On the Borromean Orbifolds: Geometry and Arithmetic

Hugh M. Hilden, María Teresa Lozano**
*José María Montesinos-Amilibia**

Introduction

This paper is a continuation of earlier work by the authors on universal knots, links, and groups. (**[HLM1]**, **[HLM2]**, **[HLMW]**). A knot or link in S^3 is ***universal*** if every closed oriented 3-manifold occurs as a branched covering of S^3 with branch set the knot or link. A finitely generated group of hyperbolic isometries, or Kleinian group, U, is called ***universal*** if the orbit space of the action of U on $\mathbb{H}^3$ is homeomorphic to S^3 and if every closed oriented 3-manifold M^3 occurs as the orbit space of a finite index subgroup $G(M^3)$ of U.

The concept of universal group grew naturally out of the concept of universal link. If the image of the axes of rotation of U is a knot or link k in S^3, the natural map $\mathbb{H}^3/G(M^3) \to \mathbb{H}^3/U = S^3$ is a branched covering with branch set k, so the knot or link k is universal. The group U acting on $\mathbb{H}^3$ endows its quotient S^3 with the structure of hyperbolic orbifold. The singular set is the knot or link k.

In **[HMLW]**, it was shown that universal groups existed and in **[HML2]** we studied in detail a particularly simple example of a universal group, the universal group of the Borromean rings (see Figure 1). (That is, the link k is the Borromean rings.)

Walter Neumann and Alan Reid pointed out to the authors that the universal group of the Borromean rings, which we studied in **[HLM2]**, (the group $B(4,4,4)$ in notation we shall shortly introduce), is in fact an 'arithmetic' group, as follows from results of Vinberg (**[Vi]**). Thus this group has 'more structure' (**[HLM2]**).

It follows directly from this observation, and the results of **[HLMW]**, that every closed oriented 3-manifold has the structure of an 'arithmetic orbifold'. So an immediate question arises as to how rare a flower is an arithmetic orbifold in the garden of hyperbolic orbifolds.

Evidence that arithmetic orbifolds are rare in dimension two was obtained by Takeuchi (**[T3]**) who produced the complete, but finite list of arithmetic groups among the infinitude of triangle groups. In fact he showed that for fixed signature σ there are only finitely many conjugacy classes of arithmetic Fuchsian groups of signature σ (**[T4]**).

Further evidence can be found in Reid's thesis (**[R]**) where arithmetic Kleinian groups and their Fuchsian subgroups are studied. Also, Borel (**[B]**) showed that the set of volumes of arithmetic hyperbolic 3-orbifolds is a discrete subset of $\mathbb{R}$.

* This research was supported by grants PB85-0336 and PB89-0105. The first author expresses his appreciation to the DGICYT for financial support while he was in Spain.

In this paper we produce a three parameter family $\widehat{B}(m,n,p)$, $3 \leqq m,n,p \leqq \infty$, of hyperbolic orbifolds with singular set the Borromean rings. (The 'angle' at the three components is $2\pi/m$, $2\pi/n$, $2\pi/p$.) In this family exactly eleven members are arithmetic: $(3,3,3)$, $(4,4,4)$, $(6,6,6)$, $(3,4,4)$, $(3,6,6)$, (∞,∞,∞), $(3,\infty,\infty)$, $(4,\infty,\infty)$, $(3,3,\infty)$, $(3,4,\infty)$, $(4,4,\infty)$.

Analogously, in another paper, **[HLM3]**, which relies on **[HKM]**, we classify the arithmetic figure eight orbifolds. (There are exactly six.)

The organization of the paper is as follows:

The first section deals with hyperbolic geometry preliminaries. The relationship between the Beltrami-Klein model of $\mathbb{H}^3$ and the Poincaré model of $\mathbb{H}^3$ is made via the 'intermediate' model used in **[HKM]** which facilitates the computation of isometries.

In the second section the basic definition of arithmetic groups and arithmetically definable groups are explained. Certain results (widely dispersed in the literature) are collected and set down.

In the third section we construct the orbifolds $\widehat{B}(m,n,p)$ in the Klein model of hyperbolic 3-space, and their Kleinian groups $B_{m,n,p} \leqq \mathrm{SL}(2,\mathbb{C})$.

In the fourth section, using the characterization of Vinberg (**[Vi]**) of arithmetic subgroups of $\mathbf{O}(F_o,\mathbb{R})$ generated by reflections we obtain the list of arithmetic triples.

Finally, in the last section, we compute the quaternion algebras for the eleven arithmetic cases of Section 4, and we compute the orders in the quaternion algebras that determine their arithmeticity. We also compile some arithmetic information about the field $\mathbb{Q}(\alpha)$, where $\alpha^4+\alpha^2-1=0$, and about the quaternion algebra $\left(\frac{-1,-1}{\mathbb{Q}(\alpha)}\right)$, the relevant field and algebra for the universal arithmetic orbifold $\widehat{B}(4,4,4)$. In the appendix we use Reid's criterion to show non-arithmeticity in the cases $m,n,p \notin \{3,4,6,\infty\}$.

§1. Preliminaries on hyperbolic geometry

1. The points of hyperbolic 3-space $\mathbb{H}^3$ in the standard Beltrami-Klein model are the interior points of the unit ball centered at the origin in $\mathbb{R}^3$. In homogeneous coordinates, $(x:y:z:t)$, for $\mathbb{R}P^3$, the equation of S^2 is

$$x^2+y^2+z^2-t^2=0. \tag{1.1}$$

2. The connection between this model of $\mathbb{H}^3$, and the Poincaré half space model is made via the stereographic projection of S^2 on its equatorial plane $\mathbb{C}P^1$ from the point $(0:0:1:1)$.

The connection between the two models is clarified if we use a model which we shall call the ***intermediate model***. (Compare **[F]** and **[HKM]**.) We choose new coordinates for $\mathbb{C}P^3$:

$$\theta_1 = x+iy, \quad \theta_2 = z-t, \quad \theta_3 = z+t, \quad \theta_4 = -x+iy. \tag{1.2}$$

The equation of the sphere S^2 becomes

$$\det\begin{vmatrix}\theta_1 & \theta_2\\ \theta_3 & \theta_4\end{vmatrix} = 0.$$

The intermediate model of $\mathbb{H}^3$ consists of the points of $\mathbb{R}P^3$ interior to the sphere

$$\{(\theta_1:\theta_2:\theta_3:\theta_4) \mid \theta_1\theta_4-\theta_2\theta_3=0, \quad \theta_2=\bar\theta_2, \quad \theta_3=\bar\theta_3, \quad \theta_1=-\bar\theta_4\}.$$

The points of $\mathbb{H}^3$, which we shall represent by matrices, satisfy

$$\det\begin{vmatrix}\theta_1 & \theta_2\\ \theta_3 & \theta_4\end{vmatrix} > 0; \quad \theta_2=\bar\theta_2, \quad \theta_3=\bar\theta_3, \quad \theta_1=-\bar\theta_4.$$

We call this model intermediate because the point

$$\begin{vmatrix}\theta_1 & \theta_2\\ \theta_3 & \theta_4\end{vmatrix}; \quad \theta_2=\bar\theta_2, \quad \theta_3=\bar\theta_3, \quad \theta_1=-\bar\theta_4,$$

also represents a circle in $\mathbb{C}P^1$. In fact the equation

$$z = \frac{\theta_1\bar z+\theta_2}{\theta_3\bar z+\theta_4} \tag{1.3}$$

is the equation of a circle whose squared radius is $\det\begin{vmatrix}\theta_1 & \theta_2\\ \theta_3 & \theta_4\end{vmatrix}\Big/\theta_3^2$. Thus the circles of radius zero in $\mathbb{C}P^1$ (the 'points' at $\mathbb{C}P^1$) are represented by the points $\begin{bmatrix}\theta_1 & \theta_2\\ \theta_3 & \theta_4\end{bmatrix}$ with determinant zero.

The function which assigns to a point $z \in \mathbb{C}P^1$ the circle of radius zero and center z, represented by the point $\begin{bmatrix}\theta_1 & \theta_2\\ \theta_3 & \theta_4\end{bmatrix}$ of the intermediate model, is the stereographic projection of $\mathbb{C}P^1$ on S^2 from the south pole of S^2. Moreover, we know that the stereographic projection assigns to a circle of radius different from zero (it can be real or purely imaginary) a circle of S^2. Now if the circle taken in $\mathbb{C}P^1$ is that of equation (1.3) its stereographic image is a circle of S^2 whose pole is $\begin{bmatrix}\theta_1 & \theta_2\\ \theta_3 & \theta_4\end{bmatrix}$.

3. An immediate corollary to this observation is a convenient procedure for finding the equation in the Poincaré model of the reflection in a plane P in the Beltrami-Klein model. One proceeds as follows:

(i) Calculate the point $P^\perp$, the pole of P with respect to S^2, in coordinates $\begin{pmatrix}\theta_1 & \theta_2\\ \theta_3 & \theta_4\end{pmatrix}$ of the intermediate model using the change of coordinates (1.2);

(ii) The equation of reflection in P in the Poincaré model is

$$z' = \frac{\theta_1\bar z+\theta_2}{\theta_3\bar z+\theta_4}.$$

4. In the following section we mention, in passing, another representation of $\mathbb{H}^3$, known as the hyperboloid model. This is one of the leaves of the hyperboloid determined by the equation $f = -1$, where f is a quadratic form on $\mathbb{R}^4$ of signature $(3,1)$. This defines a structure of Minkowski space in $\mathbb{R}^4$. The metric induced in one of the leaves of $f = -1$ is Riemannian and defines the hyperboloid model of $\mathbb{H}^3$.

Letting F represent the matrix of f, we denote by $O(F,\mathbb{R})$ the group of matrices, M, in $\mathrm{GL}(4,\mathbb{R})$ such that $M^TFM = F$. The index two subgroup leaving invariant each leaf of the hyperboloid $f = -1$ is the group $\mathrm{Iso}\,\mathbb{H}^3$ of isometries of $\mathbb{H}^3$.

§2. Arithmetically Defined Groups: Preliminaries ([R], [R1])

1. Motivation and history. Let G be a locally compact topological group with a fixed left invariant Haar measure. A subgroup $\Gamma \leqq G$ is a ***lattice*** if it is discrete and if the homogeneous space G/Γ has finite measure. We say Γ has ***finite co-volume***. The group Γ is ***co-compact*** if G/Γ is compact.

As an example consider $G = \mathrm{SL}(n,\mathbb{R})$ and $\Gamma = \mathrm{SL}(n,\mathbf{Z})$. The group G is a semi-simple Lie group and Γ is a lattice in G. (It is true, but not at all obvious, that Γ has finite co-volume.) The lattice Γ is ***non co-compact***.

As a second example let $G = \mathbb{R}^n$ and $\Gamma_0 = \mathbb{Z}^n$. In this example every lattice Γ in G is 'arithmetic', that is there is an automorphism $\pi : \mathbb{R}^n \to \mathbb{R}^n$ such that $\pi(\Gamma) = \mathbb{Z}^n$.

This second example serves as motivation to study a two part problem. Given G:

1. Define when a lattice $\Gamma \leqq G$ is 'arithmetic'.
2. Determine whether every lattice is 'arithmetic'.

For the first part of the problem we shall need to apply 'arithmetic methods' to do the study of G. It turns out that the most convenient class of groups to work with is the class of *connected semi-simple Lie groups with trivial center*, because a group G of this type is always a *linear algebraic group* defined over $\mathbb{Q}$.

Of course, the two Lie groups in our examples have non trivial centers, but the study of the general case reduces to the study of the trivial center case via Lie theory.

For these groups there is a general construction of arithmetic lattices due to Borel and Harish-Chandra that we shall describe later. (See **[Z**, pp. 1–5] or **[BH]**.)

The second part of the problem has the following solution. If the $\mathbb{R}$-rank of G is greater than one (the dimension of a maximal torus is greater than one) every lattice is arithmetic. This is a theorem of Margulis.

But the case where the $\mathbb{R}$-rank of G is one, the case that we are interested in, is different. In fact if G is $\mathrm{Iso}^+\,\mathbb{H}^3$, the group of direct isometries of hyperbolic three space, non arithmetic lattices exist. (Makarov, Vinberg.)

Vinberg considered $\mathrm{Iso}^+\,\mathbb{H}^3$ as a *real* simple connected Lie group with trivial center. He adapted the Borel and Harish-Chandra definition of arithmeticity of a lattice and characterized the lattices generated by reflections. He obtained non arithmetic lattices. (His arithmeticity criteria is given in terms of the Gram matrix of a polytope that is the fundamental domain of Γ.)

But Vinberg did not notice that $\mathrm{Iso}^+\,\mathbb{H}^3$ is also a complex Lie group (isomorphic to $\mathrm{PSL}(2,\mathbb{C})$) (see the appendix to the translation of **[Vi]**). Serre observed that if $\mathrm{Iso}^+\,\mathbb{H}^3$ is considered as a complex Lie group there are other possibilities for constructing arithmetic lattices via the Borel and Harish-Chandra method. In fact there are more arithmetically definable subgroups than those considered by Vinberg. This follows simply from the fact that $\mathbb{C}$ contains more algebraic number fields than $\mathbb{R}$.

Therefore for the moment we shall distinguish, following Vinberg, between ***real-arithmetic*** and ***complex-arithmetic*** groups.

The study of real-arithmetic groups probably began with Fricke and Klein, the complex-arithmetic groups with Bianchi. A characterization of the arithmetic subgroups of $\mathrm{Iso}^+\,H^2$ was given by Takeuchi **[T2]**. This characterization was generalized to $\mathrm{Iso}^+\,\mathbb{H}^3$ by Reid in his thesis **[R]**.

Our interest in these groups arises from the study of a particular subgroup of $\mathrm{Iso}^+\,\mathbb{H}^3$, the group $B(4,4,4)$. (The notation will be explained later.) This group has the following *universal* property:

For every closed orientable three manifold M^3 there exists $\Gamma(M^3)$ of finite index $\leqq B(4,4,4)$ such that $\mathbb{H}^3/\Gamma(M^3) = M^3$.

It turns out that $B(4,4,4)$ is 'arithmetic'. We suspect that this fact will have interesting consequences in the theory of three manifolds. Therefore we shall study the arithmeticity of $B(4,4,4)$, as well as that of a family of groups $B(m,n,p)$ naturally associated with $B(4,4,4)$, in a very concrete way.

2. Linear algebraic groups; arithmetic subgroups.

Definition. A ***linear algebraic group defined over*** k, where k is a finite extension of $\mathbb{Q}$, is a subgroup G of $\mathrm{GL}(n,\mathbb{C})$ defined as follows.

$$G = \{(a_{ij}) \in \mathrm{GL}(n,\mathbb{C}) \mid p(a_{ij}, \det(a_{ij})^{-1}) = 0 \text{ for every } p \text{ in } I\} \tag{1}$$

Here I is an ideal in the polynomial ring $k[X_{11},\cdots,X_{nn},Y]$. Note that I is finitely generated so that it suffices to consider a finite set of polynomials in (1). Note also that the entries of a linear algebraic group defined over k need not lie in k. $\mathrm{SL}(n,\mathbb{C})$ is a linear algebraic group defined over $\mathbb{Q}$.

The significance of this definition is that G is at the same time a group and an affine subvariety of $\mathrm{GL}(n,\mathbb{C})$ defined over k. In effect we identify $\mathrm{GL}(n,\mathbb{C})$ with the affine subvariety V of $\mathbb{C}^{n^2+1}$ given by the equation

$$\det(X_{ij})Y = 1.$$

Here the matrix (a_{ij}) is identified with the point $(a_{11},\cdots,a_{nn},\det(a_{ij})^{-1})$. The coordinate ring of the variety V is

$$\mathbb{C}[a_{11},\cdots,a_{nn},\det(a_{ij})^{-1}].$$

For every ideal $I \subset k[a_{11},\cdots,a_{nn},\det(a_{ij})^{-1}]$ we obtain an affine subvariety of $\mathrm{GL}(n,\mathbb{C})$ defined over k (see **[Re]**). This affine subvariety is sometimes a group.

If B is a subring of $\mathbb{C}$ we define

$$\mathrm{GL}(n,B) = \{(a_{ij}) \in \mathrm{GL}(n,\mathbb{C}) \mid a_{ij} \in B, \det(a_{ij}) \text{ is a unit of } B\}.$$

We shall denote $G \cap \mathrm{GL}(n,B)$ by G_B. Note that $G_{\mathbb{R}}$ and $G_{\mathbb{C}}$ make sense because a field is a ring and that $G_{\mathbb{C}} = G$.

For every embedding σ of the algebraic number field k in $\mathbb{C}$ we define the linear algebraic group G^σ as follows:

$$G^\sigma = \{(a_{ij}) \in \mathrm{GL}(n,\mathbb{C}) \mid p^\sigma(a_{ij}, \det(a_{ij})^{-1}) = 0 \text{ for every } p \in I\}.$$

Here p^σ is obtained from p by applying σ to the coefficients of p.

Definition. Let G be a linear algebraic group defined over k. A subgroup $\Gamma \leqq G$ is ***arithmetic*** if Γ is commensurable with $G_{O(k)}$ ($\Gamma \cap G_{O(k)}$ has finite index in both Γ and $G_{O(k)}$). Here $O(k)$ is the ring of algebraic integers of k.

In the definition we do not insist that Γ is a lattice. Under certain conditions it can be proven that an arithmetic subgroup of a linear algebraic group G defined over k is a lattice.

Theorem 2.1 (Borel and Harish-Chandra). *Let G be a semi-simple Lie group which is a linear algebraic group defined over k. Let Γ be an arithmetic subgroup of G. Then Γ is finitely generated and moreover*

1. *Γ is a lattice in $G_\mathbb{R}$ if and only if $\Gamma \leqq G_\mathbb{R}$ and*
   (i) *k is totally real;*
   (ii) *$G^\sigma_\mathbb{R}$ is compact for every $\sigma : k \to \mathbb{R}$ such that $\sigma \neq$ identity. (In this case we say $G_\mathbb{R}$ is **admissible**.)*
2. *Γ is a lattice in G if and only if $\Gamma \leqq G$ and*
   (i) *k has exactly one complex place (one pair of complex conjugate embeddings);*
   (ii) *$G^\sigma_\mathbb{R}$ is compact for every $\sigma : k \to \mathbb{R}$ such that $\sigma \neq$ id or complex conjugation. (In this case we say G is **admissible**.)* □

Example 1. Let F be a symmetric matrix with entries in $k \subset \mathbb{R}$ and equivalent over $\mathbb{R}$ to $(1,1,1,-1)$. Define

$$\mathrm{SO}(F,\mathbb{C}) = \{(a_{ij}) \in \mathrm{GL}(n,\mathbb{C}) \mid (a_{ij})^t F(a_{ij}) = F, \det(a_{ij}) = 1\}.$$

Then $\mathrm{SO}(F,\mathbb{C})$ is a Lie group with center equal to $\pm I$. The group $\mathrm{Ad}\,\mathrm{SO}(F,\mathbb{C})$ of inner automorphisms of $\mathrm{SO}(F,\mathbb{C})$ is a connected simple Lie group with trivial center. It is also a linear algebraic group defined over k, although it is not easy to see why. It can be shown that every automorphism of $\mathrm{SO}(F,\mathbb{C})$ is inner and that a linear map from $\mathbb{C}^{n^2}$ to itself leaves $\mathrm{SO}(F,\mathbb{C})$ invariant and restricts to an automorphism of $\mathrm{SO}(F,\mathbb{C})$ if and only if a finite number of polynomial conditions are satisfied.

The group $\mathrm{Ad}\,\mathrm{SO}(F_0,\mathbb{C})_\mathbb{R} = \mathrm{Ad}\,\mathrm{SO}(F_0,\mathbb{R})$ is identified with $\mathrm{Iso}^+\,\mathbb{H}^3$ where F_0 is the diagonal matrix $(1,1,1,-1)$. This is a linear algebraic group defined over $\mathbb{Q}$. It is clear that $\mathrm{Ad}\,\mathrm{SO}(F,\mathbb{R})$ is isomorphic to $\mathrm{Ad}\,\mathrm{SO}(F_0,\mathbb{R}) = \mathrm{Iso}^+\,\mathbb{H}^3$. The isomorphism is of a special type that we shall now consider.

Definition. A homomorphism $f : H \to G$ between two linear algebraic groups defined over k is said to be defined over ℓ, where ℓ is a finite extension of k, if in the expression

$$f(h_{k\ell}) = (g_{ij})$$

the entry g_{ij} is expressable as a polynomial function of the variables $h_{11}, \cdots, h_{nn}$, $(\det(h_{ij}))^{-1}$ with coefficients in ℓ.

If f is an isomorphism and both f and f^{-1} are defined over ℓ for some finite extension ℓ then H is said to be a ***k-form of*** G.

Example 1 (continued). Since F is $\mathbb{R}$-equivalent to F_0, there exists T such that $T^t F_0 T = F$. The entries of T lie in a finite extension ℓ of k. It follows that $\mathrm{Ad}\,\mathrm{SO}(F,\mathbb{C})$ is a k-form of $\mathrm{Ad}\,\mathrm{SO}(F_0,\mathbb{C})$ induced by

$$f : \mathrm{SO}(F,\mathbb{C}) \to \mathrm{SO}(F_0,\mathbb{C}),$$
$$M \longmapsto TMT^{-1}.$$

Vinberg **[Vi]** proved that the k-forms of $\mathrm{Ad}\,\mathrm{SO}(F_0,\mathbb{C})$ are precisely the $\mathrm{Ad}\,\mathrm{SO}(F,\mathbb{C})$.

Remark. In this example we observed that the group $\mathrm{Ad}\,\mathrm{SO}(F,\mathbb{C})$ is isomorphic to $\mathrm{SO}(F,\mathbb{C})/\pm I$, the usual definition of $\mathrm{Iso}^+\,\mathbb{H}^3$. We needed to consider $\mathrm{Ad}\,\mathrm{SO}(F,\mathbb{C})$ in order to establish that $\mathrm{Iso}^+\,\mathbb{H}^3$ has the structure of a linear algebraic group defined over k.

The arithmetic subgroups of $\mathrm{SO}(F,\mathbb{C})$ are those commensurable with $\mathrm{SO}(F,\mathbb{C})_{O(k)}$.

Example 2. Let D be a generalized quaternion algebra over the field k. This means that as a k-vector space

$$D = \{x_1 + x_2 i + x_3 j + x_4 ij \mid x_1, x_2, x_3, x_4 \in k\}.$$

And there are two non zero elements a, b in k such that multiplication is determined by the rules $i^2 = a$, $j^2 = b$, $ij = -ji$ and multiplication is to be bilinear over k. The algebra D turns out to be an associative central simple algebra and we denote it by

$$D = \left(\frac{a,b}{k}\right).$$

The algebra D has a 'reduced norm' and 'reduced trace' given by the formulas

$$N(x_1 + x_2 i + x_3 j + x_4 ij) = x_1^2 - a x_2^2 - b x_3^2 + ab x_4^2,$$
$$T(x_1 + x_2 i + x_3 j + x_4 ij) = 2x_1.$$

The multiplicative group of invertible elements $D^\star$ of D can be made to operate on D by conjugation $x \longmapsto \{y \mapsto xyx^{-1}\}$. Conjugation preserves both the reduced norm and reduced trace and therefore leaves the three dimensional vector space of elements of trace zero invariant. The reduced norm when restricted to this subspace is a quadratic form represented by the symmetric matrix F with respect to the basis $\{i, j, ij\}$ where

$$F = \begin{bmatrix} -a & 0 & 0 \\ 0 & -b & 0 \\ 0 & 0 & ab \end{bmatrix}.$$

The action by conjugation is trivial only for non zero elements of the center $k^\star$ of $D^\star$. Thus we obtain an isomorphism

$$D^\star/k^\star \to \mathrm{SO}(F,\mathbb{C})_k.$$

In the special case where $k = \mathbb{C}$, $D = M(2,\mathbb{C})$ (there is only the one quaternion algebra over $\mathbb{C}$), $D^\star = \mathrm{GL}(2,\mathbb{C})$ and $D^\star/k^\star = \mathrm{PSL}(2,\mathbb{C})$. In the case where $a = b = -1$ $\mathrm{SO}(F,\mathbb{C}) = \mathrm{SO}(3,\mathbb{C})$, in the usual notation, and we have shown that $\mathrm{PSL}(2,\mathbb{C})$ is a linear algebraic group defined over $\mathbb{Q}$.

It is known that the k-forms of $\mathrm{SO}(3,\mathbb{C})$ are exactly the linear algebraic groups $\mathrm{SO}(3,F)$ defined over k.

The group $\mathrm{PSL}(2,\mathbb{C})$ is also isomorphic to $\mathrm{Iso}^+\,\mathbb{H}^3$. Thus $\mathrm{Iso}^+\,\mathbb{H}^3$ has the structure of a complex Lie group as well as that of a real Lie group. It is connected and has trivial center.

The group $\mathrm{SL}(2,\mathbb{C})$, the universal cover of $\mathrm{PSL}(2,\mathbb{C})$, is easily seen to be a complex Lie group and a linear algebraic group defined over $\mathbb{Q}$. Its k-forms are the universal covers of the k-forms of $\mathrm{PSL}(2,\mathbb{C})$ and are the groups of elements of norm 1 in the algebra $D \otimes_k \mathbb{C}$, denoted D^1.

The isomorphism $D \otimes_k \mathbb{C} \cong M(2,\mathbb{C})$ restricts to the isomorphism $D^1 \cong \mathrm{SL}(2,\mathbb{C})$ needed to define the k-form.

3. Arithmetically definable groups. Given a connected semi-simple Lie group with trivial center $\widetilde{G}$ there are two constructions of arithmetic lattices considered by Borel and Harish-Chandra.

First construction (real arithmetic lattices). For this construction $\widetilde{G}$ must be a real Lie group with the structure of a linear algebraic group defined over $\mathbb{Q}$.

First we choose a Lie group isomorphism $\varphi : \widetilde{G} \to G_{\mathbb{R}}$. (There may be many to choose from. Here G is a linear algebraic group defined over $\mathbb{Q}$.)

Next we choose a totally real field k. (Since $\mathbb{Q} \leqq k$, G is defined over k also.)

Thirdly we choose a k-form of G. That is, a linear algebraic group H defined over k and an isomorphism $\lambda : G_{\mathbb{R}} \to H_{\mathbb{R}}$ defined over some finite extension ℓ of k. (Again, there may be many choices of H and λ.)

However, there is a condition that must be satisfied by H and k. For any $\sigma \neq id$, $\sigma : k \to \mathbb{R}$, $H^\sigma_{\mathbb{R}}$ must be compact.

Fourthly we choose any subgroup of $H_{\mathbb{R}}$ commensurable with $H_{O(k)}$, call it $\widehat{\Gamma}$.

Finally, we choose any group, call it Γ, conjugate in $\widetilde{G}$ to $\varphi^{-1}\lambda^{-1}\widehat{\Gamma}$.

The group Γ is a lattice of $\widetilde{G}$ by Theorem 2.1. Any such group (there are typically many because of the five choices) is called a ***real arithmetic lattice***.

Second Construction (complex arithmetic lattices). For this construction $\widetilde{G}$ must be a complex Lie group with the structure of a linear algebraic group defined over $\mathbb{Q}$.

First we choose a Lie group isomorphism $\varphi : \widetilde{G} \to G$. (Here $G = G_{\mathbb{C}}$ is a linear algebraic group defined over $\mathbb{Q}$. There may be many isomorphisms to choose from.)

Next we choose a number field k with exactly one complex place. (One pair of complex conjugate embeddings of k in $\mathbb{C}$. The rest, if any, are real. Since $\mathbb{Q} \leqq k$, G is defined over k also.)

Thirdly we choose a k-form of G. That is, a linear algebraic group defined over k and an isomorphism $\lambda : G \to H$ defined over some finite extension ℓ of k. (Again, there are many choices of H and λ.)

However, there is a condition that must be satisfied by H and k. For any ***real*** embedding $\sigma : k \to \mathbb{R}$, $H^\sigma_{\mathbb{R}}$ must be compact.

Fourthly we choose any subgroup of $H = H_{\mathbb{C}}$ commensurable with $H_{O(k)}$, call it $\widehat{\Gamma}$.

Finally, we choose any group, call it Γ, conjugate in $\widetilde{G}$ to $\varphi^{-1}\lambda^{-1}\Gamma$.

The group Γ is a lattice of $\widetilde{G}$ by Theorem 2.1. Any such group is called a ***complex arithmetic lattice***.

Thus $\Gamma \leqq G$ is a real arithmetic lattice if it can be constructed via the first construction and a complex arithmetic lattice if it can be constructed via the second.

The reader may wonder what happens if, for example, k has two complex places or the 'condition' isn't satisfied. There is a theory for these groups too, expounded in **[BH]**, but it appears to us to have no three dimensional topological application, so we don't deal with it in this paper.

4. The special case $G_{\mathbb{R}} = \mathrm{Ad}\,\mathrm{SO}(F_0,\mathbb{R}) = \mathrm{Iso}^+\,\mathbb{H}^3$. Specializing the previous definition to the case of the real connected centerless Lie group $\mathrm{Ad}\,\mathrm{SO}(F_0,\mathbb{R}) = \mathrm{Iso}^+\,\mathbb{H}^3$ we shall say that $\Gamma \leqq \mathrm{Iso}^+\,\mathbb{H}^3$ is ***real arithmetic*** if, following Vinberg (**[Vi]**),

1. There exists a finite extension k of $\mathbb{Q}$, and a 4×4 symmetric matrix F with entries in k which is ***admissible***, i.e.:
   (i) k is totally real
   (ii) F is equivalent to F_0 over $\mathbb{R}$
   (iii) F^σ is *definite* for every non identity embedding $\sigma : k \to \mathbb{R}$;
2. There exists an isomorphism $\lambda : \mathrm{Ad}\,\mathrm{SO}(F_0,\mathbb{R}) \to \mathrm{Ad}\,\mathrm{SO}(F,\mathbb{R})$ such that $\lambda(\Gamma)$ is an arithmetic subgroup of $\mathrm{Ad}\,\mathrm{SO}(F,\mathbb{C})_{\mathbb{R}}$. (This means $\lambda(\Gamma)$ is commensurable with $\mathrm{Ad}\,\mathrm{SO}(F,\mathbb{C})_{O(k)}$).

We shall say that $\Gamma \leqq \mathrm{Iso}\,\mathbb{H}^3$ is real arithmetic if $\Gamma \cap \mathrm{Iso}^+\,\mathbb{H}^3$ is real arithmetic as a subgroup of $\mathrm{Iso}^+\,\mathbb{H}^3$.

(*Remark.* The isomorphism λ need not coincide with the isomorphism defined over $\ell \leqq k$ that defines $\mathrm{Ad}\,\mathrm{SO}(F,\mathbb{C})$ as a k-form of $\mathrm{Ad}\,\mathrm{SO}(F_0,\mathbb{C})$.)

This definition reduces to the previous one because $\mathrm{Ad}\,\mathrm{SO}(F;\mathbb{R}) \cong \mathrm{Ad}\,\mathrm{SO}(4)$ is compact and, as was explained before, the k-forms of $\mathrm{Ad}\,\mathrm{SO}(F_0,\mathbb{C})$ are precisely the $\mathrm{Ad}\,\mathrm{SO}(F,\mathbb{C})$. Thus a real arithmetic subgroup $\Gamma \leqq \mathrm{Iso}\,\mathbb{H}^3$ is a lattice.

At this point, it is convenient to introduce another definition of Vinberg (**[Vi]**). A lattice Γ of $\mathrm{Ad}\,\mathrm{SO}(F_0,\mathbb{R}) = \mathrm{Iso}^+\,\mathbb{H}^3$ (or of $\mathrm{Iso}\,\mathbb{H}^3$) is ***quasi-arithmetic*** if there exists an isomorphism

$$\lambda : \mathrm{Ad}\,\mathrm{SO}(F_0,\mathbb{R}) \to \mathrm{Ad}\,\mathrm{SO}(F,\mathbb{R})$$

where

1. F is admissible;
2. $\lambda(\Gamma)$ has a finite index subgroup contained in $\mathrm{Ad}\,\mathrm{SO}(f,\mathbb{C})_k$.

Note that in order for a *quasi-arithmetic* group Γ to be real arithmetic it is necessary and sufficient that Γ is commensurable with $\operatorname{Ad} \mathrm{SO}(F, \mathbb{C})_{O(k)}$.

The following can be proven. Let $\langle x, y\rangle$ be defined as equal to xF_0y^t. Then a lattice $\Gamma \leqq \operatorname{Iso} \mathbb{H}^3 (= \operatorname{Ad} O(F, \mathbb{R}))$ is quasi-arithmetic if there is a basis $\{e_1, e_2, e_3, e_4\}$ of $\mathbb{R}^4$ such that the matrix $F = (\langle e_i, e_j\rangle)$ satisfies:

(i) F has entries in the totally real number field k;
(ii) F^σ is definite for every $\sigma : k \to \mathbb{R}$, $\sigma \neq id$;
(iii) There exists $\Gamma_1 \leqq \Gamma$, of finite index, whose elements, written as matrices with respect to the basis $\{e_1, \cdots, e_4\}$ have their entries in k.

The lattice Γ is real arithmetic if also

(iv) There exists $\Gamma_1 \leqq \Gamma$ if finite index, whose elements written as matrices with respect to the basis $\{e_1, \cdots, e_4\}$ have their entries in $O(k)$.

A real arithmetic lattice is *co-compact* if and only if it satisfies one of the following conditions:

(i) the field k is not $\mathbb{Q}$;
(ii) the field k is $\mathbb{Q}$, but the form F doesn't represent zero over $\mathbb{Q}$.

5. The special case $G = \mathrm{PSL}(2, \mathbb{C}) = \mathrm{Iso}^+ \mathbb{H}^3$. Now we specialize the definition of complex arithmetic groups to the case $G = \mathrm{PSL}(2, \mathbb{C}) = \mathrm{Iso}^+ \mathbb{H}^3$.

The quaternion algebra $D = (\frac{a,b}{k})$ is ***admissible*** if

(i) k has exactly one complex place (pair of complex conjugate embeddings);
(ii) D is *ramified* at every real place. ($D \otimes_{k^\sigma} \mathbb{R} = \mathbb{H}$, where $\mathbb{H}$ is the Hamilton quaternion algebra. Here k^σ is the real image of k under the embedding σ.)

Note that D defines a k-form for $\mathrm{PSL}(2, \mathbb{C}) = \mathrm{SO}(F, \mathbb{C})$ where

$$F = \begin{pmatrix} -a & & \\ & -b & \\ & & ab \end{pmatrix}.$$

To say that D is admissible is to imply that $\mathrm{SO}(F^\sigma, \mathbb{C})_{\mathbb{R}} = \mathrm{SO}(3, \mathbb{R})$ which is compact or that $D^1 \otimes_{k^\sigma} \mathbb{R} = S^3$ is compact also.

Definition (Compare Borel **[B]**). $\Gamma \leqq \mathrm{PSL}(2, \mathbb{C}) = \mathrm{Iso}^+ \mathbb{H}^3$ is ***complex arithmetic*** if there exists an admissible quaternion algebra $D = (\frac{a,b}{k})$ and an isomorphism $\lambda : \mathrm{PSL}(2, \mathbb{C}) \to \mathrm{SO}(F, \mathbb{C})$ such that $\lambda(\Gamma)$ is an arithmetic subgroup of $\mathrm{SO}(F, \mathbb{C})$ (a subgroup commensurable with $\mathrm{SO}(F, \mathbb{C})_{O(k)}$).

Definition (Compare **[V]**, **[R]**). A discrete subgroup $\widetilde{\Gamma} \leqq \mathrm{SL}(2, \mathbb{C})$ is ***complex arithmetic*** if there exists an admissible quaternion algebra $D = (\frac{a,b}{k})$ and an order θ of D, such that $\widetilde{\Gamma}$ is commensurable with $f(\theta^1)$ where $\theta^1 = \theta \cap D^1$ and

$$f : D^1 \to D^1 \otimes \mathbb{C} = \mathrm{SL}(2, \mathbb{C}) \quad \text{is the canonical embedding.}$$

If $\widetilde{\Gamma}$ is of finite index in $f(\theta^1)$ we say that $\widetilde{\Gamma}$ is derived from a quaternion algebra.

Remark. As we noted earlier, $D^1 \otimes \mathbb{C}$ can be studied as a linear algebraic group defined over k. Its arithmetic subgroups are precisely those which like $\widetilde{\Gamma}$ are commensurable with $f(\theta^1)$, where θ is an order.

Proposition. *$\widetilde{\Gamma} \leqq \mathrm{SL}(2, \mathbb{C})$ is complex arithmetic if and only if $\Gamma \leqq \mathrm{PSL}(2, \mathbb{C})$ is complex arithmetic where $\widetilde{\Gamma}$ is the inverse image of Γ in the map $\mathrm{SL}(2, \mathbb{C}) \to \mathrm{PSL}(2, \mathbb{C})$.*

The proof follows from the fact that the image of $\theta^1 = \theta \cap D^1$ is commensurable with $\mathrm{SO}(F, \mathbb{C})_{O(k)}$ under the map μ

$$\begin{aligned} \mu : D^1 &\to \mathrm{SO}(F, \mathbb{C})_k \\ g &\longmapsto \{d \mapsto gdg^{-1}\}. \end{aligned}$$

□

An important consequence of this proposition is that it is usually unnecessary to distinguish between Γ and $\widetilde{\Gamma}$.

We deduce from Theorem 2.1 that Γ is complex arithmetic and a lattice. This lattice is co-compact if and only if D is a division algebra. If this is not the case, then k has no real place. In effect $D \otimes_k K$ is not a division algebra for any extension K of k.

The relationship between real- and complex-arithmetic groups is given by the following theorem of Reid (**[R]**):

Theorem (Reid). *The set of complex-arithmetic subgroups of $\mathrm{Iso}^+ \mathbb{H}^3$ that contain Fuchsian subgroups (lattices in $\mathrm{Iso}^+ H^2$) coincides with the set of real-arithmetic subgroups of $\mathrm{Iso}^+ \mathbb{H}^3$.*

The Russian school (Makarov, Vinberg, Nikulin, etc.) works with groups generated by reflections and they study real arithmeticity. The following proposition in combination with Reid's theorem above, shows that for reflection groups, real arithmeticity is no more special than complex arithmeticity. The groups studied in this paper are commensurable with groups generated by reflections, so from here on we simply speak about 'arithmetic subgroups' of $\mathrm{Iso}^+ \mathbb{H}^3$.

Proposition. *Let $\Gamma \leq \operatorname{Iso} \mathbb{H}^3$ be a group generated by reflections in the faces of a polytope. Then Γ contains Fuchsian subgroups (we follow the conventions of* **[Vi]** *about polytopes).*

Proof. The reflection planes in Γ decompose $\mathbb{H}^3$ in polytopes. Each of them is a fundamental domain for Γ. Take a plane r containing a face of one polytope. Then the stabilizer in Γ of r contains a Fuchsian subgroup G. In fact, r is tessellated by copies of faces of a polytope. Taking a copy for each face of the polytope we obtain a union of finitely many faces in r. This union is a fundamental domain for G. □

Corollary. *Every complex-arithmetic subgroup $\Gamma \leq \mathrm{Iso}\, \mathbb{H}^3$ which is commensurable with a group generated by reflections is real-arithmetic.* □

6. Characterization of arithmetic subgroups of $\mathrm{Iso}^+\,\mathbb{H}^3$. Reid in his thesis **[R]**, following work of Takeuchi in the case $\mathrm{SL}(2,\mathbb{R})$, characterized subgroups of $\mathrm{SL}(2,\mathbb{C})$ which are arithmetic.

Theorem 2.2 (Reid). *Let* $\Gamma \leqq \mathrm{SL}(2,\mathbb{C})$ *be a subgroup of finite co-volume. If* Γ *is derived from a quaternion algebra then*

(1) $K = \mathbb{Q}(\mathrm{tr}\, g : g \in \Gamma)$ *is a number field with one complex place;*
(2) $\mathrm{tr}(g)$ *is an algebraic integer, for every* $g \in \Gamma$*;*
(3) *For every embedding* $\sigma : K \to \mathbb{R}$, $\sigma(\mathrm{tr}(\Gamma)) \subset [-2, 2]$.

Conversely if Γ *satisfies*

(4) $K = \mathbb{Q}(\mathrm{tr}(g) : g \in \Gamma)$ *is a number field not totally real;*
(5) *(same as (2) above);*
(6) *For every embedding* $\sigma : K \to \mathbb{C}, \sigma \neq id$ *or conjugation,* $\sigma(\mathrm{tr}(\Gamma))$ *is bounded, then* Γ *is derived from a quaternion algebra.* □

Theorem 2.3 (Reid). *A subgroup* $\Gamma \leqq \mathrm{SL}(2,\mathbb{C})$ *is arithmetic if and only if* Γ^2 *is derived from a quaternion algebra, where* Γ^2 *is the group generated by squares of elements of* Γ. □

Vinberg, in **[Vi]**, characterized the subgroups of $\mathrm{Iso}\,\mathbb{H}^3$ generated by reflections in the faces of a polyhedron Π in $\mathbb{H}^3$ that are arithmetic, in terms of the Gram matrix of Π.

Suppose that Π is contained in the hyperboloid model of $\mathbb{H}^3$ (see 1.4). We take vectors $e_1, \ldots, e_n$ in the Minkowski space $\mathbb{R}^4$ that are orthogonal to the faces of Π. We normalize the vectors e_i such that $f(e_i, e_i) = 1$. The Gram matrix of Π is then $G = [a_{ij}]$ where $a_{ij} = f(e_i, e_j)$.

Let $b_{i_1 \cdots i_m}$ be the cyclic products, i.e., the numbers $a_{i_1 i_2} a_{i_2 i_3} \cdots a_{i_m i_1}$, for any ordered sequence of indices of the set $\{1, \ldots, n\}$, $m \geq 1$.

Theorem 2.4 (Vinberg). *Let* Γ *be a discrete subgroup of* $\mathrm{Iso}\,\mathbb{H}^3$ *of finite co-volume, and generated by reflections in the faces of* Π. *Let* $\widetilde{K}$ *be the number field generated by the entries* a_{ij} *of the Gram matrix, and let* K *be the subfield generated by all the cyclic products. Let* D *be the determinant of an arbitrary principal submatrix of* G *of order 4 that is adjacent to a principal submatrix* C^+ *of order 3, where* C^+ *is the Gram matrix of a simplicial angle of* Π. *Then* Γ *is quasi-arithmetic if and only if*

(i) $\widetilde{K}$ *is a totally real number field;*
(ii) D *is a primitive element of the field* K*;*
(iii) *All the conjugates of* D *are positive.*

Alternatively Γ *is quasi-arithmetic if and only if* $\widetilde{K}$ *is totally real and for every embedding* $\sigma : \widetilde{K} \to \mathbb{R}$ *which is not the identity on* K *the matrix* $G^\sigma = [\sigma(a_{ij})]$ *is positive semidefinite.*

Γ *is arithmetic if and only if* Γ *is quasi-arithmetic and*

(iv) *the numbers* $2a_{ij}$ *are algebraic integers.* □

§3. The geometric description of the Borromean hyperbolic orbifolds $\widehat{B}(m,n,p)$

Let $f = \frac{x^2}{A^2} + \frac{y^2}{B^2} + \frac{z^2}{C^2} - t^2$, with A, B, C real positive, be a quadratic form on $\mathbb{R}P^3$ defined in homogeneous co-ordinates $(x : y : z : t)$. The component $E(A,B,C)$ of $\mathbb{R}P^3 - (f = 0)$, that contains the origin $(0:0:0:1)$ is the interior of an ellipsoid with longitudinal semiaxes A, B, C and serves as a Beltrami-Klein model for hyperbolic 3-space $\mathbb{H}^3$.

Consider the polyhedron $P(\widehat{a}, \widehat{b}, \widehat{c})$ of Figure 1. Only the positive octant is shown in Figure 1. The rest is obtained by reflections in the coordinate planes. We shall call $P(\widehat{a}, \widehat{b}, \widehat{c})$ a ***pyritohedron***.

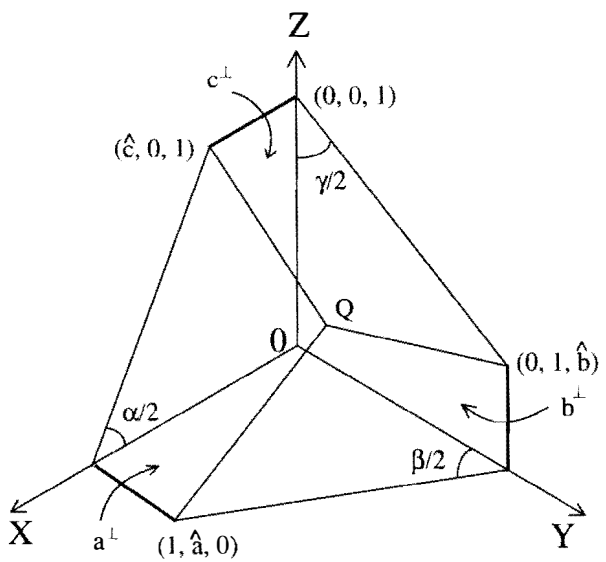

Figure 1

We think of the pyritohedron $P(\widehat{a}, \widehat{b}, \widehat{c})$ as being contained in the model $E(A,B,C)$ of $\mathbb{H}^3$. We shall find conditions on A, B, C, $\widehat{a}$, $\widehat{b}$, $\widehat{c}$ such that the dihedral angles at the three edges converging at the point Q are right angles.

Thus we consider the projective equations of the planes $a^\perp$, $b^\perp$, $c^\perp$:

$$a^\perp = \{(x : y : z : t) \mid x + (1 - \widehat{c})z - t = 0\},$$
$$b^\perp = \{(x : y : z : t) \mid y + (1 - \widehat{a})x - t = 0\},$$
$$c^\perp = \{(x : y : z : t) \mid z + (1 - \widehat{b})y - t = 0\}.$$

The poles of these planes, a, b, c with respect to the quadric $f = 0$ are

$$a = (A^2 : 0 : (1-\widehat{c})C^2 : 1),$$
$$b = ((1-\widehat{a})A^2 : B^2 : 0 : 1),$$
$$c = (0 : (1-\widehat{b})B^2 : C^2 : 1).$$

Since we wish to have $\cos(a^\perp, b^\perp) = \cos(b^\perp, c^\perp) = \cos(c^\perp, a^\perp) = 0$ we must have

$$aFb^t = bFc^t = cFa^t = 0$$

where F is the matrix of the form f. This immediately gives rise to the equations

$$(1-\widehat{a})A^2 = (1-\widehat{b})B^2 = (1-\widehat{c})C^2 = 1.$$

Thus we see that the dihedral angles at the edges of $P(\widehat{a},\widehat{b},\widehat{c})$ concurrent with Q are right angles if and only if

$$\widehat{a} = 1 - A^{-2}; \quad \widehat{b} = 1 - B^{-2}; \quad \widehat{c} = 1 - C^{-2}.$$

In this case the poles of $a^\perp, b^\perp, c^\perp$ are

$$a = (A^2 : 0 : 1 : 1); \quad b = (1 : B^2 : 0 : 1); \quad c = (0 : 1 : C^2 : 1).$$

Finally, given angles α, β, γ (see Figure 1) we would like to determine A, B, C in such a way that the condition that the three dihedral angles converging at the point Q be right angles is satisfied.

Thus we consider the plane $a'^\perp$ symmetric to $a^\perp$ with respect to $y = 0$. Its pole, a', with respect to $f = 0$, will be Euclidean symmetric to a with respect to $y = 0$ as this plane passes through the center of the ellipsoid. Thus we shall have for the planes symmetric to $a^\perp$, $b^\perp$, and $c^\perp$ with respect to $y = 0$, $z = 0$, $x = 0$ the poles

$$a' = (A^2 : 0 : -1 : 1),$$
$$b' = (-1 : B^2 : 0 : 1),$$
$$c' = (0 : -1 : C^2 : 1).$$

Then

$$-\cos\alpha = \frac{aFa'^t}{\sqrt{aFa^t}\sqrt{a'Fa'^t}} = \frac{aFa'^t}{aFa^t} = \frac{A^2 - C^{-2} - 1}{A^2 + C^{-2} - 1} = \frac{1 + C^2(1-A^2)}{1 - C^2(1-A^2)}.$$

From this we derive the equations:

$$C^2(A^2-1)(1+\cos\alpha) = 1 - \cos\alpha$$
$$C^2(A^2-1) = \tan^2(\frac{\alpha}{2}).$$

Therefore we have, given α, β, γ,

$$C^2(A^2-1) = \tan^2(\frac{\alpha}{2}),$$
$$A^2(B^2-1) = \tan^2(\frac{\beta}{2}),$$
$$B^2(C^2-1) = \tan^2(\frac{\gamma}{2}).$$

We deduce also that α, β, γ can take values in the internal $[0,\pi)$. We sum up what has been demonstrated so far in the following proposition.

Proposition 3.1. *The pyritohedron $P(\widehat{a},\widehat{b},\widehat{c})$ contained in the ellipsoidal model, $E(A,B,C)$, of $\mathbb{H}^3$ has hyperbolic right angles for the dihedral angles at the edges concurrent at Q if and only if:*

$$\widehat{a} = 1 - A^{-2}, \quad \widehat{b} = 1 - B^{-2}, \quad \widehat{c} = 1 - C^{-2}.$$

Moreover, the values of the hyperbolic angles α, β, γ satisfy

$$\tan^2(\frac{\alpha}{2}) = C^2(A^2-1), \ \tan^2(\frac{\beta}{2}) = A^2(B^2-1), \ \tan^2(\frac{\gamma}{2}) = B^2(C^2-1).$$

The angles α, β, γ can take any value in the interval $[0,\pi)$. □

Next, we shall obtain generators for a discrete subgroup $B(m,n,p)$ of $\mathrm{Iso}^+\mathbb{H}^3$ such that the quotient $\widehat{B}(m,n,p) := \mathbb{H}^3/B(m,n,p)$ is the ***Borromean orbifold*** with underlying topological space S^3 and singular locus the Borromean rings and such that the isotropy groups of the components of the rings are cyclic of orders m, n, p (see Figure 2) where $m > 2$, $n > 2$, $p > 2$

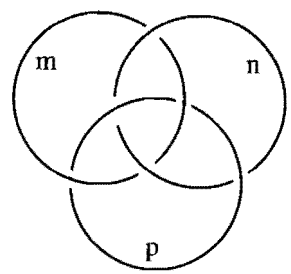

Figure 2

It is well known (see for example **[Th]**, **[HLMW]**) that $B(m,n,p)$ is generated by g_a, g_b, g_c, which are, by definition, rotations of $\frac{2\pi}{m}$, $\frac{2\pi}{n}$, $\frac{2\pi}{p}$ in the axes $\langle(1:0:0:1), (1:\widehat{a}:0:1)\rangle$, $\langle(0:1:0:1), (0:1:\widehat{b}:1)\rangle$, $\langle(0:0:1:1), (\widehat{c}:0:1:1)\rangle$ respectively.

Our desire is to determine the group $B(m,n,p)$ as a subgroup of $\mathrm{PSL}(2,\mathbb{C})$ in the Poincaré half-space model. To achieve this it is convenient to represent g_a, g_b, g_c as

products of hyperbolic reflections. In effect letting r_a, r_b, r_c be reflections in the planes $a^\perp$, $b^\perp$, $c^\perp$ and r_x, r_y, r_z reflections in the planes yz, xz, xy we have

$$g_a = r_a r_z, \quad g_b = r_b r_x, \quad g_c = r_c r_y.$$

As we have indicated in Section 2, it is easy to obtain a reflection in the half-space model when one knows the pole of the plane of reflection in the Beltrami-Klein model. We pass from the Beltrami-Klein model to the intermediate model via the two following co-ordinate changes:

$$X = \frac{x}{A}e, \quad Y = \frac{y}{B}, \quad Z = \frac{z}{C}, \quad T = t;$$

$$\theta_1 = X + iY, \quad \theta_2 = Z - T, \quad \theta_3 = Z + T, \quad \theta_4 = -X + iY.$$

These changes carry f to the form

$$\det \begin{bmatrix} \theta_1 & \theta_2 \\ \theta_3 & \theta_4 \end{bmatrix}$$

which defines the intermediate model.

In the intermediate model the planes of reflection of r_a, r_b, r_c, r_x, r_y, r_z are determined by the coordinates of their poles

$$a = \begin{pmatrix} A & C^{-1}-1 \\ C^{-1}+1 & -A \end{pmatrix}, \quad b = \begin{pmatrix} A^{-1}+iB & -1 \\ 1 & -A^{-1}+iB \end{pmatrix}, \quad c = \begin{pmatrix} iB^{-1} & C-1 \\ C+1 & iB^{-1} \end{pmatrix};$$

$$(1:0:0:0) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad (0:1:0:0) = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}, \quad (0:0:1:0) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Then, in the Poincaré half-space model these reflections correspond to the following antihomographies of $\mathbb{CP}^1$.

$$r_a \equiv z' = \frac{A\bar{z} + C^{-1} - 1}{(C^{-1}+1)\bar{z} - A}, \quad r_b \equiv z' = \frac{(A^{-1}+iB)\bar{z} - 1}{\bar{z} - A^{-1} + iB}, \quad r_c \equiv z' = \frac{iB^{-1}\bar{z} + C - 1}{(C+1)\bar{z} + iB^{-1}};$$

$$r_x \equiv z' = -\bar{z}, \quad r_y \equiv z' = +\bar{z}, \quad r_z \equiv z' = \frac{1}{\bar{z}}.$$

Thus we have:

Theorem 3.2. *The orbifold $\widehat{B}(m,n,p)$ of Figure 2 is hyperbolic for $3 \leqq m,n,p \leqq \infty$. The group $B(m,n,p)$ of the orbifold $\widehat{B}(m,n,p)$ is generated by the following homographies of $\mathbb{C}P^1$ which act on the Poincaré half-space model:*

$$g_a \equiv z' = \frac{(C^{-1}-1)z + A}{-Az + C^{-1} - 1}, \quad g_b \equiv z' = \frac{(A^{-1}+iB)z + 1}{z + A^{-1} - iB}, \quad g_c \equiv z' = \frac{iB^{-1}z + C - 1}{(C+1)z + iB^{-1}},$$

where A, B, C satisfy

$$C^2(A^2-1) = \tan^2(\frac{\pi}{m}), \quad A^2(B^2-1) = \tan^2(\frac{\pi}{n}), \quad B^2(C^2-1) = \tan^2(\frac{\pi}{p}).$$

The homographies g_a, g_b, g_c are images of the following elements of $\mathrm{SL}(2,\mathbb{C})$*:*

$$h_a = \cos\frac{\pi}{m}\begin{pmatrix} 1-C & AC \\ -AC & 1+C \end{pmatrix}, \quad h_b = \cos\frac{\pi}{n}\begin{pmatrix} 1+iAB & A \\ A & 1-iAB \end{pmatrix},$$

$$h_c = \cos\frac{\pi}{p}\begin{pmatrix} 1 & iB(1-C) \\ -iB(1+C) & 1 \end{pmatrix},$$

which generate a subgroup of $\mathrm{SL}(2,\mathbb{C})$ *that we shall denote by $B_{m,n,p}$, and that projects to $B(m,n,p)$.* □

Remark 1. The orbifold $\widehat{B}(\infty,\infty,\infty)$ should be viewed as the exterior of the Borromean rings. It is an open hyperbolic manifold, as can be deduced from our construction. In effect for $\alpha = \beta = \gamma = 0$, one deduces that $A = B = C = 1$; that the ellipsoid is the sphere of radius one with center the origin. Moreover $\widehat{a} = \widehat{b} = \widehat{c} = 0$. The pyritohedron degenerates to a rhombododecahedron inscribed in the sphere. This is exactly Thurston's construction in **[Th]** to give the complement of the Borromean rings a complete hyperbolic structure.

Remark 2. $\widehat{B}(2,2,2)$ is Euclidean (see Thurston (**[Th]**) for example). This can be deduced from our result on setting $A = B = C$ so that f can be written $f = x^2 + y^2 + z^2 - A^2t^2$. As $\alpha = \beta = \gamma$ tends to π, $\tan^2(\frac{\alpha}{2})$ tends to infinity and A, B, C tend to infinity. The form f represents the sphere of infinite radius and the geometry induced in $\mathbb{R}^3$ tends to be Euclidean. (The pyritohedron becomes small relative to the sphere as the sphere grows. In the limit its geometry is Euclidean.) The pyritohedron tends toward a regular cube as $\widehat{a} = \widehat{b} = \widehat{c}$ tend to one. This is the construction, using a cube, that Thurston made for $\widehat{B}(2,2,2)$. (Compare **[Ho**, 4.19].)

§4. The groups $B_{m,n,p}$ that are arithmetic

Since the groups $B(m,n,p)$ of the orbifolds $\widehat{B}(m,n,p)$ are subgroups of $O(F,\mathbb{C})$ where

$$F = \begin{bmatrix} A^{-2} & 0 & 0 & 0 \\ 0 & B^{-2} & 0 & 0 \\ 0 & 0 & C^{-2} & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

(compare 1.4), we can investigate which ones are arithmetic and which ones are quasi-arithmetic. We shall see that the quasi-arithmetic groups are exactly those for which m, n, and p belong to $\{3,4,6,\infty\}$ and the arithmetic groups are exactly those corresponding to the eleven unordered triples $(6,6,6)$, $(4,4,4)$, $(3,3,3)$, $(4,4,3)$, $(6,6,3)$, (∞,∞,∞), $(\infty,\infty,3)$, $(\infty,\infty,4)$, $(\infty,3,3)$, $(\infty,4,3)$, $(\infty,4,4)$.

As our group $B_{m,n,p}$ is not generated by reflections we cannot directly apply Theorem 2.4 of Vinberg. But if we denote by $R(m,n,p)$ the group generated by reflections in the faces of the ***octant*** Π of Figure 1 we have:

Lemma 4.1. *The group $B(m,n,p)$ is an index eight subgroup of $R(m,n,p)$. Then $B(m,n,p)$ is arithmetic (resp. quasi-arithmetic) if and only if $R(m,n,p)$ is arithmetic (resp. quasi-arithmetic).* □

Now we use Theorem 2.4 of Vinberg. Let d, e, f be the poles of the coordinate planes yz, xz, xy. The following normalized vectors are orthogonal to the faces of the octant Π:

$$\begin{aligned}
a &= \rho(A^2,0,1,1), & \rho &= -\cos\frac{\pi}{m}C;\\
b &= \mu(1,B^2,0,1), & \mu &= -\cos\frac{\pi}{n}A;\\
c &= \nu(0,1,C^2,1), & \nu &= -\cos\frac{\pi}{p}B;\\
d &= \alpha(-1,0,0,0), & \alpha &= A;\\
e &= \beta(0,-1,0,0), & \beta &= B;\\
f &= \gamma(0,0,-1,0), & \gamma &= C.
\end{aligned}$$

Therefore the Gram matrix $G=[a_{ij}]$ of Π is:

$$G=\begin{bmatrix}
1 & 0 & 0 & -CA\cos\frac{\pi}{m} & 0 & -\cos\frac{\pi}{m}\\
0 & 1 & 0 & -\cos\frac{\pi}{n} & -AB\cos\frac{\pi}{n} & 0\\
0 & 0 & 1 & 0 & -\cos\frac{\pi}{p} & -BC\cos\frac{\pi}{p}\\
 & & & & 1 & 0 & 0\\
 & & \bigstar & & 0 & 1 & 0\\
 & & & & 0 & 0 & 1
\end{bmatrix}.$$

Therefore

$$\begin{aligned}
\widetilde{K} &= \mathbb{Q}(\{a_{ij}\}) = \mathbb{Q}(\cos\frac{\pi}{m},\cos\frac{\pi}{n},\cos\frac{\pi}{p},CA,AB,BC),\\
K &= \mathbb{Q}(\{bi_1,\ldots,i_m\}) = \mathbb{Q}(A^2,B^2,C^2).
\end{aligned}$$

This last is a consequence of the fact that the field K is generated by cyclic products, the cyclic products comprise the diagonal elements (all one), the squares of the entries of G, $(\cos^2\frac{\pi}{m},\cos^2\frac{\pi}{n},\cos^2\frac{\pi}{p},C^2A^2,C^2B^2,A^2B^2)$ and the element $a_{14}a_{42}a_{25}a_{53}a_{36}a_{61} = A^2B^2C^2\cos^2\frac{\pi}{m}\cos^2\frac{\pi}{n}\cos^2\frac{\pi}{p}$, and the elements $\cos^2\frac{\pi}{m}$, $\cos^2\frac{\pi}{n}$, and $\cos^2\frac{\pi}{p}$ belong to $\mathbb{Q}(A^2,B^2,C^2)$.

Lemma 4.1.1. *There is an integer j prime to the positive integer ℓ and belonging to the interval $(1,\ell/2)$ if and only if $\ell\neq 2,\ 3,\ 4,\ 6,\ \infty$.* □

Proposition 4.2. *If one of m, n, p is not equal to 3, 4, 6, or ∞, then the group $R(m,n,p)$ is not quasi-arithmetic.*

Proof. Suppose one of the numbers m, n, p is not 3, 4, 6 or ∞, let it be m, and let j be the integer given by Lemma 4.1.1, prime to m and in the interval $(1,m/2)$.

Using the fact that the arithmetic series $\{j+im \mid i\geqq 0\}$ contains infinitely many primes (Dirichlet's Theorem), we choose one, $q=j+im$, which also is prime to n and p. Let k' and ℓ' be (the unique) integers such that:

$$\begin{aligned}
q &\equiv k' \bmod n, & |k'| &\in [1,n/2),\\
q &\equiv \ell' \bmod p, & |\ell'| &\in [1,p/2),
\end{aligned}$$

and let us denote $|k'|$ and $|\ell'|$ by k and ℓ respectively.

Note that $\cos\frac{2\pi}{m}q=\cos\frac{2\pi}{m}j$, $\cos\frac{2\pi}{n}q=\cos\frac{2\pi}{n}k$, and $\cos\frac{2\pi}{p}q=\cos\frac{2\pi}{p}\ell$. Next, we apply the non trivial automorphism

$$\theta:\cos\frac{2\pi}{c}\longmapsto\cos\frac{2\pi}{c}q$$

to the field $\mathbb{Q}(\cos^2\frac{\pi}{m},\cos^2\frac{\pi}{n},\cos^2\frac{\pi}{p})\leqq\mathbb{Q}(\cos\frac{2\pi}{c})$ where c is the least common multiple of m, n, and p. This induces one or more non trivial embeddings of $\mathbb{Q}(A^2,B^2,C^2)$ in $\mathbb{R}$. These embeddings are found via the equations

$$\begin{aligned}
\widehat{C}^2(\widehat{A}^2-1) &= \tan^2\frac{\pi}{m}j,\\
\widehat{A}^2(\widehat{B}^2-1) &= \tan^2\frac{\pi}{n}k,\\
\widehat{B}^2(\widehat{C}^2-1) &= \tan^2\frac{\pi}{p}\ell,
\end{aligned}\tag{4.1}$$

which give rise to embeddings $\{A^2\to\widehat{A}^2,\ B^2\to\widehat{B}^2,\ C^2\to\widehat{C}^2\}$ where $\widehat{A}^2$, $\widehat{B}^2$, $\widehat{C}^2$ are solutions of 4.1. Since

$$0<\frac{\pi}{m}j<\frac{\pi}{2},\quad 0<\frac{\pi}{n}k<\frac{\pi}{2},\quad 0<\frac{\pi}{p}\ell<\frac{\pi}{2},$$

Proposition 3.1 guarantees us that there exist solutions with $\widehat{A}^2$, $\widehat{B}^2$, $\widehat{C}^2$ ***positive*** numbers. The embedding σ thus obtained of K in $\mathbb{R}$ is non trivial and the quadratic form

$$\frac{x^2}{\widehat{A}^2}+\frac{y^2}{\widehat{B}^2}+\frac{z^2}{\widehat{C}^2}-t^2$$

is of type (3.1).

We extend $\sigma:K\to\mathbb{R}$ to $\widetilde{\sigma}:\widetilde{K}\to\mathbb{R}$ and form the matrix $\widetilde{\sigma}(G)$. This matrix and the $\widehat{G}$ corresponding to the octant of the pyritohedron $P(\widehat{a},\widehat{b},\widehat{c})$ given by Proposition 3.1 have *equal* corresponding cyclic products.

Therefore the type of the matrix $\widetilde{\sigma}(G)$ coincides with the type of the matrix $\widehat{G}$. Since this one is indefinite, we deduce that $\widetilde{\sigma}(G)$ is indefinite. It follows then from Theorem 2.4 of Vinberg that $R(m,n,p)$ is not quasi-arithmetic. □

We shall study the cases $R(m,n,p)$, m, n, p in $\{3,4,6,\infty\}$ one at a time. We shall take as principal submatrix C^+ of order 3 (see 2.4) the first box of G. We shall

take as D:

$$D = \det \begin{bmatrix} 1 & 0 & 0 & -AC\cos\frac{\pi}{m} \\ 0 & 1 & 0 & -\cos\frac{\pi}{n} \\ 0 & 0 & 1 & 0 \\ -AC\cos\frac{\pi}{n} & -\cos\frac{\pi}{n} & 0 & 1 \end{bmatrix} = 1 - A^2C^2\cos^2\frac{\pi}{n} - \cos^2\frac{\pi}{n}.$$

We shall prove that:

(i) $\widetilde{K} = \mathbb{Q}(\cos\frac{\pi}{m}, \cos\frac{\pi}{n}, \cos\frac{\pi}{p}, AC, BC, AB)$ is totally real;

(ii) D is a primitive element of $K = \mathbb{Q}(A^2, B^2, C^2)$;

(iii) the conjugates of D are positive in all cases.

This implies that all the $R(m,n,p)$ with m, n, p in $\{3,4,6,\infty\}$ are quasi-arithmetic. Finally we shall show

(iv) $2a_{ij}$ is an algebraic integer for every a_{ij} in G.

When this is also the case the group $R(m,n,p)$ is arithmetic.

In the sequel we shall calculate A, B, C by means of the following formulas. Let α, β, γ denote $\tan^2\frac{\pi}{m}$, $\tan^2\frac{\pi}{n}$, $\tan^2\frac{\pi}{p}$ respectively. Then

$$\alpha = \tan^2\frac{\pi}{m} = C^2(A^2-1),$$
$$\beta = \tan^2\frac{\pi}{n} = A^2(B^2-1),$$
$$\gamma = \tan^2\frac{\pi}{p} = B^2(C^2-1).$$

We obtain

$$A^2 = 1 + \cfrac{\alpha}{1 + \cfrac{\gamma}{1 + \cfrac{\beta}{A^2}}}.$$

Then:

$$A = \sqrt{\frac{\alpha+\gamma+1-\beta+\sqrt{\Delta}}{2(\gamma+1)}}.$$

Analogously

$$B = \sqrt{\frac{\alpha+\beta+1-\gamma+\sqrt{\Delta}}{2(\alpha+1)}},$$

$$C = \sqrt{\frac{\beta+\gamma+1-\alpha+\sqrt{\Delta}}{2(\beta+1)}},$$

where $\Delta = \alpha^2+\beta^2+\gamma^2+2(\alpha\beta+\alpha\gamma+\beta\gamma)+4\alpha\beta\gamma+2(\alpha+\beta+\gamma)+1$.

CASE (6, 6, 6). Here $\cos\frac{\pi}{6} = \frac{\sqrt{3}}{2}$; $\alpha = \beta = \gamma = \frac{1}{3}$; $\sqrt{\Delta} = \frac{4}{9}\sqrt{21}$, $A^2 = B^2 = C^2 = \frac{3+\sqrt{21}}{6}$; $D = -\frac{\sqrt{21}}{8}$, $K = \mathbb{Q}(\sqrt{21}) = \mathbb{Q}(D)$, $\sigma(D) = \frac{\sqrt{21}}{8} > 0$. $\widetilde{K} = \mathbb{Q}(\sqrt{3}, \sqrt{21})$ is totally real. Thus $R(6,6,6)$ is quasi-arithmetic.

Since $2\cos\frac{\pi}{m}CA = \sqrt{3}\cdot\frac{3+\sqrt{21}}{6} = \frac{\sqrt{3}+\sqrt{7}}{2} = x$ and x satisfies $x^4 - 5x + 1 = 0$ we see that $R(6,6,6)$ is arithmetic.

CASE (4, 4, 4). Here $\cos\frac{\pi}{4} = \frac{\sqrt{2}}{2}$; $\alpha = \beta = \gamma = 1$; $\sqrt{\Delta} = 2\sqrt{5}$, $A^2 = B^2 = C^2 = \frac{1+\sqrt{5}}{2}$; $D = \frac{1-\sqrt{5}}{4}$, $\sigma(D) = \frac{1+\sqrt{5}}{4} > 0$, $K = \mathbb{Q}(\sqrt{5}) = \mathbb{Q}(D)$. $\widetilde{K} = \mathbb{Q}(\sqrt{5}, \sqrt{2})$ is totally real. Thus $R(4,4,4)$ is quasi-arithmetic.

Since $2\cos\frac{\pi}{m}AC = \sqrt{2}\frac{1+\sqrt{5}}{2}$ is an algebraic integer, $R(4,4,4)$ is arithmetic.

CASE (3, 3, 3). Here $\cos\frac{\pi}{3} = \frac{1}{2}$; $\alpha = \beta = \gamma = 3$; $\sqrt{\Delta} = 4\sqrt{13}$, $A^2 = B^2 = C^2 = \frac{1+\sqrt{13}}{2}$; $D = \frac{-1-\sqrt{13}}{8}$, $\sigma(D) = \frac{-1+\sqrt{13}}{8} > 0$, $K = \mathbb{Q}(\sqrt{13}) = \mathbb{Q}(D)$. $\widetilde{K} = \mathbb{Q}(\sqrt{13})$ is totally real. Thus $R(3,3,3)$ is quasi-arithmetic.

Since $2\cos\frac{\pi}{m}CA = \frac{1+\sqrt{13}}{2}$ is an algebraic integer, $R(3,3,3)$ is arithmetic.

CASE (6, 6, 3). Here $\cos\frac{\pi}{6} = \frac{\sqrt{3}}{2}$, $\cos\frac{\pi}{3} = \frac{1}{2}$; $\alpha = \frac{1}{3}$, $\beta = \frac{1}{3}$, $\gamma = 3$; $\sqrt{\Delta} = \frac{4}{3}\sqrt{13}$, $A^2 = \frac{3+\sqrt{13}}{6}$, $B^2 = \frac{-1+\sqrt{13}}{2}$, $C^2 = \frac{3+\sqrt{13}}{2}$; $D = -\frac{3}{8}(3+\sqrt{13})$, $\sigma(D) = \frac{-3}{8}(3-\sqrt{13}) > 0$, $K = \mathbb{Q}(\sqrt{13}) = \mathbb{Q}(D.)$. $\widetilde{K} = \mathbb{Q}(\sqrt{13})$ is totally real. Thus $R(6,6,3)$ is quasi-arithmetic.

Since $2\cos\frac{\pi}{6}AC = \sqrt{\frac{11+3\sqrt{13}}{2}}$, $2\cos\frac{\pi}{6}AB = \sqrt{\frac{5+\sqrt{13}}{2}}$, $2\cos\frac{\pi}{3}BC = \sqrt{\frac{5+\sqrt{13}}{2}}$ are algebraic integers $R(6,6,3)$ is arithmetic.

CASE (6, 6, 4). Here $\cos\frac{\pi}{6} = \frac{\sqrt{3}}{2}$, $\cos\frac{\pi}{4} = \frac{\sqrt{2}}{2}$; $\alpha = \frac{1}{3}$, $\beta = \frac{1}{3}$, $\gamma = 1$; $\sqrt{\Delta} = \frac{2}{3}\sqrt{17}$, $A^2 = \frac{3+\sqrt{17}}{6}$, $B^2 = \frac{1+\sqrt{17}}{4}$, $C^2 = \frac{3+\sqrt{17}}{4}$; $D = \frac{-3}{16}(3+\sqrt{17})$, $\sigma(D) = \frac{-3}{16}(3-\sqrt{17}) > 0$, $K = \mathbb{Q}(\sqrt{17}) = \mathbb{Q}(D)$. $\widetilde{K}$ is totally real so $R(6,6,4)$ is quasi-arithmetic. But since $2\cos\frac{\pi}{m}AC = \sqrt{\frac{13+3\sqrt{17}}{4}}$ is not an algebraic integer, $R(6,6,4)$ is not arithmetic.

CASE (6, 4, 4). Here $\cos\frac{\pi}{4} = \frac{\sqrt{2}}{2}$, $\cos\frac{\pi}{6} = \frac{\sqrt{3}}{2}$; $\alpha = 1$, $\beta = 1$, $\gamma = \frac{1}{3}$; $\sqrt{\Delta} = \frac{4}{3}\sqrt{7}$, $A^2 = \frac{1+\sqrt{7}}{2}$, $B^2 = \frac{2+\sqrt{7}}{3}$, $C^2 = \frac{1+\sqrt{7}}{3}$; $D = -\frac{1}{6}(1+\sqrt{7})$, $\sigma(D) = \frac{-1}{6}(1-\sqrt{7}) > 0$, $K = \mathbb{Q}(\sqrt{7}) = \mathbb{Q}(D)$. Then $\widetilde{K}$ is totally real. But since $2\cos\frac{\pi}{m}AC = \sqrt{\frac{8+2\sqrt{7}}{3}}$ is not an algebraic integer it follows that $R(6,4,4)$ is quasi-arithmetic but not arithmetic.

CASE (6, 3, 3). Here $\cos\frac{\pi}{3} = \frac{1}{2}$, $\cos\frac{\pi}{6} = \frac{\sqrt{3}}{2}$; $\alpha = 3$, $\beta = 3$, $\gamma = \frac{1}{3}$; $\sqrt{\Delta} = \frac{4}{3}\sqrt{37}$, $A^2 = \frac{1+\sqrt{37}}{2}$, $B^2 = \frac{5+\sqrt{37}}{6}$, $C^2 = \frac{1+\sqrt{37}}{6}$; $D = \frac{-1}{24}(1+\sqrt{37})$, $\sigma(D) > 0$, $K = \mathbb{Q}(\sqrt{37}) = \mathbb{Q}(\sqrt{D})$. $\widetilde{K}$ is totally real so $R(6,3,3)$ is quasi-arithmetic.

But since $2\cos\frac{\pi}{m}AC = \sqrt{\frac{19+\sqrt{37}}{6}}$ is not an algebraic integer, $R(6,3,3)$ is not arithmetic.

CASE (4, 4, 3). Here $\cos\frac{\pi}{4} = \frac{\sqrt{2}}{2}$, $\cos\frac{\pi}{3} = \frac{1}{2}$; $\alpha = 1$, $\beta = 1$, $\gamma = 3$; $\sqrt{\Delta} = 4\sqrt{3}$, $A^2 = \frac{1+\sqrt{3}}{2}$, $B^2 = \sqrt{3}$, $C^2 = 1+\sqrt{3}$; $D = -\frac{1}{2}(1+\sqrt{3})$, $\sigma(D) = -\frac{1}{2}(1-\sqrt{3}) > 0$, $K = \mathbb{Q}(\sqrt{3}) = \mathbb{Q}(D)$. $\widetilde{K}$ is totally real.

Since also, $2\cos\frac{\pi}{m}AC = \sqrt{4+2\sqrt{3}}$, $2\cos\frac{\pi}{n}AB = \sqrt{3+\sqrt{3}}$, $2\cos\frac{\pi}{p}BC = \sqrt{3+\sqrt{3}}$ are all algebraic integers, $R(4,4,3)$ is arithmetic.

CASE (6, 4, 3). Here $\cos\frac{\pi}{6} = \frac{\sqrt{3}}{2}$, $\cos\frac{\pi}{4} = \frac{\sqrt{2}}{2}$, $\cos\frac{\pi}{3} = \frac{1}{2}$; $\alpha = \frac{1}{3}$, $\beta = 1$, $\gamma = 3$; $\sqrt{\Delta} = \frac{2}{3}\sqrt{73}$, $A^2 = \frac{5+\sqrt{73}}{12}$, $B^2 = \frac{-1+\sqrt{73}}{4}$, $C^2 = \frac{7+\sqrt{73}}{6}$; $D = \frac{-5-\sqrt{73}}{8}$, $\sigma(D) = \frac{-5+\sqrt{73}}{8} > 0$, $K = \mathbb{Q}(\sqrt{73}) = \mathbb{Q}(D)$. $\widetilde{K}$ is totally real; and $R(6,4,3)$ is quasi-arithmetic.

But since $2\cos\frac{\pi}{n}AB = \sqrt{\frac{17+\sqrt{73}}{6}}$ is not an algebraic integer we deduce that $R(6,4,3)$ is not arithmetic.

CASE (4,3,3). Here $\cos\frac{\pi}{4} = \frac{\sqrt{2}}{2}$, $\cos\frac{\pi}{3} = \frac{1}{2}$; $\alpha = 1$, $\beta = 3$, $\gamma = 3$; $\sqrt{\Delta} = 10$, $A^2 = \frac{3}{2}$, $B^2 = 3$, $C^2 = 2$; $D = -\frac{3}{4}$. Therefore $K = \mathbb{Q}$ and $\widetilde{K}$ is totally real so $R(4,3,3)$ is quasi-arithmetic.

But since $2\cos\frac{\pi}{m}AB = \frac{3\sqrt{2}}{2}$ is not an algebraic integer, $R(4,3,3)$ is not arithmetic. The cases with $m = \infty$ are proven analogously and we obtain

Theorem 4.3. *The groups $R(m,n,p)$, $B(m,n,p)$ are quasi-arithmetic exactly when m, n, and p belong to $\{3,4,6,\infty\}$. Among these the arithmetic ones are the triples* $(6,6,6)$, $(4,4,4)$, $(3,3,3)$, $(4,4,3)$, $(6,6,3)$, (∞,∞,∞), $(\infty,\infty,3)$, $(\infty,\infty,4)$, $(\infty,3,3)$, $(\infty,4,3)$, $(\infty,4,4)$. □

§5. Trace computation lemmas

We want to compute the fields $K_1 = \mathbb{Q}(\mathrm{tr}(g) \mid g \in B_{m,n,p})$, $K_2 = \mathbb{Q}(\mathrm{tr}(g) \mid g \in B^2_{m,n,p})$. For this we utilize the following lemmas:

Lemma 5.1 ([Vo], Compare [Ma]). *Let Γ be a finitely generated subgroup of* $\mathrm{SL}(2,\mathbb{C})$. *Let $\{\delta_1,\ldots,\delta_r\}$ be a set of generators of Γ. Let $t_{i_1\ldots i_s} = \mathrm{tr}(\delta_{i_1}\ldots\delta_{i_s})$, $1 \leqq s \leqq r$, $1 \leqq i_1 < i_2 < \ldots < i_s \leqq r$. Then, $\mathrm{tr}(\gamma)$, for $\gamma \in \Gamma$, is a polynomial with rational coefficients in the traces $t_{i_1\ldots i_s}$, where $1 \leqq s \leqq 3$.*

The proof makes use of the formulas

$$\mathrm{tr}(\alpha\beta) + \mathrm{tr}(\alpha^{-1}\beta) = \mathrm{tr}(\alpha)\cdot\mathrm{tr}(\beta)$$
$$\mathrm{tr}(\alpha\beta) = \mathrm{tr}(\beta\alpha)$$

and an induction argument on the length of a word in the generators. The case $s \leqq r$, which is all we need in this paper, is fairly easy to prove. The case $1 \leqq s \leqq 3$ is more difficult. □

Lemma 5.2. *Let $g_1,\cdots,g_n \in \mathrm{SL}(2,\mathbb{C})$ and suppose $\mathrm{tr}(g_i) \neq 0$ for $i = 1,\cdots,k$. Then*

$$\Pi_{k=1}^n g_k = (\Pi_{k=1}^n(\mathrm{tr}(g_k))^{-1})\Pi_{k=1}^n(\mathrm{id}+g_k^2),$$
$$(\Pi_{k=1}^n g_k)^2 = (\Pi_{k=1}^n(\mathrm{tr}(g_k))^2)^{-1}(\Pi_{k=1}^n(\mathrm{id}+g_k^2))^2.$$

Proof. The first formula follows immediately from the Cayley-Hamilton theorem. The second formula is just the square of the first formula. □

Lemma 5.3. *Let $\Gamma \subset \mathrm{SL}(2,\mathbb{C})$ be generated by $g_1,\cdots,g_n$. Let $\Gamma^{(2)}$ be the group generated by squares of elements of Γ. Suppose $\mathrm{tr}(g_i) \neq 0$ for $i = 1,\cdots,n$. Let $\Gamma^{SQ} = \langle g_1^2,\cdots,g_n^2\rangle$ be the subgroup of Γ generated by squares of the g_i, $i = 1,\cdots,n$. Then k^2, the trace field of $\Gamma^{(2)}$, equals the trace field of Γ^{SQ}.*

Proof. From the formula $g_i^2 - \mathrm{tr}(g_i)g_i + id = 0$, it follows that $(\mathrm{tr}(g_i))^2 = \mathrm{tr}(g_k^2)+2$. Substituting this expression in the formula given by Lemma 5.2, (in the case of a *product* of squares of elements of Γ, not just one), and taking the trace, we see that the trace of an element of $\Gamma^{(2)}$ belongs to the trace field of Γ^{SQ}. On the other hand $\Gamma^{SQ} \subset \Gamma^{(2)}$. □

Lemmas 5.2 and 5.3, although fairly trivial, can simplify the computation of the trace field of $\Gamma^{(2)}$ considerably. The group generated by $g_1^2, \ldots, g_n^2$ has the same number of generators as Γ. The index of $\Gamma^{(2)}$ in Γ is, typically, 2^n, and many more than n generators may be needed to generate $\Gamma^{(2)}$. Roughly speaking, the number of traces that need to be computed in a group with n generators is proportional to n factorial.

Thus to compute $K_1 = \mathbb{Q}(\mathrm{tr}(g) \mid g \in B_{m,n,p})$ and $K_2 = \mathbb{Q}(\mathrm{tr}(h) \mid h \in B^2_{m,n,p}) = \mathbb{Q}(\mathrm{tr}(k) \mid k \in B^{SQ}_{m,n,p})$, we calculate the traces of h_a, h_b, h_c, h_ah_b, h_ah_c, h_bh_c, $h_ah_bh_c$ which we denote by t_a, t_b, t_{ab}, t_{ac}, t_{bc}, t_{abc}, and the traces of h_a^2, h_b^2, h_c^2, $h_a^2h_b^2$, $h_a^2h_c^2$, $h_b^2h_c^2$, $h_a^2h_b^2h_c^2$, which we denote by T_a, T_b, T_c, T_{ab}, T_{ac}, T_{bc}, T_{abc}. We obtain the following. (The generators h_a, h_b, h_c can be found in the statement of Theorem 3.2.)

$$t_a = 2\cos\frac{\pi}{m}, \quad t_b = 2\cos\frac{\pi}{n}, \quad t_c = 2\cos\frac{\pi}{p},$$
$$t_{ab} = 2\cos\frac{\pi}{m}\cos\frac{\pi}{n}(1-iABC), \quad t_{ac} = 2\cos\frac{\pi}{m}\cos\frac{\pi}{p}(1-iABC),$$
$$t_{bc} = 2\cos\frac{\pi}{n}\cos\frac{\pi}{p}(1-iABC), \quad t_{abc} = 2\cos\frac{\pi}{m}\cos\frac{\pi}{n}\cos\frac{\pi}{p}(1-iABC)^2,$$

$$T_a = 4\cos^2\frac{\pi}{m} - 2, \quad T_b = 4\cos^2\frac{\pi}{n} - 2, \quad T_c = 4\cos^2\frac{\pi}{p} - 2,$$

$$T_{ab} = \frac{1}{2}t_a^2 t_b^2(1 - iABC) - t_a^2 - t_b^2 + 2, \text{ etc. } \ldots,$$

$$T_{abc} = 2\left[(\frac{t_a^2}{2} - 1)(\frac{t_b^2}{2} - 1)(\frac{t_c^2}{2} - 1) + \frac{t_a^2}{2}\frac{t_b^2}{2}\frac{t_c^2}{2}(iABC - A^2B^2C^2)\right].$$

Then the following proposition is an immediate consequence of the previous calculation.

Proposition 5.4.

$$K_1 = \mathbb{Q}(\cos\frac{\pi}{m}, \cos\frac{\pi}{n}, \cos\frac{\pi}{p}, iABC)$$
$$K_2 = \mathbb{Q}(\cos^2\frac{\pi}{m}, \cos^2\frac{\pi}{n}, \cos^2\frac{\pi}{p}, iABC) \qquad \square$$

The field $K_2 = \mathbb{Q}(\cos^2\frac{\pi}{m}, \cos^2\frac{\pi}{n}, \cos^2\frac{\pi}{p}, iABC)$ is an extension of the field

$$k = \mathbb{Q}(\cos^2\frac{\pi}{m}, \cos^2\frac{\pi}{n}, \cos^2\frac{\pi}{p}) = \mathbb{Q}(\cos\frac{2\pi}{m}, \cos\frac{2\pi}{n}, \cos\frac{2\pi}{p})$$
$$= \mathbb{Q}(\cos\frac{2\pi}{c})$$

where c is the least common multiple of m, n and p.

§6. Computation of the quaternion algebras and the special case $B_{4,4,4}$

In this section we compute the quaternion algebras for the eleven arithmetic cases of Section 4. We also compute the orders in the quaternion algebras that define their arithmeticity. We go into considerably more detail in the one case $B_{4,4,4}$.

It was shown (**[HLMW]**, **[HLM2]**) that this particular group is ***universal***. That is, given any closed oriented 3-manifold M^3 there is a finite index subgroup $G(M^3)$ of $B_{4,4,4}$ such that M^3 is homomorphic to the orbit space $\mathbb{H}^3/G(M^3)$, and because of its potential application to the study of 3-manifolds, we wish to explain its arithmetic and algebraic properties in more detail.

Theorem 6.4 of this section, in the case $B_{4,4,4}$ is implicit in **[R]**. We repeat it here explicitly to make it more accessible.

Also the number theoretic properties of the field $\mathbb{Q}(iA)$ are in the literature. We make no claim to originality in this section; the justification for Lemma 6.8 through Theorem 6.16 is again that of accessibility.

In Section 3, Theorem 3.2, generators for $B_{m,n,p}$ in $\mathrm{SL}(2,\mathbb{C})$ are given by

$$h_a = \cos\frac{\pi}{m}\begin{pmatrix} 1-C & AC \\ -AC & 1+C \end{pmatrix},$$
$$h_b = \cos\frac{\pi}{n}\begin{pmatrix} 1+iAB & A \\ A & 1-iAB \end{pmatrix}, \tag{6.1}$$
$$h_c = \cos\frac{\pi}{p}\begin{pmatrix} 1 & iB(1-C) \\ -iB(1-C) & 1 \end{pmatrix}.$$

It follows immediately from Proposition 5.4 that the trace field of $B^2_{m,n,p}$ is $\mathbb{Q}(iABC)$. (In the eleven cases we are considering now, m, n, and p belong to $\{3, 4, 6, \infty\}$. So the squares of the cosines appearing in Proposition 5.4 are rational.)

Following Reid (**[R]**) we construct two interesting geometric objects from $B_{m,n,p}$. Let O_R denote the ring of integers of the field $\mathbb{Q}(iABC)$ and define

$$H = \left\{\sum_{i=1}^{n} k_i g_i \mid g_i \in B^2_{m,n,p},\ k_i \in \mathbb{Q}(iABC)\right\},$$
$$O = \left\{\sum_{i=1}^{n} r_i g_i \mid g_i \in B^2_{m,n,p},\ r_i \in O_R\right\}. \tag{6.2}$$

From the formulas (6.1), using the equation $X^2 = (\mathrm{tr}(X))X - id$, valid for X in $\mathrm{SL}(2,\mathbb{C})$, we obtain the following expressions:

$$h_a^2 = (2\cos^2\frac{\pi}{m} - 1)id + 2\cos^2\frac{\pi}{m}\begin{bmatrix} -C & AC \\ -AC & C \end{bmatrix},$$
$$h_b^2 = (2\cos^2\frac{\pi}{n} - 1)id + 2\cos^2\frac{\pi}{n}\begin{bmatrix} iAB & A \\ A & -iAB \end{bmatrix}, \tag{6.3}$$
$$h_c^2 = (2\cos^2\frac{\pi}{p} - 1)id + 2\cos^2\frac{\pi}{p}\begin{bmatrix} 0 & iB - iBC \\ -iB - iBC & 0 \end{bmatrix}.$$

Now define matrices $\widehat{I}$ and $\widehat{J}$:

$$\widehat{I} = \begin{bmatrix} -C & 0 \\ 0 & C \end{bmatrix}, \qquad \widehat{J} = \begin{bmatrix} 0 & iB \\ -iB & 0 \end{bmatrix}. \tag{6.4}$$

Let $\widehat{K} = \widehat{I}\widehat{J}$ and observe that $\widehat{I}\widehat{J} = -\widehat{J}\widehat{I}$. The following set of formulas is obtained by straightforward manipulation of (6.3). (We wish to show that $\widehat{I}$ and $\widehat{J}$ belong to H.)

$$\begin{aligned}
\frac{h_a^2 - (2\cos^2\frac{\pi}{m} - 1)id}{2\cos^2\frac{\pi}{m}} &= \widehat{I} + \left(\frac{-iABC}{B^2}\right)\widehat{J},\\
\frac{h_b^2 - (2\cos^2\frac{\pi}{n} - 1)id}{2\cos^2\frac{\pi}{n}} &= \left(\frac{-iABC}{C^2}\right)\widehat{I} + \left(\frac{iABC}{B^2C^2}\right)\widehat{K},\\
\frac{h_c^2 - (2\cos^2\frac{\pi}{p} - 1)id}{2\cos^2\frac{\pi}{p}} &= \widehat{J} + \widehat{K}.
\end{aligned} \tag{6.5}$$

Let α, β, γ represent $\tan^2(\frac{\pi}{m})$, $\tan^2(\frac{\pi}{n})$, $\tan^2(\frac{\pi}{p})$ respectively. These are rational numbers in the eleven cases we consider, where m, n, $p \in \{3, 4, 6, \infty\}$.

According to Theorem 3.2 the numbers A, B, C satisfy the following equations:

$$\begin{aligned}
C^2A^2 - C^2 &= \alpha,\\
A^2B^2 - A^2 &= \beta,\\
B^2C^2 - B^2 &= \gamma.
\end{aligned} \tag{6.6}$$

If we multiply the first of the equations in (6.6) by B^2 and add it to the third we can solve for B^2 in terms of $A^2B^2C^2$. We can similarly solve for A^2 and C^2 obtaining

$$\begin{aligned}
A^2B^2C^2 - \gamma &= (\alpha + 1)B^2,\\
A^2B^2C^2 - \alpha &= (\beta + 1)C^2,\\
A^2B^2C^2 - \beta &= (\gamma + 1)A^2.
\end{aligned} \tag{6.7}$$

In particular we note that A^2, B^2, and C^2 belong to the trace field $\mathbb{Q}(iABC)$ in the eleven cases.

The equations (6.5) can be considered a single matrix equation of form $\vec{v} = M\vec{w}$. We see by inspection that all the entries of the matrix M lie in the field $\mathbb{Q}(iABC)$ and we compute that the determinant of M equals $A^2 - iAB^{-1}C^{-1}$, which is not zero as A, B, and C are positive real numbers. Consequently the system is invertible and $\widehat{I}$, $\widehat{J}$, $\widehat{K}$ can be written as linear combinations of 1, h_a^2, h_b^2, h_c^2 with coefficients in the field $\mathbb{Q}(iABC)$.

Theorem 6.1. *The algebra H is the quaternion algebra $\left(\frac{C^2, B^2}{\mathbb{Q}(iABC)}\right)$.*

Proof. We need to show that H is a vector space of dimension four. Let $\{1^\star, h_a^\star, h_b^\star, h_c^\star\}$ be the dual basis of $\{1, h_a^2, h_b^2, h_c^2\}$ with respect to the trace form on $M(2, \mathbb{C})$ (i.e., the non degenerate bilinear form $(X, Y) \longmapsto \operatorname{tr} XY$). Then given $g \in B^2_{m,n,p}$, $g = a_1 1^\star + a_2 h_a^\star + a_3 h_b^\star + a_4 h_c^\star$, with the coefficients a_i in $\mathbb{C}$. In fact, the a_i belong to O_R. To see that, for example, a_3 belongs to O_R multiply both sides of this equation by h_b^2 and take the trace. We see that $a_3 = \operatorname{tr}(h_b^2 g)$. But we saw in Section 4 that in each of the eleven cases the traces of the elements of $B^2_{m,n,p}$ were algebraic integers in O_R. Thus H, which is a vector space over $\mathbb{Q}(iABC)$, is contained in the $\mathbb{Q}(iABC)$-span of $1^\star$, $h_a^\star$, $h_b^\star$, $h_c^\star$, a vector space of dimension four. So dimension of H is four. We may use 1, $\widehat{I}$, $\widehat{J}$, $\widehat{K}$ as a new basis for the quaternion algebra H. Since $\widehat{I}\widehat{J} = -\widehat{J}\widehat{I}$ and $\widehat{I}^2 = C^2 \cdot 1$ and $\widehat{J}^2 = B^2 \cdot 1$, H is the quaternion algebra

$$\left(\frac{C^2, B^2}{\mathbb{Q}(iABC)}\right). \qquad \square$$

Suppose $\varphi\colon \mathbb{Q}(iABC) \to \mathbb{R}$ is a real embedding of the field $\mathbb{Q}(iABC)$. Let $\widehat{A^2}$, $\widehat{B^2}$, $\widehat{C^2}$ be the images of the elements A^2, B^2, C^2 under the embedding φ.

Then $-A^2B^2C^2$, the square of $iABC$, is sent to a positive real number and $\widehat{A^2}\widehat{B^2}\widehat{C^2}$ is negative.

The numbers $C^2(A^2-1)$, $A^2(B^2-1)$, $B^2(C^2-1)$ are all positive rational numbers so that $\widehat{C^2}(\widehat{A^2}-1)$, $\widehat{A^2}(\widehat{B^2}-1)$, and $\widehat{B^2}(\widehat{C^2}-1)$ are also positive rational.

Since $\widehat{A^2}\widehat{B^2}\widehat{C^2}$ is negative either all three factors are negative or one is negative and the other two are positive. But if, say, $\widehat{A^2}$ and $\widehat{B^2}$ are positive then so is $\widehat{B^2}\widehat{C^2}$ since $\widehat{B^2}(\widehat{C^2}-1)$ is positive. So we see that all three are negative.

It follows that the quaternion algebra $\left(\frac{C^2, B^2}{\mathbb{Q}(iABC)}\right) \otimes_\varphi \mathbb{R} \cong \left(\frac{\widehat{C^2}, \widehat{B^2}}{\mathbb{R}}\right)$ is the quaternion algebra of Hamilton and not $M(2, \mathbb{R})$.

Since in all eleven cases the field $\mathbb{Q}(iABC)$ has exactly one complex place we have the following.

Theorem 6.2. *The field $\mathbb{Q}(iABC)$ has exactly one complex place and the quaternion algebra $H = \left(\frac{C^2, A^2}{\mathbb{Q}(iABC)}\right)$ is ramified at every real place.* $\square$

The next step is to show that the ring O of (6.2) is an order.

Theorem 6.3. *The ring O is an order in the eleven cases of Theorem 4.2.*

Proof. To show that O is an order it suffices to show that O is a ring, (clear from its definition), that O contains O_R, (obvious), that O contains a basis for H over $\mathbb{Q}(iABC)$, ($\{1, h_a^2, h_b^2, h_c^2\}$), and that O is of finite type as an O_R module.

But $O \subset O_R 1^\star + O_R h_a^\star + O_r h_b^\star + O_R h_c^\star$ by the same argument as in the proof of Theorem 6.1. Moreover, the elements $1^\star$, $h_a^\star$, $h_b^\star$, $h_c^\star$ can be written as linear combinations of 1, h_a^2, h_b^2, h_c^2 with coefficients in $\mathbb{Q}(iABC)$. There is a rational integer m such that all the coefficients in these linear combinations lie in the ring O_R, after they have first been multiplied by m. Thus $m(O_R 1^\star + O_R h_a^\star + O_r h_b^\star + O_R h_c^\star) \subset O$, and it follows that O is of finite type. $\square$

Corollary 6.3.1. *In the eleven cases, the group $B^2_{m,n,p}$ is derived from a quaternion algebra and therefore the group $B_{m,n,p}$ is arithmetic.* $\square$

We wish to study the special case $B_{4,4,4}$ further. In this case $A = B = C$ and we have seen that A^2 belongs to the field $\mathbb{Q}(iABC) = \mathbb{Q}(iA^3)$. Thus iA belongs to $\mathbb{Q}(iA^3)$ and $\mathbb{Q}(iA^3) = \mathbb{Q}(iA)$.

In general, for quaternion algebras $(\frac{a,b}{k}) \cong (\frac{ax^2,by^2}{k})$ for any non zero x, y in k. Therefore $(\frac{C^2,B^2}{\mathbb{Q}(iA)}) = (\frac{A^2,A^2}{\mathbb{Q}(iA)}) = (\frac{-(iA)^2-(iA)^2}{\mathbb{Q}(iA)}) = (\frac{-1,-1}{\mathbb{Q}(iA)})$.

Theorem 6.4. *The group $B^2_{4,4,4}$ is derived from the quaternion algebra $\left(\frac{-1,-1}{\mathbb{Q}(iA)}\right)$ where iA is a complex root of the equation $x^4 + x^2 - 1 = 0$.* □

(Remark: We can show that in all eleven cases the quaternion algebra is $\left(\frac{-1,-1}{\mathbb{Q}(iABC)}\right)$. The argument is tedious and it goes case by case so we don't include it. We don't know whether or not this follows from some more general argument, nor do we understand its geometric significance.)

Next we gather some facts about the quaternion algebra $\left(\frac{-1,-1}{\mathbb{Q}(iA)}\right)$.

There are three archimedean valuations of the field $\mathbb{Q}(iA)$, a complex valuation arising from the identity map $\mathbb{Q}(iA) \to \mathbb{C}$, and two real valuations, arising from the maps determined by sending iA to the two real roots of $x^4 + x^2 - 1 = 0$.

A quaternion algebra H over a field k is said to be ***ramified*** at the valuation v if the algebra $H \otimes_k k_v$ is a division algebra over k_v, the completion of k at v. For $H = (\frac{-1,-1}{\mathbb{Q}(iA)})$ the two algebras corresponding to the real valuations are $(\frac{-1,-1}{\mathbb{R}})$, which equal the Hamilton quaternions.

The element $x \cdot 1 + yI + zJ$ has the norm $x^2 + y^2 + z^2$ in $(\frac{-1,-1}{k})$. Consequently the algebra $\left(\frac{-1,-1}{k}\right) \otimes_k k_v$ is unramified if $x^2 + y^2 + z^2 = 0$ has a nontrivial solution in k_v. We shall show this equation has a nontrival solution in the completion of $\mathbb{Q}(iA)$ with respect to any non-archimedean valuation.

Lemma 6.5. *The equation $x^2 + y^2 + z^2 = 0$ has a nontrivial solution in $\mathbb{Q}_p$ for any $p \neq 2$.*

Proof. If -1 is a square in $\mathbb{Q}_p$, say $-1 = x^2$, then $x^2 + 1^2 = 0$ works, so assume that -1 is not a square in $\mathbb{Q}_p$.

By Hensel's lemma, there is a nontrivial solution of $x^2 + y^2 + z^2 = 0$ in $\mathbb{Z}_p$, with at least one of x, y, z a unit, if and only if there is a nontrivial solution of $\bar{x}^2 + \bar{y}^2 + \bar{z}^2 = \bar{0}$ in the residue class field $\mathbb{Z}$ (mod p). Let $B = \{\bar{x}^2 \in \mathbb{Z}(\mathrm{mod}\, p) \mid \bar{x} \neq 0\}$ and let $C = \{-\bar{z}^2 \in \mathbb{Z}(\mathrm{mod}\, p) \mid \bar{z} \neq 0\}$. Then $\sharp B = \sharp C = \frac{1}{2}(p-1)$, and $B \cap C = \emptyset$ (or -1 would be a square). Also let $B + B = \{\bar{x}^2 + \bar{y}^2 \mid \bar{x} \neq 0, \bar{y} \neq 0\}$. Then $\sharp(B+B) \geqq \frac{1}{2}(p-1)$ (or -1 would be a square). If $(B+B) \cap C \neq \emptyset$ we are done, as then the congruence $\bar{x}^2 + \bar{y}^2 + \bar{z}^2$ has a nontrivial solution. If $(B+B) \cap C = \emptyset$, then $B + B = B$, as there are exactly $p-1$ non zero elements of $\mathbb{Z}$ (mod p). But this is absurd as B would then contain $\bar{1}$, $\bar{1} + \bar{1} = \bar{2}$, $\bar{1} + \bar{2} = \bar{3}, \ldots$. □

Corollary 6.5.1. *The algebra $\left(\frac{-1,-1}{k_v}\right)$ is not a division algebra if k_v is the completion of $\mathbb{Q}(iA)$ with respect to the valuation v where v is an extension of the p-adic valuation with $p \neq 2$.*

Proof. k_v contains $\mathbb{Q}_p$. □

We note that $x^2 + y^2 + z^2 = 0$ has no nontrivial solutions in $\mathbb{Q}_2$ because the square of a unit is congruent to zero mod eight.

The 2-adic valuation on $\mathbb{Q}$ has a unique extension to the field $\mathbb{Q}(\sqrt{5})$ because $x^2 - 5$ is irreducible over $\mathbb{Q}_2$. The extension is given by $|a + b\sqrt{5}| = (|a^2 - 5b^2|_2)^{\frac{1}{2}}$.

Lemma 6.6. *$x^2 + y^2 + z^2 = 0$ has a nontrivial solution in $\mathbb{Q}(\sqrt{5})_v$ where v is the unique extension of the 2-adic valuation in $\mathbb{Q}$.*

Proof. $$[\frac{1}{2}(\sqrt{5}-1)]^2 + [\frac{1}{2}(\sqrt{5}+1)]^2 + [\sqrt{5}]^2 = 8 \equiv 0(\mathrm{mod}\, 8)$$

Since $|\sqrt{5}|_v = 1$, and $(|2\sqrt{5}|_v)^2 = \frac{1}{4}$, and $|[\sqrt{5}]^2 + [\frac{1}{2}(\sqrt{5}-1)]^2 + [\frac{1}{2}(\sqrt{5}+1)]^2|_v = \frac{1}{8} < \frac{1}{4}$, by Hensel's lemma the equation $z^2 + [\frac{1}{2}(\sqrt{5}-1)]^2 + [\frac{1}{2}(\sqrt{5}+1)]^2 = 0$ has a nontrivial solution in $\mathbb{Q}(\sqrt{5})_v$. □

Corollary 6.6.1. *$(\frac{-1,-1}{k_v})$ is unramified for v an extension of the 2-adic valuation on $\mathbb{Q}$ to the field $\mathbb{Q}(iA)$.* □

We summarize the preceding in a theorem.

Theorem 6.7. *The quaternion algebra $\left(\frac{-1,-1}{\mathbb{Q}(iA)}\right)$ is ramified exactly at its two real valuations.* □

The ring of algebraic integers O_R of the field $\mathbb{Q}(iA)$ is of interest to us and we wish to explicitly exhibit a $\mathbb{Z}$-basis for O_R.

Lemma 6.8. *Let $\mu = \frac{1}{2}(\sqrt{5}+1)$. A $\mathbb{Z}$-basis for the integers of $\mathbb{Q}(\sqrt{5})$ is $\{1, \mu\}$.*

Proof. A number in a quadratic extension E/F is integral over F if and only if both its norm and trace are integers of F.

Since $t = \mathrm{tr}_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}}(a + b\mu) = 2a + b$ and $N = N_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}}(a + b\mu) = a^2 + ab - b^2$ and $t^2 - 4N = 5b^2$, we see that, if $a + b\mu$ is an integer, then $b \in Z$ and $2a \in Z$. If $a = \frac{m}{2}$ then $2N = 2(\frac{m^2}{4} + \frac{m}{2}b - b^2) \in \mathbb{Z}$ which implies $\frac{1}{2}m^2 \in \mathbb{Z}$, i.e. m is even. Thus a, $b \in \mathbb{Z}$. □

The field $\mathbb{Q}(iA)$ is obtained by adjoining $\sqrt{-\mu}$ to $\mathbb{Q}(\sqrt{5})$ because $\sqrt{-\mu} = i\sqrt{\mu}$, and since $A^4 - A^2 - 1 = 0$ we see that $A^2 = \mu$.

Lemma 6.9. *If $a + b\sqrt{-\mu}$ is an integer of $\mathbb{Q}(iA)$ over $\mathbb{Q}(\sqrt{5})$ with a, $b \in \mathbb{Q}(\sqrt{5})$, then a and b are integers of $\mathbb{Q}(\sqrt{5})$.*

Proof. Let $t = \mathrm{tr}_{\mathbb{Q}(iA)/\mathbb{Q}(\sqrt{5})}(a+b\sqrt{-\mu}) = 2a$ and $N = N_{\mathbb{Q}(iA)/\mathbb{Q}(\sqrt{5})}(a+b\sqrt{-\mu}) = a^2+\mu b^2$. Then t and N are integers of $\mathbb{Q}(\sqrt{5})$ as is $t^2-4N = 4\mu b^2$. But μ is a unit of $\mathbb{Q}(\sqrt{5})$, $(\mu^{-1} = \mu - 1)$, so $4b^2$ is an integer of $\mathbb{Q}(\sqrt{5})$ as is $2b$.

Let $2a = \ell + m\mu$ and $2b = n + p\mu$ with $\ell, m, n, p \in Z$. Using $\mu^2 = 1+\mu$ we compute

$$N = \frac{1}{4}\left[(\ell^2+m^2+2np+p^2) + (2m\ell+m^2+n^2+2np+2p^2)\mu\right].$$

Therefore

(i) $\ell^2+m^2+2np+p^2 \equiv 0 \pmod 4$;

(ii) $2m\ell+m^2+n^2+2np+2p^2 \equiv 0 \pmod 4$.

It's clear from (ii) that m and n have the same parity. If both are even then (i) implies $\ell^2+p^2 \equiv 0 \pmod 4$ which is only possible with ℓ and p even, so all four integers are even.

On the other hand, if m and n are both odd, (i) cannot be satisfied with p even, so p must be odd. If m, n, and p are odd then (i) implies ℓ is even. With these values for ℓ, m, n, and p equation (ii) becomes

$$m^2+n^2+2np+2p^2 \equiv 0 \pmod 4,$$

which isn't satisfied for m, n, p are odd. Thus we have shown that equations (i) and (ii) imply all four integers ℓ, m, n, p are even, which implies a, b are integers in $\mathbb{Q}(\sqrt{5})$. □

Theorem 6.10. *The set $\{1, iA, (iA)^2, (iA)^3\}$ is a $\mathbb{Z}$-basis for $\mathcal{O}_R$.*

Proof. This follows immediately from the preceding lemma, together with the fact that x in $\mathbb{Q}(iA)$ is integral over $\mathbb{Q}$ if it is integral over $\mathbb{Q}(\sqrt{5})$. □

The ring of integers of an algebraic number field is not necessarily a unique factorization domain, or a principal ideal domain. The standard example seems to be $\mathbb{Q}(\sqrt{-5})$ where 6 has the factorizations $2\cdot 3$ and $(1+\sqrt{-5})(1-\sqrt{-5})$.

However the ring O_R is in fact a Euclidean domain, which implies it is both a unique factorization domain and a principal ideal domain. This has been known to algebraic number theorists for a long time, but we shall present a proof anyway, because an explicit algorithm might prove useful, for example in decision problems about 3-manifolds.

Before describing the algorithm, we establish some elementary propositions using calculus.

Proposition 6.11. *Let $f(x,y) = x^2+xy-y^2$. Then $|f(x,y)| \leqq \frac{245}{256}$ on the rectangle $|x|$, $|y| \leqq 7/8$.*

Proof. (Calculus). The gradient vanishes only at $(0,0)$ where $f=0$, so the maximum and minimum are attained on the boundary. Since $f(a,b) = f(-a,-b)$ and $f(-a,b) = -f(b,a)$ we only need to check one side. We see that $g(y) = f(\frac{7}{8}, y) = \frac{5}{4}(\frac{7}{8})^2 - (y - \frac{7}{16})^2$ and $\frac{5}{4}(\frac{7}{8})^2 = \frac{245}{256}$. □

Proposition 6.12. *Let*

$$f(x,y) = (x-1+y)^2+y^2,$$
$$g(x,y) = (x-1+y)^2-(x-1)^2,$$
$$h(x,y) = (x-1+y)^2-y^2.$$

Then $0 \leqq f(x,y) \leqq \frac{1}{2}$ and $\frac{-3}{4} \leqq g(x,y)$, $h(x,y) \leqq \frac{1}{4}$ for (x,y) in the triangle $x+y \geqq \frac{1}{2}$, $0 \leqq x$, $y \leqq \frac{1}{2}$.

Proof. (Calculus). The gradients of f, g, and h do not vanish inside the triangle so its enough to check boundary values, where, in effect, f, g, and h become functions of one variable. It is an easy exercise to find their maxima. □

Proposition 6.13. *Let $Z = (a+b\mu)+(c+d\mu)\sqrt{-\mu} \in \mathbb{Q}(iA)$ with $a,b,c,d \in \mathbb{Q}$. Then*

$$N_{\mathbb{Q}(iA)/\mathbb{Q}(\sqrt{5})}(Z) = (a^2+b^2+(c+d)^2-c^2) + ((a+b)^2-a^2+(c+d)^2+d^2).$$

Proof. This is precisely the same computation that was done in Lemma 6.8.

To show that $\mathbb{Q}(iA)$ has a Euclidean algorithm we must describe how to find an integer X in $\mathbb{Q}(iA)$ given a number x in $\mathbb{Q}(iA)$ such that $|N_{\mathbb{Q}(iA)/\mathbb{Q}}(X-x)| \leqq \delta < 1$.

This is the same as showing how to choose integers $A, B, C, D \in Z$, given $a,b,c,d \in \mathbb{Q}$, such that $|N_{\mathbb{Q}(iA)/\mathbb{Q}}[(A-a)+(B-b)\mu + \{(C-c)+(D-d)\}\sqrt{-\mu}]| \leqq \delta$. We will describe how to do this in the rest of this section. □

Let $\underline{A}$ be the greatest integer less than or equal to a and let $\bar{A}$ be the smallest integer greater than or equal to a, and similarly define $\underline{B}$, $\underline{C}$, $\underline{D}$, $\bar{B}$, $\bar{C}$, $\bar{D}$.

We shall always choose A to be either $\underline{A}$ or $\bar{A}$ and similarly for B, C, D. Let $\widehat{A}$ be either $\underline{A}$ or $\bar{A}$ whichever is nearest to a with $\widehat{A} = \underline{A}$ in case of a tie.

We begin by choosing C and D.

Choose $D = \widehat{D}$ once and for all. Let $y = d - D$ and let $x = c - \widehat{C}$. If x and y have opposite signs or if x and y have the same sign but $|x+y| \leqq \frac{1}{2}$ choose $C = \widehat{C}$. If x and y have opposite signs and $|x+y| > \frac{1}{2}$ choose C to be the other nearest integer, not $\widehat{C}$.

Proposition 6.14.
$$0 \leqq (c-C+d-D)^2+(d-D)^2 \leqq \frac{1}{2},$$
$$\frac{-3}{4} \leqq (c-C+d-D)^2-(c-C)^2 \leqq \frac{1}{4}.$$ □

Proof. In the case where $y = d-D$ and $x = c-C$ have opposite signs or $|x=y| \leqq \frac{1}{2}$ this is clear since $|x|, |y| \leqq \frac{1}{2}$.

In the case where $x = d-D$ and $y = c-C$ have opposite signs and $|x+y| > \frac{1}{2}$, this follows from Proposition 6.11 since $(c-C+d-D)^2 = (1-x+y)^2$. □

Now we choose A and B.

Again set $x = a - \widehat{A}$ and $y = b - \widehat{B}$. Again, if either x and y have opposite signs, or x and y have the same sign and $|x+y| \leqq \frac{1}{2}$, choose $A = \widehat{A}$ and $B = \widehat{B}$. The inequalities $x^2 + y^2 \leqq \frac{1}{2}$ and $\frac{-1}{4} \leqq (x+y)^2 - x^2$ are satisfied.

Suppose x and y have the same sign but $|x+y| > \frac{1}{2}$. Observe that the triangle $0 \leqq x,\ y \leqq \frac{1}{2},\ x + y \geqq \frac{1}{2}$ is contained in the union of the two discs $x^2 + (1-y)^2 \leqq \frac{5}{8}$, $(1-x)^2 + y^2 \leqq \frac{5}{8}$. If the first inequality is satisfied, set $A = \widehat{A}$ and B equals the second nearest integer to b. If the first inequality is not satisfied, the second will be. Then set $B = \widehat{B}$ and A equals the 'second nearest' integer.

Proposition 6.15.
$$0 \leqq (a-A)^2 + (b-B)^2 \leqq \frac{5}{8},$$
$$\frac{-3}{4} \leqq (a - A + b - B)^2 - (a-A)^2 \leqq \frac{1}{4}.$$

Proof. The first inequality follows easily from the choices of A and B and the second follows from Proposition 6.11. □

Theorem 6.16.
$$\left| N_{\mathbb{Q}(iA)/\mathbb{Q}} \left[(a-A) + (b-B)\mu + \{(c-C) + (d - D\mu)\} \sqrt{-\mu} \right] \right| \leqq \frac{245}{256}.$$

The ring O_R is a Euclidean domain, unique factorization domain, and principal ideal domain.

Proof. The inequality follows directly from the formula for the norm (Proposition 6.12), the inequalities in Propositions 6.14 and 6.15, from
$$N_{\mathbb{Q}(iA)/\mathbb{Q}} = N_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}} \cdot N_{\mathbb{Q}(iA)/\mathbb{Q}(\sqrt{5})},$$
and Proposition 6.10.

The second statement follows from the fact that a Euclidean domain is both a principal ideal domain and unique factorization domain. □

Appendix. The non arithmeticity properties using Reid's criterion

For its potential geometric significance we shall prove the following proposition using Reid's criterion.

Proposition. *If one of the indices m, n, p is not equal to 3, 4, 6, or ∞, the field $K_2 = \mathbb{Q}(\mathrm{tr}(g) \mid g \in B^2_{m,n,p})$ has more than one complex place. In this case $B_{m,n,p}$ is not arithmetic.*

Proof. Suppose that one of m, n, p, say it is m, is not equal to 3, 4, 6, or ∞. Let j be an integer prime to m and in the interval $(1, m/2)$.

Using the fact that the arithmetic series $\{j + im \mid i \geqq 0\}$ contains infinitely many primes (Dirichlet's Theorem), we choose one, $q = j + im$, which also is prime to n and p. Let k' and ℓ' be (the unique) integers such that:
$$q \equiv k' \bmod n, \quad |k'| \in [1, n/2),$$
$$q \equiv \ell' \bmod p, \quad |\ell'| \in [1, p/2),$$
and let us denote $|k'|$ and $|\ell'|$ by k and ℓ respectively.

Note that $\cos\frac{2\pi}{m}q = \cos\frac{2\pi}{m}j$, $\cos\frac{2\pi}{n}q = \cos\frac{2\pi}{n}k$, and $\cos\frac{2\pi}{p}q = \cos\frac{2\pi}{p}\ell$. Let c be the least common multiple of m, n, and p.

Next, apply the non trivial automorphism θ_q, which sends $\cos\frac{2\pi}{c}$ to $\cos\frac{2\pi q}{c}$, to the field k, using the integer q that we have just defined. This automorphism induces one or more non trivial embeddings of the field $K_2 = k(iABC)$ in $\mathbb{C}$ or in $\mathbb{R}$. These embeddings are found as follows.

The numbers A, B, and C satisfy the following system of equations
$$\begin{aligned} C^2(A^2 - 1) &= \tan^2\frac{\pi}{m}, \\ A^2(B^2 - 1) &= \tan^2\frac{\pi}{n}, \\ B^2(C^2 - 1) &= \tan^2\frac{\pi}{p}. \end{aligned} \tag{A.1}$$

The number $A^2B^2C^2$ satisfies the following equation, which is found by eliminating the terms A^2B^2, A^2C^2, and B^2C^2 from (A.1) and multiplying the three resulting equations together:
$$\begin{aligned} &(A^2B^2C^2 - \tan^2\frac{\pi}{m})(A^2B^2C^2 - \tan^2\frac{\pi}{n})(A^2B^2C^2 - \tan^2\frac{\pi}{p}) = \\ &\qquad A^2B^2C^2(1 + \tan^2\frac{\pi}{m})(1 + \tan^2\frac{\pi}{n})(1 + \tan^2\frac{\pi}{p}). \end{aligned} \tag{A.2}$$

Apply the automorphism/embedding θ_q to the elements on the right hand side of (A.2) obtaining a new set of equations with the right hand sides replaced by $\tan^2\frac{\pi}{m}j$, $\tan^2\frac{\pi}{n}k$, $\tan^2\frac{\pi}{p}\ell$.

Because $0 < \frac{\pi}{m}j,\ \frac{\pi}{n}k,\ \frac{\pi}{p}\ell < \frac{\pi}{2}$, Proposition 3.1 guarantees us that there are solutions of the new equations, $\widehat{A}$, $\widehat{B}$, $\widehat{C}$, in which the numbers $\widehat{A}^2$, $\widehat{B}^2$, $\widehat{C}^2$ and therefore $\widehat{A}^2\widehat{B}^2\widehat{C}^2$ are real and positive.

The number $i\widehat{A}\widehat{B}\widehat{C}$ has negative, non zero square and so is pure imaginary. It solves a sixth degree equation (obtained by applying θ_q to the coefficients of (A.2)) with coefficients in k. Consequently the embedding θ_q of k extends to a necessarily complex embedding of $k(iABC)$ in $\mathbb{C}$. Since $k(iABC) = K_2$, the field K_2 has more than one complex place. This proves the proposition. □

References

[Bi] L. Bianchi, Sui gruppi di sostituzioni lineari con coefficienti appartenenti a corpi quadratici immaginari, Math. Ann. 40 (1892), 332–412.

[B] A. Borel, Commensurability classes and volumes of hyperbolic 3-manifolds, Ann. Scuola Norm. Sup. Pisa 8 (1981), 1–33.

[B1] A. Borel, Density and maximality of arithmetic subgroups, J. Reine Angew. Math. 224 (1966), 78–89.

[BH] A. Borel, Harish-Chandra, Arithmetic subgroups of algebraic groups, Ann. of Math. 75 (1962), 485–535.

[F] W. Fenchel, "Elementary Geometry in Hyperbolic Space", Stud. Math. 11, Walter de Gruyter, Berlin (1989).

[HKM] H. Helling, A. C. Kim, J. L. Mennicke, On Fibonacci groups, (to appear).

[HLM1] H. M. Hilden, M. T. Lozano, J. M. Montesinos, On knots that are universal, Topology 24 (1985), 499–504.

[HLM2] H. M. Hilden, M. T. Lozano, J. M. Montesinos, On the universal group of the Borromean rings, in "Proceedings of the 1987 Siegen conference on Differential Topology", ed. U. Koschorke. LNM 1350, Springer Verlag (1988), 1-13.

[HLM3] H. M. Hilden, M. T. Lozano, J. M. Montesinos, The arithmeticity of the figure eight knot orbifolds, (these Proceedings).

[HLMW] H. M. Hilden, M.T. Lozano, J. M. Montesinos, W. C. Whitten, On universal groups and three manifolds, Inventiones mathematicae 87 (1987), 441–456.

[Ho] C. D. Hodgson, Degeneration and regeneration of geometric structures on 3-manifolds, Ph.D. Thesis, Princeton (1986).

[M] Maclachlan C., A. Reid, Commensurability classes of arithmetic Kleinian groups and their Fuchsian subgroups, Math. Proc. Camb. Phil. Soc. 102 (1987), 251–257.

[Ma] W. Magnus, Rings of Fricke characters and automorphism groups of free groups, Math. Z. 170 (1980), 91–103.

[R] A. W. Reid, Arithmetic Kleinian groups and their Fuchsian subgroups, Ph.D. Thesis (1987), University of Aberdeen (part is in [M]).

[R1] A. W. Reid, Arithmetic Fuchsian groups: a survey, Master of Science Th., Aberdeen (1985).

[Re] N. Reid, "Undergraduate algebraic geometry", London Math. Society Student Texts 12, Cambridge University Press (1988).

[S] H. P. F. Swinnerton-Dyer, Arithmetic groups, in "Discrete groups and automorphic functions", ed. W. J. Harvey, London: Academic Press (1977), 307–401.

[T1] K. Takeuchi, On some discrete subgroups of $SL(2,\mathbb{R})$, J. Fac. Sci. Univ. Tokyo Sec 1, 16 (1969), 97–100.

[T2] K. Takeuchi, A characterization of arithmetic Fuchsian groups, J. Math Soc. Japan 27 (1975), 600–612.

[T3] K. Takeuchi, Arithmetic triangle groups, J. Math. Soc. Japan 29 (1977), 91–106.

[T4] K. Takeuchi, Arithmetic Fuchsian groups of signature (1; e), J. Math. Soc. Japan 35 (1983).

[Th] W. Thurston, The geometry and topology of 3-manifolds, Lecture Notes, Princeton University 1978.

[V] M. F. Vigneras, "Arithmetique des Algèbres de Quaternions", LNM 800, Springer Verlag (1980).

[Vi] E. B. Vinberg, Discrete groups generated by reflections in Lobachevskii space, Math Sb. 114 (1967), 471–488.

[Vo] H. Vogt, Sur les invariants fondamentaux des équations differentielle linéaire du second ordre, Ann. Sci. Ecole Norm Sup. (3) 6 Suppl. 3-72 (1889) Thèse. Paris.

[Z] Robert J. Zimmer, "Ergodic theory and semi simple groups", Birkhauser (1984).

Department of Mathematics, University of Hawaii at Manoa, Honolulu, HI 96822

Department of Mathematics, University of Zaragoza, 50009 Zaragoza, Spain

Department of Mathematics, Universidad Complutense, 28040 Madrid, Spain