Thesis submitted for the degree of Doctor Philosophiae

Actions of $PSL(2,q)$ on hyperbolic 3-manifolds

Candidate:

Monique A. GRADOLATO

Supervisor:

PROF. Bruno ZIMMERMANN

Academic Year 1992/93

La solidarité par la science

La science n'a pas de nationalité; elle est aussi bien allemande, anglaise, italienne, russe ou japonaise que française. Elle progresse par les petites nations aussi bien que par les grandes; chacune apporte son concours à l'œuvre commune, et c'est pourquoi tous les peuples civilisés sont solidaires. Toute perte éprouvée par l'un d'eux ou infligée à l'un d'eux est une perte pour l'ensemble de l'humanité.

Quand ces vérités seront enseignées par tous et auront pénétré tous les esprits dans les couches sociales les plus élevées des aristocraties aussi bien que dans les couches populaires les plus profondes des démocraties, on aura compris que la véritable loi des intérêts humains n'est pas une loi de lutte et d'égoïsme, mais une loi d'amour. Voilà comment la science proclame que le but final de ses enseignements est la solidarité et la fraternité universelles.

Berthelot

Contents

Introduction 1

1 Geometric preliminaries 3
- 1.1 Surfaces 3
- 1.2 Braids 4
- 1.3 Maximally symmetric 3-manifolds 5
- 1.4 Bounding actions 7

2 The Projective Linear Groups over Finite Fields 13
- 2.1 Preliminary notions 13
- 2.2 Subgroups and Generators 22
- 2.3 The Isomorphic Unitary Groups 23

3 Actions of $PSL(2,q)$ and $PGL(2,q)$ 27
- 3.1 First example 27
- 3.2 Hurwitz actions 30

4 Applications 49
- 4.1 The group $C[4,3,5]^+$ maps onto $PSL(2,31)$ 49
  - 4.1.1 Maps of $C[4,3,5]^+$ onto $PSL(2,p)$ 50
  - 4.1.2 Decreasing the order of the target 51
- 4.2 The bounded 3-dimensional hyperbolic Coxeter tetrahedra 54
- 4.3 Non-orientable hyperbolic 3-manifolds 57

5 Tables and programs 61

6 Final remarks 77
- 6.1 Other Hurwitz groups 77
- 6.2 The group $C[4,3,5]^+$ does not map onto A_7 78

A Appendix 81
- A.1 Congruences and primes 81
- A.2 Applying Čebotarev's theorem on prime numbers 82

Introduction

Let G be a finite group of orientation preserving isometries of a closed orientable hyperbolic 2-manifold $\mathcal{F}_g$ of genus $g > 1$ (or equivalently, a finite group of conformal automorphisms of a closed Riemann surface). We say that the G-action on $\mathcal{F}_g$ *bounds a hyperbolic 3-manifold* $\mathcal{M}$ if $\mathcal{M}$ is a compact orientable hyperbolic 3-manifold with totally geodesic boundary $\mathcal{F}_g$ (as the only boundary component) such that the G-action on $\mathcal{F}_g$ extends to a G-action on $\mathcal{M}$ by isometries. "Symmetrically" we will also say that the 3-manifold $\mathcal{M}$ *bounds the given G-action.* We are especially interested in *Hurwitz actions*, i.e. finite group actions on surfaces of maximal possible order $84(g-1)$; the corresponding finite groups are called *Hurwitz groups.* First examples of bounding and non-bounding Hurwitz actions have been given in [33].
An important family of finite groups are the linear groups over finite fields, in particular the *projective special linear groups* $PSL(2,q)$ which are simple groups. We consider the case of Hurwitz actions of type $G \cong PSL(2,q)$, which have been classified by Macbeath [15]. Our method allows to construct various infinite families of bounding Hurwitz actions of this type and gives strong evidence for the general conjecture that all Hurwitz actions of type $PSL(2,q)$ should bound hyperbolic 3-manifolds, with the only exception of the smallest Hurwitz group $PSL(2,7)$ of order 168 acting on Klein's quartic curve of genus 3 (see [6]), which does not bound. We also construct an infinite family of non-bounding Hurwitz actions.

For the proofs we shall use the theory of hyperbolic 3-orbifolds. In fact our 3-manifolds which bound a given Hurwitz action will be regular coverings of a certain kind of hyperbolic 3-orbifolds with a small number of vertices and edges in the singular graph (it seems to be indeed the minimal possible choice). Depending on the given group $PSL(2,q)$ and on the orbifold in this class, we get certain number theoretical conditions which guarantee that a covering of the orbifold bounds the given $PSL(2,q)$ action. This allow us to construct various infinite families of bounding $PSL(2,q)$-actions. It seems that the method gives a positive answer for each fixed value of q, for example we have found that all Hurwitz actions of type $PSL(2,q)$, for $q = p$ prime, $7 < p < 1000$.In particular, forgetting about the group actions, all the corresponding hyperbolic surfaces bound hyperbolic 3-manifolds, a fact we do not know for Klein's quartic curve. The necessary computations have been done with the aid of a computer VAX. All these results bring us to strongly believe that any Hurwitz action of $PSL(2,q)$ type should bound, but a general solution seems to require some intricate number-theoretical considerations.

We underline that all hyperbolic 3-manifolds considered, together with their $PSL(2,q)$-actions, are maximally symmetric with respect to the equivariant Heegaard genus for 3-manifolds with boundary (see [32], [33]): they admit a Heegaard splitting, invariant under the group action, into a handlebody of genus g and a product-with-handles such that the group action is of maximal possible order $12(g-1)$. This is due to our choice of the quotient orbifolds. Of course also the order $84(g-1)$ is maximal for finite group actions on compact 3-manifolds with one boundary component of genus $g > 1$; in particular the Hurwitz $PSL(2,q)$-actions on hyperbolic 3-manifolds constructed in this work coincide with the orientation preserving isometry group. So the constructed actions are maximal both from a 2- and 3-dimensional point of view.

We have further applied the main Theorem 3.2.10 to the case of closed tetrahedral manifolds, that is the 3-manifolds that admit a quotient orbifold with a tetrahedron as singular set. A further development of the above number theoretical conditions allows us to show the existence of actions of $PSL(2,q)$-type also on non-orientable manifolds of tetrahedral type, thus giving a 3-dimensional analogue of the H^*-groups considered by Singerman in [25].

Let us briefly describe the contents of the various Chapters.

In the first, we collect some geometric constructions and observations, which will be needed later; in particular we introduce the class of hyperbolic 3-orbifolds we shall use. We refer to [29, Ch.13] and [30, Ch.5] for the theory of hyperbolic 3-orbifolds and to [33] for the maximally symmetric 3-manifolds with respect to the Heegaard decomposition.

The second Chapter contains definitions and properties of the projective linear groups. The main references are [8] and [15]. We have also referred to [10] and [11].

In the third Chapter we discuss the number theoretical conditions for the existence of a $PSL(2,q)$-action on a hyperbolic 3-manifold bounding a given Hurwitz action.

In the fourth Chapter we apply the framework of the third Chapter to manifolds of tetrahedral type.

In the fifth Chapter we present the tables and the computer programs, that were used to check the number theoretical conditions. The programs are written in the Pascal language.

We have added an appendix to describe some number theoretical tools and applications belonging to our context. In particular we describe an application of the Čebotarev's density theorem on prime numbers; a similar application is done by Mushtaq in [18, §4.3, §5.5] and [19, p.3882]. A good and recent introductory book on elementary number theory is the work of Rosen [22].

Acknowledgements I would like to express my sincere and grateful thanks to prof. Bruno Zimmermann for having devote part of his precious time to this thesis.

Chapter 1

Geometric preliminaries

All manifolds and orbifolds are supposed orientable and hyperbolic if the contrary is not explicitely mentioned.

1.1 Surfaces

Let p, q, m be integers bigger or equal to 2. Take a spherical, euclidean or hyperbolic triangle with angles π/p, π/q and π/m. The reflections in the sides of the triangle generate the *extended triangle group* $[p, q, m]$ while the subgroup of index 2 of orientation preserving elements is the *triangle group* (p, q, m) [2, §10.6]. These groups have presentation as follows

1.1.1
$$\begin{aligned}
&(p,q,m) = \langle x, y, t \mid x^p = y^q = t^m = 1, x\,y = t\rangle \\
&[p,q,m] = \langle r_1, r_2, r_3 \mid r_1^2 = r_2^2 = r_3^2 = 1, \\
&\qquad\qquad (r_1\,r_2)^p = (r_2\,r_3)^q = (r_1\,r_3)^m = 1\rangle \\
&\textit{where } x = r_1\,r_2,\ y = r_2\,r_3 \textit{ and } t = r_1\,r_3.
\end{aligned}$$

In particular $(2, 2, m)$ is the dihedral group $\mathbb{D}_m$ of order $2m$, whereas $(2, 3, 3)$, $(2, 3, 4)$ resp. $(2, 3, 5)$ are the tetrahedral group A_4, the octahedral group S_4 resp. the dodecahedral group A_5. If $1/p + 1/q + 1/m < 1$ then (p, q, m) is a hyperbolic triangle group and $\mathbb{H}^2/(p, q, m)$, where $\mathbb{H}^2$ denotes the hyperbolic plane, is a hyperbolic 2-orbifold denoted by $\mathcal{S}^2(p, q, m)$: it has the 2-sphere $\mathcal{S}^2$ as underlying topological space, and as branch set 3 branch points of orders p, q and m.

Suppose the finite group G is a surjective image of the hyperbolic triangle group (p, q, m) with torsion free kernel: we have the exact sequence

$$\mathbb{I} \longrightarrow ker\,\varphi \longrightarrow (p,q,m) \xrightarrow{\varphi} G \longrightarrow \mathbb{I}.$$

Then $\mathbb{H}^2/ker\,\varphi$ is a hyperbolic (or Riemann) surface $\mathcal{F}$ of genus $g > 1$ on which G acts discontinously by isometries (or conformal automorphisms) [2], [11]. Moreover the fundamental group $\pi_1(\mathcal{F})$ coincides with $ker\,\varphi$ and the genus $g_{\mathcal{F}}$ of $\mathcal{F}$ is given by

$$g_{\mathcal{F}} = 1 + (1 - 1/p - 1/q - 1/m)\,|G|/2,$$

where $|G|$ denotes the order of G. The Riemann surface $\mathcal{F}$ is a regular covering of the good 2-orbifold $\mathcal{S}^2(p,q,m)$. The group of isometries (or conformal automorphisms) is finite and its order is bounded by $84(g-1)$. When the bound is attained the action is called Hurwitz (see [6] for the theory of Hurwitz actions).

Suppose the group G admits a Hurwitz action on $\mathcal{F}_g$. Then the quotient $\mathcal{F}_g/G$ is the hyperbolic 2-orbifold $\mathcal{S}^2(2,3,7)$, and the action is determined by a surjection with torsion-free kernel

$$\varphi : (2,3,7) = \pi_1(\mathcal{S}^2(2,3,7)) \twoheadrightarrow G$$

(up to automorphisms of G). Here $\pi_1(\mathcal{S}^2(2,3,7))$ denotes the orbifold fundamental group. In fact, the G-action on $\mathcal{F}_g$ is given by the regular orbifold covering of $\mathcal{S}^2(2,3,7)$ corresponding to the kernel of φ isomorphic to $\pi_1(\mathcal{F}_g)$. For more general finite group actions on surfaces, one replaces the triangle group by a more general Fuchsian group.

Remark: *Working with triangle groups the Riemann surface structure on $\mathcal{F}_g$ is uniquely determined, because the Teichmüller space of a triangle is one point only.*

1.2 Braids

Let fix three strings. The group of braids in three strings is generated by two elements σ_1 and σ_2 [7, p.62]:

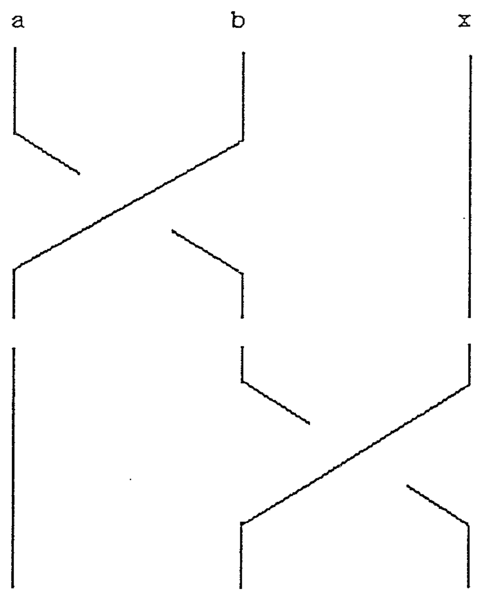


Fig.1

σ_1 is a positive half-turn between the first and the second string, σ_2 the same but between the second and the third. There is only one relation between the two generators, namely

$$\sigma_1\,\sigma_2\,\sigma_1 = \sigma_2\,\sigma_1\,\sigma_2.$$

To each string we may associate a generator of the free group of rank 3: call a, b and x the generators. Suppose that, from left to right, the strings are named a, b respectively x. Then we consider a braid σ also as an automorphism of the free group and precisely

$$\begin{array}{lll} \sigma_1(a) := b; & \sigma_1(b) := b^{-1}\,a\,b; & \sigma_1(x) := x \\ \sigma_2(a) := a; & \sigma_2(b) := x; & \sigma_2(x) := x^{-1}\,b\,x \end{array}.$$

We write the product of braids (and of the corresponding automorphism) as composition, i.e. reading from right to left when going down from top to bottom.

1.3 Maximally symmetric 3-manifolds

Analogously to the Hurwitz bound $84(g-1)$ for closed Riemann surfaces of genus $g > 1$, the maximal possible order of a finite group G of orientation preserving homeomorphisms of the orientable 3-dimensional handlebody V_g of genus $g > 1$ is $12(g-1)$ [33]. The role of the triangle group $(2,3,7)$ is played by the following four products with amalgamation:

1.3.1 $\quad \mathbb{G}_m := (2,2,m) \underset{Z_m}{*} (2,3,m), \quad m = 2,3,4,5,$

i.e. the maximal handle-body groups G are exactly the finite groups that are surjective images of $\mathbb{G}_i$, for at least one $i = 1,2,3,4$, such that the surjection is injective restricted to the amalgamated groups $(2,k,m)$.

The quotient orbifold has the 3-ball as underlying topological space, singular space as in the figure below

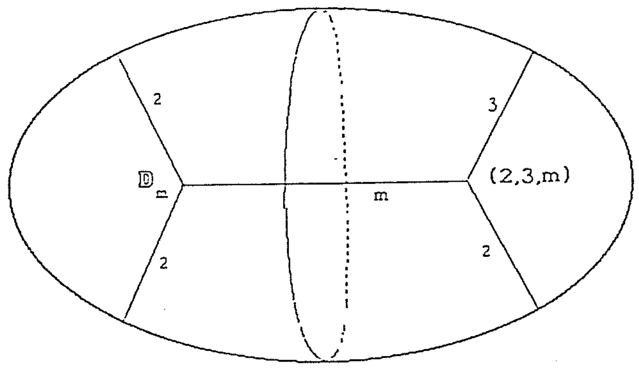


Fig.2

and fundamental group $\mathbb{G}_m$.

Notice that the vertex groups of the singular set of a 3-orbifold are submitted to conditions described in the main Theorem of [16, p. 379] and Figure 6 [16, p.389]: the possible choices are $\mathbb{Z}_m$, $\mathbb{D}_m$, $\mathbb{A}_4$, $\mathbb{S}_4$ or $\mathbb{A}_5$. So the picture around a vertex of the singular set must be one of the following:

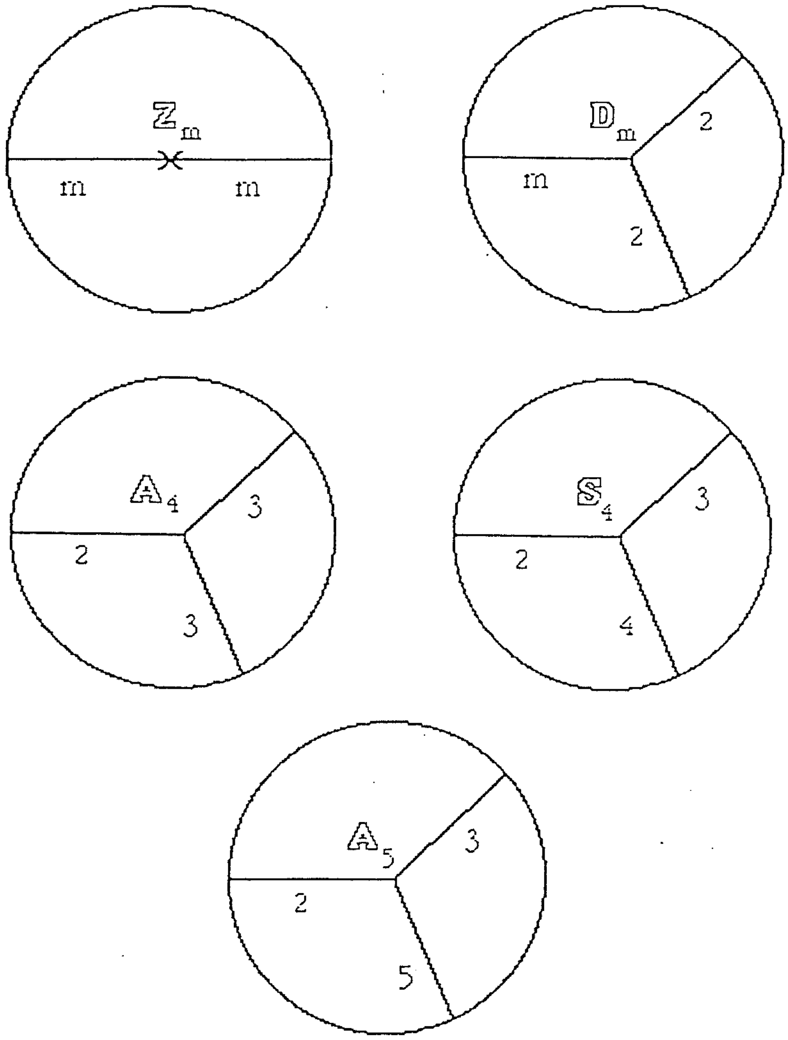


Fig.3

A closed orientable 3-manifold is called *maximally symmetric* if $\mathcal{M}$ has a Heegaard splitting of genus $g > 1$ and a finite group G of orientation preserving homeomorphisms of maximal possible order $12(g-1)$ which preserves both handlebodies of the Heegaard splitting (but does not leave invariant a Heegaard splitting of genus 0 and 1). Also the G-action is called *maximally symmetric.* Moreover G is a $\mathbb{G}_m$-group, i.e. a quotient of $\mathbb{G}_m$ by a torsion free normal subgroup. The maximally symmetric 3-orbifolds $(\mathcal{M}, G)$ are exactly the finite regular coverings of an orbifold with underlying topological space S^3 and singular set as in figure below:

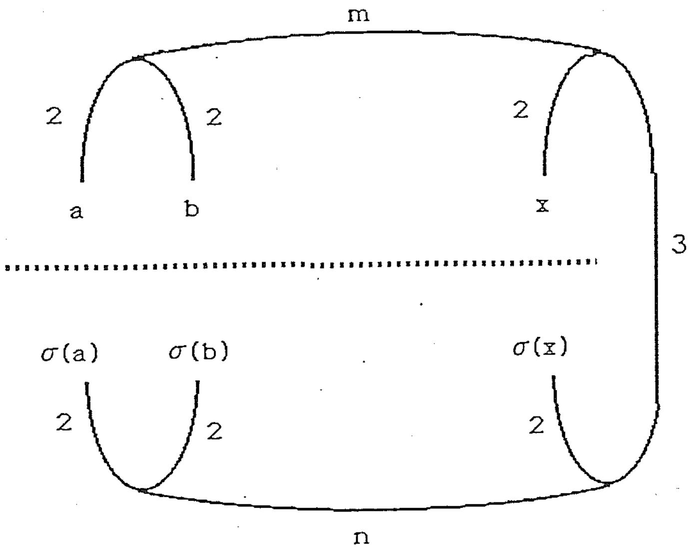


Fig.4

The concept of maximally symmetric 3-manifold is extended to 3-manifolds with boundary. In particular we will consider totally geodesic boundaries with one or two components. The groups acting on these general maximally symmetric 3-manifolds are now $\mathbb{G}_m$-groups for arbitrary m bigger than 2.

1.4 Bounding actions

Now from groups acting on surfaces we want to obtain actions on 3-manifolds with the starting surfaces as totally geodesic boundary.

We give the following:

1.4.1 Definition *The G-action on a hyperbolic surface $\mathcal{F}_g$* bounds a hyperbolic 3-manifold $\mathcal{M}$ *if $\mathcal{M}$ is a compact orientable hyperbolic 3-manifold with totally geodesic boundary $\mathcal{F}_g$ (as the only boundary component), such that the G-action on $\mathcal{F}_g$ extends to a G-action on $\mathcal{M}$ by isometries. "Symmetrically" we will say that $\mathcal{M}$* bounds the G-action *on $\mathcal{F}_g$.*

The following Proposition will assure later that we have only one boundary component.

1.4.2 Proposition *Let E be the fundamental group of a hyperbolic (good) compact 3-orbifold Q, closed or with totally geodesic boundary. Suppose we are given a surjection onto a finite group G*

$$\phi : E \twoheadrightarrow G,$$

whose kernel K is torsion free, and a connected subset Ω of Q. Then the number of connected components in the preimage of Ω in $\mathcal{M}$, the hyperbolic 3-manifold *which regularly covers Q with G as group of covering transformations, equals the index of $\phi(i_* \pi_1(\Omega))$ in G.*

Proof

The universal covering $\widehat{Q}$ of Q is $\mathbb{H}^3$ or a subset of $\mathbb{H}^3$ bounded by hyperbolic planes. Then $E = \pi_1(Q)$ acts as group of hyperbolic isometries on the universal covering of Q. Since $K = ker\phi$ is torsion free and normal in E, the quotient $\mathcal{M} := \widehat{Q}/K$ is a manifold and a regular covering of Q. The group G is exactly the group of deck transformations of $\mathcal{M}$ over Q.

Assume the index of $\phi(i_* \pi_1(\Omega))$ in G be equal to n. Take n elements

$$g_1 = 1,\ g_2,\ \ldots,\ g_n$$

from the different cosets of $\phi(i_* \pi_1(\Omega))$. The set

$$\{g_i\, \phi(i_* \pi_1(\Omega))\}_{i=1,\ldots,n}$$

is a coset decomposition of G. Let $e_1, \ldots, e_n$ be n elements in E such that

$$\phi(e_i) = g_i, \quad i = 1, \ldots, n.$$

Since $\phi(i_* \pi_1(\Omega))$ is a subgroup in $G \cong E/K$ of index n, there exists a subgroup F of index n in E such that $\phi(F) = \phi(i_* \pi_1(\Omega))$.

Suppose it is $e \in F$. Then there exists $f \in i_* \pi_1(\Omega)$ such that

$$\phi(e) = \phi(f) \quad \text{and so} \quad e\, f^{-1} \in K.$$

Fix a component $\widehat{\Omega}$ in the preimage of Ω. Then all the subsets $e(\widehat{\Omega})$, $e \in F$, collapse to one subset $\mathcal{N}_1$ in $\mathcal{M}$. Similarly happens to the subsets $e_i\, e(\widehat{\Omega})$, $e \in F$, separately for any i, $i = 2, \ldots, n$. We obtain exactly n different subsets $\mathcal{N}_1, \mathcal{N}_2, \ldots \mathcal{N}_n$ in $\mathcal{M}$ such that

$$\mathcal{N}_i = g_i(\mathcal{N}_1), \quad i = 2, \ldots, n.$$

■

And in particular we are interested in the following

1.4.3 Corollary *In the above hypothesis, suppose the fundamental group of the subset Ω maps onto G. Then the preimage of Ω in $\mathcal{M}$ is connected.* ■

In particular consider a Hurwitz action G on $\mathcal{F}_g$, which bounds a hyperbolic 3-manifold $\mathcal{M}$. Then the quotient $\mathcal{M}/G$ is a hyperbolic 3-orbifold having $\mathcal{F}_g/G = \mathcal{S}^2(2,3,7)$ as totally geodesic boundary, $\mathcal{F}_g = \partial\mathcal{M}$.

We will also consider the case of $n = 2$. Then the boundary has exactly two connected components, isomorphic to each other.

We shall define now a class of 3-orbifolds which will be used in Chapter 3.

The underlying topological space is the 3-disk $\mathcal{D}^3$, the boundary the 2-orbifold $\mathcal{S}^2(2,3,m)$, and the singular set is as in Fig.5. It is a graph of groups, where each edge is a rotational axis and the numbers stand for the order, e.g. the number m denotes a rotation axis of order m, i.e. local group $\mathbb{Z}_m$. Also we shall always assume $m \geq 7$, so that $\mathcal{S}^2(2,3,m)$ is a hyperbolic 2-orbifold, and $n \in \{2,3,4,5\}$ resulting in the indicated local groups of the vertices.

$m \geq 7, \quad n \in \{2,3,4,5\}$

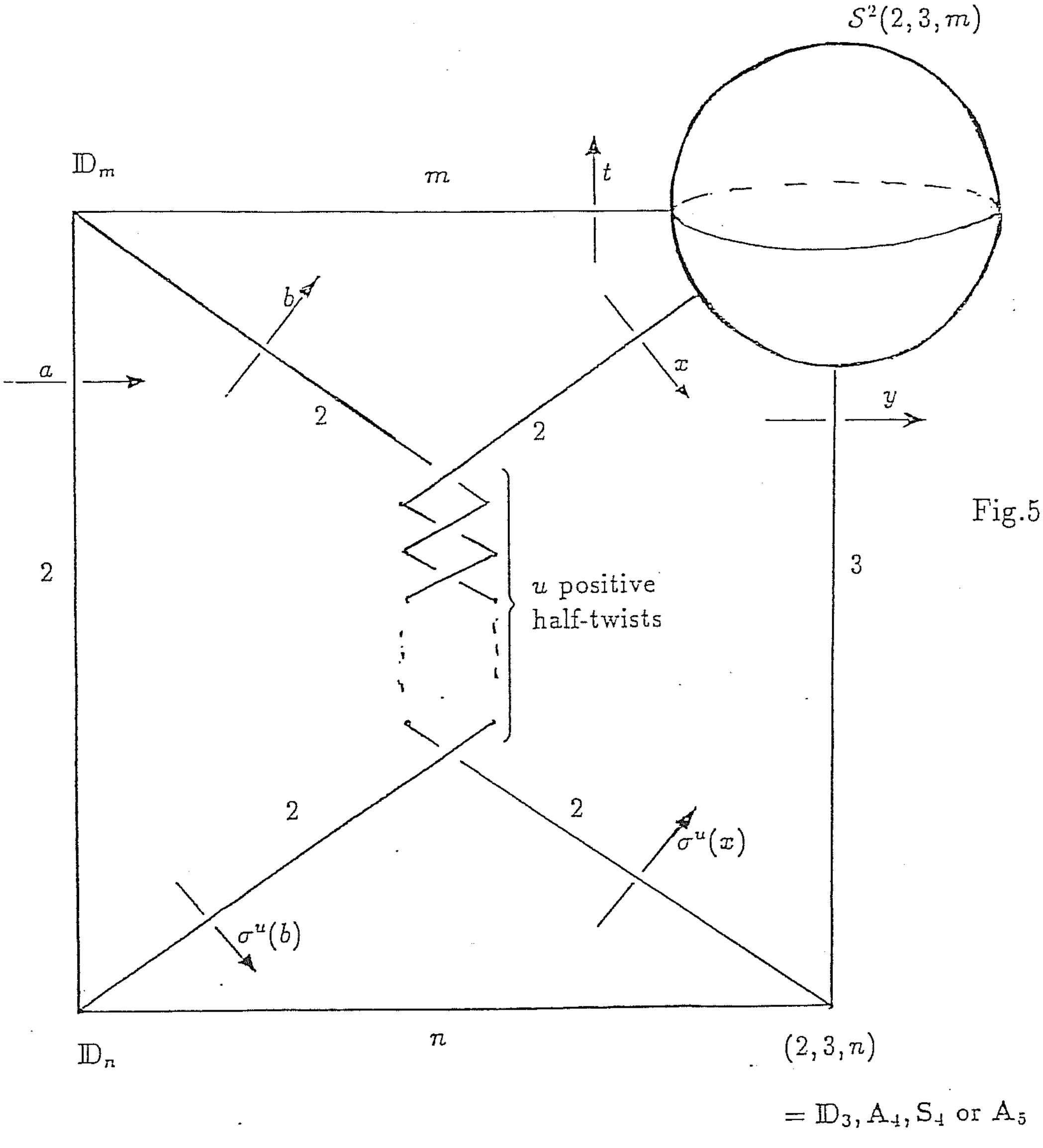


Fig.5

We shall denote the orbifold in Fig.5 by $\mathcal{D}^3(\sigma^u, m, n)$, where $\sigma = \sigma_2$ denotes the positive half-twist between strings b and x. It has been noticed in [33], using hyperbolic Dehn surgery on a 3-orbifold in which the braid σ^u has been replaced by a cusp, that, at least for u large enough, the orbifolds $\mathcal{D}^3(\sigma^u, m, n)$ are hyperbolic with totally geodesic boundary $\mathcal{S}^2(2,3,m)$. In fact, they are all hyperbolic except in the case $u = 0$, where they are reducible resp. bad orbifolds, and $u = \pm 1$, $n = 2$, where they are twisted line bundles (see Lemma 1.4.5 and the remark following it). If $u = \pm 1$, the singular set is a tetrahedron truncated at one vertex (or triangular prism); if also $n > 2$, the hyperbolicity may also be seen by applying Andreev's theorem for hyperbolic tetrahedra, see [29, ch. 13]. In particular, for $u \neq 0$ the 3-orbifolds are good, and therefore the local groups at the vertices as well as $\pi_1\mathcal{S}^2(2,3,m)$ inject into the orbifold fundamental group $\pi_1\mathcal{D}^3(\sigma^u, m, n)$. This group can be computed in exactly the same way, from the singular set, as the Wirtinger presentation is obtained from a planar projection of a knot or link (see [33, Prop.1], [21, §3.D]); the apposite generators are indicated in Fig.5. Alternatively one may apply the orbifold Van Kampen's theorem. The result is as follows (part *b)* is a short calculation using that b and x have order 2 in $\pi_1\mathcal{D}^3(\sigma^u, m, n)$):

1.4.4 Lemma

a)
$$\begin{aligned}\pi_1\mathcal{D}^3(\sigma^u, m, n) &= \langle a, b, x, y \mid abxy = 1, a^2 = b^2 = (ab)^m = 1, \\ &\qquad\qquad x^2 = y^3 = (xy)^m = 1, (a\sigma^u(b))^n = 1\rangle \\ &\cong \left(\mathbb{D}_m \underset{\mathbf{Z}_m}{*} (2,3,m)\right) / \langle\langle (a\sigma^u(b))^n \rangle\rangle .\end{aligned}$$

b) $\sigma^u(b) = b(bx)^u, \quad \sigma^u(x) = x(bx)^u.$

Remark: Given the 3-manifold $\mathcal{M}$ that bounds a Hurwitz G-action of a surface $\mathcal{F}$, the singular set of the quotient orbifold $\mathcal{M}/G$ contains at least 3 interior vertices and 6 edges.

In fact, the boundary orbifold has three cone (or branch) points of respective order 2, 3, and 7, each incident to a rotational axis of same order. Since interior singular points carry spherical groups, these axes can not be all three concurrent. The interior vertex incident to the rotational axis of order 7 carries necessarily the group $\mathbb{D}_7$,so is the origin of two other rotational axes of order 2 (whose "product" is of order 7). None of these latter can be incident to a boundary singular point and, in view of minimal choices, they can not concur in a same interior point. Then there are at least 3 interior singular vertices and consequentely at least 6 edges. This minimal number is effectively attained.

1.4.5 Lemma *Let be $u = \pm 1$ and $n = 2$. Then $\pi_1\mathcal{D}^3(\sigma^{\pm 1}, m, 2)$ is isomorphic to the extended triangle group $[2,3,m]$.*

Proof

We use the presentations 1.1.1 and 1.4.4.a). An isomorphism

$$\psi : \pi_1 \mathcal{D}^3(\sigma, m, 2) \rightarrow [2, 3, m]$$

is given by

$$\psi(a) = r_1, \psi(b) = r_1 r_3 r_1, \psi(x) = x = r_1 r_2, \psi(y) = y = r_2 r_3.$$

∎

Geometrically, $\mathcal{D}^3(\sigma^{\pm 1}, m, 2)$ is a twisted line bundle over its boundary; its interior has a complete hyperbolic structure of infinite volume, but with totally geodesic boundary it can be realized only in the $(\mathbb{H}^2 \times \mathbb{R})$-geometry.

Note that, for $u \neq 0$, there is a canonical injection of $(2, 3, m)$ into $\pi_1 \mathcal{D}^3(\sigma^u, m, n)$, mapping x to x and y to y. We shall consider $(2, 3, m)$ as a subgroup of $\pi_1 \mathcal{D}^3(\sigma^u, m, n)$ in the following.

We give now the bounding and non-bounding criteria which we will apply in Chapter 3.

1.4.6 Lemma *Suppose the surjection with torsion free kernel*

$$\varphi : (2, 3, m) \twoheadrightarrow G, \quad G \text{ finite}, \quad m \geq 7,$$

extends to a surjection (also with torsion-free kernel)

$$\phi : \pi_1 \mathcal{D}^3(\sigma^u, m, n) \twoheadrightarrow G, \quad \text{for some } u \neq 0, \ n \in \{2, 3, 4, 5\}.$$

Then the G-action on a surface $\mathcal{F}_g$ corresponding to the surjection φ bounds a hyperbolic 3-manifold.

Proof

Suppose $\mathcal{D}^3(\sigma^u, m, n)$ is hyperbolic with totally geodesic boundary $S^2(2, 3, m)$. Take the regular orbifold covering of $\mathcal{D}^3(\sigma^u, m, n)$ corresponding to the kernel of the surjection ϕ extending φ. This is a hyperbolic 3-manifold $\mathcal{M}$ (because the kernel of ϕ is torsion free) with totally geodesic boundary $\mathcal{F}_g$, and G acts on $\mathcal{M}$ by isometries as the group of covering transformations, restricting to the G-action on $\mathcal{F}_g$ corresponding to the surjection φ. If $\mathcal{D}^3(\sigma^u, m, n)$ is not hyperbolic with totally geodesic boundary (e.g. $u = \pm 1, n = 2$) let v be the order of $\varphi(bx)$ in G. Using 1.4.4.b), we have

$$\varphi(\sigma^{u+\mu v}(b)) = \varphi(b(bx)^{u+\mu v}) = \varphi(b(bx)^u) = \varphi(\sigma^u(b)).$$

Then, looking at the presentation 1.4.4.a) of $\pi_1 \mathcal{D}^3(\sigma^u, m, n)$, it is clear that we have also an extension of φ to a surjection with torsion-free kernel of $\pi_1 \mathcal{D}^3(\sigma^{u+\mu v}, m, n)$ onto G. If $u + \mu v$ is large enough the new 3-orbifold will be hyperbolic with totally geodesic boundary. ∎

1.4.7 Lemma *Suppose the surjection with torsion-free kernel*

$$\varphi : (2,3,m) \longrightarrow\!\!\!\!\!\rightarrow G, \quad G \text{ finite, } m \geq 7,$$

does not extend to a surjecton of $\mathbb{D}_m \underset{\mathbb{Z}_m}{*} (2,3,m)$ *onto* G, *i.e.* $\varphi(t)$ *does not lie in a dihedral subgroup of order* $2m$ *in* G. *Then the* G*-action on a surface* $\mathcal{F}_g$ *corresponding to* φ *does not bound any compact* 3*-manifold with boundary* $\mathcal{F}_g$.

<u>Proof</u>

Suppose the G-action of $\mathcal{F}_g$ extends to a compact 3-manifold $\mathcal{M}$ with $\partial\mathcal{M} = \mathcal{F}_g$. Then the 3-orbifold $\mathcal{M}/G$ has exactly one boundary component, namely $\mathcal{F}_g/G = \mathcal{S}^2(2,3,m)$. At the branch point of order m on $\mathcal{S}^2(2,3,m)$ starts a rotation axis of order $m \geq 7$, which has to finish in a singular point with local group $\mathbb{D}_m$. This local group injects into the orbifold fundamental group of $\mathcal{M}/G$ and then, via φ, also into G which is a contradiction. ∎

Remark: *If two surjections differ by an inner automorphism of* G, *their kernels are conjugate and the quotients by the kernels are isomorphic manifolds.*

Chapter 2

The Projective Linear Groups over Finite Fields

Let once for all p and n denote a prime number respectively a positive integer. We denote by $\mathbb{F}_q$ the unique (up to isomorphism) Galois field on $q = p^n$ elements. We briefly write $x \equiv_{\mathrm{p}} y$ for $x \equiv y \ (mod\, q)$. Obviously in $\mathbf{Z}_p$ all elements have a positive representative. Nevertheless any element has an opposite. So it will be understand that $\pm x$, $x \in \mathbf{Z}_p$, stands for both x and its opposite $p - x \equiv_{\mathrm{p}} -x$.

2.1 Preliminary notions

Consider the *general linear group* $GL(2,q)$ of two by two non-singular matrices with entries in the Galois field $\mathbb{F}_q$ with $q = p^n$ elements. The *special linear group* $SL(2,q)$ is the subgroup of matrices whose determinant is equal to 1. The quotient of $GL(2,q)$ resp. $SL(2,q)$ by the center, i.e. the subgroup of scalar matrices, is the *projective general linear group* $PGL(2,q)$ resp. the *projective special linear group* $PSL(2,q)$. If $p = 2$ these two groups coincide, but if $p > 2$ the group $PSL(2,q)$ is a subgroup of index 2 in $PGL(2,q)$. This depends on the field $\mathbb{F}_q$. In fact if $p = 2$ each element of $\mathbb{F}_q$ has a square root in the field, but if $p > 2$ this is true only for half of the non-zero elements: the so-called *squares* [8, §61] (or *quadratic residues* [12, 22]). It happens that in $GL(2,q)$ all the matrices with determinant a square project to $PSL(2,q)$.
The group $PSL(2,q)$ is simple and its order is $q(q-1)(q+1)/2$ if $p > 2$ resp. $(q-1)q(q+1)$ if $p = 2$ [8, §108,p.88]).
It is useful to keep in mind that $PGL(2,q)$ is represented as the group of transformations

$$z \mapsto \frac{a\,z + b}{c\,z + d}, \qquad a, b, c, d \in \mathbb{F}_q, \quad a\,d - b\,c \neq 0.$$

Let X be in $PGL(2,q)$. The determinants of two matrices representing X differ by a square factor. Fix a non-square, in particular a generator ϱ of the multiplicative group $\mathbb{F}_q \setminus \{0\}$, a so-called *primitive root* of $\mathbb{F}_q$ [8, p.12]. We

choose to represent X by a normalized matrix of determinant 1 if X belongs to $PSL(2,q)$ resp. ϱ if X belongs to $PGL(2,q) \setminus PSL(2,q)$. Warning: the product of two or more normalized matrices is not in general normalized.
In the set of the normalized representatives of X there are two matrices X_1 and X_2. They are related by

$$X_2 = -X_1, \; detX_2 = detX_1 \quad \text{and} \quad trX_2 = -trX_1.$$

So $det(X)$, the *determinant* of X, may be well defined, but trX, the *trace* of X, will be defined only up to sign. The two characteristic equations of X_1 and X_2 are resumed by

2.1.1
$$\lambda^2 - (trX)\,\lambda + detX = 0$$

the *characteristic equation* of X.

Before discuss it let us observe the following.

To make available, when $p > 2$, the square roots of each element of $\mathbb{F}_q$, we need to pass to the quadratic extension. Its construction looks like the passage from $\mathbb{R}$ to $\mathbb{C}$ (although in this case the resulting field is not algebraically closed) and can be so described.

Take a non-square in $\mathbb{F}_q$, in particular the primitive root ϱ. Let $\imath$ be a symbol such that $\imath^2 = \varrho$. Then a model for the quadratic extension of $\mathbb{F}_q$ is

$$\mathbb{F}_q[x]/(x^2 - \varrho) = \{z_1 + z_2\,\imath \,|\; z_1, z_2 \in \mathbb{F}_q\}.$$

Since it has q^2 elements it is just the Galois field $\mathbb{F}_{q^2}$.
The involution

$$z = z_1 + z_2\,\imath \longmapsto z_1 - z_2\,\imath = z^q = \overline{z}$$

defines a conjugation that behaves exactly as in $\mathbb{C}$:

$$z + \overline{z}, \quad z\,\overline{z} \in \mathbb{F}_q \; whereas \quad z - \overline{z} \in \imath\,\mathbb{F}_q.$$

Return now to the equation (2.1.1). The two solutions coincide if and only if

$$(trX)^2 - 4\,detX = 0.$$

Remember that we are working with normalized representatives, so $detX$ is either 1 or ϱ. Since trX belongs to $\mathbb{F}_q$ and ϱ is a non-square, the only possibility is $detX = 1$, which in turn implies $trX = \pm 2$. Such matrices and elements are called *parabolic*. Any parabolic matrix of $GL(2,q)$ is conjugate to $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ by some matrix in $SL(2,q^2)$. But if we want to remain in $GL(2,q)$, a parabolic matrix is conjugate to $\begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}$, for some $\mu \in \mathbb{F}_q$. Two such matrices $\begin{pmatrix} 1 & \mu_1 \\ 0 & 1 \end{pmatrix}$

and $\begin{pmatrix} 1 & \mu_2 \\ 0 & 1 \end{pmatrix}$ are conjugate in $GL(2,q)$ if and only if $\mu_1\,\mu_2^{-1}$ is a square in $\mathbb{F}_q$.
In particular it is immediate to verify that $\begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}$ is conjugate to $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ in $GL(2,q)$ if and only if μ is a square in $\mathbb{F}_q$.

If the discriminant of (2.1.1) is a square in $\mathbb{F}_q$, there are, in $\mathbb{F}_q$, two distinct solutions of the characteristic equation. The element X is said *hyperbolic.* If the discriminant is a non-square then there are two distinct conjugate solutions in $\mathbb{F}_{q^2}$. The element X is said *elliptic.* An elliptic element over $\mathbb{F}_q$ is however hyperbolic over $\mathbb{F}_{q^2}$. It means that working with the quadratic extension, any non-parabolic element has a representative that is conjugate to a diagonal matrix by a matrix in $SL(2,q)$ resp. $SL(2,q^2)$ [8, §101, §214].
Two non-parabolic elements are conjugate if and only if they have the same trace and determinant. The "if" follows because they have the same characteristic equation and are so conjugate to the same diagonal matrix. The "only if" implication is obvious.

In all cases the trace characterizes the order of an element in $PGL(2,q)$. Let's see how.
Remember that, if we work with normalized forms, the trace is well defined up to sign. Otherwise it is defined up to a non-null multiplicative factor.

Consider in $PSL(2,q^2)$ the diagonal element of order $l \geq 2$ (to avoid cumbersome distinctions the *bar* denotes also the inverse: if $\lambda \in \mathbb{F}_q$ then $\overline{\lambda} := \lambda^{-1}$)

$$R = \pm \begin{pmatrix} \lambda & 0 \\ 0 & \overline{\lambda} \end{pmatrix}, \quad \lambda\overline{\lambda} = 1, \quad \lambda \neq \overline{\lambda}.$$

Then $\lambda^l = \overline{\lambda}^l = \pm 1$ and

$$0 = \lambda^l - \overline{\lambda}^l = (\lambda - \overline{\lambda})\,(\sum_{k=o}^{l-1} \lambda^{l-1-k}\overline{\lambda}^k).$$

The right-hand factor is a polynomial that can be transformed, by means of $\tau = \lambda + \overline{\lambda}$, into a polynomial in τ. Since $\lambda\,\overline{\lambda} = 1$ the terms are powers of λ or of $\overline{\lambda}$ that may be collected in pairs. Each binomial $\lambda^k + \overline{\lambda}^k$ transforms easily into a polynomial in τ: e.g.

$$\lambda^2 + \overline{\lambda}^2 = (\lambda + \overline{\lambda})^2 - 2 = \tau^2 - 2.$$

If $l > 2$ is even, the result is a polynomial without the constant term. We define $Q_l(\tau)$ to be, when l is odd or equal to 2, the polynomial obtained, while, when $l > 2$ is even, the polynomial obtained divided by τ.

We have in particular:

2.1.2 Table: TRACE'S POLYNOMIAL up to 7

l	$Q_l(\tau) = Q_{l,1}(\tau) \cdot Q_{l,2}(\tau)$
2	τ
3	$\tau^2 - 1 = (\tau - 1)(\tau + 1)$
4	$\tau^2 - 2 = (\tau - \sqrt{2})(\tau + \sqrt{2})$
5	$\tau^4 - 3\tau^2 - 1 = (\tau^2 - \tau - 1)(\tau^2 + \tau - 1)$
7	$\tau^6 - 5\tau^4 + 6\tau^2 - 1 = (\tau^3 + \tau^2 - 2\tau - 1)(\tau^3 - \tau^2 - 2\tau + 1)$

We call $Q_l(\tau)$ the *trace's polynomial* of order l. Since $Q_l(\tau) = Q_l(-\tau)$ and the trace of an element in projective linear groups is defined up to sign, the polynomial Q_l seems to represent the right tool to characterize the order of a given element. Indeed

2.1.3 Lemma *Let R belong to $PGL(2, q)$. Then*

$$R \text{ has order } l \geq 2 \quad \text{if and only if} \quad Q_l(trR/\sqrt{detR}) = 0.$$

Proof

The trace is invariant under conjugation. So it is not restrictive to suppose, when R is non-parabolic,

$$R = \pm \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}, \lambda_1 \lambda_2 \neq 0, \ \lambda_1 \neq \lambda_2, \text{in } PGL(2, q) \text{ or in } PGL(2, q^2),$$

respectively, when R is parabolic,

$$R = \pm \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}, \quad \mu \in \mathbb{F}_q \setminus \{0\}.$$

In the first case R is of order l if and only if $\lambda_1^s = \lambda_2^s$ for $s = l$, but not for $1 < s < l$. (Note that we cannot ask $\lambda_1^l = \lambda_2^l = \pm 1$, because although we wish to work with normalized forms, the product is not always so.)
We get

$$0 = \lambda_1^l - \lambda_2^l = (\lambda_1 - \lambda_2)(\sum_{k=0}^{l-1} \lambda_1^{l-1-k} \lambda_2^k).$$

Since $\lambda_1 \neq \lambda_2$, the element R has order l if and only if the right-hand factor vanishes.
In the second case, when R is parabolic, it follows that

$$R^l = \pm \begin{pmatrix} 1 & \mu l \\ 0 & 1 \end{pmatrix} = \pm I \quad \textit{if and only if} \quad p \mid l.$$

The polynomial $\lambda_1^s - \lambda_2^s$ obviously vanishes for any s, because $\lambda_1 = \lambda_2 = \pm 1$; but

$$\sum_{k=0}^{l-1} \lambda_1^{l-1-k} \lambda_2^k = \sum_{k=0}^{l-1} 1 = l \text{ is equal to } 0 \quad \textit{if and only if} \quad p \mid l.$$

We may conclude in any case that

$$R \text{ has order } l \quad \textit{if and only if} \quad \sum_{k=0}^{l-1} \lambda_1^{l-1-k} \lambda_2^k = 0,$$

where λ_1, λ_2, the two eigenvalues of R, are determined up to sign.

If R belongs to $PSL(2,q)$, the conclusion is at hand because $trR = trR/\sqrt{detR}$. Otherwise, the element R is necessarily non-parabolic, then in $PGL(2,q^2)$ we may factorize

$$R = \pm \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} = \pm \begin{pmatrix} \frac{\lambda_1}{\sqrt{detR}} & 0 \\ 0 & \frac{\lambda_2}{\sqrt{detR}} \end{pmatrix} \begin{pmatrix} \sqrt{detR} & 0 \\ 0 & \sqrt{detR} \end{pmatrix}.$$

Now, $\frac{1}{\sqrt{detR}} R$ belongs to $PSL(2,q^2)$ and has exactly the same order of R. ∎

> Remark: *Remember that although some elements of $PGL(2,q)$ are represented into $PGL(2,q^2)$, the trace and the determinant belong always to $\mathbb{F}_q$.*

Recall here two results about polynomials over finite fields (see 1.69 on p. 28 and 2.15 on p. 52 in [14]):

2.1.4 Lemma *The polynomial $f \in \mathbb{F}[x]$ of degree 2 or 3 is irreducible in $\mathbb{F}_q[x]$ if and only if f has no root in $\mathbb{F}_q$.* ∎

2.1.5 Lemma *Let f be an irreducible polynomial of degree m in $\mathbb{F}_q[x]$. Then the splitting field of f over $\mathbb{F}_q$ is given by $\mathbb{F}_{q^m}$ (i.e. we have to consider $\mathbb{F}_{q^m}$ to find the m roots of f).* ∎

In particular consider $Q_{5,2}(x) = x^2 + x - 1$. Since $Q_{5,2}(0) = 1 = Q_{5,2}(1)$ the polynomial $Q_{5,2}(x)$ is irreducible in $\mathbb{F}_2[x]$. But it is reducible in $\mathbb{F}_4$ and in any $\mathbb{F}_{4^n}$, $n \geq 1$.

Moreover for the solutions of the quadratic equation in $\mathbb{F}_{2^n}$ the following more general result [8, §40] will be useful:

2.1.6 Theorem *The polynomial $x^p - x - \beta$ is irreducible in $\mathbb{F}_{p^n}$ if and only if*

$$\beta^{p^{n-1}} + \beta^{p^{n-2}} + \ldots + \beta^p + \beta \not\equiv_{\mathrm{p}} 0.$$

∎

This gives another way to prove the reducibility respectively the irreducibility of $Q_{5,2}$.

Now we would like to know which are the orders admited in $PGL(2,q)$.
Let us first see that:

2.1.7 Lemma *An odd order non-parabolic element in $PGL(2,q)$, $p > 2$, belongs to $PSL(2,q)$.*

The parabolic elements already belong to the projective special linear group $PSL(2,q)$ and, if $p = 2$ there is nothing to prove because $PGL(2,2^n) \equiv PSL(2,2^n)$.
<u>Proof</u>
Let R be non-parabolic in $PGL(2,q)$. Then, up to conjugation,

$$R = \pm \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}, \quad \lambda_1 \lambda_2 = \begin{cases} 1 \\ \varrho \end{cases}$$

either in $PGL(2,q)$ or in $PGL(2,q^2)$. If $\lambda_1 \lambda_2 = 1$ then there is nothing to prove. So let us suppose $\lambda_1 \lambda_2 = \varrho$ and the order of R be equal to $2s+1$. It follows that

$$\lambda_1^{2s+1} = \lambda_2^{2s+1} = \mu \quad \text{and} \quad \mu^2 = (\lambda_1 \lambda_2)^{2s+1} = \varrho^{2s+1}.$$

Observe that μ belongs to $\mathbb{F}_q$. This is obvious if R is hyperbolic. If R is elliptic then $\lambda_2 = \overline{\lambda_1}$. So it follows from $\mu = \lambda_1^{2s+1} = \overline{\lambda_1^{2s+1}}$.
Then the relation $\varrho^{2s+1} = \mu^2$ gives the desired contradiction, because the left-hand side is a non-square, while the right-hand side is a square in $\mathbb{F}_q$. ∎

The detailed discussion of Dickson in (see [8, ch. XII]) implies that:

2.1.8 Proposition *There exist elements of order s in $PSL(2,q)$, $q = p^n$, $p > 2$, if and only if $s \,|\, (q-1)/2$, $s \,|\, (q+1)/2$ or $s = p$.*

There exist elements of order s in $PSL(2,q)$, $q = 2^n$, if and only if $s \,|\, (q-1)$, $s \,|\, (q+1)$ or $s = 2$. ∎

The elements of order $s = p$ are exactly the parabolic ones.

Before discussing some particular orders, it will be useful to recall that:

2.1.9 Theorem[8, §62] *The non-squares of any $\mathbb{F}_{p^n}$, $p > 2$, are non-squares or squares in $\mathbb{F}_{p^{nm}}$ according as m is odd or even.* ∎

Since the field $\mathbb{Z}_p$ is contained as a subfield in any field $\mathbb{F}_q$ with $q = p^n$, we have the following

2.1.10 Corollary *A non-square x in $\mathbb{Z}_p$ is a non-square in $\mathbb{F}_{p^n}$ if and only if n is odd.* ■

Given an integer number x it is possible to characterize by a congruence or a system of congruences the set of primes p such that x is a square in $\mathbb{F}_p$ (see e.g. [12] or [22] for proofs of the used results). This means in particular that there are infinitely many primes p with the required property (see Appendix A).

Let us now discuss the orders 2, 3, 4, 5 and 7.

There are always elements of order 2 in $PSL(2,q)$: they are of the form

$$\pm \begin{pmatrix} \mu & \nu \\ \omega & -\mu \end{pmatrix}, \quad \mu, \nu, \omega \in \mathbb{F}_q, \quad -\mu^2 - \nu\,\omega \neq 0.$$

Also there are always elements of order 3. Indeed the trace's equation gives simply $\tau = \pm 1$. Alternatively, suppose it is $p \neq 3$. Then among the three consecutive integers $q-1$, q and $q+1$ at least one is divisible by 3, and it is not q because $p \neq 3$. The above proposition applies - if p is greater than 2 both $q-1$ and $q+1$ are even.

Elements of order 4 exist in $PSL(2,q)$ if and only if $4 \,|\, (q \pm 1)/2$, i.e. $q \equiv_8 \pm 1$. It is the right condition for the existence in $\mathbb{F}_q$ of $\sqrt{2}$, the trace of an element of order 4.
Suppose it is $q \not\equiv_8 \pm 1$ and d in $\mathbb{F}_q$ non-square. Then $2\,d$ is a square in $\mathbb{F}_q$ and there exist elements with trace $\sqrt{2\,d}$ in $PGL(2,q) \setminus PSL(2,q)$: e.g. $\pm \begin{pmatrix} 0 & -1 \\ d & \sqrt{2\,d} \end{pmatrix}$.
For $p = 2$ we have no elements of order 4, because $\tau^2 = 2$ reduces to $\tau = 0$. So any such element would already be of order 2.

Elements of order 5 exist in $PSL(2,p^n), p > 2$, if and only if 5 divides $(q-1)/2$ or $(q+1)/2$ (i.e. $q \equiv_{10} \pm 1$) or if $p = 5$. These are the conditions to get a solution in $\mathbb{F}_q$ of the trace's equation

$$\tau^2 \pm \tau - 1 = 0.$$

In fact the discriminant is 5 and $\sqrt{5}$ exists in $\mathbb{F}_q$ if and only if $q \equiv_{10} \pm 1$ or $p = 5$. Then the trace is

$$\tau = \pm(1 + \sqrt{5})/2 \quad \text{or} \quad \pm\,(1 - \sqrt{5})/2.$$

If $p = 2$ we conclude both by the condition of Proposition 2.1.8 and by those given in Lemmas 2.1.4 and 2.1.5 that the required elements and traces in $PSL(2,q)$

exists for any $q = 4^n$, $n \geq 1$.

The case of elements of order $s = 7$ is presented by Macbeath in [15, thm. 8], where more he proves that

2.1.11 *$PSL(2,q)$ is a Hurwitz group if and only if*

i) $q = 7$

ii) $q = p, \;\; p \equiv_7 \pm 1$

iii) $q = p^3, \;\; p \equiv_7 \pm 2$ *or* $p \equiv_7 \pm 3$.

Suppose it is $q = 7$. The elements of order 7 are parabolic. Accordingly $\tau = \pm 2$ is the only solution of

$$\tau^3 \pm \tau^2 - 2\,\tau \mp 1 = 0.$$

Suppose it is $q > 7$. There are, up to sign, at most three different possible traces for elements of order 7 in $PSL(2,q)$, with q as in (2.1.11). Let T be such an element. We will prove that the traces of T, T^2 and T^3 are all three different but also that, up to conjugation, all the three elements of order 7 are determined if we have individuated one.
The three powers of T all belong to $PSL(2,q)$: so the determinant is 1 and is the trace that depicts the conjugation class. Obviously they have all order 7. Let us first prove the following

<u>Claim</u>: If two among T, T^2 and T^3 are conjugate then all three are so.

<u>Proof</u>
Suppose it is $T = R^{-1}\,T^2\,R$, for some $R \in PSL(2,q)$ or $PSL(2,q^2)$. Then $T^3 = R^{-1}\,T^6\,R = R^{-1}\,T^{-1}\,R$, because $T^7 = 1$. Since $trT^{-1} = trT$, i.e. T^{-1} is conjugate to T, it follows that T^3 is conjugate to T. ∎

If all three elements are conjugate, then all three traces coincide. And

<u>Claim</u>: The three traces of order 7 all coincide exactly in $\mathbb{F}_7$.

<u>Proof</u>
We already know that in $\mathbb{F}_7$ they coincide. Let us prove the converse. It is not restrictive to suppose T represented by a matrix $T_1 = \begin{pmatrix} \lambda & 0 \\ 0 & \overline{\lambda} \end{pmatrix}, \lambda\,\overline{\lambda} = 1, \;\; \lambda^7 = 1$ (if necessary just replace T by T^2). Let

2.1.12 $\quad g_1 = \lambda + \overline{\lambda}; \;\; g_2 = \lambda^2 + \overline{\lambda}^2 = g_1^2 - 2; \;\; g_3 = \lambda^3 + \overline{\lambda}^3 = g_1^3 - 3\,g_1.$

It follows that

$$\prod_{i=1}^{3}(x - g_1) = x^3 + x^2 - 2\,x - 1$$

and so that

$$\begin{cases} g_1 + g_2 + g_3 & \equiv_{\mathrm{p}} \; -1 \\ g_1\, g_2 + g_1\, g_3 + g_2\, g_3 & \equiv_{\mathrm{p}} \; -2 \\ g_1\, g_2\, g_3 & \equiv_{\mathrm{p}} \;\;\; 1. \end{cases}$$

Since we have supposed $g_1 = g_2 = g_3 = g$ we get

$$\begin{cases} 3\,g & \equiv_{\mathrm{p}} \; -1 \\ 3\,g^2 & \equiv_{\mathrm{p}} \; -2 \\ g^3 & \equiv_{\mathrm{p}} \;\;\; 1. \end{cases}$$

Then

$$9 \equiv_{\mathrm{p}} 9\,g^3 = (3\,g)\,(3\,g^2) \equiv_{\mathrm{p}} 2 \text{ hence } 7 \equiv_{\mathrm{p}} 0.$$

The last congruence occurs if and only if $p = 7$. ∎

This means that the equation $x^3 + x^2 - 2\,x - 1 = 0$ has exactly three different solutions in the cases 2.1.11.ii and 2.1.11.iii. For the case 2.1.11.iii the three traces are different but conjugate under the automorphisms of the field $\mathbb{F}_q$ (that induce automorphisms of the group $PSL(2,q)$). Indeed $\mathbb{F}_q$, $q = p^3$, is a finite field and a Galois extension of $\mathbb{F}_p$. The Galois group, i.e. the group of automorphisms that are the identity on $\mathbb{F}_p$, is generated by the so-called *Frobenius automorphism*

$$\pi : x \mapsto x^p.$$

Suppose as above that it is $\lambda^7 = 1$ and remember that $(\overline{\lambda})^{-1} = \lambda$.
Since $Q_7(g) = 0$ and π is an automorphism, it follows that $Q_7(\pi(g)) = 0 = Q_7(\pi^2(g))$. A direct computation shows that

$$\pi(g) = \pi(\lambda + \overline{\lambda}) = \begin{cases} \lambda^p + \overline{\lambda}^p = \lambda^2 + \overline{\lambda}^2 & = \; g_2 \quad \text{if } p \equiv_7 \pm 2 \\ \lambda^p + \overline{\lambda}^p = \lambda^3 + \overline{\lambda}^3 & = \; g_3 \quad \text{if } p \equiv_7 \pm 3 \end{cases}$$

2.2 Subgroups and Generators

The subgroups of $PSL(2,q)$ are classified by Dickson in [8]. A recent reference is the book of Suzuki [28]. Macbeath in [15] classifies the pairs of elements by means of the subgroup they generate.

Let us present a quick review of the results.

The subgroups of $PSL(2,q)$ fall into three families. These are however not disjoint.

Class I: <u>Exceptional subgroups</u>

These are the finite triangle groups: the dihedral group $\mathbb{D}_m$ of order $2m$, the tetrahedral group A_4, the octahedral group S_4 and the dodecahedral group A_5. Obviously the order q of the field must be such that $PSL(2,q)$ admits elements of the right order.

Class II: <u>Affine subgroups</u>

These are the conjugates of the subgroup of superdiagonal elements in $PSL(2,q)$

$$\pm\begin{pmatrix}\alpha & \beta\\ 0 & \overline{\alpha}\end{pmatrix}, \alpha \neq 0, \text{ in } \mathbb{F}_q,$$

and to the subgroup in $PSU(2,q^2)$ of the elements

$$\pm\begin{pmatrix}\alpha & 0\\ 0 & \overline{\alpha}\end{pmatrix}, \ \alpha\in\mathbb{F}_{q^2},\ \alpha\,\overline{\alpha}=1.$$

Class III: <u>Projective subgroups</u>

These are the conjugates of the subgroups of the form $PSL(2,p^s)$ and $PGL(2,p^s)$.

And $PSL(2,p^s)$ is a subgroup od $PSL(2,p^n)$ when $\mathbb{F}_{p^s}$ is a subfield of $\mathbb{F}_{p^n}$, i.e. when $s\,|\,n$. Whereas $PGL(2,p^s)$ is a subgroup od $PSL(2,p^n)$ when $\mathbb{F}_{p^{2s}}$ is a subfield of $\mathbb{F}_{p^n}$, i.e. when $2s\,|\,n$.

Consider the triples (A_1,A_2,A_3) of matrices in $SL(2,q)$, such that

$$A_1\,A_2\,A_3=1;$$

we call $\alpha_i = tr(A_i),\ m_i = order(A_i),\quad i=1,2,3.$

A triple is called *exceptional* if (m_1,m_2,m_3) is one of the following

$$(2,2,m),\ \text{for any } m\geq 2, (2,3,3), (2,3,4), (2,3,5),$$

$$(2,5,5), (3,3,3), (3,4,4), (3,3,5), (3,5,5), (5,5,5).$$

If A_1, A_2 generate an exceptional subgroup, then the triple is exceptional.

A triple generates an affine group if

- $\alpha_1^2 + \alpha_2^2 + \alpha_3^2 - \alpha_1\,\alpha_2\,\alpha_3 = 4$

or

- $(\alpha_1, \alpha_2, \alpha_3)$ is one among $(2,2,2), (2,-2,-2), (-2,2,-2), (-2,-2,2)$.

This triple is called *singular*.

A triple is called *irregular* if the subfield generated by the traces, say $\mathbb{F}_r$, is a quadratic extension of another subfield $\mathbb{F}_s$, and if one of the traces of the triple lies in $\mathbb{F}_s$ while the other two are both square roots in $\mathbb{F}_r$ of non-squares in $\mathbb{F}_s$, or zero. In this case the triple generates $PGL(2, \sqrt{r})$.

The following theorem resumes the contents of Theorems 4, 5 and 6 of [15] and of §7.5 [7, pp.93-94]:

2.2.1 Theorem *A triple which is neither exceptional nor singular generates a projective group. If moreover we also suppose it is not irregular it generates a projective group isomorphic to $PSL(2,q)$, where $\mathbb{F}_q$ is the field generated by the traces. For $q \neq 9$, the group $PSL(2,q)$ is a factor group of the modular group $PSL(2,\mathbb{Z})$.*
For all q, the group $PSL(2,q)$ is generated by two elements one of which is an involution.

In particular $PSL(2,p)$, p prime, is generated by two elements

$$\pm\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad \textit{of order } p, \quad \textit{and} \quad \pm\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \textit{of order } 2,$$

whose product has order 3.

∎

2.3 The Isomorphic Unitary Groups

To conclude this chapter we exhibit, into $PGL(2,q^2)$, the conjugate subgroups of $PSL(2,q)$ and of $PGL(2,q)$, that contain the diagonal forms for elliptic elements. This will semplify computations when $p > 2$, although we move to the quadratic extension of $\mathbb{F}_q$.

Let us before prove a Lemma. Recall that

Theorem:[8, §64]
If $\nu = +1$ or -1 according as $-\alpha_1\,\alpha_2$ is a square or a non-square in the field $\mathbb{F}_{p^n}$, $p > 2$, the equation belonging to the field

$$\alpha_1\,\xi_1^2 + \alpha_2\,\xi_2^2 = \kappa \quad (\alpha_1 \neq 0, \alpha_2 \neq 0),$$

has $p^n - \nu$ or $p^n + (p^n - 1)\,\nu$ sets of solutions according as $\kappa \neq 0$ or $\kappa = 0$.

A direct application of the above Theorem gives us:

2.3.1 Lemma *The equation*

$$z\,\overline{z} = k, \quad k \in \mathbb{F}_q \setminus \{0\}, \quad p > 2,$$

has $q+1$ *solutions in* $\mathbb{F}_{q^2}$.

Proof

Substituting $z = x + y\imath$ we get the quadratic equation

$$x^2 - \varrho\, y^2 = k \quad \text{in } \mathbb{F}_q;$$

it has, by the Theorem above, $q+1$ pairs of solutions. ∎

The *unitary group* is

$$U(2,q^2) = \left\{ \begin{pmatrix} \delta & \varepsilon \\ -\overline{\varepsilon} & \overline{\delta} \end{pmatrix} \,\middle|\, \delta, \varepsilon \in \mathbb{F}_{q^2},\ \delta\,\overline{\delta} + \varepsilon\overline{\varepsilon} \neq 0 \right\}$$

and the *special unitary group* is

$$SU(2,q^2) = \left\{ \begin{pmatrix} \delta & \varepsilon \\ -\overline{\varepsilon} & \overline{\delta} \end{pmatrix} \,\middle|\, \delta, \varepsilon \in \mathbb{F}_{q^2},\ \delta\,\overline{\delta} + \varepsilon\overline{\varepsilon} = 1 \right\}$$

The *projective groups* $PU(2,q^2)$ and $PSU(2,q^2)$ are the quotients of $U(2,q^2)$ and $SU(2,q^2)$ by their respective centers. Note that $\delta\,\overline{\delta} + \varepsilon\overline{\varepsilon} \in \mathbb{F}_q$, because $\delta\,\overline{\delta}$ and $\varepsilon\overline{\varepsilon}$ belong to $\mathbb{F}_q$. We have the following [8, §144, Corollary, §138, §137, Corollary II]

2.3.2 Proposition *The projective unitary groups and the projective linear groups are two-by-two isomorphic:*

$$PU(2,q^2) \cong PGL(2,q) \quad \text{and} \quad PSU(2,q^2) \cong PSL(2,q).$$

Proof

Choose $k, r \in \mathbb{F}_q^2$ such that $k\,\overline{k} = 1$, $r\,\overline{r} = -1$ and consider the matrix $X = \begin{pmatrix} k & 1 \\ r\,\overline{k} & r \end{pmatrix}$ and its inverse $X^{-1} = \frac{1}{r(k-\overline{k})} \begin{pmatrix} r & -1 \\ -r\,\overline{k} & k \end{pmatrix}$.

Then

$$X^{-1}\, PU(2,q^2)\, X = PGL(2,q)$$

and under this conjugation $PSU(2,q^2)$ corresponds to $PSL(2,q)$.

Take an element in $PU(2,q^2)$ represented by $\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}$. Then its conjugate $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ is equal to

$$\frac{1}{r(k-\overline{k})} \begin{pmatrix} (a\,k - \overline{a}\,\overline{k})\,r + b\,r^2\,\overline{k} + \overline{b}\,k & (a - \overline{a})\,r + b\,r^2 + \overline{b} \\ -(a - \overline{a})\,r - b\,r^2\,\overline{k}^2 - \overline{b}\,k^2 & -(a\,\overline{k} - \overline{a}\,k)\,r - b\,r^2\,\overline{k} - \overline{b}\,k \end{pmatrix}.$$

By the general investigation about invariant forms, Dickson obtains that

$$\alpha\,\overline{\delta}, \alpha\,\overline{\gamma}, \alpha\overline{\beta}, \beta\,\overline{\delta}, \gamma\,\overline{\delta} \;\; \in \; \mathbb{F}_q.$$

This may be proved also directly verifying that each of the above products coincides with its conjugate in $\mathbb{F}_{q^2}$.

It follows that in any case there exists a non-null factor $\omega \in \mathbb{F}_q^2$ such that

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \omega \begin{pmatrix} \alpha_1 & \beta_1 \\ \gamma_1 & \delta_1 \end{pmatrix}$$

with $\alpha_1, \beta_1, \gamma_1, \delta_1 \in \mathbb{F}_q$.

Conversely start from an element of $PGL(2,q)$ represented by $\pm \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Then

$$X \begin{pmatrix} a & b \\ c & d \end{pmatrix} X^{-1} = \begin{pmatrix} \dfrac{a\,k - d\,\overline{k} - b + c}{k - \overline{k}} & \dfrac{-a\,k + d\,k + b\,k^2 - c}{r\,(k - \overline{k})} \\ -\dfrac{-a\,\overline{k} + d\,\overline{k} + b\,\overline{k^2} - c}{r\,(k - \overline{k})} & \dfrac{a\,\overline{k} - d\,k - b + c}{k - \overline{k}} \end{pmatrix}$$

belongs to $PU(2,q^2)$. If $\;a\,d - b\,c = 1\;$ the conjugate element belongs to $PSU(2,q^2)$. ∎

Chapter 3

Actions of $PSL(2,q)$ and $PGL(2,q)$

We wish to extend the Hurwitz actions of $PSL(2,q)$ on 2-manifolds to actions of either $PSL(2,q)$ itself or $PGL(2,q)$ on maximally symmetric 3-manifolds bounded by those 2-manifolds. We will extensively use the necessity's and sufficiency's criteria described in Chapter 1.

3.1 First example

As an easy case consider first the actions (only for $p = 7$ it will be Hurwitz!) corresponding to the surjections

3.1.1
$$\begin{array}{rcl} \varphi_p & : & (2,3,p) \twoheadrightarrow PSL(2,p), \qquad p \geq 7 \\ x & \longmapsto & X = \pm\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \\ y & \longmapsto & Y = \pm\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \\ t & \longmapsto & T = \pm\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \end{array}$$

where x, y, t are defined in 1.1.1. In fact the elements X and Y generate $PSL(2,p)$ 2.2.1. Moreover they have orders 2 resp. 3, so the surjections φ_p have torsion free kernel. (All surjections considered in the sequel will have torsion free kernel. *And throughout the work we will use small latin letters for the elements in the domains and the corresponding capitol letters for their images.*)

We have the following:

3.1.2 Theorem *The surjection 3.1.1 extends to a surjection*

$$\phi_p : \mathbb{D}_p \underset{\mathbb{Z}_p}{*} (2,3,p) \twoheadrightarrow \begin{cases} PSL(2,p) & \text{if and only if} \quad p \equiv_4 1 \\ PGL(2,p) & \text{if and only if} \quad p \equiv_4 3. \end{cases}$$

Proof

We have to find an element $A \in PSL(2,p)$ or $PGL(2,p)$, $A \neq 1$, such that

$$A^2 = 1 \text{ and } (TA)^2 = 1, \text{ i.e. } A^{-1}T A \; = T^{-1}.$$

Take

$$A = \pm \begin{pmatrix} \delta & \varepsilon \\ \zeta & -\delta \end{pmatrix}, \text{ where } \delta, \varepsilon, \zeta \in \mathbf{Z}_p \text{ satisfy } -\delta^2 - \varepsilon\,\zeta = \begin{cases} 1 \\ \varrho \end{cases}.$$

We obtain

$$T\,A = \pm \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \delta & \varepsilon \\ \zeta & -\delta \end{pmatrix} = \pm \begin{pmatrix} \delta+\zeta & \varepsilon-\delta \\ \zeta & -\delta \end{pmatrix},$$

and so $T\,A$ has order 2 if and only if $\zeta = 0$. The determinant condition becomes $\delta^2 = \begin{cases} -1 \\ -\varrho \end{cases}$. The equation $\delta^2 = -1$ can be solved in $\mathbf{Z}_p$ if and only if $p \equiv_4 1$, i.e. when -1 is a square [12, Thm. 82, p. 69]. Whereas the equation $\delta^2 = -\varrho$ can be solved in $\mathbf{Z}_p$ if and only if $-\varrho$ is a square, i.e. when -1 is a non-square, so if and only if $p \equiv_4 3$. ∎

Remark: *Any element of order p in $PSL(2,p)$ is, up to conjugation, of the form*

$$T = \pm \begin{pmatrix} 1 & \kappa \\ 0 & 1 \end{pmatrix}, \quad \kappa \in \mathbf{Z}_p \setminus \{0\} \text{ and } order(\kappa) = p.$$

It follows that the conditions $p \equiv_4 1$ resp. $p \equiv_4 3$ do not depend upon the particular surjection of $(2,3,p)$ onto $PSL(2,p)$.

We are ready to prove the following:

3.1.3 Corollary *The action of $PSL(2,p)$ corresponding to the surjection 3.1.1 bounds a hyperbolic 3-manifold if and only if $p \equiv_4 1$.*

Proof

Suppose that the action bounds. Then the conclusion follows from the criterion 1.4.7 and the above theorem.

Conversely, define

$$\Phi : \pi_1(\mathcal{D}^3(\sigma,p,2)) \longrightarrow\!\!\!\!\!\rightarrow PSL(2,p)$$

by

$$\begin{aligned} \Phi|_{(2,3,p)} &\equiv \varphi \\ \Phi(a) &= A = \pm \begin{pmatrix} \delta & 0 \\ 0 & -\delta \end{pmatrix}, \; \delta \in \mathbf{Z}_p \text{ and } \delta^2 = -1, \end{aligned}$$

where a is as in 1.4.4.a). The map Φ is well defined because $b = (x\, y\, a)^{-1} = (t\, a)^{-1}$ and we already know from the proof of 3.1.2 that $(T\, A)^2 = 1$. Moreover $a\, \sigma(b) = a\, x$ and

$$A\, X = \pm \begin{pmatrix} \delta & 0 \\ 0 & -\delta \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \pm \begin{pmatrix} 0 & -\delta \\ -\delta & 0 \end{pmatrix}$$

has order 2. We conclude by criterion 1.4.6. ∎

3.1.4 Corollary *There exist infinitely many non-bounding Hurwitz actions.*

Proof

Consider Klein's quartic curve $\mathcal{F}_3 = \mathbb{H}^2 / ker\, \varphi_7$ and, for each integer $m > 1$, the composite map

$$\psi_m : \pi_1(\mathcal{F}_3) \twoheadrightarrow \mathbb{Z}^6 \twoheadrightarrow (\mathbb{Z}_m)^6$$

where the first map is abelianization and the second is quotient $mod\, m$. It is easy to check that the subgroups $ker\, \psi_m$ are characteristic in $ker\, \varphi_7 = \pi_1(\mathcal{F}_3)$ and so normal in $(2,3,7)$. Let K_m, L_m resp. $\mathcal{F}^{(m)}$ be $(2,3,7)/ker\, \psi_m$, $ker\, \varphi_7 / ker\, \psi_m$ resp. $\mathbb{H}^2 / ker\, \psi_m$. Then the action of K_m on $\mathcal{F}^{(m)}$ is Hurwitz; moreover $K_m / L_m \cong PSL(2,7)$. Then the K_m-action on $\mathcal{F}^{(m)}$, for each $m > 1$, does not bound any compact hyperbolic 3-manifold, because by 3.1.3 the $PSL(2,7)$-action on $\mathcal{F}_3$ does not. ∎

Remark: *In the case $p \equiv_4 3$ of 3.1.3 there exists already a cyclic subgroup of the $PSL(2,p)$-action which does not bound any compact 3-manifold.*

Let $\langle T \rangle \cong \mathbb{Z}_p$ be the subgroup of $PSL(2,p)$ generated by $T = \varphi_p(t)$. The normalizer of $\langle T \rangle$ in $PSL(2,p)$ consists of all matrices of the form

$$\pm \begin{pmatrix} \alpha & \beta \\ 0 & \overline{\alpha} \end{pmatrix}$$

and has $p(p-1)/2$ elements, so that $\langle T \rangle$ has index $(p-1)/2$ in its normalizer. In $(2,3,p)$ there is exactly one conjugacy class of cyclic subgroups of order p, with representative $\langle t \rangle$. Let $F := \varphi_p^{-1}(\langle T \rangle)$ be the preimage of $\langle T \rangle$ in $(2,3,p)$. Then F contains exactly $(p-1)/2$ conjugacy classes of cyclic subgroups of order p (for an element $g \in (2,3,p)$, the conjugate $g^{-1} \langle t \rangle\, g$ is again a subgroup of F if and only if $\varphi_p(g)$ lies in the normalizer of $\langle T \rangle$ in $PSL(2,p)$). Therefore the 2-orbifold $\mathbb{H}^2/F$ has exactly $(p-1)/2$ singular points of order p. If $p \equiv_4 3$ this number $(p-1)/2$ is odd; similarly as in the proof of Lemma 1.4.7 it follows that the T-action on $\mathbb{H}^2/kernel\, \varphi_p$ does not bound any compact 3-manifold.

3.1.5 Corollary *Given the action of $PSL(2,p)$ corresponding to the surjection (3.1.1), there exists an action of $PGL(2,p)$ that bounds a hyperbolic 3-manifold if and only if $p \equiv_4 3$. The elements in $PGL(2,p) \setminus PSL(2,p)$ exchange the two boundary components.*

Proof
The map Φ defined in Corollary (3.1.3) maps now onto $PGL(2,q)$. ∎

3.2 Hurwitz actions

Let us now focus to the Hurwitz actions of $PSL(2,q)$, q as in (2.1.11) on page 20. To define the surjection of the triangle group $(2,3,7)$ onto $PSL(2,q)$, we choose the images of the elements x and t of respective order 2 and 7. Since we are interested on the action up to isomorphism, it is not restrictive to do a conjugation.
We start from the element T of order 7 that, up to conjugation, is $T = \pm\begin{pmatrix} \lambda & 0 \\ 0 & \overline{\lambda} \end{pmatrix}$ where the trace $\gamma = \pm(\lambda + \overline{\lambda})$ satisfies

3.2.1 $$\gamma^3 + \gamma^2 - 2\gamma - 1 = 0,$$

that in particular becomes

$$\gamma^3 + \gamma^2 + 1 = 0 \quad \text{in } \mathbb{F}_8 \quad \text{and} \quad \gamma^3 + \gamma^2 + \gamma - 1 = 0 \quad \text{in } \mathbb{F}_{27}.$$

Next we choose the element X of order 2: we take $\pm\begin{pmatrix} \mu & \nu \\ \omega & -\mu \end{pmatrix}$, where

3.2.2 $$a)\quad -\mu^2 - \nu\,\omega = 1 \qquad\qquad b)\quad \mu(\lambda - \overline{\lambda}) = \pm 1 \text{ i.e. } \mu = \frac{\pm 1}{\lambda - \overline{\lambda}} \neq 0,$$

and $\omega = -\overline{\nu}$, $-\mu = \overline{\mu}$ if $7 \mid q+1$. The first relation is the determinant condition, the second comes from $X\,T = Y$ because Y must have order 3.

Putting together the two relations 3.2.2 we get

3.2.3 $$\nu\,\omega = -\mu^2 - 1 = -\frac{1}{(\lambda - \overline{\lambda})^2} - 1 = \frac{3 - (\lambda + \overline{\lambda})^2}{(\lambda + \overline{\lambda})^2 - 4} = \frac{3 - \gamma^2}{\gamma^2 - 4};$$

that becomes

$$\nu\,\omega = \frac{1 + \gamma^2}{\gamma^2} = \gamma \quad \text{in } \mathbb{F}_8 \qquad \text{and} \qquad \frac{-\gamma^2}{\gamma^2 - 1} \quad \text{in } \mathbb{F}_{27}.$$

Remember that $\gamma^2 - 4 = (\lambda - \overline{\lambda})^2 \neq 0$ because T is non-parabolic. The map so defined on the generators x and t is surjective by Theorem 2.2.1.

With the above meanings and relations we set

3.2.4 Definition *The map*

$$\varphi_\gamma : (2,3,7) \twoheadrightarrow PSL(2,q), \ \ q \text{ as in 2.1.11}, \ \ q > 7,$$

is the surjection given by

$$x \longmapsto X \text{ and } \quad t \longmapsto T.$$

Note that in any case we cannot define such a map onto $PGL(2,q)$. Indeed T and Y have odd orders, so belong to $PSL(2,q)$. This forces also $X (= Y T^{-1})$ to belong to $PSL(2,q)$.

3.2.5 Remark*:*

1) *The product $\nu\,\omega$ is non-null because $\gamma^2 = 3$ would bring a contradiction when filled into 3.2.1.*
2) *The construction works also for $(2,3,m)$, $m \neq 7$. But for $m \leq 5$ and $q > 5$ the map will be no longer onto. Indeed the triangle group $(2,3,m)$ is isomorphic to a subgroup of $PSL(2,q)$ (see section 2.2).*

The freedom in the choice of ν is not effective. In fact different ν's do not give rise, up to automorphisms of $PSL(2,q)$, to different surjections.

3.2.6 Lemma *Let φ_γ be defined as above, and let $\widetilde{\varphi_\gamma}$ be such that*

$$\widetilde{\varphi_\gamma}(t) := \varphi_\gamma(t) \quad \text{and} \quad \widetilde{\varphi_\gamma}(x) = \widetilde{X} := \pm \begin{pmatrix} \mu & \widetilde{\nu} \\ \widetilde{\omega} & -\mu \end{pmatrix}.$$

Then φ_γ and $\widetilde{\varphi_\gamma}$ differ by an automorphism of $PSL(2,q)$.

<u>Proof</u>

Both X and $\widetilde{X}$ belong to $PSL(2,q)$. They have the same trace so they are conjugate: there exists $P \in PSL(2,q)$ such that $\widetilde{X} = P^{-1}\,X\,P$.

Let us determine the form of P to see how it operates on T. Take $P = \pm \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ and impose the above relation:

$$\pm \begin{pmatrix} \mu & \widetilde{\nu} \\ \widetilde{\omega} & -\mu \end{pmatrix} = \pm \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix} \begin{pmatrix} \mu & \nu \\ \omega & -\mu \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \text{ and } \alpha\,\delta - \beta\,\gamma = 1.$$

It leads to the system

$$\begin{cases} \alpha\,\delta + \beta\,\gamma = \pm 1 \\ \alpha\,\delta - \beta\,\gamma = 1 \\ \delta\,\nu\,\gamma - \beta\,\omega\,\alpha = 0. \end{cases}$$

The first two equations give $\alpha\,\delta = \begin{cases} 1 \\ 0 \end{cases}$ and $\beta\,\gamma = \begin{cases} 0 \\ -1 \end{cases}$ and so as candidates

$$\pm\begin{pmatrix} \alpha & \beta \\ 0 & \overline{\alpha} \end{pmatrix}, \quad \text{or} \quad \pm\begin{pmatrix} \alpha & 0 \\ \gamma & \overline{\alpha} \end{pmatrix}, \quad \text{with } \alpha \neq 0,$$

respectively

$$\pm\begin{pmatrix} 0 & \beta \\ -\overline{\beta} & \delta \end{pmatrix}, \quad \text{or} \quad \pm\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & 0 \end{pmatrix}, \quad \text{with } \beta \neq 0.$$

Since $\nu\,\omega = \widetilde{\nu}\,\widetilde{\omega} \neq 0$, with the third equation the candidates reduce to

$$\pm\begin{pmatrix} \alpha & 0 \\ 0 & \overline{\alpha} \end{pmatrix}, \quad \alpha \neq 0, \quad \text{or} \quad \pm\begin{pmatrix} 0 & \beta \\ -\overline{\beta} & 0 \end{pmatrix}, \quad \beta \neq 0.$$

Suppose first it is $P = \pm\begin{pmatrix} \alpha & 0 \\ 0 & \overline{\alpha} \end{pmatrix}$. Then $P^{-1}\,T\,P = T$ because diagonal matrices commute. So

$$\widetilde{\varphi_\gamma} = \theta_P \circ \varphi_\gamma, \qquad \text{where } \theta_P \text{ is the inner automorphism determined by } P.$$

Suppose now it is $P = \pm\begin{pmatrix} 0 & \beta \\ -\overline{\beta} & 0 \end{pmatrix}$. Then $P^{-1}\,T\,P = T^{-1}$. Observe that in $PSL(2,q)$ the inner automorphism Ψ associated to $\pm\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ maps each non-zero element to its inverse. Since $\widetilde{X} \equiv \widetilde{X}^{-1}$, it follows that

$$\widetilde{\varphi_\gamma} = \Psi \circ \theta_P \circ \varphi_\gamma.$$

■

> **Remark:** For $q > 7$, the possible different surjections of $(2,3,7)$ onto $PSL(2,q)$ are classified, up to automorphism of $PSL(2,q)$, by the conjugacy classes of T. There are exactly three conjugacy classes. But in case 2.1.11.iii) the three traces are equivalent under automorphisms of $PSL(2,p^3)$ (induced by automorphisms of $\mathbb{F}_{p^3}$, see section 2.1 at page 21). Therefore all three kernels are equal.

Now, the first step is to verify the necessity criterion (1.4.7). As we will easily see

3.2.7 Lemma *Any Hurwitz surjection 3.2.4 extends to* $\mathbb{D}_7 \underset{\mathbb{Z}_7}{*} (2,3,7)$ *both onto* $PSL(2,q)$ *and* $PGL(2,q)$.

Proof

We need A such that $A^2 = 1 = (TA)^2$. Then take $A = \pm \begin{pmatrix} \delta & \varepsilon \\ \zeta & -\delta \end{pmatrix}$. It follows that $TA = \pm \begin{pmatrix} \lambda\,\delta & \lambda\,\varepsilon \\ \overline{\lambda}\,\zeta & -\overline{\lambda}\,\delta \end{pmatrix}$ and since $\lambda - \overline{\lambda} \neq 0$, the trace will be zero if and only if $\delta = 0$. So exactly the elements $A = \pm \begin{pmatrix} 0 & \varepsilon \\ \zeta & 0 \end{pmatrix}$, where $\varepsilon\,\zeta \neq 0$, provide such an extension: onto $PSL(2,q)$ if $-\varepsilon\,\zeta$ is a square in $\mathbb{F}_q$, onto $PGL(2,q)$ otherwise. ■

In the sequel we will supposed the representative of A normalized in determinant, i.e. $-\varepsilon\,\zeta = \begin{cases} 1 \\ \varrho \end{cases}$. Remember that anyway the product of normalized representatives is no more normalized unless at most one does not belong to $PSL(2,q)$.

At this point we need to find a braid σ on three strings such that

3.2.8 $$(A\,\sigma(B))^l = 1, \quad for \;\; l = 2, 3, 4 \;\; or \; 5.$$

First of all let us analyze the special case $\sigma = \sigma_2^u$ with $u = 1$.
Then

$$A\,\sigma(B) = A\,X = \pm \begin{pmatrix} \varepsilon\,\omega & -\varepsilon\,\mu \\ \zeta\,\mu & \zeta\,\nu \end{pmatrix}.$$

The condition 3.2.8 becomes

3.2.9 $$\varepsilon\,\omega + \zeta\,\nu = \tau\,|A|^{1/2},$$

where $|A| := detA = -\varepsilon\,\zeta = \begin{cases} 1 \\ \varrho \end{cases}$ and τ, defined only up to sign, is the trace of an element of order l (see Table (2.1.2)). We obtain, multiplying by ε ($\neq 0$), the quadratic equation

$$\omega\,\varepsilon^2 - \tau\,|A|^{1/2}\,\varepsilon - \nu\,|A| = 0.$$

If $p \neq 2$ we may compute the discriminant, and using 3.2.3 we get

$$\Delta = |A|\,(\tau^2 + 4\,\nu\,\omega) = |A|\,\left(\tau^2 + 4\,\frac{3-\gamma^2}{\gamma^2-4}\right) = \frac{\tau^2\,(\gamma^2-4) + 4\,(3-\gamma^2)}{\gamma^2-4}\,|A|$$

which always belongs to $\mathbb{F}_q$. So there exists r in $\mathbb{F}_{q^2}$ such that $\Delta = r^2$. We have the solutions

$$\varepsilon_\pm = (\tau\,|A|^{1/2} \pm r)(2\,\omega)^{-1}$$

and from (3.2.9)

$$\zeta_\pm = (\tau\,|A|^{1/2} \mp r)(2\,\nu)^{-1}.$$

There are indeed good chances these provide a solution because

$$\varepsilon_\pm \cdot \zeta_\pm = (\tau\,|A|^{1/2} \pm r)\,(\tau\,|A|^{1/2} \mp r)\,(4\,\nu\,\omega)^{-1} = (\tau^2\,|A| - \Delta)\,(4\,\nu\,\omega)^{-1} = -|A|.$$

But we still have to verify we are in the right field and we have the right meanings for symbols.
If $7 \mid q-1$, i.e. $\lambda \in \mathbb{F}_q$, we have

$$\varepsilon_\pm \in \mathbb{F}_q \quad \textit{if and only if} \quad r \in \mathbb{F}_q.$$

The product of two squares or of two non-squares is a square, while the product of a square with a non-square is a non-square [12, Thm.85,p.69]. Since $\gamma^2 - 4 = (\lambda - \overline{\lambda})^2$ is a square in $\mathbb{F}_q$, the solutions $\varepsilon_\pm$ belongs $\mathbb{F}_q$ if and only if $(\tau^2\,(\gamma^2 - 4) + 4\,(3 - \gamma^2))\,|A|$ is a square in $\mathbb{F}_q$. In particular since $\varepsilon_\pm \cdot \zeta_\pm = -|A| \neq 0$ we have that both ε_+ and ε_- cannot be null.
If $7 \mid q+1$, i.e. $\lambda \notin \mathbb{F}_q$, then $\omega = -\overline{\nu}$, and ζ must be $-\overline{\varepsilon}$. Since τ is in $\mathbb{F}_q$, so coincide with its conjugate and moreover is defined up to sign, we have

$$-\overline{\varepsilon_\pm} = -(\tau\,|A|^{1/2} \pm \overline{r})(-2\,\nu)^{-1} = (\tau\,|A|^{1/2} \pm \overline{r})(2\,\nu)^{-1}.$$

So

$$\zeta = -\overline{\varepsilon} \quad \textit{if and only if} \quad r + \overline{r} = 0.$$

This is equivalent to require $r \in \imath\,\mathbb{F}_q$, i.e. Δ non-square in $\mathbb{F}_q$ or zero. But $\gamma^2 - 4$ is a non-square in $\mathbb{F}_q$ and again the condition turns out to be

$$(\tau^2\,(\gamma^2 - 4) + 4\,(3 - \gamma^2))\,|A| \quad \textit{square in} \quad \mathbb{F}_q.$$

Although $|A|$ is involved in the condition, there is no contradiction with the fact that we are computing the entries of A. Indeed the only feature needed in the condition is $A \in PSL(2,q)$ or $A \in PGL(2,q) \setminus PSL(2,q)$.

> Remark: *As we should have expected, the seemingly free parameter ν is not involved in the condition obtained.*

Define

$$C(\tau, \gamma) := \tau^2\,(\gamma^2 - 4) + 4\,(3 - \gamma^2).$$

If $C(\tau,\gamma)$ is a square then the element A must belong to $PSL(2,q)$; while if $C(\tau,\gamma)$ is a non-square then A must belong to $PGL(2,q) \setminus PSL(2,q)$. In the last case also $A\,X$ belongs to $PGL(2,q) \setminus PSL(2,q)$, forcing the order of $A\,X$ to be even (Lemma 2.1.7).

If $p = 2$ to solve the quadratic equation we have to proceed in a different way, as we cannot apply the usual formula. Moreover $PGL(2,8)$ coincide with $PSL(2,8)$, so we have $|A| = 1$.
Suppose it is $\tau = 0$. We have simply

$$\omega\,\varepsilon^2 - \nu = 0.$$

So

$$\varepsilon^2 = \frac{\nu}{\omega} = \frac{\nu\,\omega}{\omega^2} = \frac{\gamma}{\omega^2}.$$

Since all elements are squares in $\mathbb{F}_8$, we obtain

$$\varepsilon = \frac{\sqrt{\gamma}}{\omega}.$$

Suppose it is $\tau \neq 0$. Then the only possibility is $\tau = 1$, because we have no elements of order 4 or 5. We get

$$\omega\,\varepsilon^2 - \varepsilon - \nu = 0.$$

With the substitution $\varepsilon = z\,\omega^{-1}$ it becomes

$$z^2 - z + \gamma = 0.$$

We may apply Theorem 2.1.6 to verify that this equation has no solutions in $\mathbb{F}_8$. We have $p = 2$ and $n = 3$. Then we have to compute

$$\gamma^{2^2} + \gamma^2 + \gamma = \gamma^4 + \gamma^2 + \gamma = (\gamma^3 + \cancel{\gamma}) + \gamma^2 + \cancel{\gamma} = (\gamma^2 + 1) + \gamma^2 = 1 \neq 0.$$

All above resumes into the following theorem:

3.2.10 Theorem *Let $\tau = \tau(l)$ be the trace of an element of order l in $PSL(2,q)$, i.e. let τ be a zero of Q_l (see (2.1.2)).*
Suppose it is $p > 2$. The surjection 3.2.4

$$\varphi_\gamma : (2,3,7) \twoheadrightarrow PSL(2,q)$$

extends to a surjection

$$\phi_\gamma : \pi_1(\mathcal{D}^3(\sigma_2,7,l)) \twoheadrightarrow PSL(2,q), \ \textit{for} \quad l = 2,3,4 \ \textit{or}\ 5,$$

if and only if

$$\text{(C)} \quad \tau \in \mathbb{F}_q \quad \textit{and} \quad C(\tau,\gamma) \quad \text{is a square in } \mathbb{F}_q.$$

While, if $\ l = 2\ $ or 4, it extends to

$$\Phi_\gamma : \pi_1(\mathcal{D}^3(\sigma_2,7,l)) \twoheadrightarrow PGL(2,q)$$

if and only if

$$\text{(C')} \quad \tau^2\,\varrho \ \text{ is a square in } \mathbb{F}_q \quad \textit{and} \quad C(\tau,\gamma) \ \text{ is a non-square in } \mathbb{F}_q.$$

Suppose it is $p = 2$. Then φ_γ extends to ϕ_γ if and only if $\tau = 0$.

For $l = 4$ and 5 there must exist in $PGL(2,q)$ both elements of order l and 7, so two congruence relations must be satisfied. There are, by the Chinese remainder theorem, infinitely many numbers that satisfy both (see Appendix A).

3.2.11 Remark:

a) The function $C(.,.)$ may be rewritten as

$$C(\tau,\gamma) = \tau^2\gamma^2 - 4(\tau^2+\gamma^2) + 12.$$

So we see that it is in fact symmetric in $\tau = tr(\sigma(A)\,\sigma(B))$ and $\gamma = tr(T)$, and that their role may be interchanged. This fact is supported and explained by the observation that the resulting condition must be the same also if we start from a diagonal form for $R = \sigma(A)\,\sigma(B)$ and proceed starting backwards. However in this case we could have also elements R of even order belonging to $PGL(2,q) \setminus PSL(2,q)$, whose diagonal form is $\pm \begin{pmatrix} \lambda & 0 \\ 0 & \overline{\lambda} \end{pmatrix}$, $\lambda\overline{\lambda} = \varrho$: the choice falling before on A, has to be done now, from the beginning on R. To mantain the computations, also in between, as closer as possible to the ones already done, the role of X has to be taken by B.

b) From Definition 3.2.4 to Theorem 3.2.10, the hypothesis $Q_7(\gamma) = 0$ has been applied to prove that $\nu\omega$ is non-null (as γ^2 can not be 3). If we allow γ to be the trace of an element of whatsoever order m, we find in particular that

$$\gamma^2 \equiv_{\mathrm{p}} 3 \quad if \quad \begin{array}{ll} 1) & \gamma = 0 \;\; and \;\; p = 3 \\ 2) & \gamma = \pm 1 \;\; and \;\; p = 2 \\ 3) & \gamma = \gamma(5) \;\; and \;\; q = 4^n, n \geq 1. \end{array}$$

In case 1) the element T is parabolic and in cases 2) and 3) the element X is parabolic. Since for the applications we will always require $order(T) = m \geq 4$ the cases 1) and 2) will be excluded. The fact $\nu\,\omega \neq 0$ has been applied in the proof of Lemma 3.2.6. It is easy to see that also in case 3) there exists an (inner) automorphism of $PSL(2,2^n)$ such that X and $\widetilde{X}$ (now parabolic) result conjugate, but T remains fixed. In all other cases the computations applies verbatim.

c) Still for $order(T) = m \neq 7$ the value $\gamma^2 - 4 = (\lambda - \overline{\lambda})^2 \neq 0$ is a square in $\mathbb{F}_q$ when $\lambda \in \mathbb{F}_q$ ($m \mid q-1$) and a non-square otherwise ($m \mid q+1$). So $\gamma = \gamma(m)$, $\tau = \tau(l) \in \mathbb{F}_q$ and $C(\tau,\gamma)$ square in $\mathbb{F}_q$ is the condition to be satisfied to extend φ_γ to ϕ_γ from $\pi_1(\mathcal{D}^3(\sigma,m,l))$ onto $PSL(2,q)$.

From criterion 1.4.6 we get

3.2.12 Corollary *The Hurwitz action corresponding to 3.2.4 bounds a hyperbolic 3-manifold if condition 3.2.10(C) is satisfied.*

If instead is satisfied condition 3.2.10(C'), the Hurwitz action extends to a $PGL(2, q)$-action bounding a hyperbolic 3-manifold with 2 isomorphic boundary components. ∎

What we would like to obtain is an infinite answer expressed by a characterization of the order of the field q, on which the condition seems ultimately to depend. In this direction the following Lemma helps us:

3.2.13 Lemma *Supposed g_1, g_2, g_3 are as in (2.1.12), for a fixed τ the product*

$$\prod_{i=1}^{3} C(\tau, \pm g_i) = -7\,\tau^6 + 28\,\tau^4 - 64$$

depends only on τ.

Proof

It is not restrictive to suppose $\lambda^7 = 1$ (see Chapter 2). It follows that $\lambda^{7-i} = \lambda^{-i} = (\overline{\lambda})^i$ and we have

$$g_1^2 = g_2 + 2; \qquad g_2^2 = g_3 + 2; \qquad g_3^2 = g_1 + 2.$$

Then

$$\tau^2(g_1^2 - 4) + 4\,(3 - g_1^2) = \tau^2\,(g_2 - 2) + 4\,(1 - g_2) = (4 - 2\,\tau^2) - (4 - \tau^2)\,g_2,$$

and similarly for g_2 and g_3. Since for $l = 2, 3, 4$ or 5 the trace τ is such that $\tau^2 \neq 4$, we may write

$$\begin{aligned}
\prod_{i=1}^{3} C(\tau, \pm g_i) &= \prod_{i=1}^{3} \left((4 - 2\tau^2) - (4 - \tau^2) g_i\right) \\
&= (4 - \tau^2)^3 \prod_{i=1}^{3} \left(\frac{4 - 2\tau^2}{4 - \tau^2} - g_i\right) \\
&= (4 - \tau^2)^3\, P\left(\frac{4 - 2\tau^2}{4 - \tau^2}\right) \\
&= -7\,\tau^6 + 28\,\tau^4 - 64. \blacksquare
\end{aligned}$$

When $q = p$, $p \equiv_7 \pm 1$, we get an infinite but indefinite answer respect to the particular surjection. In fact

if $\qquad -7\,\tau^6 + 28\,\tau^4 - 64 \qquad$ is a square in $\mathbb{F}_q$

then among the $C(\tau, \pm g_i)$, $i = 1,2,3$, there are 1 or 3 squares; while if is a non-square there are among the factors 0 or 2 squares. We will see, as an application of the *Čebotarev density theorem* (see Appendix A), that all 4 possibilities occur infinitely many times.

Lemma 3.2.13 is very useful when $q = p^3$. Indeed remember that the three traces $\pm g_i$, $i = 1,2,3$, are conjugate under the automorphism group of the field $\mathbb{F}_q$ (section 2.1 on page 21). Then so is any expression that contains them. It means that the values $C(\tau, \pm g_i)$, $i = 1,2,3$, are all three squares or all three non-squares. By the above Lemma we need only to check if $-7\,\tau^6 + 28\,\tau^4 - 64$ is a square or not.

Let us discuss now condition 3.2.10(C) with respect to the various values of the order l.

Take first $l = 2$ (i.e. $\tau = 0$). Then $C(0, \gamma) = 4\,(3 - \gamma^2)$ and the condition being or not a square falls on $3 - \gamma_i^2$, $i = 1,2,3$. Lemma 3.2.13 gives

$$\prod_{i=1}^{3} C(\tau, \pm g_i) = -64 = -1 \cdot 8^2.$$

Since -1 is a square if and only if $p \equiv_4 1$, we get

3.2.14 Corollary *Let $p \equiv_4 1$ or $p = 2$.*

a) Let $q = p^3$, $p \equiv_7 \pm 2, \pm 3$. Then the unique Hurwitz action of $PSL(2,q)$ bounds a hyperbolic 3-manifold.

b) Let $q = p$, $p \equiv_7 \pm 1$. Then at least one of the 3 Hurwitz actions of $PSL(2,q)$ bounds a hyperbolic 3-manifold.

■

Remark: *Theorem 3.2.10 read in this particular case ($\tau = 0$, $l = 2$) gives the main algebraic result of* [4]*. At first glance the conditions seems to be different, but the dictionary is provided by Lemma 2 (in* [4]*) and subsequent discussion.*

Now suppose it is $l = 3$, i.e. $\tau = \pm 1$. Then

$$\prod_{i=1}^{3} C(\pm 1, \pm g_i) = -43.$$

This is a square if and only if $p \equiv_{86} r$, where

$r \in \mathcal{R} := \{1,9,11,13,15,17,21,23,25,31,35,41,47,49,53,57,59,67,79,81,83\}.$

Equivalently -43 is square if and only if $p \equiv_{43} s$ where

$s \in \mathcal{S} := \{1,4,6,9,10,11,13,14,15,16,17,21,23,24,25,31,35,36,38,40,41\},$

and $\mathcal{S}$ is the set of squares in $\mathbb{Z}_{43}$.
The set $\mathcal{R}$ is obtained by an application of the Gauß Lemma [12, Thm. 92], [22, Lemma 9.2] and $\mathcal{S}$ by the Quadratic Reciprocity Law [22, Thm. 9.6], [12, Thm. 98].

Analogously to 3.2.14 we have

3.2.15 Corollary *Let $p \equiv_{86} r$, where $r \in \mathcal{R}$, or $p = 43$. Then*

a) the unique Hurwitz action of $PSL(2,q)$, $q = p^3$, $p \equiv_7 \pm 2, \pm 3$, bounds a hyperbolic 3-manifold;

b) at least one of the 3 Hurwitz actions of $PSL(2,q)$, $q = p$, $p \equiv_7 \pm 1$, bounds a hyperbolic 3-manifold.

■

> **Remark:** In $PSL(2,3^3)$ the elements of order 3 are parabolic. So $Y = XT$ is parabolic, and in this case also AX. This fact does not trouble the computations: the parabolic elements are characterized by the trace being equal to ± 2 and indeed $\pm 1 \equiv_3 \mp 2$.

The case $l = 4$, i.e. $\tau = \pm\sqrt{2}$ (which exists if $q \equiv_8 \pm 1$), does not enlarge the infinite set of order satisfying the conditions because

$$\prod_{i=1}^{3} C(\pm\sqrt{2}, \pm g_i) = -8 \quad \text{is a square} \qquad \textit{if and only if} \quad p \equiv_8 1.$$

Moreover the condition 3.2.10 (C) in case $l = 4$ can be obtained by the knowledge of the same condition for $l = 2$. Indeed we already know that $g_2 = g_1^2 - 2$, $g_3^2 = g_1^3 - 3\,g_1$ and that $g_1\, g_2\, g_3 = 1$ (see 2.1.12 and what follows). Let $g := g_1$. Then

$$1 = g \cdot (g^2 - 2) \cdot (g^3 - 3\,g) = g^2 \cdot (g^2 - 2) \cdot (g^2 - 3).$$

So $(g^2 - 2)(g^3 - 3)$ is a square. It follows that $g^2 - 2$ and $g^2 - 3$ are both squares or both non-squares. And so $2 - g^2$ and $3 - g^2$.

Then we conclude that in $\mathbb{F}_q$, $q \equiv_8 \pm 1$

$$C(0, \pm g_i) = 4\,(3 - g_i^2) \quad \text{is a square} \quad \textit{if and only if} \quad C(\pm\sqrt{2}, \pm g_i) = 2(2 - g_i^2) \text{ is;}$$

and that in $\mathbb{F}_q$, $q \equiv_8 \pm 3$ (now $\sqrt{2} \in \mathbb{F}_{q^2}$)

$$C(0, \pm g_i) = 4\,(3 - g_i^2) \quad \text{is a square} \quad \textit{if and only if} \quad C(\pm\sqrt{2}, \pm g_i) = 2(2 - g_i^2) \text{ is not.}$$

Last, when $l = 5$ (remember the restriction: $q \equiv_{10} \pm 1$ or $p = 5$) we have $\tau = \pm\dfrac{1-\sqrt{5}}{2}$ or $\pm\dfrac{1+\sqrt{5}}{2}$. Lemma 3.2.13 gives $\prod_{i=1}^{3} C(\tau, \pm g_i) = -29 \pm 14\sqrt{5}$.

Since we cannot get rid of the term $\sqrt{5}$, we cannot give a new corollary like 3.2.14 and 3.2.15. In fact the answer depends more closely on q as we need the specific value of $\sqrt{5}$ in each $\mathbb{F}_q$.

At this point the above corollaries and results assure that the surface actions of $PSL(2,q)$ do bound a hyperbolic 3-manifold for infinitely many values of q. Anyway the precise answer about a given action is known for $q = p^3$ but not for $q = p$. For the latter we need to really compute the function $C(.,.)$ with the relative entries.

In particular we may state the following

3.2.16 Corollary *For $q = p^3$, $p \equiv_7 \pm 2, \pm 3$ and $2 \leq p < 100$, $p \neq 3$, the unique Hurwitz action of $PSL(2,q)$ bounds a hyperbolic 3-manifold.*

Proof

By the above corollaries we have positive answer for $q = 2^3$ and 5^3, but the case $q = 3^3$ remains open. The next values $q = p^3$,

The values $p \equiv_7 \pm 2$,or ± 3 up to 100, are

$$p = 11, 17, 19, 23, 31, 37, 47, 53, 59, 61, 67, 73, 79 \text{ and } 89.$$

All of these except $p = 3$ and 19 are covered by Corollaries 3.2.14 and 3.2.15. For $p = 19$ the case $l = 5$ gives a positive answer: in fact in $\mathbb{F}_{19}$ we have $\sqrt{5} = 9$ and $-29 - 14\sqrt{5} \equiv_{19} 16 = 4^2$. There are no elements of order 5 in $PSL(2,27)$. Only three values of the form (2.1.11.iii), namely $q = 2^3$, 3^3 and 5^3 are less than 1000. ∎

For $q = p$, $p \equiv_7 \pm 1$ we have done a systematic check by computer up to 1000. We have produced a Table (Chapter 5 on page 62) with the values of $C(\tau(l), \gamma)$ for $l = 2, 3, 5$. We have up to 1000 fourteen values that are not covered by Corollaries 3.2.14 and 3.2.15, namely

$$71, 211, 223, 419, 463, 491, 503, 587, 631, 727, 743, 811, 839, 911.$$

The complete computations shows that also in these cases there are actions that bound. So at this point we may resume that

> *"For $q + p$, $p \equiv_7 \pm 1$, and $7 < q < 1000$, at least one Hurwitz action of $PSL(2,q)$ bounds a hyperbolic 3-manifold."*

The situation is different if we consider each action individually. There are gaps: exactly 24 over 165 up to 1000, corresponding to the 14,54%, and the first occurs already for $q = 13$, $g = 10$.

So return to condition 3.2.8 and assume it is $\sigma = \sigma_2^2$. It follows that

$$A\,\sigma(B) = AXBX = AXTAX, \quad \text{as} \quad B = TA.$$

Since we have already find a 3-manifold which bounds by $PSL(2,8)$, we will no more consider the case $p = 2$.
So let be $p > 2$ and remind that

$$T = \pm \begin{pmatrix} \lambda & 0 \\ 0 & \overline{\lambda} \end{pmatrix}, \text{ where } \gamma = \pm g, \quad g = \lambda + \overline{\lambda}$$

$$X = \pm \begin{pmatrix} \mu & \nu \\ \omega & -\mu \end{pmatrix}, \quad \text{where} \quad \mu^2 = 1/(\gamma^2 - 4), \quad \nu\,\omega = \frac{3-\gamma^2}{\gamma^2-4};$$

and

$$\nu\,\omega = \frac{1+\gamma^2}{\gamma^2} = \gamma \quad \text{in } \mathbb{F}_8 \quad \text{and} \quad \frac{-\gamma^2}{\gamma^2-1} \quad \text{in } \mathbb{F}_{27}.$$

$$A = \pm \begin{pmatrix} 0 & \varepsilon \\ \zeta & 0 \end{pmatrix}, \quad -\varepsilon\,\zeta = \begin{cases} 1 \\ \varrho \end{cases}$$

Then

$$AXTAX = \pm \begin{pmatrix} \varepsilon\,\omega & -\varepsilon\,\mu \\ \zeta\mu & \zeta\nu \end{pmatrix} \begin{pmatrix} \lambda & 0 \\ 0 & \overline{\lambda} \end{pmatrix} \begin{pmatrix} \varepsilon\,\omega & -\varepsilon\,\mu \\ \zeta\mu & \zeta\nu \end{pmatrix} =$$

$$= \pm \begin{pmatrix} \lambda\,\varepsilon\,\omega & -\overline{\lambda}\,\varepsilon\,\mu \\ \lambda\,\zeta\mu & \overline{\lambda}\,\zeta\nu \end{pmatrix} \begin{pmatrix} \varepsilon\,\omega & -\varepsilon\,\mu \\ \zeta\mu & \zeta\nu \end{pmatrix} =$$

$$= \pm \begin{pmatrix} \varepsilon(\lambda\,\varepsilon\,\omega^2 - \overline{\lambda}\,\zeta\,\mu^2) & -\mu\,\varepsilon(\lambda\,\varepsilon\,\omega + \overline{\lambda}\,\zeta\,\nu) \\ \zeta\,\mu(\lambda\,\varepsilon\,\omega + \overline{\lambda}\,\nu\zeta) & \zeta(-\lambda\,\varepsilon\,\mu^2 + \overline{\lambda}\,\zeta\nu^2) \end{pmatrix}.$$

Now, contrary to the case $\sigma = \sigma_2$, the trace of $A\,\sigma(B) = AXTAX$ is not sign independent from the trace of T. Indeed there are two occurences of both A and X, but only one of T. The change of the SL-representative of T produce the change of the SL-representative of $A\,\sigma(B)$, whereas this does not happen for A and X.
Let be $t := |A|^{-1}\,tr\left(A\,X \begin{pmatrix} \lambda & 0 \\ 0 & \overline{\lambda} \end{pmatrix} A\,X\right)$. Then the condition (3.2.8) becomes

3.2.17 $$\pm\lambda\,\varepsilon^2\,\omega^2 \pm \left(\frac{g}{\gamma^2-4} - t\right)\,|A| \pm \overline{\lambda}\,\zeta^2\,\nu^2 = 0.$$

So it is enough to solve

3.2.18 $$\lambda\,\varepsilon^2\,\omega^2 + \left(\frac{g}{\gamma^2-4} - t\right)\,|A| + \overline{\lambda}\,\zeta^2\,\nu^2 = 0.$$

Multiply the equation by $\varepsilon^2(\gamma^2-4)\neq 0$:

$$\lambda(\gamma^2-4)\,\omega^2\,\varepsilon^4+\Big(g-t(\gamma^2-4)\Big)\;|A|\,\varepsilon^2+\overline{\lambda}\,|A|^2\,\nu^2(\gamma^2-4)=0.$$

The discriminant of this biquadratic equation in the unknown ε^2 is

$$\Delta=|A|^2\left((g-t(\gamma^2-4))^2-4(3-\gamma^2)^2\right)$$

and belongs to $\mathbb{F}_q$. In particular there exists $r\in\mathbb{F}_{q^2}$ such that

$$r^2=(g-t(\gamma^2-4))^2-4(3-\gamma^2)^2$$

and we always have in $\mathbb{F}_{q^2}$ the solutions

$$\varepsilon_\pm^2=\frac{(-g+t(\gamma^2-4))\pm r}{2\lambda\,\omega^2(\gamma^2-4)}\,|A|.$$

From (3.2.18)

$$\zeta_\pm^2=\frac{(-g+t(\gamma^2-4))\mp r}{2\overline{\lambda}\,\nu^2(\gamma^2-4)}\,|A|.$$

A careful computations shows that

$$\varepsilon_\pm^2\cdot\zeta_\pm^2=|A|^2,$$

so we are on the right direction. As before, now we have to verify that the solutions stay in the right field.

Suppose it is $7\,|\,q-1$, i.e. $\lambda\in\mathbb{F}_q$. Then ε must belong to $\mathbb{F}_q$, so we require

i) $r\in\mathbb{F}_q$, i.e. $(g-t(\gamma^2-4))^2-4(3-\gamma^2)^2$ square in $\mathbb{F}_q$;

and

ii) $\dfrac{(-g+t(\gamma^2-4))+r}{2\lambda}\,|A|$ or $\dfrac{(-g+t(\gamma^2-4))-r}{2\lambda}\,|A|$ square in $\mathbb{F}_q$.

Suppose it is $7\,|\,q+1$, i.e. $\lambda\notin\mathbb{F}_q$. Now $\omega=-\overline{\nu}$ and we do computations in the quadratic extension $\mathbb{F}_{q^2}$. Also $\zeta=-\overline{\varepsilon}$. Then we have that

$$\overline{\varepsilon_\pm^2}=\frac{-g+t(\gamma^2-4)\pm\overline{r}}{2\overline{\lambda}\,\nu^2(\gamma^2-4)}\,|A|\quad\text{ is equal to }\zeta_\pm^2\ \textit{if and only if}\ \ \overline{r}+r=0,$$

which as before is equivalent to require $r\in\imath\mathbb{F}_q$, i.e. Δ non-square in $\mathbb{F}_q$ or zero. Let us write $r=\chi\,\imath$, where $\chi\in\mathbb{F}_q$; the subsequent condition is to check when

$$\frac{(-g+t(\gamma^2-4))\pm\chi\,\imath}{2\lambda\overline{\nu}^2(\gamma^2-4)}\,|A|\ \ \textit{is a square in}\ \ \mathbb{F}_{q^2}.$$

This is enough because any element in $\mathbb{F}_{q^2}$ is a square if and only if its conjugate is a square.
Since we have no general formula to express $\overline{\nu}^2$, which anyway is already a square, we need merely to discuss when

$$z_0 + z_1 \imath = \frac{(-g + t(\gamma^2 - 4)) \pm \chi \imath}{2\lambda(\gamma^2 - 4)} |A| = (h_0 + h_1 \imath)^2, \quad \text{for some} \quad h_0, h_1 \in \mathbb{F}_q.$$

A first constrain is provided by

$$\varepsilon \overline{\varepsilon} = |A|, \quad \varepsilon = (h_0 + h_1 \imath)/\overline{\nu}.$$

It implies

$$h_0^2 - h_1^2 \varrho = (h_0 + h_1 \imath)(h_0 - h_1 \imath) = \nu \overline{\nu} |A| = \frac{\gamma^2 - 3}{\gamma^2 - 4} |A|.$$

From

$$\lambda + \overline{\lambda} = g \quad \text{and} \quad \lambda - \overline{\lambda} = \mu^{-1}$$

we get

$$2\lambda = g + \mu^{-1}.$$

Since

$$\mu^{-2} = \gamma^2 - 4 = (\lambda - \overline{\lambda})^2 \quad \text{and} \quad \lambda \notin \mathbb{F}_q,$$

it follows that $\mu^{-1} \in \imath \mathbb{F}_q$.
If

$$\mu^{-1} = \pm \beta \imath, \quad \beta \in \mathbb{F}_q,$$

we obtain

$$2\lambda = g \pm \beta \imath \quad \text{and} \quad 2\overline{\lambda} = g \mp \beta \imath.$$

Supposing $2\lambda = g + \beta \imath$, we have

$$z_0 = \frac{1}{4} \frac{g(t(\gamma^2 - 4) - g) \mp \chi \beta \varrho}{\gamma^2 - 4} |A|$$

and

$$z_1 = \frac{1}{4} \left(\frac{(\pm \chi + \beta) g}{\gamma^2 - 4} - \beta t \right) |A|.$$

Now

$$z_0 + z_1 \imath = (h_0 + h_1 \imath)^2 \quad \textit{if and only if} \quad \text{the system} \quad \begin{cases} h_0^2 + \varrho h_1^2 = z_0 \\ h_0 h_1 = z_1/2 \end{cases}$$

has a solution (h_0, h_1) in $(\mathbb{F}_q)^2$.

There would be nothing to prove if $z_1 = 0$, because $z_0 \in \mathbb{F}_q$ is always a square in

$\mathbb{F}_{q^2}$. So we assume $z_1 \neq 0$. Then both h_0 and h_1 are non-zero.
As $h_1 = z_1/(2h_0)$, we have

$$h_0^2 + \varrho\, z_1^2/(4\, h_0^2) - z_0 = 0.$$

Multiply by h_0^2 to obtain

$$h_0^4 - z_0\, h_0^2 + \varrho\, z_1^2/4 = 0.$$

The solutions in h_0^2 are

$$(h_0^2)_\pm = \frac{z_0 \pm \sqrt{z_0^2 - \varrho\, z_1^2}}{2}.$$

Since

$$z_0^2 - \varrho\, z_1^2 = \varepsilon^2\, \nu^2\, \overline{\varepsilon^2}\, \overline{\nu^2} = |A|^2\, (\nu\, \overline{\nu})^2 = |A|^2 \left(\frac{\gamma^2 - 3}{\gamma^2 - 4}\right)^2$$

the discriminant is a square. But the choice of the sign of the square root is forced because

$$\begin{aligned} |A|\, \nu\overline{\nu} = h_0^2 - \varrho\, h_1^2 &= h_0^2 + \varrho\, h_1^2 - 2\, \varrho\, h_1^2 = z_0 - 2\, \varrho\, z_1^2/(4\, h_0^2) \\ &= z_0 - \frac{z_1^2\, \varrho}{z_0 \pm \sqrt{z_0^2 - \varrho\, z_1^2}} = z_0 - \frac{z_1^2\, \varrho\, z_0 \pm \sqrt{z_0^2 - \varrho\, z_1^2}}{\varrho\, z_1^2} = \\ &= \pm\sqrt{z_0^2 - \varrho\, z_1^2} = \pm|A|\nu\overline{\nu}. \end{aligned}$$

So

$$h_0^2 = \frac{z_0 + (\gamma^2 - 3)(\gamma^2 - 4)^{-1}\, |A|}{2} = \frac{z_0(\gamma^2 - 4) + |A|(\gamma^2 - 3)}{2(\gamma^2 - 4)}.$$

Substituting the expression of z_0, the right hand side becomes

$$|A|\, (t\, g \mp \chi\beta^{-1} + 3)/2$$

and must be a square in $\mathbb{F}_q$. This completes the condition for the existence of the extension for $\sigma = \sigma_2^2$.

We observe that there is no global condition for both cases $7 \mid q-1$ and $7 \mid q+1$.

Define

$$C_2(t, g) := (g - t\,(g^2 - 4))^2 - 4\,(g^2 - 3)^2.$$

We may formulate the following

3.2.19 Theorem *Let $\tau = \tau(l)$ be the trace of an element of order l in $PSL(2,q)$, i.e. let τ be a zero of Q_l (see (2.1.2)). Moreover suppose it is $p > 2$. When $q \equiv_7 1$ the surjection 3.2.4*

$$\varphi_7 : (2,3,7) \longrightarrow\!\!\!\!\!\rightarrow PSL(2,q)$$

extends to a surjection

$$\phi_7 : \pi_1(\mathcal{D}^3(\sigma_2^2, 7, l)) \longrightarrow\!\!\!\!\!\rightarrow PSL(2,q), \text{ for } \quad l = 2,3,4 \text{ or } 5,$$

if and only if

$\tau \in \mathbb{F}_q$, $\quad C_2(t,g) = r^2$ *with* $r \in \mathbb{F}_q$ *and, for at least one choice of the sign, there exists* $k \in \mathbb{F}_q$ *such that* $\dfrac{-g + t\,\mu^{-2} \pm r}{2} = k^2$;

while, if $l = 2$ *or 4, it extends to*

$$\Phi_7 : \pi_1(\mathcal{D}^3(\sigma_2^2, 7, l)) \longrightarrow\!\!\!\!\!\rightarrow PGL(2,q)$$

if and only if

$\tau \in \mathbb{F}_q$, $\quad C_2(t,g) = r^2$ *with* $r \in \mathbb{F}_q$ *and, for at least one choice of the sign, there exists* $k \in \mathbb{F}_q$ *such that* $\dfrac{-g + t\,\mu^{-2} \pm r}{2}\,\varrho = k^2$.

When $q \equiv_7 1$ the surjection 3.2.4

$$\varphi_7 : (2,3,7) \longrightarrow\!\!\!\!\!\rightarrow PSL(2,q)$$

extends to a surjection

$$\phi_7 : \pi_1(\mathcal{D}^3(\sigma_2^2, 7, l)) \longrightarrow\!\!\!\!\!\rightarrow PSL(2,q), \text{ for } \quad l = 2,3,4 \text{ or } 5,$$

if and only if

$\tau \in \mathbb{F}_q$, $\quad C_2(t,g) = \chi^2\,\varrho$ *with* $\chi \in \mathbb{F}_q$ *and, for at least one choice of the sign,*

there exists $k \in \mathbb{F}_q$ *such that* $\dfrac{t\,g \mp \chi\beta^{-1} + 3}{2} = k^2$, *where* $\beta^2\,\varrho = g^2 - 4$;

while, if $l = 2$ *or 4, it extends to*

$$\Phi_7 : \pi_1(\mathcal{D}^3(\sigma_2^2, 7, l)) \longrightarrow\!\!\!\!\!\rightarrow PGL(2,q)$$

if and only if

$\tau \in \mathbb{F}_q$, $\quad C_2(t,g) = \chi^2\,\varrho$ *with* $\chi \in \mathbb{F}_q$ *and, for at least one choice of the sign, there exists* $k \in \mathbb{F}_q$ *such that* $\dfrac{t\,g \mp \chi\beta^{-1} + 3}{2}\,\varrho = k^2$.

With the program for algebraic manipulation Macsyma, we have obtained a correspondent of Lemma 3.2.13

3.2.20 Lemma *The product of the three values the function $C_2(.,.)$ takes on the traces g_1, g_2 and g_3, for a fixed t, depends only on t. Namely*

$$\prod_{i=1}^{3} C_2(t, g_i) = 49t^6 - 196t^5 - 98t^4 + 938t^3 - 343t^2 - 1078t + 637.$$

∎

It solves only the first part of the condition: anyway it does not help to get an infinite answer because of the second condition. But it is anyway useful especially when $q = p^3$, providing a first selection of the possible solutions.

We have checked by computer if the Hurwitz actions of $PSL(2,q)$, $q = p$, p prime less than 1000, which do not bound for $\sigma = \sigma_2$, do bound for $\sigma = \sigma_2^2$. We do enlarge the set of positive answers, but we do not yet get positive answer for all surjections.

We have then considered the case $\sigma = \sigma_2^3$. No algebraic pattern seemed to emerge for increasing powers of σ_2 and the computations got cumbersome. We so have decided to do a systematic check on the remaining cases just working with the candidate matrices A of Lemma 3.2.7. We have obtained that all Hurwitz actions of $PSL(2,q)$, for $q = p$, $p < 1000$ do bound for $\sigma = \sigma_2^u$, $u \leq 3$.
We conclude that

3.2.21 Proposition *For $q = p$ prime, $p \doteq_7 \pm 1$, $7 < q < 1000$, any Hurwitz action of $PSL(2,q)$ bounds a hyperbolic 3-manifold.*

The case $q = 27$ remains open at this point, considering only the braid $\sigma = \sigma_2$. Now consider the braid $\sigma = \sigma_2^2$. We have already seen that in case $q = p^3$ the three traces are conjugate under the action, on the field, of the Frobenius automorphism. Then the same happens for any expression in the traces and also for $C_2(t, g_i)$, $i = 1, 2, 3$. So, to check the condition on $C_2(.,.)$, we need merely to analyse the polynomial of Lemma 3.2.20 for the various values of t. Since we are now in the case $7 \mid q + 1$, the condition is $C_2(.,.)$ non-square.

For $t = 0$ the product of Lemma 3.2.20 is $637 \equiv_3 1$. Since it is a square the necessary condition is not satisfied. The product for $t = 1$ and $t = -1$ are respectively $-91 \equiv_3 2$ and $581 \equiv_3 2$: both values are non-squares. Unfortunately, doing computations in a concrete model for $\mathbb{F}_{27}$ we have verified that the second part of the condition of Theorem 3.2.19 is not satisfied, neither for $t = 1$ nor for $t = -1$.

Then we have done a systematic check on candidates for the element A. It turns out that the braids $\sigma = \sigma_2^u$ provide no 3-manifold that bounds. Indeed

$$\sigma_2^u(a)\, \sigma_2^u(b) \longrightarrow \; A\,X\,(T\,A\,X)^{u-1}, \;\; u \geq 1$$

and there are no candidates A for which this product has order 2 or 3 in $PSL(2,27)$. This is not so difficult to check because the maximal order of the cyclic subgroups of $PSL(2,27)$ is not so high.

So the next step was to consider more general braids involving also σ_1. We have written a Pascal program, that given the length, i.e. the total number of half-turns, generates all the possible braids that starts and ends with σ_2 (see on page 68). But the check becomes much longer in increasing length bigger than 10 (also on a VAX). It seems that up to 15 half-twists there is no braid that gives the positive answer.

So, up to now, we may conclude that

3.3.1 Corollary *For $q = p^3$, $p \equiv_7 \pm 2, \pm 3$ and $2 \le p < 100$, $p \ne 3$, the unique Hurwitz action of $PSL(2,q)$ bounds a hyperbolic 3-manifold.*

Chapter 4

Applications

The theorems developed in Chapter 3 applies to find maximally symmetric tetrahedral 3-manifolds, that is 3-manifolds that admit a quotient orbifold with a Coxeter tetrahedron as singular set. A further development of the number theoretical conditions allows us to analyse the case of non-orientable tetrahedral 3-manifolds.

4.1 The group $C[4,3,5]^+$ maps onto $PSL(2,31)$

The *Coxeter group* $C[4,3,5]$ is generated by the reflections in the sides of the tetrahedron $T_{4,3,5}$

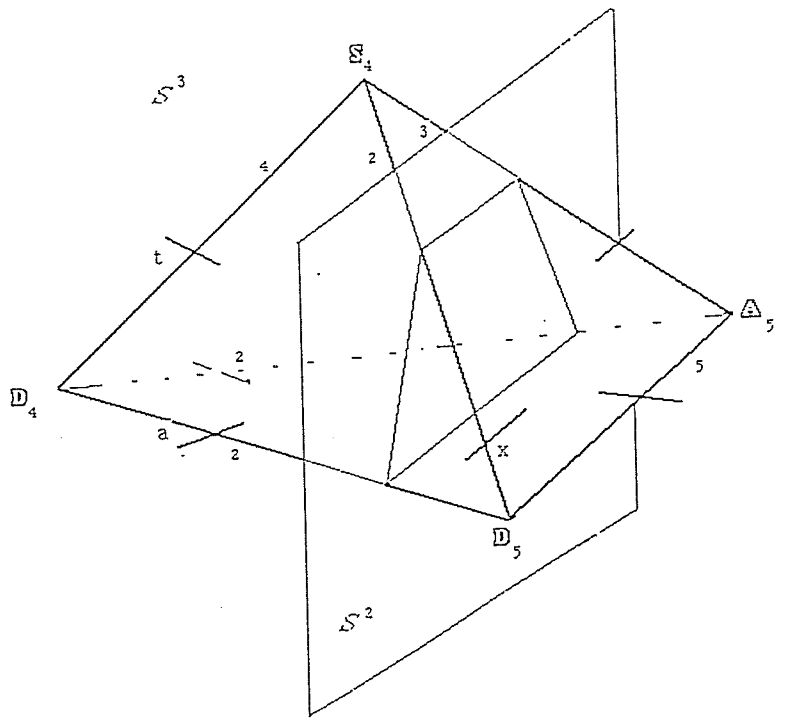


Fig.6

(The notation of Coxeter and Moser in [7] lacks the $\mathcal{C}$. We have added it to distinguish this group from an extended triangle one).
As in Chapter 1, a number m at an edge denotes it is the corner of a dihedral hyperbolic angle π/m. We denote by $\mathcal{C}[4,3,5]^+$ the subgroup of index 2 of orientation preserving isometries of the hyperbolic 3-space $\mathbb{H}^3$: it is called the *tetrahedral group* associated to $T_{4,3,5}$. An edge labelled m has stabilizer Z_m in $\mathcal{C}[4,3,5]^+$, and each vertex has the stabilizer as indicated in Fig.6.

The tetrahedral group $\mathcal{C}[4,3,5]^+$ is an infinite properly discontinuous group of isometries of $\mathbb{H}^3$. The quotient $\mathbb{H}^3/\mathcal{C}[4,3,5]^+$ is an orbifold Q, whose underlying topological space is S^3 and whose singular set is the 1-skeleton of $T_{4,3,5}$.

As in Chapter 1 a presentation for $\mathcal{C}[4,3,5]^+$ is obtained from the singular set, as the Wirtinger presentation is obtained from a planar projection of a knot or link. Let the generators be chosen as in Fig.6, then we have

$$\mathcal{C}[4,3,5]^+ = \langle t, x, a \,|\, t^4 = x^2 = a^2 = (tx)^3 = (ta)^2 = (xa)^5 = 1 \rangle.$$

The plane in Fig.6 stands for an embedded 2-sphere that meets the singular set of Q in four points of orders 2, 2, 2 and 3. This 2-sphere divides the 3-orbifold into two 3-orbifolds with boundary, both of Euler characteristic $-1/12$ [29, Ch.13] and [30, Ch.5].

Let U be any normal torsion free subgroup of finite index in $\mathcal{C}[4,3,5]^+$. Its existence is assured by the Selberg's Lemma:

> Lemma:*Any finitely generated subgroup of the general linear group $GL(n,\mathbb{C})$ has a torsion free subgroup of finite index.*

Let K be $\mathcal{C}[4,3,5]^+/U$. Then the K-action on $\mathcal{M} := \mathbb{H}^3/U$ is maximal [33, §3] and the quotient orbifold $\mathcal{M}/K$ is exactly Q. Moreover we have the relation $|K| = 12(g-1)$, where g is the genus of the 2-surface covering the embedded 2-sphere of Q (Fig.6). Certainly we are looking for subgroups of small index, as done in [32] for the hyperbolic tetrahedral group $\mathcal{C}[5,3,5]^+$ (which maps onto A_5). But the quotient of $\mathcal{C}[4,3,5]^+$ cannot be a spherical group. Then the next finite simple groups to investigate are the projective linear groups.

4.1.1 Maps of $\mathcal{C}[4,3,5]^+$ onto $PSL(2,p)$

Since we are interested in torsion free kernels we need to find three elements T, X and A, the classes of which generate $PSL(2,p)$, and such that

$$T^4 = X^2 = A^2 = (T\,X)^3 = (T\,A)^2 = (X\,A)^5 = 1.$$

There are elements of order 4 and 5 in $PSL(2,p)$ if and only if $p \equiv_8 \pm 1$ and $p \equiv_5 \pm 1$. Then by the Chinese Remainder theorem (see Appendix A) there are infinitely many values that satisfy both congruences: the smallest is $p = 31$.

Now we apply the procedure developed to determine the extensions of the maps φ_γ. We start from the subgroup $\mathrm{S}_4 = (2,3,4)$.

Let us choose up to conjugation, a diagonal form for T, either in $PSL(2,p)$ or in $PSU(2,p^2)$. We proceed as in Chapter 3, in particular we refer to Theorem 3.2.10.

We choose T and X as in Definition 3.2.4. Then we need to find the element A. Now the trace of T is $\gamma = \pm\sqrt{2}$ and the trace of A is $\tau = \pm(1+\sqrt{5})/2$ or $\pm(1-\sqrt{5})/2$. By Remark 3.2.11, to find A in $PSL(2,p)$ the value of the function $C(\tau,\gamma) = 4-2\tau^2$ must be a square. For $p = 31$ the function C assumes the values 26 and $7 = 10^2$. So the latter permit us to find the element A in $PSL(2,p)$.

> Remark:*In Definition 3.2.4 the element T (of order 7) and the element X (of order 2) already generate $PSL(2,p)$, but here the situation does not repeat. In fact the present T and X generate an octahedral subgroup S_4 of $PSL(2,p)$. The extra element A cannot belong to this octahedral subgroup because XA has order 5 and there are no elements of order 5 in S_4 (by the Lagrange theorem on the order of the subgroups). Then the subgroup generated by T, X and A properly contains an S_4 (and also an A_5): by the classification of subgroups of a projective special linear group it must coincide with $PSL(2,p)$ itself.*

So there exists a short exact sequence

$$\mathbb{I} \to U \to C[4,3,5]^+ \to PSL(2,31) \to \mathbb{I}.$$

Since $|PSL(2,31)| = 14880$ the equivariant Heegaard genus of $\mathbb{H}^3/U$ is

$$1 + 14880/12 = 1241.$$

4.1.2 Decreasing the order of the target

Since we are interested in finding surjective maps onto groups of order as smaller as possible, we are going to check if some $PSL(2,p^n)$, $n > 1$, or $PGL(2,p^n)$, $n \geq 1$, of order less than 14·880 already admits a surjection of $C[4,3,5]^+$.

Let us first review the simple groups $PSL(2,p^n)$.
Since there are no elements of order 4 in any $PSL(2,2^n)$, the values p^n for $p = 2$ are excluded.

So we have still to examine $PSL(2,9)$ and $PSL(2,25)$.

A model for $\mathbb{F}_9$ is

$$\mathbb{F}_3[x]/(x^2+1) := \{0, \pm1, \pm x, \pm(1+x), \pm(1-x)\}$$

where in computations we have to remember that $x^2 \equiv -1 \equiv_3 2$.

The table of squares is

z	±1	$\pm x$	$\pm(1+x)$	$\pm(1-x)$
z^2	1	-1	$-x$	x

The trace γ of an element of order 4 is the solution of

$$\gamma^2 - 2 = 0$$

which in this model of $\mathbb{F}_9$ is $\gamma = \pm x$.

The trace of an element of order 5 is

$$\tau = \pm(1+\sqrt{5})/2 = \mp(1+x) \quad \text{or} \quad \pm(1-\sqrt{5})/2 = \mp(1-x)$$

because $5 \equiv_3 -1$, $\sqrt{-1} = \pm x$ and $2^{-1} \equiv_3 -1$.

Then

$$C(\tau,\gamma) = \tau^2\gamma^2 - 4(\tau^2+\gamma^2) + 12 = 1 \mp x.$$

Both values are non-squares. So we can not find a surjection onto $PSL(2,9)$.

Turn us to $PSL(2,25)$.

Since the squares in $\mathbb{F}_5$ are ± 1 and the non-squares are ± 2, a model for $\mathbb{F}_{25}$ is

$$\mathbb{F}_5[x]/(x^2-2) = \{0, \pm 1, \pm 2, \pm x, \pm 2x, ..., \pm(2-2x)\}$$

where $x^2 \equiv 2$ and so $\pm\sqrt{2} = \pm x$. (We will not need the table of squares!)

The trace $\tau = \tau(5)$ is $\pm 1/2 = \pm 3 = \mp 2$ because $5 \equiv_5 0$. Indeed the elements of order 5 in $\mathbb{F}_{25}$ are exactly the parabolic ones. Then

$$C(\tau,\gamma) = 1$$

is really a square in $\mathbb{F}_{25}$.

> Remark: *The fact that AX is parabolic does not trouble the developments and computations. We start with T of order 4 in diagonal form. Then choose X and last A (all as in Theorem 3.2.10). The condition on AX is that the trace squared is equal to 4: the right characterization of parabolic elements.*

We may compute explicitely the images of the generators:

$$T = \pm\begin{pmatrix} x & 0 \\ 0 & -2x \end{pmatrix}, \quad X = \pm\begin{pmatrix} x & 1 \\ 2 & -x \end{pmatrix}, \quad A = \pm\begin{pmatrix} 0 & -2+x \\ 1-2x & 0 \end{pmatrix}.$$

So we have found that the group $C[4,3,5]^+$ acts on a tetrahedral hyperbolic 3-manifold with Heegaard equivariant genus equal to $1 + 7800/2 = 651$.

Let us review now the groups $PGL(2,q)$. The order obstruction leaves the following possibilities:

$$PGL(2,5), PGL(2,9), PGL(2,11), PGL(2,19).$$

The order of $PGL(2,25)$ is already bigger than 14·880.

Note that the condition (C') of Theorem 3.2.10 reads now

$$\gamma^2\,\varrho \textit{ square in } \mathbb{F}_q \textit{ and } C(\tau,\gamma) \textit{ non-square in } \mathbb{F}_q,$$

where as usual γ is the trace of T, which has now even order. (As before ϱ is a non-square, and in particular a primitive root, in $\mathbb{F}_q$.)

Let us analyze the condition in each of the above groups.

In the group $PGL(2,5)$ we find elements of order 4 because $[\gamma(4)]^2 \cdot \varrho$ is a square in $\mathbb{F}_5$. We already know that $\tau = \tau(5) = \pm 2$ and $C(\tau,\gamma) = 1$. So condition (C') is not satisfied.

We exclude also $PGL(2,9)$ because the value $[\gamma(4)]^2\,\varrho$ is non square in $\mathbb{F}_9$.

But $[\gamma(4)]^2\,\varrho$ is square in $\mathbb{F}_{11}$: the table of squares in $\mathbb{F}_{11}$ is

z	± 1	± 2	± 3	± 4	± 5
z^2	1	4	9	5	3

so 2 is a non-square (it is also a primitive root). Take $\varrho = 2$.

Since $\sqrt{5} = 4$ and $1/2 = 6$, we have $\tau = \tau(5) = \pm 8 \equiv_{11} \mp 3$ or $\mp 7 = \pm 4$.

The possible values taken by the function $C(.,.)$ are:

$$C(\mp 3, \pm\sqrt{2}) = -25 \equiv_{11} 8$$

and

$$C(\pm 4, \pm\sqrt{2}) = -17 \equiv_{11} 5 = (\pm 4)^2.$$

Since the last value satifies the condition, let us exhibit the effective surjection.

As $11 \equiv_8 3$ implies $11 \equiv_4 -1$, it follows $4 \,|\, 11+1$ and T is elliptic in $PGL(2,11)$, i.e. the value of λ is to be found in

$$\mathbb{F}_{121} = \mathbb{F}_{11}[x]/(x^2-2) = \{a + b\imath \;\mid\; a, b \in \mathbb{F}_{11} \text{ and } \imath^2 = \varrho = 2\}.$$

Finally

$$T = \pm\begin{pmatrix} 1 \mp 4\imath & 0 \\ 0 & 1 \pm 4\imath \end{pmatrix}, \quad X = \pm 4\imath \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

For A we get two possible different values:

$$A = \pm\begin{pmatrix} 0 & -\imath \\ \imath & 0 \end{pmatrix}, \quad \text{and} \quad A = \pm\begin{pmatrix} 0 & -4\imath \\ 3\imath & 0 \end{pmatrix}.$$

So we have defined a map in $PGL(2,11)$. It remains to check if it is a surjection. Since $PGL(2,11)$ is a subgroup of $PSL(2,121)$, the subgroups of the former are subgroups of the latter. Moreover $\langle X, T, A\rangle$ properly contains both A_5 and S_4, and it can not be $PSL(2,11)$, to which such a map could not even be defined. Then by the classification of subgroups of $PSL(2,121)$ it must coincide with $PGL(2,11)$.

We have so lost any interest for bigger groups, and we do not even consider the case $PGL(2,19)$.

4.2 The bounded 3-dimensional hyperbolic Coxeter tetrahedra

The tetrahedron $T_{4,3,5}$ is one of the nine bounded Coxeter tetrahedra in $\mathbb{H}^3$, i.e. the hyperbolic 3-dimensional simplices with dihedral angles integral submultiples of π [7, p.132]. Denote by $T(s_1, s_2, s_3; m_1, m_2, m_3)$ a tetrahedron where π/s_i are the three dihedral angles at the edges of a face, and π/m_i the dihedral angles at the opposite edges of the tetrahedron.

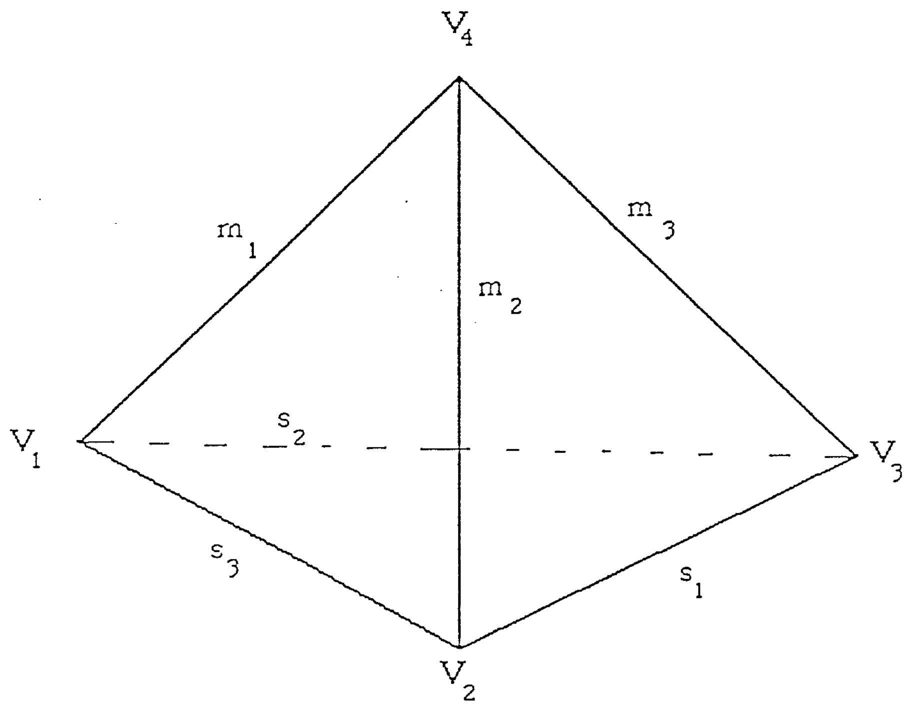


Fig.7

Let us call the vertices of the tetrahedron V_i, $i = 1, 2, 3, 4$ and r_i the face opposite to the vertex V_i, $i = 1, 2, 3, 4$.

Let us denote with the same letter r_i the reflection in the plane opposite to the vertex V_i, $i = 1, 2, 3, 4$.

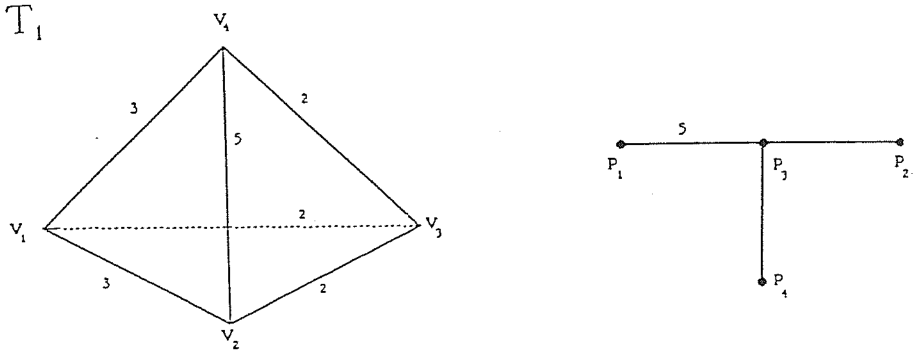
The group $G = G(s_1, s_2, s_3; m_1, m_2, m_3)$ generated by the reflections in the faces of the tetrahedron $T(s_1, s_2, s_3; m_1, m_2, m_3)$ has presentation

$$\begin{aligned} \langle r_1, r_2, r_3, r_4 \mid r_1^2 = r_2^2 = r_3^2 = r_4^2 = 1 \\ (r_1 r_2)^{m_3} = (r_2 r_3)^{m_1} = (r_1 r_3)^{m_2} = 1 \\ (r_1 r_4)^{s_1} = (r_2 r_4)^{s_2} = (r_3 r_4)^{s_3} = 1 \rangle. \end{aligned}$$

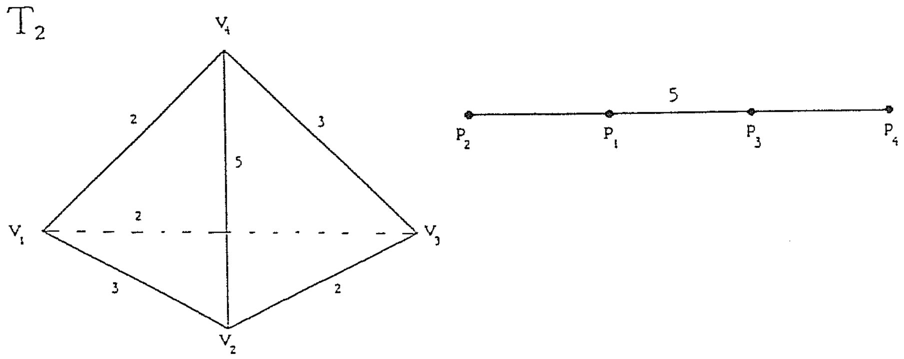
The group G is a group of isometries of the hyperbolic space $\mathbb{H}^3$.

We picture the nine Coxeter tetrahedra, following notations in [31, p.41]. For each tetrahedron we give also the Coxeter graph: each vertex corresponds to a face and two vertices are adjacent if the correspondent faces form a dihedral angle π/m, $m \geq 3$ (when $m \geq 4$, we mark the edge of the graph with m).

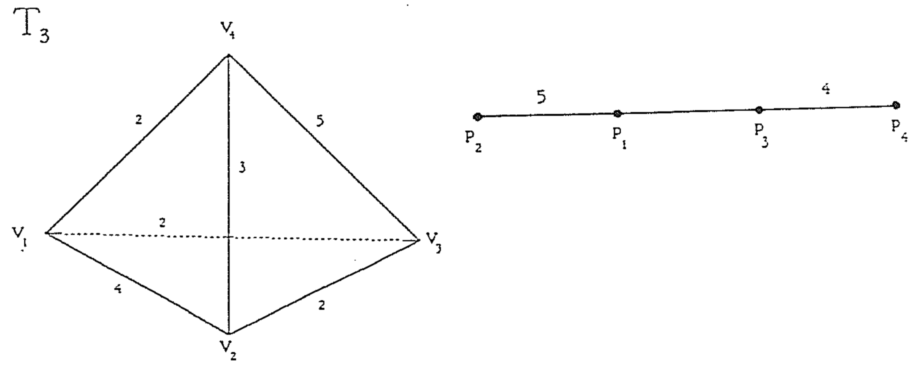
$T_1 = T(2,2,3;3,5,2)$



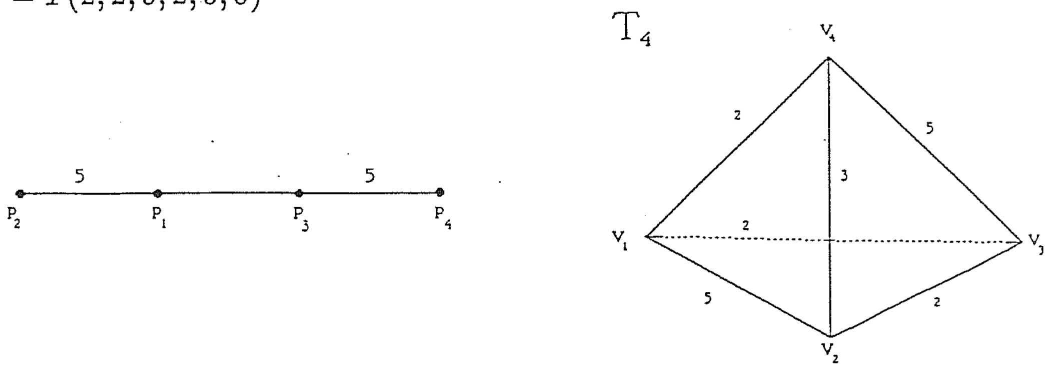
$T_2 = T(2,2,3;2,5,3)$



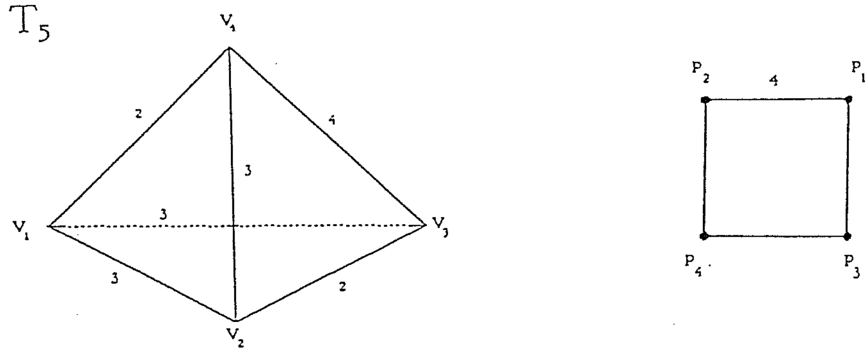
$T_3 = T(2,2,4;2,3,5)$



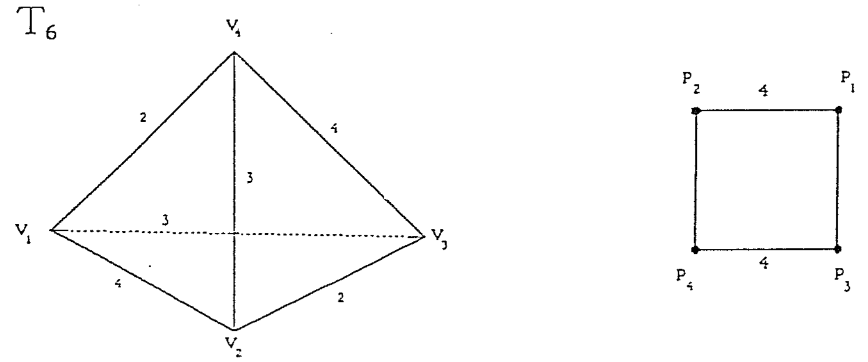
$T_4 = T(2,2,5;2,3,5)$



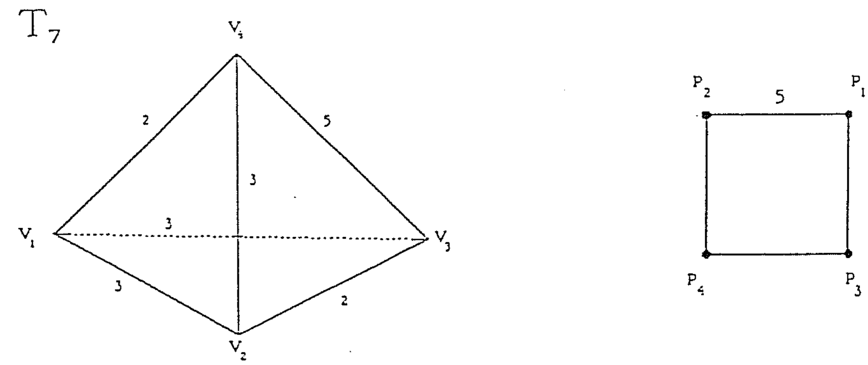
$T_5 = T(2,3,3;2,3,4)$



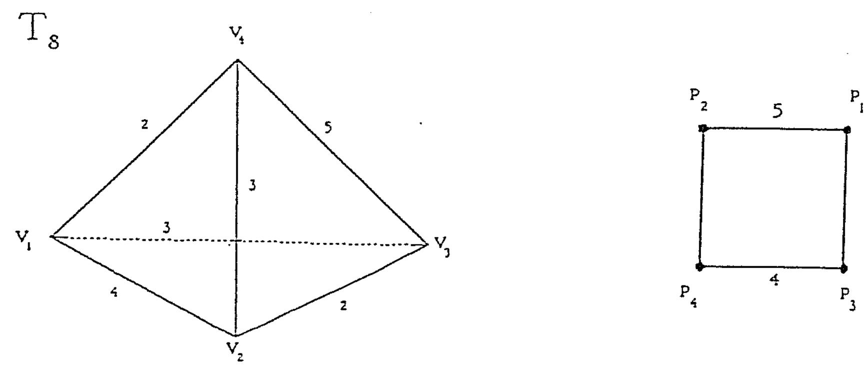
$T_6 = T(2,3,4;2,3,4)$



$T_7 = T(2,3,3;2,3,5)$

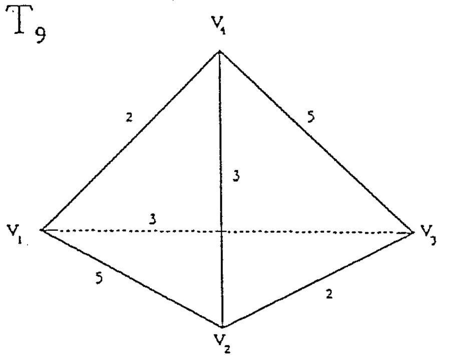


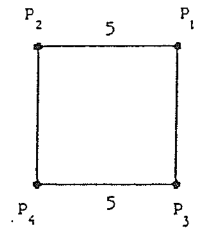
$T_8 = T(2,3,4;2,3,5)$



$T_9 = T(2,3,5;2,3,5)$

$T_9 = T(2,3,5;2,3,5)$





We will briefly call G_i the group generated by the reflections in the faces of T_i, and G_i^+ its subgroup of index 2 of orientation preserving elements.

4.3 Non-orientable hyperbolic 3-manifolds

We will now consider as an application the non-orientable (compact) hyperbolic 3-manifolds of tetrahedral type.

Let us first explain the situation by the 2-dimensional analogue [25]: take a Coxeter triangle

$m, s, k \in \mathbb{N}$ such that $1/m + 1/s + 1/k < 1$

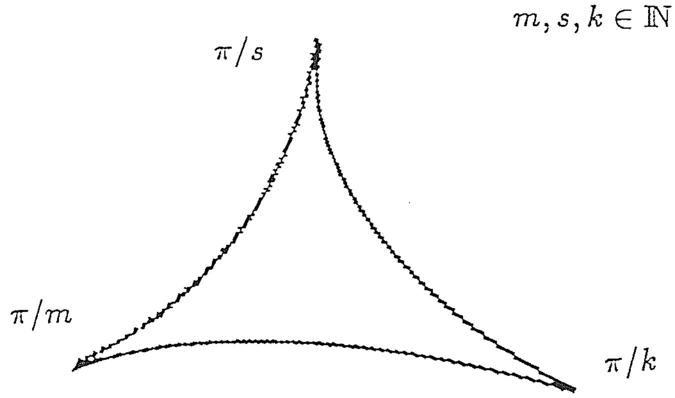


Fig.8

As we have already said in Chapter 1, the group of reflections in the sides of the triangle is the extended triangle group $[m, s, k]$ and represents a discrete subgroup of isometries of the hyperbolic plane. The triangle group (s, k, m) is the subgroup of index 2 of the orientation preserving isometries. Suppose we are given the exact diagram of groups

$$\begin{array}{ccccccccc} 1 & \longrightarrow & ker\,\varphi & \longrightarrow & (m,s,k) & \overset{\varphi}{\searrow} & & & \\ & & \downarrow & & \downarrow & & PSL(2,q) & \longrightarrow & 1 \\ 1 & \longrightarrow & ker\,\phi & \longrightarrow & [m,s,k] & \underset{\phi}{\nearrow} & & & \end{array}$$

then $ker\,\varphi$ is a subgroup of index 2 in $ker\,\phi$. The group $ker\,\varphi$ is a Fuchsian group and $PSL(2,q)$ acts on the Riemann surface $\mathcal{F} = \mathbb{H}^2/ker\,\varphi$. The geometric diagram of covering spaces is in Fig.9. The orbifold $\mathcal{O}$ has no boundary and the edges of the underlying topological space are silvered, see [30, Ex. 5.2.4] and [17, p.83]. Moreover according to [17, pp. 85, 87] the orbifold $\mathcal{O}$ is non-orientable.

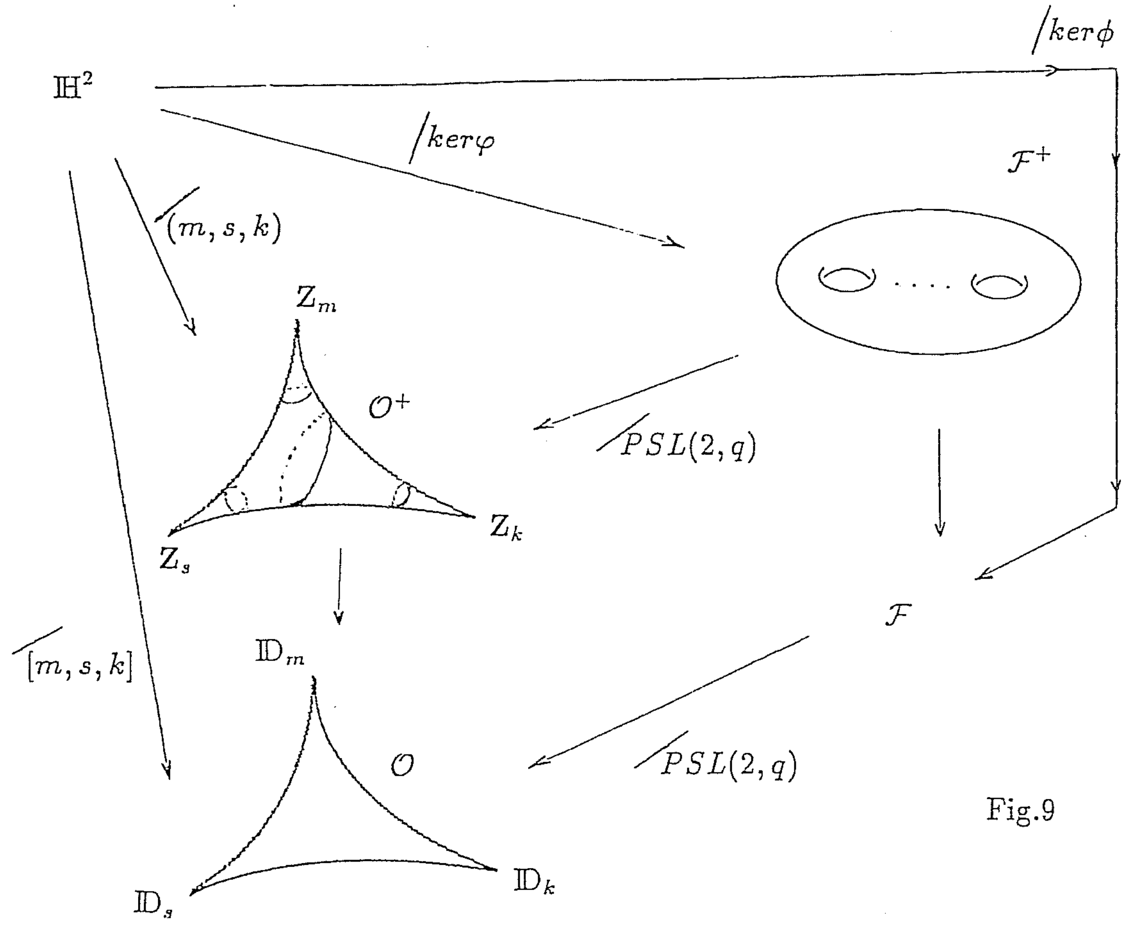


Fig.9

The Riemann surface $\mathcal{F}^+$ is a 2-fold covering of $\mathcal{F}$ by an orientation reversing involution. Indeed the group $ker\,\varphi$ is the maximal subgroup without orientation reversing elements and has index 2 in $ker\,\phi$. Since the orientation reversing transformations already apply in the quotient from $\mathcal{F}^+$ to $\mathcal{F}$, it is clear that $\mathcal{F}$ is a non-orientable surface and $\mathcal{F}^+$ is its canonical double [25, Ch.2, Thm.1] and [3, §9].

In the 3-dimensional case the underlying topological space of the orbifold $\mathbb{H}^3/G_i$ is the tetrahedron $\mathcal{T}_i$. Each vertex group is the extended triangle group in the labels of the concurrent edges, and each edge group is the dihedral group of order the correspondent label.

If G_i maps onto the simple group $PSL(2,q)$, then automatically the group G_i^+, of index 2 in G_i, maps onto $PSL(2,q)$. The tetrahedron is then a non-orientable orbifold with the faces silvered.

In each hyperbolic Coxeter tetrahedron there is always at least one vertex labelled $[2,3,m]$, $m = 4$ or 5. We know how to define a surjective map of $(2,3,m)$, $m = 4$ or 5, onto $PSL(2,q)$ and moreover we have determined the exact condition to be able to extend to a surjection from $[2,3,m]$. Since the presentation we used early for $[2,3,m]$ is

$$\langle x,t,a \mid x^2 = t^m = (x\,t)^3 = a^2 = (t\,a)^2 = (x\,a)^2 = 1\rangle$$

we are motivated to consider a different presentation also for G_i, namely

$$\langle x,t,a,r \mid x^2 = t^m = (x\,t)^3 = a^2 = (t\,a)^2 = (x\,a)^2 = 1$$
$$r^2 = (r\,a)^k = (r\,a\,t)^l = (r\,a\,x)^s = 1\rangle.$$

The group $[2,3,m]$ may be always placed at the vertex V_4. Then the generators t and x are the rotations of order m and 2, suitable product of two reflections among r_1, r_2 and r_3. The generator a is the common reflection to x and t, and r is the reflection r_4 ("opposite" to the vertex V_4).

Resuming the situation:
for $\mathcal{T}_1$

$$t \mapsto r_3\,r_1,\quad x \mapsto r_1\,r_2 \text{ which implies } (r\,a)^2 = (r\,a\,t)^3 = (r\,a\,x)^2 = 1$$

for $\mathcal{T}_2$

$$t \mapsto r_1\,r_3,\quad x \mapsto r_3\,r_2 \text{ which implies } (r\,a)^3 = (r\,a\,t)^2 = (r\,a\,x)^2 = 1$$

for $\mathcal{T}_i$, $i \geq 3$,

$$t \mapsto r_2\,r_1,\quad x \mapsto r_3\,r_2 \text{ which implies } (r\,a)^{s_2} = (r\,a\,t)^2 = (r\,a\,x)^{s_3} = 1.$$

We suppose to have already at hand a map of $[2,3,m]$ in $PSL(2,q)$ given by Theorem 3.2.10 and Remarks. Remind that

$$T = \pm\begin{pmatrix} \lambda & 0 \\ 0 & \overline{\lambda} \end{pmatrix}, \text{ where } \gamma = \pm g,\quad g = \lambda + \overline{\lambda}$$

$$X = \pm\begin{pmatrix} \mu & \nu \\ \omega & -\mu \end{pmatrix}, \quad \text{where} \quad \mu^2 = 1/(\gamma^2 - 4),\quad \nu\,\omega = \frac{3-\gamma^2}{\gamma^2-4}.$$

$$A = \pm\begin{pmatrix} 0 & \varepsilon \\ -\overline{\varepsilon} & 0 \end{pmatrix}, \quad \varepsilon\,\overline{\varepsilon} = 1.$$

Now the trace τ of Theorem 3.2.10 is equal to zero, so

$$\varepsilon = \pm r/(2\,\omega) \quad \text{and } \overline{\varepsilon} = \pm r/(2\,\nu), \text{ where } r^2 = 4\,\nu\,\omega \text{ in } \mathbb{F}_{q^2}.$$

So we have to determine an element of order 2

$$R = \pm \begin{pmatrix} \delta & \xi \\ \eta & -\delta \end{pmatrix}, \quad -\delta^2 - \xi\,\eta = 1,$$

such that

$$R\,A = \pm \begin{pmatrix} -\xi\,\overline{\varepsilon} & \delta\,\varepsilon \\ \delta\,\overline{\varepsilon} & \eta\,\varepsilon \end{pmatrix} \text{ has order } l,$$

$$R\,A\,T = \pm \begin{pmatrix} -\xi\,\overline{\varepsilon}\,\lambda & \delta\,\varepsilon\,\overline{\lambda} \\ \delta\,\overline{\varepsilon}\,\lambda & \eta\,\varepsilon\,\overline{\lambda} \end{pmatrix} \text{ has order } s,$$

$$R\,A\,X = \pm \begin{pmatrix} -\xi\,\overline{\varepsilon}\,\mu + \delta\,\varepsilon\,\omega & -\xi\,\overline{\varepsilon}\,\nu - \delta\,\varepsilon\,\mu \\ \delta\,\overline{\varepsilon}\,\mu + \eta\,\varepsilon\,\omega & \delta\,\overline{\varepsilon}\,\nu - \eta\,\varepsilon\,\mu \end{pmatrix} \text{ has order } k.$$

We get the system

$$\begin{cases} -\xi\,\overline{\varepsilon} + \eta\,\varepsilon = w \\ -\xi\,\overline{\varepsilon}\,\lambda + \eta\,\varepsilon\,\overline{\lambda} = v \\ -\mu(\xi\,\overline{\varepsilon} + \eta\,\varepsilon) + \delta\,(\varepsilon\,\omega + \overline{\varepsilon}\,\nu) = \kappa \end{cases}$$

where w, v and κ are the traces of elements of respective order l, s and k. (We are looking for maps onto $PSL(2,q)$, so all representatives are supposed normalized: it follows that w, v and κ are roots of Q_l, Q_s and respectively Q_κ.)

Observe that

$$\varepsilon\,\omega + \overline{\varepsilon}\,\nu = \pm r.$$

The system gives the solutions

$$\delta = (\pm r)^{-1} \left(\kappa + \mu \frac{w\,g - 2\,v}{\lambda - \overline{\lambda}}\right)$$

$$\xi = 2\,\nu\,(\pm r)^{-1}\,\frac{w\,\overline{\lambda} - v}{\lambda - \overline{\lambda}}, \qquad \eta = 2\,\omega\,(\pm r)^{-1}\,\frac{w\,\lambda - v}{\lambda - \overline{\lambda}}$$

We have to check now if there are values of w, v, κ (compatible with our requests) such that

$$-\delta^2 - \xi\,\eta = 1$$

i.e. substituting

$$-\Delta^{-1}\left(\kappa + \mu\,\frac{w\,g - 2\,v}{\lambda - \overline{\lambda}}\right)^2 - \mu^2(w^2 - v\,w\,g + v^2) = 1.$$

Since w, v, κ are not all 3 contemporaneously different from zero, it is more simple to consider separately three cases, namely $\mathcal{T}_1$ and $\mathcal{T}_2$, then $\mathcal{T}_3$ and $\mathcal{T}_4$, and last all the remaining tetrahedra $\mathcal{T}_i$, $5 \leq i \leq 9$.

The above condition applies also to the case of totally geodesic boundary. The non-orientable orbifold to consider is now a truncated tetrahedron.

Chapter 5

Tables and programs

Here we have collected tables and programs supporting the stated results.

We give first the table for the detailed analysis of condition 3.2.10(C) when $q = p$, p prime, $p \equiv_7 \pm 1$, $7 < p < 1000$. The entries are explained by the headings. The table is divided into seven columns; from the left we encounter

- the order q of the field,
- the trace g_i, $i = 1, 2, 3$, (there are three for each q, each with its proper row),
- the values of $C(\tau(l), \pm g_i)$, $l = 2, 3$ and 5, for a total of four columns (the two columns for $l = 5$ correspond to the two values for $\tau(5)$; no entries in these columns means that there are no elements of order 5),

and last, a service-column with

- an arrow at each row that gives negative answer to condition 3.2.10 (C) for all $l = 2, 3$ or 5.

All numbers that are squares in Z_q appear with the respective root, also the traces to allow the comparison of our results with those in [4]..

The entries of the table are produced by a computer program written in the Pascal computer language. The program follows the table. It has been run on a VAX which reserves 32 bit for a variable-word of integer type. So the integer range is

$$\pm(2^{31} - 1) = \pm 2{\cdot}147{\cdot}483{\cdot}647 = \pm(46{\cdot}340.95)^2.$$

Then the built in arithmetic operations allow computations in Z_p, for any p up to 46·340. The most troubling operation is obviously multiplication. Since we keep p under 1000 we would be allowed to do products also of three factors, without intermediate reductions modulo p, but in any case not of four.

TABLE

q	g_i	$C(0,g_i)$	$C(\pm 1,g_i)$	$C(\pm\frac{1+\sqrt{5}}{2},g_i)$	$C(\pm\frac{1-\sqrt{5}}{2},g_i)$	$u \geq 2$
	7	11	$4=2^2$			
13	8	$3=4^2$	11			
	$10=6^2$	2	7			←
	3	$5=11^2$	10	11	14	
29	$7=6^2$	19	$6=8^2$	15	$13=10^2$	
	18	21	$22=14^2$	$28=12^2$	17	
	14	7	35	26	$31=20^2$	
41	30	$20=15^2$	14	13	$9=3^2$	
	$37=18^2$	30	$1=1^2$	3	11	
	8	$14=10^2$	$31=17^2$			
43	$15=12^2$	$15=12^2$	$21=8^2$			
	19	30	$0=0^2$			
	$4=2^2$	$19=27^2$	31	68	$6=19^2$	
71	14	$9=3^2$	59	$12=15^2$	14	
	52	59	61	$8=24^2$	$45=20^2$	
	$10=33^2$	$27=39^2$	$40=17^2$			
83	15	$25=5^2$	80			
	57	47	55			←
	$25=5^2$	34	$73=48^2$			
97	30	$1=1^2$	$24=11^2$			
	41	78	$9=3^2$			
	$9=3^2$	27	$104=45^2$			
113	24	$81=9^2$	$88=38^2$			
	79	21	43			←
	24	$121=11^2$	58			
127	$36=6^2$	$35=17^2$	57			
	66	114	$21=23^2$			
	$5=12^2$	$51=32^2$	72	$0=0^2$	26	
139	23	$120=26^2$	$89=28^2$	$96=42^2$	$51=32^2$	
	110	123	126	76	40	←
	$19=55^2$	71	$94=42^2$			
167	$25=5^2$	17	$137=53^2$			
	$122=17^2$	95	$112=46^2$			
	$37=47^2$	$147=50^2$	$64=8^2$	$169=13^2$	57	
181	$43=62^2$	$37=47^2$	72	19	160	
	$100=10^2$	$13=70^2$	54	85	$64=8^2$	
	95	$160=95^2$	119			
197	140	18	111			←
	$158=54^2$	35	$173=31^2$			
	18	$193=68^2$	91	$101=34^2$	190	
211	$81=9^2$	$143=96^2$	159	$54=73^2$	$69=51^2$	
	111	102	181	$45=16^2$	$185=94^2$	

(continued)

TABLE(cont.)

q	g_i	$C(0,g_i)$	$C(\pm1,g_i)$	$C(\pm\frac{1+\sqrt{5}}{2},g_i)$	$C(\pm\frac{1-\sqrt{5}}{2},g_i)$	$u\geq 2$
223	92	52	$38=22^2$			
	142	$82=64^2$	$172=29^2$			
	$211=65^2$	$105=95^2$	22			
239	$6=22^2$	107	139	173	137	$\leftarrow$
	$34=89^2$	168	$125=84^2$	154	53	
	$198=26^2$	219	223	$48=54^2$	$163=101^2$	
251	$106=68^2$	248	185	26	30	$\leftarrow$
	$190=21^2$	188	$140=89^2$	234	$249=91^2$	
	$205=74^2$	82	186	$66=98^2$	159	
281	47	168	$125=94^2$	177	30	
	240	$32=34^2$	23	243	75	
	$274=67^2$	97	142	166	$163=43^2$	
293	$54=126^2$	$68=19^2$	50			
	$254=66^2$	$81=9^2$	$133=96^2$			
	$277=34^2$	$160=63^2$	119			
307	$63=129^2$	$100=10^2$	74			
	267	59	120			$\leftarrow$
	283	$164=85^2$	$122=95^2$			
337	143	$107=118^2$	332			
	$227=100^2$	140	$104=21^2$			
	303	106	247			$\leftarrow$
349	133	103	338	237	325	$\leftarrow$
	237	$92=21^2$	$68=106^2$	10	102	
	$327=26^2$	170	$301=67^2$	65	319	
379	$205=179^2$	188	140	317	$294=108^2$	
	$219=149^2$	321	145	$36=6^2$	78	
	$333=43^2$	265	$103=122^2$	274	$149=161^2$	
419	$196=14^2$	$121=11^2$	404	$62=30^2$	$191=97^2$	
	285	$256=16^2$	$191=97^2$	83	234	
	356	58	$252=154^2$	$136=107^2$	143	
421	116	76	56	151	362	$\leftarrow$
	$322=208^2$	382	$75=51^2$	$165=43^2$	$99=138^2$	
	403	$400=20^2$	$299=126^2$	42	34	
433	62	224	$167=159^2$			
	378	$36=6^2$	$26=66^2$			
	$425=138^2$	189	249			$\leftarrow$
449	43	$249=105^2$	298	$295=173^2$	$350=203^2$	
	$51=167^2$	384	$287=130^2$	$128=209^2$	$349=221^2$	
	354	281	$322=188^2$	292	$393=217^2$	
461	221	112	83	$367=132^2$	231	
	$266=95^2$	42	261	8	$272=46^2$	
	434	$323=28^2$	$126=204^2$	$402=223^2$	$114=110^2$	

(continued)

TABLE(cont.)

q	g_i	$C(0,g_i)$	$C(\pm 1,g_i)$	$C(\pm\frac{1+\sqrt{5}}{2},g_i)$	$C(\pm\frac{1-\sqrt{5}}{2},g_i)$	$u \geq 2$
	$67 = 175^2$	$113 = 24^2$	431			
463	75	199	$264 = 46^2$			
	320	$167 = 104^2$	$240 = 59^2$			
	$227 = 182^2$	116	86	$321 = 199^2$	312	
491	$291 = 42^2$	78	$303 = 57^2$	259	$81 = 9^2$	
	$463 = 44^2$	313	$111 = 137^2$	384	$127 = 40^2$	
	111	$22 = 81^2$	267			
503	$144 = 12^2$	$63 = 165^2$	$172 = 41^2$			
	247	434	$73 = 24^2$			
	$54 = 222^2$	382	12			$\leftarrow$
547	$179 = 267^2$	393	$157 = 269^2$			
	$313 = 163^2$	335	387			$\leftarrow$
	$204 = 70^2$	$256 = 16^2$	$191 = 144^2$			
587	445	362	$564 = 218^2$			
	524	$572 = 137^2$	428			
	292	$324 = 18^2$	$242 = 38^2$	427	$576 = 24^2$	
601	388	38	328	$392 = 103^2$	$554 = 69^2$	
	$521 = 73^2$	255	$40 = 190^2$	34	$432 = 178^2$	
	$16 = 4^2$	222	474			$\leftarrow$
617	254	471	$198 = 94^2$			
	346	$557 = 55^2$	571			
	$79 = 292^2$	$288 = 134^2$	$215 = 171^2$	$388 = 152^2$	600	
631	560	$40 = 157^2$	$29 = 241^2$	$81 = 9^2$	597	
	622	319	396	$32 = 255^2$	206	
	20	341	$94 = 105^2$			
643	224	$567 = 247^2$	$585 = 218^2$			
	$398 = 236^2$	$394 = 275^2$	$616 = 221^2$			
	$58 = 306^2$	$395 = 151^2$	$460 = 200^2$	640	$345 = 193^2$	
659	67	$508 = 205^2$	$380 = 229^2$	279	$353 = 75^2$	
	533	431	$487 = 289^2$	490	$540 = 281^2$	
	$85 = 249^2$	51	542			$\leftarrow$
673	94	$337 = 195^2$	420			
	493	301	393			$\leftarrow$
	$388 = 33^2$	$696 = 145^2$	$521 = 169^2$	2	$164 = 133^2$	
701	$485 = 177^2$	$555 = 69^2$	240	147	18	
	$528 = 349^2$	$167 = 332^2$	650	372	$9 = 3^2$	
	41	558	54			$\leftarrow$
727	$225 = 15^2$	$345 = 156^2$	76			
	460	$567 = 152^2$	606			
	21	$477 = 165^2$	$171 = 266^2$			
743	$282 = 140^2$	$663 = 94^2$	$682 = 202^2$			
	439	362	642			$\leftarrow$

(continued)

TABLE(cont.)

q	g_i	$C(0,g_i)$	$C(\pm 1,g_i)$	$C(\pm\frac{1+\sqrt{5}}{2},g_i)$	$C(\pm\frac{1-\sqrt{5}}{2},g_i)$	$u \geq 2$
757	136	$214 = 224^2$	$538 = 53^2$			
	294	217	$351 = 89^2$			
	$326 = 75^2$	342	634			$\leftarrow$
769	$311 = 43^2$	704	$527 = 36^2$	$371 = 348^2$	$506 = 132^2$	
	594	552	$413 = 201^2$	$486 = 264^2$	201	
	632	$298 = 303^2$	$607 = 379^2$	$749 = 127^2$	$5 = 92^2$	
797	$100 = 10^2$	659	$294 = 280^2$			
	262	$401 = 374^2$	$499 = 36^2$			
	434	550	$13 = 356^2$			
811	179	$797 = 191^2$	394	61	$324 = 18^2$	
	$221 = 365^2$	$99 = 76^2$	$276 = 198^2$	543	186	
	410	742	$150 = 31^2$	13	$506 = 155^2$	
827	63	$676 = 26^2$	506			
	$104 = 350^2$	$579 = 140^2$	$640 = 378^2$			
	659	415	517			$\leftarrow$
839	$442 = 74^2$	$504 = 231^2$	$377 = 165^2$	$56 = 77^2$	$571 = 352^2$	
	521	753	$354 = 110^2$	495	$653 = 279^2$	
	714	$437 = 353^2$	117	167	$586 = 138^2$	
853	376	$47 = 30^2$	674			
	$629 = 133^2$	616	461			$\leftarrow$
	700	206	$580 = 104^2$			
881	$98 = 294^2$	$360 = 191^2$	269	$862 = 157^2$	$466 = 164^2$	
	$792 = 304^2$	$44 = 366^2$	$32 = 168^2$	$420 = 299^2$	513	
	$871 = 426^2$	$493 = 56^2$	589	$128 = 336^2$	265	
883	120	$690 = 250^2$	75			
	270	685	292			$\leftarrow$
	$492 = 260^2$	$407 = 113^2$	$525 = 396^2$			
911	$123 = 299^2$	$533 = 38^2$	$171 = 376^2$	$152 = 218^2$	739	
	236	423	544	573	$636 = 150^2$	
	551	$882 = 52^2$	$205 = 277^2$	630	14	
937	$105 = 54^2$	$888 = 435^2$	$665 = 275^2$			
	$115 = 189^2$	$521 = 313^2$	$624 = 388^2$			
	$716 = 167^2$	$481 = 266^2$	594			
953	$232 = 152^2$	94	546			$\leftarrow$
	266	$29 = 364^2$	$259 = 94^2$			
	454	846	$157 = 63^2$			
967	$256 = 16^2$	$892 = 458^2$	668			
	745	$144 = 12^2$	107			
	932	914	$201 = 153^2$			

```
program checking_condition_C(input,output);
var q {the size ""q"" in the text}, qd2:integer;
    g:array[1..3] of integer;
    ex: boolean;
    u2:file of integer;
    t:integer;
    primes:array[0..1000] of boolean;
    root, square: array[0..1000] of integer;
    i:integer;

{================ tools ==========================================}

procedure Eratostene_sieve(n:integer);
var k,i:integer;

begin
 for i:=2 to n do primes[i]:= true;
 for i:=2 to trunc(sqrt(n)) do
     if primes[i] then  for k:=2 to n div i do  primes[k*i] := false;
end;

              {*****          ***          ******}

procedure tools(q:integer);
var k,i:integer;

begin
 qd2 := (q+1) div 2; {1/2 in Z_q}
 root[0] := 0; square[0] :=0;
 for i:=1 to q do  root[i] := -1;
 k:=0;
 for i:=1 to  qd2-1 do
   begin
     k:= ( k + 2*i - 1) mod q;
     root[k] := i;
     square[i]:= k; square[q-i] := k;
   end;
end;

              {*****          ***          ******}

procedure traces(k:integer;var t1,t2,t3 : integer);
var t,i :integer;  tr : array[1..3] of integer;
begin
  t:=1;
  for  i := 0 to k-1 do if (i*i*i + i*i - 2*i-1) mod k = 0
                              then begin tr[t] := i;
                                         t := t+1
                                   end;
  t1 := tr[1]; t2:=tr[2]; t3 := tr[3]

end;

              {*****          ***          ******}
```

```
procedure condition(tau,gamma:integer);
var c,r:integer;

begin
    c:=(square[tau]*square[gamma] - 4*(square[tau]+square[gamma]) + 12) mod q;
    r:=root[c];
    write(gamma, tau);
    if r<>-1 then begin  writeln(c,'=',r,'^2');
                         ex:=true;
                  end
              else writeln{('Condition (C) not satisfied')};
end;

{==================================================================}

begin
 open(u2,'power2.dat');
 rewrite(u2);
 Eratostene_sieve(1000);
  for q := 2 to  1000 do
  if primes[q] and ((q mod 7 = 1) or (q mod 7 = 6)) then
   begin
    tools(q);
    traces(q,g[1],g[2],g[3]);
    writeln(q);
    for i:=1 to 3 do
     begin
      ex := false;
      condition(0,g[i]);
      condition(1,g[i]);
      if (q mod 5 = 1) or (q mod 5 = 4) then
       begin
         t:=(qd2 * (1 + root[5])) mod q;
         condition(t,g[i]);
         t:=(qd2 * (1 - root[5])) mod q;
         condition(t,g[i]);
       end;
      writeln;
      if not(ex) then {save the trace and the order for a check with
                        higher power of the braid}

                      begin u2^:=q; put(u2);
                            u2^:=g[i]; put(u2);
                      end;
     end;  {of for i}
 end; {of mod7}
 close(u2);
end.
```

The program for the inspection of conditions of Theorem 3.2.19 is not essentially different from the previous program: the tools are the same. But the program results longer because we have to distinguish the two case $7 \mid q-1$ and $7 \mid q+1$. Since the previous program produces the file 'power2.dat' with the cases without positive answer for $\sigma = \sigma_2$ (those emphasized by an arrow in the TABLE), we may check only these ones.

The program for the systematic check on the candidates in $PSL(2,p)$, p prime, is similar to the following program, which does the computations for the case $PSL(2,27)$. It is simpler because we do computations modulus a prime and we check the braids

$$\sigma = \sigma_2^{u-1}, \quad u \geq 2.$$

So let us turn to the case $PSL(2,27)$. The concrete model used for computations in $\mathbb{F}_{27}$ is

$$Z_3[x]/(x^3 - x^2 + 1).$$

Each element is a polynom that we represent, in the program, as the linear matrix of the coefficients; also let us simply write the coefficients in sequence without commas

$$a_2 a_1 a_0 := a_2\, x^2 + a_1\, x + a_0.$$

The multiplication table of $\mathbb{F}_{27}$ is the following (obviously we need only half of the non-zero elements):

MULTIPLICATION TABLE of $\mathbb{F}_{27}$

·	001	010	011	012	100	101	102	110	111	112	120	121	122
001	001												
010	010	100											
011	011	110	121										
012	012	120	102	111									
100	100	102	202	002	122								
101	101	112	210	011	222	020							
102	102	122	221	020	022	121	220						
110	110	202	012	122	221	001	111	120					
111	111	212	020	101	021	102	210	200	011				
112	112	222	001	110	121	200	012	010	122	201			
120	120	002	122	212	020	110	200	022	112	202	021		
121	121	012	100	221	120	211	002	102	220	011	111	202	
122	122	022	111	200	220	012	101	212	001	120	201	020	112

The program that follows, established the necessary tools, generates all braids up to a fixed total number of half-twists and verifies the trace of the correspondent elements in $PSL(2,27)$.

```
program braids_for_PSL{2,27} (input,output);

const len=65535; {i.e. the maximum length allowed,
                  Reference Manual VAX Pascal 2.3.3}
      lem=65535; {the Pascal compiler requires in the heading
                  of a procedure identifiers, so any integer
                  has to be definied as a constant. We need
                  two names for the same because the compiler
                  does not admit the same constant identifier to be
                  repeated in one heading}

type parts = (Re,Im);
     elem = array[0..2] of integer;
     comp = array[Re..Im] of elem;
     matrix = array[1..2] of comp;

var one {one}, zero {zero}, g { trace}: elem;

    ro {primitive element}, ro_inv {its inverse} : elem;

    Lambda : comp;

    Nu : comp;

    square, root, inv : array[0..2,0..2,0..2] of elem;

    mu_sqr_inv {gamma square -4}, mu_sqr {its inverse}, beta : elem;

    data:varying[65535] of char; {the string}

    work,wa:varying[65535] of char;{the letters to which the string applies
                                    and their returned images}

    k,leng:integer;


{############### to write a variable of type elem or matrix ###############}

procedure wri(a:elem);
begin
  write(a[2]:1,a[1]:1,a[0]:1);
end;

procedure wri_m(A:matrix);
begin
  wri(A[1][Re]);write(' + i . ');wri(A[1][Im]); writeln;
  wri(A[2][Re]);write(' + i . ');wri(A[2][Im]); writeln;
end;
{##########################################################################}


{=============  the product in F(27) =====================================}


procedure p  (a,b : elem; var c:elem);
begin
 c[2] := (a[2]*b[0]+a[1]*b[1]+a[0]*b[2]+a[2]*b[1]+a[1]*b[2]+a[2]*b[2])mod 3;
 c[1] := (a[1]*b[0]+a[0]*b[1]-a[2]*b[2]) mod 3;
 c[0] := (a[0]*b[0]-a[2]*b[1]-a[1]*b[2]-a[2]*b[2]) mod 3;
end;

{=========================================================================}
```

```
{********************** the tools  *************************************}

procedure tools;
var a,c:elem;
    a2,a1,a0,k : integer;

procedure inverse(h:elem; var b:elem);
label 3;
var a,temp : elem;
    a2,a1,a0 : integer;
begin
  if (h[2] = 0) and (h[1] = 0) and (h[0] = 0) then
              begin b[0] := -1; b[1] := -1; b[2] := -1 end
     else
      for a2:=2 downto 0 do
        for a1:=2 downto 0 do
          for a0:=2 downto 0 do
           begin
             a[2]:=a2;a[1]:=a1;a[0]:=a0;
             p(h,a,temp);
             if (temp[2]=0) and (temp[1]=0) and (temp[0]=1) then
             begin b:=a;
                   goto 3
             end;
           end;
3 : end;


begin {procedure tools}

  one[2]:=0; one[1]:=0; one[0]:=1;
  zero[2]:=0;zero[1]:=0;zero[0]:=0;
  for a2:=2 downto 0  do
   for a1:=2 downto 0 do
    for a0:=2 downto 0 do
            for k:=2 downto 0 do root[a2,a1,a0][k]:=-1;

  for a2:=2 downto 0 do
   for a1:=2 downto 0 do
    for a0:=2 downto 0 do
     begin
      a[2]:=a2;a[1]:=a1;a[0]:=a0;
      p(a,a,c);
      for k :=2 downto 0 do square[a2,a1,a0][k]:=c[k];
      root[c[2],c[1],c[0]] := a;
      inverse(a,inv[a2,a1,a0]);
     end;

end;


procedure primit(var ro : elem);
label 2;
var a2,a1,a0,count:integer;
    d,y,x:elem;
begin
  for a2:=2 downto 0 do
```

```
    for a1:=2 downto 0 do
     for a0:=2 downto 0 do
      begin
       y[2]:=a2;y[1]:=a1;y[0]:=a0;
       count:=1; x:=y;
       if not((y[2]=0) and (y[1]=0) and (y[0]=0)) then
        begin
         while not((x[2]=0) and (x[1]=0) and (x[0]=1)) do
          begin p(y,x,d);
                count:=count+1;
                x:=d;
          end;
         if count=26 then begin ro:=y;   goto 2   end;
        end;
       end;
2 : end;
{&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&}

procedure trace(var g:elem);
label 1;
var a,b,c,d,h:elem;
    a2,a1,a0,k:integer;
begin
  d:=zero;
  for a2:=2 downto 0 do
   for a1:=2 downto 0 do
    for a0:=2 downto 0 do
     begin
      a[2]:=a2;a[1]:=a1;a[0]:=a0;
      h:=square[a2,a1,a0];
      for k:=2 downto 0 do b[k]:= (a[k] + one[k]) mod 3;
      p(h,b,d);
      for k:=2 downto 0 do c[k] := (d[k] + a[k] - one[k]) mod 3;
      if (c[2]=0) and (c[1]=0) and (c[0]=0) then
       begin
          g:= a;    goto 1
       end;
     end;
1 : end;


procedure Compute_Nu(var Nu:comp);
label 5;
var a,h,v,temp : elem;
    a2,a1,a0,k:integer;
begin
  v:=zero; {initialization}
  for a2:=2 downto 0 do
   for a1:=2 downto 0 do
    for a0:=2 downto 0 do
     if not((a2=0) and (a1=0) and (a0=0)) then
     begin
      a[2]:=a2;a[1]:=a1;a[0]:=a0;
      h:= square[a2,a1,a0];
      p(h,ro,v);
      for k:=2 downto 0 do v[k] := (v[k] + mu_sqr[k] + one[k]) mod 3;
      if (root[v[2],v[1],v[0]][2] <> -1) and
         (not((v[2]=0)and(v[1]=0)and(v[0]=0))) then
       begin Nu[Re] := root[v[2],v[1],v[0]];
             Nu[Im] := a;
             goto 5
       end;
```

```
      end;
5 : end;

procedure Compute_Lambda(var Lambda:comp);
var f,h:elem;
    k:integer;
begin
  f:=zero;
  h:=square[g[2],g[1],g[0]];
  h[0] := (h[0] - 1) mod 3;
  p(h,ro_inv,f);
  Lambda[Im]:= root[f[2],f[1],f[0]];
  for k:=2 downto 0 do Lambda[Re][k]:=(-g[k]) mod 3;

end;

{&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&}

procedure normalizes(var w:varying[len] of char);

{ the elements a, b, x of the group have order 2, so we want to get
  rid of the squares that may have appeared }

var i:integer;
    ok:boolean;
    s:varying[65535] of char;
begin
 for i:=1 to length(w)-1 do if w[i+1]=w[i] then ok:=false;
 while not(ok) do
  begin s:='';
   i:=0;
   repeat
     i:=i+1;
     if w[i]='t' then   s:=s+w[i]   else begin  { a, b and x have order 2}
         if w[i+1]<>w[i] then s:=s+w[i]
                              else i:=i+1; end;
   until i >= length(w)-1;
   if w[length(w)]<>w[length(w)-1] then s:=s+w[length(w)];
   ok:=true;
   for i:=1 to length(s)-1 do if (s[i]<>'t')and(s[i+1]=s[i]) then ok:=false;
    w:=s;
   end;
end;{normalizes}

procedure sigma_data(data:varying[len] of char;
                     var work:varying[lem] of char);

{ applies the braid given as the product of the generators denoted by 1 and
  2 in the variable 'data', to the element in 'work'.
  The result will be a sequence of a, b, x  and it is placed in 'work' again}

var s,h:varying[65535] of char;
    i,j:integer;
    ok:boolean;

begin
for i:=1 to length(data) do
begin  ok:=true;
 if data[i]='1' then
  begin
     h:='';
     for j:=1 to length(work) do
            begin if work[j]='a' then h:=h+'b';
```

```
                    if work[j]='b' then h:=h+'bab';
                    if work[j]='x' then h:=h+'x';
                end;
   work:=h;

  normalizes(work);

 end;


 if data[i]='2' then
  begin
     h:='';
     for j:=1 to length(work) do
             begin if work[j]='a' then h:=h+'a';
                   if work[j]='b' then h:=h+'x';
                   if work[j]='x' then h:=h+'xbx';
             end;
    work:=h;
    normalizes(work)
   end;

   end;
end;{sigma_data}
{***************************************************************************}

procedure Matrix_Prod(A,B:matrix;  var C:matrix);
var z,w,v,x:elem;
    k:integer;

begin
 p(A[1][Im],B[1][Im],z);
 p(A[2][Im],B[2][Im],w);
 for k:=2 downto 0 do v[k]:=(z[k]+w[k]) mod 3;
 p(v,ro,z);
 v:=z;
 p(A[1][Re],B[1][Re],z);
 p(A[2][Re],B[2][Re],w);
 for k:=2 downto 0 do v[k]:=(v[k]+z[k]-w[k]) mod 3;
 C[1][Re]  :=v;

 p(A[1][Im],B[1][Re],z);
 p(A[1][Re],B[1][Im],w);
 p(A[2][Im],B[2][Re],v);
 p(A[2][Re],B[2][Im],x);
 for k:=2 downto 0 do v[k]:=(-v[k]+x[k]+z[k]+w[k]) mod 3;
 C[1][Im]:=v;

 p(A[1][Im],B[2][Im],z);
 p(A[2][Im],B[1][Im],w);
 for k:=2 downto 0 do v[k]:=(z[k]-w[k]) mod 3;
 p(v,ro,z);
 v:=z;
 p(A[1][Re],B[2][Re],z);
 p(A[2][Re],B[1][Re],w);
 for k:=2 downto 0 do v[k]:=(v[k]+z[k]+w[k]) mod 3;
 C[2][Re]:=v;

 p(A[1][Re],B[2][Im],z);
 p(A[1][Im],B[2][Re],w);
 p(A[2][Im],B[1][Re],v);
 p(A[2][Re],B[1][Im],x);
 for k:=2 downto 0 do v[k]:=(v[k]-x[k]+z[k]+w[k]) mod 3;
 C[2][Im]:=v;

  end;
```

```
{%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%}
procedure powers;
label 6;
var a2,a1,a0,b2,b1,b0,k:integer;
    e_1,e_2,h,mde:elem;
    A, B, X, T,  M, Q, S : matrix;

begin {powers}


  for a2:=2 downto 0 do
  for a1:=2 downto 0 do
  for a0:=2 downto 0 do
  begin

   for b2:=2 downto 0 do
   for b1:=2 downto 0 do
   for b0:=2 downto 0 do
   begin

    e_1 := square[a2,a1,a0];
    e_2:=square[b2,b1,b0];
    p(e_2,ro,h);
    for k:=2 downto 0 do mde[k]:=(-h[k] + e_1[k]) mod 3;
    if (mde[2]=0) and (mde[1]=0) and (mde[0]=1) then
     begin
         A[1][Re]:=zero;
         A[1][Im]:=zero;
         A[2][Re][2]:=a2; A[2][Re][1]:=a1; A[2][Re][0]:=a0;
         A[2][Im][2]:=b2; A[2][Im][1]:=b1; A[2][Im][0]:=b0;

         T[1][Re]:=Lambda[Re];
         T[1][Im]:=Lambda[Im];
         T[2][Re]:=zero;
         T[2][Im]:=zero;

         X[1][Re]:=zero;
         X[1][Im]:=beta;
         X[2][Re]:=Nu[Re];
         X[2][Im]:=Nu[Im];

         Matrix_Prod(T, A, B);

   {the initialization for the product of the matrices }

          M[1][Re]:=one;
          M[1][Im]:=zero;
          M[2][Re]:=zero;
          M[2][Im]:=zero;

      for k:=1 to length(work) do
       begin
        if work[k]='a' then Q := A;

        if work[k]='b' then Q := B;

        if work[k]='x' then Q := X;

        Matrix_Prod(M, Q, S);

        M := S;
```

```
      end;
      if (M[1][Re][1]=0) and (M[1][Re][2]=0) then
       begin
          writeln('eureka');
          writeln('candidate : ',a2:1,a1:1,a0:1,' + ',b2:1,b1:1,b0:1,' i');
          writeln(data); writeln(work);
       end;
      end;
     end;
  end;

6 : end;{powers}

{*************************************************************************}

procedure make_data( s:integer; data:varying[len] of char);
var i:integer;
    d:varying[256] of char;
begin
  if s >= 1 then
  begin
     for i:=1 to 2 do
     if i=1 then begin  d:=data+'1'; make_data(s-1,d); end
                 else begin d:=data+'2';  make_data(s-1,d) end
   end
            else begin    d:='2'+data+'2';
                          wa:='a';
                          sigma_data(d,wa);
                          work:='b';
                          sigma_data(d,work);
                          work:=wa+work;
                          normalizes(work);
                          powers;
                 end
end; {make_data}


{************** the body of the program **********************************}

begin
  tools;
  trace(g);
  primit(ro);
  ro_inv := inv[ro[2],ro[1],ro[0]];
  for k:= 2 downto 0 do
                mu_sqr_inv[k] := (square[g[2],g[1],g[0]][k] - one[k]) mod 3;
  mu_sqr := inv[mu_sqr_inv[2],mu_sqr_inv[1],mu_sqr_inv[0]];
  p(mu_sqr,ro_inv,beta);
  beta:=root[beta[2],beta[1],beta[0]];
  write('the primitive root ');wri(ro);writeln;
  Compute_Lambda(Lambda);
  writeln('Lambda');
  wri(Lambda[Re]);write(' +  i .');wri(Lambda[Im]);writeln;
  Compute_Nu(Nu);
  writeln('Nu');
  wri(Nu[Re]);write(' +  i .');wri(Nu[Im]);writeln;
  readln(leng);
  for k:=1 to leng do
     begin
       data:='';
       make_data(k,data);
     end;
 end.

{*************************************************************************}
```

Chapter 6

Final remarks

6.1 Other Hurwitz groups

There exists also an infinite family of non-bounding Hurwitz actions by simple groups. These are the *Ree groups* $G_2^*(q)$ of order $q^3\,(q^3+1)\,(q-1)$, where $q = 3^p$, $p > 3$ prime, see [23, p.31,Prop.2.7]. There are three conjugacy classes of elements of order 3 in $G_2^*(q)$, denoted by T, T^{-1} and X in [23, proof of Prop.2.7]. In particular, T and T^{-1} are not conjugate, so do not lie in a subgroup $\mathbb{D}_3$, S_4 or A_5 of $G_2^*(q)$. Now in [23, Prop.2.7] Hurwitz actions

$$\varphi : (2,3,7) \longrightarrow G_2^*(q)$$

are constructed such that

$$\varphi(y) = T \quad \text{or} \quad T^{-1}.$$

If such an action bounds a compact 3-manifold, the axis of order 3 starting from the branch point of order 3 on $S^2(2,3,7)$ has to end in a point with local group A_4 by the above. But then from this point another axis of order 3 emanates associated again to the element T or T^{-1}, so continuing we get infinitely many points with local group A_4 which is impossible by compactness. Therefore all these Hurwitz actions do not bound. Moreover, the number of different Hurwitz actions of this type, for a fixed q, becomes arbitrarily large with q ([23, Prop.2.7]).

The orders of the Ree groups are quite large. Among the simple Hurwitz groups of low order, other than of type $PSL(2,q)$, there are the *Janko group* J_1 and the *Hall-Janko group* J_2 [6]. There are 7 resp. 5 different Hurwitz actions, the corresponding surjection extends from $(2,3,7)$ to $[2,3,7]$ ([5, §2], so at least one Hurwitz action of J_1 and also of J_2 bounds a hyperbolic 3-manifold.

Similar remarks apply to the *alternating groups* A_n: for all $n \geq 168$, there exist bounding Hurwitz actions of A_n because the corresponding surjections again extend from $(2,3,7)$ to $[2,3,7]$, see the comments in [4, Introduction] on H^*-groups. However, one would suspect that there are also many non-bounding Hurwitz actions of the groups A_n.

6.2 The group $C[4,3,5]^+$ does not map onto A_7

The group $C[4,3,5]^+$ maps onto infinitely many groups of $PSL(2,q)$ type, and $PSL(2,25)$ is the simple group with lowest order.

Among the simple groups that contain elements of order 4 and 5 and has order less than 7800, there is only the alternating group A_7 (see [8],[1],[9]).

But let us show that:

6.2.1 Proposition *The alternating group* A_7 *can not be a surjective image of* $C[4,3,5]^+$.

We read the product of permutations from left to right.

Proof

We have to find three elements T, X and A in A_7 such that

$$T^4 = X^2 = A^2 = (T\,X)^3 = (T\,A)^2 = (X\,A)^5 = 1.$$

The cycle decomposition of the even permutation T has to contain a cycle of length 4. Since the latter is odd and we are left with 3 elements, we assume that, up to conjugation, T equals the permutation $(1,2,3,4)(5,6)$.

Being of order 2 and even, the permutation X must decompose into 2 disjoint transpositions. The same applies to A.

Since moreover $(X\,T)^3 = 1 = (X\,A)^5$, the only possibilities are

$$X = (j,k)(5,i), \quad 1 \le j < k \le 4, \quad i = 6 \text{ or } 7.$$

$$A = (j,5)(k,d), \quad d \ne i.$$

Let us now compute the order of $T\,A$. Suppose first it is $d \in \{1,2,3,4\} \setminus \{j,k\}$: applying T and then A we obtain

$$\begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 5 & 6 & 7 & 1 \\ . & . & . & . & 6 & j & 7 \end{array}$$

The product $T\,A$ is $(.,5,6,j,.)(...)$ and so has order at least 3, because $j < 4$.

If d is equal to 7 we have

$$\begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 5 & 6 & 7 & 1 \\ . & . & . & . & 6 & j & k \end{array}$$

and so we conclude as above.

If d is equal to 6, i.e. $A = (j,5)(k,6)$, we have

$$\begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 5 & 6 & 7 & 1 \\ . & . & . & . & k & j & 7 \end{array}$$

Since $1 < k$ and $j < 4$, we may write

$$T(k-1) = k \quad \text{and} \quad T(j) = j+1.$$

Then there is a cycle of $T\,A$ that contains the sequence

$$.,k-1,6,j,\ ..$$

If $j \neq k-1$, the order of $T\,A$ is bigger than 2.
If $j = k-1$ then

$$T = (1,2,3,4)(5,6) = (.,j,k,s)(5,6), \quad s \neq 5.$$

Since the permutation A fixes s, a cycle of $T\,A$ contains the sequence

$$.,5,k,s,.$$

and also in this case $T\,A$ has order bigger than 2.

We have exhausted all the possibilities, so the Proposition is achieved.
∎

Appendix A

A.1 Congruences and primes

Throughout the work we have encountered congruences and systems of congruences. The well known *Chinese Remainder Theorem* for numbers assures that there are infinitely many integers that satisfy a system of congruence supposed they are taken modulo coprime natural numbers. The proof may be found in particular in [12, Thm.121], [22, §3.3,Thm.3.12].

A.1.1 Theorem *Let m_1, m_2, ... , m_s be $s \geq 1$ positive integers. Suppose m_i and m_j, $i, j = 1, ..., s$, $i \neq j$, are relatively prime. Then there exists an integer x such that*

$$x \equiv_{\mathrm{m}_1} k_1, \quad x \equiv_{\mathrm{m}_2} k_2, ..., \quad x \equiv_{\mathrm{m}_s} k_s.$$

Any other solution y of the system is congruent modulo $m_1 \cdot m_2 \cdot ... \cdot m_s$ to x. □

But do there exist prime numbers satisfying some given congruence?
A direct check on the correspondent sequence of primes, answers positively. And the Dirichlet's prime number theorem (e.g. [20, Ch.V, §6]) says us even more:

A.1.2 Theorem*(*on prime numbers of Dirichlet*)* *In any arithmetic progression*

$$a, a + m, a + 2m, a + 3m, ...$$

a, m natural and relatively prime numbers, there are infinitely many prime numbers.

A.2 Applying Čebotarev's theorem on prime numbers

Consider the maps 3.2.4

$$\varphi_{\gamma_i} : (2,3,7) \twoheadrightarrow PSL(2,q), \quad i = 1,2,3,$$

and the possible extensions

$$\phi_{\gamma_i} : [2,3,7] \twoheadrightarrow PSL(2,q).$$

If $p \equiv_4 1$ there exist 1 or 3 maps ϕ_{γ_i}, whereas if $p \equiv_4 3$ there exist 2 maps ϕ_{γ_i} or none. We have seen that all four possibilities really occur. Actually, as a consequence of Čebotarev's theorem on prime ideals in Galois extensions, each case occurs infinitely many times. To see how, we give, by the example, a quick introduction to the theorem and to the way to apply it. For proofs and detailed definitions about general theory we refer to [13, Ch.12],[24], [26] and [27].

Consider now the equation

$$P(x) = x^3 + x^2 - 2x - 1 = 0, \quad \text{over} \quad \mathbb{R}.$$

Its solutions g_1, g_2, g_3 belong to $\mathbb{R} \setminus \mathbb{Q}$ and we know that

$$g_2 = g_1^2 - 2 \quad \text{and} \quad g_3 = g_2^2 - 2.$$

Then the algebraic number field $\mathbb{Q}(g_1, g_2, g_3)$ is just $\mathbb{Q}(g)$, $g := g_1$ and $\{1, g, g^2\}$ is a basis over $\mathbb{Q}$. The extension is Galois and of degree $d = 3$. The Galois group is the cyclic group of order 3 generated by the automorphism π defined by

$$\pi(g) := g^2 - 2.$$

(Indeed the order of G is the degree of the extension and the image of g is itself a solution of $P(x) = 0$. So there are no other choices up to isomorphism. In this case we are easily forced by the general theory.)

To state the Čebotarev's theorem we need some more definitions.
The elements $z \in \mathbb{Q}(g)$ such that

$$z^s + a_1 z^{s-1} + \ldots + a_{s-1} + a_s = 0, \text{ for some } s \in \mathbb{N}, \ a_i \in \mathrm{Z}$$

are called *algebraic integers* and form a subring D, that is preserved by the elements of the Galois group G. Since the minimal polynomial $P(x)$ of g belongs to $\mathrm{Z}[x]$, the set $\{1, g, g^2\}$ is a basis also of D. The trace and the norm of elements in $\mathbb{Q}(g)$ may be computed by the characterizations in terms of G

$$trace(z) = z + \pi(z) + \pi^2(z) \text{ and } norm(z) = z \cdot \pi(z) \cdot \pi^2(z).$$

Then the discriminant of D (and of $\mathbb{Q}(g)$) is

$$\Delta(1, g, g^2) := det(trace(g^i g^j))_{i,j=0,2} = (-1)^{d(d-1)/2} norm(P'(g)) = 49.$$

Let's outline the computations with the latter formula. Keep in mind that $g^3 = 1 + 2g - g^2$ and $g^4 = g + 2g^2 - g^3 = -1 - g + 3g^2$.
We have

$$\pi(g) = g^2 - 2; \quad \pi(g^2) = (\pi(g))^2 = g^4 - 4g^2 + 4 = 3 - g - g^2$$
$$\pi^2(g) = \pi(g^2 - 2) = 3 - g - g^2 - 2 = 1 - g - g^2$$
$$\pi^2(g^2) = \pi(3 - g - g^2) = 3 - g^2 - 2 - 3 + g + g^2 = 2 + g.$$

so

$$\pi(P'(g)) = \pi(3g^2 + 2g - 2) = 3 - 3g - g^2$$
$$\pi^2(P'(g)) = 6 + g - 2g^2.$$

Finally a careful computation shows that

$$norm(P'(g)) = P'(g) \cdot \pi(P'(g)) \cdot \pi^2(P'(g)) = -49.$$

The discriminant is always an integer.

In D every ideal is the product of prime ideals in a unique way. In particular for any prime p in $\mathbf{Z}$ there exist $s\,(\geq 1)$ prime ideals $\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_s$ of D such that

- the ideal generated by p in D factorizes as $(p) = \mathcal{P}_1^e \mathcal{P}_2^e ... \mathcal{P}_s^e$, $e \geq 1$;
- the finite fields $D/\mathcal{P}_i$, $i = 1, ..., s$, have p^f, $f \geq 1$, elements and are Galois extensions of their (commun) prime field $\mathbf{Z}_p$;
- the three numbers e, f and s are related by the formula

$$e\,f\,s = d = 3.$$

The exponent e is greater than 1 if and only if p divides the discriminant, in the present example if and only if $p = 7$. Always the primes that divide the discriminant are finitely many. Moreover when $e = 1$ the Galois group G_i of the finite field $D/\mathcal{P}_i$ is isomorphic to the group of the automorphisms of G that preserve the ideal $\mathcal{P}_i$. But G_i is cyclic of order f: its canonical generator is the *Frobenius automorphism* defined by

$$h: \; z \mapsto z^p, \quad \text{for any } \; z \in D/\mathcal{P}_i.$$

Then h coincides with some automorphism $\pi \in G$.

A.2.1 Theorem (restricted version of Čebotarev's density theorem)

Let L be an algebraic number field, D its subring of algebraic integers and π an element of the Galois group. The subset of primes $p \in \mathbf{Z}$, non dividing the discriminant, such that the Frobenius automorphism of $D/\mathcal{P}_i$, for a factor $\mathcal{P}_i$ of (p) in D, coincides with π is infinite and depends only on the conjugacy class of π in G.

As the identity belongs to G the following is immediate:

A.2.2 Corollary *There are infinitely many prime numbers $p \in \mathbb{Z}$, non dividing the discriminant, such that*

$$D/\mathcal{P}_i \equiv \mathbb{Z}_p, \quad \textit{where } \mathcal{P}_i \textit{ is a factor of } (p) \quad \textit{in } D.$$

■

In specific example, if $p \neq 7$ the possibilities are $G(D/\mathcal{P}_i) \equiv \mathbb{I}$, when $f = 1$, $s = 3$, or $G(D/\mathcal{P}_i) \cong G$ when $f = 3$, $s = 1$. There are no other possibilities because $f\,s = 3$. By the Čebotarev's theorem both occur for infinitely many primes. Since $D/\mathcal{P}_i = \mathbb{Z}_p(g)$, we are in particular interested in the case $f = 1$ because it implies that $\mathbb{Z}_p(g) \equiv \mathbb{Z}_p$ and so that g belongs to $\mathbb{Z}_p$.

Now $c_i = C(0, \pm g_i)$, $i = 1, 2, 3$, belong to $\mathbb{Q}(g)$, but not so their square roots. Anyway we may repeat the process and consider the Galois extensions $\mathbb{Q}(g, c_i)$, $i = 1, 2, 3$, $\mathbb{Q}(g, c_i, c_j)$, $i, j = 1, 2, 3$, $i \neq j$, $\mathbb{Q}(g, c_1, c_2, c_3)$ and reapply Corollary A.2.2.

For any prime $p \in \mathbb{Z}$ such that $D(g, c_1, c_2, c_3)/\mathcal{P}_i = \mathbb{Z}_p(g, c_1, c_2, c_3) \equiv \mathbb{Z}_p$ we have obviously that $\mathbb{Z}_p(g, c_i, c_j) \equiv \mathbb{Z}_p$ and $\mathbb{Z}_p(g, c_i) \equiv \mathbb{Z}_p$. But the converse implications are not true. Indeed there are infinitely many primes such that $\mathbb{Z}_p(g, c_i, c_j) \supset \mathbb{Z}_p(g, c_i)$: just apply Čebotarev's theorem to the Galois extension $\mathbb{Q}(g, c_i, c_j)$ of $\mathbb{Q}(g, c_i)$. Since $c_1^2 c_2^2 c_3^2 = -1 \cdot 8^2$, we have that $\mathbb{Z}_p(g, c_i, c_j) \equiv \mathbb{Z}_p$ implies $\mathbb{Z}_p(g, c_1, c_2, c_3) \equiv \mathbb{Z}_p$ if and only if $p \equiv_4 1$.

The same result is true for $C(\pm 1, \pm g_i)$ and $C(\tau, \pm g_i)$, $\tau = \tau(5)$. In the last case we start from the Galois extension $\mathbb{Q}(\sqrt{5})$.

Bibliography

[1] M. Aschbacher. *Finite groups.* Cambridge University Press, Cambridge, 1986.

[2] A.F. Beardon. *The geometry of discrete groups.* Springer-Verlag, New York, 1983.

[3] R.P. Bryant and D. Singerman. Foundations of the theory of maps on surfaces with boundary. *Quart. J. Math. Oxford (2)*, 36: 17–41, 1985.

[4] M. Conder. Groups of minimal genus including C_2 extensions of $PSL(2,q)$ for certain q. *Quart. J. Math. Oxford (2)*, 38: 449–460, 1987.

[5] M. Conder. Maximal automorphism groups of symmetric Riemann surfaces with small genus. *J. Algebra*, 114: 16–28, 1988.

[6] M. Conder. Hurwitz groups: a brief survey. *Bull. Amer. Math. Soc. (New series)*, 23(2): 359–370, 1990.

[7] H.S. Coxeter and W.O. Moser. *Generators and Relations for Discrete Groups.* Springer-Verlag, Berlin, 1957.

[8] L.E. Dickson. *Linear groups with an exposition of the Galois field theory.* Dover Publications, New York, 1958.

[9] D. Gorenstein. *Finite simple groups.* Plenum Press, New York, 1983.

[10] H. Glover and D. Sjerve. Representing $PSl_2(q)$ on a Riemann Surface of least genus. *L'Ens. Math.*, 31: 305–325, 1985.

[11] H. Glover and D. Sjerve. The genus of $PSl_2(q)$. *J. reine angew. Math.*, 380: 59–86, 1987.

[12] G.H. Hardy and E.M. Wright. *An introduction to the theory of numbers.* Clarendon Press, Oxford, 1979.

[13] K. Ireland and M. Rosen. *A classical introduction to modern number theory.* Springer Verlag, New York, 1982.

[14] R. Lidl and H. Niederreiter. *Finite fields* in *Encyclopedia of Mathematics and its applications, vol. 20.* Addison-Wesley, Reading,Mass.,1983.

[15] A.M. Macbeath. Generators of the linear fractional groups. *Proc. Symp. Pure Math.*, NUMBER THEORY, vol. XII:14–32, 1968.

[16] D. Mc Cullough, A. Miller and B. Zimmermann. Group actions on handlebodies. *Proc. London Math. Soc.*, 59: 373–416, 1989.

[17] J.M. Montesinos-Amilibia. *Classical tessellations and three-manifolds.* Springer Verlag, Berlin, 1987.

[18] Q. Mushtaq. *Coset diagrams for the modular group.* D.Phil. thesis,University of Oxford, 1983.

[19] Q. Mushtaq. Coset diagrams for the Hurwitz groups. *Comm. in Algebra*, 18(11):3857–3888, 1990.

[20] J. Neukirch. *Class field theory.* Springer Verlag, Berlin, 1986.

[21] D. Rolfsen. *Knot theory*, Math. Lecture Series. Publish or Perish Inc., Houston, Texas, 1976.

[22] K.H. Rosen. *Elementary number theory and its applications.* Addison-Wesley Publishing Company, 1988.

[23] C.H. Sah. Groups related to compact Riemann surfaces. *Acta Math.*, 123: 13–42, 1969.

[24] P. Samuel. *Algebraic theory of numbers.* Hermann, Paris, 1970. *translated by A.J. Silberger from "Théorie algébrique the nombres".* Hermann, Paris, 1967.

[25] D. Singerman. Automorphisms of compact non-orientable Riemann surfaces. *Glasgow Math. J.*, 12: 50–59, 1971.

[26] I. Stewart. *Galois theory*, (math. series). Chapman and Hall, London, 1973.

[27] I. Stewart and D.Tall. *Algebraic number theory, 2nd ed*, (math. series). Chapman and Hall, London, 1987.

[28] M. Suzuki. *Group theory.* Vol.I, Springer Verlag, New York, 1982.

[29] W.P. Thurston. *The geometry and topology of 3-manifolds.* Princeton University Lecture Notes, 1978-79.

[30] W.P. Thurston. *The geometry and topology of 3-manifolds.* draft version, 1991.

[31] B. Zimmermann. Generators and relations for discontinuous groups. in A. Barlotti et al. *Generators and relations in groups and geometries*, Kluver Academic Publisher, Netherland, 1991.

[32] B. Zimmermann. Finite group actions on handlebodies and equivariant Heegaard genus for 3-manifolds. *Topology Appl.*,43: 263–274, 1992.

[33] B. Zimmermann. Hurwitz groups and finite group actions on hyperbolic 3-manifolds. preprint: Università di Trieste.