as described in the Introduction.

The group-theoretical obstruction. Recall that a acts on N via the matrix $\begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix}$, which is inverted by $\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$. Hence there is $\varphi \in \text{Aut}(G)$, of order 2, which maps a to a^3 and acts on L via the matrix $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ (like a does) and on N via the matrix $\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$ (that is, $y\varphi = zy$, $z\varphi = z$, $v\varphi = v$ and $w\varphi = w^2$). We will show:

There is no $\rho \in \text{Aut}(G)$ which differs on Λ from φ by a central automorphism, and induces on Γ a central automorphism.

Let $\sigma \in \text{Aut}(G)$, and assume that σ maps $LN a$ to $LN a^3$, i.e., that σ induces a non-trivial automorphism on $G/LN \cong \langle a \rangle$. We claim that there is a conjugacy class of G contained in LN which is not fixed by σ . Note that σ acts on L via the matrices $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ or $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ (the only invertible matrices which centralize the action of a on L). Hence we may assume, after modifying σ by conjugation with a if necessary, that σ fixes all elements of L . Assume that σ fixes the conjugacy classes of all elements in LN . Let $n \in N$. Then there is $g \in G$ such that $y(n\sigma) = (yn)\sigma = y^g n^g$, that is, $g \in C_G(y) =$

$LN\langle a^2 \rangle$. Consequently $n\sigma = n$ or $n\sigma = n^2$, and since $n \in N$ was chosen arbitrary, it follows that σ acts on N by multiplication with a scalar. But then $(n\sigma)^a = (n^a)\sigma = n\sigma^{a\sigma}$ for all $n \in N$, and we obtain the contradiction $(a\sigma)a^{-1} \in LNa^2 \cap C_G(N) = \emptyset$.

Now assume that there is $\rho \in \text{Aut}(G)$ which differs on Λ from φ by a central automorphism and induces on Γ a central automorphism. As Γ naturally projects onto the commutative ring $\mathbb{Z}G/LN$, the automorphism ρ induces the identity mapping on G/LN . Note that φ fixes the conjugacy classes of all elements in L and in N . Hence it follows from the description of $\mathbb{Z}G$ as a pull-back that $\varphi\rho^{-1}$ (as automorphism of $\mathbb{Z}G$) fixes the class sums of all elements in LN . But then $\varphi\rho^{-1}$ induces the identity mapping on G/LN , as we have just seen, and we arrive at the contradiction that φ induces the identity mapping on G/LN .

The Sylow 2-subgroup S of G . We shall construct a unit $\gamma_1 \in \mathbb{Z}S$ of order 2 such that the conjugation with γ_1 agrees with φ on $\mathbb{Z}S/(9, 1+z)$. An isomorphism

$$\Theta : \mathbb{Q}S \rightarrow \mathbb{Q}S/M \oplus \text{Mat}_2(\mathbb{Q}) \oplus \text{Mat}_2(\mathbb{Q})$$

is given by $z\Theta = (\bar{z}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix})$, $y\Theta = (\bar{y}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix})$ and $a\Theta = (\bar{a}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix})$. As a consequence of Schur's relations (cf. [5, V.5.7]), $(\mathbb{Z}S)\Theta$ contains $\text{Mat}_2(8\mathbb{Z}) \oplus \text{Mat}_2(8\mathbb{Z})$, and Θ provides an isomorphism between $\mathbb{Z}S/(9, 1+z)$ and $\text{Mat}_2(\mathbb{Z}/9\mathbb{Z}) \oplus \text{Mat}_2(\mathbb{Z}/9\mathbb{Z})$, i.e., an element x of $\mathbb{Z}S$ is contained in the ideal $(9, 1+z)$ if and only if the integral entries of the matrices X_i , defined by $x\Theta = (\bar{x}, X_1, X_2)$, are divisible by 9.

The automorphism φ fixes the blocks which do not contain M in their kernel, and is, via the given isomorphism, the conjugation with $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ on each of these blocks. This matrix has determinant -1 , but we can temporarily modify φ by conjugation with y to obtain conjugation with $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ on both blocks. As a product of elementary matrices, $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$, which is modulo 9 the same as $\begin{bmatrix} 1 & 0 \\ -8 & 1 \end{bmatrix} \begin{bmatrix} 1 & 8 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -8 & 1 \end{bmatrix} = \begin{bmatrix} -63 & 8 \\ 496 & -63 \end{bmatrix}$. Thus, if we put $u_1 = (\bar{y}, \begin{bmatrix} -63 & -8 \\ 496 & 63 \end{bmatrix}, \begin{bmatrix} -63 & -8 \\ 496 & 63 \end{bmatrix})$, then $u_1\Theta^{-1}$ is a unit in $\mathbb{Z}S$, and conjugation with $u_1\Theta^{-1}$ agrees with φ on $\mathbb{Z}S/(9, 1+z)$. Note that u_1 has order 2. For technical reasons, we choose $\gamma_1 = a^2(u_1\Theta^{-1})$. (Note that a^2 is a central element of S of order 2.) We mention that, as a linear combination of group elements,

$$\gamma_1 = a^2[y + (1-z)(-32y + 124a - 124ya - 2a^3 - 2ya^3)].$$

The Frobenius group F . We will construct a unit $\gamma_2 \in \mathbb{Z}F$ of order 2 such that conjugation with γ_2 agrees with φ on $\mathbb{Z}F/(2, \tilde{N})$. An isomorphism

$\Omega : \mathbb{Z}F \rightarrow \mathbb{Q}F/N \oplus \text{Mat}_4(\mathbb{Q}) \oplus \text{Mat}_4(\mathbb{Q})$ is given by

$$\begin{aligned} a\Omega &= \left(\bar{a}, \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \right), \\ v\Omega &= \left(\bar{v}, \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & -1 \end{bmatrix} \right), \\ w\Omega &= \left(\bar{w}, \begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \right). \end{aligned}$$

As in the previous paragraph, it follows that $\text{Mat}_4(9\mathbb{Z}) \oplus \text{Mat}_4(9\mathbb{Z}) \subset (\mathbb{Z}F)\Omega$, and that an element $x \in \mathbb{Z}F$ is contained in the ideal $(2, \hat{N})$ if and only if the integral entries of the matrices X_i , defined by $x\Omega = (\bar{x}, X_1, X_2)$, are divisible by 2. The automorphism φ fixes the blocks of (4×4) -matrices over \mathbb{Q} , and is given by conjugation with the matrices

$$A_1 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad A_2 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

on the first and second block, respectively. The unit γ_2 is obtained by modifying the element va^2 of order 2,

$$va^2\Omega = \left(\bar{v}\bar{a}^2, \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & -1 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & -1 \end{bmatrix} \right),$$

by an element of $\text{Mat}_4(9\mathbb{Z}) \oplus \text{Mat}_4(9\mathbb{Z})$. The second entry is easily modified (see the unit u_2 below). To modify the third entry $(va^2\Omega)_3$ one could observe that there is $C \in \text{SL}_4(\mathbb{Z})$ such that $C^{-1}(va^2\Omega)_3C$ is equivalent to A_2 modulo 2; for example, one could take

$$C = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \in \text{SL}_4(\mathbb{Z}).$$

Then one could write C as a product of elementary matrices, and “lift” these matrices, as in the previous paragraph, to get the modified entry. However,

this may lead to matrices with large entries. We checked that

$$u_2 = \left(\bar{v}a^2, \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 8 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} -10 & -10 & 0 & -9 \\ 18 & 10 & 9 & 18 \\ 18 & 9 & 10 & 18 \\ -9 & 0 & -10 & -10 \end{bmatrix} \right)$$

is a unit of order 2, and that $u_2\Omega^{-1} \in \mathbb{Z}F$, since u_2 is obtained from $va^2\Omega$ by adding an element of $\text{Mat}_4(9\mathbb{Z}) \oplus \text{Mat}_4(9\mathbb{Z})$. Moreover, the second and third entries are congruent to A_1 and A_2 modulo 2, respectively, so we may choose $\gamma_2 = u_2\Omega^{-1}$. We mention that, as a linear combination of group elements,

$$\begin{aligned} \gamma_2 &= va^2 + (v-1)[(-3v+3vw+3vw^2)+3(1+v)a^2 \\ &\quad + (-2-3v+3vw+w+w^2)a + (-2-3v+3vw^2+w+w^2)a^3]. \end{aligned}$$

We are now ready to complete the proof of Theorem A.

Note that y maps to a central element of order 2 in G/M . Thus $y\gamma_2$ is a unit in $\mathbb{Z}G$ whose image in $\mathbb{Z}G/M$ has order 2, and conjugation with $y\gamma_2$ agrees with φ on $(\mathbb{Z}G/M)/(2, \hat{N})$. Both γ_1 and $y\gamma_2$ map to the image of a^2y in $\mathbb{Z}G/NM$. Hence the pair $(\gamma_1, y\gamma_2)$ gives rise to a unit $\gamma \in \Gamma$ of order 2 such that conjugation with γ agrees with φ on

$$(\mathbb{Z}G/M)/(2, \hat{N}) \oplus (\mathbb{Z}G/N)/(9, \hat{M}).$$

It follows that there is an automorphism α of $\mathbb{Z}G$ of order 2 which is the conjugation with γ on Γ (and therefore preserves the augmentation), and agrees with φ on Λ . Since we have already shown that α has no Zassenhaus factorization, Theorem A is proved.

THEOREM B. *There is a group G of order 1200 ($= 2^4 \cdot 3 \cdot 5^2$), with abelian Sylow subgroups and Sylow tower, such that $\mathbb{Z}G$ has a normalized automorphism which has no Zassenhaus factorization.*

The group G is a semidirect product $G = (M \times N) \rtimes (\langle a \rangle \times \langle b \rangle)$, where $M = \langle s, t \rangle \cong C_5 \times C_5$ and $N = \langle v, w \rangle \cong C_2 \times C_2$ are elementary abelian groups of order 25 and 4, respectively, and the elements a and b are of order 3 and 4, respectively. The element a acts on M via the matrix $A_1 = \begin{bmatrix} 1 & 4 \\ 3 & 3 \end{bmatrix} \in \text{GL}_2(\mathbb{F}_5)$ (i.e., $s^a = st^4$, and so on), and on N via the matrix $A_2 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \in \text{GL}_2(\mathbb{F}_2)$. The element b acts on M via the matrix $B = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} \in \text{GL}_2(\mathbb{F}_5)$, and trivially on N (so that G has abelian Sylow subgroups). Note that M and N are characteristic subgroups of G , and that G has a Sylow tower.

The matrix $C_1 = \begin{bmatrix} 1 & 0 \\ 3 & 4 \end{bmatrix} \in \text{GL}_2(\mathbb{F}_5)$ inverts A_1 , and $C_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \in \text{GL}_2(\mathbb{F}_2)$ inverts A_2 . Both matrices have order 2, so there is $\varphi \in \text{Aut}(G)$, of order 2, which maps a to a^{-1} , fixes b , acts on M via C_1 and on N via C_2 .

Again, let $\Lambda = \mathbb{Z}G/(\hat{M}, \hat{N})$, and let Γ be the image of $\mathbb{Z}G$ under the natural map $\mathbb{Z}G \rightarrow \mathbb{Z}G/M \oplus \mathbb{Z}G/N$. Let $K = \langle a, b \rangle$. The quotients G/M and G/N

will be identified with NK and MK , respectively. We first prove the following group-theoretical obstruction.

There is no $\rho \in \text{Aut}(G)$ which differs on Λ from φ by a central automorphism, and induces on Γ a central automorphism.

By way of contradiction, assume that there is $\rho \in \text{Aut}(G)$ with these properties, and let $\sigma = \varphi\rho^{-1}$. As Γ projects onto the commutative ring $\mathbb{Z}G/MN$, the automorphism ρ induces the identity mapping on G/MN . Consequently, σ maps MNa to MNa^{-1} . Since $\text{Aut}(N)$ is the symmetric group of order 6, it follows that $\sigma^2|_N = \text{id}|_N$, and there is $1 \neq n \in N$ with $n\sigma = n$. Since σ induces a central automorphism of Λ , it follows from Lemma 2.4 that σ fixes the conjugacy classes of all elements in MN . Let $m \in M$. Then there is $k \in K$ such that $(mn)\sigma = (mn)^k$, that is, $m\sigma = m^k$ and $n = n\sigma = n^k$. Since $C_K(n) = \langle b \rangle$, it follows that $k \in \langle b \rangle$, and $m\sigma = m^i$ for some $i \in \mathbb{N}$. Since $m \in M$ can be chosen arbitrarily, it follows that σ acts on M by multiplication with a scalar, and there is $c \in \langle b \rangle$ with $m\sigma = m^c$ for all $m \in M$. Thus $m^{ac} = (m^a)\sigma = m\sigma^{ac} = m^{ca^{-1}} = m^{a^{-1}c}$, that is, $m^{a^2} = m$, again for all $m \in M$. But a^2 acts on M by inversion, so we have reached a contradiction.

There is $u_1 \in \text{V}(\mathbb{Z}N\langle a \rangle)$ with $u_1\varepsilon_N = \varepsilon_N$, and conjugation with u_1 agrees with φ on $\mathbb{Z}(NK)/(25, \hat{N})$.

Note that $N\langle a \rangle$ is the alternating group of order 12, and that the semidirect product $H = N\langle a \rangle \rtimes \langle \phi \rangle$ is the symmetric group of order 24. The faithful irreducible representation of the alternating group $N\langle a \rangle$ is the restriction of a 3-dimensional rational representation Θ of H with $\det(\Theta(\varphi)) = 1$. Since b is central in NK and $b\varphi = b$, the assertion follows from Corollary 2.3.

There is $u_2 \in \text{V}(\mathbb{Z}MK)$ with $u_2\varepsilon_M = \varepsilon_M$, and conjugation with u_2 agrees with φ on $\mathbb{Z}(MK)/(4, \hat{M})$.

Let $H = MK \rtimes \langle f \rangle$ with $f^2 = 1$ and $x^f = x\varphi$ for all $x \in MK$. Let $U = \langle M, b, f \rangle \leq H$. There are normal subgroups $L_1 = \langle st, f \rangle$ and $L_2 = \langle s, b^2f \rangle$ of U with $U/L_i \cong C_5 \rtimes C_4$, a Frobenius group which has exactly one faithful irreducible character which comes from a 4-dimensional representation over the rationals. Let λ_i be the irreducible character of U with kernel L_i and put $\zeta_i = \lambda_i^H|_{MK}$. Then ζ_i is a faithful character of degree 12 of the Frobenius group MK , and therefore irreducible (see [5, V.16.13]). Moreover, by Mackey's Theorem, $\lambda_i^H|_{M\langle b \rangle} = \bigoplus_{x \in \langle a \rangle} {}^x\lambda_i|_{M\langle b \rangle}$, and since the kernels of $\lambda_1|_M$ and $\lambda_2|_M$, which are $\langle st \rangle$ and $\langle s \rangle$, respectively, are not conjugate by an element of $\langle a \rangle$, it follows that $\zeta_1 \neq \zeta_2$, and that ζ_1 and ζ_2 are irreducible characters of MK which do not have M in their kernel. Since $\det(\lambda_i(f)) = 1$, and $\lambda_i(1)$ is even, it follows that $\det(\lambda_i^H(f)) = 1$. The assertion now follows from Corollary 2.3.

Altogether, it follows that there is a unit γ of Γ which maps to u_1 in $\mathbb{Z}NK$ and to u_2 in $\mathbb{Z}MK$, and an augmentation preserving automorphism α of $\mathbb{Z}G$ which is the conjugation with γ on Γ and which agrees with φ on Λ (as shown above). Since we have already shown that α has no Zassenhaus factorization, Theorem B is proved.

REFERENCES

- [1] P. F. Blanchard, *Exceptional group ring automorphisms for some metabelian groups. I, II*, Comm. Algebra **25** (1997), 2727–2733, 2735–2742. MR **98k**:20007
- [2] F. M. Bleher and T. Chinburg, *Operations on ring structures preserved by normalized automorphisms of group rings*, J. Algebra **215** (1999), 531–542. MR **2000b**:16051
- [3] C. W. Curtis and I. Reiner, *Methods of representation theory, Vol. II*, Wiley-Interscience, New York, 1987.
- [4] M. Hertweck, *Eine Lösung des Isomorphieproblems für ganzzahlige Gruppenringe von endlichen Gruppen*, Ph.D. Thesis, University of Stuttgart, 1998, ISBN 3-8265-6055-8.
- [5] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, Berlin, 1967.
- [6] W. Kimmerle, *On automorphisms of $\mathbb{Z}G$ and the Zassenhaus conjectures*, Canad. Math. Soc. Conf. Proc. **18** (1996), 383–397.
- [7] W. Kimmerle and K. W. Roggenkamp, *Projective limits of group rings*, J. Pure Appl. Algebra **88** (1993), 119–142. MR **94f**:20008
- [8] L. Klingler, *Construction of a counterexample to a conjecture of Zassenhaus*, Comm. Algebra **19** (1991), 2303–2330.
- [9] K. W. Roggenkamp and L. L. Scott, *On a conjecture of Zassenhaus for finite group rings*, manuscript, November 1988.
- [10] L. L. Scott, *On a conjecture of Zassenhaus, and beyond*, Proceedings of the International Conference on Algebra, Part 1 (Novosibirsk, 1989), Amer. Math. Soc., Providence, RI, 1992, pp. 325–343. MR **93g**:20010
- [11] H. Zassenhaus, *Brauer invariance II*, Tagungsbericht 24/1988, Mathematisches Forschungsinstitut Oberwolfach, 1988.

MATHEMATISCHES INSTITUT B, UNIVERSITÄT STUTTGART, PEAFFENWALDRING 57, D-70569 STUTTGART, GERMANY

E-mail address: hertweck@mathematik.uni-stuttgart.de