Canad. Math. Bull. Vol. **32** (1) 1989

EFFICIENT PRESENTATIONS OF THE GROUPS $PSL(2, 2p)$ AND $SL(2, 2p)$

BY

E. F. ROBERTSON AND P. D. WILLIAMS

ABSTRACT. Presentations which have a minimal number of defining relations are given for the groups $SL(2, 2p)$ and $PSL(2, 2p)$ where p is a prime greater than 3.

1. **Introduction.** A finite group G is efficient if it has a presentation with n generators and $n + d$ relations where d is the minimal number of elements required to generate the Schur multiplier, $M(G)$, of G. For any positive integer m, define $SL(2, m)$ to be the group of 2×2 matrices with determinant 1 over the ring of integers modulo m. Define $PSL(2, m) = SL(2, m)/\langle \pm I \rangle$ where I denotes the identity matrix.

For p an odd prime, several efficient presentations of $PSL(2, p)$ have been found (see [4], [5]). An efficient presentation of $SL(2, m)$, m odd, appears in [3]. In this paper we shall show the groups $SL(2, 2p)$ and $PSL(2, 2p)$ are efficient where p is an odd prime greater than three. It is well known that $M(PSL(2, 2p)) \cong C_2$ while $M(SL(2, 2p))$ is trivial [2]. Consequently, an efficient presentation of $PSL(2, 2p)$ requires one more relation than generator whereas an efficient presentation of $SL(2, 2p)$ requires an equal number of generators and relations. Notice that in view of the results of [2], on the Schur multiplier of $SL(2, m)$, the deficiency zero presentation in Theorem 4 of this paper is a type of limiting case since, when 4 divides m, $SL(2, m)$ has multiplier C_2 and so cannot be presented with an equal number of generators and relations.

It is well known that, for any $m = p_1^{a_1}p_2^{a_2} \dots p_r^{a_r}$, ($p_i$ distinct primes), $SL(2, m)$ is the direct product of the groups $SL(2, p_i^{a_i})$. In particular, $SL(2, 2p)$ is the direct product of $SL(2, p)$ and S_3, the symmetric group of degree three (since $S_3 \cong SL(2, 2) = PSL(2, 2)$). Similarly, $PSL(2, 2p)$ is the direct product of $PSL(2, p)$ and S_3.

A group C is called a stem extension of the finite group G if $A \leqq Z(C) \cap C'$ with $C/A \cong G$. If, in addition $A \cong M(G)$ then C is a covering group of G. In particular, $PSL(2, 2p)$ has two non-isomorphic covering groups, one of these

Received by the editors September 9, 1986, and, in revised form, November 4, 1987.

AMS Subject Classification (1980): 20F05.

https://doi.org/10.4153/CMB-1989-001-1 Published online by Cambridge University Press

being $SL(2, 2p)$. For any group G, we use G' to denote the derived group of G. We also use the notation $x \leftrightarrow y$ to mean x and y commute.

2. **A presentation of** $PSL(2, 2p)$. Let q be a prime and let $Z^{(q)}$ denote the ring

$$\{x/q^t | x,\ t \text{ integers}\}.$$

A presentation of $SL(2, Z^{(q)})$ was obtained by Behr and Mennicke [1]. By choosing $q = 2$ they obtained a presentation of $PSL(2, p)$, p an odd prime. If one repeats the steps of that paper with $q = 3$ one may obtain the following presentation of $PSL(2, p)$, $p \neq 3$:

$$\langle x, y | x^2 = y^p = (xy)^3 = (xy^3xy^{2\beta})^2 = (xy^3xy^{\beta})^3 = 1\rangle \tag{1}$$

where $3\beta \equiv 1 \pmod p$. We outline this procedure. Using the notation of section 4 of [1] we have that $SL(2, Z^{(3)})$ has defining relations

$$B^2 = (AB)^3,\ B^4 = 1,\ U^{-1}AU = A^9,\ (UB)^2 = B^2$$

$$U^{-1}B^{-1}A^{-3}U^{-1}B^{-1}A^{-3}U^{-1} = A^3B^{-1} \tag{D1}$$

$$U^{-1}B^{-1}A^{-6}U^{-1}B^{-1}A^{-6}U^{-1} = A^2B^{-1}A^2B \tag{D2}$$

$$UA^{-1}BA^8U^{-1} = B^{-1}A^9B^{-1}A \tag{I1}$$

$$UA^{-2}BA^4U^{-1} = BA^4B^{-1}A^{-2}B \tag{I2}$$

$$UA^5BA^{-2}U^{-1} = B^{-1}A^2BA^5B^{-1} \tag{I3}$$

$$UA^3U^{-1}B^{-1}A^{-6}U^{-1} = B^{-1}A^{-3}B^{-1}A^{-1} \tag{L1}$$

$$UA^{-6}U^{-1}B^{-1}A^3U^{-1} = B^{-1}ABA^{-2}B^{-1} \tag{L2}$$

$$UA^3BAB^{-1}A^{-3}U^{-1} = B^{-1}A^{-4}BA^2B^{-1} \tag{M1}$$

$$UA^{-3}BAB^{-1}A^3U^{-1} = B^{-1}A^2BA^{-4}B^{-1}. \tag{M2}$$

The relations of type (G), (N) and the remaining relations of type (I), (L) and (M) are consequences of these relations above and the fact that B^2 is central. For $p \neq 3$, p a prime, the normal closure of $A^p = \left[\begin{smallmatrix}1 & 0\\ p & 1\end{smallmatrix}\right]$ is a full congruence subgroup of $SL(2, Z^{(3)})$ (see [2]) and so adding the relation $A^p = 1$ gives a set of defining relations for $SL(2, p)$. Further, by adding the relation $B^2 = 1$ we obtain a set of defining relations for $PSL(2, p)$. We rewrite (D1) as $(A^3BU)^3 = 1$. The remaining relations (D2)-(M2) are now consequences of the other six relations showing that

$$\begin{aligned} PSL(2, p) \cong \langle A, B, U | A^p = B^2 = (AB)^3 = (UB)^2 \\ = (A^3BU)^3 = 1,\ U^{-1}AU = A^9\rangle. \end{aligned}$$

Let β be the multiplicative inverse of 3 (mod p). Then we rewrite

$$U^{-1}AU = A^9 \quad \text{as } U^{-1}A^{\beta}U = A^3.$$

From $(A^3BU)^3 = 1$ we obtain $U^{-1} = A^3BA^{\beta}BA^3B$. If we eliminate U from this presentation and put $x = B$, $y = A$, we obtain the required presentation (1).

Throughout the rest of this paper we shall use p to denote an odd prime greater than three. Our first theorem gives a two generator, five relation presentation of $PSL(2, 2p)$.

THEOREM 1. *The group*

$$G_p = \langle x, y \mid x^2 = y^{2p} = (xy)^3 = (xy^3xy^{2\beta})^2 = (xy^3xy^{\beta})^3 = 1\rangle$$

where $3\beta \equiv 1 \pmod{2p}$, *is isomorphic to* $PSL(2, 2p)$.

PROOF. Let $z = y^3xy^{\beta}xy^3x \in G_p$. As $xz = xy^3xy^{\beta}xy^3x = y^{-\beta}xy^{-3}xy^{-\beta} = y^{-\beta}(xy^{-3}xy^{-2\beta})y^{\beta}$ then

$$(2) \qquad (xz)^2 = 1.$$

From $y^{-3}zy^{\beta}z^{-1} = (xy^{-\beta}xy^{-3})^3 = 1$ we deduce the relations

$$(3) \qquad z^{-1}yz = y^{\beta^2},\ zyz^{-1} = y^{3^2}.$$

Raising (2) to the power k gives

$$(4) \qquad xz^k = z^{-k}x$$

and conjugation of the relations in (3) by powers of z gives

$$(5) \qquad z^{-k}yz^k = y^{\beta^{2k}},\ z^kyz^{-k} = y^{3^{2k}}.$$

Relations (4) and (5) together with $z^k(yx)^3 = z^k$ give

$$(6) \qquad z^{2k} = y^{3^{2k}}xy^{\beta^{2k}}xy^{3^{2k}}x.$$

Similarly, from $z^{k+1} = z^ky^3xy^{\beta}xy^3x$ we obtain

$$(7) \qquad z^{2k+1} = y^{3^{2k+1}}xy^{\beta^{2k+1}}xy^{3^{2k+1}}x.$$

We combine (6) and (7) into the single relation

$$(8) \qquad z^r = y^{3^r}xy^{\beta^r}xy^{3^r}x.$$

Define $h(k) = 1 - 3 + 3^2 - \dots + (-1)^{k-1}3^{k-1}$ and $g(k) = 1 + 3 + 3^2 + \dots + 3^{k-1}$. An inductive proof shows that

$$(9) \qquad xy^4xy^{h(k)}x = z^{-k}y^{(-3)^kh(k)}xy^{(-\beta)^k4}$$

and

$$(10) \qquad xy^{-2}xy^{g(k)}x = z^{-k}y^{3^kg(k)}xy^{-2\beta^k}.$$

https://doi.org/10.4153/CMB-1989-001-1 Published online by Cambridge University Press

The inductive step for (10) is:

$$\begin{aligned} xy^{-2}xy^{g(k+1)}x &= xy^{-2}xy^{g(k)}x \cdot xy^{3^k}x \\ &= z^{-k}y^{3^k g(k)}xy^{-2\beta^k}z^{-k}y^{-3^k}xy^{-\beta^k} \\ &= z^{-k}y^{3^k g(k)}z^k xy^{-3^{k+1}}xy^{-\beta^k} \\ &= z^{-k}y^{3^k g(k)}z^k z^{-k-1}y^{3^{k+1}}xy^{-2\beta^{k+1}} \\ &= z^{-k-1}y^{3^{k+2}g(k)+3^{k+1}}xy^{-2\beta^{k+1}}. \end{aligned}$$

Suppose s is such that $3^s \equiv \pm 1 \pmod{2p}$. Then from (8) we see that $z^s = 1$. We now consider three cases. If $3^s \equiv 1 \pmod{2p}$ and s is odd then $g(s) \equiv p \pmod{2p}$. From (10) we obtain

$$xy^{-2}xy^p x = y^p xy^{-2}.$$

If $3^s \equiv -1 \pmod{2p}$ and s is even then $g(s) \equiv p - 1 \pmod{2p}$. Again from (10) we have

$$xy^{-2}xy^{p-1}x = y^{p+1}xy^2.$$

Therefore,

$$\begin{aligned} xy^{-2}xy^p &= y^{p+1}xy^2xy \\ &= y^p yxyyxy \\ &= y^p xy^{-2}x \quad \text{using } (xy)^3 = 1. \end{aligned}$$

If $3^s \equiv -1 \pmod{2p}$ and s is odd then $h(s) \equiv p \pmod{2p}$. From (9) we obtain

$$xy^4xy^p x = y^{-p}xy^4 = y^p xy^4.$$

As $y^p \leftrightarrow xy^4x$ then $y^p \leftrightarrow (xy^4x)^{(p+1)/2} = xy^2x$. In all three cases we have shown

$$y^p \leftrightarrow xy^2x \quad \text{and } y^2 \leftrightarrow xy^p x.$$

Let $H = \langle y^2, xy^2x \rangle$ and $K = \langle y^p, xy^p x \rangle$. Then $[H, K] = 1$. Since

$$y = (y^2)^{(p+1)/2}y^p$$

and

$$x = yxyxy = y(xy^2x)^{(p+1)/2}xy^p xy$$

then $G_p = HK$ and $H \lhd G_p$, $K \lhd G_p$. A presentation of G_p/H is obtained by adding the relation $y^2 = 1$ to the relations of G_p. After simplifying the relations, one may obtain the presentation

$$G_p/H \cong \langle x, y \mid x^2 = y^2 = (xy)^3 = 1 \rangle$$

which is isomorphic to S_3. Similarly, by adding $y^p = 1$ to the relations of G_p we obtain a presentation of G_p/K. This presentation reduces to (1) showing $G_p/K \cong PSL(2, p)$. However, in K,

$$\begin{aligned} y^pxy^pxy^p &= y^pxy^{p-1}xxyxy^p \\ &= xy^{p-1}xy^pxyxy^p \quad \text{since } y^p \leftrightarrow xy^2x \\ &= xy^pxyxy^{p+1}xyxy^p \\ &= xy^pxyxy^pxy^{p-1} \\ &= xy^pxy^pxy^px. \end{aligned}$$

As $y^{-p} = y^p$ then $(y^pxy^px)^3 = 1$. Also $(y^p)^2 = (xy^px)^2 = 1$ which shows $K \cong S_3$. The isomorphisms $G_p/H \cong K/(K \cap H) \cong S_3$ imply $H \cap K = 1$. Therefore $G_p = H \times K$ and the proof is complete.

3. **Efficient presentation of** $PSL(2, 2p)$. We now proceed to give an efficient presentation of $PSL(2, 2p)$. The first step is to remove the redundant relation from the presentation given in Theorem 1.

LEMMA 2. *The group* $PSL(2, 2p)$ *may be presented as*

$$\langle x, y | x^2 = y^{2p} = (xy)^3 = (xy^3xy^{2\beta})^2 = 1\rangle$$

where $3\beta \equiv 1 \pmod{2p}$.

PROOF. Let G be the group presented above. By Theorem 1 it is sufficient to show that $(xy^3xy^{\beta})^3 = 1$ holds in G. But

$$\begin{aligned} (xy^3xy^{\beta})^3 &= xy^3xy^{2\beta}y^{-3\beta}y^{2\beta}xy^3xy^{\beta}xy^3xy^{\beta} \\ &= y^{-2\beta}xy^{-3}xy^{-1}xy^{-3}xy^{-2\beta}y^{-\beta}xy^{-3}xy^{-\beta} \\ &= y^{-2\beta}xy^{-3}xy^{-1}xy^{-3}xy^{-1}xy^{-3}xy^{-\beta} \\ &= 1 \end{aligned}$$

on repeated use of $(xy)^3 = 1$ and $y^{3\beta} = y$.

By combining two of the relations in this presentation we are able to give an efficient presentation of $PSL(2, 2p)$. However, to ensure the factor by the derived group is cyclic of order 2 we must consider different cases depending on the congruence class of p modulo 18.

THEOREM 3. $PSL(2, 2p)$ *is efficient. For* $p \not\equiv 1, 5 \pmod{18}$ *then*

$$PSL(2, 2p) \cong \langle x, y | x^2 = (xy)^3 = (xy^3xy^{\alpha})^2y^{2p} = 1\rangle.$$

If $p \equiv 1, 5 \pmod{18}$ *then*

$$PSL(2, 2p) \cong \langle x, y | x^2 = (xy)^3 = (xy^3xy^{\alpha})^2y^{-2p} = 1\rangle.$$

In these presentations the value of α is

$$\alpha = \begin{cases} (4p + 2)/3 & \text{if } p \equiv 1 \pmod 6 \\ (2p + 2)/3 & \text{if } p \equiv 5 \pmod 6. \end{cases}$$

PROOF. We prove the result for $p \not\equiv 1, 5 \pmod{18}$; the other two cases may be proved similarly. Let G^+ be the first of the two groups presented above. As $y^{-2p} = (xy^3xy^\alpha)^2$ then $y^{2p} \leftrightarrow xy^3x$. Further

$$(11) \qquad y^{2p} \leftrightarrow xy^\alpha xy^3xy^{\alpha+2p}x.$$

The conditions on p ensure that either $3|\alpha$ or $3|\alpha + 2p$. So (11) reduces to $y^{2p} \leftrightarrow xyx$ or $xy^{-1}x$ which, on using $(xy)^3 = 1$, shows

$$y^{2p} \leftrightarrow x.$$

If we abelianise the relations of G^+ then we see that $y^{2p} \in G^{+\prime}$. So $\langle y^{2p}\rangle \leqq Z(G^+) \cap G^{+\prime}$. By Lemma 2, $G^+/\langle y^{2p}\rangle \cong PSL(2, 2p)$ which means that G^+ is a stem extension of $PSL(2, 2p)$ and $|\langle y^{2p}\rangle| \leqq 2$. Therefore $y^{4p} = 1$.

Define $z = y^3xy^\beta xy^3x$ where

$$\beta = \begin{cases} (2p + 1)/3 & \text{if } p \equiv 1 \pmod 6 \\ (4p + 1)/3 & \text{if } p \equiv 5 \pmod 6. \end{cases}$$

A proof similar to that of Lemma 2 shows that $(xy^3xy^\beta)^3 = 1$ if $p \equiv 1 \pmod 6$ while $(xy^3xy^\beta)^3 = y^{2p}$ if $p \equiv 5 \pmod 6$. As in the proof of Theorem 1 it may be shown that

$$(xz)^2 = y^{2p}$$

and

$$(12) \qquad z^r = y^{3^r}xy^{\beta^r}xy^{3^r}xy^{2p\delta(r)}$$

where

$$\delta(r) = \begin{cases} 0 & \text{if } r \equiv 0, 1 \pmod 4 \\ 1 & \text{if } r \equiv 2, 3 \pmod 4. \end{cases}$$

Suppose s is such that $3^s \equiv \pm 1 \pmod p$. We consider three cases. If s is odd and $3^s \equiv 1 \pmod p$ then $3^s \equiv \beta^s \equiv 2p - 1 \pmod{4p}$ and $3^{2s} \equiv 1 \pmod{4p}$.

From (12), with $r = s$ we have

$$z^s = (y^{2p-1}x)^3y^{2p\delta(s)} = y^{2p(\delta(s)+1)}$$

and if $r = 2s$ then

$$z^{2s} = (yx)^3y^{2p\delta(2s)} = y^{2p} \quad \text{since } 2s \equiv 2 \pmod 4.$$

https://doi.org/10.4153/CMB-1989-001-1 Published online by Cambridge University Press

Therefore, $y^{2p} = y^{4p(\delta(s)+1)} = 1$. Similarly if s is odd and $3^s \equiv -1 \pmod p$ then $y^{2p} = 1$. If s is even and $3^s \equiv -1 \pmod p$ then $3^s \equiv \beta^s \equiv 2p - 1 \pmod{4p}$. If we let $r = s$ in (12) then

$$z^s = y^{2p(1+\delta(s))}. \tag{13}$$

Also, with $r = s + 1$ in (12),

$$\begin{aligned} z^{s+1} &= y^{-3}xy^{-\beta}xy^{-3}xy^{2p(1+\delta(s+1))} \\ &= xz^{-1}xy^{2p(1+\delta(s+1))} \\ &= zy^{2p\delta(s+1)} \end{aligned}$$

which implies

$$z^s = y^{2p\delta(s+1)}. \tag{14}$$

Relations (13) and (14) imply that $y^{2p} = 1$ since $\delta(s + 1) = \delta(s)$ in this case.

In all three cases the relation $y^{2p} = 1$ holds in G^+. By Lemma 2, $G^+ \cong PSL(2, 2p)$.

4. **An efficient presentation of** $SL(2, 2p)$. We exploit the fact that $SL(2, 2p)$ is a covering group of $PSL(2, 2p)$ in order to give an efficient presentation of $SL(2, 2p)$. As with Theorem 3, the given presentation of $SL(2, 2p)$ depends on the congruence class of p modulo 18.

THEOREM 4. *The group $SL(2, 2p)$ is efficient. If $p \not\equiv 1, 5 \pmod{18}$ then*

$$SL(2, 2p) \cong \langle x, y \mid x^2 = (xy)^3, (xy^3xy^\alpha)^2y^{2p}x^{2m} = 1\rangle$$

where

$$m = \begin{cases} (\alpha + p - 2)/3 & \text{if } p \equiv 7, 17 \pmod{18} \\ (\alpha + p - 4)/3 & \text{if } p \equiv 11, 13 \pmod{18}. \end{cases}$$

If $p \equiv 1, 5 \pmod{18}$ then

$$SL(2, 2p) \cong \langle x, y \mid x^2 = (xy)^3, (xy^3xy^\alpha)^2y^{-2p}x^{2m} = 1\rangle$$

where

$$m = \begin{cases} (\alpha - p - 4)/3 & \text{if } p \equiv 1 \pmod{18} \\ (\alpha - p - 2)/3 & \text{if } p \equiv 5 \pmod{18}. \end{cases}$$

The value of α is as defined in Theorem 3.

PROOF. Let G be either of the groups presented above. The condition on m ensures that $G/G' \cong C_2$. Now $x^2 \leftrightarrow x$ and as $x^2 = (xy)^3$ then $x^2 \leftrightarrow xy$ which shows $x^2 \in Z(G)$. Further, $x^2 \in G'$ and $G/\langle x^2\rangle \cong PSL(2, 2p)$ by Theorem 3. Therefore G is a stem extension of $PSL(2, 2p)$ but cannot be $PSL(2, 2p)$ as G

https://doi.org/10.4153/CMB-1989-001-1 Published online by Cambridge University Press

has too few relations. Moreover, $|G| \leqq 2|PSL(2, 2p)| = |SL(2, 2p)|$. The mapping

$$x \rightarrow \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \; y \rightarrow \begin{pmatrix} -1 & 0 \\ -1 & -1 \end{pmatrix}$$

extends to a homomorphism from G to $SL(2, 2p)$ showing that $G \cong SL(2, 2p)$ as required.

References

1. H. Behr and J. Mennicke, *A presentation of the groups* $PSL(2, q)$, Canad. J. Math. **20** (1968), pp. 1432-1438.

2. F. R. Beyl, *The Schur multiplicator of* $SL(2, Z/mZ)$ *and the congruence subgroup property*, Math. Z. **191** (1986), pp. 23-42.

3. C. M. Campbell and E. F. Robertson, *A deficiency zero presentation for* $SL(2, p)$, Bull. London Math. Soc. **12** (1980), pp. 17-20.

4. ———, *The efficiency of simple groups of order* $<10^5$, Comm. Alg. **10** (1982), pp. 217-225.

5. J. G. Sunday, *Presentations of the groups* $SL(2, m)$ *and* $PSL(2, m)$, Canad. J. Math. **24** (1972), pp. 1129-1131.

Mathematical Institute
University of St Andrews
St Andrews KY16 9SS
Scotland

California State University
San Bernardino
California 92407
U.S.A.

https://doi.org/10.4153/CMB-1989-001-1 Published online by Cambridge University Press