

AUTOMORPHISMS OF A CLASS OF METABELIAN GROUPS. II

BY

S. BACHMUTH AND H. Y. MOCHIZUKI

1. **Introduction.** This paper finishes the investigations begun in [3] on the automorphism groups of $U = F/F''(F')^m$. (The notation used is, unless indicated otherwise, consistent with that employed in [1], [2], and [3].) The purpose of this paper is to reduce the case of an arbitrary integer $m > 1$ to the case of the prime divisors in m and then to deal directly with the cases where the primes occur to a power greater than 1. We will briefly describe the organization and main results.

In §2, we collect all the necessary ring theoretic preliminaries. In particular we include a discussion and complete classification of units in $Z_m(F/F')$ although this is a little more than we need for the applications. In §3, we show (Corollary 3.3) that the representation of the IA-automorphism group of $F/F''(F')^m$ as a group of matrices over $Z_m(F/F')$ (see §2 of [3]) is decomposable into a direct product of representations of the IA-automorphisms of $F/F''(F')^{p_i^{e_i}}$, where $p_i^{e_i}$ is the highest power of the prime p_i dividing m . This in part is based upon (Theorem 3.1) the formulation of a necessary and sufficient condition for a $q \times q$ matrix over $Z_m(F/F')$ to represent an IA-automorphism of $F/F''(F')^m$. (The formulation parallels that of Theorem 1 of [1].) Thus, all problems considered here can now be reduced to the various prime power situations. A typical result is as follows: First note that an automorphism α of U induces in an obvious manner an automorphism of $U(k)$, where $U(k) = F/F''(F')^{p_k^{e_k}}$, for each p_k dividing m . We now have: an automorphism α of U/U_n is induced by an automorphism of U if and only if, when considered as an automorphism of $U(k)/U(k)_n$ for each k , α is induced by an automorphism of $U(k)$. This, in effect, because of previous work, completely solves the problem when m is squarefree. When m is not squarefree, the problem is reduced to the case where m is a power of a prime. This is dealt with in §4, where we show the following. (Refer to [2] for the meaning of $N_1(\alpha)$.)

THEOREM. *For $U = F/F''(F')^{p^e}$, an automorphism α of U/U_n ($n \geq 4$) is induced by an automorphism of U if and only if trace $N_1(\alpha)$ is divisible by p . (Recall that for m such that Z_m contains no nilpotent elements $\neq 0$, the situation was trace $N_1(\alpha) = 0$.)*

Unlike the case where Z_m contains no nontrivial nilpotent elements, we have the following:

Presented to the Society, April 4, 1966 under the title *Ideals and automorphisms of metabelian groups*; received by the editors February 14, 1966.

THEOREM. *Assume Z_m contains nilpotent elements $\neq 0$. There exists automorphisms of U/U_4 ($U = F/F''(F'')^m$) which are induced by automorphisms of U , but which cannot be induced by automorphisms of the free group F (or in fact not even by automorphisms of F/F'').*

2. Ring theory and linear algebra. Let R be a commutative ring (all rings considered will have identities) with minimum condition on ideals. Then $R = A_1 \oplus \cdots \oplus A_r$ where the A_i are generated by primitive orthogonal idempotents f_i . $1 = f_1 + \cdots + f_r$. Each A_i is a local ring with minimum condition on ideals and with identity f_i .

Let $M = F/F'$ be a free (multiplicative) abelian group with free generators s_1, \dots, s_q . It is evident that the group ring $R(M) = A_1(M) \oplus \cdots \oplus A_r(M)$. If $R(M)^*$ and $A_i(M)^*$ denote the respective groups of units, then $R(M)^* = A_1(M)^* \oplus \cdots \oplus A_r(M)^*$ (to abuse notation), i.e., $u \in R(M)^*$ if and only if $u = u_1 + \cdots + u_r$ where $u_i \in A_i(M)^*$. Therefore, the problem of determining the units of $R(M)$ reduces to the situation where R is local. We first state the following proposition, due to Bass.

PROPOSITION 2.1. *Let M be as above and assume R has no nilpotent element $\neq 0$ and no nontrivial idempotents (we do not assume minimum condition on ideals). Then $R(M)$ has only the units $us_1^{\alpha_1} \cdots s_q^{\alpha_q}$ where u is a unit of R and the α_i are integers. Furthermore, $R(M)$ inherits the above properties of R .*

Proof. H. Bass (Proposition 11.2, [4]) proved the proposition for $q=1$. The general case follows easily by induction.

We now assume that R is a commutative local ring with minimum condition on ideals and with Jacobson radical J , the unique maximal nilpotent ideal of R . We consider s_1, \dots, s_q as algebraically independent elements over R and R/J . According to the remarks on p. 13 of [5], the radical of $R[s_1, \dots, s_q] = R[s_i]$ is $J[s_1, \dots, s_q] = J[s_i]$; in fact, $J[s_i]$ is the unique maximal nilpotent ideal of $R[s_i]$. The set $S = \{\prod_{i=1}^n s_i^{\alpha_i} : \text{the } \alpha_i \text{ are nonnegative integers}\}$ is a multiplicatively closed set of nonzero divisors in $R[s_i]$. Hence, we can form $R[s_i]_S$, the ring of quotients with respect to S . We have $R[s_i]_S \cong R[s_i^{\pm 1}] \cong R(M)$. By §6, pp. 14–17, of [6],

$$R[s_i]_S / J[s_i]_S \cong (R[s_i] / J[s_i])_S \cong (R/J)[s_i]_S = (R/J)(M).$$

If $P \in R(M)$, we denote its image in $(R/J)(M)$ by \bar{P} under the natural map $R(M) \rightarrow (R/J)(M)$.

Assume P is a unit in $R(M)$. Then \bar{P} is a unit in $(R/J)(M)$ where (R/J) has no nilpotent elements $\neq 0$ and has no nontrivial idempotents. By Proposition 2.1, $\bar{P} = \bar{u}\pi s_i^{\alpha_i}$ where \bar{u} is a unit in R/J . We may choose u to be a unit in R . Therefore, $P = u\pi s_i^{\alpha_i} + Q$ where $Q \in J[s_i]_S$. On the other hand, any element of this form is a unit in $R[s_i]_S$.

In the general case under consideration, we have $R = A_1 \oplus \dots \oplus A_r$, where each ideal A_i is a local ring with minimum condition on ideals. From the above discussion, it now follows easily that any unit in $R(M)$ has the unique form

$$(2.1) \quad P = (u_1 \pi s_{f_1}^{e_1} + Q_1) + \dots + (u_r \pi s_{f_r}^{e_r} + Q_r)$$

where the $u_i \pi s_{f_i}^{e_i}$ are trivial units in $A_i(M)$, i.e., u_i is a unit in A_i , and Q_i is nilpotent in $A_i(M)$.

Let $R = R_1 \oplus R_2$ be a commutative ring which is the direct sum of ideals R_1 and R_2 . If $M = (a_{ij})$ is an $n \times n$ matrix over R , then $a_{ij} = a_{ij}^{(1)} + a_{ij}^{(2)}$, where $a_{ij}^{(k)} \in R_k$. If $M_k = (a_{ij}^{(k)})$, $k = 1, 2$, we have the following proposition.

PROPOSITION 2.2. $\det M = \det M_1 + \det M_2$.

Proof. $\det M = \sum_{\sigma \in S_n} (-1)^{\varepsilon(\sigma)} a_{1\sigma(1)} \dots a_{n\sigma(n)}$ where S_n is the symmetric group on n letters and $\varepsilon(\sigma) = +1$ or -1 according as σ is even or odd.

$$\begin{aligned} \det M &= \sum (-1)^{\varepsilon(\sigma)} (a_{1\sigma(1)}^{(1)} + a_{1\sigma(1)}^{(2)}) \dots (a_{n\sigma(n)}^{(1)} + a_{n\sigma(n)}^{(2)}) \\ &= \sum_{k=1}^2 \sum (-1)^{\varepsilon(\sigma)} a_{1\sigma(1)}^{(k)} \dots a_{n\sigma(n)}^{(k)} \\ &= \det M_1 + \det M_2. \end{aligned}$$

REMARK. We note that M is invertible if and only if M_k is invertible over R_k .

3. Reduction to the prime power case. We use the notation of [1], [2], and [3]. Let $U = F/F''(F')^m$ where F is the free group of rank q , and a_1, a_2, \dots, a_q are free generators of U . We have the following faithful representation of $A(U; U/U')$ into the ring of $q \times q$ matrices over $Z_m[s_i^{\pm 1}]$ where $Z_m = Z/(m)$ is the ring of integers mod m and s_1, \dots, s_q are commuting indeterminates over Z_m (see [3], §2). For α in $A(U; U/U')$ which is described by

$$(3.1) \quad \alpha: a_i \rightarrow a_i \prod_{j < k} [a_j, a_k]^{P_{ijk}}, \quad P_{ijk} \in Z_m[s_i^{\pm 1}],$$

we have

$$(3.2) \quad M(\alpha) = I + N(\alpha),$$

where I is the identity matrix and $N(\alpha) = (d_{uv})$ is defined by

$$(3.3) \quad d_{uv} = s_u \left[\sum_{h > v} (1 - s_h) P_{uvh} - \sum_{h < v} (1 - s_h) P_{uhv} \right].$$

The following theorem tells us when a matrix over $Z_m[s_i^{\pm 1}]$ represents an IA-automorphism of U .

THEOREM 3.1. *A $q \times q$ matrix (P_{ij}) over $Z_m[s_i^{\pm 1}]$ represents an IA-automorphism of U if and only if*

- (1) $\det (P_{ij})$ is a unit in $Z_m[s_i^{\pm 1}]$,
- (2) $\sum_{j=1}^q P_{ij}(1 - s_j) = (1 - s_i)$, $i = 1, 2, \dots, q$.

For the proof see §3 of [1]. The only modification necessary is as follows: In the proof of Lemma 1, we need to know that if $\gamma_1(1-s_1)+\gamma_2(1-s_2)+\gamma_3(1-s_3)=0$, then $\gamma_3=Q(1-s_1)+R(1-s_2)$ for some elements Q, R in $Z_m[s_i^{\pm 1}]$. Setting $(1-s_1)=(1-s_2)=0$, we see that $\bar{\gamma}_3(1-s_3)=0$ where $\bar{\gamma}_3$ is the image of γ_3 under the substitution. But $(1-s_3)$ is not a zero divisor in $Z_m[s_3^{\pm 1}]$. Thus $\bar{\gamma}_3=0$, i.e., γ_3 is in the ideal generated by $(1-s_1)$ and $(1-s_2)$.

REMARK. It is easy to see that $\det(P_{ij})$ are precisely those units described by (2.1) which are mapped into 1 under the augmentation map which sends each s_i into 1.

Let $m=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$ where the p_i are distinct primes. Then $Z_m=A_1\oplus\cdots\oplus A_r$ where A_j is an ideal of Z_m which is isomorphic to $Z_{p_j^{e_j}}$ as rings. Let f_1, \dots, f_r be the respective idempotents. $Z_m[s_i^{\pm 1}]=A_1[s_i^{\pm 1}]\oplus\cdots\oplus A_r[s_i^{\pm 1}]$. Furthermore, this direct sum decomposition carries over to the ring of $q\times q$ matrices. If (P_{ij}) is a $q\times q$ matrix over $Z_m[s_i^{\pm 1}]$, then we have a unique expression

$$(3.4) \quad (P_{ij}) = (P_{ij}^{(1)}) + \cdots + (P_{ij}^{(r)}),$$

with $(P_{ij}^{(k)})$ a $q\times q$ matrix over $A_k[s_i^{\pm 1}]$.

Using (3.4), we may now state as an immediate corollary to Theorem 3.1 and Proposition 2.2:

COROLLARY 3.2. *A $q\times q$ matrix (P_{ij}) over $Z_m[s_i^{\pm 1}]$ represents an IA-automorphism of U if and only if for $k=1, 2, \dots, r$,*

- (i) $\det(P_{ij}^{(k)})$ is a unit in the ring $A_k[s_i^{\pm 1}]$,
 - (ii) $\sum_{j=1}^q P_{ij}^{(k)}(f_k - f_k s_j) = (f_k - f_k s_i)$, for $i=1, 2, \dots, q$.
- (Recall $1 = \sum f_k$ is the decomposition of 1 in Z_m into orthogonal primitive idempotents.)

Let us henceforth, when convenient, identify the rings $A_k[s_i^{\pm 1}]$ and $Z_{p_k^{e_k}}[s_i^{\pm 1}]$. Corollary 3.2 tells us that (P_{ij}) represents an IA-automorphism of U if and only if each $(P_{ij}^{(k)})$ represents an IA-automorphism of $U(k)=F/F''(F')^{p_k^{e_k}}$, for $k=1, 2, \dots, r$. We thus have the following important corollary:

COROLLARY 3.3. $A(U; U/U') \cong A(U(1); U(1)/U(1)') \times \cdots \times A(U(r); U(r)/U(r)'),$ (direct product of groups).

Proof. Let $\alpha, \beta \in A(U; U/U')$ be represented by (P_{ij}) and (Q_{ij}) respectively over $Z_m[s_i^{\pm 1}]$. Using the notation of equation (3.4) we see that

$$(P_{ij})(Q_{ij}) = (P_{ij}^{(1)})(Q_{ij}^{(1)}) + \cdots + (P_{ij}^{(r)})(Q_{ij}^{(r)}).$$

This shows that the obvious (1-1) correspondence is an isomorphism.

These preceding corollaries in effect reduce all problems we consider to the case where m is a prime power. These will be considered in the next section. As a typical consequence of the preceding corollaries we might mention here the following extension of Theorem 1 of [3]. We adhere to the above notation.

THEOREM 3.4. *Assume U has two free generators and let m be a squarefree integer. Then any IA-automorphism of U is uniquely expressible as a product of inner automorphisms of $U(k)$ for $k=1, 2, \dots, r$.*

At the conclusion of this section, it might perhaps be worthwhile to remark that, although as shown above, the IA-automorphism group of $U=F/F''(F')^m$ is a direct product of the IA-automorphism groups of $U(k)=F/F''(F')^{p_k^e}$ for each prime power p_k^e dividing m , it is not true that U itself is a direct product of the $U(k)$. However, as is clear (either by direct observation or by considering the subgroup of the IA-automorphisms of U consisting of inner automorphisms), U may be embedded in a natural and obvious manner in the direct product of the $U(k)$.

4. Induced automorphisms for prime power p^e . We assume $m=p^e$, p a prime and $e > 1$. Let Σ denote the ideal of $Z_m[s_i^{\pm 1}]$ generated by the $\sigma_i=(1-s_i)$ for $i=1, 2, \dots, q$. The proof of the following has already been discussed (cf. Lemma 2 of [3]).

PROPOSITION 4.1. *If $\alpha \in A(U; U/U_n)$, then $M(\alpha) \equiv I \pmod{\Sigma^{n-1}}$.*

We wish to determine the elements $\alpha' \in A(U/U_n; U/U_{n-1})$, $n \geq 4$, which are induced by $\alpha \in A(U)$. α' can be described by

$$(4.1) \quad \alpha': a_i \rightarrow a_i \prod_{j < k} [a_j, a_k]^{P_{ijk}}$$

where the P_{ijk} are in Σ^{n-2} . We then define $M(\alpha')=I+N(\alpha')$ exactly as in (3.2) and (3.3). Then $N'(\alpha')$ will denote the image of $N(\alpha')$ modulo Σ^{n-1} . (Remark: For reasons which will soon become apparent, we have here switched notation from that used in the introduction and in the previous work. $N'(\alpha')$ is what had heretofore been denoted by $N_1(\alpha')$.) We now state

THEOREM 4.2. *$\alpha' \in A(U/U_n; U/U_{n-1})$, $n \geq 4$, is induced by $\alpha \in A(U)$ if and only if $\text{trace } N(\alpha') \equiv 0 \pmod{pZ_m[s_i^{\pm 1}] + \Sigma^{n-1}}$, i.e., p divides $\text{trace } N'(\alpha')$.*

Before proving Theorem 4.2 we note the following: If we factor the ring $Z_m[s_i^{\pm 1}]/(p)$ by the ideal $\bar{\Sigma}^{n-1}$ where $\bar{\Sigma}$ denotes the ideal generated by the $\sigma_i=(1-s_i)$, then the resulting ring is (isomorphic to) $Z_m[s_i^{\pm 1}]/(p, \Sigma^{n-1})$. Furthermore, we get the same result if $Z_m[s_i^{\pm 1}]/\Sigma^{n-1}$ is factored by the ideal generated by p ; i.e., factoring successively by the ideal generated by p and a power of the augmentation ideal is a commutative operation.

Proof of Theorem 4.2. The theorem was proved in [3] for $e=1$. The condition in that situation reads $\text{tr } N'(\alpha)=0$. We now assume $e > 1$.

(\Rightarrow) Let $V=F/F''(F')^p$. Suppose α' in $A(U/U_n; U/U_{n-1})$ is induced by $\alpha \in A(U)$ and is given by (4.1). Let $\beta' \in A(V/V_n; V/V_{n-1})$ be defined by

$$\beta': b_i \rightarrow b_i[b_j, b_k]^{Q_{ijk}}$$

where the b_i are the obvious free generators of V/V_n and Q_{ijk} is the image of P_{ijk} modulo p . If $\tilde{M}(\alpha)$ denotes the image of $M(\alpha)$ modulo p , then it is clear that $\tilde{M}(\alpha) = M(\beta')$. β' is induced by $\beta \in A(V)$ where β is that automorphism of V induced by α in the natural manner. Thus, $\text{tr } N'(\beta') = 0$ by Theorem 3 of [3]. But, by the discussion preceding this proof, $N'(\beta')$ equals the image of $N'(\alpha')$ modulo p , and hence we have $\text{tr } N'(\alpha') \equiv 0$ modulo p .

(\Leftarrow) The proof is the same as that for Lemma 7, §5, of [2] and Theorem 3, §4, of [3] with the following modifications.

Using the same notation as in §5 of [2] and §4 of [3], we find that the condition on $\text{tr } N'(\alpha')$ is equivalent to the following system of linear equations over Z_m ,

$$(4.2) \quad \sum_{i < k} a_{iik}(t/\sigma_k) - \sum_{i > j} a_{ijj}(t/\sigma_j) = p^e q_t,$$

where $(p, q_t) = 1$. Here, $1 \leq e_t \leq e$, and there is one such equation for each monomial t in the σ_i . It is understood that the sum is over all pairs i, k and i, j such that t is divisible by σ_k and σ_j respectively. We recall from §5 of [2] that any automorphism of V corresponding to a sum of solutions of (4.2) is realized as the product of automorphisms corresponding to the respective solutions. The general solution to (4.2) is the sum of a particular solution of the nonhomogeneous system and a solution of the homogeneous system. Using the proof of Lemma 7 of [2], we can construct an automorphism of U corresponding to any homogeneous solution. A particular solution of the nonhomogeneous system (4.2) can be obtained as the sum of particular solutions of the system with all but one equation homogeneous. Hence, the proof of the theorem reduces to showing that for any monomial t of the form specified in (4.2), the solution $a_{iik}(t/\sigma_k) = p^e q_t$ for fixed i and k , $i < k$, and all other a 's equal to zero is induced by an automorphism of U . But this follows since in fact the mapping

$$(4.3) \quad a_i \rightarrow a_i [a_i, a_k]^{t p^e q_t}, \quad a_j \rightarrow a_j, \quad i \neq j$$

is an automorphism α of U . Indeed, we have $\det M(\alpha) = 1 + t p^e q_t$, which is of the form $1 + Q$ where Q is a nilpotent element in $Z_m[s_i^{\pm 1}]$. By equation (2.1), $\det M(\alpha)$ is a unit. This completes the proof.

5. Induced automorphisms for arbitrary m .

$$m = p_1^{e_1} \cdots p_r^{e_r}, \quad \text{and} \quad Z_m[s_i^{\pm 1}] = A_1[s_i^{\pm 1}] \oplus \cdots \oplus A_r[s_i^{\pm 1}].$$

Let $\alpha \in A(U; U/U_n)$. We write $I = I_1 + \cdots + I_r$ where I_k is the $q \times q$ matrix with f_k down the diagonal and zero elsewhere. Then

$$(5.1) \quad M(\alpha) = M_1(\alpha) + \cdots + M_r(\alpha)$$

where

$$(5.2) \quad M_k(\alpha) = I_k + N_k(\alpha), \quad N_k(\alpha) \text{ a } q \times q \text{ matrix over } A_k[s_i^{\pm 1}],$$

$$(5.3) \quad N(\alpha) = N_1(\alpha) + \cdots + N_r(\alpha).$$

Denote by Σ_k the ideal ($\subseteq A_k[s_i^{\pm 1}]$) of $Z_m[s_i^{\pm 1}]$ generated by the $f_k \sigma_i$ ($i=1, 2, \dots, q$). Note that $\Sigma^n = \Sigma_1^n + \dots + \Sigma_r^n$, $n \geq 1$, and hence

$$Z_m[s_i^{\pm 1}]/\Sigma^n = A_1[s_i^{\pm 1}]/\Sigma_1^n \oplus \dots \oplus A_r[s_i^{\pm 1}]/\Sigma_r^n.$$

The following proposition (Corollary to Lemma 4.1) is now obvious.

PROPOSITION 5.1. *If $\alpha \in A(U; U/U')$ corresponds to*

$$(\alpha_1, \dots, \alpha_r) \in \prod_{k=1}^r A(U(k); U(k)/U(k)')$$

(direct product), then the following are equivalent.

- (i) $\alpha \in A(U; U/U_n)$,
- (ii) $M(\alpha) \equiv I \pmod{\Sigma^{n-1}}$,
- (iii) $M_k(\alpha) \equiv I_k \pmod{\Sigma_k^{n-1}}$, for $k=1, \dots, r$,
- (iv) $\alpha_k \in A(U(k); U(k)/U(k)_n)$, for $k=1, \dots, r$.

For $\alpha' \in A(U/U_n; U/U_{n-1}) = A$, we define $M(\alpha')$ as in §4. Then $N'(\alpha') = N'_1(\alpha') + \dots + N'_r(\alpha')$ where $N'_k(\alpha')$ is the image of $N_k(\alpha')$ modulo Σ_k^{n-1} .

THEOREM 5.2. *Let $\alpha' \in A \leftrightarrow (\alpha'_1, \dots, \alpha'_r) \in \prod A(U(k)/U(k)_n; U(k)/U(k)_{n-1})$. Then the following are equivalent.*

- (i) $\text{tr } N'(\alpha'_k)$ is divisible by p when we identify

$$A_k[s_i^{\pm 1}] \text{ and } Z_{p^k}[s_i^{\pm 1}].$$

- (ii) α'_k is induced by some $\alpha_k \in A(U(k))$, for $k=1, \dots, r$.
- (iii) α' is induced by some $\alpha \in A(U)$.

Proof. (i) \Leftrightarrow (ii) is Theorem 4.2. If α in $A(U; U/U')$ corresponds to $(\alpha_1, \dots, \alpha_r)$ in $\prod A(U(k); U(k)/U(k)')$, then α' is induced by α if and only if α'_k is induced by α_k . This is clear by the commutative diagram

$$\begin{array}{ccc} A(U; U/U') & \cong & \prod A(U(k); U(k)/U(k)') \\ \downarrow & & \downarrow \\ A & \cong & \prod A(U(k)/U(k)_n; U(k)/U(k)_{n-1}) \end{array}$$

where the vertical maps are the obvious ones. Thus (ii) \Leftrightarrow (iii) follows.

COROLLARY 5.3. *There are automorphisms of U which are not induced by automorphisms of $\Phi = F/F''$ (and therefore F).*

Proof. The automorphism of U described by (4.3) is such an example. In fact, any $\alpha \in A(U; U/U')$ such that $\det M(\alpha) = \prod s_i^{a_i} + Q$, $Q \neq 0$ nilpotent, cannot be induced by an automorphism of Φ .

REFERENCES

1. S. Bachmuth, *Automorphisms of free metabelian groups*, Trans. Amer. Math. Soc. **118** (1965), 93–104.
2. ———, *Induced automorphisms of free groups and free metabelian groups*, Trans. Amer. Math. Soc. **122** (1966), 1–17.
3. ———, *Automorphisms of a class of metabelian groups*, Trans. Amer. Math. Soc. **127** (1967), 284–293.
4. H. Bass, *The Dirichlet unit theorem, induced characters, and Whitehead groups of finite groups*, Columbia University Report CU-21-NSF-GP-1904-M, 1964.
5. N. Jacobson, *Structure of rings*, Colloq. Publ., Vol. 37, Amer. Math. Soc., Providence, R. I., 1956.
6. M. Nagata, *Local rings*, Interscience, New York.

UNIVERSITY OF CALIFORNIA
SANTA BARBARA, CALIFORNIA