JOURNAL DE THÉORIE DES NOMBRES DE BORDEAUX

TED CHINBURG

EDUARDO FRIEDMAN

Hilbert symbols, class groups and quaternion algebras

Journal de Théorie des Nombres de Bordeaux, tome 12, nº 2 (2000), p. 367-377

<http://www.numdam.org/item?id=JTNB_2000__12_2_367_0>

Journal de Théorie des Nombres
de Bordeaux **12** (2000), 367–377

Hilbert symbols, class groups and quaternion algebras

par TED CHINBURG* et EDUARDO FRIEDMAN**

To Jacques Martinet

RÉSUMÉ. Soit B une algèbre de quaternions définie sur un corps de nombres k. Nous associons à tout couple de symboles de Hilbert $\{a, b\}$ et $\{c, d\}$ pour B un invariant $\rho = \rho_R\big([\mathcal{D}(a, b)], [\mathcal{D}(c, d)]\big)$ dans un quotient du groupe des classes au sens restreint de k. Cet invariant a son origine dans l'étude des sous-groupes finis d'un groupe kleinien arithmétique maximal. Il mesure la distance entre les ordres $\mathcal{D}(a, b)$ et $\mathcal{D}(c, b)$ dans B associés à $\{a, b\}$ et $\{c, d\}$. Si $a = c$, nous calculons $\rho_R([\mathcal{D}(a, b)], [\mathcal{D}(c, d)])$ en termes de l'arithmétique du corps $k(\sqrt{a})$. Le problème d'étendre ce calcul au cas général conduit à l'étude d'un graphe fini lié aux différents symboles de Hilbert pour B. Nous considérons en détail un exemple issu de la détermination de la plus petite variété hyperbolique arithmétique de dimension trois.

ABSTRACT. Let B be a quaternion algebra over a number field k. To a pair of Hilbert symbols $\{a, b\}$ and $\{c, d\}$ for B we associate an invariant $\rho = \rho_R([\mathcal{D}(a, b)], [\mathcal{D}(c, d)])$ in a quotient of the narrow ideal class group of k. This invariant arises from the study of finite subgroups of maximal arithmetic Kleinian groups. It measures the distance between orders $\mathcal{D}(a, b)$ and $\mathcal{D}(c, d)$ in B associated to $\{a, b\}$ and $\{c, d\}$. If $a = c$, we compute $\rho_R([\mathcal{D}(a, b)], [\mathcal{D}(c, d)])$ by means of arithmetic in the field $k(\sqrt{a})$. The problem of extending this algorithm to the general case leads to studying a finite graph associated to different Hilbert symbols for B. An example arising from the determination of the smallest arithmetic hyperbolic 3-manifold is discussed.

Manuscrit reçu le 28 février 2000.
* Partially supported by NSF grant DMS97-01411.
** Research partially supported by FONDECYT grant 198-1170 and by a Chilean Presidential Chair grant.

1. Introduction

Two non-zero elements a and b of a number field k determine a quaternion algebra $B = B(a,b)$ with center k, namely the 4-dimensional k-algebra with k-basis 1, x, y and xy with the multiplicative relations

$$(1.1) \qquad x^2 = a, \qquad y^2 = b, \qquad xy = -yx.$$

Since there are many other pairs c and d in k determining the same algebra $B = B(a,b)$, it is natural to ask whether there is any interesting structure on the set of pairs determining isomorphic quaternion algebras.

Motivated by a problem in arithmetic hyperbolic 3-orbifolds, we consider the B^*-conjugacy class of an order $\mathcal{D} = \mathcal{D}(a,b)$ closely related to the ring $\mathcal{O}_k[x,y] \subset B$.

To define $\mathcal{D}$, we replace $\mathcal{O}_k[x,y]$ by a maximal order over a Dedekind domain $\mathcal{O}_k^R$, where $\mathcal{O}_k^R$ is obtained from $\mathcal{O}_k$ by inverting a finite set R of primes ideals of $\mathcal{O}_k$. Namely,

$$(1.2) \qquad R = R(a,b) := \mathrm{Ram}_{\mathfrak{f}}(B) \cup \{\text{dyadic primes}\} \cup \mathrm{Odd}(a,b),$$

where $\mathrm{Ram}_{\mathfrak{f}}(B)$ is the set of prime ideals of $\mathcal{O}_k$ at which B ramifies, the dyadic primes are all those above the rational prime 2, and $\mathrm{Odd}(a,b)$ consists of the prime ideals $\mathfrak{p}$ at which $\mathrm{ord}_{\mathfrak{p}}(a)$ or $\mathrm{ord}_{\mathfrak{p}}(b)$ is odd, the valuation $\mathrm{ord}_{\mathfrak{p}}$ being normalized so that its value group is $\mathbb{Z}$. Let $\mathcal{O}_{\mathfrak{p}}$ and $k_{\mathfrak{p}}$ be the $\mathfrak{p}$-completions of $\mathcal{O}_k$ and k, respectively. For $\mathfrak{p} \notin R$, $\mathrm{ord}_{\mathfrak{p}}(a)$ and $\mathrm{ord}_{\mathfrak{p}}(b)$ are even integers, so we let

$$(1.3) \qquad \hat{x}_{\mathfrak{p}} = c_{\mathfrak{p}} x, \qquad \hat{y}_{\mathfrak{p}} = d_{\mathfrak{p}} y,$$

where $c_{\mathfrak{p}}$ and $d_{\mathfrak{p}}$ in $k_{\mathfrak{p}}$ are such that $\mathrm{ord}_{\mathfrak{p}}\big(\mathrm{nr}(\hat{x}_{\mathfrak{p}})\big) = \mathrm{ord}_{\mathfrak{p}}\big(\mathrm{nr}(\hat{y}_{\mathfrak{p}})\big) = 0$, where nr is the reduced norm. We can choose $\hat{x}_{\mathfrak{p}} = x$ and $\hat{y}_{\mathfrak{p}} = y$ for all but finitely many $\mathfrak{p}$. Note that the subsets $\mathcal{O}_{\mathfrak{p}}\hat{x}_{\mathfrak{p}}$ and $\mathcal{O}_{\mathfrak{p}}\hat{y}_{\mathfrak{p}}$ of $B_{\mathfrak{p}} := B \otimes_k k_{\mathfrak{p}}$ do not depend on the choice of $c_{\mathfrak{p}}$ or $d_{\mathfrak{p}}$. We define the $\mathcal{O}_k^R$-order $\mathcal{D} = \mathcal{D}(a,b) \subset B$ by requiring that its completions $\mathcal{D}_{\mathfrak{p}} = \mathcal{D} \otimes_{\mathcal{O}_k} \mathcal{O}_{\mathfrak{p}}$ be given by

$$(1.4) \qquad \mathcal{D}_{\mathfrak{p}} = \mathcal{D}(a,b)_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}[\hat{x}_{\mathfrak{p}}, \hat{y}_{\mathfrak{p}}], \qquad (\mathfrak{p} \notin R).$$

Then $\mathcal{D}$ is a maximal $\mathcal{O}_k^R$-order of B since the reduced discriminant [V, p. 24] of $\mathcal{O}_{\mathfrak{p}}[\hat{x}_{\mathfrak{p}}, \hat{y}_{\mathfrak{p}}]$ is readily computed to be $4\hat{x}_{\mathfrak{p}}^2\hat{y}_{\mathfrak{p}}^2\mathcal{O}_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}$.

The Skolem-Noether theorem [R, p. 103] shows that x and y in (1.1) are uniquely determined by a and b, up to conjugation by an element of B^*. Thus, starting from a and b in k^* we have obtained a conjugacy class $[\mathcal{D}(a,b)]$ of maximal $\mathcal{O}_k^R$-orders. Note that, again by the Skolem-Noether theorem, the $\mathcal{O}_k^R$-isomorphism class of an order $\mathcal{D} \subset B$ coincides with its B^*-conjugacy class, usually known as its type.

We will assume from now on the

Eichler condition. B is unramified at some archimedean place of k.

Then the set of conjugacy types of maximal $\mathcal{O}_k^R$-orders is classically known to be in non-canonical bijection with the group $T_R(B)$ of fractional $\mathcal{O}_k^R$-ideals of k modulo the subgroup generated by squares of fractional ideals and by principal ideals $(\alpha) = \alpha\mathcal{O}_k^R$ such that $\alpha \in k^*$ and $\alpha > 0$ at all real places that ramify in B [V, p. 89] [CF1, Lemma 3.2].

Although the map from a, b to the type $[\mathcal{D}(a,b)]$ seems quite interesting to us, it is hard to describe because there is no canonical description of types. In particular, it is not even clear what one would mean by computing this map. However, given two types $[\mathcal{D}]$ and $[\mathcal{E}]$ of maximal orders $\mathcal{O}_k^R$-orders of B, there is a canonical R-distance $\rho_R([\mathcal{D}], [\mathcal{E}]) \in T_R(B)$, which is the image in $T_R(B)$ of the order-ideal [R, p. 49] $\rho(\mathcal{D}, \mathcal{E})$ of the finite $\mathcal{O}_k^R$-module $\mathcal{D}/(\mathcal{E} \cap \mathcal{D})$. Under the Eichler condition, it is known [V, p. 89] [CF1, Lemma 3.2] that two $\mathcal{O}_k^R$-orders $\mathcal{D}$ and $\mathcal{E}$ are B^*-conjugate (or, equivalently, isomorphic) if and only if the R-distance between them is trivial. In fact, the non-canonical bijection mentioned above is obtained by arbitrarily fixing some type $[\mathcal{E}]$ and mapping $[\mathcal{D}]$ to $\rho_R([\mathcal{D}], [\mathcal{E}])$.

We can now state our

Main Problem. *Compute the map that takes two pairs (a,b) and (c,d), assuming $B(a,b) \cong B(c,d)$, to $\rho_R\big([\mathcal{D}(a,b)], [\mathcal{D}(c,d)]\big) \in T_R(B)$, where $R = R(a,b) \cup R(c,d)$ (see (1.1) to (1.4) for notation).*

Here we regard the $\mathcal{O}_k^{R(a,b)}$-order $\mathcal{D}(a,b)$ as an $\mathcal{O}_k^R$-order by inverting ideals in $R - R(a,b)$, and similarly for $\mathcal{D}(c,d)$. The Eichler condition is tacitly assumed.

In this generality, we have no idea how to solve the main problem. We present here a solution of sorts in the special case $a = c$.

Theorem. *Suppose a, b and d are elements of a number field k such that the quaternion algebras over k corresponding to (a,b) and (a,d) coincide. Suppose also that this algebra B satisfies the Eichler condition and let $R = R(a,b) \cup R(a,d)$.*

If $a \in k^{*2}$, then $bd\mathcal{O}_k^R = \mathfrak{q}^2$ and $\rho_R\big([\mathcal{D}(a,b)], [\mathcal{D}(a,d)]\big)$ is the class in $T_R(B)$ of the fractional $\mathcal{O}_k^R$-ideal $\mathfrak{q}$.

Assume now that $a \notin k^{*2}$, and let $K = k(\sqrt{a})$. Then $\rho_R\big([\mathcal{D}(a,b)], [\mathcal{D}(a,d)]\big)$ is the class in $T_R(B)$ of $Norm_{K/k}(\mathfrak{a})$, where the fractional $\mathcal{O}_K^R$-ideal $\mathfrak{a}$ is found by taking any $z \in K$ such that $Norm_{K/k}(z) = bd$, and writing $z\mathcal{O}_K^R = \mathfrak{a}^{1-\sigma}\mathfrak{c}$. Here σ is the non-trivial element of $Gal(K/k)$ and $\mathfrak{c}$ is the extension to K of a fractional $\mathcal{O}_k^R$-ideal of k.

We shall see that the existence of z as above follows from the assumption $B(a,b) \cong B(a,d)$. By $\mathcal{O}_K^R$ we mean the integral closure of $\mathcal{O}_k^R$ in K.

In §2 we give a proof of the Theorem. In §3 we show how to apply the Theorem to the computation of torsion subgroups of arithmetic Kleinian groups. We also give a numerical example in which k is a sextic field, showing that one can sometimes avoid having to find $z \in K$ by computing instead inside a narrow ideal class group of K.

We now turn to a curious finite graph whose definition is suggested by the Theorem. Suppose $B(a,b) \cong B(c,d)$, and define $R = R(a,b) \cup R(c,d)$. We would like to compute $\rho_R\big([\mathcal{D}(a,b)],[\mathcal{D}(c,d)]\big)$. The Theorem does not apply directly if (a,b) and (c,d) have no common entry. However, note that

$$\rho_R([\mathcal{D}_1],[\mathcal{D}_N]) = \sum_{i=1}^{N-1} \rho_R([\mathcal{D}_i],[\mathcal{D}_{i+1}]), \tag{1.5}$$

where the $\mathcal{D}_i$ $(1 \le i \le N)$ are any N maximal $\mathcal{O}_k^R$-orders of B (cf. [V, ch. II, §2] or [CF1, eq. (3.1)]). Suppose there are pairs (a,e) and (e,d) such that $B(a,b) \cong B(a,e) \cong B(e,d)$ and that $\mathrm{ord}_\mathfrak{p}(e)$ is even for $\mathfrak{p} \notin R$. Then $R(a,e)$ and $R(e,d)$ are contained in $R = R(a,b) \cup R(c,d)$. From (1.5) we obtain $\rho_R\big([\mathcal{D}(a,b)],[\mathcal{D}(c,d)]\big)$ as

$$\rho_R\big([\mathcal{D}(a,b)],[\mathcal{D}(a,e)]\big) + \rho_R\big([\mathcal{D}(a,e)],[\mathcal{D}(e,d)]\big) + \rho_R\big([\mathcal{D}(e,d)],[\mathcal{D}(c,d)]\big),$$

where each term can be computed by the Theorem.

This suggests defining a graph as follows. Fix a quaternion algebra B and a finite set R of primes of k containing all finite primes ramified in B and all primes above 2. Start with all pairs $(a,b) \in k^* \times k^*$ such that $B \cong B(a,b)$ and $R(a,b) \subset R$, *i. e.*, a and b are even at $\mathfrak{p}$ if $\mathfrak{p} \notin R$. We should make some further identifications since, as $\mathcal{O}_k^R$-orders,

$$\mathcal{D}(a,b) \cong \mathcal{D}(b,a) \cong \mathcal{D}(a,-ab) \cong \mathcal{D}(e^2a, f^2b), \tag{1.6}$$

for any e and f in k^*. The first isomorphism is clear from (1.1) on switching x and y, the second on replacing y by xy and observing that $(xy)^2 = -ab$ has even valuation for $\mathfrak{p} \notin R$. The last isomorphism in (1.6) follows from (1.3), since $\widehat{x}_\mathfrak{p} = \widehat{ex}_\mathfrak{p}$ and $\widehat{y}_\mathfrak{p} = \widehat{fy}_\mathfrak{p}$.

For the purpose of computing $[\mathcal{D}(a,b)]$, we may therefore identify $(a,b) \sim (b,a) \sim (a,-ab) \sim (e^2a, f^2b)$ for e and f in k^*. We let $\{a,b\}$ be the equivalence class of (a,b) under the transitive closure of the above relation $\sim$, with B and R fixed.

Define the vertices of the graph $G = G(B,R)$ to be the set of classes $\{a,b\}$. This is a finite, possibly empty, set since the extension $k(\sqrt{a})/k$, which determines a modulo squares, is one of finitely many extensions K/k unramified outside R with $[K:k] \le 2$.

Two vertices $\{a,b\}$ and $\{c,d\}$ are connected by an edge whenever these equivalence classes have, respectively, representatives of the form (a',b') and (a',d'). In other words, we connect two vertices whenever the Theorem allows us to compute ρ_R of the corresponding types.

The motivation for defining G is that successive application of the Theorem and of (1.5) allows us to compute the R-distance between any types corresponding to the same connected component of the graph G.

When B is the matrix algebra $\mathrm{M}_2(k)$, G is connected for rather trivial reasons. Indeed, if $B(a,b) \cong B(c,d) \cong \mathrm{M}_2(k)$, then

$$\{a,b\},\ \{a,1\},\ \{1,d\},\ \{c,d\}$$

is a path in G from $\{a,b\}$ to $\{c,d\}$. In some other simple cases G is also connected, but we do not see why this should hold in general. As long as one cannot solve the main problem above, it would be interesting to compute the number of connected components of G.

2. Proof of Theorem

We now prove the first assertion in the Theorem. Namely,

If $a \in k^{*2}$, then $bd\mathcal{O}_k^R = \mathfrak{q}^2$ and $\rho_R\big([\mathcal{D}(a,b)],[\mathcal{D}(a,d)]\big)$ is the class in $T_R(B)$ of the fractional $\mathcal{O}_k^R$-ideal $\mathfrak{q}$.

By (1.2), for $\mathfrak{p} \notin R$ we have $\mathrm{ord}_\mathfrak{p}(b) = 2r_\mathfrak{p}$ and $\mathrm{ord}_\mathfrak{p}(b) = 2s_\mathfrak{p}$ for some $r_\mathfrak{p},\ s_\mathfrak{p} \in \mathbb{Z}$. Hence

$$bd\mathcal{O}_k^R = \prod_{\mathfrak{p}\notin R} \mathfrak{p}^{2(s_\mathfrak{p}+r_\mathfrak{p})} = \mathfrak{q}^2.$$

Recall that we are assuming $B(a,b) \cong B(a,d)$. Since $a \in k^{*2}$, $B(a,b) = B(a,d) = \mathrm{M}_2(k)$. By (1.6), we might as well assume $a = 1$. Now, since the elements x and y of B satisfying (1.1) are uniquely determined up to B^*-conjugacy by a and b (as follows from the Skolem-Noether theorem [R, p. 103]), we can assume

$$x = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad y = \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}.$$

Let $\pi_\mathfrak{p} \in \mathcal{O}_k$ satisfy $\mathrm{ord}_\mathfrak{p}(\pi_\mathfrak{p}) = 1$. Then in (1.3),

$$\widehat{x}_\mathfrak{p} = x = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad \widehat{y}_\mathfrak{p} = \begin{pmatrix} 0 & \pi_\mathfrak{p}^{r_\mathfrak{p}} u_\mathfrak{p} \\ \pi_\mathfrak{p}^{-r_\mathfrak{p}} v_\mathfrak{p} & 0 \end{pmatrix}, \tag{2.1}$$

for some local units $u_\mathfrak{p}, v_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}^*$. Recall that $\mathcal{D}(1,b)_\mathfrak{p}$ in (1.4) is defined as $\mathcal{O}_\mathfrak{p} + \mathcal{O}_\mathfrak{p}\widehat{x}_\mathfrak{p} + \mathcal{O}_\mathfrak{p}\widehat{y}_\mathfrak{p} + \mathcal{O}_\mathfrak{p}\widehat{x}_\mathfrak{p}\widehat{y}_\mathfrak{p}$. A short calculation using (2.1) shows that

$$\mathcal{D}(1,b)_\mathfrak{p} = \begin{pmatrix} \mathcal{O}_\mathfrak{p} & \pi_\mathfrak{p}^{r_\mathfrak{p}}\mathcal{O}_\mathfrak{p} \\ \pi_\mathfrak{p}^{-r_\mathfrak{p}}\mathcal{O}_\mathfrak{p} & \mathcal{O}_\mathfrak{p} \end{pmatrix}, \tag{2.2}$$

where we used the fact that $\mathfrak{p} \notin R$ cannot be above 2, by (1.2).

Similarly,

$$\mathcal{D}(1,d)_\mathfrak{p} = \begin{pmatrix} \mathcal{O}_\mathfrak{p} & \pi_\mathfrak{p}^{s_\mathfrak{p}}\mathcal{O}_\mathfrak{p} \\ \pi_\mathfrak{p}^{-s_\mathfrak{p}}\mathcal{O}_\mathfrak{p} & \mathcal{O}_\mathfrak{p} \end{pmatrix}. \tag{2.3}$$

From (2.2) and (2.3) we obtain

$$\mathcal{D}(1,b)_{\mathfrak{p}} \cap \mathcal{D}(1,d)_{\mathfrak{p}} = \begin{pmatrix} \mathcal{O}_{\mathfrak{p}} & \pi_{\mathfrak{p}}^{\max(s_{\mathfrak{p}},r_{\mathfrak{p}})}\mathcal{O}_{\mathfrak{p}} \\ \pi_{\mathfrak{p}}^{-\min(s_{\mathfrak{p}},r_{\mathfrak{p}})}\mathcal{O}_{\mathfrak{p}} & \mathcal{O}_{\mathfrak{p}} \end{pmatrix}.$$

Hence the finite $\mathcal{O}_{\mathfrak{p}}$-module $\mathcal{D}(1,b)_{\mathfrak{p}}/\big(\mathcal{D}(1,b)_{\mathfrak{p}} \cap \mathcal{D}(1,d)_{\mathfrak{p}}\big)$ is isomorphic to $\mathcal{O}_{\mathfrak{p}}/\pi_{\mathfrak{p}}^{\pm(s_{\mathfrak{p}}-r_{\mathfrak{p}})}\mathcal{O}_{\mathfrak{p}}$, the sign being chosen so that the exponent of $\pi_{\mathfrak{p}}$ is non-negative.

We have thus found that $\rho_R\big([\mathcal{D}(a,b)],[\mathcal{D}(a,d)]\big)$ is the class in $T_R(B)$ of the ideal $\prod_{\mathfrak{p}\notin R}\mathfrak{p}^{\pm(s_{\mathfrak{p}}-r_{\mathfrak{p}})}$. As $T_R(B)$ has exponent 2, $\rho_R\big([\mathcal{D}(a,b)],[\mathcal{D}(a,d)]\big)$ is also the class in $T_R(B)$ of $\mathfrak{q} = \prod_{\mathfrak{p}\notin R}\mathfrak{p}^{(s_{\mathfrak{p}}+r_{\mathfrak{p}})}$, which proves the first claim in the Theorem.

We now turn to the second assertion in the Theorem.

Assume that $a \notin k^{*2}$, and let $K = k(\sqrt{a})$. Then $\rho_R\big([\mathcal{D}(a,b)],[\mathcal{D}(a,d)]\big)$ is the class in $T_R(B)$ of $\mathrm{Norm}_{K/k}(\mathfrak{a})$, where the fractional $\mathcal{O}_K^R$-ideal $\mathfrak{a}$ is found by taking any $z \in K$ such that $\mathrm{Norm}_{K/k}(z) = bd$, and writing $z\mathcal{O}_K^R = \mathfrak{a}^{1-\sigma}\mathfrak{c}$. Here σ is the non-trivial element of Gal(K/k) and $\mathfrak{c}$ is the extension to K of a fractional $\mathcal{O}_k^R$-ideal of k.

We note that while $\mathfrak{a}$ in the factorization $z\mathcal{O}_K^R = \mathfrak{a}^{1-\sigma}\mathfrak{c}$ is not unique, the class of $\mathrm{Norm}_{K/k}(\mathfrak{a})$ in $T_R(B)$ is unambiguously defined. Indeed, suppose $\mathrm{Norm}_{K/k}(z') = bd$ and $z'\mathcal{O}_K^R = \mathfrak{a}'^{1-\sigma}\mathfrak{c}'$. Taking the norm to k, we find $\mathfrak{c}^2 = \mathfrak{c}'^2$, where for convenience we do not distinguish notationally between $\mathfrak{c}$ and $\mathfrak{c}\cap\mathcal{O}_k^R$. Hence $\mathfrak{c} = \mathfrak{c}'$ and $(\mathfrak{a}'\mathfrak{a}^{-1})^{1-\sigma} = (z'/z)\mathcal{O}_K^R$. Since $\mathrm{Norm}_{K/k}(z'/z) = 1$, and K/k is quadratic, Hilbert's Theorem 90 shows that that $z'/z = \gamma^{1-\sigma}$ for some $\gamma \in K^*$. Thus $(\mathfrak{a}'\mathfrak{a}^{-1}\gamma^{-1})^{1-\sigma} = \mathcal{O}_k^R$. Since R contains all the primes of k which ramify in K, we conclude from this that $\mathfrak{a}'\mathfrak{a}^{-1}\gamma^{-1} = \mathfrak{c}^{\dagger}\mathcal{O}_k^R$ for some ideal $\mathfrak{c}^{\dagger}$ of k. Hence $\mathrm{Norm}_{K/k}(\mathfrak{a}'\mathfrak{a}^{-1}) = (\mathfrak{c}^{\dagger})^2\mathrm{Norm}_{K/k}(\gamma)$. Recall that by the definition of $T_R(B)$, a principal $\mathcal{O}_k^R$-ideal (α) has trivial class in $T_R(B)$ if $\alpha > 0$ at all real places of k ramified in B. Since $K = k(\sqrt{a})$ embeds in B, for any $\beta \in K^*$ the class of $\big(\mathrm{Norm}_{K/k}(\beta)\big)$ is trivial in $T_R(B)$. As $T_R(B)$ has exponent 2, we see that the class in $T_R(B)$ of $\mathrm{Norm}_{K/k}(\mathfrak{a}'\mathfrak{a}^{-1})$ is trivial. This shows that the class of $\mathrm{Norm}_{K/k}(\mathfrak{a})$ in $T_R(B)$ is indeed well-defined since we will show below that z exists.

As we are assuming $B(a,b) = B(a,d)$, we have the equality of local Hilbert symbols $\{a,b\}_v = \{a,d\}_v$ [V, p. 74] for all places v of k. Hence $\{a,d/b\}_v$ is trivial for all v, showing that d/b is everywhere locally a norm. By the Hasse-Minkowski theorem [V, p. 75], d/b is a global norm. Thus, there is a $w \in k(\sqrt{a})$ such that $\mathrm{Norm}_{k(\sqrt{a})/k}(w) = d/b$. We can take $z = bw$.

Let $x, y \in B^*$ be as in (1.1), so that $x^2 = a$, $y^2 = b$ and $xy = -yx$. As $a \notin k^{*2}$, there is a k-isomorphism of fields $k(x) \cong k(\sqrt{a}) = K$. We therefore identify $K = k(x) \subset B$. We have just seen that there are e and f in k such that $w = e + fx \in K$ satisfies $d/b = \mathrm{nr}(w) = e^2 - af^2$. Set $t = wy \in B$ and compute

$$t^2 = (e+fx)y(ey+fxy) = (e+fx)y(ye-yfx) = (e+fx)y^2(e-fx) = d,$$

since $y^2 = b$ is in the center k of B. As $w \in k(x)$,

$$xt = xwy = wxy = -wyx = -tx.$$

This means that we can use x, y to compute $\mathcal{D}(a,b)$ and x, t to compute $\mathcal{D}(a,d)$.

Now,

$$\mathcal{D}(a,b)_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}} + \mathcal{O}_{\mathfrak{p}}\widehat{x}_{\mathfrak{p}} + \mathcal{O}_{\mathfrak{p}}\widehat{y}_{\mathfrak{p}} + \mathcal{O}_{\mathfrak{p}}\widehat{x}_{\mathfrak{p}}\widehat{y}_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}} + \mathcal{O}_{\mathfrak{p}}\widehat{x}_{\mathfrak{p}} + (\mathcal{O}_{\mathfrak{p}} + \mathcal{O}_{\mathfrak{p}}\widehat{x}_{\mathfrak{p}})\widehat{y}_{\mathfrak{p}},$$

while

$$\mathcal{D}(a,d)_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}} + \mathcal{O}_{\mathfrak{p}}\widehat{x}_{\mathfrak{p}} + \mathcal{O}_{\mathfrak{p}}\widehat{wy}_{\mathfrak{p}} + \mathcal{O}_{\mathfrak{p}}\widehat{x}_{\mathfrak{p}}\widehat{wy}_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}} + \mathcal{O}_{\mathfrak{p}}\widehat{x}_{\mathfrak{p}} + \widehat{w}_{\mathfrak{p}}(\mathcal{O}_{\mathfrak{p}} + \mathcal{O}_{\mathfrak{p}}\widehat{x}_{\mathfrak{p}})\widehat{y}_{\mathfrak{p}}.$$

Thus, as $\mathcal{O}_{\mathfrak{p}}$-modules,

$$\text{(2.4)} \qquad \frac{\mathcal{D}(a,b)_{\mathfrak{p}}}{\mathcal{D}(a,b)_{\mathfrak{p}} \cap \mathcal{D}(a,d)_{\mathfrak{p}}} \cong \frac{\mathcal{O}_{\mathfrak{p}} + \mathcal{O}_{\mathfrak{p}}\widehat{x}_{\mathfrak{p}}}{(\mathcal{O}_{\mathfrak{p}} + \mathcal{O}_{\mathfrak{p}}\widehat{x}_{\mathfrak{p}}) \cap \big(\widehat{w}_{\mathfrak{p}}(\mathcal{O}_{\mathfrak{p}} + \mathcal{O}_{\mathfrak{p}}\widehat{x}_{\mathfrak{p}})\big)}.$$

A prime $\mathfrak{p} \notin R$ cannot ramify in $k(x)/k$. Assume first that $\mathfrak{p}$ is not split in the quadratic extension $k(x)/k$. Then $F := k_{\mathfrak{p}}(x) = k_{\mathfrak{p}}(\widehat{x}_{\mathfrak{p}})$ is a quadratic field extension of $k_{\mathfrak{p}}$ containing the elements $\widehat{x}_{\mathfrak{p}}$ and $\widehat{w}_{\mathfrak{p}}$. However, $\mathrm{Norm}_{F/k_{\mathfrak{p}}}(\widehat{w}_{\mathfrak{p}}) = \mathrm{nr}(\widehat{w}_{\mathfrak{p}}) \in \mathcal{O}_{\mathfrak{p}}^*$, implies $\widehat{w}_{\mathfrak{p}} \in \mathcal{O}_F^*$. As $\mathfrak{p} \notin R$ is not above 2 and $\widehat{x}_{\mathfrak{p}}^2 \in \mathcal{O}_{\mathfrak{p}}^*$, we have $\mathcal{O}_{\mathfrak{p}} + \mathcal{O}_{\mathfrak{p}}\widehat{x}_{\mathfrak{p}} = \mathcal{O}_F$. It follows that

$$\mathcal{O}_{\mathfrak{p}} + \mathcal{O}_{\mathfrak{p}}\widehat{x}_{\mathfrak{p}} = \widehat{w}_{\mathfrak{p}}(\mathcal{O}_{\mathfrak{p}} + \mathcal{O}_{\mathfrak{p}}\widehat{x}_{\mathfrak{p}}),$$

so from (2.4) we see that there is no contribution at $\mathfrak{p}$ to $\rho_R\big([\mathcal{D}(a,b)], [\mathcal{D}(a,d)]\big)$ in the non-split case.

Now suppose $\mathfrak{p}$ splits as $\mathfrak{p}\mathcal{O}_{k(x)} = \mathfrak{p}_1\mathfrak{p}_2$. Then $x^2 = a = r_{\mathfrak{p}}^2$ for some $r_{\mathfrak{p}} \in k_{\mathfrak{p}}$, so we can assume $\widehat{x}_{\mathfrak{p}}^2 = 1$. Hence there is a $k_{\mathfrak{p}}$-algebra isomorphism $f_{\mathfrak{p}} : k_{\mathfrak{p}}(\widehat{x}_{\mathfrak{p}}) \mapsto k_{\mathfrak{p}} \times k_{\mathfrak{p}}$ mapping 1 to $(1,1)$ and $\widehat{x}_{\mathfrak{p}}$ to $(1,-1)$. Thus $f_{\mathfrak{p}}(\mathcal{O}_{\mathfrak{p}} + \mathcal{O}_{\mathfrak{p}}\widehat{x}_{\mathfrak{p}}) = (\mathcal{O}_{\mathfrak{p}}, \mathcal{O}_{\mathfrak{p}})$ and $\mathrm{nr}(s) = v_1v_2$ if $f_{\mathfrak{p}}(s) = (v_1, v_2)$, $s \in k_{\mathfrak{p}}(x)$. From (1.3),

$$\text{(2.5)} \quad f_{\mathfrak{p}}(\widehat{w}_{\mathfrak{p}}) = (c_1\pi_{\mathfrak{p}}^{a_{\mathfrak{p}}}, c_2\pi_{\mathfrak{p}}^{-a_{\mathfrak{p}}}), \quad c_1, c_2 \in \mathcal{O}_{\mathfrak{p}}^*,$$
$$a_{\mathfrak{p}} = \frac{1}{2}\big(\mathrm{ord}_{\mathfrak{p}_1}(w) - \mathrm{ord}_{\mathfrak{p}_2}(w)\big),$$

where $\pi_{\mathfrak{p}} \in k_{\mathfrak{p}}$ satisfies $\mathrm{ord}_{\mathfrak{p}}(\pi_{\mathfrak{p}}) = 1$. Recall that $\mathrm{ord}_{\mathfrak{p}}(d/b)$ is even for $\mathfrak{p} \notin R$ and

$$\mathrm{ord}_{\mathfrak{p}}(d/b) = \mathrm{ord}_{\mathfrak{p}}\big(\mathrm{nr}(w)\big) = \mathrm{ord}_{\mathfrak{p}_1}(w) + \mathrm{ord}_{\mathfrak{p}_2}(w).$$

Hence in (2.5), $a_{\mathfrak{p}} = \frac{1}{2}\mathrm{ord}_{\mathfrak{p}}(d/b) - \mathrm{ord}_{\mathfrak{p}_2}(w)$ is an integer. We order $\mathfrak{p}_1$ and $\mathfrak{p}_2$ so that $a_{\mathfrak{p}} \geq 0$. From (2.4) and (2.5) we find that $f_{\mathfrak{p}}$ induces an isomorphism of $\mathcal{O}_{\mathfrak{p}}$-modules

$$\frac{\mathcal{O}_{\mathfrak{p}} + \mathcal{O}_{\mathfrak{p}}\widehat{x}_{\mathfrak{p}}}{(\mathcal{O}_{\mathfrak{p}} + \mathcal{O}_{\mathfrak{p}}\widehat{x}_{\mathfrak{p}}) \cap \big((\widehat{w}_{\mathfrak{p}}(\mathcal{O}_{\mathfrak{p}} + \mathcal{O}_{\mathfrak{p}}\widehat{x}_{\mathfrak{p}})\big)} \cong \frac{(\mathcal{O}_{\mathfrak{p}}, \mathcal{O}_{\mathfrak{p}})}{(\mathcal{O}_{\mathfrak{p}}, \mathcal{O}_{\mathfrak{p}}) \cap (\pi_{\mathfrak{p}}^{a_{\mathfrak{p}}}\mathcal{O}_{\mathfrak{p}}, \pi_{\mathfrak{p}}^{-a_{\mathfrak{p}}}\mathcal{O}_{\mathfrak{p}})} \cong \frac{\mathcal{O}_{\mathfrak{p}}}{\pi_{\mathfrak{p}}^{a_{\mathfrak{p}}}\mathcal{O}_{\mathfrak{p}}}.$$

Thus $\rho_R\big([\mathcal{D}(a,b)], [\mathcal{D}(a,d)]\big)$ is the class in $T_R(B)$ of the ideal

$$\mathfrak{q} := \prod_{\substack{\mathfrak{p} \notin R \\ \mathfrak{p} \text{ split}}} \mathfrak{p}^{a_{\mathfrak{p}}}, \tag{2.6}$$

where $a_{\mathfrak{p}}$ is given by (2.5) and "split" refers to the quadratic extension $K = k(\sqrt{a})$.

If $\mathfrak{p}_1^{\alpha}\mathfrak{p}_2^{\alpha'}$ is the piece above $\mathfrak{p}$ of the factorization of $w\mathcal{O}_K^R$, we can write

$$\mathfrak{p}_1^{\alpha}\mathfrak{p}_2^{\alpha'} = \mathfrak{p}_1^{(\alpha-\alpha')/2}\mathfrak{p}_2^{-(\alpha-\alpha')/2}(\mathfrak{p}_1\mathfrak{p}_2)^{(\alpha+\alpha')/2} = \big(\mathfrak{p}_1^{a_{\mathfrak{p}}}\big)^{1-\sigma}(\mathfrak{p}\mathcal{O}_K^R)^{(\alpha+\alpha')/2},$$

where σ is the non-trivial element of $\mathrm{Gal}(K/k)$. Thus $w\mathcal{O}_K^R = \mathfrak{a}^{1-\sigma}\mathfrak{f}$, where

$$\mathfrak{a} = \prod_{\substack{\mathfrak{p} \notin R \\ \mathfrak{p} \text{ split}}} \mathfrak{p}_1^{a_{\mathfrak{p}}},$$

and $\mathfrak{f}$ is the extension to K of a fractional $\mathcal{O}_k^R$-ideal in k. As $\mathrm{Norm}_{K/k}(\mathfrak{a}) = \mathfrak{q}$ in (2.6), the proof is done on letting $z = bw$ and $\mathfrak{c} = b\mathfrak{f}$.

3. Application to 3-orbifolds

We now describe our geometric motivation for the main problem posed in §1. In [CF2] we studied torsion in maximal arithmetic Kleinian groups Γ and found that computing dihedral subgroups of Γ is closely connected with the map $(a,b) \mapsto [\mathcal{D}(a,b)]$ described in §1. The connection with Hilbert symbols in the case of a 4-group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is straight-forward: If $B \cong B(a,b)$ is generated as a k-algebra by x and y as in (1.1), then the subgroup $H = H(a,b) \subset B^*/k^*$, generated by the natural projective images $\overline{x}$ and $\overline{y}$, is in fact a 4-group. Conversely, any 4-group $H \subset B^*/k^*$ is conjugate to a subgroup of the form $H(a,b)$, where a and b are unique modulo k^{*2}, except that one can switch a and b or replace b by $-ab$ [CF2, Lemma 2.4].

The list of conjugacy classes of 4-subgroups $H \subset B^*/k^*$ is therefore in bijection with the list of pairs of (a,b) such that $B \cong B(a,b)$, where we again take a and b modulo k^{*2} and allow the same trivial modifications. A problem left unresolved in [CF2] is how to actually find which (conjugacy classes of) maximal discrete subgroups of B^*/k^* contain a given 4-subgroup $H(a,b)$. We now explain how this problem is equivalent to that of computing the map $(a,b) \mapsto [\mathcal{D}(a,b)]$.

Borel [Bo] showed that any arithmetic Kleinian group is conjugate in $\mathrm{PGL}(2,\mathbb{C})$ to a discrete subgroup $\Gamma \subset B^*/k^* \subset \mathrm{PGL}(2,\mathbb{C})$, where B is a quaternion algebra over a number field k having exactly one pair of complex conjugate embeddings, and B ramifies at all of the real places of k. This complex place is used to embed B^*/k^* in $\mathrm{PGL}(2,\mathbb{C})$. Borel constructed a list $\{\Gamma_{S,\mathcal{D}}\}_{S,\mathcal{D}}$ of discrete subgroups $\Gamma_{S,\mathcal{D}} \subset B^*/k^*$ such that any maximal (with respect to inclusion) discrete subgroup $\Gamma \subset B^*/k^*$ is conjugate to some $\Gamma_{S,\mathcal{D}}$. Here S is any finite set of prime ideals of $\mathcal{O}_k$ disjoint from $\mathrm{Ram_f}(B)$, and $\mathcal{D}$ is any maximal $\mathcal{O}_k$-order of B. When S is empty, $\Gamma_{S,\mathcal{D}}$ is just the normalizer of $\mathcal{D}$, *i. e.*, the image in B^*/k^* of those $y \in B^*$ for which $y\mathcal{D}y^{-1} = \mathcal{D}$. We denote this group by $\Gamma_{\mathcal{D}}$.

The definition of $\Gamma_{S,\mathcal{D}}$ for a general S is similar, except for a local twist at primes in S, as we now explain. For each $\mathfrak{p} \in S$ choose a maximal order $E_\mathfrak{p} \subset B_\mathfrak{p}$ such that $[\mathcal{D}_\mathfrak{p} : \mathcal{D}_\mathfrak{p} \cap E_\mathfrak{p}] = \mathrm{Norm}_{k/\mathbb{Q}}(\mathfrak{p})$. Say that $\overline{x} \in B^*/k^*$ fixes $\{\mathcal{D}_\mathfrak{p}, E_\mathfrak{p}\}$ if $x\mathcal{D}_\mathfrak{p}x^{-1} = \mathcal{D}_\mathfrak{p}$ and $xE_\mathfrak{p}x^{-1} = E_\mathfrak{p}$, or if $x\mathcal{D}_\mathfrak{p}x^{-1} = E_\mathfrak{p}$ and $xE_\mathfrak{p}x^{-1} = \mathcal{D}_\mathfrak{p}$. Here $\overline{x} = xk^* \in B^*/k^*$ for $x \in B^*$. Then [Bo] [CF1, §4]

$$\Gamma_{S,\mathcal{D}} := \left\{\overline{x} \in B^*/k^* \;\middle|\; x\mathcal{D}_\mathfrak{p}x^{-1} = \mathcal{D}_\mathfrak{p} \text{ for } \mathfrak{p} \notin S,\ \overline{x} \text{ fixes } \{\mathcal{D}_\mathfrak{p}, E_\mathfrak{p}\} \text{ for } \mathfrak{p} \in S\right\}.$$

Up to B^*/k^*-conjugacy, $\Gamma_{S,\mathcal{D}}$ does not depend on the choice of $E_\mathfrak{p}$ nor on the completions $\mathcal{D}_\mathfrak{p}$ at places in

$$R_S := S \cup \mathrm{Ram_f}(B) \qquad \text{[CF1, §4].}$$

A given non-cyclic subgroup of B^*/k^* is contained in only a few $\Gamma_{S,\mathcal{D}}$. More precisely:

([CF2, Theorem 5.1]) *Let B be a quaternion algebra satisfying the Eichler condition over a number field k, and let H be a non-cyclic finite subgroup of B^*/k^*. Then there are two finite sets $s = s(H)$ and $t = t(H)$ consisting of prime ideals of k not in $\mathrm{Ram_f}(B)$, and a type $T(H)$ of maximal $\mathcal{O}_k^{R_t}$-orders of B with the following property: A B^*/k^*-conjugate of H is contained in $\Gamma_{S,\mathcal{D}}$ if and only if $s \subset S \subset t$ and $\mathcal{D}^{R_t} \in T(H)$. Here $\mathcal{D}^{R_t} := \mathcal{O}_k^{R_t} \otimes_{\mathcal{O}_k} \mathcal{D} \subset B$ is the extension of $\mathcal{D}$ to $\mathcal{O}_k^{R_t}$.*

The sets s and t are easily computed and given explicitly in [CF2, §5], but the type $T(H)$ is subtler. When $H = H(a,b)$ is a 4-group, we have

$$s = \mathrm{Odd}_{a,b} - \mathrm{Ram_f}(B), \quad t = \mathrm{Odd}_{a,b} \cup \{\text{dyadic primes}\} - \mathrm{Ram_f}(B),$$
$$R_t = R(a,b),$$

in the notation of (1.2). Moreover a review of the proof (see the local computations in the proof of Lemma 4.1 of [CF2]) shows that $T\big(H(a,b)\big) = [\mathcal{D}(a,b)]$ as types of maximal $\mathcal{O}_k^{R_t}$-orders. This was our original motivation for investigating the problem posed in §1.

We conclude with a numerical example which we hope illustrates the kind of difficulties resolved by the Theorem. We first encountered the following example while tracking down the smallest arithmetic hyperbolic 3-manifold [CFJR]. There we treated this case by geometric methods.

Let $k = \mathbb{Q}(\beta)$, where $\beta^6 - \beta^5 - 2\beta^4 - 2\beta^3 + \beta^2 + 3\beta + 1 = 0$. PARI shows that k is a sextic field of discriminant $-215811 = -3^3 \cdot 7993$, having exactly one complex place, 2 stays prime in $\mathcal{O}_k$, but $3\mathcal{O}_k = \mathfrak{p}_{27}^2$, where $\mathfrak{p}_{27}$ has norm 27. Also, k has class number one and narrow class number 2, where narrow is taken in the strictest sense, involving all real places of k. Thus, modulo squares, there are four distinct totally positive units $\varepsilon_1 = 1$, ε_2, ε_3, $\varepsilon_4 = \varepsilon_2\varepsilon_3$. The prime $\mathfrak{p}_{27}$ splits in $k(\sqrt{-3})/k$, so the narrow Hilbert class field of k is $k(\sqrt{-3}) = k(\sqrt{-\varepsilon_2})$, say.

Let B be the quaternion algebra ramified only at the four real places of k. The problem faced in [CFJR] was:

Given any maximal $\mathcal{O}_k$-order $\mathcal{D}$ of B, does $\Gamma_{\mathcal{D}}$ contain a 4-subgroup?

Since S and $\mathrm{Ram}_{\mathrm{f}}(B)$ are empty and 2 remains prime in $\mathcal{O}_k$, we find $R_t = R_{t(H)} = \{2\mathcal{O}_k\}$ for any 4-group H. As k has narrow class number 2, B has exactly 2 types of maximal $\mathcal{O}_k$-orders, say $\mathcal{E}$ and $\mathcal{F}$. We can distinguish these maximal orders intrinsically. Namely, from [CF1, Theorem 3.3] we find that one of these maximal orders, say $\mathcal{E}$, contains a primitive cube root ζ_3 of unity and the other one does not (ζ_3 "selects" one of the types). Likewise, only $\mathcal{E}$ contains a square root of $-\varepsilon_2$. Since $B = B(-1,-1)$ is isomorphic to the standard Hamilton quaternion algebra over k, we recognize $\mathcal{E}$ as the order containing the Hurwitz order $\mathcal{O}_k + \mathcal{O}_k\mathbf{i} + \mathcal{O}_k\mathbf{j} + \mathcal{O}_k(1+\mathbf{i}+\mathbf{j}+\mathbf{ij})/2$, where $\mathbf{i}^2 = \mathbf{j}^2 = -1$ and $\mathbf{ij} = -\mathbf{ji}$ (since $(1+\mathbf{i}+\mathbf{j}+\mathbf{ij})/2$ is a primitive cubic root of unity). Note that $\mathcal{E}^{R_t}$ and $\mathcal{F}^{R_t}$ remain in distinct $\mathcal{O}_k^{R_t}$-types and that $\mathcal{E}^{R_t}$ and $\mathcal{F}^{R_t}$ can be intrinsically distinguished from each other exactly as $\mathcal{E}$ and $\mathcal{F}$.

A short calculation shows that there are (up to B^*/k^*-conjugation) exactly five 4-groups $H(a,b)$ contained in $\Gamma_{\mathcal{E}}$ or $\Gamma_{\mathcal{F}}$. These are

$$(3.1)\quad H(-1,-1),\ H(-1,-\varepsilon_2),\ H(-1,-\varepsilon_3),\ H(-1,-\varepsilon_4),\ H(-\varepsilon_2,-\varepsilon_3).$$

In this computation one uses that a and b must be totally negative, $H(a,b) = H(a,-ab) = H(b,a)$, that $s\big(H(a,b)\big) = \mathrm{Odd}_{a,b} - \mathrm{Ram}_{\mathrm{f}}(B)$ must be empty (since S is empty), and that $B \cong B(-1,-1)$ with the sextic field k having one place above 2 and having class number 1.

Our earlier question can now be rephrased as:

In which of $\Gamma_{\mathcal{E}}$ or $\Gamma_{\mathcal{F}}$ is each one of the five 4-groups listed above?

Since a and b are units, we have $\widehat{x}_{\mathfrak{p}} = x$, $\widehat{y}_{\mathfrak{p}} = y$ in (1.3) for all $\mathfrak{p}$. Thus, the $\mathcal{O}_k^{R_t}$-order $\mathcal{D}[a,b]$ in (1.4) is just $\mathcal{O}_k^{R_t}[x,y]$.

As we saw above, the maximal $\mathcal{O}_k^{R_t}$-order $\mathcal{E}^{R_t}$ is characterized up to isomorphism by containing $\sqrt{-\varepsilon_2}$ (or ζ_3). As $\mathcal{O}_k^{R_t}$-types,

$$(3.2)\qquad [\mathcal{D}(-1,-\varepsilon_2)] = [\mathcal{D}(-\varepsilon_2,-\varepsilon_3)] = [\mathcal{D}(-1,-1)] = [\mathcal{E}^{R_t}],$$

as the first two orders contain $\sqrt{-\varepsilon_2}$ and the third one ζ_3. Hence, if $\Gamma_{\mathcal{F}}$ contains a 4-group, it must be $H(-1,-\varepsilon_3)$ or $H(-1,-\varepsilon_4)$, in which case at least one of $[\mathcal{D}(-1,-\varepsilon_3)]$ or $[\mathcal{D}(-1,-\varepsilon_4)]$ would equal $[\mathcal{F}^{R_t}]$.

To show that $\Gamma_{\mathcal{F}}$ in fact does contain a 4-group, we turn to the Theorem with $a=b=-1$ and $d=-\varepsilon_i$, with i determined as follows. PARI tells us that $K:=k(\sqrt{-1})$ has class number 2 (*a priori* this class number is only divisible by 2). Thus, all ideals classes are fixed by $\mathrm{Gal}(K/k)$ and the norm map induces an isomorphism from the class group of K to the narrow class group of k.

Let $\mathfrak{a}$ be any ideal of K with non-trivial class. Then $(z):=\mathfrak{a}^{1-\sigma}$ for some $z\in K$, since the class group is fixed by the Galois group. Thus, $\varepsilon:=\mathrm{Norm}_{K/k}(z)=\varepsilon_i b^2$ for some $1\le i\le 4$ and some $b\in\mathcal{O}_k^*$. Applying the Theorem, we find that $\rho_{R^t}([\mathcal{D}(-1,-1)],[\mathcal{D}(-1,-\varepsilon_i)])$ is non-trivial, as it equals the class of $\mathrm{Norm}_{K/k}(\mathfrak{a})$ in $T_{R_t}(B)\cong\mathbb{Z}/2\mathbb{Z}$. Thus, $[\mathcal{D}(-1,-\varepsilon_i)]\ne[\mathcal{D}(-1,-1)]=[\mathcal{E}^{R_t}]$, since otherwise the R^t-distance would be trivial. From (3.2) we see that $[\mathcal{D}(-1,-\varepsilon_i)]=[\mathcal{F}^{R_t}]$ and that $i=3$ or 4. Hence all $\Gamma_{\mathcal{D}}$'s contain a 4-group. One can actually show (applying (3.2), $\varepsilon_4=\varepsilon_2\varepsilon_3$ and the Theorem to $(-1,-1)$ and $(-1,-\varepsilon_2)$) that $[\mathcal{D}(-1,-\varepsilon_3)]=[\mathcal{D}(-1,-\varepsilon_4)]=[\mathcal{F}^{R_t}]$.

References

[B] A. Borel, *Commensurability classes and volumes of hyperbolic 3-manifolds.* Ann. Scuola Norm. Sup. Pisa **8** (1981), 1–33. Also in Borel's *Oeuvres*, Berlin Springer (1983).

[CF1] T. Chinburg, E. Friedman, *An embedding theorem for quaternion algebras.* J. London Math. Soc. (2) **60** (1999), 33–44.

[CF2] T. Chinburg, E. Friedman, *The finite subgroups of maximal arithmetic Kleinian groups.* Ann. Institut Fourier **50** (2000), 1765–1798.

[CFJR] T. Chinburg, E. Friedman, K.N. Jones , A.W. Reid, *The arithmetic hyperbolic 3-manifold of smallest volume.* Ann. Scuola Norm. Sup. Pisa (to appear).

[R] I. Reiner, *Maximal Orders.* Acad. Press London (1975).

[V] M.-F. Vignéras, *Arithmétique des algèbres de Quaternions.* Lecture Notes in Math. **800**, Springer-Verlag Berlin (1980).

Ted Chinburg
The University of Pennsylvania
Philadelphia
PA 19104
U. S. A.
E-mail : ted@math.upenn.edu

Eduardo Friedman
Facultad de Ciencias
Universidad de Chile
Casilla 653
Santiago 1
Chile
E-mail : friedman@uchile.cl