Proceedings of the Edinburgh Mathematical Society (1987) **30**, 143–151

$PSL(2,q)$ AS AN IMAGE OF THE EXTENDED MODULAR GROUP WITH APPLICATIONS TO GROUP ACTIONS ON SURFACES

by DAVID SINGERMAN*

(Received 10th August, 1985)

1. Introduction

The modular group $PSL(2,\mathbb{Z})$, which is isomorphic to a free product of a cyclic group of order 2 and a cyclic group of order 3, has many important homomorphic images. In particular, Macbeath [7] showed that $PSL(2,q)$ is an image of the modular group if $q \neq 9$. (Here, as usual, q is a prime power.) The extended modular group $PGL(2,\mathbb{Z})$ contains $PSL(2,\mathbb{Z})$ with index 2. It has a presentation

$$\langle U, V, W \mid U^2 = V^2 = W^2 = (UV)^2 = (VW)^3 = I \rangle,$$

the subgroup $PSL(2,\mathbb{Z})$ being generated by UV and VW.

A simple group which is an image of $PGL(2,\mathbb{Z})$ is also an image of $PSL(2,\mathbb{Z})$. For many reasons connected with $PSL(2,q)$ actions on surfaces (which we discuss in Section 4) it is important to know when $PSL(2,q)$ is also an image of $PGL(2,\mathbb{Z})$. We will prove

Theorem 1. *$PSL(2,q)$ is a homomorphic image of the extended modular group for all q except for $q=7$, 11 and 3^n, where $n=2$ or n is odd.*

The case where q is a prime $\equiv 1 \bmod 4$ or $q = 2^m$ were proved in [**5**] and [**3**]. Some other cases appear in [**4**].

2. Antipodal generating sets

Theorem 1 follows from a result, given in Theorem 2, which applies to a wider class of groups, namely groups with two generators A, B with $A^2 = I$ (i.e. images of Hecke groups). We call $\{A, B\}$ an *antipodal generating set* if there exists $Z \in G = gp\ \langle A, B\rangle$ such that

$$Z^2 = (AZ)^2 = (BZ)^2 = I.$$

*This paper forms part of the Proceedings of the conference Groups–St Andrews 1985.

(The motivation for this terminology appears in Section 4.)

It is useful to note the following:

Lemma A. *Let B have order 3 so that G is an image of the modular group. If $\{A, B\}$ is an antipodal generating set then G is an image of the extended modular group.*

Proof. If $\{A, B\}$ is an antipodal generating set then G is generated by A, B, Z obeying

$$A^2 = B^3 = Z^2 = (AZ)^2 = (BZ)^2 = I$$

so that $U \to AZ$, $V \to Z$, $W \to BZ$ extends to a homomorphism from $PGL(2, \mathbb{Z})$ onto G. □

Now suppose that $PSL(2, q)$ is generated by A, B with $A^2 = I$. Then by conjugating we may assume that

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

(representing the elements of $PSL(2, q)$ by matrices in the usual way).

Let $$B = \begin{pmatrix} x & y \\ z & w \end{pmatrix}, \ xw - yz = 1 \quad \text{so that} \quad AB = \begin{pmatrix} z & w \\ -x & -y \end{pmatrix}.$$

Write $z + w = \beta$, $z - y = \gamma$. Then following Macbeath [7] we associate to the pair $\{A, B\}$ the quadratic form

$$Q(\xi, \eta, \zeta) = \xi^2 + \eta^2 + \zeta^2 + \beta\xi\eta + \gamma\xi\zeta.$$

(More generally there is a term in $\eta\zeta$ whose coefficient is the trace of A.)

If q is not a power of 2 then the discriminant of this form is

$$\Delta = \Delta(A, B) = \begin{vmatrix} 1 & \beta/2 & \gamma/2 \\ \beta/2 & 1 & 0 \\ \gamma/2 & 0 & 1 \end{vmatrix} = 1 - \beta^2/4 - \gamma^2/4.$$

We then have:

Theorem 2. *Let $PSL(2, q)$, $(q \neq 2^n)$, be generated by A, B as above. Then $\{A, B\}$ is an antipodal generating set if and only if Δ is a square in $GF(q)$.*

Proof. We suppose first that $\{A, B\}$ is an antipodal generating set. Then there exists $Z \in PSL(2, q)$ with

$$Z^2 = (AZ)^2 = (BZ)^2 = I.$$

An element of $PSL(2, q)$ of order 2 has zero trace so that trace Z = trace AZ = trace $BZ = 0$. From trace Z = trace $AZ = 0$ we get

$$Z = \begin{pmatrix} a & b \\ b & -a \end{pmatrix}, \quad a^2 + b^2 = -1$$

and trace $BZ = 0$ gives

$$a(x-w) + b(y+z) = 0 \tag{1}$$

Thus $b^2(y+z)^2 = (-1-b^2)(x-w)^2$ and hence $b^2((y+z)^2 + (x-w)^2) = -(x-w)^2$.

Using $xw - yz = 1$ we obtain

$$b^2((w+x)^2 + (y-z)^2 - 4) = -(x-w)^2$$

so that

$$b^2(\beta^2 + \gamma^2 - 4) = -(w-x)^2$$

and thus

$$4b^2\Delta = (w-x)^2.$$

Therefore if $b \neq 0$, Δ is a square in $GF(q)$.

If $b = 0$ then $a^2 = -1$ so that -1 is a square. From (2), $x = w$ which gives

$$\Delta = 1 - x^2 - \frac{(z-y)^2}{4} = -\tfrac{1}{4}(y+z)^2$$

and as -1 is a square, Δ is a square.

For the converse we suppose that Δ is a square in $GF(q)$. As A and B generate $PSL(2, q)$ it follows by Theorem 2 of [7] that $\Delta \neq 0$. To prove the existence of a matrix Z with $Z^2 = (AZ)^2 = (BZ)^2 = I$ we need to find $a, b \in GF(q)$ such that $a^2 + b^2 = -1$ and (1) holds.

We assume first that $x \neq w$. Then we can find $a_1, b_1 \in GF(q)$ such that

$$a_1(x-w) + b_1(y+z) = 0, \qquad (b_1 \neq 0).$$

Then

$$\frac{a_1^2 + b_1^2}{b_1^2} = \frac{(x-w)^2 + (y+z)^2}{(x-w)^2} = \frac{-4\Delta}{(x-w)^2}$$

so that $d = -(a_1^2 + b_1^2)$ is a non-zero square.

https://doi.org/10.1017/S001309150001806X Published online by Cambridge University Press

Let $a=a_1/\sqrt{d}$, $b=b_1/\sqrt{d}$, then

$$a^2+b^2=-1, \quad a(x-w)+b(y+z)=0$$

as required.

If $x=w$ then

$$\Delta=\frac{-(y+z)^2}{4}$$

and as Δ is a square, -1 is also a square. Then

$$Z=\begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix} \in PSL(2,q)$$

and obeys $Z^2=(AZ)^2=(BZ)^2=I$. Thus in both cases $\{A,B\}$ is an antipodal generating set. □

We have a corresponding result for $p=2$. We now use the quadratic form directly.

Theorem 3. *Let $PSL(2,2^n)$ be generated by $\{A,B\}$ with $A^2=I$. Then $\{A,B\}$ is an antipodal generating set.*

Proof. By [7] Theorem 2, the quadratic form

$$Q(\xi,\eta,\zeta)=\xi^2+\eta^2+\zeta^2+\beta\zeta\eta+\gamma\xi\gamma$$

is non-singular. Now the form is singular if and only if there is a factorization

$$Q(\xi,\eta,\zeta)=(\xi+v\eta+u\zeta)(\xi+v^{-1}\eta+u^{-1}\zeta)$$

where if necessary u,v lie in the quadratic extension of $GF(2^n)$.

If $\beta=\gamma$ then such a factorization is possible

$$\xi^2+\eta^2+\zeta^2+\beta\xi\eta+\beta\xi\gamma=(\xi+u\eta+u\zeta)(\xi+u^{-1}\eta+u^{-1}\zeta)$$

where $u+u^{-1}=\beta$, so that for a non-singular form with coefficients in $GF(2^n)$, $\beta\neq\gamma$ and hence $x-w\neq y+z$. We can now find $a_1,b_1\in GF(2^n)$ satisfying

$$a_1(x-w)+b_1(y+z)=0, \qquad a_1\neq b_1.$$

As $a_1^2+b_1^2=d$ is a non-zero square (as all elements of $GF(2^n)$ are squares) we let $a=a_1/\sqrt{d}$, $b=b_1/\sqrt{d}$. Then

$$a(x-w)+b(y+z)=0, \quad a^2+b^2=-1$$

which, as we have seen, shows that $\{A,B\}$ is an antipodal generating set. □

3. The proof of Theorem 1

Our deduction depends heavily on the results of Macbeath's paper [7]. The question answered there was to find the subgroup generated by two non-identity elements A, $B \in PSL(2,q)$ and in particular to see when A, B generate the whole group. Because of our interests we shall assume that A has order 2 and B has order 3 (so that trace $A=0$ and trace $B=\pm 1$). In Theorem 6 of [7] it is shown that if $q \neq 9$ then such a generating pair exists. In the case when q is a power of 2, Theorem 1 now follows from Theorem 3 and Lemma A. From now on we will assume that q is not a power of 2 so we can consider the discriminant $\Delta(A, B)=\frac{1}{4}(3-\gamma^2)$.

In [7] it is shown that either

(i) AB has order 2, 3, 4, or 5; or

(ii) $\Delta(A, B)=0$; or

(iii) A, B generate a projective subgroup of $PSL(2,q)$.

(i) and (ii) correspond to the exceptional and singular cases of Macbeath's classification and in (iii) the projective subgroup is isomorphic to either $PSL(2,q_1)$ or $PGL(2,q_2)$ where q_1 and q_2 divide q.

We need to know when A, B generate the whole of $PSL(2,q)$. This occurs if $\gamma=$ trace AB does not belong to a proper subfield of $GF(q)$ and if γ^2 is not a non-square in $GF(\sqrt{q})$. This final condition only makes sense, of course, if q is a square. It is included because if γ does not belong to a proper subfield of $GF(q)$ but γ^2 is a non-square in $GF(q)$ then A, B may generate a subgroup isomorphic to $PGL(2, \sqrt{q})$.

Now (i) and (ii) can be formulated in terms of the trace γ. For AB has order 2, 3, 4 or 5 if and only if $\gamma^2=0, 1, 2$ or $\gamma^2 \pm \gamma - 1 = 0$ respectively and $\Delta(A, B)=0$ if and only if $\gamma^2=3$.

Let us call an element $\gamma \in GF(q)$ *admissible* if

(a) $\gamma^2 \neq 0, 1, 2, 3$ or $\gamma^2 \pm \gamma - 1 \neq 0$,

(b) γ does not belong to a proper subfield of $GF(q)$,

(c) γ^2 is not a non-square in $GF(\sqrt{q})$.

Given an admissible $\gamma \in GF(q)$ we know by Theorem 1 of [7] that there exist $A, B \in PGL(2,q)$ with $A^2=B^3=I$ and trace $AB=\gamma$ and then A, B generate $PSL(2,q)$. Furthermore, by Theorem 2, $\{A, B\}$ is an antipodal generating set if and only if $4\Delta(A, B)=3-\gamma^2$ is a square in $GF(q)$. By Lemma A we deduce

Lemma B. *$PSL(2,q)$ is an image of the extended modular group if there exists $A, B \in PSL(2,q)$ with $A^2=B^3=I$, $\gamma=$ trace AB is admissible and $3-\gamma^2$ is a square where $\gamma=$ trace AB.*

Corollary ([5]). *If $p \equiv 1 \bmod 4$ is prime then $PSL(2,p)$ is an image of the extended modular group.*

https://doi.org/10.1017/S001309150001806X Published online by Cambridge University Press

Proof. By reduction mod p of the "standard" generators of $PSL(2, \mathbb{Z})$ we know that

$$A=\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad B=\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$$

generate $PSL(2,q)$ with $A^2=B^3=I$. As $\gamma=\text{trace } AB=2, 3-\gamma^2=-1$ which is a square in $GF(p)$ as $p\equiv 1 \bmod 4$. Also 2 is admissible in $GF(p)$ (for $p\equiv 1 \bmod 4$) except when $p=5$; but in this case $A^2=B^3=(AB)^5=I$ so that A, B generate $PSL(2,5)\cong A_5$. The result follows from Lemma B.

We now prove Theorem 1. We have already considered the case $p=2$ and we shall deal with $p=3$ later, so we assume that $q=p^n$, $p>3$. Now $3-\gamma^2$ is a square if and only if there exists $\mu\in GF(q)$ such that $\gamma^2+\mu^2=3$. Let C denote the conic $x^2+y^2=3$ defined over $GF(q)$. By Dickson ([**2**], §64) we find that C has s points on it where

$$s=\begin{cases} q+1 & \text{if } -1 \text{ is not a square in } GF(q) \\ q-1 & \text{if } -1 \text{ is a square in } GF(q). \end{cases}$$

Now if 3 is not a square in $GF(q)$ then for each γ such that $3-\gamma^2$ is a square there are two values of μ such that $(\gamma,\mu)\in C$. If 3 is a square then $(\sqrt{3},0)$, $(-\sqrt{3},0)\in GF(q)$ and then for every value of $\gamma\neq\pm\sqrt{3}$ such that $3-\gamma^2$ is a square there are two values of μ such that $(\gamma,\mu)\in C$. Thus we find that the number of $\gamma\in GF(q)$ such that $3-\gamma^2$ is a square is

$$t=\begin{cases} s/2 & \text{if 3 is not a square in } GF(q) \\ 1+(s/2) & \text{if 3 is a square in } GF(q). \end{cases}$$

We thus obtain

Lemma C. *The number of values of $\gamma\in GF(q)$ such that $3-\gamma^2$ is a square is*

$$\begin{cases} (q+1)/2 & \textit{if } -3 \textit{ is a square} \\ (q+3)/2 & \textit{if } -1 \textit{ is a non-square, } 3 \textit{ is a square} \\ (q-1)/2 & \textit{if } -1 \textit{ is a square, } 3 \textit{ is a non-square.} \end{cases}$$

At any rate, the number of values of γ such that $3-\gamma^2$ is a square is not less than $(q-1)/2=(p^n-1)/2$.

Now the number of values of γ not obeying (a) is at most 11, the number of values of γ not obeying (b) is p^{n-1} and the number of values of γ not obeying (c) is $\varepsilon p^{n/2}$ where $\varepsilon=1$ if n is even and $\varepsilon=0$ if n is odd. Thus the number of non-admissible $\gamma\in GF(q)$ is at most

$$p^{n-1}+\varepsilon p^{n/2}+11.$$

Hence by Lemmas B and C it follows that if

$$\frac{p^n-1}{2}>p^{n-1}+\varepsilon p^{n/2}+11$$

https://doi.org/10.1017/S001309150001806X Published online by Cambridge University Press

then $PSL(2, q)$ is an image of the extended modular group. This is true for all values of $p^n > 25$ except for 49. As we are assuming that $p \neq 2$ or 3 and as we have dealt with the case when $q = p \equiv 1 \bmod 4$ in the corollary to Lemma B we need only consider the cases where $p^n = 49$, 25, 23 or 19. We do this in the table where, in each case, we list a point $(\gamma, \mu) \in C$, where γ is admissible.

q	(γ, μ)
49	$(2-2\sqrt{5}, 3-\sqrt{5})$
25	$(1+2\sqrt{2}, -1+2\sqrt{2})$
23	$(13,15)$
19	$(6, 9)$

We now deal with $q = 3^n$. As $PSL(2, 3) \cong A_4$, all its involutions lie in the subgroup of order 4 so it is not an image of the extended modular group; nor is $PSL(2, 9)$, as it is not an image of the modular group ([7], Theorem 6) and it is simple. Thus we can assume that $n > 2$. Then, as above, we see that there are many admissible γ in $GF(3^n)$. Now $3 - \gamma^2 = -\gamma^2$ is a square if and only if -1 is a square. As the multiplicative group of $GF(q)$ is cyclic of order $q - 1$ this occurs if and only if $q \equiv 1 \bmod 4$, i.e. n is even.

Finally, we note that $PSL(2, 7)$ and $PSL(2, 11)$ are not images of the extended modular group. In both cases all points on the conic $x^2 + y^2 = 3$ correspond to non-admissible γ. For example, when $q = 7$ we find that $\gamma = 1, 3, 4, 6$. As $1^2 = 6^2 = 1$ and $3^2 = 4^2 = 2$, we see that $(AB)^3 = I$ or $(AB)^4 = I$ so the whole group is not generated.

4. Applications to group actions on surfaces

(a) If G is a finite group with generators $\{A, B\}$ satisfying $A^2 = B^m = (AB)^n = I$ then there is a regular map $\mathscr{M}$ of type $\{m, n\}$ on a compact orientable surface X which admits G as a group of sense-preserving automorphisms. If $m = 3$ then we can choose $\mathscr{M}$ be a triangulation. If $\{A, B\}$ is an antipodal generating set then there is also a regular map $\mathscr{N}$ on a non-orientable surface Y which also admits G as a group of automorphisms, ([1], §8.1). Here X is the canonical two-sheeted orientable cover of Y and $\mathscr{M}$ is the lift of $\mathscr{N}$ to X. The surface X then admits a sense-reversing fixed-point free homeomorphism of order two (the covering transformation) which is also an automorphism of $\mathscr{M}$. The elements of G commute with this covering transformation so that $C_2 \times G$ is a group of automorphisms of $\mathscr{M}$.

An example of this situation is given by the icosahedron. This admits $A_5 \cong PSL(2, 5)$ as its automorphism group. By Theorem 1, $PSL(2, 5)$ has an antipodal generating set $\{A, B\}$ with $A^2 = B^3 = (AB)^5 = I$ so that there is a regular map of type $\{3, 5\}$ on the projective plane and the covering transformation is the antipodal map of the sphere which is a sense-reversing automorphism of order two of the icosahedron. By contrast, $A_4 \cong PSL(2, 3)$ does not admit any antipodal generating set $\{A, B\}$ with $A^2 = B^3 = I$. This corresponds to the tetrahedron *not* admitting a fixed-point free sense-reversing automorphism of order two. (It does admit a sense-reversing automorphism of order two which does have fixed points.) More generally all the groups of Theorem 1 give regular triangular maps on non-orientable surfaces, or equivalently, regular maps on orientable surfaces which admit a sense-reversing fixed-point free automorphism of order two, which we can regard as a generalized antipodal map.

(b) If G is a group of automorphisms of a regular map on an orientable surface X then we can also regard G as acting as a group of conformal automorphisms of some Riemann surface homeomorphic to X ([**9**], §8). The groups of Theorem 1 then give a class of Riemann surfaces admitting a fixed-point free anticonformal involution (or *symmetry* as it is called in [**9**]) and the groups then act as dianalytic automorphisms on the non-orientable Klein surfaces without boundary obtained as the quotient of X by the symmetry. A particularly interesting case is that of the *Hurwitz groups* when A has order 2, B has order 3 and AB has order 7, for these act as groups of $84(g-1)$ conformal automorphisms of a surface of genus g, the maximum possible number. In [**7**], Theorem 8, it is proved that $PSL(2,q)$ is a Hurwitz group if and only if $q=7$, $q=p\equiv\pm1 \bmod 7$ or $q=p^3$, $p\equiv\pm2,\ \pm3 \bmod 7$. If $\{A,B\}$ generates such a group G with $A^2=B^3=(AB)^7=I$ then by Theorem 2 we deduce that G acts as a "maximal" group of dianalytic automorphisms of a non-orientable Klein surface without boundary iff $3-\gamma^2$ is a square in $GF(q)$, a result already found by Wendy Hall in her Southampton thesis [**6**]. (Also see [**8**].) She used this result to show that this occurs if and only if $q=p\equiv1$ or $13 \bmod 28$ or $q=p^3$, where $p=2$ or $p\equiv5, 9, 17$ or $25 \bmod 28$.

(c) An image of the extended modular group for which the elements U, V, W, UV, VW (in the presentation of Section 1) do not map to the identity is called an M^*-group. These groups occur as $12(g-1)$ dianalytic automorphisms of a bordered compact Klein surface of algebraic genus g, the maximum possible number ([**3**], [**5**]). All the groups of Theorem 1 are M^*-groups with the exception of $PSL(2,2)\cong S_3$.

Acknowledgement. I would like to thank the referee whose suggestion, to count the number of points on the conic, enabled me to considerably strengthen my original Theorem 1.

REFERENCES

1. H. S. M. Coxeter and W. O. J. Moser, *Generators and relations for discrete groups* (Springer-Verlag 1965).

2. L. E. Dickson, *Linear groups with an exposition of the Galois field theory* (Leipzig 1901; reprinted by Dover, 1960).

3. J. J. Etayo-Gordejuela, Klein surfaces with maximal symmetry and their groups of automorphisms, *Math. Ann.* **268** (1984), 533–538.

4. J. J. Etayo-Gordejuela and C. Perez-Chirinos, Bordered and unbordered Klein surfaces with maximal symmetry, *J. Pure Appl. Algebra* **42** (1986), 29–35.

5. N. Greenleaf and C. L. May, Bordered Klein surfaces with maximal symmetry, *Trans. Amer. Math. Soc.* **274** (1982), 265–283.

6. W. Hall, *Automorphisms and coverings of Klein surfaces* (Thesis, University of Southampton, 1978).

7. A. M. MACBEATH, *Generators of the linear fractional groups* (Proc. Symp. Pure Math. Houston 1967).

8. D. SINGERMAN, Automorphisms of compact non-orientable Riemann surfaces, *Glasgow Math. J.* **12** (1971), 50–59.

9. D. SINGERMAN, Symmetries of Riemann surfaces with large automorphism group, *Math. Ann.* **210** (1974), 17–32.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF SOUTHAMPTON
SOUTHAMPTON SO9 5NH