The Genus of $SL_2(F_q)$

SHU-NAN VOON

1. Introduction

Hurwitz showed that the group of (conformal) automorphisms of a compact Riemann surface has order less than or equal to $84(g-1)$, provided that $g \geq 2$. More generally, Greenberg [7] showed that given any nontrivial finite group G and any closed Riemann surface S, there exists a closed Riemann surface T and a normal branched covering T of S, whose group of covering transformations is isomorphic to G, and is the full group $\mathrm{Aut}(T)$ of conformal automorphisms of T. This opens up a related question: Given a finite group, what is the minimum genus of a surface for which this is a group of automorphisms? This has been solved completely for the following series of groups: cyclic [8], abelian [14], $PSL_2(q)$ [4; 5], and alternating [1]. More recently, Conder, Wilson, and Woldar [2] have computed the minimum genera of the sporadic simple groups, except the Fischer Fi_{23}, the Monster M, and the Baby Monster B. Here we take up the unimodular linear group $SL_2(q)$ over a finite field of q elements, where $q = p^n$. Moreover, we also compute the corresponding group $\mathrm{Aut}(S_g)$, where S_g is any Riemann surface of least genus on which $SL_2(q)$ acts. By definition, the (strong symmetric) genus of a finite group G is the least integer g so that G acts, as a group of homeomorphisms, effectively and orientably on the closed orientable surface S_g. According to the positive solution of the Nielsen realization problem [9], the surface S_g may be given a Riemann structure such that G acts on the Riemann surface S_g conformally. In other words, we may assume that G acts effectively on a closed Riemann surface S_g as a group of (conformal) automorphisms of S_g.

Let D be the upper half-plane, $\{z \in \mathbf{C}: \mathrm{Im}(z) > 0\}$. Any conformal automorphism of D is a Möbius transformation of the form

$$w = \frac{az+b}{cz+d},$$

where $a, b, c, d \in \mathbf{R}$ with $ad-bc=1$. Thus, the group of conformal automorphisms of D can be identified with the Lie group $PSL_2(\mathbf{R})$. A discrete subgroup Γ of $PSL_2(\mathbf{R})$ is called a *Fuchsian* group. We will be concerned

Received February 6, 1992.
Michigan Math. J. 40 (1993).

only with those Fuchsian groups for which the orbit spaces D/Γ are compact. Such a group is called a *cocompact* Fuchsian group, and is known to have the following presentation.

Generators: $a_1, b_1, a_2, b_2, \ldots, a_h, b_h, c_1, c_2, \ldots, c_s$.

Relations: $[a_1, b_1][a_2, b_2]\cdots[a_h, b_h]c_1c_2\cdots c_s = c_1^{m_1} = c_2^{m_2} = \cdots = c_s^{m_s} = 1$.

Here, $[a, b] = aba^{-1}b^{-1}$. In particular, if Γ is torsion-free then Γ is isomorphic to the fundamental group of a compact orientable surface of genus h. Thus, a torsion-free Fuchsian group is a surface group. Another important type of Fuchsian group occurs when the orbit genus $h = 0$ and the number of branched points $s = 3$. These are known as *triangle* groups and will be denoted by $T(r, s, t)$, where r, s, t are the periods.

Using results of MacBeath [13], we show that $SL_2(q)$ can be generated by an (r, s, t)-triple, as defined below, and hence $SL_2(q)$ acts on some compact Riemann surface of genus g, with S^2 as the orbit space and $2g-2 = |SL_2(q)|(1-1/r-1/s-1/t)$. Next we show that if g is the genus of $SL_2(q)$ then there is a regular branched covering $S_g \xrightarrow{\pi} S^2$ with three branch points, and as a consequence we obtain the following genus formula

$$2(\text{genus}(SL_2(q))-1) = |SL_2(q)| \min_{(r,s,t)}(1-1/r-1/s-1/t),$$

where the minimum is taken over all triples of integers (r, s, t) for which $SL_2(q)$ admits a generating (r, s, t)-triple.

Before we state our main results, we will need a couple of definitions.

DEFINITION 1.1. Given a triple (r, s, t) of integers, an (r, s, t)-*triple* of a group G is a triple (A, B, C) of elements of G of respective orders (r, s, t) such that $ABC = 1$.

DEFINITION 1.2. Given a prime power p^n, $d \equiv d_n$ denotes the smallest integer satisfying the following conditions:

(i) $d \mid p^n - 1$ or $d \mid p^n + 1$;

(ii) $d \nmid p^m \pm 1$ for all $m \mid n$, $m \neq n$;

(iii) $d \neq 2, 3, 4, 6$.

Since $SL_2(2^n) = PSL_2(2^n)$, and since the genus of $PSL_2(2^n)$ has been determined by Glover and Sjerve [5], in what follows we will restrict ourselves to the odd characteristic p.

TERMINOLOGY. The genus of a finite group G is said to be *determined by* an (r, s, t)-triple if there exists a generating (r, s, t)-triple for G satisfying $2(\text{genus}(G)-1) = |G|(1-1/r-1/s-1/t)$.

THEOREM 1.3. *The genus of* $SL_2(p)$ *is determined by the following triple:*

(i) $(3, 3, 4)$ *when* $p = 3$;

(ii) $(3, 4, 5)$ *when* $p = 5$;

(iii) $(3, 3, d)$ *when* $p \geq 7$.

THEOREM 1.4. *The genus of $SL_2(p^6)$ is determined by a $(3,5,7)$-triple if $d \geq 105$, and by a $(3,3,d)$-triple if $d \leq 105$.*

REMARK. In Voon [16], Warren Sinnott shows that there are infinitely many primes p such that if d is the smallest integer with the properties

(i) $d \mid p^6-1$ or $d \mid p^6+1$ and
(ii) $d \nmid p^3 \pm 1$, $d \nmid p^2 \pm 1$,

then $d > 105$. Similarly, there are infinitely many primes for which $d \leq 105$.

THEOREM 1.5. *The genus of $SL_2(p^n)$, $2 \leq n \neq 6$, is determined by a $(3,3,d)$-triple.*

Finally, we compute the full group $\mathrm{Aut}(S_g)$ of automorphisms of the Riemann surface S_g, where $g = \mathrm{genus}(SL_2(p^n))$. It should be kept in mind that the Riemann structure on S_g is given by a short exact sequence of groups $\Delta \to T(r,s,t) \xrightarrow{\theta} SL_2(p^n)$, where θ is period-preserving and g is determined by an (r,s,t)-triple of the group $SL_2(p^n)$. Thus, the Riemann structure on S_g is the unique structure which makes the map $S_g \cong D/\Delta \xrightarrow{\pi} D/T(r,s,t) \cong \mathbf{C}P^1$ analytic. With this understanding, the results are summarized in the following theorem.

THEOREM 1.6. (a) *Let $g = \mathrm{genus}(SL_2(p^n))$. If g is determined by a $(3,3,d)$-triple, then $\mathrm{Aut}(S_g)$ is isomorphic to a subgroup of $GL_2(p^{2n})$ which is a 2-fold extension of $SL_2(p^n)$. Indeed, $\mathrm{Aut}(S_g) \cong SL_2(p^n)\colon \mathbf{Z}_2$, a semidirect product. Moreover, for $d \mid p^n-1$,*

$$\mathrm{Aut}(S_g) \cong SL_2^{\pm}(p^n)$$

$(\{A \in GL_2(F_q) \mid \det(A) = \pm 1\})$ if and only if $2d \mid p^n-1$; for $d \mid p^n+1$,

$$\mathrm{Aut}(S_g) \cong SL_2^{\pm}(p^n)$$

if and only if $2d \nmid p^n+1$.

(b) *If $g = \mathrm{genus}(SL_2(3))$, then $\mathrm{Aut}(S_g) \cong SL_2^{\pm}(3)$.*

(c) *If $g = \mathrm{genus}(SL_2(5)$, then $\mathrm{Aut}(S_g) \cong SL_2(5)$.*

(d) *Let $g = \mathrm{genus}(SL_2(p^6))$. If $d \leq 105$ then $\mathrm{Aut}(S_g) \cong SL_2(p^6)\colon \mathbf{Z}_2$. If $d > 105$ then $\mathrm{Aut}(S_g) \cong SL_2(p^6)$.*

In contrast, we would like to mention the following conjecture proposed by Glover.

CONJECTURE (Glover). Let G be a finite simple group and let S be a surface of least genus on which G acts. Then $S/G \cong S^2$, $S \to S/G$ is a three-point branched covering, and S can be chosen as a Riemann surface such that $\mathrm{Aut}(S) \cong G$.

2. Preliminary Results

In this section, we collect the background material concerning the subgroup structure of $PSL_2(p^n)$ as outlined in [5]. This is followed by the methods of determination of various subgroups of $PSL_2(p^n)$, as developed in [13]. We begin with an elementary lemma which will be useful in our later investigations of generators of $SL_2(p^n)$.

LEMMA 2.1. *Let* $|A|$ *denote the order of an element* A *of* $SL_2(p^n)$, *and let* $\alpha = \operatorname{tr} A$.

(a) $|A|=3 \Leftrightarrow \alpha=-1$.
(b) $|A|=4 \Leftrightarrow \alpha=0$.
(c) $|A|=5 \Leftrightarrow \alpha^2+\alpha-1=0$.
(d) $|A|=6 \Leftrightarrow \alpha=1$.
(e) $|A|=7 \Leftrightarrow \alpha^3+\alpha^2-2\alpha-1=0$.
(f) $|A|=8 \Leftrightarrow \alpha^2=2$.
(g) $|A|=9 \Leftrightarrow \alpha^3-3\alpha^2+1=0$.
(h) $|A|=10 \Leftrightarrow \alpha^2-\alpha-1=0$.
(i) $|A|=11 \Leftrightarrow \alpha^5+\alpha^4-4\alpha^3-3\alpha^2+3\alpha+1=0$.
(j) $|A|=p \Leftrightarrow A \neq 1$ *and* $\alpha=2$.

These are easily established by the following observation: Given $A \in SL_2(p^n)$, the characteristic polynomial of A is $x^2-\alpha x+1$. Therefore, $A^2=\alpha A-1$. Define recursively the polynomials $S_n(x)$ over F_p as follows: $S_1(x)=1$, $S_2(x)=x$, and $S_n(x)=xS_{n-1}(x)-S_{n-2}(x)$. Thus, $A^2=S_2(\alpha)A-S_1(\alpha)$, and, by induction, $A^n=S_n(\alpha)A-S_{n-1}(\alpha)$, of which the following lemma is an immediate consequence (cf. [11]).

LEMMA 2.2. *Let* $A \in SL_2(p^n)$, $A \neq \pm 1$, *and* $\operatorname{tr} A=\alpha$. *Then:*

(a) $A^n=1 \Leftrightarrow S_n(\alpha)=0$ *and* $S_{n-1}(\alpha)=-1$;
(b) $A^n=-1 \Leftrightarrow S_n(\alpha)=0$ *and* $S_{n-1}(\alpha)=1$.

Proof of Lemma 2.1. (a)–(i) All of these may be easily verified by the above lemma and the following list of the polynomials $S_n(x)$:

(a) $S_3(x)=x^2-1$;
(b) $S_4(x)=x(x^2-2)$;
(c) $S_5(x)=(x^2+x-1)(x^2-x-1)$;
(d) $S_6(x)=x(x^2-1)(x^2-3)$;
(e) $S_7(x)=(x^3+x^2-2x-1)(x^3-x^2-2x+1)$;
(f) $S_8(x)=x(x^2-2)(x^4-4x^2+2)$;
(g) $S_9(x)=(x^2-1)(x^3-3x-1)(x^3-3x+1)$;
(h) $S_{10}(x)=x(x^2-x-1)(x^2+x-1)(x^4-5x^2+5)$;
(i) $S_{11}(x)=(x^5-x^4-4x^3+3x^2+3x-1)(x^5+x^4-4x^3-3x^2+3x+1)$.

(j) A p-Sylow subgroup Q consists of matrices of the form

$$X=\begin{pmatrix}1 & 0\\ \lambda & 1\end{pmatrix},$$

where $\lambda\in F_{p^n}$. If A has order p, then $A\in BQB^{-1}$ for some $B\in SL_2(p^n)$. Thus $A=BXB^{-1}$ for some $X\in Q$, $X\neq 1$. Therefore, $\operatorname{tr}A=\operatorname{tr}X=2$, as desired. Next, if $\operatorname{tr}A=2$ then $A^2=2A-1$, and hence by induction $A^n=nA+1-n$ for any integer n. In particular, $A^p=pA+1-p=1$. □

Subgroups of $PSL_2(p^n)$ are classified by Dickson [3]. We will follow the presentation of Glover and Sjerve [5]; see also MacBeath [13]. There are three types of subgroups of $PSL_2(p^n)$, as outlined below.

Type I (projective subgroups): If $m\mid n$ then F_{p^m} is a subfield of F_{p^n} and therefore $PSL_2(p^m)$ is a subgroup of $PSL_2(p^n)$. If also $2m\mid n$ and $p>2$ then $PGL_2(p^m)$ is a subgroup of $PSL_2(p^n)$. Any subgroup conjugate within $PSL_2(p^n)$ to either $PSL_2(p^m)$ or $PGL_2(p^m)$ is called a *projective* subgroup.

Type II (affine subgroups): Consider the subgroups of $PSL_2(p^n)$ which have one of the following forms: either

$$\left\{\begin{bmatrix}a & b\\ 0 & a^{-1}\end{bmatrix}: a\in F_{p^n}^*,\ b\in F_{p^n}\right\}\quad\text{or}\quad\left\{\begin{bmatrix}\lambda & 0\\ 0 & \bar{\lambda}\end{bmatrix}: \lambda\in F_{p^{2n}}^*,\ \lambda^{p^n+1}=1\right\}.$$

Then any subgroup of $PSL_2(p^n)$ conjugate to a subgroup of one of the above is called an *affine* subgroup.

Type III (exceptional subgroups): The finite noncyclic triangle groups are:

$T(2,2,t)=$ the dihedral group D_{2t} of order $2t$, $t\geq 2$;
$T(2,3,3)=$ the tetrahedral group $\cong A_4$;
$T(2,3,4)=$ the octahedral group $\cong S_4$;
$T(2,3,5)=$ the icosahedral group $\cong A_5$.

Subgroups of $PSL_2(p^n)$ isomorpic to one of these are called *exceptional* subgroups.

REMARK. Every subgroup of $PSL_2(p^n)$ falls into one of these three types. However, the types of subgroups are not exclusive. For example, type I and type III may intersect, as well as type II and type III. On the other hand, type I and type II do not intersect, a fact which will be used later on.

DEFINITION 2.3. A triple (α,β,γ) of F_{p^n} is called *singular* if the following ternary quadratic form,

$$Q(x,y,z)=x^2+y^2+z^2+\alpha yz+\beta zx+\gamma xy,$$

splits into a product of two linear factors over the extension field $F_{p^{2n}}$.

DEFINITION 2.4. A triple (α,β,γ) of F_{p^n} is called *irregular* if the subfield κ generated by α,β,γ is a quadratic extension of another subfield κ_0, and if

one of the elements of the triple lies in κ_0 while the other two are both square roots in κ of nonsquares in κ_0, or zero.

DEFINITION 2.5. Let $A, B, C \in SL_2(p^n)$ with $ABC = 1$, and let $a, b, c \in PSL_2(p^n)$ be the corresponding images of A, B, C under the canonical homomorphism of $SL_2(p^n)$ onto $PSL_2(p^n)$. Such a triple (A, B, C) of $SL_2(p^n)$ is called

(a) *exceptional* if $\langle a, b, c\rangle$ is an exceptional subgroup of $PSL_2(p^n)$;
(b) *singular* if the triple $(\operatorname{tr} A, \operatorname{tr} B, \operatorname{tr} C)$ of traces is singular;
(c) *irregular* if the triple $(\operatorname{tr} A, \operatorname{tr} B, \operatorname{tr} C)$ of traces is irregular.

LEMMA 2.6 [5]. *Given* $\alpha, \beta, \gamma \in F_{p^n}$, $\{\alpha, \beta, \gamma\} \neq \{\pm 2\}$, *the triple* (α, β, γ) *is singular if and only if* $\alpha^2+\beta^2+\gamma^2-\alpha\beta\gamma = 4$.

THEOREM 2.7 [13]. (a) *A triple* (A, B, C) *of* $SL_2(p^n)$ *is singular if and only if it generates an affine subgroup* $\langle a, b, c\rangle$ *of* $PSL_2(p^n)$.

(b) *A triple* (A, B, C) *of* $SL_2(p^n)$ *which is neither singular nor exceptional generates a projective subgroup* $\langle a, b, c\rangle$ *of* $PSL_2(p^n)$.

(c) A triple (A, B, C) *of* $SL_2(p^n)$ *which is neither exceptional, singular, nor irregular generates in* $PSL_2(p^n)$ *a projective subgroup* $\langle a, b, c\rangle$ *isomorphic to* $PSL_2(\kappa)$, *where* κ *is the subfield generated by* $\operatorname{tr} A, \operatorname{tr} B, \operatorname{tr} C$ *over the ground field* F_p.

3. Generators of $SL_2(p^n)$

In this section we show that $SL_2(p^n)$ can be generated by an (r, s, t)-triple, where $(r, s, t) = (3, 4, p)$, $(3, 3, d)$, or $(3, 5, 7)$, depending on the values of p and n. As far as the genus of $SL_2(p^n)$ is concerned, this is the most efficient way of generating the group $SL_2(p^n)$.

LEMMA 3.1. *If* $-3 \in F_p^*$ *is not a square, then* $SL_2(p)$ *does not admit any* $(3, 3, p)$*-triple.*

Proof. It suffices to show that $AB = 1$ whenever $\operatorname{tr} A = \operatorname{tr} B = -1$ and $\operatorname{tr} AB = 2$. Let

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} x & y \\ z & t \end{pmatrix},$$

where $a+d = x+t = -1$ and $ax+bz+cy+dt = 2$. If $bc = 0$ then $1 = \det(A) = ad-bc = a(-a-1)$, so that $a^2+a+1 = 0$, which has no solution in F_p; hence $A \notin SL_2(p)$, a contradiction. Therefore, $bc \neq 0$, and similarly $yz \neq 0$. Now $a(-a-1)-bc = 1$, so $c = -(1+a+a^2)/b$, and similarly $z = -(1+x+x^2)/y$. Hence, $ax-b(1+x+x^2)/y-y(1+a+a^2)/b+(1+a)(1+x) = 2$. Putting $\lambda = y/b$, we obtain $x^2+x(1-\lambda-2a\lambda)+\lambda^2(1+a+a^2)+\lambda(1-a)+1 = 0$, which has discriminant $-3(1+\lambda)^2$. Therefore, we must have $\lambda = -1$; that is, $y = -b$. Similarly, $z = -c$. Hence $0 = ax+bz+cy+dt-2 = (2a+1)(x+a+1)$.

(a) Case $2a+1 \neq 0$. Then $x=-1-a=d$, so that

$$B=\begin{pmatrix} x & y \\ z & t \end{pmatrix}=\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}=A^{-1};$$

that is, $AB=1$.

(b) Case $2a+1=0$. Then $d=-1-a=a$ and $4a^2=-2a=1$. Therefore, $bc+1=ad=a^2$ and $1=\det(B)=x(-1-x)-yz=x(-1-x)-(-b)(-c)=-x^2-x-bc$; that is, $0=x^2+x+a^2$. Equivalently, $0=4x^2+4x+4a^2=4x^2+4x+1=(2x+1)^2$. Thus $2x+1=0$, and hence $x=a$. Therefore $x=t=a=d$, which, together with $y=-b$ and $z=-c$, implies as before that $AB=1$. □

LEMMA 3.2. *Let d be any divisor of $p-1$ or $p+1$, $d \neq 2, 3, 4, 6$. Then any $(3, 3, d)$-triple generates $SL_2(p)$.*

REMARK. A $(3, 3, 2)$-triple does not exist in $SL_2(p)$. A $(3, 3, 3)$-triple is singular, and hence does not generate $SL_2(p)$. Any $(3, 3, 4)$-triple or $(3, 3, 6)$-triple generates a subgroup ($\cong SL_2(3)$) of order 24, as may be easily verified by an elementary argument. This explains why $d \neq 2, 3, 4, 6$.

Proof of Lemma 3.2. Let (A, B, C) be a $(3, 3, d)$-triple, and let $\operatorname{tr} C=\lambda$. By Lemma 2.6, (A, B, C) is singular if and only if $\lambda=2$ or $\lambda=-1$. Thus (A, B, C) is singular if and only if $d=3$ or $d=p$. Since d does not equal 3 or p, it follows that (A, B, C) is nonsingular.

Let (a, b, c) be the corresponding triple in $PSL_2(p)$. If we can show that (A, B, C) is not an exceptional triple, then $\langle a, b, c\rangle$ is a projective subgroup of $PSL_2(p)$ and hence $\langle a, b, c\rangle \doteq PSL_2(p)$, since $PSL_2(p)$ is the only projective subgroup of itself. It would then follow that $\langle A, B, C\rangle = SL_2(p)$.

(i) Case $d \neq 5$. Suppose $d \neq 8, 10$. Then (a, b, c) is a $(3, 3, d_0)$-triple in $PSL_2(p)$ where $d_0 > 5$. Thus $\langle a, b, c\rangle$ is not an exceptional subgroup of $PSL_2(p)$. When $d=8$, (a, b, c) is a $(3, 3, 4)$-triple in $PSL_2(p)$. It is clear that $\langle a, b, c\rangle$ is neither cyclic nor dihedral; $\langle a, b, c\rangle \ncong A_4, A_5$, since both A_4 and A_5 do not have 4 torsion, and $\langle a, b, c\rangle \ncong S_4$, since S_4 does not admit any $(3, 3, 4)$-triple. Therefore, (A, B, C) is not an exceptional triple. When $d=10$, we note that $(-A)^6=B^3=(-C)^{10}=(-A)(B)(-C)=1$, and that $\langle A, B\rangle = \langle -A, B\rangle$. Let $X=-A$, $Y=B$, and $Z=-C$. Then (X, Y, Z) is a $(6, 3, 10)$-triple and $\langle A, B\rangle = \langle X, Y\rangle$. Since $Y^3=1$, we have

$$\operatorname{tr} Y^2X=(\operatorname{tr} Y)(\operatorname{tr} X)-\operatorname{tr} YX=-1-\gamma,$$

where $\gamma^2-\gamma-1=0$. It is easily verified, by Lemma 2.1, that $|Y^2X| \neq 2, 3, 4, 5, 6, 8$, or 10. Therefore, the image $y^2x \in PSL_2(p)$ of Y^2X is an element of order ≥ 7. Thus (A, B, C) is not an exceptional triple.

(ii) Case $d=5$. Here (a, b, c) is a $(3, 3, 5)$-triple of $PSL_2(p)$. Again, it is clear that $\langle a, b, c\rangle$ is neither cyclic nor dihedral. $\langle a, b, c\rangle \ncong A_4, S_4$, since both A_4 and S_4 do not have 5 torsion. We claim that $\langle a, b, c\rangle \ncong A_5$. Suppose, to the contrary, that $\langle a, b, c\rangle \cong A_5$. Let $\hat{A}_5 = \langle A, B, C\rangle$. Then $|\hat{A}_5| = 2^3 \cdot 3 \cdot 5$. By

[15, Thm. 6.17] we must have $\hat{A}_5 \cong SL_2(5)$, which is a contradiction since $SL_2(5)$ does not admit any $(3,3,5)$-triple (by Lemma 3.1). Thus (A,B,C) is not an exceptional triple. □

LEMMA 3.3. *Any* $(3,4,p)$*-triple generates* $SL_2(p)$.

Proof. This is proved by the same argument as in the preceding lemma, and is therefore omitted.

THEOREM 3.4. *Let* (A,B,C) *be a* $(3,3,d)$*-triple of* $SL_2(p^n)$, $n \geq 2$. *If* $\langle A,B,C\rangle = SL_2(p^n)$ *then*

(i) *either* $d \mid p^n - 1$ *or* $d \mid p^n + 1$; *and*
(ii) $d \nmid p^m \pm 1$ *for all* $m \mid n$, $m \neq n$.

Proof. (i) The torsion of $SL_2(p^n)$ is p, $2p$, or divisors of $p^n \pm 1$. Thus it is enough to show that $d \neq p, 2p$. Suppose $d = p$ or $2p$; then $\operatorname{tr} C = \pm 2$. Hence the smallest subfield κ of F_{p^n} containing $-1, -1, \pm 2$ is F_p. By Theorem 2.7, we have $\langle a,b,c\rangle \cong PSL_2(\kappa)$. Since $\langle a,b,c\rangle = PSL_2(F_{p^n})$, it follows that $F_{p^r} = \kappa = F_p$, and hence $n = 1$, which is a contradiction.

(ii) Suppose $d \mid p^m \pm 1$ for some $m \mid n$. We will show that $m = n$. Let κ be the smallest subfield of F_{p^n} containing $\operatorname{tr} C \equiv \gamma$. As before, we have $\kappa = F_{p^n}$. Since $|C| \neq p, 2p$ we have $\gamma = \nu + \nu^{-1}$, where $\nu \in F_{p^{2n}}$ is of order d; here ν, ν^{-1} are the roots of the characteristic equation $x^2 - \gamma x + 1 = 0$ of C. If $d \mid p^m - 1$ then $\nu^{p^m - 1} = 1$, so that $\nu^{p^m} = \nu$ and hence $\nu \in F_{p^m}$. Thus $\gamma = \nu + \nu^{-1} \in F_{p^m}$. If $d \mid p^m + 1$ then $\nu^{p^m + 1} = 1$, so that $\nu^{p^m} = \nu^{-1}$ and hence $\gamma^{p^m} = (\nu + 1/\nu)^{p^m} = \nu^{p^m} + (1/\nu)^{p^m} = \nu^{-1} + \nu = \gamma$. Thus $\gamma \in F_{p^m}$. Therefore, in either case we have $\gamma \in F_{p^m}$ and hence $F_{p^m} \supseteq \kappa = F_{p^n}$. Therefore $n \mid m$, and hence $m = n$, as desired. □

REMARK. Theorem 3.4 is valid for any generating (r,s,t)-triple (A,B,C) of $SL_2(p^n)$, where $\operatorname{tr} A, \operatorname{tr} B \in F_p$.

THEOREM 3.5. *Let* (A,B,C) *be any* $(3,3,d)$*-triple of* $SL_2(p^n)$, $n \geq 2$. *Suppose* d *satisfies the following conditions:*

(i) $d \mid p^n - 1$ *or* $d \mid p^n + 1$; *and*
(ii) $d \nmid p^m \pm 1$ *for all* $m \mid n$, $m \neq n$.

Then $\langle A,B,C\rangle = SL_2(p^n)$.

Proof. $(p,p) = (2p,p) = p$ and $(p^n \pm 1, p) = 1$, so that condition (i) implies that $d \neq p, 2p$. Also, condition (ii) implies that $d \neq 2, 3, 4, 6$ since, for $p \geq 5$, $p \pm 1$ always contains the factors 2, 3, 4, and 6; for $p = 3$, $d \neq 3, 6$, because $d \mid 3^n \pm 1$. Also, $p \pm 1 = 2, 4$, so that $d \neq 2, 4$.

As in the proof of Lemma 3.2, any such $(3,3,d)$-triple is nonexceptional. On the other hand, it is easily verified that any $(3,3,d)$-triple is neither singular nor irregular. Thus $\langle A,B,C\rangle \cong SL_2(\kappa)$, where κ is the smallest subfield of F_{p^n} containing $-1, -1, \gamma \equiv \operatorname{tr} C$. We claim that $\kappa = F_{p^n}$. By condition (i),

we have $\gamma = \nu + 1/\nu$, where ν is an element of $F_{p^{2n}}$ of order d; here ν and $1/\nu$ are roots of the characteristic equation $x^2 - \gamma x + 1 = 0$. Now, $\kappa = F_{p^m}$ for some $m \mid n$. Since $\gamma \in F_{p^m}$, we have $\gamma^{p^m} = \gamma$; that is, $\nu^{p^m} + (1/\nu)^{p^m} = \nu + 1/\nu$. Thus ν^{p^m} is also a root of the equation $x^2 - \gamma x + 1 = 0$. Hence $\nu^{p^m} = \nu$ or $\nu^{p^m} = 1/\nu$. Therefore, $\nu^{p^m \pm 1} = 1$, and hence $d \mid p^m \pm 1$. By condition (ii), we conclude that $m = n$. Thus $\kappa = F_{p^m} = F_{p^n}$, and hence $\langle A, B, C \rangle = SL_2(p^n)$. □

LEMMA 3.6. *Let (A, B, C) be an (r, s, t)-triple of $SL_2(p^n)$, $n \geq 2$, such that*

(i) $\langle A, B, C \rangle = SL_2(p^n)$ *and*

(ii) $1/r + 1/s + 1/t > 1/3 + 1/3 + 1/d$. *We say that (r, s, t) "beats" $(3, 3, d)$, where d is the smallest integer with respect to the following properties:*

(a) $d \mid p^n - 1$ *or* $d \mid p^n + 1$;

(b) $d \nmid p^m \pm 1$ *for all* $m \mid n$, $m \neq n$.

Then $(r, s, t) = (3, 5, 7)$ and $d > 105$.

Proof. Without loss of generality, we may assume that $r \leq s \leq t$. If $r \geq 5$, then $1/r + 1/s + 1/t \leq 3/5 < 1/3 + 1/3 + 1/d$, contradicting (ii). Thus $r = 3$ or 4, and hence we have the following possibilities:

(i) $(r, s, t) = (3, 3, t)$, where $3 \leq t < d$;
(ii) $(r, s, t) = (3, 4, t)$, where $4 \leq t \leq 11$;
(iii) $(r, s, t) = (3, 5, t)$, where $5 \leq t \leq 7$;
(iv) $(r, s, t) = (4, 4, t)$, where $4 \leq t \leq 5$.

We claim that all the above triples can be eliminated, except possibly (3, 5, 7).

Case (i) $SL_2(p^n)$ is generated by an (r, s, t)-triple. By Theorem 3.4, t satisfies the same properties as d does. By the choice of d, we cannot have $t < d$.

Case (ii) First consider the case where $t = 4$, 5, 6, 8, or 10. Here $\langle a, b, c \rangle = PSL_2(p^n)$ and (a, b, c) is an (l, m, n)-triple, where

$$(l, m, n) \in \{(3, 2, 2), (3, 2, 3), (3, 2, 4), (3, 2, 5)\}.$$

The corresponding triangle group $T(l, m, n) \cong D_6$, A_4, S_4, or A_5. Evidently, for $n \geq 2$, $PSL_2(p^n)$ cannot be a homomorphic image of any of these triangle groups (cf. [4]).

Next, consider the case where $t = 7$, 9, or 11. By the remark after Theorem 3.4, t satisfies the same properties as d does. Therefore $t \geq d$, and hence $1/3 + 1/4 + 1/t < 1/3 + 1/3 + 1/d$, contradicting the choice of t.

Case (iii) We will show that the triples (3, 5, 5) and (3, 5, 6) can be replaced by a (3, 3, 5)-triple which beats both triples. Let $\gamma = \operatorname{tr} B$. Then

$$(\operatorname{tr} A, \operatorname{tr} B, \operatorname{tr} C) = (-1, \gamma, \gamma) \text{ or } (-1, \gamma, 1).$$

Let κ be the smallest subfield of F_{p^n} containing γ. Then

$$SL_2(p^n) = \langle A, B, C \rangle = SL_2(\kappa),$$

so that $\kappa = F_{p^n}$. By Lemma 2.1, we must have $n = 2$, and hence $p \neq 5$ and $p \not\equiv \pm 1 \pmod 5$, as the polynomial $x^2 + x - 1$ over F_p has a root in F_p if and

only if $p=5$ or $p\equiv\pm1 \pmod 5$. Now 5 is a torsion of $SL_2(p^2)$ and $p\neq 5$. Therefore, either $5|p^2-1$ or $5|p^2+1$ (in fact, $5|p^2+1$). Therefore, we have $5|p^2-1$ or $5|p^2+1$ and $5\nmid p\pm1$. Therefore, $SL_2(p^2)$ can be generated by a (3, 3, 5)-triple, by Theorem 3.5. Furthermore, (3, 3, 5) beats both (3, 5, 5) and (3, 5, 6).

Case (iv) It suffices to remark that (2, 2, 2) and (2, 2, 5) are both spherical triples, and hence the corresponding triple (a, b, c) cannot generate $PSL_2(p^n)$.

Therefore, the only remaining triple is (3, 5, 7), which beats $(3, 3, d)$ if and only if $d>105$. □

LEMMA 3.7. *Let (A, B, C) be a (3, 5, 7)-triple of $SL_2(p^n)$. Then $\langle A, B, C\rangle \cong SL_2(\kappa)$, where κ is the smallest subfield of F_{p^n} containing* tr B *and* tr C.

Proof. Let $\beta=\operatorname{tr} B$ and $\gamma=\operatorname{tr} C$. Then β, γ satisfy the respective equations $\beta^2+\beta-1=0$ and $\gamma^3+\gamma^2-2\gamma-1=0$. By Lemma 2.6, (A, B, C) is not singular. Since (a, b, c) is a (3, 5, 7)-triple, (A, B, C) is not exceptional. We will show that (A, B, C) is not irregular case by case.

Case (i) $F_p(\beta)=F_p\neq F_p(\gamma)$. In this case, $\kappa=F_p(\gamma)=F_{p^3}$ and hence κ is not a quadratic extension of any subfield. Thus, (A, B, C) is not irregular.

Case (ii) $F_p(\gamma)=F_p\neq F_p(\beta)$. In this case, $\kappa=F_p(\beta)=F_{p^2}$ and κ is a quadratic extension of $\kappa_0\equiv F_p$. However, $-1, \gamma\in\kappa_0$, and so the κ-triple $(-1, \beta, \gamma)$ is not irregular.

Case (iii) $F_p(\beta)\neq F_p$ and $F_p(\gamma)\neq F_p$. Here $\kappa=F_p(\beta, \gamma)=F_{p^6}$ and κ is a quadratic extension of $\kappa_0\cong F_p(\gamma)=F_{p^3}$. Again, $-1, \gamma\in\kappa_0$, so that the κ-triple $(-1, \beta, \gamma)$ is not irregular.

Case (iv) $F_p(\beta)=F_p(\gamma)=F_p$. The conclusion here is immediate, as $\kappa=F_p$.

Therefore, in all cases, the triple (A, B, C) is neither singular, exceptional, nor irregular. Hence, $\langle A, B, C\rangle\cong SL_2(\kappa)$, by Theorem 2.7. □

COROLLARY 3.8. *$SL_2(p^n)$ can be generated by an (r, s, t)-triple, where $1/r+1/s+1/t>2/3$.*

Proof. $SL_2(3)$ (resp. $SL_2(5)$) can be generated by a (3, 3, 4)-triple (resp. a (3, 4, 5)-triple). For $p\geq 7$, $SL_2(p)$ can be generated by a $(3, 3, d)$-triple. For $n\geq 2$, $SL_2(p^n)$ can be generated by a $(3, 3, d)$-triple or a (3, 5, 7)-triple. Thus $SL_2(p^n)$ can be generated by an (r, s, t)-triple, where $1/r+1/s+1/t>2/3$. □

4. Genus of $SL_2(p^n)$

In this section, we show that the genus of $SL_2(p^n)$ is determined by an (r, s, t)-triple, where $(r, s, t)=(3, 4, 5)$, $(3, 3, d)$, or (3, 5, 7), depending on the various values of p and n. We begin with the following fundamental lemma.

LEMMA 4.1. *If S_g is a Riemann surface of least genus on which $G\equiv SL_2(p^n)$ acts as a group of automorphisms, then the regular branched covering*

$$S_g \xrightarrow{\pi} S_g/G$$

has zero orbit genus with three branch points.

Proof. Let $S_h = S_g/G$. By the Riemann–Hurwitz formula, we have

$$2g-2 = |G|\left[2h-2+\sum_{j=1}^{b}(1-1/m_j)\right], \tag{1}$$

where $(h; m_1, m_2, \ldots, m_b)$ is the branching data of the covering. We are to show that $h=0$ and that $b=3$. From Corollary 3.8, G is generated by an (r,s,t)-triple, where $1/r+1/s+1/t>2/3$. According to [8, Thm. 3], there exists a short exact sequence of groups $\Delta \to T(r,s,t) \xrightarrow{\theta} G$, where Δ is a torsion-free subgroup of the triangle group $T(r,s,t)$. Therefore, we have a commutative diagram of topological spaces:

$$\begin{array}{ccccc} & & D/\Delta \cong S & & \\ & \nearrow & & \searrow & \\ D & & \downarrow & & S/G \\ & \searrow & & \swarrow & \cong \\ & & D/T \cong S^2. & & \end{array}$$

Here S denotes the compact Riemann surface D/Δ, and S^2 is the 2-sphere D/T, where $T=T(r,s,t)$. Thus, $2\,\text{genus}(S)-2=|G|(1-1/r-1/s-1/t)$. By assumption, $g \le \text{genus}(S)$; that is,

$$2h-2+\sum_{j=1}^{b}(1-1/m_j) \le 1-(1/r+1/s+1/t). \tag{2}$$

Hence, $2h-2 \le 1-(1/r+1/s+1/t)$, from which it follows that $h=0$ or $h=1$.

Suppose $h=1$. Then $\sum_{j=1}^{b}(1-1/m_j) \le 1-(1/r+1/s+1/t)$. If $b \ge 1$ then, since $m_j \ge 2$, we have $1/2 \le b/2 \le 1-(1/r+1/s+1/t)$. Therefore, $1/r+1/s+1/t \le 1/2 < 2/3$, a contradiction. If $b=0$, then $S_g \to S_1$ is a regular unbranched covering of the torus S_1 with G as the group of covering transformations, which is impossible, as G is not abelian. Therefore, we must have $h=0$, and hence inequality (2) reduces to

$$-2+\sum_{j=1}^{b}(1-1/m_j) \le 1-(1/r+1/s+1/t),$$

which implies $b \le 4$. While it is clear that $b \ne 0, 1$, we consider the following cases.

(a) Suppose $b=2$. Then $2g-2=|G|[-2+(1-1/m_1)+(1-1/m_2)]<0$, so that $g=0$, and hence, from equation (1), $2=|G|/m_1+|G|/m_2$. Therefore, $|G|=m_1=m_2$. Thus, the number of fixed points is equal to the number of branch points. Let y_1, y_2 be the fixed points, and let x_1, x_2 be the respective branch points. Then

$$S^2\backslash\{y_1, y_2\} \to S^2\backslash\{x_1, x_2\}$$

is a regular unbranched covering with G as a group of covering transformations, and hence we have a short exact sequence of groups, $\mathbf{Z} \to \mathbf{Z} \to G$. Therefore, G is abelian, a contradiction.

(b) Suppose $b=4$. Without loss of generality, we may assume that $m_1 \leq m_2 \leq m_3 \leq m_4$. From inequality (2), we have

$$-2+\sum_{j=1}^{4}(1-1/m_j) \leq 1-(1/r+1/s+1/t) < 1/3,$$

that is, $5/3 < \sum_{j=1}^{4}(1/m_j)$, the only solution of which is $(2, 2, 2, n)$ with $n \geq 2$. By the Riemann existence theorem, we have $G=\langle z_1, z_2, z_3, z_4\rangle$, where $z_1^2 = z_2^2 = z_3^2 = z_4^n = z_1 z_2 z_3 z_4 = 1$. Since G has a unique element of order 2, $z_1 = z_2 = z_3$, so that $z_4 = z_3$ and hence $G = \mathbf{Z}_2$, which again is a contradiction.

Therefore, we are left with the only alternative—namely, $b=3$. The proof is now complete. □

As an immediate consequence, we have the following genus formula.

COROLLARY 4.2.

$$2(\text{genus}(SL_2(p^n))-1) = |SL_2(p^n)| \min_{(r,s,t)}(1-1/r-1/s-1/t),$$

where the minimum is taken over all triples (r, s, t) such that $SL_2(p^n)$ can be generated by an (r, s, t)-triple.

THEOREM 4.3. *The genus of $SL_2(p)$, $p \geq 7$, is determined by a $(3, 3, d)$-triple, where d is the smallest divisor of $p-1$ or $p+1$, $d \neq 2, 3, 4, 6$.*

Proof. Case (i) $p \equiv \pm 1 \pmod 5$. Here $d=5$, and by Corollary 4.2 it is clear that the genus of $SL_2(p)$ is determined by a $(3, 3, 5)$-triple.

Case (ii) $p \not\equiv \pm 1 \pmod 5$. Here $d \geq 7$, and $SL_2(p)$ does not have 5 torsion. Consider a generating (r, s, t)-triple (A, B, C) of $SL_2(p)$, where $3 \leq r \leq s \leq t$ and $1/3+1/3+1/d < 1/r+1/s+1/t$. We distinguish the following two subcases.

(a) $(r, s) = (3, 4)$ and $4 \leq t$. Then $2/3 < 1/3+1/3+1/d < 1/3+1/4+1/t$, so that $t \leq 11$. Since $SL_2(p)$ does not have 5 torsion, $t \neq 5, 10$. Thus, for $t \geq 7$, we have $t \geq d$, by the definition of d. Thus $1/3+1/4+1/t < 1/3+1/3+1/t \leq 1/3+1/3+1/d$, contradicting the choice of $(r, s, t) \equiv (3, 4, t)$. Therefore, $t = 4$ or 6.

(b) $r=4$. A similar computation shows that $s=4$ and $t=4$ or 5.

It is clear that $r<5$. Thus, if (r, s, t) beats $(3, 3, d)$ then

$$(r, s, t) \in \{(3, 4, 4), (3, 4, 6), (4, 4, 4), (4, 4, 5)\}.$$

The corresponding triples in $PSL_2(p)$ are $(3, 2, 2)$, $(3, 2, 3)$, $(2, 2, 2)$, $(2, 2, 5)$, which are all spherical triples. Since $p \geq 7$, $PSL_2(p)$ cannot be generated by such spherical triples (cf. [4]). Thus, for any (r, s, t)-triple (A, B, C) of $SL_2(p)$ where (r, s, t) beats $(3, 3, d)$, we have $\langle A, B, C\rangle \neq SL_2(p)$. □

COROLLARY 4.4. *If g is the genus of $SL_2(p)$, $p \geq 7$, then $g \equiv 1 \pmod{p}$.*

Proof. We have

$$g-1 = |SL_2(p)|(1/3-1/d)/2 = p(p-1)(p+1)(d-3)/2\cdot 3\cdot d.$$

Since $d \mid p-1$ or $d \mid p+1$, and $p \neq 2, 3$, the conclusion follows at once. □

REMARK. Kulkarni [10] shows that if a group G acts on S_g then $g \equiv 1 \pmod{N}$, where N is the integer which measures the cyclic deficiency of the group G. It turns out that $N=1$ for $SL_2(p)$, and hence the congruence $g \equiv 1 \pmod{N}$ becomes trivial. Corollary 4.4 says a bit more about genus$(SL_2(p))$.

For completeness, we include the following theorem, the proof of which is analogous and therefore omitted.

THEOREM 4.5. *The genus of $SL_2(3)$ is determined by a $(3, 3, 4)$-triple, and that of $SL_2(5)$ by a $(3, 4, 5)$-triple.*

THEOREM 4.6. *The genus of $SL_2(5^n)$ is determined by a $(3, 3, d)$-triple, where d is the smallest integer such that:*

(i) *$d \mid 5^n-1$ or $d \mid 5^n+1$; and*
(ii) *$d \nmid 5^m \pm 1$ for all $m \mid n$, $m \neq n$.*

Proof. We note that $x^2+x-1 = (x-2)^2$, and distinguish the following cases.

Case (i) $n=3$. We have $7 \mid 5^3+1$ and $7 \nmid 5 \pm 1$. By Theorem 3.5, $SL_2(5^3)$ is generated by a $(3, 3, 7)$-triple, and $(3, 3, 7)$ beats $(3, 5, 7)$. Therefore, the genus of $SL_2(5^3)$ is determined by a $(3, 3, 7)$-triple.

Case (ii) $n \neq 3$. Let (A, B, C) be any $(3, 5, 7)$-triple of $SL_2(5^n)$, $\alpha = \operatorname{tr} A$, $\beta = \operatorname{tr} B$, and $\gamma = \operatorname{tr} C$. Then $\alpha = -1$, $\beta = 2$, and $\gamma^3+\gamma^2-2\gamma-1 = 0$. Let κ be the smallest subfield of F_{5^n} containing γ. Since $\gamma^3+\gamma^2-2\gamma-1=0$ has no solutions in F_5, it follows that $\kappa = F_5(\gamma) = F_{5^3}$, and hence

$$\langle A, B, C\rangle \cong SL_2(\kappa) \cong SL_2(5^3).$$

Thus, for $n \neq 3$, $SL_2(5^n)$ cannot be generated by any $(3, 5, 7)$-triple. The conclusion now follows, by Lemma 3.6. □

THEOREM 4.7. *The genus of $SL_2(7^n)$ is determined by a $(3, 3, d)$-triple, where d is the smallest integer such that:*

(i) *$d \mid 7^n-1$ or $d \mid 7^n+1$; and*
(ii) *$d \nmid 7^m \pm 1$ for all $m \mid n$, $m \neq n$.*

Proof. The same argument is used as in the proof of Theorem 4.6, modulo the following observations:

$$\gamma^3+\gamma^2-2\gamma-1 = (\gamma-2)^3,$$

and the equation $\beta^2+\beta-1=0$ has no solutions within F_7, so that $F_7(\gamma) = F_7 \subseteq F_7(\beta) = F_{7^2}$. □

THEOREM 4.8. (a) *The genus of* $SL_2(p^n)$, $2 \le n \ne 6$, *is determined by a* $(3, 3, d)$*-triple, where* d *is the smallest integer such that:*

(i) $d \mid p^n - 1$ *or* $d \mid p^n + 1$;

(ii) $d \nmid p^m \pm 1$ *for all* $m \mid n$, $m \ne n$.

(b) *The genus of* $SL_2(p^6)$ *is either determined by a* $(3, 3, d)$*-triple as above when* $d \le 105$, *or a* $(3, 5, 7)$*-triple when* $d > 105$.

Proof. Let (A, B, C) be any generating $(3, 5, 7)$-triple of $SL_2(p^n)$. As before, $(\operatorname{tr} A, \operatorname{tr} B, \operatorname{tr} C) = (-1, \beta, \gamma)$, where $\beta^2 + \beta - 1 = 0$ and $\gamma^3 + \gamma^2 - 2\gamma - 1 = 0$. By Theorems 4.6 and 4.7, we may assume that $p \ne 5$ or 7. As $\langle A, B, C \rangle = SL_2(p^n)$ and $n \ge 2$, we cannot have $F_p(\beta) = F_p = F_p(\gamma)$. Therefore, we are left with the following cases.

Case (i) $F_p(\beta) = F_p \subseteq F_p(\gamma) = F_{p^3}$. From $F_p(\beta) = F_p$, we have $p \equiv \pm 1 \pmod 5$. From $F_p(\gamma) = F_{p^3}$, we have $p^3 \equiv \pm 1 \pmod 7$ and $p \not\equiv \pm 1 \pmod 7$. Thus, $SL_2(p^3)$ is generated by a $(3, 3, 7)$-triple, and $(3, 3, 7)$ beats $(3, 5, 7)$.

Case (ii) $F_p(\gamma) = F_p \subseteq F_p(\beta) = F_{p^2}$. From $F_p(\gamma) = F_p$, we obtain $p \equiv \pm 1 \pmod 7$. From $F_p(\beta) = F_{p^2}$, we obtain $p^2 \equiv \pm 1 \pmod 5$ and $p \not\equiv \pm 1 \pmod 5$. Thus, $SL_2(p^2)$ is generated by a $(3, 3, 5)$-triple, and $(3, 3, 5)$ beats $(3, 5, 7)$.

Case (iii) $F_p(\beta) = F_{p^2}$ and $F_p(\gamma) = F_{p^3}$. From $F_p(\beta) = F_{p^2}$, we obtain $p \equiv \pm 2 \pmod 5$. From $F_p(\gamma) = F_{p^3}$, we obtain $p \equiv \pm 2$ and $p \equiv \pm 3 \pmod 7$. In this case, $F_p(\beta, \gamma) = F_{p^6}$. Thus, the genus of $SL_2(p^6)$ is either determined by a $(3, 5, 7)$-triple or a $(3, 3, d)$-triple as stated. For $n \ne 6$, the genus is determined by a $(3, 3, d)$-triple. □

COROLLARY 4.9. *If* g *is the genus of* $SL_2(p^n)$, *then* $g \equiv 1 \pmod{p^n}$.

Proof. Same as for Corollary 4.4. □

5. Automorphism Group of Genus Surfaces

In this section we compute the full group $\operatorname{Aut}(S_g)$ of automorphisms of a Riemann surface S_g, where g is the genus of $SL_2(p^n)$. From Section 1 we recall that the underlying Riemann structure of S_g comes from the homeomorphism $S_g \equiv D/T(r, s, t)$ and the homomorphism $T(r, s, t) \to SL_2(p^n)$, where the genus g is determined by an (r, s, t)-triple of $SL_2(p^n)$. In order to compute $\operatorname{Aut}(S_g)$, we give a basic lemma which exhibits a $(3, 3, d)$-triple explicitly and also shows a particular property of any such $(3, 3, d)$-triple. Here d is assumed to be nonparabolic; that is, either $d \mid p^n - 1$ (hyperbolic case), or $d \mid p^n + 1$ (elliptic case). If d satisfies the conditions of Theorem 3.5, then we have a generating $(3, 3, d)$-triple of $SL_2(p^n)$.

LEMMA 5.1 (elliptic case). *For each divisor* d *of* $q+1$, *there is a* $(3, 3, d)$*-triple* (A, B, C) *of* $SL_2(q)$. *Moreover, for each such* $(3, 3, d)$*-triple, there is a* $D \in GL_2(q^2)$ *such that* $\det D = -1$, $D^2 = 1$, *and* $DAD = B$; $D \in SL_2^{\pm}(q)$ *if and only if* $2d \nmid q+1$.

Proof. Pick an element $\xi \in F_{q^2}^*$ of order d, and let

$$C=\begin{pmatrix} \xi & 0 \\ 0 & \xi^q \end{pmatrix}, \qquad A=\begin{pmatrix} \alpha & \beta \\ -\beta^q & \alpha^q \end{pmatrix},$$

and $B=(CA)^{-1}$, where $\alpha=-\beta^{q+1}/(1+\xi)$ and $\beta^{q+1}=(1+\xi+\xi^2)/(1+\xi)^2$. Clearly, $C \in SU_2(q)$ is an element of order d. Since $\operatorname{tr} CA=\operatorname{tr} A=\alpha+\alpha^q=\alpha(1+\xi)=-1$, we have $|CA|=|A|=3$. Therefore (A, B, C) is a $(3, 3, d)$-triple of $SU_2(q)$. To find the matrix D, we note that ξ is a square in $F_{q^2}^*$, say $\xi_1^2=\xi$ for some $\xi_1 \in F_{q^2}$. Let

$$D=\begin{pmatrix} \xi_1\alpha & \xi_1\beta \\ \beta^q/\xi_1 & -\xi_1\alpha \end{pmatrix}.$$

It is now a routine matter to verify that $\det D=-1$, $D^2=1$, and $DA=BD$. Finally, let $\alpha_1=\xi_1\alpha$ and $\beta_1=\xi_1\beta$. Then $\alpha_1^q=\xi_1^{q+1}\alpha$ and $\beta_1^q=\xi_1^q\beta^q$. Therefore, $\bar{D}^tD=-1$ if and only if $\xi_1^{q+1}=-1$.

Write $ds=q+1$ for some integer s. Since $\xi_1^d=-1$, we have $\xi_1^{q+1}=(\xi_1^d)^s=(-1)^s$. Therefore, $\xi_1^{q+1}=-1$ if and only if s is odd, that is, $2d \nmid q+1$. Thus, $\bar{D}^tD=-1$ if and only if $2d \nmid q+1$. Since the two groups $SL_2(q)$ and $SU_2(q)$ are conjugate within $GL_2(q^2)$, we may assume that everything takes place in $SL_2(q)$. The proof is now complete. □

REMARK. In [16] it is shown that there exists a $Q \in GL_2(q^2)$ such that

(i) $QSL_2(q)Q^{-1}=SU_2(q)$ and

(ii) $QSL_2^{\pm}(q)Q^{-1}=\{D \in GL_2(q^2): \bar{D}^tD=\pm 1\}$.

LEMMA 5.2 (hyperbolic case). *Let $\xi \in F_q^*$ be an element of order d. Let*

$$A=\begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix}, \qquad B=\begin{pmatrix} e & f \\ g & h \end{pmatrix},$$

and $C=(AB)^{-1}$, where $e=-1/(1+\xi)$, $h=e\xi$, $fg=eh-1$, and $fg \neq -1$. For each divisor d of $q-1$, there exists a $(3, 3, d)$-triple (A, B, C) of $SL_2(q)$. Moreover, for each such $(3, 3, d)$-triple there exists a $D \in GL_2(q^2)$ such that $\det D=-1$, $D^2=1$, and $DAD=B$; $D \in SL_2^{\pm}(q)$ if and only if $2d \mid q-1$.

Proof. Pick an element $\xi \in F_q^*$ or order d. Let $e=-1/(1+\xi)$ and $h=e\xi$, and choose any $f, g \in F_q$ such that $fg \neq -1$ and $fg=eh-1$. Let

$$C=\begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix}, \qquad A=\begin{pmatrix} e & f \\ g & h \end{pmatrix},$$

and $B=(CA)^{-1}$. As in the proof of Lemma 5.1, it is easily verified that (A, B, C) is a $(3, 3, d)$-triple. Finally, choose $\xi_1 \in F_{q^2}$ such that $\xi_1^2=\xi$, and let

$$D=\begin{pmatrix} e\xi_1 & f\xi_1 \\ -g/\xi_1 & -e\xi_1 \end{pmatrix}.$$

Then $\det D=-1$, $D^2=1$, and $DAD=B$; ξ is a square in F_q if and only if $2d \mid q-1$. Thus, $\xi_1 \in F_q$; that is, $D \in SL_2^{\pm}(q)$ if and only if $2d \mid q-1$. □

The following is an immediate consequence of the preceding lemmas.

COROLLARY 5.3. *Let* $G = SL_2(q)$, $H = \langle D \rangle \subseteq GL_2(q^2)$, *and* $\tilde{G} = GH$. *Then:*

(i) $\tilde{G}$ *is a subgroup of* $GL_2(q^2)$;
(ii) $[\tilde{G}: G] = 2$;
(iii) $\tilde{G} = \langle D, A \rangle$, *where* $D^2 = A^3 = (DA)^{2d} = 1$; *that is,* $\tilde{G}$ *is generated by a* $(2, 3, 2d)$*-triple; and*
(iv) $\tilde{G} \cong G: \mathbf{Z}_2$, *a semidirect product.*

In what follows, we will continue with the use of the preceding notation.

THEOREM 5.4. *Suppose* S_g *is a Riemann surface of least genus on which* $SL_2(q)$ *acts conformally and effectively. If* g *is determined by a* $(3, 3, d)$*-triple of* $SL_2(q)$, *then* $\mathrm{Aut}(S_g) \cong \tilde{G}$.

Proof. We first show that there is a commutative diagram with short exact rows:

$$\begin{array}{ccccc} \Delta & \to & T(2,3,2d) & \to & \tilde{G} \\ \uparrow & & \uparrow & & \uparrow \\ \Delta & \to & T(3,3,d) & \to & G, \end{array}$$

where the vertical homomorphisms are either the identity or inclusions, and $G = SL_2(q)$.

Let $T(2, 3, 2d) = \langle t, y \mid t^2 = y^3 = (ty)^{2d} = 1 \rangle$, and let $x = tyt = t^{-1}yt$. Then $|x| = 3$ and $xy = (tyt)t = (ty)^2$, so that $|xy| = d$. Thus $T(3, 3, d) = \langle x, y \mid x^3 = y^3 = (xy)^d = 1 \rangle$. The homomorphism $\tilde{\theta}$ is determined by $\tilde{\theta}(t) = D$ and $\tilde{\theta}(y) = A$; $\tilde{\theta}$ is well-defined, since $D^2 = A^3 = (DA)^{2d} = 1$. We note that

$$\tilde{\theta}(x) = \tilde{\theta}(tyt) = \tilde{\theta}(t)\tilde{\theta}(y)\tilde{\theta}(t) = DAD = B.$$

Hence, $\tilde{\theta}$ induces the natural homomorphism $T(3, 3, d) \xrightarrow{\theta} G$. Clearly, both $\tilde{\theta}$ and θ are torsion-preserving, so that the respective kernels are torsion-free subgroups of the corresponding groups. We claim that $\ker \tilde{\theta} = \ker \theta$. Let $\Delta = \ker \theta$. Since θ is a restriction of $\tilde{\theta}$, we have $\Delta \subseteq \ker \tilde{\theta}$. Let $W \in T(3, 3, d)$ and suppose that $\tilde{\theta}(Wt) = 1$. Then $1 = \tilde{\theta}(Wt) = \tilde{\theta}(W)\tilde{\theta}(t) = wD$, where $w = \tilde{\theta}(W) = \theta(W) \in G$. Thus $D = w^{-1} \in G$, a contradiction; therefore, $Wt \notin \ker \tilde{\theta}$. Since $T(2, 3, 2d) = T(3, 3, d) \cup T(3, 3, d)t$, it follows that $\ker \tilde{\theta} = \ker \theta = \Delta$. Therefore, we have the commutative diagram with exact rows:

$$\begin{array}{ccccc} \Delta & \to & T(2,3,2d) & \to & \tilde{G} \\ \uparrow & & \uparrow & & \uparrow \\ \Delta & \to & T(3,3,d) & \to & G. \end{array}$$

Let $g = \mathrm{genus}(G)$. Since g is determined by a $(3, 3, d)$-triple, the short exact sequence $\Delta \to T(3, 3, d) \to G$ implies that $\Delta \cong \pi_1(S_g, *)$. The short exact sequence $\Delta \to T(2, 3, 2d) \to \tilde{G}$ implies that $\tilde{G}$ is isomorphic to a subgroup of $\mathrm{Aut}(S_g)$. From the theory of covering spaces, we know that $\mathrm{Aut}(S_g) \cong N/\Delta$, where N is the normalizer of Δ in $PSL_2(\mathbf{R})$. Since Δ is a discrete subgroup

of $PSL_2(\mathbf{R})$, so is its normalizer [12]. Because $\Delta \trianglelefteq T(2,3,2d)$, we see that $T(2,3,2d) \subseteq N$. Therefore, denoting $T(2,3,2d)$ by $\tilde{T}$, we have the following commutative diagram:

$$\begin{array}{ccc} N & \to & \mathrm{Aut}(S_g) \\ \uparrow & & \uparrow \\ \tilde{T} & \to & K \cong \tilde{G} \\ \uparrow & & \uparrow \\ \Delta & \to & 1. \end{array}$$

Since $\mathrm{Aut}(S_g)$ is a finite group, it follows that $[N: T(2,3,2d)]$ is finite. By [6, Thm. 3B], $T(2,3,2d)$ is finitely maximal; that is, $T(2,3,2d)$ is not a subgroup of finite index of any Fuchsian subgroup of $PSL_2(\mathbf{R})$. Therefore, we must have $N = T(2,3,2d)$, and hence $\mathrm{Aut}(S_g) = N/\Delta = T(2,3,2d)/\Delta \cong \tilde{G}$, as desired. □

COROLLARY 5.5.

(i) (elliptic case) $\mathrm{Aut}(S_g) \cong SL_2^{\pm}(q)$ *if and only if* $2d \nmid q+1$.
(ii) (hyperbolic case) $\mathrm{Aut}(S_g) \cong SL_2^{\pm}(q)$ *if and only if* $2d \mid q-1$.

Proof. These are immediate consequences of Lemmas 5.1 and 5.2. □

For the sake of completeness, we include the following theorem. The proof is entirely analogous to that of Theorem 5.4, modulo these facts: The triangle groups $T(3,4,5)$ and $T(3,5,7)$ are finitely maximal in $PSL_2(\mathbf{R})$.

THEOREM 5.6.

(i) $\mathrm{Aut}(S_g) \cong SL_2(5)$, *where* $g = \mathrm{genus}(SL_2(5))$.
(ii) *Let* $g = \mathrm{genus}(SL_2(p^6))$. *If* g *is determined by a* $(3,5,7)$*-triple then* $\mathrm{Aut}(S_g) \cong SL_2(p^6)$.

ACKNOWLEDGMENT. This is the bulk of the author's Ph.D. thesis at Ohio State University, supervised by Professor Henry Glover. The author would like to take this opportunity to express his sincere thanks to Prof. Glover for his guidance and encouragement over the years when the thesis was carried out.

References

[1] M. D. E. Conder, *Generators for alternating and symmetric groups,* J. London Math. Soc. (2) 22 (1980), 75–86.
[2] M. D. E. Conder, R. A. Wilson, and A. J. Woldar, *The symmetric genus of sporadic groups: announced results,* Preprint.
[3] L. E. Dickson, *Linear groups with an exposition of the Galois field theory,* Teubner, Leipzig, 1901; reprinted Dover, New York, 1960.
[4] H. Glover and D. Sjerve, *Representing $PSl_2(p)$ on a Riemann surface of least genus,* Enseign. Math. (2) 31 (1985), 305–325.

[5] ———, *The genus of $PSl_2(q)$*, J. Reine Angew. Math. 380 (1987), 59–86.
[6] L. Greenberg, *Maximal Fuchsian groups,* Bull. Amer. Math. Soc. 69 (1963), 569–573.
[7] ———, *Maximal groups and signatures,* Discontinuous groups and Riemann surfaces, Ann. of Math. Stud., 79, pp. 207–226, Princeton Univ. Press, Princeton, NJ, 1974.
[8] W. J. Harvey, *Cyclic groups of automorphisms of a compact Riemann surface,* Quart. J. Math. Oxford Ser. (2) 17 (1966), 86–97.
[9] S. Kerckhoff, *The Nielsen realization problem,* Ann. of Math. (2) 117 (1983), 235–265.
[10] R. S. Kulkarni, *Symmetries of surfaces,* Topology 26 (1987), 195–203.
[11] U. Langer and G. Rosenberger, *Erzeugende endlicher projektiver linearer Gruppen,* Resultate Math. 15 (1989), 119–148.
[12] J. Lehner, *Lectures on modular forms,* National Bureau of Standards, Applied Math. Series 61, U.S. Government Printing Office, Washington, DC, 1969.
[13] A. M. MacBeath, *Generators of the linear fractional groups,* Proc. Sympos. Pure Math., 12, pp. 14–32, Amer. Math. Soc., Providence, RI, 1969.
[14] C. Maclachlan, *Abelian groups of automorphisms of compact Riemann surfaces,* Proc. London Math. Soc. (3) 15 (1965), 699–712.
[15] M. Suzuki, *Group theory,* Springer, Berlin, 1982.
[16] S. N. Voon, *The genus of $SL_2(F_q)$*, Ph.D. Thesis, Ohio State University, 1991.

Department of Mathematics
Ohio State University
Columbus, OH 43210