ANNALES DE L'INSTITUT FOURIER

TED CHINBURG
EDUARDO FRIEDMAN

The finite subgroups of maximal arithmetic kleinian groups

Annales de l'institut Fourier, tome 50, n° 6 (2000), p. 1765-1798
<http://www.numdam.org/item?id=AIF_2000__50_6_1765_0>

Ann. Inst. Fourier, Grenoble
50, 6 (2000), 1765–1798

THE FINITE SUBGROUPS OF MAXIMAL ARITHMETIC KLEINIAN GROUPS

by T. CHINBURG*, E. FRIEDMAN**

1. Introduction.

The finite subgroups of $\mathrm{PGL}(2,\mathbb{C})$ have been known since Klein's time to be isomorphic to a cyclic group, a dihedral group, A_4, S_4 or A_5. In the study of hyperbolic 3-orbifolds, especially in connection with volumes estimates [7] [8] [9], it is useful to know which of these finite groups appear as subgroups of a given Kleinian group $\Gamma \subset \mathrm{PGL}(2,\mathbb{C})$. In this generality, it seems that the problem can only be solved at the level of finding an algorithm which computes, in terms of a presentation, all the isomorphism classes of finite groups which are realized as subgroups of Γ. We treat here the more restricted problem of computing the finite subgroups of a Kleinian group corresponding to a minimal arithmetic hyperbolic 3-orbifold, where minimal means that the orbifold does not properly cover any other orbifold. The arithmetic hyperbolic 3-manifold of smallest volume has been identified recently using a combination of computational Kleinian group theory, analytic number theory, lists of number fields of small degree and the results of this paper [4].

* Partially supported by NSF grant DMS92-01016 and NSA grant MDA904-90-H-4033.
** Research partially supported by FONDECYT grant 198-1170.
Keywords: Kleinian groups – 3-orbifolds – Finite subgroups – Quaternion algebras – Arithmetic groups – Arithmetic manifolds.
Math. classification: 20G30 – 11F06 – 11R52.

While our interest in the subject of finite subgroups of arithmetic Kleinian groups originated in the study of hyperbolic 3-manifolds, it turned out that the subject is linked to interesting aspects of indefinite quaternion algebras over a number field. Thus, the results of this paper required a prior study [2] of the embeddability of a commutative order into a maximal order. This uncovered, in certain exceptional cases, the existence of a global obstruction affecting exactly half of the maximal orders. Another surprising aspect is an assignment, linked to dihedral subgroups of arithmetic Kleinian groups, of an ideal class to a pair of global Hilbert symbols. This is discussed following Theorem B below.

Borel [1] associated to an arithmetic Kleinian group $\Gamma \subset \mathrm{PGL}(2,\mathbb{C})$ a quaternion algebra B over a number field k. The field k has exactly one complex place and the algebra B ramifies at a set of places $\mathrm{Ram}(B)$ which includes all real places of k. Let $\mathcal{D}$ be a maximal order of B, and let S be a finite set of prime ideals of k such that $S \cap \mathrm{Ram}(B) = \phi$. Borel defined a subgroup $\Gamma_{S,\mathcal{D}} \subset B^*/k^* \subset \mathrm{PGL}(2,\mathbb{C})$ for each such $\mathcal{D}$ and S, and showed that Γ is conjugate to a subgroup of $\Gamma_{S,\mathcal{D}}$ for some $\mathcal{D}$ and S. Thus, arithmetic Kleinian groups Γ can be identified with subgroups of some B^*/k^* and maximal Γ are among the $\Gamma_{S,\mathcal{D}}$.

When $S = \phi$ is empty, we have by definition

$$\Gamma_{\phi,\mathcal{D}} = \Gamma_{\mathcal{D}} = \{\overline{x} \in B^*/k^* |\ x\mathcal{D}x^{-1} = \mathcal{D}\}.$$

Here $\overline{x} \in B^*/k^*$ denotes the class of $x \in B^*$. The complex place of k is used to embed $\Gamma_{\mathcal{D}}$ into $\mathrm{PGL}(2,\mathbb{C})$. For a general S, the definition of $\Gamma_{S,\mathcal{D}}$ is similar, except for a local twist at the places in S. Details are given in §3.

In this paper we identify the finite subgroups of $\Gamma_{S,\mathcal{D}}$ up to B^*/k^*-conjugacy. First, in §2, we determine explicit parameters (*i. e.*, invariants) for all finite subgroups $H \subset B^*/k^*$, where H is taken up to B^*/k^*-conjugacy. The main tools used in §2 are Klein's list and the classical theory of quaternion algebras. In the case of A_4, S_4 and A_5, we relied on Alan Reid's kind help, as well as on the results of [8, §9]. The net result is that, up to conjugation, there is in B^*/k^* at most one subgroup isomorphic to each of A_4, S_4, A_5 or to a cyclic group of order at least 3. In each case we give necessary and sufficient conditions for this subgroup to exist. Thus, no parameters are needed to identify these subgroups. On the other hand, there are infinitely many non-conjugate dihedral subgroups of B^*/k^* and we give parameters for them. We do the same for cyclic subgroups of order 2.

Next, in Theorem 3.3, §3, we identify the cyclic subgroups of B^*/k^* which are actually in $\Gamma_{S,\mathcal{D}}$. We give here the result for $\Gamma_{\mathcal{D}}$.

THEOREM A. — *Let B be a quaternion algebra over a number field k having exactly one complex place, let B ramify at all real places of k, let $\mathcal{O}_k$ denote the ring of algebraic integers of k, and suppose $n > 2$ is an integer. If k contains a primitive n-th root of unity ζ_n, then $\Gamma_{\mathcal{D}}$ contains a cyclic subgroup C_n of order n if and only if B is isomorphic to the matrix algebra $\mathrm{M}(2,k)$. Assume now that $\zeta_n \notin k$. Then $\Gamma_{\mathcal{D}}$ contains a C_n-subgroup if and only if conditions* (1) *and* (2) *below hold:*

(1) *There is an $\mathcal{O}_k$-embedding of $\mathcal{O}_k[\zeta_n]$ into $\mathcal{D}$. If $n = 2\ell^r$ for some prime $\ell \geqslant 3$, then also the full ring of integers $\mathcal{O}_{k(\zeta_n)}$ embeds into $\mathcal{D}$.*

(2) *If a prime $\mathfrak{l}$ of k divides a rational prime $\ell \geqslant 2$, $n = 2\ell^r$ and $\mathfrak{l} \notin \mathrm{Ram}(B)$, then the absolute ramification index $e_{\mathfrak{l}}$ is divisible by $\varphi(n)$, where φ is the Euler function.*

For most n, Theorem A simplifies to

COROLLARY. — *Let B and ζ_n be as above and assume that $n > 2$ is not twice a prime power. If $\zeta_n \in k$, then $\Gamma_{\mathcal{D}}$ contains a C_n-subgroup if and only if $B \cong \mathrm{M}(2,k)$. If $\zeta_n \notin k$, then $\Gamma_{\mathcal{D}}$ contains a C_n-subgroup if and only if $\mathcal{D}$ contains a primitive n-th root of unity.*

The case $n = 2$ of Theorem A is given in Theorem 3.6 below. Condition (1) in Theorem A, which is the only one involving $\mathcal{D}$, is analyzed in [2]. In Theorem 3.3 below we give simple necessary and sufficient conditions under which an embeddability obstruction vanishes, so that (1) can be replaced by an elementary criterion (1′) that only involves k and $\mathrm{Ram}(B)$.

In §4 we study dihedral subgroups of $\mathrm{PGL}_2(F)$, where F is a local field. In §5 we put this together with the results of §2 to list, for a given non-cyclic finite subgroup $H \subset B^*/k^*$, the $\Gamma_{S,\mathcal{D}}$ which contain a conjugate of H. Such a subgroup H, unlike a cyclic one, "selects" only a few $\Gamma_{S,\mathcal{D}}$, as we now explain.

Define two maximal orders $\mathcal{F}$ and $\mathcal{D}$ of B to be in the same S-type if there is an $x \in B^*$ such that the $\mathfrak{p}$-adic completions of $\mathcal{D}$ and $\mathcal{F}$ satisfy $\mathcal{F}_{\mathfrak{p}} = x\mathcal{D}_{\mathfrak{p}}x^{-1}$ for all $\mathfrak{p} \notin S$. The reason for introducing S-types is that $\Gamma_{S,\mathcal{D}}$ is conjugate to $\Gamma_{S,\mathcal{F}}$ if $\mathcal{F}$ and $\mathcal{D}$ belong to the same S-type. When S is empty, an S-type is just a conjugacy class of maximal orders, *i. e.*, a type

in the usual sense [5] [13]. Just as in the classical case, the set of S-types of maximal orders is finite and in bijection with a quotient T_S of the 2-part of the narrow ideal class group of k [13, p. 88] [2, Lemma 3.2].

The results of §5 can be summarized as

THEOREM B. — *Let the algebra B be as in Theorem A and let H be a non-cyclic finite subgroup of B^*/k^*. Then there exist two finite sets S_{m} and S_{M} of primes of k, and an S_{M}-type $T(H)$ of maximal orders of B with the following property: a B^*/k^*-conjugate of H is contained in $\Gamma_{S,\mathcal{D}}$ if and only if $\mathcal{D}$ belongs to the S_{M}-type $T(H)$ and $S_{\mathrm{m}} \subset S \subset S_{\mathrm{M}}$.*

We give in the proof of Theorem 5.1 an explicit description of S_{m} and S_{M} in terms of the invariants of H described in §2. In §6 we compute some examples of Theorems A and B of varying complexity.

The assignment given in Theorem B of an S_{M}-type $T(H)$ to a non-cyclic subgroup H remains mysterious in the case of dihedral subgroups. Take, for example, the case of a 4-group, so $H \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. In Lemma 2.4 we show that such subgroups of B^*/k^* are classified, up to B^*/k^*-conjugacy, by pairs $(a,b) \in k^*/k^{*2} \times k^*/k^{*2}$ such that their global Hilbert symbol coincides with that of the quaternion algebra B. Thus, $H = H_{a,b}$. It is perfectly straightforward (see §5) to determine $S_{\mathrm{m}}(H_{a,b})$ and $S_{\mathrm{M}}(H_{a,b})$ from (a,b). However, we are at a loss to give a global description of the function given by $(a,b) \mapsto T(H_{a,b})$ assigning an S_{M}-type to a symbol. Our proof yields only a description of this map in terms of local maximal orders.

To make this problem more concrete, we replace types by ideal classes as follows. There is a canonical "distance map" ρ between two S_{M}-types, with values in a quotient $T_{S_{\mathrm{M}}}$ of the narrow ideal class group of k (see §3). Fixing S_{M}, this gives rise to a canonical map

$$\big((a,b),(c,d)\big) \mapsto \big(H_{a,b}, H_{c,d}\big) \mapsto \rho\big(T(H_{a,b}), T(H_{c,d})\big)$$

which associates to two pairs (a,b) and (c,d), with coinciding global Hilbert symbols and satisfying certain local conditions, a well-defined class in $T_{S_{\mathrm{M}}}$. It would be interesting to elucidate this map using solely the arithmetic of k.

Finally, we note that while our main interest is in finite subgroups of a maximal arithmetic Kleinian group $\Gamma \subset \mathrm{PGL}(2,\mathbb{C})$, we actually deal throughout with the more general case of a maximal irreducible arithmetic group $\Gamma \subset \mathrm{PGL}(2,\mathbb{R})^n \times \mathrm{PGL}(2,\mathbb{C})^m$.

2. Finite subgroups of B^*/k^*.

In this section we describe the finite subgroups of B^*/k^*, where B is a quaternion algebra over a number field k. Thus, k is a finite extension of $\mathbb{Q}$ and the algebra B is a 4-dimensional k-vector space with basis $1, x, y$ and xy with the multiplication rules

$$x^2 = c, \qquad y^2 = d, \qquad yx = -xy,$$

where $c\ (= c \cdot 1), d \in k^*$ and 1 is the multiplicative identity of B. We summarize this by saying that B has Hilbert symbol (c, d), or simply $B = (c, d)$. In this section B may be definite or indefinite at any real place of k.

We denote the reduced norm, reduced trace and canonical involution [13, p. 1] of B by nr, tr and ι, respectively. We use $\mathfrak{p}$, $\mathfrak{l}$, and "prime of k" exclusively to denote non-archimedean places of k.

LEMMA 2.1. — *Let $n > 2$ be an integer and let ζ_n be a primitive n-th root of unity in some algebraic closure of k. Then B^*/k^* contains a cyclic subgroup C_n of order n if and only if* (1) *and* (2) *below hold:*

(1) $\zeta_n + \zeta_n^{-1} \in k$. *If B is a division algebra, $\zeta_n \notin k$.*

(2) *If $\mathfrak{p} \in \mathrm{Ram}(B)$, then $\mathfrak{p}$ is not split in the quadratic extension $k(\zeta_n)/k$.*

The subgroup C_n is unique up to conjugation by an element of B^*/k^*. It can be described as follows. If $\zeta_n \in k$, so $B = \mathrm{M}(2, k)$, then the class of $\begin{pmatrix} 1 & 0 \\ 0 & \zeta_n \end{pmatrix}$ in $\mathrm{PGL}(2, k) = B^*/k^*$ generates a C_n. If, on the other hand, $\zeta_n \notin k$, then conditions (1) *and* (2) *are equivalent to the existence of a $\zeta \in B^*$ satisfying $\zeta^n = 1$, $\zeta^{n/d} \neq 1$ for any proper divisor d of n. For any such ζ, $k(\zeta)/k$ is a quadratic field extension, $k(\zeta)^*/k^* \subset B^*/k^*$ contains a unique C_n and the class of $1 + \zeta$ in B^*/k^* generates C_n. Moreover, if n is odd and $\zeta_n \notin k$ (respectively, $\zeta_n \in k$) then the class of ζ (respectively, $\begin{pmatrix} \zeta_n & 0 \\ 0 & \zeta_n^{-1} \end{pmatrix}$) also generates C_n.*

We note that the lemma implies that for odd n, any $C_n \subset B^*/k^*$ is contained in a C_{2n}.

Proof. — As before, we denote by $\overline{x}$ an element of B^*/k^* represented by $x \in B^*$. Let us prove the existence of a C_n when (1) and (2) hold.

Suppose first that $\zeta_n \in k$. Then (1) implies $B = \mathrm{M}(2,k)$, so that $\begin{pmatrix} 1 & 0 \\ 0 & \zeta_n \end{pmatrix}$ represents an element of B^*/k^* generating a C_n. Now suppose $\zeta_n \notin k$. Condition (2) implies that $k(\zeta_n)/k$ embeds in B [13], p. 78. Let ζ be the image of ζ_n under this embedding, and let d be the order of ζ in B^*/k^*. Then $d|n$ and $\zeta_n^d \in k$, so (1) implies $\mathbb{Q}(\zeta_n + \zeta_n^{-1}, \zeta_n^d) \subset k$. Because $\zeta_n \notin k$, we conclude that $d = n$ if n is odd and $d = n/2$ if n is even. Hence $(1+\zeta)^2\zeta^{-1} = 2 + \zeta + \zeta^{-1} \in k^*$, shows that $\overline{1+\zeta}$ generates a C_n.

Suppose now that B^*/k^* contains a C_n. Equivalently, suppose there exists an $x \in B^*$ satisfying $x^n \in k^*$, $x^{n/d} \notin k$ for any proper divisor d of n. We first consider the case in which $k(x) \subset B$ is not a field. Then $B \cong \mathrm{M}(2,k)$, so (2) is vacuously true. The eigenvalues of x must lie in k, since otherwise $k(x)$ would be a field. Hence $x \in B^* \cong \mathrm{GL}(2,k)$ is conjugate, by an element of $\mathrm{GL}(2,k)$, to a scalar multiple of $\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$ or $\begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix}$ for some t and λ in k. The first matrix we may discard since it is either the identity (if $t = 0$) or of infinite order in $\mathrm{PGL}(2,k)$. The second matrix has order n in $\mathrm{PGL}(2,k)$ if and only if $\lambda \in k^*$ is a primitive n-th root of unity. Thus, $\zeta_n \in k$. In particular, $\zeta_n + \zeta_n^{-1} \in k$ proving (1) in the case that $k(x)$ is not a field. We have also shown that up to conjugation there is at most one subgroup of $C_n \subset B^*/k^*$ of order $n > 2$ having a generator represented by an $x \in B^*$ such that $k(x)$ is not a field. Such a C_n exists if and only if $\zeta_n \in k$ and $B \cong \mathrm{M}(2,k)$.

Suppose now that $k(x) \subset B$ is a quadratic field extension of k, as is necessarily the case if B is a division algebra. Let σ be the non-trivial automorphism of $k(x)$ fixing k. Let $\zeta = \sigma(x)/x$. Then, as $x^n \in k$, we have $\zeta^n = \sigma(x^n)/x^n = 1$. If for some proper divisor d of n, $\zeta^{n/d} = 1$, then $\sigma(x^{n/d}) = x^{n/d}$, which contradicts $x^{n/d} \notin k$. Hence ζ is a primitive n-th root of unity. Since $x = \sigma(\sigma(x)) = \sigma(\zeta x) = \sigma(\zeta)\zeta x$, we find that $\sigma(\zeta) = \zeta^{-1}$. As $n > 2$, we conclude that $\zeta \notin k$. Therefore k contains no primitive n-th root of unity ζ_n. From $\mathrm{Tr}_{k(x)/k}(\zeta) = \zeta + \zeta^{-1}$ we conclude that $\zeta_n + \zeta_n^{-1} \in \mathbb{Q}(\zeta + \zeta^{-1}) \subset k$, which proves (1). Since $k(x) = k(\zeta) \cong k(\zeta_n)$ (where ζ maps to some ζ_n^j), we see that $k(\zeta_n)/k$ embeds in B. Hence no prime in $\mathrm{Ram}(B)$ splits in $k(\zeta_n)/k$ [13], p. 78. This proves (2). We note that by replacing x by x^j for some integer j relatively prime to n, we may assume that ζ is mapped to ζ_n under the k-isomorphism $k(\zeta) \cong k(\zeta_n)$.

We now prove the uniqueness claimed for C_n in the case that $k(x)$ is a field. From $\mathrm{Tr}_{k(x)/k}(x) = x + \sigma(x) = x(1+\zeta)$ and $n > 2$ we see that $\overline{x}$ and $\overline{1+\zeta}$ generate the same subgroup of B^*/k^*. But, by the Skolem-Noether

theorem [13], p. 6, $1+\zeta \in B$ is the unique (up to conjugation) solution of its minimal equation. Hence there is, up to conjugation, a unique C_n admitting a generator represented by an x such that $k(x)$ is a field.

We have also seen above that there is a unique C_n when $k(x)$ is not a field. However, in that case, $\zeta_n \in k$, while in the present case $\zeta_n \notin k$. Finally, the last statement in Lemma 2.1 follows from $(1+\zeta)^2\zeta^{-1} \in k^*$. □

The above lemma completely describes the cyclic subgroups of B^*/k^* of order $n > 2$. We now turn to the case $n = 2$. Suppose $w \in k^*$ and that there is some $x = x_w \in B^*$ satisfying $x \notin k^*$, $x^2 = w$. Then, $\overline{x} \in B^*/k^*$ has order 2. If $w \notin k^{*2}$, then x_w (if it exists in B) is unique up to conjugation by B^*, again by the Skolem-Noether theorem [13], p. 6. In the case that $w = x^2 \in k^{*2}$, we must have $B \cong \mathrm{M}(2,k)$, and a scalar multiple of x must be conjugate in B to $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. If $w \notin k^{*2}$, then x_w exists if and only if $k(\sqrt{w})$ embeds in B. As this amounts to a local condition at places in $\mathrm{Ram}(B)$ [13], p. 78, we have

LEMMA 2.2. — *The subgroups of order 2 of B^*/k^*, taken up to B^*/k^*-conjugacy, are in bijection with the cosets $wk^{*2} \subset k^*/k^{*2}$, where w runs over all elements of k^* such that no place $v \in \mathrm{Ram}(B)$ splits in $k(\sqrt{w})/k$. When $w \in k^{*2}$ this condition is taken to mean that $B \cong \mathrm{M}(2,k)$. The bijection is obtained by mapping an $\overline{x} = x\,k^* \in B^*/k^*$, having order 2, to x^2k^{*2}. Conversely, given a coset wk^{*2} as above, there is an $x \in B^*$, $x \notin k^*$, such that $x^2 = w$. This $\overline{x}$ is unique up to conjugation and $k(x)$ is a field if and only if $w \notin k^{*2}$. If $w \in k^{*2}$, then x is conjugate to a scalar multiple of $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.*

We now turn to the dihedral subgroups of B^*/k^*.

LEMMA 2.3. — *Let $C_n \subset B^*/k^*$ be a cyclic group of order $n \geqslant 2$. Then there exists a dihedral group $H \subset B^*/k^*$ of order $2n$ containing C_n.*

Given a dihedral group $H \subset B^*/k^*$ of order $2n$ ($n \geqslant 2$), let $x \in B^*$ represent any generator of a cyclic group $C_n \subset H$ of order n. Let $y \in B^*$ represent the generator of a cyclic subgroup $C_2' \subset H$ of order 2 which is not contained in C_n. Let ζ_n denote a primitive n-th root of unity in some algebraic closure of k. Then B is given by Hilbert symbols $B = (d,w)$, where d, $w \in k^*$, $w = y^2$ and $d = (\zeta_n + \zeta_n^{-1})^2 - 4$ for $n > 2$, $d = x^2$ if $n = 2$.

Conversely, suppose B has Hilbert symbol (d, w) for some d and w in k^* . If $n > 2$, assume also that B satisfies conditions (1) and (2) in Lemma 2.1, and assume that $d = \big((\zeta_n + \zeta_n^{-1})^2 - 4\big)a^2$ for some $a \in k^*$. Then there exists $y \in B^*$, with $y^2 = w$, and a cyclic subgroup $C_n \subset B^*/k^*$ of order n such that C_n and $\overline{y}$ generate a dihedral subgroup H of B^*/k^* of order $2n$. Furthermore, if $n = 2$, the nontrivial element $\overline{x}$ of C_2 is represented by an $x \in B^*$ such that $x^2 = d$ and $xy = -yx$.

Proof. — We note that for any $s \in B$, the reduced norm and trace satisfy $\mathrm{nr}(s) = s \cdot \iota(s)$, $\mathrm{tr}(s) = s + \iota(s)$, where ι is the canonical involution of B. Hence, $\iota(k(s)) \subset k(s)$ for $s \in B$, and $\iota(s) = s$ if and only if $s \in k$. If B is a division algebra and $s \in B$, $s \notin k$, then ι induces the non-trivial Galois automorphism of $k(s)/k$. If $k(s)$ is not a field, so $B = M(2, k)$ and

$$\iota\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix},$$

then ι again restricts to the unique non-trivial k-involution of $k(s)$.

Assume first that $C_n \subset B^*/k^*$ and let $\overline{x}$ generate C_n. By the Skolem-Noether theorem, there is a $y \in B^*$ such that $ysy^{-1} = \iota(s)$ for all $s \in k(x)$. As conjugation by y induces a non-trivial k-involution of $k(x)$, $y \notin k(x)$. Now, $x = \iota\big(\iota(x)\big) = y^2xy^{-2}$, shows that $w = y^2 \in k(x)$. As $\iota(w) = ywy^{-1} = yy^2y^{-1} = w$, we see that $w \in k^*$. Furthermore, for $j \in \mathbb{Z}$, $yx^j \notin k^*$ as $y \notin k(x)$. Now, $\iota(x) = \mathrm{nr}(x)x^{-1}$ implies $\overline{y}\,\overline{x}\,\overline{y}^{-1} = \overline{x}^{-1}$. Thus, $\overline{x}$ and $\overline{y}$ indeed generate a dihedral subgroup of $H \subset B^*/k^*$ of order $2n$ containing C_n, proving the first claim in Lemma 2.3.

Now suppose C_n is contained in some dihedral subgroup $H \subset B^*/k^*$ of order $2n$, and let $\overline{y} \in H$, $\overline{y} \notin C_n$. Let us show that $B = (d, w)$, with $w = y^2$ and $d = x^2$ if $n = 2$, $d = (\zeta_n + \zeta_n^{-1})^2 - 4$ if $n > 2$. Note that $\overline{y}$ has order 2 and $\overline{y}\,\overline{x}\,\overline{y}^{-1} = \overline{x}^{-1}$. Then $w := y^2 \in k^*$ and $yxy^{-1} \in k(x)$. Hence conjugation by y induces a k-involution of $k(x)$. If this were the trivial automorphism, then $y \in k(x)$ and $\overline{x}^{-1} = \overline{x}$. Thus $n = 2$. But then $x^2 \in k$, $y^2 \in k$ and $k(x) = k(y)$ imply that $x^{-1}y \in k$, contradicting $\overline{y} \notin C_n$. Hence conjugation by y induces the non-trivial k-involution of $k(x)$ for any $n \geqslant 2$. Let $z = x - \iota(x)$, so $yzy^{-1} = \iota(z) = -z$. For $n > 2$, Lemma 2.1 implies that for some $a \in k^*$, $(z/a)^2 = (\zeta_n + \zeta_n^{-1})^2 - 4 = d$. Here the main point to check is that z^2, taken modulo k^{*2}, is independent of the chosen generator $\overline{x}$ of C_n. But this follows from $\big(x - \iota(x)\big)^{-1}\big(x^j - \iota(x^j)\big) \in k^*$, since this quotient is fixed by ι. Likewise, for $n = 2$, Lemma 2.2 implies

$(z/a)^2 = x^2 = d$ for $a = 2$. As $(z/a)^2 = d$, $y^2 = w$ and $y(z/a)y^{-1} = -z/a$, we have shown that $B = (d, w)$.

We now prove the converse claim. If $n = 2$, the hypothesis $B = (d, w)$ implies the existence of x and y in B^* such that $x^2 = d$, $y^2 = w$ and $xy = -yx$. Hence $\overline{x}$ and $\overline{y}$ generate a Klein subgroup of B^*/k^* as claimed in the lemma when $n = 2$. Assume now $n > 2$. Lemma 2.1 implies the existence of a $C_n \subset B^*/k^*$ with a generator represented by $x \in B^*$ as described in that lemma. By the hypothesis on d and the definition of the Hilbert symbol $B = (d, w)$, we can find y and z in B^* satisfying

$$y^2 = w, \qquad z^2 = d = a^2\big((\zeta_n + \zeta_n^{-1})^2 - 4\big), \qquad yzy^{-1} = -z,$$

for some $a \in k^*$. Now, $z \notin k^*$ and satisfies $(z/a)^2 = d = (\zeta_n - \zeta_n^{-1})^2 = \big(x - \iota(x)\big)^2$ for some $x \in B^*$ representing a generator of C_n, as follows from Lemma 2.1. Hence z/a is conjugate to $x - \iota(x)$. After simultaneously conjugating z and y, we may assume $z/a = x - \iota(x)$. Hence $k(z) = k(x)$. As $y(z/a)y^{-1} = -z/a$, conjugation by y induces ι on $k(x)$. As we saw at the beginning of the proof, this implies that $\overline{x}$ and $\overline{y}$ generate a dihedral subgroup $H \subset B^*/k^*$ of order $2n$. □

Having settled the problem of the existence of dihedral subgroups of B^*/k^*, we turn to their classification up to B^*/k^*-conjugacy. Let us first fix a dihedral subgroup $H \subset B^*/k^*$ of order $2n$ and examine the effect on d and w of varying the choices allowed in Lemma 2.3. When $n > 2$, there is a unique cyclic subgroup $C_n \subset H$ of order n. We saw in the proof of the previous lemma that the coset $d\,k^{*2} = \big(x - \iota(x)\big)^2 k^{*2}$ is independent of the choice of x. However, the subgroup $C_2' = \{1, \overline{y}\}$ is not unique. It can be replaced by $\{1, \overline{y}\,\overline{x}^j\} = \{1, \overline{y'}\}$ for any $j \in \mathbb{Z}$. Let $w' := y'^2$. One calculates that either $w^{-1}w' \in k^{*2}$ or $w^{-1}w'\mathrm{nr}(x) \in k^{*2}$, depending on the parity of j. If $\zeta_n \notin k$, Lemma 2.1 implies $\mathrm{nr}(x) = a^2(\zeta_n + \zeta_n^{-1} + 2)$ for some $a \in k^*$. If $\zeta_n \in k$, this still holds as, calculating modulo k^{*2},

$$\mathrm{nr}(x) \equiv \zeta_n \equiv \zeta_n(1 + \zeta_n^{-1})^2 = \zeta_n + \zeta_n^{-1} + 2.$$

When $n = 2$ there is an additional choice involved in Lemma 2.3, as $C_n = C_2 \subset H$ is not unique. We can replace x by y or xy, leading to d being replaced by w or $-dw$. Also, y can be replaced by xy, which has the effect of replacing w by $-dw$.

In conclusion, for each fixed n (and B), we obtain from H a well-defined conjugacy invariant $[H] = [d, w] \in \big(k^*/k^{*2} \times k^*/k^{*2}\big)/\sim$, where $\sim$

is the equivalence relation generated by the relation

$$(d\,k^{*2}, w\,k^{*2}) \sim (d\,k^{*2}, (\zeta_n + \zeta_n^{-1} + 2)w\,k^{*2}),$$

where

$$B = (d, w), \quad n > 2, \quad \frac{d}{(\zeta_n + \zeta_n^{-1})^2 - 4} \in k^{*2},$$

or by the relations

$$(d\,k^{*2}, w\,k^{*2}) \sim (w\,k^{*2}, d\,k^{*2}) \sim (d\,k^{*2}, -dw\,k^{*2}) \qquad (B = (d, w),\ n = 2).$$

We remark that when n is odd, there is actually no equivalence imposed on w, beyond taking it modulo k^{*2}, simply because $(\zeta_n + \zeta_n^{-1} + 2) \in k^{*2}$. By Lemma 2.3, any equivalence class $[d, w]$ as above can be realized as $[H] = [d, w]$, for some dihedral subgroup $H \subset B^*/k^*$ of order $2n$. We now prove that, for a fixed n, $[H]$ is the only conjugacy invariant of such dihedral subgroups.

LEMMA 2.4. — *Two dihedral subgroups H_1 and H_2 of B^*/k^* having the same order $2n$ are conjugate in B^*/k^* if and only if $[H_1] = [H_2]$ in $(k^*/k^{*2} \times k^*/k^{*2})/\sim$, as defined above.*

Proof. — From the preceding discussion, one sees that $[H_1] = [H_2]$ when H_1 and H_2 are conjugate. To prove the converse, note that by Lemmas 2.1 and 2.2 we may assume, after conjugating H_2, that $C_n \subset H_1 \cap H_2$ for a cyclic group C_n of order n. Let $\overline{x}$ generate C_n and let $\overline{y_i}$ generate a subgroup of H_i of order 2, disjoint from C_n. As we are assuming $[H_1] = [H_2]$, after possibly replacing $\overline{y_2}$ by $\overline{x}\,\overline{y_2}$, we may assume that $y_2^2 = y_1^2$. As we saw in the proof of Lemma 2.3, we have then $y_1 x y_1^{-1} = \iota(x) = y_2 x y_2^{-1}$. Thus, $y_1^{-1} y_2 \in k(x)^*$, as $y_1^{-1} y_2$ commutes with x. Write $y_2 = y_1 h$, $h \in k(x)^*$. Then $\mathrm{nr}(h) = 1$, as $\mathrm{nr}(y_1) = \mathrm{nr}(y_2)$.

If $k(x)$ is a field, Hilbert's Theorem 90 shows that there is a $g \in k(x)^*$ such that $h = g\iota(g)^{-1}$. Since conjugation by y_1 induces ι on $k(x)$, we have $\iota(g) y_1 = y_1 g$. Hence, $\iota(g) y_1 \iota(g)^{-1} = y_1 g \iota(g)^{-1} = y_1 h = y_2$. As $\iota(g) \in k(x)^*$, $\iota(g) x \iota(g)^{-1} = x$. Hence H_1 and H_2 are conjugate, as claimed.

If $k(x)$ is not a field, Lemmas 2.1 and 2.2 show that $k(x)$ is (isomorphic to) the k-algebra $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$, with $a, b \in k$. But $\mathrm{nr}(h) = 1$ shows $h = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} = g\iota(g)^{-1}$, where $g = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \in k(x)^*$. Thus the above argument applies in this case too. □

Remark. — A review of the proofs of Lemmas 2.1 to 2.4 shows that they are all valid if k is a finite extension of an ℓ-adic field $\mathbb{Q}_\ell$. Actually, some statements simplify in the local case. For example, we can drop (2) in Lemma 2.1, since a prime cannot split in a nontrivial local extension. In particular, $[d, w]$ classifies dihedral subgroups of $\mathrm{PGL}(2, F)$ up to conjugacy when F is a local field. We shall use this in §4.

We define the parity of $\alpha \in k^*$ (or of $\alpha\, k^{*2} \in k^*/k^{*2}$) at $\mathfrak{l}$ as the parity of $\mathrm{ord}_\mathfrak{l}(\alpha)$, where the valuation $\mathrm{ord}_\mathfrak{l}$ is normalized so that its value group is $\mathbb{Z}$. Similarly, we shall say that $x \in B^*$ (or $\overline{x} \in B^*/k^*$) is odd or even at $\mathfrak{l}$ depending on the parity of $\mathrm{ord}_\mathfrak{l}\big(\mathrm{nr}(x)\big)$. To determine when a cyclic or dihedral subgroup $G \subset B^*/k^*$ lies in $\Gamma_{S,\mathcal{D}}$, we will need to determine whether G contains an element which is odd at some prime $\mathfrak{l}$ of k.

LEMMA 2.5. — *Let $\mathfrak{l}$ be a prime of k lying above the rational prime $\ell \geqslant 2$, and let H be a dihedral subgroup of B^*/k^* of order $2n$ and invariant $[H] = [d, w]$. If $n = 2$, then H contains an element which is odd at $\mathfrak{l}$ if and only if d or w is odd at $\mathfrak{l}$. If $n = 2\ell^r$, with $r \geqslant 1$, then H contains an element which is odd at $\mathfrak{l}$ if and only if w is odd at $\mathfrak{l}$, or if the absolute ramification index $e_\mathfrak{l}$ is not divisible by $\varphi(n)$, where φ is the Euler function. For other n, H contains an element which is odd at $\mathfrak{l}$ if and only if w is odd at $\mathfrak{l}$.*

When $n = 2$, it is easy to see that the conditions on d and w given in the lemma are independent of the choice of d and w permitted by the equivalence relation used in defining $[H]$. For $n > 2$, this amounts to showing that $\mathrm{ord}_\mathfrak{l}(\zeta_n + \zeta_n^{-1} + 2)$ is odd if and only if $e_\mathfrak{l}$ is not divisible by $\varphi(n)$. This is done in the course of the proof below.

Proof. — Let x and y represent generators of H as in Lemma 2.3. H contains an element which is odd at $\mathfrak{l}$ if and only if $\mathrm{nr}(x)$ or $\mathrm{nr}(y)$ is odd at $\mathfrak{l}$. When $n = 2$, the lemma is clear since $\mathrm{nr}(x) = -x^2 = -d$ and $\mathrm{nr}(y) = -w$. For $n > 2$, we must show that $\mathrm{nr}(x)$ is odd at $\mathfrak{l}$ if and only if $n = 2\ell^r$ and $e_\mathfrak{l}$ is not divisible by $\varphi(n)$. As we saw after the proof of Lemma 2.3, $\mathrm{nr}(x) \equiv \zeta_n + \zeta_n^{-1} + 2 (\text{modulo } k^{*2})$. As $\zeta_n + \zeta_n^{-1} + 2 = (1 + \zeta_n)(1 + \zeta_n^{-1})$, we conclude [12, p. 12] that $\mathrm{ord}_\mathfrak{l}(\zeta_n + \zeta_n^{-1} + 2) \neq 0$ if and only if $n = 2\ell^r$. Thus, we can assume $n = 2\ell^r$. Then $\zeta_n + \zeta_n^{-1} + 2$ is a generator of the prime $\mathfrak{l}_0$ of $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ lying above ℓ. As $\mathfrak{l}_0$ has absolute ramification index $e_{\mathfrak{l}_0} = \frac{\varphi(n)}{2}$,

$$\mathrm{ord}_\mathfrak{l}(\zeta_n + \zeta_n^{-1} + 2) = e_{\mathfrak{l}/\mathfrak{l}_0} \mathrm{ord}_{\mathfrak{l}_0}(\zeta_n + \zeta_n^{-1} + 2) = e_{\mathfrak{l}/\mathfrak{l}_0} = \frac{e_\mathfrak{l}}{e_{\mathfrak{l}_0}} = \frac{2e_\mathfrak{l}}{\varphi(n)}.$$

This last integer is odd if and only if $\varphi(n)$ does not divide $e_\mathfrak{l}$. □

In the course of the preceding proof we established when a cyclic subgroup of B^*/k^* contains an odd element, which we now record.

LEMMA 2.6. — *Let $\mathfrak{l}$ be a prime of k lying above the rational prime $\ell \geqslant 2$, and let C_n be a cyclic subgroup of B^*/k^* of order $n > 2$. Then C_n contains an element which is odd at $\mathfrak{l}$ if and only if $n = 2\ell^r$ and if the absolute ramification index $e_{\mathfrak{l}}$ is not divisible by $\varphi(n)$.*

LEMMA 2.7. — *Let $\mathfrak{l}$ be as above, let C_2 be a cyclic subgroup of B^*/k^* of order 2 whose generator is represented by $x \in B^*$, and set $w = x^2 \in k^*$. Then C_2 contains an element which is odd at $\mathfrak{l}$ if and only if $\mathrm{ord}_{\mathfrak{l}}(w)$ is odd.*

We now turn to noncyclic and nondihedral finite subgroups of B^*/k^*.

LEMMA 2.8 ([8]). — *B^*/k^* contains a subgroup isomorphic to S_4 if and only if it contains a subgroup isomorphic to A_4. This happens if and only if B has Hilbert symbol $(-1,-1)$. A subgroup isomorphic to A_5 is contained in B^*/k^* if and only if $B = (-1,-1)$ and $\sqrt{5} \in k$.*

Two noncyclic, nondihedral finite subgroups of B^*/k^* (i.e., isomorphic to A_4, S_4 or A_5) are B^*/k^*-conjugate if and only if they are isomorphic as abstract groups.

Proof. — Assume first that $B = (-1,-1)$. Then, by definition of the Hilbert symbol, there are elements $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k} \in B^*$ with the usual Hamilton quaternion multiplication rules. Following the notation of [8, pp. 3635-3637], let $\alpha_2 = (1+\mathbf{i}+\mathbf{j}+\mathbf{k})/2$, so $\alpha_2^3 = -1$. Then A_4 is isomorphic to the subgroup of B^*/k^* generated by the images of $\mathbf{i}$ and α_2 in B^*/k^*. S_4 is isomorphic to the subgroup of B^*/k^* generated by the images of $1+\mathbf{i}$ and α_2. If $\sqrt{5} \in k$, let $\tau = (1+\sqrt{5})/2 \in \mathcal{O}_k^*$ and $\alpha_4 = (\tau + \tau^{-1}\mathbf{i} + \mathbf{j})/2 \in B^*$, so $\alpha_4^5 = -1$. Then A_5 is isomorphic to the subgroup of B^*/k^* generated by the images of α_2 and α_4 in B^*/k^*.

For the rest of the proof, we will suppose conversely that B^*/k^* contains a subgroup H isomorphic to A_4. As before, let $\overline{x}$ be the image of $x \in B^*$ in B^*/k^*. Consider the restriction to H of the map $N : B^*/k^* \mapsto k^*/k^{*2}$ induced by the reduced norm.

As A_4 has no nontrivial homomorphic image of exponent 2, H must be entirely contained in the kernel of N. Hence there are elements $x, z \in B$ of reduced norm 1 such that $\overline{x}$ and $\overline{z}$ are of elements of order two and three in H, respectively. As $x^2 \in k^*$ but $x \notin k^*$, we have $x^2 = -\mathrm{nr}(x) = -1$. Define $y = zxz^{-1}$. Then $\overline{x}$ and $\overline{y}$ generate the Klein subgroup of H. As y

is conjugate to x, $y^2 = x^2 = -1$. By Lemma 2.3, $B = (x^2, y^2) = (-1, -1)$. We may therefore let $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$, α_2 and α_4 in B^* be as in the first part of the proof.

By Lemma 2.4, there is a $\beta \in B^*$ such that $\beta x \beta^{-1} \in k^*\mathbf{i}$ and $\beta y \beta^{-1} \in k^*\mathbf{j}$. Since $x^2 = y^2 = -1 = \mathbf{i}^2 = \mathbf{j}^2$, we can conjugate H and multiply x by ± 1 in order to be able to assume that $x = \mathbf{i}$ and $y = zxz^{-1} = \pm\mathbf{j}$. By replacing z by $\mathbf{i}z$, $\mathbf{j}z$, or $\mathbf{k}z$, if necessary, we may assume that $z\mathbf{i}z^{-1} = \mathbf{j}$ and $z\mathbf{j}z^{-1} = \mathbf{k}$. The first condition $z\mathbf{i}z^{-1} = \mathbf{j}$ determines z up to left multiplication by an element of $k(\mathbf{j})^*$, while the second condition $z\mathbf{j}z^{-1} = \mathbf{k}$ determines z up to left multiplication by an element of $k(\mathbf{k})^*$. Since the intersection of the multiplicative groups $k(\mathbf{j})^*$ and $k(\mathbf{k})^*$ is just k^*, this proves z is unique up to multiplication by an element of k^*. Hence the class $\overline{z}$ of z in B^*/k^* must be in the subroup we explicitly constructed before, using $\overline{\mathbf{i}}$ and $\overline{\alpha_2}$. This proves H must be conjugate to this group, so all subgroups of B^*/k^* isomorphic to A_4 are conjugate.

If B^*/k^* contains a subgroup isomorphic to S_4, then clearly B^*/k^* contains a subgroup isomorphic to A_4. Hence $B = (-1, 1)$, by what we have just proved. We constructed in the first part of the proof a subgroup T of B^*/k^* which is isomorphic to S_4. Suppose T' is another subgroup of B^*/k^* isomorphic to T. Let H and H' be the unique subgoups of index 2 in T and T', respectively. Since H and H' are isomorphic to A_4, they are conjugate in B^*/k^* by what we have already shown. Hence to prove that T and T' are conjugate in B^*/k^*, we can reduce to the case in which $H = H'$ is the group constructed in the first part of the proof using $\mathbf{i}$, $\mathbf{j}$ and α_2.

We shall now show that $T = T'$ follows from $H = H'$. One readily checks that the automorphism group of A_4 is isomorphic to S_4 via the conjugation action of S_4 on A_4. Take $\overline{y} \in T'$ and consider its conjugation action on H. There must be $\overline{x} \in T$ inducing the same conjugation action on H. But then $z := yx^{-1}$ acts trivially by conjugation on H. Hence $z\mathbf{i}z^{-1} = \pm\mathbf{i}$ and $z\mathbf{j}z^{-1} = \pm\mathbf{j}$. As above, we find that z, after possibly multiplying it by an element of H, must be in the center k^*. Hence $\overline{z} \in H$, $\overline{y} \in T$, and so $T = T'$.

Suppose now that B^*/k^* contains a subgroup isomorphic to A_5. As A_5 contains an element of order 5, Lemma 2.1 implies that $\mathbb{Q}(\zeta_5 + \zeta_5^{-1}) = \mathbb{Q}(\sqrt{5}) \subset k$. We have already shown that $B = (-1, -1)$.

It only remains to show that any two subgroups $W_i \subset B^*/k^*$ isomorphic to A_5 are B^*/k^*-conjugate. Fix an embedding $k \hookrightarrow \mathbb{C}$. This

gives an embedding $B^*/k^* \hookrightarrow \mathrm{PGL}_2(\mathbb{C})$, so we may view the W_i as subgroups of $\mathrm{PGL}_2(\mathbb{C})$. It is well-known that all subgroups of $\mathrm{PGL}_2(\mathbb{C})$ isomorphic to A_5 are conjugate. For lack of a good reference we will sketch a proof. Identify $\mathrm{PGL}_2(\mathbb{C})$ with $\mathrm{PSL}_2(\mathbb{C})$, and let $\pi : \mathrm{SL}_2(\mathbb{C}) \to \mathrm{PSL}_2(\mathbb{C})$ be the natural surjection. It is shown in [6, Lemmas 1-3] that $G_i = \pi^{-1}(W_i)$ is abstractly isomorphic to $G = \mathrm{SL}_2(\mathbb{Z}/5)$, which has exactly two faithful, irreducible, 2-dimensional representations $\rho_i : G \mapsto \mathrm{GL}_2(\mathbb{C})$ and has an automorphism $A : G \mapsto G$ such that $\rho_2 = \rho_1 \circ A$. Consider the inclusion $G_i \subset \mathrm{SL}_2(\mathbb{C})$ as giving a 2-dimensional, faithful irreducible representation of G. Although the representations ρ_i are different, they have the same image in $\mathrm{SL}_2(\mathbb{C})$ since $\rho_2 = \rho_1 \circ A$. Thus, $\mu G_1 \mu^{-1} = G_2$ for some $\mu \in \mathrm{GL}_2(\mathbb{C})$. Applying π, we find $\overline{\mu} W_1 \overline{\mu}^{-1} = W_2$, $\overline{\mu} \in \mathrm{PGL}_2(\mathbb{C})$.

To wind up the proof we will show that $\overline{\mu} \in B^*/k^* \subset \mathrm{PGL}(2, \mathbb{C})$. Choose a subgroup $H = H_1$ of W_1 isomorphic to A_4. Then $\overline{\mu} H \overline{\mu}^{-1} = H_2$ is a subgroup of $W_2 \subset B^*/k^*$ isomorphic to A_4. By what we have already shown, H_1 and H_2 are conjugate in B^*/k^*. So to prove W_1 conjugate to W_2 inside B^*/k^*, we can reduce to the case in which $\overline{\mu} H \overline{\mu}^{-1} = H$. Then conjugation by $\overline{\mu}$ induces an automorphism of H. As above, there must be $\overline{x} \in T \subset B^*/k^*$ such that $\overline{x} = \overline{\mu}$. Hence, $\overline{\mu} \in B^*/k^*$, as claimed. □

Remark. — The foregoing proof shows that a subgroup of B^*/k^* isomorphic to A_4 is conjugate to the subgroup of B^*/k^* generated by the class of $\alpha_2 = (1 + \mathbf{i} + \mathbf{j} + \mathbf{k})/2$ and $\mathbf{i}$. For S_4 we can take instead $1 + \mathbf{i}$ and α_2. For A_5, assuming $\tau = (1 + \sqrt{5})/2 \in k$, we can take α_2 and $\alpha_4 = (\tau + \tau^{-1}\mathbf{i} + \mathbf{j})/2$.

We end this section by noting the odd elements of A_4, A_5 and S_4.

LEMMA 2.9. — *If $H \subset B^*/k^*$ is a group isomorphic to A_4 or A_5, then no element of H is odd at any prime of k.*

Let $H \subset B^*/k^*$ be a group isomorphic to S_4 and $\mathfrak{p}$ a prime of k. If $\mathfrak{p}$ does not lie above 2, then all elements of H are even at $\mathfrak{p}$. If $\mathfrak{p}$ lies above 2, then H contains an element which is odd at $\mathfrak{p}$ if and only if the absolute ramification index $e_{\mathfrak{p}}$ is odd.

Proof. — A_4 and A_5 have no non-trivial homomorphisms to $\mathbb{Z}/2$, hence can contain no odd element at any prime. Suppose now $H \cong \mathrm{S}_4$. By the remark above, we can suppose that H is generated by a subgroup isomorphic to A_4 and by $\overline{1 + \mathbf{i}}$. But $\mathrm{ord}_{\mathfrak{p}}(\mathrm{nr}(1 + \mathbf{i})) = \mathrm{ord}_{\mathfrak{p}}(2)$, which is either $e_{\mathfrak{p}}$, if $\mathfrak{p}$ is above 2, or 0. □

3. Finite cyclic subgroups of $\Gamma_{S,\mathcal{D}}$.

We begin with Borel's definition of the group $\Gamma_{S,\mathcal{D}}$ mentioned in §1. Let $k_\mathfrak{p}$ denote the $\mathfrak{p}$-adic completion of k at a prime ideal $\mathfrak{p}$ of k and let $B_\mathfrak{p} = B \otimes_k k_\mathfrak{p}$. Define $\mathcal{O}_k$ to be the ring of integers of k and let $\mathcal{O}_{k_\mathfrak{p}}$ be the ring of integers of $k_\mathfrak{p}$. Let $\mathcal{T}_\mathfrak{p}$ be the tree whose vertices are the maximal $\mathcal{O}_{k_\mathfrak{p}}$-orders $D_\mathfrak{p}$ of $B_\mathfrak{p}$, and whose edges are unordered pairs $\{E_\mathfrak{p}, F_\mathfrak{p}\}$ of maximal orders of $B_\mathfrak{p}$ such that $[E_\mathfrak{p} : E_\mathfrak{p} \cap F_\mathfrak{p}] = \mathrm{Norm}_{k/\mathbb{Q}}(\mathfrak{p})$. If $\mathfrak{p} \notin \mathrm{Ram}(B)$, then $\mathcal{T}_\mathfrak{p}$ is the tree associated to $B_\mathfrak{p} \cong \mathrm{PGL}(2, k_\mathfrak{p})$ in [11]. Otherwise, $B_\mathfrak{p}$ is a division algebra and $\mathcal{T}_\mathfrak{p}$ reduces to a single vertex.

We shall say that $x \in B_\mathfrak{p}^*$ fixes the vertex $D_\mathfrak{p}$ of $\mathcal{T}_\mathfrak{p}$ if $xD_\mathfrak{p}x^{-1} = D_\mathfrak{p}$. An edge $\{E_\mathfrak{p}, F_\mathfrak{p}\}$ of $\mathcal{T}_\mathfrak{p}$ is fixed by $x \in B_\mathfrak{p}^*$ (or by its class $\overline{x} \in B_\mathfrak{p}^*/k_\mathfrak{p}^*$) if x fixes $E_\mathfrak{p}$ and $F_\mathfrak{p}$, or if $xE_\mathfrak{p}x^{-1} = F_\mathfrak{p}$ and $xF_\mathfrak{p}x^{-1} = E_\mathfrak{p}$. For each $\mathfrak{p} \in S$, so $\mathfrak{p} \notin \mathrm{Ram}(B)$, let us choose an edge $\{E_\mathfrak{p}, F_\mathfrak{p}\}$ of $\mathcal{T}_\mathfrak{p}$. With these preliminaries, Borel's definition is

(3.0)
$$\Gamma_{S,\mathcal{D}} = \left\{\overline{x} \in B^*/k^* \,\middle|\, x \text{ fixes } \mathcal{D}_\mathfrak{p} \text{ for all } \mathfrak{p} \notin S, \text{ and } x \text{ fixes } \{E_\mathfrak{p}, F_\mathfrak{p}\} \text{ for } \mathfrak{p} \in S\right\},$$

where $\mathcal{D}_\mathfrak{p} = \mathcal{D} \otimes_{\mathcal{O}_k} \mathcal{O}_{k_\mathfrak{p}}$.

We do not incorporate the choice of edges $\{E_\mathfrak{p}, F_\mathfrak{p}\}$ in (3.0) into the notation since a different choice of edges would merely result in a subgroup of B^*/k^* conjugate to $\Gamma_{S,\mathcal{D}}$ [2, Lemma 4.0]. Moreover, the conjugacy is realized by an element of $\overline{x} \in B^*/k^*$ which fixes $\mathcal{D}_\mathfrak{p}$ for all $\mathfrak{p} \notin S$. We point out that the notation $\Gamma_{S,\mathcal{D}}$ differs slightly from Borel's. His $\Gamma_{S,S'}$ coincides with our $\Gamma_{S,\mathcal{D}}$ when his $\mathcal{D}(S')$ [1, pp. 9, 12] equals our $\mathcal{D}$.

To apply the results of [2] and pass from cyclic subgroups of B^*/k^* to those of $\Gamma_{S,\mathcal{D}}$, we need to assume that B satisfies the Eichler condition. Thus, we now assume that B is a quaternion algebra over a number field k and

$$B_v = B \otimes_k k_v \cong \mathrm{M}(2, k_v) \tag{3.1}$$

for some archimedean place v of k. This is automatically satisfied by a B associated to an arithmetic hyperbolic 3-orbifold. More generally, Borel has shown [1] that any irreducible arithmetic subgroup of $\mathrm{PGL}(2,\mathbb{R})^n \times \mathrm{PGL}(2,\mathbb{C})^m$ is conjugate to a subgroup of $\Gamma_{S,\mathcal{D}}$, as defined in (3.0), associated to a quaternion algebra B satisfying the Eichler condition.

For $y \in B$, let $\mathrm{Disc}(y) = \big(\mathrm{tr}(y)\big)^2 - 4\mathrm{nr}(y) \in k$. We now quote [2, Theorem 4.3]:

THEOREM 3.1. — *Let k be a number field, let B be a quaternion algebra over k satisfying the Eichler condition (3.1), and let $\Gamma_{S,\mathcal{D}}$ be as in (3.0). If a conjugate of $\overline{y} \in B^*/k^*$ is contained in $\Gamma_{S,\mathcal{D}}$, then the following three conditions hold:*

3.1a) $\mathrm{Disc}(y)/\mathrm{nr}(y) \in \mathcal{O}_k$.

3.1b) *If y is odd at $\mathfrak{p}$, then $\mathfrak{p} \in S \cup \mathrm{Ram}(B)$.*

3.1c) *For each $\mathfrak{p} \in S$ at least one of the following four conditions holds:*
- *$y \in k$.*
- *y is odd at $\mathfrak{p}$.*
- *$k(y) \otimes_k k_{\mathfrak{p}}$ is not a field.*
- *$\mathfrak{p}$ divides $\mathrm{Disc}(y)/\mathrm{nr}(y)$.*

Conversely, if 3.1a, 3.1b and 3.1c hold, then a conjugate of $\overline{y}$ is contained in $\Gamma_{S,\mathcal{D}}$, except possibly when the following three conditions hold:

3.1d) *$k(y) \subset B$ is a quadratic field extension of k.*

3.1e) *The extension $k(y)/k$ and the algebra B are unramified at all finite places and ramify at exactly the same (possibly empty) set of real places of k. Furthermore, all $\mathfrak{p} \in S$ split in $k(y)/k$.*

3.1f) *All $\mathfrak{p}$ dividing $\mathrm{Disc}(y)/\mathrm{nr}(y)$ split in $k(y)/k$.*

Suppose now that 3.1a to 3.1f all hold. In this case the number of S-types of maximal orders $\mathcal{D}$ of B is even and the $\mathcal{D}$ for which a conjugate of $\overline{y}$ belongs to $\Gamma_{S,\mathcal{D}}$ comprise exactly half of the S-types. These $\mathcal{D}$ are exactly those maximal orders which contain a conjugate (by B^*) of the ring $\mathcal{O}_{k(y)}$ of algebraic integers of $k(y)$.

The last statement in Theorem 3.1 can be made more explicit. To do this, we need to explain how to compute with S-types of maximal orders. Given two maximal orders $\mathcal{D}$ and $\mathcal{E}$, define their distance ideal $\rho(\mathcal{D},\mathcal{E})$ to be the order-ideal of the finite $\mathcal{O}_k$-module $\mathcal{D}/(\mathcal{E} \cap \mathcal{D})$. Recall that the order-ideal of a finite $\mathcal{O}_k$-module isomorphic to $\oplus_i(\mathcal{O}_k/\mathfrak{a}_i)$ is the $\mathcal{O}_k$-ideal $\prod_i \mathfrak{a}_i$. Let $T_S(B)$ be the group of fractional ideals of k modulo the subgroup generated by squares of fractional ideals, primes in $S \cup \mathrm{Ram}(B)$ and principal ideals (α) for which $\alpha \in k^*$ satisfies $\alpha > 0$ at all real places in $\mathrm{Ram}(B)$. Let $\rho_S(\mathcal{D},\mathcal{E})$ be the class of the ideal $\rho(\mathcal{D},\mathcal{E})$ in $T_S(B)$. Then $\rho_S(\mathcal{D},\mathcal{E}) = \rho_S(\mathcal{D}',\mathcal{E})$ if and only if $\mathcal{D}$ and $\mathcal{D}'$ belong to the same S-type [2, Lemma 3.2]. Thus, if we fix $\mathcal{E}$, the map $\mathcal{D} \to \rho_S(\mathcal{D},\mathcal{E})$ determines a bijection between the S-types and $T_S(B)$. If S is empty we write $T(B)$ for $T_S(B)$.

We consider, slightly more generally than at the end of Theorem 3.1, a commutative $\mathcal{O}_k$-order $\Omega \subset B$. We quote [2, Theorem 3.3]:

THEOREM 3.2. — *Let B be a quaternion algebra over a number field k, let $\Omega \subset B$ be a commutative $\mathcal{O}_k$-order and assume that B satisfies the Eichler condition (3.1). Then every maximal order of B contains a conjugate (by B^*) of Ω, except when the following three conditions hold:*

(1) *Ω is an integral domain and its quotient field $L \subset B$ is a quadratic extension of k.*

(2) *The extension L/k and the algebra B are unramified at all finite places and ramify at exactly the same (possibly empty) set of real places of k.*

(3) *All prime ideals of k dividing the relative discriminant ideal $d_{\Omega/\mathcal{O}_k}$ of Ω are split in L/k.*

Suppose now that (1), (2) and (3) hold. Then B has an even number of conjugacy classes of maximal orders. The maximal orders $\mathcal{D}$ containing some conjugate of Ω make up exactly half of these conjugacy classes. If $\mathcal{D}$ and $\mathcal{E}$ are maximal orders and $\mathcal{E}$ contains a conjugate of Ω, then $\mathcal{D}$ contains a conjugate of Ω if and only if the image by the reciprocity map $\mathrm{Frob}_{L/k}$ of the distance ideal $\rho(\mathcal{D}, \mathcal{E})$ is the trivial element of $\mathrm{Gal}(L/k)$.

We can now prove a more detailed and general version of Theorem A in §1.

THEOREM 3.3. — *Let B satisfy the Eichler condition (3.1), let $n > 2$ and let ζ_n denote a primitive n-th root of unity in some algebraic closure of k. If $\zeta_n \in k$, then $\Gamma_{S,\mathcal{D}}$ contains a cyclic subgroup C_n of order n if and only if B is isomorphic to the matrix algebra $M(2,k)$. Assume now that $\zeta_n \notin k$. Then $\Gamma_{S,\mathcal{D}}$ contains a C_n if and only if conditions (1) through (3) below hold:*

(1) *There is an $\mathcal{O}_k$-embedding of $\mathcal{O}_k[\zeta_n]$ into $\mathcal{D}$. If $n = 2\ell^r$ for some prime $\ell \geqslant 3$, then also $\mathcal{O}_{k(\zeta_n)}$ embeds into $\mathcal{D}$.*

(2) *If a prime $\mathfrak{l}$ of k divides a rational prime $\ell \geqslant 2$, $n = 2\ell^r$ and $\mathfrak{l} \notin \mathrm{Ram}(B) \cup S$, then the absolute ramification index $e_{\mathfrak{l}}$ is divisible by $\varphi(n)$, where φ is the Euler function.*

(3) *For each $\mathfrak{p} \in S$ at least one of the following three conditions holds:*

- *$\mathfrak{p}$ is split in $k(\zeta_n)/k$,*
- *$\mathfrak{p}$ divides a rational prime $\ell \geqslant 3$, $n = 2\ell^r$ and $e_{\mathfrak{p}}$ is not divisible by $\varphi(n)$,*
- *$\mathfrak{p}$ divides a rational prime $\ell \geqslant 2$ and $n = \ell^r$.*

Furthermore, if n is neither a prime power nor twice a prime power, and

(a) $\mathrm{Ram}(B) \neq \{\textit{all real places of } k\}$,

then (1) may be replaced by

(1′) $\zeta_n + \zeta_n^{-1} \in k$ *and no* $\mathfrak{p} \in \mathrm{Ram}(B)$ *is split in* $k(\zeta_n)/k$.

If $n = 2\ell^r$ with $\ell \geqslant 3$ prime, (1) above may be replaced by (1′) if (a) holds or if some prime of k dividing ℓ ramifies in $k(\zeta_n)/k$. If $n = \ell^r$ with $\ell \geqslant 2$ prime, (1) may be replaced by (1′) if (a) holds or if some prime of k dividing ℓ is not split in $k(\zeta_n)/k$.

Proof. — Note that $\zeta_n \notin k$ and (1) imply that $k(\zeta_n)/k$ is a quadratic extension. Hence, "split" above is unambiguous.

We consider first the case $\zeta_n \in k$. If $C_n \subset \Gamma_{S,\mathcal{D}}$, then Lemma 2.1 shows $B = \mathrm{M}(2,k)$. Conversely, if $B = \mathrm{M}(2,k)$, let $x = \begin{pmatrix} 1 & 0 \\ 0 & \zeta_n \end{pmatrix}$. Then, as $k(x)$ is not a field, Theorem 3.1 readily implies that a conjugate of $\overline{x} \in \Gamma_{S,\mathcal{D}}$. Thus $C_n \subset \Gamma_{S,\mathcal{D}}$.

We may therefore assume for the rest of this proof that $\zeta_n \notin k$. Suppose first that $C_n \subset \Gamma_{S,\mathcal{D}}$. Lemma 2.1 shows that $\zeta_n + \zeta_n^{-1} \in k$ and that there is a primitive n-th root of unity $\zeta \in B^*$ such that $\overline{1+\zeta} \in \Gamma_{S,\mathcal{D}}$ generates C_n. Thus, $[k(\zeta_n) : k] = 2$ and the Galois conjugate of ζ_n over k is ζ_n^{-1}. Moreover, we can assume $\zeta_n \mapsto \zeta$ under a k-isomorphism $k(\zeta_n) \cong k(\zeta)$. If we set $y = 1 + \zeta$ in Theorem 3.1, we are led to calculate

$$\frac{\mathrm{Disc}(y)}{\mathrm{nr}(y)} = \frac{(2 + \zeta_n + \zeta_n^{-1})^2 - 4(1+\zeta_n)(1+\zeta_n^{-1})}{(1+\zeta_n)(1+\zeta_n^{-1})} = (\zeta_n - 1)(\zeta_n^{-1} - 1). \tag{3.2}$$

This is a unit, except when $n = \ell^r$ is a prime power, in which case every prime of k lying above ℓ divides it. Also, $\mathrm{nr}(y)$ is a unit unless $n = 2\ell^r$ is twice a prime power, with $\ell \geqslant 2$.

We take up first the case $n \neq \ell^r$, $n \neq 2\ell^r$. Then (2) in Theorem 3.3 is vacuous and (3) follows from 3.1c. To prove (1), let $\Omega = \mathcal{O}_k[\zeta]$ in Theorem 3.2. The relative discriminant ideal $d_{\Omega/\mathcal{O}_k} = (\zeta_n - \zeta_n^{-1})^2 \mathcal{O}_k$ is a unit in this case. Thus $\mathcal{O}_{k(\zeta_n)} = \mathcal{O}_k[\zeta_n]$ and $k(\zeta_n)/k$ is unramified at all finite places. Theorem 3.2 implies that $\mathcal{O}_{k(\zeta_n)}$ embeds in $\mathcal{D}$, except (possibly) when $\mathrm{Ram}(B)$ exactly consists of all real places of k. In proving (1), we may therefore assume this. Applying Theorem 3.1 to $y = 1 + \zeta$, we find that 3.1d to 3.1f all hold. As $C_n \subset \Gamma_{S,\mathcal{D}}$ and $\mathcal{D}$ contains a conjugate of $\mathcal{O}_{k(\zeta_n)}$, the last statement of Theorem 3.1 implies (1) in Theorem 3.3.

Assume now that $n = 2\ell^r$, with $\ell \geqslant 3$ a prime. Condition (2) in Theorem 3.3 follows from 3.1b and Lemma 2.6, while (3) follows from 3.1c and (3.2). To prove (1), let $\Omega = \mathcal{O}_{k(\zeta_n)}$ in Theorem 3.2. Then again, $\mathcal{O}_{k(\zeta_n)}$ embeds in all maximal orders, unless $\mathrm{Ram}(B)$ exactly consists of all real places of k and $k(\zeta_n)/k$ is unramified at all finite places. We can again assume this. Consider 3.1d to 3.1f for $y = 1+\zeta$. Amongst these conditions, the only one which is not obvious is that all $\mathfrak{p} \in S$ split in $k(y)/k$. In view of 3.1c, we have to rule out $1+y$ being odd at some place. Here we have already used $\ell > 2$ to ensure that $\mathrm{Disc}(y)/\mathrm{nr}(y)$ is a unit. Hence, by (3.2), $\mathrm{ord}_{\mathfrak{l}}\big(\mathrm{nr}(y)\big) = \mathrm{ord}_{\mathfrak{l}}\big(\mathrm{Disc}(y)\big) = \mathrm{ord}_{\mathfrak{l}}\big((\zeta_n - \zeta_n^{-1})^2\big)$, and the latter must be even since $k(y)/k$ is unramified. Thus, again, 3.1d to 3.1f all hold, proving (1).

The case $n = \ell^r$ is very similar. The new feature in this case is that $\mathrm{Disc}(y)/\mathrm{nr}(y)$ is divisible by $\mathfrak{l}$ if and only if $\mathfrak{l}$ lies above ℓ. When $\mathcal{O}_k[\zeta_n]$ does not embed into all maximal orders, as we may assume in proving (1), Theorem 3.2 implies that all primes above ℓ split in $k(y)/k$, as required by 3.1f.

We now assume, conversely, conditions (1) to (3) in Theorem 3.3. By (1), we may again let $y = 1+\zeta$ in Theorem 3.1. By (3.2), condition 3.1a holds. Conditions 3.1b follows from Lemma 2.6 and (2) in Theorem 3.3, while 3.1c follows from (3). By Theorem 3.1, a conjugate of $\overline{1+\zeta} \in \Gamma_{S,\mathcal{D}}$ (and therefore $C_n \subset \Gamma_{S,\mathcal{D}}$) unless 3.1d-f) all hold. In this case, $C_n \subset \Gamma_{S,\mathcal{D}}$ if and only if $\mathcal{O}_{k(\zeta_n)}$ embeds in $\mathcal{D}$. When $n \neq \ell^r$ this is implied by (1). Indeed, when $n = 2\ell^r$ this is explicitly assumed in (1). For other $n \neq \ell^r$, $\mathcal{O}_k[\zeta_n] = \mathcal{O}_{k(\zeta_n)}$, as we saw above. When $n = \ell^r$, Theorem 3.2 implies that half the S-types contain a conjugate of $\mathcal{O}_{k(\zeta_n)}$. By 3.1f, the same holds for $\mathcal{O}_k[\zeta_n]$. As $\mathcal{O}_k[\zeta_n] \subset \mathcal{O}_{k(\zeta_n)}$, $\mathcal{D}$ contains a conjugate of $\mathcal{O}_k[\zeta_n]$ if and only if it contains a conjugate of $\mathcal{O}_{k(\zeta_n)}$. Hence $C_n \subset \Gamma_{S,\mathcal{D}}$ in this case too.

To conclude the proof, we now determine when (1) may be replaced by (1′), still under the assumption that $\zeta_n \notin k$. From the proof of Lemma 2.1, or directly [13], p. 78, it is clear that (1) implies (1′), with no further assumptions. Thus, $C_n \subset \Gamma_{S,\mathcal{D}}$ implies (1′). Conversely, assume (1′). This is equivalent to assuming that $k(\zeta_n)$ embeds in B [13], p. 78. Let $\Omega = \mathcal{O}_{k(\zeta_n)}$ if $n = 2\ell^r$ with $\ell \geqslant 3$, and $\Omega = \mathcal{O}_k[\zeta_n]$ otherwise. By (1′) we can regard $\Omega \subset B$. Apply Theorem 3.2 to Ω. If $n \neq \ell^r$, $n \neq 2\ell^r$, we find that a conjugate of Ω is contained in every maximal order (that is, (1) holds) if and only if (a) holds. If $n = 2\ell^r$ with $\ell \geqslant 3$ a prime, we must require (a) and that $k(\zeta_n)/k$ be ramified at some finite prime, which is necessarily above

ℓ. If $n = \ell^r$ with $\ell \geqslant 2$ a prime, we must add to (a) the requirement that some prime of k above ℓ is not split in $k(\zeta_n)/k$. □

Remark. — We have also shown that the hypotheses given in Theorem 3.3 under which (1) may be replaced by (1′) are sharp. Namely, if they fail but (1′), (2) and (3) hold, then $\Gamma_{S,\mathcal{D}}$ contains a conjugate of C_n for $\mathcal{D}$ belonging to exactly half of the S-types.

COROLLARY 3.4. — *Let $\ell \geqslant 3$ be a prime. If $\zeta_\ell \in k$, then $\Gamma_{S,\mathcal{D}}$ contains an element of order ℓ if and only if $B \cong \mathrm{M}(2,k)$. If $\zeta_\ell \notin k$, then $\Gamma_{S,\mathcal{D}}$ contains an element of order ℓ if and only if the following hold:*

(i) $\zeta_\ell + \zeta_\ell^{-1} \in k$.

(ii) *If $\mathfrak{p} \in \mathrm{Ram}(B)$, then $\mathrm{Norm}_{k/\mathbb{Q}}(\mathfrak{p}) \not\equiv 1$ (modulo ℓ). If $\mathfrak{p} \in \mathrm{Ram}(B)$ lies above ℓ, then $\mathfrak{p}$ is not split in $k(\zeta_\ell)/k$.*

(iii) *If $\mathfrak{p} \in S$, then $\mathrm{Norm}_{k/\mathbb{Q}}(\mathfrak{p}) \not\equiv -1$ (modulo ℓ).*

(iv) *$\mathcal{D}$ contains an element $y \neq 1$ such that $y^\ell = 1$.*

Furthermore, condition (iv) is implied by (i) and (ii) (and so may be dropped), except when B is unramified at all finite primes, B ramifies at all real places of k, and all primes of k lying above ℓ split in $k(\zeta_\ell)/k$.

Proof. — When $\zeta_\ell \in k$, the corollary is immediate. Assume $\zeta_\ell \notin k$ and $C_\ell \subset \Gamma_{S,\mathcal{D}}$. Then, as we saw in the proof of Theorem 3.3, (1) and (1′) hold. Hence (iv) and (i) hold. The splitting law in cyclotomic extensions and (i) imply $\mathrm{Norm}_{k/\mathbb{Q}}(\mathfrak{p}) \equiv \pm 1$ (modulo ℓ) for $\mathfrak{p}$ not dividing ℓ. Furthermore, such a prime splits in $k(\zeta_\ell)/k$ if and only if $\mathrm{Norm}_{k/\mathbb{Q}}(\mathfrak{p}) \equiv 1$ (modulo ℓ). Hence (ii) and (iii) follows from (1′) and (3), respectively. The converse is proved in the same way. The fact that (iv) is implied by (i) and (ii), except as described above, follows from the last statement in Theorem 3.3. □

In much the same way we obtain

COROLLARY 3.5. — *If $\sqrt{-1} \in k$, then $\Gamma_{S,\mathcal{D}}$ contains an element of order 4 if and only if $B \cong \mathrm{M}(2,k)$. If $\sqrt{-1} \notin k$, then $\Gamma_{S,\mathcal{D}}$ contains an element of order 4 if and only if the following hold:*

(i) *If $\mathfrak{p} \in \mathrm{Ram}(B)$, then $\mathrm{Norm}_{k/\mathbb{Q}}(\mathfrak{p}) \not\equiv 1$ (modulo 4). If $\mathfrak{p} \in \mathrm{Ram}(B)$ lies above 2, then $\mathfrak{p}$ is not split in $k(\sqrt{-1})/k$.*

(ii) *If $\mathfrak{p} \in S$, then $\mathrm{Norm}_{k/\mathbb{Q}}(\mathfrak{p}) \not\equiv -1$ (modulo 4).*

(iii) *Any prime of k lying above 2, and not contained in $S \cup \mathrm{Ram}(B)$, has an even absolute ramification index.*

(iv) *$\mathcal{D}$ contains an element y such that $y^2 = -1$.*

Furthermore, condition (iv) is implied by (i) (and so may be dropped), except when B is unramified at all finite primes, B ramifies at all real places of k, and all primes of k lying above 2 split in $k(\sqrt{-1})/k$.

We now turn to cyclic subgroups of $\Gamma_{S,\mathcal{D}}$ of order 2. Lemma 2.2 states that the cyclic subgroups of order 2 of B^*/k^* are parametrized up to conjugacy by elements wk^{*2} of k^*/k^{*2} such that $k(\sqrt{w})$ embeds in B. We denote by C_w the cyclic subgroup of order 2 of B^*/k^* corresponding to wk^{*2}. Thus, the nontrivial element $\overline{x}$ of $C_w \subset B^*/k^*$ is represented by $x \in B^*$ satisfying $x^2 = w$.

THEOREM 3.6. — *A conjugate of a group $C_w \subset B^*/k^*$ of order 2 is contained in $\Gamma_{S,\mathcal{D}}$ if and only if wk^{*2} is in the set $\mathcal{C}_2 = \mathcal{C}_2(S,\mathcal{D}) \subset k^*/k^{*2}$ defined as follows. The trivial coset k^{*2} is in $\mathcal{C}_2$ if and only if $B \cong M(2,k)$. A non-trivial coset wk^{*2} is in $\mathcal{C}_2$ if and only if $w \in k^*$ satisfies conditions (1) to (3) below:*

(1) *There is an embedding over $\mathcal{O}_k$ of the ring of integers $\mathcal{O}_{k(\sqrt{w})}$ into $\mathcal{D}$.*

(2) *Write the principal fractional ideal $(w) = \mathfrak{a}^2\mathfrak{b}$, where $\mathfrak{a}$ is a fractional ideal and $\mathfrak{b}$ is a square-free integral ideal. Then any $\mathfrak{p}$ dividing $\mathfrak{b}$ is in $S \cup \mathrm{Ram}(B)$.*

(3) *If $\mathfrak{p} \in S$ does not divide 2, then either $\mathfrak{p}$ is split in $k(\sqrt{w})/k$, or $\mathfrak{p}$ divides the ideal $\mathfrak{b}$ in condition (2) above.*

Furthermore, if

(a) *$\mathrm{Ram}(B) \neq \{$the real places of k at which w is negative$\}$, or $k(\sqrt{w})/k$ ramifies at some finite prime of k, or a prime of k lying above 2 is not split in $k(\sqrt{w})/k$,*

then (1) above can be replaced by

(1′) *w is negative at all real places $v \in \mathrm{Ram}(B)$ and no prime $\mathfrak{p} \in \mathrm{Ram}(B)$ is split in $k(\sqrt{w})/k$.*

Proof. — The proof goes exactly as that of Theorem 3.3. Namely, we again apply Theorem 3.1 to the generator $\overline{x} \in B^*/k^*$ of a cyclic group of order 2. The only new feature worth remarking is that $\mathrm{Disc}(x)/\mathrm{nr}(x) = -4$

regardless of $w = x^2$. Because of 3.1c and 3.1f, the primes above 2 therefore play a special role in Theorem 3.6. □

The set C_2 is finite because (2) implies that $k(\sqrt{w})/k$ is a quadratic extension unramified outside the infinite places, the places above 2 and the places in $S \cup \mathrm{Ram}(B)$. Thus C_2 can be calculated by classfield theory. As in the case of Theorem 3.3, the hypotheses under which (1) may be replaced by (1′) are sharp. When (a) fails for some w, but (1′), (2) and (3) in Theorem 3.6 hold, then a conjugate of C_w is contained in $\Gamma_{S,\mathcal{D}}$ for $\mathcal{D}$'s belonging to exactly half of the S-types.

4. Local orders fixed by dihedral subgroups.

In this section F is a finite extension of the ℓ-adic field $\mathbb{Q}_\ell$, π denotes a uniformizer of F, ord_F the valuation, normalized to have value group $\mathbb{Z}$, $\mathcal{O}_F$ its local ring and κ its residue field. An element $x \in \mathrm{GL}(2,F)$, or its class $\overline{x} \in \mathrm{PGL}(2,F)$, is odd if $\mathrm{ord}_F\big(\det(x)\big)$ is odd. The group $\mathrm{PGL}(2,F)$ acts by conjugation $D \mapsto xDx^{-1}$ on the tree $\mathcal{T} = \mathcal{T}_F$ whose vertices are the maximal orders of $\mathrm{M}(2,F)$ [13, p. 40] [11]. Recall that two such maximal orders D and D' determine an edge $\{D, D'\}$ of $\mathcal{T}$ if $[D : D \cap D'] = \mathrm{card}(\kappa)$. Exactly $\mathrm{card}(\kappa)+1$ edges meet at each vertex. An edge $\{D, D'\}$ is fixed by $\overline{x} \in \mathrm{PGL}(2,F)$ if either

$$\Big[xDx^{-1} = D \text{ and } xD'x^{-1} = D'\Big] \text{or} \Big[xDx^{-1} = D' \text{ and } xD'x^{-1} = D\Big].$$

An equivalent definition of $\mathcal{T}$, which we apply below, is to let a vertex $[\Lambda]$ be the F^*-homothety class of an $\mathcal{O}_F$-lattice $\Lambda \subset F \times F$. Two such vertices are joined by an edge $\{[\Lambda], [\Lambda']\}$ when there is a choice of representative lattices such that $\pi\Lambda \subset \Lambda' \cap \Lambda \subset \Lambda$ with $[\Lambda : \Lambda' \cap \Lambda] = \mathrm{card}(\kappa)$. An $\overline{x} \in \mathrm{PGL}(2,F)$ maps $[\Lambda]$ to $[\Lambda x]$, where we write elements of $\Lambda \subset F \times F$ as row vectors and $x \in \mathrm{M}(2,F)$ acts by right multiplication. To match both definitions of $\mathcal{T}$, one maps $[\Lambda]$ to the maximal order $D = \mathrm{End}_{\mathcal{O}_F}(\Lambda)$. We refer to [11] and [13, pp. 37-42] for further background concerning $\mathcal{T}$.

LEMMA 4.1. — *Let $H \subset \mathrm{PGL}(2,F)$ be a dihedral group of order $2n$ and invariant $[H] = [d,w]$, as described in Lemma 2.4 and the remark following it. If H contains an odd element, then H fixes an edge but no vertex of $\mathcal{T}$.*

Assume now that H contains no odd element. Then H fixes a vertex D of $\mathcal{T}$. If $\ell = 2$, D is unique, except when $n = 2^r$. If $\ell > 2$, D is the unique

vertex fixed by H, except when $n = \ell^r$ and $w \in F^{*2}$. In the two excepted cases, H fixes both vertices of some edge of $\mathcal{T}$.

Proof. — Since $H \subset \mathrm{PGL}(2,F)$ is compact, it fixes some vertex $D = \mathrm{End}_{\mathcal{O}_F}(\Lambda)$ or some edge $\{D, D'\}$. If H contains an odd element, then it cannot fix a vertex. Hence H fixes an edge and there is actually nothing more to the lemma in this case.

We therefore assume that H contains no odd element. Define an $\mathcal{O}_F$-order $\mathcal{E} = \mathcal{E}(H) \subset \mathrm{M}(2,F)$ as follows. Let $\overline{x}$ generate a cyclic subgroup $C_n \subset H$ and let $\overline{y} \in H$ be an element of order 2 not in C_n. As H contains no odd element, by multiplying by elements of F^* we can assume that $\mathrm{nr}(x)$ and $\mathrm{nr}(y)$ are units of $\mathcal{O}_F$. Thus, referring to the proof of Lemma 2.3,

$$\det(x), \det(y), y^2 \in \mathcal{O}_F^*, \quad yxy^{-1} = \iota(x), \tag{4.1}$$

where ι is the canonical involution of $\mathrm{M}(2,F)$. Since x and y are integral over $\mathcal{O}_F$ and $yxy^{-1} = \iota(x) = -x + \mathrm{tr}(x) \in \mathcal{O}_F[x]$, the ring $\mathcal{E} = \mathcal{E}(H) \subset \mathrm{M}(2,F)$ generated over $\mathcal{O}_F$ by x and y is an $\mathcal{O}_F$-order.

Let $D = \mathrm{End}_{\mathcal{O}_F}(\Lambda)$ be a maximal order fixed by H. As $\overline{x} \in H$, $\Lambda x = \lambda\Lambda$ for some $\lambda \in F^*$. Actually, we must have $\Lambda x = \Lambda$ because $\det(x) \in \mathcal{O}_F^*$. Hence $x \in D = \mathrm{End}_{\mathcal{O}_F}(\Lambda)$. As the same is true for y, it follows that $\mathcal{E} \subset D$. Using (4.1), one computes [13], p. 24, the reduced discriminant ideal $\mathrm{Disc}(\mathcal{E}) = \Big(\big(\mathrm{tr}(x)\big)^2 - 4\det(x)\Big)\mathcal{O}_F$.

We consider the various possible x, as given in Lemmas 2.1 and 2.2. If $n = 2$, then $\mathrm{Disc}(\mathcal{E}) = 4\mathcal{O}_F$. In particular, $\mathcal{E}(H)$ is a maximal order if $\ell \neq 2$. Thus, when $n = 2$ and $\ell \neq 2$, $D = \mathcal{E}(H)$ and so H fixes the unique vertex $\mathcal{E} = \mathcal{E}(H)$, as claimed in Lemma 4.1.

Consider next the case $n > 2$ and $\zeta_n \in F$. Then x is conjugate to $\begin{pmatrix} 1 & 0 \\ 0 & \zeta_n \end{pmatrix}$. One finds then $\mathrm{Disc}(\mathcal{E}) = \Big(\big(\mathrm{tr}(x)\big)^2 - 4\mathrm{nr}(x)\Big)\mathcal{O}_F = (1-\zeta_n)^2\mathcal{O}_F$. If $n \neq \ell^r$, then $1 - \zeta_n$ is a unit [12, pp. 9, 12].

Consider now the case $\zeta_n \notin F$. Then $x = (1+\zeta)/\pi^r$, where $F(\zeta) = F(x)$ is a field, $\zeta \in \mathrm{M}(2,F)$ is a primitive n-th root of unity and r is such that $\mathrm{nr}(x) \in \mathcal{O}_F^*$. As in the proof of Lemma 2.1, $\iota(\zeta) = \zeta^{-1}$. We now calculate

$$\begin{aligned}
&\big(\mathrm{tr}(x)\big)^2 - 4\mathrm{nr}(x) = \pi^{-2r}\big((1+\zeta+1+\zeta^{-1})^2 - 4(1+\zeta)(1+\zeta^{-1})\big) \\
&= \pi^{-2r}\Big(\big((1+\zeta)(1+\zeta^{-1})\big)^2 - 4(1+\zeta)(1+\zeta^{-1})\Big) = \mathrm{nr}(x)(\zeta+\zeta^{-1}-2) \\
&= -\mathrm{nr}(x)\mathrm{nr}(\zeta-1).
\end{aligned}$$

As $\mathrm{nr}(x) \in \mathcal{O}_F^*$, we again find that $\mathrm{Disc}(\mathcal{E})$ is a unit, unless $n = \ell^r$. We conclude that $\mathcal{E}$ is a maximal order of $\mathrm{M}(2, F)$, except when $n = \ell^r$. It follows that $\mathcal{E} = D$ unless $n = \ell^r$. Thus H fixes the unique vertex $\mathcal{E} = \mathcal{E}(H)$, except possibly when $n = \ell^r$.

We therefore assume, for the rest of this proof, that $n = \ell^r$ and that H contains no odd elements. Thus H fixes a vertex $[\Lambda]$. Suppose first that $\ell = 2$. Consider the action of the 2-group H on the set of vertices adjacent to $[\Lambda]$. This is a set of odd cardinality, since the residue characteristic is ℓ. The action must therefore have a fixed point $[\Lambda']$. Thus H fixes an edge $\{[\Lambda], [\Lambda']\}$, as claimed when $n = 2^r$.

Assume now that $n = \ell^r$, where ℓ is odd. It follows from the last part of Lemma 2.1 that we can choose x so that $x^n = 1 = \mathrm{nr}(x)$ and y as in (4.1). Then,

$$yxy^{-1} = x^{-1}, \quad y^2 = w, \quad x^{\ell^r} = 1. \tag{4.2}$$

As we saw above, $\Lambda x = \Lambda y = \Lambda$. Now, x and y fix a vertex $[\Lambda']$ adjacent to $[\Lambda]$ if and only if $\Lambda/\pi\Lambda$ has a 1-dimensional κ-subspace $\left(= \Lambda/(\Lambda \cap \Lambda')\right)$ which is invariant under $\widetilde{x}$ and $\widetilde{y}$. Here the $\widetilde{\ }$ denotes the reduction map from $\mathrm{End}_{\mathcal{O}_F}(\Lambda) \cong \mathrm{M}(2, \mathcal{O}_F)$ to $\mathrm{End}_\kappa(\Lambda/\pi\Lambda) \cong \mathrm{M}(2, \kappa)$. Suppose κv is such a subspace, so $v\widetilde{x} = \lambda_x v$ and $v\widetilde{y} = \lambda_y v$ for some λ_x, $\lambda_y \in \kappa$ and $v \in \Lambda/\pi\Lambda$.

Though we have been writing scalar multiplication on the left, it will now be convenient to allow scalar multiplication on the right by identifying scalars with multiples of the identity matrix. Then $v\widetilde{w} = v\widetilde{y}^2 = v\lambda_y^2$. Thus, if y fixes two adjacent vertices, then $\widetilde{w} \in \kappa^{*2}$. As $\mathrm{char}(\kappa) = l \neq 2$, Hensel's lemma shows $w \in F^{*2}$, as claimed in Lemma 4.1.

Now assume, conversely, that $w \in F^{*2}$ and that H fixes $[\Lambda]$. We must show that H fixes a vertex adjacent to $[\Lambda]$. As $w = y^2$ and $w \in F^{*2}$, after multiplying y by an element in F^*, we may assume $y^2 = 1$. As in the case $\ell = 2$, the cyclic subgroup $C_{\ell^r} \subset H$ generated by $\overline{x}$ must fix a vertex adjacent to $[\Lambda]$. That is, there is a 1-dimensional $\widetilde{x}$-invariant subspace $\kappa v \subset \Lambda/\pi\Lambda$. But $x^{\ell^r} = 1$, implies $\lambda_x^{\ell^r} = 1$. As κ has characteristic ℓ, $\lambda_x = 1$, and so $v\widetilde{x} = v$. If $v\widetilde{y} = -v$, then κv is certainly a nontrivial H-invariant subspace of $\Lambda/\pi\Lambda$. If $v\widetilde{y} \neq -v$, let $v' = v + v\widetilde{y} \in \Lambda/\pi\Lambda$. Note that $v' \neq 0$ and $v'\widetilde{y} = v'$, since $\widetilde{y}^2 = 1$. From (4.2),

$$v'\widetilde{x} = v\widetilde{x} + v\widetilde{y}\widetilde{x} = v + v\widetilde{x}^{-1}\widetilde{y} = v + v\widetilde{y} = v',$$

which shows that $\kappa v'$ is a nontrivial H-invariant subspace of $\Lambda/\pi\Lambda$. Hence H fixes a vertex adjacent to $[\Lambda]$. □

5. Noncyclic finite subgroups of $\Gamma_{S,\mathcal{D}}$.

We can now prove Theorem B in §1 for slightly more general quaternion algebras.

THEOREM 5.1. — *Let B be a quaternion algebra satisfying the Eichler condition* (3.1) *over a number field k, and let H be a non-cyclic finite subgroup of B^*/k^*. Then there are two finite sets $S_{\mathrm{m}} = S_{\mathrm{m}}(H)$ and $S_{\mathrm{M}} = S_{\mathrm{M}}(H)$ consisting of prime ideals of k not in* $\mathrm{Ram}(B)$, *and an S_{M}-type of maximal orders $T(H)$ with the following property: A B^*/k^*-conjugate of H is contained in $\Gamma_{S,\mathcal{D}}$ if and only if $\mathcal{D} \in T(H)$ and $S_{\mathrm{m}} \subset S \subset S_{\mathrm{M}}$.*

Remark. — We will prove the following explicit description of S_{m} and S_{M}:

(A_5) If $H \cong \mathrm{A}_5$, then S_{m} and S_{M} are both empty.

(A_4) If $H \cong \mathrm{A}_4$, then S_{m} is empty and S_{M} consists of all $\mathfrak{p}$ above 2 for which the residue degree $f_{\mathfrak{p}} = \dim_{\mathbb{F}_2}(\mathcal{O}_k/\mathfrak{p})$ is even.

(S_4) If $H \cong \mathrm{S}_4$, then $S_{\mathrm{m}} = S_{\mathrm{M}}$ and consists of those $\mathfrak{p}$ above 2 for which the residue degree $f_{\mathfrak{p}}$ is even and the absolute ramification index $e_{\mathfrak{p}}$ is odd.

If $H \subset B^*/k^*$ is a dihedral subgroup D_n of order $2n$ and conjugacy invariant $[H] = [d, w]$, as described in §2, we need to distinguish four cases:

(D_n) If $n > 2$ is neither a prime power nor twice a prime power, then $S_{\mathrm{m}} = S_{\mathrm{M}}$ and consists of all $\mathfrak{p} \notin \mathrm{Ram}(B)$ for which $\mathrm{ord}_{\mathfrak{p}}(w)$ is odd.

($\mathrm{D}_{2\ell^r}$) If $n = 2\ell^r$, with $\ell \geqslant 2$ prime and $r \geqslant 1$, then S_{m} consists of all $\mathfrak{p} \notin \mathrm{Ram}(B)$ for which $\mathrm{ord}_{\mathfrak{p}}(w)$ is odd, together with all primes $\mathfrak{l} \notin \mathrm{Ram}(B)$ dividing ℓ for which $e_{\mathfrak{l}}$ is not divisible by $\varphi(n)$. If $\ell \geqslant 3$, then $S_{\mathrm{M}} = S_{\mathrm{m}}$. If $\ell = 2$, then S_{M} consists of S_{m} together with all $\mathfrak{p} \notin \mathrm{Ram}(B)$ lying above 2.

(D_{ℓ^r}) If $n = \ell^r$, with $\ell \geqslant 3$ prime, then S_{m} consists of all $\mathfrak{p} \notin \mathrm{Ram}(B)$ for which $\mathrm{ord}_{\mathfrak{p}}(w)$ is odd. S_{M} consists of S_{m} together with all primes $\mathfrak{l} \notin \mathrm{Ram}(B)$ dividing ℓ which split in $k(\sqrt{w})/k$ (we clarify that if $k(\sqrt{w}) = k$, we regard $\mathfrak{l}$ as split).

(D_2) If $n = 2$, then S_{m} consists of all $\mathfrak{p} \notin \mathrm{Ram}(B)$ for which $\mathrm{ord}_{\mathfrak{p}}(w)$ or $\mathrm{ord}_{\mathfrak{p}}(d)$ is odd. S_{M} consists of S_{m} together with all primes $\mathfrak{l}$ not in $\mathrm{Ram}(B)$ dividing 2.

Any infinite place v of k gives rise to an injection of B^*/k^* into a subgroup of $\mathrm{PGL}(2,\mathbb{C})$. Hence, the above is a complete list of the possible isomorphism types of non-cyclic finite subgroups of $\Gamma_{S,\mathcal{D}}$.

Proof. — Let us first show that any finite subgroup $H \subset B^*/k^*$ is contained in a B^*/k^*-conjugate of some $\Gamma_{S,\mathcal{D}}$. Take $\mathcal{E}$ to be any maximal order of B and let $x \in B^*$. Then, $x\mathcal{E}x^{-1}$ is also a maximal order. Hence, $x\mathcal{E}_{\mathfrak{p}}x^{-1} = \mathcal{E}_{\mathfrak{p}}$ for all primes $\mathfrak{p}$ outside some finite set. As H is finite, $x\mathcal{E}_{\mathfrak{p}}x^{-1} = \mathcal{E}_{\mathfrak{p}}$ for all x representing elements $\overline{x} \in H$ and all $\mathfrak{p}$ outside some finite set R. For each $\mathfrak{p}$, the compact group H must fix a vertex $D_{\mathfrak{p}}$ or an edge $\{G_{\mathfrak{p}}, F_{\mathfrak{p}}\}$ of $\mathcal{T}_{\mathfrak{p}}$. Let

$$S_{\mathrm{m}} = S_{\mathrm{m}}(H) = \left\{\mathfrak{p} \notin \mathrm{Ram}(B) \middle| \ H \text{ fixes an edge but no vertex of } \mathcal{T}_{\mathfrak{p}}\right\},$$

so that $S_{\mathrm{m}} \subset R$. If H contains an odd element, H must fix an edge but no vertex of $\mathcal{T}_{\mathfrak{p}}$. If H does not contain any odd element and yet fixes an edge, H must fix both vertices at that edge. Hence,

$$S_{\mathrm{m}} = \left\{\mathfrak{p} \notin \mathrm{Ram}(B) \middle| \ H \text{ contains an element which is odd at } \mathfrak{p}\right\}. \tag{5.1}$$

Let $\mathcal{F}$ be the maximal order of B such that $\mathcal{F}_{\mathfrak{p}} = \mathcal{E}_{\mathfrak{p}}$ for $\mathfrak{p} \notin R$, $\mathcal{F}_{\mathfrak{p}} = F_{\mathfrak{p}}$ for $\mathfrak{p} \in S_{\mathrm{m}}$ and $\mathcal{F}_{\mathfrak{p}} = D_{\mathfrak{p}}$ for $\mathfrak{p} \in R - S_{\mathrm{m}}$. Then definition (3.0) immediately implies that H is contained in a conjugate of $\Gamma_{S_{\mathrm{m}},\mathcal{F}}$ (we cannot strictly write $H \subset \Gamma_{S_{\mathrm{m}},\mathcal{F}}$ since the choice of edge for $\mathfrak{p} \in S_{\mathrm{m}}$ is left arbitrary in (3.0)).

Define

$$S_{\mathrm{M}} = S_{\mathrm{M}}(H) = \left\{\mathfrak{p} \notin \mathrm{Ram}(B) \middle| \ H \text{ fixes an edge of the tree } \mathcal{T}_{\mathfrak{p}}\right\}.$$

It is immediate that $S_{\mathrm{m}} \subset S_{\mathrm{M}}$ and that these sets depend only on the B^*/k^*-conjugacy class of H. Since $\mathcal{T}_{\mathfrak{p}}$ is a tree and H fixes $\mathcal{F}_{\mathfrak{p}}$, this is the unique vertex fixed by H for $\mathfrak{p} \notin S_{\mathrm{M}}$. We shall show below that S_{M} is finite. Assuming this for now, we can finish the proof of Theorem 5.1 as follows. Let $T(H)$ be the S_{M}-type containing $\mathcal{F}$. Suppose a conjugate $H' = \overline{x}H\overline{x}^{-1}$ of H is contained in some $\Gamma_{S,\mathcal{D}}$. Equivalently, suppose $H \subset \Gamma_{S,\mathcal{D}'}$, where $\mathcal{D}' = x\mathcal{D}x^{-1}$. Then H fixes an edge of $\mathcal{T}_{\mathfrak{p}}$ for $\mathfrak{p} \in S$. Hence $S \subset S_{\mathrm{M}}$. As H fixes no vertex for $\mathfrak{p} \in S_{\mathrm{m}}$, we must have $S_{\mathrm{m}} \subset S$. But, for $\mathfrak{p} \notin S_{\mathrm{M}}$, H fixes the unique vertex $\mathcal{F}_{\mathfrak{p}}$ of $\mathcal{T}_{\mathfrak{p}}$. Therefore $\mathcal{D}'_{\mathfrak{p}} = \mathcal{F}_{\mathfrak{p}}$ for $\mathfrak{p} \notin S_{\mathrm{M}}$, which is to say that $\mathcal{F}$ and $\mathcal{D}$ are in the same S_{M}-type.

Conversely, given that $\mathcal{D} \in T(H)$ and $S_{\mathrm{m}} \subset S \subset S_{\mathrm{M}}$, we must show that a conjugate of H is contained in $\Gamma_{S,\mathcal{D}}$. After conjugating H, we may

assume that $\mathcal{D}_\mathfrak{p} = \mathcal{F}_\mathfrak{p}$ for $\mathfrak{p} \notin S_\mathrm{M}$. By definition, H fixes an edge $\{G_\mathfrak{p}, F_\mathfrak{p}\}$ of $\mathcal{T}_\mathfrak{p}$ for $\mathfrak{p} \in S_\mathrm{M}$. By (5.1), H must fix both $G_\mathfrak{p}$ and $F_\mathfrak{p}$ for $\mathfrak{p} \in S_\mathrm{M} - S_\mathrm{m}$. By transitivity of the action of $\mathrm{SL}_2(k_\mathfrak{p})$ on the edges of $\mathcal{T}_\mathfrak{p}$ [11] and the Strong Approximation Theorem [13, p. 81], we can find $x \in B^*$ which fixes $\mathcal{D}_\mathfrak{p}$ for $\mathfrak{p} \notin S_\mathrm{M}$, and which, for $\mathfrak{p} \in S_\mathrm{M}$, takes the edge $\{G_\mathfrak{p}, F_\mathfrak{p}\}$ to $\{\mathcal{D}_\mathfrak{p}, C_\mathfrak{p}\}$, for some maximal order $C_\mathfrak{p}$ adjacent to $\mathcal{D}_\mathfrak{p}$. It follows that a conjugate H' of H fixes $\mathcal{D}_\mathfrak{p}$ for $\mathfrak{p} \notin S_\mathrm{m}$, and fixes both vertices of an edge $\{\mathcal{D}_\mathfrak{p}, C_\mathfrak{p}\}$ for $\mathfrak{p} \in S_\mathrm{M} - S_\mathrm{m}$. As $S_\mathrm{m} \subset S \subset S_\mathrm{M}$, we find $H' \subset \Gamma_{S,\mathcal{D}}$, as claimed.

We must still prove that S_m and S_M are as described just after Theorem 5.1, which will also prove that S_M is finite. It is worth noting that Theorems 3.3 and 3.6 imply that $S_\mathrm{M}(H)$ is infinite for any cyclic group H.

Consider first the case $H \cong \mathrm{A}_5$. By Lemma 2.9, H contains no odd elements at $\mathfrak{p}$ for any $\mathfrak{p}$. Therefore, by (5.1), $S_\mathrm{m}(H)$ is empty. We claim that $S_\mathrm{M}(H)$ is also empty. For suppose that H fixes some edge of $\mathcal{T}_\mathfrak{p}$ for some $\mathfrak{p}$. Then H must fix both vertices at that edge. But H contains a Klein group with no odd elements at $\mathfrak{p}$. Lemma 4.1 shows that H fixes no edge of $\mathcal{T}_\mathfrak{p}$ unless $\mathfrak{p}$ is above 2. Now, A_5 also contains a subgroup isomorphic to D_3 ($\cong \mathrm{S}_3$), namely the subgroup generated by two permutations whose cycle decompositions are (1 2 3) and (2 3) (4 5), respectively. Lemma 4.1 shows that a subgroup of H isomorphic to D_3 cannot fix an edge of $\mathcal{T}_\mathfrak{p}$, except possibly at $\mathfrak{p}$ dividing 3. Hence $S_\mathrm{M}(H)$ is empty.

Suppose now that $H \cong \mathrm{S}_4$. By Lemma 2.9, H contains an element which is odd at $\mathfrak{p}$ if and only if $\mathfrak{p}$ lies above 2 and $e_\mathfrak{p}$ is odd. As $B = (-1, -1)$ and $e_\mathfrak{p}$ is odd, $\mathfrak{p} \notin \mathrm{Ram}(B)$ is equivalent to $f_\mathfrak{p}$ being even. Hence $S_\mathrm{m}(\mathrm{S}_4)$ is as claimed. As S_4 contains a subgroup isomorphic to D_3 and a Klein subgroup with no odd elements, we again conclude that $S_\mathrm{m} = S_\mathrm{M}$.

If H is dihedral one immediately obtains the above description of $S_\mathrm{m}(H)$ and $S_\mathrm{M}(H)$ from (5.1) and Lemmas 2.5 and 4.1.

Consider finally the case $H \cong \mathrm{A}_4$. By Lemma 2.9, H contains no odd elements. As before, we conclude that $S_\mathrm{m}(H)$ is empty and that H fixes no edge of $\mathcal{T}_\mathfrak{p}$ except possibly when $\mathfrak{p}$ is above 2 and $\mathfrak{p} \notin \mathrm{Ram}(B)$. Suppose $\mathfrak{p} \in S_\mathrm{M}(H)$, *i.e.*, H fixes an edge of $\mathcal{T}_\mathfrak{p}$. Then a cyclic group of order 3 fixes an edge. As $\mathfrak{p}$ is not above 3, this happens if and only if $k_\mathfrak{p}$ contains a primitive third root of unity (Lemma 2.1 and [2, Lemma 2.2]). This, in turn, is equivalent to the residue degree $f_\mathfrak{p}$ being even.

Conversely, assume that $\mathfrak{p}$ is above 2 and that $f_{\mathfrak{p}}$ is even. We must show that $H \cong \mathrm{A}_4$ fixes two adjacent maximal orders of $B_{\mathfrak{p}}$. By Lemma 2.8, $B_{\mathfrak{p}} = A \otimes_{\mathbb{Q}_2} k_{\mathfrak{p}}$, where A is the unique quaternion division algebra over $\mathbb{Q}_2$. Thus A is generated over $\mathbb{Q}_2$ by the usual Hamilton quaternions $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$. As $f_{\mathfrak{p}}$ is even, $\mathfrak{p} \notin \mathrm{Ram}(B)$. By the remark preceding Lemma 2.9, after conjugating we may assume that H is generated by the projective images of $\mathbf{i}$ and of $\alpha_3 = (1+\mathbf{i}+\mathbf{j}+\mathbf{k})/2$. Let $F \subset k_{\mathfrak{p}}$ be the unramified extension of $\mathbb{Q}_2$ of degree $f_{\mathfrak{p}}$. Since $f_{\mathfrak{p}}$ is even, F splits the division algebra A, *i.e.*, $B_F = A \otimes_{\mathbb{Q}_2} F \cong \mathrm{M}(2,F)$. Let $R \subset A$ be the unique maximal order of A and let $R_F = R \otimes_{\mathbb{Z}_2} \mathcal{O}_F \subset B_F$. Note that H fixes any maximal order of B_F containing R since H is generated by the class of $\mathbf{i}$ and α_3, which are units in R. Let D be any maximal order of B_F containing R_F (as R_F has discriminant $2\mathcal{O}_F$, it is not maximal). Let $\alpha \in A^*$ satisfy $\mathrm{ord}_2\big(\mathrm{nr}(\alpha)\big) = 1$. Then α, considered as an element of B_F, is odd since $F/\mathbb{Q}_2$ is unramified. Thus $D_\alpha := \alpha D \alpha^{-1} \neq D$. But $R \subset D_\alpha$ since $R \subset D$ and $\alpha R \alpha^{-1} = R$. We conclude that H fixes two distinct maximal orders of B_F. Since $\mathcal{T}_{\mathcal{F}}$ is a tree, we see that H must fix two adjacent maximal orders of B_F. On tensoring up to $k_{\mathfrak{p}}$, the same holds for $B_{\mathfrak{p}}$. □

In applications to 3-orbifolds [4] the following is useful.

COROLLARY 5.2. — *Let S be a finite set of primes of k disjoint from* $\mathrm{Ram}(B)$, *let $\mathcal{D}$ be a maximal order of B, and let $\widetilde{S}$ be the union of S and all primes of k lying above 2 and not in* $\mathrm{Ram}(B)$. *Assume that B has only one $\widetilde{S}$-type of maximal orders. Then $\Gamma_{S,\mathcal{D}}$ contains a Klein group if and only if there exist d and w in k^* such that the following three conditions hold:*

- $B = (d, w)$,
- $\{\mathfrak{p} \notin \mathrm{Ram}(B) \big|\ d \text{ or } w \text{ is odd at } \mathfrak{p}\} \subset S$,
- $S \subset \{\mathfrak{p} \notin \mathrm{Ram}(B) \big|\ d \text{ or } w \text{ is odd at } \mathfrak{p}, \text{ or } \mathfrak{p} \text{ divides } 2\}$.

$\Gamma_{S,\mathcal{D}}$ contains a dihedral group of order 8 if and only if $\Gamma_{S,\mathcal{D}}$ contains a cyclic group of order 4 and if there is a $w \in k^*$ for which the three conditions above hold with $d = -1$.

6. Examples.

We now give some sample calculations to illustrate the results of §3 and §5. As we are mainly interested in $\mathrm{PGL}(2,\mathbb{C})$, all our numbers fields k below have exactly one complex place and $\mathrm{Ram}(B)$ includes all real places of k.

Example 1. — Let $k = \mathbb{Q}(x)$, where x is a root of $x^3 - x - 1 = 0$. This is the unique cubic field of discriminant -23, $\mathcal{O}_k = \mathbb{Z}[x]$, x is a fundamental unit, $x = 1.32\cdots$ at the real place v_∞ of k, the primes 2 and 3 remain prime in $\mathcal{O}_k$ and there is exactly one prime $\mathfrak{p}_5 = (2 - x)$ of norm 5. Let B be the quaternion algebra over k ramified only at v_∞ and $\mathfrak{p}_5$. Up to conjugation, there is a unique maximal order $\mathcal{D} \subset B$ because the narrow class group of k is trivial. Let us first find the finite subgroups of B^*/k^*. As k contains no subfield $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ other than $\mathbb{Q}$, condition (1) in Lemma 2.3 implies that B^*/k^* cannot contain cyclic subgroups C_n with $n > 4$. Since $\mathfrak{p}_5$ is split in $k(\sqrt{-1})$, (2) in Lemma 2.3 rules out a C_4. By the same lemma, there is a (unique up to conjugation) C_3 in B^*/k^*. There are, of course, infinitely many (non-conjugate) C_2's in B^*/k^*. By Lemma 2.3, there are infinitely many D_3's and D_2's, *i.e.*, S_3's and Klein groups, in B^*/k^*. As $B \neq (-1,-1)$ (since 2 is inert and $[k : \mathbb{Q}]$ is odd [13, p. 33]), there is no A_4, S_4 or A_5 in B^*/k^*.

Let us now take S empty and see which of the above groups is contained in $\Gamma_\mathcal{D} = \Gamma_{\phi,\mathcal{D}}$. By Lemma 2.3 and (D_{ℓ^r}) following Theorem 5.1, an $S_3 \subset \Gamma_\mathcal{D}$ if and only if for some $w \in k^*$ we have

(1) $B = (-3, w)$.

(2) w is even at all primes $\mathfrak{p} \neq \mathfrak{p}_5$.

As $\mathcal{O}_k$ has narrow class number 1 and we can always change w modulo squares, it follows from (2) that $\pm w$ is one of 1, x, $x - 2$ or $x(x - 2)$. By (1), w must be negative at v_∞ and the local Hilbert symbols must be $(-3, w)_{\mathfrak{p}_5} = -1$, $(-3, w)_\mathfrak{p} = 1$ for $\mathfrak{p} \neq \mathfrak{p}_5$. This leaves $w = x - 2$ or $w = x(x - 2)$ as the only possibilities. Note that both of these w are generators of $\mathfrak{p}_5$. Now, -3 is not a square in $k_{\mathfrak{p}_5} \cong \mathbb{Q}_5$, hence $(-3, x-2)_{\mathfrak{p}_5} = -1 = \big(-3, x(x-2)\big)_{\mathfrak{p}_5}$. As $w \in \mathcal{O}_{k_3}^*$, $(-3, w)_3 = 1$ if and only if w is a square in k_3. This in turn happens if and only if w is a square in $\mathcal{O}_k/(3) \cong \mathbb{F}_3[x]/(x^3 - x - 1)$. Over $\mathbb{F}_3$, $x \equiv (x^2 + x - 1)^2$ (modulo $x^3 - x - 1$) and $x - 2 \equiv (x^2 + 1)^2$ (modulo $x^3 - x - 1$). As there is only one prime above 2, we conclude that $B = \big(-3, x(x - 2)\big) = \big(-3, x - 2\big)$. This shows that there are two S_3's in $\Gamma_\mathcal{D}$. By Lemma 2.4, they are not B^*/k^*-conjugate. The point here is that x is not a square.

Let us now compute the C_2's in $\Gamma_\mathcal{D}$. By Theorem 3.6, these correspond to $w = x - 2$, $w = x(x - 2)$ or $w = -x$. Corollary 5.2 yields that the only (up to conjugation) Klein group in $\Gamma_\mathcal{D}$ corresponds to $B = (-x, x - 2)$. To verify $(-x, x - 2)_{\mathfrak{p}_5} = -1$, one can use the isomorphism $\mathcal{O}_k/\mathfrak{p}_5 \cong \mathbb{Z}[x]/(x^3 - x - 1, x - 2) \cong \mathbb{Z}/5$ taking x to 2 (modulo 5). Note that $B = \big(-x, x(x - 2)\big)$ corresponds to the same Klein group, by Lemma 2.4. Hence we have found the complete list of finite subgroups of $\Gamma_\mathcal{D}$.

Elementary group theory [4, Lemma 2.2.1] now shows any torsion-free subgroup of $\Gamma_{\mathcal{D}}$ has index divisible by 12. In fact, there is a torsion-free subgroup $\widetilde{\Gamma} \subset \Gamma_{\mathcal{D}}$ of index 12 which can be described as follows. Let $\mathcal{D}^1$ consist of the elements of $\mathcal{D}$ of reduced norm 1 and set $\Gamma^1_{\mathcal{D}} = \mathcal{D}^1/\{\pm 1\}$. Since k has class number 1, $\Gamma^1_{\mathcal{D}}$ is isomorphic to a subgroup of index 4 in $\Gamma_{\mathcal{D}}$ [1, §8.5, 8.6]. Set $\widetilde{\Gamma} = \{u \in \mathcal{D}^1 \mid u \in 1 + \mathcal{M}\}$, where $\mathcal{M}$ is the maximal ideal of the maximal order in the local division algebra $B_{\mathfrak{p}_5}$. Then $\widetilde{\Gamma}$ injects into $\Gamma^1_{\mathcal{D}}$ and $\widetilde{\Gamma}$ is torsion-free because it embeds in a pro-5-group while $\Gamma_{\mathcal{D}}$ has no 5-torsion. Working in $B_{\mathfrak{p}_5}$ one finds $[\Gamma^1_{\mathcal{D}} : \widetilde{\Gamma}] = 3$. Hence $\widetilde{\Gamma} \subset \Gamma_{\mathcal{D}}$ with index 12 and $\widetilde{\Gamma}$ is torsion-free. By the results in [4], the 3-manifold corresponding to $\widetilde{\Gamma}$ is the Weeks manifold, that being the one of smallest volume among all arithmetic, hyperbolic 3-manifolds.

In the foregoing example we were able to quickly calculate all finite subgroups of $\Gamma_{\mathcal{D}}$. When the unit rank or the class group grows, this can become a more difficult task, as the next few examples show.

Example 2. — Let $k = \mathbb{Q}(x)$, where x is a root of $f(x) = x^5 + x^4 - 3x^3 - 2x^2 + x - 1 = 0$, and let B be the algebra ramified at all three real places and at $\mathfrak{p}_3 = (x+2)$, the prime of norm 3. This field is the unique quintic of discriminant $-9759 = -3 \cdot 3253$, having ring of integers $\mathbb{Z}[x]$. The prime 2 is inert in $k/\mathbb{Q}$ and k has narrow class number 1, as discriminant estimates show [10, pp. 161, 185]. Just as in the example above, one quickly rules out all cyclic subgroups of B^*/k^* other than a C_2 or C_3. Let us show that there is no C_3. We have

$$f(x) \equiv (x+2)^2(x^3 - x + 2) \text{ (modulo 3)},$$

showing that 3 splits in k as $(3) = \mathfrak{p}_3^2\,\mathfrak{p}_{27}$, where $\mathfrak{p}_{27}$ is a prime of norm 27. Hence $f(x) = q_2(x)q_3(x)$, where $q_2(x), q_3(x) \in \mathbb{Z}_3[x]$ are irreducible 3-adic polynomials of degree 2 and 3, respectively. Thus $k_{\mathfrak{p}_3} = \mathbb{Q}_3(\sqrt{D})$, where D is the discriminant of $q_2(x)$. We find that $f(x)$ factors uniquely modulo 9 as

$$f(x) \equiv (x^2 - 2x + 4)(x^3 + 3x^2 - x + 2) \text{ (modulo 9)}.$$

Thus, $D \equiv -3$ (modulo 9) and so $k_{\mathfrak{p}_3} = \mathbb{Q}_3(\sqrt{-3}) = \mathbb{Q}_3(\zeta_3)$. It follows that $\mathfrak{p}_3$ splits in $k(\zeta_3)$. Condition (2) in Lemma 2.1 implies then that there is no C_3 in B^*/k^*. Hence $\Gamma_{\mathcal{D}}$ contains at most C_2's and Klein groups for any maximal order $\mathcal{D}$. The computation of all C_2's and Klein groups is possible (as fundamental units are readily calculated), but quite tedious since $\mathcal{O}_k^*$ has

$\mathbb{Z}$-rank 3. There is at least one Klein group in $\Gamma_{\mathcal{D}}$ since $B = (-1, -x-2)$. In this example, $\Gamma_{\mathcal{D}}$ has no torsion-free subgroup of index 4 [4].

Example 3. — Let $k = \mathbb{Q}(x)$, where x is a root of $x^4 + x^3 - 2x - 1 = 0$, and let B be the algebra ramified only at the two real places. This is the unique quartic field of discriminant $-275 = 5^2 \cdot 11$. It is a quadratic extension of $\mathbb{Q}(\sqrt{5})$ and has narrow class number one. Since 2 is inert in $k/\mathbb{Q}$, $B = (-1, -1)$. Hence $\Gamma_{\mathcal{D}}$ contains an A_5, but no S_4. Again, one could compute all the smaller finite subgroups of $\Gamma_{\mathcal{D}}$. In [3] it is shown that $\Gamma_{\mathcal{D}}$ gives rise to the arithmetic hyperbolic 3-orbifold of smallest volume.

Example 4. — Let $k = \mathbb{Q}(\sqrt[4]{6})$ and let $B = (-1, -1)$ be the algebra ramified exactly at the two real places of k. As in example 1, only C_n for $n \leqslant 4$ need be considered. In this case $k(\zeta_3) = k(\sqrt{-3}) = k(\sqrt{-2})$, so the unique prime $\mathfrak{p}_3$ above 3 splits in $k(\zeta_3)$ (Proof: 3 splits in $\mathbb{Q}(\sqrt{-2})/\mathbb{Q}$). One computes the narrow class number of k to be 2. Thus there are two conjugacy types of maximal orders in B. Let us pick $\mathcal{D}$ in one type, $\widetilde{\mathcal{D}}$ in the other type. Using Theorems 3.1 to 3.3, we conclude that for maximal orders in just one type, say that of $\mathcal{D}$, there is a C_3 in $\Gamma_{\mathcal{D}}$. In contrast, $\Gamma_{\widetilde{\mathcal{D}}}$ has no elements of odd order. Note that $\mathcal{D}$ contains a primitive third root of unity and $\widetilde{\mathcal{D}}$ does not. Theorem 5.1 also shows that $\Gamma_{\mathcal{D}}$ contains an S_4, but no A_5.

We now consider the subgroups of order 2 in $\Gamma_{\mathcal{D}}$ or $\Gamma_{\widetilde{\mathcal{D}}}$. Theorem 3.6 shows that there is a bijection $C_{-\varepsilon_i} \leftrightarrow \varepsilon_i$ between such subgroups and all totally positive units of k modulo squares of units. A short calculation shows that this latter group has order 4. A subgroup (in the B^*/k^*-conjugacy class) corresponding to $C_{-\varepsilon_i}$ is in $\Gamma_{\mathcal{D}}$ or $\Gamma_{\widetilde{\mathcal{D}}}$, or both, depending on whether $\mathcal{O}_{k(\sqrt{-\varepsilon_i})}$ embeds in $\mathcal{D}$ or $\widetilde{\mathcal{D}}$, or both. For exactly one unit, say ε_1, we have $k(\sqrt{-\varepsilon_1}) = k(\zeta_3)$, that being the narrow Hilbert class field. The prime $\mathfrak{p}_2$ above 2 is either ramified ($i \neq 1$) or inert ($i = 1$) in $k(\sqrt{-\varepsilon_i})/k$. To see this for $i = 1$, note that $\mathfrak{p}_2$ has norm 2. It is therefore inert to the narrow Hilbert classfield $k(\zeta_3)$. Hence Theorem 3.6, especially condition (a), shows that each $C_{-\varepsilon_i}$ is in both $\Gamma_{\mathcal{D}}$ and $\Gamma_{\widetilde{\mathcal{D}}}$. Similarly, Corollary 3.5 shows that both $\Gamma_{\mathcal{D}}$ and $\Gamma_{\widetilde{\mathcal{D}}}$ contain a C_4, the point being that $k(\sqrt{-1})/k$ ramifies at $\mathfrak{p}_2$.

It remains to check for dihedral 2-groups $H \cong D_{2^r}$. But $S_{\mathrm{M}} = S_{\mathrm{M}}(H) = \{\mathfrak{p}_2\}$ generates $T(B)$. Hence there is just one S_{M}-type of maximal order. By Theorem 5.1, a conjugate of H is in $\Gamma_{\mathcal{D}}$ if and only if it is in $\Gamma_{\widetilde{\mathcal{D}}}$. By Corollary 5.2, the Klein groups in $\Gamma_{\mathcal{D}}$ correspond to all pairs $[-\varepsilon_i, -\varepsilon_j]$,

with identifications as explained in §2. Similarly, the dihedral subgroups of order 8 are in bijection with the ε_j, as $B = (-1, -\varepsilon)$ for any totally positive $\varepsilon \in \mathcal{O}_k^*$.

Example 5. — We give an example in which $\Gamma_{\mathcal{D}}$ contains elements of order two, but contains no dihedral group. Let k be a cubic field of narrow class number 1, having one complex place. Thus there is only one type of maximal order. For example, the field in example 1 will do. Let α be a generator of $\mathcal{O}_k^*/\{\pm 1\}$ such that $\alpha > 0$ at the real place of k. Choose a prime $\mathfrak{p}$ of k completely decomposed in $k(\sqrt{-1}, \sqrt{-\alpha})$ and let B ramify only at $\mathfrak{p}$ and at the real place. Let us check that $\Gamma_{\mathcal{D}}$ contains no dihedral 2-group. Suppose $w \in k^*$ represents an element of $\mathcal{C}_2 = \mathcal{C}_2(\phi, \mathcal{D}) \subset k^*/k^{*2}$ as in Theorem 3.6. Condition (2) in that theorem and the assumption that k has narrow class number one imply that $w = \pm 1, \pm\alpha, \pm\beta$ or $\pm\alpha\beta \pmod{k^{*2}}$, where $(\beta) = \mathfrak{p}$ and $\beta > 0$. All the + signs can be dismissed since condition (1) does not allow the real place to split in $k(\sqrt{w})$. Similarly, $w = -1$ or $w = -\alpha$ are ruled out by the hypothesis that $\mathfrak{p}$ splits in $k(\sqrt{-1}, \sqrt{-\alpha})$. Hence $\mathcal{C}_2$ consists of the two elements $-\beta$ and $-\alpha\beta \pmod{k^{*2}}$. We claim that the local Hilbert symbols $(w, w')_{\mathfrak{p}}$ are trivial if w, w' represent elements of $\mathcal{C}_2$. For example, consider

$$(-\beta, -\alpha\beta)_{\mathfrak{p}} = (-\beta, -\alpha)_{\mathfrak{p}}\,(-\beta, \beta)_{\mathfrak{p}}.$$

The first symbol on the right is $+1$ since $\mathfrak{p}$ splits in $k(\sqrt{-\alpha})$. The last symbol is $+1$ trivially. The proof that the other local symbols $(w, w')_{\mathfrak{p}}$ equal 1 is similar. Theorem 5.1 now shows that $\Gamma_{\mathcal{D}}$ contains no Klein group.

Example 6. — We conclude with an example of a torsion-free $\Gamma_{\mathcal{D}}$. The main difficulty is to make sure that $\Gamma_{\mathcal{D}}$ has no element of order 2. Let $N = \mathbb{Q}(x)$ be the quintic field generated over $\mathbb{Q}$ by a root x of $f(X) = X^5 - 2X^4 - 2X^3 + 2X^2 + X + 1$. Since $f(X)$ has discriminant -32411 and 32411 is prime, N has discriminant -32411 and $\mathcal{O}_N = \mathbb{Z}[x]$. The field N has 3 real places and 1 complex place. By hand or computer calculations one finds that N has class number one and narrow class number 2.

Suppose now that k is any quintic field having exactly three real places, odd wide class number and even narrow class number (for example, the field N above). Then there is a quadratic extension H/k unramified at all non-archimedean primes and ramified at least at one real place. Actually, such an H must be ramified at exactly two real places because the reciprocity map, from ideles of k to $\mathrm{Gal}(H/k) = \{\pm 1\}$, is both trivial

and equal to $(-1)^{(\text{number of ramified real places})}$ when evaluated at the global idele -1. Note that by classfield theory a prime $\mathfrak{p}$ of k which is inert to H cannot have trivial image in Cl_+/Cl_+^2, the narrow ideal class group of k modulo squares.

Let $F \subset k^*$ be the subgroup consisting of those $\gamma \in k^*$ which are either totally positive or totally negative and such that the principal ideal (γ) equals $\mathfrak{a}^2$ for some fractional ideal $\mathfrak{a} = \mathfrak{a}_{(\gamma)}$ of k. Let L be the compositum of all the $k(\sqrt{\gamma})$ for $\gamma \in F$. To see that L/k is a finite extension, note that $\gamma^h = \alpha\beta^2$, where h is the wide class number, α is a unit of k and $\beta \in k^*$. Because h is odd, $k(\sqrt{\gamma}) = k(\sqrt{\gamma^h}) = k(\sqrt{\alpha})$. Hence $[L : k] \leqslant [\mathcal{O}_k^* : (\mathcal{O}_k^*)^2] = 2^4$. Let $L' = L(\zeta_3) = L(\sqrt{-3})$. By Kummer theory, any quadratic extension F/k with $F \subset L'$ is of the form $k(\sqrt{\gamma})$ or $k(\sqrt{-3\gamma})$ for some $\gamma \in F$. In particular, either all or none of the three real places of k ramify in F. Hence, if H is the field defined above, $H \cap L' = k$. We may therefore fix a prime $\mathfrak{p}$ of k relatively prime to 3 which is completely decomposed in L'/k and inert in H/k.

Let B be the algebra ramified at $\mathfrak{p}$ and at the three real places. Theorem 3.3 implies that the only possible $C_n \subset \Gamma_{\mathcal{D}}$, with n odd, is a C_3. But, by construction, $\mathfrak{p} \in \mathrm{Ram}(B)$ splits to $k(\sqrt{-3})$ as $\mathfrak{p}\mathcal{O}_{k(\sqrt{-3})} = \mathfrak{p}'\mathfrak{p}''$. Hence $\mathrm{Norm}_{k/\mathbb{Q}}(\mathfrak{p}) = \mathrm{Norm}_{k(\sqrt{-3})/\mathbb{Q}}(\mathfrak{p}') = \mathrm{Norm}_{k(\sqrt{-3})/\mathbb{Q}}(\mathfrak{p}'') \equiv 1 \bmod 3$. Hence, Theorem 3.3 shows that $\Gamma_{\mathcal{D}}$ contains no elements of odd order.

To prove the same for the 2-part, we now show that $\mathcal{C}_2 = \mathcal{C}_2(\phi, \mathcal{D})$ in Theorem 3.6 is empty. Suppose $w \in k^*$ represents an element of $\mathcal{C}_2$. From (1) and (2) in Theorem 3.6, we find that w is totally negative and that either $w \in F$ or $(w) = \mathfrak{a}^2\mathfrak{p}$ for some fractional ideal $\mathfrak{a}$. The latter possibility would imply that $\mathfrak{p}$ has trivial image in Cl_+/Cl_+^2, which we showed above is impossible because $\mathfrak{p}$ is inert in H. Thus $w \in F$. But by construction $\mathfrak{p}$ is split to $k(\sqrt{w})$, contradicting condition (1) in Theorem 3.6. We conclude that $\mathcal{C}_2$ is empty and so $\Gamma_{\mathcal{D}}$ is torsion-free.

BIBLIOGRAPHY

[1] 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.

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

[3] T. Chinburg and E. Friedman, The smallest arithmetic hyperbolic 3-orbifold, Invent. Math., 86 (1986), 507-527

[4] T. CHINBURG, E. FRIEDMAN, K. JONES and A. W. REID, The arithmetic hyperbolic 3-manifold of smallest volume, Ann. Scuola Norm. Sup. Pisa (to appear).

[5] M. DEURING, Algebren, Springer Verlag, Berlin, 1935.

[6] W. FEIT, Exceptional subgroups of GL_2, Appendix to chapter XI of Introduction to Modular Forms by S. Lang, Berlin, Springer Verlag, 1976.

[7] F. W. GEHRING and G. J. MARTIN, 6-torsion and hyperbolic volume, Proc. Amer. Math. Soc., 117 (1993), 727-735.

[8] F. W. GEHRING, C. MACLACHLAN, G. J. MARTIN and A. W. REID, Arithmeticity, discreteness and volume, Trans. Amer. Math. Soc., 349 (1997), 3611-3643.

[9] K. N. JONES and A. W. REID, Minimal index torsion-free subgroups of Kleinian groups, Math. Ann., 310 (1998), 235-250.

[10] J. MARTINET, Petits discriminants des corps de nombres. In J. Armitage, editor, Number Theory Days, 1980 (Exeter 1980). London Math. Soc. Lecture Notes Ser. 56, Cambridge: Cambridge Univ. Press, 1982.

[11] J.-P. SERRE, Trees, Springer Verlag, Berlin, 1980.

[12] L. WASHINGTON, Introduction to Cyclotomic Fields, Springer Verlag, Berlin, 1982.

[13] M.-F. VIGNÉRAS, Arithmétique des algèbres de Quaternions, Lecture Notes in Math. 800, Springer Verlag, Berlin, 1980.

Manuscrit reçu le 18 octobre 1999,
accepté le 27 avril 2000.

T. CHINBURG,
University of Pennsylvania
Departement of Mathematics
Philadelphia, PA 19104 (U.S.A.)
ted@math.upenn.edu

E. FRIEDMAN,
Universidad de Chile, Facultad de Ciencias
Depto de Matematicas
Casilla 653
Santiago 1 (Chile).
friedman@abello.dic.uchile.cl