PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 123, Number 7, July 1995

ON THE FINITE IMAGES OF SOME ONE-RELATOR GROUPS

D. MOLDAVANSKI AND N. SIBYAKOVA

(Communicated by Ronald Solomon)

ABSTRACT. It is shown that the group $G = \langle a, b; a^{-1}ba = b^k\rangle$ $(k \neq 0)$ is determined in the class of all residually finite one-relator groups by the set of its finite images.

Let $\mathscr{F}(G)$ denote the set of all finite homomorphic images of a group G. Also let $G_k(m)$ be the group with presentation

$$\langle a, b; a^{-1}ba = b^k, b^m = 1\rangle,$$

where the integers $k \neq 0$ and $m > 0$ are coprime.

G. Baumslag has noted in [1] that there exist integers k, l, m (e.g. $m = 25, k = 6, l = 11$) such that the groups $G_k(m)$ and $G_l(m)$ are not isomorphic but $\mathscr{F}(G_k(m)) = \mathscr{F}(G_l(m))$. In fact, the situation is entirely described by the following statement: $\mathscr{F}(G_k(m)) = \mathscr{F}(G_l(m))$ if and only if the cosets $k + m\mathbb{Z}$ and $l + m\mathbb{Z}$ generate the same cyclic subgroups of the group $\mathbb{Z}_m^*$, the multiplicative group of integers relatively prime to m in the ring $\mathbb{Z}_m$ of integers modulo m. Moreover, $G_k(m) \simeq G_l(m)$ if and only if $k + m\mathbb{Z} = (l + m\mathbb{Z})^{\pm 1}$.

The "if" part of the first assertion as well as the second assertion was proved in [1], and the "only if" part of the first assertion was proved in [2].

Any group $G_k(m)$ is a factor group of the one-relator group

$$G_k = \langle a, b; a^{-1}ba = b^k\rangle \qquad (k \neq 0),$$

and by contrast with the above result we have

Theorem 1. *$\mathscr{F}(G_k) = \mathscr{F}(G_l)$ if and only if $k = l$.*

Proof. For any integers $r > 0$ and $s > 0$ satisfying the condition $k^r \equiv 1 (\mathrm{mod}\, s)$ we define $G_k(r, s)$ to be the group with presentation

$$\langle a, b; a^{-1}ba = b^k, a^r = 1, b^s = 1\rangle.$$

It is well known that $G_k(r, s)$ is a finite metacyclic group of order rs. Any element of $G_k(r, s)$ is uniquely representable in the form $a^\alpha b^\beta$ where $0 \leq \alpha < r$, $0 \leq \beta < s$. We notice also that the commutator subgroup of the group $G_k(r, s)$ is the cyclic subgroup generated by the element b^{k-1}.

Received by the editors May 5, 1993 and, in revised form, November 22, 1993.
1991 *Mathematics Subject Classification.* Primary 20F05; Secondary 20E26.
The work of the first author was supported by a grant of the High School Committee of Russia.

Let φ be a homomorphism of the group G_k into some finite group, and let r and s be the respective orders of the elements $a\varphi$ and $b\varphi$. The relation $a^{-\alpha}ba^{\alpha} = b^{k^{\alpha}}$ which holds in the group G_k for all $\alpha \geq 0$ shows that the integers r and s satisfy the condition $k^r \equiv 1 (\bmod s)$. This implies that any homomorphism of the group G_k into a finite group passes through some group $G_k(r, s)$.

In particular we see that if $k \neq 1$, then the group G_k has a non-abelian finite image. Therefore if $\mathscr{F}(G_k) = \mathscr{F}(G_l)$, then $k = 1$ if and only if $l = 1$, and we can assume in what follows that the numbers k and l are not equal to 1.

Now we prove two lemmas.

Lemma 1. *If $\mathscr{F}(G_k) \subseteq \mathscr{F}(G_l)$, then for every prime p and for any integer $t \geq 0$ $p^t | k - 1$ implies $p^t | l - 1$.*

(Here and everywhere below the notation $r|s$ will mean that the integer r divides the integer s. (r, s) denotes the greatest common divisor of r and s.)

To prove this assertion let us write the integers k and l in the form

$$k = 1 + p^r u, \qquad l = 1 + p^s v,$$

where $r \geq 0$, $s \geq 0$, and $(u, p) = (v, p) = 1$. If $r > 0$, then $k^p \equiv 1 (\bmod p^{r+1})$ and we may consider the group $G_k(p, p^{r+1})$. This group must be an image of the group G_l and, therefore, of some group $G_l(p^m, p^n)$. Since the group $G_k(p, p^{r+1})$ is non-abelian, $n > s$. Hence the commutator subgroup of $G_l(p^m, p^n)$, generated by the element $b^{p^s v}$, has the order $p^s = (p^s v, p^n)$. Since the order of the commutator subgroup of the group $G_k(p, p^{r+1})$ is equal to p^r, we must have $s \geq r$.

Lemma 2. *Let $\mathscr{F}(G_k) \subseteq \mathscr{F}(G_l)$. Then every prime divisor of l divides k.*

Proof. Suppose that there is a prime number p such that $p|l$ and $p \nmid k$. Since $p \nmid l - 1$, by Lemma 1, $p \nmid k - 1$. Therefore the group $G_k(p - 1, p)$ is not abelian and its commutator subgroup is of order p. Any epimorphism φ of G_l onto $G_k(p-1, p)$ passes through some group $G_l(r, s)$ where s is the order of $b\varphi$, and therefore $(s, l) = 1$. Consequently, the commutator subgroup of $G_k(p - 1, p)$ is generated by the element $(b^{l-1})\varphi$. Hence the element $(b\varphi)^{l-1}$ is of order p, but this is impossible since $p|l$ and $(s, l) = 1$.

Suppose now that for some integers k and l the equality $\mathscr{F}(G_k) = \mathscr{F}(G_l)$ holds. It follows from Lemma 1 that the integers $k - 1$ and $l - 1$ are distinguished at most by sign. Therefore if $k \neq l$ one must have $k + l = 2$. Let $k = 2^r k_1$ and $l = 2^s l_1$ where $r \geq 0$, $s \geq 0$, and k_1 and l_1 are odd. Lemma 2 implies that the integers k and l have the same prime divisors, and therefore, since $k + l = 2$, $k_1, l_1 = \pm 1$. If we assume, without loss of generality, that $r \leq s$, then the equality $2^r(k_1 + 2^{s-r} l_1) = 2$ implies $r = 0$ or $r = 1$. If $r = 0$, then $s = r$ because the integer $k_1 + 2^{s-r} l_1$ must be even. Hence $k_1 = l_1 = 1$, and so $k = l$. Let $r = 1$. Then $k_1 + 2^{s-1} l_1 = 1$ and therefore $k_1 = -1$, $l_1 = 1$, and $s = 2$. Thus in this case $k = -2$, $l = 4$. Consequently, it remains to show that $\mathscr{F}(G_{-2}) \neq \mathscr{F}(G_4)$.

To do this, we shall show that if the elements f and g of the group $G_4(2, 5)$ satisfy the condition $f^{-1} g f = g^{-2}$, then $g = 1$.

Let these elements be written in the form

$$f = a^\alpha b^\beta, \quad g = a^\gamma b^\delta \qquad (0 \le \alpha, \gamma < 2, 0 \le \beta, \delta < 5).$$

By factorization of the group $G_4(2, 5)$ by the subgroup generated by the element b the equality $f^{-1}gf = g^{-2}$ becomes $a^{3\gamma} = 1$, and we must have $\gamma = 0$. Therefore $f^{-1}gf = b^{-\beta}a^{-\alpha}b^\delta a^\alpha b^\beta = b^{\delta 4^\alpha}$ and $g^{-2} = b^{-2\delta}$. Thus

$$\delta(4^\alpha + 2) \equiv 0 \pmod 5,$$

and it follows that $\delta = 0$. The proof of Theorem 1 is completed.

It is worthwhile to make some additional remarks. At first, what can one say about a one-relator group G such that $\mathscr{F}(G) = \mathscr{F}(G_k)$? In the general case the answer is unknown, but the question can be easily answered when G is residually finite.

Corollary. *If G is a residually finite one-relator group and if for some integer k, $\mathscr{F}(G) = \mathscr{F}(G_k)$, then $G \simeq G_k$.*

To prove this, it is enough to notice that the group G_k and therefore all groups in $\mathscr{F}(G_k)$ are metabelian. Consequently, G is metabelian since G is a subdirect product of the family $\mathscr{F}(G) = \mathscr{F}(G_k)$. Since G is not cyclic, by [3], G is isomorphic to some group G_l. From Theorem 1 it follows that $l = k$.

Following [4], we denote by σG the sequence whose nth term, $\sigma_n G$, is the number of subgroups of index n of a group G. It turns out that for any finitely generated groups G and H, $\mathscr{F}(G) = \mathscr{F}(H)$ implies $\sigma G = \sigma H$.

Indeed, if N is a normal subgroup of G, then for any number $n \ge 1$ we have $\sigma_n G \ge \sigma_n(G/N)$, equality holding if and only if all subgroups of index n of G contain N. Since the group G is finitely generated, it contains only a finite number of subgroups of index n, and therefore their intersection U_n is a subgroup of finite index of G. Consequently the quotient group G/U_n is isomorphic to some H/N, and therefore

$$\sigma_n H \ge \sigma_n(H/N) = \sigma_n(G/U_n) = \sigma_n G.$$

The next result and Theorem 1 show in particular that the converse of the above statement is false.

Theorem 2. *For any integer $n \ge 1$, $\sigma_n(G_k)$ is the sum of all positive divisors of n that are coprime with k, and $\sigma_n(G_k(m))$ is the sum of all positive common divisors of m and n.*

We give a sketch of the proof of Theorem 2. Let $H(p, q, r)$ be the subgroup of G_k generated by two elements $a^p b^r$ and b^q, where $p > 0$, $q > 0$, and q is coprime with k. The following assertions can be easily verified and produce the required proof:

(1) Every subgroup of finite index of G_k coincides with some $H(p, q, r)$.

(2) $[G_k : H(p, q, r)] = pq$.

(3) $H(p_1, q_1, r_1) = H(p_2, q_2, r_2)$ if and only if $p_1 = p_2$, $q_1 = q_2$, and $r_1 \equiv r_2 \pmod{q_1}$.

(4) The subgroup $H(p, q, r)$ contains the normal closure in G_k of the element b^m if and only if q divides m.

It can also be shown that the subgroup $H(p, q, r)$ of the group G_k is isomorphic to the group G_l, where $l = k^p$. Thus Theorem 1 shows the existence of two groups, G and H, having isomorphic normal subgroups A and B of finite index such that $G/A \simeq H/B$ and $\mathscr{F}(G) \neq \mathscr{F}(H)$.

Finally, we want to mention the question of the existence of an infinite family of one-relator groups which are not isomorphic in pairs and have the same finite images. One example of such a family is prompted by a note of G. Baumslag [5]. Let H_m be the group with presentation

$$\langle a, b; a^{-m}b^{-1}a^m ba^{-m}ba^m = b^2\rangle \qquad (m > 0).$$

It is shown in [5] that $\mathscr{F}(H_1)$ coincides with $\mathscr{F}(\mathbb{Z})$, the set of all finite cyclic groups, and the same arguments show the validity of the equality $\mathscr{F}(H_m) = \mathscr{F}(\mathbb{Z})$ for any $m > 0$. The normal closure N_m of the element b in H_m is the unique invariant subgroup of H_m whose quotient is infinite cyclic. The group N_m is the free product of m freely indecomposable groups. Therefore the groups H_m and H_n are not isomorphic if $m \neq n$. Nevertheless the groups H_m are not residually finite. The problem of the existence of an analogous family of residually finite one-relator groups is still open.

Acknowledgment

The authors are very grateful to the referee for pointing to [2] and for comments which have promoted the simplification of the original proof of Theorem 1.

References

1. G. Baumslag, *Residually finite groups with the same finite images*, Compositio Math. **29** (1974), 249–252.
2. M. Burrow and A. Steinberg, *On a result of G. Baumslag*, Compositio Math. **71** (1989), 241–245.
3. W. Magnus, *Uber diskontinuierliche gruppen mit einer definieren den relation* (*der Freiheitssatz*), J. Reine Angew. Math. **163** (1930), 141–165.
4. G. Baumslag, *Some problems on one-relator groups*, Proc. Second Internat. Conf. Theory of Groups, Canberra, 1973, pp. 75–81.
5. ______, *A non-cyclic one-relator group all of whose finite quotients are cyclic*, J. Austral. Math. Soc. **10** (1969), 497–498.

Department of Mathematics, Ivanovo State University, Ivanovo, 153002, Russia
E-mail address: svi@ivgu.ivanovo.su