Arch. Math., Vol. 65, 281–288 (1995)

0003-889X/95/6504-0281 $ 3.10/0

Nilpotent metacyclic irreducible linear groups of odd order

By

L. G. Kovács and Hyo-Seob Sim *)

Let $\mathbb{F}$ be an arbitrary field, G a nilpotent metacyclic group of odd order, and $G^{\mathrm{Aut}\,G}$ the subgroup consisting of those elements of G which are fixed by every automorphism of G. We show that the images of two faithful irreducible $\mathbb{F}$-representations of G are linearly isomorphic if and only if the restrictions of the representations to $G^{\mathrm{Aut}\,G}$ are equivalent. If the centre of G is cyclic and the characteristic of $\mathbb{F}$ does not divide the order of G, then the number of linear isomorphism types of the irreducible $\mathbb{F}$-linear groups that are abstractly isomorphic to G is precisely the number of equivalence types of faithful irreducible $\mathbb{F}$-representations of $G^{\mathrm{Aut}\,G}$. For groups of this kind, we also show how to calculate the order of $G^{\mathrm{Aut}\,G}$.

1. Introduction. The set of those elements of a group G which are fixed by every automorphism of G is a subgroup called the *autocentre* (or *absolute centre*) of G; we shall denote it by $G^{\mathrm{Aut}\,G}$. This subgroup plays an unexpected role here.

Theorem 1.1. *Let $\mathbb{F}$ be a field, G a nilpotent metacyclic group of odd order, and ϱ, σ faithful irreducible representations of G over $\mathbb{F}$. The images of ϱ and σ are linearly isomorphic if and only if the restrictions of ϱ and σ to $G^{\mathrm{Aut}\,G}$ are equivalent.*

It is well-known that the existence of faithful irreducible $\mathbb{F}$-representations for G is equivalent to the centre of G being cyclic and the characteristic of $\mathbb{F}$ not being a divisor of the order of G. We show (as Lemma 3.1) that if such representations exist then they all have the same degree. Two $\mathbb{F}$-linear groups are called *linearly isomorphic* if they have the same degree and when the vector spaces on which they act are identified (along some $\mathbb{F}$-isomorphism) the groups become conjugate subgroups of the relevant general linear group.

For comparison with Theorem 1.1, we mention a special case of Theorem 3.1 of [7]: under the hypotheses of Theorem 1.1, the representations ϱ and σ are equivalent if and only if their restrictions to the centre of G are equivalent.

*) Part of the work reported here was done during the conference "Groups-Korea 1994" in Pusan, and the first author is grateful to the organizers for the financial assistance and hospitality which enabled his participation. The second author was supported in part by the Non-Directed Research Fund, Korea Research Foundation, 1994.

Corollary 1.2. *If the centre of G is cyclic and the characteristic of $\mathbb{F}$ does not divide the order of G, then the number of linear isomorphism types of the irreducible $\mathbb{F}$-linear groups that are abstractly isomorphic to G is precisely the number of equivalence types of faithful irreducible $\mathbb{F}$-representations of the cyclic group $G^{\mathrm{Aut}\,G}$.*

In order to facilitate applications of these results, we give an explicit description of $G^{\mathrm{Aut}\,G}$. It is clear that $G^{\mathrm{Aut}\,G}$ is the direct product of the $P^{\mathrm{Aut}\,P}$ where P ranges through the Sylow subgroups of G. Thus it suffices to describe $G^{\mathrm{Aut}\,G}$ under the assumptions that G is a nonabelian metacyclic p-group with cyclic centre Z, and $p > 2$. If G is a semidirect product of two cyclic groups, we shall see (in Lemma 2.1) that every automorphism of Z is the restriction of some automorphism of G, whence it follows that $G^{\mathrm{Aut}\,G} = 1$. It was proved by Lindenberg [3] that if G has no such semidirect decomposition then G has a presentation

$$G = \langle a, b \mid a^{p^\alpha} = b^{p^\beta}, b^{p^{\beta+\gamma}} = 1, a^{-1} b a = b^{1+p^\gamma} \rangle \tag{1}$$

with

$$\alpha > \beta > \gamma > 0\,. \tag{2}$$

(If G is defined by (1) and the parameters α, β, γ satisfy (2), then the order of the commutator subgroup G' is p^β while the factor group G/G' is the direct product of a cyclic group of order p^α and a cyclic group of order p^γ, so these parameters are invariants of G.)

Theorem 1.3. *If $p > 2$ and α, β, γ satisfy* (2), *then the autocentre $G^{\mathrm{Aut}\,G}$ of the group defined by* (1) *is $\langle a^{p^\delta} \rangle$ where $\delta = \max\{\beta + \gamma, \alpha - \beta + 2\gamma\}$; in particular,*

$$|G^{\mathrm{Aut}\,G}| = \min\{p^{\alpha-\beta}, p^{\beta-\gamma}\}\,.$$

Concerning representations and linear groups, we depend on [7] and keep to the terminology that was used there. Appeals to [7] do not really need the odd order assumption: for those, it would be sufficient to assume that the nilpotency class of the Sylow 2-subgroup of G is at most 2. However, the pursuit of this slight generalization does not seem justified here.

2. Restricting automorphisms to the centre.

Lemma 2.1. *Let G be a semidirect product of two cyclic p-groups, let Z be the centre of G, and suppose that Z is cyclic. Then* $(\mathrm{Aut}\,G)\downarrow_Z = \mathrm{Aut}\,Z$.

Proof. Say, $G = \langle a \rangle \ltimes \langle b \rangle$. In this case G has a presentation of the form

$$G = \langle a, b \mid a^{p^m} = b^{p^n} = 1, a^{-1} b a = b^k \rangle\,.$$

Each element of G can be written as $a^i b^j$. If $a^i b^j$ is central, then it commutes with b, so a^i also commutes with b, so a^i is central; similarly, b^j is central. This proves that Z is the product of its intersections with $\langle a \rangle$ and $\langle b \rangle$. The two cyclic subgroups being disjoint,

this product is direct. A cyclic p-group has no nontrivial direct decomposition, so here one of the direct factors must be trivial. As $\langle b\rangle$ is a nontrivial normal subgroup and G is nilpotent, $\langle b\rangle$ cannot avoid Z. The only option left is that Z avoids $\langle a\rangle$ and lies in $\langle b\rangle$.

The defining relations of the presentation above hold equally well with a and b^s in place of a and b, as long as $p \nmid s$. From this, one can see that each automorphism of $\langle b\rangle$, and hence also each automorphism of Z, is the restriction of some automorphism of G. □

Next we make a strictly temporary definition. Given any group Z, we call a subgroup A of $\operatorname{Aut} Z$ *good* (in $\operatorname{Aut} Z$) if, for some subgroup of Z, A consists of all those automorphisms of Z which fix that subgroup elementwise. For example, if Z is cyclic of order n, then each element of $\operatorname{Aut} Z$ is of the form $\zeta_k: z \mapsto z^k$ with k prime to n, and the good A may be indexed by the divisors d of n: they are the subgroups of the from $\{\zeta_k \mid k \equiv 1 \bmod d\}$. It is easy to see that, when Z is finite and cyclic, A is good if and only if the restriction of A to each Sylow subgroup of Z is good (in the automorphism group of that Sylow subgroup). Indeed, this is true whenever Z is a finite nilpotent group.

Given a group G, it makes sense to ask whether the restriction of $\operatorname{Aut} G$ to the centre of G is good (in the automorphism group of the centre of G). The answer may be yes or no, depending on G. Again, it is an elementary exercise to see that for finite nilpotent G answer is "yes" if and only if the answer is "yes" for each Sylow subgroup of G.

The pivotal point of this note is the following.

Lemma 2.2. *Let G be a finite nilpotent metacyclic group of odd order, let Z be the centre of G, and suppose that Z is cyclic. Then* $(\operatorname{Aut} G)\downarrow_Z$ *is good* (*in* $\operatorname{Aut} Z$).

Proof. By the discussion above, we may assume that G is a p-group. If G is a semidirect product of two cyclic groups, the claim follows from Lemma 2.1. It was proved in Lindenberg [4] that if a metacyclic p-group G of odd order is not such a semidirect product then $\operatorname{Aut} G$ is a p-group. Our description above of the good subgroups of the automorphism group of a cyclic group shows that each p-subgroup of the automorphism group of a cyclic p-group, with p odd, is good. □

3. The linear isomorphism problem. The aim of this section is to prove Theorem 1.1 and Corollary 1.2. The first lemma could be avoided, but it completes the picture and will ease the exposition.

Lemma 3.1. *If G is a finite nilpotent metacyclic group of odd order and $\mathbb{F}$ is an arbitrary field, then all faithful irreducible $\mathbb{F}$-representations of G have the same degree.*

Proof. When the characteristic of $\mathbb{F}$ is nonzero, this is a special case of Theorem 3.3 of [6]. The assumption on the characteristic of $\mathbb{F}$ is used there only once (at the beginning of the third paragraph of the proof of Theorem 3.1), and then only to ensure that the Schur index of an irreducible representation of a certain subgroup of G is 1. By a result of Roquette [5], all irreducible representations of nilpotent groups of odd order have Schur index 1, so in the present case the arguments of [6] may be used without that assumption. □

We also need a piece of routine.

Lemma 3.2. *Let $\mathbb{F}$ be an arbitrary field, Z a finite cyclic group, C a subgroup of Z, and $\mu: Z \to \mathrm{GL}(d, \mathbb{F})$, $v: Z \to \mathrm{GL}(d, \mathbb{F})$ faithful irreducible representations whose restrictions to C are equivalent. Then $\mathrm{GL}(d, \mathbb{F})$ has an inner automorphism, β say, such that $\mu\downarrow_C = (v\beta)\downarrow_C$ and $Z\mu = Zv\beta$.*

Proof. This is just a variation on the case $C = 1$, which is certainly well known ("if a general linear group has irreducible cyclic subgroups of a given finite order, then these form a single conjugacy class of subgroups"): for example, it is a direct consequence of Theorem B, 9.8 in the book [1] of Doerk and Hawkes. We paraphrase and extend the relevant claims proved in [1], leaving it to the reader to adapt and extend the proofs.

Denote the order of Z by n. (Since Z is assumed to admit faithful irreducible representations over $\mathbb{F}$, the characteristic of $\mathbb{F}$ cannot divide n.) Let $\mathbb{E}$ be the splitting field of the polynomial $x^n - 1$ over $\mathbb{F}$: our d is precisely the degree of the field extension $\mathbb{E} | \mathbb{F}$. Write $\mathbb{E}^1$ for $\mathbb{E}$ viewed as a 1-dimensional vector space over $\mathbb{E}$ and so an d-dimensional vector space over $\mathbb{F}$. Write $\mathbb{E}_1$ for the $\mathbb{F}$-algebra of all $\mathbb{E}$-linear transformations of $\mathbb{E}^1$, and $\mathbb{F}_d$ for the $\mathbb{F}$-algebra of all $\mathbb{F}$-linear transformations of $\mathbb{E}^1$. Note that the Galois group of $\mathbb{E} | \mathbb{F}$ is a subgroup in the group of units of $\mathbb{F}_d$, and that $\mathrm{GL}(d, \mathbb{F})$ may be thought of as this group of units. There is an obvious isomorphism from $\mathbb{E}$ to $\mathbb{E}_1$. The inner automorphisms of $\mathbb{F}_d$ induced by the elements of the Galois group leave $\mathbb{E}_1$ setwise invariant, and each $\mathbb{F}$-automorphism of $\mathbb{E}_1$ arises as the restriction to $\mathbb{E}_1$ of one of these inner automorphisms of $\mathbb{F}_d$.

Let C_1 be any finite subgroup of the multiplicative group of nonzero elements of $\mathbb{E}_1$, and let ζ be an inner automorphism of $\mathbb{F}_d$ that leaves C_1 setwise invariant. We claim that *then $\mathbb{F}_d$ has an inner automorphism which on C_1 agrees with ζ and which leaves $\mathbb{E}_1$ setwise invariant.* Let $\mathbb{E}'$ denote the $\mathbb{F}$-linear span of C_1. This is a subfield of $\mathbb{E}_1$, it is setwise invariant under ζ, and the restriction $\zeta\downarrow_{\mathbb{E}'}$ is an $\mathbb{F}$-automorphism of $\mathbb{E}'$. As $\mathbb{E}_1$ is a Galois extension of $\mathbb{E}'$, $\zeta\downarrow_{\mathbb{E}'}$ extends to an $\mathbb{F}$-automorphism of $\mathbb{E}_1$, and we have seen above that each $\mathbb{F}$-automorphism of $\mathbb{E}_1$ extends to an inner automorphisms of $\mathbb{F}_d$. The claim of this paragraph now follows.

For the present application, the key point in Theorem B, 9.8 of [1] is that each faithful irreducible $\mathbb{F}$-representation of Z is equivalent to one whose image lies in $\mathbb{E}_1$. Since the multiplicative group of the field $\mathbb{E}_1$ has only one subgroup of order n, it follows that $\mathbb{F}_d$ has inner automorphisms, γ and δ say, such that $Z\mu\gamma = Zv\delta \subseteqq \mathbb{E}_1$. Since $C\mu\gamma$ is the only subgroup of order $|C|$ in $Z\mu\gamma$, we also have that $C\mu\gamma = Cv\delta$.

Given that the restrictions to C of μ and v are equivalent, the same holds for $\mu\gamma$ and $v\delta$ as well. The equivalence of $(\mu\gamma)\downarrow_C$ to $(v\delta)\downarrow_C$ means that F_d has an inner automorphism, ζ say, such that $(\mu\gamma)\downarrow_C = (v\delta\zeta)\downarrow_C$. By the second last paragraph above (applied with $C_1 = C\mu\gamma = Cv\delta$), this ζ can be chosen so that it leaves $\mathbb{E}_1$ setwise invariant. Since $Zv\delta$ is the only multiplicative subgroup of order n in $\mathbb{E}_1$, we then also have $Z\mu\gamma = Zv\delta = Zv\delta\zeta$, and so $\delta\zeta\gamma^{-1}$ (restricted to $\mathrm{GL}(d, \mathbb{F})$) will do as the required β. This completes the proof of the lemma. □

Proof of Theorem 1.1. Let Z denote the centre of G, and let μ, v be irreducible constituents of the restrictions $\varrho\downarrow_Z$, $\sigma\downarrow_Z$, respectively. By Clifford's Theorem, $\varrho\downarrow_Z$ is a direct sum of copies of μ, and $\sigma\downarrow_Z$ is a direct sum of copies of v. Thus the

assumption that ϱ and σ are faithful representations of G implies that μ and ν are faithful representations of Z. In view of the easy special case of Lemma 3.1 with the cyclic Z in place of G, μ and ν have the same degree, and so if the degrees of ϱ and σ are equal then the multiplicity of μ in $\varrho\downarrow_Z$ is equal to the multiplicity of ν in $\sigma\downarrow_Z$.

Write $G^{\mathrm{Aut}\,G}$ simply as C, and assume that the images $G\varrho$ and $G\sigma$ linearly isomorphic. It follows from Theorem 4.1 of [7] that there is an α in $(\mathrm{Aut}\,G)\downarrow_Z$ such that the composite $\alpha\mu$ is equivalent to ν. In view of the preceding paragraph, if $\alpha\mu$ is equivalent to ν then $\alpha(\varrho\downarrow_Z)$ is equivalent to $\sigma\downarrow_Z$, and then (as α is trivial on C) $\varrho\downarrow_C$ is equivalent to $\sigma\downarrow_C$. This proves the "only if" part of our theorem.

For the proof of the "if" part, assume that $\varrho\downarrow_C$ is equivalent to $\sigma\downarrow_C$. Then $\mu\downarrow_C$ is equivalent to $\nu\downarrow_C$: that is, $\mu\downarrow_C = (\nu\eta)\downarrow_C$ for some inner automorphism η of $\mathrm{GL}(d,\mathbb{F})$. We may now apply Lemma 3.2 with $\nu\eta$ in place of ν, and conclude that $\mathrm{GL}(d,\mathbb{F})$ has an inner automorphism β such that $\mu\downarrow_C = (\nu\eta\beta)\downarrow_C$ and $Z\mu = Z\nu\eta\beta$. It follows that Z has an automorphism α (loosely speaking, $\alpha = \nu\eta\beta\mu^{-1}$) which fixes each element of C and is such that $\alpha\mu$ is equivalent to ν. By Lemma 2.2, any such α must lie in $(\mathrm{Aut}\,G)\downarrow_Z$. Thus Theorem 4.1 of [7] yields that $G\varrho$ and $G\sigma$ are linearly isomorphic, as required. □

Proof of Corollary 1.2. Keep the notation $C = G^{\mathrm{Aut}\,G}$. The irreducible linear groups over $\mathbb{F}$ which are abstractly isomorphic to G are precisely the groups of the form $G\varrho$ with ϱ a faithful irreducible $\mathbb{F}$-representation of G. Define a map from the set of all such representations of G to the set of equivalence types of faithful irreducible $\mathbb{F}$-representations of C as follows: map ϱ to the common equivalence type of the irreducible constituents of $\varrho\downarrow_C$. The corollary will be proved by showing that this map is surjective, and that $G\varrho$ is linearly isomorphic to $G\sigma$ if and only if this map takes ϱ and σ to the same equivalence type of representations of C.

To see this, recall that characteristic of $\mathbb{F}$ does not divide the order of G. It is an elementary exercise to show that any given faithful irreducible $\mathbb{F}$-representation $\varkappa$ of C is a constituent in the restriction to C of some faithful irreducible $\mathbb{F}$-representation μ of Z. Let ϱ be an irreducible constituent of the representation of G induced from μ: then $\varrho\downarrow_Z$ is a direct sum of copies of μ, so ϱ is faithful, and $\varrho\downarrow_C$ is a direct sum of copies of $\varkappa$. This shows that each faithful irreducible $\mathbb{F}$-representation of C occurs in the restriction of some faithful irreducible $\mathbb{F}$-representation of G. It follows from Lemma 3.1 (applied also with C in place of G) that the relevant multiplicities are all the same: thus if $\varrho\downarrow_C$ and $\sigma\downarrow_C$ have a common constituent then they are equivalent. Theorem 1.1 now gives our claim. □

4. The autocentre of the group. It remains to prove Theorem 1.3. The assumptions of that theorem will apply throughout this section.

We begin with some computation with elements of G. We shall write conjugates as usual: $b^a = a^{-1}ba$, and so on. The derived group G' is $\langle b^{p^\gamma}\rangle$, a cyclic group of order p^β. It follows (see Huppert [2], III.10.2.c and III.10.8.g) that G is a regular p-group and

$$(3) \qquad (xy)^{p^n} = x^{p^n} y^{p^n} \quad \text{whenever} \quad x, y \in G \text{ and } n \geqq \beta.$$

In particular,

$$(4) \qquad (ab)^{p^\alpha} = a^{p^\alpha} b^{p^\alpha} = b^{p^\beta + p^\alpha} = (b^{1+p^{\alpha-\beta}})^{p^\beta},$$

and if r and s are nonnegative integers then

$$(a^{1+rp^\beta}b^s)^{p^\beta} = a^{(1+rp^\beta)p^\beta}b^{sp^\beta} = a^{(1+rp^\beta)p^\beta}a^{sp^\alpha} = (a^{p^\beta})^{1+rp^\beta+sp^{\alpha-\beta}}. \tag{5}$$

Denote the centre of G by Z and set $z = a^{p^\beta}$: it is easy to verify that $Z = \langle z\rangle$ and

$$C_G(\langle b\rangle) = (\langle a\rangle \cap C_G(\langle b\rangle))\langle b\rangle = Z\langle b\rangle = \langle z, b\rangle.$$

Lemma 4.1. *Our group G has an automorphism which maps z to $z^{1+p^{\alpha-\beta}}$.*

Proof. Let $a\theta = ab$, $b\theta = b^{1+p^{\alpha-\beta}}$. By (4), the elements so defined can take the places of a and b in the first defining relation of (1). As $\langle b\theta\rangle = \langle b\rangle$, and as a and $a\theta$ lie in the same coset modulo the centralizer $\langle z, b\rangle$ of this subgroup, the second and third defining relations also remain valid after this substitution. This proves that θ extends to an endomorphism of G. As $\langle a\theta, b\theta\rangle = G$, this endomorphism is in fact an automorphism, and (5) read with $r = 0$, $s = 1$ shows that it has the required action on z. □

Let N be the subgroup of Aut G consisting of the automorphisms which fix $\langle b\rangle$ setwise.

Lemma 4.2. *The elements of N map z to elements of the form $z^{1+rp^\beta+sp^{\alpha-\beta}}$.*

Proof. The coset of a modulo the centralizer $\langle z, b\rangle$ of $\langle b\rangle$ can be characterized as

$$\{g \in G \mid x^g = x^{1+p^\gamma} \text{ for all } x \text{ in } \langle b\rangle\},$$

and therefore this coset must be fixed setwise by each element of N. Thus the elements of N map a to elements of the form az^rb^s, and so by (5) they act on z as claimed. □

Next, set $c = a^{p^{\beta-\gamma}}$. The elementary congruence

$$(1+p^m)^{p^n} \equiv 1 + p^{m+n} \bmod p^{2m+n}$$

is easily proved (for example, by induction on n) for all positive integers m, n (only the initial step $n = 1$ needing the assumption that our prime p is odd). Here it yields that $(1+p^\gamma)^{p^{\beta-\gamma}} \equiv 1 + p^\beta \bmod p^{\beta+\gamma}$, and so

$$b^c = b^{1+p^\beta}. \tag{6}$$

The proof of (3) above may now be imitated to show that

$$(xy)^{p^n} = x^{p^n}y^{p^n} \quad \text{whenever} \quad x, y \in \langle c, b\rangle \text{ and } n \geqq \gamma. \tag{7}$$

We use (6) also to deduce that $b^{ac^t} = b^{(1+p^\gamma)(1+p^\beta)^t} = b^{1+p^\gamma+tp^\beta}$ for each nonnegative integer t, whence $(c^{tp^{\alpha-\beta}}b)^{ac^t} = c^{tp^{\alpha-\beta}}b^{ac^t} = c^{tp^{\alpha-\beta}}b^{1+p^\gamma+tp^\beta}$. On the other hand,

$$\begin{aligned}(c^{tp^{\alpha-\beta}}b)^{1+p^\gamma} &= c^{tp^{\alpha-\beta}}b(c^{tp^{\alpha-\beta}}b)^{p^\gamma}\\ &= c^{tp^{\alpha-\beta}}b\,c^{tp^{\alpha-\beta+\gamma}}b^{p^\gamma} \quad \text{by (7)}\\ &= c^{tp^{\alpha-\beta}}b^{1+p^\gamma+tp^\beta} \qquad \text{since } c^{p^{\alpha-\beta+\gamma}} = a^{p^\alpha} = b^{p^\beta}.\end{aligned}$$

We have proved that

(8) $$(c^{t\,p^{\alpha-\beta}}b)^{a\,c^t} = (c^{t\,p^{\alpha-\beta}}b)^{1+p^\gamma}.$$

It is much easier to see, using only the defining relations and (3), that

$$(a\,c^t)^{p^\alpha} = (a^{p^\alpha})^{1+t\,p^{\beta-\gamma}} = (b^{p^\beta})^{1+t\,p^{\beta-\gamma}} \text{ and } (c^{t\,p^{\alpha-\beta}}b)^{p^\beta} = c^{t\,p^\alpha}b^{p^\beta} = (b^{p^\beta})^{1+t\,p^{\beta-\gamma}},$$

so

(9) $$(a\,c^t)^{p^\alpha} = (c^{t\,p^{\alpha-\beta}}b)^{p^\beta},$$

and then of course

(10) $$(c^{t\,p^{\alpha-\beta}}b)^{p^{\beta+\gamma}} = (a\,c^t)^{p^{\alpha+\gamma}} = 1\,.$$

Equations (8), (9), (10) are just the tools needed for proving the following.

Lemma 4.3. *To each nonnegative integer t, there exists an automorphism of G which maps b to $a^{t\,p^{\alpha-\gamma}}b$ and z to $z^{1+p^{\beta-\gamma}}$.*

Proof. Show that $a\mapsto a\,c^t$, $b\mapsto c^{t\,p^{\alpha-\beta}}b$ extends to an automorphism of the required kind. □

Lemma 4.4. *Each automorphism of G maps $\langle b\rangle$ to one of the subgroups $\langle a^{t\,p^{\alpha-\gamma}}b\rangle$.*

Proof. Let Y be the image of $\langle b\rangle$ under some automorphism of G. Then Y also contains the derived group G', and Y/G' is the image of $\langle b\,G'\rangle$ under some automorphism of G/G'. We shall use that $G/G' = \langle a\,G'\rangle \times \langle b\,G'\rangle$ with the order, p^α, of the first cyclic direct factor being strictly larger than the order, p^γ, of the second. If Y/G' met $\langle a\,G'\rangle$ nontrivially, then some nontrivial element of Y/G' would be a $p^{\alpha-1}$th power in G/G'. Since this is impossible in a direct factor whose order is smaller than p^α, we conclude that also $G/G' = \langle a\,G'\rangle \times (Y/G')$. The direct complements of $\langle a\,G'\rangle$ in G/G' are all of the form $\langle (a\,G')^{t\,p^{\alpha-\gamma}}(b\,G')\rangle$. It follows from Lemma 4.3 that $\langle a^{t\,p^{\alpha-\gamma}}b\rangle \geqq G'$, so for some t we must have $Y/G' = \langle a^{t\,p^{\alpha-\gamma}}b\rangle/G'$, that is, $Y = \langle a^{t\,p^{\alpha-\gamma}}b\rangle$. □

Proof of Theorem 1.3. It suffices to prove that

$$G^{\mathrm{Aut}\,G} = \{g\in Z \mid g^{p^{\alpha-\beta}} = g^{p^{\beta-\gamma}} = 1\}\,.$$

Lemma 4.1 and Lemma 4.3 with $t=1$ show that the left hand side is contained in the right hand side. Lemma 4.2 yields that the centralizer in Aut G of the right hand side contains N. The automorphisms discussed in Lemma 4.3 also lie in that centralizer, and Lemma 4.4 implies that each coset of Aut G modulo N contains at least one of these automorphisms: thus the centralizer must be all of Aut G. □

We note that it would be easy to expand these arguments into a proof of Satz 1 in Lindenberg [4], which gives the precise order of Aut G. That would make this paper independent of [4], though we would still depend on his result (Satz 2.9 in [3]) that each metacyclic p-group of odd order is either a semidirect product of cyclic groups or admits a presentation of the form (1).

References

[1] K. DOERK and T. HAWKES, Finite soluble groups. Expositions in Mathematics **4**, Berlin-New York 1992.
[2] B. HUPPERT, Endliche Gruppen I. Berlin-Heidelberg-New York 1967.
[3] W. LINDENBERG, Struktur und Klassifizierung bizyklischer p-Gruppen. Ber. Gesellsch. Math. und Datenverarb. **40** (1971).
[4] W. LINDENBERG, Eine Klasse von p-Gruppen, deren Automorphismengruppen p-Gruppen sind. Period. Math. Hungar. **5**, 171–183 (1974).
[5] P. ROQUETTE, Realisierung von Darstellungen endlicher nilpotenter Gruppen. Arch. Math. **9**, 241–250 (1958).
[6] H.-S. SIM, Degrees of irreducible representations of metacyclic groups. Comm. Algebra **21**, 3773–3777 (1993).
[7] H.-S. SIM, Faithful irreducible representations of metacyclic groups. J. Algebra **170**, 907–915 (1994).

Eingegangen am 30. 1. 1995

Anschrift der Autoren:

L. G. Kovács
School of Mathematical Sciences
Australian National University
Canberra ACT 0200
Australia

Hyo-Seob Sim
Department of Natural Sciences
Pusan National University of Technology
Pusan 608-739
South Korea