# SOME COMPUTATIONAL APPROACHES TO GROUPS GIVEN BY A FINITE PRESENTATION[1]

**Joachim Neubüser**
Lehrstuhl D für Mathematik
RWTH Aachen, 5100 Aachen
West Germany

**Said Sidki**
Departamento de Matemática
Universidade de Brasília
70910 - Brasília DF
Brasil

## 0. Introduction

"What is this group like?" could be an alternative title for this paper. Our special interest is in groups which are presented to us as being generated by a small set of elements, be these permutations of vertices of a graph, matrices describing automorphisms of linear codes, or classes of homotopies of a knot described only by the relations that they satisfy (see [Hac 87]).

Although the axioms that define the notion of a group are rather simple, and in spite of the abundance of knowledge about large classes of groups, one is frequently frustrated by the paucity of methods for dealing with groups described by a small set of generators and relations that hold between them.

What is lacking in the standard texts of classical algebra and group theory is a counterpart of numerical methods in differential equations. Yet, such computational methods in group theory have been developed along the years under the influence of external problems as well as from within, especially by the needs of the classification of finite simple groups and the Burnside Groups problem.

It should be emphasized that the present computational methods build on careful analysis of algorithmic aspects of known theories. Also, that the practical use of these algorithms became possible in a meaningful way only with the advent of computer technology.

We will present in this article some of the known computational methods for investigating groups given by generators and relations, comment

[1] Published as: Alguns Procedimentos Computacionais Para Grupos Dados Por Uma Apresentação Finita, Mathemática Universitaria No. 7, (1988) 77 – 120, Rio de Janeiro

upon their theoretical background, and illustrate them by way of worked-out examples.

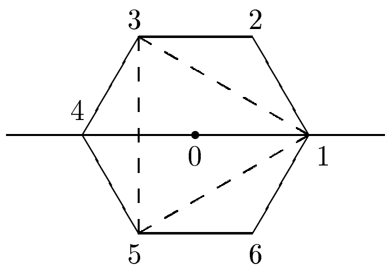
We have made an effort to reduce the requirements to a minimum and have developed some calculations in detail. The reader who wishes to pursue this topic further can learn about the state of the art in [Atk 84].

## Contents

## 1. Free groups and presentations

The identification of a group given by generators and relations may be likened humorously to a detective story where the available clues are few yet sufficient to pin down the suspect.

As an example, let us consider $D_{12}$ and $D_6$, the groups of the Euclidean symmetries of the regular hexagon 123456, and the regular triangle 135.




By direct enumeration , $D_{12}$ has twelve elements and $D_6$ has six elements. Call the anticlockwise rotation by $\frac{2\pi}{6}$ around 0 by $A$, further $A^2$ by $A_2$, and the reflection in the line 14 by $B$. Then $A$, $B$ are symmetries of the hexagon, and $A_2$, $B$ are symmetries of the triangle. We observe that

$$A^6 = 1,\ B^2 = 1,\ B^{-1}AB = A^{-1},\ \text{and}\ A_2^3 = 1,\ B^2 = 1,\ B^{-1}A_2B = A_2^{-1}.$$

From $A_2^3 = 1$, we have $(A_2^3)^2 = A_2^6 = 1$.

The relation $B^{-1}AB = A^{-1}$ implies, for any integers $i, j \geq 0$, that

$$B^{-j}AB^j = B^{-1}(\ldots B^{-1}(B^{-1}AB)B\ldots)B = A^{(-1)^j},$$

and

$$B^{-j}A^iB^j = (B^{-j}AB^j)^i = A^{(-1)^j i},$$

that is,

$$A^iB^j = B^jA^{(-1)^j i},$$

which allows the transport of $B^j$ from the right to the left of $A^i$. The elements of the subgroup $H$ of $D_{12}$ generated by $A$, $B$, therefore have the form $B^jA^i$ for $0 \leq i < 6$, $0 \leq j < 2$, and one can easily see this to be a normal form. It follows that $H$ has twelve elements and $H = D_{12}$. Similarly, one shows that $D_6$ is generated by $A_2$ and $B$.

Now suppose that the information provided about a suspect group is that it is generated by two elements $a$, $b$ subject to the relations

$$a^6 = 1, b^2 = 1, b^{-1}ab = a^{-1},$$

can one identify this group, up to isomorphism, to be $D_{12}$? And then, how about $D_6$? The answer to such a question requires the formal introduction of the concept of a free group and of a presentation of a group.

Let $X = \{x_1, \ldots, x_n, x_1^{-1}, \ldots, x_n^{-1}\}$ be a set of $2n$ different elements. A finite sequence $(y_1, \ldots, y_k)$ with $y_i \in X$, such that no two subsequent elements are of the form $x_i, x_i^{-1}$ or $x_i^{-1}, x_i$ as well as the empty sequence ( ) is called a "reduced word" $w(x_i)$. It can be proved that the set of all reduced words is a group if one defines "multiplication" of two such sequences by their concatenation

$$(y_1, \ldots, y_k)(y_{k+1}, \ldots, y_l) = (y_1, \ldots, y_k, y_{k+1}, \ldots, y_l)$$

followed by the removal of all consecutive pairs of the form $x_i, x_i^{-1}$ and $x_i^{-1}, x_i$. (To show that one arrives at the same result irrespective of the sequence in which removals are performed, is the main part of the proof.) The empty sequence obviously is the neutral element in this group, and the inverse of a sequence is formed by reversing it and changing each $x_i$ for $x_i^{-1}$ and each $x_i^{-1}$ for $x_i$. This group is clearly generated by the sequences $(x_i), i = 1, \ldots, n$. As customary, we shall just write a "formal product" $y_1 y_2 \cdots y_k$ for a sequence $(y_1, \ldots, y_k)$ with $y_i \in X$, and 1 for the empty sequence ( ). This group is called the free group $F_n$ of rank $n$, freely generated by $x_1, \ldots, x_n$.

Now let $G$ be any group generated by a set $\{g_1, \ldots, g_n\}$. The fact that each element in $F_n$ has a unique reduced form which therefore is a normal form in the generators $x_1, \ldots, x_n$ shows that the function $\phi : x_i \mapsto g_i$ extends to an epimorphism $\phi$ of $F_n$ onto $G$. Hence by the homomorphism theorem $G$ is isomorphic to the factor group of $F_n$ by the kernel of $\phi$, that is $G \cong F_n/ker\ \phi$. This kernel consists exactly of those words $r(x_i)$, for which the "value" $\phi(r(x_i))$, i.e. the element $r(g_i) \in G$ obtained by replacing each $x_i^{\pm 1}$ by $g_i^{\pm 1}$, is the neutral element of $G$ (which we also denote by 1). This is what is meant by saying that these elements $r(x_i)$ are "relators" corresponding to "relations" $r(g_i) = 1$ for the generating set $\{g_i\}$ of $G$.

Any set $R = \{r_j(x_i)\} \subseteq ker\ \phi$ such that $ker\ \phi$ is the normal closure of $R$, (i.e. the smallest normal subgroup of $F_n$ containing $R$) is called a "defining set of relators" for $G$ with respect to the generating set $\{g_i\}$ and the corresponding set of relations $\{r_j(g_i) = 1\}$ a "defining set of relations". A set of generators together with a defining set of relations (relators) is called a presentation, and the group $G$ is called finitely presented, if not only the set of generators, but also the defining set of relations is finite.

It is time we return to the question whether the generators $a$, $b$ together with the defining relations $a^6 = 1$, $b^2 = 1$, $b^{-1}ab = a^{-1}$, provide a presentation for $D_{12}$. In other words, is the factor group of the free group $F_2$ by the normal closure $N$ of $\{x_1^6, x_2^2, x_2^{-1}x_1x_2x_1\}$ isomorphic to $D_{12}$? The kernel of the epimorphism $\phi : F_2 \to D_{12}$ defined by $\phi : x_1 \mapsto A$, $x_2 \mapsto B$, contains $x_1^6, x_2^2, x_2^{-1}x_1x_2x_1$. Is $N = ker\ \phi$ ? Here we repeat the calculations done for the normal form of the elements in $D_{12}$ in the case of $F_2/N$, generated by $Nx_1, Nx_2$, and reach the conclusion that $F_2/N$ has at most twelve elements. However, as $N \subseteq ker\ \phi$, $F_2/N$ has a multiple of 12 elements, and so $N = ker\ \phi$.

Before continuing let us add two remarks:

(i) A nontrivial group has many generating sets and to each can belong many different defining sets of relations;

(ii) We may reverse the process described above. Let $W = \{w_j(x_i)\}$ be an arbitrary set of elements of $F_n$ and $N$ be the normal closure of $W$, then $\{w_j(x_i)\}$ is a defining set of relators for $F_n/N$. So any presentation defines (uniquely up to isomorphism) some group. Such presentations are in fact used very often in certain branches of mathematics, such as topology (see [Hac 87]) to describe groups about which very little is known otherwise, often not even whether they are finite or not.

This was the case, for instance, with the following class of presentations

$$C_q = \langle\ a, b\ \mid\ aba^{-2}bab^{-1} = 1,\ a(b^{-1}a^3b^{-1}a^{-3})^q = 1\ \rangle$$

which were sent to one of us in November 1984 by A. Cavicchioli. Although the original question, whether the groups $C_q$ and $C_{q'}$ are non-isomorphic for $q \neq q'$, has meanwhile been answered by a different approach (see [Cav 86]) they furnish a nice example for the demonstration of computational methods.

This request about $C_q$ fits within problems posed by Max Dehn in 1911 [Deh 11] about the existence of universal algorithms for deciding three questions in the class $FP$ of finitely presented groups: let $G_1$, $G_2$ be $FP$ groups, furthermore let $\phi_i : F_{n_i} \to G_i \;\; (i = 1, 2)$ be the epimorphisms that provide the given finite presentations for these groups,

(1) (Word Problem) given $w \in F_{n_1}$, decide whether or not $w \in ker\ \phi_1$,

(2) (Conjugacy Problem) given $u, v \in F_{n_1}$, decide whether or not $\phi_1(u)$ and $\phi_1(v)$ are conjugate in $G_1$,

(3) (Isomorphism Problem) decide whether or not $G_1$ and $G_2$ are isomorphic groups.

## 2. Abelian groups and the elementary divisor algorithm

**(1)** The canonical decomposition of finitely presented abelian groups has an algorithmic proof that leads directly to an easy implementation and also to a positive answer to Dehn's word and isomorphism problems for this specific class of groups. Here, obviously, the conjugacy and word problems are equivalent.

Let $A$ be an abelian group generated by the set $\{a_1, a_2, \ldots, a_n\}$ satisfying a possibly empty defining set of relations $\{r_i(a_j) = 1 \mid 1 \leq i \leq m\}$. That is, $A$ affords the presentation

$$\langle a_1, a_2, \ldots, a_n \mid [a_i, a_j] = 1 \text{ for } 1 \leq i < j \leq n,\ r_i(a_j) = 1 \text{ for } 1 \leq i \leq m \,\rangle$$

where the symbol $[a_i, a_j]$ denotes the commutator $a_i^{-1} a_j^{-1} a_i a_j$. The kernel $K$ of the epimorphism $\phi : F_n \to A$ defined by $\phi : x_i \mapsto a_i$ contains the derived group $F_n'$ which is the normal closure of the set $\{[x_i, x_j] \mid 1 \leq i < j \leq n\}$. Thus, $\phi$ induces the epimorphism $\bar{\phi} : \bar{F}_n \to A$ where $\bar{F}_n = F_n / F_n'$ is the free abelian group of rank $n$.

On rewriting the group operation of $\bar{F}_n$ additively, we have that $\bar{K}$ is generated by

$$r_i(\bar{x}_j) \;=\; \sum_{j=1}^{n} m_{ij} \bar{x}_j \qquad (1 \leq i \leq m)$$

where the $m_{ij}$ are integers. We may apply to the $n \times m$ matrix $M = (m_{ij})$ the usual elementary transformations with the exception of multiplication of rows or columns by integers $\neq \pm 1$. These operations produce new bases for $\bar{F}_n$ and generating sets for $\bar{K}$.

Following the procedure which will be described below, $M$ can be transformed into its normal form

$$\left(\begin{array}{cccc|c} d_1 & & & & \\ & d_2 & & & 0 \\ & & \ddots & & \\ & & & d_k & \\ \hline & & 0 & & 0 \end{array}\right)$$

where the set $\{d_1, d_2, \ldots, d_k\}$ of positive integers, when nonempty, will have the divisibility property $d_1 \mid d_2 \mid \ldots \mid d_k$ – the elementary divisors of $A$.

The matrix in normal form provides us with a basis $\bar{y}_1, \ldots, \bar{y}_n$ of $\bar{F}_n$ such that $r_1'(\bar{y}_i) = d_1\bar{y}_1, \ \ldots, \ r_k'(\bar{y}_i) = d_k\bar{y}_k$ is a basis for $\bar{K}$, and so,

$$A \ \cong \ \bar{F}_n/\bar{K} \ \cong \ \langle \bar{K} + \bar{y}_1 \rangle \ \oplus \ldots \oplus \ \langle \bar{K} + \bar{y}_n \rangle$$

where

$$\begin{array}{lll} \langle \bar{K} + \bar{y}_i \rangle \cong \mathbf{Z}_{d_i} & \text{(cyclic of order } d_i) & \text{for } 1 \leq i \leq k, \\ \qquad\qquad \cong \mathbf{Z} & \text{(infinite cyclic)} & \text{for } k+1 \leq i \leq n. \end{array}$$

Thus we have arrived at a presentation for $A$ of the form

$$\langle z_1, \ldots, z_n \mid \ [z_i, z_j] \ = \ 1 \ \ (1 \leq i < j \leq n), \quad z_1^{d_1} \ = \ldots = \ z_k^{d_k} \ = 1, \\ \text{with } \ d_i \geq 1, \ \text{ and } \ d_1 \mid d_2 \mid \ \ldots \ \mid d_k \ \rangle.$$

If $d_1 = d_2 = \ldots = d_l = 1$, and $d_{l+1} \neq 1$, then $A$ has the canonical decomposition

$$A \ \cong \ \mathbf{Z}_{d_{l+1}} \oplus \ldots \oplus \mathbf{Z}_{d_k} \oplus \underbrace{\mathbf{Z} \oplus \ldots \oplus \mathbf{Z}}_{n-k}$$

and $\{d_{l+1}, \ \ldots, \ d_k \ ; \ n-k\}$ is the set of invariants that characterizes $A$.

**(2)** To demonstrate the algorithm, it suffices to bring $M$ into the form

$$M_1 = \left(\begin{array}{c|c} x & 0 \\ \hline 0 & M' \end{array}\right)$$

where $x \mid m'_{ij}$ for all entries $m'_{ij}$ of $M'$. This is done as follows for $M \neq 0$.

1. Select $m_{ij} \in M$ with $0 \neq | m_{ij} | \leq | m_{rs} |$ for all $0 \neq m_{rs} \in M$.

2. Interchange rows $R_i$ and $R_1$;
   interchange columns $C_j$ and $C_1$;
   (*now* $0 \neq | m_{11} | \leq | m_{rs} |$ *for all* $0 \neq m_{rs} \in M$)
   multiply $R_1$ by $\pm 1$ to make $m_{11} > 0$.

3. For $j = 2, \ldots, n$
   write $m_{1j} = c_j m_{11} + r_j$ with $0 \leq r_j < m_{11}$;
   if $c_j \neq 0$,
   subtract $c_j C_1$ from $C_j$.
   (*Now* $0 \leq m_{1j} < m_{11}$ *for* $j = 2, \ldots, n$).

4. If there exists $m_{1j} \neq 0$ for $j \neq 1$,
   exchange $C_1$ and $C_j$;
   go back to 3.
   (*This stops when* $R_1 = (m_{11}, 0, \ldots, 0)$).

5. If $m_{11}$ does not divide all entries of $M$,
   select $m_{ij}$, such that $m_{11} \not| m_{ij}$;
   if $j \neq 1$, add $C_1$ to $C_j$;
   write $m_{ij} = d_{ij} m_{11} + r_{ij}$ with $0 < r_{ij} < m_{11}$;
   substract $d_{ij} R_1$ from $R_j$;
   (*so, now* $0 < m_{ij} < m_{11}$)
   go back to 1.
   (*Since* $m_{11}$ *keeps decreasing, eventually* $m_{11} \mid m_{ij}$ *for all* $i, j$ *and we come to point 6*).

6. For $i = 2, \ldots, m$
   write $m_{i,1} = d_i m_{11}$;
   if $d_i \neq 0$,
   subtract $d_i R_1$ from $R_i$.

**(3)** Given the good grasp we have on finitely presented abelian groups, one of the first methods we apply to a group $G$ which is finitely presented as

$$\langle\, g_1, \ldots, g_n \mid r_1(g_i) \;= \ldots =\; r_m(g_i) \;= 1 \,\rangle$$

is the study of its abelianization $\bar{G} = G/G'$ which has the presentation

$$\langle a_1, \ldots, a_n \mid [a_i, a_j] \;=\; 1 \; (1 \leq i < j \leq n),\; r_1(a_i) = \ldots =\; r_m(a_i) \;= 1 \,\rangle.$$

For instance for $C_q$:

$$\bar{C}_q = \langle\, a, b \mid [a,b] = 1,\ aba^{-2}bab^{-1} = 1,\ a(b^{-1}a^3b^{-1}a^{-3})^q = 1 \,\rangle.$$

As a and b commute in $\bar{C}_q$, the second and third relation may be rewritten as

$$1 = aa^{-2}abbb^{-1} = b,\ 1 = ab^{-q}a^{3q}b^{-q}a^{-3q} = ab^{-2q},$$

or as

$$b = 1\ ,\ a = b^{2q}.$$

So

$$a = b = 1 \text{ in } \bar{C}_q.$$

That is, $\bar{C}_q$ is trivial, or what is the same, $C_q$ is a perfect group. An immediate consequence is that the minimal nontrivial finite quotients of $C_q$, if any, are noncyclic simple groups.

## 3. Novikov's theorem and the Todd–Coxeter method

While in the last section we saw that Dehn's problems have a very elegant solution for finitely presented abelian groups, in 1955 P. S. Novikov [Nov 55] published a proof that the word problem is unsolvable. In fact he proved that there exists a finitely presented group $G$ that will defeat any algorithm that claims to decide in a finite number of steps if a given word in the generators of $G$ represents the identity or not. Soon after, also Dehn's other problems were proved to be algorithmically unsolvable as well as other questions, e. g. to decide from a given presentation if the group presented is finite [Rab 58]. These results leave room only for a more modest attempt than the solution of Dehn's problems and such a more modest approach had in fact been proposed already in 1936 by J. Todd and H.S.M. Coxeter [ToC 36].

Their method can best be characterized as a "verification method": if the group described by a finite presentation is in fact finite, the method will eventually (i. e. after a finite number of steps) stop, having verified this fact, but no bound can be given from the presentation, when this will happen; so if the method has not been successful after a given time, <u>no</u> conclusion can be drawn; it is <u>not</u> a decision algorithm.

The Todd-Coxeter method actually deals with a slightly more general situation: Given a finite presentation

$$G \;=\; \langle\; g_1, \ldots, g_n \mid r_1(g_i) \;=\; 1,\; \ldots,\; r_m(g_i) \;=\; 1 \;\rangle$$

and a finite set of words

$$\{\; s_1(g_i),\; \ldots,\; s_p(g_i) \;\},$$

it tries to determine the index of the subgroup $U \;=\; \langle\; s_1(g_i),\; \ldots,\; s_p(g_i)\;\rangle$ in $G$ by constructing the permutation representation of $G$ on the set of right cosets of $U$ in $G$:

$$\varphi_U \;:\; g \;\mapsto\; \begin{pmatrix} Uh \\ Uhg \end{pmatrix} \quad \text{for all} \quad g,\; h \in G.$$

This is done for the generators of $G$ in a trial-and-error fashion: Cosets of $U$ will be given numbers $1, 2, 3, \ldots$ starting with $1 := U$, but only if the method finishes successfully, will it be certain that different numbers represent different cosets: during the process several numbers may be given inadvertently to the same coset.

For each subgroup generator

$$s(g_i) \;=\; g_{i_1}\; \ldots\; g_{i_e},\;\; g_{i_j} \;\in\; \{g_1,\; \ldots,\; g_n, g_1^{-1},\; \ldots,\; g_n^{-1}\} \;=:E,$$

a one-line "subgroup table"

$$\begin{array}{c|c|ccc|c}
 & g_{i_1} & g_{i_2} & \cdots & g_{i_e} & \\
\hline
1 & & & & & 1
\end{array}$$

is set up, expressing the fact that $Us(g_i) \;=\; U$. Likewise for each relation $r(g_i) = g_{i_1} \ldots g_{i_t} = 1$ a "relation table",

$$\begin{array}{c|c|ccc|c}
 & g_{i_1} & g_{i_2} & \cdots & g_{i_t} & \\
\hline
1 & & & & & 1 \\
2 & & & & & 2 \\
\vdots & & & & & \vdots \\
k & & & & & k \\
\vdots & & & & & \vdots
\end{array}$$

having one line for each coset number defined in the process, reflects the fact that for each coset $k := Uh$ we have $k \cdot r(g_i) = k$.

A single "coset table" is used for the bookkeeping of the recursive definition of the meaning of the coset numbers:

| | $g_1$ | $\dots$ | $g_n$ | $g_1^{-1}$ | $\dots$ | $g_n^{-1}$ |
|---|---|---|---|---|---|---|
| 1 | | | | | | |
| 2 | | | | | | |
| $\vdots$ | | | | | | |
| $k$ | | | | | | |
| $\vdots$ | | | | | | |

The method proceeds by defining each new coset number $l$ by an equation of the form $l := k \cdot g$, where $k$ is a previously defined coset number, $g$ a generator or its inverse and the place for this definition in the coset table is still vacant. Together with $l := kg$ the entry $k = lg^{-1}$ is made in the coset table and then both these definitions are inserted into all subgroup and relation tables. Whenever a line closes in one of the subgroup or relation tables, it yields an information of the kind $kg = l$, called a "consequence". Comparing this with the state of the coset table one of three cases can occur:

(i) both of the entries for $kg$ and for $lg^{-1}$ in the coset table are still empty. Then this new information is entered into both places of the coset table and used in the same way as the definitions before;

(ii) these places already contain this information. Then nothing needs to be done;

(iii) one of the places contains a different information, say $kg = l' \neq l$. Then we learn that in fact the <u>coset numbers</u> $l$ and $l'$ denote the same coset, and we have to eliminate one (the bigger) of them. Doing so, we may in fact find more such so-called "coincidences".

Let us demonstrate the beginning of the method for the first of Cavicchioli's groups. We write its presentation in the form

$$C_1 = \langle\, a, b \;\mid\; a^{-2}bab^{-1}ab = 1,\; a^3b^{-1}a^{-2}b^{-1} = 1 \,\rangle$$

Note that the relations have been cyclically permuted, i.e. conjugated. Transformations like this often are advantageous in order to get neater enumerations. We try to enumerate the cosets of $U := \langle a \rangle$, so we have one subgroup table

| | $a$ |
|---|---|
| 1 | 1 |

which tells us immediately that $1a = 1$ (and $1a^{-1} = 1$). Introducing these and a first definition $1b =: 2$ (and $2b^{-1} = 1$) into coset table and relation tables we have

Relation tables:

| | $a^{-1}$ | $a^{-1}$ | $b$ | $a$ | $b^{-1}$ | $a$ | $b$ |
|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 2 | | | | 1 |
| 2 | | | | 2 | 1 | 1 | 2 |

| | $a$ | $a$ | $a$ | $b^{-1}$ | $a^{-1}$ | $a^{-1}$ | $b^{-1}$ |
|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | | | 2 | 1 |
| 2 | | | | | | | 2 |

Coset table:

| | $a$ | $b$ | $a^{-1}$ | $b^{-1}$ |
|---|---|---|---|---|
| 1 | 1 | 2 | 1 | |
| 2 | | | | 1 |

After the further definitions $1b^{-1} =: 3$ and $2a =: 4$, the first line of the second relation table closes

| | $a$ | $a$ | $a$ | $b^{-1}$ | $a^{-1}$ | $a^{-1}$ | $b^{-1}$ |
|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 3 | 4 | 2 | 1 |
| . | . | . | . | . | . | . | . |

and yields as a first "consequence" $3a^{-1} = 4$ which together with $4a = 3$ is entered into the coset table.

The complete sequence of definitions, consequences, and one elimination together with the tables can be found in the Appendix. We just point to two events in this enumeration: after the 9th definition (of coset number 10) it is found that coset numbers 9 and 8 define the same coset, the number 9 is eliminated then. Rather than renumbering, we leave this gap and continue with the definition of coset number 11.

After the definition of coset number 13 all tables are filled without any further "coincidence" of coset numbers pending. No definitions satisfying the original restriction are possible.

It can be shown from a more general discussion of the procedure (see e. g. [Neu 82]) that whenever this happens, the columns of the coset table give the permutations that multiplication from the right with the generators induces on the cosets of $U$. This assignment of permutations to the generators of the finitely presented group $G$ defines the permutation representation $\varphi_U$. Its kernel is

$$ker\ \varphi_U = \{\ g\ \mid\ g \in G,\ Uh = Uhg,\ \forall h \in G\ \} = \bigcap_{h \in G} h^{-1}Uh,$$

hence in particular $ker\ \varphi_U \leq U$. By the homomorphism theorem $\varphi_U(G) \cong G/ker\ \varphi_U$ and for the indices $G : U = \varphi_U(G) : \varphi_U(U)$, and

$$|\varphi_U(G)| = G : ker\ \varphi_U = (G : U) \cdot |\varphi_U(U)|.$$

In our case of Cavicchioli's group $C_1$, the permutations obtained for the generators are

$a \mapsto A = (2\ 4\ 3\ 7\ 6)(5\ 8\ 11\ 13\ 10)$
$b \mapsto B = (1\ 2\ 5\ 8\ 3)(6\ 10\ 12\ 11\ 7)$

(remember we have permutations on $1, \ldots, 13$, omitting 9).

Since $C_1 : \langle a \rangle = 12$ and $|\langle A \rangle| = 5$, we have

$$C_1 : ker\ \varphi_U = 12 \cdot 5 = 60 = |\langle A, B \rangle|.$$

Of course, if we would enumerate the cosets of the unit group, we might get the order of $C_1$, but as we shall see later, this would require much more space. Rather, in section 6 we can determine the order of $C_1$ by a variation of the presently used enumeration. Before this, in the next two sections, we turn to $C_2$. We remark in conclusion of this section that analysing the Todd-Coxeter procedure further, N. Mendelsohn has shown that it has indeed the claimed property of a verification method(see e.g. [Neu82]).

## 4. $C_2$ and the "low index" method

If we start to investigate

$$C_2\ =\ \langle\ a, b \mid aba^{-2}bab^{-1}\ =\ 1,\ a(b^{-1}a^3b^{-1}a^{-3})^2\ =\ 1\ \rangle$$

by trying again to enumerate the cosets of $\langle a \rangle$, this time even by computer, we experience disappointment: after having defined several hundred thousand coset numbers, the computer runs out of space, the method has not come to an end and so no conclusion about $C_2$ has been reached.

Of course, just taking further chances by trying other sets of words as subgroup generators would not be very satisfactory. Instead, one would prefer a method that would systematically search for <u>all</u> subgroups up to a given small upper bound for the index, $k$ say.

Such a method, using the idea of a coset table has been proposed by C. Sims. Let us describe it again generally for a finitely presented group

$$G = \langle\, g_1, \ldots, g_n \mid r_1(g_i) = 1, \ \ldots, \ r_m(g_i) = 1 \,\rangle.$$

It starts a Todd-Coxeter enumeration without using any subgroup generators; if this enumeration has produced more than $k$ coset numbers, then clearly, if this was the enumeration of the cosets of a subgroup $U$ of index $\leq k$, some of these coset numbers must represent the same coset. Saying that coset numbers $x$ and $y$, representing cosets defined in the process recursively by representatives $t_x(g_i)$ and $t_y(g_i)$ do in fact define the same coset, amounts to saying that $t_x(g_i)t_y(g_i)^{-1} \in U$. So forcing "coincidence" of the cosets with numbers $x$ and $y$ and eliminating one of them from the coset table is tantamount to restricting the enumeration to subgroups containing $t_x(g_i)t_y(g_i)^{-1}$. In Sims' algorithm such "forced coincidences" are studied in some lexicographical order, making sure by a backtrack search that each subgroup of index $\leq k$ is found exactly once. A further refinement gives just one representative from each conjugacy class of subgroups. (For details see again [Neu 82]).

For each class, the number of subgroups in the class is given and for one representative subgroup $U$ of each class a set of generators of $U$ as words in the generators of $G$ as well as the coset table of $U$. The coset table of course provides us with the images $\varphi_U(g_1), \ldots, \varphi_U(g_n)$ of the generators $g_1, \ldots, g_n$ of $G$ under the permutation representation $\varphi_U$ of $G$ on the cosets of $U$.

Applied by computer to $C_2$ with index bound 15 the method yields:

10 classes of subgroups of index 11,
8 classes of subgroups of index 12,
6 classes of subgroups of index 13.

## 5. The Schreier-Sims algorithm for permutation groups

The information we have obtained about the group $C_2$ may not seem to be very strong. However, as we have seen at the end of section 3, because of

$$G/ker\ \varphi_U \cong \varphi_U(G)$$

we can obtain such factor groups from the (permutation) images of the generators of $G$ that are provided by the "low index" method. In the case of $C_1$ it was easy to obtain the order of $\varphi_U(G)$ since $\varphi_U(U)$ was cyclic; in general we have to generate the permutation group $\varphi_U(G)$ from its generators. A very powerful method for this task is due to C. Sims, we now present the basic idea of this so-called Schreier-Sims method; the reader interested in technical details and practical organization of the method (that are in fact crucial for any efficient implementation) is referred to [Leo 80a,b].

Let $H$ be a group of permutations of the set $\Omega = \{1, 2, \ldots, z\}$. We define the "stabilizer chain"

$$H^0 := H,\ \ H^i := \ Stab_{H^{i-1}}(i) \ = \ \{\ h \ \mid \ h \in H^{i-1},\ h : i \mapsto i\ \}.$$

Then $H = H^0 \geq H^1 \geq \ldots \geq H^{z-1} = \langle 1 \rangle$. We shall first make use of the natural $1-1$ correspondence between the cosets of $H^i$ in $H^{i-1}$ and the points in the orbit $i^{H^{i-1}} = \{\ j \in \Omega \ \mid \ \exists\ h \in H^{i-1}$ with $h : i \mapsto j\ \}$ of the point $i$ under the action of $H^{i-1}$.

Starting with $H$ we can obtain the orbit of 1 under the action of $H$ by applying in turn the generators of $H$ to 1 and then to the images of 1 until no further image is found. Listing alongside with each point in the orbit the generator that produced it as image of an already known one, we obtain simultaneously coset representatives of the cosets as products of such generators.

Let us demonstrate the Schreier-Sims method using the output provided by the "low index" method for a particular subgroup, say $S$, of index 12 in $C_2$. This output tells us that the generators $a$ and $b$ of $C_2$ are represented by

$$\begin{aligned} \varphi_S(a) &= A = (2\ 4\ 8\ 11\ 12\ 10\ 9\ 5\ 3\ 7\ 6) \\ \varphi_S(b) &= B = (1\ 2\ 5\ 4\ 3)(6\ 10\ 12\ 11\ 7) \end{aligned}$$

and that the subgroup $S$ is generated by $a^{-1}$, $b^2ab$, $bab^2$, and $b^{-1}a^3b^{-1}$.

Since we know that $C_2 : S = \langle A, B\rangle : \varphi_S(S) = 12$, it suffices to find the order of $S^* := \varphi_S(S)$ which is generated by

$$\varphi_S(a^{-1}) = A^{-1}, \ldots, \ \varphi_S(b^{-1}a^3b^{-1}) = B^{-1}A^3B^{-1}.$$

We therefore compute these products of permutations:

$$\begin{array}{lll} A^{-1} & = & (2\ 6\ 7\ 3\ 5\ 9\ 10\ 12\ 11\ 8\ 4) \\ B^2AB & = & (2\ 8\ 7\ 9\ 4)(5\ 6\ 12\ 10\ 11) \\ BAB^2 & = & (3\ 5\ 8\ 6\ 9)(4\ 10\ 11\ 12\ 7) \\ B^{-1}A^3B^{-1} & = & (2\ 3\ 10\ 8\ 6\ 5\ 12\ 4\ 7\ 9\ 11). \end{array}$$

We see that $B^{-1}A^3B^{-1} = A^{-3}$, hence $S^*$ is generated by $X := A^{-1}$, $Y := B^2AB$, and $Z := BAB^2$. From these we get the orbit of 2 (each first finding of a point in the orbit is underlined):

$$\begin{array}{llllllll} 2X = \underline{6} & 6X = \underline{7} & 8X = \underline{4} & 7X = \underline{3} & 12X = \underline{11} & 9X = 10 & 4X = 2 & 3X = \underline{5} \\ 2Y = \underline{8} & 6Y = \underline{12} & 8Y = 7 & 7Y = 9 & 12Y = \underline{10} & 9Y = 4 & 4Y = 2 & 3Y = 3 \\ 2Z = 2 & 6Z = \underline{9} & 8Z = 6 & 7Z = 4 & 12Z = 7 & 9Z = 3 & 4Z = 10 & 3Z = 5 \end{array}$$

At this stage of the computation we see that $S^*$ is transitive on the 11 points $2, \ldots, 12$ and from the computation we also have coset representatives $T_2, \ldots, T_{12}$ of $Stab_{S^*}(2)$ which we list parallel to the points in the orbit.

$$\begin{array}{rclclclclcl} 2 & = & 2id & & & \Rightarrow & T_2 & = & id & & \\ 3 & = & 7X & = & 2X^3 & \Rightarrow & T_3 & = & X^3 & = & (2\ 3\ 10\ 8\ 6\ 5\ 12\ 4\ 7\ 9\ 11) \\ 4 & = & 8X & = & 2YX & \Rightarrow & T_4 & = & YX & = & (2\ 4\ 6\ 11\ 9)(3\ 5\ 7\ 10\ 8) \\ 5 & = & 3X & = & 2X^4 & \Rightarrow & T_5 & = & X^4 & = & (2\ 5\ 11\ 6\ 9\ 8\ 7\ 10\ 4\ 3\ 12) \\ 6 & = & 2X & & & \Rightarrow & T_6 & = & X & = & (2\ 6\ 7\ 3\ 5\ 9\ 10\ 12\ 11\ 8\ 4) \\ 7 & = & 6X & = & 2X^2 & \Rightarrow & T_7 & = & X^2 & = & (2\ 7\ 5\ 10\ 11\ 4\ 6\ 3\ 9\ 12\ 8) \\ 8 & = & 2Y & & & \Rightarrow & T_8 & = & Y & = & (2\ 8\ 7\ 9\ 4)(5\ 6\ 12\ 10\ 11) \\ 9 & = & 6Z & = & 2XZ & \Rightarrow & T_9 & = & XZ & = & (2\ 9\ 11\ 6\ 4)(3\ 8\ 10\ 7\ 5) \\ 10 & = & 12Y & = & 2XY^2 & \Rightarrow & T_{10} & = & XY^2 & = & (2\ 10\ 11\ 9\ 5)(3\ 12\ 6\ 4\ 7) \\ 11 & = & 12X & = & 2XYX & \Rightarrow & T_{11} & = & XYX & = & (2\ 11\ 3\ 7\ 5)(6\ 10\ 12\ 9\ 8) \\ 12 & = & 6Y & = & 2XY & \Rightarrow & T_{12} & = & XY & = & (2\ 12\ 5\ 4\ 8)(3\ 6\ 9\ 11\ 7) \end{array}$$

Having thus found coset representatives of $Stab_{S^*}(2)$ in $S^*$, we can now invoke a classical theorem of O. Schreier:

**Theorem:** Let the group $G$ be generated by $E := \{g_1, \ldots, g_n\}$, let $U$ be a subgroup of $G$, and $T = \{t_1, \ldots, t_x\}$ be a set of coset representatives (a "transversal") of $U$ in $G$. Then $U$ is generated by the set of "Schreier generators"

$$\{s_{t,g} \mid s_{t,g} = tg\overline{tg}^{-1},\ t \in T,\ g \in E\}$$

where $\overline{tg}$ denotes the coset representative from $T$ of the coset containing the product $tg$.

In our example, we can obviously now compute these Schreier generators, e. g. for the first generator $X$, we get the following list:

$$\begin{array}{llll}
S_{2,X} & = T_2X\overline{T_2X}^{-1} & = T_2XT_6^{-1} & = id \\
S_{3,X} & = T_3X\overline{T_3X}^{-1} & = T_3XT_5^{-1} & = id \\
S_{4,X} & = T_4X\overline{T_4X}^{-1} & = T_4XT_2^{-1} & = (3\ 9\ 6\ 8\ 5)(4\ 7\ 12\ 11\ 10) \\
S_{5,X} & = T_5X\overline{T_5X}^{-1} & = T_5XT_9^{-1} & = (3\ 9\ 6\ 8\ 5)(4\ 7\ 12\ 11\ 10) \\
S_{6,X} & = T_6X\overline{T_6X}^{-1} & = T_6XT_7^{-1} & = id \\
S_{7,X} & = T_7X\overline{T_7X}^{-1} & = T_7XT_3^{-1} & = id \\
S_{8,X} & = T_8X\overline{T_8X}^{-1} & = T_8XT_4^{-1} & = id \\
S_{9,X} & = T_9X\overline{T_9X}^{-1} & = T_9XT_{10}^{-1} & = (3\ 6\ 5\ 9\ 8)(4\ 12\ 10\ 7\ 11) \\
S_{10,X} & = T_{10}X\overline{T_{10}X}^{-1} & = T_{10}XT_{12}^{-1} & = (3\ 9\ 6\ 8\ 5)(4\ 7\ 12\ 11\ 10) \\
S_{11,X} & = T_{11}X\overline{T_{11}X}^{-1} & = T_{11}XT_8^{-1} & = id \\
S_{12,X} & = T_{12}X\overline{T_{12}X}^{-1} & = T_{12}XT_{11}^{-1} & = id
\end{array}$$

We see that all the Schreier generators $S_{i,X}$ are powers of the element $(3\ 9\ 6\ 8\ 5)(4\ 7\ 12\ 11\ 10)$ and by just doing permutation multiplications the reader can verify that the remaining Schreier generators $S_{i,Y}$ and $S_{i,Z}$ are also powers of this element. Hence the group $Stab_{S^*}(2)$ is cyclic of order 5 and we have $|S^*| = 11 \cdot 5 = 55$ and $|\langle A, B\rangle| = 12 \cdot 55 = 660$. Moreover $\langle A, B\rangle$ is twofold transitive, and because of this property and its order $\langle A, B\rangle$ must be isomorphic to $PSL(2, 11)$.

In our example things were made easy by the fact that $Stab_{S^*}(2)$ turned out to be cyclic. This need not be so easy in general. Indeed the growth of the number of Schreier generators from step to step poses a problem. This is solved - again only stating the basic idea - by the following observation: let at some stage a Schreier generator $s$ be obtained that fixes points $1, \ldots, i-1$, that is: $s \in H^{i-1}$, and let $s$ map $i$ to $j \neq i$, then $s$ is contained in the coset of $H^i$ in $H^{i-1}$ that is characterized by this property. If we have already listed a coset representative $r$ of this coset (obtained, e.g., previously as a Schreier generator) then instead of keeping $s$, we may keep $sr^{-1}$, because $s$ and $r$ generate the same subgroup as $sr^{-1}$ and $r$. However, $sr^{-1}$ will also fix

$i$, hence will be contained in a subgroup "further down" the stabilizer chain. From this remark we see that we will never have to keep more generators for any subgroup than the maximal number of possible cosets in all the steps of the stabilizer chain, i.e. no more than $z + (z-1) + \ldots + 1 = z(z+1)/2$. Practical implementations again improve greatly on this.

Let us now see, what an implementation of the Schreier-Sims method tells us about Cavicchioli's group $C_2$. As explained in section 4, we have the permutations $\varphi_U(a)$ and $\varphi_U(b)$ for a representative subgroup $U$ of each of the 24 classes of conjugate subgroups of $C_2$ that were found by the low index method. The orders of the permutation groups

$$\langle\, \varphi_U(a),\ \varphi_U(b)\, \rangle \ \cong\ C_2/\cap_{g\in G}\ U^g$$

obtained by the Schreier-Sims algorithm are given in the second line of the following table:

| $C_2 : U$ | 11 | 12 | 12 | 11 | 12 | 13 |
|---|---|---|---|---|---|---|
| $C_2 : \cap_{g\in G}\ U^g$ | 660 | 660 | 95040 | 11! / 2 | 12! / 2 | 13! / 2 |
| No. of classes | 2 | 1 | 4 | 8 | 3 | 6 |
| No. of kernels | 1 | | 2 | 8 | 3 | 6 |

Since $C_2$ was equal to its commutator group, so are the factor groups $C_2/\cap_{g\in G}\ U^g$. Comparison with the known list of finite simple groups indeed shows that they are simple and that in a few cases the same normal subgroup of $C_2$ was found as intersection of different classes of conjugate subgroups of $C_2$, which explains the last line of the table. What remains are the following different factor groups. Once $PSL(2,11)$, twice the Mathieu group $M_{12}$, 8 times $A_{11}$, 3 times $A_{12}$, 6 times $A_{13}$.

Now, if $S_i = G/N_i,\ i = 1,\ldots,k$ are simple nonabelian factor groups of a group $G$ with $N_i \neq N_j$ for $i \neq j$, then $G/\bigcap_{i=1}^k N_i$ is isomorphic to the direct product $\times_{i=1}^k S_i$. So we can conclude that $C_2$ has a factor group isomorphic to

$$PSL(2,11) \times M_{12}^{\times 2} \times A_{11}^{\times 8} \times A_{12}^{\times 3} \times A_{13}^{\times 6} \ \text{ of order } \sim 1.9 \cdot 10^{153},$$

a result surely not expected at first sight from the meager looking list of subgroups obtained at the end of section 4.

We close this section by remarking that C. Sims has used refinements of this approach to construct several of the sporadic simple groups as permutation groups. His most spectacular achievement in this field was the construction of the "Baby-Monster" as a permutation group of degree 13571955000, which of course involved much more theory and very special programming.

## 6. Reidemeister's theorem, a modified Todd-Coxeter method, and more about $C_1$ and $C_2$

In the preceding section we have exhibited factor groups of $C_1$ and $C_2$ that suggest that $C_1$ may be finite and $C_2$ perhaps not. To show this, we return to Schreier's theorem which gave us generators for a subgroup $U$ from those of the whole group $G$ and coset representatives of $U$ in $G$. Since in our application we worked with permutations, this was sufficient. However, if we work with abstract generators, in order to proceed similarly, a defining set of relators for the Schreier generators is needed. This is provided by Reidemeister's theorem:

**Theorem.** Let the group $G$ have the finite presentation

$$G = \langle\, g_1, \ldots, g_n \ \mid\ r_1(g_i) = 1,\ \ldots,\ r_m(g_i) = 1 \,\rangle,$$

let $U \leq G$ and $T = \{t_1, \ldots, t_x\}$ be a transversal of $U$ in $G$, then $U$ has the following presentation with respect to the set $\{s_{t,g}\}$ of Schreier generators:

$$U = \langle\, s_{t_l, g_i} \mid\ \tau(t_l r_j t_l^{-1}) = 1,\ s_{t_l, g_i} = \tau(t_l g_i \overline{t_l g_i}^{-1}) \,\rangle$$

where $j = 1, \ldots, m;\ l = 1, \ldots, x;\ i = 1, \ldots, n$, and where $\tau$ is the "Reidemeister rewriting". This rewrites a product of the generators $g_i$ which lies in $U$ into a product of the Schreier generators of $U$ by the following rule: if

$$u = g_{i_1}^{\varepsilon_1} \cdots g_{i_r}^{\varepsilon_r} \in U \quad \text{with} \quad \varepsilon_j = \pm 1,$$

then

$$\tau(u) = s_{p_1, g_{i_1}}^{\varepsilon_1} \cdots s_{p_r, g_{i_r}}^{\varepsilon_r}$$

where

$$p_j = \overline{g_{i_1} \cdots g_{i_{j-1}}} \quad \text{if} \quad \varepsilon_j = 1$$

and

$$p_j = \overline{g_{i_1} \cdots g_{i_j}} \quad \text{if} \quad \varepsilon_j = -1.$$

The correctness of this rewriting is easily seen by just inserting the definition of Schreier generators into the claimed result; for the proof of the theorem the reader is referred to [Joh 80]. For our purpose it is essential to note that Reidemeister rewriting of such a word can be performed, if there is a coset table for the cosets with representatives $t_l$: Since

$$\overline{g_{i_1} \cdots g_{i_j}} = \overline{\overline{g_{i_1} \cdots g_{i_{j-1}}} g_{i_j}},$$

the needed representatives of such products can be looked up recursively in the coset table: if $\overline{g_{i_1} \cdots g_{i_{j-1}}}$ is the representative of a coset with number $c$, then the number of the coset with representative $\overline{g_{i_1} \cdots g_{i_j}}$ is found in the column belonging to the generator $g_{i_j}$ in row number $c$.

Based on this observation, G. Havas has implemented a program which determines the Reidemeister presentation of a subgroup $U$ from its coset table in $G$. Of course the number of (Schreier-) generators and (Reidemeister-) relations thus obtained will be large (depending on the index of $U$) and so Havas' program is equipped with a heuristic program for the elimination of as many as possible of these generators.

Applying Havas' program to the subgroup $S$ of $C_2$ of index 12, used already in section 5, one ends up with the following presentation for the subgroup $S$ on four generators:

$$\begin{aligned} S = \langle\ t_1, t_2, t_3, t_4 \ \mid\ & t_1 t_2 t_1^{-1} t_2^{-1} = 1,\quad t_1^5 t_2^{-2} = 1,\quad t_1^2 t_3 t_1^{-2} t_4 t_3^{-1} t_1 t_4^{-1} = 1, \\ & t_1 t_2 t_4 t_1^{-1} t_3 t_4^{-1} t_2^{-1} t_1^{-1} t_3^{-1} = 1,\quad t_1^3 t_2 t_4 t_1^{-3} t_2^{-1} t_4^{-1} = 1\ \rangle. \end{aligned}$$

If we abelianize, the first and the last relation become trivial and we get the following relation matrix for the commutator factor group $S/S'$ of $S$:

$$\begin{array}{c} \begin{array}{cccc} \bar t_1 & \bar t_2 & \bar t_3 & \bar t_4 \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & 0 \\ 5 & -2 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \end{array}$$

The elementary divisor algorithm transforms this

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 5 & -2 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 5 & -2 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

hence we see that $S/S'$ is isomorphic to a direct product of a cyclic group of order 2 with two infinite cyclic groups: $S/S' \cong \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z} \oplus \mathbf{Z}$, hence is infinite and hence also $C_2$ is an infinite group.

We might use the same program on $C_1$ and its subgroup $\langle a \rangle$ of index 12. Prima facie the number of Schreier generators of the subgroup would be 24. Although, using a special version of Reidemeister's theorem, this reduces to 13, this is rather inadequate since we know that $\langle a \rangle$ is cyclic! It is therefore desirable to have an algorithm that will give a presentation for a subgroup with respect to given generators. In fact a modification of the Todd-Coxeter method will do this. Considering the numbers $1, 2, \ldots$ introduced in it not as denoting cosets but as denoting coset representatives with the neutral element as representative of $U$ we see that the closing of the first subgroup table for a subgroup generator $h = h(g_i) = g_{i_1} \ldots g_{i_x} \ldots g_{i_r}$ only yields a consequence of the form $kg_{i_x} = hl$ instead of $kg_{i_x} = l$ for coset numbers $k$ and $l$:

$$\begin{array}{c|c|c|c} & g_{i_1} \quad \cdots & g_{i_x} \quad \cdots & g_{i_r} \\ \hline 1 & \ldots \quad k & hl \quad \ldots & h1 \end{array}$$

Introducing this form of consequences of the closing of a subgroup table into the coset table, further subgroup tables and the relation tables, we see that their entries will also get modified by products of the given subgroup generators. Now in considering the three possible cases that could occur when one has to enter a consequence into the coset table (see section 3) we see that in case (ii) we may have the same coset number but different words $w_1$ and $w_2$ in the subgroup generators from the new consequence and from the coset table. In such a case $w_1(h_j)l = w_2(h_j)l$, and we conclude that $w_1(h_j)w_2(h_j)^{-1} = 1$ is a relation holding for the given subgroup generators. It can be proved (see e.g. [Neu 82] and papers quoted there) that the set of all relations thus arising is a defining set of relations for $U$ with respect to the given generators. The computation is done for $C_1$ in the appendix and the 13th and 14th consequences yield that $h^{10} = 1$, i.e. the subgroup $\langle a \rangle$ of $C_1$ is of order 10. Since the index $C_1 : \langle a \rangle = 12$, the group $C_1$ has order 120 and can then easily be identified as being isomorphic to $SL(2,5)$. It should be mentioned that the implementation of the modified Todd-Coxeter method needs further thoughts in order to keep control of the growing length of the words in the subgroup generators in the case that there are more than one of them (cf [ARo 84]).

## 7. Using $\mathbf{SL(2,.)}$ representations

The study of the complex matrix representations of a group is an essential approach in the theory of finite groups. Here problems on representations translate efficiently into problems about traces of matrices and enter the domain of the theory of characters.

Given a finitely presented group

$$G \; = \; \langle \; g_1, \ldots, g_n \mid r_1(g_s), \ldots, r_m(g_s) \; \rangle,$$

a representation $\phi : G \; \to \; SL(d, \mathbf{F})$ is determined by

$$\phi(g_s) \; = \; X_s \; = \; (x_{ij}^{(s)}) \quad (1 \; \leq \; s \; \leq \; n),$$

where the entries are solutions of the set of polynominal equations in many variables

$$det(X_s) \; = \; 1, \quad r_i(X_s) \; = \; 0, \quad (1 \leq s \leq n, \quad 1 \leq i \leq m),$$

for some dimension $d$, and some field $\mathbf{F}$.

W. Magnus advocates in [Mag 81] the use of representations into $SL(2, \mathbf{C})$ as a tool in combinatorial group theory and expounds on known methods and results, especially on some trace formulas which however do not attain the stature of a general character theory.

We present below some examples where the straightforward study of representations produces definite results for the groups in question.

We define three classes of groups, the second factor groups of the first, and, as shown in (3) below, the third factor groups of the second, which lead to the Cavicchioli groups. For $i, j, k, l, q$ nonzero integers let

$$\begin{array}{lcl} G(i,j,k) & = & \langle \; a, b \mid a^i b a^j b a^k b^{-1} \; \rangle, \\ G(i,j,k,l) & = & \langle \; a, b \mid a^i b a^j b a^k b^{-1}, \;\; [a, b a^l b] \; \rangle, \\ G(i,j,k,l,q) & = & \langle \; a, b \mid a^i b a^j b a^k b^{-1}, \;\; a(b^{-1} a^{-l} b^{-1} a^l)^q \; \rangle. \end{array}$$

Then, clearly, $\;C_q \; = \; G(1, -2, 1, -3, q)$.

**(1)** Suppose $\mathbf{F}$ is a field and

$$\phi : G(i,j,k) \to SL(2,\mathbf{F})$$

is a representation such that in the image group

$$\phi(a) = A = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}, \quad \phi(b) = B = \begin{pmatrix} \beta_{11} & \beta_{12} \\ \beta_{21} & \beta_{22} \end{pmatrix}$$

where $\beta_{12}\beta_{21} \neq 0$. Then we can make $\beta_{21} = 1$ by conjugating the image group by

$$M = \begin{pmatrix} 1 & 0 \\ 0 & \beta_{21} \end{pmatrix}.$$

We should note that in general $\phi(a)$ has one of the Jordan canonical forms

$$\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}, \begin{pmatrix} \pm 1 & 0 \\ 1 & \pm 1 \end{pmatrix}$$

in some extension of $\mathbf{F}$. Our choice of the first form was done to facilitate the calculations.

The following computations are direct:

$$A^iB = \begin{pmatrix} \alpha^i\beta_{11} & \alpha^i\beta_{12} \\ \alpha^{-i} & \alpha^{-i}\beta_{22} \end{pmatrix}, \; BA^{-k} = \begin{pmatrix} \beta_{11}\alpha^{-k} & \beta_{12}\alpha^{k} \\ \alpha^{-k} & \beta_{22}\alpha^{k} \end{pmatrix},$$

$$A^iBA^jB = \begin{pmatrix} \alpha^{i+j}\beta_{11}^2 + \alpha^{i-j}\beta_{12} & \alpha^{i+j}\beta_{11}\beta_{12} + \alpha^{i-j}\beta_{12}\beta_{22} \\ \alpha^{-i+j}\beta_{11} + \alpha^{-i-j}\beta_{22} & \alpha^{-i+j}\beta_{12} + \alpha^{-i-j}\beta_{22}^2 \end{pmatrix}.$$

The relation

$$A^iBA^jB = BA^{-k}$$

is equivalent to the equations:

$$\begin{array}{llcl}
(11) & \alpha^{i+j}\beta_{11}^2 + \alpha^{i-j}\beta_{12} & = & \beta_{11}\alpha^{-k} \\
(12) & \alpha^{i+j}\beta_{11}\beta_{12} + \alpha^{i-j}\beta_{12}\beta_{22} & = & \beta_{12}\alpha^{k} \\
(21) & \alpha^{-i+j}\beta_{11} + \alpha^{-i-j}\beta_{22} & = & \alpha^{-k} \\
(22) & \alpha^{-i+j}\beta_{12} + \alpha^{-i-j}\beta_{22}^2 & = & \beta_{22}\alpha^{k}
\end{array}$$

From (12), as $\beta_{12} \neq 0$, we have

$$(12)' \qquad \alpha^{i+j}\beta_{11} + \alpha^{i-j}\beta_{22} = \alpha^k$$

which together with (21) give,

$$(21)' \qquad \alpha^{2(i-k)} \;=\; 1.$$

Now

$$\begin{array}{lrcl} (11)' & \beta_{12} & = & \alpha^{-i+j-k}\beta_{11} - \alpha^{2j}\beta_{11}^2 \\ (12)'' & \beta_{22} & = & \alpha^{-i+j+k} - \alpha^{2j}\beta_{11} \end{array} \quad ,$$

which when substituted in (22) give

$$\alpha^{-i+j}(\alpha^{-i+j-k}\beta_{11}-\alpha^{2j}\beta_{11}^2)+\alpha^{-i-j}(\alpha^{-i+j+k}-\alpha^{2j}\beta_{11})^2 \;=\; (\alpha^{-i+j+k}-\alpha^{2j}\beta_{11})\alpha^k,$$

and this in turn leads to

$$\alpha^{j+k}(\alpha^{-4k} - 2\alpha^{-2k} + \alpha^{2i-2k})\beta_{11} \;=\; \alpha^i - \alpha^{-i}.$$

Since $\alpha^{2i} = \alpha^{2k}$, we get

$$\alpha^{j+k}(\alpha^{-2i} - 1)^2\beta_{11} \;=\; \alpha^i(1 - \alpha^{-2i});$$

thus, again using $\alpha^{2i} = \alpha^{2k}$,

$$(22)' \qquad \alpha^{2i} \;=\; 1 \quad \text{or} \quad \beta_{11} \;=\; \frac{\alpha^{i-j+k}}{\alpha^{2i}-1}$$

Using $(12)''$, $(11)'$ in the determinant equation $\beta_{11}\beta_{22} - \beta_{12} = 1$ gives the same result as $(22)'$.

Let us suppose $\alpha^{2i} \neq 1$. Then, from $(11)'$ we get

$$(11)'' \qquad \beta_{12} = -\frac{\alpha^{4i} - \alpha^{2i} + 1}{(\alpha^{2i}-1)^2} \quad ,$$

and from $(12)''$ we get

$$(12)''' \qquad \beta_{22} = -\frac{\alpha^{-i+j+k}}{\alpha^{2i}-1} \quad ;$$

observe that $\beta_{22} = -\alpha^{-2i+2j}\beta_{11}$.

Hence, we have: For any possible choice $\alpha \in \mathbf{F}$ such that

$$\alpha^{2(i-k)} = 1 \neq \alpha^{2i}$$

the map

$$\phi(a) = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}, \quad \phi(b) = \begin{pmatrix} \dfrac{\alpha^{i-j+k}}{\alpha^{2i}-1} & -\dfrac{\alpha^{4i}-\alpha^{2i}+1}{(\alpha^{2i}-1)^2} \\ 1 & -\dfrac{\alpha^{-i+j+k}}{\alpha^{2i}-1} \end{pmatrix}$$

extends to a representation of $G(i,j,k)$ into $SL(2,\mathbf{F})$.

Let $C = A^j B$. Then, $det(C) = 1$, and

$$trace(C) = \frac{\alpha^{i+k} - \alpha^{-i+k}}{\alpha^{2i}-1} = \alpha^{-i+k} = \pm 1.$$

Therefore, the characteristic polynomial for $C$ is

$$x^2 - trace(C)x + det\, C = x^2 \mp x + 1, \quad (\text{a factor of } x^3 \pm 1).$$

By the Cayley-Hamilton theorem, $C$ satisfies its characteristic equation; so, $C^3 = \mp I$, and hence the order of $C$ is 6 or 3.

**(2)** We propose to obtain a representation

$$\bar{\phi} : G(i,j,k,l) \rightarrow SL(2,\mathbf{F})$$

from $\phi$ of the previous section. For such a purpose, $A$ should commute with $BA^lB$. Now, as $A$ is a diagonal noncentral matrix, $BA^lB$ is also a diagonal matrix. By direct calculation, we obtain $\alpha^{2(l+i-j)} = 1$. Therefore $\bar{\phi}$ is a representation for any choice of $\alpha$ such that

$$\alpha^{2i} \neq 1 = \alpha^{2(i-k)} = \alpha^{2(l+i-j)}.$$

Using this as well as $\alpha^{2k} = \alpha^{2i}$, we obtain

$$BA^lB = \begin{pmatrix} -\alpha^{-l} & 0 \\ 0 & -\alpha^l \end{pmatrix} = -A^{-l}, \text{ hence } (A^lB)^2 = -I.$$

**(3)** Let $G := G(i,j,k,l,q)$. Then, the last relation $(b^{-1}a^{-l}b^{-1}a^l)^q = a^{-1}$ implies that $a$ commutes with $b^{-1}a^{-l}b^{-1}$ since by it $a$ is a power of $b^{-1}a^{-l}b^{-1}a^l$, and this shows that $G$ is a factor group of $G(i,j,k,l)$. By substituting $A, B$ in this last relation of $G$, we conclude that $\bar{\phi}$ induces a representation $\bar{\bar{\phi}} : G \to SL(2,\mathbf{F})$ if and only if, in addition to the previous conditions on $\alpha$,

$$\alpha^{2ql+1} = (-1)^q.$$

Thus, we have accumulated the following torsion relations:

$$A^{2ql+1} = (-1)^q I, \ (A^j B)^3 = \pm I, \ \text{and} \ (A^l B)^2 = -I,$$

which constitute a strong set of relations. It is well-known for instance that

$$\langle\, x, y \mid x^5, y^3, (xy)^2 \,\rangle \ \text{ is a presentation for } A_5,$$

and easily then, the image of $C_1$ by $\bar{\bar{\phi}}$ is isomorphic to $PSL(2,5)$ or $SL(2,5)$.

**(4)** To illustrate a line of development in the study of $\bar{\bar{G}} := \bar{\bar{\phi}}(G)$, we restrict our considerations to finite fields $\mathbf{F}$, and come to the conclusion that if $3|ql$ and $|2ql+1| > 5$, then $\bar{\bar{G}}$ has an infinite number of non-isomorphic quotient groups of type $PSL(2,p^s)$ and hence that $\bar{\bar{G}}$ is an infinite group. Since $C_q = G(1,-2,1,-3,q)$, the above holds for $C_q$, provided $q > 1$.

In order to reach such a deep understanding it is not surprising that we have to appeal to the classification of the subgroup structure of $PSL(2,p^s)$ by L.E. Dickson (cf [Hup 67], vol. 1, p. 213), which states in part, that the nonsolvable subgroups of $PSL(2,p^s)$ are isomorphic to $PSL(2,p^{s'})$ where $s'|s$, to $PGL(2,p^{s'})$ where $2s'|s$, or to $A_5$ if $p = 5$ or $p^s \equiv \pm 1 \ (mod\ 10)$.

By requiring that $3|ql$, the orders of $A$, $A^j B$, and $A^l B$ become relatively prime in $SL(2,\mathbf{F})$ modulo the center $\langle -I \rangle$. Therefore by abelianization, we see that $\bar{\bar{G}}$ is a perfect group.

How do we choose finite fields $\mathbf{F}$ to fit our purpose?
Fix $(i,j,k,l,q)$ such that $ijklq \neq 0$, $3|ql$, and for $N = 2ql+1$,

$$i \not\equiv 0 \ (mod\ N), \ \ k \equiv i \ (mod\ N), \ \text{ and } \ j \equiv i + l \ (mod\ N).$$

For every prime $p$ not dividing $N$, let $m(p,N)$, abbreviated by $m$, be the minimal natural number such that $p^m \equiv 1 \ (mod\ N)$ and let $\mathbf{F}_p$ be the finite field $GF(p^m)$. Then, $\mathbf{F}_p$ contains an element $\alpha$ having the multiplicative order $|N|$.

For every such choice of $\mathbf{F}_p$, the image $\bar{\bar{G}}$ of

$$\bar{\bar{\phi}} : G(i,j,k,l,q) \to SL(2, \mathbf{F}_p)$$

is isomorphic to $SL(2, \mathbf{F}_p)$. By applying Dickson's theorem, we have for $|N| > 5$ that $G(i,j,k,l,q)$ has a factor group isomorphic to

$$\times_{\mathbf{P}} PSL(2, \mathbf{F}_p)$$

for any finite set $\mathbf{P}$ of primes $p \not| N$. This brings us to the end of the line, and in particular to the infiniteness of the Cavicchioli groups $C_q$ for $q > 1$.

## 8. Another example, the nilpotent quotient algorithm

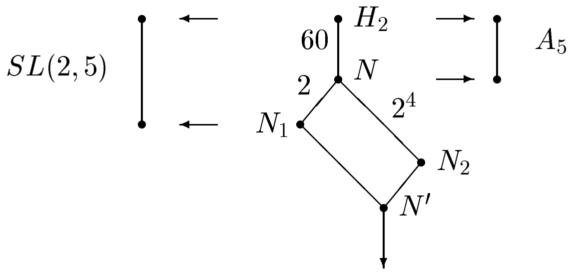
The mixture of different methods outlined in the example of Cavicchioli's groups has been applied successfully in the investigation of several presentations. We mention one of them which needed the invocation of a further very powerful algorithm.

H. Heineken (private communication) posed the problem to investigate the groups $H_1$ and $H_2$, defined by the presentations :

$$H_1 = \langle\, a, b, c \mid [a,b] = c,\ [b,c] = a,\ [c,a] = b \,\rangle,$$

$$H_2 = \langle\, a, b, c \mid [a,[a,b]] = c,\ [b,[b,c]] = a,\ [c,[c,a]] = b \,\rangle.$$

Both are obviously equal to their respective commutator groups. $H_1$ can be shown to be trivial by a Todd-Coxeter run (defining more than 100 coset numbers before this conclusion is reached). Attempts to get the order of $H_2$ via the Todd-Coxeter method failed. The "low index" method produces a class of subgroups of index 5, the Schreier-Sims algorithm shows that the factor group by their intersection $N$ is isomorphic to $A_5$. Reidemeister-Schreier produces a rather complicated presentation for $N$, abelianizing, one gets that $N/N'$ is isomorphic to a direct product of 5 copies of the cyclic group of order 2. So now we have a factor group $H_2/N'$ of order $60 \cdot 2^5$ of $H_2$. Further it can be shown that $N/N'$ under the action of $H_2$ is the direct product of a chief factor $N_2/N'$ of order 2 and a chief factor $N_1/N'$ of order $2^4$, and that $H_2/N_1$ is isomorphic to $SL(2,5)$. The method of $SL(2,\cdot)$ representations, applied to an extension of $H_2$ (using the formula manipulation system MAPLE [MAP85]) shows that this is in fact the only $SL(2,\cdot)$ factor group of $H_2$.




The hope to prove $H_2$ to be infinite by exhibiting a free abelian factor group of a subgroup of small index, however, has failed. We may ask then, if we can find other factor groups of $N$. If these are to be nilpotent, then by Burnside's basis theorem they must be groups of order a power of 2 which can be generated by 5 generators.

A method to find such is the nilpotent quotient algorithm of I.D. Macdonald [Mac 74]. This algorithm constructs inductively for a group $G$ given by a finite presentation

$$G = \langle\, g_1, \ldots, g_n \;\mid\; R\,\rangle$$

(where $R$ is a finite defining set of relations for $G$) and for a given prime $p$ the factor groups of the "descending p-central series" defined by

$$G_0 := G, \;\; G_i := [G_{i-1}, G]G_{i-1}^p.$$

(Here the relative commutator group $[U, V]$ of two subgroups $U$ and $V$ of $G$ is the normal closure of the set of all commutators $[u, v]$, $u \in U$, $v \in V$, and $U^p$ is the normal closure of the set of $p^{th}$ powers of the elements of $U$. If $G_k = \langle 1 \rangle$ but $G_{k-1} \neq \langle 1 \rangle$, we shall say that $G$ is of $p$-class $k$. For each factor group $G/G_i$ a special kind of presentation will be constructed that we first have to discuss.

Let $P$ be a $p$-group and

$$P_0 := P \; > \; P_1 \; > \ldots > \; P_r \; = \; \langle 1 \rangle$$

be a series of normal subgroups $P_i \lhd P$ such that $P_{i-1}/P_i$ is of order $p$ and contained in the centre of $G/P_i$, then this is called a $p$-step central series of $P$. Choosing for each $i = 1, \ldots, r$ an element $a_i$ such that $\langle P_i a_i \rangle \; = \; P_{i-1}/P_i$, we obtain a generating set $\{a_1, \ldots, a_r\}$ of $P$ for which defining relations of the form

$$a_i^p = a_{i+1}^{\nu_{i,i+1}} \cdots a_r^{\nu_{i,r}} \quad \text{for } i = 1, \ldots, r$$

(*)

$$[a_j, a_i] = a_{j+1}^{\nu_{j,i,i+1}} \cdots a_r^{\nu_{j,i,r}} \quad \text{for } j > i$$

can be found. Each element in $P$ can be written in the form

$$a_1^{\alpha_1} \cdots a_r^{\alpha_r} \quad \text{with } 0 \leq \alpha_i < p,$$

and multiplication of two elements in this form can be performed by "collecting" the product into such a form using the relations in a fashion similar to that explained in section 2 for the dihedral groups.

Now any set of relations of the form (*) clearly defines a $p$-group of order $\leq p^r$. That it need not be of order $p^r$ is seen by the example of the presentation

$$\langle\, a_1, a_2, a_3 \mid a_1^2 = a_2,\ a_2^2 = a_3,\ a_3^2 = 1,\ [a_2, a_1] = a_3,\ [a_3, a_1] = 1,\ [a_3, a_2] = 1 \rangle.$$

The group defined by it is not of order $2^3$ but of order $2^2$, and this is seen in a systematic way by evaluating $a_1^3$ in two ways:

$$a_1 a_2 = a_1 a_1^2 = a_1^3 = a_1^2 a_1 = a_2 a_1 = a_1 a_2 [a_2, a_1] = a_1 a_2 a_3,$$

and so $a_3 = 1$.

Calling a presentation (*) "consistent" if it defines a $p$-group of order $p^r$, one can prove that one can check consistency by analogous systematic two-way evaluation of a finite set of test words of the forms

$$a_i^{p+1},\ \ a_j a_i^p,\ \ a_j^p a_i, \text{ and } a_k a_j a_i \text{ with } \ k > j > i.$$

(See [New 76] for details).

Having defined these terms we can now state that the nilpotent quotient algorithm determines recursively a consistent presentation of form (*) for each factor group $G/G_i$ of the descending $p$-central series of $G$.

Consider again a finitely presented group

$$G = \langle\, g_1, \ldots, g_n \mid R \,\rangle.$$

$G/G_1$ is the largest elementary abelian $p$-factor group of $G$, so it can be obtained by performing the elementary divisor algorithm modulo $p$. This will yield a presentation

$$(1) \qquad G/G_1 = \langle\, a_1, \ldots, a_d \mid a_i^p = 1,\ [a_j, a_i] = 1 \,\rangle$$

where the $a_i$ may be chosen from the cosets $\bar{g}_i = G_1 g_i$ of the generators $g_i$ of $G$ in the given presentation. Note that by Burnside's basis theorem the minimal number of generators of any $p$-factor group $G$ will be at most $d$. $G/G_1$ also has a presentation

$$(2) \quad G/G_1 = \langle\, g_1, \ldots, g_n,\ a_1, \ldots, a_d \mid R,\ g_i = \prod a_k^{\nu_k},\ a_k^p = 1,\ [a_j, a_k] = 1 \,\rangle$$

in which for each $a_k$ there will be a relation $a_k = g_{i_k}$. These will be called the "definitions" of the $a_k$ and will not be changed in the sequel.

The computation of $G/G_2$ from $G/G_1$ (and quite analogously $G/G_i$ from $G/G_{i-1}$) is now done in three steps.

(i) For the first step we define a $p$-cover $C(H)$ of a $p$-group $H$ of $p$-class $b$ to be a $p$-group $K$ of $p$-class $b+1$ with $K/K_b \cong H$, which is maximal with this property. A presentation for the $p$-cover $C(G/G_1)$ is obtained from the presentation (1) of $G/G_1$ by modifying all relations in (1) that are not definitions into congruences modulo newly introduced central generators $a_k$ of order $p$.

(ii) The presentation of $C(G/G_1)$, so obtained, is of form (*) but need not be consistent. Evaluating the consistency testwords, we get a finite number of equations between the newly introduced generators. Since these are all central of order $p$, we thus have to solve a system of homogeneous linear equations over the field of $p$ elements in order to eliminate redundant generators and to get a consistent presentation of type (*) for $C(G/G_1)$.

(iii) In a third step, those relations in (2) that express the $g_i$ in terms of the $a_k$, and that are not tabooed as being definitions of the $a_k$, are also modified by new generators (made central and of order $p$). Then these expressions for the $g_i$ are used to eliminate the $g_i$, that is, to write the relations $R$ in terms of $a_k$'s. These are then collected and possibly lead to further homogeneous linear equations between the newly introduced generators and hence to further eliminations.

After the three steps, we now have a consistent presentation for $G/G_2$ of type (*) and can start the construction of $G/G_3$ and so on. This nilpotent quotient algorithm has had its most interesting applications to Burnside groups, it was used e.g. by M. F. Newman and G. Havas to show that the restricted Burnside group $\bar{B}(4,4)$, i.e. the largest nilpotent group on 4 generators, having exponent 4, has order $2^{422}$. See [HaN 80] for a report on these applications as well as for a good description of the method.

Applying this nilpotent quotient algorithm to the presentation of the normal subgroup $N$ of Heineken's group $H_2$, we obtain that $N$ has a maximal 2-factor group of order $2^{24}$, so altogether we have a factor group of order $60 \cdot 2^{24}$ of $H_2$. At this point we have reached the end of present day's exploration of $H_2$, several attempts to investigate presentations of other subgroups have not brought any further information, so we may very well be at the end of today's computational possibilities without having been able to settle the question if $H_2$ is in fact of order $60 \cdot 2^{24}$ or perhaps even infinite.

New methods, e.g. for finding soluble quotients have recently been proposed and are presently being implemented, may be they will allow us to tell more about this and other groups.

So this example may serve to show that the methods of computational group theory of course have their limits, but also that it is a field still very much in development and open for new ideas.

## 9. Implementations and computers[2]

All methods that have been mentioned in this article have been implemented, in most cases with many improvements and refinements too technical to be described here, as well as many other algorithms in computational group theory. The most comprehensive system of group theoretical programs is CAYLEY [Can 84]; it builds on the storage management system STACKHANDLER and has its own problem oriented language which can be used to write programs combining the algorithms implemented in the system. CAYLEY has originally been written in FORTRAN, nowadays a translation into C is available. More specialized systems are CAS [NPP 84] for the interactive work with characters, SOGOS [LNS 84] for working with soluble groups, and SPAS for the calculation with presentations, containing

[2]This section has been revised and updated by the first author on June, $7^{\text{th}}$, 1989.

i.a. Todd-Coxeter, Modified Todd-Coxeter, Reidemeister-Schreier and Low-Index methods. CAMAC is a system for the application of group theory in combinatorics and coding theory.

A new system, GAP, has recently been released which is designed in a different way. It has a small kernel, written in C that contains dynamic storage management, an interpreter of the GAP language, and basic operations. The GAP language is a PASCAL-like programming language with special datatypes such as permutations, finite field elements, vectors, and matrices. The programming language allows to write algorithms in their most general setting, e.g. the same piece of code could be used to compute the orbit of a point under a permutation group, of a vector under a matrix group, or the conjugacy class of an element in any kind of group. An interactive programming environment eases writing, debugging and improving programs. It allows, for example, to trace program execution, to inspect the situation in great detail after an error has occured, or to time the execution to identify the time critical parts. GAP comes with a library of group theoretical algorithms for computing with groups, e.g. for finding the centralizer of an element in a permutation group. All the algorithms are written in the GAP programming language, and thus can easily be modified by the user if necessary.

While CAYLEY is sold commercially for several thousand dollars, the other systems are distributed freely for refund of the cost of the material, i.e. the floppy or cartridge and the manual.

Contact addresses are:

| | |
|---|---|
| CAYLEY: | J. Cannon, Department of Pure Mathematics,<br>University of Sydney, Sydney, NSW 2006,<br>Australia. |
| CAS, SOGOS,<br>SPAS, GAP: | J. Neubüser, Lehrstuhl D für Mathematik, RWTH,<br>D5100 Aachen, West Germany. |
| CAMAC: | J. Leon, Department of Mathematics,<br>University of Illinois at Chicago,<br>Box 4348, Chicago, Ill. 60680, USA. |

In addition to these, there exist "stand-alone" implementations of single algorithms. In addition to the ones given above a good address (e.g. for Todd-Coxeter, nilpotent quotient etc.) is:

G. Havas: Key Center for Software Technology,
Department of Computer Science,
University of Queensland,
St. Lucia, Queensland 4067, Australia.

All these programs run very well on workstations having something like $\geq 40$ MByte accessible through virtual store management and a CPU equivalent to a Motorola 68020. UNIX is becoming the operating system of choice for many implementations, but there are e.g. VAX implementations under VMS for CAYLEY, CAS, SOGOS, SPAS, and GAP. Because of its structure GAP works on even smaller computers like MAC II and ATARI ST.

## 10. An epilogue

The methods of "computational group theory", of which only a few could be sketched in this paper, as well as those of "computer algebra" dealing with polynomial arithmetic and integration of functions and differential equations in closed form have become powerful tools in research. Therefore they should also find their place in teaching mathematics. This does not necessarily mean the introduction of new courses, the discussion of such methods can be integrated into the existing ones, enriching them with algorithmic aspects. Moreover, at the graduate level, students can learn to both implement and use such methods in the context of their masters theses.

In Brazil, universities will soon face the problem that they will have to train a majority of their MSc students for later work in industry, as is already the case in highly industrialized countries. If pure mathematics is to play its rôle in this, such a combination of acquiring the abilities of logical analysis and reasoning that the training as a mathematician has always given with the skills of the use of the computer for their application, will be ideal for this aim.

## 11. Appendix

The appendix contains the calculation of the modified coset table for the group $C_1$ with subgroup $U = \langle a \rangle$.

Definitions, consequences, the elimination of coset number 9 and the finding of the relations for the subgroup generator are listed in a protocole in the order in which they occur. Definitions and consequences are numbered separately by $D1, \dots$, and $C1, \dots$, respectively.

In the relation tables, places that yield consequences are underlined. Each new consequence is marked with its number in the protocole, which is put at the end below the underlining. Duplications of already known consequences are underlined by dashed lines. The conseqences yielding the defining relator for the subgroup generator are underlined with dotted lines.

In the coset table, definitions are underlined, entries that are consequences are marked with the number of the respective consequence in the protocole.

Before the coset number 9 is eliminated, it occurs in several places in the relation tables. There it is crossed out and its replacement is put next to it.

If all entries are stripped of the powers of $h$, the original Todd-Coxeter procedure is regained.

$$C_1 = \langle\, a, b \mid a^{-2}bab^{-1}ab = 1,\ a^3b^{-1}a^{-2}b^{-1} = 1 \,\rangle, \quad U = \langle a \rangle, \quad h := a$$

**Subgroup table**

| | $a$ |
|---|---|
| 1 | $h1$ |

**First relation table**

| | $a^{-1}$ | $a^{-1}$ | $b$ | $a$ | $b^{-1}$ | $a$ | $b$ |
|---|---|---|---|---|---|---|---|
| **1** | $h^{-1}\mathbf{1}$ | $h^{-2}\mathbf{1}$ | $h^{-2}\mathbf{2}$ | $h^{-2}\mathbf{4}$ | $h^{-3}\mathbf{4}$ | **3** | **1** |
| **2** | **6** | $h^{-2}\mathbf{7}$ | $h^{-1}\mathbf{6}$ | $h^{-1}\mathbf{2}$ | [2] $h^{-1}\mathbf{1}$ | **1** | **2** |
| **3** | $h^{-3}\mathbf{4}$ | $h^{-3}\mathbf{2}$ | [4] $h^{-3}\mathbf{5}$ | $\cancel{h^{-3}}\ \cancel{\mathbf{9}}\ h\mathbf{8}$ | $h^{-4}\mathbf{5}$ | **8** | **3** |
| **4** | **2** | **6** | $h^{-1}\mathbf{10}$ | $h^{-1}\mathbf{5}$ | [7] $h^{-1}\mathbf{2}$ | $h^{-1}\mathbf{4}$ | **4** |
| **5** | **10** | **13** | [5] $h^{-1}\mathbf{13}$ | $h^{-1}\mathbf{10}$ | **6** | **2** | **5** |
| **6** | $h^{-2}\mathbf{7}$ | $h^{-2}\mathbf{3}$ | [11] $h^{-2}\mathbf{1}$ | $h^{-1}\mathbf{1}$ | $h^{-1}\mathbf{3}$ | $h^{-1}\mathbf{7}$ | **6** |
| **7** | **3** | $h^{-3}\mathbf{4}$ | $h^{-2}\mathbf{4}$ | $h\mathbf{3}$ | $h\mathbf{8}$ | **11** | **7** |
| **8** | $h^{-4}\mathbf{5}$ | $h^{-4}\mathbf{10}$ | $h^{-4}\mathbf{12}$ | $h^{-5}\mathbf{12}$ | $h^{-5}\mathbf{10}$ | [8] $h^{-5}\mathbf{5}$ | **8** |
| $\cancel{\mathbf{9}}$ | $\cancel{\mathbf{5}}$ | $\cancel{\mathbf{10}}$ | | [9] | | | $\cancel{\mathbf{9}}$ |
| **10** | **13** | $h^{-2}\mathbf{11}$ | $h^{-2}\mathbf{7}$ | **6** | $h^{-1}\mathbf{7}$ | $h\mathbf{6}$ | **10** |
| **11** | $h\mathbf{8}$ | [12] $h^{-3}\mathbf{5}$ | $h^{2}\mathbf{8}$ | $h\mathbf{11}$ | $h^{-4}\mathbf{12}$ | $h^{-5}\mathbf{12}$ | **11** |
| **12** | $h\mathbf{12}$ | $h^{2}\mathbf{12}$ | $h^{7}\mathbf{11}$ | $h^{9}\mathbf{13}$ | $h^{10}\mathbf{13}$ | **10** | **12** |
| **13** | $h^{-2}\mathbf{11}$ | $h^{-1}\mathbf{8}$ | $h^{-1}\mathbf{3}$ | $h^{-1}\mathbf{7}$ | $h^{-1}\mathbf{11}$ | [13] $h\mathbf{13}$ | **13** |

**Second relation table**

| | $a$ | $a$ | $a$ | $b^{-1}$ | $a^{-1}$ | $a^{-1}$ | $b^{-1}$ |
|---|---|---|---|---|---|---|---|
| **1** | $h\mathbf{1}$ | $h^2\mathbf{1}$ | $h^3\mathbf{1}$ | $h^3\mathbf{3}$ | $\mathbf{4}$ | $\mathbf{2}$ | $\mathbf{1}$ |
| **2** | $\mathbf{4}$ | $h^3\mathbf{3}$ | $h^3\mathbf{7}$ | $h^3\mathbf{11}$ | 1 $\cancel{\mathbf{9}}\; h^4\mathbf{8}$ | $\mathbf{5}$ | $\mathbf{2}$ |
| **3** | $\mathbf{7}$ | $h^2\mathbf{6}$ | $h^2\mathbf{2}$ | $h^2\mathbf{1}$ | $h\mathbf{1}$ | $\mathbf{1}$ | $\mathbf{3}$ |
| **4** | $h^3\mathbf{3}$ | 3 $h^3\mathbf{7}$ | $h^5\mathbf{6}$ | $h^4\mathbf{7}$ | $h^4\mathbf{3}$ | $h\mathbf{4}$ | $\mathbf{4}$ |
| **5** | $\cancel{\mathbf{9}}\; h^4\mathbf{8}$ | $h^3\mathbf{11}$ | $h^5\mathbf{13}$ | $h^6\mathbf{13}$ | $h^4\mathbf{11}$ | $h^5\mathbf{8}$ | $\mathbf{5}$ |
| **6** | $\mathbf{2}$ | $\mathbf{4}$ | $h^3\mathbf{3}$ | $h^3\mathbf{8}$ | $h^{-1}\mathbf{5}$ | $h^{-1}\mathbf{10}$ | $\mathbf{6}$ |
| **7** | $h^2\mathbf{6}$ | $h^2\mathbf{2}$ | $h^2\mathbf{4}$ | $h\mathbf{4}$ | 6 $h\mathbf{2}$ | $h\mathbf{6}$ | $\mathbf{7}$ |
| **8** | $h^{-1}\mathbf{11}$ | $h\mathbf{13}$ | $h\mathbf{10}$ | $h^2\mathbf{6}$ | $\mathbf{7}$ | $\mathbf{3}$ | $\mathbf{8}$ |
| $\cancel{\mathbf{9}}$ | | | | | | | $\cancel{\mathbf{9}}$ |
| **10** | $\mathbf{5}$ | $h^4\mathbf{8}$ | $h^3\mathbf{11}$ | $h^{-2}\mathbf{12}$ | $h^{-1}\mathbf{12}$ | $\mathbf{12}$ | $\mathbf{10}$ |
| **11** | $h^2\mathbf{13}$ | $h^2\mathbf{10}$ | $h^2\mathbf{5}$ | 10 $h^2\mathbf{2}$ | $h^2\mathbf{6}$ | $\mathbf{7}$ | $\mathbf{11}$ |
| **12** | $h^{-1}\mathbf{12}$ | $h^{-2}\mathbf{12}$ | $h^{-3}\mathbf{12}$ | $h^{-3}\mathbf{10}$ | $h^{-3}\mathbf{13}$ | $h^5\mathbf{11}$ | $\mathbf{12}$ |
| **13** | $\mathbf{10}$ | $\mathbf{5}$ | $h^4\mathbf{8}$ | $h^{-1}\mathbf{5}$ | $h^{-1}\mathbf{10}$ | 14 $h^{-1}\mathbf{13}$ | $\mathbf{13}$ |

**Coset table**

| | $a$ | $b$ | $a^{-1}$ | $b^{-1}$ |
|---|---|---|---|---|
| **1** | $h\mathbf{1}_{\,0}$ | $\underline{\mathbf{2}}$ | $h^{-1}\mathbf{1}_{\,0}$ | $\underline{\mathbf{3}}$ |
| **2** | $\underline{\mathbf{4}}$ | $\underline{\mathbf{5}}$ | $\underline{\mathbf{6}}$ | $\underline{\mathbf{1}}$ |
| **3** | $\underline{\mathbf{7}}$ | $\underline{\mathbf{1}}$ | $h^{-3}\mathbf{4}_{\,1}$ | $\underline{\mathbf{8}}$ |
| **4** | $h^{3}\mathbf{3}_{\,1}$ | $h\mathbf{4}_{\,2}$ | $\underline{\mathbf{2}}$ | $h^{-1}\mathbf{4}_{\,2}$ |
| **5** | $\cancel{\mathbf{9}}\ h^{4}\mathbf{8}_{\,6}$ | $h^{5}\mathbf{8}_{\,7}$ | $\underline{\mathbf{10}}$ | $\underline{\mathbf{2}}$ |
| **6** | $\underline{\mathbf{2}}$ | $h^{-1}\mathbf{10}_{\,5}$ | $h^{-2}\mathbf{7}_{\,3}$ | $h^{-1}\mathbf{7}_{\,4}$ |
| **7** | $h^{2}\mathbf{6}_{\,3}$ | $h\mathbf{6}_{\,4}$ | $\underline{\mathbf{3}}$ | $\underline{\mathbf{11}}$ |
| **8** | $h^{-1}\mathbf{11}_{\,8}$ | $\underline{\mathbf{3}}$ | $h^{-4}\mathbf{5}_{\,6}$ | $h^{-5}\mathbf{5}_{\,7}$ |
| $\cancel{\mathbf{9}}$ | | | $\underline{\cancel{\mathbf{5}}}$ | |
| **10** | $\underline{\mathbf{5}}$ | $\underline{\mathbf{12}}$ | $\underline{\mathbf{13}}$ | $h\mathbf{6}_{\,5}$ |
| **11** | $h^{2}\mathbf{13}_{\,12}$ | $\underline{\mathbf{7}}$ | $h\mathbf{8}_{\,8}$ | $h^{-5}\mathbf{12}_{\,10}$ |
| **12** | $h^{-1}\mathbf{12}_{\,9}$ | $h^{5}\mathbf{11}_{\,10}$ | $h\mathbf{12}_{\,9}$ | $\underline{\mathbf{10}}$ |
| **13** | $\underline{\mathbf{10}}$ | $h^{-1}\mathbf{13}_{\,11}$ | $h^{-2}\mathbf{11}_{\,12}$ | $h\mathbf{13}_{\,11}$ |

**Protocol** (D=Definition, C=Consequence)

$$
\begin{array}{lllllll}
C0 & & & 1a = h1, & 1a^{-1} = h^{-1}1 & & \\
D1 & 1b & =:\ 2 & & & & \\
D2 & 1b^{-1} & =:\ 3 & & & & \\
D3 & 2a & =:\ 4 & & & & \\
C1 & & & 3a^{-1} = h^{-3}4, & 4a = h^{3}3 & & \\
C2 & & & 4b^{-1} = h^{-1}4, & 4b = h4 & & \\
D4 & 2b & =:\ 5 & & & & \\
D5 & 2a^{-1} & =:\ 6 & & & & \\
D6 & 3a & =:\ 7 & & & & \\
C3 & & & 7a = h^{2}6, & 6a^{-1} = h^{-2}7 & & \\
C4 & & & 7b = h6, & 6b^{-1} = h^{-1}7 & & \\
D7 & 3b^{-1} & =:\ 8 & & & & \\
D8 & 5a & =:\ 9 & & & & \\
D9 & 5a^{-1} & =:\ 10 & & & & \\
C5 & & & 6b = h^{-1}10, & 10b^{-1} = h6 & & \\
C6 & & & 8a^{-1} = h^{-4}5, & 5a = h^{4}8 & \Longrightarrow & 9 = h^{4}8 \\
 & & & \text{from coset table} & 5a = 9 & & \\
C7 & & & 8b^{-1} = h^{-5}5, & 5b = h^{5}8 & & \\
D10 & 7b^{-1} & =:\ 11 & & & & \\
C8 & & & 11a^{-1} = h8, & 8a = h^{-1}11 & & \\
D11 & 10b & =:\ 12 & & & & \\
C9 & & & 12a = h^{-1}12, & 12a^{-1} = h12 & & \\
C10 & & & 11b^{-1} = h^{-5}12, & 12b = h^{5}11 & & \\
D12 & 10a^{-1} & =:\ 13 & & & & \\
C11 & & & 13b = h^{-1}13, & 13b^{-1} = h13 & & \\
C12 & & & 13a^{-1} = h^{-2}11, & 11a = h^{2}13 & & \\
C13 & & & & h^{10}13a = 10 & \Longrightarrow & \underline{h^{10} = 1} \\
 & & & \text{from coset table} & 13a = 10 & & \\
C14 & & & & h^{-3}13a^{-1} = h^{5}11 & \Longrightarrow & \underline{h^{10} = 1} \\
 & & & \text{from coset table} & h^{-3}13a^{-1} = h^{-5}11 & & 
\end{array}
$$

## 12. Bibliography


[Atk 84] M.D. Atkinson, ed., Computational group theory. Academic Press, London (1984).

[ARo 84] D.G. Arrell, E.F. Robertson, A modified Todd-Coxeter Algorithm. pp. 27-32 in [Atk 84].

[Can 84] J.J. Cannon, An introduction to the group theory language, Cayley. pp. 145-183 in [Atk 84].

[Cav 86] A. Cavicchioli, A countable class of non-homeomorphic homology spheres with Heegard genus 2. Geom. Dedicata 20 (1986) 345-348.

[Deh 11] M. Dehn, Über unendliche diskontinuierliche Gruppen. Math. Annalen 71 (1911) 116-144.

[Hac 86] D. Hacon, O invariante de Jones e outros invariantes de nos. Matematica Universitaria No 3 (1986) 61-83.

[HaN 80] G. Havas, M.F. Newman, Application of computers to questions like those of Burnside. Lecture Notes in Math. 806, Springer, Berlin (1980) 211-230.

[Hup 67] B. Huppert, Endliche Gruppen I. Springer-Verlag (1967).

[Joh 80] D.L. Johnson, Topics in the theory of group presentations. LMS Lecture Notes Series 42, Cambridge U.P. (1980).

[Leo 80a] J.S. Leon, Finding the order of a permutation group. pp. 511-517 in: B. Cooperstein, G. Mason, eds.: Proc. Symp. Pure Math. 37, AMS (1980).

[Leo 80b] J.S. Leon, On an algorithm for finding a base and a strong generating set for a group given by generating permutations. Math. Comp. 35 (1980) 941-974.

[LNS 84] R. Laue, J. Neubüser, U. Schoenwaelder, Algorithms for finite soluble groups and the SOGOS system. pp. 105-135 in [Atk 84].

[Mac 74] I.D. Macdonald, A computer application to finite p-groups. J. Austral. Math. Soc. 17 (1974) 102-112.

[Mag 81] W. Magnus, The uses of 2 by 2 matrices in combinatorial group theory. A survey. Resul. der Mat. 4 (1981) 171 - 192.

[MAP 85] B.W. Char, K.O. Geddes, G.H. Gonnet, S.M. Watt, MAPLE Reference Manual. Symbolic Computation Group, Department of Computer Science, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1 (1985).

[Neu 82] J. Neubüser, An elementary introduction to coset table methods in computational group theory. pp. 1-45 in: C. Campbell, E. Robertson, eds.: Groups St. Andrews 81, LMS Lecture Note Series 71, Cambridge U.P. (1982).

[New 76] M.F. Newman, Calculating presentations for certain kinds of quotient groups, pp. 2-8 in: R.D. Jenks, ed.: SYMSAC 76, Assoc. Comp. Mach., New York, (1976).

[NPP 84] J. Neubüser, H. Pahlings, W. Plesken, CAS; Design and use of a system for the handling of characters of finite groups. pp. 195-247 in [Atk 84].

[Nov 55] P.S. Novikov, On the algorithmic unsolvability of the word problem in group theory. Trudy Mat. Inst. im Steklov 44 (1955) 143pp; AMS Translations, ser. 2, 9 (1958) 1-122.

[Rab 58] M.O. Rabin, Recursive unsolvability of group theoretic problems. Ann. of Math., 67 (1958) 172-194.

[ToC 36] J.A. Todd, H.S.M. Coxeter, A practical method for enumerating cosets of a finite abstract group. Proc. Edinburgh Math. Soc. 5 (1936) 26-34.