Projective Linear Groups as Maximal Symmetry Groups

Anna Torstensson
Centre for Mathematical Sciences
Box 118, SE-221 00 Lund, Sweden
Email: annat@maths.lth.se

Abstract

A maximal symmetry group is a group of isomorphisms of a three-dimensional hyperbolic manifold of maximal order in relation to the volume of the manifold. In this paper we determine all maximal symmetry groups of the types $PSL(2,q)$ and $PGL(2,q)$. Depending on the prime p there are one or two such groups with $q = p^k$ and k always equals $1, 2$ or 4.

AMS 2000 classification numbers: 20B25, 20G40.

1 Maximal symmetry groups of hyperbolic three-manifolds

An orientable n-dimensional hyperbolic manifold is a quotient space $M = \mathbb{H}^n/K$, where K is some torsion-free discrete subgroup of $\mathrm{Iso}^+(\mathbb{H}^n)$, the group of orientation-preserving isometries of n-dimensional hyperbolic space. For each n there is an upper bound on the quotient $\frac{|\mathrm{Iso}^+(M)|}{\mathrm{vol}(M)}$ taken over all hyperbolic n-manifolds and this bound is attained for certain manifolds M. For dimension n higher than 3 this is a consequence of the fact that the set of volumes is discrete ([12]).

For $n = 2$ there is a well known theorem by Hurwitz which states that any compact Riemann surface of genus $g \geq 2$ has at most $84(g-1)$ automorphisms. The automorphism groups of maximal order $84(g-1)$ are called Hurwitz groups. There has been a lot of research on finding out if certain groups are Hurwitz. The result that is most interesting in this context is the following theorem which can be found in [7]:

Theorem 1 *The simple group* $\mathrm{PSL}(2, q)$ *is Hurwitz precisely when* q *equals* 7*, or some prime* p *congruent to* ± 1 *modulo* 7*, or* p^3 *for some prime* p *congruent to* ± 2 *or* ± 3 *modulo* 7*.*

In this paper we will study the 3-dimensional analogue of Hurwitz groups, that is, groups that are automorphism groups of hyperbolic 3-manifolds for which the quotient $\frac{|\mathrm{Iso}^+(M)|}{\mathrm{vol}(M)}$ is maximal among all such manifolds. We will call such groups maximal symmetry groups of hyperbolic 3-manifolds, and prove a result analogous to the one mentioned above.

Let us first examine the quotient $\frac{|\mathrm{Iso}^+(M)|}{\mathrm{vol}(M)}$ for a manifold $M = \mathbb{H}^n/K$. Now the isometry group $\mathrm{Iso}^+(M)$ is isomorphic to N/K where N is the normaliser of K in $\mathrm{Iso}^+(\mathbb{H}^n)$, and with O defined by

$$O = \mathbb{H}^n/N \cong (\mathbb{H}^n/K)/(N/K) \cong M/\mathrm{Iso}^+(M),$$

it is clear that $\mathrm{vol}(O) = \mathrm{vol}(M)/|\mathrm{Iso}^+(M)|$, and hence that $\frac{|\mathrm{Iso}^+(M)|}{\mathrm{vol}(M)}$ is maximal precisely when $O = \mathbb{H}^n/N$ is of minimal volume. Note that O depends only on the normaliser $N(K)$ of K in $\mathrm{Iso}^+(\mathbb{H}^n)$ and not on the subgroup K itself.

Now assume that we have among all orientable n-dimensional orbifolds found one of minimal volume, say $O_1 = \mathbb{H}^n/N_1$. Then the manifolds with maximal symmetry group are those of the form $\mathbb{H}^n/K$ with $N(K) = N_1$. Note that if $N_1 \subseteq N(K)$ then we must have $N_1 = N(K)$, because otherwise $O' = \mathbb{H}^n/N(K)$ would have smaller volume than O_1, contrary to our assumption. Consequently, $N_1 = N(K)$ if and only if $N_1 \subseteq N(K)$, that is, if K is a normal subgroup of N_1. This leads us to study normal torsion-free subgroups K of N_1 and the corresponding quotients $N_1/K \cong \mathrm{Iso}^+(\mathbb{H}^n/K) = \mathrm{Aut}(\mathbb{H}^n/K)$.

In the case $n = 2$ the smallest orientable orbifold is the Hurwitz orbifold $O_1 = \mathbb{H}^2/\triangle(2,3,7)$, where $\triangle(2,3,7)$ is the orientation-preserving subgroup of the group of reflections in the sides of a triangle in the hyperbolic plane with angles $\pi/2$, $\pi/3$ and $\pi/7$. Since the area of the hyperbolic triangle is $\pi(1-1/2-1/3-1/7) = \pi/42$, the area of the fundamental domain of O_1 is $\pi/21$. Now the area of a Riemann surface S of genus $g \geq 2$ is $4\pi(g-1)$, and so it follows that

$$|\mathrm{Aut}(S)| = |\mathrm{Iso}^+(S)| \leq \mathrm{vol}(S)/\mathrm{vol}(0_1) = 84(g-1),$$

with equality if and only if $S = \mathbb{H}^2/K$ where K is a normal torsion-free subgroup of $\triangle(2,3,7)$.

From the presentation

$$\triangle(2,3,7) = \langle x, y | x^2 = y^3 = (xy)^7 = 1\rangle$$

of the triangle group it is clear that its abelianisation is trivial, or in other words the group is perfect. It follows that all Hurwitz groups, being quotients of $\triangle(2,3,7)$, also are perfect. In particular, since $[\mathrm{PGL}(2,q), \mathrm{PGL}(2,q)] = \mathrm{PSL}(2,q)$, we do not have any Hurwitz groups of the type $\mathrm{PGL}(2,q)$ unless q is a power of two so that $\mathrm{PGL}(2,q) = \mathrm{PSL}(2,q)$ and $\mathrm{PSL}(2,q)$ is Hurwitz. Thus all projective linear groups that are Hurwitz are those mentioned in theorem 1

Recently it has been shown that the discrete subgroup of $\mathrm{Iso}(\mathbb{H}^3)$ of smallest co-volume is the normaliser $\tilde{\Gamma}$ of the $[3,5,3]$-Coxeter group (as described in detail in the next section). This was achieved in a series of papers by Martin and Gehring ([3], [4], [2] and [5]) together with analyses of some special cases most of which can be found in [9] and [10]. We will therefore study quotients of Γ, the orientation-preserving subgroup of $\tilde{\Gamma}$, by normal torsion-free subgroups since these quotients will correspond to maximal symmetry groups in the 3-dimensional case. In [1] we proved the existence of infinitely many maximal symmetry groups of certain types. Concerning projective linear groups we obtained the following result:

Theorem 2 *For each prime p there is some power $q = p^k$ such that either* $\mathrm{PSL}(2,q)$ *or* $\mathrm{PGL}(2,q)$ *is a maximal symmetry group.*

It should be noted that the existence of infinitely many maximal symmetry groups of type $\mathrm{PSL}(2,q)$ also is a special case of an earlier result in [6] stating that for *any* hyperbolic three-manifold $\mathbb{H}^3/K$, the fundamental group K has an infinite number of quotients of the type $\mathrm{PSL}(2,F_p)$, F_p a field of prime cardinality.

In this paper we will make a more detailed study of which groups of the types $\mathrm{PSL}(2,q)$ and $\mathrm{PGL}(2,q)$ are maximal symmetry groups. The full answer to this question is given by theorem 10.

This problem has been studied before in [11] were a partial answer was obtained stating exactly for which $q \equiv 1$ modulo 10 at least one of the groups $\mathrm{PSL}(2,q)$ or $\mathrm{PGL}(2,q)$ is a maximal symmetry group. In this special case our results agree with those of Paoluzzi. (For a detailed comparison see the remark after theorem 10.)

2 The extended [3,5,3] Coxeter group

In the following let C be the $[3,5,3]$ Coxeter group, that is the group generated by four elements a, b, c and d subject to the defining relations

$$a^2 = b^2 = c^2 = d^2 = (ab)^3 = (bc)^5 = \\ = (cd)^3 = (ac)^2 = (ad)^2 = (bd)^2 = 1.$$

This group C can be interpreted as a group of hyperbolic isometries, generated by reflections in the faces of a hyperbolic tetrahedron in which the angle between two faces equals π/m where m is the order of the product of the reflections in the corresponding faces. Thus C is generated by the reflections in the faces of a tetrahedron having two faces intersecting at an angle $\frac{\pi}{5}$, each intersecting another face at an angle $\frac{\pi}{3}$, and all other angles being $\frac{\pi}{2}$.

The symmetry of the tetrahedron (which is naturally exhibited also in the Dynkin diagram of the Coxeter group) indicates that we can find some hyperbolic isometry that preserves the tetrahedron. It is not hard to see that such an isometry is given by a rotation interchanging the faces a and d and the faces b and c. (By abuse of notation we denote a face by the same letter as the reflection in that face - although it should always be clear from the context what we mean - and in the same way we use the letter denoting a hyperbolic rotation also to denote the axis of that rotation.) Extending our group by adding that rotation as a fifth generator, which we denote by t, gives us the following finitely-presented group:

$$\tilde{\Gamma} = \langle\, a, b, c, d, t \mid a^2 = b^2 = c^2 = d^2 = t^2 = atdt = btct \\ = (ab)^3 = (ac)^2 = (ad)^2 = (bc)^5 = (bd)^2 = (cd)^3 = 1 \,\rangle.$$

From this presentation it is not difficult to derive a presentation for the orientation preserving subgroup Γ generated by $x = ac$, $y = ad$, $z = ab$ and t:

$$\Gamma = \langle\, x, y, z, t \mid x^2 = y^2 = z^3 = t^2 = (yz)^2 = (xz)^5$$
$$= (xy)^3 = tyty = txtz^2t = tztxy = 1\,\rangle.$$

We will also use an alternative presentation of this group which has the advantage of containing only two generators. Expressed in $u = ty$, $v = z$ and $w = (uv)^2(uv^2)^2$ we get the following presentation of Γ (see [8]):

$$\Gamma = \langle u, v | u^2 = v^3 = w^5 = (v^2w^2)^2 = 1\rangle \tag{1}$$

This group is now known to be the discrete subgroup of $\mathrm{Iso}^+(\mathbb{H})$ of smallest co-volume [2]. Its torsion-free subgroups act fixed-point-freely on hyperbolic 3-space, and therefore give rise to 3-manifolds with maximal symmetry group. We will therefore examine which projective linear groups can be obtained as quotients of Γ by torsion-free subgroups.

3 Torsion subgroups

As we have seen the problem of finding maximal symmetry groups boils down to finding quotients of the finitely presented group Γ by normal, torsion-free subgroups. Next we will demonstrate that the subgroup we divide out always is torsion-free unless the quotient is trivial or cyclic of order two. To do this we will use a description of the torsion elements of Γ derived in [1], which says that a subgroup H of Γ is torsion-free if and only if none of its elements are conjugate to any element of the set

$$S = \{ab, ac, ad, bc, abac, bd, abad, cd, t, adt\}$$

If $g \in \Gamma$ and $H = \langle g \rangle$ this result says that g is a torsion element if and only if some power of g is conjugate to some element of S. We use this fact in the proof of the following lemma:

Lemma 3 *Let Γ be the group with presentation (1). Then all normal subgroups of Γ of index more than two are torsion-free.*

Proof: Assume that N is a normal subgroup of Γ containing a torsion element n. We have that $\Gamma = F/R$, where F is the free group on two generators and R the normal closure of the relators in the presentation (1) of Γ. Then $N = F_1/R$ for some subgroup F_1 of F. Some power of $n = f_1R$ is conjugate to some element sR of S and N being normal we must have that $sr \in F_1$ for some $r \in R$. Expressing each element of S in x, y, z and t we obtain the set $\{x, y, z, t, z^2x, zx, z^2y, zy, xy, yt\}$. In each case it is easy to see that including sr in $F_1 \subseteq F$ we get a subgroup of F of index one or two. Such a subgroup must be normal so $\Gamma/N \cong F/F_1$ and consequently $|\Gamma : N| = |F : F_1| \leq 2$. This shows that dividing out a normal subgroup with torsion elements the quotient can only have order one or two. ♦

4 Homomorphisms from Γ into projective linear groups

Lemma 4 *There exists a homomorphism from Γ into $PSL(2, q)$ if and only if the polynomial $g(s) = s^8 - 6s^6 + 12s^4 - 9s^2 + 1$ has a zero in F_q. If $s_1, s_2, \ldots, s_k$ are the zeroes of g in F_q then all such homomorphisms up to conjugacy in $PSL(2, q)$ are given by*

$$u \mapsto \begin{bmatrix} x & y \\ s_i + y - x & -x \end{bmatrix} v \mapsto \begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}$$

where for each s_i we can choose y as any element with $-3y^2 - 4s_iy - 4$ a square α^2 and then x as one of the two values $\frac{y \pm \alpha}{2}$. For each s_i there is at least one y satisfying this condition.

Note: The necessity part of this proof can be found in [8]. We repeat it here for the sake of completeness and because some of the arguments are used also in the sufficiency part of the proof.

Proof: We first prove that g must have a root in F_q for a homomorphism from Γ into $PSL(2,q)$ to exist. Assume that ϕ is such a homomorphism and let U and V be representatives of $\phi(u)$ and $\phi(v)$ in $SL(2,q)$ chosen such that $U^2 = -I$ and $V^3 = -I$. This is always possible since $V^3 = \pm I$ and we may replace V by $-V$ in case $V^3 = I$ and $U^2 = -I$ always holds for matrices of determinant one and projective order two. Having defined U and V we can define W as we defined w in the presentation (1). We will repeatedly use the identity $tr(XY) = tr(X)tr(Y) - tr(XY^{-1})$ which holds in $SL(2,K)$ for any field K in order to express the traces of the images of the relators of Γ in terms of $s = trace(UV)$. We have that $t = trace([U,V]) = s^2 - 1$ and $trace(W) = (s^2-1)(s^2-2) = t(t-1)$. Moreover

$$tr(V^{-1}W^2) = trace(W)(trace(W) - 1) - 1 = t^4 - 2t^3 + t - 1$$

(For details see section 4.7.2 in [8]). Now ϕ is a homomorphism so $\phi(v^{-1}w^2) = V^{-1}W^2$ must have projective order two or equivalently $h(t) = t^4 - 2t^3 + t - 1$ must be zero. We have that $h(t) = h(s^2-1) = s^8 - 6s^6 + 12s^4 - 9s^2 + 1 = g(s)$ so it follows that s, the trace of $\phi(uv)$ (up to sign) must be a root of $g(s)$ lying in F_q. Letting $s_1, s_2, \ldots, s_k$ be the roots of g in F_q we can now proceed to construct all possible homomorphisms into $PSL(2,q)$. Fix a root $s = s_j$ and assume that $\phi(uv)$ has trace s. Now all elements of order three in

$PSL(2,q)$ are conjugate so we may assume that

$$v \mapsto V = \begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}$$

The matrix $\phi(u)$ is of projective order two and hence of the form

$$U = \begin{bmatrix} x & y \\ z & -x \end{bmatrix}$$

Using $s = trace(UV) = x - y + z$ to substitute for z the condition $det(U) = 1$ becomes $x^2 - yx + sy + y^2 + 1 = 0$ which has the solutions $x = \frac{y \pm \alpha}{2}$ if $-3y^2 - 4sy - 4$ is a square with square root α and no solutions otherwise. Hence the existence of solutions depends on the choice of y, but for any expression $ay^2 + by + c$, $a \in F_q^*$ $b, c \in F_q$ there is some $y \in F_q$ that makes it a square. This can be seen simply by noting that there are $\frac{q-1}{2}$ non-squares in F_q and $ay^2 + by + c$ assumes $\frac{q+1}{2}$ different values. It now remains to check that the image of ϕ satisfies the relations of Γ. By the above computations we know that $trace(V^{-1}W) = s^8 - 6s^6 + 12s^4 - 9s^2 + 1 = 0$ so that $(V^{-1}W)^2 = 1$. Moreover $trace(W) = (s^2-2)(s^2-1)$ and a simple computation shows that $trace(W)^4 - 3trace(W)^2 + 1 = g(s)^2 + (2s^4 - 6s^2 + 4)g(s) = 0$. Now a matrix with determinant one is of projective order five if and only if its trace t satisfies $t^4 - 3t^2 + 1 = 0$. This shows that W is of order five and hence completes the proof. ♦

5 The images of the homomorphisms

Since finding the $PSL(2,q)$ and $PGL(2,q)$ that are maximal symmetry groups is equivalent to finding all surjective homomorphisms $\Gamma \to PSL(2,q)$ and $\Gamma \to PGL(2,q) \subset PSL(2,q^2)$

we need a way to find the images of the homomorphisms constructed in the above lemma. A very straightforward description of the subgroup generated by two given elements of $PSL(2,q)$ is given in the article [7] by Macbeath. Using his results we get the following theorem:

Theorem 5 *Let p be a prime and assume that $g(s) = s^8 - 6s^6 + 12s^4 - 9s^2 + 1$ factorises into $g_1 g_2 \cdots g_k$ in $F_p(s)$. Then $PGL(2,p^m)$ is a maximal symmetry group if and only if there is a factor g_i that is an even polynomial in s of order $2m$ and $PSL(2,p^m)$ is a maximal symmetry group if and only if g has a factor of degree m which is not an even polynomial.*

Proof: By MacBeath's results a subgroup of $PSL(2,K)$ generated by two elements U and V is determined by the triple

$$(\alpha, \beta, \gamma) = (trace(U), trace(V), trace(UV))$$

of elements in K. He classifies the triples into four different types: singular, exceptional, irregular and normal, according to the kind of group U and V generate. If U and V are images of a homomorphism from Γ into some $PSL(2,q)$ we know by Lemma 4 that $(\alpha, \beta, \gamma) = (0,1,s)$ where s is a zero of g. A triple is singular if the quadratic form $x^2 + y^2 + z^2 + \alpha yz + \beta zx + \gamma xy$ splits into linear factors in the algebraic closure of F_q. Now $x^2 + y^2 + z^2 + zx + sxy$ cannot be factorised as $(x + ay + bz)(x + cy + dz)$ over any field since eliminating c and d from the equations obtained by equating the coefficients gives the system $a(s-a) = 1, b(1-b) = 1, b(s-a) + a(1-b) = 0$ which implies that $s^2 = 3$ contradicting the fact that s is a zero of g. All exceptional triples are listed in Macbeath's article and the only ones starting with $0, 1$ are $(0,1,1)$, $(0,1,t)$ where $t^2 = 2$ (which is equivalent to t being the trace of a matrix of projective order four), and $(0,1,t)$ where $t^4 - 3t^2 + 1 = 0$ (which is equivalent to t being the trace of a matrix of projective order five). Now s cannot satisfy $s^2 = 2$ or $s^4 - 3s^2 + 1 = 0$ so our triple is not exceptional.

Triples that are neither singular nor exceptional are either irregular or normal. They are called irregular if the subfield K of F_q generated by the elements of the triple is a quadratic extention of a field K_0 and K_0 contains one element of the triple while the other two either are zero or elements $r \in K \backslash K_0$ with $r^2 \in K_0$. Clearly our triple $(0, 1, s)$ is irregular exactly when $K = F_p(s)$ is a quadratic extension of $K_0 = F_p(s^2)$ which in turn is equivalent to the minimal polynomial of s over F_p being even. The main conclusion in Macbeath's article is that the subgroup generated by U and V is $PSL(2, K)$ if the corresponding triple of traces is normal and $PGL(2, K_0)$ if the triple is irregular. The statement in our theorem now follows from this fact. ♦

By the above theorem the powers m that make $PSL(2, p^m)$ or $PGL(2, p^m)$ a maximal symmetry group are determined by the factorisation of g modulo p. Let us look at the factorisation for some small primes p to see which symmetry groups we get.

We will now try to describe the degrees occurring in the factorisation of $g(s)$ in terms of the prime we factorise modulo. One fact that is striking looking at the table is that g always factorises into two polynomials of degree four, which in some cases can be factorised further into factors of degree one or two. Let us first deal with the simplest case which is primes congruent to ± 1 modulo 10.

Proposition 6 *If p is a prime congruent to ± 1 modulo 10 then $g(s) = s^8 - 6s^6 + 12s^4 - 9s^2 + 1$ has a factorisation $(s^4 - 3s^2 + \alpha_1)(s^4 - 3s^2 + \alpha_2)$ where $\alpha_1 = \frac{3+\sqrt{5}}{2}$ and $\alpha_2 = \overline{\alpha_1} = \frac{3-\sqrt{5}}{2}$. If $\beta_k = 9 - 4\alpha_k$ is a square then the factor containing α_k factorises into a product of two even polynomials. In case $6 + 2\sqrt{\beta_k}$ is not a square these polynomials are irreducible and otherwise they can be further decomposed into four linear factors. If β_k is not a square the factor containing α_k is a product of two irreducible polynomials of degree two that are not even.*

Table 1: Maximal symmetry groups $PSL(2, p^m)$ and $PGL(2, p^m)$ for small primes p.

Prime	Factorisation of g(s)	Maximal symmetry groups
2	$(s^4 + s + 1)^2$	$PSL(2, 2^4)$
3	$(s^4 + s^2 + 2)(s^4 + 2s^2 + 2)$	$PGL(2, 3^2)$
5	$(s^2 + 2s + 3)^2(s^2 + 3s + 3)^2$	$PSL(2, 5^2)$
7	$(s^4 + 2s^3 + 6s^2 + 2s + 6)(s^4 + 5s^3 + 6s^2 + 5s + 6)$	$PSL(2, 7^4)$
11	$(s^2 + 4)^2(s^2 + 3s + 3)(s^2 + 8s + 3)$	$PSL(2, 11^2), PGL(2, 11)$
13	$(s^4 + s^3 + 4s^2 + s + 12)(s^4 + 12s^3 + 4s^2 + 12s + 12)$	$PSL(2, 13^4)$
17	$(s^4 + 8s^3 + 12s^2 + 6s + 16)(s^4 + 9s^3 + 12s^2 + 11s + 16)$	$PSL(2, 17^4)$
19	$(s^2 + 7)(s^2 + 9)(s^2 + 7s + 4)(s^2 + 12s + 4)$	$PSL(2, 19^2), PGL(2, 19)$
23	$(s^4 + 8s^2 + 11)(s^4 + 9s^2 + 21)$	$PGL(2, 23^2)$
29	$(s + 2)(s + 12)(s + 17)(s + 27)(s^2 + 7s + 23)(s^2 + 22s + 23)$	$PSL(2, 29), PSL(2, 29^2)$
31	$(s^2 + 14s + 19)(s^2 + 15s + 18)(s^2 + 16s + 18)(s^2 + 17s + 19)$	$PSL(2, 31^2)$
37	$(s^2 + s + 15)(s^2 + 5s + 32)(s^2 + 32s + 32)(s^2 + 36s + 15)$	$PSL(2, 37^2)$
41	$(s^2 + 14)(s^2 + 24)(s^2 + 14s + 35)(s^2 + 27s + 35)$	$PSL(2, 41^2), PGL(2, 41)$
43	$(s^4 + 3s^3 + 23s^2 + 7s + 42)(s^4 + 40s^3 + 23s^2 + 36s + 42)$	$PSL(2, 43^4)$
47	$(s^4 + 10s^2 + 43)(s^4 + 31s^2 + 35)$	$PGL(2, 47^2)$
53	$(s^2 + 14s + 31)(s^2 + 22s + 41)(s^2 + 31s + 41)(s^2 + 39s + 31)$	$PSL(2, 53^2)$
59	$(s + 10)(s + 27)(s + 32)(s + 49)(s^2 + 21)(s^2 + 35)$	$PSL(2, 59), PGL(2, 59)$
61	$(s^2 + 21)(s^2 + 37)(s^2 + 10s + 18)(s^2 + 51s + 18)$	$PSL(2, 61^2), PGL(2, 61)$
67	$(s^4 + 16s^2 + 53)(s^4 + 45s^2 + 43)$	$PGL(2, 67^2)$
71	$(s + 11)(s + 33)(s + 38)(s + 60)(s^2 + 25)(s^2 + 43)$	$PSL(2, 71), PGL(2, 71)$
73	$(s^4 + 13s^3 + 45s^2 + 24s + 72)(s^4 + 60s^3 + 45s^2 + 49s + 72)$	$PSL(2, 73^4)$
79	$(s^2 + 4)(s^2 + 72)(s^2 + 38s + 49)(s^2 + 41s + 49)$	$PSL(2, 79^2), PGL(2, 79)$
83	$(s^4 + 38s^3 + 55s^2 + 56s + 82)(s^4 + 45s^3 + 55s^2 + 27s + 82)$	$PSL(2, 83^4)$
89	$(s^2 + 28s + 79)(s^2 + 33s + 9)(s^2 + 56s + 9)(s^2 + 61s + 79)$	$PSL(2, 89^2)$
97	$(s^2 + 21s + 66)(s^2 + 36s + 72)(s^2 + 61s + 72)(s^2 + 76s + 66)$	$PSL(2, 97^2)$

Proof: In this proof we will use the Legendre symbol so first of all we recall that for any odd prime p the Legendre symbol, $\left(\frac{a}{p}\right)$, which is defined for any a not divisible by p, equals 1 when a is a quadratic residue modulo p and -1 otherwise. We also recall that three basic properties of the Legendre symbol are multiplicativity, $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, quadratic reciprocity, $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{1}{4}(p-1)(q-1)}$, and Eulers criterion, $\left(\frac{a}{p}\right) \equiv a^{\frac{1}{2}(p-1)}(\text{mod } p)$. Now assume that p is congruent to ± 1 modulo 10. Then

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) \equiv p^2 \equiv 1(\text{mod } 5) \tag{2}$$

so 5 is a quadratic residue modulo p. This shows that α_1 and α_2 are elements of F_p and hence gives the factorisation into two factors of degree four. Let us now examine such a factor $g_k(s) = s^4 - 3s^2 + \alpha_k$. A factorisation into two even polynomials $(s^2 + a)(s^2 + b)$ is possible if and only if the system $a + b = -3, ab = \alpha_k$ has a solution or equivalently $\beta_k = 9 - 4\alpha_k$ is a square. Moreover it is easy to verify that the roots of g_k are $\pm\frac{\sqrt{6\pm 2\sqrt{\beta_k}}}{2}$ and hence the possibility of further factorisation depends on whether $6 + 2\sqrt{\beta_k}$ and $6 - 2\sqrt{\beta_k}$ are squares or not. These two numbers are squares simultaneously because

$$\left(\frac{6 + 2\sqrt{\beta_k}}{p}\right)\left(\frac{6 - 2\sqrt{\beta_k}}{p}\right) = \left(\frac{36 - 4\beta_k}{p}\right) = \left(\frac{16\alpha_k}{p}\right) = \left(\frac{\alpha_k}{p}\right) = 1$$

The last equality holds because whenever p is congruent to ± 1 modulo 10 $PSL(2,p)$ is of order divisible by five and hence has an element of order five. The trace condition for an element of $PSL(2,p)$ to be of order five is that $t^4 - 3t^2 + 1 = 0$. Let γ be such a trace. Then γ^2 equals either α_1 or α_2 showing that at least one of them is a square. However their product is one so again we can conclude from their Legendre symbols that they are squares simultaneously, which in this case means that they both are squares. This concludes the case where β_k is a quadratic residue modulo p. Let us now assume that it is not. Then it is clear that g_k has no roots in F_p so all we can hope for is to write g_k as a product of two factors of degree two. On the other hand this is always possible because we will see that all we need is that one of the numbers $5 - 2\alpha_k$ and $1 + 2\alpha_k$ is a square. That this is the case is clear from the computation:

$$\left(\frac{5-2\alpha_k}{p}\right)\left(\frac{1+2\alpha_k}{p}\right) = \left(\frac{9-4\alpha_k}{p}\right) = \left(\frac{\beta_k}{p}\right) = -1$$

If $5-2\alpha_k$ is a square δ^2 we get the factorisation $g_k = (s^2+\delta s+1-\alpha_k)(s^2-\delta s+1-\alpha_k)$ and if $1 + 2\alpha_k$ equals δ^2 we can factorise g_k as $(s^2 + \delta s - 1 + \alpha_k)(s^2 - \delta s - 1 + \alpha_k)$. It is straightforward to verify that δ never equals zero in either of these two factorisations which shows that the factors are not even polynomials. This concludes the proof of the lemma. ♦

Corollary 7 *Let p be a prime congruent to ± 1 modulo 10 and let β_k be defined as in Proposition 6. Further let $\gamma_k = 6 + 2\sqrt{\beta_k}$ in case β_k is a square. Then all maximal symmetry groups of type $PSL(2,p^k)$ or $PGL(2,p^k)$ are given by:*

- *$PSL(2,p^2)$ if no β_k is a square*
- *$PSL(2,p^2)$ and $PSL(2,p)$ if exactly one β_k is a square and the corresponding γ_k is a square.*
- *$PSL(2,p^2)$ and $PGL(2,p)$ if exactly one β_k is a square and the corresponding γ_k is not a square.*
- *$PSL(2,p)$ if both β_k and both γ_k are squares.*
- *$PSL(2,p)$ and $PGL(2,p)$ if both β_k and exactly one γ_k are squares.*
- *$PGL(2,p)$ if both β_k but no γ_k are squares.*

Proof: This is a immediate consequence of Theorem 5 and Proposition 6. ♦

Remark: All the six cases in the corollary occur. Instances of primes exemplifying each case are given by 31, 29, 11, 229, 59 and 269 in that order.

Let us now move on to the case where p is not congruent to ± 1 modulo 10.

Proposition 8 *Let p be a prime not congruent to ± 1 modulo 10. Then $g(s)$ is a product of two irreducible polynomials of degree four unless both the conditions*

1. $p \equiv 1$ *modulo* 4

2. $p \equiv 1, 3, 4, 5, 9$ *modulo* 11

are satisfied in which case we have a factorisation into four non-even irreducible polynomials of degree two. When we have irreducible factors of degree four they are even when only the second condition is satisfied and otherwise non-even.

Remark: For odd primes the conditions (1) and (2) can be expressed in terms of the Legendre symbols

$$\left(\frac{-1}{p}\right), \left(\frac{-11}{p}\right), \left(\frac{11}{p}\right)$$

and as we will see the value of these Legendre symbols determine the existence of different types of factorisations of g. Computing the Legendre symbols above we find that

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

equals one if and only if (1) holds. Also, we have that

$$\left(\frac{-11}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{11}{p}\right) = \left(\frac{p}{11}\right) \equiv p^5 \text{ modulo } 11 \tag{3}$$

and the latter expression is one exactly when condition (2) is satisfied. The last of our Legendre symbols can be computed from the ones already examined, because

$$\left(\frac{11}{p}\right) = \left(\frac{-11}{p}\right)$$

if (1) holds and

$$\left(\frac{11}{p}\right) = -\left(\frac{-11}{p}\right)$$

if (1) does not hold. Consequently 11 is a quadratic residue if either both or none of the conditions (1) and (2) hold.

Proof: Throughout this proof we will assume that p is a prime $\not\equiv \pm 1$ modulo 10. For $p = 2, 5$ the result is clear from the factorisations given in table 1. For the rest of the proof we will assume that $p \neq 2, 5$. Let us first note that $g(s) = s^8 - 6s^6 + 12s^4 - 9s^2 + 1$ has no zeroes in F_p because if t is a zero then $(2t^4 - 6t^2 + 3)^2 = 5$. Now this is a contradiction because it follows from the computation (2) that 5 is a square in F_p for an odd prime $p \neq 5$ if and only if $p \equiv \pm 1$ modulo 10.

Now for each prime p we will find a factorisation as a product of two polynomials of order four and then analyse which of these can be broken down further into factors of order two. We will look at three different cases depending on the residue of p modulo 4 and 11.

First assume that $p \equiv 1$ modulo 4. In this case -1 is a square in F_p so we may use the field elements $4 + 2\sqrt{-1}$ and $4 - 2\sqrt{-1}$ in our factorisation. Noting that

$$\left(\frac{4+2\sqrt{-1}}{p}\right)\left(\frac{4-2\sqrt{-1}}{p}\right) = \left(\frac{20}{p}\right) = \left(\frac{5}{p}\right) = -1$$

it is clear that exactly one of these two elements is a square. Denoting that element by α we obtain the factorisation

$$g(s) = (s^4+\sqrt{\alpha}s^3+(\frac{\alpha}{2}-3)s^2+\frac{\sqrt{\alpha}}{2}(\frac{\alpha}{2}-5)s-1)(s^4-\sqrt{\alpha}s^3+(\frac{\alpha}{2}-3)s^2-\frac{\sqrt{\alpha}}{2}(\frac{\alpha}{2}-5)s-1) \quad (4)$$

Next we look at the case when -11 is a quadratic residue modulo p. Then

$$\left(\frac{6+2\sqrt{-11}}{p}\right)\left(\frac{6-2\sqrt{-11}}{p}\right) = \left(\frac{80}{p}\right) = \left(\frac{5}{p}\right) = -1$$

and similarly to in the above case we denote the element among $6+2\sqrt{-11}$ and $6-2\sqrt{-11}$ which is a square by β and then obtain the factorisation:

$$g(s) = (s^4+(-3-\frac{\sqrt{\beta}}{2})s^2+\frac{\beta}{8}+\frac{3\sqrt{\beta}}{4}+\frac{3}{2})(s^4+(-3+\frac{\sqrt{\beta}}{2})s^2+\frac{\beta}{8}-\frac{3\sqrt{\beta}}{4}+\frac{3}{2}) \quad (5)$$

Finally we consider the case when 11 is a square. Then we have that

$$\left(\frac{8+2\sqrt{11}}{p}\right)\left(\frac{8-2\sqrt{11}}{p}\right) = \left(\frac{20}{p}\right) = \left(\frac{5}{p}\right) = -1$$

and letting γ be the element of $8+2\sqrt{11}$ and $8-2\sqrt{11}$ that is a square we can again factorise g:

$$(s^4+\sqrt{\gamma}s^3+(\frac{\gamma}{2}-3)s^2+\frac{\sqrt{\gamma}}{2}(\frac{\gamma}{2}-7)s-1)(s^4-\sqrt{\gamma}s^3+(\frac{\gamma}{2}-3)s^2-\frac{\sqrt{\gamma}}{2}(\frac{\gamma}{2}-7)s-1) \quad (6)$$

We have now found three factorisations of g, one that is possible when p is congruent to 1 modulo 4, one that is possible when -11 is a square in F_p and one that is occurs when

11 is a square in F_p. Noting that

$$\left(\frac{-11}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{11}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{11}{p}\right)$$

is is clear that at least one of these factorisations always is possible because if p is not congruent to 1 modulo 4, then exactly one of the numbers 11 and -11 is a quadratic residue modulo p.

Since we have no roots, and hence no linear factors, this leaves us with the following possibilities: either g is a product of two irreducible polynomials of degree four or g is the product of two polynomials of order four, at least one of which can be decomposed into two irreducible factors of degree two. In the first case let $g(s) = f(s)h(s)$. Then $g(s) = g(-s) = f(-s)h(-s)$ is another factorisation and from uniqueness either f and h are even or $f(s) = h(-s)$. In the second case it follows from the fact that $g(s) = g(-s)$ that the order two factors can be paired together to form even polynomials of order four so that g is a product of two even polynomials of order four. Altogether we have shown that any decomposition of g in factors of degree four is either a product $f(s)f(-s)$ or a product $f(s)h(s)$ of even polynomials.

From this fact we will show that there are no other decompositions of g into two factors of degree four than the ones of the three types given above. Let us start with the case of even factors. Having a factorisation $g(s) = (s^4 + as^2 + b)(s^4 + cs^2 + d)$ is equivalent to the system of equations:

$$\begin{cases} a + c = -6 \\ b + d + ac = 12 \\ ad + bc = -9 \\ bd = 1 \end{cases} \tag{7}$$

being satisfied. Substituting for c and d using the first and last equation we get two equations in a and b. After the substitution we subtract a times the second equation from the third equation which results in

$$-9 + 6b + 2ab - 12a - 6a^2 - a^3 = 0$$

Now if $a = -3$ we must have $a = c = -3$ and $b + d = 3$, $bd = 1$, which implies that $(b-d)^2 = (b+d)^2 - 4bd = 5$ contradicting that 5 is not a square in F_p. If $a \neq -3$ we must have that $b = \frac{a^2+3a+3}{2}$ and substituting into one of the two equations in a and b we find that $a(a^4 + 12a^3 + 51a^2 + 90a + 59) = 0$. There is no solution of 7 with $a = 0$. Hence we must have

$$\frac{(4(a+3)^2 - 6)^2}{4} = 4(a^4 + 12a^3 + 51a^2 + 90a + 59) - 11 = -11$$

so -11 is a square and $(a+3)^2 = \frac{3 \pm \sqrt{-11}}{2}$ if we let $\sqrt{-11}$ denote one of the square roots. It follows that a is as in the factorisation 5 given above.

Now for the factorisations of type $g(s) = f(s)f(-s)$. Similarity to the above case we consider the system of equations:

$$\begin{cases} 2b - a^2 = -6 \\ 2d - 2ac + b^2 = 12 \\ 2bd - c^2 = -9 \\ d^2 = 1 \end{cases}$$

arising from the identity $g(s) = (s^4 + as^3 + bs^2 + cs + d)(s^4 - as^3 + bs^2 - cs + d)$. The possible values of d are ± 1 but for $d = 1$ we obtain the system of equations:

$$\begin{cases} 2b - a^2 = -6 \\ -2ac + b^2 = 10 \\ 2b - c^2 = -9 \end{cases} \tag{8}$$

Squaring the second equation we get $4a^2c^2 = b^4 - 20b^2 + 100$ and solving for a^2 and c^2 in the first and third equation respectively $4a^2c^2 = 4(2b+6)(2b+9) = 16b^2 + 120b + 216$. It is easily verified that no solution of 8has $b = -3$, so it follows that

$$\frac{(b^2-8)^2}{(2b+6)^2} = \frac{b^4 - 16b^2 + 64}{4b^2 + 24b + 36} = \frac{20b^2 + 120b + 180}{4b^2 + 24b + 36} = 5$$

so contradictory to our assumption about p we find that 5 is a square in F_p. Hence we only need to consider solutions with $d = -1$, or equivalently solutions to the system:

$$\begin{cases} 2b - a^2 = -6 \\ -2ac + b^2 = 14 \\ 2b + c^2 = 9 \end{cases}$$

Equating $4a^2c^2$ obtained from the second and from the first and third equation respectively in the same fashion as before now results in the equation

$$0 = (14 - b^2)^2 - 4(2b+6)(9-2b) = ((b-1)^2 - 11)((b+1)^2 + 1))$$

Substituting the four possible values of b into the equations we obtain exactly the factorisations (4) and (6).

This shows that (4), (5) and (6) are all factorisations into two factors of degree four.

Next we will argue that essentially two situations are at hand here. Either exactly one of the threes types of factorisations into factors of degree four occur, and in that case the factors are irreducible, or more than one of them occur and then the factorisation of g into irreducibles is a product of four polynomials of degree two. The argument is the following:

Assume that g has a factorisation of non-even type, that is of the form (4) or (6) given above. Then either $g(s) = f(s)f(-s)$ is a product of irreducible polynomials or they both factorise further since if $f(s) = h(s)k(s)$ then $f(-s) = h(-s)k(-s)$. (As before we know that all factors are either degree four or two from the non-existence of zeroes.) Now the second case occurs if and only if there also is a factorisation of g of even type because $h(s)h(-s)$ and $k(s)k(-s)$ are even and the other direction is clear from the uniqueness of factorisation and the above comment that all irreducible factors are of the same degree. The remaining case to deal with is when there is only an even factorisation of g. We want to show that the factors are irreducible. From the form of (5) the factors only differ by the choice of square root of β so if one factor can be decomposed we obtain a decomposition of the other factor by applying the field automorphism $\sqrt{\beta} \mapsto -\sqrt{\beta}$. However, if we have such a decomposition $g(s) = f(s)f(-s)h(s)h(-s)$ then $k_1 = f(s)h(s)$, $k_2 = f(-s)h(-s)$ gives a factorisation $g(s) = h_1(s)h_s(2)$ of non-even type, contradicting our assumption. We can now conclude that the decomposition of g into irreducible polynomials is a product of two factors of degree four if only one of the factorisations (4), (5) and (6) occur and the factors are even or not according to which one it is. Otherwise g is a product of four irreducibles of degree two. This occurs exactly when more than one of the three factorisations is possible and the degree two factors are always non-even since at least one of the factorisations of degree four is non-even. From the remark after the proposition it is clear that the conditions for existence of the different types of factorisations can be reformulated as in the proposition: If both (1) and (2) are satisfied all three factorisations are possible, if (1) but not (2) holds only 4 occurs, if (1) does not hold but (2) does only 5 applies and if none of the conditions hold true we only have a factorisation of type 6. This concludes the proof of our proposition. ♦

Corollary 9 *Let p be a prime with $p \not\equiv \pm 1$ modulo 10. Then all maximal symmetry groups of type $PSL(2,p^k)$ or $PGL(2,p^k)$ are given by:*

- *$PSL(2,p^2)$ if $p \equiv 1$ modulo 4 and $p \equiv 1,3,4,5$ or 9 modulo 11.*
- *$PGL(2,p^2)$ if $p \equiv 3$ modulo 4 and $p \equiv 1,3,4,5$ or 9 modulo 11.*
- *$PSL(2,p^4)$ otherwise.*

Proof: This is an immediate result of combining the above proposition with theorem 5. ♦

This completes the investigation of maximal symmetry groups of the types $PSL(2,p^k)$ and $PGL(2,p^k)$. For easy reference we collect our results in the following theorem:

Theorem 10 *Let p be a prime. In case $p \equiv \pm 1$ modulo 10 we consider the element of F_p given by $\beta_1 = 3 - 2\sqrt{5}$, $\beta_2 = 3 + 2\sqrt{5}$ and $\gamma_k = 6 + 2\sqrt{\beta_k}$ whenever β_k is a square in F_p. Then the following is a list of all maximal symmetry groups of type $PSL(2,p^k)$ or $PGL(2,p^k)$:*

- *$PSL(2,p)$ if $p \equiv \pm 1$ modulo 10 and some γ_k exists and is a square.*
- *$PSL(2,p^2)$ if $p \equiv \pm 1$ modulo 10 and some β_k is not a square or*

$$\begin{cases} p \not\equiv \pm 1 \textit{ modulo } 10 \\ p \equiv 1 \textit{ modulo } 4 \\ p \equiv 1,3,4,5,9 \textit{ modulo } 11 \end{cases}$$

- $PSL(2,p^4)$ *if*

$$\begin{cases} p \not\equiv \pm 1 \text{ modulo 10} \\ p \equiv 2,6,7,8,10 \text{ modulo } 11 \end{cases}$$

- $PGL(2,p)$ *if* $p \equiv \pm 1$ *modulo 10 and for some* k β_k *is a square but* γ_k *is not.*

- $PGL(2,p^2)$ *if*

$$\begin{cases} p \not\equiv \pm 1 \text{ modulo } 10 \\ p \equiv 3 \text{ modulo } 4 \\ p \equiv 1,3,4,5,9 \text{ modulo } 11 \end{cases}$$

Remark: In [11] the author proves that for prime powers $q \equiv 1$ modulo 10 every homomorphism with torsion-free kernel from the orientation preserving subgroup C^0 of C onto $PSL(2,q)$ extends to a homomorphism with torsion-free kernel from Γ onto either $PSL(2,q)$ or $PGL(2,q)$. Conversely the restriction to C^0 of such a homomorphism ϕ has an image of index one or two in $Im(\phi)$ and since $PSL(2,q)$ has no subgroups of index two and it is shown in [11] that there are no surjections from C^0 onto $PGL(2,q)$ every projective quotient of Γ must arise from a projective quotient of C^0 in this way. Paoluzzi then classifies all surjections from C^0 onto groups $PSL(2,q)$ and in the case with $q \equiv 1$ modulo 10 the result is as follows:

- $PSL(2,p)$ if $p \equiv 1$ modulo 10 and $3+2\sqrt{5}$ or $3-2\sqrt{5}$ is a square in F_p
- $PSL(2,p^2)$ if $p \equiv \pm 1$ modulo 10 and $3+2\sqrt{5}$ or $3-2\sqrt{5}$ is *not* a square in F_{p^2}
- $PSL(2,p^4)$ if $p \equiv \pm 3$ modulo 10 and $3+2\sqrt{5}$ or $3-2\sqrt{5}$ is *not* a square in F_{p^2}

It is clear that the first two results agree with those given in theorem 10. To see that the results concerning fourth powers of p agree we need to show that for primes p with $p^4 \equiv 1$ modulo 10 the two conditions agree. First note that for such primes $p \equiv \pm 3$ is equivalent to $p \not\equiv \pm 1$ modulo 10 so it remains to show that when this is the case then

$3+2\sqrt{5}$ or $3-2\sqrt{5}$ is *not* a square in F_{p^2} exactly when $p \equiv 2, 6, 7, 8, 10$ modulo 11. From (3) the latter condition is equivalent to -11 not being a quadratic residue modulo p. If both $3+2\sqrt{5}$ and $3-2\sqrt{5}$ are squares then so is their product -11. On the other hand, if -11 is a square then $3+2\sqrt{5}$ is the square of $a+b\sqrt{5}$ where $b = 1/a$ and b^2 equals one of the numbers $\frac{3\pm\sqrt{-11}}{10}$. (The product of the Legendre symbols equals the Legendre symbol of 5 which is -1 for the primes considered so there is such a b.)

References

[1] Marston Conder, Gaven Martin, and Anna Torstensson. Maximal symmetry groups of hyperbolic 3-manifolds. *New Zealand J. Math.*, 35(1):37–62, 2006.

[2] F. W. Gehring and G. J. Martin. Minimal co-volume lattices, i: spherical points of a Kleinian group. *to appear.*

[3] F. W. Gehring and G. J. Martin. Precisely invariant collars and the volume of hyperbolic 3-folds. *J. Differential Geom.*, 49(3):411–435, 1998.

[4] F. W. Gehring and G. J. Martin. The volume of hyperbolic 3-folds with p-torsion, $p \geq 6$. *Quart. J. Math. Oxford Ser. (2)*, 50(197):1–12, 1999.

[5] F. W. Gehring and G. J. Martin. (p, q, r)-Kleinian groups and the Margulis constant. In *Complex analysis and dynamical systems II*, volume 382 of *Contemp. Math.*, pages 149–169. Amer. Math. Soc., Providence, RI, 2005.

[6] D. D. Long and A. W. Reid. Simple quotients of hyperbolic 3-manifold groups. *Proc. Amer. Math. Soc.*, 126(3):877–880, 1998.

[7] A. M. Macbeath. Generators of the linear fractional groups. In *Number Theory (Proc. Sympos. Pure Math., Vol. XII, Houston, Tex., 1967)*, pages 14–32. Amer. Math. Soc., Providence, R.I., 1969.

[8] Colin Maclachlan and Alan W. Reid. *The arithmetic of hyperbolic 3-manifolds*, volume 219 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2003.

[9] T. H. Marshall and G. J. Martin. Minimal co-volume lattices, ii: simple torsion in Kleinian groups. *to appear.*

[10] Bernard Maskit. *Kleinian Groups*, volume 287 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1988.

[11] Luisa Paoluzzi. $\mathrm{PSL}(2, q)$ quotients of some hyperbolic tetrahedral and Coxeter groups. *Comm. Algebra*, 26(3):759–778, 1998.

[12] Hsien Chung Wang. Topics on totally discontinuous groups. In *Symmetric Spaces (Short Courses, Washington Univ., St. Louis, Mo., 1969–1970)*, pages 459–487. Pure and Appl. Math., Vol. 8. Dekker, New York, 1972.