THESIS ON NATURAL AND EXACT SCIENCES

On additive generalisation of Voronoï's theory of perfect forms over algebraic number fields

ALAR LEIBAK

Faculty of Science
Department of Mathematics
TALLINN UNIVERSITY OF TECHNOLOGY

Dissertation was accepted for the commencement of the degree of Doctor of Philosophy in Natural Sciences on October 19, 2006

Supervisors:
Assoc. Prof. Paul Tammela, Faculty of Mathematics and Natural Sciences at TLU
Prof. Peeter Puusemp, Faculty of Science, Department of Mathematics

Opponents:
Renaud Coulangeon, University of Bordeaux 1, France
Ellen Redi, Tallinn University, Estonia

Commencement: December 8, 2006.

Declaration: Hereby I declare that this doctoral thesis, my original investigation and achievement, submitted for the doctoral degree at Tallinn University of Technology has not been submitted for any degree or examination.

/Alar Leibak/

ISSN 1406-4723
ISBN 9985-59-659-5

Contents

Introduction

A quadratic form f of m variables is called *positive definite* if $f(x) = \sum_{i,j=1}^{m} f_{ij}x_ix_j$, $f_{ij} \in \mathbb{R},\ f_{ij} = f_{ji}$, is positive for any non-zero $x \in \mathbb{R}^m$. From now on, by the quadratic form we mean the positive definite quadratic form. Assume that x varies over so called (integral) lattice $\mathbb{Z}^m$. Since any non-empty compact set K contains only finitely many points of lattice $\mathbb{Z}^m$ and f is continuous, it follows that f attains smallest non-zero value $\mu(f)$ at the set of non-zero points of the lattice $\mathbb{Z}^m$. The lattice points on which the minimum $\mu(f)$ is attained are called the representations of the minimum of f (minimal vectors of f, for short). A quadratic form f is called perfect, if it is uniquely determined by its minimal vectors and by $\mu(f)$, that is the system of linear equations

$$\sum_{i,j=1}^{m} f_{ij}v_iv_j = \mu(f), \quad v \text{ is a minimal vector of } f$$

has unique solution (f_{ij}). We write $\det(f)$ for the determinant of the symmetric positive definite matrix (f_{ij}). Consider the following function

$$\gamma(f) = \frac{\mu(f)}{\sqrt[m]{\det(f)}}$$

on the set of all positive definite quadratic forms with m variables. A quadratic form is called *extreme* (*critical*), if the function γ attains local (respectively global) maximum at f. A lattice $L \subset \mathbb{R}^m$ associated to an extreme form f gives dense lattice packing of equal spheres in the vector space $\mathbb{R}^m$. Thus, the lattice corresponding to a critical quadratic form gives the densest lattice packing in this space. Many dense lattices can be constructed using algebraic number fields (see [CS99, §7 of Chapter 8]). The generalised density (in terms of Hermite constant) for lattices over number fields can be expressed in context of quadratic forms over real numbers. As any extreme form is also perfect and the generalisation of Voronoï's algorithm can be used for finding all inequivalent perfect forms of m variables, this motivates the study of perfect forms over number fields.

The theory regarding perfect quadratic forms can be dated back to Korkine and Zolotareff. The first systematic study on perfect forms with real coefficients was published by Voronoï in 1908 [Vor08]. In his work [Vor08] Voronoï gave an algorithm for finding (at least in theory) all perfect form (up to equivalency and

scaling) of rank m starting from perfect form of rank m already known. Moreover he proved that the quadratic form

$$f(x_1, \ldots, x_m) = \sum_{i=1}^{m} \sum_{j>i}^{m} x_i x_j \tag{0.1}$$

is perfect for any $m > 1$.

His paper [Vor08] includes his well-known theorem: a positive definite quadratic form f is extreme if and only if it is perfect and eutactic[1].

Theory of perfect quadratic forms over algebraic number field is much less studied than the theory of perfect quadratic forms over reals. Let f be a positive definite quadratic form over an algebraic number field $\mathbb{K}$. Following remarks point out the difference from the situation what we have for quadratic forms over reals.

1. If $C > 0$ then there exist non-zero $v \in \mathcal{O}_{\mathbb{K}}^{\mathrm{rank} f}$ such that $f(v) < C$.
2. If $\mathbb{K}$ has complex embeddings, then a Hermitian form h should be considered instead of the quadratic form f.

These remarks motivate to consider Humbert tuples instead of a quadratic or Hermitian form.

Theory of perfect forms and extreme forms over algebraic number fields was initiated by Max Koecher [Koe60]. He considered so called trace minimums of particular tuples of quadratic forms that is minimums of quadratic forms

$$\sum_{i=1}^{r} f_i(x) + 2 \sum_{i=r+1}^{r+s} f_i(x)$$

where $f_1, \ldots, f_r$ are positive definite quadratic forms of rank m and $f_{r+1}, \ldots, f_{r+s}$ are positive definite Hermitian forms of rank m. Koecher gave an equivalent definition for the perfectness and proved:

1. the upper bound of Hermite' function on Humbert tuples of rank m over $\mathbb{K}$ is
$$\frac{4}{\sqrt[mn]{\varrho^2}} \sqrt[n]{\mathrm{disc}(\mathbb{K})},$$
where n denotes the degree of $\mathbb{K}$ and ϱ denotes the volume of the unit ball in $\mathbb{R}^{mn}$;
2. the number of perfect forms of rank m is finite up to equivalence and scaling.

[1] A quadratic form f is called eutactic, if the adjoint matrix of f lies in the open convex hull of positive semi-definite matrices vv^t, where v is a minimal vector of f.

Koecher's work regarding perfect forms was continued by H. E. Ong in the mid 1980s. Ong studied tuples of the form $((f_{ij}), (\bar{f}_{ij}))$ ($\bar{f}_{ij}$ denotes the field conjugate of f_{ij}), where (f_{ij}) is a positive definite symmetric matrix over number field $\mathbb{Q}(\sqrt{D})$ for $D = 2, 3, 5$. Ong generalised Voronoï's algorithm for real quadratic extensions, gave initial perfect forms for fields $\mathbb{Q}(\sqrt{D})$, $D = 2, 3, 5$ necessary for applying generalised Voronoï's algorithm, and presented the complete list of positive definite perfect binary forms over $\mathbb{Q}(\sqrt{D})$ for $D = 2, 3, 5$ [Ong83], [Ong86].

A different approach to the theory of perfect forms and extreme forms was started by Baeza and Icaza [BI97], [Ica97], where minimums of

$$\prod_{i=1}^{r} f_i(x) \prod_{i=r+1}^{r+s} f_i^2(x)$$

were used. Coulangeon developed it further and succeeded to generalise the well-known Voronoï's theorem [Cou01]. Icaza's work were generalised to algebraic groups by Thunder [Thu98], Ong and Watanabe [OW01], [Wat01], [Wat04], [Wat03]. The complete list of binary perfect forms over $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{5})$ together with Hermite–Humbert constant for those fields are given in [BCIO01]. Pohst and Wagner presented an algorithm for finding extreme Humbert tuples over real quadratic field with class number one if those tuples have unimodular pair of minimal vectors [PW05]. As a result, they found those extreme binary Humbert tuples for $\mathbb{Q}(\sqrt{13})$ and $\mathbb{Q}(\sqrt{17})$ and computed the Hermite–Humbert constant for $\mathbb{Q}(\sqrt{13})$.[2]

In this thesis we continue the study of perfect forms regarding trace minimal vectors. We start by generalising the Koecher's definitions of perfect forms and Hermite number to Humbert tuples. Motivated by applications (reduction theory, coding theory etc.) we proceed to study perfect forms and Hermite number for number fields.

The thesis consist of three parts. The first part is devoted to the generalisation of the Voronoï's theory to perfect forms over algebraic number fields. This part includes the necessary definitions and main results. All but one results are derived by assuming that the underlying number field $\mathbb{K}$ is totally real. Such as

1. we prove that any perfect Humbert tuple over either totally real or totally complex number field is proportional to a *conjugate tuple* (see Definition 1.2). It follows that binary perfect Humbert tuples over fields $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{5})$ are the ones found by Ong [Ong83, Ong86].

2. We present the construction for an initial perfect form of any rank m if a perfect unary form over totally real $\mathbb{K}$ is given (Theorem 1.1). Once we have

[2] It follows from the work of Baeza and Icaza (see [BI04]) that Pohst and Wagner computed the Hermite-Humbert constant for binary Humbert forms over $\mathbb{Q}(\sqrt{17})$.

an initial perfect form of m variables, then the rest of perfect forms of m variables (up to equivalence and homothety) can be found by applying the generalised Voronoï's algorithm. Therefore, the problem of finding an initial perfect form of m variables can be reduced to finding an unary perfect form.

3. If $\mathbb{K}$ is real quadratic number field or $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, where $3 \nmid n$, then we give a construction for an initial perfect quadratic form (Theorem 1.3 and Corollary 1.3).

4. We present some examples of connection between perfect polyhedras and reduction domain for unary conjugate Humbert tuples.

The second part includes a generalisation of Hermite's constant and a theoretical results concerning extreme Humbert tuples. The main results of this part include:

1. any extreme Humbert tuple f is perfect and, if $\mathrm{rank}\, f > 1$, then f is weakly eutactic (Theorem 2.1). Any extreme Humbert tuple is proportional to the conjugate tuple. The latter one is the generalisation of result by Korkin-Zolotareff to number fields and it is stronger result than the one what we have in multiplicative generalisation (see Proposition 4.1 in [Cou01]).

2. the upper and lower bounds of generalised Hermite's constant.

The developed theory in part two is connected to the so called trace norm lattices, as it is demonstrated at the end of this part. As a result, the new constructions for quadratic forms corresponding to lattices E_6 and E_8 are presented.

In the third part we apply the results of the first part and enumerate all positive definite perfect binary quadratic forms over number field $\mathbb{Q}(\sqrt{6})$. It is the continuation of the work started by Ong [Ong86], where the complete lists of binary perfect forms over $\mathbb{Q}(\sqrt{D})$, $D = 2, 3, 5$ are given. We generalise the definition of automorphism of a quadratic form f by field automorphisms. This part involves the theoretical improvement of Voronoï's algorithm, that is some theoretical result are presented, what give computational advantages in applying Voronoï's algorithm to perfect forms over normal extensions of $\mathbb{Q}$. The main idea of improvements relies on 'symmetry' arising from Galois' action on quadratic forms. Also we give a short overview of the connection between binary quadratic forms over a totally real number field $\mathbb{K}$ and the elliptic fixed points of Hilbert modular group. The number inequivalent elliptic fixed points over quadratic number field $\mathbb{Q}(\sqrt{D})$, $2 \leq D \leq 97$ is a square-free, was counted by Prestel [Pre68]. We show that our results agree with the Prestels results for elliptic points of order 3 and 6 over the field $\mathbb{Q}(\sqrt{6})$.

Symbols

$\langle , \rangle$	bilinear product
$\mathbb{C}$	the field of complex numbers
$d(f)$	determinant of a Humbert tuple f
$\mathrm{disc}(\mathbb{K})$	discriminant of the field $\mathbb{K}$
f	a positive definite quadratic form or a Humbert tuple
$\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$	Galois' group of field $\mathbb{K}$
$\mathrm{GL}(m, \blacklozenge)$	group of invertible square-matrices of m rows with entries in $\blacklozenge$
Γ	(extended) Hilbert modular group over real quadratic field $\mathbb{Q}(\sqrt{D})$
Γ_z	stabiliser of an element $z \in \mathfrak{H}$
$\gamma_{m,\mathbb{K}}$	additive Hermite constant
$\gamma^*_{m,\mathbb{K}}$	multiplicative Hermite constant
$\mathfrak{H}$	the complex upper half-plane
$\mathbb{K}$	an algebraic number field (i.e finite extension of the field $\mathbb{Q}$)
$\mathcal{M}(f)$	the set of minimal vectors of f
$\mathcal{O}_{\mathbb{K}}$	the ring of algebraic integers in $\mathbb{K}$
$\omega_1, \ldots, \omega_n$	a $\mathbb{Z}$-basis of $\mathcal{O}_{\mathbb{K}}$
$\mathcal{P}_{m,\mathbb{K}}$	the set of all Humbert tuples of rank m over $\mathbb{K}$
$\mathbb{Q}$	the field of rational numbers
$\mathbb{R}$	the field of real numbers
r	a number of real embeddings of $\mathbb{K}$
s	half of the number of complex embeddings of $\mathbb{K}$ into $\mathbb{C}$
σ_i	the i-th embedding of $\mathbb{K}$ into $\mathbb{C}$
$\mathrm{TR}(\blacklozenge)$	trace of a matrix $\blacklozenge$
$\mathbb{Z}$	ring of integers
ζ_n	a primitive n-th root of unity
$L_1 \otimes L_2$	tensor product of positive lattices L_1 and L_2
$f_1 \otimes f_2$	tensor product of quadratic forms f_1 and f_2
$a \gg 0$	an algebraic number a is totally positive
$(z_1, z_2) \not\sim (z'_1, z'_2)$	the points $(z_1, z_2), (z'_1, z'_2) \in \mathfrak{H}^2$ are non-equivalent under the group Γ
$G' \lhd G$	G' is a proper normal subgroup of a group G

1. On additive perfect forms over algebraic number fields

Let $\mathbb{K}$ be an algebraic number field with r real embeddings $\sigma_1, \ldots, \sigma_r$ and $2s$ complex embeddings $\sigma_{r+1}, \ldots, \sigma_{r+2s}$, with $\sigma_{r+s+i} = \bar{\sigma}_{r+i}$ for $1 \leq i \leq s$, where " $^-$ " denotes the complex conjugate.

Definition 1.1 ([Ica97]): *A tuple $(f_i)_{i=1}^{r+s}$ of r positive definite quadratic forms $f_1, \ldots, f_r$ of rank m and s positive definite Hermitian forms $f_{r+1}, \ldots, f_{r+s}$ of rank m is called Humbert tuple of rank m.*

A quadratic form (Hermitian form) f over a totally real number field (respectively totally complex number field) $\mathbb{K}$ is said to be positive definite if $\sigma_i(f)$ is positive definite for each $i = 1, \ldots, r$, (respectively $i = 1, \ldots, s$).

In order to formulate one of the most important result of this section we need the following definition. Let $\tau_i \colon \sigma_1(\mathbb{K}) \to \sigma_i(\mathbb{K})$, $i = 2, \ldots, r$ and $\tau'_j \colon \sigma_{r+1}(\mathbb{K}) \to \sigma_j(\mathbb{K})$, $j = r+2, \ldots, r+s$, be field isomorphisms.

Definition 1.2: *A Humbert tuple $(f_1, \ldots, f_{r+s})$ is called conjugate tuple if there exist positive definite quadratic form f over $\sigma_1(\mathbb{K})$ and hermitian form h over $\sigma_{r+1}(\mathbb{K})$, such that*

$$(f_1, \ldots, f_{r+s}) = (f, \tau_2(f), \ldots, \tau_r(f), h, \tau'_{r+2}(h), \ldots, \tau'_{r+s}(h)).$$

If $\mathbb{K}$ is totally real (totally complex) then a Humbert tuple $(f_1, \ldots, f_r)$ (respectively $(f_1, \ldots, f_s)$) is called conjugate tuple if there exist a positive definite quadratic form over $\mathbb{K}$ (respectively positive definite hermitian form h over $\mathbb{K}$) such that $(f_1, \ldots, f_r) = (\sigma_1(f), \ldots, \sigma_r(f))$ (respectively $(f_1, \ldots, f_s) = (\sigma_1(h), \ldots, \sigma_s(h))$).

If $\mathbb{K}$ is totally real (totally complex) and f is a positive definite quadratic form (respectively positive definite hermitian form) over $\mathbb{K}$, then we use the same letter f for the Humbert tuple $(\sigma_1(f), \ldots, \sigma_r(f))$ (respectively $(\sigma_1(f), \ldots, \sigma_s(f))$).

The set of all Humbert tuples of rank m over number field $\mathbb{K}$ will be denoted by $\mathcal{P}_{m,\mathbb{K}}$. Clearly, $\mathcal{P}_{m,\mathbb{K}}$ is a convex cone in $\mathbb{R}^{rm(m+1)/2} \times \mathbb{R}^{sm^2}$, that is:

1. if $f \in \mathcal{P}_{m,\mathbb{K}}$, then $\lambda f \in \mathcal{P}_{m,\mathbb{K}}$ for all positive $\lambda \in \mathbb{R}$;
2. if $f, g \in \mathcal{P}_{m,\mathbb{K}}$, then $(1-\lambda)f + \lambda g \in \mathcal{P}_{m,\mathbb{K}}$ for all $\lambda \in [0,1]$.

With each Humbert tuple $(f_i)_1^{r+s}$ we associate a tuple of r symmetric and s Hermitian matrices such that $f_i(x) = \bar{x}^t A_i x$ for each $1 \le i \le r+s$. Group $\mathrm{GL}(m,\mathbb{K})$ acts on $\mathcal{P}_{m,\mathbb{K}}$ via embedding

$$\mathrm{GL}(m,\mathbb{K}) \hookrightarrow \mathrm{GL}(m,\mathbb{R})^r \times \mathrm{GL}(m,\mathbb{C})^s, \qquad M \rightsquigarrow (\sigma_i(M))_{i=1}^{r+s}.$$

Assume that $\mathcal{A} = (A_i)_1^{r+s}$ is a tuple of matrices associated to Humbert tuple $(f_i)_1^{r+s}$ and $M \in \mathrm{GL}(m,\mathbb{K})$. The action is defined as follows

$$(\mathcal{A}, M) \rightsquigarrow (\underbrace{\ldots, \sigma_i(M)^t A_i \sigma_i(M), \ldots}_{1\le i\le r}, \underbrace{\ldots, \overline{\sigma_i(M)}^t A_i \sigma_i(M), \ldots}_{r+1\le i\le r+s}).$$

Let $f = (f_1, \ldots, f_{r+s})$ be a Humbert tuple of rank m. We write

$$\mu(f) = \min\left\{ \sum_{i=1}^{r} f_i(\sigma_i(X)) + 2\sum_{i=r+1}^{r+s} f_i(\sigma_i(X)) \;\Big|\; 0 \ne X \in \mathcal{O}_{\mathbb{K}}^m \right\}$$

and call it *a trace minimum* of f. Let $\omega_1, \ldots, \omega_n$ be a $\mathbb{Z}$-basis of $\mathcal{O}_{\mathbb{K}}$. Any algebraic integer $\alpha \in \mathcal{O}_{\mathbb{K}}$ is a value of the linear form $\omega_1 x_1 + \ldots + \omega_n x_n$ at $\mathbb{Z}^n$. Put

$$\lambda_{k;i}(x) = \sigma_i(\omega_1)x_{k,1} + \ldots + \sigma_i(\omega_n)x_{k,n}, \quad 1 \le k \le m,\ 1 \le i \le n.$$

The trace minimum coincides with the minimum of the positive definite quadratic form (over $\mathbb{R}$)

$$\begin{aligned} F(x_{1,1}, \ldots, x_{1,n}, \ldots, x_{m,n}) &= \sum_{i=1}^{r+2s} f_i(\lambda_{1;i}, \ldots, \lambda_{m;i}) = \\ &= \sum_{i=1}^{r} f_i(\lambda_{1;i}, \ldots, \lambda_{m;i}) + 2\sum_{i=r+1}^{r+s} f_i(\lambda_{1;i}, \ldots, \lambda_{m;i}) \end{aligned} \tag{1.1}$$

at $\mathbb{Z}^{nm}$, where $f_{i+s}(x) = x^t A_i \bar{x}$ for all $r+1 \le i \le r+s$. If $\mathbb{K}$ is totally real and f is a conjugate tuple, then

$$\begin{aligned} F(x_{1,1}, \ldots, x_{1,r}, \ldots, x_{m,r}) &= \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(f(x)) \\ &= \sum_{i,j=1}^{m}\sum_{k,l=1}^{r} x_{i,k}x_{j,l}\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(f_{ij}\omega_k\omega_l) \quad (f_{ij} = f_{ji}). \end{aligned} \tag{1.2}$$

(This explains the name *trace minimum*.) When no confusion arises, we write

$$\mathrm{Tr} f(X) = \sum_{i=1}^{r} f_i(\sigma_i(X)) + 2\sum_{i=r+1}^{r+s} f_i(\sigma_i(X)), \qquad X \in \mathcal{O}_{\mathbb{K}}^m.$$

By the minimal vectors of f we mean the set

$$\mathcal{M}(f) = \{X \in \mathcal{O}_{\mathbb{K}}^m \mid \mathrm{Tr} f(X) = \mu(f)\}.$$

In this thesis we do not distinguish between X and $-X$ for each $X \in \mathcal{M}(f)$.

Definition 1.3: *A Humbert tuple $(f_i)_{i=1}^{r+s}$ is called perfect, if it is uniquely determined by the set $\mathcal{M}(f)$ and the trace minimum $\mu(f)$.*

By definition, a Humbert tuple f of rank m has

$$N = r\frac{m(m+1)}{2} + sm^2$$

coefficients. Hence, if f is also perfect, then we must have $\#\mathcal{M}(f) \geq N$ (for quadratic forms over real numbers see also [GL87]).

Proposition 1.1: *Let f be a Humbert tuple of rank m. Then f is perfect if and only if there exist*

$$N = r\frac{m(m+1)}{2} + sm^2$$

minimal vectors $X_1, \ldots, X_N \in \mathcal{M}(f)$ such that the block-diagonal matrices

$$diag\{\sigma_1(X_i\overline{X_i}^t), \ldots, \sigma_{r+s}(X_i\overline{X_i}^t)\}, \qquad (i = 1, \ldots, N)$$

are linearly independent.

This was the definition for perfection given by Koecher (see [Koe60]). The proof is obvious.

Following claims give some information about perfect Humbert tuples.

Proposition 1.2 (Proposition 2 in [Lei05a]): *Let f be a Humbert tuple over $\mathbb{K}$. Assume that $\lambda_1 \in \mathbb{R}_{>0}$ is the trace minimum of f. If f is perfect, then there exist a conjugate tuple h over $\mathbb{K}$ and $a \in \mathbb{R}_{>0}$ such that $f = ah$.*

Corollary 1.1 (Corollary 1 in [Lei05a]): *If $(a_1x^2, \ldots, a_rx^2)$ is a perfect unary Humbert tuple over totally real number field $\mathbb{K}$, then $(a_1, \ldots, a_r) = (\sigma_1(a), \ldots, \sigma_r(a))$ for a totally positive algebraic number $a \in \mathbb{K}$.*

Corollary 1.2 (Corollary 2 in [Lei05a]): *Any perfect Humbert tuple over totally real (totally complex) number field $\mathbb{K}$ is proportional to a positive definite quadratic (respectively positive definite hermitian) form f over $\mathbb{K}$.*

The last corollary generalises the result already known for real perfect forms, that is, any perfect quadratic form over real numbers is proportional to a rational perfect form. (The situation is different in multiplicative generalisation. It is shown in [BCIO01] that there exists perfect Humbert tuple over $\mathbb{Q}(\sqrt{2})$ with coefficients in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.)

One main problem in the theory of perfect forms is finding all perfect forms (up to equivalence and homothety) of given rank m. For real perfect forms this problem is solved (at least in theory) by Voronoï [Vor08]. The generalisation of Voronoï's algorithm applies in our case as well (see [Ong86]) if $\mathbb{K}$ is totally real, but does not give a solution for finding an initial perfect form. Next we give a negative result first (this was motivated by an example given in [Ica97]) and later we will show how the problem can be reduced to finding an unary perfect form if $\mathbb{K}$ is totally real.

By a positive lattice we mean the lattice associated to a positive definite quadratic form.

Definition 1.4 ([Kit93, §7.1]): *A positive lattice L (over $\mathbb{Z}$) is of E-type if for any positive lattice L' the minimum vectors of $L \otimes L'$ can be written as $l \otimes l'$ where $l \in L$ and $l' \in L'$.*

We refer [Kit93] for more facts and existence of positive lattices of *E*-type.

Proposition 1.3 (Proposition 3 in [Lei05a]): *Let $f(x) = \sum f_{ij}x_ix_j$ be a perfect quadratic form over $\mathbb{Z}$ and L be the corresponding lattice. If L is of E-type, then the Humbert tuple $(f, \ldots, f)$ ($[\mathbb{K}\colon\mathbb{Q}]$ copies) is not perfect over any algebraic number field $\mathbb{K}$.*

Theorem 1.1 (Theorem 1 in [Lei05a]): *Let $\mathbb{K}$ be a totally real algebraic number field and let $\mathcal{O}_{\mathbb{K}}$ denote its ring of integers. Let ax^2 be a perfect unary quadratic form over $\mathcal{O}_{\mathbb{K}}$ with lattice L_a over $\mathbb{Z}$ and let g be a perfect quadratic form over $\mathbb{Z}$ with lattice L. If L_a or L is of E-type, then the quadratic form ag is perfect over $\mathbb{K}$.*

Theorem 1.2 (Theorem 2 in [Lei05a]): *Let $\mathbb{K}_1$ and $\mathbb{K}_2$ be totally real number fields with degree r_1 and r_2 respectively. Let f_1 and f_2 be perfect quadratic forms over $\mathbb{K}_1$ and $\mathbb{K}_2$ respectively. Denote the rank of f_i by m_i ($i = 1, 2$). We define $\mathcal{L}_2(\mathcal{M}(f))$ to be the $\mathbb{Q}$-linear space generated by $\{uu^t | u \in \mathcal{M}(f)\}$. If*

1. *$\mathbb{K}_1$ and $\mathbb{K}_2$ are linearly disjoint*[1] *and $\gcd(\mathrm{disc}(\mathbb{K}_1), \mathrm{disc}(\mathbb{K}_2)) = 1$;*
2. *$\{v \otimes w \,|\, v \in \mathcal{M}(f_1), w \in \mathcal{M}(f_2)\} \subseteq \mathcal{M}(f_1 \otimes f_2)$;*
3. *$\dim \mathcal{L}_2(\mathcal{M}(f_1)) \cdot \dim \mathcal{L}_2(\mathcal{M}(f_2)) \geqslant r_1 r_2 \frac{m_1 m_2 (m_1 m_2 + 1)}{2}$,*

then $f_1 \otimes f_2$ is a perfect quadratic form over $\mathbb{K}_1\mathbb{K}_2$.

[1] See also Ch.3 Proposition 17 in [Lan94]

Let $e > 1$ be a fundamental unit in $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$. Write $f/\mathbb{K}$ for the quadratic form over $\mathbb{K}$. As $e\sqrt{2}x^2/\mathbb{Q}(\sqrt{2})$, $ex^2/\mathbb{Q}(\sqrt{3})$ and $e\sqrt{5}x^2/\mathbb{Q}(\sqrt{5})$ being perfect and the initial quadratic form (0.1) being of E-type ([Kit93, Theorem 7.2.1]), the theorem 1.1 generalises the theorem proved by Ong ([Ong86, Theorem 3.2.1]). The perfection of forms $e\sqrt{2}x^2/\mathbb{Q}(\sqrt{2})$, $ex^2/\mathbb{Q}(\sqrt{3})$ and $e\sqrt{5}x^2/\mathbb{Q}(\sqrt{5})$ can be verified immediately or by Theorem 1.3.

Combining theorem 1.1 with the initial perfect form (0.1) being of E-type, we obtain that, in order to find an initial perfect positive form over totally real number field $\mathbb{K}$ it is sufficient to find an initial perfect unary form $ax^2/\mathbb{K}$. Once we have an initial perfect form of rank m, then the rest of perfect forms of rank m (up to equivalence and scaling) can be found by applying the generalisation of Voronoï's algorithm. This motivates the study of finding unary perfect forms. It follows from theorem 2.3, that there exists unary perfect form over totally real number field $\mathbb{K}$. But we can construct an initial unary perfect form only if $\mathbb{K}$ is either real quadratic number field or $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, where $n \not\vdots 3$ is a square-free odd integer.

Theorem 1.3 (Theorem 1 in [Lei05b]): *Let $D > 1$ be a square-free integer.*

1. *Suppose that $|k^2 - D|$ attains minimum at integer $k > 0$. If $D \equiv 2 \pmod 4$ or $D \equiv 3 \pmod 4$, then the unary form $ax^2 = (a_1 + a_2\sqrt{D})x^2$, with*

$$a_1 = 2kD, \qquad a_2 = k^2 + D - 1,$$

   is perfect and $\{1, k - \sqrt{D}\} \subseteq \mathcal{M}(ax^2)$.

2. *Let $k > 0$ be the smallest integer, such that $|(2k-1)^2 - D|$ is minimal. If $D \equiv 1 \pmod 4$, then the unary form $ax^2 = (a_1 + a_2\frac{1+\sqrt{D}}{2})x^2$, with*

$$a_1 = 1 - k^2 + (1+D)k - \frac{1+3D}{4}, \qquad a_2 = 2k^2 - 2k + \frac{1+D}{2} - 2$$

   is perfect and $\{1, -k + \frac{1+\sqrt{D}}{2}\} \subseteq \mathcal{M}(ax^2)$.

Theorem 1.4 (Theorem 4 in [Lei05a]): *Let ζ_p be a primitive p-th root of unity, where p is a prime. Unary quadratic form $(2 - \zeta_p - \zeta_p^{-1})x^2$ is a perfect quadratic form over $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$. Moreover, $\varepsilon \in \mathbb{Z}[\zeta_p + \zeta_p^{-1}]^*$ is a minimum vector of $(2 - \zeta_p - \zeta_p^{-1})x^2$ iff $\sigma(2 - \zeta_p - \zeta_p^{-1}) = (2 - \zeta_p - \zeta_p^{-1})\varepsilon^2$ holds for some $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p + \zeta_p^{-1})/\mathbb{Q})$.*

Applying Theorem 1.2, we obtain the following result.

Corollary 1.3 (Corollary 3 in [Lei05a]): *Let $n > 1$ be a square-free odd integer $n = p_1 \cdots p_k$ and $3 \not| n$. The unary quadratic form*

$$\left(\prod_{i=1}^{k} (2 - \zeta_{p_i} - \zeta_{p_i}^{-1}) \right) x^2$$

is perfect over $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$, where ζ_{p_i} is a primitive p_i-th root of unity and ζ_n is a primitive n-th root of unity.

Theorem 1.5: *If $\mathbb{K}$ is a totally real and if $m \geq 1$ is a natural number, then there exists an initial perfect form over $\mathbb{K}$ of rank m.*

It follows immediately from Theorems 2.3 and 1.1.

1.1 Perfect cones and reduction domain for unary forms over real quadratic number fields

Let $\mathbb{K}$ be a totally real number field, $[\mathbb{K} : \mathbb{Q}] = r$, and let $\mathcal{O}_{\mathbb{K}}$ its ring of integers. If f is a quadratic form over $\mathbb{K}$, then we set

$$\Pi_f = \mathbb{R}_{>0} \cdot \left\{ \sum_{X \in \mathcal{M}(f)} \rho_X(\sigma_1(XX^t), \ldots, \sigma_r(XX^t)) \, | \rho_X \geq 0, \rho_X \in \mathbb{Q} \right\}$$

and call it perfect cone. Write

$$\mathcal{F} = \{ax^2 | a \gg 0 \wedge \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(a) \leq \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(a\varepsilon^2) \; \forall \varepsilon \in \mathcal{O}_{\mathbb{K}}^*\}.$$

The set $\mathcal{F}$ is a reduction domain and it is a union of perfect cones [Koe60, Proposition 8].

We conclude this section by giving two examples if $\mathbb{K}$ is a real quadratic field.

Example 1. Let $\mathbb{K} = \mathbb{Q}(\sqrt{3})$.

The fundamental domain $\mathcal{F}$ is determined by the inequality

$$\max\left\{ \frac{a}{a'}, \frac{a'}{a} \right\} \leq e^2$$

where $e > 1$ is the fundamental unit [Lei02, Theorem 11]. Also, we have

$$\max\left\{ \frac{a}{a'}, \frac{a'}{a} \right\} \geq 1.$$

Up to equivalence and homothety, there is one unary perfect quadratic form ex^2 (it is also critical) with minimal vectors 1 and $\bar{e}$. The perfect cone

$$\Pi_{x^2} = \mathbb{R}_{>0} \cdot \{\rho_1 x^2 + \rho_2 \bar{e}^2 x^2 \mid \rho_1 \geq 0, \rho_2 \geq 0,\ \rho_1, \rho_2 \in \mathbb{Q}\}$$

coincides with the closure of the fundamental domain $\mathcal{F}$.

Example 2. Let $\mathbb{K} = \mathbb{Q}(\sqrt{31})$.

As in the previous example, the fundamental domain

$$\mathcal{F} = \{ax^2 | a \gg 0 \wedge \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}\,(a) \leq \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}\,(a\varepsilon^2)\ \forall \varepsilon \in \mathcal{O}_{\mathbb{K}}^*\}$$

is determined by inequalities

$$1 \leq \max\left\{\frac{a}{a'}, \frac{a'}{a}\right\} \leq e^2.$$

Up to equivalence and homothety there exist six unary perfect forms

$$(62 \pm 11\sqrt{31})x^2,\ (496 \pm 89\sqrt{31})x^2,\ (15562 \pm 2795\sqrt{31})x^2$$

with following sets of minimal vectors $\{1, 5 \mp \sqrt{31}, 6 \mp \sqrt{31}\}, \{6 \mp \sqrt{31}, 11 \mp 2\sqrt{31}\}, \{11 \mp 2\sqrt{31}, 39 \mp 7\sqrt{31}\}$ respctively. Perfect cones are

$\Pi_{(62+11\sqrt{31})x^2} =$
$\mathbb{R}_{>0} \cdot \{\rho_1 x^2 + \rho_2(5 - \sqrt{31})^2 x^2 + \rho_3(6 - \sqrt{31})^2 x^2 | \rho_1 \geq 0, \rho_2 \geq 0, \rho_3 \geq 0\}$,
$\Pi_{(62-11\sqrt{31})x^2} =$
$\mathbb{R}_{>0} \cdot \{\rho_1 x^2 + \rho_2(5 + \sqrt{31})^2 x^2 + \rho_3(6 + \sqrt{31})^2 x^2 | \rho_1 \geq 0, \rho_2 \geq 0, \rho_3 \geq 0\}$,
$\Pi_{(496+89\sqrt{31})x^2} =$
$\mathbb{R}_{>0} \cdot \{\rho_1(6 - \sqrt{31})^2 x^2 + \rho_2(11 - 2\sqrt{31})^2 x^2 \mid \rho_1 \geq 0, \rho_2 \geq 0\}$,
$\Pi_{(496-89\sqrt{31})x^2} =$
$\mathbb{R}_{>0} \cdot \{\rho_1(6 + \sqrt{31})^2 x^2 + \rho_2(11 + 2\sqrt{31})^2 x^2 \mid \rho_1 \geq 0, \rho_2 \geq 0\}$,
$\Pi_{(15562+2795\sqrt{31})x^2} =$
$\mathbb{R}_{>0} \cdot \{\rho_1(11 - 2\sqrt{31})^2 x^2 + \rho_2(39 - 7\sqrt{31})^2 x^2 \mid \rho_1 \geq 0, \rho_2 \geq 0\}$,
$\Pi_{(15562-2795\sqrt{31})x^2} =$
$\mathbb{R}_{>0} \cdot \{\rho_1(11 + 2\sqrt{31})^2 x^2 + \rho_2(39 + 7\sqrt{31})^2 x^2 \mid \rho_1 \geq 0, \rho_2 \geq 0\}$,

where $\rho_1, \rho_2, \rho_3 \in \mathbb{Q}$. It follows from immediate computations that $\overline{\mathcal{F}}$ is a union of these perfect cones.

2. On additive extreme forms over algebraic number fields

The *additive* Hermite's number of a Humbert tuple $f = (f_1, \ldots, f_{r+s})$ of rank m is defined as follows

$$\gamma_{\mathbb{K}}(f) = \frac{\min\{\mathrm{Tr} f(X) \,|\, 0 \neq X \in \mathcal{O}_{\mathbb{K}}^m\}}{d(f)^{\frac{1}{m\cdot[\mathbb{K}:\mathbb{Q}]}}}, \tag{2.1}$$

where

$$d(f) = \prod_{i=1}^{r} \det(f_{\sigma_i}) \cdot \prod_{i=r+1}^{r+s} \det(f_i)^2.$$

The real number $d(f)$ is called the determinant of the Humbert tuple f.

It follows from immediate computations, that $\gamma_{\mathbb{K}}(f)$ is invariant under the action by $\mathrm{GL}(m, \mathcal{O}_{\mathbb{K}})$ and multiplication by positive real scalars. Moreover, if f is a conjugate tuple, then $\gamma_{\mathbb{K}}(f)$ is invariant under $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$.

Definition 2.1: *A Humbert tuple f of rank m is called extreme (critical) if the function $\gamma_{\mathbb{K}}$ attains local maximum (respectively global maximum) at f.*

The *additive Hermite's constant* $\gamma_{m,\,\mathbb{K}}$ is defined by

$$\gamma_{m,\,\mathbb{K}} = \sup_{f \in \mathcal{P}_{m,\,\mathbb{K}}} \gamma_{\mathbb{K}}(f). \tag{2.2}$$

Definition 2.2: *The Humbert tuple f with corresponding tuple of matrices $(A_i)_{i=1}^{r+s}$ is called weakly eutactic if the adjoint matrix $\widetilde{A_i}$ lies in the open convex hull of $\sigma_i(X\overline{X}^t)$, $X \in \mathcal{M}(f)$, for all $1 \leq i \leq r+s$, that is, there exist $(r+s)$-tuples of positive reals $\rho^X \in (\mathbb{R}_{>0})^{r+s}$, $X \in \mathcal{M}(f)$, such that*

$$\widetilde{A_i} = \sum_{X \in \mathcal{M}(f)} \rho_i^X \sigma_i(X\overline{X}^t),$$

holds for all $1 \leq i \leq r+s$.

The name 'weak eutaxy' is due to Coulangeon (see [Cou01]), because he gave a stronger definition for eutaxy and generalised the Voronoï's theorem to algebraic number fields in multiplicative case. Icaza called such Humbert tuples eutactic

forms [Ica97]. For quadratic forms over real numbers this definition coincides with the usual definition of eutaxy (see [GL87, Mar03]).

Following lemma generalises the result known for the quadratic forms over real numbers.

Lemma 2.1 (Lemma 1 in [Lei05a]): *Let $f = (f_i)_{i=1}^{r+s}$ and $g = (g_i)_{i=1}^{r+s}$ be non-proportional Humbert tuples of rank m over $\mathbb{K}$. Write $n = [\mathbb{K}\colon \mathbb{Q}]$. Then $F_t = (1-t)f + tg$ is a Humbert tuple and $\varphi(t) = d(F_t)^{1/mn}$ is a strictly concave function for all $t \in [0,1]$.*

Let $\langle \cdot, \cdot \rangle$ be a symmetric positive definite bilinear form on $\mathbb{R}$-vector space

$$X = \prod_{i=1}^{r} \mathbb{R}^{m(m+1)/2} \times \prod_{i=1}^{s} \mathbb{R}^{m^2},$$

(X is spanned by Humbert tuples over $\mathbb{K}$) such that $\langle f, g \rangle > 0$ for all $f \in \mathcal{P}_{m,\mathbb{K}}$ and $g \in \overline{\mathcal{P}_{m,\mathbb{K}}}$. Therefore $\mathcal{P}_{m,\mathbb{K}}$ is a convex cone in the real vector space X. Let D be a discrete set in $\overline{\mathcal{P}_{m,\mathbb{K}}} \setminus \{0\}$, that is arbitrary compact set $K \subset \overline{\mathcal{P}_{m,\mathbb{K}}} \setminus \{0\}$ contains only finitely many points of D. For each $f \in \mathcal{P}_{m,\mathbb{K}}$ we let (see [Koe60] p. 389)

$$\mu_D(f) = \inf\{\langle f, y \rangle | y \in D\}.$$

Hence we can reformulate the lemma, which was given and proved by Koecher [Koe60].

Lemma 2.2 (Lemma 3 in [Koe60]): *For each $f \in \mathcal{P}_{m,\mathbb{K}}$ and $\varepsilon > 0$, there exists a neighbourhood $\mathcal{U} \subset \mathcal{P}_{m,\mathbb{K}}$ of f such that*

$$\mathcal{M}(g) \subseteq \mathcal{M}(f) \qquad \textit{and} \qquad |\mu_D(g) - \mu_D(f)| < \varepsilon$$

for all $g \in \mathcal{U}$.

In the thesis we fix $D = \{v\bar{v}^t | v \in \mathcal{O}_{\mathbb{K}}^m \setminus \{0\}\}$ and $\langle f, v\bar{v}^t \rangle = \mathrm{Tr} f(v)$. Thus, $\mu_D(f)$ coincides with the $\mu(f)$. Next theorem generalises (in the sense of additive generalisation) the necessary part of the Voronoï's theorem to algebraic number fields.

Theorem 2.1 (Theorem 5 in [Lei05a]): *The extreme Humbert tuple f over $\mathbb{K}$ is perfect. If an extreme Humbert tuple f has rank $m > 1$, then f is also weakly eutactic.*

Combining Corollary 1.2 with the last theorem we obtain the following corollary.

Corollary 2.1 (Corollary 4 in [Lei05a]): *If f is an extreme Humbert tuple over totally real or totally complex $\mathbb{K}$ and f has rational minimum $\mu(f)$, then f is a conjugate tuple.*

We end this chapter with giving some estimates for bounds of $\gamma_{m,\,\mathbb{K}}$. The Hermite's constant (for quadratic forms of rank ℓ over rational numbers) is denoted by γ_ℓ.

Theorem 2.2 (Theorem 6 in [Lei05a]): *For any algebraic number field $\mathbb{K}$ and for any $m \geq 1$ we have the upper bound*

$$\gamma_{m,\,\mathbb{K}} \leq \gamma_{m\cdot[\mathbb{K}:\mathbb{Q}]}|\mathrm{disc}(\mathbb{K})|^{1/[\mathbb{K}:\mathbb{Q}]}. \tag{2.3}$$

This is the best upper bound. For example, the upper bound is attained for $\gamma_{1,\,\mathbb{Q}(\sqrt{3})}$, $\gamma_{2,\,\mathbb{Q}(\sqrt{2})}$, $\gamma_{2,\,\mathbb{Q}(\sqrt{3})}$ and $\gamma_{2,\,\mathbb{Q}(\sqrt{6})}$. The second and the third case can be verified immediately using Ong's results [Ong86] and the last case can be verified using Leibak's result [Lei05b].

Unfortunately, the explicit values of γ_ℓ are known only for $2 \leq \ell \leq 8$ [OW01]. Using the upper bound

$$\gamma_l \leq \frac{4}{\sqrt[\ell]{\varrho^2}},$$

(ϱ denotes the volume of the unit ball in $\mathbb{R}^\ell$) instead of γ_ℓ we obtain the upper bound derived by Koecher [Koe60, Lemma 11].

The following corollary follows immediately from Theorem 2.2.

Corollary 2.2 (Corollary 5 in [Lei05a]): *Let f be a positive quadratic form over algebraic number field $\mathbb{K}$. If the rational quadratic form $\mathrm{Tr}f$ is critical over $\mathbb{Q}$, then f is critical over $\mathbb{K}$.*

Let $\gamma^*_{m,\mathbb{K}}$ denote the Hermite-Humbert constant introduced by Icaza (see [Ica97]).

Proposition 2.1 (Proposition 4 in [Lei05a]): *For any algebraic number field $\mathbb{K}$ of degree n over $\mathbb{Q}$, we have*

$$\gamma_{m,\mathbb{K}} \geqslant n\sqrt[n]{\gamma^*_{m,\mathbb{K}}}.$$

Theorem 2.3: *If $\mathbb{K}$ is a totally real number field, then there exists a critical unary form over $\mathbb{K}$.*

Example. Let ζ be a primitive 9-th root of unity. Consider the positive definite binary quadratic form

$$f(x,y) = (1+\zeta+\zeta^{-1})^2(x^2 + (\zeta+\zeta^{-1})xy + y^2)$$

over the field $\mathbb{K} = \mathbb{Q}(\zeta + \zeta^{-1})$. It follows from immediate computations that $\gamma_{\mathbb{K}}(f)$ attains the upper bound. Moreover, $\mathrm{Tr}\, f$ is also critical over $\mathbb{Q}$ and is equivalent to the quadratic form E_6. Using the computational algebraic number theory program KASH we found that the matrix of $\mathrm{Tr}\, f$ is

$$\frac{9}{2}\begin{pmatrix} 2 & 1 & 2 & 2 & 4 & 2 \\ 1 & 2 & 2 & 2 & 2 & 4 \\ 2 & 2 & 4 & 2 & 4 & 5 \\ 2 & 2 & 2 & 4 & 5 & 4 \\ 4 & 2 & 4 & 5 & 10 & 4 \\ 2 & 4 & 5 & 4 & 4 & 10 \end{pmatrix}.$$

Applying the transformation by matrix

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

we obtain the equivalent senary quadratic form (we omit the multiplier $\frac{9}{2}$)

$$E_6 = \begin{pmatrix} 2 & 1 & 0 & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & 1 & 1 & 1 \\ 0 & 0 & 1 & 2 & 1 & 0 \\ 0 & 0 & 1 & 1 & 2 & 0 \\ 0 & 0 & 1 & 0 & 0 & 2 \end{pmatrix}.$$

As

$$\begin{aligned} \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(1+\zeta+\zeta^{-1})^2(x^2+(\zeta+\zeta^{-1})xy+y^2) = \\ = \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}\mathrm{Nm}_{\mathbb{Q}(\zeta)/\mathbb{K}}\,(1+\zeta+\zeta^{-1})(x+\zeta y), \qquad x,y\in\mathbb{Q} \end{aligned} \tag{2.4}$$

we have that the senary quadratic form $\mathrm{Tr}\, f$ (over reals) is proportional to the quadratic form arising from the trace norm (see [CS99, p. 225])

$$N(\nu((1+\zeta+\zeta^{-1})(x+\zeta y))) = \frac{1}{2}\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(1+\zeta+\zeta^{-1})^2(x^2+(\zeta+\zeta^{-1})xy+y^2),$$

where $\nu(\alpha)$ denotes the tuple of field conjugates of the algebraic number α.

Last remark demonstrates the connection between the $\mathrm{Tr}\, f$ and the trace norm.

3. Binary additive perfect forms over number field $\mathbb{Q}(\sqrt{6})$

In this chapter we apply the theory developed in Chapters 1 and 2 to enumerate all non-equivalent binary perfect forms over number field $\mathbb{Q}(\sqrt{6})$. This work is a continuation of the Ong's work [Ong86].

We begin with recalling some definitions.

Definition 3.1: *A matrix $S \in \mathrm{GL}(m, \mathcal{O}_{\mathbb{K}})$ is called an automorph of $f \in \mathcal{P}_{m,\mathbb{K}}$, $f(x) = x^t(f_{ij})x$, if $(f_{ij}) = S^t(f_{ij})S$.*

For each $S \in \mathrm{GL}(m, \mathcal{O}_{\mathbb{K}})$ we write $\mathcal{T}_S$ for the mapping $\mathcal{P}_{m,\mathbb{K}} \to \mathcal{P}_{m,\mathbb{K}}$ defined by $\mathcal{T}_S(f) = S^t(f_{ij})S$ where $f(x) = x^t(f_{ij})x$. We call quadratic forms $f, g \in \mathcal{P}_{m,\mathbb{K}}$ equivalent and write $f \sim g$ if there exist $\mathcal{T}_S$ such that $g = \mathcal{T}_S(f)$.

For a quadratic form f and $S \in \mathrm{GL}(\mathrm{rank} f, \mathcal{O}_{\mathbb{K}})$ we write $f[S]$ for $S^t(f_{ij})S$.

Definition 3.2: *A mapping $\mathcal{T}_S$ is called an integral automorphism of f if S is an automorph of f.*

The group of all integral automorphisms of f is denoted by $\mathrm{Aut}_{Int}(f)$.

As it was mentioned already in Chapter 1, if $f(x)$ is a positive definite quadratic form over totally real number field $\mathbb{K}$, then the quadratic form $\mathrm{Tr}\, f(x)$ is a positive definite over $\mathbb{Q}$. So we are interested in exploiting the symmetry of the quadratic form $\mathrm{Tr}\, f(x)$ that can be used to 'simplify' Voronoï's algorithm. This motivates the following definition.

Definition 3.3: *By the automorphism of $f (f \in \mathcal{P}_{m,\mathbb{K}})$ we mean a mapping of the form $\tau \circ \mathcal{T}_S$, where $S \in \mathrm{GL}(m, \mathcal{O}_{\mathbb{K}})$ and $\tau \in \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ such that*

$$(\tau \circ \mathcal{T}_S)(f) = f.$$

If $\mathbb{K}$ is not a normal extension then we set $\tau = \mathrm{Id}$.

Denote by $\mathrm{Aut}(f)$ the group of all automorphisms of f.

By $\mathrm{Stab}(f)$ we mean the subgroup $\{\sigma \in \mathrm{Gal}(\mathbb{K}/\mathbb{Q}) | \sigma(f) \sim f\}$.

3.1 Voronoï's algorithm

Voronoï's algorithm is discussed in detail in [Bar57, Mar03, Ong86]. Theoretical background of perfect polyhedral cones with respect to bilinear product can be found in [Koe60, Mar03]. Here we present a short outline of the algorithm and discuss some theoretical results concerningcomputational advantages in applying Voronoï's algorithm.

Let $\mathcal{M}(f) = \{m_1, \ldots, m_t\}$. With each trace minimum vector m_k we associate a tuple of linear forms

$$\widehat{\lambda}_k = (\lambda_{k;1}, \ldots, \lambda_{k;r})$$

such that

$$\lambda_{k;i}(x) = \sigma_i(m_k) \cdot x = \sigma_i(m_{k,1})x_1 + \ldots + \sigma_i(m_{k,n})x_n.$$

Write $\widehat{\lambda}_k^2 = (\lambda_{k;1}^2, \ldots, \lambda_{k;r}^2)$. The perfect polyhedral cone Π_f associated to perfect form f with trace minimums $m_1, \ldots, m_t$ is defined as a polyhedral cone generated by tuples of quadratic forms $\widehat{\lambda}_1^2, \ldots, \widehat{\lambda}_t^2$, that is

$$\Pi_f = \left\{ \sum_{k=1}^{t} \rho_k \widehat{\lambda}_k^2 \,|\, \rho_1 \geqslant 0, \ldots, \rho_t \geqslant 0 \right\}.$$

The perfect polyhedral cones partition the set $\overline{\mathcal{P}_{n,\mathbb{K}}}$, thus two perfect polyhedral cones $\Pi_f \neq \Pi_g$ have no common inner points by Proposition 2 in [Koe60].

We write $\mathrm{Sym}_n(\mathbb{K})$ ($\mathrm{Sym}_{n,\geqslant 0}(\mathbb{K})$) for the set of all symmetric (respectively, the set of all symmetric positive semi-definite) $n \times n$-matrices with entries in $\mathbb{K}$. Let

$$\langle A, B \rangle = \sum_{i=1}^{r} \mathrm{TR}(A^{(i)} B^{(i)})$$

where $A = (A^{(1)}, \ldots, A^{(r)}), B = (B^{(1)}, \ldots, B^{(r)}) \in \mathbb{R} \otimes \mathrm{Sym}_n(\mathbb{K})$.

The perfect polyhedral cone can be described also in the terms of symmetric matrices which satisfy the certain number of homogenous linear inequalities

$$\Pi_f = \{B | B \in \mathbb{R} \otimes \mathrm{Sym}_n(\mathbb{K}), \psi_\ell(B) = \langle A_\ell, B \rangle \geqslant 0, \ell = 1, \ldots, u\}$$

where $A_\ell \in \mathbb{R} \otimes \mathrm{Sym}_{n,\geqslant 0}(\mathbb{K})$. The dimension of Π_f is $N = r\frac{n(n+1)}{2}$. The cone Π_f is determined by u hyperplanes $H_\ell = \{B \in \mathbb{R} \otimes \mathrm{Sym}_n(\mathbb{K}) | \langle \Psi_\ell, B \rangle = 0\}$, $\Psi_\ell \in \mathbb{R} \otimes \mathrm{Sym}_n(\mathbb{K})$, and bounded by u faces $W_\ell = \Pi_f \cap H_\ell$ of dimension $N-1$. Write $A_k = \big(\sigma_1(m_k m_k^t), \ldots, \sigma_r(m_k m_k^t)\big)$. Every edge

$$\Lambda_k = \{\rho A_k | \rho \in \mathbb{R}_{\geqslant 0}\}, \quad k = 1, \ldots, s$$

is the solution of a system of $N-1$ linearly independent equations $\langle \Psi_\ell, B\rangle = 0$, $\ell = 1, \ldots, N-1$. Moreover Ψ_ℓ is determined by $N-1$ linearly independent edges

$$\langle \Psi_\ell, A_k\rangle = 0, \quad k = 1, \ldots, N-1$$

with an unknown Ψ_ℓ.

To each $(N-1)$-dimensional face W of Π_f there corresponds a uniquely determined neighbouring perfect polyhedral cone Π_g with $\Pi_f \cap \Pi_g = W$, such that the perfect form g is not multiple of f (see [Koe60]; Koecher also proved that if Π_f and Π_g are arbitrary perfect polyhedral cones, then the intersection $\Pi_f \cap \Pi_g$ is an r-dimensional face of Π_f and Π_g where $0 \leqslant r < N$).

We call these forms f and g neighbouring forms along the face W, or simply, neighbouring forms. As Barnes [Bar57] pointed out the practical efficiency of Voronoï's method lies in the simplicity of the relation between neighbouring forms. Let f and g be neighbouring forms along the face $W = \{A \in \mathbb{R}\otimes \mathrm{Sym}_{n,\geqslant 0}(\mathbb{K}) | \langle \Psi, A\rangle = 0\}$ and $\Psi \in \mathbb{R} \otimes \mathrm{Sym}_n(\mathbb{K})$. Denote by $\psi(x)$ the indefinite quadratic form

$$\psi(x) = \sum_{i,j=1}^{n} b_{ij} x_i x_j \quad (b_{ij} = b_{ji})$$

corresponding to the face W, that is, if $B = (b_{ij})$, then $\Psi = (\sigma_1(B), \ldots, \sigma_r(B))$. Koecher proved [Koe60] (if $\mathbb{K}$ is a real quadratic extension see also Theorem 3.1.6 in [Ong86]) that if W is a face of Π_f determined by the $N-1$ independent edge forms $\widehat{\lambda}_1, \ldots, \widehat{\lambda}_u$, then neighbouring form g corresponding to the neighbouring cone Π_g along the face W i.e. $W = \Pi_f \cap \Pi_g$ is

$$g = f + \lambda\psi$$

and $\lambda > 0$ is uniquely determined by

$$\lambda = \inf \left\{ \frac{\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(f(x)) - \mu(f)}{-\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\psi(x))} \Big| \, x \in \mathcal{O}_{\mathbb{K}}^n \wedge \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\psi(x)) < 0 \right\}.$$

Moreover, λ is a rational number. The edge forms $\widehat{\lambda}_1, \ldots, \widehat{\lambda}_u$ ($u \geq N-1$) determine the face W which is defined by quadratic form ψ iff

$$\begin{array}{rcll} \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\psi(m_i)) & = & 0 & (i = 1, \ldots, u), \\ \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\psi(m_i)) & > & 0 & (i > u) \end{array} \tag{3.1}$$

and the system (3.1) has rank $N-1$.

For the rest of this section we assume that $\mathbb{K}$ is a normal extension.

Proposition 3.1 (Proposition 2 in [Lei05b]): *If f is perfect quadratic form over $\mathbb{K}$, then $\sigma(f)$ is also perfect for all $\sigma \in \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$.*

Proposition 3.2 (Proposition 3 in [Lei05b]): *If f and g are neighbouring forms, then $\sigma(f)$ and $\sigma(g)$ are neighbouring forms for each $\sigma \in \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$.*

Proposition 3.3 (Proposition 4 in [Lei05b]): *The set of neighbouring forms of f is the union of the orbits by $\mathrm{Stab}(f)$.*

Proposition 3.4 (Proposition 5 in [Lei05b]): *Let W, W' be faces of Π_f and W, W' are equivalent under $\mathrm{Aut}_{Int}(f)$. Suppose that the quadratic forms ψ, ψ' correspond to W, W' respectively. Then the perfect neighbouring forms $f + \lambda\psi$ and $f + \lambda\psi'$are equivalent.*

Corollary 3.1 (Corollary 1 in [Lei05b]): *Let f be a perfect quadratic form over $\mathbb{K}$. Then $\mathrm{Aut}(f)$ decomposes the set of neighbours of f into orbits by $\mathrm{Stab}(f)$.*

We can simplify our computations by making following observations:

1. If f is perfect, then $\sigma(f)$ is also perfect for any $\sigma \in \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$.
2. If f and g are neighbouring forms, then $\sigma(f)$ and $\sigma(g)$ are neighbouring forms too for any $\sigma \in \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$. Once we have the neighbouring forms of f, then we have also the neighbouring forms of $\sigma(f)$ for any field automorphism $\sigma \neq 1$ without applying Voronoï's algorithm.
3. The set of neighbours of f is a union of orbits by $\mathrm{Stab}(f)$ (see Proposition 3.3).
4. Equivalent faces W, W' of Π_f under action by $\mathrm{Aut}_{Int}(f)$ yield equivalent neighbouring forms g, g' (see Proposition 3.4). Let $\varphi \in \mathrm{Aut}(f)$ and let the face W be determined by minimum vectors $m_1, \ldots, m_u \in \mathcal{M}(f)$ by (3.1). Write $\varphi = \tau \circ \mathcal{T}_S$, where $\tau \in \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ and $S \in \mathrm{GL}(\mathrm{rank} f, \mathcal{O}_{\mathbb{K}})$. If the positive semi-definite quadratic form ψ corresponds to the face W, then by permuting minimum vectors by $x \rightsquigarrow S\tau^{-1}(x)$, we obtain a new face, say W', determined by $S\tau^{-1}(m_1), \ldots, S\tau^{-1}(m_u)$

   $$\begin{aligned} \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\psi'(S\tau^{-1}(m_i))) &= \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\varphi(\psi')(m_i)) = 0 \quad (i = 1, \ldots, u), \\ \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\psi'(S\tau^{-1}(m_i))) &= \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\varphi(\psi')(m_i)) > 0 \quad (i > u). \end{aligned}$$

   Thus we may take $\varphi(\psi') = \psi$. Since S is an automorphism of f, then the faces W, W' are equivalent under $\mathrm{Aut}(f)$ (see Proposition 3.4 and Corollary 3.1). Also, we have

   $$f + \lambda\psi' = \varphi^{-1}(f) + \lambda\varphi^{-1}(\psi) = \varphi^{-1}(f + \lambda\psi).$$

   The group $\mathrm{Aut}(f)$ partitions set $\{M \subseteq \mathcal{M}(f) | \#M = N - 1\}$ into orbits $\mathcal{K}_1, \ldots, \mathcal{K}_U$. According to Corollary 3.1 we apply Voronoï's algorithm to the representatives of $\mathcal{K}_1, \ldots, \mathcal{K}_U$ only.

Starting with any perfect form f, we find all its inequivalent neighbours, discarding any equivalent one to f. We now find all inequivalent neighbours of these forms, discarding any equivalent form to perfect forms already found, and so on. This process stops after finite number of steps because there exist only finitely many inequivalent (up to homothety) perfect forms (see Proposition 8 in [Koe60]). At each step (i.e. finding all inequivalent neighbours of a perfect form f), if the group $\mathrm{Aut}(f)$ is non-trivial, then we partition the set $\mathcal{M}(f)$ into orbits of $\mathrm{Aut}(f)$ and study the representatives of each orbit. Then we apply the Corollary 3.1 to the result.

The total number of systems of $N-1$ linear equations is $\binom{\#\mathcal{M}(f)}{N-1}$ and it can be very large even when we have used the partition by $\mathrm{Aut}(f)$, thus computer algorithm was used to study those systems.

3.2 Binary perfect forms and elliptic fixed points of Hilbert modular group

In this section we recall some basic facts about binary perfect forms and elliptic fixed points of Hilbert modular group. We refer to [Fre90] for more facts about Hilbert modular groups. We attach to each matrix $M \in \mathrm{GL}(2,\mathbb{K})$ the tuple

$$(\sigma_1(M),\ldots,\sigma_r(M)) \in \mathrm{GL}(2,\mathbb{R})^r$$

and obtain the imbedding

$$\mathrm{GL}(2,\mathbb{K}) \hookrightarrow \mathrm{GL}(2,\mathbb{R})^r. \tag{3.2}$$

Write $\mathrm{GL}^+(2,\mathbb{K}) = \{M \in \mathrm{GL}(2,\mathbb{K}) | \det(M) \text{ is totally positive}\}$. Let $\mathfrak{H} = \{z \in \mathbb{C} | \Im(z) > 0\}$. Using the imbedding (3.2) one defines the action of $\mathrm{GL}^+(2,\mathbb{K})$ on $\mathfrak{H}^r$ as a componentwise fractional-linear transformation, that is if $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}^+(2,\mathbb{K})$ and $(z_1,\ldots,z_r) \in \mathfrak{H}^r$, then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}(z_1,\ldots,z_r) = \left(\frac{\sigma_i(a)z_i + \sigma_i(b)}{\sigma_i(c)z_i + \sigma_i(d)}\right)_{i=1}^{r}.$$

We shall identify the matrix $M \in \mathrm{GL}^+(2,\mathbb{K})$ and its image under the embedding into $\mathrm{GL}(2,\mathbb{R})^r$.

Let $f(x,y) = ax^2 + bxy + cy^2$ be a positive definite binary quadratic form over $\mathbb{K}$ and assume that $\sigma_i(f)$ can be factored as follows

$$\sigma_i(a)(\sigma_i(x) - \tau_i\sigma_i(y))(\sigma_i(x) - \bar{\tau}_i\sigma_i(y)), \quad (\tau_1,\ldots,\tau_r) \in \mathfrak{H}^r.$$

Here $\bar{\tau}_i$ denotes the complex conjugate of τ_i . Therefore we obtain the map from the set of all positive definite binary quadratic forms over $\mathbb{K}$ into $\mathfrak{H}^r$

$$f \rightsquigarrow (\tau_1,\ldots,\tau_r).$$

Write $\Gamma = \mathrm{SL}(2, \mathcal{O}_{\mathbb{K}})$ for the Hilbert modular group of $\mathbb{K}$.

It is known that the Hilbert modular group acts discontinuously on $\mathfrak{H}^r$ [Fre90, Remark 2]. The points z, $z' \in \mathfrak{H}^r$ are called equivalent and will be denoted by $z \sim z'$, if there exists a $M \in \Gamma$ such that $Mz = z'$. One can show that if positive definite quadratic forms f and f' satisfies $\alpha f' = f[M]$ for some $M \in \Gamma$ ($M \in \mathrm{GL}^+(2, \mathcal{O}_{\mathbb{K}})$) and totally positive $\alpha \in \mathbb{K}$, then the corresponding points z, $z' \in \mathfrak{H}^r$ are equivalent under Γ (under $\mathrm{GL}^+(2, \mathcal{O}_{\mathbb{K}})$ respectively).

By the elliptic fixed point of Γ we mean the point $z \in \mathfrak{H}^r$ if its stabiliser $\Gamma_z \leqslant \Gamma$ is not equal to $\{\pm E\}$. Moreover, Γ_z is finite and $\Gamma_z/\{\pm E\}$ is cyclic [Fre90, Remark 2.14].

For a real quadratic number field $\mathbb{K}$ with totally positive fundamental unit ε we write $\Gamma_{(\varepsilon)} = \mathrm{GL}^+(2, \mathcal{O}_{\mathbb{K}})/\{M \in \mathrm{GL}^+(2, \mathcal{O}_{\mathbb{K}}) | \det(M) = \varepsilon^{2l}, l \in \mathbb{Z}\}$ for the extended Hilbert modular group. Since $\mathbb{K} = \mathbb{Q}(\sqrt{6})$ has a totally positive fundamental unit $\varepsilon = 5 + 2\sqrt{6}$, we consider elliptic fixed points with respect to the extended Hilbert modular group $\Gamma_{(\varepsilon)}$ too.

Some binary perfect forms have a large automorphism group, hence the points in $\mathfrak{H}^r$ associated to those forms are elliptic fixed points. The number of inequivalent elliptic fixed points of order e ($e \in \{2, \ldots, 6\}$) for real quadratic extension $\mathbb{Q}(\sqrt{D})$ with $D \leq 97$ was computed by A. Prestel [Pre68]. As a result of our computation for enumeration the inequivalent binary perfect forms over $\mathbb{Q}(\sqrt{6})$ we found:

1) one class of perfect forms corresponding to the elliptic fixed point of order 6 under the action by $\Gamma_{(\varepsilon)}$. The representative of this class is[1]

$$\phi_8 = \frac{24 - 8\sqrt{6}}{3}x^2 + 2 \cdot 4xy + \frac{24 + 8\sqrt{6}}{3}y^2$$

and the corresponding elliptic point is

$$(z_1, z_2) = \left(\frac{-3 + \sqrt{-3}}{2(3 - \sqrt{6})}, \frac{-3 + \sqrt{-3}}{2(3 + \sqrt{6})}\right). \tag{3.3}$$

Under the action by Γ the points (z_1, z_2), (z_2, z_1) are inequivalent and have order 3;

2) one class of perfect form corresponding to elliptic fixed point of order 4 with respect to the group $\Gamma_{(\varepsilon)}$. The quadratic form is

$$\phi_9 = \frac{24 + 6\sqrt{6}}{3}x^2 + 2\frac{12 + 8\sqrt{6}}{3}xy + \frac{24 + 4\sqrt{6}}{3}y^2$$

with corresponding elliptic fixed point

$$(w_1, w_2) = \left(\frac{-(3 + 2\sqrt{6}) + \sqrt{-3\varepsilon}}{2(3 + \sqrt{6})}, \frac{-(3 - 2\sqrt{6}) + \sqrt{-3\varepsilon^{-1}}}{2(3 - \sqrt{6})}\right). \tag{3.4}$$

[1] We use the same notation for binary perfect form as in the Table 3.3 at page 20.

Under the action by Γ the points $(w_1, w_2) \not\sim (w_2, w_1)$ are of order 2;

3) two classes of perfect binary forms corresponding to the elliptic fixed point of order 3. The representatives of these classes are the initial perfect form and its field conjugate

$$\begin{aligned} \phi_0 &= (8+3\sqrt{6})(x^2+xy+y^2), \\ \overline{\phi_0} &= (8-3\sqrt{6})(x^2+xy+y^2). \end{aligned}$$

The corresponding elliptic fixed point of order 3 with respect to the groups $\Gamma_{(\varepsilon)}$ and Γ is (τ, τ), where $\tau = \frac{-1+\sqrt{-3}}{2} \in \mathfrak{H}$ is the elliptic fixed point of order 3 with respect to the group $\mathrm{SL}(2, \mathbb{Z})$. Since ϕ_0 and $\overline{\phi_0}$ are homothetic, they correspond to the same point $z \in \mathfrak{H}^2$.

This result coincides with the number of elliptic fixed points of orders 6 and 3 found by Prestel [Pre68, p. 208]. Under the action by Γ the inequivalent elliptic fixed points of order 3 are

$$(\tau, \tau), \quad (z_1, z_2) \quad \text{and} \quad (z_2, z_1).$$

With respect to the $\Gamma_{(\varepsilon)}$ there is an elliptic fixed point (z_1, z_2) is of order 6 and an (τ, τ) is of order 3.

3.3 List of binary perfect forms over $\mathbb{Q}(\sqrt{6})$

The main idea of finding perfect forms relies on applying the generalisation of Voronoï's algorithm to inequivalent perfect forms already found.

Proposition 3.5 (Corollary 2 in [Lei05b]): *Unary form $(8+3\sqrt{6})x^2$ is perfect over $\mathbb{Q}(\sqrt{6})$.*

The list of binary perfect forms is computed as follows. Combining the Proposition 3.5 with the Theorem 1.1, we obtain an initial perfect form

$$\phi_0 = (8+3\sqrt{6})(x^2+xy+y^2).$$

Starting with the initial perfect form ϕ_0, we find all its inequivalent neighbours (by applying the generalisation of Voronoï's algorithm to ϕ_0), discarding any neighbour equivalent to ϕ_0. We now find all inequivalent neighbours of these forms, discarding any equivalent form to perfect ones already found, and so on. This process stops after finite number of steps because there exist only finitely many inequivalent (up to homothety) perfect forms (see Proposition 8 in [Koe60]). At each step (i.e. finding all inequivalent neighbours of a perfect form f), if f is not equivalent to its field conjugate $\bar{f}$, we obtain the inequivalent neighbours of f by applying

Proposition 3.1 to the neighbours of f. If both g and $\bar{g}$ come out as inequivalent neighbours of f, then we apply the generalisation of Voronoï's algorithm to g only.

At each step the generalisation of Voronoï's algorithm requires the investigation of system of $\binom{\#\mathcal{M}(f)}{5}$ ($6 \leq \#\mathcal{M}(f) \leq 12$) equations, a computer algorithm was used to study those systems.

Since neither explicit description of the reduction domain for binary quadratic forms over $\mathbb{Q}(\sqrt{6})$ nor the reduction algorithm has been published until now, we shall compare invariants such as determinant of quadratic form and norm of the determinant in order to detect the inequivalence of quadratic forms. If $\mathrm{Nm}\det(f) = \mathrm{Nm}\det(g)$ for binary perfect quadratic forms f, g, then we study further those forms to determine whether they are equivalent or not. For example, from $f \sim g$ it follows that $\#\mathcal{M}(f) = \#\mathcal{M}(g)$ and $\mathrm{Aut}(f) \cong \mathrm{Aut}(g)$.

Theorem 3.1 (Theorem 2 in [Lei05b]): *There exist exactly* 22 *classes of binary perfect forms with coefficients in* $\mathbb{Q}(\sqrt{6})$.

Table 3.1: **List of binary perfect forms over number field $\mathbb{Q}(\sqrt{6})$.**

Perfect form f	field conjugate of $\overline{f}$
ϕ_0:$(8+3\sqrt{6})(x^2+xy+y^2)$	$\overline{\phi_0}$:$(8-3\sqrt{6})(x^2+xy+y^2)$
ϕ_1:$(8+3\sqrt{6})x^2-(4+2\sqrt{6})xy+(8+3\sqrt{6})y^2$	$\overline{\phi_1}$:$(8-3\sqrt{6})x^2-(4-2\sqrt{6})xy+(8-3\sqrt{6})y^2$
ϕ_2:$(8+3\sqrt{6})x^2+2\frac{20+9\sqrt{6}}{5}xy+(8+3\sqrt{6})y^2$	$\overline{\phi_2}$:$(8-3\sqrt{6})x^2+2\frac{20-9\sqrt{6}}{5}xy+(8-3\sqrt{6})y^2$
ϕ_3:$(8+3\sqrt{6})x^2+2xy+\frac{16+5\sqrt{6}}{2}y^2$	$\overline{\phi_3}$:$(8-3\sqrt{6})x^2+2xy+\frac{16-5\sqrt{6}}{2}y^2$
ϕ_4:$(8+3\sqrt{6})x^2+4xy+\frac{16+\sqrt{6}}{2}y^2$	$\overline{\phi_4}$:$(8-3\sqrt{6})x^2+4xy+\frac{16-\sqrt{6}}{2}y^2$
ϕ_5:$(8+3\sqrt{6})x^2-(6+2\sqrt{6})xy+\frac{24-7\sqrt{6}}{3}y^2$	$\overline{\phi_5}$:$(8-3\sqrt{6})x^2-(6-2\sqrt{6})xy+\frac{24+7\sqrt{6}}{3}y^2$
ϕ_6:$(8+\sqrt{6})x^2+(6+\sqrt{6})xy+(8+3\sqrt{6})y^2$	$\overline{\phi_6}$:$(8-\sqrt{6})x^2+(6-\sqrt{6})xy+(8-3\sqrt{6})y^2$
ϕ_7:$(8+3\sqrt{6})x^2+4xy+(8-3\sqrt{6})y^2$	ϕ_7
ϕ_8:$\frac{24-8\sqrt{6}}{3}x^2+8xy+\frac{24+8\sqrt{6}}{3}y^2$	ϕ_8
ϕ_9:$\frac{24+8\sqrt{6}}{3}x^2+2\frac{12+8\sqrt{6}}{3}xy+\frac{24+4\sqrt{6}}{3}y^2$	ϕ_9
ϕ_{10}:$(8+3\sqrt{6})x^2+(6+\sqrt{6})xy+\frac{96+13\sqrt{6}}{12}y^2$	$\overline{\phi_{10}}$:$(8-3\sqrt{6})x^2+(6-\sqrt{6})xy+\frac{96-13\sqrt{6}}{12}y^2$
ϕ_{11}:$(8+3\sqrt{6})x^2+2\frac{2\sqrt{6}}{3}xy+(8-3\sqrt{6})y^2$	ϕ_{11}
ϕ_{12}:$(8+3\sqrt{6})x^2+(6+\sqrt{6})xy+\frac{96-31\sqrt{6}}{12}y^2$	$\overline{\phi_{12}}$:$(8-3\sqrt{6})x^2+(6-\sqrt{6})xy+\frac{96+31\sqrt{6}}{12}y^2$

Abstract

In this thesis, the additive generalisation of the Voronoï's theory for algebraic number fields and the complete enumeration of binary perfect quadratic forms over $\mathbb{Q}(\sqrt{6})$ were presented. In the former case, the additive Hermite's constant was defined. The definitions of perfect forms, extreme forms, critical forms, weak eutactic forms and conjugate tuple were also given. In this thesis it was shown, that any perfect Humbert tuple over totally real or totally complex number field $\mathbb{K}$ is proportional to a conjugate tuple over $\mathbb{K}$. This thesis also includes an overview of Voronoï's algorithm for algebraic number fields. Since the algorithm requires an initial perfect form, the constructions for perfect form were studied. Assuming $\mathbb{K}$ being totally real, new constructions of perfect forms based on tensor product of quadratic forms were given. One of those constructions based on the assumption that we have an initial unary perfect form over $\mathbb{K}$, thus the constructions for an unary perfect form were presented if $\mathbb{K}$ is either real quadratic field or totally real maximal subfield of the cyclotomic field $\mathbb{Q}(\zeta_n)$, where $n > 4$ is a square-free odd integer with $3 \nmid n$. Moreover, the existence of an initial unary perfect form over totally real $\mathbb{K}$ with $m \geq 1$ variables was proved.

The necessary part of the well-known Voronoï's theorem was generalised if eutaxy is replaced by weak eutaxy.[2] The upper and lower bounds of the additive Hermite's constant were derived. The presented upper bound is better than the one given by Koecher [Koe60, Lemma 11].

As a result of the theory, the complete enumeration of binary perfect forms over the quadratic field $\mathbb{Q}(\sqrt{6})$ was given. The number field $\mathbb{Q}(\sqrt{6})$ was chosen as a continuation of Ong's work (see [Ong86]). The Voronoï's algorithm was studied and some improvement based on the Galois' action were presented. These improvements give computational advantages in applying generalised Voronoï's algorithm. Also new constructions for the quadratic forms corresponding to the lattices E_6 and E_8 were given.

[2] The claim for weak eutaxy holds iff the number of variables is at least 2.

Kokkuvõte

1908. aastal ilmus G. F. Voronoi artikkel, kus ta esitas *Voronoi teooria* põhitulemused. Oma artiklis käsitles ta reaalarvuliste kordajatega positiivselt määratud ruutvorme. Pool sajandit hiljem uuris Koecher positiivselt määratud ruutvorme üle algebraliste arvukorpuste. 1960. aastal ilmunud artiklis vaatles ta ruutvormide asemel nn. Humbert'i korteeže ning selle järjendi elementide summa teatud miinimume. Koecher esitas täiuslikkuse definitsiooni ja üldistas ka Hermite'i arvu mõistet algebralistele arvukorpustele. 1983. aastal üldistas Ong Voronoi algoritmi reaalsetele ruutlaienditele ning esitas täiuslike binaarsete ruutvormide (Ong vaatles ainult ruutvormidele vastavaid Humbert'i korteeže, kuid mitte üldjuhtu) loetelu üle korpuste $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ ja $\mathbb{Q}(\sqrt{5})$.

Käesolevas töös uuriti täiuslike ruutvormide Voronoi teooria aditiivset üldistust arvukorpustele ning esitati binaarsete täiuslike ruutvormide loetelu üle korpuse $\mathbb{Q}(\sqrt{6})$. Üldistati Hermite'i arvu mõiste, defineeriti üldistatud Hermite'i konstant ning tuletati üldistatud Hermite'i konstandi ülemine ja alumine tõke. Tõestati, et iga kriitiline Humbert'i korteež f on täiuslik ja juhul kui Humbert'i korteeži f muutujate arv on vähemalt 2, siis f on nõrgalt eutaktiline. Veel tõestati, et kui põhikorpus on täielikult reaalne, siis leidub alati kriitiline unaarne Humbert'i korteež. Näidati, et kui põhikorpus on kas täielikult reaalne või täielikult kompleksne, siis iga täiuslik Humbert'i korteež on proportsionaalne kaaselementidest moodustatud ruutvormide või Hermite'i vormide korteežiga. Saadud tulemus näitab, et täiuslike ruutvormide loetelu üle täielikult reaalse arvukorpuse $\mathbb{K}$ langeb kokku täiuslike Humbert'i korteežide loeteluga üle $\mathbb{K}$ ning täiuslike binaarsete ruutvormide loetelud, mida esitas Ong, on täiuslike binaarsete Humberti korteežide loetelud üle vastavate ruutlaiendite. Töö üheks põhitulemuseks on täiusliku ruutvormi ehitamise üldine algoritm muutujate arvu $m \geq 2$ korral, kui põhikorpuseks on täielikult reaalne arvukorpus ja on teada unaarne täiuslik ruutvorm. Täiusliku unaarse ruutvormi ehitamise algoritm tuletati juhtudel, kui põhikorpuseks on kas reaalne ruutlaiend või korpus $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$, kus ζ_n on primitiivne n-astme ühejuur ja $n \not\vdots 3$ on paaritu ruuduvaba naturaalarv. Täiuslikku ruutvormi muutujate arvuga m on vaja selleks, et Voronoi algoritmi üldistuse abil leida kõik ülejäänud (ruutvormide ekvivalentsi täpsusega) täiuslikud ruutvormid m-muutujast üle korpuse $\mathbb{K}$. Teades kõiki täiuslikke ruutvorme m-muutujast, saame nende jaoks arvutada üldistatud Hermite'i arvu ning nende ruutvormide hulgst otsida nn. ekstremaalseid ruutvorme (st. ruutvorme, millele vastavad võred annavad "tiheda"

võrelise pakkimise).

Uuriti täiuslike ruutvormide omadusi Galois' rühma toime suhtes. Näidati, kuidas saab Galois' rühma kasutada Voronoi algoritmi arvutusmahu vähendamiseks (rakendades täiuslikule ruutvormile korpuse automorfismi saame jällegi täiusliku ruutvormi, viimase naabrid saame esimese naabritest, kui rakendame neile sama automorfismi jne.).

Binaarsete täiuslike ruutvormide loetelu koostamisel üle korpuse $\mathbb{Q}(\sqrt{6})$ vaadeldi ka nendele ruutvormidele vastavaid elliptilisi püsipunkte ülemise komplekspoolttasandi otseruudus. Näidati, et kolmandat ja kuuendat järku elliptiliste püsipunktide arv langeb kokku tulemusega, mille esitas Prestel 1968. aastal.

Esitati ruutvormide E_6 ja E_8 uued konstruktsioonid.

References

[Bar57] E. S. Barnes. The complete enumeration of extreme senary forms. *Phil. Trans. Roy. Soc. London*, 249:461–506, 1957.

[BCIO01] Ricardo Baeza, Renaud Coulangeon, Maria Ines Icaza, and Manuel O'Ryan. Hermite's Constant for Quadratic Number Fields. *Experimental Mathematics*, 10(4):543–552, 2001.

[BI97] Ricardo Baeza and Maria Ines Icaza. On Humbert-Minkowski's constant for a number field. *Proc. Am. Math. Soc.*, 125:3195–3202, 1997.

[BI04] Ricardo Baeza and Maria Ines Icaza. On the unimodularity of minimal vectors of Humbert forms. *Arch. Math.*, 83:528–535, 2004.

[Cou01] Renaud Coulangeon. Voronoï theory over algebraic number fields. *Monographies de l'Enseignement Mathématique*, (37):147 – 162, 2001.

[CS99] J. H. Conway and N.J.A. Sloane. *Sphere packings, lattices and groups. Third edition.*, volume 290 of *Grundlehren der mathematischen Wissenschaften*. Springer, 1999.

[Fre90] Eberhard Freitag. *Hilbert modular forms*. Springer-Verlag, 1990.

[GL87] P.M. Gruber and C.G. Lekkerkerker. *Geometry of numbers*. North-Holland, 1987.

[Ica97] Maria Ines Icaza. Hermite constant and extreme forms. *J. London Math. Soc.*, 55:11–22, 1997.

[Kit93] Yoshiyuki Kitaoka. *Arithmetic of quadratic forms*. Cambridge University Press, 1993.

[Koe60] Max Koecher. Beiträge zu einer Reduktionstheorie in Positivitätsbereichen I. *Mat. Annalen*, 141:384–432, 1960.

[Lan94] Serge Lang. *Algebraic Number Theory*. Number 110 in Graduate texts in mathematics. Springer, second edition, 1994.

[Lei02] Alar Leibak. Some results on reduction of positive quadratic forms over totally real cyclic number fields. In *International Conference on*

Analytic and Probabilistic Number Theory in Palanga, pages 162–168. TEV, 2002.

[Lei05a] Alar Leibak. On additive generalization of Voronoï's theory for algebraic number fields. *Proc. Estonian Acad. Sci. Phys. Math.*, 54(4):195–211, 2005.

[Lei05b] Alar Leibak. The complete enumeration of binary perfect forms over algebraic number field $\mathbb{Q}(\sqrt{6})$. *Proc. of Estonian Acad. of Sci. Phys. Math.*, 54(4):212–234, 2005.

[Mar03] Jacques Martinet. *Perfect lattices in euclidean spaces*, volume 327 of *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag, 2003.

[Ong83] Heidrun E. Ong. *Volkommene quadratische Formen über reell-lquadratischen Zahlkörpern*. PhD thesis, Frankfurt, 1983.

[Ong86] Heidrun E. Ong. Perfect quadratic forms over real quadratic number fields. *Geometriae Dedicata*, 20:51–77, 1986.

[OW01] Shin Ohno and Takao Watanabe. Estimates of Hermite Constants for Algebraic Number Fields. *Comm. Mat. Univ. St. Pauli*, 50(1):53–63, 2001.

[Pre68] Alexander Prestel. Die elliptischen Fixpunkte der Hilbertschen Modulgruppen. *Math. Annalen*, 177:181–209, 1968.

[PW05] Michael E. Pohst and Marcus Wagner. On the computation of Hermite-Humbert constants for real quadratic number fields. *Journal de Théorie des Nombres de Bordeaux*, 17:905–920, 2005.

[Shi76] Takuro Shintani. On evaluation of zeta functions of totally real algebraic number fields at non-positive integers. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 23(2):393–417, 1976.

[Thu98] Jeffrey Lin Thunder. Higher-dimensional analogues of Hermite's constant. *Michigan Math. J.*, 45:301–314, 1998.

[Vor08] G. Voronoï. Sur quelques propriétés des formes quadratiques positives parfaites. *J. Reine Angew. Math.*, 133:97 – 178, 1908.

[Was97] Lawrence C. Washington. *Introduction to Cyclotomic Fields*, volume 83 of *Graduate Texts in Mathematics*. Springer, Berlin, second edition, 1997.

[Wat01] Takao Watanabe. A survey and a complement of fundamental Hermite constant. *Contemporary Mathematics*, 344(339–350), 2001.

[Wat03] Takao Watanabe. Fundamental Hermite constants of linear algebraic groups. *J. Mat. Soc. Japan*, 55(4):1061–1080, 2003.

[Wat04] Takao Watanabe. Certain Inequalities Satisfied by the Hermite Constants for Global Fields. *Commentarii Matematici Universitatis Sancti Pauli*, 53(1):77–83, 2004.

Appendices

Proofs

Appendix 1: Proof of theorem 1.4

Let ζ be a primitive p-th root of unity ($p > 3$). Write $\mathbb{K} = \mathbb{Q}(\zeta + \zeta^{-1})$.

The proof will be divided into three steps.

Step 1. We show there exist $r = \frac{p-1}{2}$ units $\varepsilon_1, \ldots, \varepsilon_r$ in $\mathbb{Z}[\zeta + \zeta^{-1}]$, such that

$$\mathrm{Tr}((2 - \zeta - \zeta^{-1})\varepsilon_i^2) = \mathrm{Tr}((2 - \zeta - \zeta^{-1})\varepsilon_j^2), \quad \text{for each } 1 \leq i, j \leq r\ .$$

We start with the observation that

$$2 - (\zeta + \zeta^{-1}) = (1 - \zeta) \cdot (1 - \zeta^{-1}) = (1 - \zeta) \cdot \overline{(1 - \zeta)} = \mathrm{Nm}_{\mathbb{Q}(\zeta)/\mathbb{K}}(1 - \zeta).$$

Suppose $\sigma \in \mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \triangleleft \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. Let us consider the fraction

$$\begin{aligned}
\frac{\sigma(2 - (\zeta + \zeta^{-1}))}{2 - (\zeta + \zeta^{-1})} &= \frac{\sigma(1 - \zeta)}{1 - \zeta} \cdot \frac{\sigma(\overline{1 - \zeta})}{\overline{1 - \zeta}} && \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \text{ is an Abelian group and } \sigma, ^{-} \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \\
&= \frac{\sigma(1 - \zeta)}{1 - \zeta} \cdot \overline{\frac{\sigma(1 - \zeta)}{1 - \zeta}} && \sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}), \text{ thus } \sigma(\zeta) = \zeta^k, \text{ for } 1 \leq k \leq r \\
&= \frac{1 - \zeta^k}{1 - \zeta} \cdot \overline{\frac{1 - \zeta^k}{1 - \zeta}}.
\end{aligned}$$

But $\dfrac{1 - \zeta^k}{1 - \zeta} \in \mathbb{Z}[\zeta]^*$ since

$$\frac{1 - \zeta^k}{1 - \zeta} = 1 + \zeta + \ldots + \zeta^{k-1} \in \mathbb{Z}[\zeta] \quad \text{and} \quad \mathrm{Nm}_{\mathbb{Q}(\zeta)/\mathbb{Q}}\left(\frac{1 - \zeta^k}{1 - \zeta}\right) = 1.$$

Therefore

$$\frac{\sigma(1 - \zeta)}{1 - \zeta} \cdot \frac{\sigma(\overline{1 - \zeta})}{\overline{1 - \zeta}} = \zeta^b \varepsilon \cdot \overline{\zeta^b \varepsilon} = \zeta^b \overline{\zeta^b} \varepsilon^2 = \varepsilon^2, \quad \varepsilon \in \mathbb{Z}[\zeta + \zeta^{-1}]^*$$

by [Was97, Proposition 1.5]. Hence

$$\sigma(2-(\zeta+\zeta^{-1}))=(2-(\zeta+\zeta^{-1}))\varepsilon^2,\quad \varepsilon\in\mathbb{Z}[\zeta+\zeta^{-1}]^*$$

Since $\#\mathrm{Gal}(\mathbb{K}/\mathbb{Q})=r$, there exist r units $\varepsilon_1,\dots,\varepsilon_r$ as required. Moreover we may take $\varepsilon_1=1$.

Step 2. We prove that $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}\left((2-\zeta-\zeta^{-1})\beta^2\right)\geq p$ for any $0\neq\beta\in\mathbb{Z}[\zeta+\zeta^{-1}]$.

Write $\mathfrak{p}^r=p\mathcal{O}_{\mathbb{K}}$. Clearly $2-\zeta-\zeta^{-1}\in\mathfrak{p}$. Since $\mathfrak{p}$ is inert in $\mathbb{Z}[\zeta+\zeta^{-1}]$, it follows that

$$\sigma(2-\zeta-\zeta^{-1})\in\mathfrak{p}\quad\text{for each}\quad\sigma\in\mathrm{Gal}(\mathbb{K}/\mathbb{Q}).$$

Therefore $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}\left((2-\zeta-\zeta^{-1})\beta^2\right)\in\mathfrak{p}\cap\mathbb{Z}=p\mathbb{Z}$ i.e. $p|\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}\left((2-\zeta-\zeta^{-1})\beta^2\right)$ as claimed.

Step 3. If we prove that the vectors

$$(1,\dots,1)^t,\ (\sigma_1(\varepsilon_2^2),\dots,\sigma_r(\varepsilon_2^2))^t,\dots,(\sigma_1(\varepsilon_r^2),\dots,\sigma_r(\varepsilon_r^2))^t$$

are linearly independent over $\mathbb{R}$, then the theorem follows. Let $1,\omega_2,\dots,\omega_r$ be the $\mathbb{Z}$-basis of $\mathbb{Z}[\zeta+\zeta^{-1}]$. As

$$\begin{pmatrix}1&1&\dots&1\\ \sigma_1(\omega_2)&\sigma_2(\omega_2)&\dots&\sigma_r(\omega_2)\\ \vdots&\vdots&\vdots&\vdots\\ \sigma_1(\omega_r)&\sigma_2(\omega_r)&\dots&\sigma_r(\omega_r)\end{pmatrix}\begin{pmatrix}1&\sigma_1(\varepsilon_2^2)&\dots&\sigma_1(\varepsilon_r^2)\\ 1&\sigma_2(\varepsilon_2^2)&\dots&\sigma_2(\varepsilon_r^2)\\ \vdots&\vdots&\vdots&\vdots\\ 1&\sigma_r(\varepsilon_2^2)&\dots&\sigma_r(\varepsilon_r^2)\end{pmatrix}=$$
$$=\begin{pmatrix}\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}\,1&\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}\,\varepsilon_2^2&\dots&\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}\,\varepsilon_r^2\\ \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}\,\omega_2&\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}\,\omega_2\varepsilon_2^2&\dots&\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}\,\omega_2\varepsilon_r^2\\ \vdots&\vdots&\vdots&\vdots\\ \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}\,\omega_r&\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}\,\omega_r\varepsilon_2^2&\dots&\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}\,\omega_r\varepsilon_r^2\end{pmatrix}\in\mathrm{Mat}_{r\times r}(\mathbb{Z})$$

we have that the columns of the matrix

$$\begin{pmatrix}1&\sigma_1(\varepsilon_2^2)&\dots&\sigma_1(\varepsilon_r^2)\\ 1&\sigma_2(\varepsilon_2^2)&\dots&\sigma_2(\varepsilon_r^2)\\ \vdots&\vdots&\vdots&\vdots\\ 1&\sigma_r(\varepsilon_2^2)&\dots&\sigma_r(\varepsilon_r^2)\end{pmatrix}$$

should be linearly independent. Seeking a contradiction, assume there exists a tuple $(\beta_1,\dots,\beta_r)^t\in\mathbb{Q}^r$ such that

$$\begin{pmatrix}1&\sigma_1(\varepsilon_2^2)&\dots&\sigma_1(\varepsilon_r^2)\\ 1&\sigma_2(\varepsilon_2^2)&\dots&\sigma_2(\varepsilon_r^2)\\ \vdots&\vdots&\vdots&\vdots\\ 1&\sigma_r(\varepsilon_2^2)&\dots&\sigma_r(\varepsilon_r^2)\end{pmatrix}\begin{pmatrix}\beta_1\\ \beta_2\\ \vdots\\ \beta_r\end{pmatrix}=\begin{pmatrix}0\\ 0\\ \vdots\\ 0\end{pmatrix}.$$

Therefore we have also

$$\begin{pmatrix} \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}\,1 & \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}\,\varepsilon_2^2 & \dots & \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}\,\varepsilon_r^2 \\ \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}\,\omega_2 & \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}\,\omega_2\varepsilon_2^2 & \dots & \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}\,\omega_2\varepsilon_r^2 \\ \vdots & \vdots & \vdots & \vdots \\ \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}\,\omega_r & \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}\,\omega_r\varepsilon_2^2 & \dots & \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}\,\omega_r\varepsilon_r^2 \end{pmatrix} \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_r \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Write $\varepsilon_1 = 1$ and $a = 2 - \zeta - \zeta^{-1}$. We have

$$0 = \sum_{i=1}^{r} \beta_i \varepsilon_i^2 = \left(\sum_{i=1}^{r} \beta_i \varepsilon_i^2 \right) a = \sum_{i=1}^{r} \beta_i \varepsilon_i^2 a = \sum_{i=1}^{r} \beta_i \sigma_i(a).$$

After taking trace, we obtain

$$0 = \sum_{i=1}^{r} \beta_i \mathrm{Tr}(a) \Longrightarrow 0 = \sum_{i=1}^{r} \beta_i.$$

Thus

$$0 = \sum_{i=1}^{r} \beta_i \sigma_i(a) = \sum_{i=1}^{r} \beta_i \sigma_i(2 - \zeta - \zeta^{-1}) = \sum_{i=1}^{p-1} \beta_i \zeta^i, \quad \beta_i = \beta_{p-i}.$$

Since $\{1, \zeta, \dots, \zeta^{p-1}\}$ is a basis of $\mathbb{Q}(\zeta)$ we conclude that $\beta_1 = \beta_2 = \ldots = \beta_r = 0$, as required.

Theorem is proved.

Appendix 2: Proof of theorem 2.3

Let $\mathbb{K}$ be a totally real number field with r distinct embeddings $\sigma_1, \dots, \sigma_r$. If $b \in (\mathbb{R}_{>0})^r$ we write $\mathrm{Tr}\, b = b_1 + \ldots + b_r$ and $\mathrm{Nm}\, b = b_1 \cdots b_r$. The multiplication of tuples is defined componentwise. The mapping $j\colon \mathbb{K} \to \mathbb{R}^r$ is defined by $j(a) = (\sigma_1(a), \dots, \sigma_r(a))$. Write $U^2 = \{\varepsilon^2 | \varepsilon \in \mathcal{O}_{\mathbb{K}}^*\}$. Thus U^2 is a subgroup of a group of totally positive units in $\mathcal{O}_{\mathbb{K}}$. By Lemma 3 of [Shi76] there exists a finite set $M \subset U^2$ such that

$$\begin{aligned} \{b \in (\mathbb{R}_{>0})^r \mid \mathrm{Tr}\, b \le \mathrm{Tr}\, bj(\varepsilon), \ \forall \varepsilon \in M\} = \\ = \left\{b \in (\mathbb{R}_{>0})^r \mid \mathrm{Tr}\, b \le \mathrm{Tr}\, bj(\varepsilon), \ \forall \varepsilon \in U^2\right\}. \end{aligned}$$

The condition

$$\mathrm{Tr}\, b \le \mathrm{Tr}\, bj(\varepsilon), \ \forall \varepsilon \in U^2, \quad b \in (\mathbb{R}_{>0})^r$$

means that the unary Humbert tuple $(b_1 x^2, \dots, b_r x^2)$ is reduced. It follows that the set

$$\mathcal{H} = \{b \in (\mathbb{R}_{>0})^r \mid \mathrm{Nm}\, b = 1 \ \wedge \mathrm{Tr}\, b \le \mathrm{Tr}\, bj(\varepsilon), \ \forall \varepsilon \in M\}$$

is bounded and closed in $\mathbb{R}^r$, hence compact. The function

$$\gamma(b) = \frac{\min\{\mathrm{Tr}\, bj(l^2) \,|\, 0 \neq l \in \mathcal{O}_{\mathbb{K}}\}}{\sqrt[r]{\mathrm{Nm}\, b}}$$

is continuous, hence it attains its maximum value on $\mathcal{H}$.
Theorem is proved.

Annexes/ Lisad

Alar Leibak. On additive generalization of Voronoï's theory for algebraic number fields. *Proc. Estonian Acad. Sci. Phys. Math.*, 54(4):195–211, 2005.

Alar Leibak. The complete enumeration of binary perfect forms over algebraic number field $\mathbb{Q}(\sqrt{6})$. *Proc. of Estonian Acad. of Sci. Phys. Math.*, 54(4):212–234, 2005.

Alar Leibak. Some results on reduction of positive quadratic forms over totally real cyclic number fields. In *International Conference on Analytic and Probabilistic Number Theory in Palanga*, pages 162–168. TEV, 2002.

Anal. Probab. Methods Number Theory, pp. 162–168
A. Dubickas *et al.* (Eds)

SOME RESULTS ON REDUCTION OF UNARY POSITIVE QUADRATIC FORMS OVER TOTALLY REAL CYCLIC NUMBER FIELDS[1]

ALAR LEIBAK
Tallinn Technical University, Ehitajate tee 5, 19086 Tallinn, Estonia
e-mail: alar@staff.ttu.ee

ABSTRACT

In this paper, we study the reduction theory of positive definite generalized quadratic forms over totally real cyclic number field. Based on the works by Koecher (1960, 1961), Venkov (1940), and Shintani (1976) we present more detailed results on the reduction domain. As a result, we present an explicit description of the reduction domain for certain families of number fields of degrees 2 and 3.

1. INTRODUCTION

The reduction theory of positive definite quadratic forms has been studied by several people but the main open question is to find an explicit description of the reduction domain. For positive quadratic forms over real numbers, an explicit description of Minkowski's reduction domain is known only for dimension up to 7. For positive definite quadratic forms over an algebraic number field, no explicit description of the reduction domain is known.

Shintani (1976) derived a finite set of units (this set will be denoted by M) neccessary for constructing the reduction domain of positive definite unary quadratic forms over a totally real number field.

In this paper, we derive more refined results for the reduction domain in the sense of reduction theory developed by Koecher (1960, 1961) of unary positive quadratic forms over totally real cyclic number fields. For certain families of number fields of degree 2 or 3, we derive an explicit description of the reduction domain.

This paper is organized as follows. In the next section, we introduce the notation and definitions. For the convenience of the reader, we recall the description of the set M in Section 3. In Section 4, we present the main theorems. Next two sections are dedicated to derive explicit descriptions of the fundamental domain of unary positive quadratic forms over real quadratic number fields and a certain family of cyclic cubic fields, respectively.

2. NOTATION

Let $\mathbb{K}$ be a totally real Galois extension of $\mathbb{Q}$ with degree r and $\mathcal{O}_{\mathbb{K}}$ be its ring of integers. We denote the field conjugates of $\mathbb{K} = \mathbb{K}_1$ by $\mathbb{K}_2, \ldots, \mathbb{K}_r$. Let $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) = \{1, \tau_2, \ldots, \tau_r\}$

[1]This work was partially supported by ESF grant no. 4291.

Definition 1. We call the tuple $(a_1x^2, a_2\tau_2(x^2)\ldots, a_r\tau_r(x^2))$ of unary quadratic forms a generalized unary quadratic form. A generalized unary form $(a_1x^2, a_2\tau_2(x^2)\ldots, a_r\tau_r(x^2))$ is called positive definite, if a_ix^2 is a positive definite quadratic form over $\mathbb{K}_i$ for all $i = 1, \ldots, r$.

It is clear that a generalized unary form $(a_1x^2, a_2\tau_2(x^2)\ldots, a_r\tau_r(x^2))$ is positive definite iff $a_1, \ldots, a_r$ are all positive. We call such a tuple positive. Therefore, we can consider the tuple of coefficients $(a_1, \ldots, a_r)$ only as an element in $\mathbb{R}^r$.

Let $(a_1, \ldots, a_r)$ and $(b_1, \ldots, b_r)$ be positive tuples. Now we apply the definitions of the reduction theory developed by Koecher (1960, 1961) and Venkov (1940).

Tuples $(a_1, \ldots, a_r)$ and $(b_1, \ldots, b_r)$ are called equivalent if there exists a unit $u \in \mathcal{O}_{\mathbb{K}}^*$ such that

$$(a_1, a_2, \ldots, a_r) = \big(b_1u^2, b_2\tau_2(u^2), \ldots, b_r\tau_r(u^2)\big).$$

We have a natural embedding $j\colon \mathbb{K} \to \mathbb{R}^r$ defined by $j(a) = (a, \tau_2(a), \ldots, \tau_r(a))$ for $a \in \mathbb{K}$. The ith coordinate of $j(a)$ is denoted by $j(a)_{(i)}$.

Definition 2. A positive tuple $(a_1, \ldots, a_r)$ is called reduced with respect to the positive tuple $(b_1, \ldots, b_r)$ iff the inequality

$$\sum_{i=1}^{r} a_ib_i \leqslant \sum_{i=1}^{r} a_ib_i\, j(u^2)_{(i)} \tag{1}$$

holds for all units $u \in \mathcal{O}_{\mathbb{K}}^*$.

The set of all positive tuples that are reduced with respect to a positive tuple b is denoted by $\mathcal{F}_b$. If b is a positive rational number, then write $\mathcal{F}_b$ instead of $\mathcal{F}_{j(b)}$.

Sometimes, we consider the set $\{j(a) \mid a \in \mathbb{K}_{\gg 0}\}$ due to the algebraic background (we have a natural way to apply Galois automorphisms and to use the trace and norm). Most of the results could be generalized to the set of all positive definite generalized unary quadratic forms. The reduction domain with respect to a totally positive algebraic number b in $\{j(a) \mid a \in \mathbb{K}_{\gg 0}\}$ will be denoted by $\mathcal{F}_b^j$.

We identify the Galois group $G = \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ with a subgroup G' of S_r (the symmetric group on r letters) as follows: a Galois automorphism τ is identified with $\hat{\tau} \in S_r$ such that $j(\tau a) = \hat{\tau}(j(a))$ for all $a \in \mathbb{K}$. Due to isomorphism, we can "apply" the Galois automorphism to the generalized unary quadratic form.

Koecher proved that the set $\mathcal{F}_b$ has finite number of faces (Koecher, 1960, Satz 8). (Koecher gave a proof for positive definite generalized quadratic forms of arbitrary dimension.) Shintani gave the proof in the case where the number field $\mathbb{K}$ is totally real and tuples are of the form $j(a)$, where $a \in \mathbb{K}$ and reduction was done with respect to the tuple $j(1)$ in $\mathbb{K} \otimes_{\mathbb{Q}} \mathbb{R}$ (Shintani, 1976). Advantage of Shintani's proof is that he gave an explicit construction for the finite set M of units that are sufficient for constructing the reduction domain with respect to the tuple $j(1)$.

3. THE SET M

For the convenience of the reader, we recall here the definition of the set M (Shintani, 1976, p. 401).

Let u_i $(i = 1, \ldots, r)$ be totally positive units such that $j(u_i)_{(i)} > r$. For a nonempty proper

subset $S \in \{1, \dots, r\}$, let $u(S)$ be the totally positive unit such that $j(u(S))_{(i)} > 1$ iff $i \in S$. Denote the set $\{i\}$ by S_i. Let

$$t_i \geqslant 1 + \frac{j(u(S_i))_{(i)} - 1}{1 - j(u(S_i))_{(k)}}, \quad \forall k \neq i,$$

for $i = 1, \dots, r$. Let N be the set of totally positive units u such that $j(u)_{(i)} \leqslant t_i$ for all $i = 1, \dots, r$.

$$M = \{u_1, \dots, u_r\} \cup \left\{u(S) \mid \forall \emptyset \neq S \subset \{1, \dots, r\}\right\} \cup N.$$

In this paper, we consider the set $\{u^2 \mid u \in \mathcal{O}_{\mathbb{K}}^*\}$ instead of the set of totally positive units of $\mathbb{K}$. It is easy to see that the following corollary holds.

COROLLARY 3. *If $\mathbb{K}$ is a totally real cyclic Galois extension of degree r, then $\inf t_i = \inf t_k$ for all $i, k \in \{1, \dots, r\}$, where $\inf t_i$ denotes the smallest possible value for t_i.*

4. MAIN THEOREMS

THEOREM 4. *Let $p = \#\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ be a prime number, and let N be the number of faces of the reduction domain $\mathcal{F}_1^j$. Then $p \mid N$.*

Proof. Let $\mathcal{O}_{\mathbb{K},\gg 0}^*$ be the set all totally positive units. We assume that $[\mathcal{O}_{\mathbb{K},\gg 0}^*\colon \mathcal{O}_{\mathbb{K}}^{*^2}] = 1$. Let $H_v = \mathcal{F}_1^j \cap \mathcal{F}_v^j$ be a face of $\mathcal{F}_1$. Shintani proved that v also is a totally positive unit. Hence, $v = u^2$ for some $u \in \mathcal{O}_{\mathbb{K}}^*$, and the face H_v is defined as follows:

$$H_v = \left\{a \mid a \in \mathbb{K}_{\gg 0}, \mathrm{tr}(a) = \mathrm{tr}(au^2)\right\}.$$

It is easy to see that $\tau H_v = H_{\tau v}$ for all $\tau \in G$. We need the following lemma.

LEMMA 5. *There are no faces of $\mathcal{F}_1^j$ which are invariant under Galois' action.*

Proof. Assume that $H_v = \mathcal{F}_1^j \cap \mathcal{F}_v^j$ is invariant under the Galois action, i.e., $H_v = H_{\tau v}$ for all $\tau \in G$. Therefore, H_v consists of totally positive numbers a such that $\mathrm{tr}(a) = \mathrm{tr}(a\tau(u^2))$ for each $\tau \in G$.

$$p \cdot \mathrm{tr}(a) = \sum_{\tau \in G} \mathrm{tr}(a\tau(u^2)) = \mathrm{tr}(a \cdot \mathrm{tr}(u^2)) = \mathrm{tr}(u^2)\mathrm{tr}(a) \geqslant p \cdot \sqrt[p]{\mathrm{Nm}(u^2)} \cdot \mathrm{tr}(a) = p \cdot \mathrm{tr}(a).$$

The equality holds iff $u^2 = 1$, i.e., $v = 1$. If $v = 1$, we get $H_1 = \mathcal{F}_1^j$. This is a contradiction, since H_v is a face.

The lemma is proved.

If $[\mathcal{O}_{\mathbb{K},\gg 0}^*\colon \mathcal{O}_{\mathbb{K}}^{*^2}] > 1$, then we fix $u^2 \in M$, where M is the set defined in (Shintani, 1976, p. 401). A face of $\mathcal{F}_1^j$ is defined by the equation $\mathrm{tr}(a) = \mathrm{tr}(a\tau(u^2))$. Applying the same argument as in the proof of Lemma 5, we get that there are no faces which are invariant under the Galois action.

Denote the set of faces of $\mathcal{F}_1^j$ by $\mathcal{H}$. We call faces H and H' equivalent iff there exists $\tau \in G$ such that $\tau H = H'$. The corresponding partition into equivalence classes is denoted by $\mathcal{H}^{\mathrm{Gal}}$. For arbitrary face $H \in \mathcal{H}$, there are no nontrivial stabilizers due to the assumption that the order of G is a prime. Due to Lemma 5, all equivalence classes of $\mathcal{H}^{\mathrm{Gal}}$ contain exactly p elements.

The theorem is proved.

COROLLARY 6. *If $r = \#\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) = p^k$ for a prime number p, then the number of faces of $\mathcal{F}_1^j$ is divisible by p.*

Proof. The number of elements in a equivalence class of $\mathcal{H}^{\mathrm{Gal}}$ is divisible by p, and the corollary follows.

THEOREM 7. *Let p be a prime number. If $\#\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) = p^k$, then the number of faces of $\mathcal{F}_1$ is divisible by p.*

Proof. Obviously, $\mathcal{F}_1^j \subseteq \mathcal{F}_1$ and any face of $\mathcal{F}_1$ contains a face of $\mathcal{F}_1^j$. If H is a face of $\mathcal{F}_1$, then $H \cap \{j(a) \mid a \in \mathbb{K}_{\gg 0}\}$ is a face of $\mathcal{F}_1^j$. Theorem 7 follows from Corollary 6.

COROLLARY 8. *Let $\mathbb{K}$ be a cyclic extension of prime degree and $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) = \langle\tau\rangle$. The number of faces of $\mathcal{F}_1$ equals to $\#\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ iff the system of linear equations*

$$\begin{cases} \mathrm{tr}(a(u^2-1)) = 0, \\ \mathrm{tr}(\tau(a)(u^2-1)) = 0 \end{cases} \tag{2}$$

has a solution in $\mathcal{F}_1$ for a nontrivial unit $u \in \mathcal{O}_{\mathbb{K}}^*$.

Proof. If a is the solution of (2) and $a \in \mathcal{F}_1^j$, then $H = \{a \mid \mathrm{tr}(a(u^2-1)) = 0, a \in \mathbb{K}_{\gg 0}\}$ is a face of $\mathcal{F}_1$. Hence, $a \in H \cap \tau H$. Applying τ^k to $H \cap \tau H$, we get $\tau^k(a) \in \tau^k H \cap \tau^{k+1} H$ for $k = 1, \ldots, \#\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) - 1$, i.e., the faces $\tau^k H \cap \tau^{k+1} H$ intersect in $\mathcal{F}_1$. If $k = \#\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) - 1$, then $\tau^k H \cap \tau^{k+1} H = \tau^k H \cap H$, and we have the cycle of "pairwise consecutive" faces

$$\langle \tau^k H, \tau^{k+1} H\rangle \quad \text{for } k = 0, \ldots, \#\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) - 1.$$

If the number of faces of $\mathcal{F}_1$ equals $\#\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$, then a face of $\mathcal{F}_1$ is defined by equation $\mathrm{tr}(a(u^2-1)) = 0$. Hence, there exists $1 \neq \tau' \in \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ such that $\mathrm{tr}(\tau'(a)(u^2-1)) = 0$, and these faces meet each other.

Let us denote by $\partial\mathcal{F}_1^j$ the boundary of $\mathcal{F}_1^j$.

LEMMA 9. *Let $b \in \mathbb{K}_{\gg 0}$ and $b \notin \partial\mathcal{F}_1^j$. There are no faces of $\mathcal{F}_b^j$ which are invariant under* $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$.

Proof. Let a be in the face $H \subset \mathcal{F}_b^j$ defined by the equality $\mathrm{tr}(ab) = \mathrm{tr}(abu^2)$ for a fixed $u^2 \in M$. Assume that H is invariant under the action of $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$. Then

$$\mathrm{tr}(a)\mathrm{tr}(b) = \sum_{\tau \in \mathrm{Gal}(\mathbb{K}/\mathbb{Q})} \mathrm{tr}(\tau(a)b) = \sum_{\tau \in \mathrm{Gal}(\mathbb{K}/\mathbb{Q})} \mathrm{tr}(\tau(a)bu^2) = \mathrm{tr}(a)\mathrm{tr}(bu^2).$$

Hence, $\mathrm{tr}(b) = \mathrm{tr}(bu^2)$, i.e., $b \in \partial\mathcal{F}_1^j$, a contradiction.

The lemma is proved.

The condition $b \notin \partial\mathcal{F}_1^j$ cannot be removed, as we show in the following example. Let $\mathbb{K}$ be a real quadratic number field such that the fundamental unit u is totally positive. The reduction domain is computed explicitly in Section 5. Due to Theorem 11, we have $\partial\mathcal{F}_1^j = u^{-1}\mathbb{Q}_{>0} \cup u\mathbb{Q}_{>0} \cup \{0\}$, where $\mathbb{Q}_{>0}$ denotes the set of all positive rational numbers. Let $b = ku$ for a positive rational k. From Theorem 12 we obtain that $\mathbb{Q}_{>0} \cup \{0\}$ is a face of $\mathcal{F}_b^j$. But this face $\mathbb{Q}_{>0} \cup \{0\}$ is invariant under the Galois action.

5. REAL QUADRATIC NUMBER FIELDS

Let $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, where $d > 1$ is a squarefree integer. Let u be a fundamental unit such that $\log|u| > 0$. The unit group is isomorphic to $\langle -1\rangle \times C_\infty$, where C_∞ is the infinite cyclic group generated by u.

LEMMA 10. *For a real quadratic number field $\mathbb{K}$, the set $M = \{u^2, u^{-2}\}$.*

Proof. It is sufficient to show that $N = \{u^2, u^{-2}\}$. Due to Corollary 3, we have

$$t = 1 + \frac{u^2 - 1}{1 - u^{-2}} = 1 + u^2.$$

The image of an arbitrary totally positive unit v under the map $j\colon \mathbb{K} \to \mathbb{R} \times \mathbb{R}$ is (v, v^{-1}). Therefore, we need only to consider the fundamental unit and its even powers. It is easy to see that the set of totally positive units v which satisfy $\max\{v, v^{-1}\} \leqslant t$ consists of 1, u^2, and u^{-2} only. We exclude 1, since it is irrelevant for constructing the fundamental domain $\mathcal{F}_1$.

Denote by $(ax^2, a'\bar{x}^2)$ the generalized positive unary quadratic form and by $\bar{x}$ the conjugate field of x.

THEOREM 11. *The fundamental domain $\mathcal{F}_1$ is defined by the inequality*

$$\max\left\{\frac{a}{a'}, \frac{a'}{a}\right\} \leqslant u^2. \tag{3}$$

Let $(bx^2, b'\bar{x}^2)$ be the positive generalized unary quadratic form.

THEOREM 12. *The fundamental domain $\mathcal{F}_{(b,b')}$ is defined by the inequalities*

$$\frac{a'}{a} \leqslant \frac{b}{b'}u^2 \quad \textit{and} \quad \frac{a}{a'} \leqslant \frac{b'}{b}u^2. \tag{4}$$

Theorems 11 and 12 follow from the inequalities

$$\begin{cases} abu^2 + a'b'\bar{u}^2 \geqslant ab + a'b', \\ ab\bar{u}^2 + a'b'u^2 \geqslant ab + a'b', \end{cases}$$

where $(ax^2, a'\bar{x}^2)$ is a positive generalized unary quadratic form.

6. TOTALLY REAL CYCLIC CUBIC FIELDS

Let $\mathbb{K}$ be a totally real cyclic cubic field and $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) = \langle\tau\rangle$. Let u be a fundamental unit such that u and $\tau(u)$ generate the maximal torsion-free subgroup of $\mathcal{O}_{\mathbb{K}}^*$, i.e., $u, \tau(u)$ is a fundamental system of units. Such unit u exists due to Theorem 3.9 of (Narkiewicz, 1974, p. 109). Without loss of generality we can assume that $j(u^2)_{(1)} > 1 > \max\{j(u^2)_{(2)}, j(u^2)_{(3)}\}$ (we can replace u^2 by u^{-2}, if necessary, and choose one of u^2, $\tau(u^2)$, and $\tau^2(u^2)$).

THEOREM 13. *Let $\{u, \tau(u)\}$ be a fundamental system of units such that $1/2 > j(u^2)_{(2)} > j(u^2)_{(3)}$ and $j(u^2)_{(1)} j(u^4)_{(2)} > 2$. Then the number of faces of $\mathcal{F}_1$ is equal to 3 or 6.*

Proof. Let u be such a unit. The Galois automorphism τ acts on the triple $j(a)$, where $a \in \mathcal{O}_{\mathbb{K}}^*$, as a cyclic permutation. In this proof, we fix the action to be clockwise rotation, i.e., $j(\tau(a)) = (j(a)_{(3)}, j(a)_{(1)}, j(a)_{(2)})$.

Under the assumptions made, we have $j(u^2)_{(1)} > 4$ and $u_i = \tau^{i-1}(u^2)$ for $i = 1, 2, 3$. If S is a proper nonempty subset of $\{1, 2, 3\}$, then it has one or two elements. If $\#S = 1$, then we can take $u(\{i\}) = u_i$ and $u(\{1, 2, 3\} \setminus \{i\}) = u_i^{-1}$ for all $i = 1, 2, 3$. Finally, we have to construct the set N. We exclude the unit 1, since it gives us the trivial identity $\mathrm{tr}(a) = \mathrm{tr}(a)$. Due to Corollary 3, we need to compute the upper bound for

$$\max\left\{1 + \frac{j(u^2)_{(1)} - 1}{1 - j(u^2)_{(2)}}, 1 + \frac{j(u^2)_{(1)} - 1}{1 - j(u^2)_{(3)}}\right\}$$
$$= \max\left\{\frac{j(u^2)_{(1)} - j(u^2)_{(2)}}{1 - j(u^2)_{(2)}}, \frac{j(u^2)_{(1)} - j(u^2)_{(3)}}{1 - j(u^2)_{(3)}}\right\} = \frac{j(u^2)_{(1)} - j(u^2)_{(2)}}{1 - j(u^2)_{(2)}}.$$

Under the assumptions made, we have that $2j(u^2)_{(1)}$ is an upper bound.

Let $w = u^l \tau(u)^k$ and $k > l > 0$. Then w^2 is a totally positive unit.

$$j(w^2)_{(1)} = j(u^{2k}\tau(u)^{2l})_{(1)} = j(u)_{(1)}^{2k-2l}\left(j(u^2)_{(1)} j(\tau(u^2))_{(1)}\right)^l > 2j(u^2)_{(1)}.$$

Using

$$\prod_{i=1}^{3} j\left(\tau^{i-1}(u^2)\right)_{(1)} = 1$$

and the assumption $j(u^2)_{(2)} < 1/2$, we obtain $2 < j(u^2)_{(1)} j(u^2)_{(3)}$, and the last inequality follows.

If $l > k > 0$, then we apply the previous argument to $j(w^2)_{(2)}$.

Let $k = l > 1$. Then

$$j(w^2)_{(2)} = j(u^{2k}\tau(u)^{2k})_{(2)} = |j(\tau(u)^k)_{(2)}| \cdot |j(\tau(u))_{(2)} j(u^2)_{(2)}|^k$$
$$= |j(u)_{(1)}^k| \cdot |j(u)_{(1)} j(u^2)_{(2)}|^k > 2^{\frac{k}{2}} |j(u)_{(1)}^k| > 2j(u^2)_{(1)}.$$

Completing the proof for the remaining cases of k and l, it follows that

$$j(w^2)_{(i)} = j\left(u^{2k}\tau(u)^{2l}\right)_{(i)} > 2j(u^2)_{(1)}$$

for a suitably chosen i, except for $|k| = |l| = 1$. Hence,

$$N = \left\{u^{2k}\tau(u)^{2l} \mid |k| = |l| = 1\right\}.$$

But $u^{-2}\tau(u)^{-2} = u_3$ and $u^2\tau(u)^2 = u(\{1, 2\})$. Therefore, $\#M = 8$, a contradiction to Theorem 7. Hence, the set N is irrelevant and $M = \{u_i, u_i^{-1} \mid i = 1, 2, 3\}$. The theorem is proved.

If the system of linear equations

$$\begin{cases} \operatorname{tr}(a(u^2 - 1)) = 0, \\ \operatorname{tr}(\tau(a)(u^2 - 1)) = 0 \end{cases}$$

has a solution in $\mathcal{F}_1$, then the number of faces of $\mathcal{F}_1$ is 3. Otherwise, $\mathcal{F}_1$ has 6 faces.

COROLLARY 14. *Under the assumptions of Theorem* 13*, the reduction domain $\mathcal{F}_1$ is defined by the inequalities*

$$a \in \mathcal{F}_1 \iff \operatorname{tr}(a(u_i - 1)) \geqslant 0 \wedge \operatorname{tr}(a(u_i^{-1} - 1)) \geqslant 0 \quad \textit{for all } i = 1, 2, 3.$$

7. CONCLUSIONS AND FUTURE WORK

In this paper, we obtained some results for the reduction domain $\mathcal{F}_1$ of generalized positive unary forms over totally real number fields. It was proved that if $\#\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) = p^k$ for a prime number p, then the number of faces of $\mathcal{F}_1$ is divisible by p. Moreover, if the system of linear equations (2) has a solution in $\mathcal{F}_1$ and $\#\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ is a prime number, then $\mathcal{F}_1$ has exactly $\#\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ faces. As a result, applying those propositions to Shintani's work (1976), an explicit descriptions of the reduction domain is presented if the number field is either a real quadratic field or totally real cyclic number field satisfying the assumptions of Theorem 13.

The future work includes to extend Theorem 13 to all totally real cyclic cubic fields, to study the reduction theory over arbitrary Galois extensions, and to generalize those results to positive definite generalized quadratic forms of higher dimensions as well.

Acknowledgement

Author wishes to thank prof. Paul Tammela at Tallinn Pedagogical University for his invitation to the field of geometry of numbers.

REFERENCES

Koecher, M. (1960). Beiträge zu einer Reduktionstheorie in Positivitätsbereichen. I. *Math. Ann.* **141**, 384–432.

Koecher, M. (1961). Beiträge zu einer Reduktionstheorie in Positivitätsbereichen. II. *Math. Ann.* **144**, 175–182.

Narkiewicz, W. (1974). *Elementary and Analytic Theory of Algebraic Numbers*. Warszawa.

Shintani, T. (1976). On evaluation of zeta functions of totally real algebraic number fields at non-positive integers. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **23**(2), 393–417.

Venkov, B. A. (1940). On reduction of positive quadratic forms. *Bull. Acad. Sci. URSS Ser. Math.* **4**, 37–52.

Annex 4/ Lisa 4

Elulookirjeldus

1. Isikuandmed:

Ees- ja perekonnanimi: Alar Leibak
Sünniaeg ja -koht: 03.07.1973, Tallinn
Kodakondsus: Eesti
Perekonnaseis: vallaline
Lapsed: –

2. Kontaktandmed:

Aadress: Idakaare 25-3
Telefon: (+372) 5209389
E-posti aadress: alar@staff.ttu.ee

3. Hariduskäik:

Õppeasutus	Lõpetamise aeg	Haridus (eriala/kraad)
Tallinna Tehnikaülikool	1997	loodusteaduste magister, tehniline füüsika
Tallinna 43. Keskkool	1991	keskharidus

4. Keelteoskus:

Keel	Tase
Inglise	Kesktase
Vene	Algtase

5. Täiendõpe:

Õppimise aeg	Õppeasutus või muu organisatsiooni nimetus
2000	*Suvekool teemal: elliptilised kõverad, lõplikud korpused ja krüptograafia*, NTNU, Bergeni Ülikool, Oslo Ülikool ja Tromsø Ülikool
1998	*Krüptoloogia ja andmeturbe suvekool*, Århusi Ülikool

6. Teenistuskäik:

Ülikooli, teadusasutuse või muu organisatsiooni nimetus	Töötamise aeg	Ametikoht
Tallinna Tehnikaülikool	1997 -	assistent
AS Cybernetica	1997 -1998	teadur
Küberneetika Instituudi Infotehnoloogia osakond	1993 - 1997	insener

7. Kaitstud lõputööd

Magistritöö teemal *Assotsiatiivsuse samasustest graafialgebrates.*

8. Teadustegevus

2003 –	HM teema *Algebralised struktuurid ja matemaatilise analüüsi rakendused* täitja.
2000–2003	ETF grant nr. 4291 *Rühmade ja poolrühmade esitused* täitja.
1998–2002	HM teema *Algebra ja matemaatilise analüüsi rakendusmeetodid* täitja.
1996–1999	ETF grant nr. 2136 *Rühmade esitused* täitja.

Konverentsi "5th International Conference *Simulation and Optimization in Business and Industry*", 17-20 mai, 2006, Tallinn, korralduskomitee liige.

Alar Leibak. Some results on reduction of positive quadratic forms over totally real cyclic number fields. In *International Conference on Analytic and Probabilistic Number Theory in Palanga*, (Dubickas, A. et al., eds.) pages 162–168. TEV, 2002.
Alar Leibak. On additive generalization of Voronoï's theory for algebraic number fields. *Proc. Estonian Acad. Sci. Phys. Math.*, 54(4):195–211, 2005.
Alar Leibak. The complete enumeration of binary perfect forms over algebraic number field $\mathbb{Q}(\sqrt{6})$. *Proc. of Estonian Acad. of Sci. Phys. Math.*, 54(4):212–234, 2005.
Alar Leibak. Some remarks of the lower bound of the additive Hermite constant for number fields. In *International Conference on Operational Research: Simulation and Optimization in Business and Industry*, (Pranevičius, H. et al. eds.), pages 105–108, TECHNOLOGIJA, Kaunas, 2006.
5th International Conference on Operational Research: Simulation and Optimization in Business and Industry. Programme and Abstracts. May 17–20, 2006. (Leibak, A. et al. eds.), Tallinn, 2006
Riid, Andri; Leibak, Alar; Rüstern, Ennu. Fuzzy backing control of truck and two trailers. IEEE-ICCC 2006, 4th IEEE International Conference on Computational Cybernetics, Tallinn, August 20–22, 2006 Tallinn, Estonia. 2006, 107 - 112.

9. Teadustöö põhisuunad.

Arvude geomeetria üle arvukorpuste ja selle rakendused.

Annex 4/ Lisa 4

Curriculum Vitae

1. Personal information:

Name: Alar Leibak
Place and date of birth: 03.07.1973, Tallinn
Citizenship: Estonian
Marital status: single
Children: none

2. Contact information:

Address: Idakaare 25-3
Telephone: (+372) 5209389
Email: alar@staff.ttu.ee

3. Education:

Institution	Graduation date	Education
Tallinn University of Technology	1997	MSc in Natural Sciences, Technical Physics
Tallinn Secondary School No. 43	1991	

4. Languages:

Language	Level
English	Medium
Russian	Basic

5. Special Courses:

Date	Organisation
2000	*Summer School in Elliptic Curves, Finite Fields and Cryptography*, NTNU, University of Bergen, University of Oslo, University of Tromsø
1998	*Summer School in Cryptology and Data Security*, Århus University

6. Professional Employment

Organisation	Date	Position
Tallinn University of Technology	1997 -	Teaching Assistant
Cybernetica Ltd.	1997 -1998	Researcher
Dep. of Information Technology at Institute of Cybernetics	1993 - 1997	Engineer

7. Theses

Master thesis *On associative like identities in graph algebras.*

8. Scientific Work

2003 –	Algebraic structures and applications of mathematical analysis. *Funded by the Ministery of Education and Research.*
2000–2003	G4291 Representations of groups and semigroups. *Estonian Science Foundation Grant*.
1998–2002	Applications of algebra and mathematical analysis. *Funded by the Ministery of Education and Research.*
1996–1999	G2136 Representations of semigroups. *Estonian Science Foundation Grant*.

A member of organising committee of the 5th International Conference *Simulation and Optimization in Business and Industry, Tallinn, May 17–20, 2006*.

Alar Leibak. Some results on reduction of positive quadratic forms over totally real cyclic number fields. In *International Conference on Analytic and Probabilistic Number Theory in Palanga*, (Dubickas, A. et al., eds.) pages 162–168. TEV, 2002.

Alar Leibak. On additive generalization of Voronoï's theory for algebraic number fields. *Proc. Estonian Acad. Sci. Phys. Math.*, 54(4):195–211, 2005.

Alar Leibak. The complete enumeration of binary perfect forms over algebraic number field $\mathbb{Q}(\sqrt{6})$. *Proc. of Estonian Acad. of Sci. Phys. Math.*, 54(4):212–234, 2005.

Alar Leibak. Some remarks of the lower bound of the additive Hermite constant for number fields. In *International Conference on Operational Research: Simulation and Optimization in Business and Industry*, (Pranevičius, H., et al., eds.), pages 105–108, TECHNOLOGIJA, Kaunas, 2006.

5th International Conference on Operational Research: Simulation and Optimization in Business and Industry. Programme and Abstracts. May 17–20, 2006. (Leibak, A., et al., eds.), Tallinn, 2006

Riid, Andri; Leibak, Alar; Rüstern, Ennu. Fuzzy backing control of truck and two trailers. IEEE-ICCC 2006, 4th IEEE International Conference on Computational Cybernetics, Tallinn, August 20–22, 2006 Tallinn, Estonia. 2006, 107 - 112.

9. Main Areas of Scientific Work

Geometry of numbers over algebraic number fields and its applications.