

On an effective determination of Shintani's decomposition of the cone R_t

岡崎龍太郎

新制
理
792
京大附図

学位申請論文

岡崎龍太郎

On an effective determination of Shintani's decomposition of the cone $\mathbf{R}_+^n$

Ryotaro Okazaki

September 24, 1992

1. Introduction

1.1. Problem

Let K be a totally real algebraic number field of degree $n \geq 2$, o_K the ring of integers of K , o_K^+ the set of all totally positive elements of o_K , E_K^+ the totally positive unit group of K and φ_i for $i = 1, 2, \dots, n$ the distinct embeddings of K into $\mathbf{R}$. We embed K into $\mathbf{R}^n$ (considered as vectors) by identifying each element α of K with ${}^t(\varphi_1(\alpha), \varphi_2(\alpha), \dots, \varphi_n(\alpha))$. Then, the group E_K^+ acts on the cone $\mathbf{R}_+^n$ by componentwise multiplication. Further, we define the open polyhedral cone $C(v_1, v_2, \dots, v_r)$ generated by $v_1, v_2, \dots, v_r$ to be

$$C(v_1, v_2, \dots, v_r) = \mathbf{R}_+ v_1 + \mathbf{R}_+ v_2 + \dots + \mathbf{R}_+ v_r \quad (1)$$

for $v_1, v_2, \dots, v_r \in \mathbf{R}_+^n$. An open polyhedral cone $C(v_1, v_2, \dots, v_r)$ is called an open simplicial cone of rank r if $v_1, v_2, \dots, v_r$ are linearly independent. Shintani [3] proved a theorem which insists that there is a fundamental domain D of form

$$D = \bigcup_{j \in J} C(v_{j1}, v_{j2}, \dots, v_{jr(j)}) \quad (\text{disjoint}) \quad (2)$$

for the action of E_K^+ on $\mathbf{R}_+^n$, where J is a finite index set, $r(j)$ is an integer depending on j such that $1 \leq r(j) \leq n$ and $v_{jk} \in o_K^+$ (in the sense K is embedded into $\mathbf{R}^n$) such that $v_{j1}, v_{j2}, \dots, v_{jr(j)}$ are linearly independent. Although his proof is effective, there remains a gap between this theorem and

actual determination of a fundamental domain so that fundamental domains are known only for real quadratic fields [3] and totally real cubic fields [4]. The purpose of this paper is to describe an applicable and effective method for determining a fundamental domain of form (2) in the case of number fields of higher degree.

1.2. Main Result and Method

To this aim, we have developped a method which can be thought of as a generalization of Hirzebruch's continued fraction expansion working in the case of real quadratic fields (see [3]). The Hirzebruch's continued fraction expansion is a computation of a sequence of adjacent integers on the boundary of the convex hull of the set of all quadratic integers in $\mathbf{R}_+^2$. Thus, we firstly study the structure of the boundary of the convex hull of the set $\mathcal{O}_K^+$ in Theorem 8. We will find a notion of adjacency between hyperpolyhedras on the boundary. This adjacency between hyperpolyhedras can be considered as a generalization of adjacency between integers in the case of quadratic fields, because two integers are adjacent if and only if the two edges, which are to the "right" of those integers, are adjacent. Secondly, we will construct a fundamental domain for the action of E_K^+ on $\mathbf{R}_+^n$ by an effective method in Theorem 11. We note that our construction works without knowing generators of the unit group beforehand, and also gives generators of the totally positive unit group as a side effect. Therefore, our construction can be also viewed as an algorithm for determining the totally positive unit group of a totally real number field. In this sense, our method can be thought of as a "positive" version of the generalized Lagrange algorithm of Buchmann [1]. The following modification of the Buchmann's algorithm makes the similarity to our method clearer although it is slower than the original graph theoretic version: attach an abstract simplex to each minimal subset, consider elements of a minimal set as vertices of the simplex, construct a suitable complex, compute a non-associated maximal connected family of simplices on that complex and then one has enough information of the unit group.

2. Preparation

We will give some notations and terminologies which will be used in this paper together with those introduced in §1 and we also recall some basic facts. We note that some terminologies differ from standard ones for the sake of simplicity of the argument on the topic dealt here.

2.1. Unit Theorem

We use the Dirichlet's unit theorem in the following form:

Proposition 1. *The totally positive unit group E_K^+ of K has the following properties.*

- (i) *Let k be an integer such that $1 \leq k \leq n$. Then, there is a unit $\epsilon_k \in E_K^+$ such that*

$$\begin{cases} 0 < \varphi_i(\epsilon_k) < 1 & \text{for } i \neq k, \\ 1 < \varphi_k(\epsilon_k). \end{cases} \quad (3)$$

- (ii) *The group E_K^+ acts on $\mathbf{R}_+^n/\mathbf{R}_+$ and has a fundamental domain whose topological closure is compact in the natural topology.*

2.2. Convex Sets

A subset B of $\mathbf{R}^n$ is called convex if the segment connecting arbitrary two points of B is contained in B . The convex hull B of a set S is the smallest convex set containing S , i.e., the set of all points of form $t_1 p_1 + t_2 p_2 + \cdots + t_r p_r$ with a positive integer r , positive real numbers $t_1, t_2, \dots, t_r$ such that $t_1 + t_2 + \cdots + t_r = 1$ and points $p_1, p_2, \dots, p_r$ of S . A hyperplane π is called a support hyperplane of a convex set B provided

- (i) The hyperplane π contains a boundary point of B and
- (ii) π divides $\mathbf{R}^n$ into the disjoint union of a closed half-space which completely contains B and an open half-space which is disjoint with B .

The following fact is well known.

Proposition 2. *Let p be a boundary point of a convex set B in $\mathbf{R}^n$. Then, there exists a support hyperplane π of B containing the point p .*

2.3. Faces

We denote by $\overline{B}$ the topological closure of a set B in $\mathbb{R}^n$. Let B be a convex set. Then, the intersection F of the set $\overline{B}$ and a support hyperplane of B is called a face of B .

Definition 3. Let B be a convex set in $\mathbb{R}^n$. Then a face P of B is called a hyperface of B if the dimension of P is $n - 1$. and a face E of B is called a hyperedge of B if the dimension of E is $n - 2$.

Definition 4. Two distinct hyperfaces P and P' of a convex set of the dimension n are called adjacent at a hyperedge E if P and P' contain E .

Clearly, any hyperface can have at most one hyperface adjacent at a single hyperedge.

Definition 5. A family $\mathcal{F}$ of hyperfaces of a convex set is called connected if an arbitrary pair of distinct hyperfaces $P, P' \in \mathcal{F}$ has a sequence $P = P_1, P_2, \dots, P_k = P'$ of hyperfaces in $\mathcal{F}$ such that P_i and P_{i+1} are adjacent for $i = 1, 2, \dots, k - 1$.

Let $p_1, p_2, \dots, p_r$ be points in $\mathbb{R}^n$. Then we denote by $P(p_1, p_2, \dots, p_r)$ the convex hull of $p_1, p_2, \dots, p_r$. If the set $P(p_1, p_2, \dots, p_r)$ has the dimension $n - 1$, it is called a convex hyperpolyhedra. In this case, we denote by $\pi(p_1, p_2, \dots, p_r)$ the unique hypeplane containing points $p_1, p_2, \dots, p_r$. We finish this section by defining the notion of open faces.

Definition 6. Let $P = P(p_1, p_2, \dots, p_r)$ be a face of a convex set B . Then, the set $P^\circ = P^\circ(p_1, p_2, \dots, p_r)$ is defined by

- (i) $P^\circ = P$ if P has the dimension 0 or
- (ii) $P^\circ = \{\sum_{i=1}^r t_i p_i \mid t_1, t_2, \dots, t_r \in \mathbb{R}_+, \sum_{i=1}^r t_i = 1\}$ otherwise.

The set P° is called an open hyperface spanned by $p_1, p_2, \dots, p_r$.

3. Theorems

3.1. The Family of Hyperfaces

Let A be a finite set of points in $\mathbf{R}_+^n$, S_A the union $o_K^+ \cup A$, B_A the convex hull of S , Δ_A the boundary set of B_A and $\mathcal{D}_A$ the family of all hyperfaces of B_A . The set A is called an auxiliary set and its elements are called auxiliary points for the reason which will be stated before Theorem 15. We omit the subscript A when the set A is empty. For brevity, elements of S_A are called S_A -points.

The following lemma is fundamental:

Lemma 7. *Let π be a support hyperplane of B_A . Then, the hyperplane π has an equation of the form*

$$c_1x_1 + c_2x_2 + \cdots + c_nx_n = 1 \quad (4)$$

where $c_1, c_2, \dots, c_n > 0$. Moreover, B_A is contained in the closed half-space

$$c_1x_1 + c_2x_2 + \cdots + c_nx_n \geq 1. \quad (5)$$

This further implies that there are at most finitely many S_A -points on any segment on Δ_A .

Proof of Lemma 7. Let N be the map defined by

$$N : {}^t(x_1, x_2, \dots, x_n) \in \mathbf{R}_+^n \longmapsto x_1x_2 \cdots x_n \in \mathbf{R}_+ \quad (6)$$

and set $a = \min(N(A) \cup o_K^+) = \min(N(A) \cup \{1\}) > 0$. Then, the set S_A is contained in the convex set

$$x_1x_2 \cdots x_n \geq a. \quad (7)$$

This implies that all boundary points of B_A and, in particular, a point $p = (p_1, p_2, \dots, p_n)$ on π are contained in $\mathbf{R}_+^n$. Write the equation of π :

$$c_1x_1 + c_2x_2 + \cdots + c_nx_n = c \quad (8)$$

and assume that the set B_A is contained in the half-space

$$c_1x_1 + c_2x_2 + \cdots + c_nx_n \geq c. \quad (9)$$

On the other hand, one has a unit ϵ_k for $1 \leq k \leq n$ as stated in Proposition 1. Applying inequality (9) to sufficiently high power of ϵ_k , one sees that c_k 's are non-negative and that $c \leq 0$ if one of c_k 's is zero. However, applying equation (8) to the point $p \in \mathbf{R}_+^n$ mentioned after (7), one has that

$$c_1 p_1 + c_2 p_2 + \cdots + c_n p_n = c. \quad (10)$$

One sees that c is positive because some of c_k 's must be non-zero. Therefore, all of c_k 's and c are positive. One gets the desired form of equation by dividing coefficients of equation (8) by c . The last assertion is proved by observing that the support hyperplane π of B_A at the middle point of a segment σ has the form (4) and that π contains σ . ■

Using this lemma, we describe the structure of B_A as follows:

Theorem 8. *The set B_A , Δ_A and $\mathcal{D}_A$ have the following properties:*

- (i) *the set B_A is a closed set in $\mathbf{R}^n$ and each face of B_A is of the form $P(p_1, p_2, \dots, p_r)$ with S_A -points $p_1, p_2, \dots, p_r$;*
- (ii) *there are at most finitely many faces of B_A intersecting a given bounded set;*
- (iii) *the set Δ_A is a union of all hyperfaces of B_A ;*
- (iv) *the set Δ_A forms a system of representatives for $\mathbf{R}_+^n/\mathbf{R}_+$;*
- (v) *there are exactly two hyperfaces containing a given hyperedge;*
- (vi) *the family $\mathcal{D}_A$ is connected and*
- (vii) *the set Δ_A is uniquely decomposed into a union of all open faces of B_A .*

Proof of Theorem 8. Let p be a boundary point of B_A . Then, there is a support hyperplane π containing p of the form (4) by Proposition 2 and Lemma 7. We denote by π_t the hyperplane defined by

$$c_1 x_1 + c_2 x_2 + \cdots + c_n x_n = 1 + t \quad (11)$$

Clearly, one can find a small positive real number t such that the set

$$1 < c_1 x_1 + c_2 x_2 + \cdots + c_n x_n < 1 + t \quad (12)$$

does not contain S_A -points because the hyperplane π_i together with all of coordinate hyperplanes enclose a bounded set. Let $p_1, p_2, \dots, p_r$ be all of S_A -points on π and P the convex set $P = P(p_1, p_2, \dots, p_r)$. Assertion (i) follows if one shows $p \in P$. Take an arbitrary point p' in B_A which is close to p . Then, p' can be written as

$$p' = t_1 p_1 + t_2 p_2 + \dots + t_r p_r + t_{r+1} p_{r+1} + \dots + t_{r'} p_{r'} \quad (13)$$

where $p_{r+1}, p_{r+2}, \dots, p_{r'}$ are S_A -points outside π and $t_1, t_2, \dots, t_{r'}$ are non-negative real numbers such that $t_1 + t_2 + \dots + t_{r'} = 1$. From this, one sees that there are positive real numbers s, s' , a point q on P and a point q' in the opposite side of the hyperplane π_i to the origin such that $p' = sq + sq'$. This further implies that p' is on the segment connecting a point on P and a point on $\pi_i \cap \mathbf{R}_+^n$. Hence, the point p' is in $M = P(p_1, p_2, \dots, p_r, q_1, q_2, \dots, q_n)$ where q_i is the intersection of π_i and the i -th axis. Now, one has that p is in M , since p' can be chosen arbitrary close to p . It is, however, obvious that M is closed and that the intersection $\pi \cap M$ is P . This implies that p is in fact on P , proving assertion (i).

Let M be a bounded set. We assume, without loss of generality, that M is of the form

$$M = \{^t(x_1, x_2, \dots, x_n) \in \mathbf{R}_+^n \mid x_1 + x_2 + \dots + x_n < m\} \quad (14)$$

where m is a positive integer. Let P be a hyperface of B_A intersecting M . Then, by assertion (i), P can be written as $P = P(p_1, p_2, \dots, p_r)$ with S_A -points $p_1, p_2, \dots, p_r$. The assumption on the shape of M guarantees that at least one of p_i 's, say $p = p_1$, is contained in M . There are at most finitely many such p 's since M is bounded. Observe that the segments $P(p, p_i)$ are on Δ_A and one sees that assertion (ii) follows if one shows that there are at most finitely many S_A -points q 's such that segments $P(p, q)$'s are on Δ_A . Suppose contrary, that there are infinitely many such q 's. Draw a small sphere Σ at p and look at the set of intersections of $P(p, q)$'s and that sphere. Then, there is an accumulating point p_∞ on Σ of those intersection points since Lemma 7 guarantees that there are at most finitely many S_A -points on a segment in Δ_A . By Proposition 2, there is a support hyperplane π of B_A containing p_∞ of the form (4). Let $c' > 1$ be a constant such that the hyperplane π' defined by

$$c_1 x_1 + c_2 x_2 + \dots + c_n x_n = c' \quad (15)$$

does not intersect Σ . When q is in the opposite side of π' to the origin, the intersection of $P(p, q)$ and Σ is in the set $P(p, q'_1, q'_2, \dots, q'_n)$ where q'_i is the intersection of π' and the i -th axis. On the other hand there are finitely many S_A points in the region

$$c_1x_1 + c_2x_2 + \dots + c_nx_n \leq c'. \quad (16)$$

Thus, p_∞ must contact $P(p, q'_1, q'_2, \dots, q'_n)$. This together with the definition of π' implies that p and q must coincide. But q must differ p by the radius of Σ . This contradiction proves assertion (ii). Assertion (iii) follows from assertion (i), (ii) and that Δ_A has the dimension $n - 1$. Assertion (iv) follows from Lemma 7. Assertion (v) follows from assertion (i) and (ii). Assertion (iv) guarantees that given pair of points on Δ_A can be connected by a path γ on Δ_A which does not intersect any face of dimension lower than $n - 2$ except at the given initial and terminal points. Applying this statement to the barycenters of given hyperfaces P and P' , one sees that there is a sequence $P_1 = P, P_2, \dots, P_k = P'$ such that successive pair P_i and P_{i+1} are adjacent by taking as P_i 's the hyperfaces through which the path γ goes in order. Assertion (vi) is proved. Assertion (vii) is obvious. ■

On the other hand, we have the obvious action of E_K^+ on the family of subsets of $\mathbf{R}_+^n$ defined by $e \in E_K^+$: $G \subset \mathbf{R}_+^n \mapsto eG = \{ep \mid p \in G\}$. Two subsets G and G' of $\mathbf{R}_+^n$ are called associated if there is a unit e in E_K^+ such that $G = eG'$, and a family $\mathcal{F}$ of subsets of $\mathbf{R}^n$ is called non-associated if no pair of distinct sets from $\mathcal{F}$ are associated. When the auxiliary set is empty, the group E_K^+ acts on $B = B_\phi$, on $\Delta = \Delta_\phi$ and on the family of all support hyperplanes of B . Thus, The group E_K^+ also acts on the family $\mathcal{D} = \mathcal{D}_\phi$. This action has the following properties:

Theorem 9. *Assume that the auxiliary set A is empty. Then, one firstly has that $\mathcal{D}$ decomposes into finitely many E_K^+ -orbits. Secondly, let $\mathcal{M}$ be a maximal connected non-associated family of hyperfaces of B . Then, $\mathcal{M}$ is finite and is a system of representatives for the action of E_K^+ . Lastly, let $\mathcal{E}$ be the family of all hyperedges contained in exactly one hyperface in $\mathcal{M}$. Then, there is exactly one unit $\epsilon(E) \neq 1$ in E_K^+ such that $\epsilon(E)E \in \mathcal{E}$. The group E_K^+ is generated by those units $\{\epsilon(E) \mid E \in \mathcal{E}\}$.*

Proof of Theorem 9. By assertion (iv) of Theorem 8, Δ is thought of as $\mathbf{R}_+^n/\mathbf{R}_+$. Proposition 1 says that there is a compact closure D_0 of a

fundamental domain of the action of E_K^+ on the set Δ . Let $\mathcal{M}_0$ be the family of all hyperfaces which intersect D_0 . Then, the family $\mathcal{M}_0$ is finite by assertion (ii) of Theorem 8. This implies that any non-associated family of hyperfaces is finite, i.e., Δ decomposes into finitely many E_K^+ -orbits. Thus, the first assertion is proved. Now, it is clear that there is a maximal connected non-associated family $\mathcal{M}$. The family $\mathcal{M}$ is finite by the first assertion. To see that $\mathcal{M}$ is a system of representatives, we pick up an arbitrary hyperface P from $\mathcal{D}$ and a hyperface P' from $\mathcal{M}$. Assertion (vi) of Theorem 8 guarantees the existence of a sequence $P_1 = P, P_2, \dots, P_k = P'$ in which successive hyperfaces are adjacent. We will shorten this sequence by substituting P_1 by an associated hyperface while $k > 1$ as follows. Firstly, we substitute P' by P_{k-1} if P_{k-1} belongs to $\mathcal{M}$. If this is not the case, there must be the associated hyperface P'' of P_{k-1} in $\mathcal{M}$ from the maximality of $\mathcal{M}$. Let ϵ be the unit which transfers P_{k-1} to P'' . We substitute P by ϵP , P' by P'' and the sequence $P_1, P_2, \dots, P_k$ by the sequence $\epsilon P_1, \epsilon P_2, \dots, \epsilon P_{k-1}$. We obviously get a shorter sequence in either case. Repeating these procedures, we will finally reach to a sequence of length 1, i.e., the associated hyperface in $\mathcal{M}$ of the original P . This proves that the family $\mathcal{M}$ is system of representatives. This argument also proves the last assertion except the uniqueness of $\epsilon(E)$. Let E be a hyperedge in $\mathcal{E}$ and assume that a unit $\epsilon \in E_K^+$ carries E to a hyperface ϵE which also belongs to $\mathcal{E}$. Further, let P be the hyperface in $\mathcal{M}$ containing E and P' the hyperface in $\mathcal{M}$ containing ϵE . Then, $\epsilon^{-1}P'$ must be the adjacent hyperface to P at E . Thus, the hyperface P' is determined as the unique representative in $\mathcal{M}$ of the orbit of the adjacent hyperface of P at E . Therefore, the condition $\epsilon E \in \mathcal{E}$ uniquely determines the unit $\epsilon(E) = \epsilon$. $\blacksquare$

In fact, Theorem 9 is the key to the construction of a fundamental domain for the action of E_K^+ on $\mathbf{R}_+^n$ as follows:

Theorem 10. *Let $\mathcal{M}$ be a maximal connected non-associated family of hyperfaces of B , D_1 the union of all hyperfaces in $\mathcal{M}$ and $\mathcal{M}^\circ$ the family of all open faces contained in D_1 . Then, one can find a subfamily $\mathcal{M}_0^\circ$ of $\mathcal{M}^\circ$ such that the union*

$$D_0 = \bigcup_{F \in \mathcal{M}_0^\circ} F \quad (\text{disjoint}) \quad (17)$$

is a fundamental domain for the action of E_K^+ on Δ . Moreover, one has the

fundamental domain D for the action of E_K^+ on $\mathbf{R}_+^n$ defined by

$$D = \mathbf{R}_+ D_0 \quad (18)$$

$$= \bigcup_{F \in \mathcal{M}_0^o} \mathbf{R}_+ F \quad (\text{disjoint}) \quad (19)$$

where, $\mathbf{R}_+ F$'s are open polyhedral cones. The fundamental domain D has a decomposition into a disjoint union of open simplicial cones.

Proof of Theorem 10. The theorem follows from Theorem 8 and 9. ■

3.2. Effectivity

For speaking on the effectivity, we assume that a generator α of K over $\mathbf{Q}$ is given by its minimal equation, that a basis $\beta_1 = 1, \beta_2, \dots, \beta_n$ of the integral ring of integers is given by a set polynomials in α and that the following operations are effective:

- (i) the basic operations of real numbers to the desired precision (i.e. addition, subtraction, multiplication and division),
- (ii) the exact basic operations of algebraic integers (i.e. addition, subtraction, multiplication, test for divisibility and division in the divisible case.)

Now, we present the following algorithm for finding a fundamental domain and later fill in the details of that algorithm.

Theorem 11. *The following algorithm effectively leads to a fundamental domain D for the action of E_K^+ on $\mathbf{R}_+^n$:*

- *Firstly, find out one particular hyperface of B by the method to be described in Proposition 15.*
- *Secondly, using the method to be described in Proposition 14, successively search for adjacent hyperfaces which are adjacent to one of hyperfaces so far found and associated to none of hyperfaces so far found. We surely reaches to a maximal connected non-associated family $\mathcal{M}$ of hyperfaces in finite steps.*

–

- Thirdly, divide the hyperfaces (found in the second step) into open faces, then select maximal non-associated family of faces from those.
- Lastly, we divide the faces (found in the third step) into open simplices to find a family $\mathcal{S}$ of simplices on Δ spanned by o_K^+ -points. Now, the union $D = \bigcup_{\sigma \in \mathcal{S}} \mathbf{R}_+ \sigma$ is the desired form of a fundamental domain.

Furthermore, let $\mathcal{E}$ be the family of all hyperedges which are contained in exactly one hyperface of $\mathcal{M}$. Then, there exists exactly one unit $\epsilon(E) \neq 1$ of K such that $\epsilon(E)E$ belongs to $\mathcal{E}$, and the totally positive unit group E_K^+ is generated by $\{\epsilon(E) \mid E \in \mathcal{E}\}$.

Proof of Theorem 11. The effectivity of the first and the second steps will be proved by Propositions 14, 15 and the fact that non-associatedness of hyperfaces can be checked by computing quotients of their vertices. The third and fourth steps are no doubt effective. Therefore, Theorems 9 and 10 guarantee that the repetition in the second step terminates and that the set D is a fundamental domain for the action of E_K^+ on $\mathbf{R}_+^n$. We note that the faces found in the third step are not always simplices so that the last step is necessary. The second assertion is a part of Theorem 9. ■

Lemma 12. *Let $P = P(p_1, p_2, \dots, p_r)$ be a hyperface of B_A and assume that vectors $p_1, p_2, \dots, p_n$ are linearly independent. Then, points $p_1, p_2, \dots, p_{n-1}$ are contained in a hyperedge of B_A if and only if all determinants $|p_1, p_2, \dots, p_{n-1}, p_i|$ for $i = n, n+1, \dots, r$ are simultaneously non-negative or non-positive. Moreover, if $p_1, p_2, \dots, p_{n-1}$ are contained in a hyperedge E , then one has that $E = P(p_{\ell(1)}, p_{\ell(2)}, \dots, p_{\ell(r)})$ where $\ell(i)$'s are all of indices such that the determinants $|p_1, p_2, \dots, p_{n-1}, p_{\ell(i)}| = 0$.*

Proof of Lemma 12. We note that r must be greater than or equal to n for P to be a hyperface. The proof of this lemma is obvious and therefore is omitted. ■

Let $p_1, p_2, \dots, p_n$ be linearly independent vectors in $\mathbf{R}_+^n$. We denote by $\pi_t = \pi_t(p_1; p_2, \dots, p_n)$ the hyperplane containing $tp_1, p_2, p_3, \dots, p_n$. When π_t does not pass through the origin, we denote by $\mathbf{c}_t = \mathbf{c}_t(p_1; p_2, \dots, p_n)$ the normal vector of π_t such that $\pi_t = \{p \in \mathbf{R}^n \mid (\mathbf{c}_t, p) = 1\}$. When $\mathbf{c}_t$ consists of positive entries, we denote by $t_\infty = t_\infty(p_1; p_2, \dots, p_n)$ the real number $\inf \{t \in \mathbf{R}_+ \mid \mathbf{c}_t \in \mathbf{R}_+^n\}$. We also denote by $k(p_1; p_2, \dots, p_n)$ the index

$\min \{i \mid i\text{-th entry of } \mathbf{c}_{t_\infty} \text{ is zero}\}$. Well-definedness of these numbers are easily verified as follows. Let q_i be the intersection of π_t and the i -th axis for $i = 1, 2, \dots, n$. Then, q_i 's approach to the origin as t goes to 0. But π_t contains a point p_2 . Thus, the coordinate of one of q_i 's, say, q_k , becomes negative at a small t , for otherwise $p_2 \in \mathbf{R}_+^n$ must be arbitrary close to the origin. This implies that the coordinate of q_k becomes 0 or q_k diverges at certain t before q_k has a negative coordinate since coordinate of q_k is written as a linear fractional function of t . However, the q_k can't be the origin except at $t = 0$. Therefore, q_k diverges at certain t such that $0 < t < 1$. It is clear, that $\mathbf{c}_k$ becomes zero at this point. Well-definedness of t_∞ and $k(p_1; p_2, \dots, p_n)$ follows since there are finitely many indices k .

Lemma 13. *Let E be a hyperedge of B_A whose S_A -points are known, P a hyperface of B_A containing E , P' the hyperface adjacent to P at E , p_1 a point on P which is not on E , $p_2, p_3, \dots, p_n$ linearly independent points on E , p'_1 a vector in $\mathbf{R}^n$ whose entries are zero except the $k = k(p_1; p_2, \dots, p_n)$ -th entry is the inverse of the k -th entry of $\mathbf{c}_1(p_1; p_2, \dots, p_n)$ (i.e., the intersection of the k -th axis and $\pi(p_1, p_2, \dots, p_n)$) and $U_s = P(0, sp'_1, p_2, p_3, \dots, p_n)$ for real number $s > 1$. Then, U_s for sufficiently large s contains a point from S_A which does not belong to E . Moreover, one can effectively determine the minimum s_0 of such s and the set $V = S_A \cap \pi(s_0 p'_1, p_2, p_3, \dots, p_n)$ including a point q outside E provided that A consists of points of K . The set V spans the hyperface P' .*

Proof of Lemma 13. Proposition 1 says that there exists a unit $\epsilon \in E_K^+$ such that each component $\varphi_i(\epsilon)$ is less than 1 except $\varphi_k(\epsilon) > 1$. Taking sufficiently high power of ϵ , one finds an algebraic integer ϵ' which is very close to the k -th axis. It is clear, that ϵ' is contained in U_s for sufficiently large s . We proved the first assertion. The last assertion is clear. For the second assertion, we adopt the following algorithm which determines the minimum of s .

- Firstly, compute all integral points within U_s for $s = 2, 4, 8, \dots$ until an integral point in $U_s - E$ is found. Let s_1 be the second s such that $U_s - E$ is found to contain an integral point and $q_1, q_2, \dots, q_r$ all of integral point in $U_{s_1} - E$.
- Secondly, compute determinants

$$|q_j, p_2 - q_i, p_3 - q_i, \dots, p_n - q_i| \quad (20)$$

for $1 \leq i, j \leq r'$ to the absolute precision of $1/(4m^n)$ with $m \in \mathbb{Z}$ such that $mA \subset o_K$. Then, one finds a $q = q_\ell$ such that

$$|q_j, p_2 - q, p_3 - q, \dots, p_n - q| / |q_\ell, p_2 - q, p_3 - q, \dots, p_n - q| \quad (21)$$

is greater than or equal to 1 for $1 \leq j \leq r'$ (comparison should be done paying respect to the precision).

- Lastly, compute the intersection p_1'' of $\pi(q, p_2, p_3, \dots, p_n)$ and the k -th axis. Then, the number s_0 is the quotient of the k -th coordinates of p_1'' and p_1' . Moreover, the point $q \notin E$ is on the hyperplane $\pi(s_0 p_1', p_2, p_3, \dots, p_n)$ and the set V is the union of the S_A -point on E and the set of all q_j 's such that the quotient (21) equals to 1 (comparison are done paying respect to the precision).

The first assertion guarantees that this algorithm terminates. On the other hand, it is clear that this algorithm computes the desired result if computation could be exact. Thus, we only need to verify that the precision referred to in the second step is sufficient for obtaining the correct answer. Let d be the discriminant of K . Then, determinants $|q_j, p_2 - q_i, p_3 - q_i, \dots, p_n - q_i|$ are *a priori* known to be greater than or equal to $\sqrt{d}/m^n$. Therefore, the precision of $1/4m^n$ is sufficient. ■

A face F of B_A is said to be effectively determined if all of S_A -points on F is effectively determined.

Proposition 14. *Assume that the auxiliary set A consists of algebraic numbers of K . And let $P = P(p_1, p_2, \dots, p_r)$ be a hyperface of B_A whose S_A -points are known. Then, one can effectively list all hyperedges contained in P by computing determinants $|p_{\ell(1)}, p_{\ell(2)}, \dots, p_{\ell(n)}|$ for all possible injections $\ell : \{1, 2, \dots, n\} \longrightarrow \{1, 2, \dots, r\}$, as stated in Lemma 12.*

Let E be a hyperedge contained in P and P' the hyperface adjacent to P at E . And assume that $p_2, p_3, \dots, p_n$ are independent points on E and that p_1 is on $P - E$. Then, by Lemma 13, one can effectively determine P' .

Proof of Proposition 14. The proof is obvious. ■

To find one hyperface from which we can compute successive hyperfaces, we fake the method of Proposition 14 by adjoining auxiliary points to S to form a “known” hyperface.

Proposition 15. *One can effectively find a basis $\beta'_1 = 1, \beta'_2, \dots, \beta'_n$ of $\mathcal{o}_K$ consisting of totally positive integers. Set $\gamma_i = \beta'_i / \text{tr} \beta'_i$ for $1 \leq i \leq n$ and $A_i = \{\gamma_{i+1}, \gamma_{i+2}, \dots, \gamma_n\}$ for $0 \leq i \leq n$, (in particular, $A_n = \emptyset$.) Then, the set $P_1 = P(\gamma_1, \gamma_2, \dots, \gamma_n)$ is a hyperface of B_{A_1} such that $S_A \cap P_1 = A_0$. One can inductively and effectively define P_i 's which are hyperfaces of B_{A_i} 's as follows: One can effectively determine a hyperedge $E_i \subset P_i - \{\gamma_{i+1}\}$ by Lemma 12 and the adjacent hyperface P_{i+1} of P_i at E_i by Lemma 13. In particular, P_n is an effectively determined hyperface of B .*

Proof of Proposition 15. The first assertion is verified by recalling that each algebraic integer can be computed to the precision of $1/2$. The second assertion is proved by the fact that the hyperplane $\pi : x_1 + x_2 + \dots + x_n = n$ contacts the convex set $x_1 x_2 \dots x_n \geq 1$, which contains all totally positive integers, at $(1, 1, \dots, 1)$. The third and the fourth assertions are clear. ■

3.3. Example

For a demonstration of Theorems 9 and 11, we give the following example. Let ζ be a primitive 11-th root of unity, θ be the sum of ζ and its complex conjugate. Then θ has the minimal polynomial

$$X^5 + X^4 - 4X^3 - 3X^2 + 3X + 1.$$

We take the field $\mathbb{Q}(\theta)$ as K . Then, the field K is totally real number field of degree 5 and has the discriminant 14641. One can take

$$1, \theta, \theta^2, \theta^3, \theta^4$$

as a basis for $\mathcal{o}_K$. Computation shows that one can take $\mathcal{M}$ to be the family consisting of the following 9 hyperfaces:

$$\begin{aligned} &P(\alpha_1, \alpha_3, \alpha_5, \alpha_8, \alpha_{10}), \\ &P(\alpha_5, \alpha_9, \alpha_{10}, \alpha_{11}, \alpha_{12}), \\ &P(\alpha_1, \alpha_2, \alpha_3, \alpha_5, \alpha_8, \alpha_9), \\ &P(\alpha_1, \alpha_5, \alpha_8, \alpha_9, \alpha_{10}, \alpha_{16}), \\ &P(\alpha_2, \alpha_3, \alpha_5, \alpha_7, \alpha_8, \alpha_{10}), \\ &P(\alpha_5, \alpha_7, \alpha_{10}, \alpha_{13}, \alpha_{14}, \alpha_{18}), \\ &P(\alpha_8, \alpha_9, \alpha_{10}, \alpha_{12}, \alpha_{13}, \alpha_{19}), \\ &P(\alpha_8, \alpha_9, \alpha_{10}, \alpha_{15}, \alpha_{16}, \alpha_{17}), \\ &P(\alpha_2, \alpha_4, \alpha_5, \alpha_6, \alpha_7, \alpha_8, \alpha_9, \alpha_{10}, \alpha_{12}, \alpha_{13}) \end{aligned}$$

where α_i 's are given as follows:

$$\begin{aligned}
\alpha_1 &= -1 - 3\theta + 5\theta^2 + \theta^3 - \theta^4, \\
\alpha_2 &= -1 - 4\theta + \theta^2 + 5\theta^3 + 2\theta^4, \\
\alpha_3 &= -1 - 4\theta + 4\theta^2 + 3\theta^3, \\
\alpha_4 &= -2\theta - \theta^2 + 3\theta^3 + 2\theta^4, \\
\alpha_5 &= \theta^2, \\
\alpha_6 &= \theta^2 + 2\theta^3 + \theta^4, \\
\alpha_7 &= 2\theta^2 + \theta^3, \\
\alpha_8 &= 1 - 2\theta - \theta^2 + 2\theta^3 + \theta^4, \\
\alpha_9 &= 1 - 2\theta^2 + \theta^4, \\
\alpha_{10} &= 1, \\
\alpha_{11} &= 1 + \theta - 2\theta^2 - \theta^3 + \theta^4, \\
\alpha_{12} &= 1 + 2\theta - 2\theta^2 - \theta^3 + \theta^4, \\
\alpha_{13} &= 1 + 2\theta + \theta^2, \\
\alpha_{14} &= 1 + 5\theta + 6\theta^2 - 2\theta^3 - 2\theta^4, \\
\alpha_{15} &= 10 - 5\theta - 12\theta^2 + 2\theta^3 + 3\theta^4, \\
\alpha_{16} &= 2 - 3\theta + \theta^3, \\
\alpha_{17} &= 3 - 2\theta - 3\theta^2 + \theta^3 + \theta^4, \\
\alpha_{18} &= 3 + 11\theta + 5\theta^2 - 4\theta^3 - 2\theta^4, \\
\alpha_{19} &= 4 - 4\theta^2 + \theta^4.
\end{aligned}$$

It turns out that there are too many lower dimensional faces to list up here. Therefore, we only list association between hyperedges. Association between hyperedges within the family $\mathcal{E}$ of Theorem 9 are as follows:

$$\begin{aligned}
P(\alpha_4, \alpha_6, \alpha_{13}, \alpha_{12}) &= \eta_7 P(\alpha_5, \alpha_9, \alpha_{10}, \alpha_{11}), \\
P(\alpha_2, \alpha_4, \alpha_8, \alpha_9) &= \eta_4 P(\alpha_5, \alpha_{10}, \alpha_{11}, \alpha_{12}), \\
P(\alpha_2, \alpha_5, \alpha_6, \alpha_7) &= \eta_3 P(\alpha_9, \alpha_{10}, \alpha_{11}, \alpha_{12}), \\
P(\alpha_7, \alpha_8, \alpha_{10}, \alpha_{13}) &= \eta_{10} P(\alpha_5, \alpha_9, \alpha_{11}, \alpha_{12}), \\
P(\alpha_5, \alpha_{10}, \alpha_{12}, \alpha_{13}) &= \eta_{11} P(\alpha_1, \alpha_8, \alpha_9, \alpha_{16}), \\
P(\alpha_1, \alpha_8, \alpha_{10}, \alpha_{16}) &= \eta_9 P(\alpha_5, \alpha_{10}, \alpha_{13}, \alpha_{18}), \\
P(\alpha_2, \alpha_7, \alpha_8, \alpha_{13}) &= \eta_4 P(\alpha_5, \alpha_{10}, \alpha_{14}, \alpha_{18}),
\end{aligned}$$

One can check that units $\eta_1, \eta_2, \dots, \eta_{12}$ are written as products of powers of

$$\begin{aligned}\eta_2 &= \theta^2, \\ \eta_5 &= (\theta - 1)^2(\theta + 1)^2, \\ \eta_7 &= (\theta + 1)^2, \\ \eta_{10} &= \theta + 2.\end{aligned}$$

Moreover, one has the identity $\eta_2\eta_5\eta_{10}(\theta^2 - 3)^2 = 1$. This implies that the group E_K^+ is generated by square units. Thus, the unit group E_K of K is generated by

$$\theta, \theta + 1, \theta - 1, \theta^2 - 3.$$

This is consistent with a result in [2].

References

- [1] J. Buchmann, *On the computation of units and class numbers by a generalization of Lagrange's algorithm*, J.Number Theory 26 (1987), pp 8-30
- [2] M. Pohst, P.Weiler and H. Zassenhaus, *On Effective computation of fundamental units. II* Math. Comp. 38 (1982) pp 293-329
- [3] T. Shintani, *On evaluation of zeta functions of totally real algebraic number fields at non-positive integers*. J. Fac. Sci. Univ. Tokyo Sect. IA 23 (1976) pp 393-417
- [4] E. Thomas and A. T. Vasquez, *On the resolution of cusp singularities and the Shintani decomposition in totally real cubic number fields*. Math. Ann. 247 (1980) pp 1-20