Mathematica Bohemica

Jan Horníček; Miroslav Kureš; Lenka Macálková

Some properties of orders of quaternion algebras with regard to the discrete norm

Mathematica Bohemica, Vol. 141 (2016), No. 3, 385–405

Persistent URL: http://dml.cz/dmlcz/145900

SOME PROPERTIES OF ORDERS OF QUATERNION ALGEBRAS WITH REGARD TO THE DISCRETE NORM

Jan Horníček, Miroslav Kureš, Lenka Macálková, Brno

Received August 31, 2015. First published July 11, 2016.
Communicated by Radomír Halaš

Abstract. Quaternion algebras $(\frac{-1,b}{\mathbb{Q}})$ are investigated and isomorphisms between them are described. Furthermore, the orders of these algebras are presented and the uniqueness of the discrete norm for such orders is proved.

Keywords: order in an imaginary quadratic field; order in a quaternion algebra; discretely normed ring; isomorphism; primitive algebra

MSC 2010: 11R52, 16H05, 16H20

1. Introduction

It has been pointed out recently that orders of imaginary quadratic fields have served as a very remarkable example for the understanding of linear algebras over rings, in particular in a detection of elementary second order matrices among invertible second order matrices, see [4]. Thus, we are motivated to use orders of quaternion algebras in the same situation. It turns out, however, that the issue here is much more difficult and deserves a deeper study. We present our first results in this paper where we discuss primarily a number of properties of quaternion algebras. The main part is focused on the so called primitive algebras, i.e. quaternion algebras $(\frac{-1,b}{\mathbb{Q}})$ and their isomorphisms. Several results about orders and suborders of these algebras are also presented.

The research has been supported by Brno University of Technology, the specific research plan No. FSI-S-14-2290 (the first and the second author), and by the Ministry of Education, Youth and Sports of the Czech Republic within the National Sustainability Program I (NPU I), grant No. LO1415, and the project CzeCOS, No. LM2010007 (the third author).

In particular, we start with the discretely normed rings defined by Cohn in [1]. We present the orders of imaginary quadratic fields and mainly the orders of quaternion algebras (which will play an important role in our investigation). That is why some properties of Hurwitz and Lipschitz quaternions and their suborders are mentioned and then our attention concentrates on primitive algebras and their maximal orders. It is aimed to describe of $\mathbb{Q}$-algebra isomorphism of $(\frac{-1,b}{\mathbb{Q}})$ and $(\frac{-1,Nb}{\mathbb{Q}})$ in the first part. The final section deals with the question of uniqueness of the discrete norm.

Results in the paper are new or with our original proof. Our intention is to present a widely intelligible research paper having also some didactic value.

In the paper, we suppose R is a ring with identity.

2. Discretely normed rings

2.1. The discrete norm.

Definition 2.1. A mapping $|\ |\colon R \to \mathbb{R}^+$ ($\mathbb{R}^+$ are nonnegative real numbers) is called a *norm on the ring* R if

(N1) $|x| = 0$ if and only if $x = 0_R$;

(N2) $|x + y| \leqslant |x| + |y|$;

(N3) $|xy| = |x||y|$

for all x, y are satisfied. A ring R with a fixed norm is called a *normed ring*.

Clearly, then R has no zero divisors, therefore normed rings are always integral domains (though not necessarily commutative).

Definition 2.2. Let R be a normed ring. If the conditions

(N4) $|x| \geqslant 1$ for all $0_R \neq x \in R$ and $|x| = 1$ if and only if $x \in \mathrm{U}(R)$;

(N5) there exists no $x \in R$ such that $1 < |x| < 2$

are satisfied, then the norm is called a *discrete norm on the ring* R and R is called a *discretely normed ring*.

In [1], (5.5), one more condition is used for certain purposes:

(N0) if $|x| = 1$ and $|x + 1| = 2$, then $x = 1_R$.

R e m a r k 2.3. Furthermore, we recall two definitions from the number field theory and add an important remark. In general, for a number field which is a finite extension of $\mathbb{Q}$, there are d monomorphisms $\sigma_1, \ldots, \sigma_d$ from such a field to $\mathbb{C}$ assigning to the minimal polynomial its roots. Then, for an element x of the number field, the norm N and the trace Tr of x are defined by

$$\mathrm{N}(x) = \prod_{i=1}^{d} \sigma_i(\alpha), \quad \mathrm{Tr}(x) = \sum_{i=1}^{d} \sigma_i(\alpha).$$

But we strictly distinguish between N and $|\ |$. For our purposes one can take $\sqrt{\mathrm{N}(x)} = |x|$ and then $|\ |$ meets Definition 2.1.

2.2. Imaginary quadratic orders. First, we recall well-known imaginary quadratic orders. We assume that d is a negative square-free integer and C a positive integer. We will distinguish two cases:

(I) $d \equiv 1 \pmod 4$,

(II) $d \equiv 2$ or $d \equiv 3 \pmod 4$.

Further, we set

$$\varepsilon = \begin{cases} 1 & \text{for the case (I)}, \\ 0 & \text{for the case (II)}; \end{cases}$$

we will use this ε for formal unification of the two cases described above to a single one in a number of formulas below. Let

$$\theta = \sqrt{d} + \frac{\varepsilon}{2}(1 - \sqrt{d}) \quad \text{and} \quad D = -d + \frac{\varepsilon}{4}(1 + 3d).$$

(It is evident that always $D \geqslant 1$.) Further, we denote by $\mathbb{Z}[C\theta]$ the order of the imaginary quadratic field $\mathbb{Q}[\sqrt{d}]$, so

$$\mathbb{Z}[C\theta] = \{x_0 + x_1 C\theta \colon\ x_0, x_1 \in \mathbb{Z}\}.$$

We take the norm $|\ |\colon\ \mathbb{Z}[C\theta] \to \mathbb{R}^+$ to be equal to the complex numbers absolute value. Then for $x = x_0 + x_1 C\theta \in \mathbb{Z}[C\theta]$ we have

$$|x|^2 = x_0^2 + \varepsilon x_0 x_1 C + x_1^2 C^2 D.$$

Then the following assertion holds (formulated by Cohn, [1]). (The claim is not new, but we write it here for the text to be more self-contained and, in particular, we present also a proof which remains usually skipped by most of the authors.)

Proposition 2.4. *The order $\mathbb{Z}[C\theta]$ with the norm defined above is a normed ring. Moreover, it is a discretely normed ring with the exception for $d = -1, -2, -3, -7, -11$ and $C = 1$ for which the condition* (N5) *is not satisfied* (*The condition* (N4) *is satisfied for all cases*).

P r o o f. Although we have the usual complex absolute value, we demonstrate some known computations in the proof. As $\Re\mathfrak{e}\, x = x_0 + \frac{1}{2}\varepsilon x_1 C$, $\Im\mathfrak{m}\, x = \big(1 - \frac{1}{2}\varepsilon\big) x_1 C\sqrt{-d}$ and $|x|^2 = (\Re\mathfrak{e}\, x)^2 + (\Im\mathfrak{m}\, x)^2$, it is clear that (N1) is satisfied. One can verify (N2) and (N3) directly.

In particular, for $\mathbb{Q}[d]$, $\mathrm{N}(x) = x \cdot \overline{x}$, $|x| = \sqrt{\mathrm{N}(x)}$. For (N3), one can show by direct evaluation that $\overline{xy} = \overline{x} \cdot \overline{y}$. Then

$$\mathrm{N}(xy) = (xy) \cdot (\overline{xy}) = x \cdot y \cdot \overline{y} \cdot \overline{x} = x \cdot \mathrm{N}(y) \cdot \overline{x} = \mathrm{N}(x) \cdot \mathrm{N}(y).$$

For square roots, the equality remains valid.

For (N2), we first observe that

$$\mathrm{N}(x+y) = (x+y) \cdot (\overline{x} + \overline{y}) = x\overline{x} + y\overline{y} + x\overline{y} + y\overline{x} = \mathrm{N}(x) + \mathrm{N}(y) + 2\,\mathrm{Tr}(x\overline{y})$$

and then, for square roots, we obtain $|x+y| \leqslant |x| + |y|$.

As to (N4), it is clear that for $|x|^2 > 0$ we in fact have $|x|^2 \geqslant 1$ because x_0, x_1, C and ε are integers and $D \geqslant 1$. Thus, if x is a unit, $|x| = 1$ because $|x^{-1}| \geqslant 1$ and $|x||x^{-1}| = 1$. On the other hand, for $|x|^2 = 1$ we have

(1) $x_0^2 = 0$ and $x_1^2 C^2 D = 1$: thus, $x_1^2 = 1$, $C = 1$ and $D = 1$;

(2) $x_0^2 = 1$ and $\varepsilon x_0 x_1 C + x_1^2 C^2 D = 0$: thus,

(2a) $\varepsilon = 0$ and $x_1 = 0$ or

(2b) $\varepsilon = 1$: then we have ($C \in \mathbb{N}$)

$$x_1(x_0 + x_1 CD) = 0;$$

it follows that $x_1 = 0$ or $x_1 CD = -x_0 = 1$ or $x_1 CD = -x_0 = -1$.

For verification of (N5), we search for integer solutions of

$$(*) \qquad 1 < x_0^2 + \varepsilon x_0 x_1 C + x_1^2 C^2 D < 4.$$

For $C \geqslant 2$ there is no integer solution for $(*)$ obviously. So we can suppose that $C = 1$. If $d \equiv 1 \pmod 4$ then the inequalities $1 < x_0^2 + x_1 x_2 + x_1^2 \left(\frac{1-d}{4}\right) < 4$ have solutions for $d = -3$ ($x_0 = x_1 = 1$), $d = -7$ ($x_0 = 0$, $x_1 = 1$) and $d = -11$ ($x_0 = 0$, $x_1 = 1$). If $d \equiv 2, 3 \pmod 4$ we get solutions for $d = -2$ ($x_0 = x_1 = 1$) and $d = -1$ ($x_0 = x_1 = 1$). □

2.3. Quaternion orders. We consider quaternion algebras over $\mathbb{Q}$ with the Hilbert symbol $\left(\frac{a,b}{\mathbb{Q}}\right)$ having elements of the form $x_0 + x_1 i + x_2 j + x_3 k$ where $i^2 = a$, $j^2 = b$, $ij = -ji = k$, where a, b are negative integers. As $\left(\frac{a,b}{\mathbb{Q}}\right) \cong \left(\frac{b,a}{\mathbb{Q}}\right) \cong \left(\frac{au^2,bv^2}{\mathbb{Q}}\right)$ for any negative a, b and nonzero u, v, there is no restriction to suppose that both a, b are square-free and $a \geqslant b$.

In particular, for $a = -1$, b square-free and $a \geqslant b$, the quaternion algebras $\left(\frac{-1,b}{\mathbb{Q}}\right)$ of this type will be called *primitive (rational quaternion) algebras*. This case will be studied in more detail.

We recall that the *discriminant* $d(a,b)$ of $\left(\frac{a,b}{\mathbb{Q}}\right)$ is

$$d(a,b) = \prod_{p \in X} p$$

where X is the set of all prime numbers for which $(a,b)_p = -1$, $(a,b)_p$ being the *Hilbert symbol* in the field $\mathbb{Q}_p$. Its explicit formula is (for details see [3])

$$(a,b)_p = \begin{cases} (-1)^{(r^2-1)/8} \cdot (-1)^{(u-1)(v-1)/2} & \text{if } p = 2, \\ \left(\frac{r \pmod p}{p}\right) & \text{if } p \neq 2, \end{cases}$$

where

$$r = (-1)^{ij} u^j v^{-i}$$

with

$$a = p^i u, \quad b = p^j v, \quad i,j \in \mathbb{Z},\ u,v \in \mathbb{Z}_p^\times.$$

Now, we define (for details see [5]) that an *order* $\mathcal{O}$ of $\left(\frac{a,b}{\mathbb{Q}}\right)$ is a complete $\mathbb{Z}$-lattice which is also a ring with 1. We also recall that the norm $\mathrm{N}(\alpha)$ and the trace $\mathrm{Tr}(\alpha)$ of an element α from a $\mathbb{Z}$-lattice lie in $\mathbb{Z}$, cf. [5], Lemma 2.2.4. Thus, the trivial result is that

$$\mathbb{Z}[1,i,j,k]\Big(\frac{a,b}{\mathbb{Q}}\Big) = \{x_0 + x_1 i + x_2 j + x_3 k\colon\ x_i \in \mathbb{Z},\ i = 0,1,2,3\}$$

is the order for each a, b; let us call it the *order of Lipschitz-like quaternions*. We observe also that if $x = x_0 + x_1 i + x_2 j + x_3 k$ is an element of an order $\mathcal{O}$ of $\left(\frac{a,b}{\mathbb{Q}}\right)$ then $2x_0 \in \mathbb{Z}$.

An order is *maximal* if it is maximal with respect to inclusion. In particular, the following results hold.

Proposition 2.5. *Let $A = \left(\frac{-1,b}{\mathbb{Q}}\right)$ be a primitive algebra.*

(i) *If $b \equiv 1 \pmod 4$, then*

$$\mathbb{Z}\Big[\frac{1+j}{2}, \frac{i+k}{2}, j, k\Big]\Big(\frac{-1,b}{\mathbb{Q}}\Big)$$

is the maximal order of A.

(ii) *If b is even, there is no unique description of the basis of the maximal order of A valid for all even b.*

P r o o f. (i) This is Theorem 6.1 in [2].

(ii) Let $A_1 = \left(\frac{-1,-2}{\mathbb{Q}}\right), A_2 = \left(\frac{-1,-10}{\mathbb{Q}}\right)$ with bases $\{\hat{1},\hat{i},\hat{j},\hat{k}\}$, $\{\tilde{1},\tilde{i},\tilde{j},\tilde{k}\}$ and take $B = \left(\frac{-1,-1}{\mathbb{Q}}\right)$, which is isomorphic to both A_1, A_2 and has the basis $\{1,i,j,k\}$ (we will discuss isomorphisms in more detail in Section 4, in particular in 4.1) and the maximal order $\mathbb{Z}[(1+i+j+k)/2,i,j,k]\left(\frac{-1,-1}{\mathbb{Q}}\right)$. The isomorphisms can be expressed explicitly as

$$\varphi_{B\to A_1}(1) = \hat{1},\ \ \varphi_{B\to A_1}(i) = \hat{i},\ \ \varphi_{B\to A_1}(j) = \frac{\hat{j}+\hat{k}}{2},\ \ \varphi_{B\to A_1}(k) = \frac{-\hat{j}+\hat{k}}{2},$$
$$\varphi_{B\to A_2}(1) = \tilde{1},\ \ \varphi_{B\to A_2}(i) = \tilde{i},\ \ \varphi_{B\to A_2}(j) = \frac{3\tilde{j}+\tilde{k}}{10},\ \ \varphi_{B\to A_2}(k) = \frac{-\tilde{j}+3\tilde{k}}{10}.$$

It is sufficient to find images of $(1+i+j+k)/2$ in both the isomorphisms:

$$\varphi_{B\to A_1}\Big(\frac{1+i+j+k}{2}\Big) = \frac{1+\hat{i}+\hat{k}}{2},$$
$$\varphi_{B\to A_2}\Big(\frac{1+i+j+k}{2}\Big) = \frac{1+\tilde{i}}{2} + \frac{\tilde{j}+2\tilde{k}}{10};$$

we have just computed $\mathcal{O}_{A_1} = \mathbb{Z}\big[(1+\hat{i}+\hat{k})/2,\hat{i},(\hat{j}+\hat{k})/2,(-\hat{j}+\hat{k})/2\big]\left(\frac{-1,-2}{\mathbb{Q}}\right)$, $\mathcal{O}_{A_2} = \mathbb{Z}[(1+\tilde{i})/2 + (\tilde{j}+2\tilde{k})/10,\tilde{i},(3\tilde{j}+\tilde{k})/10,(-\tilde{j}+3\tilde{k})/10]\left(\frac{-1,-10}{\mathbb{Q}}\right)$ as maximal orders of A_1, A_2 and it can be easily computed that these two orders are mutually distinct. We remark that it implies that the Theorem 6.2 in [2] is not correct.[1] □

R e m a r k 2.6. The algorithm how to derive maximal orders of quaternion algebras can be found in the paper [6] of Voight.

3. Hurwitz and Lipschitz quaternions and their suborders

The case of the algebra $\left(\frac{-1,-1}{\mathbb{R}}\right)$ is classical and its maximal orders (as well as for the algebra $\left(\frac{-1,-1}{\mathbb{Q}}\right)$) are Hurwitz quaternions

$$\mathbb{Z}\Big[\frac{1+i+j+k}{2},i,j,k\Big]\Big(\frac{-1,-1}{\mathbb{R}}\Big)$$

For fixed $C_0, C_1, C_2, C_3 \in \mathbb{N}$, let us take

$$\mathcal{H}(C_0,C_1,C_2,C_3) = \mathbb{Z}\Big[C_0\frac{1+i+j+k}{2},C_1i,C_2j,C_3k\Big]\Big(\frac{-1,-1}{\mathbb{R}}\Big)$$

[1] The exact quote from [2]: *Let* $B = \left(a,b/\mathbb{Q}\right)$ *with* $a \equiv 3 \pmod 4$, *b even, and ab squarefree. Then* $\mathcal{L} = \mathbb{Z}[1,i,(1+i+j)/2,(j+k)/2]$ *is a maximal order in* B. We have shown the inadequacy of this description.

and determine whether $\mathcal{H}(C_0, C_1, C_2, C_3)$ has a structure of a ring. (We remark that we consider rings with multiplication given by $i^2 = j^2 = -1$ and $ij = k = -ji$ and having 1 as the neutral element of the multiplication.) First, it is well known that the answer is affirmative for $\mathcal{H}(1,1,1,1)$ and $\mathcal{H}(2,1,1,1)$, *Hurwitz quaternions* and *Lipschitz quaternions*, respectively. Looking for other examples, we observe that if $\mathcal{H}(C_0, C_1, C_2, C_3)$ is a subset of $\mathcal{H}(\overline{C}_0, \overline{C}_1, \overline{C}_2, \overline{C}_3)$, then $C_0 \leqslant \overline{C}_0$, $C_1 \leqslant \overline{C}_1$, $C_2 \leqslant \overline{C}_2$ and $C_3 \leqslant \overline{C}_3$. Now, in general, we have:

Lemma 3.1.

(i) *If* $\mathcal{H}(C_0, C_1, C_2, C_3)$ *is a ring, then* $C_0 = 1$ *or* $C_0 = 2$.
(ii) *If* $\mathcal{H}(1, C_1, C_2, C_3)$ *is a ring, then* $C_1 = C_2 = C_3 = 1$.

P r o o f. (i) If $C_0 \geqslant 3$, then $1 \notin \mathcal{H}(C_0, C_1, C_2, C_3)$.
(ii) The same reasoning. □

So, suborders different from Hurwitz and Lipschitz quaternions are proper suborders of Lipschitz quaternions $\mathcal{H}(2, C_1, C_2, C_3)$. Now, we take Lipschitz quaternions

$$\mathbb{Z}[1, i, j, k]\Big(\frac{-1, -1}{\mathbb{R}}\Big)$$

and similarly, for fixed $C_0, C_1, C_2, C_3 \in \mathbb{N}$, we consider

$$\mathcal{L}(C_0, C_1, C_2, C_3) = \mathbb{Z}[C_0, C_1 i, C_2 j, C_3 k]\Big(\frac{-1, -1}{\mathbb{R}}\Big)$$

and determine whether $\mathcal{L}(C_0, C_1, C_2, C_3)$ has a structure of a ring; again, if $\mathcal{L}(C_0, C_1, C_2, C_3)$ is a subset of $\mathcal{L}(\overline{C}_0, \overline{C}_1, \overline{C}_2, \overline{C}_3)$, then $C_0 \leqslant \overline{C}_0$, $C_1 \leqslant \overline{C}_1$, $C_2 \leqslant \overline{C}_2$ and $C_3 \leqslant \overline{C}_3$. We have already proved that if $\mathcal{L}(C_0, C_1, C_2, C_3)$ is a ring, then $C_0 = 1$.

Let us denote by $\langle S \rangle$ the ring generated by a set S with the above described multiplication.

Lemma 3.2. $\langle \mathcal{L}(1, C_1, C_2, C_3) \rangle = \langle \mathcal{L}(1, C_1, C_2, \gcd(C_1 C_2, C_3)) \rangle$.

P r o o f. Evidently, in $\langle \mathcal{L}(1, C_1, C_2, C_3) \rangle$ there coexist $C_1 i C_2 j = C_1 C_2 k$ and $C_3 k$. Thus, $\gcd(C_1 C_2, C_3) k \in \langle \mathcal{L}(1, C_1, C_2, C_3) \rangle$, too. □

Analogously,

$$\langle \mathcal{L}(1, C_1, C_2, C_3) \rangle = \langle \mathcal{L}(1, C_1, \gcd(C_1 C_3, C_2), C_3) \rangle = \langle \mathcal{L}(1, \gcd(C_2 C_3, C_1), C_2, C_3) \rangle.$$

We can formulate the following result.

Proposition 3.3. $\mathcal{L}(1, C_1, C_2, C_3) = \langle \mathcal{L}(1, C_1, C_2, C_3) \rangle$ *if and only if* $C_1 \mid C_2 C_3$, $C_2 \mid C_1 C_3$ *and* $C_3 \mid C_1 C_2$.

P r o o f. Let us suppose that $\{x_0 + x_1C_1i + x_2C_2j + x_3C_3k\colon\ x_0, x_1, x_2, x_3 \in \mathbb{Z}\}$ represents a ring. As $C_1iC_2j = C_1C_2k$ belongs to this ring, C_1C_2 must be a multiple of C_3. The properties $C_2 \mid C_1C_3$ and $C_3 \mid C_1C_2$ are derived in the same way.

The proof of the opposite implication is trivial. □

Because of symmetric properties of C_1, C_2 and C_3, it is no restriction to consider $C_1 \leqslant C_2 \leqslant C_3$. (The "simplest" example of a proper suborder is $\mathcal{L}(1, 1, 2, 2)$.)

4. Primitive quaternion algebras

We start with the following assertion.

Lemma 4.1. *The discriminant of a primitive algebra* $\left(\frac{-1,b}{\mathbb{Q}}\right)$ *is a non-prime number if and only if* $-b$ *has a form* $2^l(4k+1)$ *which is not a sum of two squares* ($k \in \mathbb{N}$, $l \in \{0, 1\}$).

P r o o f. We use the explicit formula for the discriminant given above. First, let $p = 2$. We have $i = 0$, $u = -1$, $j = l$ and $v = -4k - 1$. We compute $r = -1$ and $(a, b)_2 = -1$. Hence $d(a, b)$ is even.

Second, let $p \neq 2$ be a prime number which divides $4k + 1$. Then $4k + 1 = pn$, where p does not divide n. Now, we have $i = 0$, $u = -1$, $j = 1$ and $v = -2^l n$ and we compute $r = -1$ and $(a, b)_p = \left(\frac{p-1}{p}\right)$. So, $d(a, b)$ is a multiple of p if $\left(\frac{p-1}{p}\right) = -1$.

We have $4k + 1$ square-free and morever not a sum of two squares. It follows $4k + 1$ is not a prime number. Thus, $4k + 1$ is a product of different prime numbers p_i, $i = 1, \ldots, h$, and one of them, say p_1, has a form $4m_1+3$. However, it is impossible that all other p_i have a form $4m_i + 1$ because the product has a form $4k + 1$. Hence we have at least two primes which factorize $4k+1$ and have a form $4m_i+3$, say with indexes $i = 1, 2$. Then $\left(\frac{p_1-1}{p_1}\right) = \left(\frac{p_2-1}{p_2}\right) = -1$ and both p_1 and p_2 divide $d(a, b)$. □

Corollary 4.2. *There is no primitive algebra* $\left(\frac{-1,b}{\mathbb{Q}}\right)$ *with a discriminant which is a product of exactly two prime factors.*

P r o o f. We have proved that the discriminant is even and if it has a divisor $p_1 \neq 2$, it has one more different divisor p_2. □

4.1. $\mathbb{Q}$-algebra isomorphisms of quaternion algebras $\left(\frac{-1,b}{\mathbb{Q}}\right)$ and $\left(\frac{-1,Nb}{\mathbb{Q}}\right)$. It is known that there exist infinitely many non-isomorphic quaternion algebras $\left(\frac{a,b}{\mathbb{Q}}\right)$. Isomorphisms preserve maximal orders. We want to find some conditions under which two primitive algebras are isomorphic. It is well known that algebras $\left(\frac{-1,b}{\mathbb{Q}}\right)$

and $\left(\frac{-1,bu^2}{\mathbb{Q}}\right)$, $u \in \mathbb{N}$ are isomorphic; however, we aim at describing when two primitive algebras are isomorphic: so, we recall that b is assumed negative square-free and, for $\left(\frac{-1,Nb}{\mathbb{Q}}\right)$ to be primitive, Nb is negative square-free, too.

4.1.1. Binding equations. So, let us consider algebras $A_1 = \left(\frac{-1,b}{\mathbb{Q}}\right)$ with the base $(1, i, j, k)$ and the discriminant d_1 and $A_2 = \left(\frac{-1,Nb}{\mathbb{Q}}\right)$ with the base $(1, I, J, K)$ and the discriminant d_2, $b \in \mathbb{Z}^-$, $N \in \mathbb{N} - \{1\}$ and a homomorphism $\varphi\colon\ A_1 \to A_2$,

$$\begin{aligned}
\varphi(1) &= 1,\\
\varphi(i) &= \varphi_{10} + \varphi_{11}I + \varphi_{12}J + \varphi_{13}K,\\
\varphi(j) &= \varphi_{20} + \varphi_{21}I + \varphi_{22}J + \varphi_{23}K,\\
\varphi(k) &= \varphi_{30} + \varphi_{31}I + \varphi_{32}J + \varphi_{33}K
\end{aligned}$$

with φ_{uv} rational. If we search for $\mathbb{Q}$-algebra homomorphisms, $\varphi(k)$ is given by multiplication. Further, $-1 = \varphi(i^2)$ gives $\varphi_{10} = 0$ and

$$-1 = -\varphi_{11}^2 + \varphi_{12}^2 Nb + \varphi_{13}^2 Nb, \tag{4.1}$$

$b = \varphi(j^2)$ gives $\varphi_{20} = 0$ and

$$b = -\varphi_{21}^2 + \varphi_{22}^2 Nb + \varphi_{23}^2 Nb \tag{4.2}$$

and finally $\varphi(ij) = -\varphi(ji)$ gives

$$0 = \varphi_{11}\varphi_{21} - \varphi_{12}\varphi_{22}Nb - \varphi_{13}\varphi_{23}Nb \quad (= -\varphi_{30}). \tag{4.3}$$

Hence every $\mathbb{Q}$-algebra homomorphism $\varphi\colon\ A_1 \to A_2$ has a form

$$\begin{aligned}
\varphi(1) &= 1,\\
\varphi(i) &= \varphi_{11}I + \varphi_{12}J + \varphi_{13}K,\\
\varphi(j) &= \varphi_{21}I + \varphi_{22}J + \varphi_{23}K,\\
\varphi(k) &= (\varphi_{13}\varphi_{22} - \varphi_{12}\varphi_{23})NbI + (\varphi_{13}\varphi_{21} - \varphi_{11}\varphi_{23})J + (\varphi_{11}\varphi_{22} - \varphi_{12}\varphi_{21})K,
\end{aligned}$$

with conditions (4.1), (4.2) and (4.3) necessarily fulfilled. (Of course, it is possible to express the $\mathbb{Q}$-algebra homomorphism only in three φ_{uv}-s and without additional conditions. But the obtained form is rather complicated.)

Proposition 4.3. *Every $\mathbb{Q}$-algebra homomorphism described above is a $\mathbb{Q}$-algebra isomorphism.*

P r o o f. The determinant of the transformation above equals

$$\varphi_{11}^2\varphi_{22}^2 - 2\varphi_{11}\varphi_{12}\varphi_{21}\varphi_{22} + \varphi_{12}^2\varphi_{21}^2 + \varphi_{11}^2\varphi_{23}^2 - 2\varphi_{11}\varphi_{13}\varphi_{21}\varphi_{23} + \varphi_{13}^2\varphi_{21}^2 \\ - (\varphi_{12}^2\varphi_{23}^2 - 2\varphi_{12}\varphi_{13}\varphi_{22}\varphi_{23} + \varphi_{13}^2\varphi_{22}^2)Nb$$

and we obtain the same expression as $\varphi(k^2)/Nb$.

It is evident from the form of $\mathbb{Q}$-algebra homomorphism that $\varphi(k)$ is nonzero if and only if at least one minor of the order 2 of the matrix $\begin{pmatrix} \varphi_{11} & \varphi_{12} & \varphi_{13} \\ \varphi_{21} & \varphi_{22} & \varphi_{23} \end{pmatrix}$ is nonzero, i.e. the rank of the matrix is 2. First, let us notice that $(\,\varphi_{11}\ \ \varphi_{12}\ \ \varphi_{13}\,) = (\,0\ \ 0\ \ 0\,)$ and $(\,\varphi_{21}\ \ \varphi_{22}\ \ \varphi_{23}\,) = (\,0\ \ 0\ \ 0\,)$ are impossible due to (4.1) and (4.2), respectively. So, let us suppose $(\,\varphi_{11}\ \ \varphi_{12}\ \ \varphi_{13}\,) \neq (\,0\ \ 0\ \ 0\,)$, $c \neq 0$ and $(\,\varphi_{21}\ \ \varphi_{22}\ \ \varphi_{23}\,) = c\,(\,\varphi_{11}\ \ \varphi_{12}\ \ \varphi_{13}\,)$. Then (4.3) gives $0 = c\varphi_{11}^2 - c\varphi_{12}^2Nb - c\varphi_{13}^2Nb$. But this contradicts (4.1). Hence $\varphi(k)$ is nonzero and the transformation is nonsingular. □

Let us remark that (4.1) yields

$$|\varphi_{11}| = \sqrt{1 + (\varphi_{12}^2 + \varphi_{13}^2)Nb} \quad \text{which implies } \varphi_{11} \in [-1, 1] \cap \mathbb{Q} \tag{4.4}$$

and (4.2) yields

$$|\varphi_{21}| = \sqrt{-b + (\varphi_{22}^2 + \varphi_{23}^2)Nb} \quad \text{which implies } \varphi_{21} \in [-\sqrt{-b}, \sqrt{-b}] \cap \mathbb{Q}. \tag{4.5}$$

4.1.2. Special cases. First, let us consider the case $|\varphi_{11}| = 1$. Then, due to (4.4) and (4.3), $\varphi_{12} = \varphi_{13} = \varphi_{21} = 0$ and (4.2) reads

$$\frac{1}{\varphi_{22}^2 + \varphi_{23}^2} = N. \tag{4.6}$$

Evidently, neither φ_{22} nor φ_{23} can be integer because $N \in \mathbb{N} - \{1\}$. If $\alpha, \beta \in \mathbb{N}_0$ and $N = \alpha^2 + \beta^2$, we find a rational solution $\varphi_{22} = \alpha/(\alpha^2 + \beta^2)$, $\varphi_{23} = \beta/(\alpha^2 + \beta^2)$.[2] But one can even find infinitely many rational solutions, see e.g. [3]. Moreover, no other case can occur as we show in the following lemma.

Lemma 4.4. *If $1/(\tau^2 + \upsilon^2) = N \in \mathbb{N}$ for rational τ, υ, then $N = \alpha^2 + \beta^2$, $\alpha, \beta \in \mathbb{N}_0$.*

[2] In particular, for $N = 2$ we find easily isomorphisms $\varphi(i) = \pm I$, $\varphi(j) = \frac{1}{2}J + \frac{1}{2}K$, $\varphi(k) = -\frac{1}{2}J \pm \frac{1}{2}K$.

P r o o f. Let $\tau = a/b$, $\upsilon = c/d$, $a, b, c, d \in \mathbb{Z}$, $\gcd(a, b) = 1$, $\gcd(c, d) = 1$. Then

$$b^2d^2 = N(a^2d^2 + c^2b^2).$$

It is well known that a number M is a sum of two squares if and only if in the prime factorization of M, every prime congruent to 3 modulo 4 occurs an even number of times, i.e. $M = 2^\kappa p_1^{\lambda_1} \dots p_r^{\lambda_r} q_1^{2\mu_1} \dots q_s^{2\mu_s}$ where p_i, $i = 1, \dots, r$, are different prime numbers congruent to 1 modulo 4 and q_j, $j = 1, \dots, s$, are different prime numbers congruent to 3 modulo 4, $\kappa \in \mathbb{N}_0$, $\lambda_i, \mu_j \in \mathbb{N}$. If N is not a sum of two squares, there exist a prime number q congruent to 3 modulo 4 and $\mu \in \mathbb{N}$ such that $q^{2\mu-1} \mid N$ and $q^{2\mu} \nmid N$. However, this q must be an even number of times in the factorization of b^2d^2 on the left hand side. Thus, there exist $\bar{\mu} \in \mathbb{N}$ such that $q^{2\bar{\mu}-1} \mid (a^2d^2 + c^2b^2)$ and $q^{2\bar{\mu}} \nmid (a^2d^2 + c^2b^2)$, but this contradicts the fact that $a^2d^2 + c^2b^2$ is the sum of two squares. □

Thus we have proved

Proposition 4.5. *If $\varphi\colon A_1 \to A_2$ is a $\mathbb{Q}$-algebraic homomorphism with $|\varphi_{11}| = 1$, then A_1 and A_2 are isomorphic and N is necessarily a sum of squares.*

Second, let us consider the case $|\varphi_{11}| \neq 1$. We start with an example.

E x a m p l e 4.6. Let $b = -2$, $\varphi_{11} = 1/2$. Then (4.1) gives

$$\frac{8N}{3}(\varphi_{12}^2 + \varphi_{13}^2) = 1.$$

E.g., for $N = 3$, the equation has a rational solution $\varphi_{12} = 1/4$, $\varphi_{13} = 1/4$. (Cf. Theorem 2.3 from [3].) Using (4.3) and (4.2), we continue with the equation

$$\frac{15}{2}\varphi_{22}^2 + 9\varphi_{22}\varphi_{23} + \frac{15}{2}\varphi_{23}^2 = 1,$$

which, after the linear transformation $\xi = 2\varphi_{22} + 2\varphi_{23}$, $\eta = \varphi_{22} - \varphi_{23}$, reads

$$\frac{3}{2}\xi^2 + \frac{3}{2}\eta^2 = 1,$$

which has no rational solution (using also Theorem 2.3 from [3]).[3]

[3] We can also take another solution: e.g. $\varphi_{12} = 1/20$, $\varphi_{13} = 7/20$; then we continue with the equation

$$\frac{159}{50}\varphi_{22}^2 + \frac{63}{25}\varphi_{22}\varphi_{23} + \frac{591}{50}\varphi_{23}^2 = 1.$$

Proposition 4.7. *If $N \equiv 3 \pmod 4$, then there is no $\mathbb{Q}$-algebra homomorphism from A_1 to A_2.*

P r o o f. If $|\varphi_{11}| = 1$, then N must be a sum of squares due to Proposition 4.5 which contradicts $N \equiv 3 \bmod 4$. For $|\varphi_{11}| \neq 1$, we put $\gamma = \varphi_{21}/(1-\varphi_{11})$. We compute easily $\gamma^2 = (\varphi_{21} + \varphi_{11}\gamma)^2$.

Let us express the equation $(4.2) + 2\gamma(4.3) + \gamma^2(4.1)$:

$$\begin{aligned} b - \gamma^2 = & -\varphi_{21}^2 - 2\gamma\varphi_{21}\varphi_{11} - \gamma^2\varphi_{11}^2 \\ & + Nb(\varphi_{22}^2 + 2\gamma\varphi_{22}\varphi_{12} + \gamma^2\varphi_{12}^2 + \varphi_{23}^2 + 2\gamma\varphi_{23}\varphi_{13} + \gamma^2\varphi_{13}^2), \end{aligned}$$

i.e.

$$b - \gamma^2 = -\gamma^2 + Nb((\varphi_{22} + \gamma\varphi_{12})^2 + (\varphi_{23} + \gamma\varphi_{13})^2).$$

Hence

$$N = \frac{1}{(\varphi_{22} + \gamma\varphi_{12})^2 + (\varphi_{23} + \gamma\varphi_{13})^2}$$

and it follows that N is a sum of squares due to Lemma 4.4. Again, it contradicts $N \equiv 3 \pmod 4$. □

Theorem 4.8. *A_1 and A_2 are isomorphic if and only if N is a sum of squares.*

P r o o f. The previous propositions yield that the existence of a $\mathbb{Q}$-algebra homomorphism implies $N = \alpha^2 + \beta^2$. On the other hand, if we assume $N = \alpha^2 + \beta^2$, then

$$\begin{aligned} \varphi(1) &= 1, \\ \varphi(i) &= I, \\ \varphi(j) &= \frac{\alpha}{N}J + \frac{\beta}{N}K, \\ \varphi(k) &= -\frac{\beta}{N}J + \frac{\alpha}{N}K \end{aligned}$$

is an example of a $\mathbb{Q}$-algebra isomorphism and this completes the proof. □

4.2. Automorphisms: examples. Let $\varphi\colon A_1 \to A_2$ and $\overline{\varphi}\colon A_2 \to A_1$ be isomorphisms, then $\varphi \circ \overline{\varphi}\colon A_1 \to A_1$ is clearly an automorphism of A_1. We remark that there is a nontrivial structure of such automorphisms with all these possibilities:

(i) $\alpha^n = \mathrm{id}$ for some $n \in \mathbb{N}$,

(ii) $\alpha^n \neq \mathrm{id}$ for every $n \in \mathbb{N}$,

(iii) α is *unipotent* which means $\alpha - \mathrm{id}$ is nilpotent, i.e. $(\alpha - \mathrm{id})^n$ is the zero endomorphisms for some $n \in \mathbb{N}$.

We will demonstrate it in the following examples. For representation of φ we can take its matrix form $\varphi = \{\varphi_{ij}\}$, $i,j = 0,\dots,3$ described in the previous sections. For simplicity, we can use in the next considerations only the submatrix

$$\Phi = \begin{pmatrix} \varphi_{11} & \varphi_{12} & \varphi_{13} \\ \varphi_{21} & \varphi_{22} & \varphi_{23} \\ \varphi_{31} & \varphi_{32} & \varphi_{33} \end{pmatrix}.$$

The identity matrix corresponding to id is denoted by I.

E x a m p l e 4.9. (Case (i).)

(1) Let $A_1 = \left(\frac{-1,-1}{\mathbb{Q}}\right)$, $A_2 = \left(\frac{-1,-2}{\mathbb{Q}}\right)$ and let φ_1, φ_2 be given by the matrices

$$\varphi_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 1 & 1 \end{pmatrix}, \quad \varphi_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} \\ 0 & -\frac{1}{2} & \frac{1}{2} \end{pmatrix};$$

then it is easy to compute that

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} \\ 0 & -\frac{1}{2} & \frac{1}{2} \end{pmatrix} = I, \quad \text{so we have } n = 1.$$

(2) Let $A_1 = \left(\frac{-1,-1}{\mathbb{Q}}\right)$, $A_2 = \left(\frac{-1,-2}{\mathbb{Q}}\right)$ and let φ_1, φ_2 be given by the matrices

$$\varphi_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & -1 & 1 \end{pmatrix}, \quad \varphi_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} \\ 0 & -\frac{1}{2} & \frac{1}{2} \end{pmatrix};$$

then

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} \\ 0 & -\frac{1}{2} & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix} \neq I$$

and

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}^4 = I \quad \text{i.e. } n = 4.$$

Nevertheless,

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix} - I = \begin{pmatrix} 0 & 0 & 0 \\ 0 & -1 & 1 \\ 0 & -1 & -1 \end{pmatrix}$$

has nonzero determinant and that is why the condition (iii) is not fulfilled.

E x a m p l e 4.10. (Case (ii).) We will prove that for the matrix $A=\begin{pmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ -\frac{4}{3} & \frac{2}{3} & -\frac{1}{3} \\ -\frac{4}{3} & -\frac{1}{3} & \frac{2}{3} \end{pmatrix}$ there exists no $n \in \mathbb{N}$ such that $A^n = I$.

First we need to realize that for arbitrary $i \in \mathbb{N}$ we can express A^i in the special form

$$A^i = \begin{pmatrix} a & b & b \\ c & d & e \\ c & e & d \end{pmatrix}, \quad a, b, c, d, e \in \mathbb{Q}.$$

But this is easy, because

$$\begin{pmatrix} a & b & b \\ c & d & e \\ c & e & d \end{pmatrix} \begin{pmatrix} x & y & y \\ z & u & t \\ z & t & u \end{pmatrix} = \begin{pmatrix} ax + 2bz & ay + b(u+t) & ay + b(u+t) \\ cx + z(d+e) & cy + du + et & cy + du + et \\ cx + z(d+e) & cy + eu + dt & cy + eu + dt \end{pmatrix}$$

and we have only finitely many + and $\cdot$ for numbers in $\mathbb{Q}$.

Now suppose $n \in \mathbb{N}$ is minimal such that $A^n = I$, and distinguish two cases:

(1) Let n be odd ($n = 2k + 1$), put $i = k$, so $A^k = \begin{pmatrix} a & b & b \\ c & d & e \\ c & e & d \end{pmatrix}$ and

$$(A^k)^2 = \begin{pmatrix} a^2 + 2bc & b(a+d+e) & b(a+d+e) \\ c(a+d+e) & bc + d^2 + e^2 & bc + 2de \\ c(a+d+e) & bc + 2de & bc + d^2 + e^2 \end{pmatrix} = A^{n-1} = \begin{pmatrix} \frac{1}{3} & -\frac{1}{3} & -\frac{1}{3} \\ \frac{4}{3} & \frac{2}{3} & -\frac{1}{3} \\ \frac{4}{3} & -\frac{1}{3} & \frac{2}{3} \end{pmatrix},$$

where $A^{n-1} = A^{-1}$, which can be easily computed. However, if we solve the above set of equations for rational numbers a, b, c, d and e, we obtain a contradiction, because $a = \pm\sqrt{2/3}$.

(2) Let n be even ($n = 2k + 2$), put $i = k$, so $A^k = \begin{pmatrix} a & b & b \\ c & d & e \\ c & e & d \end{pmatrix}$ and

$$(A^k)^2 = \begin{pmatrix} a^2 + 2bc & b(a+d+e) & b(a+d+e) \\ c(a+d+e) & bc + d^2 + e^2 & bc + 2de \\ c(a+d+e) & bc + 2de & bc + d^2 + e^2 \end{pmatrix} = A^{n-2} = (A^{-1})^2$$
$$= \begin{pmatrix} -\frac{7}{3} & -\frac{2}{9} & -\frac{2}{9} \\ \frac{8}{9} & \frac{1}{9} & -\frac{8}{9} \\ \frac{8}{9} & -\frac{8}{9} & \frac{1}{9} \end{pmatrix}.$$

It this case we also obtain a contradiction, again by computing irrational solution. Nevertheless the computation is a little bit more complicated than in the first case.

E x a m p l e 4.11. (Case (iii).) We present the following example of an automorphism which is not unipotent. Let $A_1 = \left(\frac{-1,-1}{\mathbb{Q}}\right)$, $A_2 = \left(\frac{-1,-4}{\mathbb{Q}}\right)$ and let φ and $\overline{\varphi}$ be given by matrices

$$\Phi = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & -2 \end{pmatrix}, \quad \overline{\Phi} = \begin{pmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{2}{3} & -\frac{1}{3} & \frac{1}{6} \\ \frac{2}{3} & \frac{1}{6} & -\frac{1}{3} \end{pmatrix}.$$

We compute

$$\Phi\overline{\Phi} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & -2 \end{pmatrix} \begin{pmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{2}{3} & -\frac{1}{3} & \frac{1}{6} \\ \frac{2}{3} & \frac{1}{6} & -\frac{1}{3} \end{pmatrix} = \begin{pmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ -\frac{4}{3} & \frac{2}{3} & -\frac{1}{3} \\ -\frac{4}{3} & -\frac{1}{3} & \frac{2}{3} \end{pmatrix} = M$$

and it could be shown that there does not exist $n \in \mathbb{N}$ for which $(M-I)^n$ is the zero matrix.

R e m a r k 4.12. We notice that some automorphisms above are nothing but rotations given by actions of the group $\mathrm{SO}(3,\mathbb{Q})$. Nevertheless, *non-rotational automorphisms* also exist. For instance, such an automorphism in $A = \left(\frac{-1,-2}{\mathbb{Q}}\right)$ is given by the matrix

$$\begin{pmatrix} 0 & -\frac{1}{2} & -\frac{1}{2} \\ 1 & -\frac{1}{2} & \frac{1}{2} \\ -1 & -\frac{1}{2} & \frac{1}{2} \end{pmatrix}.$$

Of course, it would be interesting to describe geometric transformations corresponding to non-rotational automorphisms.

We say that an order $\mathcal{O}$ in $\left(\frac{a,b}{\mathbb{Q}}\right)$ is *in the canonical position* if $\mathcal{O} \subseteq \mathbb{Z}[1,i,j,k]\left(\frac{a,b}{\mathbb{Q}}\right)$ or $\mathbb{Z}[1,i,j,k]\left(\frac{a,b}{\mathbb{Q}}\right) \subseteq \mathcal{O}$.

R e m a r k 4.13. Let us formulate an easy observation about suborders of maximal orders of primitive algebras. If we take Lipschitz-like orders of primitive algebras, it is not difficult to see that the property from Proposition 3.3 is preserved for this case, too.

Thus, for the description of the whole structure of orders it remains to determine the structure between the maximal order and the Lipschitz-like order.

5. On the uniqueness of discrete norm

5.1. Integers. In this section, we prove assertions on the uniqueness of the discrete norm. We start with classical integers.

Proposition 5.1. *For $R = \mathbb{Z}$, there is one and only one norm satisfying conditions* (N1)–(N5).

P r o o f. Let $k \in \mathbb{N}$. Using (N2) we obtain

$$|k| = |\underbrace{1 + \ldots + 1}_{k\text{-times}}| \leqslant \underbrace{|1| + \ldots + |1|}_{k\text{-times}} = k,$$

so we have $|k| \leqslant k$, which can be rewritten into the form $|k| = k - Q(k)$, where $Q(k) \in \mathbb{R}^+$, $0 \leqslant Q(k) < k$. It is easy to see that for every norm this gives the map $Q\colon \mathbb{N} \to \mathbb{R}^+$. If we suppose that there exists $k_0 \in \mathbb{N}$, $k_0 \neq 1$, for which $Q(k_0) < Q(k_0 - 1)$, then

$$|k_0| = k_0 - Q(k_0) > k_0 - Q(k_0 - 1) = (k_0 - 1) - Q(k_0 - 1) + 1,$$

but of course $(k_0 - 1) - Q(k_0 - 1) = |(k_0 - 1)|$ and $1 = |1|$ by (N4), so we have

$$|k_0| > |k_0 - 1| + |1|,$$

which contradicts (N2). Thus, there is no such k_0 for which $Q(k_0) < Q(k_0 - 1)$, hence Q is nondecreasing. Finally, let us evaluate $|\ |$ at some points: $|1| = 1$ by (N4) and $|2| = 2$ by (N4), (N5) and $|k| \leqslant k$. Moreover, by (N3) it is easy to deduce $|2^n| = 2^n$ for all $n \in \mathbb{N}$, so $Q(2^n) = 2^n - |2^n| = 0$. Q is nondecreasing, it is identically equal to 0. Thus, $|k| = k$ for every $k \in \mathbb{N}$. Clearly, $|0| = 0$ and as $1 = |1| = |(-1)(-1)| = |-1||-1|$, where $|\ |$ is nonnegative, so $|-1| = 1$. Hence for every $k \in \mathbb{N}$, $|-k| = |-1||k| = |k|$. Altogether, the discrete norm $|\ |\colon \mathbb{Z} \to \mathbb{R}^+$ satisfying (N1)–(N5) is unique and it is nothing but the standard absolute value. □

R e m a r k 5.2. We note that the weakening of the definition of the discretely normed ring by omitting (N4) leads to the non-uniqueness. Certainly, one can express $m \in \mathbb{Z}$ by the formally infinite product

$$m = \operatorname{sgn}(m) \prod_{p \in \mathbb{P}} p^{e(m,p)}$$

where $\mathbb{P}$ is the set of prime numbers. Now, for a prime number p, we define the *p-norm* $|\ |_p\colon \mathbb{Z} \to \mathbb{R}^+$ on $\mathbb{Z}$ by

$$|m|_p = \frac{1}{p^{e(m,p)}} \quad \text{for } m \neq 0,\ |0|_p = 0.$$

The conditions (N1), (N3) and (N5) are satisified evidently, the verification of (N2) requires a straightforward calculation which is left to the reader. It is clear that there are integers not belonging to $\mathrm{U}(\mathbb{Z}) = \{-1, 1\}$ having the p-norm $1/p^0 = 1$; therefore (N4) is not satisfied. We thank Professor Ladislav Skula for his kind interest and for pointing out this nice example.

5.2. Imaginary quadratic orders.

Proposition 5.3. *For $R = \mathbb{Z}[C\theta]$, there is one and only one norm satisfying* (N1)–(N5).

P r o o f. Let $x = x_0 + x_1 C\theta \in \mathbb{Z}[C\theta]$ and let us take the number $\overline{x} = x_0 + \varepsilon x_1 C - x_1 C\theta$. Then

$$x\overline{x} = x_0^2 + \varepsilon x_0 x_1 C + \frac{\varepsilon(1+3d) - 4d}{4} x_1^2 C^2 \in \mathbb{Z}$$

and thus

$$|x||\overline{x}| = |x\overline{x}| = x_0^2 + \varepsilon x_0 x_1 C + \frac{\varepsilon(1+3d) - 4d}{4} x_1^2 C^2.$$

Now we would like to show $|x| = |\overline{x}|$. Suppose that there exists some $x \neq 0$ (we trivially have $|0| = |\overline{0}|$) such that $|x| \neq |\overline{x}|$, without loss of a generality $|x| > |\overline{x}|$. It means that $|x| = q\sqrt{|x\overline{x}|}$, $q > 1$, since $|x||\overline{x}| = q\frac{1}{q}\sqrt{|x\overline{x}|}\sqrt{|x\overline{x}|}$.

For every $n \in \mathbb{N}$ we can calculate the n-th power of x, denote it by $y = y_0 + y_1 C\theta$. Using (N2), (N3), $\left|1 - \frac{1}{2}\varepsilon\right| = \left|\frac{1}{2}\sqrt{4 - 3\varepsilon}\right|$ for both cases and $|y_1 C\sqrt{d}| = |y_1 C\sqrt{-d}|$

$$\begin{aligned}\big(\text{noting that}\quad |y_1 C\sqrt{d}| &= \sqrt{|y_1 C\sqrt{d}||y_1 C\sqrt{d}|} = \sqrt{|y_1^2 C^2 d|} = \sqrt{|y_1^2 C^2(-d)||-1|} \\ &= \sqrt{|y_1^2 C^2(-d)|} = \sqrt{|y_1 C\sqrt{-d}||y_1 C\sqrt{-d}|} = |y_1 C\sqrt{-d}|\big)\end{aligned}$$

we obtain

$$\begin{aligned}|y| = |y_0 + y_1 C\theta| &= \Big|y_0 + \frac{\varepsilon}{2} y_1 C + \Big(1 - \frac{\varepsilon}{2}\Big) y_1 C\sqrt{d}\Big| \\ &\leqslant \Big|y_0 + \frac{\varepsilon}{2} y_1 C\Big| + \Big|\Big(1 - \frac{\varepsilon}{2}\Big)\Big|\big|y_1 C\sqrt{d}\big| \\ &= \Big|y_0 + \frac{\varepsilon}{2} y_1 C\Big| + \Big|\frac{1}{2}\sqrt{4 - 3\varepsilon}\,\Big|\big|y_1 C\sqrt{-d}\big| = \Big|y_0 + \frac{\varepsilon}{2} y_1 C\Big| + \Big|\frac{1}{2}\sqrt{4 - 3\varepsilon}\, y_1 C\sqrt{-d}\Big|.\end{aligned}$$

On the other hand,

$$\begin{aligned}|y| = |x^n| = |g^n\sqrt{|x\overline{x}|}^n| &= q^n\sqrt{|x^n\overline{x}^n|} = q^n\sqrt{|y\overline{y}|} = \\ &= q^n\sqrt{\Big|y_0^2 + \varepsilon y_0 y_1 C + \frac{\varepsilon(1+3d) - 4d}{4} y_1^2 C^2\Big|} = \\ &= q^n\sqrt{\Big|y_0^2 + \varepsilon y_0 y_1 C + \frac{\varepsilon^2}{4} y_1^2 C^2 + \frac{1}{2}(4 - 3\varepsilon)(-d y_1^2 C^2)\Big|},\end{aligned}$$

because $\varepsilon = \varepsilon^2$ for both cases and finally

$$|y| = q^n \sqrt{\Big(y_0 + \frac{\varepsilon}{2} y_1 C\Big)^2 + \Big(\frac{1}{2}\sqrt{4-3\varepsilon}\, y_1 C\sqrt{-d}\Big)^2}.$$

Altogether we have

$$q^n \sqrt{\Big(y_0 + \frac{\varepsilon}{2} y_1 C\Big)^2 + \Big(\frac{1}{2}\sqrt{4-3\varepsilon}\, y_1 C\sqrt{-d}\Big)^2} \leqslant \Big|y_0 + \frac{\varepsilon}{2} y_1 C\Big| + \Big|\frac{1}{2}\sqrt{4-3\varepsilon}\, y_1 C\sqrt{-d}\Big|$$

or

$$q^n \leqslant \frac{\big|y_0 + \frac{1}{2}\varepsilon y_1 C\big| + \big|\frac{1}{2}\sqrt{4-3\varepsilon}\, y_1 C\sqrt{-d}\big|}{\sqrt{\big(y_0 + \frac{1}{2}\varepsilon y_1 C\big)^2 + \big(\frac{1}{2}\sqrt{4-3\varepsilon}\, y_1 C\sqrt{-d}\big)^2}},$$

where $\big(y_0 + \frac{\varepsilon}{2} y_1 C\big), \big(\frac{1}{2}\sqrt{4-3\varepsilon} y_1 C\sqrt{-d}\big) \in \mathbb{R}^2 \setminus \{(0,0)\}$.

But the function $D(s,t) = (|s|+|t|)/\sqrt{s^2+t^2}$ is bounded by $\sqrt{2}$ and because $q > 1$, there exists $n_0 \in \mathbb{N}$ such that

$$\forall\, n \geqslant n_0, \quad q^n > \sqrt{2} \geqslant \frac{\big|y_0 + \frac{1}{2}\varepsilon y_1 C\big| + \big|\frac{1}{2}\sqrt{4-3\varepsilon}\, y_1 C\sqrt{-d}\big|}{\sqrt{\big(y_0 + \frac{1}{2}\varepsilon y_1 C\big)^2 + \big(\frac{1}{2}\sqrt{4-3\varepsilon}\, y_1 C\sqrt{-d}\big)^2}},$$

which contradicts our previous assumption.

So we have $|x| = |\overline{x}| = \sqrt{|x\overline{x}|}$, where $x\overline{x} \in \mathbb{Z}$, which means $|x\overline{x}|$ is given uniquely by Proposition 5.1 and we have one and only one norm satisfying (N1)–(N5) for $R = \mathbb{Z}[C\theta]$. □

5.3. Quaternion orders. Now we would like to extend the proposition about uniqueness of the norm to the quaternion algebra. First, we will formulate some lemmas. We denote by $\mathcal{J} = \big\{x_0 + x_1 i + x_2 j + x_3 k \in \big(\frac{a,b}{\mathbb{Q}}\big) \colon\ 0 \leqslant x_n < 1,\ n = 0,1,2,3\big\}$ the left-closed and right-open unit quaternion interval.

Lemma 5.4. *Let $\mathcal{O}$ be an order of $\big(\frac{a,b}{\mathbb{Q}}\big)$ and $x = x_0 + x_1 i + x_2 j + x_3 k \in \mathcal{J} \cap \mathcal{O}$. Then $x_0 \in \{0, 1/2\}$.*

P r o o f. Let $\hat{x} \in \mathcal{J}$. Then:

(1) For $\hat{x}_0 = 0$, the lemma is trivially satisfied.

(2) For $\hat{x}_{1,2,3} = 0$ and $x_0 \neq 0$ we easily get contradiction with the definition of a $\mathbb{Z}$-lattice.

(3) For $\hat{x} \in \mathcal{J}_1 = \{x \in \mathcal{J} \colon\ x_{0,1} \neq 0\}$, because $\hat{x} \in \mathcal{J}_1$, $|\mathcal{J}_1| \geqslant 1$ and because of $\mathcal{J}_1$ being a $\mathbb{Z}$-lattice, we have $|\mathcal{J}_1| < \infty$, so there exists $x_{1\min} \in (0,1) \cap \mathbb{Q}$ such that exists $\tilde{x} \in \mathcal{J}_1$, $\tilde{x}_1 = x_{1\min}$ and for all $x \in \mathcal{J}_1$, $x_1 \geqslant \tilde{x}_1 = x_{1\min}$. Now suppose $\hat{x}_1 = \tilde{x}_1$ and:

(a) $\hat{x}_0 \in (0, 1/2)$. It is not difficult to see that, there exists $K \in \mathcal{L}(1,1,1,1)$ such that $\hat{\hat{x}} = \hat{x}^2 + K$ lies in $\mathcal{J}_1$. But $\hat{\hat{x}}_1 = 2\hat{x}_0\hat{x}_1 < \tilde{x}_1$, is a contradiction.

(b) $\hat{x}_0 \in (1/2, 1)$. Put $\hat{\hat{x}} = 1 - \hat{x}$; as in the previous paragraph one can see that, there exists $K \in \mathcal{L}(1,1,1,1)$ such that $\hat{\hat{\hat{x}}} = 1 - \hat{\hat{x}}^2 + K$ lies in $\mathcal{J}_1$. But also one can compute $\hat{\hat{\hat{x}}}_1 < \tilde{x}_1$.

Altogether, $\hat{x}_1 = \tilde{x}_1$ implies $\hat{x}_0 = 1/2$.

On the other hand, suppose $\hat{x}_1 > \tilde{x}_1$, it means $\hat{x}_1 = n\tilde{x}_1 + r$, $n \in \mathbb{N}$, $r \in \langle 0, \hat{x}_1) \cap \mathbb{Q}$.

(a′) $r = 0$, compute $\hat{\hat{x}} = \hat{x} - n\tilde{x}$. $\hat{\hat{x}}_0 = \hat{x}_0 - n/2$ and for $\hat{x}_0 \neq 1/2$, $\hat{\hat{x}}_0 - \hat{x}_0 = n/2 \Rightarrow 2\hat{\hat{x}}_0 \notin \mathbb{Z}$, so there exists $K \in \mathcal{L}(1,1,1,1)$ such that $\hat{\hat{\hat{x}}} = \hat{\hat{x}} + K$ lies in $\mathcal{J}$ and $\hat{\hat{\hat{x}}}_1 = 0$, for which a contradiction is shown in paragraphs (4), (5) of this proof. So $r = 0 \Rightarrow \hat{x}_0 = 1/2$.

(b′) $r \neq 0$, put $\hat{\hat{x}} = \hat{x} - n\tilde{x} + K$ for a suitable $K \in \mathcal{L}(1,1,1,1)$, which yields a contradiction $\hat{\hat{x}}_1 = r < \tilde{x}_1$.

(4) $\hat{x} \in \mathcal{J}_2 = \{x \in \mathcal{J} \colon\ x_{0,2} \neq 0,\ x_1 = 0\}$. We find $x_{2\min} \in (0,1) \cap \mathbb{Q}$ such that exists $\tilde{x} \in \mathcal{J}_2$, $\tilde{x}_2 = x_{2\min}$ and for all $x \in \mathcal{J}_2$, $x_2 \geqslant \tilde{x}_2 = x_{2\min}$. Then we use totally the same technique as in the paragraph (3).

(5) $\hat{x} \in \mathcal{J}_3 = \{x \in \mathcal{J} \colon\ x_{0,3} \neq 0,\ x_{1,2} = 0\}$. We find $x_{3\min} \in (0,1) \cap \mathbb{Q}$ such that exists $\tilde{x} \in \mathcal{J}_3$, $\tilde{x}_3 = x_{3\min}$ and for all $x \in \mathcal{J}_3$, $x_3 \geqslant \tilde{x}_3 = x_{3\min}$ and repeat our ideas once more. Only if there is some $\hat{\hat{x}}$ such that $\hat{\hat{x}}_3 = 0$ ($\hat{\hat{x}}_1, \hat{\hat{x}}_2 = 0$ holds now), we find the final contradiction as in paragraph (2). □

Corollary 5.5. *Let $\mathcal{O}$ be an order of $\left(\frac{a,b}{\mathbb{Q}}\right)$. Then for all $x = x_0 + x_1 i + x_2 j + x_3 k \in \mathcal{O}$, $2x_0 \in \mathbb{Z}$.*

Proof. $\mathcal{L}(1,1,1,1) \subset \mathcal{O}$ and for all $x \in \mathcal{O}$ there exists $K \in \mathcal{L}(1,1,1,1)$ such that $x + K \in \mathcal{J} = \{x \in \mathcal{O} \colon\ x_n \in \langle 0,1) \cap \mathbb{Q},\ n = 0,1,2,3\}$ □

Proposition 5.6. *Let $\mathcal{O}$ be an order of $\left(\frac{a,b}{\mathbb{Q}}\right)$. Then by* (N1)–(N5) *the norm is given uniquely.*

Proof. Let $x \in \mathcal{O}$ be arbitrary. Then, because (by Corollary 5.5) $2x_0 \in \mathbb{Z} \subset \mathcal{O}$, we can put $\overline{x} = 2x_0 - x$. So $x\overline{x} = 2x_0 \in \mathbb{Z}$. Finally $|x| = |\overline{x}| = \sqrt{|x||\overline{x}|}$ can be proved using the same technique as in the proof of Proposition 5.3 and boundedness of function $D(s,t,u,v) = (|s| + |t| + |u| + |v|)/\sqrt{s^2 + t^2 + u^2 + v^2} \geqslant 4$, which with $|x||\overline{x}| = |x\overline{x}| \in \mathbb{Z}$ completes the proof. □

Lemma 5.7. *Any order $\mathcal{O} = \mathcal{L}(1, r_1, r_2, r_3)$ with basis $\mathbb{B} = \{1, r_1 i, r_2 j, r_3 k\}$ can be discretely normed if and only if inequalities $-r_1^2 a \geqslant 4$, $-r_2^2 b \geqslant 4$, $r_3^2 ab \geqslant 4$ are satisfied.*

P r o o f. $\Longrightarrow$: Suppose without loss of generality that $-r_1^2 a < 4$, then

(1) $|r_1 i| > 1$, thus $1 < |r_1 i| = \sqrt{(r_1 i)(-r_1 i)} = \sqrt{-r_1^2 a} < 2$ contradicts (N5);

(2) $|r_1 i| = 1$, thus $r_1 = 1$, $1 = 1^2 = |i|^2 = -i^2$ and for $1 + i \in \mathcal{O}$, $|1 + i| = \sqrt{1 - i^2} = \sqrt{2}$ also contradicts (N5).

$\Longleftarrow$: Let x, y be any elements of $\mathcal{O}$.

(N1) The inequality $a, b < 0$ is an easy consequence of $-r_1^2 a, -r_2^2 b, r_3^2 ab \geqslant 4$ as

$$0 = |x| = \sqrt{x_0^2 - x_1^2 a - x_2^2 b + x_3^2 ab} \overset{a,b<0}{\Longrightarrow} x_n = 0 \ \forall\, n \Rightarrow x = 0.$$

(N2) By straightforward calculation

$$\begin{aligned} |x + y| \leqslant |x| + |y| \Longleftrightarrow \sqrt{(x_0 + y_0)^2 - (x_1 + y_1)^2 a - (x_2 + y_2)^2 b + (x_3 + y_3)^2 ab} \\ \leqslant \sqrt{x_0^2 - x_1^2 a - x_2^2 b + x_3^2 ab} + \sqrt{y_0^2 - y_1^2 a - y_2^2 b + y_3^2 ab}. \end{aligned}$$

(N3) Also by straightforward calculation

$$|x_0 + x_1 i + x_2 j + x_3 k||y_0 + y_1 i + y_2 j + y_3 k| = |(x_0 + x_1 i + x_2 j + x_3 k)(y_0 + y_1 i + y_2 j + y_3 k)|.$$

(N4) For $x \neq 0$ we have $|x| \geqslant 1$, because $|x| < 1$ implies that all x_n have absolute value smaller than 1, but only $0 \in \mathcal{O}$ has this property. Further $1 = |x| = \sqrt{x\overline{x}} \Longleftrightarrow x\overline{x} = 1$, hence $|x| = 1 \Longleftrightarrow x \in \mathrm{U}(\mathcal{O})$.

(N5) (a) Suppose at least one of x_1, x_2, x_3 is nonzero. Without loss of generality $x_1 \neq 0$, so $x_1^2 \geqslant 1$. Then

$$x\overline{x} = x_0^2 - x_1^2 r_1^2 a - x_2^2 r_2^2 b + x_3^2 r_3^2 ab \geqslant -x_1^2 r_1^2 a \geqslant -r_1^2 a \geqslant 4,$$

whence $|x| = \sqrt{x\overline{x}} \geqslant 2$.

(b) All of x_1, x_2, x_3 are zeros, so $x = x_0$. Then $|x| = |x_0|$, where $x_0 \in \mathbb{Z}$.

Altogether, the norm is well defined. □

References

[1] *P. M. Cohn*: On the structure of the GL_2 of a ring. Publ. Math., Inst. Hautes Études Sci. Publ. Math. *30* (1966), 5–53.

[2] *D. G. James*: Quaternion algebras, arithmetic Kleinian groups and **Z**-lattices. Pac. J. Math. *203* (2002), 395–413.

[3] *K. Kato, N. Kurokawa, T. Saito*: Number Theory I. Fermat's Dream. Translations of Mathematical Monographs. Iwanami Series in Modern Mathematics 186, AMS, Providence, 2000.

[4] *M. Kureš, L. Skula*: Reduction of matrices over orders of imaginary quadratic fields. Linear Algebra Appl. *435* (2011), 1903–1919.

[5] *C. Maclachlan, A. W. Reid*: The Arithmetic of Hyperbolic 3-Manifolds. Graduate Texts in Mathematics 219, Springer, New York, 2003.
[6] *J. Voight*: Identifying the matrix ring: algorithms for quaternion algebras and quadratic forms. Quadratic and Higher Degree Forms (K. Alladi et al., eds.). Developments in Mathematics 31, Springer, New York, 2013, pp. 255–298.

Authors' addresses: *Jan Horníček*, *Miroslav Kureš*, Institute of Mathematics, Brno University of Technology, Technická 2, 616 69 Brno, Czech Republic, e-mail: `hhornicek@seznam.cz`, `kures@fme.vutbr.cz`; *Lenka Macálková*, Global Change Research Centre Czech Academy of Sciences, v. v. i., Bělidla 4a, 603 00 Brno, Czech Republic, and Department of Mathematics and Statistics, Faculty of Science, Masaryk University, Kotlářská 2, 611 37 Brno, Czech Republic, e-mail: `macalkoval@gmail.com`.