Journal of Number Theory 132 (2012) 888–895

Contents lists available at SciVerse ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Rotations and units in quaternion algebras ☆

Capi Corrales-Rodrigáñez *

Departamento de Álgebra, Facultad de Matemáticas, Universidad Complutense de Madrid, Madrid, Spain

ARTICLE INFO

Article history:
Received 31 March 2010
Revised 9 April 2011
Accepted 2 December 2011
Available online 3 February 2012
Communicated by Tsit Yuen Lam

Keywords:
Quaternion algebras
Quadratic fields
Special orthogonal group of the space of pure quaternions in a quaternion algebra over a quadratic field

ABSTRACT

Unit groups of orders in quaternion algebras over number fields provide important examples of non-commutative arithmetic groups. Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field with $d < 0$ a square-free integer such that $d \equiv 1 (\mathrm{mod}\ 8)$, and let R be its ring of integers. In this note we study, through its representation in $SO_3(R)$, the group of units of several orders in the quaternion algebra over K with basis $\{1, i, j, k\}$ satisfying the relations $i^2 = j^2 = -1$, $ij = -ji = k$.

1. Introduction

The Pell equation is the equation $x^2 - dy^2 = 1$, for a given nonzero integer $d > 1$, to be solved in integers. One may rewrite this equation as $(x + \sqrt{d})(x - \sqrt{d}) = 1$ and, so, finding a solution is equivalent to finding a non-trivial unit of norm 1 in the ring $\mathbb{Z}[\sqrt{d}]$. If the solutions are ordered by magnitude, this reformulation allows us to express the nth solution (x_n, y_n) in terms of the first one (x_1, y_1), by $x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$. Accordingly, the first solution is called the fundamental solution to the Pell equation, and solving the Pell equation comes down to finding a fundamental unit in the group $\mathbb{Z}[\sqrt{d}]^*$. This connection to Pell's equation made the group of units in a quadratic number field an important object of study for number theorists since the seventeenth century [12]. In the study of group rings of finite groups over number rings, emerges the Diophantine equation $x^2 - ay^2 - bz^2 + abt^2 = 1$, which can be considered an analogue to Pell equation, in the sense that the solutions to Pell equation form a discrete subgroup of an algebraic torus isomorphic to $\mathbb{Z}$, and the integral solutions to this equation form an arithmetic subgroup of $\mathrm{SL}_2(\mathbb{R})$ commensurable with the

☆ Research partially supported by CICYT of Spain, No. MTM 2006-14688.
* Fax: +34 913944662.
E-mail address: capi_corrales@mat.ucm.es.

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2011.12.009

group of units of an order in a quaternion algebra over $\mathbb{Q}$, quaternion algebras being non-commutative analogues of quadratic fields.

In general, if K is a number field with ring of integers R, a quaternion algebra A over K is a four-dimensional algebra over K with basis $\{1, i, j, k\}$ satisfying the relations $i^2 = a$, $j^2 = b$, $ij = -ji = k$ for $a, b \in K^*$. It is well known that the algebra A, denoted by $A = (\frac{a,b}{K})$, is a central simple algebra. An order $\mathcal{O}$ in A is an R-lattice (i.e., a finitely generated R-module such that $K \cdot \mathcal{O} = A$) that is a subring. If $\mathcal{O}$ is an order in A, its group of units $\mathcal{O}^*$ is commensurable with $(Z\mathcal{O})^* \times \mathcal{O}^1$, where $Z\mathcal{O}$ is the center of $\mathcal{O}$ and $\mathcal{O}^1$ is the subgroup of elements of reduced norm 1. Here the reduced norm map is the quadratic form $q : A \to K$ that multiplies each quaternion $x_0 + x_1 i + x_2 j + x_3 k$ by its conjugate $x_0 - x_1 i - x_2 j - x_3 k$. Therefore, the study of the structure of $\mathcal{O}^*$ is reduced to that of $(Z\mathcal{O})^*$ and $\mathcal{O}^1$. Since the Dirichlet Unit Theorem explains the structure of $(Z\mathcal{O})^*$, only $\mathcal{O}^1$ needs to be investigated. We observe that the elements of $\mathcal{O}^1$ correspond to solutions over $(Z\mathcal{O})^*$ of the equation $x^2 - ay^2 - bz^2 + abt^2 = 1$. We identify $\mathcal{O}^1$ with classical groups in two ways.

The field $K[i]$ is a maximal subfield of A, and the Galois group of the extension $K[i]/K$ is a cyclic group of order two generated by the restriction σ of the inner automorphism of A induced by j, that is $\sigma(x) = jxj^{-1}$, for every $x \in K$. Thus, $A = K[i] \oplus K[i]j$ can be embedded in $M_2(\mathbb{C})$ by the map

$$x + yj \overset{\iota}{\mapsto} \begin{pmatrix} x & y \\ b\sigma(y) & \sigma(x) \end{pmatrix}.$$

The embedding ι maps the elements of reduced norm 1 into $\mathrm{SL}_2(\mathbb{C})$, and we may identify $\mathcal{O}^1$ with an arithmetic group of the group $\mathrm{SL}_2(\mathbb{C})$. Since $\mathrm{PSL}_2(\mathbb{C})$ is the group of orientation preserving isometries of the three-dimensional hyperbolic space H^3, the group $\mathcal{O}^1$ acts on H^3, and we can use this action to study $\mathcal{O}^*$. The best situation is when this action is discontinuous, since in this case we can use Poincaré's method to find a fundamental domain for the action $\mathcal{O}^1$ on H^3 which will give us, in turn, a presentation of $\mathcal{O}^1$ [10,2,9,5]. It should be noted, though, that it is not easy in general to apply Poincaré's method.

Next, we consider the K-vector space with basis $B = \{i, j, k\}$ consisting in the elements with trace 0 in A. It is denoted by A_0 and is stable under conjugation by elements of A. There is an exact sequence of groups [8, Theorem 3.1],

$$1 \to K^* \to A^* \overset{\tau}{\to} SO_3(K) \to 1 \tag{1}$$

where, for $y \in A^*$, $\tau(y)$ is the matrix which represents conjugation of the elements of A_0 by y with respect to B, and $SO_3(K)$ is the orthogonal group with respect to the quadratic form q restricted to A_0. Restriction of the map τ allows us to investigate $\mathcal{O}^1$ trough the study of its action on A_0. The action of $\mathcal{O}^1$ on H^3 is discontinuous only in six cases: (a) when A is a totally definite quaternion algebra; (b) when $A = M_2(\mathbb{Q})$; (c) when $A = M_2(\mathbb{Q}[\sqrt{d}])$ with $0 > d \in \mathbb{Z}$; (d) when $A = (\frac{a,b}{\mathbb{Q}})$ is a division algebra with a or b positive; (e) when $A = (\frac{a,b}{K})$, K is totally real and A ramifies at all real embeddings of K but one, and (f) when $A = (\frac{a,b}{K})$, K has exactly two complex embeddings and A is a division algebra that ramifies at all the real embeddings of K. In the first three situations $\mathcal{O}^1$ is known to be, respectively, a finite group, a group commensurable with $\mathrm{SL}_2(\mathbb{Z})$ and a Bianchi group [6,5], and cases (d) and (e) were amply studied in, respectively, [1] and [11]. The first example of unit group of type (f) was computed in [4], with $A = (\frac{-1,-1}{K})$, $K = \mathbb{Q}(\sqrt{-7})$, R ring of integers of K and $\mathcal{O} = R[1, i, j, ij]$.

In general, little is known about the structure of $SO_3(R)$ when R is the ring of integers of a number field. In [4], Poincaré's method was used to find a presentation of $\mathcal{O}^*$; next, the cokernel of $\tau : \mathcal{O}^* \to SO_3(R)$ was described, and the previously found presentation of $\mathcal{O}^*$ was used to give a presentation of $SO_3(R)$ as well. The simplest examples of type (e), are provided by orders $\mathcal{O}$ of quaternion algebras $A = (\frac{-1,-1}{K})$, where $K = \mathbb{Q}(\sqrt{d})$ and $d < 0$ is a square-free integer, such that the center of $\mathcal{O}$ is the ring of integers R of K. Quaternion algebras of this type are division algebras, and not matrix algebras, if and only if $d \equiv 1 \pmod 8$. In this note we consider such orders, and we describe the cokernel of the restriction to $\mathcal{O}^*$ of map τ in (1). It should be noted that among the fields considered, only $\mathbb{Q}[\sqrt{-7}]$ has class number 1, a condition which significantly simplifies the situation; for example, in general the cokernel of the restriction to $\mathcal{O}^*$ of map τ in (1), is isomorphic to a subgroup of a quotient of the class group of K [7, Theorem 7.2.20], trivial when the class number is 1. If, with adequate computer programs, we were to obtain a presentation of $\mathcal{O}^*$ via the action of $\mathcal{O}^1$ on H^3, this identification would allow us to translate it into a presentation of $SO_3(R)$.

2. Description of the results

Let A be the quaternion algebra $A = (\frac{-1,-1}{K})$, with $K = \mathbb{Q}(\sqrt{d})$ and $d < 0$ a square-free integer such that $d \equiv 1 (\mathrm{mod}\ 8)$. Let $R = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ be the ring of integers of K, and let $R[1/2] = \{x/2^k \mid x \in R, k \in \mathbb{Z}\}$. The ideal $2R$ splits completely in two distinct primes. We set $2R = \wp\bar{\wp}$ and we define

$$\delta = \begin{cases} 1 & \text{if there exists } x \in K^* \text{ with } v_\ell(x) \text{ even for all } \ell \neq \wp \text{ and } v_\wp(x) \text{ odd}, \\ 0 & \text{else}, \end{cases} \tag{2}$$

where, for any nonzero prime ideal ℓ of R and any $a \in K^*$, $v_\ell(a)$, the ℓ-adic valuation of a, is the power of ℓ appearing in the factorization of the fractional ideal Ra.

Let $A_R = R[1, i, j, k]$, $\Lambda_R = R[1, i, j, k, \frac{1+i+j+k}{2}]$ and $A_{R[1/2]} = R[1/2][1, i, j, k]$. Our aim in these pages is to identify the cokernel of the restriction to A_R^* of map τ in (1). In order to do so, we will successively consider the restrictions of τ to the chain of groups $A_R^* \subset \Lambda_R^* \subset A_{R[1/2]}^* \subset A^*$. It is known [7, Theorem 7.2.20] that there is an exact sequence

$$1 \to R[1/2]^* \to A_{R[1/2]}^* \xrightarrow{\tau} SO_3\big(R[1/2]\big) \xrightarrow{\psi} \mathrm{Cl}\big(R[1/2]\big)_2, \tag{3}$$

where $\mathrm{Cl}(R[1/2])_2$ is the 2-torsion part of the class group $\mathrm{Cl}(R[1/2]) = \mathbb{I}(R[1/2])/\mathbb{P}(R[1/2])$, with $\mathbb{I}(R[1/2])$ the group of fractional ideals of $R[1/2]$ and $\mathbb{P}(R[1/2])$ its subgroup of fractional principal ideals.[1] We will see that, as a consequence of our Lemma 1, the image under τ of $A_{R[1/2]}^*$ is, in fact, contained in $SO_3(R)$, and we will successively study the cokernels B_1, B_2 and B_3 of ψ in the three upper rows of the following commutative diagram with exact rows and inclusions in the vertical maps,

$$\begin{array}{ccccccccccc} 1 & \longrightarrow & R^* & \longrightarrow & A_R^* & \xrightarrow{\tau} & SO_3(R) & \xrightarrow{\psi} & B_3 & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & & & \\ 1 & \longrightarrow & R^* & \longrightarrow & \Lambda_R^* & \xrightarrow{\tau} & SO_3(R) & \xrightarrow{\psi} & B_2 & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & & & \\ 1 & \longrightarrow & R[1/2]^* & \longrightarrow & A_{R[1/2]}^* & \xrightarrow{\tau} & SO_3(R) & \xrightarrow{\psi} & B_1 & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & & & \\ 1 & \longrightarrow & K^* & \longrightarrow & A^* & \xrightarrow{\tau} & SO_3(K) & \longrightarrow & 1. & & \end{array} \tag{4}$$

We will start by defining the map ψ. Next, in Lemma 2 we will see that every prime factor q of d can be expressed as a sum of four squares in qR; this fact will be used in Theorem 3 to show that $B_1 \simeq \mathrm{Cl}(R[1/2])_2$.

[1] It is essential in the proof of this result as well as to our strategy, that the smallest ring in which the matrix with respect to $\{i, j, k\}$ of the bilinear form associated to the sums of squares form is invertible is $R[1/2]$, with the ideal $2R$ splitting completely in R. In the general case, with $i^2 = a$, $j^2 = b$, $a, b \in K^*$, the corresponding matrix has determinant $8a^2b^2$, and the situation gets much more complicated.

In Lemma 4 we will describe the quotient group $A^*_{R[1/2]}/R[1/2]^*\Lambda^*_R$. Knowledge of this group and of B_1 will allow us to prove in Theorem 5 that

$$B_2 \simeq \{a \in K^*;\ v_\ell(a) \text{ even for all prime ideals } \ell \neq \wp, \bar{\wp}\}/K^{*2}R^*.$$

Finally, in Lemma 6 we will give a description Λ^*_R/A^*_R, which we will then use in Theorem 7 to show that B_3 is isomorphic to a semi-direct product of $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$ and B_2, its action to be specified later.

3. Proofs of the results

The image under map τ in (1) of any element $y \in A^*$ is given by the matrix $\tau(y) = \frac{1}{q(y)}(m_{rs})$, with

$$(m_{rs}) = \begin{pmatrix} y_0^2+y_1^2-y_2^2-y_3^2 & 2(y_1y_2-y_0y_3) & 2(y_0y_2+y_1y_3) \\ 2(y_0y_3+y_1y_2) & y_0^2-y_1^2+y_2^2-y_3^2 & 2(y_2y_3-y_0y_1) \\ 2(y_1y_3-y_0y_2) & 2(y_0y_1+y_2y_3) & y_0^2-y_1^2-y_2^2+y_3^2 \end{pmatrix}. \tag{5}$$

Lemma 1. *Let $A(\mathbb{Q}_2)$ be the quaternion ring over the 2-adic field. For $y \in A(\mathbb{Q}_2)$, the matrix which represents the map $A(\mathbb{Q}_2) \to A_0(\mathbb{Q}_2)$ defined by $x \to yxy^{-1}$ with respect to the basis $\{i, j, k\}$ of $A_0(\mathbb{Q}_2)$, has all of its entries in $\mathbb{Z}_2$.*

Proof. It suffices to show that $yiy^{-1} \in A_0(\mathbb{Z}_2)$. If $y = y_0 + y_1 i + y_2 j + y_3 k$, $y_i \in \mathbb{Q}_2$, matrix (5) tells us that $q(y)yiy^{-1} = (y_0^2+y_1^2-y_2^2-y_3^2)i + 2(y_0y_3+y_1y_2)j + 2(-y_0y_2+y_1y_3)k$.

We may write $y = y_0 + y_1 i + y_2 j + y_3 k = \frac{a_0}{2^n} + \frac{a_1}{2^n}i + \frac{a_2}{2^n}j + \frac{a_3}{2^n}k$, with $n \in \mathbb{Z}$, $a_i \in \mathbb{Z}_2$ and a_r odd for at least one value of r. Hence,

$$(a_0^2+a_1^2+a_2^2+a_3^2)yiy^{-1} = (a_0^2-a_1^2+a_2^2-a_3^2)i + 2(a_0a_3+a_1a_2)j + 2(-a_0a_2+a_1a_3)k,$$

with $a_r \in \mathbb{Z}_2$ for all r, and a_r^2 odd for at least one value of i. Since $a_0^2+a_1^2+a_2^2+a_3^2 \equiv a_0^2-a_1^2+a_2^2-a_3^2 \equiv \pm a_0a_r + a_sa_t \pmod 2$ for all r, s, t, all coefficients of yiy^{-1} are in $\mathbb{Z}_2$. $\square$

Corollary. *As a consequence of Lemma 1, the image of $A^*_{R[1/2]}$ under τ is contained in $SO_3(R)$.*

In order to define the map ψ, we consider the ring $S = \{a \in K \mid v_\ell(a) \geqslant 0,\ \text{all } \ell \neq \wp\}$, with $R \subset S$ and $\mathrm{Cl}(S) = \mathrm{Cl}(R)/\langle[\wp]\rangle = \mathrm{Cl}(R[1/2])$. We have the following commutative diagram with exact rows,

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \{\pm 1\} & \longrightarrow & \{a \in K^* \mid v_\ell(a) \text{ even for all } \ell\}/K^{*2} & \xrightarrow{\omega} & \mathrm{Cl}(R)_2 & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow{\scriptstyle\alpha} & & \\ 1 & \longrightarrow & S^*/S^{*2} & \longrightarrow & \{a \in K^* \mid v_\ell(a) \text{ even for all } \ell \neq \wp\}/K^{*2} & \xrightarrow{\omega} & \mathrm{Cl}(R[1/2])_2 & \longrightarrow & 1 \end{array} \tag{6}$$

where $S^* = \{\pm 1\}\epsilon^{\mathbb{Z}}$ for some fundamental $\wp$-unit ϵ with $v_\ell(\epsilon) = 0$ for all $\ell \neq \wp$ and, with some abuse of notation, $\omega(a) = \prod \ell^{v_\ell(a)/2}$, the product running along the prime ideals ℓ in the corresponding ring. Thus, $\mathrm{Cl}(R[1/2])_2 \overset{\phi}{\simeq} \{a \in K^* \mid v_\ell(a) \text{ even for all } \ell \neq \wp\}/S^*K^{*2}$, where ϕ maps each class of order 2 in $\mathrm{Cl}(R[1/2])_2$ to the generator of its square modulo S^*K^{*2}, and $\phi^{-1} = \omega$. The isomorphism ϕ allows us to identify $\mathrm{Cl}(R[1/2])_2$ with a quotient of a subset of K^*.

Finally, we must check that for each quaternion y such that $\tau(y) \in SO_3(R)$, $v_\ell(q(y))$ is even for all prime ideals $\ell \neq \wp, \bar{\wp}$ of R. Suppose that for some prime ideal $\ell \neq \wp, \bar{\wp}$, $v_\ell(q(y))$ is odd; say $v_\ell(q(y)) = 2k+1$ with $k \in \mathbb{Z}$. We know [4, Lemma 5.1] that τ induces an isomorphism

$$\{y = y_0 + y_1 i + y_2 j + y_3 k \in A^* \mid 4y_r y_s \in q(y)R, \text{ for all } 1 \leqslant r, s \leqslant 3\}/K^* \simeq SO_3(R) \tag{7}$$

and, thus, since $\tau(y) \in SO_3(R)$, it is $4 \in q(y)R$, and, consequently, $q(y)$ divides $4y_i^2$ for $i = 0, 1, 2, 3$. This implies that $v_\ell(y_i) \geqslant \frac{2k+1}{2}$ and, hence, $v_\ell(y_i) \geqslant k+1$ for each i. But then $v_\ell(q(y)) \geqslant 2k+2$, which is a contradiction. We can now define ψ as the map that sends each matrix s in $SO_3(R)$ to the image under ω of the norm $q(y)$ of a quaternion y for which $\tau(y) = s$, as described by the composition of maps in the following diagram

$$SO_3(R) \hookrightarrow SO_3(K) \simeq A^*/K'' \xrightarrow{q} \{a \in K^* \mid v_\ell(a) \text{ even for all } \ell \neq \wp\}/S^* K^{*2} \xrightarrow{\omega} \mathrm{Cl}\big(R[1/2]\big)_2.$$

Lemma 2. *If q is a prime factor of d and $qR = \mathcal{Q}^2$, with $\mathcal{Q}$ prime ideal in R, then q can be expressed as a sum of four squares in $\mathcal{Q}$.*

Proof. Since the ideal $\mathcal{Q}$ is generated as a $\mathbb{Z}$ module by q and $\sqrt{d}$, it suffices to write q as $q = \sum_{s=0}^{3}(q \cdot a_s + \sqrt{d} \cdot b_s)^2$ with $a_s, b_s \in \mathbb{Z}$ for $0 \leqslant s \leqslant 3$. Let z_1, z_2 be positive integers such that $z_1 \cdot q + z_2 \cdot \frac{d}{q} = 1$. We can find $t \in \mathbb{Z}$ such that $t \cdot \frac{-d}{q} + z_1 \equiv 2 (\mathrm{mod}\ 4)$ and, since $\frac{-d}{q}$ is odd, necessarily $t \equiv z_1 (\mathrm{mod}\ 2)$. We take $x_1 = t \cdot \frac{-d}{q} + z_1$ and $x_2 = t \cdot q + z_2$. Then we have $x_1 \cdot q + x_2 \cdot \frac{d}{q} = 1$, where $x_2 \equiv z_2 + t \cdot q \equiv z_2 + z_1 \cdot q \equiv 1 (\mathrm{mod}\ 2)$. Thus, $x_1 x_2 \equiv 2 (\mathrm{mod}\ 4)$ and, not being of the form $4^n(8m+7)$, it can be expressed as the sum of three squares.

It follows that $x_1 x_2 = A^2 + B^2 + C^2$ for certain integers A, B, C. In other words, the norm of the quaternion $Ai + Bj + Ck$ is $x_1 x_2$. Consequently, there are two integral quaternions $u = a_0 + a_1 i + a_2 j + a_3 k$ and $v = b_0 + b_1 i + b_2 j + b_3 k$ with $\sum_{s=0}^{3} {a_s}^2 = x_1$ and $\sum_{s=0}^{3} {b_s}^2 = x_2$, such that $u \cdot v = Ai + Bj + Ck$, and so, $\sum_{s=0}^{3} a_s b_s = 0$. If we let $\alpha_s = q \cdot a_s + \sqrt{d} \cdot b_s$, then

$$\sum_{s=0}^{3} {\alpha_s}^2 = q^2 \sum_{s=0}^{3} {a_s}^2 + d \sum_{s=0}^{3} {b_s}^2 + 2q\sqrt{d} \sum_{s=0}^{3} a_s b_s = q^2 \cdot x_1 + d \cdot x_2 = q. \qquad \square$$

Theorem 3. *The map $SO_3(R)/\tau(A^*_{R[1/2]}) \xrightarrow{\psi_1} \mathrm{Cl}(R[1/2])_2$ induced by ψ is an isomorphism.*

Proof. Since sequence (3) is exact, we know that ψ_1 is well defined and injective. Let us see that it is also surjective. Applying the Snake Lemma in (6), we obtain the exact sequence

$$1 \to Ker\,\alpha \to S^*/\{\pm 1\}S^{*2} \to \Gamma \to \mathrm{Cl}\big(R[1/2]\big)_2/\alpha\big(\mathrm{Cl}(R)_2\big) \to 1, \tag{8}$$

where $S^*/\{\pm 1\}S^{*2}$ is a group of order 2 and the group $\Gamma = \{a \in K^*;\ v_\ell(a) \text{ even all } \ell \neq \wp\}/\{a \in K^*;\ v_\ell(a) \text{ even all } \ell\}$ has order 1 or 2, and it is not trivial if and only if there exists $x \in K$ with all valuations even except the $\wp$-adic one. Since taking 2-torsion is left exact, $Ker\,\alpha = (\langle[\wp]\rangle)_2$. If the order of $[\wp]$ in $\mathrm{Cl}(R)$ is odd, then $(\langle[\wp]\rangle)_2$ is trivial, α is injective and (8) becomes

$$1 \to S^*/\{\pm 1\}S^{*2} \to \Gamma \to \mathrm{Cl}\big(R[1/2]\big)_2/\alpha\big(\mathrm{Cl}(R)_2\big) \to 1.$$

Consequently, the fundamental $\wp$-unit ϵ must have odd $\wp$-valuation, the map $S^*/\{\pm 1\}S^{*2} \to \Gamma$ is surjective and α is an isomorphism. Let r be the number of prime factors of d; then, $\mathrm{Cl}(R[1/2])_2 \simeq \mathrm{Cl}(R)_2 \simeq (\mathbb{Z}/2\mathbb{Z})^{r-1}$ and it is generated by the classes of the prime factors of d. If the order of $[\wp]$

in $\mathrm{Cl}(R)$ is even, then $\mathit{Ker}\,\alpha$ has order 2 and, from the exactness of (8), we deduce that the fundamental $\wp$-unit ϵ has even $\wp$-valuation and $\Gamma \to \mathrm{Cl}(R[1/2])_2/\alpha(\mathrm{Cl}(R)_2)$ is an isomorphism. Consequently, if $[\wp] \notin \mathrm{Cl}(R)^2$, the map α is surjective and $\mathrm{Cl}(R[1/2])_2 \simeq \mathrm{Cl}(R)_2/\langle[\wp]\rangle_2 \simeq (\mathbb{Z}/2\mathbb{Z})^{r-2}$; while if $[\wp] \in \mathrm{Cl}(R)^2$, the map α is not surjective and there exists a non-trivial element $\xi \in K^* \setminus S^*$ with odd $\wp$-valuation and even ℓ-valuation for all $\ell \neq \wp$. In this case, $\mathrm{Cl}(R[1/2])_2 \simeq (\mathbb{Z}/2\mathbb{Z})^{r-1}$ and it is generated by the $r-2$ classes in $\alpha(\mathrm{Cl}(R)_2)$ and the class image under ω of ξ. We conclude that

$$\mathrm{Cl}\big(R[1/2]\big)_2 \simeq (\mathbb{Z}/2\mathbb{Z})^{r-2+\delta}, \tag{9}$$

with δ as defined in (2).

We now prove that ψ_1 is surjective. Since the product of two sums of four squares is also a sum of four squares, it suffices to take x either a prime divisor of d, or $x \in K^*$ with $v_\wp(x)$ odd and $v_\ell(x) = 0$ for all $\ell \neq \wp$. For x a prime divisor of d, let $xR = \mathcal{Q}^2$ with $\mathcal{Q}$ prime ideal of R. Using the isomorphism (7), it suffices to find $y \in A_R$ with coefficients in $\mathcal{Q}$ and such that $q(y) = x$. This is equivalent to writing x as sum of four squares in $\mathcal{Q}$, which is Lemma 2. Let next $x \in K^*$ with $v_\wp(x)$ odd and $v_\ell(x) = 0$ for all $\ell \neq \wp$. We know that every element in R can be expressed as a sum of four squares [3, p. 536], which easily implies that every element in K is the reduced norm of a quaternion in A. As a consequence, there exists $y \in A$ such that $q(y) = x$ and, by Lemma 1, $\tau(y) \in SO_3(R)$. □

Lemma 4. *In the situation described in diagram* (4), *we have*

$$A^*_{R[1/2]}/R[1/2]^*\Lambda^*_R \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}. \tag{10}$$

Proof. We consider the following diagram,

$$\begin{array}{ccccccc} 1 & \longrightarrow & R^* & \longrightarrow & R[1/2]^* & \xrightarrow{\ \beta\ } & \mathbb{Z}\times\mathbb{Z} \\ & & \downarrow & & \downarrow & & \downarrow{\scriptstyle 2} \\ 1 & \longrightarrow & \Lambda^*_R & \longrightarrow & A^*_{R[1/2]} & \xrightarrow{\ \beta'\ } & \mathbb{Z}\times\mathbb{Z} \end{array} \tag{11}$$

where $\beta(u) = (v_\wp(u), v_{\bar\wp}(u))$ for $u \in R[1/2]^*$, $\beta'(x) = (v_\wp(q(x)), v_{\bar\wp}(q(x)))$ for $x \in A^*_{R[1/2]}$ and the map $\mathbb{Z}\times\mathbb{Z} \xrightarrow{2} \mathbb{Z}\times\mathbb{Z}$ is defined by $(a,b) \to (2a,2b)$. Then, $A^*_{R[1/2]}/R[1/2]^*\Lambda^*_R \simeq \beta'(A^*_{R[1/2]})/2\beta(R[1/2]^*)$, with $2\beta(R[1/2]^*) \subset \beta'(A^*_{R[1/2]}) \subset \beta(R[1/2]^*) \subset \mathbb{Z}\times\mathbb{Z}$.

The image $\beta(R[1/2]^*)$ contains $(1,1) = \beta(2)$. Also, if t is the order of $[\wp]$ in $\mathrm{Cl}(R)$, it is $\wp^t = \zeta R$, with $\zeta \in R$ and $v_\ell(\zeta) = 0$ for all $\ell \neq \wp$. Thus, $\zeta \in R[1/2]^*$ and $(t,0) = (v_\wp(\zeta), v_{\bar\wp}(\zeta)) \in \beta(R[1/2]^*)$. Next, as $\{(t,0),(1,1)\}$ are linearly independent over $\mathbb{Z}$, it is $\beta(R[1/2]^*) = (1,1)\mathbb{Z} + (t,0)\mathbb{Z}$, a lattice of index t in $\mathbb{Z}\times\mathbb{Z}$, and $2\beta(R[1/2]^*) = 2((1,1)\mathbb{Z} + (t,0)\mathbb{Z})$. Finally, on the one hand $(1,1) = \beta'(1+i) \in \beta'(A^*_{R[1/2]})$ and on the other, since every element of R can be expressed as sum of four squares in R [3, p. 536], there exists $x \in A^*_{R[1/2]}$ with $q(x) = \zeta$, so $(t,0) = \beta'(x) \in \beta'(A^*_{R[1/2]})$. Consequently, $\beta'(A^*_{R[1/2]}) = (1,1)\mathbb{Z} + (t,0)\mathbb{Z}$ and $A^*_{R[1/2]}/R[1/2]^*\Lambda^*_R \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. □

Remark. We have $A^*_R \subset \Lambda^*_R \subset A^*_{R[1/2]}$. On the one hand, diagram (11) implies that Λ^*_R is a normal subgroup of $A^*_{R[1/2]}$. On the other, A^*_R is stable under conjugation by elements of $A^*_{R[1/2]}$ and, thus, also normal in $A^*_{R[1/2]}$. Consequently, $\tau(A^*_R)$ is normal in $SO_3(R)$.

Theorem 5. *Let* $B_2 = \{a \in K^*;\ v_\ell(a) \text{ even if } \ell \neq \wp, \bar\wp\}/K^{*2}R^*$. *The map* $SO_3(R)/\tau(\Lambda^*_R) \xrightarrow{\psi_2} B_2$ *induced by* ψ *is an isomorphism.*

Proof. Let $s \in SO_3(R)$ and $y = y_0 + y_1 i + y_2 j + y_3 k \in A$ with $\tau(y) = s$. If $y' \in A$, $y' \neq y$ and $\tau(y') = s$, then $y/y' \in K^*$ and, hence, $q(y)$ and $q(y')$ differ in a square in K^*. As was argued when defining the map ψ, for each prime ideal $\ell \neq \wp, \bar{\wp}$ of R, $v_\ell(q(y))$ is even. We finally observe that $\psi(\tau(\Lambda_R^*)) \subset R^*/K^{*2}$. This shows that the map ψ_2 is a well-defined homomorphism.

Suppose, next, that $q(y) = a^2 u$, $a \in K^*$, $u \in R^*$. Substituting y by y/a, we may assume $q(y) \in R^*$. This implies that the entries in matrix (5) defining $\tau(y)$ are all in R. As a consequence of this, $4y_i^2 \in R$ for all i and, hence, $v_\ell(y) \geqslant 0$ if $\ell \neq \wp, \bar{\wp}$. Taking sums and differences of the elements in the diagonal of (5), we verify that $v_\wp(2(y_i^2 \pm y_j^2)) \geqslant 0$ and $v_{\bar{\wp}}(2(y_i^2 \pm y_j^2)) \geqslant 0$. Since 2 does not ramify in R, this implies that $y_i \equiv y_j (\mathrm{mod}\ 2)$ for each i, j, $y \in \Lambda_R^*$ and, so, the sequence $1 \to R^* \to \Lambda_R^* \xrightarrow{\tau_2} SO_3(R) \xrightarrow{\psi} B_2$ is exact and the map ψ_2 injective.

Let us see that ψ_2 is also surjective. There is an exact sequence $1 \to \mathrm{Cl}(R)_2 \xrightarrow{\phi} B_2 \xrightarrow{\bar{\beta}} \prod_{v|2} \mathbb{Z}/2\mathbb{Z}$, where ϕ sends each class to a generator of its square and $\bar{\beta}(x) = (v_\wp(x)(\mathrm{mod}\ 2), v_{\bar{\wp}}(x)(\mathrm{mod}\ 2))$ for $x \in B$. We set $\beta(x) = (v_\wp(x), v_{\bar{\wp}}(x))$, so $\bar{\beta}(x) = \beta(x)(\mathrm{mod}\ 2)$. Then, $(1,1) = \beta(2) \in \mathit{Im}\,\bar{\beta}$ and we know that there exists $x \in K^*$ with $v_\wp(x)$ odd and $v_\ell(x)$ even for $\ell \neq \wp$ if and only if $\delta = 1$. Thus, $\mathit{Im}\,\bar{\beta} = (\mathbb{Z}/2\mathbb{Z})^{1+\delta}$ and

$$B_2 \simeq (\mathbb{Z}/2\mathbb{Z})^{r+\delta}. \tag{12}$$

On the other hand, we have the following commutative diagram,

$$\begin{array}{ccccccccccc}
1 & \longrightarrow & R^* & \longrightarrow & \Lambda_R^* & \xrightarrow{\tau} & SO_3(R)/\tau(\Lambda_R^*) & \xrightarrow{\psi} & \psi(SO_3(R)/\tau(\Lambda_R^*)) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & R[1/2]^* & \longrightarrow & A_{R[1/2]}^* & \xrightarrow{\tau} & SO_3(R)/\tau(A_{R[1/2]}^*) & \xrightarrow{\psi} & \mathrm{Cl}(R[1/2])_2 & \longrightarrow & 1.
\end{array}$$

Using the Snake Lemma, (9), (10) and (12) on this diagram, we get $\psi(SO_3(R)/\tau(\Lambda_R^*)) = B_2$ and the theorem is proved. □

Lemma 6. *In the situation described in diagram* (4), *it is* $\Lambda_R^*/A_R^* \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Proof. Direct computations show that for $x \in \Lambda_R^*$ and $y \in A_R^*$, $xyx^{-1} \in A_R^*$ and A_R^* is a normal subgroup of Λ_R^*. We start by giving a characterization of the elements of Λ_R^*/A_R^*. Writing every $x \in \Lambda_R^*$ as $x = \frac{a+(a+2b)i+(a+2c)j+(a+2d)k}{2}$, we may define a map $\sigma = (\sigma_1, \sigma_2): \Lambda_R^* \to R \times R$ by

$$\frac{a + (a+2b)i + (a+2c)j + (a+2d)k}{2} \mapsto (a, b+c+d).$$

It is easy to check that for $x, y \in \Lambda_R^*$,

$$xy^{-1} \in A_R^* \quad \Leftrightarrow \quad \sigma_1(x)\sigma_2(y) + \sigma_1(y)\sigma_2(x) \equiv 0 (\mathrm{mod}\ 2R). \tag{13}$$

Since $|R/2R| = 4$ and, as a consequence of (13), σ is injective, it is $|\Lambda_R^*/A_R^*| \leqslant 16$. Furthermore, the element $u = \frac{1+i+j+k}{2}$ has order 3 in Λ_R^*/A_R^*, which implies that $|\Lambda_R^*/A_R^*| \in \{3, 6, 9, 12, 15\}$. Computing $\sigma(u)$ and $\sigma(u^2)$, (13) guarantees that, for $x \in \Lambda_R^*/A_R^*$ it is

$$\begin{cases} x \in A_R^* \quad \Leftrightarrow \quad \sigma_1(x) \equiv 0 (\mathrm{mod}\ 2R), \\ x \equiv u \big(\mathrm{mod}\ A_R^*\big) \quad \Leftrightarrow \quad \sigma_2(x) \equiv 0 (\mathrm{mod}\ 2R), \\ x \equiv u^2 \big(\mathrm{mod}\ A_R^*\big) \quad \Leftrightarrow \quad \sigma_2(x) \not\equiv 0 (\mathrm{mod}\ 2R) \text{ and } \sigma_1(x) \equiv \sigma_2(x) (\mathrm{mod}\ 2R). \end{cases} \tag{14}$$

If we set $d = 1 - 8k$ with $k \in \mathbb{N}$, the integer $8k + 3$ is not of the form $4^n(8m + 7)$, so there exist $w_0^2, w_1^2, w_2^2 \in 1+8\cdot\mathbb{Z}$ with $8k+3 = w_0^2 + w_1^2 + w_2^2$, and we may choose w_r such that $w_r \equiv -1 (\mathrm{mod}\ 4)$ for all r. The element $w = \frac{w_0+w_1 i+w_2 j+\sqrt{d}k}{2}$ has order 3 in Λ_R^*/A_R^* and it verifies $\sigma_1(w) \equiv 0 (\mathrm{mod}\ 2R)$ while $\sigma_2(w) \equiv \frac{1+\sqrt{d}}{2} \not\equiv 0, 1 (\mathrm{mod}\ 2R)$, which implies, using (14), that it is not in $\langle u\rangle A_R^*$. We deduce that $\Lambda_R^*/A_R^* \simeq \langle u, w\rangle \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. □

Theorem 7. *Let $\rho = \tau(u)$, $\mu = \tau(w)$ with u, w as in the proof of Lemma* 6. *Then $SO_3(R)/\tau(A_R^*) \simeq \langle \rho, \mu\rangle \rtimes SO_3(R)/\tau(\Lambda_R^*)$, and the action of $SO_3(R)/\tau(\Lambda_R^*)$ on $\langle \rho, \mu\rangle$ is given by*

- $\rho^x \equiv \mu (\mathrm{mod}\ \tau(A_R^*))$ *and* $\mu^x \equiv \rho (\mathrm{mod}\ \tau(A_R^*))$ *if* $v_{\wp}(\psi(x))$ *odd and* $v_{\bar{\wp}}(\psi(x))$ *even*;
- $\rho^x \equiv \mu^2 (\mathrm{mod}\ \tau(A_R^*))$ *and* $\mu^x \equiv \rho^2 (\mathrm{mod}\ \tau(A_R^*))$ *if* $v_{\wp}(\psi(x))$ *even and* $v_{\bar{\wp}}(\psi(x))$ *odd*;
- $\rho^x \equiv \rho (\mathrm{mod}\ \tau(A_R^*))$ *and* $\mu^x \equiv \mu (\mathrm{mod}\ \tau(A_R^*))$ *if* $v_{\wp}(\psi(x)) \equiv v_{\bar{\wp}}(\psi(x)) \equiv 0 (\mathrm{mod}\ 2)$;
- $\rho^x \equiv \rho^2 (\mathrm{mod}\ \tau(A_R^*))$ *and* $\mu^x \equiv \mu^2 (\mathrm{mod}\ \tau(A_R^*))$ *if* $v_{\wp}(\psi(x)) \equiv v_{\bar{\wp}}(\psi(x)) \equiv 1 (\mathrm{mod}\ 2)$.

Proof. Similar arguments to those used in Theorem 5, together with Lemma 6 and (14), give us Theorem 7. □

Acknowledgments

The author thanks Ángel del Río and René Schoof for their help with earlier versions of this manuscript, Jorge Jiménez for his help with the proof of Lemma 2 and the anonymous reviewer, whose accurate and detailed observations have been of great help.

References

[1] M. Alsina, P. Bayer, Quaternion Orders, Quadratic Forms and Shimura Curves, CRM Monogr. Ser., vol. 22, Amer. Math. Soc., 2004.
[2] A.F. Beardon, The Geometry of Discrete Groups, Springer, Berlin, 1983.
[3] H. Cohn, G. Pall, Sums of four squares in a quadratic ring, Trans. Amer. Math. Soc. 105 (3) (1962) 536–556.
[4] C. Corrales-Rodrigáñez, G. Leal, E. Jespers, A. del Río, On the group of units of an order in a non-split quaternion algebra, Adv. Math. 186 (2004) 498–524.
[5] J. Elstrodt, F. Grunewald, J. Mennicke, Groups Acting on Hyperbolic Space, Harmonic Analysis and Number Theory, Springer, 1998.
[6] B. Fine, The Algebraic Structure of the Bianchi Groups, Marcel Dekker, 1989.
[7] A.J. Hahn, O.T. O'Meara, The Classical Groups and K-Theory, Grundlehren Math. Wiss., vol. 291, Springer-Verlag, 1989.
[8] T.Y. Lam, Introduction to Quadratic Forms over Fields, Grad. Stud. Math., vol. 67, Amer. Math. Soc., 2005.
[9] B. Maskit, Kleinian Groups, Springer, 1988.
[10] H. Poincaré, Mémoire sur le groupes, kleinéens, Acta Math. 3 (1883) 49–92.
[11] J. Voight, Computing Automorphic forms on Shimura curves over fields with arbitrary class number, in: Algorithmic Number Theory, Proceedings of ANTS IX, Nancy, France, 2010, in: Lecture Notes in Comput. Sci., vol. 6197, Springer, Berlin, 2010, pp. 357–371.
[12] A. Weil, Number Theory, an Approach Through History, Birkhäuser, Boston, 1984.