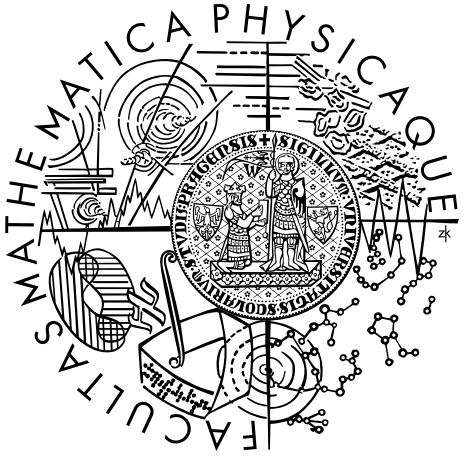
Charles University in Prague
Faculty of Mathematics and Physics

BACHELOR THESIS



Josef Svoboda

Universal Quadratic Forms over Number Fields

Department of Algebra

Supervisor of the bachelor thesis: Mgr. Vítězslav Kala, Ph.D.
Study programme: Mathematics
Study branch: General mathematics

Prague 2016

I declare that I carried out this bachelor thesis independently, and only with the cited sources, literature and other professional sources.

I understand that my work relates to the rights and obligations under the Act No. 121/2000 Sb., the Copyright Act, as amended, in particular the fact that the Charles University in Prague has the right to conclude a license agreement on the use of this work as a school work pursuant to Section 60 subsection 1 of the Copyright Act.

In ..... date ..... signature of the author

Title: Universal Quadratic Forms over Number Fields

Author: Josef Svoboda

Department: Department of Algebra

Supervisor: Mgr. Vítězslav Kala, Ph.D., Department of Algebra

Abstract: The aim of this work is to study universal quadratic forms over biquadratic fields. In the thesis we define biquadratic fields and describe their structure. In particular, we study some distinguished (totally positive and additively indecomposable) elements, their norms and traces. Then we describe the theory of universal quadratic forms and use special elements to find a lower bound for the number of variables of a universal quadratic form over some biquadratic fields.

Abstrakt: Cílem této práce je studium univerzálních kvadratických forem nad bikvadratickými tělesy. V práci defininujeme bikvadratická tělesa a popisujeme jejich strukturu. Konkrétně studujeme některé význačné (totálně kladné a aditivně nerozložitelné) prvky, jejich normy a stopy. Poté popisujeme teorii univerzálních kvadratických forem a používáme význačné prvky k důkazu dolního odhadu počtu proměnných univerzální kvadratické formy v některých bikvadratických tělesech.

Keywords: universal quadratic form, number field, biquadratic, additively indecomposable integer, totally positive

I would like to thank my supervisor Vítězslav Kala for his inspiring and useful advice. I am very grateful for his patience and the time he devoted to me during the preparation of this thesis.

Contents

List of Notations

$\mathbb{C}$	field of complex numbers
$\mathbb{R}$	field of real numbers
$\mathbb{Q}$	field of rational numbers
$\mathbb{Z}$	ring of rational integers
K	number field
$\mathcal{O}_K$	ring of integers of K
$\mathcal{O}_K^+$	ring of totally positive integers of K
U_K	group of units of $\mathcal{O}_K$
U_K^+	group of totally positive units of $\mathcal{O}_K$
U_K^2	group of squares of units of $\mathcal{O}_K$
$\sigma_1, \sigma_2, \ldots, \sigma_d$	embeddings of K into $\mathbb{C}$
r	number of real embeddings of K
s	number of conjugate pairs of complex embeddings of K
$\alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(d)}$	conjugates of $\alpha \in K$
$\alpha \succ \beta$	$\alpha^{(i)} > \beta^{(i)}$ for every $i \in \{1, 2, \ldots, d\}$
$N(\alpha)$	norm of α
$\mathrm{Tr}(\alpha)$	trace of α
$\widehat{\alpha}$	maximum of $\lvert\alpha^{(i)}\rvert$, $i \in \{1, 2, \ldots, d\}$
$\langle v, w \rangle$	standard dot product of vectors v, w in $\mathbb{R}^d$
$[G : H]$	index of subgroup H in the group G

Introduction

In 1770, Lagrange proved his famous Four-Square theorem – every positive integer can be expressed as the sum of four squares of integers. This result can be generalized in several ways. For example, we can ask whether there are other quadratic forms which represents all positive integers. Forms with this property are called universal. We can also consider quadratic forms over different rings than rational integers, typically the ring of integers of a number field K.

These two generalizations were extensively studied. As an example, Manjul Bhargava and Jonathan P. Hanke [BH] proved that any quadratic form over rational integers represents all positive integers if and only if it represents numbers $1, 2, \ldots, 290$. Carl L. Siegel [Sie45] proved that the sum of any number of squares is universal only for $K = \mathbb{Q}$ and $K = \mathbb{Q}(\sqrt{5})$.

My supervisor Vítězslav Kala with Valentin Blomer [Kal16b] [BK15] recently proved a theorem stating that for every N there exists a squarefree integer D such that every universal quadratic form over the ring of integers of $\mathbb{Q}(\sqrt{D})$ has more than $N - 1$ variables.

The proof of this theorem uses the continued fraction of $\sqrt{D}$. The roots of polynomials of higher degree have more complicated continued fractions and proving similar theorem in case of a general field K seems to be very difficult. We completely do not understand the relationship between the continued fraction and the arithmetic of the field K and it is not clear if such a relation even exists. In this thesis we study universal forms over biquadratic fields $\mathbb{Q}(\sqrt{p}, \sqrt{q})$. These fields are first in line after quadratic fields because they are still relatively easy to handle and share many of their properties with quadratic fields (where we know much more).

In the first introductory chapter we give basic definitions and facts from algebraic number theory and then introduce totally real fields and totally positive elements. The second chapter describes biquadratic fields and their properties. In particular, we study the ring of integers and the group of units. We also describe the subgroup of totally positive units and study the indices of this group and the group of the squares of units in the group of all units.

In the third chapter we introduce additively indecomposable integers. These elements are "difficult to represent" by a quadratic form, so they play an important role in the proof of Theorem 26 and related theory. We prove several bounds concerning trace and norm of totally positive and indecomposable integers in quadratic and biquadratic fields. The results concerning biquadratic fields are original, although they are analogous to the results in quadratic case. In the last section we present Theorem 21 which gives a general upper bound on the norms of indecomposable integers and is due Brunotte [Bru82, Bru83]. We present an original geometric proof of Lemma 20 which is an essential part of the proof of the theorem.

In the fourth chapter we deal with universal forms and present some of Kala's results – we provide more detailed proofs of Lemma 24 and Proposition 25. Finally we use this results and the bounds from the preceding chapter to prove a new Theorem 27 which is an analogy of Theorem 26 for biquadratic fields.

1. Basis definitions and facts

This chapter summarizes basic notations and facts we will need throughout the thesis.

1.1 Number fields

Definition 1. Let K be a field. We say that K is a *number field of degree d* if it is a finite extension of $\mathbb{Q}$ of degree d, i.e. d-dimensional vector space over $\mathbb{Q}$.

Proposition 2. *Let K be a number field of degree d. Then there are precisely d field homomorphisms $\sigma_i : K \hookrightarrow \mathbb{C}$.*

For proof see [Mil15].

Definition 3. Let $a \in K$. Then we define norm of a as $N(a) = \prod_{i=1}^{d} \sigma_i(a)$ and trace of a as $\mathrm{Tr} = \sum_{i=1}^{d} \sigma_i(a)$.

Definition 4. Number field K is called *Galois over* $\mathbb{Q}$ if every σ_i is an automorphism of K.

Definition 5. Let K be a number field. By its *ring of integers* $\mathcal{O}_K$ we mean a subring of K consisting of all roots of the monic polynomials with integer coefficients in K. We call the usual integers in $\mathbb{Z}$ *rational integers* to avoid a confusion.

Proposition 6. *If $a \in \mathcal{O}_K$, then $N(a)$ and $Tr(a)$ are rational integers.*

For proof see [Mil15].

One of the basic facts in algebraic number theory is that the ring $\mathcal{O}_K$ is a free $\mathbb{Z}$-module with dimension $[K : \mathbb{Q}]$. Its basis over $\mathbb{Z}$ is called *integral basis*.

Ring of integers $\mathcal{O}_K$ has an important number invariant called *discriminant*. For totally real fields, it describes the volume of fundamental domain of lattice $\mathcal{L}$ which is formed by points $(\sigma_1(a), \sigma_2(a), \ldots, \sigma_d(a))$ in $\mathbb{R}^d$ where $a \in K$. Formal definition of discriminant is rather technical and we will not need it. For more details see [Mil14].

1.2 Totally positive elements

Definition 7. Number field K is called *totally real* if every embedding $\sigma : K \to \mathbb{C}$ has range in $\mathbb{R}$.

Definition 8. Let K be a number field of degree d over $\mathbb{Q}$ and $\mathcal{O}_K$ its ring of integers. An element α of K is said to be *totally positive* if $\sigma(\alpha) > 0$ for every real embedding $\sigma : K \to \mathbb{R}$. We denote K^+ the set of all totally positive elements and $\mathcal{O}_K^+$ the set of all totally positive integers in $\mathcal{O}_K$.

Let $a, b \in K$. We write $a \succ b$ if $\sigma(a) > \sigma(b)$ for every embedding $s : K \to \mathbb{R}$. It is easy to see that $\succ$ is a preorder relation on K. Clearly an element a is totally positive totally positive if and only if $a \succ 0$.

Since the norm of $a \in K$ is the product of all $\sigma_i(a)$, we have $N(a) > 0$. Analogically, trace of a is a sum of all $\sigma_i(a)$, so $\mathrm{Tr}(a) > 0$.

2. Biquadratic fields

In this chapter, we introduce biquadratic fields and investigate some of their properties. Throughout the text, let p and q be two distinct nonzero squarefree integers (not necessarily primes). It is easy to see that this condition implies that $\sqrt{q} \notin \mathbb{Q}(\sqrt{p})$ and $\sqrt{p} \notin \mathbb{Q}(\sqrt{q})$.

A Biquadratic field $\mathbb{Q}(\sqrt{p}, \sqrt{q})$ is the smallest extension of $\mathbb{Q}$ which contains $\sqrt{p}$ and $\sqrt{q}$. Its degree over $\mathbb{Q}$ is 4. It is the splitting field of the polynomial $(x^2-p)(x^2-q)$, so it is always Galois extension of $\mathbb{Q}$ with Galois group isomorphic to Klein group $\mathbb{Z}_2^2$. It has exactly three quadratic subfields $\mathbb{Q}(\sqrt{p})$, $\mathbb{Q}(\sqrt{p})$, $\mathbb{Q}(\sqrt{r})$ where

$$r = \frac{pq}{\gcd(p,q)^2}.$$

For example, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ has three quadratic subfields $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{6})$.

2.1 Ring of integers of $\mathbb{Q}(\sqrt{p}, \sqrt{q})$

It is well known that rings of integers in quadratic fields $K = \mathbb{Q}(\sqrt{p})$ (where p is squarefree) are of the form

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}\left[\sqrt{p}\right] & \text{if } p \equiv 2,3 \pmod 4, \\ \mathbb{Z}\left[\frac{1+\sqrt{p}}{2}\right] & \text{if } p \equiv 1 \pmod 4. \end{cases}$$

Similar, but slightly more complicated situation occurs in the case of biquadratic fields. The following theorem describes the structure of rings of integers in biquadratic fields.

Theorem 9 (characterization of $\mathcal{O}_K$ in $\mathbb{Q}(\sqrt{p}, \sqrt{q})$)**.** *Let $K = \mathbb{Q}(\sqrt{p}, \sqrt{q})$ be a biquadratic field, where $p \neq q$ are distinct squarefree integers. Let us recall that $r = \frac{pq}{\gcd(p,q)^2}$. Then without loss of generality there are only four possibilities:*

1. $p \equiv 3 \pmod 4$, $q \equiv r \equiv 2 \pmod 4$;
2. $p \equiv 1 \pmod 4$, $q \equiv r \equiv 2 \pmod 4$;
3. $p \equiv 1 \pmod 4$, $q \equiv r \equiv 3 \pmod 4$;
4. $p \equiv 1 \pmod 4$, $q \equiv r \equiv 1 \pmod 4$.

In these cases, $\mathcal{O}_K$ has an integral basis of the form:

1. $\left(1, \sqrt{p}, \sqrt{q}, \frac{\sqrt{q}+\sqrt{r}}{2}\right)$;
2. $\left(1, \frac{1+\sqrt{p}}{2}, \sqrt{q}, \frac{\sqrt{q}+\sqrt{r}}{2}\right)$;
3. $\left(1, \frac{1+\sqrt{p}}{2}, \sqrt{q}, \frac{\sqrt{q}+\sqrt{r}}{2}\right)$;
4. $\left(1, \frac{1+\sqrt{p}}{2}, \frac{1+\sqrt{q}}{2}, \frac{(1+\sqrt{p})(1+\sqrt{q})}{4}\right)$.

The discriminant of $\mathcal{O}_K$ is 1) $64pqr$, 2) $16prq$, 3) $16prq$ and 4) pqr.

Proof. Full proof can be found in [Jar07, Prop. 8.22]. We only show one inclusion in the first case $p \equiv 3 \pmod 4$, $q \equiv r \equiv 2 \pmod 4$ to gain some intuition about where the half-integers come from.

It is obvious that, $\sqrt{p}$ and $\sqrt{q}$ are in $\mathcal{O}_K$ since they are roots of quadratic polynomials $x^2 - p$ and $x^2 - q$, respectively. An element of the field K lies in $\mathcal{O}_K$ if and only if the coefficients of its minimal polynomial are rational integers. These coefficients can be expressed as the symmetric polynomials in roots of this polynomial, i.e. conjugates of α. So we only need to compute $N\left(\frac{\sqrt{q}+\sqrt{r}}{2}\right)$ and $\mathrm{Tr}\left(\frac{\sqrt{q}+\sqrt{r}}{2}\right)$ and two other symmetric polynomials to check that $\frac{\sqrt{q}+\sqrt{r}}{2}$ really is an algebraic integer.

If we do it, we get that the minimal polynomial of $\frac{\sqrt{q}+\sqrt{r}}{2}$ is

$$x^4 - \frac{q+r}{2}x^2 + \left(\frac{q-r}{4}\right)^2.$$

and clearly all coefficients are integers since $q \equiv r \pmod 4$.

The discriminant can be computed as the determinant of the matrix 4×4 whose rows contain all conjugates of the elements of integral basis. □

2.2 Group of units of $\mathbb{Q}(\sqrt{p}, \sqrt{q})$

In this section we study units in the ring of integers of biquadratic field $\mathbb{Q}(\sqrt{p}, \sqrt{q})$. In particular, we are interested in totally positive units. Recall that a unit u is totally positive if $u \succ 0$ which means that all conjugates of u are positive. As we will see later, totally positive units are important for understanding the structure of indecomposable elements. They also play a role in constructions of universal forms.

First we present a classical result due to Dirichlet.

Theorem 10 (Dirichlet unit theorem)**.** *Let K be a number field and U_K the group of units in $\mathcal{O}_K$. Let r be the number of real embeddings of K and s the number of pairs of conjugate complex embeddings of K. Then the group U_K is finitely generated with rank $r + s - 1$. Its torsion subgroup consist of roots of unity in K, hence is finite.*

Proof. For the proof see Milne [Mil14]. The proof uses Minkowski's *geometry of numbers.* □

In the case of totally real biquadratic field K, Dirichlet theorem states that the group of units U_K is isomorphic to $\mathbb{Z}^3 \oplus \mathbb{Z}/2\mathbb{Z}$, because the only real roots of unity are 1 and -1 and a totally real biquadratic field has no complex and exactly four real embeddings.

Lemma 11. *Let K be a totally real field. By U_K^+ we mean the subgroup of U_K consisting of totally positive units. The subgroup U_K^+ has finite index in U_K and it is a free abelian group of rank $r - 1$.*

Proof. Every subgroup of a finitely generated abelian group G is finitely generated. Moreover, a subgroup of finite index has the same rank as G. Let U_K^2 be the subgroup of squares in U_K. Then we have $U_K^2 \subseteq U_K^+ \subset U_K$ since every square in K is totally positive (all conjugates are the squares of a real number).

The subgroup U_K^2 has a finite index in U_K. The group U_K is isomorphic $\mathbb{Z}^{r-1} \oplus \mathbb{Z}/2\mathbb{Z}$ and we have a surjective map from $\mathbb{Z}^{r-1} \oplus \mathbb{Z}/2\mathbb{Z}$ to $(\mathbb{Z}/2\mathbb{Z})^{r-1} \oplus \mathbb{Z}/2\mathbb{Z}$ which sends an element $(x_1, x_2, \ldots, x_{r-1}, a)$ to $(x_1 + 2\mathbb{Z}, x_2 + 2\mathbb{Z}, \ldots, x_{r-1} + 2\mathbb{Z}, a)$ where $x_i \in \mathbb{Z}$ and $a \in \mathbb{Z}/2\mathbb{Z}$. The kernel of this map is precisely the subgroup $2\mathbb{Z}$ which is isomorphic to U_K^2. We obtain that

$$U_K/U_K^2 \simeq (\mathbb{Z}/2\mathbb{Z})^{r-1} \oplus \mathbb{Z}/2\mathbb{Z} \simeq (\mathbb{Z}/2\mathbb{Z})^r$$

so U_K^+ has index 2^r in U_K. This argument can be illustrated by the following commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U_K^2 & \longrightarrow & U_K & \longrightarrow & U_K/U_K^2 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & 2\mathbb{Z}^{r-1} & \longrightarrow & \mathbb{Z}^{r-1} \oplus \mathbb{Z}/2\mathbb{Z} & \longrightarrow & (\mathbb{Z}/2\mathbb{Z})^{r-1} \oplus \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 0 \end{array}$$

where the downward arrows are isomorphisms and the rows are exact.

The subgroup U_K^+ has also finite index since it lies between U_K and U_K^+. Its torsion consist of all roots of unity in U_K^+, but the only totally positive root of unity is 1, so the torsion subgroup is trivial. This implies that U_K^+ is a free abelian group of rank $r - 1$. □

Specially, if K is a totally real biquadratic field, then the rank of U_K and U_K^+ is 3. The subgroup of squares U_K^2 has index 16 in U_K and we have

$$16 = [U_K : U_K^2] = [U_K : U_K^+][U_K^+ : U_K^2],$$

hence we obtain that the index of U_K^+ in U_K is a divisor of 16 and the index of U_K^2 in U_K^+ is a divisor of 8 (by absence of torsion elements). It is not easy to say more about this indices. Garbanati [Gar76] observed that $U_K^+ = U_K^2$ if and only if there is a unit of the norm -1 in U_K. In biquadratic field, we can transfer this question to its quadratic subfields. However, even in the quadratic field is probably not known any simple condition[1] describing the existence of a unit of the norm -1.

Proposition 12. *Let K be a totally real biquadratic field. If there exist a unit of norm -1 in U_K then there exist an (integral) unit of the norm -1 in all quadratic subfields of K.*

Proof. First observe, that if α is a unit of the norm -1, then α does not lie in any of quadratic subfields of K. If α would lie in some quadratic subfields, then it would have two pairs of conjugates which are mutually equal. So the norm would be a square of real number, hence it would be positive.

[1] One condition states that there is a unit of the norm -1 in $U_{\mathbb{Q}(\sqrt{D})}$ if and only if the period of the continued fraction of $\sqrt{D}$ has odd length.

For every element α of the norm -1 with conjugates $\alpha = \alpha^{(1)}, \alpha^{(2)}, \alpha^{(3)}, \alpha^{(4)}$ we know that each of the elements $\alpha^{(1)}\alpha^{(2)}, \alpha^{(1)}\alpha^{(3)}$ and $\alpha^{(1)}\alpha^{(4)}$ is fixed by one of three (distinct) automorphisms of K, so each of them lies in one of (distinct) quadratic subfields of K. Each of this elements has the norm -1 in its quadratic field, for example if $\alpha^{(1)}\alpha^{(2)}$ lies in a quadratic subfield L, then

$$N_L(\alpha^{(1)}\alpha^{(2)}) = (\alpha^{(1)}\alpha^{(2)})(\alpha^{(3)}\alpha^{(4)}) = \alpha^{(1)}\alpha^{(2)}\alpha^{(3)}\alpha^{(4)} = N_K(\alpha) = -1$$

□

Example. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. The equation $x^2 - 3y^2 = -1$ has no solution in $\mathbb{Z}$ as can be seen if we use quadratic residues modulo 3. So in the $\mathbb{Q}(\sqrt{3})$ there is no unit of the norm -1. From Proposition 12 we obtain that there is no unit of the norm -1 in K, too. The result of Garbanati then implies that not every totally positive unit is a square.

As can easily be seen, the group of totally positive units U_K^+ is generated by the (mutually conjugate) units

$$\begin{aligned}\alpha &= 2 - \sqrt{2}/2 + \sqrt{6}/2,\\ \beta &= 2 - \sqrt{2}/2 - \sqrt{6}/2,\\ \gamma &= 2 + \sqrt{2}/2 - \sqrt{6}/2.\end{aligned}$$

The subgroup of squares is generated by units

$$\begin{aligned}\alpha\beta &= 3 - 2\sqrt{2} = (1 - \sqrt{2})^2,\\ \beta\gamma &= 5 + 2\sqrt{6} = (\sqrt{2} + \sqrt{3})^2,\\ \gamma\alpha &= 2 + \sqrt{3} = (\sqrt{2}/2 + \sqrt{6}/2)^2.\end{aligned}$$

Subgroup U_K^2 has index 2 in U_K^+ since it is generated by products of listed generators α, β, γ of U_K^+. Note that the units $\alpha\beta, \beta\gamma$ and $\gamma\alpha$ are exactly the fundamental units of quadratic subfields $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{6})$ and $\mathbb{Q}(\sqrt{3})$, respectively.

3. Indecomposable integers

3.1 Indecomposable integers in quadratic fields

Definition 13. A totally positive element $\alpha \in \mathcal{O}_K$ is (additively) *decomposable*, if $\alpha = \beta + \gamma$ for $\beta, \gamma \in \mathcal{O}_K^+$. Otherwise, it is called *indecomposable*.

Lemma 14. *Let K be a totally real fields and $\alpha \in U_K$ be a unit. Then α is indecomposable.*

Proof. For contradiction, suppose that $\alpha = \beta + \gamma$ is an expression of a unit α as a sum of totally positive elements. The norm of an element equals to the product of all its conjugates. Therefore

$$1 = N(\alpha) = N(\beta+\gamma) = (\beta^{(1)}+\gamma^{(1)})(\beta^{(2)}+\gamma^{(2)})\dots(\beta^{(n)}+\gamma^{(n)}) \geq N(\beta)+N(\gamma) \geq 2$$

because all conjugates $\beta^{(i)}$ and $\gamma^{(i)}$ are positive. This is contradiction. □

In the case of quadratic fields we can obtain a stronger result using the mixed terms in the product $\prod(\beta^{(i)} + \gamma^{(i)})$. Moreover, in a totally real quadratic field $\mathbb{Q}(\sqrt{D})$ (so D is squarefree positive integer), there is a complete description of indecomposable elements in terms of continued fraction of $\sqrt{D}$. See [Kal16a].

We define $\delta = 2\sqrt{D}$ if $D \equiv 2, 3 \pmod 4$ and $\delta = \sqrt{D}$ if $D \equiv 1 \pmod 4$.

Lemma 15. *Let $\alpha \in \mathbb{Q}(\sqrt{D})$ be a totally positive element, $\alpha \notin \mathbb{Z}$. Then*

$$Tr(\alpha) > \delta.$$

Proof. Suppose that $D \equiv 2, 3 \pmod 4$ (so that $\delta = 2\sqrt{D}$). We can write $\alpha = x + y\sqrt{D}$ where $x, y \in \mathbb{Z}$. We have

$$x + y\sqrt{D} > 0$$

$$x - y\sqrt{D} > 0.$$

In other words x is strictly larger than $|y\sqrt{D}|$ which implies $x > \sqrt{D}$, because $y \neq 0$ is an integer. Finally we have

$$\mathrm{Tr}(\alpha) = (x + y\sqrt{D}) + (x - y\sqrt{D}) = 2x > 2\sqrt{D} = \delta.$$

The second case $D \equiv 1 \pmod 4$ is analogous. □

Proposition 16. *Let $\alpha \in O_{\mathbb{Q}(\sqrt{D})}$ be an integer satisfying $N(\alpha) < \delta$ and $n \nmid \alpha$ for every $n \in \mathbb{N}$. Then α is indecomposable.*

Proof. For contradiction, suppose that α is decomposable. Then we have

$$\begin{aligned} \delta > N(\alpha) &= (\beta^{(1)} + \gamma^{(1)})(\beta^{(2)} + \gamma^{(2)}) \\ &= \beta^{(1)}\beta^{(2)} + \gamma^{(1)}\gamma^{(2)} + (\beta^{(1)}\gamma^{(2)} + \beta^{(2)}\gamma^{(1)}) \\ &= N(\beta) + N(\gamma) + \mathrm{Tr}(\beta^{(1)}\gamma^{(2)}). \end{aligned} \tag{3.1}$$

We see that $\delta > \mathrm{Tr}(\beta^{(1)}\gamma^{(2)})$ but then Lemma 15 implies that $\beta^{(1)}\gamma^{(2)} \in \mathbb{N}$. This yields $\beta^{(1)}\gamma^{(2)} = \beta^{(2)}\gamma^{(1)}$ since the Galois group acts trivially on $\mathbb{N}$. Then we get

$$\beta = \beta^{(1)} = \frac{\beta^{(2)}\gamma^{(1)}}{\gamma^{(2)}} = \frac{\beta^{(2)}\gamma^{(1)}}{\gamma^{(2)}\gamma^{(1)}}\gamma^{(1)} = \frac{\beta^{(2)}\gamma^{(1)}}{N(\gamma)}\gamma^{(1)} = \frac{u}{v}\gamma^{(1)} = \frac{u}{v}\gamma,$$

where u and v are coprime rational integers. We obtain

$$v\beta = u\gamma.$$

Since u and v are coprime, we can find x and $y \in \mathbb{Z}$ such that

$$ux + vy = 1$$

(Bézout equality). We know that u divides $v\beta$ so it divides also $vy\beta$. Moreover u divides $ux\beta$. If we add this up and use Bézout equality, we obtain that u divides β. Similarly v divides γ. Then we obtain $\beta = uc$ and $\gamma = v\frac{\beta}{u} = vc$ for some $c \in \mathcal{O}_K$, so $\alpha = (u+v)c$, which is contradiction. □

3.2 Indecomposables in biquadratic fields

Slight modification of the arguments from the previous section can be used for biquadratic fields. Let $K = \mathbb{Q}(\sqrt{p}, \sqrt{q})$ be a totally real biquadratic field and $r = \frac{pq}{(p,q)^2}$. Suppose that $\alpha \in \mathcal{O}_K$. Then we can write

$$\alpha = a + b\sqrt{p} + c\sqrt{q} + d\sqrt{r}$$

where a, b, c, $d \in \frac{1}{4}\mathcal{O}_K$. The presence of halfs and quarters of integers depends on the residues of p and q modulo 4 as we know from Theorem 9.

Lemma 17. *Suppose that $\alpha = a + b\sqrt{p} + c\sqrt{q} + d\sqrt{r} \in \mathcal{O}_K$, $\alpha \notin \mathbb{Z}$, then*

1. *If $b \neq 0$, then*

$$Tr(\alpha) > \begin{cases} 4\sqrt{p} & \text{if } p \equiv 3 \pmod 4 \ \&\ q \equiv 2 \pmod 4 \\ 2\sqrt{p} & \text{if } p \equiv 1 \pmod 4 \ \&\ q \equiv 2 \pmod 4 \\ 2\sqrt{p} & \text{if } p \equiv 1 \pmod 4 \ \&\ q \equiv 3 \pmod 4 \\ \sqrt{p} & \text{if } p \equiv 1 \pmod 4 \ \&\ q \equiv 1 \pmod 4 \end{cases}$$

2. *If $c \neq 0$, then*

$$Tr(\alpha) > \begin{cases} 2\sqrt{p} & \text{if } p \equiv 3 \pmod 4 \ \&\ q \equiv 2 \pmod 4 \\ 2\sqrt{p} & \text{if } p \equiv 1 \pmod 4 \ \&\ q \equiv 2 \pmod 4 \\ 2\sqrt{p} & \text{if } p \equiv 1 \pmod 4 \ \&\ q \equiv 3 \pmod 4 \\ \sqrt{p} & \text{if } p \equiv 1 \pmod 4 \ \&\ q \equiv 1 \pmod 4 \end{cases}$$

3. *If $d \neq 0$, then*

$$Tr(\alpha) > \begin{cases} 2\sqrt{r} & \text{if } p \equiv 3 \pmod 4 \ \&\ q \equiv 2 \pmod 4 \\ 2\sqrt{r} & \text{if } p \equiv 1 \pmod 4 \ \&\ q \equiv 2 \pmod 4 \\ 2\sqrt{r} & \text{if } p \equiv 1 \pmod 4 \ \&\ q \equiv 3 \pmod 4 \\ \sqrt{r} & \text{if } p \equiv 1 \pmod 4 \ \&\ q \equiv 1 \pmod 4 \end{cases}$$

Proof. We prove only the case $d \neq 0$ and $p \equiv 3 \pmod 4$ and $q \equiv 2 \pmod 4$. Other cases are similar. Recall that in this case the ring of integers $\mathcal{O}_K$ has an integral basis $(1, \sqrt{p}, \sqrt{q}, \frac{\sqrt{q}+\sqrt{r}}{2})$. Consequently a, b are integers and c, d are half-integers. The element α is totally positive, which means that all its conjugates are positive:

$$a + b\sqrt{p} + c\sqrt{q} + d\sqrt{r} > 0$$
$$a - b\sqrt{p} - c\sqrt{q} + d\sqrt{r} > 0$$
$$a - b\sqrt{p} + c\sqrt{q} - d\sqrt{r} > 0$$
$$a + b\sqrt{p} - c\sqrt{q} - d\sqrt{r} > 0$$

If we sum first two inequalities we get $a > -d\sqrt{r}$. By summing the second two inequalities we get $a > d\sqrt{r}$. Similar inequalities holds for c. Since d is the nonzero half-integer, the inequality $a > |d\sqrt{r}|$ implies $a > \frac{\sqrt{r}}{2}$ and hence

$$\mathrm{Tr}(\alpha) = 4a > 2\sqrt{r}.$$

□

Corollary 18. *If K is a totally real biquadratic field, $\alpha \in K$ and $\alpha \notin \mathbb{Z}$, then $Tr(\alpha) > \min(\sqrt{p}, \sqrt{q}, \sqrt{r})$.*

Proof. If $\alpha \notin \mathbb{Z}$, then at least one of b, c or d is nonzero. □

Proposition 19. *Let p, q, r be as usual and $K = \mathbb{Q}(\sqrt{p}, \sqrt{q})$. Let $\alpha \in \mathcal{O}_K^+$ be an element which satisfies $N(\alpha) < 2\min(\sqrt{p}, \sqrt{q}, \sqrt{r})$ and $n \nmid \alpha$ for every $n \in \mathbb{N}$. Then α is indecomposable.*

Proof. Denote $\delta = \min(\sqrt{p}, \sqrt{q}, \sqrt{r})$. For contradiction, suppose that $\alpha = \beta + \gamma$ where $\beta, \gamma \in \mathcal{O}_K^+$. Then we have

$$\begin{aligned} 2\delta > N(\alpha) &= (\beta^{(1)} + \gamma^{(1)})(\beta^{(2)} + \gamma^{(2)})(\beta^{(3)} + \gamma^{(3)})(\beta^{(4)} + \gamma^{(4)}) \\ &> \mathrm{Tr}(\beta^{(1)}\gamma^{(2)}\gamma^{(3)}\gamma^{(4)}) + \mathrm{Tr}(\beta^{(1)}\beta^{(2)}\beta^{(3)}\gamma^{(4)}) + \text{other (positive) members} \end{aligned}$$

The preceding corollary implies that $\beta^{(1)}\gamma^{(2)}\gamma^{(3)}\gamma^{(4)}$ or $\beta^{(1)}\beta^{(2)}\beta^{(3)}\gamma^{(4)}$ is an integer. Without loss of generality we have

$$\beta^{(1)}\gamma^{(2)}\gamma^{(3)}\gamma^{(4)} = \beta^{(2)}\gamma^{(3)}\gamma^{(4)}\gamma^{(1)} \in \mathbb{N}.$$

Now we can repeat the argument from the Proposition 16. If we divide the equality by the norm of γ, we get

$$\beta = \beta^{(1)} = \frac{\beta^{(2)}\gamma^{(3)}\gamma^{(4)}\gamma^{(1)}}{N(\gamma)}\gamma^{(1)} = \frac{u}{v}\gamma$$

where u and v are coprime natural numbers. Then as in quadratic case we have $\beta = uc$ and $\gamma = vc$ for some $c \in \mathcal{O}_K$, so $\alpha = (u+v)c$, contradiction. □

3.3 Maximal norm of indecomposables

To compute indecomposable elements on computer, we want some upper bound on their norms. We prove in Theorem 21 that elements of sufficiently large norm are always decomposable. The bound is probably very ineffective and depends on the structure of the group of units U_K. In a quadratic field $\mathbb{Q}(\sqrt{D})$ we have a better bound, namely D. This result can be found in the article [Kal16a]. It is an interesting question if there is a similar bound for other fields.

We start the proof of Theorem 21 with the following lemma. By $\widehat{\alpha}$ we mean maximum of $|\alpha^{(i)}|$ over all conjugates $\alpha^{(i)}$ of α.

Lemma 20. *Let K be a totally real field of degree d. Then there is a constant B_K satisfying the following condition. For every α in K there exists a totally positive unit $e \in U_K$ such that*

$$\widehat{\alpha e} < B_K |N(\alpha)|^{\frac{1}{d}}.$$

Proof. Let ι be a map defined as

$$\begin{aligned} \iota\colon K &\to \mathbb{R}^d \\ \alpha &\mapsto (\log|\alpha^{(1)}|, \log|\alpha^{(2)}|, \ldots, \log|\alpha^{(d)}|). \end{aligned}$$

If ε is a unit in K, then $\sum \log \varepsilon_i = \log 1 = 0$, so ε is mapped to the hyperplane $W \simeq \mathbb{R}^{d-1}$ with normal vector $(1, 1, \ldots, 1)$. By Dirichlet theorem 10, the image of U_K forms a (discrete) lattice $\mathcal{L}$ of dimension $d-1$ in W. Since the subgroup U_K^+ has finite index in U_K, its image forms a sublattice $\mathcal{L}^+$ of the same dimension. For $\alpha \in K$ we can interpret the number $\frac{\log|N(\alpha)|}{\sqrt{d}}$ as h_α, where h_α is the distance from the point $\iota(\alpha)$ to hyperplane W. Indeed,

$$h_\alpha = \frac{\iota(\alpha)\cdot(1,1,\ldots,1)}{|(1,1,\ldots,1)|} = \frac{\log|\alpha^{(1)}| + \log|\alpha^{(2)}| + \cdots + \log|\alpha^{(d)}|}{\sqrt{d}} = \frac{\log|N(\alpha)|}{\sqrt{d}}.$$

The multiplication of an element α by units shifts the point of $\iota(\alpha)$ in the hyperplane V, the hyperplane whoch contains $\iota(\alpha)$ and is parallel to hyperplane W. We want to minimize all coordinates of $\iota(\alpha\varepsilon)$ so we would like to shift the point $\iota(\alpha)$ as close as possible to the point $P = \left(\frac{\log|N(\alpha)|}{d}, \frac{\log|N(\alpha)|}{d}, \ldots, \frac{\log|N(\alpha)|}{d}\right)$.

We fix a fundamental system of totally positive units $u_1, u_2, \ldots, u_{d-1}$ (the basis of the lattice $\mathcal{L}^+$). These units form a fundamental parallelogram in the hyperplane W. We denote λ the diameter of this parallelogram, i.e. the maximal distance between two points in the parallelogram. Then for every point in W there is some point of $\mathcal{L}^+$ in the distance smaller than λ. This implies that we can shift $\iota(\alpha)$ by some vector $\iota(\varepsilon)$ of $\mathcal{L}^+$ in a such way that the distance in the plane V between the points $\iota(\alpha\varepsilon)$ and P is smaller than λ. Then the point $\iota(\alpha\varepsilon)$ lies in the ball in $\mathbb{R}^d$ with the centre P and the radius λ. So we have

$$\begin{aligned} \log|\alpha_i\varepsilon_i| &< D + \frac{\log|N(\alpha)|}{d}, \\ |\alpha_i\varepsilon_i| &< e^D |N(\alpha)|^{\frac{1}{d}}. \end{aligned}$$

We see that we can put $B_K = e^D$. □

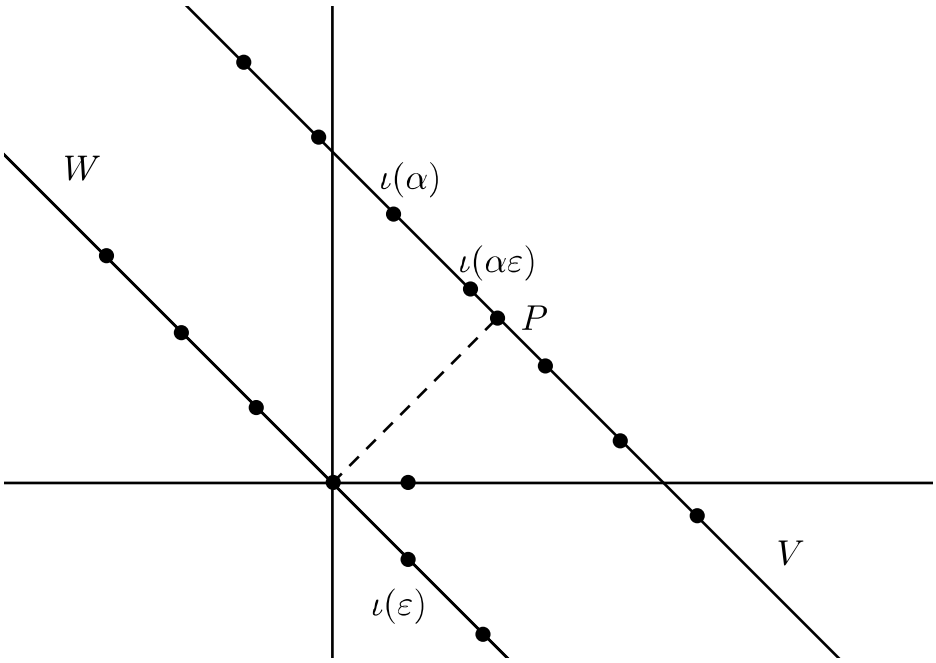


Figure 3.1: Visualization of the proof of Lemma 20

Theorem 21. *Let K be a totally real field of degree d over $\mathbb{Q}$ and $\alpha \in \mathcal{O}_K^+$. If $N(\alpha) > B_K^d$, then α is decomposable.*

Proof. Let α be an integer such that $N(\alpha) > B_K^d$. From the definition of B_K there exist a totally positive unit ε such that $\sigma(\alpha^{-1}\varepsilon) = |\sigma(\alpha^{-1}\varepsilon)| < B_K N(\alpha^{-1})^{\frac{1}{d}}$ for every σ ($\alpha^{-1}\varepsilon$ is totally positive, so every $\sigma(\alpha^{-1}\varepsilon)$ is positive). We obtain

$$\sigma(\alpha^{-1}\varepsilon)^d < B_K^d N(\alpha^{-1}) < N(\alpha)N(\alpha^{-1}) = 1.$$

which implies

$$\begin{aligned} \alpha^{-1}\varepsilon &\prec 1 \\ \varepsilon &\prec \alpha. \end{aligned}$$

We see that $\alpha - \varepsilon \succ 0$. Since we have also that $\varepsilon \succ 0$, we obtain the decomposition $\alpha = (\alpha - \varepsilon) + \varepsilon$ of α, so α is decomposable. □

4. Quadratic forms

4.1 Definition and basic properties

Definition 22. Let K be a field. *Quadratic form over* $\mathcal{O}_K$ is a quadratic polynomial in several variables with the coefficients from $\mathcal{O}_K$. Quadratic form Q is called *totally positive definite* if it has only totally positive values and zero. Equivalently the form Q is totally positive definite, if every form $Q^{(i)}$ which coefficients are i-th conjugates of coefficients of Q is positive definite in usual sense.

Definition 23. Totally positive definite form is called *universal* if it represents every totally positive integer.

Example. The form $a^2 + b^2 + c^2 + d^2$ is universal quadratic form over the field $\mathbb{Q}$ (Lagrange's theorem). There is no universal form over $\mathbb{Q}$ with three or less variables.

Example. Siegel [Sie45] proved that $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{5})$ are the only fields where the sum of four (or arbitrary many) squares is universal over the ring of integers.

4.2 Number of variables

V. Blomer and V. Kala recently proved [Kal16b] [BK15] that for every N there is a real quadratic field K such that every universal form over K has more than N variables. The start of this result is the following lemma and proposition.

Lemma 24 (Existence of lattice)**.** *Let $Q(x)$ be a positive definite quadratic n-ary form and A matrix such that $Q(x) = x^{\mathrm{T}}Ax$. Then there exist vectors $v^1, v^2, \ldots, v^n$ in $\mathbb{R}^n$ such that*

$$Q(x_1, x_2, \ldots, x_n) = |x_1 v^1 + x_2 v^2 + \cdots + x_n v^n|^2$$

In other words, there exists a lattice L in $\mathbb{R}^n$ with basis $v^1, v^2, \ldots, v^n$ such that the values of Q are equal to squares of lengths of vectors in L.

Proof. The standard result from linear algebra says that every positive definite matrix A can be written as a product $R^{\mathrm{T}}DR$ where the columns of the matrix R are eigenvectors $w^1, w^2, \ldots, w^n$ of A and the entries of D correspond to (positive) eigenvalues $\lambda_1, \lambda_1, \ldots, \lambda_n$ of A on diagonal and zero elsewhere. For the proof see [BT16, Thm. 10.32]. If we put $S = \sqrt{D}R$, we get decomposition $A = S^{\mathrm{T}}S$ and columns of S are the desired vectors $v^1, v^2, \ldots, v^n$. □

Proposition 25. *Assume that there exist totally positive integers $a_1, a_2, \ldots, a_N$ such that for all $1 \leq i \neq j \leq N$ we have that if $4a_i a_j \succeq c^2$, then $c = 0$ for all c in $\mathcal{O}_K$. Then there are no universal totally positive $(N-1)$-ary quadratic forms over $\mathcal{O}_K$.*

Proof. Let $Q = \sum_{1 \le i \le j \le n} a_{ij} x_i x_j$ be a quadratic form over $\mathcal{O}_K$ and let $A = (b_{ij})$ be its matrix with $b_{ii} = a_{ii}$ and $b_{ij} = b_{ji} = a_{ij}/2$.

For every automorphism σ of K denote $\sigma(A)$ the matrix with the entries $\sigma(b_{ij})$. Since the form Q is totally positive definite, the matrix $\sigma(A)$ is positive definite for every σ. Thus the (preceding) Lemma 24 gives us the decomposition $\sigma(A) = S_\sigma^T S_\sigma$ for some real matrix S_σ with columns v_σ^i. Denote $\mathcal{L}_\sigma$ the corresponding lattice with the basis $(v_\sigma^1, v_\sigma^2, \dots, v_\sigma^N)$.

Since Q is universal, for every totally positive element α each lattice $\mathcal{L}_\sigma$ contains a vector $w_\sigma(\alpha)$ for which $\sigma(\alpha) = \langle w_\sigma(\alpha), w_\sigma(\alpha) \rangle_\sigma$. In particular, Q represents all elements a_i so we get vectors $w_\sigma^1, w_\sigma^2, \dots w_\sigma^N \in \mathcal{L}_\sigma$ which satisfy

$$\sigma(a_i) = \langle w_\sigma^i, w_\sigma^i \rangle_\sigma.$$

We will prove that N vectors w_σ^i in the lattice $\mathcal{L}_\sigma$ are pairwise orthogonal. Then we have N linearly independent vectors, so

$$\text{number of variables of } Q = \dim(\mathcal{L}_\sigma) \ge N.$$

By the Cauchy-Schwarz inequality for $\langle \cdot, \cdot \rangle_\sigma$, we obtain

$$\sigma(a_i)\sigma(a_j) = \langle w_\sigma^i, w_\sigma^i \rangle_\sigma \langle w_\sigma^j, w_\sigma^j \rangle_\sigma \ge (\langle w_\sigma^i, w_\sigma^j \rangle_\sigma)^2 = \sigma(c)^2.$$

for some $c \in \frac{1}{2}\mathcal{O}_K$ (which is independent on σ - this follows from the definition of the lattices $\mathcal{L}_\sigma$). We see that $4a_i a_j \succeq c^2$, so $c = \langle w_\sigma^i, w_\sigma^j \rangle_\sigma = 0$ so the vectors w_i are pairwise orthogonal in lattice $\mathcal{L}_\sigma$. □

4.3 Quadratic and biquadratic case

V. Blomer and V. Kala proved the following theorem.

Theorem 26. *For every N there exist a squarefree integer D such that in $\mathbb{Q}(\sqrt{D})$ exist elements $a_1, a_2, \dots a_N$ from the preceding proposition and consequently every universal quadratic over $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ has more than $N-1$ variables.*

For the proof see [Kal16b] [BK15]. We use this theorem to prove its analogy in the case of biquadratic fields.

Theorem 27. *For every N there exist two distinct coprime squarefree integers p, q such that in $K = \mathbb{Q}(\sqrt{p}, \sqrt{q})$ every universal quadratic form in this field has more than $N-1$ variables.*

Proof. Let $Q(\sqrt{p})$ be a quadratic field in which there exist elements $a_1, a_2, \dots a_N$ from Proposition 25 and $p \equiv 3 \pmod 4$ (it is not difficult to see from the article [Kal16b] that we can do this assumption). The idea of the proof is to find some q such that in K, the elements a_i still satisfy the condition of Theorem 25. We will use the characterization of integers in K 9 and Lemma 17 which gives us the lower bound on the trace of positive elements.

We choose a squarefree integer q such that:

- $\sqrt{q} > \mathrm{Tr}(a_i a_j)$ for every $1 \le i < j \le N$.

- $q \equiv 2 \pmod 4$.
- $gcd(p, q) = 1$.

Now suppose that $4a_i a_j \succeq c^2$ for some $c \in \mathcal{O}_K$. If $c \in \mathbb{Q}(\sqrt{p})$, then also $c \in \mathcal{O}_{\mathbb{Q}}(\sqrt{p})$ because Theorem 9 implies that for $p \equiv 3 \pmod 4$ and $q \equiv 2 \pmod 4$ we have

$$\mathbb{Q}(\sqrt{p}) \cap \mathcal{O}_K = \mathbb{Z}[\sqrt{p}] = \mathcal{O}_{\mathbb{Q}(\sqrt{p})}.$$

Then the choice of elements a_i and the condition of Proposition 25 says that $c = 0$.

Suppose that $c \notin \mathbb{Q}[\sqrt{p}]$, so we can write $c = u + v\sqrt{q}$ where $u, v \in \mathbb{Q}(\sqrt{p})$ and v is nonzero. Then we get

$$c^2 = u^2 + 2uv\sqrt{q} + v^2 q.$$

We consider two cases. If u is zero, then $c^2 = v^2 q$. Then

$$\mathrm{Tr}(c^2) = q\mathrm{Tr}(v^2) \geq q \geq \sqrt{q}$$

where the inequality $\mathrm{Tr}(v^2) > q$ holds since v^2 is nonzero totally positive integer and its trace is then a positive integer. But then we have contradiction with the first condition in the definition of q. So we obtain $c = 0$.

If u is nonzero, then one of the coordinates of c^2 at $\sqrt{q}$ or $\sqrt{r}$ is nonzero so Lemma 17 implies that $\mathrm{Tr}(c^2) > \min(\sqrt{q}, \sqrt{r}) \geq \sqrt{q}$ (third condition in the definition of q implies that $r = pq > q$). But then we have

$$\mathrm{Tr}(a_i a_j) \geq \mathrm{Tr}(c^2) > \sqrt{q}$$

which is contradiction with the first condition of the definition of q. So the elements a_i satisfy the condition of Proposition 25. □

Bibliography

[BH] M. Bhargava and J. Hanke. Universal quadratic forms and the 290-theorem. *preprint*.

[BK15] Valentin Blomer and Vítězslav Kala. Number fields without n-ary universal quadratic forms. *Math. Proc. Cambridge Philos. Soc.*, 159(2):239–252, 2015.

[Bru82] Horst Brunotte. The computation of a certain metric invariant of an algebraic number field. *Math. Comp.*, 38(158):627–632, 1982.

[Bru83] Horst Brunotte. Zur Zerlegung totalpositiver Zahlen in Ordnungen totalreeller algebraischer Zahlkörper. *Arch. Math. (Basel)*, 41(6):502–503, 1983.

[BT16] Libor Barto and Jiří Tůma. *Linear Algebra*. online, 2016.

[Gar76] Dennis A. Garbanati. Units with norm -1 and signatures of units. *J. Reine Angew. Math.*, 283/284:164–175, 1976.

[Jar07] F. Jarvis. *Algebraic Number Theory*. Springer, 2007.

[Kal16a] Vítězslav Kala. Norms of indecomposable integers in real quadratic fields. *J. Number Theory*, 166:193–207, 2016.

[Kal16b] Vítězslav Kala. Universal quadratic forms and elements of small norm in real quadratic fields. *Bull. Aust. Math. Soc., to appear*, 2016.

[Mil14] J.S. Milne. *Algebraic Number Theory*. online, 2014.

[Mil15] J.S. Milne. *Fields and Galois Theory*. online, 2015.

[Sie45] Carl L. Siegel. Sums of m-th powers of algebraic integers. *Ann. of Math. (2)*, 46:313–339, 1945.