AUTOMORPHISMS OF SEMIDIRECT PRODUCTS

M.J. Curran
Department of Mathematics and Statistics, University of Otago,
Dunedin, New Zealand

[Accepted 28 March 2008. Published 18 November 2008.]

Abstract

In this note we describe the group of automorphisms of a finite semidirect product $G = HK$ that fix the normal subgroup H of G as a set. In particular if H is a characteristic subgroup of G, this group will give the full automorphism group of G.

1. Results

Suppose the finite group G is a direct product $G = H \times K$, where groups H and K have no common direct factor. Then [3, theorem 3.2] shows that the automorphism group of G, Aut G, is isomorphic to a group of 2×2 matrices of homomorphisms

$$\left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} : \begin{array}{ll} \alpha \in \mathrm{Aut}\, H, & \beta \in \mathrm{Hom}(K, Z(H)) \\ \gamma \in \mathrm{Hom}(H, Z(K)), & \delta \in \mathrm{Aut}\, K \end{array} \right\},$$

where $\mathrm{Hom}(A, Z(B))$ denotes as usual the group of homomorphisms from group A to the centre $Z(B)$ of group B. Using this isomorphism, the size and structure of Aut G can easily be determined.

In this note, we assume instead that $G = H \rtimes K$ is a semidirect product, so $G = HK$, $H \trianglelefteq G$, $K \leq G$, $H \cap K = 1$. We show that the subgroup $\mathrm{Aut}(G : H) = \{\theta \in \mathrm{Aut}\, G : \theta(H) = H\}$ of Aut G can be described straightforwardly in terms of a group of 2×2 matrices of mappings, much the same as in the direct product case. As a consequence we show in Theorem 3 that when H is abelian, $\mathrm{Aut}(G : H)$ is itself a semidirect product. This result can be found in Dietz [5, theorem 4.6], but the approach there is homological and the proof depends on a quite technical result due to Wells [10]. Of course, when H is a characteristic subgroup of G, $\mathrm{Aut}(G : H)$ $=$ Aut G. We finish by showing that the structure of some (previously known) ad hoc examples of automorphism groups can be unified using Theorem 3.

For $h \in H, k \in K$, we write $h^k = khk^{-1}$ and let

$$\mathcal{M} = \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix} : \begin{array}{l} \alpha \in \mathrm{Aut}\, H, \beta : K \to H, \delta \in \mathrm{Aut}\, K, \text{ where } \alpha, \beta, \delta \text{ satisfy} \\ (i)\ \forall k, k' \in K, \beta(kk') = \beta(k)\beta(k')^{\delta(k)} \\ (ii)\ \forall h \in H, \forall k \in K, \alpha(h^k) = \alpha(h)^{\beta(k)\delta(k)}. \end{array} \right\}$$

---

*E-mail: jcurran@maths.otago.ac.nz

doi:10.3318/PRIA.2008.108.2.205

Cite as follows: M.J. Curran, Automorphisms of semidirect products, *Mathematical Proceedings of the Royal Irish Academy* **108**A (2008), 205–210; doi:10.3318/PRIA.2008.108.2.205.

Mathematical Proceedings of the Royal Irish Academy, **108**A (2), 205–210 (2008) © Royal Irish Academy

Matrices are multiplied in $\mathcal{M}$ as usual, so

$$\begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix} \begin{pmatrix} \alpha' & \beta' \\ 0 & \delta' \end{pmatrix} = \begin{pmatrix} \alpha\alpha' & \alpha\beta' + \beta\delta' \\ 0 & \delta\delta' \end{pmatrix},$$

where $\alpha\alpha', \delta\delta'$ are compositions and $(\alpha\beta' + \beta\delta')(k) = \alpha\beta'(k)\beta\delta'(k)$. Now associate with any $\theta \in \mathrm{Aut}(G : H)$ a matrix $T(\theta) = \begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix}$, where $\alpha : H \to H, \beta : K \to H, \delta : K \to K$ are defined by $\theta(h) = \alpha(h), \forall h \in H, \theta(k) = \beta(k)\delta(k), \forall k \in K$.

Theorem 1. *If* $G = H \rtimes K$, *then* $\mathrm{Aut}(G : H) \simeq \mathcal{M}$ *under the map* T.

Proof. Suppose $\theta \in \mathrm{Aut}(G : H)$, and α, β, δ are defined as above. Then $\alpha = \theta|_H$, so $\alpha \in \mathrm{Aut}\ H$. Further $\beta(kk')\delta(kk') = \theta(kk') = \theta(k)\theta(k') = \beta(k)\delta(k)\beta(k')\delta(k') = \beta(k)\beta(k')^{\delta(k)}\delta(k)\delta(k')$, so equating components (i) follows and $\delta \in \mathrm{Hom}(K, K)$. But θ is onto, so $\delta \in \mathrm{Aut}\ K$. Also $\beta(k)\delta(k)\alpha(h) = \theta(k)\theta(h) = \theta(kh) = \theta(h^k k) = \theta(h^k)\theta(k) = \alpha(h^k)\beta(k)\delta(k)$, so (ii) follows, and thus $T(\theta) \in \mathcal{M}$. Conversely, if $M = \begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix} \in \mathcal{M}$, define $\theta : G \to G$ by $\theta(hk) = \alpha(h)\beta(k)\delta(k)$. By (i) and (ii) θ is an endomorphism on G. Further Ker $\theta = 1$, so $\theta \in \mathrm{Aut}(G : H)$ and $T(\theta) = M$. Finally it is easy to check T is a monomorphism. ■

From now on identify $\mathrm{Aut}(G : H)$ with $\mathcal{M}$. Notice $\begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} \in \mathrm{Aut}(G : H) \Leftrightarrow \beta : K \to H$ satisfies (i) $\forall k, k' \in K, \beta(kk') = \beta(k)\beta(k')^k$ and (ii) $\forall h \in H, \forall k \in K, h^k = (h^k)^{\beta(k)}$, that is, $\forall k \in K, \beta(k) \in Z(H)$. Such a map $\beta : K \to Z(H)$ satisfying (i) is often called a crossed homomorphism. We denote these maps by $\mathrm{CHom}(K, Z(H))$ and the corresponding isomorphic subgroup of $\mathrm{Aut}(G : H)$ by $B = \left\{ \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} : \beta \in \mathrm{CHom}(K, Z(H)) \right\}$. Since in fact $\rho : \mathrm{Aut}(G : H) \to \mathrm{Aut}\ H \times \mathrm{Aut}\ K$ defined by $\rho \begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix} = (\alpha, \delta)$ is clearly a homomorphism with Ker $\rho = B$, we have that $B \trianglelefteq \mathrm{Aut}(G : H)$. As usual, let $C_K(H) = \{k \in K : h^k = h, \forall h \in H\}$ and let

$T = \{\alpha \in \mathrm{Aut}\ H : \alpha(h^k) = \alpha(h)^k, \forall h \in H, \forall k \in K\} \leq \mathrm{Aut}\ H$,
$S = \{\delta \in \mathrm{Aut}\ K : k^{-1}\delta(k) \in C_K(H), \forall k \in K\} \leq \mathrm{Aut}\ K$,
$R = \{(\alpha, \delta) \in \mathrm{Aut}\ H \times \mathrm{Aut}\ K : \alpha(h^k) = \alpha(h)^{\delta(k)}\} \leq \mathrm{Aut}\ H \times \mathrm{Aut}\ K$.

Notice $\begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{Aut}(G : H) \Leftrightarrow \alpha \in T$, $\begin{pmatrix} 1 & 0 \\ 0 & \delta \end{pmatrix} \in \mathrm{Aut}(G : H) \Leftrightarrow \delta \in S$ and $\begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix} \in \mathrm{Aut}(G : H) \Leftrightarrow (\alpha, \delta) \in R$. Now define the corresponding isomorphic subgroups of $\mathrm{Aut}(G : H)$ as follows:

$$A = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix} : \alpha \in T \right\}, D = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & \delta \end{pmatrix} : \delta \in S \right\}, E = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix} : (\alpha, \delta) \in R \right\}.$$

If $\alpha \in T$ and $\delta \in S$, then $(\alpha, \delta) \in R$, so $T \times S \leq R$. Conversely the following holds.

Theorem 2. *If* $T = \text{Aut } H$ *or* $S = \text{Aut } K$ *then* $R = T \times S$, *or in terms of matrices* $E = A \times D$.

PROOF. Let $(\alpha, \delta) \in R$, so $\alpha(h^k) = \alpha(h)^{\delta(k)}, \forall h \in H, \forall k \in K$. However if $T = \text{Aut } H$, then $\alpha(h^k) = \alpha(h)^k$, so $\alpha(h)^k = \alpha(h)^{\delta(k)}$ and thus $k^{-1}\delta(k) \in C_K(H)$. That is $\delta \in S$, so $R \leq T \times S$. Thus $R = T \times S$. The proof when $S = \text{Aut } K$ is similar. ■

Theorem 2 holds, for example, if Aut H is abelian so $T = \text{Aut } H$, or if $K = \langle k \rangle$ is cyclic of order 2^n and $C_K(H) = \langle k^2 \rangle$ so $S = \text{Aut } K$.

Now if H is abelian, condition (ii) of $\mathcal{M}$ simplifies to (ii)$'$ $\forall h \in H, \forall k \in K, \alpha(h^k) = \alpha(h)^{\delta(k)}$, and this means Aut $(G : H)$ is also a semidirect product.

Theorem 3. *Let* $G = H \rtimes K$, *where* H *is abelian. Then* $\text{Aut}(G : H) = B \rtimes E \simeq \text{CHom}(K, H) \rtimes R$. *Further if* $T = \text{Aut } H$ *or* $S = \text{Aut } K$ *then* $\text{Aut}(G : H) = B \rtimes (A \times D) \simeq \text{CHom}(K, H) \rtimes (T \times S)$.

PROOF. If $\begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix} \in \text{Aut } (G : H)$ then by (ii)$'$ $\begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix} \in \text{Aut } (G : H)$, so $\begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix}^{\pm 1} \in E$ and $\begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix} \begin{pmatrix} \alpha^{-1} & 0 \\ 0 & \delta^{-1} \end{pmatrix} = \begin{pmatrix} 1 & \beta\delta^{-1} \\ 0 & 1 \end{pmatrix} \in B$. Thus $\begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix} = \begin{pmatrix} 1 & \beta\delta^{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix} \in BE$. However $B \cap E = 1$ and therefore $\text{Aut}(G : H) = B \rtimes E$. The last part follows from Theorem 2. ■

2. Examples

In the examples that follow, we sometimes interpret $H \rtimes K$ in the well-known equivalent formulation of a homomorphism $\theta : K \to \text{Aut } H$, where $h^k = \theta(k)(h)$. When θ is an isomorphism we denote $G = H \rtimes \text{Aut } H$ as usual by $\text{Hol}(H)$, the holomorph of H. When θ is just a monomorphism, so $\theta(K) \leq \text{Aut } H, G$ is called a relative holomorph of H. In either case $C_K(H) = 1$, so $S = 1$. We also denote a cyclic group of order n by C_n.

Example 1. Let $G = H \rtimes K = \langle x, y : x^n = y^k = 1, x^y = x^m \rangle$, where $H = \langle x \rangle \simeq C_n, K = \langle y \rangle \simeq C_k$ and $Z(G) = 1$. Walls [9, theorem B] has shown that Aut G $= \text{Hol}(H)$ by a calculation involving $|\text{Aut } G|$. However Theorem 3 can be used to provide the stucture of Aut G directly as follows:

(i) $Z(G) = C_H(K) \times C_K(H)$, since H and K are abelian. So if $Z(G) = 1$ then $C_K(H) = 1$ and thus G is a relative holomorph of H. That is, the order of y acting as an automorphism on H by conjugation is the same as the order of y. Thus $m^k \equiv 1 \pmod{n}$, and k is the smallest such positive integer.

(ii) $C_H(K) = 1 \Leftrightarrow (n, m-1) = 1$. For $x^i \in C_H(K) \Leftrightarrow (x^i)^y = x^i \Leftrightarrow x^{(m-1)i} = 1 \Leftrightarrow n|(m-1)i$. Thus if $(n, m-1) = 1$ then $n|i$ and $x^i = 1$. Conversely, if $(n, m-1) \neq 1$ and $i = \frac{n}{(n,m-1)}$ then $1 < i < n$ and $x^i \in C_H(K)$. Thus $[y, x] = x^y x^{-1} = x^{m-1}$ so $G' \geq H$, but G/H is abelian so $G' \leq H$. Thus $G' = H$ is characteristic, so $\mathrm{Aut}(G : H) = \mathrm{Aut}\ G$. This fact also follows from [6, lemma 10.1.1], since $C_H(K) = 1$ means y acts as a fixed-point-free automorphism on H.

(iii) Aut H is abelian, so $T = \mathrm{Aut}\ H$, and $S = 1$. Therefore by Theorem 3, $\mathrm{Aut}\ G \simeq C\mathrm{Hom}(K, H) \rtimes \mathrm{Aut}\ H$. Now if $\beta \in C\mathrm{Hom}(K, H), \beta$ is completely specified by its value at y, and if $\beta(y) = x^i$, for $0 \leq i < n$, the only requirement on i is that $\beta(y^k) = 1$. However, $\beta(y^k) = x^{(1+m+\ldots+m^{k-1})i}$ and $(1 + m + \ldots + m^{k-1})(m-1) = m^k - 1 \equiv 0 \pmod{n}$. Since $(n, m-1) = 1, 1 + m + \ldots + m^{k-1} \equiv 0 \pmod{n}$ and $\beta(y^k) = 1$, for any i. Therefore if $\beta_1(y) = x$ then $C\mathrm{Hom}(K, H) = \langle \beta_1 \rangle \simeq H$. Thus $\mathrm{Aut}\ G = H \rtimes \mathrm{Aut}\ H = \mathrm{Hol}(H)$.

A special case of this result occurs when $G = H \rtimes K = \langle x, y : x^{p^n} = y^k = 1, x^y = x^m \rangle$, where p is an odd prime. It is well-know [6, lemma 5.4.1] that $\mathrm{Aut}\ C_{p^n} \simeq C_{p^{n-1}(p-1)}$. If G is any relative holomorph of H, such that y does not act as an automorphism of p-power order, that is $k|(p^{n-1}(p-1))$ but $k \nmid p^{n-1}$, then by Beyl [1, proposition 2] if m is the corresponding primitive kth root of unity, $m \not\equiv 1 \pmod{p}$. Therefore $(p^n, m-1) = 1$ so $C_H(K) = 1$ and $Z(G) = 1$ as above. Thus for a given p^n each such group G of order $p^n k$ has the same automorphism group $\mathrm{Aut}\ G = \mathrm{Hol}(H)$. For example, each of the groups $G_1 = \langle x, y : x^7 = y^6 = 1, x^y = x^3 \rangle$, $G_2 = \langle x, y : x^7 = y^3 = 1, x^y = x^2 \rangle$, $G_3 = \langle x, y : x^7 = y^2 = 1, x^y = x^{-1} \rangle$, has $\mathrm{Hol}(C_7)$ as its automorphism group.

Furthermore, in the general case, if $k = p^{n-1}(p-1)$ and m is a primitive k th root of unity (mod p^n) then $G = \mathrm{Hol}(H)$ and $\mathrm{Aut}\ G \simeq \mathrm{Hol}(H)$; that is $Z(G) = 1$ and $\mathrm{Aut}\ G \simeq G$, so G is a complete group. In other words for each prime p, we have an infinite family of those rather rare objects, finite complete groups. For example, when $p = 3$, $G(n) = \langle x, y : x^{3^n} = y^{2.3^{n-1}} = 1, x^y = x^2 \rangle$, $n \geq 1$, is such a family of complete groups, the first group of which is the well-known case: $\mathrm{Aut}\ S_3 \simeq S_3$, the symmetric group of order 3.

If K no longer acts "faithfully" on H, say $G = \langle x, y : x^n = y^k = 1, x^y = x^m \rangle$, where $(n, m-1) = 1$ but $m^{k/s} \equiv 1 \pmod{n}$, where s is a proper divisor of k, then everything remains the same except $C_K(H) = \langle y^{k/s} \rangle$ and S may be a nontrivial subgroup of Aut K. Thus $\mathrm{Aut}\ G \simeq H \rtimes (\mathrm{Aut}\ H \times S)$. For example, if $G_4 = \langle x, y : x^7 = y^6 = 1, x^y = x^2 \rangle$, then $C_K(H) = \langle y^3 \rangle$, so $S = 1$. Thus Aut G_4 is again $\mathrm{Hol}(C_7)$, so G_4 and its automorphism group have the same order but are not isomorphic. If $G_5 = \langle x, y : x^7 = y^6 = 1, x^y = x^{-1} \rangle$, then $C_K(H) = \langle y^2 \rangle$, so $S = \mathrm{Aut}\ K \simeq C_2$ and $\mathrm{Aut}\ G_5 \simeq C_7 \rtimes (C_6 \times C_2)$.

Example 2. Let H be any abelian but not elementary abelian group, $K = \langle k \rangle \simeq C_2$ and G the dihedral group $H \rtimes K = \langle H, k : k^2 = 1, h^k = h^{-1}, \forall h \in H \rangle$. Then the well-known result that Aut $G = \mathrm{Hol}(H)$, see Rose [8, problem 488], follows from Theorem 3. First note that the elements in the complement of H in G are precisely the noncentral elements of order 2 in G, so H is characteristic. Therefore Aut $G = \mathrm{Aut}(G : H)$. Now if $\alpha \in \mathrm{Aut}\ H$, then $\alpha(h^k) = \alpha(h^{-1}) = \alpha(h)^{-1} = \alpha(h)^k, \forall h \in H$, so $T = \mathrm{Aut}\ H$, and $C_K(H) = 1$ so $S = 1$. Therefore by Theorem 3, Aut $G \simeq C\mathrm{Hom}(K, H) \rtimes \mathrm{Aut}\ H$. Further if $\beta \in C\mathrm{Hom}(K, H)$ and $\beta(k) = h$, for some $h \in H$, the only requirement on h is that $\beta(k^2) = 1$. But $\beta(k^2) = \beta(k)\beta(k)^k = hh^k = hh^{-1} = 1$. Thus we may have $\beta(k) = h$, for any $h \in H$. Hence if $H = \langle h_1 \rangle \oplus \ldots \oplus \langle h_n \rangle$, define $\beta_i(k) = h_i, 1 \leq i \leq n$, then $C\mathrm{Hom}(K, H) \simeq \langle \beta_1 \rangle \oplus \ldots \oplus \langle \beta_n \rangle \simeq H$. That is Aut $G \simeq H \rtimes \mathrm{Aut}\ H = \mathrm{Hol}(H)$.

Example 3. For p an odd prime and positive integers m and n, let $H = \langle x \rangle \simeq C_{p^m}$ and $K = \langle y \rangle \simeq C_{p^n}$. Then (see [2] for details) any nonabelian split metacyclic p-group has form $G = H \rtimes K = \langle x, y : x^{p^m} = 1 = y^{p^n}, x^y = x^{1+p^{m-r}} \rangle, m \geq 2, n \geq 1, 1 \leq r \leq \min\{m-1, n\}$. By Theorem 3, $\mathrm{Aut}(G : H) \simeq C\mathrm{Hom}(K, H) \rtimes (T \times S)$, since $T = \mathrm{Aut}\ H \simeq C_{p^{m-1}(p-1)}$ is abelian. Also since $C_K(H) = \langle y^{p^r} \rangle$, if $\delta(y) = y^{1+p^r}$, then $S = \langle \delta \rangle \simeq C_{p^{n-r}}$. Finally, it is easily seen that $C\mathrm{Hom}(K, H) = \langle \beta \rangle \simeq C_{p^{\min\{m,n\}}}$, where $\beta(y) = x$ when $n \geq m$, and $\beta(y) = x^{p^{m-n}}$ when $n < m$. The structure of Aut G is given in [2] and from that it follows that $\mathrm{Aut}(G : H)$ is a proper subgroup of index $p^{\min\{n, m-r\}}$. When $p = 2$, there are three families of metacyclic 2-groups, but the structure of $\mathrm{Aut}(G : H)$ is much the same with minor variations between the families. See [4] for details.

Example 4. For p an odd prime let $H = \langle a, b \rangle \simeq C_p \times C_p, K = \langle c \rangle \simeq C_p$ and $G = H \rtimes K = \langle a, b, c : a^p = b^p = c^p = 1, a^c = ab, b^c = b, a^b = a \rangle$, the nonabelian group of order p^3 and exponent p. By Theorem 3, $\mathrm{Aut}(G : H) \simeq C\mathrm{Hom}(K, H) \rtimes R$. Now if $\beta \in C\mathrm{Hom}(K, H)$ and $\beta(c) = h$, some $h \in H$, as in the previous examples we only require that $\beta(c^p) = 1$. However if $h = a^i b^j, 0 \leq i, j \leq p-1$, then $\beta(c^p) = h^{1+c+\ldots+c^{p-1}} = (a^{1+c+\ldots+c^{p-1}})^i (b^{1+c+\ldots+c^{p-1}})^j = (a^p b^{p\frac{(p-1)}{2}})^i (b^p)^j = 1$. Thus we may have $\beta(c) = h$, for any $h \in H$. In particular if $\beta_1(c) = a, \beta_2(c) = b$ then $C\mathrm{Hom}(K, H) = \langle \beta_1 \rangle \times \langle \beta_2 \rangle \simeq H$. Further clearly $(\alpha, \delta) \in R \Leftrightarrow \alpha \in \mathrm{Aut}\ H = GL(2, p), \delta \in \mathrm{Aut}\ K = C_{p-1}$ and (i) $\alpha(a^c) = \alpha(a)^{\delta(c)}$ (ii) $\alpha(b^c) = \alpha(b)^{\delta(c)}$. Now let $\alpha = \begin{pmatrix} i & j \\ k & l \end{pmatrix} \in GL(2, p), \delta_s \in \mathrm{Aut}\ K$, where $\delta_s(c) = c^s, 1 \leq s \leq p-1$, and let a, b correspond respectively to the basis elements $(1, 0), (0, 1)$ of H. Then from (ii) $a^k b^l = \alpha(b) = \alpha(b^c) = \alpha(b)^{\delta(c)} = (a^k b^l)^{c^s} = a^k b^{sk+l}$. Thus $sk = 0$ so $k = 0$. From (i) $a^i b^{j+l} = \alpha(ab) = \alpha(a^c) = \alpha(a)^{\delta(c)} = (a^i b^j)^{c^s} = a^i b^{si+j}$, so $l = si$. Thus $\alpha = \begin{pmatrix} i & j \\ 0 & si \end{pmatrix}$, where $1 \leq i, s \leq p-1, 0 \leq j \leq p-1$. Therefore $|R| = (p-1)^2 p$ and $|\mathrm{Aut}(G : H)| = |H||R| = (p-1)^2 p^3$. In fact, if t is a primitive root of 1 mod

p and $r_1 = \left(\begin{bmatrix} t & 1 \\ 0 & t \end{bmatrix}, \delta_1\right)$, $r_2 = \left(\begin{bmatrix} 1 & 0 \\ 0 & t \end{bmatrix}, \delta_t\right)$ and $\begin{bmatrix} t & 1 \\ 0 & t \end{bmatrix}^k = \begin{bmatrix} t & t \\ 0 & t \end{bmatrix}$, then $R = \langle r_1, r_2 : r_1^{p(p-1)} = 1 = r_2^{p-1}, r_1^{r_2} = r_1^k \rangle$. Thus $\mathrm{Aut}(G : H) \simeq H \rtimes R \simeq (C_p \times C_p) \rtimes (C_{p(p-1)} \rtimes C_{p-1})$. In fact, see [7], $|\mathrm{Aut}\ G| = p^3(p-1)^2(p+1)$ so $\mathrm{Aut}(G : H)$ is of index $p+1$ in Aut G.

REFERENCES

[1] F.R. Beyl, Cyclic subgroups of the prime residue group. *The American Mathematical Monthly* **84** (1977), 46–8.

[2] J.N.S. Bidwell and M.J. Curran, The automorphism group of a split metacyclic p-group. *Archiv der Mathematik* **87** (2006), 488–97.

[3] J.N.S. Bidwell, M.J.Curran, D.J. McCaughan, 2006 Automorphisms of direct products of finite groups, *Archiv der Mathematik* **86**, 481–9.

[4] M.J. Curran, The automorphism group of a split metacyclic 2-group. *Archiv der Mathematik* **89** (2007), 10–23.

[5] J. Dietz, Automorphisms of products of groups, in C.M. Campbell, M.R. Quick, E.F. Robertson, G.C. Smith (eds), *Groups St Andrews* , LMS Lecture Notes Series **339** (2005), 288–305.

[6] D. Gorenstein, *Finite groups*, New York, Harper and Row, 1968.

[7] F. Menegazzo, Automorphisms of p-groups with cyclic commutator subgroup. *Rendiconti del Seminario Mathematico della Universita di Padova* **90** (1993), 81–101.

[8] J.S. Rose, *A course on group theory*, London, Cambridge University Press, 1978.

[9] G.L. Walls, Automorphism groups. *The American Mathematical Monthly* **93** (1986), 459–62.

[10] C. Wells, Automorphisms of group extensions. *Transactions of the American Mathematical Society* **155** (1971), 189–94.