Journal of Nonlinear Mathematical Physics Volume 13, Supplement (2006), 55–65 AGMF Tallin '05

Description of a Class of 2-Groups

Tatjana GRAMUSHNJAK [†] *and Peeter PUUSEMP* [‡1]

[†] *Department of Mathematics, Tallinn University*
Narva road 25, 10120 Tallinn, Estonia
E-mail: tatjana@tlu.ee

[‡] *Department of Mathematics, Tallinn University of Technology*
Ehitajate tee 5, 19086 Tallinn, Estonia
E-mail: puusemp@staff.ttu.ee

This article is part of the Proceedings of the Baltic-Nordic Workshop, **Algebra, Geometry and Mathematical Physics** *which was held in Tallinn, Estonia, during October 2005.*

Abstract

Let n be an integer such that $n \geq 3$ and C_m denote a cyclic group of order m . It is proved that there exist exactly 17 non-isomorphic groups of order 2^{2n+1} which can be represented as a semidirect product $(C_{2^n} \times C_{2^n}) \leftthreetimes C_2$. These groups are given by generators and defining relations.

1 Introduction

All non-Abelian groups of order < 32 are described in [1] (table 1 at the end of the book). M.Jr.Hall and J.K.Senior [2] gave a fully description of all groups of order 2^n, $n \leq 6$. There exist exactly 51 non-isomorphic groups of order 32. In [2], these groups are numbered by 1, 2,..., 51. Among these groups, the groups with numbers 3, 14, 16, 31, 34, 39 and 41 can be presented as a semidirect product $(C_{2^2} \times C_{2^2}) \leftthreetimes C_2$, where C_m denotes the cyclic groups of order m. In this paper we describe all non-isomorphic finite groups which can be presented in a form $(C_{2^n} \times C_{2^n}) \leftthreetimes C_2$, where $n \geq 3$. Each such group G is given by three generators a, b, c and the defining relations

$$a^{2^n} = b^{2^n} = c^2 = 1,\ ab = ba,\ c^{-1}ac = a^i b^j,\ c^{-1}bc = a^k b^l \tag{1.1}$$

for some i, j, k, $l \in \mathbb{Z}_{2^n}$ ($\mathbb{Z}_{2^n}$ – the ring of residue classes modulo 2^n).

The aim of this paper is to prove the following theorem:

Theorem 1.1. *Let n be an integer such that $n \geq 3$. Then there exist exactly 17 non-isomorphic groups of order 2^{2n+1} which can be presented as a semidirect product $(C_{2^n} \times C_{2^n}) \leftthreetimes C_2$. They are:*

[1] This work was supported in part by the Estonian Science Foundation Research Grant 5900.

$G_1 =< a,b,c \mid (*),\ c^{-1}ac = a,\ c^{-1}bc = b >,$
$G_2 =< a,b,c \mid (*),\ c^{-1}ac = a^{1+2^{n-1}},\ c^{-1}bc = b^{1+2^{n-1}} >,$
$G_3 =< a,b,c \mid (*),\ c^{-1}ac = ab^{2^{n-1}},\ c^{-1}bc = b >,$
$G_4 =< a,b,c \mid (*),\ c^{-1}ac = a^{1+2^{n-1}}b^{2^{n-1}},\ c^{-1}bc = b^{1+2^{n-1}} >,$
$G_5 =< a,b,c \mid (*),\ c^{-1}ac = a^{-1},\ c^{-1}bc = b^{-1} >,$
$G_6 =< a,b,c \mid (*),\ c^{-1}ac = a^{-1+2^{n-1}},\ c^{-1}bc = b^{-1+2^{n-1}} >,$
$G_7 =< a,b,c \mid (*),\ c^{-1}ac = a^{-1}b^{2^{n-1}},\ c^{-1}bc = b^{-1} >,$
$G_8 =< a,b,c \mid (*),\ c^{-1}ac = a^{-1+2^{n-1}}b^{2^{n-1}},\ c^{-1}bc = b^{-1+2^{n-1}} >,$
$G_9 =< a,b,c \mid (*),\ c^{-1}ac = ab^{2^{n-1}},\ c^{-1}bc = a^{2^{n-1}}b^{1+2^{n-1}} >,$
$G_{10} =< a,b,c \mid (*),\ c^{-1}ac = a,\ c^{-1}bc = b^{1+2^{n-1}} >,$
$G_{11} =< a,b,c \mid (*),\ c^{-1}ac = a^{-1}b^{2^{n-1}},\ c^{-1}bc = a^{2^{n-1}}b^{-1+2^{n-1}} >,$
$G_{12} =< a,b,c \mid (*),\ c^{-1}ac = a^{-1},\ c^{-1}bc = b^{-1+2^{n-1}} >,$
$G_{13} =< a,b,c \mid (*),\ c^{-1}ac = a,\ c^{-1}bc = b^{-1+2^{n-1}} >,$
$G_{14} =< a,b,c \mid (*),\ c^{-1}ac = a^{-1},\ c^{-1}bc = b^{1+2^{n-1}} >,$
$G_{15} =< a,b,c \mid (*),\ c^{-1}ac = b,\ c^{-1}bc = a >,$
$G_{16} =< a,b,c \mid (*),\ c^{-1}ac = a,\ c^{-1}bc = b^{-1} >,$
$G_{17} =< a,b,c \mid (*),\ c^{-1}ac = a^{1+2^{n-1}},\ c^{-1}bc = b^{-1+2^{n-1}} >,$

where $(*)$ *denotes the collection* $\{a^{2^n} = b^{2^n} = c^2 = 1,\ ab = ba\}$ *of defining relations.*

Each group G, given by relations (1.1), is fully characterized by the matrix

$$A = \begin{Vmatrix} i & j \\ k & l \end{Vmatrix} \in \mathrm{GL}_2(\mathbb{Z}_{2^n}), \tag{1.2}$$

where $A^2 = I$ (I – the identity matrix) and $\mathrm{GL}_2(\mathbb{Z}_{2^n})$ is the set of all regular (2×2)-matrices over $\mathbb{Z}_{2^n}$. Therefore, first we must find all regular (2×2)-matrices of order two over $\mathbb{Z}_{2^n}$. We shall do it in the next section.

2 Matrices of order two over $\mathbb{Z}_{2^n}$

Assume that $n \geq 3$. Choose

$$A = \begin{Vmatrix} i & j \\ k & l \end{Vmatrix} \in \mathrm{GL}_2(\mathbb{Z}_{2^n})$$

and determine the conditions under which $A^2 = I$. Equating the corresponding elements of A^2 and I, we get the following system of equations for determining i, j, k and l:

$$\begin{cases} i^2 + jk \equiv 1 \pmod{2^n}, \\ i^2 - l^2 \equiv (i-l)(i+l) \equiv 0 \pmod{2^n}, \\ j(i+l) \equiv 0 \pmod{2^n}, \\ k(i+l) \equiv 0 \pmod{2^n}. \end{cases} \tag{2.1}$$

Next we solve system (2.1).

The second equation of (2.1) implies that i and l are both odd or both even. By the first equation of (2.1), il and jk have different values modulo 2. Hence we can consider four different cases for the solution of system (2.1):

I i and l are even; j and k are odd;
II i and l are odd; j or k is odd;
III i and l are odd; j and k are even; $jk \equiv 0 \pmod{2^n}$;
IV i and l are odd; j and k are even; $jk \not\equiv 0 \pmod{2^n}$.

Solving system (2.1) in cases I and II, we get the following three sets of matrices of order two:

$$\mathcal{M}_1 = \left\{ \begin{Vmatrix} i & j \\ (1-i^2)j^{-1} & -i \end{Vmatrix} \mid i \in 2\mathbb{Z}_{2^n},\ j \in \mathbb{Z}^*_{2^n} \right\},$$

$$\mathcal{M}_2 = \left\{ \begin{Vmatrix} i & j \\ (1-i^2)j^{-1} & -i \end{Vmatrix} \mid i \in \mathbb{Z}^*_{2^n},\ j \in \mathbb{Z}^*_{2^n} \right\},$$

$$\mathcal{M}_3 = \left\{ \begin{Vmatrix} i & (1-i^2)k^{-1} \\ k & -i \end{Vmatrix} \mid i \in \mathbb{Z}^*_{2^n},\ k \in \mathbb{Z}^*_{2^n} \right\},$$

where $\mathbb{Z}^*_{2^n}$ denotes the group of invertible elements of the ring $\mathbb{Z}_{2^n}$. The numbers of elements in these sets are

$$|\mathcal{M}_1| = |\mathcal{M}_2| = |\mathcal{M}_3| = 2^{2n-2}.$$

Let us consider case III. In this case

$$i,\, l \in \mathbb{Z}^*_{2^n};\quad j,\, k \in 2\mathbb{Z}_{2^n};\quad jk \equiv 0 \pmod{2^n}.$$

Under these conditions the first and second equations of system (2.1) imply $i,\, l \in \{\pm 1,\ \pm 1 + 2^{n-1}\}$. Hence

$$i + l \in \{0,\, 2,\, -2,\, 2^{n-1},\, 2 + 2^{n-1},\, -2 + 2^{n-1}\}.$$

Solving system (2.1) in these six cases for $i + l$, we get the following six sets of matrices of order two, respectively:

$$\mathcal{M}_4 = \left\{ \begin{Vmatrix} i & 2^s u \\ 2^t v & -i \end{Vmatrix} \mid \begin{array}{l} i \in \{\pm 1,\ \pm 1 + 2^{n-1}\},\ 1 \le s,\, t \le n; \\ s + t \ge n;\ u \in \mathbb{Z}^*_{2^{n-s}},\ v \in \mathbb{Z}^*_{2^{n-t}} \end{array} \right\},$$

$$\mathcal{M}_5 = \left\{ \begin{Vmatrix} 1 + 2^{n-1}w & 2^{n-1}u \\ 2^{n-1}v & 1 + 2^{n-1}w \end{Vmatrix} \mid u,\, v,\, w \in \mathbb{Z}_2 \right\},$$

$$\mathcal{M}_6 = \left\{ \begin{Vmatrix} -1 + 2^{n-1}w & 2^{n-1}u \\ 2^{n-1}v & -1 + 2^{n-1}w \end{Vmatrix} \mid u,\, v,\, w \in \mathbb{Z}_2 \right\},$$

$$\mathcal{M}_7 = \left\{ \begin{Vmatrix} i & 2^s u \\ 2^t v & -i + 2^{n-1} \end{Vmatrix} \mid \begin{array}{l} i \in \{\pm 1,\ \pm 1 + 2^{n-1}\},\ 1 \le s,\, t \le n; \\ s + t \ge n;\ u \in \mathbb{Z}^*_{2^{n-s}},\ v \in \mathbb{Z}^*_{2^{n-t}} \end{array} \right\},$$

$$\mathcal{M}_8 = \left\{ \begin{Vmatrix} 1 & 2^{n-1}u \\ 2^{n-1}v & 1 + 2^{n-1} \end{Vmatrix},\ \begin{Vmatrix} 1 + 2^{n-1} & 2^{n-1}u \\ 2^{n-1}v & 1 \end{Vmatrix} \mid u,\, v \in \mathbb{Z}_2 \right\},$$

$$\mathcal{M}_9 = \left\{ \begin{Vmatrix} -1 & 2^{n-1}u \\ 2^{n-1}v & -1 + 2^{n-1} \end{Vmatrix},\ \begin{Vmatrix} -1 + 2^{n-1} & 2^{n-1}u \\ 2^{n-1}v & -1 \end{Vmatrix} \mid u,\, v \in \mathbb{Z}_2 \right\}.$$

The numbers of elements in these sets are

$$|\mathcal{M}_4| = |\mathcal{M}_7| = 2^{n+1}n,\quad |\mathcal{M}_5| = |\mathcal{M}_6| = |\mathcal{M}_8| = |\mathcal{M}_9| = 8.$$

For the purpose of the considerations of section 3, we divide $\mathcal{M}_4$ into a union of two disjoint subsets $\mathcal{M}_4^1$ and $\mathcal{M}_4^2$, where $\mathcal{M}_4^1$ consists of all matrices of $\mathcal{M}_4$ in which $s+t=n,\ i=\pm 1+2^{n-1}$ or $s+t>n,\ i=\pm 1$, and $\mathcal{M}_4^2$ consists of all matrices of $\mathcal{M}_4$ in which $s+t=n,\ i=\pm 1$ or $s+t>n,\ i=\pm 1+2^{n-1}$. Similarly, we divide the set $\mathcal{M}_7$ into a union of two disjoint subsets $\mathcal{M}_7^1$ and $\mathcal{M}_7^2$, where $\mathcal{M}_7^1$ consists of all matrices of $\mathcal{M}_7$ in which $s+t=n,\ i\in\{-1,\ 1+2^{n-1}\}$ or $s+t>n,\ i\in\{1,\ -1+2^{n-1}\}$, and $\mathcal{M}_7^2$ consists of all matrices of $\mathcal{M}_7$ in which $s+t=n,\ i\in\{1,\ -1+2^{n-1}\}$ or $s+t>n,\ i\in\{-1,\ 1+2^{n-1}\}$.

Finally, let us consider case IV. Then j and k can be presented in the forms

$$j=2^s u,\quad k=2^t v;\ \ 1\le s,\, t\le n-1,$$

$$2\le m=s+t\le n-1,\ u\in\mathbb{Z}^*_{2^{n-s}},\ v\in\mathbb{Z}^*_{2^{n-t}}.$$

Since $i^2-1=(i-1)(i+1)\equiv -jk\,(\operatorname{mod} 2^n)$, we have

$$i-1=2^r p,\ 1\le r\le m-1,\ p\in\mathbb{Z}^*_{2^{n-r}}.$$

Then $i+1=2^r p+2$ and the first equation of system (2.1) implies

$$i^2-1=2^{r+1}p(1+2^{r-1}p)\equiv -2^m uv\,(\operatorname{mod} 2^n),$$

$$p(1+2^{r-1}p)\equiv -2^{m-r-1}uv\,(\operatorname{mod} 2^{n-r-1}). \tag{2.2}$$

For the solvability of equation (2.2), it is necessary that $r=m-1>1$ or $r=1$. In both cases $m\ge 3$. Next we consider these cases separately.

Assume that $r=m-1>1$, i.e. $r=2,\,3,\dots,\,n-2$. Then, by (2.2),

$$uv\equiv -p(1+2^{r-1}p)\,(\operatorname{mod} 2^{n-m}). \tag{2.3}$$

Choose the numbers $r,\ p,\ s,\ t,\ u,\ v$ as follows. First, let us choose arbitrary $r\in\{2,\,3,\dots,\,n-2\}$ and $p\in\mathbb{Z}^*_{2^{n-r}}$. Now choose s and t such that

$$s+t=m=r+1,\ 1\le s,\, t\le n-1.$$

After that choose an arbitrary $u_0\in\mathbb{Z}^*_{2^{n-m}}$, replace u by u_0 in (2.3) and solve equation (2.3) with respect to v. Denote this solution by v_0 ($v_0\in\mathbb{Z}^*_{2^{n-m}}$). Then the pairs $(u,\,v)$, satisfying (2.3), are

$$u=u_0+2^{n-m}k_0,\ v=v_0+2^{n-m}l_0;\ \ k_0\in\mathbb{Z}_{2^t},\ l_0\in\mathbb{Z}_{2^s}.$$

If the numbers $r,\ p,\ s,\ t,\ u,\ v$ are chosen in this way, then the corresponding numbers $i,\ j$ and k are the solutions of the first equation $i^2+jk\equiv 1(\operatorname{mod} 2^n)$ of system (2.1). Let us determine the number of solutions of this equation. For the choice of the pair $(u,\,v)$ we have $2^t\cdot 2^{n-r-2}\cdot 2^s=2^{n-1}$ possibilities. The number of choices of $(r,\,p,\,s,\,t)$ depends on r: there are r possibilities for the choice of pairs $(s,\,t)$ and 2^{n-r-1} possibilities for the choice of p. Hence we have

$$\sum_{r=2}^{n-2} r\cdot 2^{n-r-1}=3\cdot 2^{n-2}-2n$$

possibilities for the choice of $(r,\, p,\, s,\, t)$. Therefore, the number of solutions of the first equation of (2.1) in the case $r = m - 1 > 1$ is

$$2^{n-1} \cdot (3 \cdot 2^{n-2} - 2n). \tag{2.4}$$

Next assume that $r = 1$. Then (2.2) implies

$$p(1+p) \equiv -2^{m-2}uv \,(\operatorname{mod} 2^{n-m}). \tag{2.5}$$

The number $1 + p$ can be presented in the form

$$1 + p = 2^{m-2}q, \quad q \in \mathbb{Z}^*_{2^{n-1-(m-2)}} = \mathbb{Z}^*_{2^{n-m+1}}.$$

Hence (2.5) implies

$$(1 - 2^{m-2}q)q \equiv uv \,(\operatorname{mod} 2^{n-m}). \tag{2.6}$$

The choice of triples $(i,\, j,\, k)$, satisfying the first equation of system (2.1), proceeds as follows. First choose m such that $3 \le m \le n-1$. Next choose s and t such that $s + t = m$, $1 \le s, t \le n - 1$. After that choose $q \in \mathbb{Z}^*_{2^{n-m+1}}$ and calculate $p = -1 + 2^{m-2}q$, $i = 1 + 2p$. Now choose an arbitrary $u_0 \in \mathbb{Z}^*_{2^{n-m}}$, replace u by u_0 in (2.6) and solve the equation (2.6) with respect to v. Denote this solution by v_0 ($v_0 \in \mathbb{Z}^*_{2^{n-m}}$). Then the pairs $(u,\, v)$, satisfying (2.6), are

$$u = u_0 + 2^{n-m}k_0, \;\; v = v_0 + 2^{n-m}l_0; \;\; k_0 \in \mathbb{Z}_{2^t}, \;\; l_0 \in \mathbb{Z}_{2^s}.$$

If the numbers m, q, s, t, u, v are chosen in this way, then the corresponding numbers i, j and k are the solutions of the first equation $i^2 + jk \equiv 1(\operatorname{mod} 2^n)$ of system (2.1). Let us determine the number of solutions of this equation in our case. For the choice of the pair $(u,\, v)$ we have $2^t \cdot 2^{n-m-1} \cdot 2^s = 2^{n-1}$ possibilities. The number of choices of $(m,\, q,\, s,\, t)$ depends on m: there are $m - 1$ possibilities for the choice of pairs $(s,\, t)$ and 2^{n-m} possibilities for the choice of q. Hence we have

$$\sum_{m=3}^{n-1} (m-1) \cdot 2^{n-m} = 3 \cdot 2^{n-2} - 2n$$

possibilities for the choice of $(m,\, q,\, s,\, t)$. Therefore, the number of the solutions of the first equation of (2.1) in the case $r = 1$ is also give by (2.4).

We have got all solutions of the first equation of (2.1). In both cases, $r > 1$ and $r = 1$, they can be presented commonly as follows

$$i = \pm 1 + 2^{m-1}p, \;\; b = 2^s u, \;\; c = 2^t v, \tag{2.7}$$

where $p \in \mathbb{Z}^*_{2^{n-m+1}}$ and other parameters are described above. The sign + corresponds to the case $r > 1$ and the sign - corresponds to the case $r = 1$. Let us solve now system (2.1) fully.

The first and second equations of (2.1) imply $l^2 + jk \equiv 1 \,(\operatorname{mod} 2^n)$. Therefore, similarly to (2.7), we get

$$l = \pm 1 + 2^{m-1}p_1, \;\; p_1 \in \mathbb{Z}^*_{2^{n-m+1}}. \tag{2.8}$$

Assume that in (2.7) and (2.8) the signs are equal. Then $i+l=2(\pm 1+2^{m-2}(p+p_1))$ and the third equation of (2.1) implies $2\equiv 0\,(\operatorname{mod} 2^{n-s})$, i.e., $s=n-1$. This contradicts $t\geq 1$ and $m=s+t\leq n-1$. Hence the signs in (2.7) and (2.8) are different and

$$(i,\, l)=(1+2^{m-1}p,\, -1+2^{m-1}p_1)\ \text{ or }\ (i,\, l)=(-1+2^{m-1}p,\, 1+2^{m-1}p_1), \tag{2.9}$$
$$i+l=2^{m-1}(p+p_1),\quad i-l=\pm 2+2^{m-1}(p-p_1).$$

By the second equation of (2.1), we have

$$(i+l)(i-l)=2^{m-1}(p+p_1)2(\pm 1+2^{m-2}(p-p_1))\equiv 0\,(\operatorname{mod} 2^n),$$

i.e.,

$$p+p_1\equiv 0\,(\operatorname{mod} 2^{n-m}). \tag{2.10}$$

Consequently, the two first equations of (2.1) are valid only in the case when conditions (2.9) and (2.10) hold. But in this case also the two last equations of system (2.1) are valid. Hence

$$p+p_1=2^{n-m}w,\quad w\in\mathbb{Z}_2,$$
$$l=\mp 1+2^{m-1}p_1=\mp 1+2^{m-1}(-p+2^{n-m}w)=-i+2^{n-1}w,$$

and we have got the set of all matrices of order two in case IV:

$$\mathcal{M}_{10}=\left\{\begin{Vmatrix} i=\pm 1+2^{m-1}p & 2^s u\\ 2^t v & -i+2^{n-1}w\end{Vmatrix}\right\},$$

where

$$1\leq s,\, t\leq n-1,\ 3\leq m=s+t\leq n-1,\ p\in\mathbb{Z}^*_{2^{n-m+1}},\ w\in\mathbb{Z}_2,$$
$$u=u_0+2^{n-m}k_0,\ v=v_0+2^{n-m}l_0,\ k_0\in\mathbb{Z}_{2^t},\ l_0\in\mathbb{Z}_{2^s}$$

and v_0 is a solution of the equation

$$u_0v\equiv(\mp 1-2^{m-2}p)p\,(\operatorname{mod} 2^{n-m}),$$

or, equivalently,

$$u\in\mathbb{Z}^*_{2^{n-s}},\ v\in\mathbb{Z}^*_{2^{n-t}},\ uv+(\pm 1+2^{m-2}p)p\equiv 0\,(\operatorname{mod} 2^{n-m}).$$

Hence $\mathcal{M}_{10}$ can be presented as a disjoint union $\mathcal{M}_{10}=\mathcal{M}^1_{10}\cup\mathcal{M}^2_{10}\cup\mathcal{M}^3_{10}\cup\mathcal{M}^4_{10}$ of its subsets $\mathcal{M}^1_{10}$, $\mathcal{M}^2_{10}$, $\mathcal{M}^3_{10}$ and $\mathcal{M}^4_{10}$, where $\mathcal{M}^1_{10}$ consists of all matrices of $\mathcal{M}_{10}$ which satisfy the equalities $w=0$ and $uv+(\pm 1+2^{m-2}p)p\equiv 0\,(\operatorname{mod} 2^{n-m+1})$, $\mathcal{M}^2_{10}$ consists of all matrices of $\mathcal{M}_{10}$ which satisfy the equalities $w=0$ and $uv+(\pm 1+2^{m-2}p)p\equiv 2^{n-m}\,(\operatorname{mod} 2^{n-m+1})$, $\mathcal{M}^3_{10}$ consists of all matrices of $\mathcal{M}_{10}$ which satisfy the equalities $w=1,\ i=1+2^{m-1}p,\ uv+(1+2^{m-2}p)p\equiv 0\,(\operatorname{mod} 2^{n-m+1})$ or $w=1,\ i=-1+2^{m-1}p,\ uv+(-1+2^{m-2}p)p\equiv 2^{n-m}\,(\operatorname{mod} 2^{n-m+1})$, and, finally, $\mathcal{M}^4_{10}$ consists of all matrices of $\mathcal{M}_{10}$ which satisfy the equalities $w=1,\ i=1+2^{m-1}p,\ uv+(1+2^{m-2}p)p\equiv 2^{n-m}\,(\operatorname{mod} 2^{n-m+1})$ or $w=1,\ i=-1+2^{m-1}p,\ uv+(-1+2^{m-2}p)p\equiv 0\,(\operatorname{mod} 2^{n-m+1})$.

It is easy to check that

$$|\mathcal{M}_{10}|=2\cdot 2\cdot 2^{n-1}\cdot(3\cdot 2^{n-2}-2n)=2^{n+1}\cdot(3\cdot 2^{n-2}-2n).$$

If we sum up the numbers of elements of sets $\mathcal{M}_1,\ldots,\mathcal{M}_{10}$, we obtain $|\mathcal{M}|=4^{n-1}+32$.

We have proved the following theorem:

Theorem 2.1. *Assume that $n \geq 3$. Then the set $\mathcal{M}$ of all (2×2)-matrices A over $\mathbb{Z}_{2^n}$, satisfying $A^2 = I$, is the disjoint union of the sets $\mathcal{M}_1, \mathcal{M}_2, \ldots, \mathcal{M}_{10}$. The number of these matrices is $9 \cdot 4^{n-1} + 32$.*

3 Conjugate classes of matrices of order two

Let us consider the group G, given by (1.1) or, equivalently, by the corresponding matrix $A \in \mathcal{M}$, where the set $\mathcal{M}$ is described in section 2 (see (1.2)). Denote this group by $G(A)$. The matrix A determines an automorphism α of the subgroup $< a,\, b > = < a > \times < b >$ of $G(A)$: $a\alpha = a^i b^j$, $b\alpha = a^k b^l$. Then the composition rule in $G(A)$ is

$$c^u g \cdot c^v h = c^{u+v} \cdot g\alpha^v \cdot h; \quad u,\, v \in \mathbb{Z}_2; \quad g,\, h \in < a,\, b > . \tag{3.1}$$

Lemma 3.1. *Let $A,\, B \in \mathcal{M}$, and assume that A and B are conjugate: $B = C^{-1}AC$. Then the groups $G(A)$ and $G(B)$ are isomorphic.*

Proof. Assume that A and B belong to $\mathcal{M}$ and they are conjugate, $B = C^{-1}AC$. Denote by α, β and γ, respectively, the automorphisms of $< a,\, b >$ that correspond to these matrices. Using (3.1), it is easy to check that the map

$$T : G(A) \longrightarrow G(B); \quad (c^u g)T = c^u \cdot g\gamma; \quad u,\, v \in \mathbb{Z}_2; \quad g,\, h \in < a,\, b >,$$

is isomorphism between groups $G(A)$ and $G(B)$. The lemma is proved.

By lemma 3.1, it is clear that to prove theorem 1.1, we need to divide the set $\mathcal{M}$ into conjugacy classes $\mathcal{C}_1, \ldots, \mathcal{C}_m$ of matrices, choose a representative A_i from each conjugacy class $\mathcal{C}_i$, and, finally, check the isomorphism or non-isomorphism of groups $G(A_1), \ldots, G(A_m)$.

Theorem 3.1. *For a fixed $n \geq 3$, there exist 17 conjugacy classes of matrices in $\mathcal{M}$. They are*

1) $\mathcal{C}_1 = \left\{ \left\| \begin{matrix} 1 & 0 \\ 0 & 1 \end{matrix} \right\| \right\}$, *2)* $\mathcal{C}_2 = \left\{ \left\| \begin{matrix} 1+2^{n-1} & 0 \\ 0 & 1+2^{n-1} \end{matrix} \right\| \right\}$,

3) $\mathcal{C}_3 = \left\{ \left\| \begin{matrix} 1 & 2^{n-1} \\ 0 & 1 \end{matrix} \right\|, \left\| \begin{matrix} 1 & 0 \\ 2^{n-1} & 1 \end{matrix} \right\|, \left\| \begin{matrix} 1+2^{n-1} & 2^{n-1} \\ 2^{n-1} & 1+2^{n-1} \end{matrix} \right\| \right\}$,

4) $\mathcal{C}_4 = \left\{ \left\| \begin{matrix} 1 & 2^{n-1} \\ 2^{n-1} & 1 \end{matrix} \right\|, \left\| \begin{matrix} 1+2^{n-1} & 2^{n-1} \\ 0 & 1+2^{n-1} \end{matrix} \right\|, \left\| \begin{matrix} 1+2^{n-1} & 0 \\ 2^{n-1} & 1+2^{n-1} \end{matrix} \right\| \right\}$,

5) $\mathcal{C}_5 = \left\{ \left\| \begin{matrix} -1 & 0 \\ 0 & -1 \end{matrix} \right\| \right\}$, *6)* $\mathcal{C}_6 = \left\{ \left\| \begin{matrix} -1+2^{n-1} & 0 \\ 0 & -1+2^{n-1} \end{matrix} \right\| \right\}$,

7) $\mathcal{C}_7 = \left\{ \left\| \begin{matrix} -1 & 2^{n-1} \\ 0 & -1 \end{matrix} \right\|, \left\| \begin{matrix} -1 & 0 \\ 2^{n-1} & -1 \end{matrix} \right\|, \left\| \begin{matrix} -1+2^{n-1} & 2^{n-1} \\ 2^{n-1} & -1+2^{n-1} \end{matrix} \right\| \right\}$,

8) $\mathcal{C}_8 = \left\{ \left\| \begin{matrix} -1+2^{n-1} & 2^{n-1} \\ 0 & -1+2^{n-1} \end{matrix} \right\|, \left\| \begin{matrix} -1+2^{n-1} & 0 \\ 2^{n-1} & -1+2^{n-1} \end{matrix} \right\|, \left\| \begin{matrix} -1 & 2^{n-1} \\ 2^{n-1} & -1 \end{matrix} \right\| \right\}$,

9) $\mathcal{C}_9 = \left\{ \left\| \begin{matrix} 1 & 2^{n-1} \\ 2^{n-1} & 1+2^{n-1} \end{matrix} \right\|, \left\| \begin{matrix} 1+2^{n-1} & 2^{n-1} \\ 2^{n-1} & 1 \end{matrix} \right\| \right\}$, *10)* $\mathcal{C}_{10} = \mathcal{M}_8 \setminus \mathcal{C}_9$, *11)* $\mathcal{C}_{11} = \left\{ \begin{Vmatrix} -1 & 2^{n-1} \\ 2^{n-1} & -1+2^{n-1} \end{Vmatrix}, \begin{Vmatrix} -1+2^{n-1} & 2^{n-1} \\ 2^{n-1} & -1 \end{Vmatrix} \right\}$,

12) $\mathcal{C}_{12} = \mathcal{M}_9 \setminus \mathcal{C}_{11}$, *13)* $\mathcal{C}_{13} = \mathcal{M}_7^1 \cup \mathcal{M}_{10}^3$, *14)* $\mathcal{C}_{14} = \mathcal{M}_7^2 \cup \mathcal{M}_{10}^4$,

15) $\mathcal{C}_{15} = \mathcal{M}_1 \cup \mathcal{M}_2 \cup \mathcal{M}_3$, *16)* $\mathcal{C}_{16} = \mathcal{M}_4^1 \cup \mathcal{M}_{10}^1$, *17)* $\mathcal{C}_{17} = \mathcal{M}_4^2 \cup \mathcal{M}_{10}^2$.

Proof. Calculating the values of the pair $(|A|, \operatorname{Tr}(A))$ for each $A \in \mathcal{M}$, we get six different values ($\operatorname{Tr}(A)$ – the trace of A):

$$(1,\, 2),\ (1,\, -2),\ (1+2^{n-1},\, 2+2^{n-1}),$$

$$(1+2^{n-1},\, -2+2^{n-1}),\ (-1+2^{n-1},\, 2^{n-1}),\ (-1,\, 0).$$

Denote by $\mathcal{K}_1, \ldots, \mathcal{K}_6$ the sets of all matrices A of $\mathcal{M}$, for which the values of $(|A|, \operatorname{Tr}(A))$ are these six pairs, respectively. It is easy to check that

$$\mathcal{K}_1 = \mathcal{M}_5,\ \mathcal{K}_2 = \mathcal{M}_6,\ \mathcal{K}_3 = \mathcal{M}_8,\ \mathcal{K}_4 = \mathcal{M}_9,$$

$$\mathcal{K}_5 = \mathcal{M}_7^1 \cup \mathcal{M}_7^2 \cup \mathcal{M}_{10}^3 \cup \mathcal{M}_{10}^4,$$

$$\mathcal{K}_6 = \mathcal{M}_1 \cup \mathcal{M}_2 \cup \mathcal{M}_3 \cup \mathcal{M}_4 \cup \mathcal{M}_{10}^1 \cup \mathcal{M}_{10}^2.$$

Assume that $A, B \in \mathcal{M}$. If A and B are conjugate, then they have the same determinants and traces. Therefore, each set $\mathcal{K}_i$ is a union of some conjugacy classes. Our aim is to find these unions for sets $\mathcal{K}_1, \ldots, \mathcal{K}_6$.

First we divide $\mathcal{K}_1$ into conjugacy classes. Matrices

$$A_1 = \begin{Vmatrix} 1 & 0 \\ 0 & 1 \end{Vmatrix} \text{ and } A_2 = \begin{Vmatrix} 1+2^{n-1} & 0 \\ 0 & 1+2^{n-1} \end{Vmatrix}$$

belong to the centre of $\mathrm{GL}_2(\mathbb{Z}_{2^n})$. Hence we get conjugacy classes $\mathcal{C}_1 = \{A_1\}$ and $\mathcal{C}_2 = \{A_2\}$. Choose

$$A_3 = \begin{Vmatrix} 1 & 2^{n-1} \\ 0 & 1 \end{Vmatrix} \in \mathcal{K}_1 \setminus (\mathcal{C}_1 \cup \mathcal{C}_2).$$

Calculating the products $C^{-1}A_3C$ for each $C \in \mathrm{GL}_2(\mathbb{Z}_{2^n})$, we get a conjugacy class $\mathcal{C}_3 \subset \mathcal{K}_1$. Since $\mathcal{C}_1 \cup \mathcal{C}_2 \cup \mathcal{C}_3 \neq \mathcal{K}_1$, choose

$$A_4 = \begin{Vmatrix} 1+2^{n-1} & 2^{n-1} \\ 0 & 1+2^{n-1} \end{Vmatrix} \in \mathcal{K}_1 \setminus (\mathcal{C}_1 \cup \mathcal{C}_2 \cup \mathcal{C}_3).$$

Calculating the products $C^{-1}A_4C$ for each $C \in \mathrm{GL}_2(\mathbb{Z}_{2^n})$, we get a conjugacy class $\mathcal{C}_4 \subset \mathcal{K}_1$. Since $\mathcal{K}_1 = \mathcal{C}_1 \cup \mathcal{C}_2 \cup \mathcal{C}_3 \cup \mathcal{C}_4$, we have finished the dividing of $\mathcal{K}_1$ into conjugacy classes.

Similarly, we obtain the conjugacy classes for sets $\mathcal{K}_2$, $\mathcal{K}_3$ and $\mathcal{K}_4$:

$$\mathcal{K}_2 = \mathcal{C}_5 \cup \mathcal{C}_6 \cup \mathcal{C}_7 \cup \mathcal{C}_8,\ \mathcal{K}_3 = \mathcal{C}_9 \cup \mathcal{C}_{10},\ \mathcal{K}_4 = \mathcal{C}_{11} \cup \mathcal{C}_{12},$$

where $\mathcal{C}_5, \mathcal{C}_6, \ldots, \mathcal{C}_{12}$ are the conjugacy classes with representatives

$$A_5 = \begin{Vmatrix} -1 & 0 \\ 0 & -1 \end{Vmatrix},\ A_6 = \begin{Vmatrix} -1+2^{n-1} & 0 \\ 0 & -1+2^{n-1} \end{Vmatrix},$$

$$A_7 = \begin{Vmatrix} -1 & 2^{n-1} \\ 0 & -1 \end{Vmatrix}, \; A_8 = \begin{Vmatrix} -1+2^{n-1} & 2^{n-1} \\ 0 & -1+2^{n-1} \end{Vmatrix},$$

$$A_9 = \begin{Vmatrix} 1 & 2^{n-1} \\ 2^{n-1} & 1+2^{n-1} \end{Vmatrix}, \; A_{10} = \begin{Vmatrix} 1 & 0 \\ 0 & 1+2^{n-1} \end{Vmatrix},$$

$$A_{11} = \begin{Vmatrix} -1 & 2^{n-1} \\ 2^{n-1} & -1+2^{n-1} \end{Vmatrix}, \; A_{12} = \begin{Vmatrix} -1 & 0 \\ 0 & -1+2^{n-1} \end{Vmatrix},$$

respectively.

Let us divide now $\mathcal{K}_5$ into conjugacy classes. Choose two matrices $A_{13}, A_{14} \in \mathcal{K}_5$:

$$A_{13} = \begin{Vmatrix} 1 & 0 \\ 0 & -1+2^{n-1} \end{Vmatrix}, \; A_{14} = \begin{Vmatrix} -1 & 0 \\ 0 & 1+2^{n-1} \end{Vmatrix}.$$

Our aim is to find all matrices that are conjugate with these matrices. Assume that

$$C = \begin{Vmatrix} x & y \\ z & w \end{Vmatrix}$$

is an arbitrary element of $\mathrm{GL}_2(\mathbb{Z}_{2^n})$. Denote $d = xw - yz$. Since $C \in \mathrm{GL}_2(\mathbb{Z}_{2^n})$, we have $d = xw - yz \equiv 1 \,(\mathrm{mod}\, 2)$ and $x_0 w - y_0 z \equiv 1 \,(\mathrm{mod}\, 2^n)$, where $y_0 = yd^{-1}$, $x_0 = xd^{-1}$. All matrices which are conjugate with A_{13} have the form

$$C^{-1}A_{13}C = \frac{1}{d} \cdot \begin{Vmatrix} w & -y \\ -z & x \end{Vmatrix} \cdot \begin{Vmatrix} 1 & 0 \\ 0 & -1+2^{n-1} \end{Vmatrix} \cdot \begin{Vmatrix} x & y \\ z & w \end{Vmatrix} =$$

$$= \begin{Vmatrix} 1 + y_0 z \cdot 2(1-2^{n-2}) & 2y_0 w(1-2^{n-2}) \\ -2x_0 z(1-2^{n-2}) & -i_0 + 2^{n-1} \end{Vmatrix}, \tag{3.1}$$

where $i_0 = 1 + y_0 z \cdot 2(1-2^{n-2})$. Since the system

$$\begin{cases} 1 + y_0 z \cdot 2(1-2^{n-2}) = -1, \; 2y_0 w(1-2^{n-2}) = 0, \\ -2x_0 z(1-2^{n-2}) = 0, \; -i_0 + 2^{n-1} = 1 + 2^{n-1} \end{cases}$$

has no solution (x_0, y_0, z, w) in $\mathbb{Z}_{2^n}^4$, the matrices A_{13} and A_{14} are not conjugate.

Assume that

$$B = \begin{Vmatrix} i & 2^s u \\ 2^t v & -i + 2^{n-1} \end{Vmatrix} \in \mathcal{M}_7.$$

Here $i \in \{\pm 1, \; \pm 1 + 2^{n-1}\}$, $1 \le s, t \le n$; $s + t \ge n$; $u \in \mathbb{Z}_{2^{n-s}}^*$, $v \in \mathbb{Z}_{2^{n-t}}^*$. By (3.1), B is conjugate with A_{13} if and only if the system

$$\begin{cases} 1 + y_0 z \cdot 2(1-2^{n-2}) = i, \; 2y_0 w(1-2^{n-2}) = 2^s u, \\ -2x_0 z(1-2^{n-2}) = 2^t v, \; x_0 w - y_0 z = 1 \end{cases} \tag{3.2}$$

has a solution (x_0, y_0, z, w) in $\mathbb{Z}_{2^n}^4$. Let us consider the case $i = 1$. It follows from (3.2) that

$$\begin{cases} y_0 z \equiv 0 \,(\mathrm{mod}\, 2^{n-1}), \; y_0 w \equiv 2^{s-1} u (1-2^{n-2})^{-1} \,(\mathrm{mod}\, 2^{n-1}), \\ x_0 z \equiv -2^{t-1} v (1-2^{n-2})^{-1} \,(\mathrm{mod}\, 2^{n-1}), \; x_0 w - y_0 z \equiv 1 \,(\mathrm{mod}\, 2^n) \end{cases} \tag{3.3}$$

(the inverse elements are taken in $\mathbb{Z}_{2^n}^*$). Clearly, $x_0w \equiv 1 \pmod 2$ and, therefore, (3.3) implies

$$\begin{cases} y_0 \equiv 2^{s-1}uw^{-1}(1-2^{n-2})^{-1} \pmod{2^{n-1}}, \\ z \equiv -2^{t-1}vx_0^{-1}(1-2^{n-2})^{-1} \pmod{2^{n-1}}, \\ y_0z \equiv -2^{s+t-2}uvx_0^{-1}w^{-1}(1-2^{n-2})^{-2} \equiv 0 \pmod{2^{n-1}}, \\ x_0w - y_0z \equiv 1 \pmod{2^n}. \end{cases} \tag{3.4}$$

Hence it is necessary that $s+t-2 \geq n-1$, i.e. $s+t > n$. Assume that $s+t > 2$. Then, by (3.4), system (3.3) has a solution:

$$w = 1,\ x_0 = 1 + 2^{s+t-2},$$

$$y_0 = 2^{s-1}u(1-2^{n-2})^{-1},\ z = -2^{t-1}vx_0^{-1}(1-2^{n-2})^{-1}.$$

We have proved that if $i = 1$, then B is conjugate with A_{13} if and only if $s+t > n$. Similary calculations show that if $i = -1,\ i = 1+2^{n-1}, i = -1+2^{n-1}$, then system (3.2) is solvable and B is conjugate with A_{13} if and only if $s+t = n,\ s+t = n,\ s+t > n$, respectively. Consequently, the matrix $B \in \mathcal{M}_7$ is conjugate with A_{13} if and only if $B \in \mathcal{M}_7^1$. Similarly, the matrix $B \in \mathcal{M}_7$ is conjugate with A_{14} if and only if $B \in \mathcal{M}_7^2$. We have divided the set $\mathcal{M}_7$ into two part, one part consisting of elements which are conjugate with A_{13} and other part consisting of elements which are conjugate with A_{14}.

Carrying out analogous calculations for $B \in \mathcal{M}_{10}$, we obtain the following result: B is conjugate with A_{13} if and only if $B \in \mathcal{M}_{10}^3$, and B is conjugate with A_{14} if and only if $B \in \mathcal{M}_{10}^4$. Therefore, we have divided the set $\mathcal{K}_5$ into two conjugacy classes $\mathcal{C}_{13} = \mathcal{M}_7^1 \cup \mathcal{M}_{10}^3$ and $\mathcal{C}_{14} = \mathcal{M}_7^2 \cup \mathcal{M}_{10}^4$ with representatives A_{13} and A_{14}, respectively.

Finally, we must divide $\mathcal{K}_6$ into conjugacy classes. Choose three matrices $A_{15},\ A_{16},\ A_{17} \in \mathcal{K}_6$:

$$A_{15} = \begin{Vmatrix} 0 & 1 \\ 1 & 0 \end{Vmatrix},\ A_{16} = \begin{Vmatrix} 1 & 0 \\ 0 & -1 \end{Vmatrix},\ A_{17} = \begin{Vmatrix} 1+2^{n-1} & 0 \\ 0 & -1+2^{n-1} \end{Vmatrix}.$$

The centres of the groups $G(A_{15})$, $G(A_{16})$ and $G(A_{17})$ are C_{2^n}, $C_2 \times C_{2^n}$ and $C_2 \times C_{2^{n-1}}$, respectively. In view of lemma 3.1, these three matrices belong to different conjugacy classes. Similarly to the considerations in connection of matrices A_{13} and A_{14}, we obtain conjugacy classes $\mathcal{C}_{15}$, $\mathcal{C}_{16}$ and $\mathcal{C}_{17}$ which are represented by matrices A_{15}, A_{16} and A_{17}, respectively: $\mathcal{C}_{15} = \mathcal{M}_1 \cup \mathcal{M}_2 \cup \mathcal{M}_3$, $\mathcal{C}_{16} = \mathcal{M}_4^1 \cup \mathcal{M}_{10}^1$, $\mathcal{C}_{17} = \mathcal{M}_4^2 \cup \mathcal{M}_{10}^2$. The theorem is proved.

4 Proof of Theorem 1.1

By theorem 3.1, $\mathcal{M}$ consists of 17 conjugacy classes $\mathcal{C}_1, \dots, \mathcal{C}_{17}$. We preserve the notions $A_1, \dots, A_{17}$ given in the proof of theorem 3.1 for the representives of these conjugacy classes. Each group G which is given by defining relations (1.1) is isomorphic to a group $G(A_i)$ for suitable i. Theorem 1.1 will be proved if we show that the groups $G(A_1), \dots, G(A_{17})$ are non-isomorphic to each other ($G_i = G(A_i)$ in this theorem). Let us prove that in this section.

Calculating the centres of the groups $G(A_1), \dots, G(A_{17})$, we obtain the following results:

$Z(G)$	G
$C_2 \times C_{2^n} \times C_{2^n}$	$G(A_1)$
C_{2^n}	$G(A_{15})$
$C_2 \times C_{2^n}$	$G(A_{13}),\ G(A_{16})$
$C_2 \times C_{2^{n-1}}$	$G(A_{14}),\ G(A_{17})$
$C_{2^{n-1}} \times C_{2^{n-1}}$	$G(A_2),\ G(A_4),\ G(A_9)$
$C_{2^{n-1}} \times C_{2^n}$	$G(A_3),\ G(A_{10})$
$C_2 \times C_2$	$G(A_5),\ G(A_6),\ G(A_7),\ G(A_8),\ G(A_{11}),\ G(A_{12})$

Hence depending on the centre, the groups $G(A_1), \ldots, G(A_{17})$ can be divided into seven classes. Two groups of different classes are non-isomorphic to each other. To prove that two groups inside of a class are non-isomorphic we find the numbers of automorphisms of groups $G(A_2), \ldots, G(A_{14}), G(A_{16})$,
$G(A_{17})$. Doing that we get the following results:

G	$G(A_2)$	$G(A_3)$	$G(A_4)$	$G(A_5)$	$G(A_6)$	$G(A_7)$
$\lvert\mathrm{Aut}(G)\rvert$	$3 \cdot 2^{4n-1}$	2^{4n}	2^{4n-1}	$3 \cdot 2^{6n-3}$	$3 \cdot 2^{6n-5}$	2^{6n-4}

G	$G(A_8)$	$G(A_9)$	$G(A_{10})$	$G(A_{11})$	$G(A_{12})$	$G(A_{13})$
$\lvert\mathrm{Aut}(G)\rvert$	2^{6n-5}	$3 \cdot 2^{4n-2}$	2^{4n-1}	$3 \cdot 2^{6n-6}$	2^{6n-5}	2^{3n}

G	$G(A_{14})$	$G(A_{16})$	$G(A_{17})$
$\lvert\mathrm{Aut}(G)\rvert$	2^{3n+1}	2^{3n+1}	2^{3n}

Since $|\mathrm{Aut}(G(A_8)| = |\mathrm{Aut}(G(A_{12})|$, it is still necessary to check that the groups $G(A_8)$ and $G(A_{12})$ are non-isomorphic. Since the numbers of elements of order two in groups $G(A_8)$ and $G(A_{12})$ are $3+2^{2n-2}$ and $3+2^{2n-1}$, respectively, the groups $G(A_8)$ and $G(A_{12})$ are non-isomorphic. Theorem 1.1 is proved.

References

[1] Coxeter, H.S.M. and Moser, W.O.J., Generators and relations for discrete groups, Springer-Verlag, 1972.

[2] Hall, M., Jr. and Senior, J.K., The groups of order 2^n, $n \leq 6$, Macmillan, New York; Collier-Macmillan, London, 1964.