Zeitschrift: L'Enseignement Mathématique

Herausgeber: Commission Internationale de l'Enseignement Mathématique

Band: 31 (1985)

Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: REPRESENTING $PSl_2(p)$ ON A RIEMANN SURFACE OF LEAST GENUS

Autor: Glover, Henry / Sjerve, Denis

Kapitel: §2. Generating Triples for $PSl_2(p)$

DOI: https://doi.org/10.5169/seals-54572

times, namely for $p = 103$, 137 and 569 and $(2, 4, 5)$ occurs exactly six times, for $p = 199$, 239, 359, 439, 521 and 599.

If $S = H/\Delta$ is the surface of minimal genus for $PSl_2(p)$ coming from one of the extensions above then the orbit manifold $S/PSl_2(p)$ is the 2-sphere S^2 and the quotient map $S \to S^2$ is a branched covering with exactly 3 branch points. One of the most important steps in the proof of the main result of this paper is the converse, namely if S is a Riemann surface of least genus for the group $G = PSl_2(p)$ then $S/G = S^2$ and $S \to S^2$ is a branched covering with exactly 3 branch points (see section 3). Note that a related notion of genus, "the Cayley genus of a group" has been studied by others, among them Tucker [T]. Earlier results can be found in Hurwitz [H] and Burnside [B].

The remainder of this paper is organized as follows. In section 2 we describe various ways of generating $PSl_2(p)$ and then prove theorems I and II. Section 3 proves that if S is a Riemann surface of least genus for $PSl_2(p)$ then $S/PSl_2(p)$ is a 2-sphere S^2 and the branched covering $S \to S^2$ has exactly 3 branch points. The calculation of genus $(PSl_2(p))$ then follows from the results of section 2.

Finally we would like to thank Bomshik Chang for help with the group theory of $PSl_2(p)$. The first author would like to thank the University of British Columbia for its hospitality to him during the time this research was done.

§ 2. Generating Triples for $PSl_2(p)$

Our goal in this section is to find triples (r, s, t) for which there are epimorphisms $T(r, s, t) \twoheadrightarrow PSl_2(p)$. In other words, given integers $r, s, t \geqslant 2$ are there matrices $A, B, C \in PSl_2(p)$ so that A, B, C generate $PSl_2(p)$ and $A^r = B^s = C^t = ABC = 1$? Throughout this section a standard reference for the group theory is Suzuki [S].

The spherical triangle groups are given in the following table

Table I

triple	*triangle group*	*order*
$(2, 2, n)$	dihedral	$2n$
$(2, 3, 3)$	tetrahedral (A_4)	12
$(2, 3, 4)$	octahedral (S_4)	24
$(2, 3, 5)$	icosahedral (A_5)	60

Now the group $PSl_2(p)$ has an element of order p since its order is $|PSl_2(p)| = \frac{p(p^2-1)}{2}$. It therefore follows that $PSl_2(p)$ is not the image of any spherical triangle group since $PSl_2(p)$ can not be the image of any dihedral group and we are assuming $p \geqslant 7$. The following lemma then implies that $PSl_2(p)$ can only be the image of hyperbolic triangle groups.

(2.1). LEMMA. *$PSl_2(p)$ is not the image of any euclidean triangle group.*

Proof. Suppose T is one of the euclidean triangle groups, namely one of $T(3, 3, 3)$, $T(2, 4, 4)$, $T(2, 3, 6)$, and there exists an epimorphism $T \twoheadrightarrow PSl_2(p)$. Since T has $\mathbf{Z} \oplus \mathbf{Z}$ as a normal subgroup of index $\leqslant 6$ it follows that $PSl_2(p)$ has an abelian normal subgroup of index $\leqslant 6$. But this is clearly not possible. Q.e.d.

In order to decide when a triple of matrices $A, B, C \in PSl_2(p)$ generates the entire group we need detailed knowledge of the maximal subgroups. The following theorem can be found in Suzuki [S].

(2.2). THEOREM. *The maximal proper subgroups of $PSl_2(p)$ are:*

(a) *dihedral of order* $p - 1$ *or* $p + 1$.

(b) *solvable of order* $\frac{p(p-1)}{2}$.

(c) A_4 *if* $p \equiv 3, 13, 27, 37 \bmod 40$.

(d) S_4 *if* $p \equiv \pm 1 \bmod 8$.

(e) A_5 *if* $p \equiv \pm 1 \bmod 5$.

The dihedral group of order $p - 1$ can be chosen to be

$$D = \langle R, S\rangle = \left\{\begin{bmatrix}\alpha & 0\\ 0 & \alpha^{-1}\end{bmatrix}, \begin{bmatrix}0 & \alpha\\ -\alpha^{-1} & 0\end{bmatrix} \mid \alpha \in \mathbf{Z}_p^*\right\}, \quad \text{where}$$

$$R = \begin{bmatrix}x & 0\\ 0 & x^{-1}\end{bmatrix}, \; S = \begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix} \quad \text{and } x \text{ is a primitive root mod } p.$$

To realize the dihedral subgroup of order $p + 1$ we need another description of $PSl_2(p)$. The mapping

$$GF(p^2) \to GF(p^2), \; x \to x^p$$

is an automorphism of order 2. For convenience we put $\bar{x} = x^p$. Then $PSl_2(p) \cong PSU_2(p)$, where $PSU_2(p)$ is the projective special unitary group

$$PSU_2(p) = \left\{ \begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix} \mid a, b \in GF(p^2), a\,\bar{a} + b\,\bar{b} = 1 \right\}$$

Now consider the matrix $U = \begin{bmatrix} \omega & 0 \\ 0 & \bar{\omega} \end{bmatrix}$, where $\omega \in GF(p^2)$ is chosen so that $\omega^{(p+1)/2} = -1$ and $\omega^k \neq \pm 1$ for $1 \leqslant k < \dfrac{p+1}{2}$. Then the order of U as an element of $PSU_2(p)$ is $\dfrac{p+1}{2}$ and the dihedral group of order $\dfrac{p+1}{2}$ can be taken to be

$$D = \langle U, S \rangle = \left\{ \begin{bmatrix} \alpha & 0 \\ 0 & \bar{\alpha} \end{bmatrix}, \begin{bmatrix} 0 & \alpha \\ -\bar{\alpha} & 0 \end{bmatrix} \mid \alpha \in GF(p^2)^*, \alpha^{p+1} = 1 \right\}.$$

Finally the maximal solvable subgroup of order $\dfrac{p(p-1)}{2}$ can be chosen to be the subgroup of upper triangular matrices

$$H = \left\{ \begin{bmatrix} x & \lambda \\ 0 & x^{-1} \end{bmatrix} \mid x \in \mathbf{Z}_p^*,\ \lambda \in \mathbf{Z}_p \right\}.$$

Thus there is a split extension of the form

$$1 \to \mathbf{Z}_p \to H \xrightarrow{\theta} \mathbf{Z}_{(p-1)/2} \to 1,\ \theta : \begin{bmatrix} x & \lambda \\ 0 & x^{-1} \end{bmatrix} \to \pm x.$$

The kernel is generated by $T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and the splitting is induced by the matrix $\begin{bmatrix} x & 0 \\ 0 & x^{-1} \end{bmatrix}$, where x is a primitive root mod p.

The other maximal subgroups will not play much of a role in what follows. Notice that an immediate consequence of (2.2) is

(2.3). LEMMA.

(a) *The order of an element of* $PSl_2(p)$ *is one of the following: a divisor of either* $\dfrac{p-1}{2}$ *or* $\dfrac{p+1}{2}$; p; 2, 3, 4 *or* 5.

(b) *If* d *is a divisor of either* $\frac{p-1}{2}$ *or* $\frac{p+1}{2}$ *then there is an element of* $PSl_2(p)$ *having order* d.

The order of an element $A \in PSl_2(p)$ can be determined from its trace. In particular we have:

(2.4) LEMMA. *Let* $A \in PSl_2(p)$ *and* $\chi = \pm$ trace A. *Then the order of* A *is* $2, 3, 4,$ *or* 5 *respectively if, and only if,* $\chi \equiv 0\,(p)$, $\chi \equiv \pm 1\,(p)$, $\chi^2 \equiv 2\,(p)$ *or* $\chi^2 \pm \chi - 1 \equiv 0\,(p)$ *respectively.*

Definition. We say that a triple of elements (A, B, C) from $PSl_2(p)$ is an (r, s, t) triple if (a) order $A = r$, order $B = s$, order $C = t$; and (b) $ABC = 1$.

In order to construct $(2, 3, d)$ triples for $d \mid \frac{p-1}{2}$ let A, B, C be the matrices

(2.5) $A = \begin{bmatrix} 0 & -x \\ x^{-1} & 0 \end{bmatrix}$, $B = \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix}$, $C = (AB)^{-1} = \begin{bmatrix} x^{-1} & x \\ 0 & x \end{bmatrix}$

where $x \in \mathbf{Z}_p^*$. Then order $A = 2$, order $B = 3$ and

$$C^k = \begin{bmatrix} x^{-k} & x(x^{k-1} + x^{k-3} + \dots + x^{-(k-1)}) \\ 0 & x^k \end{bmatrix}$$

If $x = \pm 1$ then $C = T$ and order $T = p$. In general the order of C is given by the following lemma whose proof is elementary and hence omitted.

(2.6). LEMMA. *Assume* $x \neq \pm 1$. *Then the order of* C *in* $PSl_2(p)$ *is the least positive integer* k *so that either* $x^k = 1$ *or* $x^k = -1$.

Given $x \in \mathbf{Z}_p^*$, $x \neq \pm 1$, let k be the least positive integer so that $x^k = \pm 1$. Since we always have $x^{(p-1)/2} = \pm 1$ it follows that $1 < k \leqslant \frac{p-1}{2}$. Also $x^{2k} = 1$ and therefore $k \mid \frac{p-1}{2}$. Conversely, given any divisor d of $\frac{p-1}{2}$ there exists $x \in \mathbf{Z}_p^*$ so that d is the least positive integer k satisfying $x^k = \pm 1$.

(2.7). COROLLARY. *Suppose* $d > 1$ *is a divisor of* $\frac{p-1}{2}$. *Then there exist* $(2, 3, d)$ *triples* (A, B, C) *in* $PSl_2(p)$.

Next we determine when there are $(2, 3, d)$ triples for divisors of $\frac{p+1}{2}$. Suppose $x \in GF(p^2)^*$ is such that $x^{p+1} = 1$. Then consider the triple of matrices (A, B, C) in $PSU_2(p)$:

$$(2.8). \qquad A = \begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix}, \; B = \begin{bmatrix} \bar{x}\,\bar{a} & -xb \\ \bar{x}\,\bar{b} & xa \end{bmatrix}, \; C = \begin{bmatrix} x & 0 \\ 0 & \bar{x} \end{bmatrix}$$

where $a, b \in GF(p^2)$ satisfy $a\,\bar{a} + b\,\bar{b} = 1$.

It is easy to check that $ABC = 1$.

(2.9). LEMMA. *Let* $d > 2$ *be any divisor of* $\frac{p+1}{2}$. *Then there are* $(2, 3, d)$ *triples in* $PSl_2(p)$.

Proof. Let $x \in GF(p^2)^*$ be any element so that d is the least positive integer satisfying $x^d = \pm 1$. Then the matrix C in (2.8) has order d. Next we choose $a \in GF(p^2)^*$ so that $a(x - x^{-1}) = 1$. Since

$$GF(p) = \{b\,\bar{b} \mid b \in GF(p^2)\}$$

it follows that there exists $b \in GF(p^2)$ such that $a\,\bar{a} + b\,\bar{b} = 1$.

We now prove that the matrices A, B of (2.8) have orders 2, 3 respectively, that is we will show that $a + \bar{a} = 0$ and $ax + \bar{a}\,\bar{x} = \pm 1$. Since $x^{p+1} = 1$ we have

$$1 = a^p(x - x^{-1})^p = a^p(x^p - x^{-p}) = a^p(x^{-1} - x)\,.$$

This together with $1 = a(x - x^{-1})$ implies that $a^p = -a$, i.e., $a + \bar{a} = 0$. Finally

$$ax + \bar{a}\,\bar{x} = ax + a^p\,x^p = ax - ax^{-1} = a(x - x^{-1}) = 1\,. \qquad \text{Q.e.d.}$$

The next theorem proves one half of theorem I of the introduction.

(2.10). THEOREM. *Suppose* d *is a divisor of either* $\frac{p-1}{2}$ *or* $\frac{p+1}{2}$ *and suppose* $d > 6$. *Then there is a* $(2, 3, d)$ *triple* (A, B, C) *so that the group generated by* A, B, C *is* $PSl_2(p)$.

Proof. Let (A, B, C) be any $(2, 3, d)$ triple and set $G = \langle A, B, C \rangle$ = the subgroup generated by A, B, C. Since G has elements of order $d > 6$ it follows that G can not be a subgroup of A_4, S_4, A_5. Therefore, if $G \neq PSl_2(p)$, it follows that either $G \subseteq D$ or $G \subseteq H$, where D is a maximal dihedral subgroup and H is a maximal solvable subgroup (see (2.2)).

First we assume that $G \subseteq D$. Since B, ABA both have order 3 they must commute, i.e., $(AB)^2 = (BA)^2$. But then we have

$$(AB)^6 = (AB)^2AB(AB)^2AB = (BA\,BA)AB\,(BA\,BA)AB = BAB^2BAB^2 = 1$$

contradicting our hypothesis that $C = (AB)^{-1}$ has order $d > 6$.

Next assume that $G \subseteq H$. Since there is an extension

$$1 \to \mathbf{Z}_p \to H \xrightarrow{\theta} \mathbf{Z}_{(p-1)/2} \to 1$$

we see that $(AB)^6 \in \mathbf{Z}_p$ since A has order 2, B has order 3, and $\theta(A)$ and $\theta(B)$ commute. If $d \mid \dfrac{p-1}{2}$ then

$$1 = (AB)^{6p} = (AB)^{6\left(\frac{p-1}{2} + \frac{p-1}{2} + 1\right)} = (AB)^6 \quad \text{since} \quad (AB)^{\frac{p-1}{2}} = 1\,.$$

This contradicts the fact that AB has order $d > 6$. The argument for divisors of $\dfrac{p+1}{2}$ is similar. Q.e.d.

Summarizing we now know that $PSl_2(p)$ is generated by a $(2, 3, p)$ triple and also by any $(2, 3, d)$ triple, where $d > 6$ and d is a divisor of either $\dfrac{p-1}{2}$ or $\dfrac{p+1}{2}$. As far as the problem of minimum genus is concerned it turns out that in addition we only need determine those primes p for which $PSl_2(p)$ is generated by a triple of the form $(3, 3, 4)$, $(2, 5, 5)$, $(2, 4, 5)$.

According to (2.4) a matrix $C \in PSl_2(p)$ has order 4, respectively order 5, if, and only if, $\chi^2 \equiv 2\,(p)$, respectively $\chi^2 \pm \chi - 1 \equiv 0\,(p)$, where $\chi = \operatorname{trace} C$. But these equations are solvable over $\mathbf{Z}_p$ if, and only if, $p \equiv \pm 1\,(8)$, respectively $p \equiv \pm 1\,(5)$. Since every element of $\mathbf{Z}_p$ can arise as the trace of some matrix we have $PSl_2(p)$ has elements of order 4, respectively order 5, if, and only if, $p \equiv \pm 1\,(8)$, respectively $p \equiv \pm 1\,(5)$.

To construct $(3, 3, 4)$ triples consider matrices

(2.11). $$A = \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} a & b \\ c & -a+1 \end{bmatrix},$$

$$C = (AB)^{-1} = \begin{bmatrix} 1-a-b & a-1 \\ a-c & c \end{bmatrix}$$

where $-a^2 + a - bc \equiv 1\,(p)$.

A and B both have order 3 and C will have order 4 if, and only if, $(1-a-b+c)^2 \equiv 2\,(p)$. Therefore we need to find a, b, c satisfying

(2.12). $$-a^2 + a - bc \equiv 1\,(p) \quad \text{and} \quad (1-a-b+c)^2 \equiv 2\,(p).$$

Assume $p \equiv \pm 1\,(8)$ so that there is $\alpha \in \mathbf{Z}_p$ with $\alpha^2 \equiv 2\,(p)$. Then (2.12) is equivalent to

$$1 - a - b + c \equiv \alpha \quad \text{and} \quad a^2 - a + bc + 1 \equiv 0$$

which in turn is equivalent to finding b, c so that

(2.13). $-3 - 4bc$ is a quadratic residue mod p and

$$\frac{1 \pm \sqrt{-3 - 4bc}}{2} \equiv 1 - b + c - \alpha\,.$$

But this is the same as finding b, c so that

(2.14). $$-3 - 4bc \equiv \big(1 + 2(-b+c-\alpha)\big)^2\,.$$

Now solving for c we see that there is a solution, if, and only if, $-3b^2 + (2-4\alpha)b - 3$ is a quadratic residue for some choice of b. But quadratic polynomials always assume at least one quadratic residue and therefore it is possible to satisfy (2.12).

Thus we have proved the following theorem.

(2.15). THEOREM. *Suppose* $p \equiv \pm 1\,(8)$. *Then there are* (3, 3, 4) *triples in* $PSl_2(p)$, *one such being given by* (2.11), *where* a, b, c *are chosen to satisfy*

$$-a^2 + a - bc \equiv 1\,(p) \quad \textit{and} \quad (1-a-b+c)^2 \equiv 2\,(p)\,.$$

We still must prove that $PSl_2(p)$ can be generated by a (3, 3, 4) triple if $p \equiv \pm 1\,(8)$.

(2.16). THEOREM. *Suppose* $p \equiv \pm 1\,(8)$. *Then there are* (3, 3, 4) *triples in* $PSl_2(p)$ *and any such triple will generate* $PSl_2(p)$.

Proof. Let (A, B, C) be any (3, 3, 4) triple, which exists by (2.15), and let $G = \langle A, B, C\rangle$. We use (2.2) to prove that $G = PSl_2(p)$. First note that none of A_4, S_4, A_5 contain (3, 3, 4) triples. Secondly suppose that $G \subseteq D$, where D is a dihedral group. Since A, B are elements, of odd order (in a dihedral group) they commute and consequently AB will not have order 4.

Finally, suppose $G \subset H$, where H is a maximal solvable subgroup of $PSl_2(p)$. From the existence of the extension $1 \to \mathbf{Z}_p \to H \xrightarrow{\theta} \mathbf{Z}_{(p-1)/2} \to 1$ we see that $AB \in \mathbf{Z}_p$ since $\theta(AB)^4 = 1$ and $\theta(AB)^3 = 1$. But this is impossible since the order of AB is 4. Q.e.d.

To construct (2, 5, 5) or (2, 4, 5) triples in the case $p \equiv 1\,(5)$ consider the matrices

$$(2.17).\quad A = \begin{bmatrix} a & b \\ c & -a \end{bmatrix},\ B = \begin{bmatrix} -ax^{-1} & -bx \\ -cx^{-1} & ax \end{bmatrix},\ C = \begin{bmatrix} x & 0 \\ 0 & x^{-1} \end{bmatrix}$$

where $a, b, c, x \in GF(p)$ are chosen so that

$$-a^2 - bc = 1,\ x^5 = 1,\ x \neq \pm 1\,.$$

If we also have $p \equiv \pm 1\,(8)$ then we can choose a so that $a^2(x-x^{-1})^2 = 2$, and therefore (A, B, C) will be a (2, 4, 5) triple. On the other hand choosing a so that $\alpha = a(x-x^{-1})$ is a solution of $u^2 \pm u - 1 = 0$ will guarantee that (A, B, C) is a (2, 5, 5) triple.

In the case $p \equiv -1\,(5)$ we think of $PSl_2(p)$ as the projective special unitary group $PSU_2(p)$. Thus we have the matrices

$$(2.18).\quad A = \begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix},\ B = \begin{bmatrix} \bar{a}\,\bar{x} & -bx \\ \bar{b}\,\bar{x} & ax \end{bmatrix},\ C = \begin{bmatrix} x & 0 \\ 0 & \bar{x} \end{bmatrix}$$

where $a, b, x \in GF(p^2)$ are chosen to satisfy

$$a\,\bar{a} + b\,\bar{b} = 1,\ x^5 = 1,\ x \neq \pm 1\,.$$

x must also satisfy $x\,\bar{x} = 1$, that is $x^{p+1} = 1$. Since $p + 1 \equiv 0\,(5)$ this follows automatically.

First we choose x so that $x^5 = 1$, $x \neq \pm 1$ and then we choose a so that $a^2(x-x^{-1})^2 = 2$, assuming also that $p \equiv \pm 1\,(8)$. In other words let $\alpha \in GF(p)$ be such that $\alpha^2 = 2$ and then set $a(x-x^{-1}) = \alpha$. But then we have $a(x-x^{-1}) = \alpha = \alpha^p = a^p(x^p - x^{-p}) = a^p(x^{-1}-x) = -\bar{a}(x-x^{-1})$ and hence $a + \bar{a} = 0$. Therefore, with these choices, (2.18) is a (2, 4, 5) triple.

In a similar fashion the matrices in (2.18) will be a (2, 5, 5) triple if $a, b, x \in GF(p^2)$ are chosen to satisfy $a\,\bar{a} + b\,\bar{b} = 1$, $x^5 = 1$, $x \neq \pm 1$, $a(x-x^{-1}) = \alpha$, where $\alpha \in GF(p)$ is any solution of $u^2 \pm u - 1 = 0$. As a consequence we have the following result.

(2.19). THEOREM.

(a) *If* $p \equiv \pm 1\,(5)$ *then there are* (2, 5, 5) *triples in* $PSl_2(p)$.

(b) *If* $p \equiv \pm 1\,(5)$ *and* $p \equiv \pm 1\,(8)$ *then there are* $(2, 4, 5)$ *triples in* $PSl_2(p)$.

It still remains to prove that we can generate $PSl_2(p)$ by $(2, 5, 5)$ triples or $(2, 4, 5)$ triples.

(2.20). THEOREM. *If* $p \equiv \pm 1\,(5)$ *and* $p \equiv \pm 1\,(8)$ *then any* $(2, 4, 5)$ *triple will generate* $PSl_2(p)$.

Proof. Let (A, B, C) be any $(2, 4, 5)$ triple and let $G = \langle A, B, C\rangle$. Because of the orders of A, B, C it readily follows that $G \nsubseteq A_4, S_4, A_5$.

Suppose $G \subseteq D$, where D is a dihedral group of order $p \pm 1$. Then $BC = CB$, since elements of orders > 2 in a dihedral group commute. Therefore $(BC)^4 = C^4$. But also $(BC)^2 = 1$, and this together with $C^5 = 1$ implies that $C = 1$, a contradiction.

Finally suppose $G \subseteq H$, where H is a maximal solvable subgroup. Recall that we have an extension

$$1 \to \mathbf{Z}_p \to H \xrightarrow{\theta} \mathbf{Z}_{(p-1)/2} \to 1\,.$$

Then $C^4 \in \mathbf{Z}_p$ since $(BC)^2 = 1$ and

$$1 = \theta(BC)^4 = \theta(C^4)\,.$$

From this it follows that the order of C is p, a contradiction. Therefore $G = PSl_2(p)$. Q.e.d.

The generation of $PSl_2(p)$ by $(2, 5, 5)$ triples is more delicate since it is possible to generate A_5 by such triples.

(2.21). THEOREM. *If* $p \equiv \pm 1\,(5)$ *then there are* $(2, 5, 5)$ *triples generating* $PSl_2(p)$.

Proof. First we consider the case $p \equiv 1\,(5)$. The matrices A, B, C in (2.17) will be a $(2, 5, 5)$ triple if

$$-a^2 - bc = 1, \quad x^5 = 1, \quad x \neq \pm 1, \quad a(x - x^{-1}) = \alpha\,,$$

where $\alpha \in GF(p)$ is any solution of $u^2 \pm u - 1 = 0$. In particular $\alpha = x + x^{-1}$ is such a solution. In fact $\alpha^2 + \alpha - 1 = 0$.

As before let $G = \langle A, B, C\rangle$. By arguments similar to those of (2.20) we see that $G \nsubseteq A_4, S_4, D$ or H. To show that G can not be a subgroup of A_5 consider the matrix

$$C^2A = \begin{bmatrix} ax^2 & bx^2 \\ cx^{-2} & -ax^2 \end{bmatrix}.$$

The trace of this matrix is

$$\chi = a(x^2 - x^{-2}) = a(x - x^{-1})(x + x^{-1}) = (x + x^{-1})^2 .$$

Using (2.4) we can show that C^2A does not have order 2, 3, or 5, and this eliminates A_5. Hence $G = PSl_2(p)$ in this case.

For the case $p \equiv -1$ (5) we choose matrices A, B, C as in (2.18), where now

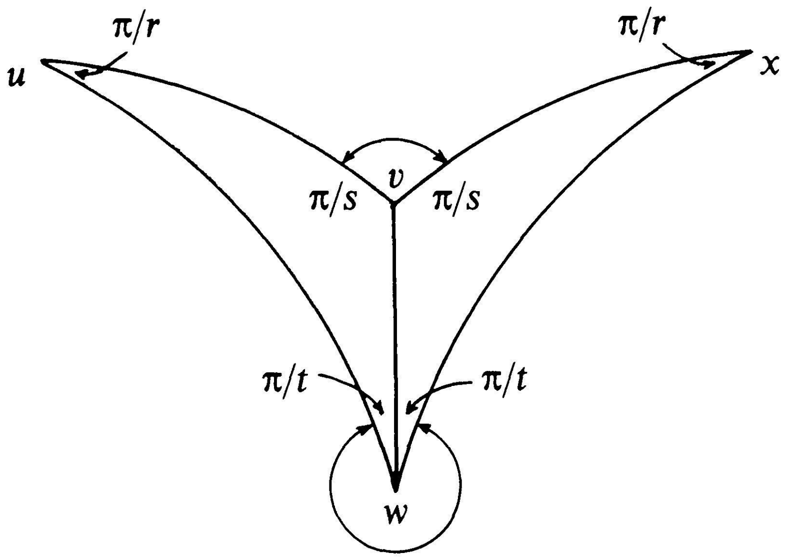
$$a\,\bar{a} + b\,\bar{b} = 1, \quad x^5 = 1, \quad x \neq \pm 1, \quad a(x - x^{-1}) = x + x^{-1} .$$

As in the first case we can show that $\langle A, B, C \rangle = PSl_2(p)$. Q.e.d.

Theorems (2.16), (2.20) and (2.21) now establish half of theorem II in the introduction. The other half follows from the result below.

(2.22). THEOREM. *Suppose* G *is a finite group and* (A, B, C) *is an* (r, s, t) *triple generating* G. *If* $1 \to \Delta \to T(r, s, t) \to G \to 1$ *is the associated extension then the genus of* H/Δ *is* $1 + \dfrac{|G|}{2}\left(1 - \dfrac{1}{r} - \dfrac{1}{s} - \dfrac{1}{t}\right)$.

Proof. A fundamental domain for the action of $T(r, s, t)$ on P, where P is the appropriate plane, consists of two copies of a triangle whose angles are π/r, π/s, π/t (see the diagram)



A, B, C are rotations about u, v, w through angles $2\pi/r$, $2\pi/s$, $2\pi/t$.

The only identifications under the action are: vu gets identified to vx and wu gets identified to wx. It follows that $P/T(r, s, t)$ is the 2 sphere and the branched covering $P/\Delta \to P/T(r, s, t)$ has 3 branch points coming from the vertices u, v, w.

Now notice that Δ is torsion free. This follows from the facts:

(1) the elements of finite order in $T(r, s, t)$ are the conjugates of A, B, C.

(2) elements of finite order in $T(r, s, t)$ map to elements of the same order in G. From this it follows that the orders of the branch points are r, s, t respectively.

Finally we consider the Riemann-Hurwitz formula:

$$\chi(P/\Delta) = |G| \left(\chi(P/T(r, s, t)) - \left(1 - \frac{1}{r}\right) - \left(1 - \frac{1}{s}\right) - \left(1 - \frac{1}{t}\right)\right)$$

i.e.,
$$2 - 2g = |G| \left(\frac{1}{r} + \frac{1}{s} + \frac{1}{t} - 1\right).$$

Therefore
$$g = 1 + \frac{|G|}{2}\left(1 - \frac{1}{r} - \frac{1}{s} - \frac{1}{t}\right)$$
Q.e.d.

§ 3. Conformal Actions on Surfaces of least Genus

If (A, B, C) is an (r, s, t) triple generating $PSl_2(p)$ then we have a short exact sequence

$$1 \to \Delta \to T(r, s, t) \to PSl_2(p) \to 1$$

where Δ is torsion free. Then it follows that $H/T(r, s, t)$ is S^2 and the branched covering $H/\Delta \to H/T(r, s, t)$ has 3 branch points with orders r, s, t.

Conversely we have:

(3.1). Theorem. *If S is a Riemann surface of least genus for $PSl_2(p)$ then $S/PSl_2(p)$ is S^2 and $\pi: S \to S/PSl_2(p)$ has 3 branch points.*

Proof. There exists a short exact sequence $1 \to \Delta \to T(2, 3, p) \to PSl_2(p) \to 1$ arising from a $(2, 3, p)$ triple and consequently

$$\text{genus}\ (H/\Delta) = 1 + \frac{|G|}{2}\left(\frac{1}{6} - \frac{1}{p}\right).$$