Symmetric presentations of Abelian groups

Miklós Abért

Abstract. We characterise the abelianisation of a group that has a presentation for which the set of relations is invariant under the full symmetric group acting on the set of generators. This improves a result of Emerson.

Symmetric presentations have been investigated for a long time (see [**Cox**], [**Eme**], [**Bee**] and [**CM**]). Recently the focus of interest has been in constructing the finite simple groups in this way. The sporadic case is investigated in [**Cu1**], [**Cu2**], [**CHB**] and [**BC**] while the Lie-type case is treated in [**CR**], [**CRW**], [**RC**] and [**CHLR**].

Definition 1. *Let* $G = (F \mid R)$ *be a presentation of the group* G. *We call this presentation symmetric if* R *is invariant under the action of the full symmetric group permuting the generating set* F.

Definition 2. *Let* $G = \langle g_1, g_2, \ldots, g_n \rangle$ *be an arbitrary group. We say that the* g_i*'s symmetrically generate* G *if the presentation belonging to that generating set is symmetric.*

In this paper we determine which finite Abelian groups can be symmetrically generated. This can be considered as a 'test of symmetric generation' for an arbitrary group G, since if G is symmetrically generated then its abelianisation G/G' is symmetrically generated as well. Our result is a generalisation of the results of Emerson (see [**Eme**]), who gives the canonical form of the abelianisation of a group, that can be defined by a single relation and all of its permutations. He expresses the canonical form from the exponent sums of the single relation. We make use of the methods of Emerson and obtain a somewhat surprising result.

Theorem 1. *Let* G *be a finite Abelian group. Then* G *can be symmetrically generated by* $n > 2$ *elements if, and only if, there are positive integers* a, b, c *such that*

(i) $G = Z_a \times Z_{ab}^{n-2} \times Z_{abc}$, *and*
(ii) $\gcd(b, c) | n$.

Comment. The case $n = 2$ is trivial, since $Z_{ab} \times Z_a \simeq \langle x, y \mid x^{ab} = y^{ab} = (xy^{-1})^a = x^{-1}y^{-1}xy = 1 \rangle$.

1991 *Mathematics Subject Classification.* Primary 20F05, 20K01.
Key words and phrases. Presentations, Abelian groups.
Research supported by the Hungarian National Grant T29132.

Proof. First we prove that if G is symmetrically generated, then (i) and (ii) hold.

Let $G = \langle g_1, g_2, \ldots, g_n \rangle$ be a symmetric generating set of G. For an arbitrary integer F that will be specified later, let us define $h_1, \ldots, h_n \in G$ in the following way:

$h_1 = g_1$
$h_i = ig_1 - \sum_{j=1}^{i} g_j \quad (1 < i < n)$
$h_n = Fg_1 - \sum_{j=1}^{n} g_j$

We claim that there is an F for which $h_1, h_2, \ldots, h_n$ is a base of G. We have to prove that $G = \langle h_1, h_2, \ldots, h_n \rangle$ and that if $\sum_{j=1}^{n} r_j h_j = 0$ then $r_j h_j = 0$ for all j.

Now $G = \langle h_1, h_2, \ldots, h_n \rangle$ directly follows from the fact that the transformation matrix of $g_i \to h_i$,

$$M = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 & 0 \\ 1 & -1 & 0 & \ldots & 0 & 0 \\ 2 & -1 & -1 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ n-2 & -1 & -1 & \ldots & -1 & 0 \\ F-1 & -1 & -1 & \ldots & -1 & -1 \end{pmatrix}$$

has $\det(M) = (-1)^{n-1}$, so it can be inverted over $\mathbb{Z}$.

Let us assume that $\sum_{j=1}^{n} r_j h_j = 0$ and there is an index $k < n$, for which $r_k h_k \neq 0$. Let k be the largest such index.

First suppose that $1 < k < n$. Taking the nonzero parts of the sum $\sum_{j=1}^{n} r_j h_j = 0$ and using the definition of h_i we get $\sum_{j=1}^{n} s_j g_j = 0$ where $s_k = -(r_k + r_n)$, $s_{k+1} = -r_n$. Now using the symmetry of the generating set $g_1, g_2, \ldots, g_n$ of G, and applying the transposition $(k, k+1)$, finally taking the difference of the two zero sums we get $r_k(g_k - g_{k+1}) = 0$. Using the symmetry again we get $r_k(g_i - g_j) = 0$ for all $i \neq j$. But then $0 \neq r_k h_k = r_k \sum_{j=1}^{k} (g_1 - g_j) = 0$, which is a contradiction.

So we have to find an F for which h_1 and h_n are independent and we will be done.

Let p be the order of $h_1 = g_1$. Then for all $g \in G$, $pg = 0$ because of the symmetry. So $\langle h_1 \rangle$ is a cyclic subgroup of maximal order in $\langle h_1, \sum_{j=1}^{n} g_j \rangle$ and, as such, it has a direct complement. So we have an integer F such that

$$\langle h_1, \sum_{j=1}^{n} g_j \rangle = \langle h_1 \rangle \oplus \langle Fh_1 - \sum_{j=1}^{n} g_j \rangle.$$

We have proved that $h_1, h_2, \ldots, h_n$ is a base of G.

Now we show (i) and (ii). Let q be the order of h_2. Then $q(g_1 - g_2) = 0$. Using the symmetry we get $q(g_i - g_j) = 0$, from which $qh_k = q \sum_{j=1}^{k} (g_1 - g_j) = 0$ follows for all $1 < k < n$. On the other hand, let us assume that there is a $z \in \mathbb{Z}$, for which $zh_k = 0$ for some $1 < k < n$. Using the definition of h_k we get $\sum_{j=1}^{n} s_j g_j = 0$, where $s_k = -z$, $s_{k+1} = 0$. Applying the transposition $(k, k+1)$ for this and subtracting the result from the former equation we get $z(g_k - g_{k+1}) = 0$. By symmetry $zh_2 = z(g_1 - g_2) = 0$ follows. So for all $1 < k < n$ the order of h_k is q.

Now let $c = p/q$ and let a be the order of h_n. Here $0 = \sum_{j=1}^n q(g_1 - g_j) = qng_1 - q\sum_{j=1}^n g_j$, so $qh_n = q(Fg_1 - \sum_{j=1}^n g_j) = (qF - qn)h_1$. Thus using the independence of h_1 and h_n we have $qh_n = 0$ and $q(F-n)h_1 = 0$, proving $a|q$ and $p|q(F-n)$, that is $c|F-n$.

Now $0 = ah_n = aFg_1 - a\sum_{j=1}^n g_j$. Applying the transposition $(1,2)$ to this equation and subtracting the result we get $0 = aF(g_1 - g_2) = aFh_2$, so $q|aF$. Let $b = q/a$, then we have $b|F$. Now let $d = \gcd(b,c)$. Then $d|F$ and $d|(F-n)$, and hence $d|n$ which is what we wanted to prove.

Conversely we show that if a finite Abelian group satisfies (i) and (ii), then it can be symmetrically generated.

Let $G = \langle h_1, h_2, \ldots, h_n\rangle$ be a canonical generating set of G, so that the i-th component of the product in (i) belongs to h_i.

We can solve the Diophantine equation $n = bx - cy$, because $\gcd(b,c)|n$. Let $F = bx$. Now $b|F$ and $c|F-n$. Let us define $g_1, \ldots, g_n$ in the following way:

$g_1 = h_1$
$g_2 = h_1 - h_2$
$g_i = h_1 + h_{i-1} - h_i \quad (2 < i < n)$
$g_n = (F - n + 1)h_1 + h_{n-1} - h_n$

We claim that $g_1, g_2, \ldots, g_n$ is a symmetric generating set of G.

The claim $G = \langle g_1, g_2, \ldots, g_n\rangle$ directly follows from the fact that the transformation matrix of $h_i \to g_i$,

$$N = \begin{pmatrix} 1 & 0 & 0 & 0 & \ldots & 0 \\ 1 & -1 & 0 & 0 & \ldots & 0 \\ 1 & 1 & -1 & 0 & \ldots & 0 \\ 1 & 0 & 1 & -1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ F-n+1 & 0 & 0 & 0 & \ldots & -1 \end{pmatrix}$$

has $\det(N) = (-1)^{n-1}$, so it can be inverted over $\mathbb{Z}$ (in fact, it is the inverse of the matrix M).

To prove the symmetry, we only have to show that for all $1 \le k < n$ the transposition $(k, k+1)$ brings all relations to a relation, because these transpositions generate the full symmetric group. Or, equivalently, we have to prove that if $\sum_{j=1}^n r_j g_j = 0$, then we have $\sum_{j=1}^{k-1} r_j g_j + r_{k+1} g_k + r_k g_{k+1} + \sum_{j=k+2}^n r_j g_j = 0$.

Using the definition of g_j and the fact, that $h_1, h_2, \ldots, h_n$ is a canonical generating set of G belonging to (i), we get the following reformulation of $\sum_{i=1}^n r_i y_i = 0$:

(1) $\sum_{i=1}^n r_i + (F-n)r_n \equiv 0 \pmod{abc}$

(2) $r_{i+1} - r_i \equiv 0 \pmod{ab}$ for all $1 < i < n$ (so these coefficients are all congruent modulo ab)

(3) $r_n \equiv 0 \pmod{a}$

All we have to prove is that this congruence system remains true if we apply the transposition $(k, k+1)$ to $(r_1, r_2, \ldots, r_n)$.

If $1 < k < n-1$ then (1) and (2) trivially remains true, while (3) even formally does not change.

Let $k = n-1$. We know that $c|F-n$ and $ab|(r_n - r_{n-1})$, so $(F-n)(r_n - r_{n-1}) \equiv 0 \pmod{abc}$.

Subtracting this congruence from (1) we obtain $\sum_{i=1}^{n} r_i + (F-n)r_{n-1} \equiv 0 \pmod{abc}$ what precisely means that (1) remains true. Now (2) remains true trivially, while (3) remains true because from (2) we infer $r_{n-1} \equiv r_n \pmod{a}$.

Lastly, if $k=1$, then we only have to check (2), the other two remaining true formally. We know that $b|F$ and $a|r_n$, so $ab|Fr_n$, from this we get $r_n \equiv -(F-1)r_n \equiv -(F-n)r_n - (n-1)r_n \equiv \sum_{i=1}^{n} r_i - (n-1)r_n \equiv r_1 \pmod{ab}$ by (2), but then we have $r_1 \equiv r_n \equiv r_2 \pmod{ab}$ and so (2) remains true. □

References

[Bee] M.J. Beetham, A set of generators and relations for the group $PSL(2,q)$, q odd, J. London Math. Soc. 3 (1971), 554–557.

[BC] J.N. Bray, R.T. Curtis, A systematic approach to symmetric presentations II. Generators of order 3, Math. Proc. Cambridge Philos. Soc. 128 (2000), 1-20.

[CHLR] C. Campbell, G. Havas, S. Linton, E. Robertson, Symmetric presentations and orthogonal groups: The atlas of finite groups: ten years on (Birmingham, 1995), 1-10, London Math. Soc. Lecture Note Ser., 249, Cambridge Univ. Press, Cambridge, 1998.

[CR] C.M. Campbell and E.F. Robertson, Some problems in group presentations, J. Korean Math. Soc. 19 (1983), 123–128.

[CRW] C.M. Campbell, E.F. Robertson and P.D. Williams, Efficient presentations of the groups $PSL(2,p) \times PSL(2,p)$, p prime, J. London Math. Soc. (2) 41 (1989), 69–77.

[Cox] H.S.M. Coxeter, Symmetrical definitions for the binary polyhedral groups, Proc. Sympos. Pure Math. 1 (1959), 64–87.

[CM] H.S.M. Coxeter and W.O.J. Moser, Generators and relations for discrete groups, 4th edition (Springer, Berlin, 1979).

[Cu1] R.T. Curtis, Symmetric presentations. I. Introduction, with particular reference to the Mathieu groups M_{12} and M_{24}, Groups, combinatorics & geometry (London Math. Soc. Lecture Note Ser., 165, Cambridge Univ. Press, Cambridge, 1992), 380–396.

[Cu2] R.T. Curtis, Symmetric presentations. II. The Janko group J_1, J. London Math. Soc. (2) 47 (1993), 294–308.

[CHB] R.T. Curtis, A.M.A. Hammas, J.N. Bray, A systematic approach to symmetric presentations I. Involutory generators, Math. Proc. Cambridge Philos. Soc. 119 (1996), 23-34.

[Eme] W. Emerson, Groups defined by permutations of a single word, Proc. Amer. Math. Soc. 21 (1969), 386–390.

[RC] E.F. Robertson and C.M. Campbell, Symmetric presentations, Group Theory (Walter de Gruyter, Berlin, New York, 1989), 497–506.

Alfréd Rényi Institute of Mathematics,, Reáltanoda utca 13-15, H-1053, Budapest, Hungary

E-mail address: `abert@renyi.hu`