Bilal Vatansever; David M. Gill; Nuran Eren A new efficient presentation for PSL(2,5) and the structure of the groups G(3,m,n)

Czechoslovak Mathematical Journal, Vol. 50 (2000), No. 1, 67-74

Persistent URL: http://dml.cz/dmlcz/127549

Terms of use:

© Institute of Mathematics AS CR, 2000

Institute of Mathematics of the Czech Academy of Sciences provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.



This document has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* http://dml.cz

A NEW EFFICIENT PRESENTATION FOR PSL(2,5) AND THE STRUCTURE OF THE GROUPS G(3, m, n)

BILAL VATANSEVER, Adana, DAVID M. GILL, Fife, and NURAN EREN, Adana

(Received February 12, 1997)

Abstract. G(3, m, n) is the group presented by $\langle a, b | a^5 = (ab)^2 = b^{m+3}a^{-n}b^ma^{-n} = 1 \rangle$. In this paper, we study the structure of G(3, m, n). We also give a new efficient presentation for the Projective Special Linear group PSL(2, 5) and in particular we prove that PSL(2, 5) is isomorphic to G(3, m, n) under certain conditions.

1. INTRODUCTION

The problem of determining which finite groups are efficient has been investigated using both computational and algebraic techniques. Here we shall also use both techniques. In [10] the structure of the group $\langle a, b | a^7 = (ab)^2 = b^{m+7}a^{-m}b^ma^{-m} =$ 1 \rangle has been studied by Vatansever and Robertson. In [11] the structure of the group $\langle a, b | a^9 = (ab)^2 = b^{m+9}a^{-m}b^ma^{-m} = 1 \rangle$ and in [12] the structure of the group $\langle a, b | a^5 = (ab)^2 = b^{m+5}a^{-m}b^ma^{-m} = 1 \rangle$ has been determined by Vatansever. Some other groups of this type were given in [9].

In this paper, we shall be interested in the group defined by the presentation of the form $\langle a, b \mid a^5 = (ab)^2 = b^{m+3}a^{-n}b^ma^{-n} = 1 \rangle$ where $m, n \in \mathbb{Z}$. We also point out the connection between $\langle a, b \mid a^5 = (ab)^2 = b^{m+3}a^{-n}b^ma^{-n} = 1 \rangle$ and PSL(2,5). We give a new efficient presentation for PSL(2,5).

The notation used in this paper is reasonably standard. For any group G, G' denotes the derived subgroup of G. Let Z(G) denote the center of G where G is a finite group. A group C of maximal order with the properties that there is a subgroup A with $A \leq Z(C) \cap C'$ and $C/A \cong G$ is called a covering group of G. In general C is not unique but A is unique and is called the Schur multiplier M(G) of G. For details see [1, 6, 14]. If G is perfect then it was proved in [2] that G has a unique covering group which we denote by G^- .

Schur [7] showed that any presentation for G with n generators requires at least $n + \operatorname{rank}(M(G))$ relations. If G has a presentation with n generators and precisely $n + \operatorname{rank}(M(G))$ relations we say that G is efficient. Swan in [8] showed that not all finite groups are efficient. He gave examples of solvable groups with trivial multiplier which are not efficient. Further details of such groups are given in [1], [5], [14].

For any integers p, q let (p,q) denote their highest common factor. For any prime number n, define SL(2,n) to be the group of 2×2 matrices with determinant 1 over the field of integers modulo n. Define $SL(2,n) = SL(2,n)/\langle \{\pm I\}\rangle$ where I denotes the identity matrix. If n is an odd prime then the Schur multiplier of PSL(2,n) is \mathbb{Z}_2 and the unique covering group of PSL(2,n) is SL(2,n) (see [5] Teorem 25.7).

2. About program

Here we give some details about the programming language CAYLEY.

CAYLEY is a high level programming language designed to support convenient and efficient computation with other algebraic structures that arise naturally in the study of groups [3].

The following CAYLEY program which will be used in Section 3 has been written in order to find out the structure of the group

$$\langle a, b \mid a^5 = (ab)^2 = (b^2 a^{-1})^2 = b^3 = 1 \rangle.$$

CAYLEY Program:

```
>cayley;
>set workspace=2000000;
>G:free(a,b);
>G.relations: a^5, (a*b)^2, (b^2*a^-1)^2, b^3;
>h=<b>;
>print index(G,h);
>f,i,k=cosact homomorphism(G,h);
>print composition factor(i);
>print order(i);
>print order(i);
>QUIT;
```

3. G(3, m, n) groups

Let G(3, m, n) denote the group with the presentation

 $\langle a, b \mid a^5 = b^{m+3}a^{-n}b^ma^{-n} = (ab)^2 = 1 \rangle.$

Lemma 1. In G(3, m, n) we have:

(i) if (5, n) = d then b^3 commutes with a^d ;

(ii) if (5, n) = 1 then b^3 commutes with a.

Proof. (i): From relation 2, i.e. $b^{m+3}a^{-n}b^ma^{-n} = 1$ we get

(3.1)
$$b^m a^{-n} b^m = b^{-3} a^n,$$

(3.2)
$$b^m a^{-n} b^m = a^n b^{-3}.$$

From (3.1) and (3.2) yield $a^n b^{-3} = b^{-3} a^n$, consequently we get $a^n b^3 = b^3 a^n$. If (5, n) = d, then b^3 commutes with a^d .

(ii) is a special case of (i).

Theorem 1. If $[m \equiv 2 \pmod{3}, m \neq 0 \pmod{5}]$ and $n \equiv 1 \pmod{5}]$ or $[m \equiv 1 \pmod{3}, m \neq 2 \pmod{5}]$ and $n \equiv 4 \pmod{5}]$ then G(3, m, n) is isomorphic to PSL(2,5) and G(3, m, n) has an efficient presentation.

Proof. Case $m \equiv 2 \pmod{3}$, $m \neq 0 \pmod{5}$ and $n \equiv 1 \pmod{5}$. Abelianizing the relations of G(3,m,n) we get $G(3,m,n)/G'(3,m,n) = \langle a,b \mid a^5 = a^2b^2 = b^{2m+3}a^{-2} = aba^{-1}b^{-1} = 1 \rangle$, which is the trivial group. Therefore G(3,m,n) = G'(3,m,n). Since (5,n) = 1 by the above Lemma, b^3 commutes with a and so $b^3 \in Z(G(3,m,n))$. Since $b^3 \in G'(3,m,n)$ we see that $b^3 \in Z(G(3,m,n)) \cap G'(3,m,n)$.

Consider the homomorphic image of G(3, m, n) by $H = \langle b^3 \rangle$, i.e.

$$G(3,m,n)/\langle b^3 \rangle = \langle a,b \mid a^5 = (ab)^2 = (b^2a^{-1})^2 = b^3 = 1 \rangle.$$

Using the CAYLEY program it can be seen that $G(3,m,n)/\langle b^3 \rangle \cong PSL(2,5)$. Since $b^3 \in Z(G(3,m,n)) \cap G'(3,m,n)$ we can deduce that $\langle b^3 \rangle \leq M(PSL(2,5)) \cong \mathbb{Z}_2$. This means $|\langle b^3 \rangle| = 1$ or 2, i.e. $G(3,m,n) \cong PSL(2,5)$ or G(3,m,n) is isomorphic to its covering group SL(2,5).

Assume $(b^3)^2 = 1$ but $b^3 \neq 1$, i.e. $G(3, m, n) \cong SL(2, 5)$.

It can be seen that G(3, m, n) is generated by a and ab, the latter element having order 2. On the other hand, SL(2, 5) has only one element of order 2, so this element has to be ab. However, SL(2, 5) is not generated by the element of order two and one other element. Therefore there is only one possibility which is $G(3, m, n) \cong$ PSL(2, 5).

U

G(3, m, n) has two generators, three relations and the Schur multiplier of G(3, m, n) is \mathbb{Z}_2 . Therefore this presentation for G(3, m, n) is efficient.

Case $[m \equiv 1 \pmod{3}, m \neq 2 \pmod{5} \text{ and } n \equiv 4 \pmod{5}]$:

Claim: If $[m \equiv 1 \pmod{3}, m \neq 2 \pmod{5} \text{ and } n \equiv 4 \pmod{5}]$ then $G(3, m, n) \cong \langle a, b \mid a^5 = (ab)^2 = b^{p+3}a^{-q}b^pa^{-q} = 1 \rangle$; here $p \equiv 2 \pmod{3}, p \neq 0 \pmod{5}$ and $q \equiv 1 \pmod{5}$.

Let $[m \equiv 1 \pmod{3}, m \neq 2 \pmod{5} \text{ and } n \equiv 4 \pmod{5}]$. Then using relation 1, $G(3, m, n) \cong \langle a, b \mid a^5 = (ab)^2 = b^{m+3}a^{-4}b^ma^{-4} = 1 \rangle$.

Using the map $b \longmapsto b^{-1}, a \longmapsto a^{-1}$ we obtain

$$G(3,m,n) \cong \langle a,b \mid a^5 = (ab)^2 = b^{-m-3}a^4b^{-m}a^4 = 1 \rangle.$$

Now let -m = p+3 and -n = q. Since $m \equiv 1 \pmod{3}$ and $m \neq 2 \pmod{5}$, we have $p \equiv 2 \pmod{3}$, $p \neq 0 \pmod{5}$. Since $n \equiv 4 \pmod{5}$, we have $q \equiv 1 \pmod{5}$. Replacing -m with p+3, -n with q in G(3, m, n) and using relation 1 yields the result as claimed.

Before proving Theorem 2 we give some details about the polyhedral group (k, m, n) defined by

$$\langle a, b \mid a^k = b^m = (ab)^n = 1 \rangle.$$

If k, m, n are all greater than 1, then we know that the group (k, m, n) is finite when $\frac{1}{k} + \frac{1}{m} + \frac{1}{n} > 1$ and infinite otherwise [4].

Now we can formulate Theorem 2.

Theorem 2. (i) If $n \equiv 0 \pmod{5}$ and $m \neq -1, -2, -3$ then the group G(3, m, n) is infinite.

(ii) If $n \equiv 0 \pmod{5}$ and (m = -1 or m = -2) then the group G(3, m, n) is trivial. (iii) If $n \equiv 0 \pmod{5}$ and m = -3 then the group G(3, m, n) is PSL(2, 5).

Proof. (i) Let $n \equiv 0 \pmod{5}$ and $m \neq -1, -2, -3$. Using relation 1, we obtain

$$G(3, m, n) \cong \langle a, b \mid a^5 = (ab)^2 = b^{2m+3} = 1 \rangle.$$

By virtue of the above statement about (k, m, n) it can be easily seen that G(3, m, n) is an infinite polyhedral group.

(ii) Let $n \equiv 0 \pmod{5}$ and (m = -1 or m = -2). Using relation 1 we conclude

$$G(3,m,n) \cong \langle a,b \mid a^5 = (ab)^2 = b^{2m+3} = 1 \rangle.$$

If m = -1 or m = -2 then it can be easily seen that G(3, m, n) is the trivial group.

(iii) Let $n \equiv 0 \pmod{5}$ and m = -3. Using relation 1 and m = -3 and rewriting relation 3 as $b^3 = 1$ we get $G(3, m, n) \cong \langle a, b | a^5 = (ab)^2 = b^3 = 1 \rangle$. Hence G(3, m, n) is the group PSL(2, 5) as claimed.

Theorem 3. If $(m \equiv 1 \pmod{3})$ and $n \equiv 1, 2$ or $3 \pmod{5}$ or $(m \equiv 2 \pmod{3})$ and $n \equiv 2, 3$ or $4 \pmod{5}$ then G(3, m, n) is the trivial group.

Proof. Case I ($m \equiv 1 \pmod{3}$) and $n \equiv 1 \pmod{5}$).

Using relation 1 we rewrite relation 3 as $b^{m+3}a^{-1}b^ma^{-1} = 1$. Since (3, m) = 1 by Lemma 1, b^3 commutes with a. Hence

$$\begin{split} b^{2m+2}a^{-1}ba^{-1} &= 1 \\ \Rightarrow b^{2m+3}b^{-1}a^{-1}ba^{-1} &= 1 \\ \Rightarrow b^{2m+3}ab^{2}a^{-1} &= 1 \text{ (using relation 2 as } a^{-1} &= bab) \\ \Rightarrow ab^{2}a^{-1} &= b^{-2}b^{3k} \text{ (where } b^{3k} \text{ is central)} \\ \Rightarrow (ab^{2}a^{-1})^{2} &= (b^{-2}b^{3k})^{2} \\ \Rightarrow ab^{4}a^{-1} &= b^{+2(-2+3k)} \\ \Rightarrow aba^{-1}b^{3} &= b^{+2(-2+3k)} \text{ (using Lemma 1)} \\ \Rightarrow aba^{-1} &= b^{t} \end{split}$$

and $\langle b \rangle \lhd G(3, m, n)$. Now $G(3, m, n)/\langle b \rangle = \langle a, b | a^5 = 1, b = 1, a^2 = 1 \rangle$, therefore $G(3, m, n)/\langle b \rangle$ is the trivial group. Hence G(3, m, n) is a cyclic group and so its order is given by the invariant factors of the relation matrix

$$M = \begin{bmatrix} 5 & 0\\ 2 & 2\\ -2n & 2m+3 \end{bmatrix}.$$

Then 1 is the only invariant factor of M. Hence G(3, m, n) is the trivial group. Case II $(m \equiv 2 \pmod{3})$ and $n \equiv 4 \pmod{5}$.

Claim: If $m \equiv 2 \pmod{3}$ and $n \equiv 4 \pmod{5}$ then G(3, m, n) is isomorphic to $\langle a, b \mid a^5 = (ab)^2 = b^{p+3}a^{-q}b^pa^{-q} = 1 \rangle$, where $p \equiv 1 \pmod{3}$ and $q \equiv 1 \pmod{5}$.

Let $m \equiv 2 \pmod{3}$ and $n \equiv 4 \pmod{5}$, then $G(3, m, n) = \langle a, b \mid a^5 = (ab)^2 = b^{m+3}a^{-4}b^ma^{-4} = 1 \rangle$ by relation 1.

Using the map $b \longmapsto b^{-1}, a \longmapsto a^{-1}$ we get

$$G(3,m,n) \cong \langle a,b \mid a^5 = (ab)^2 = b^{-m-3}a^4b^{-m}a^4 = 1 \rangle.$$

Now let -m = p + 3 and -n = q.

Since $m \equiv 2 \pmod{3}$ we have $p \equiv 1 \pmod{3}$ and since $n \equiv 4 \pmod{5}$ we have $q \equiv 1 \pmod{5}$. Replacing -m = p + 3, -n = q in G(3, m, n) and using relation 1 yields the result as claimed.

Case III $(m \equiv 1 \pmod{3})$ and $n \equiv 2 \pmod{5}$.

In this case the full proof is essentially the same as the proof of Case I, with slight modifications. Therefore it is omitted.

Case IV $(m \equiv 2 \pmod{3})$ and $n \equiv 3 \pmod{5}$.

Claim: If $m \equiv 2 \pmod{3}$ and $n \equiv 3 \pmod{5}$ then G(3, m, n) is isomorphic to $\langle a, b \mid a^5 = (ab)^2 = b^{p+3}a^{-q}b^pa^{-q} = 1 \rangle$, where $p \equiv 1 \pmod{3}$ and $q \equiv 2 \pmod{5}$.

In this case the full proof is essentially the same as the proof of the Case II, therefore it is omitted.

Case V $(m \equiv 1 \pmod{3})$ and $n \equiv 3 \pmod{5}$.

In this case the full proof is essentially the same as the proof of Case I, with slight modifications. Therefore it is omitted.

Case VI $(m \equiv 2 \pmod{3})$ and $n \equiv 2 \pmod{5}$.

Claim: If $m \equiv 2 \pmod{3}$ and $n \equiv 2 \pmod{5}$ then G(3, m, n) is isomorphic to $\langle a, b \mid a^5 = (ab)^2 = b^{p+3}a^{-q}b^pa^{-q} = 1 \rangle$, where $p \equiv 1 \pmod{3}$ and $q \equiv 3 \pmod{5}$.

In this case the full proof is essentially the same as the proof of Case II, therefore it is omitted. $\hfill \Box$

Lemma 2. If $m \equiv 0 \pmod{3}$ and $n \equiv 4 \pmod{5}$ then G(3, m, n) is isomorphic to $\langle a, b \mid a^5 = (ab)^2 = b^{p+3}a^{-q}b^pa^{-q} = 1 \rangle$, where $p \equiv 0 \pmod{3}$ and $q \equiv 1 \pmod{5}$.

Proof. Let $m \equiv 0 \pmod{3}$ and $n \equiv 4 \pmod{5}$. Then $G(3, m, n) = \langle a, b \mid a^5 = (ab)^2 = b^{m+3}a^{-4}b^ma^{-4} = 1 \rangle$ by relation 1.

Using the map $b \mapsto b^{-1}, a \mapsto a^{-1}$ we get $G(3, m, n) \cong \langle a, b \mid a^5 = (ab)^2 = b^{-m-3}a^4b^{-m}a^4 = 1 \rangle$. Now let -m = p+3 and -n = q. Since $m \equiv 0 \pmod{3}$ we have $p \equiv 0 \pmod{3}$ and since $n \equiv 4 \pmod{5}$ we have $q \equiv 1 \pmod{5}$. Replacing -m = p+3, -n = q in G(3, m, n) and using relation 1 yields the result as claimed.

Theorem 4. If $(m \equiv 0 \pmod{3})$ and $n \equiv 1 \pmod{5}$ then

- (i) G(3, m, n) is trivial, where $m \neq 0 \pmod{5}$;
- (ii) G(3, m, n) is \mathbb{Z}_5 , where $m \equiv 0 \pmod{5}$.

Proof. Let $m \equiv 0 \pmod{3}$ and $n \equiv 1 \pmod{5}$. Then $G(3, m, n) = \langle a, b \mid a^5 = (ab)^2 = b^{m+3}a^{-1}b^ma^{-1} = 1 \rangle$ using relation 1. Since (3, 1) = 1 by Lemma 1, b^3 commutes with a. Using this we can rewrite relation 3 as

(3.3)
$$b^{2m+3}a^{-2} = 1$$

 $\Rightarrow a^2 = b^{2m+3}.$

Relation 1 and (3.3) imply that $a = b^{-2(2m+3)}$. Hence G(3, m, n) is a cyclic group and so its order is given by the invariant factors of the relation matrix

$$M = \begin{bmatrix} 5 & 0\\ 2 & 2\\ -2n & 2m+3 \end{bmatrix}.$$

If $m \neq 0 \pmod{5}$, 1 is the only invariant factor of M. Hence G(3, m, n) is the trivial group as claimed in (i).

If $m \equiv 0 \pmod{5}$, 5 is the only invariant factor of M. Hence G(3, m, n) is a cyclic group of order 5, \mathbb{Z}_5 , as claimed in (ii).

Lemma 3. If $m \equiv 0 \pmod{3}$ and $n \equiv 3 \pmod{5}$ then G(3, m, n) is isomorphic to $\langle a, b \mid a^5 = (ab)^2 = b^{p+3}a^{-q}b^pa^{-q} = 1 \rangle$, where $p \equiv 0 \pmod{3}$ and $q \equiv 2 \pmod{5}$.

Proof. Let $m \equiv 0 \pmod{3}$ and $n \equiv 3 \pmod{5}$. Then $G(3, m, n) = \langle a, b \mid a^5 = (ab)^2 = b^{m+3}a^{-3}b^ma^{-3} = 1 \rangle$ by relation 1.

Using the map $b \mapsto b^{-1}, a \mapsto a^{-1}$ we get $G(3, m, n) \cong \langle a, b \mid a^5 = (ab)^2 = b^{-m-3}a^3b^{-m}a^3 = 1 \rangle$. Now let -m = p+3 and -n = q. Since $m \equiv 0 \pmod{3}$ we have $p \equiv 0 \pmod{3}$ and since $n \equiv 3 \pmod{5}$ we have $q \equiv 2 \pmod{5}$. Replacing -m = p+3, -n = q in G(3, m, n) and using relation 1 yields the result as claimed.

Theorem 5. If $(m \equiv 0 \pmod{3})$ and $n \equiv 2 \pmod{5}$ then G(3, m, n) is trivial.

Proof. Let $m \equiv 0 \pmod{3}$ and $n \equiv 2 \pmod{5}$. Then $G(3, m, n) = \langle a, b | a^5 = (ab)^2 = b^{m+3}a^{-2}b^ma^{-2} = 1 \rangle$ by relation 1. Since (3, 1) = 1 by Lemma 1, b^3 commutes with a^2 . Using this we can rewrite relation 3 as

$$b^{2m+3}a^{-4} = 1 \Rightarrow a = b^{-2m-3}$$

(using relation 1).

Hence G(3, m, n) is a cyclic group and so its order is given by the invariant factors of the relation matrix

$$M = \begin{bmatrix} 5 & 0\\ 2 & 2\\ -2n & 2m+3 \end{bmatrix}.$$

If $m \equiv 0 \pmod{3}$ and $n \equiv 2 \pmod{5}$ then 1 is the only invariant factor of M. Hence G(3, m, n) is the trivial group as claimed.

References

- [1] F.R. Beyl and J. Tappe: Group Extensions. Presentations and the Schur Multiplicator. Lecture Notes in Mathematics 958, Springer-Verlag, Berlin, 1982.
- [2] C. M. Campbell and E. F. Robertson: A deficiency zero presentation for SL(2, p). Bull. London Math. Soc. 12 (1980), 17–20.
- [3] J. J. Cannon: An introduction to the group language CAYLEY. Proc. Durham Symposium on Computational Group Theory. Academic Press, London, 1984, pp. 145–183.
- [4] H. S. Coxeter: The binary polyhedral groups and other generalizations of the quaternion group. Duke Math. J. 7 (1940), 367–379.
- [5] B. Huppert: Endliche Gruppen I. Springer, Berlin, 1967.
- [6] G. Karpilovsky: The Schur Multiplier. Oxford University Press, Oxford, 1987.
- [7] I. Schur: Untersuchungen über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen. J. Reine Angew. Math. 132 (1907), 85–137.
- [8] R. G. Swan: Minimal resolutions for finite groups. Topology 4 (1965), 193–208.
- [9] B. Vatansever: Certain Classes of Group Presentations. Ph.D. thesis University of St. Andrews, 1992.
- [10] B. Vatansever and E. F. Robertson: A new efficient presentation for PSL(2, 13) and the structure of the groups G(7, m). Doga-Tr. J. of Mathematics 17 (1993), 148–154.
- [11] B. Vatansever: A new efficient presentation for PSL(2, 37) and the structure of the groups G(9, m). J. Inst. Math. Comput. Sci. Math. Ser. 7 (1994), 207–211.
- [12] B. Vatansever: New efficient presentations for PSL(2,5) and SL(2,5); the structure of the groups G(5,m) and G(m,n,r). Acta Math. Hungar. 71 (1996), 205–210.
- [13] J. W. Wamsley: The Deficiency of Finite Groups. Ph.D. thesis University of Queensland, 1968.
- [14] J. Wiegold: The Schur Multiplier. Groups (St. Andrews, 1981) (C. M. Campbell and E. F. Robertson, eds.). LMS Lecture Notes, 71, Cambridge University Press, 1982, pp. 137–154.

Authors' addresses: B. Vatansever, N. Eren, Department of Mathematics, Faculty of Arts and Sciences, Çukurova University, 01330-Adana, Turkey; D. M. Gill, Department of Mathematical Sciences, University of St Andrews, North Haugh St Andrews, Fife KY169SS, Scotland.