A classification of $\mathbb{R}$-Fuchsian subgroups of Picard modular groups

Parkkonen, Jouni; Paulin, Frédéric

© Les auteurs et Confluentes Mathematici, 2018.

Year: 2018

Version: Published version

Copyright: © Les auteurs et Confluentes Mathematici, 2018.

Rights: In Copyright

Rights url: http://rightsstatements.org/page/InC/1.0/?language=en

Please cite the original version:

A classification of \( \mathbb{R} \)-Fuchsian subgroups of Picard modular groups

Jouni Parkkonen Frédéric Paulin

February 19, 2019

Abstract

Given an imaginary quadratic extension \( K \) of \( \mathbb{Q} \), we classify the maximal nonelementary subgroups of the Picard modular group \( \text{PU}(1, 2; \mathcal{O}_K) \) preserving a totally real totally geodesic plane in the complex hyperbolic plane \( \mathbb{H}^2_{\mathbb{C}} \). We prove that these maximal \( \mathbb{R} \)-Fuchsian subgroups are arithmetic, and describe the quaternion algebras from which they arise. For instance, if the radius \( \Delta \) of the corresponding \( \mathbb{R} \)-circle lies in \( \mathbb{N} - \{0\} \), then the stabiliser arises from the quaternion algebra \( \left( \Delta, |D_K| \right)_{\mathbb{Q}} \).

We thus prove the existence of infinitely many orbits of \( K \)-arithmetic \( \mathbb{R} \)-circles in the hypersphere of \( \mathbb{P}^2_{\mathbb{C}} \).\(^1\)

1 Introduction

Let \( h \) be a Hermitian form with signature \( (1, 2) \) on \( \mathbb{C}^3 \). The projective unitary Lie group \( \text{PU}(1, 2) \) of \( h \) contains exactly two conjugacy classes of connected Lie subgroups locally isomorphic to \( \text{PSL}_2(\mathbb{R}) \). The subgroups in one class are conjugate to \( \text{P}(\text{SU}(1, 1) \times \{1\}) \) and they preserve a complex projective line for the projective action of \( \text{PU}(1, 2) \) on the projective plane \( \mathbb{P}^2_{\mathbb{C}} \), and those of the other class are conjugate to \( \text{PO}(1, 2) \) and preserve a maximal totally real subspace of \( \mathbb{P}^2_{\mathbb{C}} \). The groups \( \text{PSL}_2(\mathbb{R}) \) and \( \text{PU}(1, 2) \) act as the groups of holomorphic isometries, respectively, on the upper halfplane model \( \mathbb{H}^2_{\mathbb{R}} \) of the real hyperbolic space and on the projective model \( \mathbb{H}^2_{\mathbb{C}} \) of the complex hyperbolic plane defined using the form \( h \).

If \( \Gamma \) is a discrete subgroup of \( \text{PU}(1, 2) \), the intersections of \( \Gamma \) with the connected Lie subgroups locally isomorphic to \( \text{PSL}_2(\mathbb{R}) \) are its Fuchsian subgroups. The Fuchsian subgroups preserving a complex projective line are called \( \mathbb{C} \)-Fuchsian, and the ones preserving a maximal totally real subspace are called \( \mathbb{R} \)-Fuchsian. In [16], we gave a classification of the maximal \( \mathbb{C} \)-Fuchsian subgroups of the Picard modular groups, and we explicit their arithmetic structures, completing work of Chinburg-Stover (see Theorem 2.2 in version 3 of [3] and [4, Theo. 4.1]) and Möller-Toledo in [11], in analogy with the result of Maclachlan-Reid [10, Thm. 9.6.3] for the Bianchi subgroups in \( \text{PSL}_2(\mathbb{C}) \). In this paper, we prove analogous results for \( \mathbb{R} \)-Fuchsian subgroups, thus completing an arithmetic description of all Fuchsian subgroups of the Picard modular groups. The classification here

\(^1\)Keywords: Picard group, ball quotient, arithmetic Fuchsian groups, Heisenberg group, quaternion algebra, complex hyperbolic geometry, \( \mathbb{R} \)-circle, hypersphere. AMS codes: 11F06, 11R52, 20H10, 20G20, 53C17, 53C55
is more involved, as in some sense, there are more \( \mathbb{R} \)-Fuchsian subgroups than \( \mathbb{C} \)-Fuchsian ones. Our approach is elementary, some of the results can surely be obtained by more sophisticated tools from the theory of algebraic groups.

Let \( K \) be an imaginary quadratic number field, with discriminant \( D_K \) and ring of integers \( \mathcal{O}_K \). We consider the Hermitian form \( h \) defined by

\[
(p(z_0, z_1, z_2), q) \mapsto -\frac{1}{2} z_0 \overline{z_2} - \frac{1}{2} z_2 \overline{z_0} + z_1 z_1^\prime.
\]

The Picard modular group \( \Gamma_K = \text{PU}(1, 2) \cap \text{PGL}_3(\mathcal{O}_K) \) is a nonuniform arithmetic lattice of \( \text{PU}(1, 2) \). In this paper, we classify the maximal \( \mathbb{R} \)-Fuchsian subgroups of \( \Gamma_K \), and we explicit their arithmetic structures. The results stated in this introduction do not depend on the choice of the Hermitian form \( h \) of signature \( (2,1) \) defined over \( K \), since the algebraic groups over \( \mathbb{Q} \) whose groups of \( \mathbb{Q} \)-points are \( \text{PU}(1, 2) \cap \text{PGL}_3(K) \) depend up to \( \mathbb{Q} \)-isomorphism only on \( K \) and not on \( h \), see for instance [20, § 3.1], so that the Picard modular group \( \Gamma_K \) is well defined up to commensurability.

Let \( I_3 \) be the identity matrix and let \( I_{1,2} \) be the matrix of \( h \). Let

\[
\text{AHI}(\mathbb{Q}) = \{ Y \in \mathcal{M}_3(K) : Y^* I_{1,2} Y = I_{1,2} \text{ and } Y Y = I_3 \}
\]

be the set of \( \mathbb{Q} \)-points of an algebraic subset defined over \( \mathbb{Q} \), whose real points consist of the matrices of the Hermitian anti-holomorphic linear involutions \( z \mapsto Y z \) of \( \mathbb{C}^3 \). For instance,

\[
Y_\Delta = \begin{pmatrix}
0 & 0 & \frac{1}{\Delta} \\
0 & 1 & 0 \\
\Delta & 0 & 0
\end{pmatrix}
\]

belongs to \( \text{AHI}(\mathbb{Q}) \) for every \( \Delta \in K^\times \). The group \( \text{U}(1,2) \) acts transitively on \( \text{AHI}(\mathbb{R}) \) by

\[
(X, Y) \mapsto X Y X^{-1}
\]

for all \( X \in \text{U}(1,2) \) and \( Y \in \text{AHI}(\mathbb{R}) \). In Section 4, we prove the following result that describes the collection of maximal \( \mathbb{R} \)-Fuchsian subgroups of the Picard modular groups \( \Gamma_K \).

**Theorem 1.1.** The stabilisers in \( \Gamma_K \) of the projectivized rational points in \( \text{AHI}(\mathbb{Q}) \) are arithmetic maximal nonelementary \( \mathbb{R} \)-Fuchsian subgroups of \( \Gamma_K \). Every maximal nonelementary \( \mathbb{R} \)-Fuchsian subgroup of \( \Gamma_K \) is commensurable up to conjugacy in \( \text{PU}(1,2) \cap \text{PGL}_3(K) \) with the stabiliser \( \Gamma_{K, \Delta} \) in \( \Gamma_K \) of the projective class of \( Y_\Delta \), for some \( \Delta \in \mathcal{O}_K - \{0\} \).

A nonelementary \( \mathbb{R} \)-Fuchsian subgroup \( \Gamma \) of \( \text{PU}(1,2) \) arises from a quaternion algebra \( \mathfrak{D} \) over \( \mathbb{Q} \) if \( \mathfrak{D} \) splits over \( \mathbb{R} \) and if there exists a Lie group epimorphism \( \varphi \) from \( \mathfrak{D}(\mathbb{R})^1 \) to the conjugate of \( \text{PO}(1,2) \) containing \( \Gamma \) such that \( \Gamma \) and \( \varphi(\mathfrak{D}(\mathbb{Z})^1) \) are commensurable. In Section 5, we use the connection between quaternion algebras and ternary quadratic forms to describe the quaternion algebras from which the maximal nonelementary \( \mathbb{R} \)-Fuchsian subgroups of the Picard modular groups \( \Gamma_K \) arise.

---

\(^2\)See for instance [6, Chap. 5] and subsequent works of Falbel, Parker, Francsics, Lax, Xie, Wang, Jiang, Zhao and many others, for information on these groups, using different Hermitian forms of signature \( (2,1) \) defined over \( K \).
Theorem 1.2. For every $\Delta \in \mathcal{O}_K - \{0\}$, the maximal nonelementary $\mathbb{R}$-Fuchsian subgroup $\Gamma_{K,\Delta}$ of $\Gamma_K$ arises from the quaternion algebra with Hilbert symbol $(\frac{2\text{Tr}_{K/Q}\Delta, N_{K/Q}(\Delta)}{q})$ if $\text{Tr}_{K/Q}\Delta \neq 0$ and from $(\frac{1}{q}) \simeq \mathcal{M}_2(\mathbb{Q})$ otherwise.

This arithmetic description has the following geometric consequence. Recall that an $\mathbb{R}$-circle is a topological circle which is the intersection of the Poincaré hypersphere

$$\mathcal{H}^n = \{[z] \in \mathbb{P}_2(\mathbb{C}) : h(z) = 0\}$$

with a maximal totally real subspace of $\mathbb{P}_2(\mathbb{C})$. It is $K$-arithmetic if its stabiliser in $\Gamma_K$ has a dense orbit in it.

Corollary 1.3. There are infinitely many $\Gamma_K$-orbits of $K$-arithmetic $\mathbb{R}$-circles in the hypersphere $\mathcal{H}^n$.

The figure below shows the image under vertical projection from $\partial_{\infty} \mathbb{H}^2_\mathbb{C}$ to $\mathbb{C}$ of part of the $\Gamma_{\mathbb{Q}(i)}$-orbit of the standard infinite $\mathbb{R}$-circle, which is $\mathbb{Q}(i)$-arithmetic. The image of each finite $\mathbb{R}$-circle is a lemniscate. We refer to Section 3 and [5, §4.4] for an explanation of the terminology. See the main body of the text for other pictures of $K$-arithmetic $\mathbb{R}$-circles.

2 The complex hyperbolic plane

Let $h$ be the nondegenerate Hermitian form on $\mathbb{C}^3$ defined by

$$h(z) = z^*I_{1,2}z = -\text{Re}(z_0\overline{z_2}) + |z_1|^2,$$

where $I_{1,2}$ is the antidiagonal matrix

$$I_{1,2} = \begin{pmatrix} 0 & 0 & -\frac{1}{2} \\ 0 & 1 & 0 \\ -\frac{1}{2} & 0 & 0 \end{pmatrix}.$$
A point \( z = (z_0, z_1, z_2) \in \mathbb{C}^3 \) and the corresponding element \( [z] = [z_0 : z_1 : z_2] \in \mathbb{P}_2(\mathbb{C}) \) (using homogeneous coordinates) is negative, null or positive according to whether \( h(z) < 0 \), \( h(z) = 0 \) or \( h(z) > 0 \). The negative/null/positive cone of \( h \) is the subset of negative/null/positive elements of \( \mathbb{P}_2(\mathbb{C}) \).

The negative cone of \( h \) endowed with the distance \( d \) defined by

\[
\cosh^2 d([z],[w]) = \frac{|\langle z, w \rangle|^2}{h(z)h(w)},
\]

where \( \langle \cdot, \cdot \rangle \) is the sesquilinear form associated with \( h \), is the complex hyperbolic plane \( \mathbb{H}^2_{\mathbb{C}} \).

The distance \( d \) is the distance of a Riemannian metric with pinched negative sectional curvature \(-4 \leq K \leq -1\). The null cone of \( h \) is the Poincaré hypersphere \( \mathcal{H} \), which is naturally identified with the boundary at infinity of \( \mathbb{H}^2_{\mathbb{C}} \).

The Hermitian form \( h \) in this paper differs slightly from the one we used in \([15, 17, 16]\) and from the main Hermitian form used by Goldman and Parker (see \([5, 13, 14]\)). Hence we will need to give some elementary computations that cannot be found in the literature. This form is a bit more appropriate for arithmetic purposes concerning \( \mathbb{R} \)-Fuchsian subgroups, as it allows us to consider \( \mathbb{Z} \)-points of our linear algebraic groups and not their \( 2\mathbb{Z} \)-points.

Let \( U(1, 2) \) be the linear group of \( 3 \times 3 \) invertible matrices with complex coefficients preserving the Hermitian form \( h \). Let \( \text{PU}(1, 2) = U(1, 2)/U(1) \) be its associated projective group, where \( U(1) = \{ \zeta \in \mathbb{C} : |\zeta| = 1 \} \) acts by scalar multiplication. We denote by 
\([X] = [a_{ij}]_{1 \leq i,j \leq n} \in \text{PU}(1, 2)\) the image of \( X = (a_{ij})_{1 \leq i,j \leq n} \in U(1, 2) \). The linear action of \( U(1, 2) \) on \( \mathbb{C}^3 \) induces a projective action of \( \text{PU}(1, 2) \) on \( \mathbb{P}_2(\mathbb{C}) \) that preserves the negative, null and positive cones of \( h \) in \( \mathbb{P}_2(\mathbb{C}) \), and is transitive on each of them.

If

\[
X = \begin{pmatrix} a & \gamma & b \\ \alpha & A & \beta \\ c & \delta & d \end{pmatrix} \in \mathcal{M}_3(\mathbb{C}), \text{ then } I_{1,2}^{-1}X^*I_{1,2} = \begin{pmatrix} \bar{d} & -2\beta & \bar{b} \\ -\frac{\delta}{2} & \bar{A} & -\gamma \frac{1}{2} \\ \bar{c} & -2\alpha \bar{d} & \bar{a} \end{pmatrix}.
\]

The matrix \( X \) belongs to \( U(1, 2) \) if and only if \( X \) is invertible with inverse \( I_{1,2}^{-1}X^*I_{1,2} \), that is, if and only if

\[
\begin{cases}
ad + \bar{c}e - \frac{1}{2}\delta\bar{e} = 1 \\
\bar{a}\alpha + \bar{c}\beta - \frac{1}{2}A\delta = 0 \\
c\bar{d} + \bar{d}\bar{c} - \frac{1}{2}A|\delta|^2 = 0 \\
A\bar{A} - 2\alpha\beta - 2\beta\bar{\alpha} = 1 \\
\bar{a}\bar{b} + b\bar{\alpha} - \frac{1}{2}|\gamma|^2 = 0 \\
\bar{b}\alpha + \bar{\alpha}\beta - \frac{1}{2}A\gamma = 0.
\end{cases}
\]

Remark 2.1. A matrix \( X \in U(1, 2) \) in the above form is upper triangular if and only if \( c = 0 \). Indeed, then the third equality in Equation (1) implies that \( \delta = 0 \). The first two equations then become \( \bar{d} = 1 \) and \( \bar{a}\alpha = 0 \), so that \( \alpha = 0 \).

The Heisenberg group

\[
\text{Heis}_3 = \{ [w_0 : w : 1] \in \mathbb{P}_2(\mathbb{C}) : \text{Re } w_0 = |w|^2 \}
\]

with law 
\([w_0 : w : 1][w'_0 : w' : 1] = [w_0 + w'_0 + 2w'w, w + w' : 1] \) is identified with \( \mathbb{C} \times \mathbb{R} \) by the coordinate mapping \([w_0 : w : 1] \mapsto (w, \text{Im } w_0) = (\zeta, v)\). It acts isometrically on \( \mathbb{H}^2_{\mathbb{C}} \).
and simply transitively on $\mathcal{H} - \{ [1 : 0 : 0] \}$ by Heisenberg translations

$$t_{\zeta,v} = \begin{bmatrix} 1 & 2 \bar{\zeta} & |\zeta|^2 + iv \\ 0 & 1 & \zeta \\ 0 & 0 & 1 \end{bmatrix} \in \text{PU}(2,1)$$

with $\zeta \in \mathbb{C}$ and $v \in \mathbb{R}$. Note that $t_{\zeta,v}^{-1} = t_{-\zeta,-v}$ and $t_{\zeta,-v} = t_{\zeta,-v}^*$. The Heisenberg dilation with factor $\lambda \in \mathbb{C}^\times$ is the element

$$h_\lambda = \begin{bmatrix} \lambda & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \frac{1}{\lambda} \end{bmatrix} \in \text{PU}(1,2),$$

which normalizes the group of Heisenberg translations. The subgroup of $\text{PU}(1,2)$ generated by Heisenberg translations and Heisenberg dilations is called the group of Heisenberg similarities.

We end this subsection by defining the discrete subgroup of $\text{PU}(1,2)$ whose $\mathbb{R}$-Fuchsian subgroups we study in this paper.

Let $K$ be an imaginary quadratic number field, with $D_K$ its discriminant, $\mathcal{O}_K$ its ring of integers, $\text{Tr} : z \mapsto z + \bar{z}$ its trace and $\text{N} : z \mapsto |z|^2 = z \bar{z}$ its norm. Recall\(^3\) that there exists a squarefree positive integer $d$ such that $K = \mathbb{Q}(i\sqrt{d})$, that $D_K = -d$ and $\mathcal{O}_K = \mathbb{Z}[\frac{1+i\sqrt{d}}{2}]$ if $d \equiv -1 \mod 4$, and that $D_K = -4d$ and $\mathcal{O}_K = \mathbb{Z}[i\sqrt{d}]$ otherwise. Note that $\mathcal{O}_K$ is stable under conjugation, and that $\text{Tr}$ and $\text{N}$ take integral values on $\mathcal{O}_K$. A unit in $\mathcal{O}_K$ is an invertible element in $\mathcal{O}_K$. Since $\text{N} : K^\times \to \mathbb{R}^\times$ is a group morphism, we have $\text{N}(x) = 1$ for every unit $x$ in $\mathcal{O}_K$.

The Picard modular group

$$\Gamma_K = \text{PU}(1,2; \mathcal{O}_K) = \text{PU}(1,2) \cap \text{PGL}_3(\mathcal{O}_K)$$

is a nonuniform lattice in $\text{PU}(1,2)$.

### 3 The space of $\mathbb{R}$-circles

A (maximal) totally real subspace $V$ of the Hermitian vector space $(\mathbb{C}^3, \langle \rangle)$ is the fixed point set of a Hermitian antiholomorphic linear involution of $\mathbb{C}^3$, or, equivalently, a 3-dimensional real linear subspace of $\mathbb{C}^3$ such that $V$ and $JV$ are orthogonal, where $J : \mathbb{C}^3 \to \mathbb{C}^3$ is the componentwise multiplication by $i$. The intersection with $\mathbb{H}^3_\mathbb{C}$ of the image under projectivization in $\mathbb{P}_2(\mathbb{C})$ of a totally real subspace is called an $\mathbb{R}$-plane in $\mathbb{H}^3_\mathbb{C}$. The group $\text{PU}(1,2)$ acts transitively on the set of $\mathbb{R}$-planes, the stabiliser of each $\mathbb{R}$-plane being a conjugate of $\text{PO}(1,2)$. Note that $\text{PO}(1,2)$ is equal to its normaliser in $\text{PU}(1,2)$.

An $\mathbb{R}$-circle $C$ is the boundary at infinity of an $\mathbb{R}$-plane. See [12], [5, §4.4] and [7, §9] for references on $\mathbb{R}$-circles (introduced by E. Cartan). An $\mathbb{R}$-circle is infinite if it contains $\infty = [1 : 0 : 0]$ and finite otherwise. The group of Heisenberg similarities acts transitively on the set of finite $\mathbb{R}$-circles and on the set of infinite $\mathbb{R}$-circles.

The standard infinite $\mathbb{R}$-circle is

$$C_\infty = \{ [x_0 : x_1 : x_2] : x_0, x_1, x_2 \in \mathbb{R}, x_1^2 - x_0 x_2 = 0 \},$$

\(^3\text{See for instance [18].}\)
which is the boundary at infinity of the intersection with $\mathbb{H}^2_\mathbb{C}$ of the image in $\mathbb{P}_2(\mathbb{C})$ of $\mathbb{R}^3 \subset \mathbb{C}^3$. For every $D \in \mathbb{C}^\times$, the set

$$C_D = \{ [z_0 : x_1 : D \overline{z_0}] : z_0 \in \mathbb{C}, \ x_1 \in \mathbb{R}, \ x_1^2 - \text{Re}(\overline{D}z_0^2) = 0 \}$$

is a finite $\mathbb{R}$-circle, which is the boundary at infinity of the intersection with $\mathbb{H}^2_\mathbb{C}$ of the fixed point set of the projective Hermitian anti-holomorphic involution

$$[z_0 : z_1 : z_2] \mapsto \left[ \frac{z_2}{D} : \overline{\lambda} : D \overline{z_0} \right].$$

We call $C_1$ the standard finite $\mathbb{R}$-circle.

Let $C$ be a finite $\mathbb{R}$-circle. The center $\text{cen}(C)$ of $C$ is the image of $\infty = [1 : 0 : 0]$ by the unique projective Hermitian anti-holomorphic involution fixing $C$. The radius $\text{rad}(C)$ of $C$ is $\lambda^2$ where $\lambda \in \mathbb{C}^\times$ is such that there exists a Heisenberg translation $t$ mapping $0 = [0 : 0 : 1]$ to the center of $C$ with $C = t \circ h\lambda(C_1)$. For instance, $\text{cen}(C_D) = 0$ and $\text{rad}(C_D) = \frac{1}{D}$, since the Heisenberg dilations preserve $0$ and $C_D = h_{\lambda}(C_1)$. For every Heisenberg translation $t$, we have $\text{cen}(tC) = t\text{cen}(C)$ and $\text{rad}(tC) = \text{rad}(C)$. For every Heisenberg dilation $h_{\lambda}$, we have $\text{cen}(h_{\lambda}C) = h_{\lambda}\text{cen}(C)$ and $\text{rad}(h_{\lambda}C) = \lambda^2\text{rad}(C)$.

The image of a finite $\mathbb{R}$-circle under the vertical projection $(\zeta, v) \mapsto \zeta$ from $\text{Heis}_3 = \partial_\infty \mathbb{H}^2 \mathbb{C} - \{ \infty \}$ to $\mathbb{C}$ is a lemniscate, see [5, §4.4.5]. The figure below shows on the left six images of the standard infinite $\mathbb{R}$-circle under transformations in $\Gamma Q(\omega)$ where $\omega = -\frac{1 + \sqrt{3}}{2}$ is the usual third root of unity, and on the right their images in $\mathbb{C}$ under the vertical projection.

Let us introduce more notation in order to describe the space of $\mathbb{R}$-circles, see [5, §2.2.4] for more background. A $3 \times 3$ matrix $Y$ with complex coefficients is called unitary-symmetric if it is Hermitian with respect to the Hermitian form $h$ and invertible with inverse equal to its complex conjugate, that is, if $Y^* I_{1,2} Y = I_{1,2}$ and $Y \overline{Y} = I_3$, where $I_3$
is the $3 \times 3$ identity matrix. Note that for instance $I_3$ and, for every $D \in \mathbb{C}^3$, the matrix

$$Y_D = \begin{pmatrix} 0 & 0 & \frac{1}{D} \\ 0 & 1 & 0 \\ D & 0 & 0 \end{pmatrix}$$

is unitary-symmetric.

Let $\mathrm{AIH} = \{ Y \in \mathcal{M}_3(\mathbb{C}) : Y^* I_{1,2} Y = I_{1,2} \text{ and } Y \overline{Y} = I_3 \}$

be the set of unitary-symmetric matrices, which is a closed subset of $\mathrm{U}(1,2)$, identified with the set of Hermitian anti-holomorphic linear involutions $z \mapsto \overline{Y} z$ of $\mathbb{C}^3$. Note that $|\det Y| = 1$ for any $Y \in \mathrm{AIH}$. Let

$$\mathbb{P} \mathrm{AIH} = \{ [Y] \in \mathrm{PU}(1,2) : Y \overline{Y} = I_3 \}$$

be the image of $\mathrm{AIH}$ in $\mathrm{PU}(1,2)$, that is, the quotient $\mathrm{U}(1) \backslash \mathrm{AIH}$ of $\mathrm{AIH}$ modulo scalar multiplications by elements of $\mathrm{U}(1)$. The group $\mathrm{U}(1,2)$ acts transitively on $\mathrm{AIH}$ by

$$(X,Y) \mapsto XY \overline{X}^{-1}$$

for all $X \in \mathrm{U}(1,2)$ and $Y \in \mathrm{AIH}$, and the stabiliser of $I_3$ is equal to $\mathrm{O}(1,2)$.

For every $Y \in \mathrm{AIH}$, we denote by $P_Y$ the intersection with $\mathbb{H}^2_\mathbb{C}$ of the image in $\mathbb{P}^2(\mathbb{C})$ of the set of fixed points of $z \mapsto \overline{Y} z$. Note that $P_Y$ is an $\mathbb{R}$-plane, which depends only on the class $[Y]$ of $Y$ in $\mathrm{PU}(1,2)$. We denote by $C_Y = \partial_x P_Y$ the $\mathbb{R}$-circle at infinity of $P_Y$, which depends only on $[Y]$. For instance, $C_\infty = C_{I_3}$ and $C_D = C_{Y_D}$.

Let $\mathcal{C}_\mathbb{R}$ be the set of $\mathbb{R}$-circles, endowed with the topology induced by the Hausdorff distance between compact subsets of $\partial_x \mathbb{H}^2_\mathbb{C}$,\footnote{for any Riemannian distance on the smooth manifold $\partial_x \mathbb{H}^2_\mathbb{C}$} and let $\mathcal{P}_\mathbb{R}$ be the set of $\mathbb{R}$-planes\footnote{which are closed subsets of $\mathbb{H}^2_\mathbb{C}$} endowed with the topology of the Hausdorff convergence on compact subsets of $\mathbb{H}^2_\mathbb{C}$.

The projective action of $\mathrm{PU}(1,2)$ on the set of subsets of $\mathbb{P}^2(\mathbb{C})$ induces continuous transitive actions on $\mathcal{C}_\mathbb{R}$ and $\mathcal{P}_\mathbb{R}$, with stabilisers of $C_\infty = C_{I_3}$ and $P_I_3$ equal to $\mathrm{PO}(1,2)$. We hence have a sequence of $\mathrm{PU}(1,2)$-equivariant homeomorphisms

$$\begin{array}{cccc}
\mathrm{PU}(1,2)/\mathrm{PO}(1,2) & \rightarrow & \mathbb{P} \mathrm{AIH} & \rightarrow & \mathcal{P}_\mathbb{R} & \rightarrow & \mathcal{C}_\mathbb{R} \\
[X] \mathrm{PO}(1,2) & \mapsto & [XY^{-1}] & \mapsto & P & \mapsto & \partial_x P.
\end{array}$$

\begin{equation}
\label{eq:2}
\end{equation}

\textbf{Lemma 3.1.} \textit{Let $Y = \begin{pmatrix} a & \overline{\gamma} & b \\ \alpha & A & \beta \\ c & \overline{\delta} & d \end{pmatrix} \in \mathrm{AIH}$.}

\begin{itemize}
\item[(1)] \textit{For every $[X] \in \mathrm{PU}(1,2)$, we have $[X] C_Y = C_{XY} X^{-1}$.}
\item[(2)] \textit{The $\mathbb{R}$-circle $C_Y$ is infinite if and only if $c = 0$.}
\end{itemize}
(3) If the $\mathbb{R}$-circle $C_Y$ is finite, then its center is
\[
\text{cen}(C_Y) = [Y] \cong [a : \alpha : c],
\]
and its radius is
\[
\text{rad}(C_Y) = \frac{\overline{\alpha}c - \alpha \delta}{\overline{\alpha}^2} = -\frac{c}{\overline{\alpha}^2} \det Y.
\]
In particular, $|\text{rad}(C_Y)| = |c|^{-1}$.

**Proof.** (1) This follows from the equivariance of the homeomorphisms in Equation (2).

(2) Recall that $C_Y$ is the intersection with $\mathbb{C} \mathbb{H}^2$ of the image in the projective plane of the set of fixed points of the Hermitian anti-holomorphic linear involution $z \mapsto Y \overline{z}$. Hence $\infty = [1 : 0 : 0]$ belongs to $C_Y$ if and only if the image of $(1,0,0)$ by $Y$ is a multiple of $(1,0,0)$, that is, if and only if $\alpha = c = 0$. Using Remark 2.1, this proves the result.

(3) The first claim follows from the fact that the center of the $\mathbb{R}$-circle $C_Y$ is the image of $\infty = [1 : 0 : 0]$ under the projective map associated with $z \mapsto Y \overline{z}$. In order to prove the second claim, we start by the following lemma.

**Lemma 3.2.** For every $[Y] \in \mathbb{P} \mathbb{AHI}$, the center of $C_Y$ is equal to $0 = [0 : 0 : 1]$ if and only if there exists $D \in \mathbb{C}^\times$ such that $[Y] = [Y_D]$.

**Proof.** We have already seen that cen($C_{Y_D}$) = cen($C_D$) = 0. By the first claim of Lemma 3.1 (3), if cen($C_Y$) = 0, we have $a = \alpha = 0$. By the penultimate equality in Equation (1), we have $\gamma = 0$. Since $Y \overline{Y} = I_3$, we have $b \overline{\alpha} = 1$, $b \delta = 0$, $b \bar{d} = 0$ and $\beta \overline{\alpha} = 0$, so that
\[
Y = \begin{pmatrix} 0 & 0 & \frac{1}{\overline{\alpha}} \\ 0 & A & 0 \\ c & 0 & 0 \end{pmatrix}
\]
with $|A| = 1$. Since $[Y] = [\frac{1}{\overline{\alpha}} Y]$, the result follows with $D = \frac{c}{\overline{\alpha}}$. \(\square\)

Now, let $\zeta = \frac{a}{\overline{c}}$, $v = \text{Im} \frac{a}{\overline{c}}$ and $X = \begin{pmatrix} 1 & 2\overline{\zeta} & |\zeta|^2 + iv \\ 0 & 1 & \zeta \\ 0 & 0 & 1 \end{pmatrix}$. Note that since $Y \in U(1,2)$, we have
\[
|\alpha|^2 \overline{\text{Re}(a \overline{\alpha})} = h(a, \alpha, c) = h(Y(1,0,0)) = h(1,0,0) = 0.
\]
Hence
\[
\text{Re}(\frac{a}{c}) = \frac{1}{|c|^2} \text{Re}(a \overline{\alpha}) = \left|\frac{\alpha}{c}\right|^2 = |\zeta|^2.
\]

The Heisenberg translation $t_{\zeta,v} = [X]$ maps $0 = [0:0:1]$ to $[\frac{a}{c}:\alpha:c:1] = \text{cen}(C_Y)$. Since
\[
\text{cen}(C_{X^{-1}YX}) = \text{cen}(t_{\zeta,v}^{-1}C_Y) = t_{\zeta,v}^{-1} \text{cen}(C_Y) = 0,
\]
and by Lemma 3.2, the element $X^{-1}YX \in \mathbb{AHI}$ is anti-diagonal. A simple computation gives
\[
X^{-1}YX = \begin{pmatrix} 0 & 0 & \frac{1}{\overline{\alpha}} \\ 0 & A - \zeta \overline{\delta} & 0 \\ c & 0 & 0 \end{pmatrix}.
\]
If $D = \frac{c}{A - \zeta \overline{\delta}}$, we hence have $[X^{-1}YX] = [Y_D]$. Therefore
\[
\text{rad}(C_Y) = \text{rad}(t_{\zeta,v}^{-1}C_Y) = \text{rad}(C_{X^{-1}YX}) = \text{rad}(C_{Y_D}) = \frac{1}{D}.
\]
Since \( \det X = 1 \), we have \( \det Y = -\frac{c}{e} (A - \zeta \overline{A}) \), so that \( D = -\frac{e^2}{\det Y} \). The result follows. \( \square \)

We end this section by describing the algebraic properties of the objects in Equation (2). We refer for instance to [23, §3.1] for an elementary introduction to algebraic groups and their Zariski topology.

Let \( G \) be the linear algebraic group defined over \( \mathbb{Q} \), with set of \( \mathbb{R} \)-points \( \text{PU}(1, 2) \) and set of \( \mathbb{Q} \)-points

\[
\text{PU}(1, 2; K) = \text{PU}(1, 2) \cap \text{PGL}_3(K).
\]

We identify \( G \) with its image under the adjoint representation for integral point purposes, so that \( G(\mathbb{Z}) = \Gamma_K \).

Since \( I_{1,2} \) has rational coefficients, the set \( \mathbb{PAHI} \) of unitary-symmetric matrices modulo scalars is the set of real points \( \mathbb{PAHI} = \mathbb{PAHI}(\mathbb{R}) \) of an affine algebraic subset \( \mathbb{PAHI} \) defined over \( \mathbb{Q} \) of \( G \), whose set of rational points is

\[
\mathbb{PAHI}(\mathbb{Q}) = \mathbb{PAHI} \cap G(\mathbb{Q}) = \mathbb{PAHI} \cap \text{PGL}_3(K).
\]

The action of \( G \) on \( \mathbb{PAHI} \) defined by \( ([X], [Y]) \mapsto [XYX^{-1}] \) is algebraic defined over \( \mathbb{Q} \). This notion of rational point in \( \mathbb{PAHI} \) will be a key tool in the next section in order to describe the maximal nonelementary \( \mathbb{R} \)-Fuchsian subgroups of \( \Gamma_K \).

4 A description of the \( \mathbb{R} \)-Fuchsian subgroups of \( \Gamma_K \)

Our first result relates the nonelementary \( \mathbb{R} \)-Fuchsian subgroups of the Picard modular group \( \Gamma_K \) to the rational points in \( \mathbb{PAHI} \). The proof of this statement is similar to the one of its analog for \( \mathbb{C} \)-Fuchsian subgroups in [16].

**Proposition 4.1.** The stabilisers in \( \Gamma_K \) of the rational points in \( \mathbb{PAHI} \) are maximal nonelementary \( \mathbb{R} \)-Fuchsian subgroups of \( \Gamma_K \). Conversely, any maximal nonelementary \( \mathbb{R} \)-Fuchsian subgroup \( \Gamma \) of \( \Gamma_K \) fixes a unique rational point in \( \mathbb{PAHI} \) and \( \Gamma \) is an arithmetic lattice in the conjugate of \( \text{PO}(1, 2) \) containing it.

**Proof.** Let \( [Y] \in \mathbb{PAHI}(\mathbb{Q}) \) be a rational point in \( \mathbb{PAHI} \). Since the action of \( G \) on \( \mathbb{PAHI} \) is algebraic defined over \( \mathbb{Q} \), the stabiliser \( H \) of \( [Y] \) in \( G \) is algebraic defined over \( \mathbb{Q} \). Note that \( H \) is semi-simple with set of real points a conjugate of (the normaliser of \( \text{PO}(1, 2) \) in \( \text{PU}(1, 2) \), hence of) \( \text{PO}(1, 2) \). Therefore by the Borel-Harish-Chandra theorem [2, Thm. 7.8], the group \( \text{Stab}_\Gamma[Y] = H(\mathbb{Z}) \) is an arithmetic lattice in \( H(\mathbb{R}) \), and in particular is a maximal nonelementary \( \mathbb{R} \)-Fuchsian subgroup of \( \Gamma_K \).

Conversely, let \( \Gamma \) be a maximal nonelementary \( \mathbb{R} \)-Fuchsian subgroup of \( \Gamma_K \). Since it is nonelementary, its limit set \( \Lambda \Gamma \) contains at least three points. Two \( \mathbb{R} \)-circles having three points in common are equal. Hence \( \Gamma \) preserves a unique \( \mathbb{R} \)-plane \( P \). Let \( Y \in \text{AHI} \) be such that \( P = P_Y \). By the equivariance of the homeomorphisms in Equation (2), \( [Y] \) is the unique point in \( \mathbb{PAHI} \) fixed by \( \Gamma \).

Let \( H \) be the stabiliser in \( G \) of \( [Y] \), which is a connected algebraic subgroup of \( G \) defined over \( \mathbb{R} \), whose set of real points is conjugated to \( \text{PO}(1, 2) \). Since a nonelementary subgroup of a connected algebraic group whose set of real points is isomorphic to \( \text{PSL}_2(\mathbb{R}) \) is Zariski-dense in it, and since the Zariski-closure of a subgroup of \( G(\mathbb{Z}) \) is defined over \( \mathbb{Q} \) (see for instance [23, Prop. 3.1.8]), we hence have that \( H \) is defined over \( \mathbb{Q} \). The action of
the \( \mathbb{Q} \)-group \( G \) on the \( \mathbb{Q} \)-variety \( \mathbb{P} \text{AHII} \) is defined over \( \mathbb{Q} \), and the Galois group \( \text{Gal} (\mathbb{C}|\mathbb{Q}) \) acts on \( \mathbb{P} \text{AHII} \) and on \( G \) commuting with this action. For every \( \sigma \in \text{Gal} (\mathbb{C}|\mathbb{Q}) \), we have \( H^\sigma = H \). Hence by the uniqueness of the point in \( \mathbb{P} \text{AHII} \) fixed by a conjugate of \( \text{PO}(1,2) \), we have that \( [Y]^\sigma = [Y] \) for every \( \sigma \in \text{Gal} (\mathbb{C}|\mathbb{Q}) \). Thus \( [Y] \) is a rational point. \( \Box \)

An \( \mathbb{R} \)-circle \( C \) is \( K \)-arithmetic if its stabiliser in \( \Gamma_K \) has a dense orbit in \( C \). Proposition 4.1 explains this terminology: The stabiliser in \( \Gamma_K \) of a \( K \)-arithmetic \( \mathbb{R} \)-circle is arithmetic (in the conjugate of \( \text{PO}(1,2) \) containing it). With \( \omega = \frac{-1+i\sqrt{3}}{2} \), the figure below shows part of the \( \Gamma_{\mathbb{Q}(\omega)} \)-orbit of the standard infinite \( \mathbb{R} \)-circle \( C_\infty \), which is \( K \)-arithmetic.

The next result reduces, up to commensurability and conjugacy in \( \text{PU}(1,2;K) \), the class of nonelementary \( \mathbb{R} \)-Fuchsian subgroups that we will study. Note that \( \text{PU}(1,2;K) \) is the commensurator of \( \Gamma_K \) in \( \text{PU}(1,2) \), see \([1, \text{Theo. 2}]\).

**Proposition 4.2.** Any maximal nonelementary \( \mathbb{R} \)-Fuchsian subgroup \( \Gamma \) of \( \Gamma_K \) is commensurable up to conjugacy in \( \text{PU}(1,2;K) \) with the stabiliser in \( \Gamma_K \) of the rational point \( [Y_\Delta] \in \mathbb{P} \text{AHII}\)\(^6\) for some \( \Delta \in \mathcal{O}_K \). If \( \Delta \in \mathbb{N} - \{0\} \) and if

\[
\gamma_0 = \begin{bmatrix}
\frac{1+i}{2\sqrt{\Delta}} & 0 & \frac{1-i}{2\sqrt{\Delta}} \\
0 & 1 & 0 \\
\frac{(1-i)\sqrt{\Delta}}{2} & 0 & \frac{(1+i)\sqrt{\Delta}}{2}
\end{bmatrix},
\]

then \( \gamma_0 \in \text{PU}(1,2) \) and we have \( \text{Stab}_{\Gamma_K}[Y_\Delta] = \gamma_0 \text{PO}(1,2)\gamma_0^{-1} \cap \Gamma_K \).

**Proof.** Let \( \Gamma \) be as in the statement. By Proposition 4.1, there exists a rational point \( [Y] \in \mathbb{P} \text{AHII}(\mathbb{Q}) \) in \( \mathbb{P} \text{AHII} \) such that \( \Gamma = \text{Stab}_{\Gamma_K}[Y] = \text{Stab}_{\Gamma_K}C_Y \). Up to conjugating \( \Gamma \) by\(^6\) or equivalently to the stabiliser in \( \Gamma_K \) of the \( \mathbb{R} \)-circle \( C_\Delta \)
an element in \( \Gamma_K \), we may assume that the \( \mathbb{R} \)-circle \( \mathcal{C}_Y \) is finite. The center of the finite \( \mathbb{R} \)-circle \( \mathcal{C}_Y \) belongs to \( \mathbb{P}_2(K) \cap (\partial_x \mathbb{H}_K^2 - \{\infty\}) \) by Lemma 3.1 (3). The group of Heisenberg translations with coefficients in \( K \) acts (simply transitively) on \( \mathbb{P}_2(K) \cap (\partial_x \mathbb{H}_K^2 - \{\infty\}) \).

Hence up to conjugating \( \Gamma \) by an element in \( \text{PU}(1,2; K) \), we may assume that the center of the \( \mathbb{R} \)-circle \( \mathcal{C}_Y \) is \( 0 = [0 : 0 : 1] \). By Lemma 3.2 (and its proof), there exists \( \Delta \in K - \{0\} \) such that \( [Y] = [Y_\Delta] \). Since for every \( \lambda \in \mathbb{C}^\times \) we have \( h_\lambda[Y_\Delta] h_\lambda^{-1} = [Y_{\Delta \lambda^{-1}}] \), up to conjugating \( \Gamma \) by a Heisenberg dilation with coefficients in \( K \), we may assume that \( \Delta \in \mathcal{O}_K \).

Fixing square roots of \( \Delta \) and \( \overline{\Delta} \) such that \( \sqrt{\overline{\Delta}} = \sqrt{\Delta} \), let
\[
\gamma_0' = \begin{bmatrix}
\frac{1+i}{2\sqrt{\Delta}} & 0 & \frac{1-i}{2\sqrt{\Delta}} \\
0 & 1 & 0 \\
\frac{(1-i)\sqrt{\Delta}}{2} & 0 & \frac{(1+i)\sqrt{\Delta}}{2}
\end{bmatrix}.
\]
One easily checks using Equation (1) that \( \gamma_0' \in \text{PU}(1,2) \). An easy computation proves that \( \gamma_0'[I_3] \gamma_0'^{-1} = \gamma_0 \gamma_0^{-1} = [Y_\Delta] \). Since the stabiliser of \( [I_3] \) for the action of \( \text{PU}(1,2) \) on \( \mathbb{AH}_H \) is equal to \( \text{PO}(1,2) \), the fact that
\[
\text{Stab}_{\Gamma_K} [Y_\Delta] = \gamma_0' \text{PO}(1,2) \gamma_0'^{-1} \cap \Gamma_K
\]
follows from the equivariance properties of the homeomorphisms in Equation (2). Furthermore, \( \gamma_0' \) is the only element of \( \text{PU}(1,2) \) satisfying this formula, up to right multiplication by an element of \( \text{PO}(1,2) \). The last claim of Proposition 4.2 follows since \( \gamma_0 = \gamma_0' \) when \( \Delta \in \mathbb{N} - \{0\} \).

Here is a geometric interpretation of the invariant \( \Delta \) introduced in Proposition 4.2: Since \( \text{rad}(C_{Y_\Delta}) = \text{rad}(C_\Delta) = \frac{1}{8} \) for every \( \Delta \in \mathbb{C}^\times \), the above proof shows that if the \( \mathbb{R} \)-circle \( C_\Gamma \) preserved by \( \Gamma \) is finite, then we may take \( \Delta \in \mathcal{O}_K - \{0\} \) squarefree (uniquely defined modulo a square unit, hence uniquely defined if \( D_K \neq -4,-3 \)) such that
\[
\Delta \in \left( \frac{\text{rad}(C_\Gamma)}{2} \right)^{-1} (\mathbb{K}^\times)^2.
\]

5 Quaternion algebras, ternary quadratic forms and \( \mathbb{R} \)-Fuchsian subgroups

In this section, we describe the arithmetic structure of the maximal nonelementary \( \mathbb{R} \)-Fuchsian subgroups of \( \Gamma_K \). By Proposition 4.2, it suffices to say from which quaternion algebra the \( \mathbb{R} \)-Fuchsian subgroup
\[
\Gamma_{K, \Delta} = \text{Stab}_{\Gamma_K} [Y_\Delta]
\]
arises for any \( \Delta \in \mathcal{O}_K - \{0\} \).

Let \( D, D' \in \mathbb{Q}^\times \). The quaternion algebra \( \mathcal{Q} = \left( \frac{D, D'}{\mathbb{Q}} \right) \) is the 4-dimensional central simple algebra over \( \mathbb{Q} \) with standard generators \( i, j, k \) satisfying the relations \( i^2 = D, j^2 = D' \) and \( ij = -ji = k \). If \( x = x_0 + x_1 i + x_2 j + x_3 k \) is an element of \( \mathcal{Q} \), we denote its conjugate by
\[
\overline{x} = x_0 - x_1 i - x_2 j - x_3 k.
\]
its (reduced) \textit{trace} by
\[
\text{tr} x = x + \overline{x} = 2x_0,
\]
and its (reduced) \textit{norm} by
\[
\mathfrak{n}(x_0 + x_1 i + x_2 j + x_3 k) = x \overline{x} = x_0^2 - D x_1^2 - D' x_2^2 + D D' x_3^2.
\]
The group of elements in \( \mathcal{D}(\mathbb{Z}) = \mathbb{Z} + i \mathbb{Z} + j \mathbb{Z} + k \mathbb{Z} \) with norm 1 is denoted by \( \mathcal{D}(\mathbb{Z})^1 \). We refer to \([22]\) and \([10]\) for generalities on quaternion algebras.

The quaternion algebra \( \mathcal{D} \) \textit{splits over} \( \mathbb{R} \) if the \( \mathbb{R} \)-algebra \( \mathcal{D}(\mathbb{R}) = \mathcal{D} \otimes \mathbb{Q} \mathbb{R} \) is isomorphic to the \( \mathbb{R} \)-algebra \( \mathcal{M}_2(\mathbb{R}) \) of 2-by-2 matrices with real entries. We say that a nonelementary \( \mathbb{R} \)-Fuchsian subgroup \( \Gamma \) of \( \text{PU}(1, 2) \) \textit{arises from} the quaternion algebra \( \mathcal{D} = \left( \frac{D}{D'} \right) \) if \( \mathcal{D} \) splits over \( \mathbb{R} \) and if there exists a Lie group epimorphism \( \varphi \) from \( \mathcal{D}(\mathbb{R})^1 \) to the conjugate of \( \text{PO}(1, 2) \) containing \( \Gamma \), with kernel the center \( Z(\mathcal{D}(\mathbb{R})^1) \) of \( \mathcal{D}(\mathbb{R})^1 \), such that \( \Gamma \) and \( \varphi(\mathcal{D}(\mathbb{Z})^1) \) are commensurable.

Let \( \mathscr{Q} \) be the set of isomorphism classes of quaternion algebras over \( \mathbb{Q} \). For every \( A \in \mathscr{Q} \), we denote by
\[
A_0 = \{ x \in A : \text{tr} x = 0 \}
\]
the linear subspace of \( A \) of \textit{pure quaternions}, generated by \( i, j, k \). Let \( \mathscr{T}_Q \) be the set of isometry classes of nondegenerate ternary quadratic forms over \( \mathbb{Q} \) with \textit{discriminant}\(^7\) a square. It is well known (see for instance \([10, \S 2.3-2.4]\) and \([22, \S 1.3]\)) that the map \( \Phi \) from \( \mathscr{Q} \) to \( \mathscr{T}_Q \), which associates to \( A \in \mathscr{Q} \) the \textit{restricted norm form} \( \mathfrak{n}_{|A_0} \), is a bijection. The map \( \Phi \) has the following properties, for every \( A \in \mathscr{Q} \).

1. If \( a, b \in \mathbb{Q}^\times \) and \( A \) is (the isomorphism class of) \( \left( \frac{a}{b} \right) \), then \( \Phi(A) \) is (the equivalence class of) \(-a x_1^2 - b x_2^2 + ab x_3^2 \), whose discriminant is \((ab)^2\).

2. If \( a, b, c \in \mathbb{Q}^\times \) with \( abc \) a square in \( \mathbb{Q} \) and if \( q \in \mathscr{T}_Q \) is (the equivalence class of) \(-a x_1^2 - b x_2^2 + c x_3^2 \), then \( \Phi^{-1}(q) \) is (the isomorphism class of) \( \left( \frac{a}{c} \right) \), since if \( abc = \lambda^2 \) with \( \lambda \in \mathbb{Q} \), then the change of variables \((x_1', x_2', x_3') = (x_1, x_2, \frac{\lambda}{abc} x_3)\) over \( \mathbb{Q} \) turns \( q \) to the equivalent form \(-a x_1^2 - b x_2^2 + ab x_3^2 \).

3. The quaternion algebra \( A \) splits over \( \mathbb{R} \) if and only if \( \Phi(A) \) is isotropic over \( \mathbb{R} \) (that is, if the real quadratic form \( \Phi(A) \) is indefinite), see \([22, \text{Coro I.3.2}]\).

4. The map \( \Theta_A \) from \( A(\mathbb{R})^\times \) to the special orthogonal group \( \text{SO}_{\Phi(A)}(A) \) of \( \Phi(A) \), sending the class of an element \( a \in A(\mathbb{R})^\times \) to the linear map \( a_0 \mapsto aa_0a^{-1} \) from \( A_0 \) to itself, is a Lie group epimorphism with kernel the center of \( A(\mathbb{R})^\times \) (see \([10, \text{Th. 2.4.1}]\)). If \( A(\mathbb{Z}) = \mathbb{Z} + i \mathbb{Z} + j \mathbb{Z} + k \mathbb{Z} \) is the usual order in \( A \), then \( \Theta_A \) sends \( A(\mathbb{Z})^1 \) to a subgroup commensurable with \( \text{SO}_{\Phi(A)}(\mathbb{Z}) \).

\textbf{Proof of Theorem 1.2.} The set \( P_\Delta \) of fixed points of the linear Hermitian anti-holomorphic involution \( z \mapsto Y_\Delta \overline{z} \) from \( \mathbb{C}^3 \) to \( \mathbb{C}^3 \) is a real vector space of dimension 3, equal to
\[
P_\Delta = \{ z \in \mathbb{C}^3 : z = Y_\Delta \overline{z} \} = \{ (z_0, z_1, z_2) \in \mathbb{C}^3 : z_1 = \overline{z}_1, \ z_2 = \Delta \overline{z}_0 \}.
\]
Let \( V \) be the vector space over \( \mathbb{Q} \) such that \( V(\mathbb{R}) = \mathbb{C}^3 \) and \( V(\mathbb{Q}) = K^3 \). Since the coefficients of the equations defining \( P_\Delta \) are in \( \mathbb{Q} \), there exists a vector subspace \( W = W_\Delta \)

\(^7\)the determinant of the associated matrix
of $V$ over $\mathbb{Q}$ such that $W(\mathbb{R}) = P_\Delta$. The restriction to $W$ of the Hermitian form $h$, which is defined over $\mathbb{Q}$, is a ternary quadratic form $q = q_\Delta$ defined over $\mathbb{Q}$, that we now compute.

Since $K = \mathbb{Q} + i\sqrt{|D_K|} \mathbb{Q}$, we write
\[ \Delta = u + i\sqrt{|D_K|} v \]
with $u, v \in \mathbb{Q}$, and the variables $z_j = x_j + i\sqrt{|D_K|} y_j$ with $x, y \in \mathbb{R}$ for $j \in \{0, 1, 2\}$. If $(z_0, z_1, z_2) \in P_\Delta$, we have
\[
h(z_0, z_1, z_2) = -\text{Re}(z_2 \overline{z_0}) + |z_1|^2 = -\text{Re}(\Delta \overline{\Delta}^2) + |z_1|^2
\]
\[= -u x_0^2 + u|D_K| y_0^2 - 2|D_K|v x_0 y_0 + x_1^2.\]

The right hand side of this formula is a ternary quadratic form $q = q_\Delta$ on $P_\Delta$, whose coefficients are indeed in $\mathbb{Q}$. It is nondegenerate and has nonzero discriminant $-w$, where
\[ w = v^2 D_K + u^2 |D_K| = N(\Delta)|D_K| \in \mathbb{Q} - \{0\}. \]

By equivariance of the homeomorphisms in Equation (2) and as $\text{Stab}_{PU(1,2)}[Y_\Delta]$ is equal to its normaliser, the map from $\text{Stab}_{PU(1,2)}[Y_\Delta]$ to the projective orthogonal group $\text{PO}_q$ of the quadratic space $(P_\Delta, q)$, induced by the restriction map from $\text{Stab}_{PU(1,2)} P_\Delta$ to $\text{O}(q)$, sending $g$ to $g|_{P_\Delta}$, is a Lie group isomorphism. It sends the lattice $\Gamma_{K,\Delta}$ to a subgroup commensurable with the lattice $\text{PO}_q(2)$ in $\text{PO}_q$. If we find a nondegenerate quadratic form $q' = q'_\Delta$ equivalent to $q$ over $\mathbb{Q}$ up to a rational scalar multiple, whose discriminant is a rational square, and which is isotropic over $\mathbb{R}$, then $\Gamma_{K,\Delta}$ arises from the quaternion algebra $\Phi^{-1}(q')$, by Properties (3) and (4) of the bijection $\Phi$.

First assume that $u = 0$. By an easy computation, we have
\[ q = -\left(-x_1^2 - \frac{|D_K|v}{2} (x_0 - y_0)^2 + \frac{|D_K|v}{2} (x_0 + y_0)^2\right). \]

The quadratic form $q' = -X_1^2 - \frac{|D_K|v}{2} X_2^2 + \frac{|D_K|v}{2} X_3^2$ over $\mathbb{Q}$ is equivalent to $q$ over $\mathbb{Q}$ up to sign. Its discriminant is the rational square $(\frac{|D_K|v}{2})^2$, and $q'$ represents $0$ over $\mathbb{R}$. By Property (2) of the bijection $\Phi$, we have $\Phi^{-1}(q') = \left(\frac{|D_K|v}{2}\right)^2 = \left(\frac{1}{2}\right)^2$. Therefore if $u = 0$, then $\Gamma_{K,\Delta}$ arises from the trivial quaternion algebra $\mathbb{H}_2(\mathbb{Q})$.

Now assume that $u \neq 0$. By an easy computation, we have
\[ q = -\frac{1}{u} \left(-u x_1^2 - (u^2 D_K^2 + u^2 |D_K|) y_0^2 + (u x_0 + |D_K|v y_0)^2\right) \]
\[= -\frac{1}{u^2 w} \left(-u^2 w x_1^2 - u w^2 y_0^2 + u w(u x_0 + |D_K|v y_0)^2\right). \]

The quadratic form $q' = -u w^2 X_1^2 - u w^2 X_2^2 + u w X_3^2$ is equivalent to $q$ over $\mathbb{Q}$ up to a scalar multiple in $\mathbb{Q}$. Its discriminant is the rational square $(uw)^4$ and it represents $0$ over $\mathbb{R}$. By Property (2) of the bijection $\Phi$, we have $\Phi^{-1}(q') = \left(\frac{uw}{\sqrt{Q}}\right)^2 = \left(\frac{u}{\sqrt{Q}}\right)^2$. Therefore if $u \neq 0$, since $u = \frac{1}{2} \text{Tr} \Delta$ and $w = N(\Delta)|D_K|$, then $\Gamma_{K,\Delta}$ arises from the quaternion algebra $\left(\frac{2 \text{Tr} \Delta, N(\Delta)|D_K|}{\mathbb{Q}}\right)$. This concludes the proof of Theorem 1.2. \[ \square \]

**Corollary 5.1.** Let $\Delta, \Delta' \in \mathcal{O}_K - \{0\}$ with nonzero traces. The maximal nonelementary $\mathbb{R}$-Fuchsian subgroups $\Gamma_{K,\Delta}$ and $\Gamma_{K,\Delta'}$ are commensurable up to conjugacy in $PU(1,2)$ if and only if the quaternion algebras $\left(\frac{2 \text{Tr} \Delta, N(\Delta)|D_K|}{\mathbb{Q}}\right)$ and $\left(\frac{2 \text{Tr} \Delta', N(\Delta')|D_K|}{\mathbb{Q}}\right)$ over $\mathbb{Q}$ are isomorphic.
Proof. Since the action of $\text{PU}(1,2)$ on the set of $\mathbb{R}$-planes $\mathcal{P}$ is transitive, this follows from the fact that two arithmetic Fuchsian groups are commensurable up to conjugacy in $\text{PSL}_2(\mathbb{R})$ if and only if their associated quaternion algebras are isomorphic (see [21]).

To complement Theorem 1.2, we give a more explicit version of its proof in the special case when $\Delta \in \mathbb{N} \setminus \{0\}$.

**Proposition 5.2.** Let $\Delta \in \mathbb{N} \setminus \{0\}$. The maximal nonelementary $\mathbb{R}$-Fuchsian subgroup $\Gamma_{K, \Delta}$ arises from the quaternion algebra $(\frac{\Delta}{Q_D})$.

**Proof.** Let $\Delta \in \mathbb{N} \setminus \{0\}$. Let $D = \frac{|D_K|}{4}$ if $D_K \equiv 0 \mod 4$ and $D = |D_K|$ otherwise, so that $O_K \cap \mathbb{R} = \mathbb{Z}$ and $O_K \cap i\mathbb{R} = i\sqrt{D}\mathbb{Z}$. Let $D' = D\Delta$. We have $D, D' \in \mathbb{N} \setminus \{0\}$. Let $\mathcal{Q} = (\frac{D}{D'})$.

The matrices

\[
e_0 = \begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix}, \quad e_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad e_2 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}
\]

form a basis of the Lie algebra $\mathfrak{sl}_2(\mathbb{R}) = \left\{ \begin{pmatrix} x_1 & -x_0 \\ x_2 & -x_1 \end{pmatrix} : x_0, x_1, x_2 \in \mathbb{R} \right\}$ of $\text{PSL}_2(\mathbb{R})$. Note that

\[-\det(x_0e_0 + x_1e_1 + x_2e_2) = -x_0x_2 + x_1^2\]

is the quadratic form restriction of $h$ to $\mathbb{R}^3 \subset \mathbb{C}^3$. We thus have a well known **exceptional isomorphism** between $\text{PSL}_2(\mathbb{R})$ and the identity component $\text{SO}_0(1,2)$ of $\text{O}(1,2)$, which associates to $g \in \text{PSL}_2(\mathbb{R})$ the matrix in the basis $(e_0, e_1, e_2)$ of the linear automorphism $\text{Ad}(g) : X \mapsto gXg^{-1}$, which belongs to $\text{GL}(\mathfrak{sl}_2(\mathbb{R}))$. We denote by $\Theta : \text{PSL}_2(\mathbb{R}) \rightarrow \text{PU}(1,2)$ the group isomorphism onto its image $\text{PO}(1,2)$ obtained by composing this exceptional isomorphism first with the inclusion of $\text{SO}_0(1,2)$ in $\text{U}(1,2)$, then with the canonical projection in $\text{PU}(1,2)$. Explicitly, we have by an easy computation

\[
\Theta : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a^2 & 2ab & b^2 \\ ac & ad + bc & bd \\ c^2 & 2cd & d^2 \end{pmatrix}.
\]

We have a map $\sigma_{D,-D'} : \mathcal{Q} \rightarrow \mathcal{M}_2(\mathbb{R})$ defined by

\[
(x_0 + x_1i + x_2j + x_3k) \mapsto \begin{pmatrix} x_0 + x_1\sqrt{D} \\ -(x_2 - x_3\sqrt{D})\sqrt{D'} \\ x_0 - x_1\sqrt{D} \end{pmatrix}.
\]

As is well-known\(^8\), the induced map $\sigma : \mathcal{Q}(\mathbb{R})^1 \rightarrow \text{PSL}_2(\mathbb{R})$ is a Lie group epimorphism with kernel $Z(\mathcal{Q}(\mathbb{R})^1)$, such that $\sigma(\mathcal{Q}(\mathbb{Z})^1)$ is a discrete subgroup of $\text{PSL}_2(\mathbb{R})$. With $\gamma_0$ as in Proposition 4.2, for all $x_0, x_1, x_2, x_3 \in \mathbb{Z}$, a computation gives that the element $\gamma_0 \Theta(\sigma(x_0 + x_1i + x_2j + x_3k)) \gamma_0^{-1}$ of $\text{PU}(1,2)$ is equal to

\[
\begin{bmatrix} a(x) & b(x) & c(x)/\Delta \\ d(x)\sqrt{\Delta} & n(x) & -d(x)/\sqrt{\Delta} \\ c(x)\Delta & b(x) & a(x) \end{bmatrix},
\]

\(^8\)see for instance [8]
where
\[
a(x) = x_0^2 + Dx_1^2 + (2D'x_2x_3)i\sqrt{D},
\]
\[
b(x) = 2(x_1x_2 + x_0x_3 + (x_1x_3 + \frac{x_0x_2}{D})i\sqrt{D})\frac{\sqrt{DD'}}{\sqrt{\Delta}},
\]
\[
c(x) = DD'x_3^2 + D'x_2^2 + 2x_0x_1i\sqrt{D},
\]
\[
d(x) = (x_0x_3 - x_1x_2 + (\frac{x_0x_2}{D} - x_1x_3)i\sqrt{D})\sqrt{DD'}.
\]

Let us consider the order $\mathcal{O}$ of $\mathcal{D}$ defined by
\[
\mathcal{O} = \{x_0 + x_1i + x_2j + x_3k \in \mathcal{D}(\mathbb{Z}) : x_1, x_2, x_3 \equiv 0 \mod D\}.
\]
Since \(\frac{\sqrt{DD'}}{\sqrt{\Delta}} = D \in \mathbb{Z}\) and \(\sqrt{DD'\Delta} = D' \in \mathbb{Z}\), the above computation shows that the subgroup $\gamma_0 \Theta(\sigma(\mathcal{E}^1)) \gamma_0^{-1}$ of $\text{PU}(1, 2)$ is contained in $\Gamma_K$. Since
\[
(D, -D') \cdot (|D_K|, -|D_K|) = (|D_K|, \Delta),
\]
the result follows. 

\[\square\]

\textbf{Remark.} Note that by Hilbert’s Theorem 90, if $\Delta' \in K$ satisfies $|\Delta'| = 1$, then there exists $\Delta'' \in \mathcal{O}_K - \{0\}$ such that $\Delta' = \frac{\Delta''}{x^r}$, so that the Heisenberg dilation $h_{\Delta''}$ commensurates $\Gamma_{K, \Delta'}$ to $\Gamma_{K, N(\Delta''')}$. Hence Proposition 5.2 implies that $\Gamma_{K, \Delta'}$ arises from the quaternion algebra $\left(\frac{N(\Delta''), |D_K|}{\mathbb{Q}}\right)$.

We conclude this paper by a series of arithmetic and geometric consequences of the above determination of the quaternion algebras associated with the maximal nonelementary $\mathbb{R}$-Fuchsian subgroups of the Picard modular groups. Their proofs follow closely the arguments in [9] pages 309 and 310, and a reader not interested in the arithmetic details may simply admit that they follow by formally replacing $-d$ by $d$ in the statements of loc. cit.

Recall that given $a \in \mathbb{Z} - \{0\}$ and $p$ an odd positive prime not dividing $a$, the Legendre symbol \(\left(\frac{a}{p}\right)\) is equal to 1 if $a$ is a square mod $p$ and to $-1$ otherwise. Recall\(^9\) that if $d \in \mathbb{Z} - \{0\}$ is squarefree, a positive prime $p$ is either
- \textit{ramified} in $\mathbb{Q}(\sqrt{d})$ when $p \mid d$ if $p$ is odd, and when $d \equiv 2, 3 \pmod{4}$ if $p = 2$,
- \textit{split} in $\mathbb{Q}(\sqrt{d})$ when $p \not\mid d$ and $\left(\frac{d}{p}\right) = 1$ if $p$ is odd, and when $d = 1 \pmod{8}$ if $p = 2$,
- \textit{inert} in $\mathbb{Q}(\sqrt{d})$ when $p \not\mid d$, and $\left(\frac{d}{p}\right) = -1$ if $p$ is odd, and when $d = 5 \pmod{8}$ if $p = 2$.

Recall that a quaternion algebra $A$ over $\mathbb{Q}$ is determined up to isomorphism by the finite (with even cardinality) set $\text{RAM}(A)$ of the positive primes $p$ at which $A$ \textit{ramifies}, that is, such that $A \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is a division algebra.

\textbf{Proposition 5.3.} Let $A$ be an indefinite quaternion algebra over $\mathbb{Q}$. If the positive primes at which $A$ is ramified are either \textit{ramified} or \textit{inert} in $\mathbb{Q}((\sqrt{|D_K|}))$, then there exists a maximal nonelementary $\mathbb{R}$-Fuchsian subgroup of $\Gamma_K$ whose associated quaternion algebra is $A$.

\(^9\)See for instance [18, page 91].
Proof. Recall\(^\text{10}\) that for all \(a, b \in \mathbb{Z} - \{0\}\) and for all positive primes \(p\), the \((p)\)-Hilbert symbol \((a, b)_p\), equal to \(-1\) if \((\frac{a \cdot b}{q_p})\) is a division algebra and \(1\) otherwise, is symmetric in \(a, b\), and satisfies \((a, bc)_p = (a, b)_p (a, c)_p\) and

\[
(a, b)_p = \begin{cases} 
(-1)^{\frac{u-1}{2} \cdot \frac{v-1}{2} + \alpha \frac{u-1}{2} \cdot \beta \frac{v-1}{2}} & \text{if } p = 2, a = 2^u u, b = 2^v v, \text{ with } u, v \text{ odd} \\
\left(\frac{a}{p}\right) & \text{if } p \neq 2, p \not| a, p \not| b, p^2 \not| b.
\end{cases}
\] (3)

Let \(d = \frac{|D_K|}{4}\) if \(D_K \equiv 0 \mod 4\) and \(d = |D_K|\) otherwise, so that \(d \in \mathbb{N} - \{0\}\) is squarefree. Given \(A\) as in the statement, we may write \(\text{RAM}(A) = \{p_1, \ldots, p_r, r_1, \ldots, r_s\}\) with \(p_i\) inert in \(\mathbb{Q}(\sqrt{d})\), and \(r_i\) ramified in \(\mathbb{Q}(\sqrt{d})\), so that the prime divisors of \(d\) are \(r_1, \ldots, r_s, s_1, \ldots, s_k\), unless some \(r_i\), say \(r_1\), is equal to \(2\) and \(d \equiv 3 \mod 4\), in which case the prime divisors of \(d\) are \(r_2, \ldots, r_s, s_1, \ldots, s_k\). As in [9, page 310], let \(q\) be an odd prime different from all \(p_i, r_i, s_i\) such that

- \(q = p_1 \cdots p_r\) \[8\] if no \(r_i\) is equal to \(2\), \(q = 5 p_1 \cdots p_r\) \[8\] if \(r_i = 2\) and \(d = 2 \mod 4\) and \(q = 3 p_1 \cdots p_r\) \[8\] if \(r_i = 2\) and \(d = 3 \mod 4\),
- for every \(i = 1, \ldots, s\), if \(r_i\) is odd, then \(\left(\frac{q}{r_i}\right) = -\left(\frac{p_1 \cdots p_r}{r_i}\right)\),
- for every \(i = 1, \ldots, k\), if \(s_i\) is odd, then \(\left(\frac{q}{s_i}\right) = \left(\frac{p_1 \cdots p_r}{s_i}\right)\).

With \(\Delta = p_1 \cdots p_r q\), which is a positive squarefree integer, let us prove that \(A\) is isomorphic to \((\frac{d, \Delta}{\mathbb{Q}})\). This proves the result by Proposition 5.2. By the characterisation of the quaternion algebras over \(\mathbb{Q}\), we only have to prove that for every positive prime \(t\) not in \(\text{RAM}(A)\), we have \((d, \Delta)_t = 1\) and for every positive prime \(t\) in \(\text{RAM}(A)\), we have \((d, \Delta)_t = -1\). We distinguish in the first case between \(t = q\), \(t = s_i\), \(t = 2\) and \(t \neq q, s_1, \ldots, s_k, 2\), and in the second case between \(t = p_i\) and \(t = r_i\). By using several times Equation (3) and the fact that \(\left(\frac{d}{q}\right) = 1\) since \(r + s\) is even as \(A\) is indefinite, the result follows (see the Appendix for details).

Recall that the \textit{wide commensurability} class of a subgroup \(H\) of a given group \(G\) is the set of subgroups of \(G\) which are commensurable up to conjugacy in \(G\). Two groups are \textit{abstractly commensurable} if they have isomorphic finite index subgroups.

**Corollary 5.4.** Every Picard modular group \(\Gamma_K\) contains infinitely many wide commensurability classes in \(\text{PU}(1, 2)\) of (uniform) maximal nonelementary \(\mathbb{R}\)-Fuchsian subgroups.

Corollary 1.3 of the introduction follows from Corollary 5.4. Note that there is only one wide commensurability class of nonuniform maximal nonelementary \(\mathbb{R}\)-Fuchsian subgroups of \(\Gamma_K\), by [10, Thm. 8.2.7].

**Proof.** As seen in Corollary 5.1, two maximal nonelementary \(\mathbb{R}\)-Fuchsian subgroups are commensurable up to conjugacy in \(\text{PU}(1, 2)\) if and only if their associated quaternion algebras are isomorphic. Two such quaternion algebras are isomorphic if and only if they ramify over the same set of primes. By Proposition 5.3, for every finite set \(I\) with even cardinality of positive primes which are inert over \(\mathbb{Q}(\sqrt{|D_K|})\), the quaternion algebra with ramification set equal to \(I\) is associated with a maximal nonelementary \(\mathbb{R}\)-Fuchsian subgroup. Since there are infinitely many inert primes over \(\mathbb{Q}(\sqrt{|D_K|})\), the result follows.

\(^{10}\)See for instance [22], in particular pages 32 and 37, and [19, Chap. III].
Corollary 5.5. Any arithmetic Fuchsian group whose associated quaternion algebra \( A \) is defined over \( \mathbb{Q} \) has a finite index subgroup isomorphic to an \( \mathbb{R} \)-Fuchsian subgroup of some Picard modular group \( \Gamma_K \).

Proof. As in [9] page 310, if \( \text{RAM}(A) = \{p_1, \ldots, p_n\} \), let \( d \in \mathbb{N} - \{0\} \) be such that \( \left( \frac{d}{p_i} \right) = -1 \) if \( p_i \) is odd and \( d = 5 \) if \( p_i = 2 \), so that \( p_1, \ldots, p_n \) are inert in \( \mathbb{Q}(\sqrt{d}) \), and take \( K = \mathbb{Q}(\sqrt{-d}) \). \( \Box \)

Corollary 5.6. For all quadratic imaginary number fields \( K \) and \( K' \), there are infinitely many abstract commensurability classes of Fuchsian subgroups with representatives in both Picard modular groups \( \Gamma_K \) and \( \Gamma_{K'} \).

Proof. There are infinitely many primes \( p \) such that \( \left( \frac{|D_K|}{p} \right) = \left( \frac{|D_{K'}|}{p} \right) = -1 \), hence infinitely many finite subsets of them with an even number of elements. \( \Box \)

Acknowledgements
The second author would like to thank the Isaac Newton Institute for Mathematical Sciences, Cambridge, for support and hospitality in April 2017 during the programme “Non-positive curvature group actions and cohomology”. This work was supported by EPSRC grant № EP/K032208/1 and by the French-Finnish CNRS grant PICS № 6950. We thank a lot John Parker, in particular for simplifying Lemma 3.1, and Yves Benoist, whose suggestion to use the relation between quaternion algebras and ternary quadratic form was critical for the conclusion of Section 5. We also thank Gaëtan Chenevier for his help with the final corollaries.

A Details on the proof of Proposition 5.3

Let us prove in preamble that

\[
\left( \frac{d}{q} \right) = 1.
\]

By using the quadratic reciprocity law for the Jacobi symbol, and its multiplicativity properties, by the second and third assumptions on \( q \), since the \( p_\ell \)'s are inert in \( \mathbb{Q}(\sqrt{d}) \), since \( r + s \) is even and \( q - p_1 \ldots p_r \equiv 0 \) \( [4] \) by the first assumption on \( q \), we have if the \( r_j \)'s, \( s_i \)'s and \( p_\ell \)'s are odd

\[
\left( \frac{d}{q} \right) = (-1)^{s+\frac{q+1}{2} \frac{d-1}{2}} \prod_j \left( \frac{p_1 \ldots p_r}{r_j} \right) \prod_i \left( \frac{p_1 \ldots p_r}{s_i} \right) = (-1)^{s+\frac{q+1}{2} \frac{d-1}{2}} \frac{p_1 \ldots p_r}{d} \left( \frac{d}{p_1 \ldots p_r} \right) = (-1)^{s+\frac{q-p_1 \ldots p_r-1}{2} \frac{d-1}{2}} \left( \frac{d}{p_1 \ldots p_r} \right) = (-1)^{s+\frac{q-p_1 \ldots p_r}{2} \frac{d-1}{2}} \prod_{\ell=1}^r \left( \frac{d}{p_\ell} \right) = (-1)^{r+s+\frac{q-p_1 \ldots p_r}{2} \frac{d-1}{2}} = 1.
\]

Recall that the Jacobi symbol satisfies \( \left( \frac{2}{n} \right) = (-1)^{n^2-1} \) for every odd positive integer \( n \). Similarly, if some \( s_i \) is not odd (which implies that the \( r_j \)'s and \( p_\ell \)'s are odd), say \( s_1 = 2 \),
then with $d' = d/2$ which is odd, since $q^2 - (p_1 \ldots p_r)^2 \equiv 0 \pmod{16}$ by the first assumption on $q$, we have

$$
\left(\frac{d}{q}\right) = \left(\frac{2}{q}\right)\left(\frac{d'}{q}\right) = (-1)^{\frac{q-1}{2} + \frac{d' - 1}{2}} \prod_{j}(\frac{p_1 \ldots p_r}{r_j}) \prod_{i \neq 1} (\frac{q}{s_i}) \\
= (-1)^{s + \frac{q-1}{2} + \frac{d'} - 1}{2} \prod_{j}(\frac{p_1 \ldots p_r}{r_j}) \prod_{i \neq 1} (\frac{q}{s_i}) \\
= (-1)^{s + \frac{q-1}{2} + \frac{d' - 1}{2}} (\frac{d'}{p_1 \ldots p_r}) \\
= (-1)^{s + \frac{q-1}{2} + \frac{d' - 1}{2}} (\frac{2}{p_1 \ldots p_r}) (\frac{d}{p_1 \ldots p_r}) \\
= (-1)^{s + \frac{q-1}{2} + \frac{d' - 1}{2} - \frac{(p_1 \ldots p_r)^2 - 1}{s}} (\frac{d}{p_1 \ldots p_r}) \\
= (-1)^{s + \frac{(q - p_1 \ldots p_r)}{2} \frac{d' - 2}{2} + \frac{2}{p_1 \ldots p_r)^2} \prod_{i = 1}^r (\frac{d}{p_i}) \\
= (-1)^{s + \frac{(q - p_1 \ldots p_r)}{2} \frac{d' - 2}{2} + \frac{2}{p_1 \ldots p_r)^2} = 1.
$$

Similarly, if some $p_\ell$ is not odd (which implies that the $r_j$’s and $s_i$’s are odd), say $p_1 = 2$, then $d = 5 \pmod{8}$ since $p_1$ is inert in $\mathbb{Q}(\sqrt{q})$, hence $\frac{d - 1}{2} \equiv 0 \pmod{2}$ and $\frac{d^2 - 1}{8} \equiv 1 \pmod{2}$. Therefore

$$
\left(\frac{d}{q}\right) = (-1)^{\frac{q-1}{2} + \frac{d - 1}{2}} (\frac{q}{d}) = (-1)^{s + \frac{q-1}{2} + \frac{d - 1}{2}} \prod_{j}(\frac{p_1 \ldots p_r}{r_j}) \prod_{i} (\frac{q}{s_i}) \\
= (-1)^{s + \frac{q-1}{2} + \frac{d - 1}{2}} \prod_{j}(\frac{p_1 \ldots p_r}{r_j}) \prod_{i} (\frac{p_1 \ldots p_r}{s_i}) \\
= (-1)^{s + \frac{q-1}{2} + \frac{d - 1}{2} \frac{2}{d}} (\frac{p_1 \ldots p_r}{d}) \\
= (-1)^{s + \frac{q-1}{2} + \frac{d - 1}{2} \frac{2}{p_2 \ldots p_r}} (\frac{d}{p_2 \ldots p_r}) \\
= (-1)^{s + \frac{q-1}{2} + \frac{d - 1}{2} \frac{2}{p_2 \ldots p_r}} \prod_{i = 2}^r (\frac{d}{p_\ell}) = (-1)^{r - 1 + s + \frac{d^2 - 1}{8} + \frac{2 - (p_2 \ldots p_r)^2}{d - 1}} \equiv 1 \pmod{2}.
$$

Similarly, assume that some $r_i$ is not odd (which implies that the $s_i$’s and $p_\ell$’s are odd), say $r_1 = 2$. Since $r_1$ is ramified in $\mathbb{Q}(\sqrt{q})$, we have either $d \equiv 2 \pmod{4}$ or $d \equiv 3 \pmod{4}$. Assume first that $d \equiv 2 \pmod{4}$. Then with $d' = d/2$ which is odd, since the first assumption $q \equiv 5 p_1 \ldots p_r \pmod{8}$ on $q$ implies that $q - p_1 \ldots p_r \equiv 0 \pmod{4}$ and that $\frac{q^2 - (p_1 \ldots p_r)^2}{8} \equiv 1 \pmod{2}$ as the
$p_\ell$'s are then odd, we have
\[
\left( \frac{d}{q} \right) = \left( \frac{2}{q} \right) \left( \frac{d'}{q} \right) = (-1)^{\frac{q-1}{2} \cdot \frac{d'-1}{2}} \left( \frac{q}{d'} \right) = (-1)^{\frac{q-1}{2} \cdot \frac{d'-1}{2}} \prod_{j \neq 1} \left( \frac{p_1 \cdots p_r}{r_j} \right) \prod_i \left( \frac{p_1 \cdots p_r}{s_i} \right)
\]
\[
= (-1)^{s-1+\frac{q-1}{2} \cdot \frac{d'-1}{2}} \prod_{j \neq 1} \left( \frac{p_1 \cdots p_r}{r_j} \right) \prod_i \left( \frac{p_1 \cdots p_r}{s_i} \right)
\]
\[
= (-1)^{s-1+\frac{q-1}{2} \cdot \frac{d'-1}{2}} \left( \frac{d}{p_1 \cdots p_r} \right)
\]
\[
= (-1)^{s-1+\frac{q-1}{2} \cdot \frac{d'-1}{2}+(\frac{q-1}{2} \cdot p_1 \cdots p_r)^2} \prod_{\ell=1}^r \left( \frac{d}{p_\ell} \right)
\]
\[
= (-1)^{r+s-1+(\frac{q-1}{2} \cdot p_1 \cdots p_r)^2} = 1.
\]
Assume secondly that $d \equiv 3 \pmod{4}$, so that as already said we have $d = r_2 \cdots r_s s_1 \cdots s_k$ which is odd. Then $\frac{d}{p_\ell}$ is odd and $\frac{q-1}{2} \cdot p_1 \cdots p_r$ is odd by the first assumption on $q$, hence as above
\[
\left( \frac{d}{q} \right) = (-1)^{\frac{q-1}{2} \cdot \frac{d-1}{2}} \left( \frac{q}{d} \right) = (-1)^{\frac{q-1}{2} \cdot \frac{d-1}{2}} \prod_{j \neq 1} \left( \frac{q}{r_j} \right) \prod_i \left( \frac{q}{s_i} \right)
\]
\[
= (-1)^{s-1+\frac{q-1}{2} \cdot \frac{d-1}{2}} \prod_{j \neq 1} \left( \frac{p_1 \cdots p_r}{r_j} \right) \prod_i \left( \frac{p_1 \cdots p_r}{s_i} \right)
\]
\[
= (-1)^{s-1+\frac{q-1}{2} \cdot \frac{d-1}{2}} \left( \frac{d}{p_1 \cdots p_r} \right)
\]
\[
= (-1)^{s-1+(\frac{q-1}{2} \cdot p_1 \cdots p_r-1) \cdot \frac{d-1}{2}} \left( \frac{d}{p_1 \cdots p_r} \right)
\]
\[
= (-1)^{s-1+(\frac{q-1}{2} \cdot p_1 \cdots p_r-1) \cdot \frac{d-1}{2}} \prod_{\ell=1}^r \left( \frac{d}{p_\ell} \right)
\]
\[
= (-1)^{r+s-1+(\frac{q-1}{2} \cdot p_1 \cdots p_r-1) \cdot \frac{d-1}{2}} = 1.
\]
This proves Equation (4).

Let $t$ be a positive prime. First assume that $t$ does not belong to $\text{RAM}(A)$. Then one of the following case occurs: $t = q$, $t = s_i \neq 2$ for some $i$, $t = s_i = 2$ for some $i$, $t = 2 \neq s_i$ for every $i$, or $t \neq q, s_1, \ldots, s_k, 2$.

If $t = q$, then $t \neq 2, t \nmid d, t \mid \Delta, t^2 \mid \Delta$, so that by the second claim of Equation (3) and by Equation (4), we have as wanted
\[
(d, \Delta)_t = \left( \frac{d}{q} \right) = 1.
\]

If $t = s_i \neq 2$ for some $i = 1, \ldots, k$, by the second claim of Equation (3) since $s_i \mid d$, $s_i^2 \nmid d$, and by the third assumption on $q$, we have as wanted
\[
(d, \Delta)_t = (d, p_1 \cdots p_r)_{s_i} (d, q)_{s_i} = \left( \frac{p_1 \cdots p_r}{s_i} \right) \left( \frac{q}{s_i} \right) = \left( \frac{q}{s_i} \right)^2 = 1.
\]
If \( t = s_i = 2 \) for some \( i = 1, \ldots, k \), then \( d \), which is squarefree, is equal to \( 2d' \) for some odd \( d' \). The \( p_i \)'s are odd, and \( q \equiv p_1 \cdots p_r \) [8] by the first assumption on \( q \), hence \( \Delta \) is odd, of the form \((2\Delta' + 1)^2 + 8\Delta'' = 1 + 8\Delta'''\) for some \( \Delta', \Delta'', \Delta''' \in \mathbb{N} \). By the first claim of Equation (3), we have as wanted

\[
(d, \Delta)_t = (-1)^{\frac{d-1}{2} \frac{\Delta-1}{2} + (\Delta^2-1)/8} = (-1)^{\frac{d-1}{2} (4\Delta'') + 2\Delta'' + 8\Delta'''^2} = 1 .
\]

If \( t = 2 \neq s_i \) for every \( i = 1, \ldots, k \), then \( \Delta \) and \( d \) are odd, and \( \Delta \equiv (p_1 \cdots p_r)^2 \) [8] by the first assumption on \( q \) so that \( \Delta \equiv 1 [4] \) since the \( p_i \)'s are odd. Hence by the first claim of Equation (3), we have as wanted

\[
(d, \Delta)_t = (-1)^{\frac{d-1}{2} \frac{\Delta-1}{2}} = 1 .
\]

Now assume that \( t \) belongs to \( \text{RAM}(A) \). In particular \( t \) is equal either to \( p_i \) for some \( i = 1, \ldots, r \) or to \( r_i \) for some \( i = 1, \ldots, s \).

If \( t = p_i \neq 2 \), then \( d \) does not divide \( d \) since \( p_i \) is inert in \( \mathbb{Q}(\sqrt{d}) \), and \( t \) divides \( \Delta \) which is squarefree. Hence by the second claim of Equation (3), since \( p_i \) is inert in \( \mathbb{Q}(\sqrt{d}) \), we have as wanted

\[
(d, \Delta)_t = \left( \frac{d}{p_i} \right) = -1 .
\]

If \( t = p_i = 2 \), then \( d \equiv 5 [8] \) since \( p_i \) is inert in \( \mathbb{Q}(\sqrt{d}) \), hence \( d \) is odd, \( \frac{d-1}{2} \) is even and \( \frac{d^2-1}{8} \) is odd. Moreover \( \Delta = 2\Delta' \) with \( \Delta' \) odd. Therefore by the first claim of Equation (3), we have as wanted

\[
(d, \Delta)_t = (-1)^{\frac{d-1}{2} \frac{\Delta'-1}{2} + (d^2-1)/8} = -1 .
\]

If \( t = r_i \neq 2 \) for some \( i = 1, \ldots, k \), then \( t \) divides \( d \) which is squarefree and does not divide \( \Delta \), hence by the second assumption on \( q \), we have as wanted

\[
(d, \Delta)_t = (d, p_1 \cdots p_r)_t (d, q)_{r_i} = \left( \frac{p_1 \cdots p_r}{r_i} \right) \left( \frac{q}{r_i} \right) = -1 .
\]

Assume at last that \( t = r_i = 2 \) for some \( i = 1, \ldots, s \). Since \( r_i \) is ramified in \( \mathbb{Q}(\sqrt{d}) \), we have either \( d \equiv 2 [4] \) or \( d \equiv 3 [4] \). If \( d \equiv 2 [4] \), then \( t \) divides \( d \) which is equal to \( 2d' \) with \( d' \) odd. But \( t \) does not divide \( \Delta \) which is odd and, by the first assumption on \( q \), we have \( \Delta = 5(2\Delta' + 1)^2 + 8\Delta'' = 5 + 8\Delta''' \) for some \( \Delta', \Delta'', \Delta''' \in \mathbb{N} \). Hence by the first claim of Equation (3), we have as wanted

\[
(d, \Delta)_t = (-1)^{\frac{d-1}{2} \frac{\Delta-1}{2} + (\Delta^2-1)/8} = (-1)^{\frac{d-1}{2} (2+4\Delta''') + 3 + 2\Delta''' + 8\Delta'''^2} = -1 .
\]

If \( d \equiv 3 [4] \), then \( d \) and \( \Delta \) are odd and, by the first assumption on \( q \), we have \( \Delta = 3(2\Delta' + 1)^2 + 8\Delta'' = 3 [4] \). Hence by the first claim of Equation (3), we have as wanted

\[
(d, \Delta)_t = (-1)^{\frac{d-1}{2} \frac{\Delta-1}{2}} = -1 .
\]

References


Department of Mathematics and Statistics, P.O. Box 35
40014 University of Jyväskylä, FINLAND.
e-mail: jouni.t.parkkonen@jyu.fi

Laboratoire de mathématique d’Orsay,
UMR 8628 Univ. Paris-Sud et CNRS,
Université Paris-Saclay,
91405 ORSAY Cedex, FRANCE
e-mail: frederic.paulin@math.u-psud.fr