Contemporary Mathematics

Voronoï's reduction theory of GL_n over a totally real number field

Takao Watanabe, Syouji Yano and Takuma Hayashi

Abstract. Let k be a totally real algebraic number field of degree r and o_k the ring of integers of k. In this paper, we study Voronoï's reduction theory and algorithm for $GL_n(\mathsf{k} \otimes_{\mathbf{Q}} \mathbf{R})$ with respect to an action of $GL(\Lambda_0)$, where $GL(\Lambda_0)$ is the stabilizer in $GL_n(\mathsf{k})$ of a projective o_k-module Λ_0 in k^n of rank n.

Introduction

Let k be a totally real algebraic number field of degree r and o_k the ring of integers of k. We write $\mathsf{k}_\mathbf{R}$ for $\mathsf{k} \otimes_{\mathbf{Q}} \mathbf{R}$. In this paper, we study Voronoï's reduction theory and algorithm for $GL_n(\mathsf{k}_\mathbf{R})$ with respect to an action of $GL(\Lambda_0)$, where $GL(\Lambda_0)$ is the stabilizer in $GL_n(\mathsf{k})$ of a projective o_k-module Λ_0 in k^n of rank n.

Voronoï's reduction theory was originally investigated by Voronoï [**16**] and was extended by Köcher [**5**] to self-dual homogeneous cones. Gunnells [**2**], Sikirić, Schürmann and Vallentin [**13**] also studied Voronoï's reduction theory. To construct a fundamental domain via Voronoï's reduction theory, we need to compute perfect forms. This is made by Voronoï algorithm. Ong [**10**], Gunnells [**2**], Opgenorth [**11**] and Martinet [**7**, §13] studied some generalizations of Voronoï algorithm. Explicit computations of perfect forms over real quadratic fields were made by Ong [**10**], Leibak [**6**], Gunnells and Yasaki [**3**]. Most of these previous works restrict us to the case that Λ_0 is a free o_k-module. We systematically study Λ_0-perfect forms and Voronoï algorithm for any projective o_k-module Λ_0 by using Ryshkov polyhedra. Some results in this paper give refinements of Köcher's theory for the case of $GL_n(\mathsf{k}_\mathbf{R})/GL_n(\mathsf{o}_\mathsf{k})$. Moreover, as we will see in §5, observations of Ryshkov polyhedra for real quadratic fields suggest some interesting problems.

To explain results in this paper, let $H_n(\mathsf{k}_\mathbf{R})$ be the space of all $n \times n$ symmetric matrices with entries in $\mathsf{k}_\mathbf{R}$, $P_n(\mathsf{k}_\mathbf{R}) = \{{}^t gg \mid g \in GL_n(\mathsf{k}_\mathbf{R})\}$ an open cone in $H_n(\mathsf{k}_\mathbf{R})$ and $P_n^-(\mathsf{k}_\mathbf{R})$ a closure of $P_n(\mathsf{k}_\mathbf{R})$ in $H_n(\mathsf{k}_\mathbf{R})$. The group $GL_n(\mathsf{k}_\mathbf{R})$ acts on both $P_n^-(\mathsf{k}_\mathbf{R})$ and $P_n(\mathsf{k}_\mathbf{R})$ by $(a, g) \mapsto a \cdot g = {}^t gag$, where $a \in P_n^-(\mathsf{k}_\mathbf{R})$ or $a \in P_n(\mathsf{k}_\mathbf{R})$ and $g \in GL_n(\mathsf{k}_\mathbf{R})$. The rational closure Ω_k of $P_n(\mathsf{k}_\mathbf{R})$ is given by the cone generated

2010 *Mathematics Subject Classification.* 11H55.

Key words and phrases. Hermite constant, Polyhedral reduction, Ryshkov polyhedron, Shintani's unit theorem, Voronoi algorithm.

by $\{x^t x \mid x \in \Lambda_0 \setminus \{0\}\}$ in $H_n(\mathsf{k}_{\mathbf{R}})$. We have $P_n(\mathsf{k}_{\mathbf{R}}) \subsetneqq \Omega_{\mathsf{k}} \subsetneqq P_n^-(\mathsf{k}_{\mathbf{R}})$ and Ω_{k} is stabilized by the action of the discrete subgroup $GL(\Lambda_0)^* = \{{}^t\gamma \mid \gamma \in GL(\Lambda_0)\}$. What we want to do is to construct a fundamental domain of $\Omega_{\mathsf{k}}/GL(\Lambda_0)^*$ from perfect domains. To do this, we need a precise study of Λ_0-perfect forms in $P_n(\mathsf{k}_{\mathbf{R}})$.

As an $\mathbf{R}$ vector space, $H_n(\mathsf{k}_{\mathbf{R}})$ is equipped with an inner product defined by

$$(a, b) = \mathrm{Tr}_{\mathsf{k}_{\mathbf{R}}/\mathbf{R}}(\mathrm{Tr}(ab))$$

for $a, b \in H_n(\mathsf{k}_{\mathbf{R}})$. We define Λ_0-minimum function $\mathsf{m}_{\Lambda_0} : P_n^-(\mathsf{k}_{\mathbf{R}}) \longrightarrow \mathbf{R}_{\geq 0}$ by

$$\mathsf{m}_{\Lambda_0}(a) = \inf_{0 \neq x \in \Lambda_0} (a, x^t x)\,.$$

If $a \in P_n(\mathsf{k}_{\mathbf{R}})$, then the set of shortest vectors

$$S_{\Lambda_0}(a) = \{x \in \Lambda_0 \mid \mathsf{m}_{\Lambda_0}(a) = (a, x^t x)\}$$

is a finite set. We call an element $a \in P_n(\mathsf{k}_{\mathbf{R}})$ is Λ_0-perfect if $\{x^t x \mid x \in S_{\Lambda_0}(a)\}$ spans $H_n(\mathsf{k}_{\mathbf{R}})$ as an $\mathbf{R}$-vector space. Okuda and Yano [**9**] proved that Λ_0-perfect forms are k-rational, i.e., if $a \in P_n(\mathsf{k}_{\mathbf{R}})$ is Λ_0-perfect with $\mathsf{m}_{\Lambda_0}(a) = 1$, then $a \in GL_n(\mathsf{k})$, and that the number of similar equivalent classes of Λ_0-perfect forms is finite. For further study of Λ_0-perfect forms, we introduce an analog of Ryshkov polyhedron, which is defined by

$$K_1(\mathsf{m}_{\Lambda_0}) = \{a \in P_n^-(\mathsf{k}_{\mathbf{R}}) \mid \mathsf{m}_{\Lambda_0}(a) \geq 1\}\,.$$

The domain $K_1(\mathsf{m}_{\Lambda_0})$ is a closed convex set in $P_n(\mathsf{k}_{\mathbf{R}})$. In §2 and §3, we will prove the following:

THEOREM. *The domain $K_1(\mathsf{m}_{\Lambda_0})$ is a locally finite polyhedron. If we denote by $\partial^0 K_1(\mathsf{m}_{\Lambda_0})$ the set of all vertices of $K_1(\mathsf{m}_{\Lambda_0})$, then $\partial^0 K_1(\mathsf{m}_{\Lambda_0})$ coincides with the set of all Λ_0-perfect forms a with $\mathsf{m}_{\Lambda_0}(a) = 1$. Furthermore, for any two vertices $a, a' \in \partial^0 K_1(\mathsf{m}_{\Lambda_0})$, there exists a finite sequence of vertices $\{a_i\}_{i=0}^k \subset \partial^0 K_1(\mathsf{m}_{\Lambda_0})$ such that $a_0 = a, a_k = a'$ and the line segment between a_i and a_{i+1} is a one-dimensional face of $\partial^0 K_1(\mathsf{m}_{\Lambda_0})$ for $i = 0, \cdots, k-1$.*

This result gives Voronoï algorithm for $\partial^0 K_1(\mathsf{m}_{\Lambda_0})$, i.e., the algorithm to determine a complete system $\{b_1, \cdots, b_t\}$ of representatives of $\partial^0 K_1(\mathsf{m}_{\Lambda_0})/GL(\Lambda_0)$.

For each $a \in \partial^0 K_1(\mathsf{m}_{\Lambda_0})$, the closed cone D_a in $P_n^-(\mathsf{k}_{\mathbf{R}})$ generated by $\{x^t x \mid x \in S_{\Lambda_0}(a)\}$ is called a perfect domain. We will prove in §4 the following polyhedral subdivision of Ω_{k}:

$$\Omega_{\mathsf{k}} = \bigcup_{a \in \partial^0 K_1(\mathsf{m}_{\Lambda_0})} D_a\,.$$

If a and a' are distinct elements of $\partial^0 K_1(\mathsf{m}_{\Lambda_0})$, then the intersection of D_a and the interior of $D_{a'}$ is empty. Since $D_{a \cdot \gamma} = D_a \cdot {}^t\gamma$ holds for any $a \in \partial^0 K_1(m_{\Lambda_0})$ and $\gamma \in GL(\Lambda_0)$, this subdivision yields the following.

THEOREM. *Let $\{b_1, \cdots, b_t\}$ be the same as above and Γ_i the stabilizer of b_i in $GL(\Lambda_0)$ for $i = 1, \cdots, t$. Then the domain*

$$\bigcup_{i=1}^{t} D_{b_i}/\Gamma_i^*$$

is a fundamental domain of $\Omega_{\mathsf{k}}/GL(\Lambda_0)^*$, where $\Gamma_i^* = \{{}^t\gamma \mid \gamma \in \Gamma_i\}$.

If the dimension n is equal to one and $\Lambda_0 = \mathsf{o}_\mathsf{k}$, then this theorem may be regarded as a precise form of Shintani's unit theorem ([**8**, (9.2)], [**15**, Proposition 4]) for the square E_k^2 of the unit group $E_\mathsf{k} = GL(\mathsf{o}_\mathsf{k})$. In this case, $\Omega_\mathsf{k}\backslash\{0\}$ equals the quadrant $\mathsf{k}_\mathbf{R}^+ = \mathbf{R}^r_{>0}$ and E_k^2 acts on $\mathsf{k}_\mathbf{R}^+$ by scalar multiplications. Since $\Gamma_i = \{\pm 1\}$ (and hence $\Gamma_i^2 = \{1\}$), we obtain a cone decomposition of $\mathsf{k}_\mathbf{R}^+/GL(\mathsf{o}_\mathsf{k}) = E_\mathsf{k}^2\backslash\mathsf{k}_\mathbf{R}^+$ as

$$E_\mathsf{k}^2\backslash\mathsf{k}_\mathbf{R}^+ = \bigcup_{i=1}^{t} D_{b_i}^* ,$$

where $D_{b_i}^* = D_{b_i} \setminus \{0\}$. If k is a real quadratic field, then $K_1(\mathsf{m}_{\mathsf{o}_\mathsf{k}})$ is a domain in $\mathbf{R}^2_{>0}$ with infinite vertices. In §5, several examples of $K_1(\mathsf{m}_{\mathsf{o}_\mathsf{k}})$ are given. We will see that there are many real quadratic fields such that the number t of elements of $E_\mathsf{k}^2\backslash\partial^0 K_1(\mathsf{m}_{\mathsf{o}_\mathsf{k}})$ is equal to one.

Notation. For a given ring R, the set of all $m \times n$ matrices with entries in R is denoted by $M_{m,n}(R)$. We write $M_n(R)$ for $M_{n,n}(R)$ and R^n for $M_{n,1}(R)$. The transpose of a given matrix $a \in M_{m,n}(R)$ is denoted by ${}^t a$. If $R = \mathbf{R}$ (resp. $R = \mathbf{C}$), then the set of symmetric matrices in $M_n(\mathbf{R})$ (resp. Hermitian matrices in $M_n(\mathbf{C})$) is denoted by $H_n(\mathbf{R})$ (resp. $H_n(\mathbf{C})$). For a constant $c \in \mathbf{R}$, $\mathbf{R}_{>c}$ and $\mathbf{R}_{\geq c}$ stand for the open interval $(c, +\infty)$ and the closed interval $[c, +\infty)$.

In this paper, k denotes an algebraic number field of degree r and o_k the ring of integers of k. Up to §3, k is an arbitrary number field. From §4, k is restricted to a totally real number field. The set of all infinite (resp. real and imaginary) places of k is denoted by p_∞ (resp. p_1 and p_2). Let k_σ be the completion of k at $\sigma \in \mathsf{p}_\infty$, i.e., $\mathsf{k}_\sigma = \mathbf{R}$ if $\sigma \in \mathsf{p}_1$ and $\mathsf{k}_\sigma = \mathbf{C}$ if $\sigma \in \mathsf{p}_2$. We use the étale $\mathbf{R}$-algebra $\mathsf{k}_\mathbf{R} = \mathsf{k} \otimes_\mathbf{Q} \mathbf{R}$, which is identified with $\prod_{\sigma\in\mathsf{p}_\infty} \mathsf{k}_\sigma$. As usual, k is embedded in $\mathsf{k}_\mathbf{R}$ by $\lambda \longrightarrow (\sigma(\lambda))_{\sigma\in\mathsf{p}_\infty}$. For $\alpha = (\alpha_\sigma) \in \mathsf{k}_\mathbf{R}$, the conjugate $\overline{\alpha}$ of α stands for $(\overline{\alpha}_\sigma)$, where $\overline{\alpha}_\sigma$ denotes the complex conjugate of $\alpha_\sigma \in \mathsf{k}_\sigma$. The trace of $\mathsf{k}_\mathbf{R}$ over $\mathbf{R}$ is defined by

$$\mathrm{Tr}_{\mathsf{k}_\mathbf{R}}(\alpha) = \sum_{\sigma\in\mathsf{p}_\infty} \mathrm{Tr}_{\mathsf{k}_\sigma/\mathbf{R}}(\alpha_\sigma)$$

for $\alpha \in \mathsf{k}_\mathbf{R}$.

1. Preliminaries

We recall results of [**9**]. Let $\mathsf{k}_\mathbf{R}^n = \mathsf{k}^n \otimes_\mathbf{Q} \mathbf{R}$. An element of $\mathsf{k}_\mathbf{R}^n$ is denoted as a column vector with entries in $\mathsf{k}_\mathbf{R}$. For $x = {}^t(\alpha_1, \cdots, \alpha_n) \in \mathsf{k}_\mathbf{R}^n$ with components $\alpha_i \in \mathsf{k}_\mathbf{R}$, $\overline{x}$ and x^* stand for ${}^t(\overline{\alpha}_1, \cdots, \overline{\alpha}_n)$ and ${}^t\overline{x}$, respectively. As an $\mathbf{R}$ vector space, $\mathsf{k}_\mathbf{R}^n$ is equipped with an inner product $\langle\ ,\ \rangle$ defined by

$$\langle x, y\rangle = \mathrm{Tr}_{\mathsf{k}_\mathbf{R}}(x^* y)$$

for $x, y \in \mathsf{k}_\mathbf{R}^n$. We set $Q(x) = \langle x, x\rangle$. For every $a \in M_n(\mathsf{k}_\mathbf{R})$, a^* stands for the adjoint matrix with respect to the inner product $\langle\ ,\ \rangle$.

The group of $\mathsf{k}_\mathbf{R}$-linear automorphisms of $\mathsf{k}_\mathbf{R}^n$ is denoted by $GL_n(\mathsf{k}_\mathbf{R})$. The group of isometries with respect to $\langle\ ,\ \rangle$ is denoted by $O_n(\mathsf{k}_\mathbf{R})$, i.e.,

$$O_n(\mathsf{k}_\mathbf{R}) = \{g \in GL_n(\mathsf{k}_\mathbf{R}) \mid \langle gx, gy\rangle = \langle x, y\rangle \text{ for all } x, y \in \mathsf{k}_\mathbf{R}^n\},$$

and the set of self-adjoint matrices in $M_n(\mathsf{k}_\mathbf{R})$ is denoted by $H_n(\mathsf{k}_\mathbf{R})$, i.e.,

$$H_n(\mathsf{k}_\mathbf{R}) = \{a \in M_n(\mathsf{k}_\mathbf{R}) \mid \langle ax, y\rangle = \langle x, ay\rangle \text{ for all } x, y \in \mathsf{k}_\mathbf{R}^n\}.$$

According to the identification $\mathsf{k}_{\mathbf{R}} \simeq \prod_{\sigma\in\mathsf{p}_\infty} \mathsf{k}_\sigma$, the group $GL_n(\mathsf{k}_{\mathbf{R}})$ and the space $H_n(\mathsf{k}_{\mathbf{R}})$ are identified with $\prod_{\sigma\in\mathsf{p}_\infty} GL_n(\mathsf{k}_\sigma)$ and $\prod_{\sigma\in\mathsf{p}_\infty} H_n(\mathsf{k}_\sigma)$, respectively.

A self-adjoint matrix $a \in H_n(\mathsf{k}_{\mathbf{R}})$ is said to be positive definite (resp. semi-positive definite) if $\langle ax, x\rangle > 0$ (resp. $\langle ax, x\rangle \geq 0$) for all $x \in \mathsf{k}_{\mathbf{R}}^n\backslash\{0\}$. We denote the set of positive definite (resp. semi-positive definite) self-adjoint matrices in $H_n(\mathsf{k}_{\mathbf{R}})$ by $P_n(\mathsf{k}_{\mathbf{R}})$ (resp. $P_n^-(\mathsf{k}_{\mathbf{R}})$). The trace TR on $H_n(\mathsf{k}_{\mathbf{R}})$ is defined to be

$$\mathrm{TR}(a) = \mathrm{Tr}_{\mathsf{k}_{\mathbf{R}}}((\mathrm{Tr}(a_\sigma))_{\sigma\in\mathsf{p}_\infty})$$

for $a \in H_n(\mathsf{k}_{\mathbf{R}})$. This defines an inner product $(\ ,\ )$ on $H_n(\mathsf{k}_{\mathbf{R}})$ by $(a, b) = \mathrm{TR}(ab)$.

An o_k-submodule Λ in $\mathsf{k}_{\mathbf{R}}^n$ is called an o_k-lattice if Λ is discrete and $\Lambda\otimes_{\mathbf{Z}}\mathbf{R} = \mathsf{k}_{\mathbf{R}}^n$. The set of all o_k-lattices in $\mathsf{k}_{\mathbf{R}}^n$ is denoted by $\mathcal{L}$. For any o_k-lattice Λ, there exists $g \in GL_n(\mathsf{k}_{\mathbf{R}})$ such that $g^{-1}\Lambda$ is a projective o_k-module in k^n. By Steinitz's theorem, any projective o_k-module in k^n is isomorphic to $\mathsf{o}_\mathsf{k}^{n-1} \oplus \mathsf{q}$ for some integral ideal q in o_k. We choose a complete system $\{\mathsf{q}_1 = \mathsf{o}_\mathsf{k}, \mathsf{q}_2, \cdots, \mathsf{q}_h\}$ of representatives of the ideal class group of k. Let $\Lambda_i = \mathsf{o}_\mathsf{k}^{n-1} \oplus \mathsf{q}_i$ for $1 \leq i \leq h$. Then the set of all o_k-lattices of $\mathsf{k}_{\mathbf{R}}^n$ is given by the disjoint union

$$\mathcal{L} = \coprod_{i=1}^{h} \mathcal{L}_i,$$

where $\mathcal{L}_i$ is the $GL_n(\mathsf{k}_{\mathbf{R}})$-orbit of Λ_i. Each $\mathcal{L}_i$ is identified with $GL_n(\mathsf{k}_{\mathbf{R}})/GL(\Lambda_i)$, where $GL(\Lambda_i)$ denotes the stabilizer of Λ_i in $GL_n(\mathsf{k}_{\mathbf{R}})$. Two o_k-lattices Λ and Λ' are said to be isometry if there exists $T \in O_n(\mathsf{k}_{\mathbf{R}})$ such that $\Lambda = T\Lambda'$. For every $\Lambda \in \mathcal{L}$, the minimum $Q(\Lambda)$, the set of shortest vectors $S(\Lambda)$ and the determinant $\det(\Lambda)$ are defined as follows:

$$Q(\Lambda) = \min_{x\in\Lambda\backslash\{0\}} \langle x, x\rangle, \qquad S(\Lambda) = \{x \in \Lambda \mid Q(x) = Q(\Lambda)\}$$

and

$$\det(\Lambda) = \left(\frac{\omega(\mathsf{k}_{\mathbf{R}}^n/\Lambda)}{\omega(\mathsf{k}_{\mathbf{R}}^n/\mathsf{o}_\mathsf{k}^n)}\right)^2,$$

where ω denotes an invariant measure on $\mathsf{k}_{\mathbf{R}}^n$.

Let $H_n(\mathsf{k}_{\mathbf{R}})^*$ denote the dual vector space of $H_n(\mathsf{k}_{\mathbf{R}})$ as an $\mathbf{R}$ vector space. Then we define $\varphi_x \in H_n(\mathsf{k}_{\mathbf{R}})^*$ for each $x \in \mathsf{k}_{\mathbf{R}}^n$ as

$$\varphi_x(a) = \langle ax, x\rangle \text{ for } a \in H_n(\mathsf{k}_{\mathbf{R}}).$$

Definition. *Let $\Lambda \subset \mathsf{k}_{\mathbf{R}}^n$ be an o_k-lattice.*

(1) *Λ is said to be perfect if $\{\varphi_x \mid x \in S(\Lambda)\}$ generates $H_n(\mathsf{k}_{\mathbf{R}})^*$.*
(2) *Λ is said to be eutactic if there exist $\rho_x \in \mathbf{R}_{>0}$ for all $x \in S(\Lambda)$ such that $\mathrm{TR} = \sum_{x\in S(\Lambda)} \rho_x\varphi_x$.*

A perfect o_k-lattice Λ is uniquely determined up to isometry by the set of shortest vectors $S(\Lambda)$ and the minimum $Q(\Lambda)$ ([**9**, Theorem3.1]). It is known that the number of similar isometry classes of perfect o_k-lattices in $\mathsf{k}_{\mathbf{R}}^n$ is finite ([**9**, Theorem 5.1]).

We define the Hermite function $\gamma_\mathsf{k}^\dagger : \mathcal{L} \longrightarrow \mathbf{R}_{>0}$ by

$$\gamma_\mathsf{k}^\dagger(\Lambda) = \frac{Q(\Lambda)}{\det(\Lambda)^{1/nr}}.$$

Since $\gamma_{\mathsf{k}}^{\dagger}$ is invariant by isometry and similarity, we may regard $\gamma_{\mathsf{k}}^{\dagger}$ as a function defined on $\mathbf{R}^{\times}O_n(\mathsf{k}_{\mathbf{R}})\backslash\mathcal{L}$. If $\gamma_{\mathsf{k}}^{\dagger}$ attains a local maximum on $\Lambda \in \mathcal{L}$, then Λ is said to be extreme. The following theorem was proved by Okuda and Yano.

THEOREM 1.1 ([**9**]). *Let $\Lambda \in \mathcal{L}$ be an o_{k}-lattice. Then Λ is extreme if and only if Λ is perfect and eutactic.*

If k is a totally real or a CM-field (i.e. a totally imaginary quadratic extension over a totally real algebraic number field), then we have the following rationality theorem of perfect forms.

THEOREM 1.2 ([**9**]). *Let k be a totally real or a CM-field. If $\Lambda = g\Lambda_i \in \mathcal{L}_i$ for $g \in GL_n(\mathsf{k}_{\mathbf{R}})$ is a perfect o_{k}-lattice with $Q(\Lambda) = 1$, then $g^*g \in M_n(\mathsf{k})$.*

2. Geometric characterizations of perfect forms

In this section, we fix a projective o_{k}-module $\Lambda_0 \subset \mathsf{k}^n$ of rank n. For $a \in P_n^-(\mathsf{k}_{\mathbf{R}})$, we define the minimum $\mathsf{m}_{\Lambda_0}(a)$ and the set of shortest vectors $S_{\Lambda_0}(a)$ by

$$\mathsf{m}_{\Lambda_0}(a) = \inf_{x\in\Lambda_0\backslash\{0\}} \langle ax, x\rangle \quad \text{and} \quad S_{\Lambda_0}(a) = \{x \in \Lambda_0 \mid \mathsf{m}_{\Lambda_0}(a) = \langle ax, x\rangle\}.$$

We write simply m and $S(a)$ for m_{Λ_0} and $S_{\Lambda_0}(a)$, respectively, if no confusions arise.

If $a = g^*g$ is positive definite with $g \in GL_n(\mathsf{k}_{\mathbf{R}})$, then we have

$$\mathsf{m}(a) = \min_{x\in\Lambda_0\backslash\{0\}} \langle gx, gx\rangle = Q(g\Lambda_0)$$

and $S(a) = S(g\Lambda_0)$. A positive definite $a \in P_n(\mathsf{k}_{\mathbf{R}})$ is said to be Λ_0-perfect if $\{\varphi_x \mid x \in S(a)\}$ generates $H_n(\mathsf{k}_{\mathbf{R}})^*$ as an $\mathbf{R}$ vector space. It is clear that $a = g^*g$ is Λ_0-perfect if and only if $g\Lambda_0$ is perfect. From $\varphi_x(a) = (a, xx^*)$ for $x \in S(a)$, it follows that a is Λ_0-perfect if and only if $\{xx^* \mid x \in S(a)\}$ generates $H_n(\mathsf{k}_{\mathbf{R}})$ as an $\mathbf{R}$ vector space.

We define an analog of Ryshkov polyhedron (cf. [**12**], [**14**]) for m by

$$K_1(\mathsf{m}) = \{a \in P_n^-(\mathsf{k}_{\mathbf{R}}) \mid \mathsf{m}(a) \geq 1\}.$$

The boundary of $K_1(\mathsf{m})$ is denoted by $\partial K_1(\mathsf{m})$, i.e.,

$$\partial K_1(\mathsf{m}) = \{a \in P_n^-(\mathsf{k}_{\mathbf{R}}) \mid \mathsf{m}(a) = 1\}.$$

For $x \in \mathsf{k}_{\mathbf{R}}^n \setminus \{0\}$, define the half-space H_x^+ in $H_n(\mathsf{k}_{\mathbf{R}})$ by

$$H_x^+ = \{a \in H_n(\mathsf{k}_{\mathbf{R}}) \mid \langle ax, x\rangle \geq 1\}.$$

Then $K_1(\mathsf{m})$ is the intersection of half-spaces H_x^+, $x \in \Lambda_0 \setminus \{0\}$. In particular, $K_1(\mathsf{m})$ is a closed convex domain in $H_n(\mathsf{k}_{\mathbf{R}})$.

LEMMA 2.1. *$K_1(\mathsf{m})$ is contained in $P_n(\mathsf{k}_{\mathbf{R}})$.*

PROOF. It is enough to show that $\mathsf{m}(a) = 0$ for any $a \in P_n^-(\mathsf{k}_{\mathbf{R}})\backslash P_n(\mathsf{k}_{\mathbf{R}})$. For $a \in P_n^-(\mathsf{k}_{\mathbf{R}})\backslash P_n(\mathsf{k}_{\mathbf{R}})$ and any $\epsilon > 0$, the set $B_{a,\epsilon} = \{x \in \mathsf{k}_{\mathbf{R}}^n \mid \langle ax, x\rangle \leq \epsilon\}$ is a symmetric convex set of infinite volume. By Minkowski's theorem on convex bodies, $B_{a,\epsilon}$ contains a non-zero element in Λ_0. Then we have $\mathsf{m}(a) \leq \epsilon$, and hence $\mathsf{m}(a) = 0$. □

PROPOSITION 2.2. *$K_1(\mathsf{m})$ is a locally finite polyhedron, i.e. the intersection of $K_1(\mathsf{m})$ and any polytope is a polytope.*

Proof. Let $\{v_k\}_{k=1}^{nr}$ be a basis of Λ_0 as a $\mathbf{Z}$-module. By this basis, we identify $\mathsf{k}_{\mathbf{R}}^n$ with $\mathbf{R}^{nr}$. For a sufficiently large constant $\theta > 0$, we set

$$X_\theta = \{a \in H_n(\mathsf{k}_{\mathbf{R}}) \mid \langle av_k, v_k\rangle \leq \theta \text{ for } k = 1, \cdots, nr\},$$
$$T_\theta = \{a \in H_n(\mathsf{k}_{\mathbf{R}}) \mid \mathrm{TR}(a) \leq \theta\}.$$

We show in three steps that both $K_1(\mathsf{m}) \cap X_\theta$ and $K_1(\mathsf{m}) \cap T_\theta$ are polytopes.

Step 1 : We prove that $X_\theta \cap P_n(\mathsf{k}_{\mathbf{R}})$ is bounded in $H_n(\mathsf{k}_{\mathbf{R}})$. For $a \in X_\theta \cap P_n(\mathsf{k}_{\mathbf{R}})$, A denotes the Gram matrix $(\langle av_i, v_j\rangle)_{ij} \in M_{nr}(\mathbf{R})$. Let $\lambda_1, \cdots, \lambda_{nr}$ be eigenvalues of A. Since a is positive definite, $\lambda_i > 0$ for all i. It is sufficient to show that λ_i is bounded for all i. One can take an orthogonal matrix $T = (t_{ij})$ such that ${}^tTAT = \mathrm{diag}(\lambda_1, \cdots, \lambda_{nr})$. Then we have

$$\langle av_k, v_k\rangle = \sum_{i=1}^{nr} \lambda_i t_{ki}^2 \leq \theta,$$

and hence

$$\sum_{k=1}^{nr}\sum_{i=1}^{nr} \lambda_i t_{ki}^2 = \sum_{i=1}^{nr} \lambda_i \leq nr\theta.$$

Step 2 : Let W be a subset consisting of all $x \in \Lambda_0 \backslash \{0\}$ such that $\langle ax, x\rangle = 1$ for some $a \in K_1(\mathsf{m}) \cap X_\theta$. We prove

$$K_1(\mathsf{m}) \cap X_\theta = \bigcap_{x \in W} (H_x^+ \cap X_\theta).$$

It is obvious by the definition of $K_1(\mathsf{m})$ that

$$K_1(\mathsf{m}) \cap X_\theta \subset \bigcap_{x \in W} (H_x^+ \cap X_\theta).$$

We suppose that there exists $a \in \bigcap_{x \in W}(H_x^+ \cap X_\theta)$ such that $a \notin K_1(\mathsf{m}) \cap X_\theta$. Fix an interior point b in $K_1(\mathsf{m}) \cap X_\theta$. Since $a \notin K_1(\mathsf{m})$ and $b \in K_1(\mathsf{m})$, the line segment between a and b crosses the boundary of $K_1(\mathsf{m})$, namely, $c = \lambda a + (1-\lambda)b \in \partial K_1(\mathsf{m})$ for some $\lambda \in (0, 1)$. Then there is an $x_0 \in \Lambda_0$ such that $\langle cx_0, x_0\rangle = 1$. Since X_θ is convex, we have $c \in \partial K_1(\mathsf{m}) \cap X_\theta$. This implies $x_0 \in W$. On the other hand, we have

$$\langle cx_0, x_0\rangle = \lambda\langle ax_0, x_0\rangle + (1 - \lambda)\langle bx_0, x_0\rangle > 1$$

since $a \in H_x^+$ for all $x \in W$ and b is an interior point in $K_1(\mathsf{m})$. This is a contradiction.

Step 3 : We prove that W is a finite set. For $a \in K_1(\mathsf{m}) \cap X_\theta$, put $B_a = \{x \in \mathsf{k}_{\mathbf{R}}^n \mid \langle ax, x\rangle \leq 1\}$. Since the interior of B_a does not contain any non-zero lattice point of Λ_0, we have

$$\omega(B_a) \leq 2^{nr}\omega(\mathsf{k}_{\mathbf{R}}^n/\Lambda_0).$$

Since $\{v_k\}_k$ is a basis of $\mathsf{k}_{\mathbf{R}}^n$ as an $\mathbf{R}$ vector space, each $x \in B_a$ is represented by a linear combination of $\{v_k\}_k$ as

$$x = \sum_{k=1}^{nr} \lambda_k v_k.$$

Fix $x \in B_a$ and k_0 such that $|\lambda_{k_0}| = \max_{1\le k\le nr} |\lambda_k|$. For $1 \le i \le nr$, we define the parallelepiped D_i of dimension $nr-1$ in $\mathsf{k}^n_{\mathbf{R}}$ as

$$D_i = \{\sum_{k\neq i}(\mu_k - \mu'_k)v_k \mid \mu_k, \mu'_k \in \mathbf{R}_{\ge 0},\ \sum_{k\neq i}(\mu_k + \mu'_k) \le \theta^{-1/2}\}.$$

In other words, D_i is the closed convex hull of $\{\pm\theta^{-1/2}v_k \mid k = 1, \cdots, nr,\ k \neq i\}$ in $\mathsf{k}^n_{\mathbf{R}}$. Let V_x be a pyramid in $\mathsf{k}^n_{\mathbf{R}}$ of the base D_{k_0} and the apex x, i.e.,

$$V_x = \{\lambda x + \mu y \mid y \in D_{k_0},\ \lambda, \mu \in \mathbf{R}_{\ge 0},\ \lambda + \mu \le 1\}.$$

Since $\theta^{-1/2}v_k \in B_a$ for all k and B_a is convex, D_{k_0} is contained in B_a. This implies $V_x \subset B_a$. We take another basis $\{u_k\}_{k=1}^{nr}$ of $\mathsf{k}^n_{\mathbf{R}}$ such that $\langle u_k, v_j\rangle = 0$ for any $k \neq j$ and $\langle u_k, u_k\rangle = 1$ for all k. Then the volume $\omega(V_x)$ of V_x equals

$$\frac{|\langle x, u_{k_0}\rangle|\mathrm{vol}(D_{k_0})}{nr}.$$

If we put $\nu = (\min_{1\le k\le nr} |\langle u_k, v_k\rangle|) \cdot (\min_{1\le i\le nr} \mathrm{vol}(D_i))$, then we obtain

$$\frac{|\lambda_{k_0}|\nu}{nr} \le \omega(V_x) \le \omega(B_a) \le 2^{nr}\omega(\mathsf{k}^n_{\mathbf{R}}/\Lambda_0).$$

Therefore,

$$\max_{1\le k\le nr} |\lambda_k| \le \frac{nr2^{nr}\omega(\mathsf{k}^n_{\mathbf{R}}/\Lambda_0)}{\nu}.$$

This estimate holds for all $x \in B_a$. Since the upper bound does not depend on $a \in K_1(\mathsf{m}) \cap X_\theta$, the union of all B_a, $a \in K_1(\mathsf{m}) \cap X_\theta$, is a bounded set in $\mathsf{k}^n_{\mathbf{R}}$. Since W is a subset of $\Lambda_0 \cap \bigcup_{a\in K_1(\mathsf{m})\cap X_\theta} B_a$, W must be a finite set.

By Step 1, $K_1(\mathsf{m})\cap X_\theta$ is bounded, and by Step 2 and Step 3, it is an intersection of finite number of half-spaces. Thus $K_1(\mathsf{m})\cap X_\theta$ is a polytope. Since $K_1(\mathsf{m})\cap T_\theta \subset K_1(\mathsf{m}) \cap X_\theta$ by the proof of Step 1, $K_1(\mathsf{m}) \cap T_\theta$ is also polytope. □

Faces of $K_1(\mathsf{m})$ are described by using shortest vectors.

LEMMA 2.3. *Let $a_1, \cdots, a_k \in \partial K_1(\mathsf{m})$ and S be a non-empty finite subset of Λ_0 such that $S \subset S(a_i)$ for all $1 \le i \le k$. Then, for any $\lambda_1, \cdots, \lambda_k \in \mathbf{R}_{\ge 0}$ with $\sum_{i=1}^k \lambda_i = 1$, one has*

$$\lambda_1 a_1 + \cdots + \lambda_k a_k \in \partial K_1(\mathsf{m}) \text{ and } S \subset S(\lambda_1 a_1 + \cdots + \lambda_k a_k).$$

The proof is easy.

For a non-empty finite subset $S \subset \Lambda_0\backslash\{0\}$, we define the subset $\mathcal{F}_S \subset \partial K_1(\mathsf{m})$ by

$$\mathcal{F}_S = \{a \in \partial K_1(\mathsf{m}) \mid S \subset S(a)\}.$$

By Lemma 2.3, $\mathcal{F}_S$ is a convex set. Let $\mathcal{H}_S$ be the affine subspace of $H_n(\mathsf{k}_{\mathbf{R}})$ generated by $\mathcal{F}_S$, i.e.

$$\mathcal{H}_S = \left\{\sum_{i=1}^k \lambda_i a_i \mid 1 \le k \in \mathbf{Z},\ a_i \in \mathcal{F}_S,\ \lambda_i \in \mathbf{R},\ \sum_{i=1}^k \lambda_i = 1\right\}$$

if $\mathcal{F}_S$ is non-empty. Since S is non-empty, $\mathcal{H}_S$ is a proper affine subspace of $H_n(\mathsf{k}_{\mathbf{R}})$. Then the following is proved by the same argument as in [**17**, Lemmas 1.5 and 1.6].

PROPOSITION 2.4. *One has $\mathcal{F}_S = \partial K_1(\mathsf{m}) \cap \mathcal{H}_S$. In particular, $\mathcal{F}_S$ is a face of $K_1(\mathsf{m})$ if $\mathcal{F}_S \neq \emptyset$. Conversely, any face of $K_1(\mathsf{m})$ is of the form $\mathcal{F}_S$ for some non-empty finite subset $S \subset \Lambda_0$.*

We denote by $\partial^0 K_1(\mathsf{m})$ the set of all 0-dimensional faces of $K_1(\mathsf{m})$. By the same argument as in [**17**, Theorem 1.4], we obtain the following:

THEOREM 2.5. *For $a \in \partial K_1(\mathsf{m})$, the following three conditions are equivalent each other.*

(1) *a is Λ_0-perfect.*
(2) *$a \in \partial^0 K_1(\mathsf{m})$.*
(3) *There exists a neighborhood $\mathcal{N}$ of a in $P_n(\mathsf{k}_{\mathbf{R}})$ such that $S(b) \subsetneq S(a)$ for any $b \in \mathcal{N} \backslash (\mathbf{R}_{\geq 0} a)$.*

The discrete group $GL(\Lambda_0)$ acts on $P_n^-(\mathsf{k}_{\mathbf{R}})$ by $a \cdot \gamma = \gamma^* a \gamma$ for $(a, \gamma) \in P_n^-(\mathsf{k}_{\mathbf{R}}) \times GL(\Lambda_0)$. The set $\partial^0 K_1(\mathsf{m})$ is stable by this action of $GL(\Lambda_0)$. By [**9**, Theorem 5.1], the orbit space $\partial^0 K_1(\mathsf{m})/GL(\Lambda_0)$ is a finite set.

For each $a \in \partial^0 K_1(\mathsf{m})$, we set

$$C_a = \{b \in H_n(\mathsf{k}_{\mathbf{R}}) \mid \langle bx, x \rangle \geq 0 \text{ for any } x \in S(a)\}.$$

The half-line $\mathbf{R}_{\geq 0} b$ generated by $b \in C_a \backslash \{0\}$ is said to be an extreme ray of C_a if for any $b_1, b_2 \in C_a$, whenever $b = (b_1 + b_2)/2$, we must have $b_1, b_2 \in \mathbf{R}_{\geq 0} b$. By the same argument as in [**17**, Lemma 1.7, Proposition 1.3], one can prove the following:

- If $\mathbf{R}_{\geq 0} b$ is an extreme ray of C_a, then $b \notin P_n^-(\mathsf{k}_{\mathbf{R}})$.
- For any 1-dimensional face L of $\partial K_1(\mathsf{m})$, there exist two vertices $a_1, a_2 \in \partial^0 K_1(\mathsf{m})$ such that $L = \{\lambda a_1 + (1 - \lambda) a_2 \mid 0 \leq \lambda \leq 1\}$.

By these properties and Proposition 2.2, we obtain the following theorem (cf. [**17**, Corollary 1.2]).

THEOREM 2.6. *$K_1(\mathsf{m})$ is the convex hull of $\partial^0 K_1(\mathsf{m})$.*

3. Voronoï algorithm for $\partial K_1(\mathsf{m})$

In this section, we show that Voronoï algorithm is effective for $\partial K_1(\mathsf{m})$, which is an algorithm to compute adjacent vertices of a given vertex in $\partial K_1(\mathsf{m})$. Here, two vertices $a_1, a_2 \in \partial^0 K_1(\mathsf{m})$ are said to be adjacent if $L = \{\lambda a_1 + (1 - \lambda) a_2 \mid 0 \leq \lambda \leq 1\}$ is an edge (= 1-dimensional face) of $\partial K_1(\mathsf{m})$. Our purpose is to show the connectedness of vertices of $\partial K_1(\mathsf{m})$, i.e. any two vertices of $\partial K_1(\mathsf{m})$ are linked with finite edges. We follow the argument of [**4**].

For $a \in \partial^0 K_1(\mathsf{m})$, the perfect domain $D_a \subset H_n(\mathsf{k}_{\mathbf{R}})$ of a is defined by

$$D_a = \left\{ \sum_{x \in S(a)} \lambda_x x x^* \mid 0 \leq \lambda_x \in \mathbf{R} \right\}.$$

Let $\mathbf{R}_{\geq 0} c_1, \cdots, \mathbf{R}_{\geq 0} c_k$ be all of extreme rays of C_a. The hyperplane in $H_n(\mathsf{k}_{\mathbf{R}})$ orthogonal to c_i is a supporting hyperplane of D_a, and D_a is the intersection of closed half-spaces $H_{c_i} = \{b \in H_n(\mathsf{k}_{\mathbf{R}}) \mid (b, c_i) \geq 0\}$, $i = 1, \cdots, k$.

LEMMA 3.1. *Let D_a° be the interior of a perfect domain D_a. Then $D_a^\circ \subset P_n(\mathsf{k}_{\mathbf{R}})$. If $D_a^\circ \cap D_{a'} \neq \emptyset$ for $a, a' \in \partial^0 K_1(\mathsf{m})$, then $a = a'$.*

PROOF. Let D_a' be a subset of D_a consisting of all elements of the form $\sum \lambda_x x x^*$ with $\lambda_x > 0$ for all $x \in S(a)$. Since a is Λ_0-perfect, D_a' is an open

convex cone in $H_n(\mathsf{k}_{\mathbf{R}})$ and the closure of D'_a coincides with D_a. Then D'_a must be equal to D°_a (cf. [**1**, Theorem 5.23]). Therefore, each $b \in D^\circ_a$ is represented by

$$b = \sum_{x \in S(a)} \lambda_x x x^*$$

with $\lambda_x > 0$. One has

$$\langle by, y\rangle = \sum_{x \in S(a)} \lambda_x \langle xx^* y, y\rangle = \sum_{x \in S(a)} \lambda_x \mathrm{Tr}_{\mathsf{k}_{\mathbf{R}}}(y^* x x^* y) = \sum_{x \in S(a)} \lambda_x \mathrm{Tr}_{\mathsf{k}_{\mathbf{R}}}((x^* y)^* x^* y)$$

for any $y \in \mathsf{k}^n_{\mathbf{R}} \backslash \{0\}$. In the right-hand side, $\mathrm{Tr}_{\mathsf{k}_{\mathbf{R}}}((x^* y) x^* y) \geq 0$ for every $x \in S(a)$. From the perfection of a, it follows $\mathrm{Tr}_{\mathsf{k}_{\mathbf{R}}}((x^* y) x^* y) > 0$ for at least one $x \in S(a)$. Therefore we have $b \in P_n(\mathsf{k}_{\mathbf{R}})$.

Next, let $b \in D^\circ_a \cap D_{a'}$. Then we have

$$(b, a) = \sum_{x \in S(a)} \lambda_x (xx^*, a) = \sum_{x \in S(a)} \lambda_x \langle ax, x\rangle = \sum_{x \in S(a)} \lambda_x$$

and

$$(b, a') = \sum_{x \in S(a)} \lambda_x (xx^*, a') = \sum_{x \in S(a)} \lambda_x \langle a'x, x\rangle \geq \sum_{x \in S(a)} \lambda_x = (b, a)$$

because of $\langle a'x, x\rangle \geq \mathsf{m}(a') = 1$. On the other hand, b is represented as

$$b = \sum_{x \in S(a')} \mu_x x x^*$$

with $\mu_x \geq 0$. The same argument yields $(b, a) \geq (b, a')$, and hence $(b, a) = (b, a')$. Since

$$\sum_{x \in S(a)} \lambda_x (xx^*, a' - a) = 0, \quad (xx^*, a') \geq (xx^*, a)$$

and $\lambda_x > 0$, we obtain $(xx^*, a - a') = 0$ for any $x \in S(a)$. This concludes $a = a'$. □

Lemma 3.2. *Let $b \in P_n(\mathsf{k}_{\mathbf{R}})$ and θ be a positive constant. Then the number of elements in $\{a \in \partial^0 K_1(\mathsf{m}) \mid (a, b) \leq \theta\}$ is finite.*

Proof. Assume that $a = gg^* \in \partial^0 K_1(\mathsf{m})$ with $g \in GL_n(\mathsf{k}_{\mathbf{R}})$ satisfies $(a, b) \leq \theta$. Let $g_k \in \mathsf{k}^n_{\mathbf{R}}$ be the k-th column vector of g. Then we have

$$(a, b) = \mathrm{TR}(gg^* b) = \mathrm{TR}(g^* b g) = \mathrm{Tr}_{\mathsf{k}_{\mathbf{R}}}(\sum_{k=1}^n g_k^* b g_k) = \sum_{k=1}^n \langle b g_k, g_k\rangle.$$

Put

$$\lambda_b = \min_{x \in \mathsf{k}^n_{\mathbf{R}} \backslash \{0\}} \frac{\langle bx, x\rangle}{\langle x, x\rangle}.$$

Then $\lambda_b > 0$ because of $b \in P_n(\mathsf{k}_{\mathbf{R}})$ and

$$\mathrm{TR}(a) = \sum_{k=1}^n \langle g_k, g_k\rangle \leq \sum_{k=1}^n \frac{\langle b g_k, g_k\rangle}{\lambda_b} = \frac{(a, b)}{\lambda_b} \leq \frac{\theta}{\lambda_b}.$$

By Proposition 2.2, a is a vertex of the polytope $K_1(\mathsf{m}) \cap T_{\theta/\lambda_b}$. □

Proposition 3.3. *For $a, a' \in \partial^0 K_1(\mathsf{m})$, there exists a finite sequence of vertices $\{a_i\}_{i=0}^k \subset \partial^0 K_1(\mathsf{m})$ such that $a_0 = a, a_k = a'$ and a_{i+1} are adjacent to a_i for $i = 0, \cdots, k-1$.*

Proof. Let $a_0 = a$ and $b \in D^\circ_{a'}$. If $b \in D_{a_0}$, then we have $a' = a_0$ by Lemma 3.1. Assume $b \notin D_{a_0}$. We choose a $c \in C_{a_0}$ such that $\mathbf{R}_{\geq 0}c$ is an extreme ray of C_{a_0} and $b \notin H_c$. Let $a_1 = a_0 + \rho c$ be the adjacent vertex to a_0 which is lying on the ray $a_0 + \mathbf{R}_{\geq 0}c$. Since $b \notin H_c$, we have

$$(a_1, b) = (a_0, b) + (\rho c, b) < (a_0, b).$$

If $b \in D_{a_1}$, then $a' = a_1$ by Lemma 3.1. Otherwise, by the same argument, we can take a vertex a_2 which is adjacent to a_1 and satisfies $(a_2, b) < (a_1, b) < (a_0, b)$. By Lemma 3.2, this process terminates at finite times. □

Voronoï algorithm for $\partial K_1(\mathsf{m})$ is summarized as follows.

(1) Fix an initial point $a_0 = a \in \partial^0 K_1(\mathsf{m})$.
(2) Calculate the set of shortest vectors $S(a)$ of a.
(3) Enumerate the extreme rays $\mathbf{R}_{\geq 0}c_1, \cdots, \mathbf{R}_{\geq 0}c_k$ of C_a.
(4) Determine the adjacent vertex of the form $a_i = a + \rho_i c_i$ for each $i = 1, \cdots, k$.
(5) Check whether a_i is equivalent with the vertex which has already been found.
(6) Repeat the operations (2) − (5) for new inequivalent vertices.

4. Polyhedral reduction of $P_n(\mathsf{k}_{\mathbf{R}})/GL(\Lambda_0)$

In the rest of this paper, we assume that k is totally real, i.e., $\mathsf{p}_\infty = \mathsf{p}_1$.

We identify $\mathbf{R}$ with its diagonally embedding in $\mathsf{k}_{\mathbf{R}} = \mathbf{R}^r$. Let

$$\mathsf{k}^+_{\mathbf{R}} = \{(\alpha_\sigma)_{\sigma \in \mathsf{p}_\infty} \in \mathsf{k}_{\mathbf{R}} \mid \alpha_\sigma > 0 \text{ for all } \sigma \in \mathsf{p}_\infty\}.$$

We put

$$H_n(\mathsf{k}) = H_n(\mathsf{k}_{\mathbf{R}}) \cap M_n(\mathsf{k}) \quad \text{and} \quad P_n(\mathsf{k}) = P_n(\mathsf{k}_{\mathbf{R}}) \cap H_n(\mathsf{k})\,.$$

For $a \in P^-_n(\mathsf{k}_{\mathbf{R}})$, the radical of a is defined to be

$$\mathrm{rad}(a) = \{x \in \mathsf{k}^n_{\mathbf{R}} \mid \langle ax, x\rangle = 0\}\,.$$

We call that $\mathrm{rad}(a)$ is defined over k if $(\mathrm{rad}(a) \cap \mathsf{k}^n) \otimes_{\mathbf{Q}} \mathbf{R} = \mathrm{rad}(a)$ holds. By Ω_{k}, we denote the set of all $a \in P^-_n(\mathsf{k}_{\mathbf{R}})$ such that $\mathrm{rad}(a)$ is defined over k. Since $\mathrm{rad}(a) = \{0\}$ if $a \in P_n(\mathsf{k}_{\mathbf{R}})$, Ω_{k} contains $P_n(\mathsf{k}_{\mathbf{R}})$.

We define other two subsets Ω_1 and Ω_2 of $P^-_n(\mathsf{k}_{\mathbf{R}})$ as follows. For $x \in \mathsf{k}^n$, $xx^* = x^t x$ is an element of $M_n(\mathsf{k})$. We consider $M_n(\mathsf{k})$ as a subset of $M_n(\mathsf{k}_{\mathbf{R}})$ by usual way. Then we put

$$\Omega_1 = \left\{ \sum_{i=1}^k \alpha_i x_i x_i^* \mid 1 \leq k \in \mathbf{Z},\ \alpha_i \in \mathsf{k}^+_{\mathbf{R}} \cup \{0\},\ x_i \in \mathsf{k}^n \right\},$$

$$\Omega_2 = \left\{ \sum_{i=1}^k \lambda_i x_i x_i^* \mid 1 \leq k \in \mathbf{Z},\ \lambda_i \in \mathbf{R}_{\geq 0},\ x_i \in \mathsf{k}^n \right\}.$$

Since $\mathbf{R}_{\geq 0} \subset \mathsf{k}^+_{\mathbf{R}} \cup \{0\}$, Ω_2 is a subset of Ω_1. In the following , we show $\Omega_{\mathsf{k}} = \Omega_1 = \Omega_2$.

Lemma 4.1. *The set* $(\mathsf{k}^\times)^2 = \{\alpha^2 \mid \alpha \in \mathsf{k}^\times\}$ *is dense in* $\mathsf{k}^+_{\mathbf{R}}$.

Proof. We define the norm $||\cdot||_{\mathsf{k}_{\mathbf{R}}}$ on $\mathsf{k}_{\mathbf{R}}$ by

$$||\alpha||_{\mathsf{k}_{\mathbf{R}}} = \max_{\sigma \in \mathsf{p}_\infty} |\alpha_\sigma|_\sigma$$

for $\alpha = (\alpha_\sigma) \in \mathsf{k}_{\mathbf{R}}$, where $|\cdot|_\sigma$ denotes the absolute value of k_σ. Since k is dense in $\mathsf{k}_{\mathbf{R}}$, $\mathsf{k}_{\mathbf{R}}^+ \cap \mathsf{k}$ is also dense in $\mathsf{k}_{\mathbf{R}}^+$. For a given $\alpha = (\alpha_\sigma) \in \mathsf{k}_{\mathbf{R}}^+$, there is a square root $\sqrt{\alpha} = (\sqrt{\alpha_\sigma}) \in \mathsf{k}_{\mathbf{R}}^+$ of α. Then, for any $\epsilon \in (0,1)$, there exists $\beta \in \mathsf{k}_{\mathbf{R}}^+ \cap \mathsf{k}$ such that

$$||\sqrt{\alpha} - \beta||_{\mathsf{k}_{\mathbf{R}}} < \frac{\epsilon}{2||\sqrt{\alpha}||_{\mathsf{k}_{\mathbf{R}}} + 1}.$$

From $||\beta||_{\mathsf{k}_{\mathbf{R}}} < ||\sqrt{\alpha}||_{\mathsf{k}_{\mathbf{R}}} + 1$, it follows that

$$||\sqrt{\alpha} + \beta||_{\mathsf{k}_{\mathbf{R}}} < 2||\sqrt{\alpha}||_{\mathsf{k}_{\mathbf{R}}} + 1.$$

Therefore, we have

$$||\alpha - \beta^2||_{\mathsf{k}_{\mathbf{R}}} \leq ||\sqrt{\alpha} - \beta||_{\mathsf{k}_{\mathbf{R}}} \cdot ||\sqrt{\alpha} + \beta||_{\mathsf{k}_{\mathbf{R}}} < \epsilon.$$

□

Let $\mathrm{Cone}((\mathsf{k}^\times)^2)$ be the cone in $\mathsf{k}_{\mathbf{R}}$ generated by $(\mathsf{k}^\times)^2$, i.e.,

$$\mathrm{Cone}((\mathsf{k}^\times)^2) = \{\sum_{i=1}^{k} \lambda_i \alpha_i^2 \mid 0 < k \in \mathbf{Z},\ \lambda_i \in \mathbf{R}_{\geq 0},\ \alpha_i \in \mathsf{k}^\times\}.$$

Lemma 4.2. $\mathsf{k}_{\mathbf{R}}^+ \cup \{0\} = \mathrm{Cone}((\mathsf{k}^\times)^2)$.

Proof. For a given $\alpha = (\alpha_\sigma) \in \mathsf{k}_{\mathbf{R}}^+$, we choose $\epsilon > 0$ so that the neighborhood

$$U = \{\beta \in \mathsf{k}_{\mathbf{R}} \mid ||\alpha - \beta||_{\mathsf{k}_{\mathbf{R}}} < \epsilon\}$$

of α is contained in $\mathsf{k}_{\mathbf{R}}^+$. For $\kappa = (\kappa_\sigma) \in \{\pm 1\}^r$, we put

$$U_\kappa = \{\beta \in U \mid \kappa_\sigma(\alpha_\sigma - \beta_\sigma) > 0 \text{ for all } \sigma \in \mathsf{p}_\infty\}.$$

By Lemma 4.1, there is a $\beta_\kappa^2 \in U_\kappa \cap (\mathsf{k}^\times)^2$. Then α is contained in the convex hull of $\{\beta_\kappa^2 \mid \kappa \in \{\pm 1\}^r\}$. This implies $\alpha \in \mathrm{Cone}((\mathsf{k}^\times)^2)$. □

Proposition 4.3. $\Omega_1 = \Omega_2$.

Proof. For any $\alpha \in \mathsf{k}_{\mathbf{R}}^+$ and $x \in \mathsf{k}^n$, we must prove $\alpha x x^* \in \Omega_2$. By Lemma 4.2, α is represented as

$$\alpha = \sum_i \lambda_i \alpha_i^2$$

with $\lambda_i \in \mathbf{R}_{\geq 0}$ and $\alpha_i \in \mathsf{k}^\times$. Then we have

$$\alpha x x^* = \sum_i \lambda_i (\alpha_i x)(\alpha_i x)^* \in \Omega_2.$$

□

Next, we prove $\Omega_{\mathsf{k}} = \Omega_1$.

Lemma 4.4. $P_n(\mathsf{k}) \subset \Omega_1$.

Proof. For $a \in P_n(\mathsf{k})$, there exists $g \in GL_n(\mathsf{k})$ such that

$$a = g \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} g^*,$$

where $\lambda_1, \cdots, \lambda_n \in \mathsf{k}^\times$. Since a is positive definite, every λ_i must be totally positive, i.e., $\lambda_i \in \mathsf{k}_{\mathbf{R}}^+ \cap \mathsf{k}$. If $e_1, \cdots e_n$ denote the standard basis of the column vector space k^n, then

$$\begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} = \lambda_1 e_1 e_1^* + \cdots + \lambda_n e_n e_n^*.$$

By putting $x_i = g e_i \in \mathsf{k}^n$, we obtain

$$a = \lambda_1 x_1 x_1^* + \cdots + \lambda_n x_n x_n^* \in \Omega_1.$$

□

LEMMA 4.5. $P_n(\mathsf{k}_{\mathbf{R}}) \subset \Omega_1$.

PROOF. We fix an $a \in P_n(\mathsf{k}_{\mathbf{R}})$ and a sufficiently small rational number $\mu > 0$ such that $a - \mu I \in P_n(\mathsf{k}_{\mathbf{R}})$, where I denotes the identity matrix. Since $P_n(\mathsf{k})$ is dense in $P_n(\mathsf{k}_{\mathbf{R}})$, for any $\epsilon \in \mathbf{Q}$, $0 < \epsilon < \mu$, there exists $a' \in P_n(\mathsf{k})$ such that

$$b = (a - \mu I) - a' \in P_n(\mathsf{k}_{\mathbf{R}})$$

and the (i,j)-component $b_{ij} \in \mathsf{k}_{\mathbf{R}}$ of b satisfies

$$||b_{ij}||_{\mathsf{k}_{\mathbf{R}}} < \epsilon$$

for all i, j. We put $c = b + \mu I \in P_n(\mathsf{k}_{\mathbf{R}})$ and

$$d = c - \sum_{i<j} \epsilon E_{ij} \in H_n(\mathsf{k}_{\mathbf{R}}),$$

where $E_{ij} = (e_i + e_j)(e_i + e_j)^* \in H_n(\mathsf{k})$. Let $c_{ij} = ((c_{ij})_\sigma)_{\sigma \in \mathsf{p}_\infty}$ and $d_{ij} = ((d_{ij})_\sigma)_{\sigma \in \mathsf{p}_\infty}$ be the (i,j) components of c and d, respectively. Then, we have

$$(d_{ij})_\sigma = \begin{cases} (c_{ii})_\sigma - (n-1)\epsilon = (b_{ii})_\sigma + \mu - (n-1)\epsilon & (i = j) \\ (c_{ij})_\sigma - \epsilon = (b_{ij})_\sigma - \epsilon < 0 & (i \neq j) \end{cases}$$

for all $\sigma \in \mathsf{p}_\infty$. Here we note that both μ and ϵ are rational numbers. If we fix i and σ, then

$$\sum_{j \neq i} |(d_{ij})_\sigma|_\sigma = \sum_{j \neq i} |(b_{ij})_\sigma - \epsilon|_\sigma < 2(n-1)\epsilon.$$

We may assume that $0 < \epsilon \in \mathbf{Q}$ is sufficiently small as

$$\{3(n-1) + 1\}\epsilon < \mu.$$

Then, by $3(n-1)\epsilon < \mu - \epsilon \leq \mu + (b_{ii})_\sigma$, we have $2(n-1)\epsilon < (d_{ii})_\sigma$, and hence

$$\sum_{j \neq i} |(d_{ij})_\sigma|_\sigma < (d_{ii})_\sigma .$$

Therefore, the matrix $d_\sigma = ((d_{ij})_\sigma)_{ij} \in M_n(\mathsf{k}_\sigma)$ is near-diagonal and its all non-diagonal elements are negative. This leads us to the following representation of d_σ:

$$d_\sigma = \sum_{i<j} \{-(d_{ij})_\sigma\}(e_i - e_j)(e_i - e_j)^* + \sum_i \left((d_{ii})_\sigma + \sum_{j \neq i} (d_{ij})_\sigma \right) e_i e_i^*.$$

We define $\alpha_{ij} \in \mathsf{k}_{\mathbf{R}}^{+}$ by

$$(\alpha_{ij})_\sigma = \begin{cases} (d_{ii})_\sigma + \sum_{k \neq i} (d_{ik})_\sigma & (i = j) \\ -(d_{ij})_\sigma & (i \neq j) \end{cases}$$

for $\sigma \in \mathsf{p}_\infty$. Then we have

$$d = \sum_{i<j} \alpha_{ij}(e_i - e_j)(e_i - e_j)^* + \sum_i \alpha_{ii} e_i e_i^* \in \Omega_1,$$

and hence

$$c = d + \sum_{i<j} \epsilon E_{ij} \in \Omega_1.$$

Since Ω_1 is a convex cone and $a' \in \Omega_1$ by Lemma 4.4, $a = c + a'$ is contained in Ω_1. This completes the proof. □

PROPOSITION 4.6. $\Omega_{\mathsf{k}} = \Omega_1$.

PROOF. We fix a non-zero $a \in \Omega_1$. Then a is represented as

$$a = \sum_i \alpha_i x_i x_i^*, \qquad (\alpha_i \in \mathsf{k}_{\mathbf{R}}^{+},\ x_i \in \mathsf{k}^n \setminus \{0\}).$$

An element $x = (x_\sigma) \in \mathsf{k}_{\mathbf{R}}^n$ is contained in $\mathrm{rad}(a)$ if and only if

$$\sum_\sigma \sum_i (\alpha_i)_\sigma (x_\sigma^* \cdot \sigma(x_i))^2 = 0.$$

Since $(\alpha_i)_\sigma > 0$, we have

$$\mathrm{rad}(a) = \{x = (x_\sigma) \in \mathsf{k}_{\mathbf{R}}^n \mid x_\sigma^* \cdot \sigma(x_i) = 0 \text{ for all } \sigma, i\}.$$

If we take a k-linear subspace

$$W = \{x \in \mathsf{k}^n \mid x^* \cdot x_i = 0\},$$

then $W = \mathrm{rad}(a) \cap \mathsf{k}^n$ and

$$W \otimes_{\mathbf{Q}} \mathbf{R} = \prod_\sigma \sigma(W) \otimes_{\mathsf{k}} \mathsf{k}_\sigma = \mathrm{rad}(a).$$

Thus a is contained in Ω_{k}.

Next we show $\Omega_{\mathsf{k}} \subset \Omega_1$ by induction of n. When $n = 1$, then $\Omega_1 = \mathsf{k}_{\mathbf{R}}^{+} \cup \{0\}$. For $a \in \Omega_{\mathsf{k}}$, its radical is either the whole $\mathsf{k}_{\mathbf{R}}$ or $\{0\}$. This means $a \in \mathsf{k}_{\mathbf{R}}^{+}$ or $a = 0$.

We consider the case of $n > 1$. Let $a \in \Omega_{\mathsf{k}}$. If $\mathrm{rad}(a) = \{0\}$, then $a \in P_n(\mathsf{k}_{\mathbf{R}})$, and hence $a \in \Omega_1$ by Lemma 4.5. Thus we assume $\mathrm{rad}(a) \neq \{0\}$. In this case, there is a non-zero $x \in \mathrm{rad}(a) \cap \mathsf{k}^n$. If we take $g \in GL_n(\mathsf{k})$ whose first column equals x, then $g^* a g$ is of the form

$$\begin{pmatrix} 0 & 0 \\ 0 & a' \end{pmatrix}, \qquad (a' \in P_{n-1}^{-}(\mathsf{k}_{\mathbf{R}})).$$

We note that

$$\mathrm{rad}(\begin{pmatrix} 0 & 0 \\ 0 & a' \end{pmatrix}) = g^{-1}\mathrm{rad}(a).$$

Let $\varphi : \mathsf{k}^n \longrightarrow \mathsf{k}^{n-1}$ be a linear map defined by $\varphi((\lambda_1, \cdots, \lambda_n)^*) = (\lambda_2, \cdots, \lambda_n)^*$. Since $\mathrm{rad}(a') = \varphi(g^{-1}\mathrm{rad}(a))$, $\mathrm{rad}(a')$ is defined over k. By the assumption of induction, a' is represented as

$$a' = \sum_i \alpha_i y_i y_i^*, \qquad (\alpha_i \in \mathsf{k}_{\mathbf{R}}^+,\ y_i \in \mathsf{k}^{n-1}).$$

Then, we obtain

$$g^* a g = \sum_i \alpha_i \begin{pmatrix} 0 \\ y_i \end{pmatrix} \begin{pmatrix} 0 \\ y_i \end{pmatrix}^* \in \Omega_1,$$

and hence $a \in (g^*)^{-1}\Omega_1 g^{-1} = \Omega_1$. □

In the following, we fix a projective o_{k}-module $\Lambda_0 \subset \mathsf{k}^n$ of rank n and use the same notations as in §2 and §3. We note that, since $\Lambda_0 \otimes_{\mathbf{Z}} \mathbf{Q} = \mathsf{k}^n$, Ω_2 (and hence Ω_{k}) is given as

$$\Omega_2 = \left\{ \sum_{i=1}^k \lambda_i x_i x_i^* \mid 1 \leq k \in \mathbf{Z},\ \lambda_i \in \mathbf{R}_{\geq 0},\ x_i \in \Lambda_0 \right\}.$$

Then, it is obvious that Ω_{k} is stabilized by the action of $GL(\Lambda_0)$ on $P_n^-(\mathsf{k}_{\mathbf{R}})$. For $a \in \Omega_{\mathsf{k}}$, define the subgroup Γ_a of $GL(\Lambda_0)$ by

$$\Gamma_a = \{\gamma \in GL(\Lambda_0) \mid a \cdot \gamma^* = \gamma a \gamma^* = a\}.$$

Lemma 4.7. *For a given non-zero $a \in \Omega_{\mathsf{k}}$ and a constant $\theta > 0$, the set*

$$[a]_\theta = \{b \in \partial^0 K_1(\mathsf{m}) \mid (a, b) \leq \theta\}$$

is Γ_a-invariant, and the number of Γ_a-orbits in $[a]_\theta$ is finite.

Proof. Since

$$(a, b \cdot \gamma) = (a \cdot \gamma^*, b) = (a, b)$$

holds for any $b \in [a]_\theta$ and $\gamma \in \Gamma_a$, $[a]_\theta$ is Γ_a-invariant. By the remark mentioned above, a is represented as

$$a = \sum_{i=1}^k \lambda_i x_i x_i^*, \qquad (\lambda_i \in \mathbf{R}_{>0},\ x_i \in \Lambda_0 \setminus \{0\}).$$

Since $\partial^0 K_1(\mathsf{m})/GL(\Lambda_0)$ is a finite set, we choose a complete system $b_1, \cdots, b_t$ of representatives of $\partial^0 K_1(\mathsf{m})/GL(\Lambda_0)$. We define the subgroup Γ of $GL(\Lambda_0)$ as

$$\Gamma = \{\gamma \in GL(\Lambda_0) \mid \gamma x_i = x_i \ \text{ for all } i = 1, \cdots, k\}.$$

Since $\Gamma \subset \Gamma_a$ and

$$[a]_\theta = \bigcup_{i=1}^t [a]_\theta \cap (b_i \cdot GL(\Lambda_0)),$$

it is sufficient to prove the finiteness of Γ-orbits in $[a]_\theta \cap (b_i \cdot GL(\Lambda_0))$ for all $i = 1, \cdots, t$. We fix $b \in [a]_\theta \cap (b_i \cdot GL(\Lambda_0))$. By replacing b_i with b if necessary, we may assume $b = b_i$. We choose a complete system $\{\gamma_j\}_j$ of representatives of $GL(\Lambda_0)/\Gamma$, which is an infinite set. We put

$$\widetilde{x} = {}^t(x_1, x_2, \cdots, x_k) \in \Lambda_0^{\oplus k}$$

and

$$\widetilde{x}_j = {}^t(\gamma_j x_1, \gamma_j x_2, \cdots, \gamma_j x_k) \in \Lambda_0^{\oplus k}.$$

If $j \neq j'$, then $\widetilde{x}_j \neq \widetilde{x}_{j'}$. For $b \in P_n(\mathsf{k}_{\mathbf{R}})$, define

$$\widetilde{b} = \begin{pmatrix} \lambda_1 b & & 0 \\ & \ddots & \\ 0 & & \lambda_k b \end{pmatrix} \in P_{kn}(\mathsf{k}_{\mathbf{R}}).$$

Then we have

$$(a, b_i \cdot \gamma_j) = \mathrm{Tr}_{\mathsf{k}_{\mathbf{R}}}({}^t\widetilde{x}_j \widetilde{b}_i \widetilde{x}_j).$$

Since $\Lambda_0^{\oplus k} \subset \mathsf{k}_{\mathbf{R}}^{kn}$ is a lattice and $\widetilde{b}_i$ is positive definite, the cardinality of the set

$$\{\widetilde{x} \in \Lambda_0^{\oplus k} \mid \mathrm{Tr}_{\mathsf{k}_{\mathbf{R}}}({}^t\widetilde{x}\widetilde{b}_i\widetilde{x}) \leq \theta\}$$

is finite. In particular, the number of γ_j satisfying $(a, b_i \cdot \gamma_j) \leq \theta$ is finite. This shows that the number of Γ-orbits in $[a]_\theta \cap (b_i \cdot GL(\Lambda_0)))$ is finite. □

Since Γ_a is a finite group if $a \in P_n(\mathsf{k}_{\mathbf{R}})$, Lemma 4.7 gives another proof of Lemma 3.2.

LEMMA 4.8. *For $a \in \Omega_{\mathsf{k}} \setminus \{0\}$, there exists $b_0 \in \partial^0 K_1(\mathsf{m})$ such that*

$$\inf_{b \in K_1(\mathsf{m})} (a, b) = (a, b_0),$$

and then $a \in D_{b_0}$.

PROOF. We choose a sufficiently large $\theta > 0$ so that $[a]_\theta \neq \emptyset$. Since $K_1(\mathsf{m})$ is the convex hull of $\partial^0 K_1(\mathsf{m})$, we have

$$\inf_{b \in K_1(m)} (a, b) = \inf_{b \in \partial^0 K_1(\mathsf{m})} (a, b) = \inf_{b \in [a]_\theta} (a, b) = \inf_{b\Gamma_a \in [a]_\theta/\Gamma_a} (a, b).$$

The existence of b_0 follows from Lemma 4.7.

By [**9**, Lemma 4.3] (or Theorem 2.5), there is a neighborhood $\mathcal{N}$ of b_0 in $P_n(\mathsf{k}_{\mathbf{R}})$ such that $S(b) \subset S(b_0)$ for any $b \in \mathcal{N}$. Let $\mathbf{R}_{\geq 0}c_1, \cdots, \mathbf{R}_{\geq 0}c_k$ be all extreme rays of C_{b_0}. We choose a sufficiently small $\epsilon > 0$ so that $b_0 + \epsilon c_i \in \mathcal{N}$ for all $i = 1, \cdots, k$. Since $\mathsf{m}(b_0 + \epsilon c_i)^{-1}(b_0 + \epsilon c_i) \in K_1(\mathsf{m})$, we have

$$(a, b_0)\mathsf{m}(b_0 + \epsilon c_i) \leq (a, b_0 + \epsilon c_i)\,.$$

Then, for $x \in S(b_0 + \epsilon c_i) \subset S(b_0)$,

$$(a, b_0)(b_0 + \epsilon c_i, xx^*) \leq (a, b_0 + \epsilon c_i)$$

holds. From $c_i \in C_{b_0}$, it follows

$$0 \leq \epsilon(a, b_0)(c_i, xx^*) \leq \epsilon(a, c_i)\,,$$

namely,

$$a \in \bigcap_{i=1}^{k} H_{c_i} = D_{b_0}\,.$$

□

By this Lemma, we have

$$\Omega_{\mathsf{k}} = \bigcup_{b \in \partial^0 K_1(\mathsf{m})} D_b.$$

Let $b_1, \cdots, b_t$ be a complete system of representatives of $\partial^0 K_1(\mathsf{m})/GL(\Lambda_0)$. For each i, Γ_i denotes the stabilizer of b_i in $GL(\Lambda_0)$, i.e.,

$$\Gamma_i = \{\gamma \in GL(\Lambda_0) \mid b_i \cdot \gamma = b_i\},$$

which is a finite subgroup. We put $GL(\Lambda_0)^* = \{\gamma^* \mid \gamma \in GL(\Lambda_0)\}$ and $\Gamma_i^* = \{\gamma^* \mid \gamma \in \Gamma_i\}$. It is easy to check that $S(a \cdot \gamma) = \gamma^{-1}S(a)$ and $D_{a\cdot\gamma} = D_a \cdot \gamma^*$ hold for all $a \in \partial^0 K_1(m)$ and $\gamma \in GL(\Lambda_0)$. In particular, the finite group Γ_i^* stabilizes D_{b_i}. Now the following theorem is obvious.

THEOREM 4.9. *Notations being as above, one has*

$$\Omega_{\mathsf{k}}/GL(\Lambda_0)^* = \bigcup_{i=1}^{t} D_{b_i}/\Gamma_i^*.$$

As an example, we consider the case of $n = 1$. In this case, $\Omega_{\mathsf{k}} \setminus \{0\}$ equals $\mathsf{k}_{\mathbf{R}}^+$. If $\Lambda_0 = \mathsf{o}_{\mathsf{k}}$, then $GL(\Lambda_0)$ equals the unit group E_{k} of o_{k}. The action of E_{k} on $\mathsf{k}_{\mathbf{R}}^+$ is given by $x \cdot \epsilon = \epsilon^2 x$ for $\epsilon \in E_{\mathsf{k}}$ and $x \in \mathsf{k}_{\mathbf{R}}$. Since $\Gamma_i = \{\pm 1\}$ trivially acts on D_{b_i}, Theorem 4.9 yields

$$\mathsf{k}_{\mathbf{R}}^+/E_{\mathsf{k}} = E_{\mathsf{k}}^2 \backslash \mathsf{k}_{\mathbf{R}}^+ = \bigcup_{i=1}^{t} D_{b_i}^*,$$

where $D_{b_i}^* = D_{b_i} \setminus \{0\}$. In other words, a fundamental domain of $E_{\mathsf{k}}^2 \backslash \mathsf{k}_{\mathbf{R}}^+$ decomposes into a union of cones.

5. Ryshkov polyhedra of real quadratic fields

In this section, we consider the simplest case, i.e., $n = 1$ and k is a real quadratic field $\mathbf{Q}(\sqrt{d})$, where d is a square free positive integer. In this case, we have $\Omega_{\mathsf{k}} \setminus \{0\} = P_1(\mathsf{k}_{\mathbf{R}}) = \mathsf{k}_{\mathbf{R}}^+ = \mathbf{R}_{>0}^2$ by identifying $\mathsf{k}_{\mathbf{R}}$ with $\mathbf{R}^2$. We denote by τ the Galois involution of k, which acts on $\mathsf{k}_{\mathbf{R}}^+$ by the reflection with respect to the line $\mathbf{R}1 = \mathbf{R}(1,1)$ of the direction $(1,1)$. Let $\Lambda_0 = \mathsf{o}_{\mathsf{k}} = \mathbf{Z}[\omega]$, where $\omega = \sqrt{d}$ if $d \equiv 2, 3 \mod 4$ or $\omega = (1 + \sqrt{d})/2$ if $d \equiv 1 \mod 4$. The Λ_0-minimum function $\mathsf{m} = \mathsf{m}_{\Lambda_0}$ is given by

$$\mathsf{m}(a) = \min_{0 \neq x \in \mathsf{o}_{\mathsf{k}}} (\alpha_1 x^2 + \alpha_2 \tau(x^2))$$

for $a = (\alpha_1, \alpha_2) \in \mathsf{k}_{\mathbf{R}}^+$. The Ryshkov polyhedron $K_1(\mathsf{m})$ is a convex domain in $\mathsf{k}_{\mathbf{R}}^+$ with infinite vertices.

LEMMA 5.1. *The Ryshkov polyhedron $K_1(\mathsf{m})$ is invariant by τ, i.e., $K_1(\mathsf{m})$ is symmetric with respect to $\mathbf{R}1$. If $a \in \partial^0 K_1(\mathsf{m})$, then $a \in \mathsf{k}_{\mathbf{R}}^+ \cap \mathsf{k}$ and $\tau(a) \in \partial^0 K_1(\mathsf{m})$.*

This is clear from $\tau(\mathsf{o}_{\mathsf{k}}) = \mathsf{o}_{\mathsf{k}}$ and Theorem 1.2.

Every o_{k}-perfect form $a \in \partial^0 K_1(\mathsf{m})$ is of the form $(\alpha, \tau(\alpha))$ with a totally positive $\alpha \in \mathsf{k}$. It is easy to prove that there is no o_{k}-perfect form on the half-line $\mathbf{R}_{>0}1$. Thus there is a unique o_{k}-perfect form $a = (\alpha, \tau(\alpha)) \in \partial^0 K_1(\mathsf{m})$ such that $\tau(\alpha)$ is minimal among o_{k}-perfect forms in $K_1(\mathsf{m}) \cap \{(\alpha_1, \alpha_2) \in \mathsf{k}_{\mathbf{R}}^+ \mid \alpha_1 < \alpha_2\}$. We call this o_{k}-perfect form the minimal o_{k}-perfect form.

Let E_{k} be the unit group of o_{k}. The action of $GL(\Lambda_0) = E_{\mathsf{k}}$ on $K_1(\mathsf{m})$ is given by $(a, u) \longrightarrow a \cdot u = u^2 a$ for $(a, u) \in K_1(\mathsf{m}) \times E_{\mathsf{k}}$. We fix a fundamental unit $\epsilon \in E_{\mathsf{k}}$ such that $\epsilon^2 < 1$. Then $\{\epsilon^{2k} a \mid k \in \mathbf{Z}\}$ is the set of elements that are equivalent with a. Let t_{k} be the number of equivalent classes in $\partial^0 K_1(\mathsf{m})$, i.e., the cardinal number of $\partial^0 K_1(\mathsf{m})/GL(\Lambda_0) = E_{\mathsf{k}}^2 \backslash \partial^0 K_1(\mathsf{m})$.

LEMMA 5.2. *Let a be the minimal o_{k}-perfect form. Then $t_{\mathsf{k}} = 1$ if and only if $\epsilon^{-2} a = \tau(a)$.*

PROOF. By Lemma 5.1, a and $\tau(a)$ are symmetric each other with respect to $\mathbf{R}1$. Obviously, a and $\tau(a)$ are equivalent if and only if $t_{\mathsf{k}} = 1$. Assume a and $\tau(a)$ are equivalent. Then $\tau(a)$ is equal to $\epsilon^{2k}a$ for some k. By the minimal condition of a, k must be equal to -1. □

LEMMA 5.3. *Let $\beta_0 = (\tau(\epsilon^2) - 1)^{-1}\sqrt{d}$ and $b_0 = (\beta_0, \tau(\beta_0)) \in \mathsf{k}_{\mathbf{R}}^+ \cap \mathsf{k}$. If $b = (\beta, \tau(\beta)) \in \mathsf{k}_{\mathbf{R}}^+ \cap \mathsf{k}$ satisfies $\beta < \tau(\beta)$ and $\tau(b) = \epsilon^{-2}b$, then b is a scalar multiple of b_0.*

PROOF. Since the slope of the line segment between b and $\tau(b) = \epsilon^{-2}b$ equals -1, we have

$$\frac{\epsilon^2\tau(\beta) - \tau(\beta)}{\tau(\epsilon^2)\beta - \beta} = -1.$$

If we put $\delta = (\tau(\epsilon^2) - 1)\beta$, then $\tau(\delta) = -\delta$. Thus δ is of the form $\xi\sqrt{d}$ with $\xi \in \mathbf{Q}$, and hence $b = \xi b_0$. □

PROPOSITION 5.4. *Let b_0 be the same as above. Then b_0 is o_{k}-perfect if and only if t_{k} is odd.*

PROOF. Let a_0 be the minimal o_{k}-perfect form. We assume that b_0 is o_{k}-perfect. Let $\{a_0, \cdots, a_k = m(b_0)^{-1}b_0\}$ be a sequence of o_{k}-perfect forms in $\partial^0 K_1(\mathsf{m})$ such that a_i and a_{i+1} are adjacent each other for $i = 0, \cdots, k-1$ and the first component of a_i is larger than that of a_{i+1} for all i. From $\tau(a_k) = \epsilon^{-2}a_k$, it follows that any two elements of $\{a_0, \cdots, a_k, \tau(a_0), \cdots, \tau(a_{k-1})\}$ can not be equivalent. This yields $t_{\mathsf{k}} = 2k+1$. Conversely, we assume that t_{k} is odd, say $t_{\mathsf{k}} = 2k+1$. We can take a complete set $\{a_0, \cdots, a_{2k}\}$ of representatives of $E_{\mathsf{k}}^2 \backslash \partial^0 K_1(\mathsf{m})$ contained in $\{(\alpha_1, \alpha_2) \in \mathsf{k}_{\mathbf{R}}^+ \mid \alpha_1 < \alpha_2\}$ so that a_i and a_{i+1} are adjacent each other for $i = 0, \cdots, 2k-1$. By comparing size of first components of $a_0, \cdots, a_{2k}, \epsilon^{-2}a_0, \cdots, \epsilon^{-2}a_{2k}$, we obtain $\tau(a_i) = \epsilon^{-2}a_{2k-i}$ for $i = 0, \cdots, 2k$, in particular, $\tau(a_k) = \epsilon^{-2}a_k$. By Lemma 5.3, a_k must be a scalar multiple of b_0. □

Let $\eta = (1+\epsilon^2)/(1-\epsilon^2)$. Since $\tau(\eta) = -\eta$, η is of the form $\theta\sqrt{d}$ with $\theta \in \mathbf{Q}$. Define the rational binary quadratic form q as

$$q(x_1, x_2) = \begin{cases} \theta x_1^2 - 2x_1x_2 + \theta d x_2^2 & (d \equiv 2, 3 \mod 4) \\ \theta x_1^2 + (\theta - 1)x_1x_2 + 4^{-1}((1+d)\theta - 2)x_2^2 & (d \equiv 1 \mod 4) \end{cases}.$$

Then, $(b_0, xx^*) = d \cdot q(x_1, x_2)$ holds for $x = x_1 + x_2\omega \in \mathsf{o}_{\mathsf{k}}$. Therefore, b_0 is o_{k}-perfect if and only if the perfection rank of q is greater than 1. See [**7**, Definition 13.1.2] for perfection rank.

EXAMPLE. When $d \leq 10000$ and $d \equiv 2, 3 \mod 4$, there are 486 d such that b_0 is o_{k}-perfect, for example,
2, 3, 10, 15, 26, 35, 58, 74, 82, 91, 106, 122, 130, 143, 170, 195, 202, 218, 226, 247, ..., 9699, 9722, 9754, 9770, 9778, 9818, 9831, 9866, 9879, 9914, 9919, 9938, 9946, 9970.

EXAMPLE. When $d \leq 10000$ and $d \equiv 1 \mod 4$, there are 1061 d such that b_0 is o_{k}-perfect, for example,
5, 13, 17, 21, 29, 37, 41, 53, 61, 65, 73, 77, 85, 89, 97, 101, 109, 113, 133, 137, ..., 9865, 9869, 9877, 9881, 9893, 9901, 9929, 9941, 9949, 9953, 9965, 9973, 9985, 9997.

PROPOSITION 5.5. *If $\epsilon \cdot \tau(\epsilon) = -1$, then t_{k} is odd.*

PROOF. Let a_0 be the minimal $\mathsf{o_k}$-perfect form. We choose a sequence $a_0, a_1, \cdots$, $a_i = (\alpha_i, \tau(\alpha_i)), \cdots$ of $\partial^0 K_1(\mathsf{m})$ such that a_{i-1} and a_i are adjacent, $\alpha_i < \tau(\alpha_i)$ and $\alpha_i < \alpha_{i-1}$ for all i. Since $a_{t_\mathsf{k}} = \epsilon^2\tau(a_0)$, we have

$$a_k = \begin{cases} \epsilon^2\tau(a_k) & \text{if}\, t_\mathsf{k} = 2k+1 \\ \epsilon^2\tau(a_{k-1}) & \text{if}\, t_\mathsf{k} = 2k \end{cases}.$$

Since a_{k-1} and a_k are adjacent each other, there exists an $x \in S(a_{k-1}) \cap S(a_k)$. If $t_\mathsf{k} = 2k$, then $\tau(\epsilon x) \in S(a_{k-1}) \cap S(a_k)$. Therefore, we have $x = \pm\tau(\epsilon x)$, and hence $\epsilon \cdot \tau(\epsilon) = 1$. This is a contradiction. □

If b_0 is not $\mathsf{o_k}$-perfect, we need to construct an initial $\mathsf{o_k}$-perfect form of Voronoï algorithm. The following proposition gives this. This initial $\mathsf{o_k}$-perfect form was also found by Gunnells and Yasaki [**3**, Proposition 6.1] by other method.

PROPOSITION 5.6. (1) *Let $d \equiv 2, 3 \mod 4$ and n be the integer such that*

$$n - 1 \leq \frac{-1 + \sqrt{4d-3}}{2} < n.$$

Then $a_0 = (\alpha, \tau(\alpha))$ defined by

$$\alpha = \frac{1}{2} + \frac{n^2 + d - 1}{4dn}\sqrt{d}$$

is $\mathsf{o_k}$-perfect and

$$S(a_0) = \begin{cases} \{\pm 1, \pm(n-\omega)\} & (d > n^2 - n + 1) \\ \{\pm 1, \pm(n-\omega), \pm(n-1-\omega)\} & (d = n^2 - n + 1) \end{cases}.$$

Moreover, $\tau(a_0) = (\tau(\alpha), \alpha)$ is the minimal $\mathsf{o_k}$-perfect form.

(2) *Let $d \equiv 1 \mod 4$ and n be the integer such that*

$$n - 1 < \frac{\sqrt{d-3}}{2} < n.$$

Then $a_0 = (\alpha, \tau(\alpha))$ defined by

$$\alpha = \frac{1}{2} + \frac{(2n-1)^2 + d - 4}{4d(2n-1)}\sqrt{d}$$

is $\mathsf{o_k}$-perfect and $S(a_0) = \{\pm 1, \pm(n-\omega)\}$. Moreover, $\tau(a_0) = (\tau(\alpha), \alpha)$ is the minimal $\mathsf{o_k}$-perfect form.

PROOF. (1) From the definition of n, it follows $n^2 - n + 1 \leq d < n^2 + n + 1$. For $x = x_1 + x_2\omega \in \mathsf{o_k}$, (a_0, xx^*) equals

$$\frac{1}{4n^2}\{2nx_1 + (n^2 + d - 1)x_2\}^2 + \frac{1}{4n^2}\{4dn^2 - (n^2 + d - 1)^2\}x_2^2.$$

If $x_2 = 0$, then $(a_0, xx^*) \geq 1$ and the equality holds for $x = \pm 1$. If $|x_2| = 1$, then we may assume $x_2 = -1$. We have $(a_0, xx^*) \geq 1$ since

$$(a_0, (x_1 - \sqrt{d})(x_1 - \sqrt{d})^*) - 1 = (x_1 - n)\{nx_1 - (d-1)\}/n$$

and $n - 1 \leq (d-1)/n < n + 1$. The equality holds for $x = \pm(n - \omega)$ and in addition $x = \pm(n - 1 - \omega)$ if $d = n^2 - n + 1$. If $|x_2| \geq 2$, then we have

$$\begin{aligned} \{4dn^2 - (n^2 + d - 1)^2\}x_2^2 - 4n^2 \geq & 4\{4dn^2 - (n^2 + d - 1)^2\} - 4n^2 \\ = & -4\{d^2 - 2d(n^2 + 1) + (n^2 - 1)^2 + n^2\}. \end{aligned}$$

This polynomial is positive if $n^2-\sqrt{3}n+1<d<n^2+\sqrt{3}n+1$ and this is the case. Hence $x=\pm 1$ and $y=\pm(n-\omega)$ are shortest vectors of a_0. Since $xx^*=(1,1)$ and $yy^*=((n-\omega)^2,(n+\omega)^2)\in \mathsf{k}_{\mathbf{R}}^+$ are linearly independent, a_0 is o_k-perfect. From $S(a_0)\cap S(\tau(a_0))=\{\pm 1\}$ and Lemma 2.3, it follows that a_0 and $\tau(a_0)$ are adjacent each other. Such an o_k-perfect form must be minimal.

(2) The integer d is bounded as $4n^2-8n+7<d<4n^2+3$. For $x=x_1+x_2\omega\in \mathsf{o}_\mathsf{k}$, (a_0,xx^*) equals

$$\begin{aligned}&\frac{1}{16(2n-1)^2}\{4(2n-1)x_1+(4n^2+d-5)x_2\}^2\\ +&\frac{1}{16(2n-1)^2}\{8(2n-1)(2n^2+dn-n-2)-(4n^2+d-5)^2\}x_2^2.\end{aligned}$$

If $x_2=0$, then $(a_0,xx^*)\geq 1$ and the equality holds for $x=\pm 1$. If $|x_2|=1$, then we may assume $x_2=-1$. Then we have $(a_0,xx^*)\geq 1$ since

$$(a_0,(x_1-\omega)(x_1-\omega)^*)-1=(x_1-n)\{2(2n-1)x_1-(2n+d-5)\}/2(2n-1)$$

and $n-1<(2n+d-5)/2(2n-1)<n+1$. The equality holds for $x=\pm(n-\omega)$. If $|x_2|\geq 2$, then we have

$$\begin{aligned}&\{8(2n-1)(2n^2+dn-n-2)-(4n^2+d-5)^2\}x_2^2-16(2n-1)^2\\ \geq&4\{8(2n-1)(2n^2+dn-n-2)-(4n^2+d-5)^2\}-16(2n-1)^2\\ =&-4\{d^2-2(4n^2-4n+5)d+16n^4-32n^3+8n^2+8n+13\}.\end{aligned}$$

This polynomial is positive if $4n^2-4n+5-2(2n-1)\sqrt{3}<d<4n^2-4n+5+2(2n-1)\sqrt{3}$ and this is the case. Hence $x=\pm 1$ and $y=\pm(n-\omega)$ are shortest vectors of a_0. This implies that a_0 is o_k-perfect and $\tau(a_0)$ is the minimal o_k-perfect form. □

By Propositon 5.6 and Lemma 5.2, we can easily determine whether $t_\mathsf{k}=1$ or not for a given k.

Example. When $d\leq 10000$ and $d\equiv 2,3 \mod 4$, there are 77 d such that $t_\mathsf{k}=1$. These are given by
2, 3, 10, 15, 26, 35, 82, 122, 143, 170, 195, 226, 255, 290, 323, 362, 399, 442, 483, 530, 626, 730, 842, 899, 962, 1023, 1090, 1155, 1226, 1295, 1370, 1443, 1522, 1599, 1763, 2026, 2210, 2402, 2602, 2703, 2810, 2915, 3026, 3135, 3363, 3482, 3599, 3722, 3970, 4226, 4355, 4490, 4623, 4762, 4899, 5042, 5183, 5330, 5626, 5930, 6083, 6242, 6562, 6890, 7055, 7226, 7395, 7570, 7743, 7922, 8099, 8282, 8463, 8835, 9026, 9215, 9410.

Example. When $d\leq 10000$ and $d\equiv 1 \mod 4$, there are 77 d such that $t_\mathsf{k}=1$. These are given by
5, 13, 21, 29, 53, 77, 85, 165, 173, 221, 229, 285, 293, 357, 365, 437, 445, 533, 629, 733, 957, 965, 1085, 1093, 1221, 1229, 1365, 1373, 1517, 1677, 1685, 1853, 2021, 2029, 2213, 2397, 2405, 2605, 2805, 2813, 3021, 3029, 3245, 3253, 3477, 3485, 3965, 3973, 4229, 4485, 4493, 4757, 4765, 5037, 5045, 5333, 5621, 5629, 5933, 6245, 6557, 6565, 6893, 7221, 7229, 7565, 7573, 7917, 8277, 8285, 8645, 8653, 9021, 9029, 9413, 9797, 9805.

These examples lead us to the following question.

Question. Are there infinitely many real quadratic fields k such that $t_\mathsf{k}=1$?

If $t_\mathsf{k}=1$, we have a simple description of the fundamental unit ϵ^{-1}.

Proposition 5.7. *Let n be the same as above. Then $t_{\mathsf{k}} = 1$ if and only if $\epsilon^{-1} = n - \tau(\omega)$.*

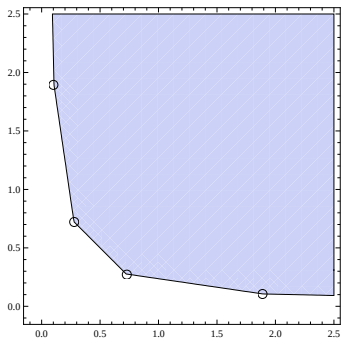
Proof. Let a_0 be the same as in Proposition 5.6. Assume $t_{\mathsf{k}} = 1$. From $\epsilon^2 a_0 = \tau(a_0)$, it follows $\epsilon^{-1} S(a_0) = S(\tau(a))$. Therefore, ϵ^{-1} must be equal to $n - \tau(\omega)$ since $\epsilon^{-1} > 1$ and $n - \tau(\omega) > 1$. Conversely, assume $\epsilon^{-1} = n - \tau(\omega)$. Then one has $S(\epsilon^2 a_0) = \epsilon^{-1} S(a_0) = S(\tau(a_0))$. Since any perfect form a is uniquely determined by $\mathsf{m}(a)$ and $S(a)$, we get $\epsilon^2 a_0 = \tau(a_0)$. □

We give some examples of $K_1(\mathsf{m})$.

Example. The case of $d = 5$. In this case, $t_{\mathsf{k}} = 1$ and the minimal o_{k}-perfect form is

$$a = \left(\frac{1}{2} - \frac{\sqrt{5}}{10}, \frac{1}{2} + \frac{\sqrt{5}}{10} \right).$$

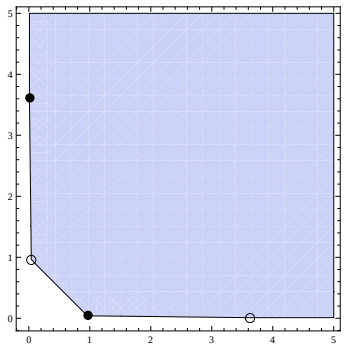
The Ryshkov domain $K_1(\mathsf{m})$ is of the following form.



Example. The case of $d = 6$. In this case, $t_{\mathsf{k}} = 2$ and the minimal o_{k}-perfect form is

$$a = \left(\frac{1}{2} - \frac{3\sqrt{6}}{16}, \frac{1}{2} + \frac{3\sqrt{6}}{16} \right).$$

An inequivalent o_{k}-perfect form is $\tau(a)$. The Ryshkov domain $K_1(\mathsf{m})$ is of the following form.



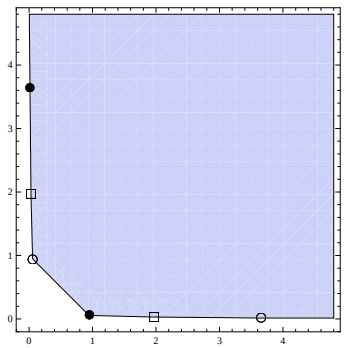
Example. The case of $d = 17$. In this case, $t_{\mathsf{k}} = 3$ and the minimal o_{k}-perfect form is

$$a = \left(\frac{1}{2} - \frac{11\sqrt{17}}{102}, \frac{1}{2} + \frac{11\sqrt{17}}{102}\right).$$

Vertices adjacent to a are $\tau(a)$ and

$$b = \left(1 - \frac{4\sqrt{17}}{17}, 1 + \frac{4\sqrt{17}}{17}\right).$$

Representatives of $E^2_{\mathsf{k}} \backslash \partial^0 K_1(\mathsf{m})$ is given by $\{a, \tau(a), b\}$.



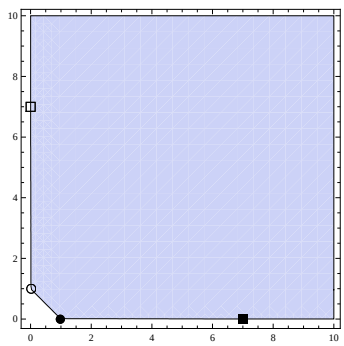
Example. The case of $d = 19$. In this case, $t_{\mathsf{k}} = 4$ and the minimal o_{k}-perfect form is

$$a = \left(\frac{1}{2} - \frac{17\sqrt{19}}{152}, \frac{1}{2} + \frac{17\sqrt{19}}{152}\right).$$

Vertices adjacent to a are $\tau(a)$ and

$$b = \left(\frac{7}{2} - \frac{61\sqrt{19}}{76}, \frac{7}{2} + \frac{61\sqrt{19}}{76}\right).$$

Representatives of $E^2_{\mathsf{k}} \backslash \partial^0 K_1(\mathsf{m})$ is given by $\{a, \tau(a), b, \tau(b)\}$.



We do not know whether t_{k} has a bound or not when k runs over all real quadratic fields.

References

[1] O. Güler, *Foundations of Optimization*, Graduate Texts in Mathemmatics 258, Springer Verlag, 2010.

[2] P. E. Gunnells, *Modular symbols for* $\mathbf{Q}$*-rank one groups and Voronoï reduction*, J. Number Theory **75** (1999), 198–219.

[3] P. E. Gunnells and D. Yasaki, *Perfect forms over totally real number fields*, preprint.

[4] D.-O. Jacquet-Chiffelle, *Énumération complète des classes de formes parfaites en dimension 7*, Ann. l'institute Fourier **43** (1993), 21–55.

[5] M. Köcher, *Beiträge zu einer Reductionstheorie in Positivitätsbereichen. I*, Math. Ann. **141** (1960), 384 – 432.

[6] A. Leibak, *On additive generalization of Voronoï's theory to algebraic number fields*. Proc. Estonian Acad. Sci. Phys. Math. **54** (2005), no.4,195–211.

[7] J. Martinet, *Perfect Lattices in Euclidean Spaces*. Grundlehren der Mathematischen Wissenschaften, Springer Verlag, 2003.

[8] J. Neukirch, *Algebraische Zahlentheorie*, Grundlehren der Mathematischen Wissenschaften, Springer Verlag, 1992.

[9] K. Okuda and S. Yano, *A generalization of Voronoï's theorem to algebraic lattices*, J. Th. Nombre de Bordeaux **22** (2010), 727 – 740.

[10] H. E. Ong, *Perfect quadratic forms over real-quadratic number fields*, Geom. Dedicata **20** (1986), no.1, 51–77.

[11] J. Opgenorth, *Dual cones and the Voronoi algorithm*, Experimental Math. **10** (2001), 599 - 608.

[12] S. S. Ryshkov, *The polyhedron* $\mu(m)$ *and some extremal problems of the geomety of numbers*, Soviet Math. Dokl. **11** (1970), 1240–1244.

[13] M. D. Sikirić, A. Schürmann and F. Vallentin, *A Generalization of Voronoi's reduction theory and its application*, Duke Math. J. **142** (2008), 127–164.

[14] A. Schürmann, *Computational Geometry of Positive Definite Quadratic Forms*, University Lecture Series 48, Amer. Math. Soc., 2008.

[15] T. Shintani, *On evaluation of zeta functions of totally real algebraic number fields at non-positive integers*, J. Fac. Sci. Univ. Tokkyo **23** (1976), 393–417.

[16] G. Voronoï, *Nouvelles applications des paramétres coninus á la théorie des formes quadratiques, premier mémoire. Sur quelques propriétés des formes quadratiques positives parfaites*, J. reine angew. Math. **133** (1908), 97–178.

[17] T. Watanabe, *A survey on Voronoï's theorem*, in "Geometry and Analysis of Automorphic Forms of Several Variables" edited by Hamahata, Ichikawa, Murase and Sugano, Series on Number Theory and Its Applications, Vol. 7, World Scientific, 2011.

Graduate School of Science, Osaka University, Toyonaka, Osaka 560-0043, Japan
E-mail address: twatanabe@math.sci.osaka-u.ac.jp; yn.showg@gmail.com