ON THE ISOMORPHISMS OF TWO METACYCLIC GROUPS

B. G. BASMAJI

1. **Introduction.** In [2] Szekeres determined all the metabelian groups of two generators and raised the question of whether a rule of selection exists to determine all the nonisomorphic ones. In this paper we find such a rule for the finite metacyclic groups. That is, we give a rule to determine all the nonisomorphic extensions of a cyclic group of order n by a cyclic group of order h.

Our approach uses strongly the defining relations of two extensions. In §2 we give the notations, the isomorphism theorem, and the rule that gives all the nonisomorphic groups. In §3 some preliminary lemmas are proved. The theorem for the case of metacyclic p-groups is proved in §4 and a remark is made that reduces the proof to a special pair of two metacyclic groups. The necessity and the sufficiency of the conditions are proved in §5 and §6 respectively. In particular we note in §6 that the isomorphism need not be of the first kind as defined by Gol'fand [1].

2. **Notations and main result.** Let G be an extension of a cyclic group of order n by a cyclic group of order h, i.e. G is a metacyclic group. Then the defining relations of $G=\{a, b\}$ are given by

$$a^n = b^{hg} = 1, \qquad a^k = b^h, \qquad ba = a^r b,$$

where $g \mid n$, $k=n/g$, $r^h \equiv 1 \pmod{n}$, and $g \mid r-1$. [Note that there is no loss of generality in assuming that $k \mid n$, and hence $k=n/g$. For if $k \nmid n$, then replacing k by $k_0=(k, n)$ and a by a^x, where x is a solution of $x \equiv k/k_0 \pmod{n/k_0}$ and $x \equiv 1 \pmod{n'}$, n' the product of distinct primes p such that $p \mid n$ and $p \nmid n/k_0$, gives the above relations.]

Let $H=\{c, d\}$ be another extension with the defining relations

$$c^n = d^{hg'} = 1, \qquad c^{k'} = d^h, \qquad dc = c^\sigma d$$

where $g' \mid n$, $k'=n/g'$, $\sigma^h \equiv 1 \pmod{n}$, and $g' \mid \sigma-1$.

For any integer s let $M(s)$ denote the multiplicative group of the reduced residues modulo s. If $(x, s)=1$, let $\{x\}_s$ denote the cyclic subgroup of $M(s)$ generated by x. For the integer n above and any x with $(x, n)=1$, we let $\{x\}_n=\{x\}$. Let t be the order of $\{r\}$ and for any $s \mid n$, let t_s be the order of $\{r\}_s$.

Now let s and s' be positive integers dividing n. We define an equiv-

Received by the editors August 14, 1968.

alence relation, $s \sim s'$, with respect to h and r. For any prime p dividing n let $p^x \| n$, i.e. $p^x | n$ and $p^{x+1} \nmid n$, $p^\pi \| h$, $p^z \| s$, and $p^{z'} \| s'$. Then $s \sim s'$ if the following conditions are satisfied:

(i) If $p \neq 2$, then either $x \geqq \pi + z$ and $x \geqq \pi + z'$ or $z = z'$.

(ii) If $p = 2$ and $4 | r-1$, then the conditions are as in (i) above.

(iii) If $p = 2$, $4 | r+1$, and $x < \pi + z$, then $z = z'$.

(iv) If $p = 2$, $4 | r+1$, $2^{x-\pi} \| r+1$, and $x \geqq \pi + z$, then $z \leqq 1$ and $z' \leqq 1$.

(v) If $p = 2$, $4 | r+1$, $2^{x-\pi+1} | r+1$, and $x \geqq \pi + z$, then $z = z'$.

Note that in (iii), (iv), and (v) we only need the cases where $z \leqq 1$ and $z' \leqq 1$.

Now we put the integers n, h, g, and g' in the canonical forms and define some other integers.

Let $n = \prod p^x$, $h = \prod p^\pi$, $g = \prod p^z$, $g' = \prod p^{z'}$, $\nu = \prod_{p | r-1} p^x$, and $\mu = n/\nu$. If a discussion is about a prime p, then the exponents x, π, $\cdots$, will have the above meanings for this prime p. However, whenever confusion is likely, we add a subscript, e.g., $x = x_p$.

Let $\eta = \nu/2$ when $n \equiv hg \equiv 0 \pmod 8$, $g - 2 \equiv r + 1 \equiv 0 \pmod 4$, and $2^\pi \nmid t_\mu$ and let $\eta = \nu$ otherwise. For $p | \nu$, let $p^u \| t_\nu$ and $p^v \| t_\mu$. Finally let

$$\theta_1 = 2n(r^{t_\mu} - 1)/(2^x, n), \qquad \theta_2 = (2, t_\nu, t_\mu, g)(r - 1),$$

$$\theta = ([[\theta_1, hg]/gh, \theta_2, k], n) = \prod p^w, \quad \text{and} \quad \lambda = \theta/\mu.$$

Now we give the main result of this paper.

THEOREM. *Let G and H be given as above. Then G and H are isomorphic if and only if $g \sim g'$, $\{r\}_\eta = \{\sigma\}_\eta$, and $\{r\}_\theta = \{\sigma\}_\theta$.*

We give the rule to determine all the nonisomorphic extensions of a cyclic group of order n by a cyclic group of order h. Let L be the set we get by taking a generator of every cyclic subgroup of $M(n, h) = \{r \in M(n) | r^h \equiv 1 \pmod n\}$. If $4 \nmid n$ or $2 \nmid h$ let $L' = L$. If $4 | n$ and $2 | h$ let $L' = \{r \in L | \ 4 | r-1\}$ and $L'' = \{r \in L | \ 4 | r+1\}$.

First, take the set L' and consider the equivalence relation between the divisors of n where $r \in L'$. [Note we may assume $4 | r-1$ for all $r \in L'$ when $L = L'$. Hence the equivalence relation is defined by (i) and (ii) only.] Let S be the set of all *smallest integers* from each equivalence class. [The smallest integer of an equivalence class divides every other integer from the class and the reason for picking this integer follows from the remark in §4.] For $g \in S$ let $L'(g) = \{r \in L' | \ g | r-1\}$. Pick an $r \in L'(g)$ and define integers η and θ as above and eliminate all σ's in $L'(g)$ satisfying the conditions of the theorem. Do this until every $r \in L'(g)$ is either picked or eliminated for all $g \in S$.

Second, take the set L'', i.e. when $4 | n$ and $2 | h$. Consider the

equivalence relation on the divisors of n given by (i) and

(ii′) If $p=2$ then either $z=z'=0$ or $z=z'=1$.

Let S' be the set of all *smallest integers* from each equivalence class. For $g\in S'$ let $L''(g)=\{r\in L''|\ g|r-1\}$. If g is odd, then pick any $r\in L''(g)$. If g is even, then pick $r\in L''(g)$ such that $2^{x-\pi+1}|r+1$ when $x\geqq\pi+1$ and any $r\in L''(g)$ when $x<\pi+1$. Now proceed as above for all $g\in S'$.

The required nonisomorphic groups have the defining relations as of G above where g runs over all elements of S and, if $4|n$ and $2|h$, over all elements of S' with the integers r selected as above.

3. **Preliminary lemmas.** The following lemmas are used extensively in the proof of the theorem. Let p be a prime and r an integer.

LEMMA 1. *Let $p\neq 2$ and $p^x\|r-1$ with $x\geqq 1$, or let $p=2$ and either $2^x\|r-1$ or $2^x\|r+1$ with $x\geqq 2$. Then $p^{x+y}\|r^{p^y}-1$ where $y>0$.*

LEMMA 2. *Let $R=\{r\}$ be a cyclic subgroup of $M(p^y)$ of order p^x. If $p\neq 2$, then $r=1+p^{y-x}$ with $0\leqq x\leqq y-1$. If $p=2$, then $r=1+2^{y-x}$ or $-1+2^{y-x}$ for $2\leqq x\leqq y-2$ and $r=1+2^{y-1}$, $-1+2^{y-1}$, or -1 for $x=1$.*

LEMMA 3. *Assume the hypothesis of Lemma* 1.

(i) *If $p^w|r^z-1$ where $w>x$, then $p^{w-x}|z$.*

(ii) *If $p^x\|r-1$, $p\nmid z$, and $w>0$, then $p^w\|1+r+\cdots+r^{zp^w-1}$.*

(iii) *If $2^x\|r+1$, $2\nmid z$, and $w>0$, then $2^{w+x-1}\|1+r+\cdots+r^{z2^w-1}$.*

LEMMA 4. *Let $(n, m)=1$, $\{r\}_n$ of order t, and $\{\sigma\}_m$ of order τ. Then $\{\sigma'\}_{nm}$ is of order $[t, \tau]$ where $\sigma'\equiv r \pmod n$ and $\sigma'\equiv\sigma \pmod m$.*

LEMMA 5. *In Lemma* 4 *replace r and σ by r^α and r^β respectively, where $(\alpha, t)=(\beta, \tau)=1$. Then $\{\sigma'\}_{nm}=\{r\}_{nm}$ if and only if $(t, \tau)|\alpha-\beta$.*

To prove Lemma 1, let $r=1+zp^x$ or $-1+z2^x$, as suitable where $p\nmid z$. The result follows by considering the binomial expansion of r^{p^y} for the given cases. The proofs of Lemmas 2 and 3 follow. For the proofs of Lemmas 4 and 5 use the Chinese remainder theorem.

From this point on we fix our notations as given in §2. Let G' and Z be the commutator group and the center of G respectively. Then $G'=\{a^{r-1}\}$ and is of order $n'=n/(r-1, n)$ and $Z=\{a^{n'}, b^t\}$ and is of order $h(r-1, n)/t$.

LEMMA 6. *If $G\cong H$ then $g\sim g'$, $(r-1, n)=(\sigma-1, n)$, and $\{r\}$ and $\{\sigma\}$ are of equal order in $M(n)$.*

PROOF. We only need to prove $g\sim g'$ since the others follow from the note above. Assume $g\nsim g'$. We take the different cases and show that G and H are not isomorphic. For some prime p let $x<\pi+z'$ and $z<z'$. Then H has an element, namely d, whose order is divisible by

$p^{\pi+z'}$. Let $m=nhg/p^x$ if $\pi+z>x$ and $m=nhg/p^{\pi+z}$ if $x\geqq\pi+x$. Then for any integer β we have $r^{\beta m}\equiv 1 \pmod{n}$. From the factorization of the last congruence and Lemma 3 we have

$$1+r^{\beta}+\cdots+r^{\beta(m-1)}\equiv 0 \pmod{n}.$$

Also we have $(a^{\alpha}b^{\beta})^m=1$ for all integers α and β. Hence there exists no element of G whose order is divisible by $p^{\pi+z'}$ and therefore $G\ncong H$.

Now assume $p=2$, $x\geqq\pi+1$, $2^{x-\pi+1}\mid r+1$, $\pi>0$, and $0=z'\neq z=1$. From Lemma 3 we have $2^x\mid 1+r+\cdots+r^{2^m-1}$. Hence the order of $a^{\alpha}b^{\beta}$ is exactly divisible by $2^{\pi+1}$ if β is odd. Assume it is possible to set $G=\{a^{\alpha}b^{\beta},\ a^{\delta}b^{\zeta}\}$ such that the order of $\{a^{\alpha}b^{\beta}\}\cap\{a^{\delta}b^{\zeta}\}$ is odd and $\{a^{\alpha}b^{\beta}\}$ is normal of order n. Then $2\mid\zeta$ and hence β is odd. Hence we only need to consider the case $x=\pi+1$. It could be shown that the normality of $\{a^{\alpha}b^{\beta}\}$ implies that the 2-Sylow subgroup of G is quaternion of order 8, a contradiction. This completes the proof of the lemma.

LEMMA 7. *If* $\{r\}=\{\sigma\}$ *and* $g=g'$, *then* $G\cong H$.

PROOF. Let $\sigma\equiv r^s \pmod{n}$ where $(s,\ t)=1$. Let β be a solution of $\beta\equiv s \pmod{t}$ and $\beta\equiv 1 \pmod{m'}$ where m' is the product of the distinct primes p, $p\mid hg$ and $p\nmid t$. Let α be the solution of $\alpha\equiv\beta \pmod{g}$ and $\alpha\equiv 1 \pmod{n'}$ where n' is the product of the distinct primes p, $p\mid n$ and $p\nmid g$. Then the map $\psi: H\to G$ where $\psi(c)=a^{\alpha}$ and $\psi(d)=b^{\beta}$ is an isomorphism.

4. **Metacyclic p-groups and a general remark.** Let p be a prime and let $n=p^z$, $h=p^{\pi}$, and $g=g'=p^x$, i.e. G and H are metacyclic p-groups. For $p=2$, $x\geqq 3$, $\pi\geqq 2$, $z=1$, and $4\mid r+1$ let $\eta=n/2=2^{x-1}$, otherwise let $\eta=n=p^x$.

LEMMA 8. *Let G and H be p-groups as above. Then $G\cong H$ if and only if* $\{r\}_{\eta}=\{\sigma\}_{\eta}$.

PROOF. If $p\neq 2$, the result is immediate from Lemmas 6, 7, and 2. The same is true when $p=2$ and $4\mid r-1$.

Now assume $\eta=n/2$, with the above conditions. If $\{r\}_{\eta}=\{\sigma\}_{\eta}$, then either $\{r\}=\{\sigma\}$ or $r+1\equiv\sigma+1+2^{x-1}\equiv 0 \pmod{2^x}$. In the first case $G\cong H$ from Lemma 7 and in the latter case $\psi: H\to G$, given by $\psi(c)=ab^{2^{\pi-1}}$ and $\psi(d)=b$, is an isomorphism.

For the necessity, from Lemmas 6 and 2, we only need to consider the case where $r+1\equiv\sigma+1+2^{x-1}\equiv 0 \pmod{2^x}$. Since $g\mid r-1$, $z=0$ or 1. For $x=2$, G and H are not isomorphic. Hence let $x\geqq 3$. Assume G and H are isomorphic and the isomorphism $\psi: H\to G$ is given by $\psi(c)=a^{\alpha}b^{\beta}$ and $\psi(d)=a^{\delta}b^{\zeta}$. These give two congruences (see §5). The first is $\beta(-2+2^{x-1})\equiv 0 \pmod{2^x}$. The second, for the case where β is even, is

$$\alpha(-1)^{\zeta} \equiv \alpha(-1 + 2^{x-1}) + 2^{x-\pi-z}\beta(-2 + 2^{x-1}) \pmod{2^x}.$$

Assume $z=0$. If $\pi>1$, then β is even, ζ is odd and hence α is even and $a^{\alpha}b^{\beta}$ is of order at most 2^{x-1}. If $\pi=1$ and $\beta=0$, then as above α is even and $a^{\alpha}b^{\beta}$ is at most of order 2^{x-1}. If $\pi=1$ and $\beta=1$, then $(a^{\alpha}b^{\beta})^2=1$. Hence in these cases $G\ncong H$.

Assume $z=1$. The only case left is when $\pi=1$. But in this case G is a generalized quaternion group and has only one cyclic subgroup of order 2, namely $\{b^2\}$. The subgroups $\{d^2\}$ and $\{cd\}$ are distinct subgroups of order 2 of H. Hence $G\ncong H$, and the proof is complete.

REMARK. We make a note on the general case. Using the integer g we define an integer g_0 as the product of all p^z where $p\mid g$ and either $x<\pi+z$ or for $p=2$ and $4\mid r+1$, $2^{x-\pi+1}\mid r+1$. Then g_0 is the smallest integer of the equivalence class containing g. Let $\zeta=1+r+\cdots+r^{h-1}$. Let β be an integer such that $\beta\equiv p^{x-\pi-z} \pmod{p^x}$ if $p\mid g$ and $x\geqq\pi+z$ for $p\neq 2$ or for $p=2$ with $4\mid r-1$. For $2\mid g$ and $4\mid r+1$ let $\beta\equiv 1 \pmod{2^x}$. Otherwise let $\beta\equiv 0 \pmod{p^x}$. Then from Lemma 3, for $p\mid g$, $x\geqq\pi+z$, where $p\neq 2$ or $p=2$ and $4\mid r-1$, we have $p^{x-z}\| \beta\zeta$. For $2\mid g$ and $4\mid r+1$ we have $2^{\delta+\pi-1}\|\beta\zeta$ where $2^{\delta}\| r+1$. Note that for $p=2$ and $4\mid r+1$ we have $z=1$ or 0 and $\delta\geqq x-\pi$.

Let α be an integer such that $\alpha(\beta\zeta/k)\equiv -1 \pmod{p^x}$ whenever $p^{x-z}\|\beta\zeta$ and $\alpha\equiv 0 \pmod{p^x}$ otherwise. [The first case also includes the case where $p=2$, $z=1$, $4\mid r+1$, and $\delta=x-\pi$.] It could be easily shown that $a^{\alpha\beta}b$ is of order hg_0. Hence G is isomorphic to a group G_0 whose defining relations are given by those of G with g_0 exchanged for g and $k_0=n/g_0$ exchanged for k.

Assume $G\cong H$ and $4\mid r+1$ with $4\mid n$ and $2\mid h$. Consider the 2-Sylow subgroups $G(2)$ and $H(2)$ of G and H respectively. Then $G(2)\cong H(2)$. From Lemma 7 the defining relations of $G(2)$ and $H(2)$ can be taken as those of G and H where n, h, g, and g' are changed to 2^x, 2^r, 2^z, and $2^{z'}$ respectively. From Lemma 6 the highest power of 2 dividing $r+1$ is the same as that dividing $\sigma+1$ except possibly when $r+1\equiv\sigma+1+2^{x-1}\equiv 0 \pmod{2^x}$. Assume $r+1\equiv\sigma+1+2^{x-1}\equiv 0 \pmod{2^x}$. If $z=z'$, then Lemma 8 implies that $\pi\geqq 2$. If $1=z\neq z'=0$ and $\pi=1$, then $G(2)\ncong H(2)$ since $G(2)$ is the quaternion group. If $0=z\neq z'=1$ and $\pi=1$, then $z'=1$ may be changed to $z'=0$ (see proof of Lemma 8) and hence $G(2)\ncong H(2)$. Hence we have $\pi\geqq 2$ in case $r+1\equiv\sigma+1+2^{x-1}\equiv 0 \pmod{2^x}$, and therefore $2^{x-\pi+1}$ divides both $r+1$ and $\sigma+1$.

The above discussion shows that the equivalence relation on the divisors of n will be the same if σ is exchanged for r provided that $G\ncong H$. Hence g_0 and k_0, as defined above, may be exchanged for g' and k' in the defining relation of H. This implies that we only need to prove the theorem for the case where $g'=g$.

5. **Proof of the necessity.** In the next two sections assume the notations of §2 and let $g=g'$. For convenience we let $m=hg=\prod p^{\nu}$ where $\pi=y-z$.

Let p be a prime dividing ν. Then using the Sylow theorem and Lemma 7, the defining relations of any p-Sylow subgroup, $G(p)$, of G is given by

$$A^{p^x} = B^{p^y} = 1, \qquad A^{p^{x-z}} = B^{p^{y-z}}, \qquad BA = A^rB.$$

Here r is of order p^{u_p} in $M(p^x)$. Similarly the p-Sylow subgroup, $H(p) = \{C, D\}$, of H, is given by exchanging C for A, D for B, and σ for r. Let η_p be defined for the prime p as done in §4. The isomorphism of $H(p)$ and $G(p)$, by Lemma 8, gives us $\sigma \equiv rs_p \pmod{\eta_p}$ where $(s_p, p) = 1$. Using Lemma 5 we have $\sigma \equiv r_p^s \pmod{\eta'}$ where η' is the product of all η_p, $p \mid \nu$ and s is an integer. Note that $\eta' = \eta$ for all cases except when $4 \mid r+1$ and $2^{\nu-1} \mid t_\mu$, in which case $\eta' = \eta/2$.

Assume the isomorphism, $\psi: H \to G$, is given by $\psi(c) = a^\alpha b^\beta$ and $\psi(d) = a^\delta b^\zeta$. Then from $\psi(dc) = \psi(c^\sigma d)$ we have

(i) $$\beta(\sigma - 1) \equiv 0 \pmod{h}$$

(ii) $$\alpha r^\zeta \equiv \alpha(1 + r^\beta + \cdots + r^{\beta(\sigma-1)}) + \delta(r^{\beta\sigma} - 1) + \beta k(\sigma - 1)/h \pmod{n}.$$

(a) $r^\beta \equiv 1 \pmod{\mu}$. Let $p \mid \mu$, then $p \nmid \sigma - 1$ and from (i), $p^\nu \mid \beta$. Assume $r^\beta \not\equiv 1 \pmod{p^x}$, then since $r^h \equiv 1 \pmod{p^x}$, from Lemma 1, $p \nmid r^\beta - 1$. Choose an integer f such that $p \nmid f$ and $q^{x_q} \mid f$, $q^{u_q} \mid f$, $q \neq p$. Then $r^{f\beta} \equiv 1 \pmod{q^{x_q}}$ for every $q \mid n$. Using this and Lemma 3, (ii) and (iii), it can be shown that $(a^\alpha b^\beta)^f = 1$, a contradiction. Hence $r^\beta \equiv 1 \pmod{\mu}$ and $t_\mu \mid \beta$.

(b) $(\alpha, \mu) = 1$ and $\sigma \equiv r^\zeta \pmod{\mu}$. Let $p \mid \mu$ and assume $p \mid \alpha$. Choose f such that $n \nmid f$, $n/p \mid f$ and $m \mid f\beta$. As above we have $(a^\alpha b^\beta)^f = 1$, a contradiction. Hence $(\alpha, \mu) = 1$. The second result follows since $\mu \mid \beta k(\sigma - 1)/h$. And since we have an isomorphism $\psi': G \to H$, we also have $(\zeta, t_\mu) = 1$.

(c) $(\alpha, t_\nu, t_\mu) = 1$. We have

$$a = (a^\alpha b^\beta)^e (a^\delta b^\zeta)^f = a^i b^{\beta e + \zeta f}$$

where $\beta e + \zeta f \equiv 0 \pmod{h}$, $i \equiv 1 \pmod{k}$, and

$$i = \alpha(1 + r^\beta + \cdots + r^{\beta(e-1)}) + \delta r^{\beta e}(1 + r^\zeta + \cdots + r^{\zeta(f-1)}).$$

If $p \mid t_\nu$ and $p \mid t_\mu$, then $p \mid \beta$ and $p \mid k$. From the above $p \mid f$, and hence from Lemma 3, p divides the last sum in the expression for i. Since $i \equiv 1 \pmod{k}$, it follows that $p \nmid \alpha$ or $(\alpha, t_\nu, t_\mu) = 1$.

(d) $\theta \mid \beta k(\sigma - 1)/h$. Clearly $k \mid \beta k(\sigma - 1)/h = n'$. To prove (θ_2, n)

divide n' we only need to show that $\beta k/h$ is an even integer when t_ν, t_μ, and g are all even. Now $\beta k/h$ is an integer since $(a^\alpha b^\beta)^k = (a^\delta b^\zeta)^h = a^{fk}$ where $(f, g) = 1$ and

$$f = \alpha(1 + r^\beta + \cdots + r^{\beta(k-1)})/k + \beta k/h.$$

Assume t_ν, t_μ, and g are all even. Then $2 \nmid \alpha$, $2 \mid \beta$, $4 \mid r^\beta - 1$, and from Lemma 3, the coefficient of α is odd. Hence $\beta k/h$ is even since f is odd.

To show that $([\theta_1, m]/m, n) \mid n'$, we only need to consider primes p dividing ν. Considering the highest power of p dividing $([\theta_1, m]/m, n)$, the result can be proved easily. Note that for $p = 2$, the cases $4 \mid r - 1$ and $4 \mid r + 1$ should be taken separately.

Now we complete the proof of the necessity. First note that if $2^{\nu-1} \mid t_\mu$ then $2^x \mid \theta$ and, from congruence (ii), $\sigma \equiv r^e \pmod{2^x}$, and hence $\sigma \equiv r^e \pmod{\eta}$. This implies $\sigma \equiv r^e \pmod{\lambda}$. For $p \mid \nu$, replacing p^w for n in congruence (ii) and using the above we have

$$\alpha r^\zeta \equiv \alpha\sigma + f p^{v+w-u'} \pmod{p^w}$$

where $p^{u'} \| t_\lambda$. [Note that the cases $p = 2$, $4 \mid r - 1$ and $p = 2$, $4 \mid r + 1$ should be taken separately.] Replacing σ by r^e in this congruence, it follows that $(t_\lambda, t_\mu) \mid s - \zeta$. Since $\theta = \lambda\mu$, using (b) above and Lemma 5 we have $\{\sigma\}_\theta = \{r\}_\theta$. It is already shown above that $\{\sigma\}_\eta = \{r\}_\eta$, which proves the necessity.

6. **Proof of the sufficiency.** The conditions of the theorem mean that there exist integers e and f such that $\sigma \equiv r^e \pmod{\eta}$ and $\sigma \equiv r^f \pmod{\theta}$ where $(e, t_\eta) = (f, t_\theta) = 1$. If $\eta = \nu/2$ then either $\sigma \equiv r^e \pmod{2^x}$ or $r + 1 \equiv \sigma + 1 + 2^{x-1} \equiv 0 \pmod{2^x}$. For the defining relations of H we assume $\{c\} \cap \{d\}$ is of order g instead of merely $c^k = d^h$.

We find integers α, β, and ζ such that the map $\psi: H \to G$, given by $\psi(c) = a^\alpha b^\beta$ and $\psi(d) = b^\zeta$, is an isomorphism. We fix e and f above and define an integer θ'.

For $p \mid \nu$ let $p^{s'} \| r^e - r^f$. Let $p^s \| \theta'$, $p \mid n$, where s is given as follows:

For $p \neq 2$ or $p = 2$ and $\sigma \equiv r^e \pmod{2^x}$, let $s = x$ if $p \mid r - 1$, $v = 0$, $z = 0$, $s' \geqq x$, or $s' \geqq x + v - u$, otherwise let $s = s'$. For $p = 2$ and $r + 1 \equiv \sigma + 1 + 2^{x-1} \equiv 0 \pmod{2^x}$, let $s = x - 1$. Define $\lambda' = \theta'/\mu$, then $\sigma \equiv r^e \pmod{\lambda'}$. Applying Lemmas 3 and 5 it could be shown that there exists f' such that $\sigma \equiv f' \pmod{\theta'}$.

Now we set the congruences (a), (b), and (c), that define integers ζ, β, and α respectively.

(a) $\zeta \equiv f' \pmod{t_{\theta'}}$ and $\zeta \equiv 1 \pmod{e'}$ where e' is the product of distinct primes p with $p \mid m$ and $p \nmid t_{\theta'}$.

(b) $\beta \equiv 0 \pmod{p^v}$ if $s = x$, $\beta \equiv p^{s-2x+y+u} \pmod{p^v}$ if $s < x$ and either $p \neq 2$ or $p = 2$ and $4 \mid r-1$, and $\beta \equiv 2^{s-x+y+1} \pmod{2^v}$ if $4 \mid r+1$.

(c) $\alpha \equiv 1 \pmod{p^z}$ if $s = x$. If $s < x$, then

$$\alpha[r^\zeta - (1 + r^\beta + \cdots + r^{\beta(\sigma-1)})] \equiv \beta k(\sigma - 1)/h \pmod{p^z}.$$

Now consider the prime $p \mid \nu$ and assume $x < s$. For p odd, from Lemma 1, $p^{x-u} \| r-1$, and from the definition of θ we have $s \geqq w \geqq x + (x-u+v) - y$ or $p^v \mid y$. For $p = 2$, two cases occur and again $2^v \mid y$. Again, using the definition of θ, $s \geqq w \geqq x - z$, and hence $h \mid \beta(\sigma - 1)$.

Now for $s < x$, $p \neq 2$, we have $p^s \| \beta k(\sigma-1)/h$. Also $r^\beta \equiv 1 \pmod{p^{s+1}}$, for otherwise $s = x$. Hence the coefficient of α in the second congruence of (c) is $r^\zeta - r^e \pmod{p^{s+1}}$. From the definition of ζ, $p^s \| r^\zeta - r^e$. For $p = 2$, two cases occur and $2^s \| r^\zeta - r^e$. Hence α exists.

From the above definitions we have $b^\zeta(a^\alpha b^\beta) = (a^\alpha b^\beta)^\sigma b^\zeta$. Again using prime divisors p of ν as above, we have $h \mid yk$. Using Lemma 3, it follows that $(a^\alpha b^\beta)^k$ is a power of a^k, say a^{fk}. Here f is given as in (d) of §5. Note that $(\alpha, n) = 1$. If $p \mid g$ then $p \mid r-1$. From Lemma 3 and the definition of β the prime p does not divide the first expression in the formula of f. If $p = 2$, $2 \mid g$, then from the definition of β we have $2 \mid \beta k/h$ in all cases and hence $2 \nmid f$. For $p \neq 2$, $s = x$, we have $p \mid \beta k/h$ and $p \nmid f$. Now let $p \neq 2$ and $s < x$ and assume $p \mid f$. Then the expression above gives $\alpha = -\beta k/h + f'p$ for some integer f'. Putting this in the second congruence of (c) we have, since $r^\beta \equiv 1 \pmod{p^{s+1}}$,

$$-\beta k(r^\zeta - \sigma)/h \equiv \beta k(\sigma - 1)/h \pmod{p^{s+1}}$$

or p^{s+1} divides $-\beta k(r^\zeta - 1)/h$. But $p^{x-u} \| r^\zeta - 1$ and $s \geqq x-u$, and hence $p \mid \beta k/h$. This implies that $p \nmid f$, a contradiction. Therefore $(f, g) = 1$ and $(a^\alpha b^\beta)^k$ is of order g and hence H and G are isomorphic. This proves the sufficiency and completes the proof of the theorem.

Bibliography

1. Y. Gol'fand, *On an isomorphism between extensions of groups*, Dokl. Akad. Nauk SSSR 60 (1948), 1123–1125.

2. G. Szekeres, *Metabelian groups with two generators*, Proc. Internat. Conf. Theory of Groups, Austral. Nat. Univ. Canberra, August 1965, pp. 323–346; Gordon and Breach, New York, 1967.

University of Nebraska at Omaha