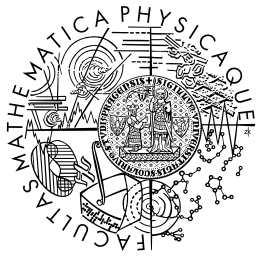


FACULTY
OF MATHEMATICS
AND PHYSICS
Charles University

DOCTORAL THESIS

Jakub Krásenský

Universal quadratic forms over orders in number fields

Department of Algebra

Supervisor of the doctoral thesis: doc. Mgr. Vítězslav Kala, Ph.D.

Study programme: Mathematics

Study branch: Algebra, number theory, and mathematical logic

Prague 2023

I declare that I carried out this doctoral thesis independently, and only with the cited sources, literature and other professional sources. It has not been used to obtain another or the same degree.

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 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 ....

Author's signature

My warmest thanks belong to all the people who supported or inspired me on my journey – both as a mathematician and as a human being. This includes my family and friends, my teachers, classmates and colleagues, and many others.

Mathematicians who directly influenced the contents of this thesis are above all my kind advisor Vítězslav Kala and my co-authors Magdaléna Tinková, Kristýna Zemková, Martin Raška, Ester Sgallová and Pavlo Yatsyna. I also learned a lot about quadratic forms from Wai Kiu Chan, Rudolf Scharlau and Karim Johannes Becher. Martin Čech contributed to the contents of the first chapter and several discussions with Alexander Slávik helped me clarify some of my thoughts.

Title: Universal quadratic forms over orders in number fields

Author: Jakub Krásenský

Department: Department of Algebra

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

Abstract: This thesis studies quadratic forms and lattices over rings of integers in number fields, and, to some extent, over non-maximal orders as well. The main focus is on universality of forms and lattices, and on the connected notion of the Pythagoras number. We mostly study totally positive definite forms and lattices over totally real fields, as this is arguably the most difficult case with very unpredictable behaviour. In some chapters we develop a general theory valid for fields of all degrees – in particular when we study the quadratic Waring's problem –, while in others we present important detailed results for families of fields in low degrees. By this we fulfill several purposes: We obtain interesting results, directly in line with questions studied by the likes of Siegel; we illustrate and further develop a multitude of techniques which could be applied in other situations; and we formulate conjectures and questions which can stimulate further research. Particular focus is put on real biquadratic fields; the first two chapters significantly advance the theory of integral quadratic forms over them.

Keywords: quadratic form, number field, sum of squares, Pythagoras number, quadratic Waring's problem

Contents

Introduction 4
- 0.1 Author's contribution . . . 4
- 0.2 General definitions and basic facts . . . 5
- 0.3 The situation in number fields . . . 5
- 0.4 Universal quadratic forms over number fields . . . 7
- 0.5 Sums of squares and Pythagoras number in totally real fields . . . 8
  - 0.5.1 Pythagoras number of orders in real biquadratic fields . . . 9
  - 0.5.2 Pythagoras number of non-maximal orders in biquadratic fields . . . 10
  - 0.5.3 A cubic ring of integers with the minimal Pythagoras number . . . 10
  - 0.5.4 Local–global principle by lattice covering . . . 11
  - 0.5.5 The connection between universal quadratic forms and Pythagoras numbers 12
- 0.6 Quadratic Waring's problem . . . 12

1 There are no universal ternary quadratic forms over biquadratic fields 15
- 1.1 Introduction . . . 15
- 1.2 Preliminaries . . . 17
  - 1.2.1 Algebraic integers . . . 17
  - 1.2.2 Biquadratic fields . . . 17
  - 1.2.3 Quadratic forms . . . 19
  - 1.2.4 Indecomposable integers . . . 20
- 1.3 Idea of the proof . . . 21
- 1.4 Preparation for the proof . . . 22
  - 1.4.1 Squares . . . 22
  - 1.4.2 Additive decompositions of rational integers . . . 23
  - 1.4.3 New indecomposable elements . . . 26
  - 1.4.4 Some useful properties of $\mathcal{M}$ and $\mathcal{S}$ . . . 32
  - 1.4.5 Unary forms . . . 35
  - 1.4.6 Direct decompositions of a quadratic lattice . . . 36
- 1.5 Proof in the main cases . . . 38
  - 1.5.1 Case (I) . . . 39
  - 1.5.2 Case (II) with 2ε not being a square . . . 39
  - 1.5.3 Case (II) with 2ε being a square . . . 39
  - 1.5.4 Case (III) with Q_0 diagonalizable . . . 40
  - 1.5.5 Case (III) with Q_0 nondiagonalizable . . . 41
- 1.6 Proof in the special cases . . . 44
  - 1.6.1 $\sqrt{3} \in K$ . . . 44
  - 1.6.2 $\sqrt{6} \in K$, $\sqrt{7} \in K$, $\sqrt{21} \in K$ or $\sqrt{33} \in K$ . . . 44
  - 1.6.3 $\sqrt{10} \in K$ . . . 44
  - 1.6.4 $\sqrt{13} \in K$ . . . 45
  - 1.6.5 $\sqrt{17} \in K$ . . . 45
  - 1.6.6 $m = 65$ . . . 46
  - 1.6.7 $m = 85$ . . . 47
  - 1.6.8 $\sqrt{2} \in K$ . . . 47
  - 1.6.9 $\sqrt{5} \in K$ . . . 49
  - 1.6.10 Remaining biquadratic fields . . . 50
- 1.7 Ternary forms over the quadratic field $\mathbb{Q}(\sqrt{10})$ . . . 52
- 1.8 Units in biquadratic fields . . . 53
- 1.9 Scheme of the main proof . . . 56

2 Pythagoras numbers of orders in biquadratic fields **57**
2.1 Introduction . . . 57
2.1.1 Historical overview . . . 57
2.1.2 Our results . . . 58
2.1.3 Structure of the paper . . . 60
2.2 Preliminaries . . . 61
2.2.1 Biquadratic fields . . . 61
2.2.2 An important convention . . . 62
2.3 Pythagoras numbers of orders in quadratic fields . . . 62
2.4 Lemmata and the use of computers . . . 64
2.4.1 Some arithmetics of biquadratic number fields . . . 64
2.4.2 The use of computers . . . 65
2.4.3 The computed data . . . 66
2.5 Results for fields with coprime m, s . . . 68
2.6 Pythagoras number is at least 5 (up to seven exceptions) . . . 72
2.6.1 The cases where $m \equiv 1 \pmod 4$ . . . 72
2.6.2 The cases where $m \not\equiv 1 \pmod 4$ . . . 73
2.6.3 The exceptional cases $s = m + 4, m + 8, m + 12$ . . . 77
2.6.4 Fields containing $\sqrt{6}$ or $\sqrt{7}$ . . . 79
2.6.5 Fields containing $\sqrt{2}$, $\sqrt{3}$ or $\sqrt{5}$ . . . 81
2.7 Fields containing $\sqrt{5}$ . . . 83
2.7.1 Lower bound in the most difficult case . . . 84
2.7.2 Upper bound . . . 88
2.8 Six is almost always a lower bound . . . 91
2.8.1 The idea . . . 92
2.8.2 The proof . . . 93
2.8.3 A conjecture . . . 95

3 A cubic ring of integers with the smallest Pythagoras number **97**
3.1 Introduction . . . 97
3.2 Preliminaries and results . . . 98
3.3 Sums of three squares . . . 99
3.4 The main proof . . . 101
3.5 Characterisation of sums of squares . . . 102
3.6 Final notes . . . 103

4 On quadratic Waring's problem in totally real number fields **104**
4.1 Introduction . . . 104
4.2 Preliminaries . . . 106
4.2.1 Quadratic forms, g-invariants . . . 106
4.2.2 Quadratic spaces and modules . . . 107
4.2.3 Free lattices . . . 107
4.2.4 Quadratic lattices . . . 107
4.2.5 Number fields, orders, Dedekind domains . . . 109
4.3 Observations about G . . . 109
4.4 The main proof . . . 111
4.5 $G(2)$ for quadratic rings of integers . . . 113
4.5.1 The case 1 mod 4 . . . 114

5 Pythagoras number of non-maximal orders in biquadratic fields **116**
5.1 Basic properties of basic orders 117
5.2 The first theorem 119
5.3 A more general result 121
5.4 The remaining 'non-coprime' cases 124

Bibliography **126**

List of publications **130**

Introduction

Quadratic forms are fundamental objects in mathematics and beyond. For example, both classical and relativistic physics are placed in a space in which distance is measured by a certain quadratic form; and Hilbert spaces, so important in functional analysis, are intimately connected with quadratic forms as well. The algebraic study of quadratic forms over fields is a vivid research area with Ernst Witt as one of the first leading figures.

This thesis studies quadratic forms from the point of view of number theory. Many number-theoretical questions about quadratic forms, including those handled in this text, are inspired by the some of the following classical problems, studied by the likes of Fermat, Lagrange, Gauss, Ramanujan, Conway, Bhargava, and many others: Is it true that all natural numbers can be expressed as a sum of four integral squares? Which numbers can be expressed in the form $x^2 + ky^2$ for a given k? Which positive definite quadratic forms over $\mathbb{Z}$ represent all natural numbers?

After a considerable effort of many mathematicians, these questions have been solved over the rational integers (although there remain innumerable related open problems). Therefore, our focus is on analogous problems for integral quadratic forms over totally real number fields. We study two strongly interrelated questions: Which quadratic forms are *universal*, i.e. capable of representing all totally positive integers? In particular, how many variables are needed for such a form? And, which numbers can be expressed as a sum of integral squares in the given field; how many squares suffice for such a representation?

The thesis consists of the following four papers, each of them presented as one chapter:

[KTZ] J. Krásenský, M. Tinková and K. Zemková, *There are no universal ternary quadratic forms over biquadratic fields*, Proc. Edinburgh Math. Soc. 63(3), 861–912 (2020).

[KRS] J. Krásenský, M. Raška and E. Sgallová, *Pythagoras numbers of orders in biquadratic fields*, Expo. Math. 40, 1181–1228 (2022).

[Kr] J. Krásenský, *A cubic ring of integers with the smallest Pythagoras number*, Arch. Math. (Basel) 118, 39–48 (2022).

[KrY] J. Krásenský and P. Yatsyna, *On quadratic Waring's problem in totally real number fields*, Proc. Amer. Math. Soc. 151, 1471–1485 (2023).

Moreover, there is a fifth chapter, based on the forthcoming paper [Kr2] J. Krásenský, *Pythagoras number of non-maximal orders in biquadratic fields*, in preparation.

The texts of the papers were left unchanged from the versions published on arXiv, only a few misprints and other minor imperfections were corrected and the references unified, updated and moved to the end of the thesis. For this reason, every chapter has a separate introduction; the notation and conventions may vary from chapter to chapter; and the respective introductions do not reflect the developments which occurred after the paper in question was accepted for publication.

Before presenting the papers, let us put them into context by first repeating the basics about quadratic forms and number fields, and then summarising the main results of each of the four papers and explaining their contribution.

0.1 Author's contribution

The paper [KTZ], which forms the first chapter, was co-written as a joint project with two other PhD students, Tinková and Zemková, and the contribution of all authors was approximately the same and hard to separate. Both co-authors of [KRS], i.e. of the second chapter, Raška and

Sgallová, were at that time less experienced than the present author, so a high proportion of the proofs and also the bulk of the text is due to him. To be more precise, the author contributed all main results with the notable exception of the contents of Section 2.5 including the important Theorem 2.1.1 (which are joint work of the other authors with the help of Tinková) and also most of the experimental data (these are due to Raška). Yatsyna suggested using the paper [Sa2] and hence played an important role as well. The paper [Kr], and thus the third chapter, was written without co-authors. The paper [KrY], forming the fourth chapter, stemmed from two independent ideas – Yatsyna came with the first formulation of the inequality between g-invariants in the free case and with an idea for a proof, while the present author simplified the proof and added the lattice formulation. Most of the paper is then joint work; only the final section where the upper bound is shown to be optimal for $G(2)$ of real quadratic fields is a separate effort by the present author. The fifth chapter and the intended paper [Kr2] is written solely by the present author. Of course, throughout all the papers, the author's advisor Kala served as an invaluable guide, suggesting problems to study, papers to look for answers in, and always willing to listen to new ideas.

0.2 General definitions and basic facts

An *n-ary quadratic form* over a commutative ring R is simply a homogeneous polynomial of degree 2 in n variables. We start by recalling some facts about quadratic forms over fields of characteristic other than two: Any quadratic form φ can be written as $\varphi(\mathbf{x}) = \mathbf{x}^{\mathrm{T}} M_\varphi \mathbf{x}$, where M_φ is a symmetric matrix. The associated symmetric bilinear form $B_\varphi(\mathbf{x}, \mathbf{y}) = \mathbf{x}^{\mathrm{T}} M_\varphi \mathbf{y}$ can also be expressed as $B_\varphi(\mathbf{x}, \mathbf{y}) = \frac{1}{2}(\varphi(\mathbf{x}+\mathbf{y}) - \varphi(\mathbf{x}) - \varphi(\mathbf{y}))$. On the other hand, for any symmetric bilinear form B, the map $\mathbf{x} \mapsto B(\mathbf{x}, \mathbf{x})$ is a quadratic form – thus, there is a bijective correspondence between quadratic forms and symmetric bilinear forms.

Two quadratic forms φ, ψ are *equivalent* if one can be obtained from the other by an invertible change of variables – equivalently, we have $M_\psi = A^{\mathrm{T}} M_\varphi A$ where A is an invertible matrix. This is indeed an equivalence relation, and one of the main advantages of working over a field is that every quadratic form is equivalent to a *diagonal* quadratic form, i.e. a form of the shape $a_1 x_1^2 + a_2 x_2^2 + \cdots + a_n x_n^2$. Such a form is often denoted as $\langle a_1, a_2, \ldots, a_n \rangle$.

For quadratic forms over rings which are not fields – even over $\mathbb{Z}$ – many complications occur immediately. Consider a Dedekind domain R with fraction field F, again excluding characteristic two (in particular, R can be the ring of integers $\mathcal{O}_F$ of a number field F). Even the meaning of 'integral quadratic form over F' varies in the literature. In the following, we consider a quadratic form φ over F *integral* if the corresponding polynomial has coefficients in R; equivalently, φ only takes values from R. However, the entries of M_φ can then have non-integral values from $\frac{1}{2}R$. We call a quadratic form *classical* (or *classically integral*) over F when this is not the case: All the mixed terms in the polynomial are divisible by 2, which is equivalent to $M_\varphi \in R^{n \times n}$. Some authors focus only on classically integral forms since these correspond to integral symmetric bilinear forms. In this thesis, the first chapter studies only classical forms, while the remaining chapters focus almost exclusively on sums of squares and forms represented by them, and these are necessarily classical; thus, non-classical forms occur only in very few places.

0.3 The situation in number fields

A number field F is a field extension of $\mathbb{Q}$ with a finite degree $d = [F : \mathbb{Q}]$. Its ring of integers $\mathcal{O}_F$ consists of elements of F which are integral over $\mathbb{Z}$; typically, the elements of $\mathcal{O}_F$ have no unique factorisation, but ideals can always be uniquely decomposed into prime ideals – $\mathcal{O}_F$ is a Dedekind domain. A subring of $\mathcal{O}_F$ which has the whole F as the fraction field is called an *order*; $\mathcal{O}_F$ is the maximal order with respect to inclusion. A non-maximal order is never a

Dedekind domain; thus, the theory of quadratic forms over such orders is more difficult and we do not include it in this preliminary section.

There are d embeddings of F into $\mathbb{C}$, denoted $\sigma_1, \dots, \sigma_d$. A field F is *totally real* if $\sigma_i(F) \subset \mathbb{R}$ for every i (all embeddings are *real*). An element $\alpha \in F$ is called *totally positive* if $\sigma_i(\alpha) > 0$ in every real embedding σ_i; this is denoted $\alpha \succ 0$. A matrix or quadratic form over a totally real field is *totally positive definite* if it is positive definite in all embeddings. We will soon see that many questions are quite well-understood except in the case of totally positive definite forms over totally real fields.

The basic question about a quadratic form φ over any ring is: Which elements are represented by φ? (We say that α is *represented* by φ if $\alpha = \varphi(\mathbf{x})$ for a suitable vector $\mathbf{x}$.) Over a number field F or its ring of integers $\mathcal{O}_F$, such a question is a particular type of Diophantine equation, and thus a complex and interesting problem. However, the case of fields has been fully solved by the following deep theorem:

Theorem (Hasse–Minkowski)**.** *Let φ be a quadratic form over a number field F and $\alpha \in F$. Then, the following are equivalent:*

1. *φ represents α over F.*
2. *For every place v on F, φ represents α over the completion F_v.*

For any number field, every place is either *infinite*, which means that it corresponds to a real or complex embedding, or *finite*, which corresponds to a prime ideal $\mathfrak{p}$. The corresponding completions $\mathbb{R}, \mathbb{C}$ and all the $F_\mathfrak{p}$ are examples of *local fields* and the theory of quadratic forms over them is very well understood, so even though 2. is a collection of infinitely many conditions, it is routine to check it in any particular example and thus to fully determine the set of all elements represented by a given form over a fixed number field.

Because number fields are examples of *global fields*, the condition 1. is often read as "φ represents α globally", while 2. can be rephrased as "φ represents α everywhere locally". Hasse–Minkowski theorem is also called the *local–global principle*.

In contrast, quadratic forms over $\mathcal{O}_F$ do not always satisfy an analogous principle. It is clearly true that an integral representation over the number field implies an integral representation over any completion, but the other implication fails in general. We say that a quadratic form φ over $\mathcal{O}_F$ *satisfies the integral local–global principle* if this equivalence holds: Namely, α is represented by φ over $\mathcal{O}_F$ if and only if it is represented in all real and complex places and integrally represented in all other completions.

If we knew that a quadratic form satisfies the integral local–global principle, the question of representation would become trivial. However, there is no clear way how to recognize such well-behaved forms. Only partial results exist: First of all, from the theory of spinor genera it follows that an integral form in at least four variables satisfies the local–global principle unless it is totally positive (or negative) semidefinite over a totally real field. Therefore, there are still deep open questions about indefinite ternary forms over $\mathbb{Z}$, but otherwise the most challenging part of the theory are integral totally positive definite forms over totally real fields (including $\mathbb{Q}$). There, a fundamental theorem of Hsia, Kitaoka and Kneser [HKK] shows that for every quadratic form over $\mathcal{O}_F$ in at least five variables, the local–global principle holds for all sufficiently large elements – but the bound is so huge that it is unfeasible to check all elements below it.

It is known that if φ represents α locally everywhere, then α is represented by some form which is equivalent to φ locally everywhere – such a form belongs to the *genus* of φ, but is not necessarily in the same equivalence class as φ. The number of equivalence classes in the genus is called the *class number* and denoted $h(\varphi)$. Clearly, $h(\varphi) = 1$ implies the integral local–global principle; however, this condition is rarely satisfied. A curious historical fact is that the important notion of the class number of a number field was first discovered under the guise of a class number of a certain binary quadratic form over $\mathbb{Z}$.

0.4 Universal quadratic forms over number fields

A totally positive definite integral quadratic form over a totally real number field F is called *(integrally) universal* if it represents all totally positive elements of $\mathcal{O}_F$. In the following, we assume all fields to be totally real and all forms to be totally positive definite, and often omit the adjective 'integral'. An archetypal example of a universal form is $x^2+y^2+z^2+w^2$ over $\mathbb{Q}$, as it represents all positive integers by Lagrange's four-square theorem. Ramanujan studied diagonal (i.e. without cross-terms) universal quadratic forms over $\mathbb{Q}$ in four variables and provided a complete list [Ram]. By an understandable mistake, he included the form $x^2+2y^2+5z^2+5w^2$ which represents all natural numbers except of 15. Universal quadratic forms over $\mathbb{Z}$ were much studied during the 20th century, culminating with the 15-theorem of Conway and Schneeberger and the 290-theorem of Bhargava and Hanke [BH]. The former claims that a classical quadratic form over $\mathbb{Q}$ is universal if and only if it represents all numbers up to 15 (and Ramanujan's mistake shows that this bound is optimal), the latter establishes a similar criterion for all integral quadratic forms over $\mathbb{Q}$. With the 290-theorem, universal quadratic forms over $\mathbb{Q}$ are very well understood.

The situation over number fields is much different, even for real quadratic fields. It is known that no quadratic form in three variables can be universal over $\mathbb{Q}$ and more generally over a field of odd degree, while Maaß [Ma] proved the universality of the sum of three squares over $\mathbb{Q}(\sqrt{5})$. Shortly afterwards, Siegel [Si] published the surprising result that the sum of any number of squares cannot be universal over any totally real field but $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{5})$. From the asymptotic local–global principle from [HKK] it follows that every totally real number field admits a universal quadratic form – but it can require a huge number of variables. Blomer and Kala showed that for every m there are infinitely many real quadratic fields such that no m-ary quadratic form is universal [BK]. Now, the same result is available in any fixed degree divisible by 2 or 3 [Ka3]. Another recent result due to Kim, Kim and Park [KKP] shows that only finitely many quadratic fields admit a universal quadratic form in 7 variables (while Kim [Ki2] showed previously that every $\mathbb{Q}(\sqrt{n^2-1})$ for square-free n^2-1 admits a universal quadratic form in 8 variables).

Their result was a significant improvement upon a nice result by Chan, Kim and Raghavan [CKR] which determines all classically integral universal quadratic forms in three variables over real quadratic fields – there is only finitely many of them and they exist only over $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{5})$. No other universal ternary quadratic form over a field of any degree is known, and an influential conjecture by Kitaoka predicts that there are only finitely many number fields admitting such a form. As mentioned, this is known for fields of odd degree, but otherwise, little is known. Very recently, a weak version of Kitaoka's conjecture was proved in [KY3].

In the first chapter (which contains the paper [KTZ]), we prove the following:

Theorem. *Let F be a totally real biquadratic field. Then F admits no classically integral universal quadratic form in three variables.*

Multiquadratic fields $\mathbb{Q}(\sqrt{n_1},\dots,\sqrt{n_k})$ where the n_i are pairwise coprime are often used as a convenient tool for exhibiting counterexamples – for example, another result about non-universality of quadratic forms in a small number of variables [KS] works precisely with such fields. Our theorem, however, works for all biquadratic fields $\mathbb{Q}(\sqrt{n_1},\sqrt{n_2})$, even those where n_1 and n_2 are far from coprime. Developing tools for handling such fields was one of the challenges in our work. The main inspiration for the chapter was provided by [CKR], but we needed to develop other tools as well. One of them is explained in the next three paragraphs.

A totally positive element of $\mathcal{O}_F$ is *(additively) indecomposable* if it cannot be written as a sum of two totally positive elements. Indecomposables are an important part of the arithmetic of a totally real number field; their importance for the theory of universal quadratic forms is most easily illustrated on the case of diagonal forms: If α is indecomposable and represented by the totally positive definite form $ax^2+by^2+cz^2$, then it must be represented by one of the

terms ax^2, by^2, cz^2, which gives strong conditions on one of the coefficients a, b, c. Thus, if in a field F one knows enough indecomposables which are independent in a certain sense, one can show that no ternary form is universal. (Similar ideas lie e.g. behind the cited results from [BK] or [KS].)

Indecomposable elements in real quadratic fields were already studied by Perron, used by Siegel [Si] and later fully described by Dress and Scharlau [DS] in terms of continued fractions, but for fields of higher degree, they remain mysterious. In a recent work [KT], Kala and Tinková fully described them for the family of *simplest cubic fields*, which also led to a very good understanding of how many variables are needed for a universal form over such fields. For biquadratic fields, some partial results were known from [Č+], but they were not sufficient for our purposes, as we needed explicit results valid for every biquadratic field. We succeeded (see Theorem 1.1.3), which not only enabled us to prove non-universality of ternary forms in biquadratic fields, but also contributed to a general understanding of the arithmetic of real biquadratic fields.

In an ongoing and as yet unpublished work, Siu Hang Man builds upon our results about the indecomposables in biquadratic fields. He solves the open question posed at the very end of Section 1.6: For every biquadratic field, there are indeed two quadratic subfields such the indecomposables from those subfields remain indecomposable in the biquadratic field; but there is an explicit example where these subfields are not $\mathbb{Q}(\sqrt{m})$ and $\mathbb{Q}(\sqrt{s})$ in the notation of the first chapter. Man's results then imply that most biquadratic fields possess many indecomposables, which again has direct implications for the rank of any universal quadratic form over them.

Beside results on biquadratic fields, the first chapter contains Theorem 1.1.2, which is a general result about Kitaoka's conjecture, and also a correction for [CKR], see Appendix 1.7.

0.5 Sums of squares and Pythagoras number in totally real fields

We already mentioned that, while the sum of three integral squares is universal over $\mathbb{Q}(\sqrt{5})$, and notoriously, four squares are universal over $\mathbb{Q}$, every other totally real number field contains an integral totally positive element which cannot be written as a sum of any number of integral squares. This naturally leads to the following definitions: Denote by $\sum R^2$ the set of all elements representable as a sum of squares in a ring R. For $\alpha \in \sum R^2$, denote by $\ell(\alpha)$ the minimal number of squares needed to represent α (so-called *length*); for example, $\ell(7) = 4$ in $\mathbb{Z}$. Now, the *Pythagoras number* of R is defined as follows:

$$\mathcal{P}(R) = \sup_{\alpha \in \sum R^2} \ell(\alpha).$$

In other words, it is the smallest number n with the property that any sum of squares in R can be rewritten as a sum of at most n squares. Pythagoras numbers are much studied for general fields (while for number fields they are easy to determine by the Hasse–Minkowski theorem). For a not-totally-real field, the above-mentioned version of integral local–global theorem yields $\mathcal{P}(\mathcal{O}_K) \leq 4$, and $\mathcal{P}(\mathcal{O}) \leq 5$ can also be deduced [Pe3]. For totally real orders, the situation is entirely different. The main result of [HKK] implies that $\mathcal{P}(\mathcal{O}_K)$ is finite for every K, but Scharlau [Sch2] has shown that it can be arbitrarily large. He conjectured that $\mathcal{P}(\mathcal{O})$ can be bounded by some function depending only on the degree of the number field, and this was confirmed in by Kala and Yatsyna [KY2] – the upper bound is provided by the so-called g-invariant of $\mathbb{Z}$, discussed in Section 0.6. In particular, $\mathcal{P}(\mathcal{O}) \leq 5$ for quadratic fields, ≤ 6 for cubic fields, ≤ 7 for quartic fields.

These results are in sharp contrast with the fact that $\mathcal{P}(K) \leq 4$ for every number field including the totally real ones. The study of Pythagoras numbers of orders in totally real fields

is difficult for the same reason as the study of universal quadratic forms: The integral local–global principle does not hold in general. For every number field, the asymptotic local–global principle from [HKK] at least ensures that there are (in a sense) only finitely many sums of integral squares which cannot be rewritten as sums of five squares, but the available results on Pythagoras numbers, including those from this thesis, suggest that this is rarely true for all sums of squares.

For quadratic orders, Kala and Yatsyna's bound was known much earlier – Peters [Pe2] proved $\mathcal{P}(\mathcal{O}) = 5$ for all but seven real quadratic orders, using results of Mordell [Mo, Mo2]; the remaining cases were treated in several papers by different authors, e.g. [Ma, Dz, CP]. We collected these scattered results in Theorem 2.3.1.

Using the upper bound by Kala and Yatsyna, Tinková [Ti] showed that in the family of *simplest cubic fields*, the Pythagoras number of a certain monogenic order (often identical with the full ring of integers) is equal to 6 with three possible exceptions. In the third chapter, we complemented her result by showing $\mathcal{P}(\,\cdot\,) = 4$ in one of these three cases. Before discussing this in Subsection 0.5.3 of this introduction, we describe the second chapter, which examines the situation in biquadratic fields.

0.5.1 Pythagoras number of orders in real biquadratic fields

The second chapter, based on a paper [KRS] with co-authors Raška and Sgallová, treats Pythagoras numbers in totally real biquadratic fields. We did not obtain complete results (partly because we again wanted to examine all fields, not just those generated by roots of coprime integers), but our results significantly improved the understanding of the behaviour of Pythagoras numbers in totally real number fields and became inspiration for further work.

First of all, we showed that the upper bound given in [KY2] is attained in a large and natural family of maximal orders:

Theorem. *There exist infinitely many totally real biquadratic fields K with $\mathcal{P}(\mathcal{O}_K) = 7$.*

For this, it suffices to pick two coprime square-free numbers $p \equiv 2$, $q \equiv 3 \pmod 4$ greater than 7, and consider $K = \mathbb{Q}(\sqrt{p}, \sqrt{q})$. In general, for most of the coprime cases we showed $\mathcal{P}(\mathcal{O}_K) \geq 6$. Without the assumption of coprimality, we obtained the following:

Theorem. *Let K be a totally real biquadratic field. Then:*

1. *$\mathcal{P}(\mathcal{O}_K) \geq 5$ for all but at most seven cases.*
2. *Fix a square-free positive $n > 7$. Then $\mathcal{P}(\mathcal{O}_K) \geq 6$ for all but finitely many totally real biquadratic fields $K \ni \sqrt{n}$.*

The seven fields probably satisfying $\mathcal{P}(\mathcal{O}_K) < 5$ are listed in the Conjecture below.

In contrast with the previous results, which provide lower bounds for $\mathcal{P}(\mathcal{O}_K)$, we also improved the upper bound in a family of fields. This was achieved by generalising inequality from [KY2] and exploiting a theorem of Sasaki [Sa2] about the $g(2)$-invariant of the ring $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$. (These ideas are vastly generalised in the fourth chapter.)

Theorem. *Let K be a quadratic extension of $\mathbb{Q}(\sqrt{5})$ and $\mathcal{O}$ any order in K containing $\frac{1+\sqrt{5}}{2}$. Then $\mathcal{P}(\mathcal{O}) \leq 5$.*

In particular, this combines with the first part of the previous theorem as follows: If K is a biquadratic field containing $\sqrt{5}$ but not $\sqrt{2}, \sqrt{3}, \sqrt{6}$ and $\sqrt{7}$, then $\mathcal{P}(\mathcal{O}_K) = 5$. On the other hand, note that the following general result includes fields which contain $\sqrt{5}$.

Theorem. *Let K be a given totally real biquadratic field. There are infinitely many orders $\mathcal{O} \subset K$ satisfying $\mathcal{P}(\mathcal{O}) = 7$.*

More generally, any totally real biquadratic order $\mathcal{O}_0$ contains an order $\mathcal{O} \subsetneq \mathcal{O}_0$ with $\mathcal{P}(\mathcal{O}) = 7$.

This theorem was announced but left unproven in [KRS] in order to decrease the length of the manuscript; we keep the same in the second chapter. The proof and related ideas will serve as a basis of the forthcoming paper [Kr2], a preliminary version of which is presented as the fifth chapter. We discuss it briefly in the introductory Subsection 0.5.2.

We also conducted some numerical experiments, systematically searching for elements of big length in $\mathcal{O}_K$ for many biquadratic fields K. Together with the knowledge of all the listed results, this led to the following unifying conjecture:

Conjecture. Let K be a totally real biquadratic field.

1. If K contains none of $\sqrt{2}$ and $\sqrt{5}$, then $\mathcal{P}(\mathcal{O}_K) \geq 6$ holds with finitely many exceptions.
2. If K contains $\sqrt{2}$ or $\sqrt{5}$, then $\mathcal{P}(\mathcal{O}_K) \leq 5$.
3. The inequality $\mathcal{P}(\mathcal{O}_K) < 5$ holds precisely for the following seven fields:
   For $K = \mathbb{Q}(\sqrt{2},\sqrt{3}), \mathbb{Q}(\sqrt{2},\sqrt{5}), \mathbb{Q}(\sqrt{3},\sqrt{5})$, where $\mathcal{P}(\mathcal{O}_K) = 3$, and
   $K = \mathbb{Q}(\sqrt{2},\sqrt{7}), \mathbb{Q}(\sqrt{3},\sqrt{7}), \mathbb{Q}(\sqrt{5},\sqrt{6}), \mathbb{Q}(\sqrt{5},\sqrt{7})$, where $\mathcal{P}(\mathcal{O}_K) = 4$.

Note that many parts of the conjecture were known to us already when we made it – for example, 2. was proved by us for $\sqrt{5}$. In a recent preprint [HH], He and Hu completed the proof of 2. by following the strategy we suggested and proving $g(2) = 5$ for the ring $\mathbb{Z}[\sqrt{2}]$; see also Section 0.6. (In collaboration with Dayoon Park, we achieved the same result independently, but did not publish it after seeing He and Hu's work.) From 3., the only open part is proving the optimal upper bounds for the seven fields. However, this might be a very hard problem: there is no clear strategy how to approach such a task. Nevertheless, recently, in an as yet unpublished work with Rudolf Scharlau, we found a proof for the field $\mathbb{Q}(\sqrt{2},\sqrt{5})$, see Subsection 0.5.4, confirming yet another part of the conjecture. However, the proof is specific and will certainly not work over the remaining six fields.

0.5.2 Pythagoras number of non-maximal orders in biquadratic fields

A strong result which shows that every real biquadratic field contains infinitely many non-maximal orders $\mathcal{O}$ with $\mathcal{P}(\mathcal{O}) = 7$ was announced but not proved in the second chapter. We prove it in the last chapter, together with a thorough examination of a certain rich family of non-maximal biquadratic orders, which we call *basic orders*. These are precisely those quartic orders which possess an integral basis of the form 1, $\sqrt{M}$, $\sqrt{S}$, $\sqrt{T}$ for $M < S < T \in \mathbb{N}$; however, as not every $\mathbb{Z}$-module generated by such elements is closed under multiplication, there are some questions to be solved even before we start examining the Pythagoras numbers. Surprisingly, it turns out that we can usually prove $\mathcal{P}(\mathcal{O}) = 7$ for such an order unless $T = MS$; this is in sharp contrast with the situation for maximal orders where our only general proof of $\mathcal{P}(\mathcal{O}_K) = 7$ is based on the assumption that $t = ms$, see Theorem 2.5.3.

We also prove that for basic orders, one can show more than that – not only does a typical basic order contain an element of length 7; orders which contain less than a given number of these elements are actually fairly rare, see Theorem 5.3.7.

0.5.3 A cubic ring of integers with the minimal Pythagoras number

Since most results about Pythagoras numbers of orders in totally real number fields went into the direction of showing that the upper bounds known from [KY2] are usually optimal, it is important to explore the other direction and find examples of fields F where $\mathcal{P}(\mathcal{O}_F)$ is as small as possible. Since 7 is not a sum of three squares $\mathbb{Q}$, the well-known Springer's theorem yields that it is not a sum of three squares in any field of odd degree. Thus $\mathcal{P}(F) \geq 4$ for every such field (and combined with the local–global principle one gets $\mathcal{P}(F) = 4$); but restricting to integral squares, we obtain $\ell(7) = 4$ in every order $\mathcal{O}$ of odd degree, implying $\mathcal{P}(\mathcal{O}) \geq 4$. The

third chapter, identical with the paper [Kr], presents the first known example of a real number field of odd degree with $\mathcal{P}(\mathcal{O}_F) = 4$.

Denote $\rho = \zeta_7 + \zeta_7^{-1}$ where ζ_7 is a primitive seventh root of unity. Consider the cubic field $K = \mathbb{Q}(\rho)$, the totally real subfield of the 7th cyclotomic field. The third chapter proves:

Theorem. *We have* $\mathcal{P}(\mathcal{O}_K) = 4$.

Furthermore, we also get a simple description of the set $\sum \mathcal{O}_K^2$: It consist of all totally positive elements α except of those with norm 7. The mysterious condition about norm may be rephrased as $\alpha \neq u^2(1 + \rho + \rho^2)$ for all units $u \in \mathcal{O}_K$. These exceptional elements are precisely the non-square indecomposables in $\mathcal{O}_K$, as proved in [KT].

These two facts can also be exploited for a construction of a universal quadratic form:

Corollary. *The totally positive definite quadratic form* $x_1^2 + x_2^2 + x_3^2 + x_4^2 + (1 + \rho + \rho^2)x_5^2$ *is universal over* $\mathcal{O}_K$.

Note that the integral local–global principle for the sum of four squares I_4 is violated in K, as every totally positive integral element is a locally a sum of four integral squares, but globally, $1 + \rho + \rho^2$ is not a sum of squares at all. However, it turns out that K is one of the rare fields where $h(I_3) = 1$; thus, the sum of three squares satisfies the integral local–global principle. This is the crucial first step in our proof of $\mathcal{P}(\mathcal{O}_K) = 4$.

The fact that $h(I_3) = 1$ for $K = \mathbb{Q}(\rho)$ was actually the reason main reason why we decided to study this field; a further inspiration was Tinková's result about the Pythagoras number of almost all simplest cubic fields, where this specific field had to be excluded.

0.5.4 Local–global principle by lattice covering

It can be shown that the following three conditions are equivalent in any number field order $\mathcal{O}$: 1) α is a sum of squares at all places. 2) α is a sum of four squares at all places. 3) α is totally nonnegative and it is a square modulo $2\mathcal{O}$. However, the fact that a number is a sum of integral squares locally everywhere does not ensure that it is indeed a sum of integral squares. An element is called *exceptional* if it is a sum of integral squares everywhere locally, but not globally. Siegel's result about non-universality of sums of squares except in $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{5})$ can be reinterpreted as the claim that every totally real order of odd discriminant except of $\mathbb{Z}$ and $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ contains at least one exceptional element. In the previous subsection, we actually showed that up to multiplication by squares of units, there is only one exceptional element in $\mathbb{Z}[\rho]$ where $\rho = \zeta_7 + \zeta_7^{-1}$, namely $1 + \rho + \rho^2$. Scharlau studied exceptional elements intensely in his thesis [Sch], and his main results is as follows:

Theorem (Scharlau)**.** *Let* $\mathcal{O}$ *be an order in a totally real number field of degree up to* 4*. Then* $\mathcal{O}$ *is without exceptional elements if and only if it is the maximal order in one of the following fields:* $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{2}, \sqrt{5})$ *and* $\mathbb{Q}\left(\sqrt{\frac{5+\sqrt{5}}{2}}\right)$.

For $\mathbb{Q}$ and the three quadratic fields, the Pythagoras number is known – but for both quartic fields, this question remained unsolved. By the inequalities from [KY2], it was at most 7; and as both the fields contain $\sqrt{5}$, our new results from the second chapter improve this upper bound to 5. However, for the biquadratic field $K = \mathbb{Q}(\sqrt{2}, \sqrt{5})$, it is easy to check that locally, three squares always suffice, and indeed, the unifying conjecture from the second chapter predicts $\mathcal{P}(\mathcal{O}_K) = 3$. However, since $h(I_3) = 2$, it is not clear how to prove this.

With Scharlau, we decided to work on this problem and to use the covering of a quadratic lattice by copies of another lattice. (As $h(K) = 1$, there is no difference between quadratic forms and quadratic lattices over K, and we are not going to go into details about lattices.) Namely, we know that every element which is locally represented by the three squares is globally represented by one of the two representatives of the genus of I_3 – i.e. if it is not represented by

I_3, then it is represented by one certain other quadratic lattice L which we explicitly computed. Afterwards, we found in the quadratic space $K \otimes L$ over K five different lattices isometric to I_3 in such a way that the lattice L was fully covered by them – every vector from L also lied in a copy of I_3. This shows that every element which is represented by L is also represented by I_3, hence every element represented locally by I_3 is also represented globally. Thus, we can announce the following result:

Theorem (K., Scharlau). *Let* $K = \mathbb{Q}(\sqrt{2}, \sqrt{5})$. *Then* $\mathcal{P}(\mathcal{O}_K) = 3$.

In this way, we provided the first example of a totally real order with $\mathcal{P}(\mathcal{O}) = 3$ other than $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{3}]$ and $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ and confirmed another part of the conjecture from the second chapter. This is an ongoing project – the proof is fully complete, but we intend to try the same technique for the remaining field without exceptional elements, namely $\mathbb{Q}\left(\sqrt{\frac{5+\sqrt{5}}{2}}\right)$.

Thus, this work is not contained in this thesis; but as it directly answers some questions raised in the second chapter, we felt it should not be entirely omitted.

0.5.5 The connection between universal quadratic forms and Pythagoras numbers

The studies of universal quadratic forms and of Pythagoras numbers are strongly related. Many of the occuring problems have similar flavour – for example, if one stays at the field level, then both questions become trivial, as $\mathcal{P}(K) \leq 4$ and there is a universal form in four variables which represents (not integrally) every totally positive element of K; in fact, the sum of four squares can be chosen as this form. The main difficulty in the work over $\mathcal{O}_K$ is the absence of an integral local–global principle; and, although evidence suggests that typically, a universal quadratic form needs many variables and the Pythagoras number is also typically close the the known upper bounds, it is true that if one allows finitely many exceptions, then five variables suffice: Almost every element is a sum of at most five squares, and there is always an 'almost-universal' quadratic form in five variables which represents all but finitely many elements (up to multiplication by squares). Both these facts are simple corollaries of [HKK].

However, there is an even stronger connection between the two topics: The knowledge of the Pythagoras number provides an explicit construction of a universal quadratic form. Remember that in the third chapter, we used the knowledge of the Pythagoras number in $\mathbb{Z}[\rho]$ together with the exact understanding of the set of sums of squares to show universality of a certain diagonal form in five variables. Generally, exploiting the fact that up to multiplication by squares of units there are only finitely many indecomposables, there is the following construction (see [KT, Prop. 7.1]):

Let K be a totally real number field with $\mathcal{P} = \mathcal{P}(\mathcal{O}_K)$ and let A be a finite set of indecomposable elements such that every indecomposable element $\alpha \in \mathcal{O}_K$ lies in $(\mathcal{O}_K^\times)^2 A$. Then the quadratic form $\sum_{\alpha \in A} \alpha(x_1^2 + \cdots + x_{\mathcal{P}}^2)$ is universal.

As a very special case, this construction includes the universality of I_3 over $\mathbb{Q}(\sqrt{5})$ and of I_4 over $\mathbb{Q}$, as 1 is essentially the only indecomposable element in these two fields. Importantly, the same construction also lies behind the successful construction of an octonary universal quadratic form in the quadratic fields $\mathbb{Q}(\sqrt{n^2-1})$, see [Ki2], and partly also behind the very good estimates of the minimal rank of a universal quadratic form over a simplest cubic field [KT]. Another general construction of universal quadratic forms, introduced in [KY3, Thm. 6], also uses Pythagoras numbers.

0.6 Quadratic Waring's problem

Arguably the strongest result of this thesis is contained in the fourth chapter, which presents a joint paper [KrY] with Yatsyna. Inspired by Proposition 2.7.5 which slightly generalises the

upper bound on the Pythagoras number from [KY2], we made a much wider generalisation – and despite the simplicity of the idea, it turned out to be strong enough to significantly improve upon the best available results for the so-called quadratic Waring's problem in totally real number fields.

If φ is a positive definite quadratic form over $\mathbb{Z}$ in n variables, one can try to express it as a sum of squares of linear forms in k variables. If such an expression exists, we consider the minimal possible number of squares used in such a representation and denote it $\ell(\varphi)$, in accordance with the notation for the length of a number which is a sum of squares. Then, in complete analogy to the Pythagoras number, we put

$$g_{\mathbb{Z}}(k) = \sup \ell(\varphi),$$

where the supremum runs only over those forms φ in k variables which are sums of integral squares. The study of this g-invariant is an intriguing problem, suggested by Mordell [Mo, Mo2] and called the *quadratic Waring's problem*. The values of $g_{\mathbb{Z}}(k)$ for $1 \leq k \leq 5$ are $k+3$ and follow directly from the fact that $h(I_{k+3}) = 1$ in these cases. However, this breaks down for $k = 6$, and only much later, Kim and Oh [KO] showed that $g_{\mathbb{Z}}(k) = 10$. For other values of k, much effort went into obtaining upper and lower bounds [KO2, Sa, Ic2, KO3], but no precise value is known. The best currently known bound valid for all k is $g_{\mathbb{Z}}(k) = O(\mathrm{e}^{(4+2\sqrt{2}+\varepsilon)\sqrt{k}})$ due to Beli, Chan, Icaza and Liu [BCIL].

Further motivation for the study of $g_{\mathbb{Z}}$ stems from the fact that it serves as an upper bound for the Pythagoras number of orders in any number field. Namely, for every order of degree d we have $\mathcal{P}(\mathcal{O}) \leq g_{\mathbb{Z}}(d)$ due to [KY2]; this bound was already mentioned several times and heavily exploited in the second chapter. One can define the invariant g_R for any ring, and an easy generalisation of the previous inequality, contained already in the second chapter, reads as follows:

Proposition. *Let $K \supset F$ be number fields, $[K : F] = d$, and $\mathcal{O} \subset K$ an order which is a free module over $\mathcal{O}_F$. Then $\mathcal{P}(\mathcal{O}) \leq g_{\mathcal{O}_F}(d)$.*

This was the key to obtaining the improved upper bounds for $\mathcal{P}(\mathcal{O})$ when $\mathcal{O}$ is a quartic order containing $\sqrt{2}$ or $\frac{1+\sqrt{5}}{2}$, since Sasaki [Sa2] and He and Hu [HH] proved $g(2) = 5$ for the ring of integers in the two quadratic fields generated by $\sqrt{5}$ and $\sqrt{2}$.

The fourth chapter contains the following broad generalisation:

Theorem. *Let $K \supset F$ be number fields, $[K : F] = d$, and $\mathcal{O}$ any order in K containing $\mathcal{O}_F$.*

1. *If $\mathcal{O}$ is a free $\mathcal{O}_F$-module, then $g_{\mathcal{O}}(k) \leq g_{\mathcal{O}_F}(kd)$. In general, $g_{\mathcal{O}}(k) \leq g_{\mathcal{O}_F}(kd+1)$.*
2. *$G_{\mathcal{O}_K}(k) \leq G_{\mathcal{O}_F}(kd)$. In particular, $\mathcal{P}(\mathcal{O}_K) \leq G_{\mathcal{O}_K}(1) \leq G_{\mathcal{O}_F}(d)$.*

Here, the G-invariant is a version of the g-invariant defined using quadratic lattices, which are more general than quadratic forms and shall be defined in Subsection 4.2.4. It turns out to be the more natural setting to work in, as can be seen from the fact that the strong condition of $\mathcal{O}$ being a free module could be omitted. Even the general statement $g_{\mathcal{O}}(k) \leq g_{\mathcal{O}_F}(kd+1)$ was actually proven using the G-invariant in an intermediate step.

Beside being interesting on its own and also providing the first proof that $g_{\mathcal{O}}(k)$ is finite for every order $\mathcal{O}$ and $k \in \mathbb{N}$, this theorem proved to be powerful enough to surpass the best available result about the quadratic Waring's problem in totally real number fields, namely [CI]: $g_{\mathcal{O}_K}(k) \leq D\mathrm{e}^{\kappa\sqrt{k}}$ for totally real number fields K of class number 1, where constants κ and D depend only on K. As a corollary of the above inequalities, we get rid of the condition on the class number while also showing that the constants only depend on the degree, not on the number field itself:

Theorem. *For every $\varepsilon > 0$, there exists a constant D_ε such that*

$$g_{\mathcal{O}}(k) \leq D_\varepsilon \mathrm{e}^{(4+2\sqrt{2}+\varepsilon)\sqrt{dk}}$$

for every order $\mathcal{O}$ in a number field K of degree d.

We also show that our upper bounds are often optimal, as we exploit them to obtain the following:

Theorem. *Let K be a real quadratic field other than $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{5})$. Then $G_{\mathcal{O}_K}(2) = 7$.*

In combination with the results of [Sa2, HH], $\mathbb{Q}(\sqrt{3})$ is the only real quadratic field where the value of $G(2)$ remains unknown. We conjecture that the correct value is 6, but it is unclear how to prove it; the only available upper bound is 7. This is one of the open questions which we would very much like to solve. However, since the exact value of $g_{\mathbb{Z}}(6)$ was determined in [KO] more than sixty years after Mordell and Ko iniciated the study of these invariants, it might be very hard.

We also showed $\mathcal{P}(\mathcal{O}_K) = G_{\mathcal{O}_K}(1)$ for all real quadratic fields, proving that at least for sums of squares in real quadratic fields, there is no big difference between unary quadratic forms and unary quadratic lattices. The question whether $g_{\mathcal{O}_K}(k) = G_{\mathcal{O}_K}(k)$ holds in general remains widely open, and among those whom we asked, there is not even the intuition as to the probable answer.

This is another direction worth pursuing in the future, as there are other questions of similar flavour, comparing invariants defined in terms of quadratic forms to their analogues involving quadratic lattices. For example: Is there a number field which admits an integral universal quadratic lattice of rank n, but not a universal form in n variables? Here, we expect an affirmative answer, but not with absolute confidence. On the other hand, since some of the best results towards Kitaoka's conjecture [KKP, KY3] actually show non-universality of lattices and not only of quadratic forms, it is probable that Kitaoka's conjecture holds even for ternary quadratic lattices, not just forms.

1. There are no universal ternary quadratic forms over biquadratic fields

This chapter contains the paper [KTZ] J. Krásenský, M. Tinková and K. Zemková, *There are no universal ternary quadratic forms over biquadratic fields*, Proc. Edinburgh Math. Soc. 63(3), 861–912 (2020).

1.1 Introduction

Several generations of number theorists have been interested in quadratic forms. One of the most beautiful topics in this area is the study of universal quadratic forms with integral coefficients. It started with Lagrange's famous theorem, which says that every nonnegative rational integer can be expressed as a sum of four squares; in modern terminology, we talk about the universality of the form $x^2+y^2+z^2+w^2$ over the ring $\mathbb{Z}$. Later, all universal forms over $\mathbb{Z}$ in four variables were characterized by Ramanujan [Ram]. In particular, no ternary (i.e., in three variables) quadratic form with integer coefficients can represent all positive elements of $\mathbb{Z}$.

Considering, instead of $\mathbb{Z}$, the ring of algebraic integers $\mathcal{O}_K$ for a totally real algebraic extension K of $\mathbb{Q}$, many directions of research appear. In [Ma], Maass showed that the sum of three squares is universal over $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$, which was followed by the result of Siegel [Si] saying that the sum of any number of squares is universal only over $\mathbb{Z}$ and $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$. Moreover, Hsia, Kitaoka and Kneser [HKK] proved that in any given number field, there always exists a universal quadratic form. This naturally leads to the question how many variables this form must have.

Blomer and Kala [BK, Ka] have shown that for any given N, there can be always found a quadratic number field in which every universal quadratic form has at least N variables. The same result can be obtained for multiquadratic fields (Kala and Svoboda [KS]) and cubic fields (Yatsyna [Ya]). On the other hand, one can ask, for a given field, what is the least possible number of variables of a universal quadratic form; Čech, Lachman, Svoboda and two present authors [Č+] started to examine this question for biquadratic fields. Kitaoka conjectured that there are only finitely many fields which admit universal ternary quadratic forms. This idea was supported by the result of Chan, Kim and Raghavan [CKR], who proved that $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{5})$ are the only quadratic fields with a universal classical totally positive definite ternary quadratic form. Inspired by this statement, we prove the following theorem.

Theorem 1.1.1. *For a totally real biquadratic field K, there is no universal classical totally positive definite ternary quadratic form over $\mathcal{O}_K$.*

The proof is divided into Sections 1.5 and 1.6. This theorem is, to the extent of our knowledge, the first result about universality of ternary forms in fields of even degree different from two. For all totally real number fields of odd degree, a proof of nonexistence of universal ternary forms can be found in [EK]. In fact, one part of our proof can be applied to prove nonuniversality of ternary forms in a broad class of number fields of arbitrary degree:

Theorem 1.1.2. *Let K be a totally real field, $\sqrt{2} \notin K$, which contains a nonsquare totally positive unit ε such that 2ε is not a square in K. Then there is no universal classical totally positive definite ternary quadratic form over $\mathcal{O}_K$.*

The proof is contained in Subsection 1.5.2. For more results on quadratic forms, see for example [BK2, De, Ki1, Ki2, Ro, Sa4].

In totally real number fields, the question of universality of quadratic forms is closely related to the study of indecomposable integers. These are exactly those elements of $\mathcal{O}_K^+$ (the set of totally positive algebraic integers of K) which cannot be written as a sum of two elements of $\mathcal{O}_K^+$. In a certain sense, it is difficult to represent them by quadratic forms, which is demonstrated in the works of Blomer, Kala or Yatsyna. Despite this fact, there is not much known about them. In quadratic fields, they were characterized by Perron [Per], Dress and Scharlau [DS], and their norms were studied by several authors [JK, Ka2, TV]. Some general statements can be found in the work of Brunotte [Br]. Considering biquadratic fields, we can draw on the results of [Č+], which we extend in this paper. In particular, we prove the following theorem.

Theorem 1.1.3. *Let $1 < m < s < t$ be square-free integers such that $\mathbb{Q}(\sqrt{m}, \sqrt{s})$ is a biquadratic field containing $\sqrt{t}$. For all $u \in \{m, s, t\}$, set*

$$\mathcal{U} = \begin{cases} \lceil\sqrt{u}\rceil + \sqrt{u} & \text{if } u \equiv 2, 3 \pmod 4, \\ \frac{\lceil\sqrt{u}\rceil^{\text{odd}} + \sqrt{u}}{2} & \text{if } u \equiv 1 \pmod 4, \end{cases}$$

where $\lceil\sqrt{u}\rceil^{\text{odd}}$ is the smallest odd integer greater than $\sqrt{u}$. Then

1. *$\mathcal{M}$ and $\mathcal{S}$ are indecomposable in $\mathbb{Q}(\sqrt{m}, \sqrt{s})$,*
2. *$2\mathcal{M} - 1$, if totally positive, is indecomposable in $\mathbb{Q}(\sqrt{m}, \sqrt{s})$,*
3. *$\mathcal{T}$ can decompose in $\mathbb{Q}(\sqrt{m}, \sqrt{s})$.*

We prove the theorem in Subsection 1.4.3. In particular, the statement of part (1) is covered by Propositions 1.4.9 and 1.4.10, and part (2) by Proposition 1.4.11. Part (3) follows from Example 1.4.7; note that this example provides an indecomposable algebraic integer from a quadratic field which decomposes in a biquadratic field, thus solving an open question from [Č+].

The indecomposability of $\mathcal{M}$ stated in Theorem 1.1.3(1) is one of the keystones in the proof of Theorem 1.1.1. Although the statement of Theorem 1.1.3(1) might seem expectable at first glance, the indecomposability of $\mathcal{M}$ and $\mathcal{S}$ in *every* biquadratic field is not immediate, as indicates part (3) of the theorem. The proof is rather technical; one of the difficulties arises from the freedom for possible decompositions, which is much greater than in the quadratic case: Instead of two coefficients and two integral bases, one has to consider four coefficients and five different types of bases. Similar obstacles occur in proofs of most of our lemmas, making them more difficult than their quadratic counterparts. This requires a careful approach and case distinction – it can be treacherous even in the quadratic case, as illustrated with the overlooked exceptional field in the paper [CKR] (see Appendix 1.7 where this omission is handled) – and also several new ideas. Moreover, any condition of the type "$\sqrt{n} \notin K$" (e.g., $\sqrt{2} \notin K$) produces an infinite family of exceptional biquadratic fields instead of just excluding the field $\mathbb{Q}(\sqrt{n})$.

The paper is organized as follows: In Section 1.2 we review some basic facts about biquadratic number fields, quadratic forms and indecomposable integers in totally real number fields. Since the proof of our main results consists of several parts, Section 1.3 provides a brief outline of the proof. In particular, we explain the reason for the subsequent case distinction.

Section 1.4 contains some preparatory statements, mostly about algebraic integers in biquadratic number fields. Above all, we are concerned with indecomposability; we prove Theorem 1.1.3 in Subsection 1.4.3. Furthermore, we show that some elements of $\mathcal{O}_K$ derived from the elements appearing in this theorem are not squares in K, and we also study decompositions of small rational integers in K. At the end of the section, we look more closely at representability of some elements by unary quadratic forms and at splitting of quadratic forms and corresponding lattices.

Section 1.5 provides the main part of our proof – the method introduced here can be applied to most biquadratic fields. The remaining cases are solved in Section 1.6; this time, we use several different methods to deal with arising difficulties, including the knowledge of some indecomposable integers in K and the method of escalation. Some computations used in proofs in Subsections 1.6.8, 1.6.9 and 1.6.10 were performed by programs written in Mathematica.

The paper is concluded by three appendices: Appendix 1.7 recovers the problematic quadratic case of $\mathbb{Q}(\sqrt{10})$ from [CKR]. In Appendix 1.8, we provide some insight into the behavior of totally positive units from a quadratic subfield when considering them as elements of the biquadratic field. Finally, to make the orientation in the different branches of the proof of Theorem 1.1.1 easier, Appendix 1.9 contains a sketch of its tree structure in the main cases.

1.2 Preliminaries

1.2.1 Algebraic integers

Let K be a totally real number field, i.e., a number field where all embeddings σ of K into $\mathbb{C}$ (including the identity) actually map K into $\mathbb{R}$. We say that $\alpha \in K$ is *totally positive*, denoted by $\alpha \succ 0$, if $\sigma(\alpha) > 0$ for each embedding σ. Let $\mathcal{O}_K$ be the ring of algebraic integers in K; the subset of totally positive elements of $\mathcal{O}_K$ will be denoted by $\mathcal{O}_K^+$. Obviously it is closed under addition and multiplication and contains the set of all squares $\mathcal{O}_K^\square$. The notation $\alpha \succcurlyeq 0$ means that α is either totally positive or 0, and we use $\alpha \succ \beta$ (resp. $\alpha \succcurlyeq \beta$) to denote $\alpha - \beta \succ 0$ (resp. $\alpha - \beta \succcurlyeq 0$). We use symbols $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)$ and $\mathcal{N}_{K/\mathbb{Q}}(\alpha)$ to denote the *trace* and the *norm* of α, i.e.,

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \sum_\sigma \sigma(\alpha) \qquad \text{and} \qquad \mathcal{N}_{K/\mathbb{Q}}(\alpha) = \prod_\sigma \sigma(\alpha)$$

where the sum and the product run over all the embeddings σ of K into $\mathbb{C}$. Obviously, if $\alpha, \beta \in \mathcal{O}_K$ satisfy $\alpha \preccurlyeq \beta$, then $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) \le \mathrm{Tr}_{K/\mathbb{Q}}(\beta)$; if, moreover, both of α and β are totally positive, then also $\mathcal{N}_{K/\mathbb{Q}}(\alpha) \le \mathcal{N}_{K/\mathbb{Q}}(\beta)$. Furthermore, norm has the following nice property: If K is of degree N over $\mathbb{Q}$ and $\alpha, \beta \in \mathcal{O}_K^+$, then

$$\sqrt[N]{\mathcal{N}_{K/\mathbb{Q}}(\alpha+\beta)} \ge \sqrt[N]{\mathcal{N}_{K/\mathbb{Q}}(\alpha)} + \sqrt[N]{\mathcal{N}_{K/\mathbb{Q}}(\beta)}; \tag{1.2.1}$$

this is essentially the generalized Hölder's inequality. Equality happens if and only if $\frac{\alpha}{\beta} \in \mathbb{Q}$.

We denote by $\mathcal{U}_K$ the set of units of $\mathcal{O}_K$, i.e., the set of algebraic integers of norm ± 1; furthermore, we write $\mathcal{U}_K^+$ (resp. $\mathcal{U}_K^\square$) for the subset of totally positive units (resp. for the subset of squares of units).

1.2.2 Biquadratic fields

Let $p, q > 1$ be two different square-free integers, put $K = \mathbb{Q}(\sqrt{p}, \sqrt{q})$ and $r = \frac{pq}{\gcd(p,q)^2}$; such a field K is called a (totally real) *biquadratic* field. Throughout the paper, K denotes only such a field. It has degree 4 and one possible $\mathbb{Q}$-vector space basis is $(1, \sqrt{p}, \sqrt{q}, \sqrt{r})$; we can find three quadratic subfields in K, namely $\mathbb{Q}(\sqrt{p})$, $\mathbb{Q}(\sqrt{q})$ and $\mathbb{Q}(\sqrt{r})$. There are four embeddings of K into $\mathbb{C}$: If $\alpha = x + y\sqrt{p} + z\sqrt{q} + w\sqrt{r} \in K$, then

$$\begin{aligned}
\sigma_1(\alpha) &= x + y\sqrt{p} + z\sqrt{q} + w\sqrt{r},\\
\sigma_2(\alpha) &= x - y\sqrt{p} + z\sqrt{q} - w\sqrt{r},\\
\sigma_3(\alpha) &= x + y\sqrt{p} - z\sqrt{q} - w\sqrt{r},\\
\sigma_4(\alpha) &= x - y\sqrt{p} - z\sqrt{q} + w\sqrt{r}.
\end{aligned}$$

Note that biquadratic fields are Galois extensions of $\mathbb{Q}$, i.e., all σ_i's are automorphisms of K.

Depending on $p, q \pmod 4$, after possibly interchanging the role of p, q and r, every case can be converted into one of the five cases listed below. The importance of distinguishing these five types of fields lies in the fact that it determines the *integral basis*, i.e., basis of $\mathcal{O}_K$ regarding it as a $\mathbb{Z}$-module (see [Ja, Section 8] and [Wi, Theorem 2]):

(B1)	$p \equiv 2 \pmod 4,\ q \equiv 3 \pmod 4,$	$\left(1, \sqrt{p}, \sqrt{q}, \frac{\sqrt{p}+\sqrt{r}}{2}\right)$
(B2)	$p \equiv 2 \pmod 4,\ q \equiv 1 \pmod 4,$	$\left(1, \sqrt{p}, \frac{1+\sqrt{q}}{2}, \frac{\sqrt{p}+\sqrt{r}}{2}\right)$
(B3)	$p \equiv 3 \pmod 4,\ q \equiv 1 \pmod 4,$	$\left(1, \sqrt{p}, \frac{1+\sqrt{q}}{2}, \frac{\sqrt{p}+\sqrt{r}}{2}\right)$
(B4)	$p \equiv 1 \pmod 4,\ q \equiv 1 \pmod 4,$ and	
(a)	$\gcd(p,q) \equiv 1 \pmod 4,$ or	$\left(1, \frac{1+\sqrt{p}}{2}, \frac{1+\sqrt{q}}{2}, \frac{1+\sqrt{p}+\sqrt{q}+\sqrt{r}}{4}\right)$
(b)	$\gcd(p,q) \equiv 3 \pmod 4$	$\left(1, \frac{1+\sqrt{p}}{2}, \frac{1+\sqrt{q}}{2}, \frac{1-\sqrt{p}+\sqrt{q}+\sqrt{r}}{4}\right)$

Note that in all these cases, we have $p \equiv r \pmod 4$, so in cases (B1), (B2) and (B3), p and r are interchangeable. In case (B4), all of p, q, r are interchangeable. The field discriminants are (B1) $64pqr$, (B2) $16pqr$, (B3) $16pqr$, (B4) pqr; these are actually just products of the discriminants of the quadratic subfields.

For convenience of the reader, we include a more explicit form of algebraic integers depending on the integral bases.

Remark 1.2.1. An element $\alpha \in K$ belongs to $\mathcal{O}_K$ if and only if there exist $a, b, c, d \in \mathbb{Z}$ such that

(B1) $\alpha = a + \frac{b}{2}\sqrt{p} + c\sqrt{q} + \frac{d}{2}\sqrt{r}$ with $b \equiv d \pmod 2$,

(B2), (B3) $\alpha = \frac{a}{2} + \frac{b}{2}\sqrt{p} + \frac{c}{2}\sqrt{q} + \frac{d}{2}\sqrt{r}$ with $a \equiv c \pmod 2$ and $b \equiv d \pmod 2$,

*(B4*a*)* either $\alpha = \frac{a}{2} + \frac{b}{2}\sqrt{p} + \frac{c}{2}\sqrt{q} + \frac{d}{2}\sqrt{r}$ with $a+b+c+d \equiv 0 \pmod 2$,
or $\alpha = \frac{a}{4} + \frac{b}{4}\sqrt{p} + \frac{c}{4}\sqrt{q} + \frac{d}{4}\sqrt{r}$ with a, b, c, d odd and $a+b+c+d \equiv 0 \pmod 4$.

*(B4*b*)* either $\alpha = \frac{a}{2} + \frac{b}{2}\sqrt{p} + \frac{c}{2}\sqrt{q} + \frac{d}{2}\sqrt{r}$ with $a+b+c+d \equiv 0 \pmod 2$,
or $\alpha = \frac{a}{4} + \frac{b}{4}\sqrt{p} + \frac{c}{4}\sqrt{q} + \frac{d}{4}\sqrt{r}$ with a, b, c, d odd and $a+b+c+d \equiv 2 \pmod 4$.

Convention 1.2.2. *Throughout this article, we use three different triples of letters for the specification of a biquadratic number field, each of them implicitly having a different property. Regardless of the notation, we always assume all the three numbers to be square-free, and any of the three numbers to be equal to the product of the remaining two divided by the second power of their greatest common divisor. Then the biquadratic field is generated by any two of these three elements. We use the following notation:*

- *p, q, r: this triple always satisfies one of the possible congruences above (and hence it is closely connected to the basis),*
- *m, s, t: always $m < s < t$,*
- *n_1, n_2, n_3: this triple does not carry any additional information.*

Moreover, to describe an element of $\mathcal{O}_K$, we usually use either a, b, c, d for integers or x, y, z, w for rational numbers; a generic element of $\mathcal{O}_K$ can be then written, e.g., as $\frac{a}{2} + \frac{b}{2}\sqrt{p} + \frac{c}{2}\sqrt{q} + \frac{d}{2}\sqrt{r}$ or as $x + y\sqrt{n_1} + z\sqrt{n_2} + w\sqrt{n_3}$.

Bearing this notation in mind, we can give the following necessary condition for the totally positive elements of $\mathcal{O}_K$. This lemma was derived in [Č+, Lemma 3.1].

Lemma 1.2.3. *If $x + y\sqrt{n_1} + z\sqrt{n_2} + w\sqrt{n_3} \in \mathcal{O}_K^+$ for some $x, y, z, w \in \mathbb{Q}$, then $x > 0$, $x > |y|\sqrt{n_1}$, $x > |z|\sqrt{n_2}$, $x > |w|\sqrt{n_3}$.*

Note that it implies that, for any fixed K, there are only finitely many totally positive integers with a given trace; this also means that for a fixed $\alpha \in \mathcal{O}_K^+$, the equation $\alpha = \beta + \gamma$ has at most finitely many solutions $\beta, \gamma \in \mathcal{O}_K^+$, and they can straightforwardly be found by a computer program. In particular, it is routine to check whether a given element α of a fixed field K is indecomposable (see Subsection 1.2.4).

In a few proofs, we make use of writing m, s, t as products $m = s_0 t_0$, $s = m_0 t_0$, $t = m_0 s_0$ where m_0, s_0 and t_0 are pairwise coprime square-free numbers, equal to $\gcd(s,t)$, $\gcd(m,t)$ and $\gcd(m,s)$, respectively. Note that the inequality $m < s < t$ translates to $m_0 > s_0 > t_0$, and in basis (B4) we have $m_0 \equiv s_0 \equiv t_0 \pmod 4$.

1.2.3 Quadratic forms

The expression

$$Q(x_1, x_2, \ldots, x_n) = \sum_{1 \le i \le j \le n} a_{ij} x_i x_j,$$

where $a_{ij} \in \mathcal{O}_K$, is called an n-ary quadratic form over $\mathcal{O}_K$. We often think of Q as acting on vectors from the lattice $\mathcal{O}_K^n$ and correspondingly write $Q(\boldsymbol{x})$ instead of $Q(x_1, x_2, \ldots, x_n)$. Given a quadratic form Q, we can construct a symmetric bilinear form $B_Q(\boldsymbol{x}, \boldsymbol{y}) = \frac{1}{2}(Q(\boldsymbol{x} + \boldsymbol{y}) - Q(\boldsymbol{x}) - Q(\boldsymbol{y}))$ such that $Q(\boldsymbol{x}) = B_Q(\boldsymbol{x}, \boldsymbol{x})$; this form is called the *polar form* of Q.

An n-ary quadratic form is said to be *totally positive definite* if $Q(\boldsymbol{x}) \succ 0$ for all nonzero vectors $\boldsymbol{x} \in \mathcal{O}_K^n$. The form Q is *classical* if 2 divides a_{ij} for all $i \neq j$. It is called *diagonal* in the case when $a_{ij} = 0$ for all $i \neq j$; in such a case, we write Q simply as $\langle a_1 \rangle \perp \langle a_2 \rangle \perp \ldots \perp \langle a_n \rangle$. More generally, the expression $Q_1 \perp Q_2$ means the quadratic form $Q_1(x_1, \ldots, x_n) + Q_2(x_{n+1}, \ldots, x_{n+m})$.

We say that Q is *universal* if it *represents* all the elements belonging to $\mathcal{O}_K^+$, i.e., for every $\alpha \in \mathcal{O}_K^+$ we can find a vector $\boldsymbol{e} \in \mathcal{O}_K^n$ such that $Q(\boldsymbol{e}) = \alpha$. Moreover, an n-ary quadratic form Q is *represented* by an m-ary quadratic form R over $\mathcal{O}_K$ if $n \le m$ and there exist n-ary linear forms ℓ_i, $i = 1, \ldots, m$, with coefficients in $\mathcal{O}_K$, such that

$$Q(x_1, \ldots, x_n) = R(\ell_1(x_1, \ldots, x_n), \ldots, \ell_m(x_1, \ldots, x_n)).$$

(E.g., the form $Q(x_1, x_2) = 2x_1^2 + 3x_2^2$ is represented by the form $R(y_1, y_2, y_3) = y_1^2 + 3y_2^2 + 5y_3^2$ over $\mathcal{O}_K$ with $K = \mathbb{Q}(\sqrt{2})$, because $Q(x_1, x_2) = R(\sqrt{2}x_1, x_2, 0)$.) Note that the case $n = 1$ yields the usual representation of an element of $\mathcal{O}_K$. In general, it is easy to see that the form R represents all the integers which are represented by the form Q (and possibly some more). Thus, we also say "R is *stronger* than Q" instead of "Q is represented by R".

From now on, by a *quadratic form*, or just simply a *form*, we mean a totally positive definite classical quadratic form.

Two n-ary quadratic forms Q_1 and Q_2 are called *equivalent*, denoted by $Q_1 \cong Q_2$, if there exists an $n \times n$ matrix M consisting of elements of $\mathcal{O}_K$ and with $\det M \in \mathcal{U}_K$, such that $Q_2(\boldsymbol{x}) = Q_1(M\boldsymbol{x})$. Note that equivalent quadratic forms represent the same elements; in particular, Q_1 is universal if and only if Q_2 is universal.

Given an n-ary quadratic form Q and a set of vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m \in \mathcal{O}_K^n$, we call the matrix $(B_Q(\boldsymbol{v}_i, \boldsymbol{v}_j))_{i,j=1}^m$ a *Gram matrix of $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m$ with respect to Q*. When this set of vectors coincides with the canonical basis of K^n, the quadratic form can be expressed as

$$Q(x_1, x_2, \ldots, x_n) = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \end{pmatrix} \cdot \begin{pmatrix} a_{11} & \frac{a_{12}}{2} & \cdots & \frac{a_{1n}}{2} \\ \frac{a_{12}}{2} & a_{22} & \cdots & \frac{a_{2n}}{2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{a_{1n}}{2} & \frac{a_{2n}}{2} & \cdots & a_{nn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix};$$

then we speak simply about the *Gram matrix associated to* Q or *the matrix of* Q.

A form is totally positive definite, resp. diagonal, if and only if its Gram matrix has the same property. To examine the total positive definiteness of Q, one can use Sylvester's criterion: Q is totally positive definite if and only if the leading principal minors of its Gram matrix are totally positive definite. Moreover, a form is classical if and only if its Gram matrix contains only integral entries.

1.2.4 Indecomposable integers

Let α be a totally positive integer in K. We say that α is *indecomposable* in K if the equation $\alpha = \beta + \gamma$ cannot be satisfied for any two elements $\beta, \gamma \in \mathcal{O}_K^+$. The structure of indecomposable integers of all the quadratic fields is well-known. Let n be a square-free positive rational integer and set

$$\omega_n = \begin{cases} \sqrt{n} & \text{if } n \equiv 2,3 \pmod 4, \\ \frac{1+\sqrt{n}}{2} & \text{if } n \equiv 1 \pmod 4. \end{cases}$$

If we take the continued fraction $[u_0, \overline{u_1, u_2, \ldots, u_l}]$ of $-\overline{\omega_n}$ (i.e., of the conjugate element to $-\omega_n$ in the quadratic field $\mathbb{Q}(\sqrt{n})$), we can consider only parts of this continued fraction and get rational numbers of the form

$$\frac{p_i}{q_i} = [u_0, u_1, \ldots, u_i].$$

We can also obtain these numbers from the recurrence relations

$$p_{i+1} = p_{i-1} + u_{i+1}p_i,$$
$$q_{i+1} = q_{i-1} + u_{i+1}q_i,$$

where $p_{-1} = 1$, $q_{-1} = 0$, $p_0 = u_0$ and $q_0 = 1$. Having this sequence of p_i and q_i, we define elements $\alpha_i = p_i + q_i\omega_n$ called *convergents* of $-\overline{\omega_n}$. However, in addition, we can consider integers of the form $\alpha_{i,k} = \alpha_i + k\alpha_{i+1}$ where $0 \le k \le u_{i+2}$. These elements are called *semiconvergents* of $-\overline{\omega_n}$ and belong to $\mathcal{O}_K^+$ if and only if i is odd. In such a case, the elements $\alpha_{i,k}$'s are all the indecomposable integers in $\mathbb{Q}(\sqrt{n})$; up to multiplication by units, there are only finitely many of them (see [Per, DS]).

In biquadratic fields, we do not have such a characterization of indecomposable integers. The only to us known result is [Č+, Th. 2.1] which claims that under certain conditions, the indecomposables from quadratic subfields remain indecomposable in the biquadratic field. The meaning of p, q and r in this theorem agrees with the one given by Convention 1.2.2.

Theorem 1.2.4. *Let $K = \mathbb{Q}(\sqrt{p}, \sqrt{q})$ be a biquadratic number field. For $k \in \{p, q, r\}$, we set $M_k = \max\{u_i;\ i \text{ odd}\}$, where $[u_0, \overline{u_1, u_2, \ldots, u_{l-1}, u_l}]$ is the continued fraction of $-\overline{\omega_k}$.*

(a) Let $\alpha \in \mathbb{Q}(\sqrt{p})$ be indecomposable.

- *If α is a convergent of $-\overline{\omega_p}$ and $\sqrt{r} > \sqrt{p}$, then α is indecomposable in K.*
- *If $\sqrt{r} > M_p\sqrt{p}$, then α is indecomposable in K.*

(b) Let $\beta \in \mathbb{Q}(\sqrt{q})$ be indecomposable.

- *In the cases (B1), (B2), (B3), β is indecomposable in K.*
- *In the case (B4), if $\sqrt{r} > \sqrt{q}$ and β is a convergent of $-\overline{\omega_q}$, then β is indecomposable in K.*
- *In the case (B4), if $\sqrt{r} > M_q\sqrt{q}$, then β is indecomposable in K.*

(c) Let $\gamma \in \mathbb{Q}(\sqrt{r})$ be indecomposable.

- *If γ is a convergent of $-\overline{\omega_r}$ and $\sqrt{p} > \sqrt{r}$, then γ is indecomposable in K.*
- *If $\sqrt{p} > M_r\sqrt{r}$, then γ is indecomposable in K.*

Nevertheless, as we shall see in Subsection 1.4.3, this theorem does not cover all the indecomposable integers originating from quadratic subfields and, moreover, we will provide an example of an element indecomposable in a quadratic subfield which decomposes in our biquadratic field K. Both was already foreshadowed in Theorem 1.1.3.

1.3 Idea of the proof

In the main part of this article, we do not use the method of escalation as developed in [BH] (the only exception will be fields containing 2 or 5 in Subsections 1.6.8, 1.6.9 and 1.6.10). Instead of that, we follow the ideas from [CKR]: Assume that Q is a universal classical totally positive definite ternary quadratic form over $\mathcal{O}_K$. Obviously Q has to represent the number 1, and hence Q can be orthogonally split into $Q \cong \langle 1\rangle \perp Q_0$ (see Corollary 1.4.23(2)). This step is one of the key ingredients for the proof, as it can actually be used repeatedly any time when a totally positive unit (not necessarily 1) happens to be represented by the form Q or any of its subforms.

Now it is easy to see that if we have "enough" totally positive units which do not differ (multiplicatively) from each other by a square, then the nonuniversality of Q follows: Suppose that ε, ε' are two totally positive units such that $\varepsilon, \varepsilon', \varepsilon\varepsilon' \notin \mathcal{U}_K^{\square}$ (in particular, $\varepsilon, \varepsilon' \neq 1$ and $\varepsilon \neq \varepsilon'$). The unary form $\langle 1\rangle$ clearly represents all squares, and in particular all elements of $\mathcal{U}_K^{\square}$, but it does not represent ε. We will see in Lemma 1.4.3 that a totally positive unit cannot be written as a sum of two elements of $\mathcal{O}_K^+$; thus, ε has to be represented by the binary form Q_0. Therefore, we can repeat the splitting and write $Q_0 \cong \langle \varepsilon\rangle \perp \langle \gamma\rangle$ for some $\gamma \in \mathcal{O}_K^+$, i.e., $Q \cong \langle 1\rangle \perp \langle \varepsilon\rangle \perp \langle \gamma\rangle$. After that, we apply the same arguments for ε'. Note that $\langle \varepsilon\rangle$ represents only elements from $\varepsilon\mathcal{O}_K^{\square}$, and so it does not represent ε'; we obtain that ε' must be represented by $\langle \gamma\rangle$, which easily gives $Q \cong \langle 1\rangle \perp \langle \varepsilon\rangle \perp \langle \varepsilon'\rangle$. But in such a case, $\varepsilon\varepsilon'$ is another nonsquare totally positive unit, and it is not represented by Q for the same reasons. Therefore, under the given assumptions, no classical totally positive definite ternary quadratic form can be universal, as we have actually shown that no such form can represent all the elements $1, \varepsilon, \varepsilon', \varepsilon\varepsilon'$ at once.

The discussion above indicates that the complexity of the problem depends heavily on the size of the factor group $\mathcal{U}_K^+/\mathcal{U}_K^{\square}$. Using Dirichlet's unit theorem, one can easily see that the group $\mathcal{U}_K/\mathcal{U}_K^{\square}$ has 16 elements. Thus, as the group $\mathcal{U}_K/\mathcal{U}_K^+$ is obviously nontrivial, we deduce from the equality $|\mathcal{U}_K/\mathcal{U}_K^{\square}| = |\mathcal{U}_K/\mathcal{U}_K^+| \cdot |\mathcal{U}_K^+/\mathcal{U}_K^{\square}|$ that the size of the factor group $\mathcal{U}_K^+/\mathcal{U}_K^{\square}$ can be only $1, 2, 4$ or 8. Let us consider the following three cases:

(I) $|\mathcal{U}_K^+/\mathcal{U}_K^{\square}| > 2$; in this case we can find $\varepsilon, \varepsilon'$ as above,

(II) $|\mathcal{U}_K^+/\mathcal{U}_K^{\square}| = 2$; here we can find a totally positive unit ε such that $\{1, \varepsilon\}$ is a system of representatives of the factor group,

(III) $|\mathcal{U}_K^+/\mathcal{U}_K^{\square}| = 1$; all units are squares, thus the only relevant unit in this case is 1.

We have solved the case (I) already, there does not exist any universal (classical, totally positive definite) ternary quadratic form. Lemma 1.8.1 hints that this is often the case.

In the case (II), it is sufficient to consider the quadratic forms $\langle 1\rangle \perp \langle \varepsilon\rangle \perp \langle \gamma\rangle$ for $\gamma \in \mathcal{O}_K^+$ (including the cases $\gamma = 1$ and $\gamma = \varepsilon$). The obvious question is whether such a form represents 2. Putting aside the case $\sqrt{2} \in K$, we have two possibilities: either $\langle \varepsilon\rangle$ does not represent 2, and hence γ has to be either 1 or 2 (see Lemma 1.4.3), or $\langle \varepsilon\rangle$ does represent 2, and we have to look for another number which is not yet represented. Note that $\langle \varepsilon\rangle$ represents 2 if and only

if 2ε is a square in $\mathcal{O}_K$; we will use this condition significantly in both cases. It is also worth pointing out Proposition 1.4.20 which summarizes some arguments used repeatedly throughout the whole proof.

The most challenging part of the proof is, of course, the case (III). We can still be lucky enough to obtain a diagonalizable binary quadratic form Q_0, and hence we consider quadratic forms $\langle 1\rangle \perp \langle \beta\rangle \perp \langle \gamma\rangle$ separately; but in general, Q_0 has the form $\alpha' y^2 + 2\beta' yz + \gamma' z^2$ with $\beta' \neq 0$. The problems here are caused mainly by the fact that β' (and the term $2\beta' yz$ in general) does not have to be totally positive, which prevents us from using estimations.

It should be clear now from the ideas above that in the cases with "not enough totally positive units", we need to find other elements which are not squares (because squares are already represented by $\langle 1\rangle$), and which are difficult to express as a sum of two elements of $\mathcal{O}_K^+$. In other words, we need to find some nonsquare indecomposable elements; this is the main purpose of the next section.

1.4 Preparation for the proof

In this section, we introduce several tools that we need for the proof of Theorem 1.1.1. As indicated at the end of the previous section, we want to know whether some given elements of $\mathcal{O}_K$ are squares and how to express some numbers as a sum of elements belonging to $\mathcal{O}_K^+$. The latter also includes the problematics of indecomposable elements in K; we provide a proof of Theorem 1.1.3. Furthermore, we take a more detailed look at representations by unary forms. Finally, for the sake of nondiagonalizable forms in the case (III), we include some lemmas about quadratic lattices.

1.4.1 Squares

If $\alpha \in \mathcal{O}_K$ has the property that, when considered as an element of the field K, it is a square, then α is actually a square in the ring $\mathcal{O}_K$, i.e., $\sqrt{\alpha} \in \mathcal{O}_K$. However obvious this may seem, it is not automatic; in fact, it is a consequence of $\mathcal{O}_K$ being algebraically closed in K. In the following, we will slightly abuse the language, and speak about algebraic integers *being* or *becoming a square in the (biquadratic) field* K, by which we actually mean that they are squares in the ring $\mathcal{O}_K$.

The following lemma generalizes [Č+, Lemma 4.1]. Note that in the statement, the meaning of n_3 is given by Convention 1.2.2 as $\frac{n_1 n_2}{\gcd(n_1,n_2)^2}$.

Lemma 1.4.1. *Let $F = \mathbb{Q}(\sqrt{n_1})$ and $K = \mathbb{Q}(\sqrt{n_1}, \sqrt{n_2})$.*

1. *Suppose that $\alpha \in \mathcal{O}_F$ is not a square in the field F but becomes a square in K. Then if $\beta = x + y\sqrt{n_1} + z\sqrt{n_2} + w\sqrt{n_3} \in \mathcal{O}_K$ is such that $\alpha = \beta^2$, it must hold that $x = y = 0$.*

2. *More generally, if $\beta = x + y\sqrt{n_1} + z\sqrt{n_2} + w\sqrt{n_3} \in K$ (not necessarily integral) satisfies $\beta^2 \in \mathbb{Q}(\sqrt{n_1})$, then either $x = y = 0$ or $z = w = 0$.*

Proof. Clearly it suffices to prove the second statement. We can write $\beta = A + B\sqrt{n_2}$ with $A = x + y\sqrt{n_1}$ and $B = z + \frac{w}{\gcd(n_1,n_2)}\sqrt{n_1}$; in particular, $A, B \in \mathbb{Q}(\sqrt{n_1})$. Then it holds that $\beta^2 = (A^2 + n_2 B^2) + 2AB\sqrt{n_2}$, thus one sees that $\beta^2 \in \mathbb{Q}(\sqrt{n_1})$ is equivalent to $2AB = 0$. If $A = 0$, then $x = y = 0$, and if $B = 0$, then $z = w = 0$. This completes the proof. □

As a corollary of this lemma, we obtain a simple yet powerful criterion for quadratic elements which become a square in the biquadratic field.

Corollary 1.4.2. *Let $F = \mathbb{Q}(\sqrt{n_1})$ and $\alpha \in \mathcal{O}_F$. Suppose that α is not a square in F but becomes a square in $K = \mathbb{Q}(\sqrt{n_1}, \sqrt{n_2})$. Then every odd divisor of $\gcd(n_2, n_3)$ divides α as well.*

Proof. From Lemma 1.4.1(1) we know that

$$\alpha = \left(\frac{c\sqrt{n_2} + d\sqrt{n_3}}{2}\right)^2 = \frac{c^2 n_2 + d^2 n_3}{4} + \frac{cd\gcd(n_2, n_3)}{2}\sqrt{n_1}$$

where the form of integral bases (B1)–(B4) ensures $c, d \in \mathbb{Z}$, $c \equiv d \pmod 2$. If c, d are even, then clearly both expressions $\frac{1}{4}(c^2 n_2 + d^2 n_3)$ and $\frac{1}{2}cd\gcd(n_2, n_3)\sqrt{n_1}$ are divisible by $\gcd(n_2, n_3)$; if they are odd, then still they are both divisible by all the odd divisors of $\gcd(n_2, n_3)$. □

1.4.2 Additive decompositions of rational integers

In the study of universality of quadratic forms in biquadratic fields, we repeatedly discuss whether our form can represent some (suitably chosen) element. This element is usually either a rational integer or an indecomposable element in K. In the first case, we often need to know in what ways we can express our chosen number as a sum of two elements $\alpha, \beta \in \mathcal{O}_K^+ \cup \{0\}$ – i.e., we examine its *additive decompositions*. If these elements are also rational integers, we will say that this decomposition is *trivial*. We will be particularly interested in the cases when one of α and β is a square.

First of all, let us focus on the additive decompositions of numbers $2, 3$ and 5.

Lemma 1.4.3. *In a biquadratic field K:*

1. *All (totally positive) units are indecomposable.*
2. *The number 2 can always decompose only trivially as $1+1$ or $0+2$.*
3. *If $\sqrt{5} \notin K$, then 3 can decompose only trivially as $1+2$ or $0+3$.*
   The only nontrivial decomposition is $\frac{3+\sqrt{5}}{2} + \frac{3-\sqrt{5}}{2}$.
4. *If $\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{13}, \sqrt{17}, \sqrt{21} \notin K$, then 5 decomposes only trivially as $2+3$, $1+4$ or $0+5$.*
   Up to embeddings, the list of all nontrivial decompositions is as follows:
   - $(2+\sqrt{2}) + (3-\sqrt{2})$,
   - $(2+\sqrt{3}) + (3-\sqrt{3})$,
   - $\frac{3+\sqrt{5}}{2} + \frac{7-\sqrt{5}}{2}$,
   - $\frac{5+\sqrt{5}}{2} + \frac{5-\sqrt{5}}{2}$,
   - $\frac{5+\sqrt{13}}{2} + \frac{5-\sqrt{13}}{2}$,
   - $\frac{5+\sqrt{17}}{2} + \frac{5-\sqrt{17}}{2}$,
   - $\frac{5+\sqrt{21}}{2} + \frac{5-\sqrt{21}}{2}$,
   - $(2+\frac{\sqrt{2}+\sqrt{6}}{2}) + (3-\frac{\sqrt{2}+\sqrt{6}}{2})$.

Remark. As we will see from the proof, parts (1) and (2) actually hold for *any* totally real field K, not only for the biquadratic ones.

Proof. Part (1) follows directly from the inequality (1.2.1), as the norm of any element of $\mathcal{O}_K^+$ is greater or equal to 1. The same idea is used in part (2): If $2 = \alpha + \beta$ for $\alpha, \beta \in \mathcal{O}_K^+$, then $2 = \sqrt[N]{\mathcal{N}_{K/\mathbb{Q}}(\alpha+\beta)} \geq \sqrt[N]{\mathcal{N}_{K/\mathbb{Q}}(\alpha)} + \sqrt[N]{\mathcal{N}_{K/\mathbb{Q}}(\beta)} \geq 1+1$; we see that α and β must be units, and, moreover, equality was attained in (1.2.1), thus $\frac{\alpha}{\beta} \in \mathbb{Q}$, which shows $\alpha = \beta = 1$.

Part (2) could also have been obtained as an easy corollary of part (3): From the list of all $\alpha \succcurlyeq 0$ such that $3 \succcurlyeq \alpha$, only $0, 1$ and 2 satisfy $2 \succcurlyeq \alpha$ as well. In a similar fashion, we can obtain (3) from the full statement of (4).

For the proof of (4), suppose $5 = \alpha + \beta$ for $\alpha, \beta \in \mathcal{O}_K^+ \cup \{0\}$. If $\alpha \in \mathbb{Q}$, we obtain precisely the trivial decompositions. For $\alpha \notin \mathbb{Q}$, we consider all possible cases:

First, $\alpha, \beta \in \mathbb{Q}(\sqrt{n})$ for some quadratic subfield of K. Without loss of generality, suppose $\mathrm{Tr}_{\mathbb{Q}(\sqrt{n})/\mathbb{Q}}(\alpha) \leq \mathrm{Tr}_{\mathbb{Q}(\sqrt{n})/\mathbb{Q}}(\beta)$, hence $\alpha = \frac{a}{2} + \frac{b}{2}\sqrt{n}$ where $0 < \frac{a}{2} \leq \frac{5}{2}$; by choosing a suitable embedding we can ensure $b > 0$. By Lemma 1.2.3 (which will be used repeatedly in the whole following proof) we have $a > b\sqrt{n}$. If $n \not\equiv 1 \pmod 4$, then $\frac{a}{2}, \frac{b}{2} \in \mathbb{Z}$, hence the only solution of the inequalities $0 < \frac{a}{2} \leq \frac{5}{2}$, $a > b\sqrt{n} > 0$ is $\frac{a}{2} = 2$, $\frac{b}{2} = 1$, $n \in \{2, 3\}$. If $n \equiv 1 \pmod 4$, half-integers are also allowed (provided that $a \equiv b \pmod 2$); the same inequalities are satisfied only by $\frac{a}{2} = \frac{3}{2}$, $\frac{b}{2} = \frac{1}{2}$, $n = 5$ and by $\frac{a}{2} = \frac{5}{2}$, $\frac{b}{2} = \frac{1}{2}$, $n \in \{5, 13, 17, 21\}$.

The second case is when, in the decomposition, exactly two of the three numbers $\sqrt{m}$, $\sqrt{s}$, $\sqrt{t}$ are multiplied by a nonzero coefficient – let us denote these two square roots by $\sqrt{n_1}$, $\sqrt{n_2}$. By looking at the bases (B1)–(B4), observe that the corresponding coefficients are half-integers since if quarter-integers are involved, all three square roots have nonzero coefficients. By first choosing α such that $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) \leq \mathrm{Tr}_{K/\mathbb{Q}}(\beta)$ and then using a suitable embedding, we have $\alpha = \frac{a}{2} - \frac{b_1}{2}\sqrt{n_1} - \frac{b_2}{2}\sqrt{n_2}$ for $a, b_1, b_2 > 0$ and $\frac{a}{2} \leq \frac{5}{2}$. Thus $\alpha \succcurlyeq 0$ if and only if $a > b_1\sqrt{n_1} + b_2\sqrt{n_2}$. From the form of the possible integral bases (B1)–(B4) we see that not all of a, b_1, b_2 can be odd at the same time. Thus either a is even, $a = 2a'$, and $4 \geq 2a' > b_1\sqrt{n_1} + b_2\sqrt{n_2}$, or without loss of generality b_1 is even and $5 \geq a > 2\sqrt{n_1} + \sqrt{n_2}$. The only square-free integers n_1, n_2 which may satisfy the latter inequality are $2, 3$ in any order; but in that case we are in the integral basis (B1) which requires a to be even; that is impossible since $4 \not> 2\sqrt{2} + \sqrt{3}$. So we are left with the former inequality $4 \geq 2a' > b_1\sqrt{n_1} + b_2\sqrt{n_2}$; here necessarily $a' = 2$, $b_1 = b_2 = 1$ and $4 > \sqrt{n_1} + \sqrt{n_2}$. This is satisfied by $\{n_1, n_2\}$ equal to $\{2, 3\}$, $\{2, 5\}$, $\{2, 6\}$ and $\{3, 5\}$; however, we have to compare these possibilities for $\alpha = 2 - \frac{1}{2}(\sqrt{n_1} + \sqrt{n_2})$ with the corresponding integral bases (B1)–(B4) to see whether they belong to $\mathcal{O}_K$. In fact, only $2 - \frac{1}{2}(\sqrt{2} + \sqrt{6})$ is an algebraic integer, so the only decomposition of this type is $5 = (2 - \frac{\sqrt{2}+\sqrt{6}}{2}) + (3 + \frac{\sqrt{2}+\sqrt{6}}{2})$ (up to embedding).

In the third and last case, all of $\sqrt{m}$, $\sqrt{s}$ and $\sqrt{t}$ are multiplied by nonzero coefficients. In this case, instead of requiring $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) \leq \mathrm{Tr}_{K/\mathbb{Q}}(\beta)$, we take α to be the summand which, in a suitable embedding, has the form $\frac{a}{4} - \frac{b}{4}\sqrt{m} - \frac{c}{4}\sqrt{s} - \frac{d}{4}\sqrt{t}$ for $b, c, d > 0$ (one of the two summands has this property). Then $\alpha \succ 0$ if and only if

$$a > b\sqrt{m} + c\sqrt{s} + d\sqrt{t}; \tag{1.4.1}$$

to arrive at a contradiction, we distinguish two subcases:

For the first subcase, suppose that quarter-integers are involved, i.e., all of a, b, c, d are odd. This necessarily means that $m \equiv s \equiv t \equiv 1 \pmod 4$, which easily implies $t \geq 65$. Applying Lemma 1.2.3 to $\beta = (5 - \frac{a}{4}) + \frac{b}{4}\sqrt{m} + \frac{c}{4}\sqrt{s} + \frac{d}{4}\sqrt{t} \succ 0$, we arrive at $(5 - \frac{a}{4}) > |\frac{d}{4}|\sqrt{t} \geq \frac{\sqrt{t}}{4} \geq \frac{\sqrt{65}}{4} > \frac{8}{4}$, thus $a \leq 11$. Plugging this into (1.4.1), we see that $\alpha \succ 0$ implies $11 > \sqrt{m} + \sqrt{s} + \sqrt{t}$. However, this never holds – if m and s are coprime, we get at least $\sqrt{5} + \sqrt{13} + \sqrt{65} \approx 13.904$; if they are not, the smallest value is $\sqrt{21} + \sqrt{33} + \sqrt{77} \approx 19.102$. So there is no decomposition of this type.

For the second subcase, suppose that no quarter-integers are involved, i.e., all a, b, c, d are even; denote $a = 2a'$. Similarly to the previous paragraph, from $\beta \succ 0$ we obtain $5 - \frac{a'}{2} > \frac{\sqrt{t}}{2}$, so except for the field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ this yields $5 - \frac{a'}{2} > \frac{\sqrt{10}}{2} > \frac{3}{2}$, i.e., $\frac{a'}{2} < \frac{7}{2}$. In the case of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, $\frac{a'}{2}$ is necessarily in $\mathbb{Z}$ and $t = 6$, so $\frac{a'}{2} \leq 3$. Thus $\frac{a'}{2} \leq \frac{6}{2}$ in all cases; by plugging this into (1.4.1), we obtain $6 > \sqrt{m} + \sqrt{s} + \sqrt{t}$. This is satisfied only by $m = 2$, $s = 3$, $t = 6$; however, even this case fails since $\frac{1}{2}(2 - \sqrt{2} - \sqrt{3} - \sqrt{6}) \notin \mathcal{O}_K$ and $\frac{1}{2}(2 - \sqrt{2} - 2\sqrt{3} - \sqrt{6})$ is not totally positive. So there are no decompositions of this kind either. □

Remark 1.4.4. We are particularly interested in decompositions of 1, 2, 3 and 5 as $\omega^2 + \beta$ with $\beta \succcurlyeq 0$. By scrutinizing the decompositions in Lemma 1.4.3, we obtain – aside of the obvious possibilities with $\omega^2 \in \{0, 1, 4\}$, and the slightly less obvious $\omega^2 \in \{2, 3, 5\}$ if the appropriate square root lies in K – only the following decompositions (up to embedding):

1. 3 can be written as $\left(\frac{\sqrt{5}+1}{2}\right)^2 + \left(\frac{\sqrt{5}-1}{2}\right)^2$;
2. 5 can be written as $\left(\frac{\sqrt{2}+\sqrt{6}}{2}\right)^2 + (3-\sqrt{3})$ or $\left(\frac{\sqrt{3}+\sqrt{7}}{2}\right)^2 + \left(\frac{\sqrt{7}-\sqrt{3}}{2}\right)^2$.

Although the additive decompositions of the form $\omega^2 + \beta$ can be fully described also for the numbers 8 and 10, we exclude biquadratic fields with small values of m in order to shorten both the statement and the proof.

Lemma 1.4.5. *Let $\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{7} \notin K$. Then:*

1. *If $8 = \omega^2 + \beta$, $\beta \succcurlyeq 0$, then either $\omega^2 \in \{0, 1, 4, 9\}$ (these possibilities always exist), or:*
   - $\omega^2 = \left(\frac{1\pm\sqrt{13}}{2}\right)^2 = \frac{7\pm\sqrt{13}}{2}$ *if* $\sqrt{13} \in K$,
   - $\omega^2 = \left(\frac{1\pm\sqrt{17}}{2}\right)^2 = \frac{9\pm\sqrt{17}}{2}$ *if* $\sqrt{17} \in K$,
   - $\omega^2 = \left(\frac{1\pm\sqrt{21}}{2}\right)^2 = \frac{11\pm\sqrt{21}}{2}$ *if* $\sqrt{21} \in K$.
2. *If $10 = \omega^2 + \beta$, $\beta \succcurlyeq 0$, then ω^2 can take the same values as listed before, with the additional possibility $\omega^2 = 9$, and also $\omega^2 = 10$ if $\sqrt{10} \in K$.*

Proof. The first part is a trivial consequence of the second one. Let us therefore consider $10 \succcurlyeq \omega^2$ for

$$\omega = \frac{a}{4} + \frac{b}{4}\sqrt{m} + \frac{c}{4}\sqrt{s} + \frac{d}{4}\sqrt{t}$$

with $a, b, c, d \in \mathbb{Z}$. By comparing traces, we get the inequality

$$10 \geq \frac{a^2}{16} + \frac{b^2}{16}m + \frac{c^2}{16}s + \frac{d^2}{16}t. \tag{1.4.2}$$

If $m > 10$, this immediately implies $\frac{|b|}{4}, \frac{|c|}{4}, \frac{|d|}{4} < 1$. For $m = 10$, the same argument holds, except for $\frac{b}{4} = \pm 1$, which yields the decomposition $10 = (\pm\sqrt{10})^2 + 0$. Further, we consider several cases:

First, b, c, d are all zeros. Then $\frac{a}{4}$ has to be an integer, and clearly the full list of its possible values is $\frac{a}{4} = 0, \pm 1, \pm 2, \pm 3$.

Second, exactly one of b, c, d is nonzero. Then ω as well as β belong to a quadratic subfield $\mathbb{Q}(\sqrt{n})$ of K where $n \in \{m, s, t\}$. If $n \not\equiv 1 \pmod 4$, then the coefficient in front of $\sqrt{n}$ is an integer, which cannot happen since it is smaller then 1 (putting aside the already discussed case of $10 = (\pm\sqrt{10})^2 + 0$). So $n \equiv 1 \pmod 4$, $n \geq 13$, and we have to consider only $10 \succcurlyeq \left(\frac{a'\pm\sqrt{n}}{2}\right)^2$ for a' odd, without loss of generality positive. This is equivalent to $40 \geq a'^2 + 2a'\sqrt{n} + n$. By plugging in $a' = 3$ and $n = 13$ we find out that $a' \geq 3$ is never possible. Thus $a' = 1$; the resulting inequality $39 \geq n + 2\sqrt{n}$ is satisfied for 13, 17 and 21 but not for 29, which gives us the remaining three decompositions from the statement.

The last possibility is when at least two of b, c, d are nonzero; we prove that this is not possible. Suppose first that there are no quarter-integers involved, i.e., all of a, b, c, d are even. Then if all of b, c, d were nonzero, (1.4.2) would yield $40 \geq m + s + t$ which can easily be checked never to hold for $m \geq 10$.

Thus if no quarter-integers are involved, exactly two of $\frac{b}{4}$, $\frac{c}{4}$, $\frac{d}{4}$ are nonzero (and thus equal to $\pm\frac{1}{2}$). So we have to find out when $10 \succcurlyeq \left(\frac{a'}{2} + \frac{\pm\sqrt{n_1}\pm\sqrt{n_2}}{2}\right)^2$ holds for some $n_1, n_2 \in \{m, s, t\}, n_1 \neq n_2$. By Lemma 1.2.3 this gives $10 - \frac{a'^2}{4} - \frac{n_1+n_2}{4} \geq \left|\pm 2\frac{\sqrt{n_1 n_2}}{4}\right|$, which implies $40 - n_1 - n_2 - 2\sqrt{n_1 n_2} \geq 0$. That never holds for $n_1 \neq n_2 \geq 10$, giving the desired contradiction.

The only remaining case is when quarter-integers are involved in the decomposition. This can only happen if $m \equiv s \equiv t \equiv 1 \pmod 4$, and all a, b, c, d are odd – especially, they cannot be zero. So the basic condition given by (1.4.2) translates to $10 \geq \frac{1+m+s+t}{16}$, i.e., $159 \geq m + s + t$. This almost never holds: Clearly m, s cannot be coprime. Thus m is a composed square-free

number satisfying $159 \geq m + (m+4) + (m+8)$; this gives $m = 21$ and $m = 33$ as the only options. Then the inequality $159 - 21 \geq s + (s+4)$ only allows the composed square-free numbers $s = 33$, $s = 57$ and $s = 65$. After computing the corresponding t's we get $\mathbb{Q}(\sqrt{21}, \sqrt{33})$ as the only case where indeed $159 \geq m + s + t$.

So we only have to prove that $10 \succcurlyeq \left(\frac{a+b\sqrt{21}+c\sqrt{33}+d\sqrt{77}}{4}\right)^2$ cannot happen for a odd and $\frac{|b|}{4}, \frac{|c|}{4}, \frac{|d|}{4} \in \{\frac{1}{4}, \frac{3}{4}\}$. This requires just straightforward calculations which we omit. □

Remark. As we will see in Subsection 1.6.2, the previous lemma is not required when $\sqrt{21} \in K$. In particular, there is no harm in avoiding the computation for the field $\mathbb{Q}(\sqrt{21}, \sqrt{33})$.

1.4.3 New indecomposable elements

Theorem 1.2.4 gives us several conditions under which indecomposable integers from quadratic subfields do not decompose in the biquadratic field. The following examples show that if these conditions are not satisfied, indecomposable elements can become decomposable in the larger field.

Example 1.4.6. Let us consider $K = \mathbb{Q}(\sqrt{2}, \sqrt{5})$ and $\alpha = 7 + 2\sqrt{10}$, which is indecomposable in $\mathbb{Q}(\sqrt{10})$. Nevertheless, α can be written as

$$\alpha = \underbrace{\frac{7}{2} + \sqrt{2} + \frac{1}{2}\sqrt{5} + \sqrt{10}}_{\beta} + \underbrace{\frac{7}{2} - \sqrt{2} - \frac{1}{2}\sqrt{5} + \sqrt{10}}_{\gamma}$$

where β and γ are both totally positive integers of $\mathbb{Q}(\sqrt{2}, \sqrt{5})$. In a similar way we can see that $\alpha' = 10 + 3\sqrt{10}$, indecomposable in $\mathbb{Q}(\sqrt{10})$, can be expressed as

$$\alpha' = \underbrace{5 + \frac{3}{2}\sqrt{2} + \sqrt{5} + \frac{3}{2}\sqrt{10}}_{\beta'} + \underbrace{5 - \frac{3}{2}\sqrt{2} - \sqrt{5} + \frac{3}{2}\sqrt{10}}_{\gamma'}.$$

for $\beta', \gamma' \in \mathcal{O}_K^+$. Thus α and α' decompose in this biquadratic field.

In the following example, we will show the case when a certain element, later called $\mathcal{T}$, decomposes in a biquadratic field. Note that this provides the proof of Theorem 1.1.3(3).

Example 1.4.7. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{21})$ and consider $\alpha = 7 + \sqrt{42}$, which is indecomposable in $\mathbb{Q}(\sqrt{42})$. Note that this element is of the form $\alpha = \lceil\sqrt{42}\rceil + \sqrt{42}$, and $42 \equiv 2 \pmod 4$. However, as before, the element α can be written as

$$\alpha = \underbrace{\frac{7}{2} + \frac{3}{2}\sqrt{2} + \frac{1}{2}\sqrt{21} + \frac{1}{2}\sqrt{42}}_{\beta} + \underbrace{\frac{7}{2} - \frac{3}{2}\sqrt{2} - \frac{1}{2}\sqrt{21} + \frac{1}{2}\sqrt{42}}_{\gamma}$$

where $\beta, \gamma \in \mathcal{O}_K^+$.

On the other hand, Theorem 1.2.4 does not cover all indecomposable integers of quadratic subfields which do not decompose in our biquadratic field. In the following part, we will show some examples of such elements, which we later use in proving nonuniversality of ternary quadratic forms.

Let $u \in \mathbb{N}$ be a square-free positive integer greater than 1. In what follows, $\lceil\sqrt{u}\rceil$ stands for the smallest element of $\mathbb{N}$ greater than $\sqrt{u}$. Furthermore, we will denote by $\lceil\sqrt{u}\rceil^{\text{odd}}$ the smallest odd positive integer greater than $\sqrt{u}$. Denote

$$\mathcal{M}_1 = \lceil\sqrt{m}\rceil + \sqrt{m}.$$

Moreover, for $m \equiv 1 \pmod 4$ put

$$\mathcal{M}_{1/2} = \frac{\lceil\sqrt{m}\rceil^{\text{odd}} + \sqrt{m}}{2}.$$

Note that for $m \equiv 1 \pmod 4$ we have both $\mathcal{M}_1$ and $\mathcal{M}_{1/2}$; in other cases, there is only $\mathcal{M}_1$. The elements $\mathcal{S}_1$, $\mathcal{S}_{1/2}$, $\mathcal{T}_1$ and $\mathcal{T}_{1/2}$ are defined in a similar way. Most importantly, we denote

$$\mathcal{M} = \begin{cases} \mathcal{M}_1 = \lceil\sqrt{m}\rceil + \sqrt{m} & \text{if } m \equiv 2,3 \pmod 4, \\ \mathcal{M}_{1/2} = \frac{\lceil\sqrt{m}\rceil^{\text{odd}} + \sqrt{m}}{2} & \text{if } m \equiv 1 \pmod 4. \end{cases}$$

Likewise, we define $\mathcal{S}$ and $\mathcal{T}$.

Now we will show that $\mathcal{M}$ is indecomposable in $\mathbb{Q}(\sqrt{m})$. All the indecomposable integers of this subfield can be obtained from the continued fraction $[u_0, \overline{u_1, u_2, \ldots, u_{l-1}, u_l}]$ of $\sqrt{m}$ or $\frac{\sqrt{m}-1}{2}$ as convergents and semiconvergents. In the case of $m \equiv 2,3 \pmod 4$, the first two convergents of $\sqrt{m}$ are $\alpha_{-1} = 1$ and $\alpha_0 = \lfloor\sqrt{m}\rfloor + \sqrt{m}$. Semiconvergents $\alpha_{-1,k}$ are consequently equal to

$$\alpha_{-1,k} = \alpha_{-1} + k\alpha_0$$

where $0 \le k \le u_1$ and $1 \le u_1$. Note that these elements are totally positive since the index -1 is odd. If $k = 1$, we have

$$\alpha_{-1,1} = \alpha_{-1} + \alpha_0 = \lfloor\sqrt{m}\rfloor + 1 + \sqrt{m} = \lceil\sqrt{m}\rceil + \sqrt{m} = \mathcal{M}_1 = \mathcal{M},$$

thus $\mathcal{M}$, as one of the totally positive semiconvergents of $\sqrt{m}$, is indecomposable in $\mathbb{Q}(\sqrt{m})$.

In the case when $m \equiv 1 \pmod 4$, we consider the first two convergents

$$\alpha_{-1} = 1 \quad \text{and} \quad \alpha_0 = \left\lfloor \frac{\sqrt{m}-1}{2} \right\rfloor + \frac{1+\sqrt{m}}{2}.$$

Let us first suppose that $\lfloor\sqrt{m}\rfloor$ is even, i.e., $\lceil\sqrt{m}\rceil$ is odd. Put $\sqrt{m} = 2l + \lambda$ for some $l \in \mathbb{Z}$ and $0 < \lambda < 1$. Then

$$\left\lfloor \frac{\sqrt{m}-1}{2} \right\rfloor = \left\lfloor \frac{2l+\lambda-1}{2} \right\rfloor = \left\lfloor l + \frac{\lambda-1}{2} \right\rfloor = l - 1 = \frac{\lfloor\sqrt{m}\rfloor}{2} - 1.$$

Therefore,

$$\begin{aligned} \alpha_{-1,1} = \alpha_{-1} + \alpha_0 &= 1 + \frac{\lfloor\sqrt{m}\rfloor}{2} - 1 + \frac{1+\sqrt{m}}{2} = \frac{\lfloor\sqrt{m}\rfloor + 1 + \sqrt{m}}{2} \\ &= \frac{\lceil\sqrt{m}\rceil^{\text{odd}} + \sqrt{m}}{2} = \mathcal{M}_{1/2} = \mathcal{M}. \end{aligned}$$

If $\lfloor\sqrt{m}\rfloor$ is odd and $\lceil\sqrt{m}\rceil$ is even, i.e, $\sqrt{m} = 2l + 1 + \lambda$ for some $l \in \mathbb{Z}$ and $0 < \lambda < 1$, we can say that

$$\left\lfloor \frac{\sqrt{m}-1}{2} \right\rfloor = \left\lfloor \frac{2l+1+\lambda-1}{2} \right\rfloor = \left\lfloor l + \frac{\lambda}{2} \right\rfloor = l = \frac{\lfloor\sqrt{m}\rfloor - 1}{2}$$

As previously, we can conclude that

$$\alpha_{-1,1} = 1 + \frac{\lfloor\sqrt{m}\rfloor - 1}{2} + \frac{1+\sqrt{m}}{2} = \frac{\lfloor\sqrt{m}\rfloor + 2 + \sqrt{m}}{2} = \frac{\lceil\sqrt{m}\rceil^{\text{odd}} + \sqrt{m}}{2} = \mathcal{M}_{1/2} = \mathcal{M}.$$

In both these cases, $\mathcal{M}$ is a semiconvergent of $\frac{\sqrt{m}-1}{2}$, thus it is indecomposable in $\mathbb{Q}(\sqrt{m})$. Moreover, the previous part does not depend on the fact whether we choose m, s or t. Thus we also know that $\mathcal{S}$ and $\mathcal{T}$ are indecomposable in the corresponding quadratic subfields.

Note that, in the same way, we can prove the indecomposability of $2\mathcal{M}-1$ in $\mathbb{Q}(\sqrt{m})$ if this element is totally positive. It is a simple matter to see that $u_1 \geq 2$ in this case and $2\mathcal{M}-1$ is the semiconvergent $\alpha_{-1,2}$.

Our next concern is to discuss the indecomposability of $\mathcal{M}$ in a general biquadratic field. Having indecomposability in $\mathbb{Q}(\sqrt{m})$, Theorem 1.2.4 gives us a partial result of this task for some special choices of m. First of all, let us focus on the integral basis (B1). If $m \equiv 3 \pmod 4$ and consequently $\mathcal{M} = \mathcal{M}_1$, Theorem 1.2.4 says that this element is indecomposable in the considered type of biquadratic fields. The same conclusion can be drawn for the integral bases (B2) and (B3) if $m \equiv 1 \pmod 4$, in which case $\mathcal{M} = \mathcal{M}_{1/2}$.

Therefore, it is natural to ask whether this element is indecomposable in the remaining cases of integral bases and m mod 4. Since $\mathcal{M}$ is a convergent of $\sqrt{m}$ or $\frac{\sqrt{m}-1}{2}$ only if $u_1 = 1$, Theorem 1.2.4 resolves this problem only in some special cases. However, as we will see in Proposition 1.4.9, the element $\mathcal{M}$ actually cannot decompose in any biquadratic field $\mathbb{Q}(\sqrt{m},\sqrt{s})$. For its proof, we first need to know how close the values of m, s and t can be. While there are infinitely many fields where $s-m=1$, the other differences cannot be arbitrarily small.

Lemma 1.4.8. *The following holds in every biquadratic field (given by the three square roots $\sqrt{m}$, $\sqrt{s}$, $\sqrt{t}$):*

1. *$\sqrt{t}-\sqrt{s} > \frac{1}{2}$; if the integral basis is of type (B4), then $\sqrt{t}-\sqrt{s} > 2$,*
2. *if $\sqrt{t}-\sqrt{s} \leq 1$, then m is even and $2\sqrt{m} > \sqrt{s}$,*
3. *$\sqrt{t}-\sqrt{m} > 1$; if the integral basis is of type (B4), then $\sqrt{t}-\sqrt{m} > 4$.*

Proof. All the three parts use the notation $m = s_0t_0$, $s = m_0t_0$, $t = m_0s_0$; recall that $m < s < t$ is then equivalent to $m_0 > s_0 > t_0$, and that in basis (B4) we have $m_0 \equiv s_0 \equiv t_0 \pmod 4$.

(1) We can compute

$$\sqrt{t}-\sqrt{s} = \sqrt{m_0}(\sqrt{s_0}-\sqrt{t_0}) = \frac{\sqrt{m_0}}{\sqrt{s_0}+\sqrt{t_0}}(s_0-t_0) > \frac{1}{2}(s_0-t_0). \tag{1.4.3}$$

The proof is concluded by observing that $s_0 - t_0 \geq 1$ and in the case (B4) $s_0 - t_0 \geq 4$.

(2) The inequality (1.4.3) implies that if $s_0 - t_0 \neq 1$, then $\sqrt{t}-\sqrt{s} > 1$, which contradicts our assumption. Therefore, $s_0 = t_0 + 1$, and it follows that $m = (t_0+1)t_0$ is even. To obtain the required inequality, we write

$$1 \geq \sqrt{t}-\sqrt{s} = \frac{\sqrt{m_0}}{\sqrt{s_0}+\sqrt{t_0}} \cdot 1 > \frac{\sqrt{m_0}}{2\sqrt{s_0}};$$

multiplying both sides by $2\sqrt{s_0t_0}$ yields the desired inequality $2\sqrt{s_0t_0} > \sqrt{m_0t_0}$.

(3) We start by proving $\sqrt{s_0}(\sqrt{s_0+1}-\sqrt{s_0-1}) > 1$: Since $x \mapsto \sqrt{x}$ is a strictly concave function, it follows that $\sqrt{s_0} > \frac{\sqrt{s_0+1}+\sqrt{s_0-1}}{2}$, which after multiplication by $(\sqrt{s_0+1}-\sqrt{s_0-1})$ yields

$$\sqrt{s_0}(\sqrt{s_0+1}-\sqrt{s_0-1}) > \frac{(s_0+1)-(s_0-1)}{2} = 1,$$

i.e., the desired inequality. Using this, we get

$$\sqrt{t}-\sqrt{m} = \sqrt{s_0}(\sqrt{m_0}-\sqrt{t_0}) \geq \sqrt{s_0}(\sqrt{s_0+1}-\sqrt{s_0-1}) > 1.$$

To prove the stronger inequality for (B4), the auxiliary inequality is $\sqrt{s_0}(\sqrt{s_0+4}-\sqrt{s_0-4}) > 4$, otherwise the proof does not change. □

On a side note, all the proven inequalities are the strongest possible, as can be seen by considering a sequence of fields with $m_0 = t_0 + 2$ and $s_0 = t_0 + 1$ (since m_0, s_0, t_0 are square-free, and hence not divisible by 4, $t_0 \equiv 1 \pmod 4$ follows) or, in the case of (B4), $m_0 = t_0 + 8$ and $s_0 = t_0 + 4$.

Now we proceed to the proof of the indecomposability of $\mathcal{M}$ in biquadratic fields. Note that the following proposition, aside from playing a key role in the proof of Theorem 1.1.1, also forms a part of Theorem 1.1.3.

Proposition 1.4.9. *The element $\mathcal{M}$ is indecomposable in $\mathbb{Q}(\sqrt{m}, \sqrt{s})$.*

Proof. Since $\mathcal{M}$ is indecomposable in the quadratic subfield $\mathbb{Q}(\sqrt{m})$, we do not have to prove its indecomposability in any of the cases where it is guaranteed by Theorem 1.2.4. In particular, it is indecomposable if $m \equiv 1 \pmod 4$ and the integral basis is not (B4).

Assume first that $\mathcal{M} = \mathcal{M}_{1/2}$. If it is decomposable, then the integral basis is (B4). Suppose that $\mathcal{M}$ decomposes as

$$\mathcal{M}_{1/2} = \frac{\lceil\sqrt{m}\rceil^{\text{odd}} + \sqrt{m}}{2} = \underbrace{\frac{a}{4} + \frac{b}{4}\sqrt{m} + \frac{c}{4}\sqrt{s} + \frac{d}{4}\sqrt{t}}_{\gamma} + \underbrace{\frac{a'}{4} + \frac{b'}{4}\sqrt{m} - \frac{c}{4}\sqrt{s} - \frac{d}{4}\sqrt{t}}_{\gamma'}$$

where $\gamma, \gamma' \in \mathcal{O}_K^+$ (in particular, $a, a', b, b', c, d \in \mathbb{Z}$). By Lemma 1.2.3 we have $\frac{a}{4} > \left|\frac{d}{4}\right| \sqrt{t}$ and $\frac{a'}{4} > \left|\frac{-d}{4}\right| \sqrt{t}$; putting these two inequalities together, we obtain

$$\left|\frac{d}{4}\right|\sqrt{t} < \min\left\{\frac{a}{4}, \frac{a'}{4}\right\} \leq \frac{1}{2}\frac{a + a'}{4} = \frac{\lceil\sqrt{m}\rceil^{\text{odd}}}{4},$$

yielding $|d|\sqrt{t} < \lceil\sqrt{m}\rceil^{\text{odd}} < \sqrt{m} + 2$. By part (3) of Lemma 1.4.8, $d = 0$.

Once we know that $d = 0$, we exploit the total positivity of γ and γ' by choosing one specific embedding to obtain the inequalities

$$\frac{a}{4} - \frac{b}{4}\sqrt{m} - \frac{|c|}{4}\sqrt{s} > 0 \quad \text{and} \quad \frac{a'}{4} - \frac{b'}{4}\sqrt{m} - \frac{|c|}{4}\sqrt{s} > 0.$$

Putting them together, we get

$$\left|\frac{c}{4}\right|\sqrt{s} < \min\left\{\frac{a - b\sqrt{m}}{4}, \frac{a' - b'\sqrt{m}}{4}\right\} \leq \frac{1}{2}\frac{a + a' - (b + b')\sqrt{m}}{4} = \frac{1}{2}\frac{\lceil\sqrt{m}\rceil^{\text{odd}} - \sqrt{m}}{2} < \frac{1}{2},$$

which clearly cannot hold for $c \neq 0$. Thus, we have $c = 0$ and $d = 0$, and hence γ, γ' are elements of $\mathbb{Q}(\sqrt{m}) \cap \mathcal{O}_K^+ = \mathcal{O}^+_{\mathbb{Q}(\sqrt{m})}$; however, we already know that $\mathcal{M}$ is indecomposable in $\mathbb{Q}(\sqrt{m})$. That proves that $\mathcal{M}_{1/2}$ is indecomposable in any biquadratic field.

Now we will handle the case when $\mathcal{M} = \mathcal{M}_1$. The proof is very similar. Start by supposing that

$$\mathcal{M}_1 = \lceil\sqrt{m}\rceil + \sqrt{m} = \underbrace{\frac{a}{2} + \frac{b}{2}\sqrt{m} + \frac{c}{2}\sqrt{s} + \frac{d}{2}\sqrt{t}}_{\gamma} + \underbrace{\frac{a'}{2} + \frac{b'}{2}\sqrt{m} - \frac{c}{2}\sqrt{s} - \frac{d}{2}\sqrt{t}}_{\gamma'}$$

where again $\gamma, \gamma' \in \mathcal{O}_K^+$. We use Lemma 1.2.3 in the same manner as above to obtain

$$\left|\frac{d}{2}\right|\sqrt{t} < \min\left\{\frac{a}{2}, \frac{a'}{2}\right\} \leq \frac{1}{2}\frac{a + a'}{2} = \frac{\lceil\sqrt{m}\rceil}{2},$$

and hence $|d|\sqrt{t} < \sqrt{m} + 1$; similarly as before, invoking part (3) of Lemma 1.4.8 yields $d = 0$.

Again, we use suitable embeddings of γ and γ' and put the resulting inequalities together:

$$\left|\frac{c}{2}\right|\sqrt{s} < \min\left\{\frac{a-b\sqrt{m}}{2}, \frac{a'-b'\sqrt{m}}{2}\right\} \leq \frac{1}{2}\frac{a+a'-(b+b')\sqrt{m}}{2} = \frac{1}{2}(\lceil\sqrt{m}\rceil - \sqrt{m}) < \frac{1}{2}.$$

This clearly implies $c = 0$. But then necessarily $\gamma, \gamma' \in \mathcal{O}^+_{\mathbb{Q}(\sqrt{m})}$, which contradicts the indecomposability of $\mathcal{M}$ in the quadratic field $\mathbb{Q}(\sqrt{m})$. □

In the following proposition, we prove the indecomposability of $\mathcal{S}$; this result, together with the previous proposition, concludes part (1) of Theorem 1.1.3. The main techniques of the proof are very similar as in the case of $\mathcal{M}$; the only problem is that the inequality $\sqrt{t} - \sqrt{s} > 1$ is not necessarily satisfied: Not only are there fields where $\sqrt{t} - \sqrt{s}$ is very close to 0.5, but in some of them $\lceil\sqrt{t}\rceil = \lceil\sqrt{s}\rceil$ actually happens. An example is the field $\mathbb{Q}(\sqrt{1806}, \sqrt{2814})$, where $t_0 = 42$, $s_0 = 43$ and $m_0 = 67$. However, in every such field, part (2) of Lemma 1.4.8 applies, which we will exploit significantly.

Proposition 1.4.10. *The element $\mathcal{S}$ is indecomposable in $\mathbb{Q}(\sqrt{m}, \sqrt{s})$.*

Proof. As in the case with $\mathcal{M}$, the element $\mathcal{S}$ is indecomposable in $\mathbb{Q}(\sqrt{s})$, so by Theorem 1.2.4 it is indecomposable if $s \equiv 1 \pmod 4$ (i.e., $\mathcal{S} = \mathcal{S}_{1/2}$) and the integral basis is not (B4), and also if $s \not\equiv 1 \pmod 4$ (i.e., $\mathcal{S} = \mathcal{S}_1$) and $s = q$.

Writing

$$\mathcal{S}_{1/2} = \frac{\lceil\sqrt{s}\rceil^{\text{odd}} + \sqrt{s}}{2} = \underbrace{\frac{a}{4} + \frac{b}{4}\sqrt{m} + \frac{c}{4}\sqrt{s} + \frac{d}{4}\sqrt{t}}_{\gamma} + \underbrace{\frac{a'}{4} - \frac{b}{4}\sqrt{m} + \frac{c'}{4}\sqrt{s} - \frac{d}{4}\sqrt{t}}_{\gamma'},$$

the case of $\mathcal{S} = \mathcal{S}_{1/2}$ in the integral basis (B4) can be treated in the same manner as $\mathcal{M} = \mathcal{M}_{1/2}$ in the proof of Proposition 1.4.9, with the minor difference that part (1) of Lemma 1.4.8 is used instead of part (3).

Let us turn our attention to the cases when $\mathcal{S} = \mathcal{S}_1$. We write

$$\mathcal{S}_1 = \lceil\sqrt{s}\rceil + \sqrt{s} = \underbrace{\frac{a}{2} + \frac{b}{2}\sqrt{m} + \frac{c}{2}\sqrt{s} + \frac{d}{2}\sqrt{t}}_{\gamma} + \underbrace{\frac{a'}{2} - \frac{b}{2}\sqrt{m} + \frac{c'}{2}\sqrt{s} - \frac{d}{2}\sqrt{t}}_{\gamma'}, \tag{1.4.4}$$

and the same approach as before yields

$$\left|\frac{d}{2}\right|\sqrt{t} < \min\left\{\frac{a}{2}, \frac{a'}{2}\right\} \leq \frac{1}{2}\frac{a+a'}{2} = \frac{\lceil\sqrt{s}\rceil}{2}, \tag{1.4.5}$$

implying $|d|\sqrt{t} < \lceil\sqrt{s}\rceil < \sqrt{s} + 1$. It is clear that $|d| \geq 2$ is impossible; however, $|d| = 1$ is not excluded by this inequality.

Suppose $|d| = 1$. If $a \neq a'$, then the inequality (1.4.5) can be improved to

$$\frac{1}{2}\sqrt{t} = \left|\frac{d}{2}\right|\sqrt{t} < \min\left\{\frac{a}{2}, \frac{a'}{2}\right\} \leq \frac{\lceil\sqrt{s}\rceil - 1}{2},$$

but $\sqrt{t} < \lceil\sqrt{s}\rceil - 1 < \sqrt{s}$ clearly cannot happen. Thus $a = a' = \frac{1}{2}\lceil\sqrt{s}\rceil$. Consequently, the inequalities $\frac{1}{2}\lceil\sqrt{s}\rceil > \left|\frac{c}{2}\right|\sqrt{s}$ and $\frac{1}{2}\lceil\sqrt{s}\rceil > \left|\frac{c'}{2}\right|\sqrt{s}$ together with the condition $c + c' = 2$ ensure that $c = c' = 1$. All in all, the assumption $d \neq 0$ leads us to a decomposition of the form

$$\mathcal{S}_1 = \lceil\sqrt{s}\rceil + \sqrt{s} = \underbrace{\frac{\lceil\sqrt{s}\rceil}{2} + \frac{b}{2}\sqrt{m} + \frac{1}{2}\sqrt{s} + \frac{1}{2}\sqrt{t}}_{\gamma} + \underbrace{\frac{\lceil\sqrt{s}\rceil}{2} - \frac{b}{2}\sqrt{m} + \frac{1}{2}\sqrt{s} - \frac{1}{2}\sqrt{t}}_{\gamma'}.$$

On a side note, γ and γ' differ only by an embedding, so total positivity of one implies total positivity of the other; therefore, we shall focus only on γ. Obviously $b > 0$; otherwise in one embedding all three signs would be negative, but the inequality $\frac{\lceil\sqrt{s}\rceil-\sqrt{s}-\sqrt{t}}{2} > 0$ clearly cannot hold. On the other hand, if we suppose $b \geq 3$, then by Lemma 1.2.3 we have

$$\frac{\lceil\sqrt{s}\rceil}{2} > \Big|\frac{b}{2}\Big|\sqrt{m} \geq \frac{3}{2}\sqrt{m}.$$

Recall that (1.4.5) implies $\sqrt{t} < \sqrt{s} + 1$, hence part (2) of Lemma 1.4.8 guarantees that m is even and $2\sqrt{m} > \sqrt{s}$. But this would yield $2\lceil\sqrt{s}\rceil > 3\sqrt{s}$; however, this inequality never holds, meaning that either $b = 1$ or $b = 2$.

If $b = 2$, then the coefficient in front of $\sqrt{m}$ is an integer, whereas in front of $\sqrt{s}$ and $\sqrt{t}$ are half-integers. Comparing this with bases (B1)–(B3), this must mean that $m = q$. Nonetheless, we also know that m is even, which is a contradiction.

If $b = 1$, then $\gamma = \frac{1}{2}\left(\lceil\sqrt{s}\rceil + \sqrt{m} + \sqrt{s} + \sqrt{t}\right)$ must be totally positive. However, that would mean $(\lceil\sqrt{s}\rceil - \sqrt{s}) - (\sqrt{t} - \sqrt{m}) > 0$, which is impossible since clearly $\lceil\sqrt{s}\rceil - \sqrt{s} < 1$, whereas $\sqrt{t} - \sqrt{m} > 1$ by Lemma 1.4.8(3).

So, although it was much more work than before, we have showed that $d = 0$. After that, we return to the usual strategy:

$$\mathcal{S}_1 = \lceil\sqrt{s}\rceil + \sqrt{s} = \underbrace{\frac{a}{2} + \frac{b}{2}\sqrt{m} + \frac{c}{2}\sqrt{s}}_{\gamma} + \underbrace{\frac{a'}{2} - \frac{b}{2}\sqrt{m} + \frac{c'}{2}\sqrt{s}}_{\gamma'}.$$

Again, on each of γ and γ' we apply one specific embedding, and putting the obtained inequalities together, we get

$$\Big|\frac{b}{2}\Big|\sqrt{m} < \min\Big\{\frac{a - c\sqrt{s}}{2}, \frac{a' - c'\sqrt{s}}{2}\Big\} \leq \frac{1}{2}\frac{a + a' - (c + c')\sqrt{s}}{2} = \frac{1}{2}(\lceil\sqrt{s}\rceil - \sqrt{s}) < \frac{1}{2},$$

which clearly implies $b = 0$. Since $\mathcal{S}$ is indecomposable in $\mathbb{Q}(\sqrt{s})$, we have proven the indecomposability of $\mathcal{S} = \mathcal{S}_1$ in any biquadratic field. □

Let us foreshadow that in the proof of Theorem 1.1.1, we use the indecomposability of $\mathcal{S}$ only in a few cases where m is a prime; in such a situation (and more generally if m and s are coprime) the proof of Proposition 1.4.10 becomes easier thanks to $t = ms$.

The following statement is interesting on its own, and forms part (2) of Theorem 1.1.3. But for the proof of Theorem 1.1.1 we need only the case when $m = 85$ (see Subsection 1.6.7), where it can also be checked directly.

Proposition 1.4.11. *If $2\mathcal{M} - 1$ is totally positive, then it is indecomposable in $\mathbb{Q}(\sqrt{m}, \sqrt{s})$.*

Proof. The proof is analogous to the ones of Propositions 1.4.9 and 1.4.10. The only tricky part is to show that if $\mathcal{M} = \mathcal{M}_1$, the decomposition

$$2\mathcal{M} - 1 = \left(\left(\lceil\sqrt{m}\rceil - \frac{1}{2}\right) + \sqrt{m} + \sqrt{s} + \frac{\sqrt{t}}{2}\right) + \left(\left(\lceil\sqrt{m}\rceil - \frac{1}{2}\right) + \sqrt{m} - \sqrt{s} - \frac{\sqrt{t}}{2}\right)$$

is not valid since $(\lceil\sqrt{m}\rceil - \frac{1}{2}) + \sqrt{m} + \sqrt{s} + \frac{\sqrt{t}}{2}$ is not a totally positive integer. To prove that, the following claim is used: If $t \equiv 1 \pmod 4$ and $\sqrt{s} - \sqrt{m} \leq \frac{1}{2}$, then $\sqrt{t} > 4\sqrt{m}$. This claim is proved similarly to Lemma 1.4.8(2). □

Remark 1.4.12. If we are interested in indecomposability of $\mathcal{T}$, the only part of Theorem 1.2.4 which is useful is the one claiming that in bases (B1), (B2) and (B3), all indecomposable integers from $\mathbb{Q}(\sqrt{q})$ remain indecomposable. Thus if $t = q$ and the integral basis is not (B4) – these conditions can be reformulated as $m \equiv s \not\equiv 1 \pmod 4$ – then $\mathcal{T}$ is indecomposable. On the other hand, Example 1.4.7 shows that sometimes $\mathcal{T}$ does decompose. To characterize the cases when that happens could be a direction of a further examination.

1.4.4 Some useful properties of $\mathcal{M}$ and $\mathcal{S}$

In the study of ternary forms over $\mathcal{O}_K$, it is also useful to know whether $n\mathcal{M}$ is a square. As we will see in Corollary 1.4.14, for $n \leq 5$, this occurs only for few cases of m and for some specific biquadratic fields. We will also analyze the same question for $\mathcal{S}$ and $2\mathcal{S}$. In order to use Lemma 1.4.1(1), we divide the question into two separate problems: First, we prove that the considered element is not a square in the appropriate quadratic subfield, and then we examine it in the biquadratic field. This approach yields the following:

Lemma 1.4.13. *Let $n \leq 5$ be a positive integer. Then*

1. *$n\mathcal{M}_1$ is a square in $\mathbb{Q}(\sqrt{m})$ if and only if*

   - *$n = 2$ and $m \in \{3, 5\}$.*

   $n\mathcal{M}_{1/2}$ is a square in $\mathbb{Q}(\sqrt{m})$ if and only if

   - *$n = 1$ or $n = 4$ and $m = 5$;*
   - *$n = 3$ and $m \in \{21, 33\}$,*
   - *$n = 5$ and $m \in \{5, 65, 85\}$.*

2. *Let $K = \mathbb{Q}(\sqrt{m}, \sqrt{s})$. Then*
   $n\mathcal{M}_1$ is a square in K but not in $\mathbb{Q}(\sqrt{m})$ if and only if

   - *$n = 3$, $m = 5$ and $K = \mathbb{Q}(\sqrt{5}, \sqrt{6})$,*
   - *$n = 5$ and either $m = 3$ and $K = \mathbb{Q}(\sqrt{3}, \sqrt{10})$, or $m = 21$ and $K = \mathbb{Q}(\sqrt{21}, \sqrt{30})$;*

   $n\mathcal{M}_{1/2}$ can only be a square in K if it is a square in $\mathbb{Q}(\sqrt{m})$.

Remark. Recall that $\mathcal{M}_1$ is defined for all square-free values of m, but $\mathcal{M}_{1/2}$ is defined only for those square-free m which satisfy $m \equiv 1 \pmod 4$; thus, the above lemma does not cover $n\mathcal{M}_{1/2}$ for $m \not\equiv 1 \pmod 4$ even though it might be an algebraic integer. Moreover, note that in (1), we do not use the fact that $m < s < t$.

Proof. (1) First, consider the odd multiples of $\mathcal{M}_1$; let $a, b \in \mathbb{Z}$ be such that $a \equiv b \pmod 2$ and

$$\left(\frac{a + b\sqrt{m}}{2}\right)^2 = (2k+1)\left\lceil\sqrt{m}\right\rceil + (2k+1)\sqrt{m}$$

for some $k \in \mathbb{Z}$, $k \geq 0$, and square-free $m \in \mathbb{Z}$, $m > 1$. Comparing the coefficients in front of $\sqrt{m}$ gives the equality $2ab = 4(2k+1)$, which cannot be satisfied with $a \equiv b \pmod 2$. Thus, $(2k+1)\mathcal{M}_1$ is not a square in $\mathbb{Q}(\sqrt{m})$ for any k and any m.

Observe that $4\mathcal{M}_1$ is a square if and only if $\mathcal{M}_1$ is a square (more generaly, for $k, l \in \mathbb{Z}$, it holds that $k^2 l\mathcal{M}$ is a square if and only if $l\mathcal{M}$ is a square). Thus, in the case of $n\mathcal{M}_1$, it only remains to deal with $n = 2$. First note that no halves can appear in the hypothetical square root of $2\mathcal{M}_1$. Hence, let $a, b \in \mathbb{Z}$ be such that

$$(a + b\sqrt{m})^2 = 2\left(\left\lceil\sqrt{m}\right\rceil + \sqrt{m}\right). \tag{1.4.6}$$

Comparing the coefficients in front of $\sqrt{m}$, we see that necessarily $a = b = \pm 1$. Then the rest of the equality yields $1 + m = 2\left\lceil\sqrt{m}\right\rceil$, which is satisfied only for $m \leq 5$. Evaluating (1.4.6) at $a = b = \pm 1$ and $m \in \{2, 3, 5\}$ gives that $2\mathcal{M}_1$ is a square if and only if $m \in \{3, 5\}$.

For the multiples of $\mathcal{M}_{1/2}$, consider $n \in \mathbb{Z}$, $n > 0$, and let $a, b \in \mathbb{Z}$ be such that $a \equiv b \pmod 2$ and

$$\left(\frac{a + b\sqrt{m}}{2}\right)^2 = n\frac{\left\lceil\sqrt{m}\right\rceil^{\text{odd}} + \sqrt{m}}{2}; \tag{1.4.7}$$

note that we can assume without loss of generality $a, b > 0$. Taking the conjugates gives

$$(a - b\sqrt{m})^2 = 2n(\lceil\sqrt{m}\rceil^{\text{odd}} - \sqrt{m}) < 4n,$$

i.e., $|a - b\sqrt{m}| < 2\sqrt{n}$, which produces the upper bound

$$m < \left(\frac{2\sqrt{n} + a}{b}\right)^2. \tag{1.4.8}$$

Comparing the coefficients in front of $\sqrt{m}$ in (1.4.7) yields $n = ab$, which gives us for a fixed value of n only a few possibilities for a, b. It is just a matter of a simple computation to check which m's satisfy both (1.4.8) and (1.4.7).

(2) Let us start with a simple observation: For a given $m_0 \in \mathbb{N}$, there are only finitely many biquadratic fields K such that $\gcd(s, t) = m_0$. This becomes obvious if we write $s = m_0 t_0$, $t = m_0 s_0$, $m = s_0 t_0$, since the inequality $m < s < t$ translates into $m_0 > s_0 > t_0$. Thus every field with $\gcd(s, t) = m_0$ is determined by the choice of s_0 and t_0, which are square-free numbers ($t_0 = 1$ is possible) smaller than m_0 such that m_0, s_0, t_0 are pairwise coprime.

Suppose now that $n\mathcal{M}_1 = n\lceil\sqrt{m}\rceil + n\sqrt{m}$ is not a square in $\mathbb{Q}(\sqrt{m})$ but becomes a square in K. Invoking Lemma 1.4.1(1), we know that this means $\left(\frac{c\sqrt{s}+d\sqrt{t}}{2}\right)^2 = n\mathcal{M}_1$ for some $c, d \in \mathbb{Z}$. Comparing the coefficients in front of $\sqrt{m}$ and writing m_0 for $\gcd(s, t)$, we obtain $\frac{2cdm_0}{4} = n$, i.e., $cdm_0 = 2n$. Thus m_0 is some divisor of $2n$, which gives us only a few concrete fields $\mathbb{Q}(\sqrt{m}, \sqrt{s})$ which have to be checked. Through realizing that $c \equiv d \equiv n \pmod 2$, one can reduce the number of possibilities for c, d, and consequently also for m_0, significantly. The few remaining cases can be checked directly, concluding this part of the proof.

For $n\mathcal{M}_{1/2}$, we proceed analogously: Again, we write m_0 for $\gcd(s, t)$; then the requirement $\left(\frac{c\sqrt{s}+d\sqrt{t}}{2}\right)^2 = n\mathcal{M}_{1/2}$ leads to $cdm_0 = n$, thus a simple computation shows that $n\mathcal{M}_{1/2}$ never becomes a square for $n = 1, 2, 4$. Furthermore, for $n = 3$ the only possible field is $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ with $m_0 = 3$; and for $n = 5$, we have $m_0 = 5$, meaning that both s_0 and t_0 are chosen from $\{1, 2, 3\}$. However, in all the resulting fields we have $m \not\equiv 1 \pmod 4$, so there is no $\mathcal{M}_{1/2}$ and considering $n\mathcal{M}_{1/2}$ is utterly irrelevant. □

In most situations, we are interested whether $n\mathcal{M}$ (equal either to $n\mathcal{M}_1$ or to $n\mathcal{M}_{1/2}$ according to the value of m) is a square without distinguishing between quadratic and biquadratic fields.

Corollary 1.4.14. *In a biquadratic field K, the following holds:*

1. *$\mathcal{M}$ and $4\mathcal{M}$ are squares if and only if $m = 5$,*
2. *$2\mathcal{M}$ is a square if and only if $m = 3$,*
3. *$3\mathcal{M}$ is a square if and only if $m \in \{21, 33\}$,*
4. *$5\mathcal{M}$ is a square if and only if $m \in \{5, 65, 85\}$ or $K = \mathbb{Q}(\sqrt{3}, \sqrt{10})$.*

The following lemma shows that $\mathcal{S}$ is almost never a square. Note that it does not say anything about $\mathcal{S}_1$ if $s \equiv 1 \pmod 4$, since then $\mathcal{S} = \mathcal{S}_{1/2}$.

Lemma 1.4.15. *The element $\mathcal{S} \in \mathcal{O}_K$ is a square only in the fields $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, $\mathbb{Q}(\sqrt{2}, \sqrt{5})$ and $\mathbb{Q}(\sqrt{3}, \sqrt{5})$; the element $2\mathcal{S}$ is a square only in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $\mathbb{Q}(\sqrt{2}, \sqrt{5})$. More specifically:*

1. *If $\mathcal{S}$ is nonsquare in $\mathbb{Q}(\sqrt{s})$, then it is nonsquare in the biquadratic field $\mathbb{Q}(\sqrt{m}, \sqrt{s})$ with the exception of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ where $\mathcal{S} = 2 + \sqrt{3} = \left(\frac{\sqrt{2}+\sqrt{6}}{2}\right)^2$.*

2. *If $2\mathcal{S}$ is nonsquare in $\mathbb{Q}(\sqrt{s})$, then it is nonsquare in the biquadratic field $\mathbb{Q}(\sqrt{m},\sqrt{s})$ with the exception of $\mathbb{Q}(\sqrt{2},\sqrt{5})$ where $2\mathcal{S}=3+\sqrt{5}=\left(\frac{\sqrt{2}+\sqrt{10}}{2}\right)^2$.*

Proof. If $\mathcal{S}$ (resp. $2\mathcal{S}$) is a square already in $\mathbb{Q}(\sqrt{s})$, then by the first part of Lemma 1.4.13 and the subsequent remark we get $s=5$ (resp. $s=3$). Thus it remains to prove the statements (1) and (2).

First we prove that if $\mathcal{S}$ or $2\mathcal{S}$ becomes a square in $\mathbb{Q}(\sqrt{m},\sqrt{s})$, then $m=2$: Observe that neither $\mathcal{S}$ nor $2\mathcal{S}$ has odd integer divisors, so if either of them is a square in $\mathbb{Q}(\sqrt{m},\sqrt{s})$, Corollary 1.4.2 gives $\gcd(m,t)=1$ or 2. The first case is clearly impossible since then $s=mt$ contradicts $m<s<t$. If $\gcd(m,t)=2$, then the required inequality $s=\frac{mt}{4}<t$ together with $2\mid m$ yields $m=2$.

So it remains to examine the field $\mathbb{Q}(\sqrt{2},\sqrt{s})$. We shall make a general observation: If a nonsquare $\alpha\in\mathcal{O}_{\mathbb{Q}(\sqrt{s})}$ becomes a square in $\mathbb{Q}(\sqrt{2},\sqrt{s})$, then 2α is a square in $\mathbb{Q}(\sqrt{s})$. Indeed, from Lemma 1.4.1(1) we get $\alpha=\left(\frac{a\sqrt{2}+b\sqrt{2s}}{2}\right)^2$, which can be rewritten as $2\alpha=(a+b\sqrt{s})^2$. This proves the observation.

In $\mathbb{Q}(\sqrt{s})$, the number $2\mathcal{S}$ is a square only for $s=3$ and $4\mathcal{S}$ only for $s=5$ (by Lemma 1.4.13 and the subsequent Remark). Thus, our observation yields that $\mathcal{S}$ can become a square only in $\mathbb{Q}(\sqrt{2},\sqrt{3})$ and $2\mathcal{S}$ only in $\mathbb{Q}(\sqrt{2},\sqrt{5})$; indeed, it is the case both for $\mathcal{S}$ and $2\mathcal{S}$. □

Our next concern is to study additive decompositions of $2\mathcal{M}$. In particular, we are interested in the question how $2\mathcal{M}$ can be expressed as a sum of a square of an algebraic integer and of a totally positive element. In some cases, $2\mathcal{M}-1$ happens to be totally positive; then it is possible for $2\mathcal{M}$ to be written as $(2\mathcal{M}-1)+1$. Therefore, in such a situation, we need to know whether $2\mathcal{M}-1$ is a square.

Lemma 1.4.16. *The element $2\mathcal{M}-1$ is a square if and only if $m=2$.*

Proof. First of all, let us note that when $\mathcal{M}=\mathcal{M}_{1/2}$, then either $2\mathcal{M}-1$ is not totally positive and thus not a square, or $2\mathcal{M}-1=\mathcal{M}_1$, which is not a square in any case of $m\equiv 1 \pmod 4$, see Lemma 1.4.13.

Let us now turn to $\mathcal{M}=\mathcal{M}_1$. First, suppose that $2\mathcal{M}_1-1$ is a square in the subfield $\mathbb{Q}(\sqrt{m})$, i.e., $2\mathcal{M}_1-1=(a+b\sqrt{m})^2$ for some $a,b\in\mathbb{Z}$. Then we have

$$2\mathcal{M}_1-1=2\lceil\sqrt{m}\rceil-1+2\sqrt{m}=a^2+b^2m+2ab\sqrt{m}.$$

It follows that $ab=1$; the resulting equality $2\lceil\sqrt{m}\rceil-1=m+1$ holds for $m=2$, whereas for $m\geq 3$ the right-hand side is too large.

Finally we prove that if $2\mathcal{M}-1$ was not a square in $\mathbb{Q}(\sqrt{m})$, it does not become one in K either: Since $2\mathcal{M}-1$ has no nontrivial odd divisor, using Corollary 1.4.2 we see that $2\mathcal{M}-1$ can become a square only in a field with $\gcd(s,t)=1$ or 2; however, there are no such fields. □

Lemma 1.4.17. *Let $2\mathcal{M}=\omega^2+\gamma$ for some $\omega\in\mathcal{O}_K$ and $\gamma\in\mathcal{O}_K^+$. Then either $\omega^2=0$ or $\omega^2=1$ with the exception of $m\in\{2,3,5\}$. In particular, if $m\notin\{2,3,5\}$, then the element $2\mathcal{M}$ cannot be written as a sum of two squares in $\mathcal{O}_K$.*

Remark. Note that $2\mathcal{M}_{1/2}=1+\gamma$ is possible if and only if $\lceil\sqrt{m}\rceil$ is even, and $2\mathcal{M}_1=1+\gamma$ is possible if and only if $\lceil\sqrt{m}\rceil-\sqrt{m}\geq\frac{1}{2}$.

Proof. In the first part of the proof, our strategy is to study all decompositions of the form $2\mathcal{M}=\gamma'+\gamma$ with $\gamma',\gamma\in\mathcal{O}_K^+\cup\{0\}$, ignoring the condition $\gamma'=\omega^2$.

Supposing first that $\gamma',\gamma\in\mathbb{Q}(\sqrt{m})$, it is easy to check that the only decompositions of $2\mathcal{M}$ are $0+2\mathcal{M}$, $\mathcal{M}+\mathcal{M}$ and possibly $1+(2\mathcal{M}-1)$. From them, 0 and 1 are squares, whereas $\mathcal{M}$ is a square only for $m=5$, $2\mathcal{M}$ only for $m=3$ (both according to Lemma 1.4.13) and $2\mathcal{M}-1$ only for $m=2$ (Lemma 1.4.16).

The next step is to show that $2\mathcal{M}$ does not admit any decomposition where exactly one of the coefficients in front of $\sqrt{s}$ and $\sqrt{t}$ is nonzero. That follows quite easily since it is possible to choose an embedding where all the nonzero coefficients in front of square roots have negative sign.

Only now we start exploiting the fact that γ' is a square: It remains to prove that $\omega^2 \preccurlyeq 2\mathcal{M}$ is never satisfied by an $\gamma' = \omega^2$ such that all coefficients in ω^2 are nonzero.

Let us first focus on $\mathcal{M}_1$. It follows quite easily that if all four coefficients in ω^2 are nonzero, then at least three coefficients in $\omega = \frac{1}{2}(a + b\sqrt{m} + c\sqrt{s} + d\sqrt{t})$ are nonzero. By comparing traces of $2\mathcal{M}$ and ω^2, we get $\frac{1}{4}(a^2 + b^2 m + c^2 s + d^2 t) \leq 2\lceil\sqrt{m}\rceil$, which implies

$$1 + m + s \leq 8\lceil\sqrt{m}\rceil\,. \tag{1.4.9}$$

From this, we see that $1 + m + (m+1) \leq 8\lceil\sqrt{m}\rceil$, which holds only for $m \leq 19$; moreover, for any fixed value of m, (1.4.9) yields an upper bound for s (e.g., for $m = 19$ we obtain $20 + s \leq 40$, which has no relevant solutions since $s = 20$ is not square-free). In this way we obtain only a few fields which have to be handled by direct computations.

If $\mathcal{M} = \mathcal{M}_{1/2}$ and the basis is not (B4), the same technique provides a stronger result: The inequality obtained by comparing traces is in this case $1 + m + s \leq 4\lceil\sqrt{m}\rceil^{\mathrm{odd}}$; however, the only $m \equiv 1 \pmod 4$ satisfying $2 + 2m \leq 4\lceil\sqrt{m}\rceil^{\mathrm{odd}}$ is $m = 5$.

If the basis is (B4) but, nevertheless, there are no quarter-integer coefficients in ω, then the inequalities from the previous paragraph still apply. If quarter-integers are involved, we obtain a weaker inequality $\frac{1}{16}(a^2 + b^2 m + c^2 s + d^2 t) \leq \lceil\sqrt{m}\rceil^{\mathrm{odd}}$; however, in that case all of a, b, c, d must be odd (in particular nonzero). Thus we get $1 + m + s + t \leq 16\lceil\sqrt{m}\rceil^{\mathrm{odd}}$; this yields $1 + m + (m+4) + (m+8) \leq 16\lceil\sqrt{m}\rceil^{\mathrm{odd}}$, which is actually satisfied only for $m \leq 33$; together with the condition $m \equiv 1 \pmod 4$ we only have to consider $m = 13$, $m = 17$ and $m = 21$ with $\lceil\sqrt{m}\rceil^{\mathrm{odd}} = 5$ and $m = 29$ and $m = 33$ with $\lceil\sqrt{m}\rceil^{\mathrm{odd}} = 7$ (ignoring $m = 5$). However, in the former three cases, the inequality $1 + m + s + t \leq 16 \cdot 5$ turns out to never hold for a field where $s \equiv t \equiv 1 \pmod 4$; in the latter two, $1 + m + s + t \leq 16 \cdot 7$ has no solution where $m = 29$ or $m = 33$. □

1.4.5 Unary forms

When looking at representability of an element by a diagonal form, it is useful to have some information on the possible representations of this element by the unary subforms. In particular, if the considered element is a rational prime p, we need to understand expressions of the form $p = \gamma\alpha^2$ for some $\alpha \in \mathcal{O}_K$ and $\gamma \in \mathcal{O}_K^+$. But the following proposition about biquadratic divisors of rational primes can be interesting on its own.

Proposition 1.4.18. *Let p be a rational prime number divisible in a biquadratic field K by α^2 for an element $\alpha \in \mathcal{O}_K \setminus \mathcal{U}_K$. Then $p = \mu\beta^2$ for some $\mu \in \mathcal{U}_K^+$ and $\beta \in \mathcal{O}_K$.*

Proof. Recall that for a biquadratic number field K, the extension $K/\mathbb{Q}$ is Galois; hence, invoking the so-called efg-theorem, we can write

$$p\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{p}_i^e \tag{1.4.10}$$

for some prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_g \subseteq \mathcal{O}_K$ with $f = [\mathcal{O}_K/\mathfrak{p}_i : \mathbb{Z}/p\mathbb{Z}]$ and $efg = 4$. Let $(\alpha^2) = \mathfrak{q}_1^2 \cdots \mathfrak{q}_t^2$ for some prime ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_t \subseteq \mathcal{O}_K$ (not necessary pairwise different). By the assumption, $(\alpha^2) \mid p\mathcal{O}_K$; therefore, $e \geq 2$. Using that $efg = 4$, we have only three possibilities for the values of e, f, g.

First, assume that $e = g = 2$ and $f = 1$. Then either $(\alpha^2) = \mathfrak{p}_1^2\mathfrak{p}_2^2 = p\mathcal{O}_K$, or $(\alpha^2) = \mathfrak{p}_1^2$ (without loss of generality). In the first case, p and α^2 differ by a unit $\mu \in \mathcal{U}_K$, and since both

of p and α^2 are totally positive, the unit μ has to be totally positive as well. In the latter case it follows that the prime ideal $\mathfrak{p}_1$ is principal; then $\mathfrak{p}_2 = \sigma(\mathfrak{p}_1)$ for some $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, and thus $\mathfrak{p}_2 = (\sigma(\alpha))$. Hence $p\mathcal{O}_K = (\alpha\sigma(\alpha))^2$, and $p = \mu\alpha^2\sigma(\alpha)^2$ for some $\mu \in \mathcal{U}_K^+$ follows.

Second, consider the case $e = f = 2$ and $g = 1$. That means that $p\mathcal{O}_K = \mathfrak{p}^2$ for some prime ideal $\mathfrak{p}$; thus necessarily $(\alpha^2) = \mathfrak{p}^2$, and it follows that $p = \mu\alpha^2$ for some $\mu \in \mathcal{U}_K^+$.

Finally, suppose that $e = 4$ and $f = g = 1$, i.e., $p\mathcal{O}_K = \mathfrak{p}^4$. In this case either $(\alpha^2) = \mathfrak{p}^2$, or $(\alpha^2) = \mathfrak{p}^4$. The ideal $p\mathcal{O}_K$ is generated by α^4 or by α^2, respectively, and thus $p = \mu\alpha^4$, or $p = \mu\alpha^2$, for some $\mu \in \mathcal{U}_K^+$. □

The previous proof also provides the information that the prime p is equal either to $\mu\alpha^2$, or $\mu\alpha^4$, or $\mu\alpha^2\sigma(\alpha)^2$ (where $\mu = 1$ is allowed). In particular, we can deduce the following corollary.

Corollary 1.4.19. *A rational prime p is divisible by a nonunit square in K if and only if $p = \mu\beta^2$ for $\mu \in \mathcal{U}_K^+$ and $\beta \in \mathcal{O}_K$. Moreover, this can happen only if p ramifies in $\mathcal{O}_K$.*

Recall that if a form R is stronger than a form Q (i.e., if Q is represented by R), then the set of elements represented by R includes all the elements which are represented by Q; in particular, if Q is universal, then R must be universal, too. When dealing with universality of diagonal forms, we are particularly interested in unary forms: For example, it is obvious that the form $\langle 1\rangle$ is stronger than the form $\langle 4\rangle$ (and thus if $Q_0 \perp \langle 4\rangle$ is universal for some form Q_0, then $Q_0 \perp \langle 1\rangle$ must be universal as well). The following proposition provides some results in this direction.

Proposition 1.4.20. *Let $\gamma \in \mathcal{O}_K^+$.*

1. *If $\langle\gamma\rangle$ represents two elements $\alpha, \beta \in \mathcal{O}_K^+$, then their product $\alpha\beta$ is a square in K.*
2. *If $\langle\gamma\rangle$ represents a unit μ, then γ itself has to be a totally positive unit. In particular, if $\mu = 1$, then $\langle\gamma\rangle \cong \langle 1\rangle$.*
3. *If $\langle\gamma\rangle$ represents $\mu\alpha^2$ with $\mu \in \mathcal{U}_K^+$ and $\alpha \in \mathcal{O}_K$, then $\langle\mu\rangle$ is stronger than $\langle\gamma\rangle$.*
4. *If $\langle\gamma\rangle$ represents $\alpha \in \mathcal{O}_K^+$, then $\langle\gamma\rangle$ is stronger than $\langle\alpha\rangle$.*
5. *If $\langle\gamma\rangle$ represents a rational prime number p, then either $\langle\gamma\rangle \cong \langle p\rangle$, or there exists $\mu \in \mathcal{U}_K^+$ (possibly $\mu = 1$) such that $\langle\mu\rangle$ is stronger than $\langle\gamma\rangle$.*

Proof. The parts (1) and (4) are trivial.

(2) Assume $\gamma z^2 = \mu$ for some $z \in \mathcal{O}_K$; the conclusion follows readily by comparing the norms. As for the second part, if $\gamma z^2 = 1$, then clearly $\gamma \in \mathcal{U}_K^{\square}$, and thus $\langle\gamma\rangle \cong \langle 1\rangle$.

(3) Suppose $\gamma z^2 = \mu\alpha^2$ for some $z \in \mathcal{O}_K$. For an arbitrary $t \in \mathcal{O}_K$, we want to prove that γt^2 is represented by $\langle\mu\rangle$: The equality $\gamma z^2 = \mu\alpha^2$ can be rewritten as $\gamma t^2 = \mu\left(\frac{\alpha t}{z}\right)^2$, where $\frac{\alpha t}{z} \in \mathcal{O}_K$, because obviously $\gamma t^2 \in \mathcal{O}_K$ and the unit μ is invertible.

(5) Let $z \in \mathcal{O}_K$ be such that $\gamma z^2 = p$. If z is a unit, then obviously $\langle\gamma\rangle \cong \langle p\rangle$. Suppose $z \notin \mathcal{U}_K$; combining Corollary 1.4.19 with part (3) of this proposition, we conclude the proof. □

1.4.6 Direct decompositions of a quadratic lattice

Until now we were mostly preparing tools to handle diagonal forms; nevertheless, not all forms are diagonalizable. To deal with this problem, we have to work with the underlying lattice and its bases. At several places in this subsection, we exploit the fact that $\mathcal{O}_K$ is a Dedekind domain by using the structure theorem for finitely generated modules over a Dedekind domain, see e.g. [Mi, Th. 3.31]. For our purposes, the following simplified version suffices:

Theorem 1.4.21. *Let M be a finitely generated torsion-free module over a Dedekind domain R. Then M is isomorphic to a direct sum of finitely many projective modules of rank one (which can be identified with fractional ideals):*

$$M \simeq I_1 \oplus \cdots \oplus I_\ell.$$

The number ℓ is uniquely given. Further, if we interpret the projective modules as fractional ideals, then $M \simeq J_1 \oplus \cdots \oplus J_\ell$ if and only if $I_1 \cdots I_\ell J_1^{-1} \cdots J_\ell^{-1}$ is a principal fractional ideal.

Before applying this theorem, we will use some more elementary tools. Recall that vectors $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n \in \mathcal{O}_K^n$ form a lattice basis of $\mathcal{O}_K^n$ if $\mathcal{O}_K^n = \mathcal{O}_K\boldsymbol{x}_1 + \cdots + \mathcal{O}_K\boldsymbol{x}_n$. Observe that in that case, the decomposition is a direct one.

If, for a given vector $\boldsymbol{e} \in \mathcal{O}_K^n$, its coordinates generate a nontrivial ideal I in $\mathcal{O}_K$, then the determinant of any matrix with entries from $\mathcal{O}_K$ containing $\boldsymbol{e}$ as one of the columns lies in I and thus is not invertible. This shows that such a vector cannot be part of a lattice basis of $\mathcal{O}_K^n$. The following lemma claims that the converse holds as well. Note that all statements in this subsection hold for *any* totally real field K.

Lemma 1.4.22. *A vector $\boldsymbol{e}$ is contained in some lattice basis of $\mathcal{O}_K^n$ if and only if its coordinates generate the trivial ideal $\mathcal{O}_K$.*

Proof. We have already seen a proof of one direction above the statement of the lemma. As for the other implication, let us first prove that the submodule $\mathcal{O}_K\boldsymbol{e}$ has a complement in $\mathcal{O}_K^n$, i.e., there is a submodule M such that $\mathcal{O}_K^n = \mathcal{O}_K\boldsymbol{e} \oplus M$. If coordinates of $\boldsymbol{e}$ generate $\mathcal{O}_K$, then there is some $\boldsymbol{d} \in \mathcal{O}_K^n$ such that $\boldsymbol{d}^{\mathrm{T}}\boldsymbol{e} = 1$. Using one such $\boldsymbol{d}$, we define a map $\pi : \mathcal{O}_K^n \to \mathcal{O}_K\boldsymbol{e}$ by putting $\pi(\boldsymbol{x}) = (\boldsymbol{d}^{\mathrm{T}}\boldsymbol{x})\boldsymbol{e}$. It is clearly a homomorphism of modules and it acts as identity on $\mathcal{O}_K\boldsymbol{e}$, whence its image is $\mathcal{O}_K\boldsymbol{e}$ and $\pi^2 = \pi$. Therefore, we can write $\mathcal{O}_K^n = \operatorname{Im}\pi \oplus \operatorname{Ker}\pi = \mathcal{O}_K\boldsymbol{e} \oplus \operatorname{Ker}\pi$. It remains to show that $\operatorname{Ker}\pi \simeq \mathcal{O}_K^{n-1}$; this follows from Theorem 1.4.21. □

An invertible change of variables (i.e., a substitution) of an n-ary form corresponds to choosing a different basis of the underlying lattice $\mathcal{O}_K^n$. Bearing this in mind, we can use the above stated lemma to deduce the following corollary. Especially its second part is almost folklore, but it is difficult to find a reference.

Corollary 1.4.23. *Let Q be an n-ary quadratic form.*

1. *If Q represents $\alpha \in \mathcal{O}_K$ in such a way that $\alpha = Q(\boldsymbol{e})$ where coordinates of $\boldsymbol{e}$ generate the trivial ideal $\mathcal{O}_K$, then there exists an n-ary quadratic form Q' equivalent to Q such that $Q'(y_1, y_2, \ldots, y_n) = \sum_{1 \le i \le j \le n} b_{ij} y_i y_j$ with $b_{11} = \alpha$.*

2. *If Q represents a unit $\mu \in \mathcal{U}_K^+$ (for example 1), then $Q \cong \langle\mu\rangle \perp Q_0$ for some $(n-1)$-ary subform Q_0.*

Proof. To prove (1), use Lemma 1.4.22 and consider a basis $(\boldsymbol{e}, \boldsymbol{x_2}, \ldots, \boldsymbol{x_n})$ of the lattice $\mathcal{O}_K^n$. Then $Q(y_1\boldsymbol{e} + \ldots + y_n\boldsymbol{x_n})$ has the desired form, since the coefficient in front of y_1^2 is $Q(\boldsymbol{e}) = \alpha$.

The statement (2) can be deduced as follows: First observe that if $Q(\boldsymbol{e}) = \mu$, then the coordinates of $\boldsymbol{e}$ generate the ideal $(\mu) = \mathcal{O}_K$, so the first part of the statement can be applied. Thus we transform the form so that the first diagonal coefficient is μ.

To erase the non-diagonal coefficients for the first variable, we need another basis transformation (which corresponds to one step of Gram–Schmidt orthogonalization): We replace the basis $(\boldsymbol{e}, \boldsymbol{x_2}, \ldots, \boldsymbol{x_n})$ by $(\boldsymbol{e}, \boldsymbol{z_2}, \ldots, \boldsymbol{z_n})$ where $\boldsymbol{z_i} := \boldsymbol{x_i} - \mu^{-1}\frac{b_{1i}}{2}\boldsymbol{e}$; indeed, for such a basis we compute

$$B_Q(\boldsymbol{e}, \boldsymbol{z_i}) = B_Q(\boldsymbol{e}, \boldsymbol{x_i}) - \mu^{-1}\frac{b_{1i}}{2}B_Q(\boldsymbol{e}, \boldsymbol{e}) = \frac{b_{1i}}{2} - \mu^{-1}\frac{b_{1i}}{2}\mu = 0.$$ □

Let us focus on the 2-dimensional case. For a vector $\boldsymbol{v} \in K^2$ we denote by $\mathcal{I}_{\boldsymbol{v}}$ the *index* of $\boldsymbol{v}$ (sometimes also called the *coefficient*), i.e.,

$$\mathcal{I}_{\boldsymbol{v}} = \left\{ \eta \in K \mid \eta \boldsymbol{v} \in \mathcal{O}_K^2 \right\};$$

note that it is a fractional $\mathcal{O}_K$-ideal, and $\mathcal{I}_{\boldsymbol{v}} \boldsymbol{v} = K\boldsymbol{v} \cap \mathcal{O}_K^2$.

Lemma 1.4.24. *Let $\boldsymbol{v} \in K^2$, $\boldsymbol{v} = \binom{v_1}{v_2}$. Then $\mathcal{I}_{\boldsymbol{v}} = (v_1, v_2)^{-1}$.*

Proof. Consider a fractional $\mathcal{O}_K$-ideal J; we have the following chain of equivalences:

$$J \supseteq (v_1, v_2) \iff J \supseteq (v_1) \;\&\; J \supseteq (v_2) \iff J^{-1}(v_1) \subseteq \mathcal{O}_K \;\&\; J^{-1}(v_2) \subseteq \mathcal{O}_K$$
$$\iff J^{-1}\tbinom{v_1}{v_2} \subseteq \mathcal{O}_K^2 \iff J^{-1} \subseteq \mathcal{I}_{\boldsymbol{v}}$$

The choice $J = (v_1, v_2)$ obviously satisfies $J \supseteq (v_1, v_2)$; thus, $(v_1, v_2)^{-1} \subseteq \mathcal{I}_{\boldsymbol{v}}$. On the other hand, setting $J = \mathcal{I}_{\boldsymbol{v}}^{-1}$ and using the other direction, we obtain $(v_1, v_2)^{-1} \supseteq \mathcal{I}_{\boldsymbol{v}}$. □

Lemma 1.4.25. *Let $\boldsymbol{e}$ be any nonzero vector from $\mathcal{O}_K^2$. Then there exists some $\boldsymbol{f} \in K^2$ such that $\mathcal{O}_K^2 = \mathcal{I}_{\boldsymbol{e}}\boldsymbol{e} \oplus \mathcal{I}_{\boldsymbol{f}}\boldsymbol{f}$, Moreover, $\boldsymbol{f}$ can be chosen in such a way that $\mathcal{I}_{\boldsymbol{f}} = \mathcal{I}_{\boldsymbol{e}}^{-1}$. That is, if $\boldsymbol{e} = \binom{e_1}{e_2}$, then $\mathcal{I}_{\boldsymbol{f}} = (e_1, e_2)$.*

Proof. Consider the $\mathcal{O}_K$-module $\mathcal{O}_K^2/\mathcal{I}_{\boldsymbol{e}}\boldsymbol{e}$. As a factor of a finitely generated module, it is finitely generated; it is simple to check that it is torsion-free as well. Over a Dedekind domain, a module with these two properties is projective (this is a corollary of Theorem 1.4.21). Using a well-known property of projective modules, there is a submodule N of $\mathcal{O}_K^2$ such that $\mathcal{O}_K^2 = \mathcal{I}_{\boldsymbol{e}}\boldsymbol{e} \oplus N$.

The next step is to observe that N must be a module of the form $K\boldsymbol{g} \cap \mathcal{O}_K^2$ for some $\boldsymbol{g} \in \mathcal{O}_K^2$; this follows from simple linear algebraic considerations ($\boldsymbol{g}$ can be chosen as any nonzero element of N).

So far we know $N = K\boldsymbol{g} \cap \mathcal{O}_K^2 = \mathcal{I}_{\boldsymbol{g}}\boldsymbol{g}$ for some $\boldsymbol{g}$ which even belongs to $\mathcal{O}_K^2$; however, we have not yet ensured that $\mathcal{I}_{\boldsymbol{g}} = \mathcal{I}_{\boldsymbol{e}}^{-1}$. We have $\mathcal{O}_K^2 = \mathcal{I}_{\boldsymbol{e}}\boldsymbol{e} \oplus \mathcal{I}_{\boldsymbol{g}}\boldsymbol{g}$. Since $\mathcal{O}_K^2$ can also be written as $\mathcal{O}_K\boldsymbol{x}_1 \oplus \mathcal{O}_K\boldsymbol{x}_2$ where $\boldsymbol{x}_1, \boldsymbol{x}_2$ is the standard basis, we have two decompositions of a module into projective modules of rank 1; in such a situation, Theorem 1.4.21 tells us that the fractional ideals $\mathcal{O}_K\mathcal{O}_K$ and $\mathcal{I}_{\boldsymbol{e}}\mathcal{I}_{\boldsymbol{g}}$ are the same up to multiplication by a principal fractional ideal, say $\mathcal{O}_K\mathcal{O}_K = (\delta)\mathcal{I}_{\boldsymbol{e}}\mathcal{I}_{\boldsymbol{g}}$. Then we can define a new vector $\boldsymbol{f} = \frac{1}{\delta}\boldsymbol{g}$ to obtain $\mathcal{I}_{\boldsymbol{e}}\mathcal{I}_{\boldsymbol{f}} = \mathcal{O}_K$. □

1.5 Proof in the main cases

In this section, we follow the proof strategy outlined in Section 1.3. Recall that we assume $Q \cong \langle 1 \rangle \perp Q_0$ to be a universal classical ternary quadratic form and that we distinguish the following three cases:

(I) $|\mathcal{U}_K^+/\mathcal{U}_K^\square| > 2$; we have solved this case immediately in Section 1.3.

(II) $|\mathcal{U}_K^+/\mathcal{U}_K^\square| = 2$ with a system of representatives $\{1, \varepsilon\}$,

(III) $|\mathcal{U}_K^+/\mathcal{U}_K^\square| = 1$, where the only relevant unit is 1.

Cases (II) and (III) are further divided into subsections according to the whether 2ε is a square, resp. according to the diagonalizability of Q_0; see Appendix 1.9 for a schematic structure of the proof. Moreover, every subsection requires its own additional conditions on K; these are always listed at the very beginning of the subsection and from the proof it will be evident why they are needed. All the omitted cases will be covered in Section 1.6.

1.5.1 Case (I)

This case has been solved in Section 1.3, but there is actually more to be said. In particular, this part covers two different types of $\mathcal{U}_K^+/\mathcal{U}_K^\square$, namely $|\mathcal{U}_K^+/\mathcal{U}_K^\square| = 4$ and $|\mathcal{U}_K^+/\mathcal{U}_K^\square| = 8$. In the former case, as we have outlined in Section 1.3, four units of $\mathcal{U}_K^+/\mathcal{U}_K^\square$ suffice to prove that every universal form over $\mathcal{O}_K$ must have at least four variables, which implies that no ternary form is universal. In the latter, having eight such units, we can claim an even stronger statement – in these fields, any universal form needs at least eight variables. In the following example, we present some biquadratic fields with this property.

Example 1.5.1. Considering possible systems of fundamental units in K, see [MU], a sufficient condition for $|\mathcal{U}_K^+/\mathcal{U}_K^\square| = 8$ to happen is that the fundamental units $\varepsilon_m, \varepsilon_s$ and ε_t of quadratic subfields are totally positive and nonsquare in K and none of the products $\varepsilon_m\varepsilon_s$, $\varepsilon_m\varepsilon_t$, $\varepsilon_s\varepsilon_t$ and $\varepsilon_m\varepsilon_s\varepsilon_t$ is a square in K. For example, these conditions are satisfied in the fields $\mathbb{Q}(\sqrt{3}, \sqrt{910})$, $\mathbb{Q}(\sqrt{21}, \sqrt{55})$ and $\mathbb{Q}(\sqrt{21}, \sqrt{110})$.

1.5.2 Case (II) with 2ε not being a square

Throughout this subsection suppose $\sqrt{2} \notin K$. In the following, we shall repeatedly exploit the first part of Proposition 1.4.20: The product of two numbers represented by the same unary form is a square.

We assume the ternary quadratic form Q to be universal, hence it must represent both 1 and ε. Using the second part of Corollary 1.4.23 twice, we end up with a diagonal form $Q \cong \langle 1\rangle \perp \langle\varepsilon\rangle \perp \langle\gamma\rangle$ (with $\gamma \in \mathcal{O}_K^+$ not yet specified). This form is supposed to be universal; hence, it represents 2. Noting that $\langle\varepsilon\rangle$ represents neither 1 nor 2 and using Lemma 1.4.3, we see that 2 has to be represented by $\langle 1\rangle \perp \langle\gamma\rangle$. Using the same lemma again, we find out that $\langle\gamma\rangle$ represents either 1 or 2, since $\langle 1\rangle$ does not represent 2 (because $\sqrt{2} \notin K$).

Similarly, we can consider the representation of 2ε. Observe that 2ε can be decomposed only as $0 + 2\varepsilon$ or $\varepsilon + \varepsilon$; otherwise multiplication by $\varepsilon^{-1} \in \mathcal{O}_K^+$ would give a nontrivial decomposition of 2, contradicting Lemma 1.4.3. Since, just as before, $\langle 1\rangle$ represents neither ε nor 2ε, the form $\langle\varepsilon\rangle \perp \langle\gamma\rangle$ represents 2ε. Further, $\langle\varepsilon\rangle$ does not represent 2ε because if 2 is not a square, then $2\varepsilon^2$ is not a square either. Therefore, $\langle\gamma\rangle$ has to represent ε or 2ε.

We have deduced that $\langle\gamma\rangle$ represents either 1 or 2 and also either ε or 2ε; however, this is impossible, since none of the four products $1 \cdot \varepsilon$, $1 \cdot 2\varepsilon$, $2 \cdot \varepsilon$ and $2 \cdot 2\varepsilon$ is a square. Thus, Q cannot be universal.

Conclusion 1.5.2. *Assuming that ε is a nonsquare totally positive unit and that 2ε is not a square, and further requiring $\sqrt{2} \notin K$, we have seen that there does not exist any ternary quadratic form which simultaneously represents $1, \varepsilon, 2, 2\varepsilon$.*

Note that the proof used neither the condition $|\mathcal{U}_K^+/\mathcal{U}_K^\square| = 2$ nor the fact that K is a biquadratic field: We only needed to know that in K, all units are indecomposable and 2 decomposes only trivially as $1 + 1$ or $0 + 2$ (both of this holds in any totally real field, see the unnumbered remark below Lemma 1.4.3), that $\sqrt{2} \notin K$ and that K contains a totally positive unit ε such that 2ε is not a square. Thus, we have actually proved the more general Theorem 1.1.2.

1.5.3 Case (II) with 2ε being a square

Observe that in this case $m \neq 2$ (i.e., $\sqrt{2} \notin K$): If both 2 and 2ε were squares, then so would be ε. Furthermore, suppose $K \neq \mathbb{Q}(\sqrt{3}, \sqrt{5})$.

Just as in the previous subsection, the only potentially universal form is $\langle 1\rangle \perp \langle\varepsilon\rangle \perp \langle\gamma\rangle$ for some $\gamma \in \mathcal{O}_K^+$. Nevertheless, in this case the subform $\langle 1\rangle \perp \langle\varepsilon\rangle$ represents all the numbers 2, 3, 4. One natural way to go would be to consider representations of 5 and 5ε. However, it turns out

to be easier to use the elements $\mathcal{M}$ and $\varepsilon\mathcal{M}$, or, in the cases with $m \in \{3,5\}$, the elements $\mathcal{S}$ and $\varepsilon\mathcal{S}$.

First assume $m \neq 3,5$. Note that both $\mathcal{M}$ and $\varepsilon\mathcal{M}$ are indecomposable: For $\mathcal{M}$ this is stated in Proposition 1.4.9, and any nontrivial decomposition of $\varepsilon\mathcal{M}$ would yield a decomposition of $\mathcal{M}$. Furthermore, if $\varepsilon\mathcal{M}$ was a square, then so would $2\mathcal{M}$; thus, by Corollary 1.4.14, neither $\mathcal{M}$ nor $\varepsilon\mathcal{M}$ is a square since $m \neq 3,5$. This can be rephrased as "$\mathcal{M}$ is represented by neither of the unary forms $\langle 1\rangle$, $\langle\varepsilon\rangle$". It is easy to see that the same holds for $\varepsilon\mathcal{M}$ as well.

Suppose now that $\mathcal{M}$ is represented by $\langle 1\rangle\perp\langle\varepsilon\rangle\perp\langle\gamma\rangle$ for some $\gamma \in \mathcal{O}_K^+$. Due to its indecomposability, it has to be represented by one of the unary subforms; from the previous paragraph, we know that it must be $\langle\gamma\rangle$. The same argument holds for $\varepsilon\mathcal{M}$. But if the unary form $\langle\gamma\rangle$ represents both $\mathcal{M}$ and $\varepsilon\mathcal{M}$, it means that their product, $\varepsilon\mathcal{M}^2$, is a square. Thus ε is a square, which is a contradiction.

Remark 1.5.3. The equality $\varepsilon = \mathcal{M}$ might hold for some integers m, in which case $\mathcal{M}$ would be already represented by the binary form $\langle 1\rangle\perp\langle\varepsilon\rangle$. However, we do not have to handle this separately, since it would mean that $\varepsilon\mathcal{M}$ is a square, which we have already discussed and rejected.

Now let $m \in \{3,5\}$; for $K \neq \mathbb{Q}(\sqrt{3},\sqrt{5})$, neither $\mathcal{S}$ nor $2\mathcal{S}$ is a square by Lemma 1.4.15, and indecomposability of $\mathcal{S}$ follows from Proposition 1.4.10. Otherwise, we can use exactly the same arguments as above, with $\mathcal{M}$ replaced by $\mathcal{S}$.

Let us summarize the above discussion.

Conclusion 1.5.4. *Suppose ε is a nonsquare totally positive unit such that 2ε is a square. Except possibly for the field $K = \mathbb{Q}(\sqrt{3},\sqrt{5})$, there does not exist any universal ternary quadratic form.*

In particular, if $m \neq 3,5$, then no ternary quadratic form is able to simultaneously represent 1, ε, $\mathcal{M}$ and $\varepsilon\mathcal{M}$, and if $m \in \{3,5\}$ but $s \neq 5$, then no ternary quadratic form is able to simultaneously represent 1, ε, $\mathcal{S}$ and $\varepsilon\mathcal{S}$.

If we put the previous two conclusions together, we obtain the following:

Conclusion 1.5.5 (Case (II))**.** *All in all: If the field K contains a nonsquare totally positive unit ε and if $m \neq 2$ and $K \neq \mathbb{Q}(\sqrt{3},\sqrt{5})$, there is no universal ternary form over K.*

1.5.4 Case (III) with Q_0 diagonalizable

For this subsection, let $\sqrt{2},\sqrt{3},\sqrt{5} \notin K$.

In this case, the form $\langle 1\rangle$ already represents all totally positive units; nonetheless, we assume the binary quadratic subform Q_0 to be diagonalizable. Thus, we have a universal ternary quadratic form $Q \cong \langle 1\rangle\perp\langle\beta\rangle\perp\langle\gamma\rangle$ with unspecified $\beta,\gamma \in \mathcal{O}_K^+$. Note that if both β and γ are rational integers, then the quadratic form Q cannot be universal by the result of Siegel [Si] invoking $\sqrt{5} \notin K$. (Alternatively, to present a self-contained proof, we can observe that $\langle n\rangle$ cannot represent $\mathcal{M}$ since $\mathcal{M}$ is not a square and $\frac{\mathcal{M}}{n}$ for $n \geq 2$ is never in $\mathcal{O}_K$.)

The form Q has to represent 2; using Lemma 1.4.3, we can see that $\langle\beta\rangle\perp\langle\gamma\rangle$ has to represent either 1 or 2.

First, assume that $\langle\beta\rangle\perp\langle\gamma\rangle$ represents 1; we can put $\beta = 1$ by Proposition 1.4.20(2). Since the form $\langle 1\rangle\perp\langle 1\rangle\perp\langle\gamma\rangle$ has to represent 3, by invoking Lemma 1.4.3 again we get that $\langle\gamma\rangle$ represents $1, 2$ or 3. Using parts (2) and (5) of Proposition 1.4.20, we get that $\gamma \in \{1,2,3\}$, as 1 is the only totally positive unit up to multiplication by a square; but a quadratic form with rational integer coefficients cannot be universal by the above mentioned argument.

Second, let $\langle\beta\rangle\perp\langle\gamma\rangle$ represent 2; by Lemma 1.4.3, we have two possibilities for the additive decomposition of 2: either $2 = 1+1$ or $2 = 2+0$. The first leads to the nonuniversal quadratic form $\langle 1\rangle\perp\langle 1\rangle\perp\langle 1\rangle$; the latter together with part (5) of Proposition 1.4.20 yields the quadratic

form $\langle 1\rangle\perp\langle 2\rangle\perp\langle\gamma\rangle$. This form has to represent 5; note that all the possible summands can be obtained by considering the inequality $5 \succcurlyeq \omega^2$ for $\omega \in \mathcal{O}_K$ (because if $5 \succcurlyeq 2\omega^2$, then $5 \succcurlyeq \omega^2$) – thus, using Remark 1.4.4 together with the assumption $\sqrt{2}, \sqrt{3}, \sqrt{5} \notin K$, we get that $\langle\gamma\rangle$ has to represent at least one of the numbers $1, 2, 3, 4, 5$. Invoking Proposition 1.4.20, each of these possibilities leads to a quadratic form with integral coefficients: More specifically, we use part (2) of this proposition to handle the case when $\langle\gamma\rangle$ represents 1, part (5) for the primes $2, 3, 5$, and finally part (3) for 4. Thus, none of the possibilities for $\langle\gamma\rangle$ leads to a universal form.

Conclusion 1.5.6. *If $\mathcal{U}_K^+ = \mathcal{U}_K^\square$ holds and $\sqrt{2}, \sqrt{3}, \sqrt{5} \notin K$, then there is no diagonalizable universal ternary form over the biquadratic field K.*

In particular, we use the representations of $1, 2, 3$ and 5 to transform each of the potential diagonalizable universal quadratic forms to a form with integral coefficients. Such a form cannot be universal by the result of Siegel [Si], and also because it does not represent $\mathcal{M}$.

1.5.5 Case (III) with Q_0 nondiagonalizable

This subsection requires the conditions $\sqrt{2}$, $\sqrt{3}$, $\sqrt{5}$, $\sqrt{6}$, $\sqrt{7}$, $\sqrt{10}$, $\sqrt{13}$, $\sqrt{17}$, $\sqrt{21} \notin K$ and $m \neq 33, 65, 85$.

In this case we assume that the binary subform Q_0 is not diagonalizable. In particular, it does not represent 1 (because if it did, we could use part (2) of Corollary 1.4.23 to obtain a diagonal form). Since $Q \cong \langle 1\rangle\perp Q_0$ represents 2 and there are only trivial additive decompositions of 2 by Lemma 1.4.3, $\sqrt{2} \notin K$ implies that 2 has to be represented by Q_0. Denote $\boldsymbol{e} = \left(\begin{smallmatrix} e_1 \\ e_2 \end{smallmatrix}\right)$ a vector from $\mathcal{O}_K^2$ such that $Q_0(\boldsymbol{e}) = 2$. To put 2 as one of the diagonal coefficients of the form Q_0, we would need to extend the vector $\boldsymbol{e}$ to a basis of $\mathcal{O}_K^2$. Referring to Lemma 1.4.22, we can see that this is possible only if the ideal (e_1, e_2) is equal to $\mathcal{O}_K$, but that may not always be the case: In general, (e_1, e_2) is an ideal the square of which divides (2), because $2 = Q_0(\boldsymbol{e})$ means that 2 is a combination of e_1^2, e_1e_2 and e_2^2.

Thanks to Lemma 1.4.25, we can at least find a vector $\boldsymbol{f} = \left(\begin{smallmatrix} f_1 \\ f_2 \end{smallmatrix}\right)$ from K^2 which forms together with $\boldsymbol{e}$ a "generalized basis" of $\mathcal{O}_K^2$ in the sense that $\mathcal{O}_K^2 = \mathcal{I}_{\boldsymbol{e}}\boldsymbol{e} \oplus \mathcal{I}_{\boldsymbol{f}}\boldsymbol{f}$; recall that $\boldsymbol{f}$ is usually not an element of $\mathcal{O}_K^2$ and it is chosen so that $\mathcal{I}_{\boldsymbol{e}}\mathcal{I}_{\boldsymbol{f}} = \mathcal{O}_K$. We have $\mathcal{I}_{\boldsymbol{f}} = (e_1, e_2)$ and $\mathcal{I}_{\boldsymbol{e}} = (f_1, f_2)$; note that it follows from the discussion above that $\mathcal{I}_{\boldsymbol{f}}^2$ divides (2).

Denote $Q_0(\boldsymbol{f}) = \gamma$ and $B_{Q_0}(\boldsymbol{e}, \boldsymbol{f}) = \beta$, where B_{Q_0} is the polar form of the quadratic form Q_0. Thus, taking a general vector $y\boldsymbol{e} + z\boldsymbol{f} \in \mathcal{O}_K^2$ with $y \in \mathcal{I}_{\boldsymbol{e}}$ and $z \in \mathcal{I}_{\boldsymbol{f}}$, we have

$$Q_0(y\boldsymbol{e} + z\boldsymbol{f}) = 2y^2 + 2\beta yz + \gamma z^2. \tag{1.5.1}$$

Multiplying by 2 and completing the square, we get

$$2Q_0(y\boldsymbol{e} + z\boldsymbol{f}) = (2y + \beta z)^2 + (2\gamma - \beta^2)z^2. \tag{1.5.2}$$

The total positive definiteness of Q_0 implies $2\gamma - \beta^2 \succ 0$. Note that it is not clear whether β and γ belong to $\mathcal{O}_K$. As it turns out, for γ it is not always the case; see Appendix 1.7 for an example. This was overlooked in [CKR]; however, for both their and our proof, the following lemma is sufficient.

Lemma 1.5.7. *For any $y \in \mathcal{I}_{\boldsymbol{e}}$ and $z \in \mathcal{I}_{\boldsymbol{f}}$, we have:*

1. $2\gamma \in \mathcal{O}_K$,
2. $2\gamma - \beta^2 \in \mathcal{O}_K^+$,
3. $\beta \in \mathcal{O}_K$,
4. $2y \in \mathcal{I}_{\boldsymbol{f}} \subseteq \mathcal{O}_K$,
5. $2y + \beta z \in \mathcal{I}_{\boldsymbol{f}} \subseteq \mathcal{O}_K$.

Proof. Obviously, (3) follows readily from (1) and (2) using $\beta \in K$; (5) is an immediate consequence of (3), (4), and the assumption on z. Thus we only need to prove (1), (2) and (4).

Since the form Q_0 represents only elements of $\mathcal{O}_K$ (when plugging in vectors from $\mathcal{O}_K^2$, which the vector $e_i\boldsymbol{f}$ certainly fulfills), we have that $Q_0(e_i\boldsymbol{f}) = \gamma e_i^2 \in \mathcal{O}_K$ for both $i = 1, 2$. Then the product $\gamma^2 e_1^2 e_2^2 \in \mathcal{O}_K$, and thus $\gamma e_1 e_2 \in \mathcal{O}_K$ as well. Therefore, $(\gamma)(e_1, e_2)^2 \subseteq \mathcal{O}_K$. As $(2) \subseteq (e_1, e_2)^2$, we obtain $(2\gamma) \subseteq (\gamma)(e_1, e_2)^2 \subseteq \mathcal{O}_K$, thus concluding (1).

As for (2), note that $2\gamma - \beta^2$ is the determinant of the matrix $\left(\begin{smallmatrix} 2 & \beta \\ \beta & \gamma \end{smallmatrix}\right)$. This is the Gram matrix of vectors $\boldsymbol{e}$, $\boldsymbol{f}$, which can be obtained from the original matrix of our form,

$$M = \begin{pmatrix} Q_0(\boldsymbol{x_1}) & B_{Q_0}(\boldsymbol{x_1}, \boldsymbol{x_2}) \\ B_{Q_0}(\boldsymbol{x_1}, \boldsymbol{x_2}) & Q_0(\boldsymbol{x_2}) \end{pmatrix}$$

(where $\boldsymbol{x_1}, \boldsymbol{x_2}$ are the vectors of the standard basis), as $\left(\begin{smallmatrix} 2 & \beta \\ \beta & \gamma \end{smallmatrix}\right) = E^{\mathrm{T}} M E$ for $E = \left(\begin{smallmatrix} e_1 & f_1 \\ e_2 & f_2 \end{smallmatrix}\right)$. Taking determinants yields $2\gamma - \beta^2 = (e_1 f_2 - e_2 f_1)^2 \cdot \det M$. Since Q_0 is an integral form, clearly $\det M \in \mathcal{O}_K^+$. Thanks to $e_1 f_2 - e_2 f_1 \in (e_1, e_2)(f_1, f_2)$ and $(e_1, e_2)(f_1, f_2) = \mathcal{I}_{\boldsymbol{f}}(f_1, f_2) = \mathcal{O}_K$, we have $(e_1 f_2 - e_2 f_1)^2 \in \mathcal{O}_K^{\square}$ and (2) is proven.

To prove (4), combine $(2y) \subseteq (2)\mathcal{I}_{\boldsymbol{f}}^{-1}$ and $(2) \subseteq \mathcal{I}_{\boldsymbol{f}}^2$ to obtain $(2y) \subseteq \mathcal{I}_{\boldsymbol{f}}$. □

Let us now take a look at how 5 can be represented by Q. Taking into account Remark 1.4.4 along with the assumptions $m \neq 2, 3, 5$, it turns out that Q_0 has to represent 4 or 5; thus, $2Q_0$ represents 8 or 10. Invoking Lemma 1.5.7, both $2y + \beta z$ and $2\gamma - \beta^2$ are elements of $\mathcal{O}_K$; hence, we are allowed to use Lemma 1.4.5. Since we suppose $\sqrt{2}$, $\sqrt{3}$, $\sqrt{5}$, $\sqrt{6}$, $\sqrt{7}$, $\sqrt{10}$, $\sqrt{13}$, $\sqrt{17}$, $\sqrt{21} \notin K$, we obtain the following possible representations:

$2Q_0(y\boldsymbol{e} + z\boldsymbol{f})$	$(2y + \beta z)^2$	$(2\gamma - \beta^2)z^2$	Case
10	0	10	(i)
	1	9	(ii)
	4	6	(iii)
	9	1	(iv)
8	0	8	(v)
	1	7	(vi)
	4	4	(vii)

(1.5.3)

Furthermore, the form Q has to represent $\mathcal{M}$. Since $\mathcal{M}$ is nonsquare by Corollary 1.4.14 whenever $m \neq 5$, and indecomposable by Proposition 1.4.9, we conclude that $\mathcal{M}$ has to be represented by Q_0, and thus the form $2Q_0$ represents $2\mathcal{M}$.

Recall that the $\mathcal{O}_K$-ideal $\mathcal{I}_{\boldsymbol{f}}^2$ must divide (2). Now we distinguish between two cases: Either $\mathcal{I}_{\boldsymbol{f}} = \mathcal{O}_K$, or $\mathcal{I}_{\boldsymbol{f}}$ is a proper ideal such that $\mathcal{I}_{\boldsymbol{f}}^2$ divides (2).

(a) First, assume that $\mathcal{I}_{\boldsymbol{f}} = \mathcal{O}_K$; then necessarily $\mathcal{I}_{\boldsymbol{e}} = \mathcal{O}_K$ as well.

In cases (ii), (iv) and (vii), we have that $(2\gamma - \beta^2)z^2$ is a square of a rational integer, and thus $2\gamma - \beta^2$ is a square in K. Looking at (1.5.2), we see that $2Q_0$ can represent only those elements of $2\mathcal{O}_K$ which can be written as a sum of two squares. This yields a contradiction because $2Q_0$ represents $2\mathcal{M}$, which cannot be written as a sum of two squares by Lemma 1.4.17 as we have $m \neq 2, 3, 5$.

The case (vi) can be rephrased as "the form $\langle 2\gamma - \beta^2 \rangle$ represents 7"; part (5) of Proposition 1.4.20 yields then that either $\langle 2\gamma - \beta^2 \rangle \cong \langle 7 \rangle$ or the unary form $\langle 2\gamma - \beta^2 \rangle$ is represented by $\langle 1 \rangle$ (as there is no nonsquare totally positive unit). Hence, one of the binary forms $\langle 1 \rangle \perp \langle 7 \rangle$ or

$\langle 1\rangle \perp \langle 1\rangle$ is stronger than $2Q_0$. But neither of these forms represents $2\mathcal{M}$: The latter is excluded in Lemma 1.4.17 explicitly, the former is ruled out by using the same lemma and noting that neither $\frac{2\mathcal{M}}{7}$ nor $\frac{2\mathcal{M}-1}{7}$ is an element of $\mathcal{O}_K$. Therefore, $2Q_0$ does not represent $2\mathcal{M}$ either.

To deal with the cases (i), (iii) and (v), let us look at the representation of $2\mathcal{M}$ by the form $2Q_0$; suppose

$$2\mathcal{M} = (2\tilde{y} + \beta\tilde{z})^2 + \left(2\gamma - \beta^2\right)\tilde{z}^2$$

for some $\tilde{y}, \tilde{z} \in \mathcal{O}_K$. Invoking Lemma 1.4.17 along with the assumptions $m \neq 2, 3, 5$, we have two possibilities for the value of $2\tilde{y}+\beta\tilde{z}$, namely 0 and ± 1. First, suppose that $2\tilde{y}+\beta\tilde{z} = 0$; then necessarily $\left(2\gamma - \beta^2\right)\tilde{z}^2 = 2\mathcal{M}$. Moreover, we have assumed that $(2\gamma - \beta^2)z^2 = 10, 6, 8$ (in cases (i), (iii), (v), respectively); therefore, we obtain that $20\mathcal{M}$, $12\mathcal{M}$, $16\mathcal{M}$, respectively, is a square in K. After reducing the integral squares, $5\mathcal{M}$, $3\mathcal{M}$, $\mathcal{M}$, respectively, is a square in K. In all cases, it is a contradiction to Corollary 1.4.14 since the conditions for this subsection imply that $m \notin \{5, 21, 33, 65, 85\}$ and $K \neq \mathbb{Q}(\sqrt{3}, \sqrt{10})$. Thus, we must have $2\tilde{y} + \beta\tilde{z} = \pm 1$; in such a case, the ideal $(2, \beta)$ is equal to the whole ring $\mathcal{O}_K$. Simultaneously, we have $2y+\beta z = 0$ or ± 2, which can be rewritten as $\beta z = 2(k-y)$ for $k = 0$ or ± 1. If $\mathfrak{q}$ is a prime ideal dividing the principal ideal (2), then $\mathfrak{q} \nmid (\beta)$, because otherwise $\mathfrak{q}$ would divide the ideal $(2, \beta) = \mathcal{O}_K$, which is impossible. It follows that $(2) \mid (z)$; in other words, $z \in (2)$, and there exists $z' \in \mathcal{O}_K$ such that $z = 2z'$. Applying this to the equality $(2\gamma - \beta^2)z^2 = 10, 6, 8$ implies $(2\gamma - \beta^2)z'^2 = \frac{10}{4}, \frac{6}{4}, \frac{8}{4}$ in cases (i), (iii), (v), respectively. Obviously, this is absurd in cases (i) and (iii), as $(2\gamma - \beta^2)z'^2 \in \mathcal{O}_K$ but $\frac{10}{4}, \frac{6}{4} \notin \mathcal{O}_K$. To deal with the case (v), we rewrite the equality $(2\gamma - \beta^2)z'^2 = 2$ as $2(\gamma z'^2 - 1) = \beta^2 z'^2$ and use the same argument again to show $(2) \mid (z'^2)$, i.e., $\frac{z'^2}{2} \in \mathcal{O}_K$. Then the equality $(2\gamma - \beta^2)\frac{z'^2}{2} = 1$ means that $\frac{z'^2}{2}$ is a unit and thus a square, implying that 2 is a square as well, which is absurd.

(b) Now assume that $\mathcal{I}_{\boldsymbol{f}} \neq \mathcal{O}_K$. Recall that $\mathcal{I}_{\boldsymbol{e}} = \mathcal{I}_{\boldsymbol{f}}^{-1}$ and $\mathcal{I}_{\boldsymbol{f}}^2 = (e_1, e_2)^2 \mid (2)$. Note that in this case, 2 has to be ramified in K, and thus this cannot happen for fields with integral basis (B4), i.e., those where $p, q, r \equiv 1 \pmod 4$: Indeed, the discriminant of such fields, which equals to pqr, is not divisible by 2, and hence 2 is not ramified in $\mathcal{O}_K$.

Recall that we have

$$2Q_0(y\boldsymbol{e} + z\boldsymbol{f}) = (2y + \beta z)^2 + (2\gamma - \beta^2)z^2$$

with $y \in \mathcal{I}_{\boldsymbol{e}}$ and $z \in \mathcal{I}_{\boldsymbol{f}} = (e_1, e_2) \subsetneq \mathcal{O}_K$; in particular, $z \notin \mathcal{U}_K$.

In the cases (ii), (iv) and (vii), we have again that $2\gamma - \beta^2$ is a square in K, and thus this case can be solved by using the same argument as in part (a), i.e., that $2\mathcal{M}$ cannot be written as a sum of two squares for $m \neq 2, 3, 5$. Alternatively, the impossibility of the case (iv) can also be seen immediately, as $(2\gamma - \beta^2)z^2 = 1$ obviously implies $z \in \mathcal{U}_K$.

In the case (vi), we have an odd rational integer in the right column, i.e., $(2\gamma - \beta^2)z^2 = 7$. Since $z \in \mathcal{I}_{\boldsymbol{f}}$, we obtain that the ideal $((2\gamma - \beta^2)z^2) = (7)$ is contained in the ideal $\mathcal{I}_{\boldsymbol{f}}^2$, and hence $(2, 7) \subseteq \mathcal{I}_{\boldsymbol{f}}^2$ as well. But that is absurd, as obviously $(2, 7) = \mathcal{O}_K$. (Note that the same method could have been used to deal with the case (ii) as well.)

In the remaining cases (i), (iii) and (v), we consider the representation of $2\mathcal{M}$ by $2Q_0$, i.e., we find $\tilde{y} \in \mathcal{I}_{\boldsymbol{e}}$ and $\tilde{z} \in \mathcal{I}_{\boldsymbol{f}}$ such that

$$2\mathcal{M} = (2\tilde{y} + \beta\tilde{z})^2 + (2\gamma - \beta^2)\tilde{z}^2;$$

as $m \neq 2, 3, 5$, Lemma 1.4.17 yields that $2\tilde{y} + \beta\tilde{z}$ is equal either to 0 or ± 1. The latter is impossible, since $2\tilde{y}+\beta\tilde{z} \in \mathcal{I}_{\boldsymbol{f}}$, and $\mathcal{I}_{\boldsymbol{f}}$ does not contain any unit. The former possibility implies $(2\gamma - \beta^2)\tilde{z}^2 = 2\mathcal{M}$; recall that we have $(2\gamma - \beta^2)z_n^2 = n$ for some $z_n \in \mathcal{I}_{\boldsymbol{f}}$ and $n = 10, 6, 8$ in cases (i), (iii), (v), respectively. Multiplying together the equalities $(2\gamma - \beta^2)\tilde{z}^2 = 2\mathcal{M}$ and $(2\gamma - \beta^2)z_n^2 = n$, we get that $2n\mathcal{M}$ is a square in K for $n = 10, 6, 8$, respectively, i.e., that $5\mathcal{M}$, $3\mathcal{M}$, $\mathcal{M}$, respectively, is a square in K. But that is a contradiction to Corollary 1.4.14, since the assumptions for this subsection imply $m \neq 5, 21, 33, 65, 85$ and $K \neq \mathbb{Q}(\sqrt{3}, \sqrt{10})$.

Conclusion 1.5.8. *Let K be a biquadratic field such that $\mathcal{U}_K^+ = \mathcal{U}_K^\square$, and assume $\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{7}, \sqrt{10}, \sqrt{13}, \sqrt{17}, \sqrt{21} \notin K$ and $m \neq 33, 65, 85$. Then no nondiagonalizable ternary form over $\mathcal{O}_K$ is universal. In particular, no such form can represent all of 1, 2, 5 and $\mathcal{M}$.*

Note that at this point, we have proven Theorem 1.1.1 for all biquadratic fields K such that $\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{7}, \sqrt{10}, \sqrt{13}, \sqrt{17}, \sqrt{21} \notin K$ and $m \neq 33, 65, 85$.

1.6 Proof in the special cases

In this section, we focus on the "special cases" of Theorem 1.1.1 which are not included in the main proof in Section 1.5. In particular, we are now interested in the fields which contain $\sqrt{2}$, $\sqrt{3}$, $\sqrt{5}$, $\sqrt{6}$, $\sqrt{7}$, $\sqrt{10}$, $\sqrt{13}$, $\sqrt{17}$, $\sqrt{21}$ or where $m \in \{33, 65, 85\}$. Note that in many of these cases, a problem arises only in one branch of the tree structure of the proof (for a basic overview, see Conclusions 1.5.5, 1.5.6 and 1.5.8). Hence, our approach is to detect the problems and solve them "locally". The exception are the cases $m = 2$ and $m = 5$; they need to be solved by a different method and we postpone them to Subsections 1.6.8 and 1.6.9. Moreover, seven most problematic fields will be treated in Subsection 1.6.10.

1.6.1 $\sqrt{3} \in K$

If the field contains $\sqrt{3}$, then the main proof fails at several places; however, we can use the fact that the fundamental unit $\varepsilon_3 = 2 + \sqrt{3}$ is totally positive and it is a square only in the field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ (which has to be handled separately). Moreover, $2\varepsilon_3 = (1 + \sqrt{3})^2$ is a square, thus we can use Conclusion 1.5.4, provided $\sqrt{5} \notin K$. All in all, only two cases remain to be treated separately: $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $\mathbb{Q}(\sqrt{3}, \sqrt{5})$; this will be done in Subsection 1.6.10.

1.6.2 $\sqrt{6} \in K$, $\sqrt{7} \in K$, $\sqrt{21} \in K$ or $\sqrt{33} \in K$

The cases where $m = 2$ are handled in Subsection 1.6.8. Otherwise, by Conclusion 1.5.5 it suffices to show that if K contains any of the aforementioned numbers $\sqrt{6}$, $\sqrt{7}$, $\sqrt{21}$ and $\sqrt{33}$, it contains a nonsquare totally positive unit.

Indeed, $\varepsilon_6 = 5 + 2\sqrt{6}$, $\varepsilon_7 = 8 + 3\sqrt{7}$, $\varepsilon_{21} = \frac{1}{2}(5 + \sqrt{21})$ and $\varepsilon_{33} = 23 + 4\sqrt{33}$ are all totally positive, and as they are equal to $(\sqrt{2} + \sqrt{3})^2$, $\left(\frac{3\sqrt{2}+\sqrt{14}}{2}\right)^2$, $\left(\frac{\sqrt{3}+\sqrt{7}}{2}\right)^2$ and $(2\sqrt{3} + \sqrt{11})^2$ respectively, they are not squares with the exception of the fields $\mathbb{Q}(\sqrt{2}, \sqrt{6})$, $\mathbb{Q}(\sqrt{2}, \sqrt{7})$, $\mathbb{Q}(\sqrt{3}, \sqrt{7})$ and $\mathbb{Q}(\sqrt{3}, \sqrt{11})$, respectively. But the first two of these exceptional fields belong to the case $m = 2$, which is handled in Subsection 1.6.8, and the latter two contain the nonsquare totally positive unit $\varepsilon_3 = 2 + \sqrt{3}$.

1.6.3 $\sqrt{10} \in K$

This case is more challenging than the ones in the previous subsections since ε_{10} is not totally positive, so we are not sure to which branch of the main proof the field K belongs. However, the only problem with $\sqrt{10} \in K$ arises from the fact that Lemma 1.4.5 allows more decompositions of 8 and 10 than usually. Thus the only place where the main proof of nonuniversality breaks down is one spot in Subsection 1.5.5 where this particular lemma is invoked. It means that here we only have to consider fields K, where all the totally positive units are squares, and forms $Q = \langle 1 \rangle \perp Q_0$, where $2Q_0(y\boldsymbol{e} + z\boldsymbol{f}) = (2y + \beta z)^2 + (2\gamma - \beta^2)z^2$ for suitable vectors $\boldsymbol{e}$ and $\boldsymbol{f}$. For the sake of brevity, denote $\Delta = 2\gamma - \beta^2$. Let us stress that although y and γ do not necessarily belong to $\mathcal{O}_K$, both z and $2\gamma - \beta^2$ always do (see Lemma 1.5.7).

Note that all fields with $m < 10$ are handled elsewhere, namely in Subsections 1.6.1, 1.6.2, 1.6.8 and 1.6.9, and the respective proofs do not require $\sqrt{10} \notin K$, since they do not depend on Lemma 1.4.5; hence, here we may assume $m = 10$.

As in the main proof, we know that since Q represents the nonsquare indecomposable element $\mathcal{M} = 4 + \sqrt{10}$, Q_0 has to represent $\mathcal{M}$, and thus $2Q_0$ represents $2\mathcal{M}$. Invoking Lemma 1.4.17, we know that there is a $z \in \mathcal{O}_K$ such that Δz^2 is either $2\mathcal{M} = 8 + 2\sqrt{10}$ or $2\mathcal{M} - 1 = 7 + 2\sqrt{10}$. Moreover, the element $\overline{\mathcal{M}} = 4 - \sqrt{10}$ has the same algebraic properties as $\mathcal{M}$, and hence there is also a $z' \in \mathcal{O}_K$ such that $\Delta z'^2$ is either $2\overline{\mathcal{M}} = 8 - 2\sqrt{10}$ or $2\overline{\mathcal{M}} - 1 = 7 - 2\sqrt{10}$.

Let us go through the possibilities: If the unary form $\langle \Delta \rangle$ represents both $2\mathcal{M}$ and $2\overline{\mathcal{M}}$, then $\mathcal{M}\overline{\mathcal{M}} = 4^2 - (\sqrt{10})^2 = 6$ must be a square – a contradiction. Similarly, if it represents $2\mathcal{M}$ and $2\overline{\mathcal{M}} - 1$, then $2\mathcal{M}(2\overline{\mathcal{M}} - 1) = 16 - 2\sqrt{10}$ should be a square, but it is not (the field $\mathbb{Q}\left(\sqrt{16 - 2\sqrt{10}}\right)$ is not biquadratic). The case with $2\overline{\mathcal{M}}$ and $2\mathcal{M} - 1$ is analogous.

The only remaining possibility is when $\Delta z^2 = 2\mathcal{M} - 1 = 7 + 2\sqrt{10}$ and $\Delta z'^2 = 2\overline{\mathcal{M}} - 1 = 7 - 2\sqrt{10}$, in which case $(2\mathcal{M} - 1)(2\overline{\mathcal{M}} - 1) = 9$ is indeed a square. Applying the norm on the equalities $\Delta z^2 = 2\mathcal{M} - 1 = 7 + 2\sqrt{10}$ and $\Delta(z^2 + z'^2) = (2\mathcal{M} - 1) + (2\overline{\mathcal{M}} - 1) = 14$, it follows that $\mathcal{N}_{K/\mathbb{Q}}(\Delta)$ divides both $\mathcal{N}_{K/\mathbb{Q}}(2\mathcal{M} - 1) = 3^4$ and $\mathcal{N}_{K/\mathbb{Q}}(14) = 2^4 \cdot 7^4$; therefore, $\mathcal{N}_{K/\mathbb{Q}}(\Delta) = \pm 1$. However, this would mean that $\Delta = 2\gamma - \beta^2$ is a totally positive unit, hence a square. But then $2\mathcal{M} - 1$ must be a square as well; according to Lemma 1.4.16, this never happens.

1.6.4 $\sqrt{13} \in K$

Just as in the previous section, the only problem caused by $\sqrt{13}$ arises from another possible decomposition in Lemma 1.4.5, so we only have to fix the case of nondiagonalizable forms. In particular, we may again assume that the only totally positive units in the field are the squares of units.

Furthermore, the proofs of the cases with $m < 10$ as well as $m = 10$ do not require the above mentioned lemma. Thus the only potentially problematical field containing $\sqrt{13}$ with $m \neq 13$ could be $\mathbb{Q}(\sqrt{11}, \sqrt{13})$; however, in this field we have a nonsquare totally positive unit $\varepsilon_{11} = 10 + 3\sqrt{11}$, and so Conclusion 1.5.5 applies. Therefore, we can suppose $m = 13$.

Denoting as before $\Delta = 2\gamma - \beta^2$, we can find $z \in \mathcal{O}_K$ such that Δz^2 is either $2\mathcal{M} = 5 + \sqrt{13}$ or $2\mathcal{M} - 1 = 4 + \sqrt{13}$ and $z' \in \mathcal{O}_K$ such that $\Delta z'^2$ is either $2\overline{\mathcal{M}} = 5 - \sqrt{13}$ or $2\overline{\mathcal{M}} - 1 = 4 - \sqrt{13}$. Again we go through all possibilities: If $\Delta z^2 = 2\mathcal{M}$ and $\Delta z'^2 = 2\overline{\mathcal{M}}$, then $\mathcal{M}\overline{\mathcal{M}} = \frac{1}{4}(5^2 - (\sqrt{13})^2) = 3$ must be a square, which it is not. If $\Delta z^2 = 2\mathcal{M} - 1$ and $\Delta z'^2 = 2\overline{\mathcal{M}} - 1$, then $(2\mathcal{M} - 1)(2\overline{\mathcal{M}} - 1) = (4^2 - (\sqrt{13})^2) = 3$ gives a contradiction in the same way. If $\Delta z^2 = 2\mathcal{M}$ and $\Delta z'^2 = 2\overline{\mathcal{M}} - 1$, then $2\mathcal{M}(2\overline{\mathcal{M}} - 1) = 7 - \sqrt{13} = \left(\frac{\sqrt{2} - \sqrt{26}}{2}\right)^2$ is a square only in $\mathbb{Q}(\sqrt{2}, \sqrt{13})$ where $m = 2$. The case with $2\mathcal{M} - 1$ and $2\overline{\mathcal{M}}$ is analogous and also collapses only in the field $\mathbb{Q}(\sqrt{2}, \sqrt{13})$.

1.6.5 $\sqrt{17} \in K$

We use the same technique as in the previous two subsections ($\sqrt{10} \in K$ and $\sqrt{13} \in K$), as the problem with $\sqrt{17} \in K$ is again only in the use of Lemma 1.4.5, and hence it arises only when dealing with the nondiagonalizable form Q_0.

Similarly as above, we may put aside fields with small values of m: All the cases with $m \leq 10$ have been solved without any application of this lemma, and hence are valid also when $\sqrt{17}$ is contained in the field. The same holds for the field $\mathbb{Q}(\sqrt{13}, \sqrt{17})$. Thus it remains to consider the fields $\mathbb{Q}(\sqrt{11}, \sqrt{17})$, $\mathbb{Q}(\sqrt{14}, \sqrt{17})$ and $\mathbb{Q}(\sqrt{15}, \sqrt{17})$; but the corresponding units $\varepsilon_{11} = 10 + 3\sqrt{11}$, $\varepsilon_{14} = 15 + 4\sqrt{14}$ and $\varepsilon_{15} = 4 + \sqrt{15}$ are here totally positive and nonsquare, enabling us to use Conclusion 1.5.5. Thus, there is no harm in assuming $m = 17$.

Just as before, we denote $\Delta = 2\gamma - \beta^2$ and use the nonsquareness and indecomposability of $\mathcal{M} = \frac{1}{2}(5 + \sqrt{17})$. Moreover, note that in this case $2\mathcal{M} - 1$ is not totally positive, thus we get only one possibility from Lemma 1.4.17: There is a $z \in \mathcal{O}_K$ such that $\Delta z^2 = 2\mathcal{M} = 5 + \sqrt{17}$,

and also a $z' \in \mathcal{O}_K$ such that $\Delta z'^2 = 2\overline{\mathcal{M}} = 5 - \sqrt{17}$. Putting the two equalities together, we find that $\mathcal{M}\overline{\mathcal{M}} = \frac{1}{4}(5^2 - (\sqrt{17})^2) = 2$ must be a square, which is a contradiction.

1.6.6 $m = 65$

The problem with $m = 65$ is that in this case, for $\mathcal{M} = \mathcal{M}_{1/2} = \frac{1}{2}(9 + \sqrt{65})$ we have $5\mathcal{M}_{1/2} = \left(\frac{1}{2}\left(5 + \sqrt{65}\right)\right)^2$ (see also Corollary 1.4.14). The only part of the main proof which fails here is if there is no nonsquare totally positive unit in K and we have a nondiagonalizable form, i.e, in Subsection 1.5.5 (see also Conclusion 1.5.8). Thus we have to use a modified approach in this branch of the proof.

The solution is simple since we do not have to change almost anything. We consider the representations of 2 and 5 in exactly the same way as before, and in the place where we used $\mathcal{M} = \mathcal{M}_{1/2}$, we use the number $A = \frac{1}{2}\left(25 + 3\sqrt{65}\right)$; the rest of the proof remains word by word the same. But we have to check the required properties of A by hand:

Lemma 1.6.1. *Let $K = \mathbb{Q}(\sqrt{65}, \sqrt{s})$ where $t > s > 65$; for the element $A = \frac{1}{2}(25 + 3\sqrt{65})$ the following holds:*

1. *A is totally positive,*
2. *A is indecomposable,*
3. *$2A \succcurlyeq \omega^2$ implies $\omega = 0$,*
4. *A, $3A$ and $5A$ are not squares.*

Proof. The claim (1) is trivial and (4) can be seen by checking that the three fields generated by $\sqrt{A}$, $\sqrt{3A}$ and $\sqrt{5A}$ are all of degree four but not biquadratic.

(2) In $\mathbb{Q}(\sqrt{65})$, A is a semiconvergent of $\frac{\sqrt{65}-1}{2}$, thus it is indecomposable in $\mathbb{Q}(\sqrt{65})$. Since $65 \equiv 1 \pmod 4$, then except for basis (B4) we have $m = q$, thus A remains indecomposable in K according to Theorem 1.2.4. In case of basis (B4), we have to check the inequality $\sqrt{t} > 7\sqrt{65}$ to be able to use Theorem 1.2.4 (7 is the biggest coefficient in the continued fraction of $\frac{\sqrt{65}-1}{2}$). If m and s are coprime, then this is clearly always satisfied thanks to $t = 65s$. If, however, they are not, we have $s = 5m_0$ and $t = 13m_0$, which means that the mentioned theorem can be used only if $\sqrt{13m_0} > 7\sqrt{65}$, i.e., if $m_0 > 7^2 \cdot 5$. The indecomposability of A in the remaining fields $\mathbb{Q}(\sqrt{65}, \sqrt{5m_0})$ with $m_0 \equiv 1 \pmod 4$, $13 < m_0 \leq 7^2 \cdot 5$ can be checked directly, e.g., by a computer program.

(3) Denote $\omega = \frac{a}{4} + \frac{b}{4}\sqrt{65} + \frac{c}{4}\sqrt{s} + \frac{d}{4}\sqrt{t}$ for integers a, b, c, d, and suppose $\omega \neq 0$; note that either all of a, b, c, d are even, or all of them are odd. By comparing the traces of $2A$ and ω^2 we obtain the inequality $25 \cdot 16 \geq a^2 + 65b^2 + sc^2 + td^2$. It is immediate that $|b|, |c|, |d| \leq \sqrt{\frac{25 \cdot 16}{65}} < 3$, which leaves the possibilities $b, c, d \in \{0, \pm 1, \pm 2\}$. It is easy to check that all b, c, d cannot be zeros at once. If one of these numbers equals ± 2, the remaining two must be zeros, and the rest of the computation is easy. If, on the other hand, one of them is ± 1, then so must be the remaining two (this follows from the form of the integral basis (B4)) and $s \equiv 1 \pmod 4$. But then we have $25 \cdot 16 \geq 1 + 65 + s + t$; clearly, if 65 and s are coprime, then $t = 65s$, which is too large. If they are not, then we have $s = 5m_0$ and $t = 13m_0$, which gives $334 \geq 18m_0$; together with the condition $m_0 \equiv 1 \pmod 4$ and $m_0 > 13$ the only theoretically possible case is $m_0 = 17$, i.e., the field $\mathbb{Q}(\sqrt{65}, \sqrt{85})$. But one can easily check that none of the possibilities in $25 + 3\sqrt{65} \succcurlyeq (\frac{1}{4}(1 \pm \sqrt{65} \pm \sqrt{85} \pm \sqrt{221}))^2$ holds. Thus, the only $\omega \in \mathcal{O}_K$ with the required property is $\omega = 0$. □

1.6.7 $m = 85$

The problem with $m = 85$ is just the same as with $m = 65$, and it appears only in Subsection 1.5.5. The solution is very similar to that for $m = 65$ (even slightly easier): In the place of the main proof where we used $\mathcal{M} = \mathcal{M}_{1/2}$, we use $\mathcal{M}_1 = 2\mathcal{M}_{1/2} - 1 = 10 + \sqrt{85}$ instead.

The properties of $\mathcal{M}_1$ for $m = 85$ which we need are:

1. $\mathcal{M}_1$ is totally positive (this is immediate),
2. $\mathcal{M}_1$ is indecomposable (this follows from Proposition 1.4.11),
3. $2\mathcal{M}_1 \succcurlyeq \omega^2$ implies $\omega^2 \in \{0, 1\}$ (which can be checked just as in Lemma 1.6.1(3); note that Lemma 1.4.17 cannot be used since here $\mathcal{M} \neq \mathcal{M}_1$),
4. $\mathcal{M}_1$, $3\mathcal{M}_1$ and $5\mathcal{M}_1$ are all nonsquare in K (this comes directly from Lemma 1.4.13).

Once we have these properties, we can replace $\mathcal{M}$ by $\mathcal{M}_1$ and then use the same procedure as in the main proof.

1.6.8 $\sqrt{2} \in K$

In any field K containing $\sqrt{2}$, i.e., in fields where $m = 2$, we exhibit four explicit elements $\lambda_1, \lambda_2, \lambda_3, \lambda_4 \in \mathcal{O}_K^+$ and show that no ternary form over $\mathcal{O}_K$ can represent these four elements at the same time. (In the next subsection we do the same for all fields containing $\sqrt{5}$.) The proof uses the key idea of the method of escalation developed in [BH]. Exceptional cases are handled in Subsection 1.6.10.

Contrary to the rest of the paper, this subsection, as well as the next two ones, uses computer programs significantly. As we will see, in an explicit field, the problem can be reduced to a finite computation. Thus, we first find a relatively small integer N, such that all fields $\mathbb{Q}(\sqrt{2}, \sqrt{s})$ with $s \geq N$ can be solved uniformly via computing determinants of a few hundreds or thousands of matrices (we used a program in Mathematica) – this reduces the infinite family to a finite one. All the remaining cases can be then solved after making some individual adjustments.

To show that four elements $\lambda_1, \ldots, \lambda_4 \in \mathcal{O}_K^+$ cannot be represented by the same ternary form Q, it suffices to prove the following:

There exists no 4×4 symmetric, totally positive semidefinite matrix with entries in $\mathcal{O}_K$ whose diagonal elements are $\lambda_1, \ldots, \lambda_4$ and which is singular.

The reason is as follows: Suppose that all four elements are represented, i.e., $Q(\boldsymbol{\ell}_i) = \lambda_i$ for $\boldsymbol{\ell}_i \in \mathcal{O}_K^3$, $i = 1, \ldots, 4$, and consider the Gram matrix G of $\boldsymbol{\ell}_1, \ldots, \boldsymbol{\ell}_4$ (defined as $G = (g_{ij})$, $g_{ij} = B_Q(\boldsymbol{\ell}_i, \boldsymbol{\ell}_j)$). As a Gram matrix of a totally positive definite form, G is symmetric and totally positive semidefinite, and from the definition it is clear that the λ_i's are its diagonal entries. Since regularity of G would imply linear independence of $\boldsymbol{\ell}_1, \ldots, \boldsymbol{\ell}_4$, it follows that G must be singular.

Therefore, our strategy is to check all possible totally positive semidefinite matrices G with the given diagonal and to prove that they are necessarily regular. If the matrix

$$G = \begin{pmatrix} \lambda_1 & \rho_{12} & \rho_{13} & \rho_{14} \\ \rho_{12} & \lambda_2 & \rho_{23} & \rho_{24} \\ \rho_{13} & \rho_{23} & \lambda_3 & \rho_{34} \\ \rho_{14} & \rho_{24} & \rho_{34} & \lambda_4 \end{pmatrix}$$

is totally positive semidefinite, Sylvester's criterion applied to 2×2 subdeterminants yields the necessary condition $\rho_{ij}^2 \preccurlyeq \lambda_i \lambda_j$ for all non-diagonal entries ρ_{ij}. It turns out that on each

of the six positions (i,j), $i<j$, there are only finitely many numbers ρ_{ij} which satisfy this condition (explicit lists for our choice of diagonal coefficients are provided in Lemma 1.6.2). Thus altogether we obtain only finitely many candidates for matrix G. By checking their determinant, we prove them all to be regular.

The method described so far can be used for *any* totally real field K (and will be used in the next two subsections as well). Now let us start with $\sqrt{2}\in K$, i.e., $m=2$. It also means that s is odd and $t=2s$. In this case, we put

$$\lambda_1=1,\quad \lambda_2=\mathcal{M}=2+\sqrt{2},\quad \lambda_3=3\quad\text{and}\quad \lambda_4=\mathcal{S}.$$

Our next aim is to determine all the possible coefficients ρ_{ij} which satisfy $\lambda_i\lambda_j\succcurlyeq\rho_{ij}^2$ for all i,j. In this case, it follows that $\rho_{12}=0$ since $\lambda_1\lambda_2=\mathcal{M}=2+\sqrt{2}$ is indecomposable in K and not a square, see Proposition 1.4.9 and Corollary 1.4.14. In the same manner, we can see that $\rho_{14}=0$, which is a consequence of the indecomposability of $\mathcal{S}$ in K, see Proposition 1.4.10, and of the fact that $\mathcal{S}$ is not a square except for the cases when $s=3$ or 5, see Lemma 1.4.15. These cases will be resolved separately in Subsection 1.6.10. Lemma 1.4.3 claims that possible values of ρ_{13} belong to the set $\{0,\pm1,\pm\sqrt{2}\}$ for $s\neq3,5$. The remaining coefficients ρ_{ij} are examined in the following lemma.

Lemma 1.6.2. *Let s be an odd square-free positive integer such that $s\neq3,5,7,11,13,15,17,19,21,29,33$, and $K=\mathbb{Q}(\sqrt{2},\sqrt{s})$.*

1. *If $3(2+\sqrt{2})\succcurlyeq\omega^2$ where $\omega\in\mathcal{O}_K$, then $\omega\in\{0,\pm1,\pm(1+\sqrt{2})\}$.*
2. *If $(2+\sqrt{2})\mathcal{S}\succcurlyeq\omega^2$ where $\omega\in\mathcal{O}_K$, then $\omega=0$.*
3. *If $3\mathcal{S}\succcurlyeq\omega^2$ where $\omega\in\mathcal{O}_K$, then $\omega\in\{0,\pm1,\pm\sqrt{2}\}$.*

Proof. We will show only part (3) of this lemma, the proofs of the other statements are analogous. First of all, let $s\equiv3\pmod4$, which implies that $\mathcal{S}=\mathcal{S}_1=\lceil\sqrt{s}\rceil+\sqrt{s}$. If

$$\omega=\frac{a}{2}+\frac{b}{2}\sqrt{2}+\frac{c}{2}\sqrt{s}+\frac{d}{2}\sqrt{2s}$$

for some $a,b,c,d\in\mathbb{Z}$, then by comparing the traces of $3\mathcal{S}$ and ω^2 we can conclude that

$$3\lceil\sqrt{s}\rceil\geq\frac{a^2}{4}+\frac{b^2}{2}+\frac{c^2}{4}s+\frac{d^2}{2}s.$$

If $\frac{s}{4}>3\lceil\sqrt{s}\rceil$, then necessarily $c=d=0$ and ω belongs to the quadratic subfield $\mathbb{Q}(\sqrt{2})$; this occurs whenever $s\geq168$. In such a case, it follows that $\omega=a'+b'\sqrt{2}$ where $a',b'\in\mathbb{Z}$, which means that

$$3\lceil\sqrt{s}\rceil+3\sqrt{s}\succcurlyeq a'^2+2b'^2+2a'b'\sqrt{2}.$$

This inequality can be satisfied only if

$$3\lceil\sqrt{s}\rceil-3\sqrt{s}\geq a'^2+2b'^2,$$

from which follows that $a'^2+2b'^2<3$. Hence $\omega\in\{0,\pm1,\pm\sqrt{2}\}$. It is easy to verify by a computer program that this is in fact also true for all $s<168$ except of the ones listed in the statement of this lemma. We can use similar argumentation for $s\equiv1\pmod4$. □

Knowing all possible values of ρ_{ij}, we are able to construct all totally positive semidefinite matrices with the given diagonal – so to finish our task, it suffices to check their determinants. A minor problem which has to be handled is that the value of $\mathcal{S}$ depends on the chosen field K, but this can easily be overcome:

Lemma 1.6.3. *There are no singular 4×4 totally positive semidefinite matrices with diagonal entries $\lambda_1 = 1$, $\lambda_2 = 2 + \sqrt{2}$, $\lambda_3 = 3$ and $\lambda_4 = \mathcal{S}$ over $\mathcal{O}_K$ for $K = \mathbb{Q}(\sqrt{2}, \sqrt{s})$ where $s \neq 3, 5, 7, 11, 13, 15, 17, 19, 21, 29, 33$.*

Proof. From Lemma 1.6.2 and the discussion above it we already know all the possible matrices G, so it suffices to show that none of them has determinant zero: Observe that $\mathcal{S}$ is the only element in the matrix which does not lie in $\mathbb{Q}(\sqrt{2})$. If we denote by Δ the determinant of the upper left 3×3 matrix, then expansion of the determinant of G along the last column gives an equality of the form $\Delta\mathcal{S} + \alpha = \det G$ for some $\alpha \in \mathbb{Q}(\sqrt{2})$.

Suppose that $\det G = 0$. By running a computer program we easily check that $\Delta \neq 0$ for all the candidate matrices, so the above equality is a nontrivial linear equation for $\mathcal{S} \notin \mathbb{Q}(\sqrt{2})$ with coefficients in $\mathbb{Q}(\sqrt{2})$; this is a contradiction. □

By this we have proven the nonexistence of universal ternary forms over $\mathbb{Q}(\sqrt{2}, \sqrt{s})$ except for eleven specific values of s. We postpone $s = 3, 5, 21, 33$ to Subsection 1.6.10 and consider all the other remaining values: The only difference for $s = 7, 11, 13, 15, 17, 19, 29$ is that we get more possibilities for the coefficient ρ_{34} (i.e., the corresponding fields contain more elements ω such that $3\mathcal{S} \succcurlyeq \omega^2$), whereas the parts (1) and (2) of Lemma 1.6.2 still hold even for these values of s. For some possible choices of ρ_{34} we cannot use the procedure introduced in the proof of Lemma 1.6.3, as they do not belong to $\mathbb{Q}(\sqrt{2})$. However, now we work in concrete fields, and in each of them, there are only finitely many possibilities for ρ_{34} (compare the traces of $3\mathcal{S}$ and ρ_{34}^2); thus, we can compute explicitly all the corresponding 4×4 determinants to check that they are nonzero. This extends Lemma 1.6.3, and thus also resolves the nonexistence of a universal ternary quadratic form, to all the values of s except for $s = 3, 5, 21, 33$.

Thus, we have proven the following conclusion.

Conclusion 1.6.4. *In a biquadratic field $K = \mathbb{Q}(\sqrt{2}, \sqrt{s})$ with $s \neq 3, 5, 21, 33$, no ternary form can simultaneously represent all the numbers 1, $\mathcal{M} = 2 + \sqrt{2}$, 3 and $\mathcal{S}$ at the same time.*

1.6.9 $\sqrt{5} \in K$

Since we postpone the fields $\mathbb{Q}(\sqrt{2}, \sqrt{5})$ and $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ (together with a few other fields) to Subsection 1.6.10, we shall require $m = 5$. We use exactly the same strategy as for $m = 2$, which was outlined at the beginning of Subsection 1.6.8. The only difference lies in the exact choice of the four elements to perform the escalation with; this time, we put

$$\lambda_1 = 1, \quad \lambda_2 = 2, \quad \lambda_3 = 6 + \sqrt{5} \quad \text{and} \quad \lambda_4 = \mathcal{S}.$$

Recall that we need to compute all values of ρ_{ij} satisfying $\lambda_i\lambda_j \succcurlyeq \rho_{ij}^2$. Clearly, $\rho_{12} \in \{0, -1, 1\}$ and $\rho_{14} = 0$ except for $s = 3, 5$ (see Lemma 1.4.15), which we have postponed to the next subsection. The sets for other coefficients are computed in the following lemma.

Lemma 1.6.5. *Let s be a square-free positive integer such that $5 \nmid s$ and $s \neq 2, 3, 6, 7, 13, 17, 21, 29, 33, 37, 53$, and let $K = \mathbb{Q}(\sqrt{5}, \sqrt{s})$.*

1. *If $6 + \sqrt{5} \succcurlyeq \omega^2$ where $\omega \in \mathcal{O}_K$, then*

$$\omega \in \left\{0, \pm 1, \pm\frac{1+\sqrt{5}}{2}, \pm\frac{1-\sqrt{5}}{2}, \pm\frac{3+\sqrt{5}}{2}\right\}.$$

2. *If $2(6 + \sqrt{5}) \succcurlyeq \omega^2$ where $\omega \in \mathcal{O}_K$, then*

$$\omega \in \left\{0, \pm 1, \pm 2, \pm\sqrt{5}, \pm(1+\sqrt{5}), \pm\frac{1+\sqrt{5}}{2}, \pm\frac{1-\sqrt{5}}{2}, \pm\frac{3+\sqrt{5}}{2}, \pm\frac{5+\sqrt{5}}{2}\right\}.$$

3. *If* $2\mathcal{S} \succcurlyeq \omega^2$ *where* $\omega \in \mathcal{O}_K$, *then* $\omega \in \{0, -1, 1\}$.

4. *If* $(6+\sqrt{5})\mathcal{S} \succcurlyeq \omega^2$ *where* $\omega \in \mathcal{O}_K$, *then*

$$\omega \in \left\{0, \pm 1, \pm\frac{1+\sqrt{5}}{2}, \pm\frac{1-\sqrt{5}}{2}, \pm\frac{3+\sqrt{5}}{2}\right\}.$$

Proof. We can use analogous argumentation as for $m = 2$: In all four cases, comparing traces yields an inequality which clearly allows only finitely many choices of ω; moreover, for s sufficiently large, $\omega \in \mathbb{Q}(\sqrt{m})$ can be proven. The rest is only a straightforward checking of inequalities, readily handled by a computer program. □

The previous lemma together with the knowledge of possible choices for ρ_{12} and ρ_{14} allows us to prove that none of the resulting Gram matrices has determinant zero by the same small trick as in Lemma 1.6.3. Thus, under the assumptions of the previous lemma, we cannot find any ternary universal quadratic form over $\mathcal{O}_K$.

If $s = 7$, we obtain more choices of ω for $2(6+\sqrt{5})$, while the other sets of coefficients remain unchanged; for $s = 29, 37, 53$, we get a larger set only in part (4), i.e., for $(6+\sqrt{5})\mathcal{S}$. However, even after including these modifications, the regularity of all the resulting 4×4 matrices over these concrete fields can be checked by a direct computation. Thus, we have proven the following statement.

Conclusion 1.6.6. *In a biquadratic field* K *where* $m = 5$ *and* $s \neq 6, 13, 17, 21, 33$, *no ternary form can simultaneously represent all the numbers* 1, 2, $6+\sqrt{5}$ *and* $\mathcal{S}$ *at the same time.*

It remains to solve the cases when $s = 2, 3, 6, 13, 17, 21, 33$. Of course, $s = 2, 3$ is absurd if $m = 5$. Moreover, the cases with $s = 6, 21, 33$ have already been solved in Subsection 1.6.2. The only remaining fields $\mathbb{Q}(\sqrt{5}, \sqrt{13})$ and $\mathbb{Q}(\sqrt{5}, \sqrt{17})$ will be handled in Subsection 1.6.10.

1.6.10 Remaining biquadratic fields

For the remaining biquadratic fields, we use the procedure introduced in Subsection 1.6.8. We find elements $\lambda_1, \lambda_2, \lambda_3, \lambda_4 \in \mathcal{O}_K^+$ such that every symmetric totally positive semidefinite matrix over $\mathcal{O}_K$ with them on the diagonal is regular, thereby showing that no ternary form can represent them all. In fact, we put $\lambda_1 = 1$ and conveniently choose the other λ_i's; if possible, we prefer indecomposable integers in these fields. Consequently, by solving inequalities $\rho_{ij}^2 \preccurlyeq \lambda_i\lambda_j$ with the help of a computer (upper bounds on coefficients ρ_{ij}^2 are, as always, obtained by comparing traces, so there are only finitely many values to be checked), we obtain all possible non-diagonal entries of totally positive semidefinite matrices with the given diagonal. To complete the proof, it suffices to compute all the determinants. In Table 1.1, we exhibit the quadruples of λ_i's which we used and for which all the resulting candidates for totally positive semidefinite Gram matrices are regular. It implies that even in these fields, there cannot exist a ternary universal quadratic form, and we even explicitly know four elements that are never represented by the same form. Note that $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ was already solved in [Č+, Subsec. 5.1] by the same method; here we list the diagonal coefficients which were used in that article.

By this, the proof of Theorem 1.1.1 is finished.

Open questions

Although we achieved our goal and proved that no totally real biquadratic field admits a ternary universal quadratic form, there are many very natural open problems. One may want to generalize this result to non-classical forms; however, the corresponding problem is, to our best knowledge, still open even for the much simpler case of quadratic fields. More interesting

m	s	t	λ_2	λ_3	λ_4
2	3	6	$4+\frac{5}{2}\sqrt{2}+2\sqrt{3}+\frac{3}{2}\sqrt{6}$	$3+\sqrt{6}$	$3-\frac{3}{2}\sqrt{2}-\sqrt{3}+\frac{1}{2}\sqrt{6}$
2	5	10	$2+\sqrt{2}$	3	$\frac{5}{2}+\frac{1}{2}\sqrt{2}+\frac{1}{2}\sqrt{5}+\frac{1}{2}\sqrt{10}$
2	21	42	$2+\sqrt{2}$	$\frac{5}{2}+\frac{1}{2}\sqrt{21}$	$5+\frac{5}{2}\sqrt{2}+\sqrt{21}+\frac{1}{2}\sqrt{42}$
2	33	66	$2+\sqrt{2}$	$\frac{7}{2}+\frac{1}{2}\sqrt{33}$	$6+\sqrt{33}$
3	5	15	$2+\sqrt{3}$	$\frac{5}{2}+\frac{1}{2}\sqrt{3}+\frac{1}{2}\sqrt{5}+\frac{1}{2}\sqrt{15}$	$3+\frac{1}{2}\sqrt{3}+\frac{1}{2}\sqrt{15}$
5	13	65	$\frac{5}{2}+\frac{1}{2}\sqrt{13}$	$4+\sqrt{13}$	$\frac{13}{4}+\frac{3}{4}\sqrt{5}+\frac{3}{4}\sqrt{13}+\frac{1}{4}\sqrt{65}$
5	17	85	$\frac{5}{2}+\frac{1}{2}\sqrt{17}$	$\frac{29}{2}+\frac{7}{2}\sqrt{17}$	$\frac{13}{4}+\frac{1}{4}\sqrt{5}+\frac{1}{4}\sqrt{17}+\frac{1}{4}\sqrt{85}$

Table 1.1: Chosen diagonal coefficients

question is, which (if any) biquadratic fields admit a quaternary universal form, and more generally, what is the lowest number of variables n such that there is a biquadratic field which admits an n-ary universal form. And for which n are there infinitely many such fields? Tools developed in this paper should prove useful in investigating these problems. A bolder generalization of our result, namely the nonexistence of universal ternary forms for all totally real multiquadratic fields, would provide strong evidence towards Kitaoka's conjecture.

Theorem 1.1.3 significantly extended our knowledge about indecomposable integers in biquadratic fields; however, there is a very natural open question: Is it possible for an element from the subfields $\mathbb{Q}(\sqrt{m})$ or $\mathbb{Q}(\sqrt{s})$ to decompose in the biquadratic extension, or can this happen only for the subfield $\mathbb{Q}(\sqrt{t})$, as evidence seems to suggest?

Appendix

1.7 Ternary forms over the quadratic field $\mathbb{Q}(\sqrt{10})$

The main source of inspiration for this article is the beautiful paper [CKR], which proves that real quadratic fields except for $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{5})$ admit no universal ternary forms, and fully describes universal ternary forms over those three fields. We have found two discrepancies in the proof of nonuniversality given there; this appendix is devoted to their corrections. Both of the problems arise when dealing with a nondiagonalizable form $\langle 1\rangle \perp Q_0$ (denoted there as $\langle 1\rangle \perp L_0$; the analogous part in this paper is Subsection 1.5.5) over a totally real quadratic field F. Just as in our proof, $\boldsymbol{e} \in \mathcal{O}_F^2$ is a vector such that $Q_0(\boldsymbol{e}) = 2$, and $\boldsymbol{f} \in F^2$ is a "complementing vector" such that $\mathcal{O}_F = \mathcal{I}_{\boldsymbol{e}}\boldsymbol{e} \oplus \mathcal{I}_{\boldsymbol{f}}\boldsymbol{f}$ and $\mathcal{I}_{\boldsymbol{e}} = \mathcal{I}_{\boldsymbol{f}}^{-1}$.

The first problem was the claim that $\gamma = Q_0(\boldsymbol{f}) \in \mathcal{O}_F$; that is not always the case, as we shall see in Example 1.7.1. However, for the rest of the proof, it is sufficient that $2\gamma \in \mathcal{O}_F$; this we have proven in Lemma 1.5.7. (We also show there that $\beta = B_{Q_0}(\boldsymbol{e}, \boldsymbol{f})$ belongs to $\mathcal{O}_F$, which was stated but not proven in [CKR].)

Example 1.7.1. In $F = \mathbb{Q}(\sqrt{10})$, consider the binary form

$$Q_0(v, w) = 7v^2 - 2 \cdot 3\sqrt{10}vw + 13w^2. \tag{1.7.1}$$

Note that it is totally positive definite, since $7 \in \mathcal{O}_F^+$ and $\det Q_0 = 7 \cdot 13 - (3\sqrt{10})^2 = 1 \in \mathcal{O}_F^+$. We show that Q_0 is not diagonalizable: If it is, then by comparing determinants it follows that $Q_0 \cong \langle 1\rangle \perp \langle 1\rangle$ (using the fact that, in this field, $\mathcal{U}_F^+ = \mathcal{U}_F^{\square}$); however, Q_0 represents 7 while it is easy to check that $\langle 1\rangle \perp \langle 1\rangle$ does not.

For $\boldsymbol{e} = (\sqrt{10}, 2)^{\mathrm{T}}$ we see that $Q_0(\boldsymbol{e}) = 2$ and $\mathcal{I}_{\boldsymbol{e}} = (\sqrt{10}, 2)^{-1} = (\frac{\sqrt{10}}{2}, 1)$. Set $\boldsymbol{f} = (1, 1 + \frac{\sqrt{10}}{2})^{\mathrm{T}}$; clearly $\mathcal{I}_{\boldsymbol{f}} = (\sqrt{10}, 2)$, so indeed $\mathcal{I}_{\boldsymbol{e}}\mathcal{I}_{\boldsymbol{f}} = \mathcal{O}_F$, and it is routine to check $\mathcal{I}_{\boldsymbol{e}}\boldsymbol{e} + \mathcal{I}_{\boldsymbol{f}}\boldsymbol{f} = \mathcal{O}_F^2$. Further, we compute

$$\gamma = Q_0(\boldsymbol{f}) = \frac{45}{2} + 7\sqrt{10}, \qquad \beta = B_{Q_0}(\boldsymbol{e}, \boldsymbol{f}) = -4 - \sqrt{10};$$

obviously, $\gamma \notin \mathcal{O}_F$ (but $2\gamma \in \mathcal{O}_F$) and $\beta \in \mathcal{O}_F$.

On a side note, there are altogether four vectors which represent 2, namely $\pm(\sqrt{10}, 2)^{\mathrm{T}}$ and $\pm(4, \sqrt{10})^{\mathrm{T}}$; the property $\mathcal{I}_{\boldsymbol{e}} = (\sqrt{10}, 2)^{-1}$ holds for all of them.

The second problem in the paper [CKR] is that the proof is not completely correct in the case of $F = \mathbb{Q}(\sqrt{10})$. The problematic claim is: *If the number* 10 *is represented by the form* $2Q_0$ *as* $2Q_0(y\boldsymbol{e} + z\boldsymbol{f}) = (2y + \beta z)^2 + (2\gamma - \beta^2)z^2$, *then* $(2y + \beta z)^2$ *is necessarily a square of an integer* (compare with Lemma 1.4.5). This is not true; it can also happen that $(2y + \beta z)^2 = (\pm\sqrt{10})^2$.

Note that $2y + \beta z = \pm\sqrt{10}$ and $(2\gamma - \beta^2)z^2 = 0$ if and only if $z = 0$ and $y = \pm\frac{\sqrt{10}}{2}$. Since $y \in \mathcal{I}_{\boldsymbol{e}}$, this implies $\mathcal{I}_{\boldsymbol{e}} \neq \mathcal{O}_F$. Moreover, $(\sqrt{10}, 2)$ is a prime ideal satisfying $(\sqrt{10}, 2)^2 = (2)$; since the square of the ideal $\mathcal{I}_{\boldsymbol{f}} = \mathcal{I}_{\boldsymbol{e}}^{-1}$ divides (2) and here we have $\mathcal{I}_{\boldsymbol{f}} \neq \mathcal{O}_F$, it follows that necessarily $\mathcal{I}_{\boldsymbol{f}} = (\sqrt{10}, 2)$. Then $\mathcal{I}_{\boldsymbol{e}} = (\sqrt{10}, 2)^{-1} = (\frac{\sqrt{10}}{2}, 1)$, hence indeed $\pm\frac{\sqrt{10}}{2} \in \mathcal{I}_{\boldsymbol{e}}$, and the vector $\pm\frac{\sqrt{10}}{2}\boldsymbol{e} + 0\boldsymbol{f}$ belongs to $\mathcal{O}_F^2$.

Remark 1.7.2. In the above paragraph, we have actually proven the following: If Q_0 is a (totally positive definite, classical) binary form over $\mathbb{Q}(\sqrt{10})$ and $\boldsymbol{e} \in \mathcal{O}_F^2$ is such that $Q_0(\boldsymbol{e}) = 2$ and $\mathcal{I}_{\boldsymbol{e}} \neq \mathcal{O}_F$, then $\mathcal{I}_{\boldsymbol{e}} = (\sqrt{10}, 2)^{-1}$.

Now we proceed to illustrate the problem on the form Q_0 given in the example above.

Example 1.7.3. Let us continue with Example 1.7.1; we consider the form Q_0 given by (1.7.1), $\boldsymbol{e} = (\sqrt{10}, 2)^{\mathrm{T}}$ and $\boldsymbol{f} = (1, 1 + \frac{\sqrt{10}}{2})^{\mathrm{T}}$. For $y \in \mathcal{I}_{\boldsymbol{e}}$ and $z \in \mathcal{I}_{\boldsymbol{f}}$, we compute

$$Q_0(y\boldsymbol{e} + z\boldsymbol{f}) = 2y^2 + 2\beta yz + \gamma z^2 = 2y^2 + 2(-4 - \sqrt{10})yz + \Big(\frac{45}{2} + 7\sqrt{10}\Big)z^2;$$

thus,

$$2Q_0(y\boldsymbol{e} + z\boldsymbol{f}) = (2y + \beta z)^2 + (2\gamma - \beta^2)z^2 = \big(2y + (-4 - \sqrt{10})z\big)^2 + (19 + 6\sqrt{10})z^2.$$

By plugging in $y = \pm\frac{\sqrt{10}}{2}$ and $z = 0$, we indeed get $10 = (\sqrt{10})^2 + 0$.

Actually, for an arbitrary form Q_0, if 2 is represented by Q_0 by a vector $\boldsymbol{e}$ such that $\mathcal{I}_{\boldsymbol{e}} \neq \mathcal{O}_F$, then 5 is automatically represented by Q_0 as well, because we have just seen that $\frac{\sqrt{10}}{2}\boldsymbol{e} \in \mathcal{O}_F^2$, and

$$Q_0\Big(\frac{\sqrt{10}}{2}\boldsymbol{e}\Big) = \Big(\frac{\sqrt{10}}{2}\Big)^2 \cdot Q_0(\boldsymbol{e}) = \frac{10}{4} \cdot 2 = 5.$$

Therefore, if $\mathcal{I}_{\boldsymbol{e}} \neq \mathcal{O}_F$, no new information can be gained by considering representations of 10 by $2Q_0$. Instead of that, we have to consider another element of $\mathcal{O}_F^+$ to show the nonexistence of a universal form.

Proposition 1.7.4. *No ternary form $\langle 1\rangle \perp Q_0$ over $F = \mathbb{Q}(\sqrt{10})$ such that $Q_0(\boldsymbol{e}) = 2$ for a vector $\boldsymbol{e} \in \mathcal{O}_F^2$ with $\mathcal{I}_{\boldsymbol{e}} \neq \mathcal{O}_F$ is universal; in fact, such a form never represents $\mathcal{M} = 4 + \sqrt{10}$.*

Proof. Since $\mathcal{I}_{\boldsymbol{e}} \neq \mathcal{O}_F$, Remark 1.7.2 implies $\mathcal{I}_{\boldsymbol{e}} = (\sqrt{10}, 2)^{-1}$. Suppose that $\langle 1\rangle \perp Q_0$ represents $\mathcal{M}$. Just as in the proof of Theorem 1.1.1, since $\mathcal{M}$ is indecomposable and nonsquare, it has to be represented by the binary form Q_0, and therefore $2\mathcal{M}$ is represented by $2Q_0$; using the representation $2Q_0(y\boldsymbol{e} + z\boldsymbol{f}) = (2y + \beta z)^2 + (2\gamma - \beta^2)z^2$, we see that $2\mathcal{M}$ decomposes as a sum of a square and a totally nonnegative number. Lemma 1.4.17 (or a simple direct computation) shows that the square is either 0 or 1. However, since $2 \in \mathcal{I}_{\boldsymbol{e}}^{-2}$, $y \in \mathcal{I}_{\boldsymbol{e}}$, $\beta \in \mathcal{O}_F$ and $z \in \mathcal{I}_{\boldsymbol{e}}^{-1}$, we get $2y + \beta z \in \mathcal{I}_{\boldsymbol{e}}^{-1} = (\sqrt{10}, 2)$, which is a nontrivial ideal, so it cannot contain ± 1.

Therefore, the only choice is $2y + \beta z = 0$ and $(2\gamma - \beta^2)z^2 = 2\mathcal{M}$; denote $\Delta = 2\gamma - \beta^2$. Observe that since $z \in (\sqrt{10}, 2)$, we get $\mathcal{N}_{F/\mathbb{Q}}(z) \in 2\mathbb{Z}$. It is also easy to compute the norm $\mathcal{N}_{F/\mathbb{Q}}(\mathcal{M}) = \mathcal{N}_{F/\mathbb{Q}}\left(4 + \sqrt{10}\right) = 6$. Now let us apply norms on the equation $\Delta z^2 = 2\mathcal{M}$: We obtain

$$\mathcal{N}_{F/\mathbb{Q}}(\Delta)\,\mathcal{N}_{F/\mathbb{Q}}(z)^2 = 4 \cdot 6.$$

Since this equals $2^3 \cdot 3$, it means that $\mathcal{N}_{F/\mathbb{Q}}(z)$ can only be ± 1 or ± 2; since the former possibility is excluded by our observation that the norm of z is even, it must hold that $\mathcal{N}_{F/\mathbb{Q}}(z) = \pm 2$. However, there is no element of norm ± 2 in F: The equality $x^2 - 10y^2 = \pm 2$ would mean $x^2 \equiv \pm 2 \pmod 5$, which is a contradiction. □

1.8 Units in biquadratic fields

In this appendix, we present some results on units in totally real biquadratic fields. In particular, we are interested in the existence of a nonsquare totally positive unit. If such a unit exists, then one of the simplest parts of the proof of Theorem 1.1.1 contained in Subsections 1.5.1 and 1.5.2 is applicable. Indeed, as we will see, this is often the case.

The units of a quadratic field are well understood: A quadratic field $\mathbb{Q}(\sqrt{n})$ contains a nonsquare totally positive unit if and only if its fundamental unit ε_n has (quadratic) norm $+1$ (in which case *every* unit is either totally positive or totally negative). That happens for almost all fields – a necessary condition for $\mathcal{N}_{\mathbb{Q}(\sqrt{n})/\mathbb{Q}}(\varepsilon_n) = -1$ is that n is divisible by no prime of the form $4k + 3$, because clearly -1 must be a quadratic residue modulo every divisor of n.

The situation in a biquadratic field is a bit more difficult (see, e.g., [MU]). Note that a totally positive fundamental unit of a quadratic subfield may become a square in the biquadratic field; in such a case, its square root is not totally positive anymore (this follows from Lemma 1.4.1(1), since no element of zero trace can be totally positive).

We start by showing that in most biquadratic fields, at least one nonsquare totally positive unit exists. Remember that the meaning of m, s, t and n_1, n_2, n_3 is fixed by Convention 1.2.2.

Lemma 1.8.1. *If $K = \mathbb{Q}(\sqrt{m}, \sqrt{s})$, then:*

- *the fundamental unit of $\mathbb{Q}(\sqrt{m})$ is not a square in K;*
- *if $m \neq 2$, then the fundamental unit of $\mathbb{Q}(\sqrt{s})$ is not a square in K.*

More generally, let K be a biquadratic number field. If $\gcd(n_2, n_3) \geq 3$, then the fundamental unit of $\mathbb{Q}(\sqrt{n_1})$ is not a square in K.

Proof. The last, most general statement follows directly from Corollary 1.4.2: Since $\gcd(n_2, n_3) \geq 3$ is square-free, it has some nontrivial odd divisor. However, no unit can have a nontrivial rational integer divisor.

The claims about $\mathbb{Q}(\sqrt{m})$ and $\mathbb{Q}(\sqrt{s})$ are simple corollaries: If $\gcd(n_2, n_3) \leq 2$, then it holds that $n_1 = \frac{n_2 n_3}{\gcd(n_2, n_3)^2} > n_2, n_3$ (i.e., $n_1 = t$) unless one of n_2, n_3 equals 2. □

Note that although Lemma 1.8.1 shows that in most cases, ε_m as well as ε_s are nonsquare units (and we already know that in most cases they are totally positive), it does *not* mean that then there are at least two independent nonsquare totally positive units in $\mathcal{O}_K$. It is quite possible that $\varepsilon_m \varepsilon_s$ is a square.

Another important piece of information for the proof of Theorem 1.1.1 is whether 2ε is a square or not. Note that since in a quadratic field the fundamental unit differs from any other positive nonsquare unit only by multiplication by a square, the following lemma actually generalizes to any positive nonsquare unit:

Lemma 1.8.2. *Let $F = \mathbb{Q}(\sqrt{n_1})$ and $\varepsilon \in F$ be the fundamental unit.*

- *If $n_1 \neq 2$, then 2ε is a square in F if and only if $\mathcal{O}_F$ contains an element of (quadratic) norm ± 2 with integer coefficients, i.e., if and only if at least one of the Pell's equations $x^2 - n_1 y^2 = \pm 2$ is solvable.*
- *Suppose 2ε is not a square in F, and the biquadratic field $K \supseteq F$ satisfies $\gcd(n_2, n_3) \geq 3$. Then 2ε is not a square in K either.*

Proof. The second part is a simple consequence of Corollary 1.4.2 (clearly 2ε cannot have any odd rational integer divisors). As for the first one, start by observing that for an element $\frac{a}{2} + \frac{b}{2}\sqrt{n_1}$ with a, b odd integers, $n_1 \equiv 1 \pmod 4$, its square is of the same form. Thus, since 2ε has always integer coefficients, its potential square root must have the form $a' + b'\sqrt{n_1}$ for some $a', b' \in \mathbb{Z}$.

If $\sqrt{2\varepsilon}$ exists in $\mathcal{O}_F$, then clearly $\mathcal{N}_{F/\mathbb{Q}}\left(\sqrt{2\varepsilon}\right) = \pm 2$, which proves one implication. As for the other, take $\alpha = x + \sqrt{n_1} y$ where $\mathcal{N}_{F/\mathbb{Q}}(\alpha) = x^2 - n_1 y^2 = \pm 2$. Then

$$\alpha^2 = (x^2 + n_1 y^2) + 2xy\sqrt{n_1} = (\pm 2 + 2n_1 y^2) + 2xy\sqrt{n_1},$$

thus $\frac{1}{2}\alpha^2 \in \mathcal{O}_F$. Moreover, $\frac{1}{2}\alpha^2$ is a unit, thus $\alpha^2 = 2\varepsilon^k$ for some $k \in \mathbb{Z}$ (it cannot be $-2\varepsilon^k$, since α^2 is positive whereas $-2\varepsilon^k$ is negative due to ε being fundamental). Clearly, if k was even, then 2 would be a square, i.e., $n_1 = 2$. Therefore $k = 2l + 1$ and we have $2\varepsilon = (\alpha \varepsilon^{-l})^2$. □

From the previous two lemmas we can make a simple but strong conclusion: Suppose that in $K = \mathbb{Q}(\sqrt{m}, \sqrt{s})$, the square-free integer m satisfies the following: The Pell's equation $x^2 - my^2 = a$ has no solution for all three right-hand sides $a = -1$, $a = -2$ and $a = 2$. Then the fundamental unit of $\mathbb{Q}(\sqrt{m})$, ε_m, is totally positive and neither ε_m nor $2\varepsilon_m$ is a square in K.

By considering quadratic residues, it is easy to see that a sufficient condition for non-solvability of all three equations is that m is divisible by

- at least one prime of the form $4k + 3$ (because of $a = -1$), and
- at least one prime of the form $8k + 3$ or $8k - 3$ (due to $a = 2$), and
- at least one prime of the form $8k - 1$ or $8k - 3$ (regarding $a = -2$).

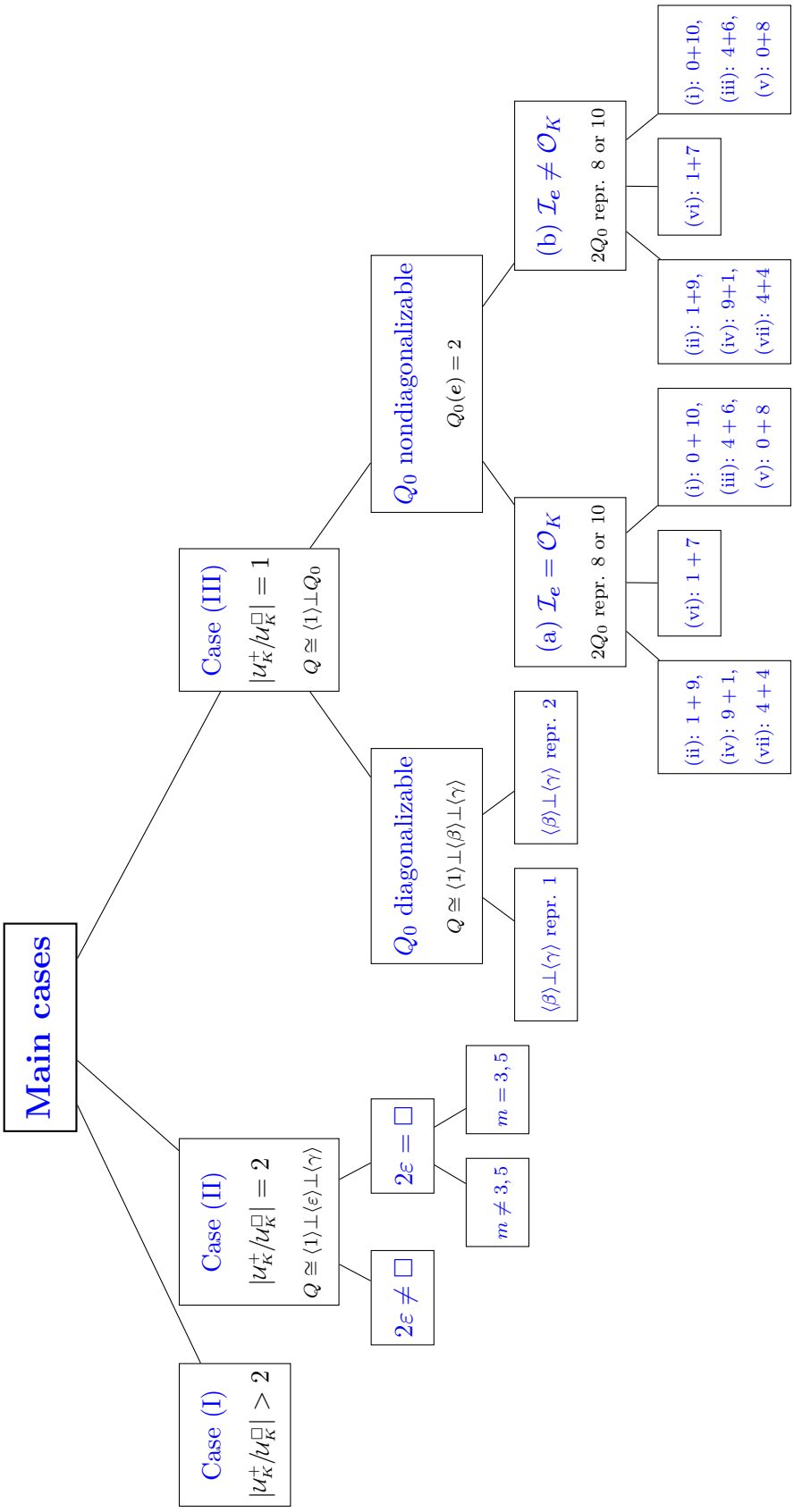
All in all, the only potentially "bad-behaving" m's are those which contain in their prime decomposition only primes 2, $8k + 1$ and one more residue class modulo 8. Clearly, the density of such integers is zero.

Of course, it is possible to continue this examination by deriving some analogy of Lemmas 1.8.1 and 1.8.2 for fields containing $\sqrt{2}$; however, the already presented results are sufficient to illustrate that fields not containing any nonsquare totally positive unit are rare and that mostly this unit multiplied by 2 is not a square either. We conclude this part by showing that for some integral bases, there is always a nonsquare totally positive unit in K.

Corollary 1.8.3. *If K contains no nonsquare totally positive unit, then either $m = 2$, or the integral basis is one of (B2) and (B4a).*

Proof. If $m \neq 2$, by Lemma 1.8.1 neither ε_m nor ε_s is a square. Thus, for a contradiction, it suffices to show that at least one of them is totally positive. It turns out that for all bases except (B2) and (B4a), at least one of the numbers m and s contains a prime divisor of the form $4k + 3$, which shows that the corresponding field contains no unit of norm -1. □

1.9 Scheme of the main proof



2. Pythagoras numbers of orders in biquadratic fields

This chapter contains the paper [KRS] J. Krásenský, M. Raška and E. Sgallová, *Pythagoras numbers of orders in biquadratic fields*, Expo. Math. 40, 1181–1228 (2022).

2.1 Introduction

The study of sums of squares has a long tradition. Already Diophantus was aware that every natural number is a sum of four squares, a fact proven by Lagrange in 1770. Maaß [Ma] proved that for any totally positive integer of $\mathbb{Q}(\sqrt{5})$, three squares are sufficient. Siegel [Si] later showed that this is a rather exceptional property: $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{5})$ are the only totally real number fields where each totally positive algebraic integer is a sum of integral squares.

To remedy this fact, it is customary to consider only those elements of a commutative ring R which can be written as a sum of squares; these elements form a set often denoted by $\sum R^2$. For $\alpha \in \sum R^2$ we define its *length* $\ell(\alpha)$ as the minimal number of squares by which we can represent α. For example, $\ell(7) = 4$ in $\mathbb{Z}$. The *Pythagoras number* of R is then

$$\mathcal{P}(R) = \sup\{\ell(\alpha) : \alpha \in \textstyle\sum R^2\},$$

i.e. the smallest number n such that any sum of squares is in fact a sum of n squares. In this terminology, $\mathcal{P}(\mathbb{Z}) = 4$ and $\mathcal{P}(\mathcal{O}_{\mathbb{Q}(\sqrt{5})}) = 3$. The Pythagoras number of an order in a number field K is always finite; in fact, if the number field K is not totally real, then $\mathcal{P}(\mathcal{O}) \leq 5$ for any order $\mathcal{O}$, and $\mathcal{P}(\mathcal{O}_K) \leq 4$ for the maximal one (see [Pf]). In the most difficult case of orders of totally real number fields, little is known. Scharlau [Sch2] has shown that the Pythagoras number of such an order can be arbitrarily large, but conjectured that it can be bounded by a function depending only on the degree of K. This was recently proven by Kala and Yatsyna [KY2]; for small degrees $2 \leq d \leq 5$, this bound is $d + 3$. (See also Subsection 2.7.2 where we prove a stronger version of their result.)

2.1.1 Historical overview

The case of orders in real quadratic fields was completely solved, the main contribution being made by Peters [Pe2]. Since we exploit this result repeatedly and since some parts of the proof are either folklore or difficult to find, we collect them separately in Section 2.3.

Besides providing an upper bound for the Pythagoras number, Peters also fully characterised which numbers are sums of squares in the orders $\mathcal{O}$ of real quadratic fields – in other words, he determined the set $\sum \mathcal{O}^2$. It is well known (see e.g. [KY2], Lemma 6) that the only *local* conditions for a number $\alpha \in \mathcal{O}_K$ to be a sum of integral squares is that it is totally positive and it is a square modulo $2\mathcal{O}_K$; it seems to be folklore that the same holds for non-maximal orders as well. In a maximal order, every number satisfying these necessary conditions is in fact *locally* a sum of four squares: In non-dyadic completions, three squares suffice, while in a dyadic completion $K_\mathfrak{p}$, three squares suffice for each square-mod-2 if and only if $[K_\mathfrak{p} : \mathbb{Q}_2]$ is even ([Sch], Kapitel 0, Lemma 1). However, these local conditions usually do not suffice to characterise the set $\sum \mathcal{O}^2$: The only real quadratic orders where every totally positive square-mod-2 is "globally" a sum of squares, are $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{3}]$ and $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$; trivially, the same holds for $\mathbb{Z}$. In Scharlau's dissertation [Sch], it is proved that only two other totally real orders of degree at most 4 share this property, namely the maximal orders of $\mathbb{Q}(\sqrt{\frac{5+\sqrt{5}}{2}})$ and of $\mathbb{Q}(\sqrt{2}, \sqrt{5})$. As a corollary of our Theorem 2.1.3 we shall see that in these two orders, five squares suffice, which

is an improvement of the upper bound 7 provided for quartic orders by [KY2] (however, in the latter order we suspect that the correct value is 3, see Conjecture 2.1.6).

This failure of local-global principle is connected with the fact that in totally real fields, the genus of the quadratic form $x^2 + y^2 + z^2$ rarely consists only of one equivalence class [Pe4]; therefore, it is difficult to prove any global results about sums of squares in these cases (already proving the tight upper bound for $\mathcal{P}(\mathbb{Z}[\sqrt{3}])$ was tricky, see the discussion below Theorem 2.3.1). Nevertheless, there are some recent results for totally real orders. Tinková [Ti] examined the Pythagoras number of orders in simplest cubic fields; one of the present authors [Kr] exhibited an exceptional case with very different behaviour. Collinet [Co] and Kala and Yatsyna [KY] investigated rings of the form $\mathcal{O}_K\left[\frac{1}{n}\right]$ where K is totally real. For real quadratic orders, B. M. Kim examined sums of non-vanishing squares with J. Y. Kim in [KK], and sums of distinct squares with P.-S. Park in [KP]. The papers [KY2, KY3] also show an application of the Pythagoras number for the construction of a universal quadratic form. A generalisation of the Pythagoras number, the so-called g-invariants, are the subject of recent study as well, see e.g. papers by Icaza and Chan [CI, Ic2], Sasaki [Sa3] or Yatsyna and one of the present authors [KrY]. We shall need them in Subsection 2.7.2 and provide a definition there.

Studying Pythagoras numbers of fields is easier. For number fields, the local-global principle yields $\mathcal{P}(\,\cdot\,) \leq 4$, so more complicated fields are studied. The case of non-formally real fields is also well understood [Pf], while the theory for formally real fields is rich – by Hoffmann [Ho], every $n \in \mathbb{N}$ appears as the Pythagoras number of such a field – and still a vivid research area. From many recent papers we mention those of Becher, Grimm, Van Geel, Leep, Hu, Tikhonov and Yanchevskii [BGV, BL, BV, Hu, TVY].

2.1.2 Our results

This paper examines the Pythagoras numbers of orders $\mathcal{O}$ in totally real biquadratic fields, i.e. in fields of the form $\mathbb{Q}(\sqrt{p}, \sqrt{q})$ where $p, q > 1$ are distinct square-free integers. Since their degree is 4, the above-mentioned result by Kala and Yatsyna gives $\mathcal{P}(\mathcal{O}) \leq 7$. This, together with the knowledge of the Pythagoras numbers of orders in quadratic fields, were essentially the only tools at our disposal. Our treatment is mostly elementary (the only exception is Subsection 2.7.2 where we use some local-global considerations) but some tricks are required to obtain a variety of well-rounded results:

Theorem 2.1.1. *There exist infinitely many totally real biquadratic fields K with $\mathcal{P}(\mathcal{O}_K) = 7$.*

Proof. Theorem 2.5.3 provides a large and natural infinite family of such fields: It suffices to pick two coprime square-free numbers $p \equiv 2$, $q \equiv 3 \pmod 4$ greater than 7, and consider $K = \mathbb{Q}(\sqrt{p}, \sqrt{q})$. □

The assumption that K is generated by roots of coprime integers is a very common one: For example, multiquadratic fields generated by roots of coprime integers were used both by Scharlau in [Sch2] and by Kala and Svoboda in [KS], in the former case to exhibit orders of arbitrarily large Pythagoras number, in the latter to construct maximal orders without a universal quadratic form of a given rank. Therefore investigating the coprime case was important, and besides the above theorem it also yielded Proposition 2.5.1.

Nevertheless, in the present paper we do not restrict to the coprime case, and prove surprisingly strong lower bounds which are valid for each totally real biquadratic field. In particular, the following two statements show that the Pythagoras number of $\mathcal{O}_K$ in most totally real biquadratic fields is not much smaller than the known upper bound 7:

Theorem 2.1.2. *Let K be a totally real biquadratic field. Then:*

1. *$\mathcal{P}(\mathcal{O}_K) \geq 5$ for all but at most seven cases.*

2. *Fix a square-free positive $n > 7$. Then $\mathcal{P}(\mathcal{O}_K) \geq 6$ for all but finitely many totally real biquadratic fields $K \ni \sqrt{n}$.*

Remark. The seven fields probably satisfying $\mathcal{P}(\mathcal{O}_K) < 5$ are $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, $\mathbb{Q}(\sqrt{2}, \sqrt{5})$, $\mathbb{Q}(\sqrt{3}, \sqrt{5})$, $\mathbb{Q}(\sqrt{2}, \sqrt{7})$, $\mathbb{Q}(\sqrt{3}, \sqrt{7})$, $\mathbb{Q}(\sqrt{5}, \sqrt{6})$, $\mathbb{Q}(\sqrt{5}, \sqrt{7})$, see also Conjecture 2.1.6.

Proof. To prove the first statement is the sole purpose of Section 2.6; the proof of the second statement is to be found in Section 2.8. □

The proofs of Theorems 2.1.1 and 2.1.2 are based on cleverly finding families of elements with length 7 (5 or 6, resp.). To handle all fields, it was necessary to divide them into several families and for each family to figure out the best approach. One difficulty is that most biquadratic fields are not generated by square roots of coprime integers, another was the necessity to handle fields containing square roots of $2, 3, 5, 6, 7$ or 13. One type of fields containing $\sqrt{5}$ was particularly difficult and required a very different approach, see Subsection 2.7.1; the developed technique is applicable to other cases, possibly beyond biquadratic fields, and may deserve attention on its own.

For some computations, especially in Theorem 2.1.2 (1), we have written a computer program, starting from scratch. It was primarily used to find elements of needed length for some fields, typically edge cases of our propositions containing square roots of small numbers. On the other hand, it also proved to be useful for finding patterns and establishing conjectures about Pythagoras numbers, which we were usually either able to prove or we formulate them below in Conjecture 2.1.6. The used algorithms are described in Subsection 2.4.2, their implementation in Python is available at `https://github.com/raskama/number-theory/tree/main/biquadratic`.

Going in the other direction, i.e. proving an upper bound, is generally much more difficult. Nevertheless, after generalising the method of Kala and Yatsyna from [KY2], we were able to apply it for quartic fields containing $\sqrt{5}$ by using a result of Sasaki [Sa3, Sa2] on 2-universal quadratic forms.

Theorem 2.1.3. *Let K be a quadratic extension of $\mathbb{Q}(\sqrt{5})$ and $\mathcal{O}$ any order in K containing $\frac{1+\sqrt{5}}{2}$. Then $\mathcal{P}(\mathcal{O}) \leq 5$.*

Proof. We prove this as Theorem 2.7.8. □

Besides requiring the use of the so-called g-invariants, part of the difficulty in proving the above theorem is that the crucial Theorem 2.7.7 is only available in Sasaki's Japanese paper [Sa2]. Moreover, the proof contained therein is very brief. For this reason we include a full proof of this result as well.

Note that by Theorem 2.1.2 (1), this improved upper bound is mostly optimal for maximal orders:

Corollary 2.1.4. *Let K be a totally real biquadratic field containing $\sqrt{5}$. Then $\mathcal{P}(\mathcal{O}_K) = 5$ except possibly when $K = \mathbb{Q}(\sqrt{2}, \sqrt{5})$, $\mathbb{Q}(\sqrt{3}, \sqrt{5})$, $\mathbb{Q}(\sqrt{5}, \sqrt{6})$ or $\mathbb{Q}(\sqrt{5}, \sqrt{7})$.*

The conclusion that there are infinitely many non-maximal orders with Pythagoras number at most 5 is also not to be overlooked. One can put it in contrast with the following theorem, which is our main result about non-maximal orders, to see that their Pythagoras number is a rich topic. Although we have a complete proof of the theorem, we did not include it in this paper to shorten the text. It will be published separately.

Theorem 2.1.5. *Let K be a given totally real biquadratic field. There are infinitely many orders $\mathcal{O} \subset K$ satisfying $\mathcal{P}(\mathcal{O}) = 7$.*

More generally, any totally real biquadratic order $\mathcal{O}_0$ contains an order $\mathcal{O} \subsetneq \mathcal{O}_0$ with $\mathcal{P}(\mathcal{O}) = 7$.

Proof. The full proof will be published separately in the article [Kr2]. Here we only announce that the orders in question are of the form $\mathbb{Z}+\mathbb{Z}\sqrt{S_0T_0}+\mathbb{Z}\sqrt{M_0T_0}+\mathbb{Z}\sqrt{M_0S_0}$ where $M_0, S_0, T_0 \geq 5$ are any numbers such that M_0S_0, M_0T_0 and S_0T_0 are not squares – compare this with the notation m_0, s_0, t_0 introduced in Subsection 2.2.2. □

It is interesting that while the proof of Theorem 2.1.1 worked with square roots of coprime integers, in the case of non-maximal orders we required the order to be generated by square roots of three integers where each two have a common divisor greater than four – a quite weak condition which nevertheless excludes coprime numbers. This illustrates that while at the first glance the proofs of lower bounds on Pythagoras numbers may all seem the same, they in fact use a variety of ideas.

Although our conclusions are not as complete as Peters' on quadratic fields (see Section 2.3), they give a very good idea about the behaviour of Pythagoras numbers of orders in biquadratic fields and thus in totally real fields in general. Regarding maximal orders in biquadratic fields, all the listed results seem to point forwards the following unifying conjecture:[1]

Conjecture 2.1.6. Let K be a totally real biquadratic field.

1. If K contains none of $\sqrt{2}$ and $\sqrt{5}$, then $\mathcal{P}(\mathcal{O}_K) \geq 6$ holds with finitely many exceptions.
2. If K contains $\sqrt{2}$ or $\sqrt{5}$, then $\mathcal{P}(\mathcal{O}_K) \leq 5$.
3. The inequality $\mathcal{P}(\mathcal{O}_K) < 5$ holds precisely for the following seven fields:
   For $K = \mathbb{Q}(\sqrt{2},\sqrt{3}), \mathbb{Q}(\sqrt{2},\sqrt{5}), \mathbb{Q}(\sqrt{3},\sqrt{5})$, where $\mathcal{P}(\mathcal{O}_K) = 3$, and
   for $K = \mathbb{Q}(\sqrt{2},\sqrt{7}), \mathbb{Q}(\sqrt{3},\sqrt{7}), \mathbb{Q}(\sqrt{5},\sqrt{6}), \mathbb{Q}(\sqrt{5},\sqrt{7})$, where $\mathcal{P}(\mathcal{O}_K) = 4$.

We collected evidence for this conjecture in Subsection 2.8.3. Here let us only recall that (2) is already proven for $\sqrt{5}$ in Theorem 2.1.3, and that the only missing part of (3) are upper bounds for the seven exceptional fields: All necessary lower bounds are contained in Theorem 2.1.2 (1) and Proposition 2.4.4.

Note that while the quadratic fields F generated by $\sqrt{2}$, $\sqrt{3}$ and $\sqrt{5}$ all have $\mathcal{P}(\mathcal{O}_F) = 3$ (see Theorem 2.3.1), their quadratic extensions behave very differently – compare the first two statements of the above Conjecture. A possible explanation is that in general, if K/L is a quadratic extension, the value of $\mathcal{P}(\mathcal{O}_K)$ is not directly dependent on $\mathcal{P}(\mathcal{O}_L)$ but rather on the invariant $g_{\mathcal{O}_L}(2)$, see Subsection 2.7.2.

2.1.3 Structure of the paper

The structure of this paper is as follows: Section 2.2 introduces biquadratic fields, repeats their important properties and fixes some notation and important conventions. Section 2.3 concisely presents the known result characterising $\mathcal{P}(\mathcal{O}_F)$ for a quadratic field F. In Section 2.4 we collected auxiliary results which are needed throughout the text. Section 2.5 deals with biquadratic fields generated by roots of coprime integers, its main but not only result being Theorem 2.1.1. Section 2.6 contains most of the proof of the first part of Theorem 2.1.2, with the hardest case postponed until the next section. Although Section 2.7 focuses on fields containing $\sqrt{5}$, its methods for producing both lower and upper bounds are fairly general; in particular, as necessary ingredients, we introduce the g-invariants and use them to generalise the upper bound of [KY2], and also provide a full proof of a result known by Sasaki [Sa2]. In Section 2.8 we proceed to prove the other half of Theorem 2.1.2 and also to discuss the evidence which supports Conjecture 2.1.6.

[1] Based on a preprint of this paper, part (2) of Conjecture 2.1.6 was proved by He and Hu [HH].

2.2 Preliminaries

In this section, we explain the used terminology and notation. First we recall a few basic notions from number theory. Then, in Subsection 2.2.1, we introduce the totally real biquadratic fields, and in Subsection 2.2.2 we fix a very important convention about the meaning of letters m, s, t used *throughout the paper*.

For a number field K, we use $\mathcal{O}_K$ to denote its ring of integers. An *order* in K is any subring $\mathcal{O} \subset \mathcal{O}_K$ which has K as its field of fractions; equivalently, $\mathcal{O}$ is both a subring of K and a $\mathbb{Z}$-module of rank $[K:\mathbb{Q}]$. We often call $\mathcal{O}_K$ the *maximal order* in K. A number field is *totally real* if the images of all its embeddings into $\mathbb{C}$ are contained in $\mathbb{R}$. For $\alpha \in K$, its *trace* is $\mathrm{Tr}(\alpha) = \sum \sigma_i(\alpha)$, where σ_i runs over all embeddings of K into $\mathbb{C}$. Purely for notational convenience, we will also use the *absolute trace* $\mathrm{Tr}_{\mathrm{abs}}$, which is the trace divided by the degree $[K:\mathbb{Q}]$.

Let K be totally real and $\alpha \in K$. If $\sigma_i(\alpha) > 0$ in all embeddings σ_i, then α is *totally positive*, denoted by $\alpha \succ 0$. If $\alpha = 0$ is allowed, we write $\alpha \succcurlyeq 0$ and call it *totally nonnegative*; further, $\alpha \succcurlyeq \beta$ simply means $\alpha - \beta \succcurlyeq 0$. By summing the inequality over all embeddings, it follows that $\mathrm{Tr}\,\alpha \geq \mathrm{Tr}\,\beta$ and $\mathrm{Tr}_{\mathrm{abs}}\,\alpha \geq \mathrm{Tr}_{\mathrm{abs}}\,\beta$. It is clear from the definition that any square and thus also any sum of squares is totally nonnegative.

The Pythagoras number $\mathcal{P}(\,\cdot\,)$ of a ring and the length $\ell(\,\cdot\,)$ of an element were already defined in the Introduction. We point out that if $\alpha = x_1^2 + \cdots + x_n^2$, then $\alpha \succcurlyeq x_i^2$ for every i and thus $\mathrm{Tr}_{\mathrm{abs}}\,\alpha \geq \mathrm{Tr}_{\mathrm{abs}}\,x_i^2$.

2.2.1 Biquadratic fields

A *(totally real) biquadratic field* is a number field $K = \mathbb{Q}(\sqrt{p}, \sqrt{q})$ where $p, q > 1$ are two distinct square-free integers. In this paper, we usually omit the words "totally real". Let us list a few basic facts about such fields. Further details including the proof of the explicit form of $\mathcal{O}_K$ can be found in [Wi].

Denote $r = \frac{pq}{\gcd(p,q)^2}$. The numbers p, q, r are the unique square-free rational integers (not counting 1) which are squares in K; one can freely interchange them in the sense that $K = \mathbb{Q}(\sqrt{p}, \sqrt{q}) = \mathbb{Q}(\sqrt{p}, \sqrt{r}) = \mathbb{Q}(\sqrt{q}, \sqrt{r})$. The only subfields of K are $\mathbb{Q}$, $\mathbb{Q}(\sqrt{p})$, $\mathbb{Q}(\sqrt{q})$ and $\mathbb{Q}(\sqrt{r})$.

The degree $[K:\mathbb{Q}] = 4$, the most natural $\mathbb{Q}$-basis of K being $(1, \sqrt{p}, \sqrt{q}, \sqrt{r})$. The field K is a Galois extension of $\mathbb{Q}$, with the following $\mathbb{Q}$-automorphisms: If $\alpha = g_0 + g_1\sqrt{p} + g_2\sqrt{q} + g_3\sqrt{r}$ with $g_i \in \mathbb{Q}$, then

$$\begin{aligned}
\sigma_1(\alpha) &= g_0 + g_1\sqrt{p} + g_2\sqrt{q} + g_3\sqrt{r},\\
\sigma_2(\alpha) &= g_0 - g_1\sqrt{p} + g_2\sqrt{q} - g_3\sqrt{r},\\
\sigma_3(\alpha) &= g_0 + g_1\sqrt{p} - g_2\sqrt{q} - g_3\sqrt{r},\\
\sigma_4(\alpha) &= g_0 - g_1\sqrt{p} - g_2\sqrt{q} + g_3\sqrt{r}.
\end{aligned}$$

In particular, $\mathrm{Tr}\,\alpha = 4g_0$ and $\mathrm{Tr}_{\mathrm{abs}}\,\alpha = g_0$, which is the reason why the latter is often more convenient to work with. Note that $\mathrm{Tr}_{\mathrm{abs}}(g_0 + g_1\sqrt{p} + g_2\sqrt{q} + g_3\sqrt{r})^2 = g_0^2 + pg_1^2 + qg_2^2 + rg_3^2$. We also see that such a field is indeed totally real.

It is well known that the integral basis of $\mathcal{O}_{\mathbb{Q}(\sqrt{n})}$ depends on the value of n modulo 4. A similar statement holds for biquadratic fields: After possibly interchanging the roles of p, q and r (so that $p \equiv r \pmod 4$), the field K falls into one of the following five distinct types. For each type we present the appropriate integral basis.

$$\begin{aligned}
&\text{(B1)} && \mathcal{O}_K = \mathrm{Span}_{\mathbb{Z}}\Big\{1, \sqrt{p}, \sqrt{q}, \tfrac{\sqrt{p}+\sqrt{r}}{2}\Big\} && \text{if } p \equiv 2,\ q \equiv 3 \pmod 4,\\
&\text{(B2)} && \mathcal{O}_K = \mathrm{Span}_{\mathbb{Z}}\Big\{1, \sqrt{p}, \tfrac{1+\sqrt{q}}{2}, \tfrac{\sqrt{p}+\sqrt{r}}{2}\Big\} && \text{if } p \equiv 2,\ q \equiv 1 \pmod 4,\\
&\text{(B3)} && \mathcal{O}_K = \mathrm{Span}_{\mathbb{Z}}\Big\{1, \sqrt{p}, \tfrac{1+\sqrt{q}}{2}, \tfrac{\sqrt{p}+\sqrt{r}}{2}\Big\} && \text{if } p \equiv 3,\ q \equiv 1 \pmod 4,\\
&\text{(B4a)} && \mathcal{O}_K = \mathrm{Span}_{\mathbb{Z}}\Big\{1, \tfrac{1+\sqrt{p}}{2}, \tfrac{1+\sqrt{q}}{2}, \tfrac{1+\sqrt{p}+\sqrt{q}+\sqrt{r}}{4}\Big\} && \text{if } p \equiv q \equiv 1, \gcd(p,q) \equiv 1 \pmod 4,\\
&\text{(B4b)} && \mathcal{O}_K = \mathrm{Span}_{\mathbb{Z}}\Big\{1, \tfrac{1+\sqrt{p}}{2}, \tfrac{1+\sqrt{q}}{2}, \tfrac{1-\sqrt{p}+\sqrt{q}+\sqrt{r}}{4}\Big\} && \text{if } p \equiv q \equiv 1, \gcd(p,q) \equiv 3 \pmod 4.
\end{aligned}$$

We shall refer to this distinction often, speaking e.g. about "fields of type (B1)". Note that the role of p and r is freely interchangeable and in the fields of type (B4), all three letters are interchangeable.

We conclude this section by introducing another point of view on biquadratic fields. Usually, a biquadratic field is given by specifying two of the three values p, q, r. However, there is another, more symmetrical way of uniquely describing a biquadratic field: One can specify the values of p_0, q_0 and r_0, where $p_0 = \gcd(q, r)$, $q_0 = \gcd(p, r)$, $r_0 = \gcd(p, q)$. These three numbers are pairwise coprime and square-free (but one of them is allowed to be 1); any triple with these properties corresponds to a unique biquadratic field and vice versa. One easily sees that $p = q_0 r_0$, $q = p_0 r_0$ and $r = p_0 q_0$.

2.2.2 An important convention

In this subsection, we collect conventions used throughout this paper. Most of them are very natural; however, one of them could easily be overlooked and cause confusion, and is therefore highlighted by a frame. The same convention was already used in [KTZ].

Unless otherwise stated, K is a totally real biquadratic field, and any biquadratic field is understood to be totally real. If we write $\mathbb{Q}(\sqrt{p}, \sqrt{q})$, we usually understand $p, q > 1$, square-free and distinct, but in important statements, we say it explicitly. When $K = \mathbb{Q}(\sqrt{p}, \sqrt{q})$, the letter r automatically stands for $r = \frac{pq}{\gcd(p,q)^2}$. We also denote $p_0 = \gcd(q, r)$ etc., see the end of the previous subsection.

In many statements, we use the letters m, s, t rather than p, q, r for the numbers whose square roots generate K. They have a precise meaning and are not interchangeable:

Convention 2.2.1. Let K be a biquadratic field. Then the letters m, s, t denote the three square-free rational integers which are squares in K, in the following order:

$$1 < m < s < t.$$

We also use $m_0 = \gcd(s, t)$, $s_0 = \gcd(m, t)$ and $t_0 = \gcd(m, s)$; the above inequality translates into $m_0 > s_0 > t_0 \geq 1$.

For example, if $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, then $m = 2$, $s = 3$, $t = 6$. The above convention is *always* in use, so e.g. if we write $K = \mathbb{Q}(\sqrt{7}, \sqrt{s})$, it automatically means (since $7 = t$ is impossible) that $m = 7 < s < t = 7s$; in particular, K is none of the fields $\mathbb{Q}(\sqrt{2}, \sqrt{7})$, $\mathbb{Q}(\sqrt{3}, \sqrt{7})$, $\mathbb{Q}(\sqrt{5}, \sqrt{7})$ and $\mathbb{Q}(\sqrt{6}, \sqrt{7})$ and s can be any square-free number satisfying $7 \nmid s$, $s > 7$.

2.3 Pythagoras numbers of orders in quadratic fields

As we noted in the Introduction, it is difficult to find references for some parts of the characterisation of $\mathcal{P}(\mathcal{O})$ where $\mathcal{O}$ is an order in a real quadratic field. Therefore we collect them below:

Theorem 2.3.1 (Peters; Cohn and Pall; Dzewas; Kneser; Maaß)**.** *Let $\mathcal{O}$ be an order in a real quadratic number field. Then*

$$\mathcal{P}(\mathcal{O}) = \begin{cases} 3 & \text{for } \mathcal{O} = \mathbb{Z}[\sqrt{2}],\ \mathbb{Z}[\sqrt{3}] \text{ and } \mathbb{Z}[\frac{1+\sqrt{5}}{2}], \\ 4 & \text{for } \mathcal{O} = \mathbb{Z}[\sqrt{6}],\ \mathbb{Z}[\sqrt{7}] \text{ and the non-maximal order } \mathbb{Z}[\sqrt{5}], \\ 5 & \text{otherwise.} \end{cases}$$

The maximal length is attained for example by:

- *Length* 3*:* $1+\sqrt{2}^2+(1+\sqrt{2})^2$, $2+(2+\sqrt{3})^2$, $2+(\frac{1+\sqrt{5}}{2})^2$*;*
- *Length* 4*:* $3+(1+\sqrt{6})^2$, $3+(1+\sqrt{7})^2$, $3+(1+\sqrt{5})^2$*;*
- *Length* 5*:* $3+(\frac{1+\sqrt{13}}{2})^2+(1+\frac{1+\sqrt{13}}{2})^2$ *in* $\mathbb{Z}[\frac{1+\sqrt{13}}{2}]$*; in all the remaining cases* $7+(1+f\sqrt{n})^2$ *or* $7+(f\frac{1+\sqrt{n}}{2})^2$ *in* $\mathbb{Z}[f\sqrt{n}]$ *and* $\mathbb{Z}[f\frac{1+\sqrt{n}}{2}]$*, respectively. Here* n *is square-free and the integer* f*, called the conductor, can take any positive value.*

In the following paragraphs, we explain in which reference to find which part of the proof of this theorem.

As far as we know, the upper bound $\mathcal{P}(\,\cdot\,) \leq 5$ is due to Peters [Pe2], and in all but the seven exceptional cases (i.e. maximal orders in $\mathbb{Q}(\sqrt{n})$, $n = 2, 3, 5, 6, 7, 13$ and the non-maximal order $\mathbb{Z}[\sqrt{5}]$), he also exhibits the element of length 5.

The sufficiency of three squares for $n = 2$ and $n = 5$ stems from the fact that over these fields, the genus of $x^2+y^2+z^2$ contains only one class (Peters cites Dzewas [Dz] but the results are at least partially older, see e.g. [Ma]). Showing the same for $\mathbb{Z}[\sqrt{3}]$ is more involved, since there the genus contains two non-equivalent forms; however, using a nice trick one sees that anything represented by the other form is also represented by three squares. Scharlau, in his dissertation [Sch], Kapitel 0, Satz III (iv), attributes this result to "Kneser, unpublished".

The sufficiency of four squares in $\mathbb{Z}[\sqrt{6}]$ and $\mathbb{Z}[\sqrt{7}]$ is contained in Section 4e of [CP], together with the curious fact that $12+2\sqrt{13}$ is in fact the *only* (up to conjugation and multiplication by squares of units) element of length 5 in $\mathbb{Z}[\frac{1+\sqrt{13}}{2}]$. This explains why Peters did not find this element (he was clearly unaware of Cohn's and Pall's paper). The sufficiency of four squares in $\mathbb{Z}[\sqrt{5}]$ is not stated in [CP] explicitly, but it follows by the same method as for $\sqrt{6}$ and $\sqrt{7}$, namely using Theorems 2 and 6 and checking elements of small norms.

Note that Peters' upper bound 5 is one instance of the bound given by Kala and Yatsyna in [KY2], which is in turn generalised by our Proposition 2.7.5. Also observe that proving all the listed lower bounds is straightforward – in Subsection 2.4.2 we explain that determining the length of a given element in any fixed order is only a computational task, and in quadratic orders this is easily done with pen and paper, even keeping f and n as parameters in the last two cases. We show a slight variation of this in Observation 2.3.2.

Let us remark that the seven problematic orders for which the element $7+(1+f\sqrt{n})^2$ or $7+(1+f\frac{1+\sqrt{n}}{2})^2$ has length less than 5, namely the rings of integers in $\mathbb{Q}(\sqrt{n})$ for $n = 2, 3, 5, 6, 7, 13$, together with $\mathbb{Z}[\sqrt{5}]$, are exactly those where $\ell(7) < 4$. In particular, $7 = (\frac{1+\sqrt{13}}{2})^2 + (\frac{1-\sqrt{13}}{2})^2$.

We shall sometimes exploit parts of the above theorem, namely the information that a particular element has length 5 (or sometimes 3 or 4) in the ring of integers of a quadratic subfield. The knowledge of the quadratic case was the starting point of our examination since it provides a hint on how to construct elements with big length.

Observation 2.3.2. Peters' choice $7+(f\frac{1+\sqrt{n}}{2})^2$ for the element of length 5 is certainly possible, but for non-maximal orders, it is not the simplest one. In this observation, we suggest an alternative. Denote $N = f^2 n$; then every quadratic order is either $\mathbb{Z}[\sqrt{N}]$ or $\mathbb{Z}[\frac{1+\sqrt{N}}{2}]$ with $N \equiv 1 \pmod 4$, where N is no longer square-free, only non-square. Then in $\mathbb{Z}[\sqrt{N}]$ with $N \geq 8$,

the element $7+(1+\sqrt{N})^2$ has length 5 (this was proven by Peters), while in $\mathbb{Z}[\frac{1+\sqrt{N}}{2}]$ with $N \equiv 1 \pmod 4$, $N \geq 17$, we claim that

$$\ell\Big(7+\Big(\frac{1+\sqrt{N}}{2}\Big)^2\Big) = 5.$$

We provide the proof of this fact since it is a good and much simpler illustration of what happens later in some of our proofs. Write $\frac{29+N}{4} + \frac{\sqrt{N}}{2} = \sum\big(\frac{a_i+b_i\sqrt{N}}{2}\big)^2$, $a_i \equiv b_i \pmod 2$. This is equivalent to the two equalities $29+N = \sum a_i^2 + N\sum b_i^2$ and $1 = \sum a_i b_i$. Since changing signs inside of the squares does not affect anything, assume $b_i \geq 0$. Clearly there is a nonzero b_i, so $\sum b_i^2 \geq 1$. If $\sum b_i^2 \geq 3$, the first equality yields $29+N \geq 3N$, a contradiction. If $\sum b_i^2 = 2$, we can assume $b_1 = b_2 = 1$; then a_1 and a_2 are odd and all other a_i, b_i are even, which contradicts the equality $1 = \sum a_i b_i$.

Therefore $\sum b_i^2 = 1$, say $b_1 = 1$ and $b_i = 0$ otherwise. We have $1 = \sum a_i b_i = a_1$, so the first summand is $\big(\frac{1+\sqrt{N}}{2}\big)^2$ and all the others are squares of rational integers. Since their sum is 7, there must be at least four of them, which concludes the proof.

Let us note that while the Pythagoras numbers of real quadratic orders are known, the effort to understand sums of squares in these orders continues: See e.g. the already cited papers by B. M. Kim, J. Y. Kim, P.-S. Park [KK, KP]; one of the present authors recently investigated [Ra] the following question: When does $\sum \mathcal{O}_F^2$ contain all totally positive elements of $m\mathcal{O}_F$ for a given $m \in \mathbb{N}$ and real quadratic field F?

2.4 Lemmata and the use of computers

The first part of this section contains some general auxiliary results about arithmetics of biquadratic number fields. In the second part we explain how one can use a simple algorithm to prove a lower bound for the Pythagoras number of a given order $\mathcal{O}$. Since we used these self-written computer programs whenever a general "pen-and-paper" proof failed, in the third part we provide a list of statements proven in this way, to be referenced in later sections.

2.4.1 Some arithmetics of biquadratic number fields

Given an algebraic integer α in a quadratic subfield F of our biquadratic field K, it is quite possible that α is not a square in F but becomes a square in K; a typical example is $2+\sqrt{3} = \big(\frac{1}{2}(\sqrt{2}+\sqrt{6})\big)^2$. (Bear in mind that α is a square in F, resp. K, if and only if it is a square in $\mathcal{O}_F$, resp. $\mathcal{O}_K$.) However, the resulting square root of α satisfies a strong condition:

Lemma 2.4.1. *Let $K = \mathbb{Q}(\sqrt{n_1}, \sqrt{n_2})$ with $n_1, n_2 > 1$ square-free and distinct; put $n_3 = \frac{n_1 n_2}{\gcd(n_1,n_2)^2}$.*

If $\beta = x + y\sqrt{n_1} + z\sqrt{n_2} + w\sqrt{n_3} \in K$ (with $x, y, z, w \in \mathbb{Q}$) satisfies $\beta^2 \in \mathbb{Q}(\sqrt{n_1})$, then either $x = y = 0$ or $z = w = 0$.

Proof. This is Lemma 4.1 of [KTZ]; as far as we know, the original reference is [Č+]. □

The fields of type (B4) are the only ones where quarter-integers (i.e. numbers from $\mathbb{Z}+\frac{1}{4}$) occur as coefficients of algebraic integers in the vector space basis. The following lemma shows how such elements behave when squared. Remember that in (B4), the elements p, q, r are freely interchangeable.

Lemma 2.4.2. *Let $K = \mathbb{Q}(\sqrt{p}, \sqrt{q})$ be a biquadratic field of type (B4) and $\gamma \in \mathcal{O}_K$ be of the form $\frac{a+b\sqrt{p}+c\sqrt{q}+d\sqrt{r}}{4}$ with a, b, c, d odd. Then γ^2 is of the same form.*

Proof. This is just a straightforward computation which uses the fact that $p \equiv q \equiv r \equiv 1 \pmod 4$. It suffices to check one of the four coefficients of γ^2 in the vector space basis $(1, \sqrt{p}, \sqrt{q}, \sqrt{r})$; if one of them is in $\mathbb{Z} + \frac{1}{4}$, then the others must be as well, since γ^2 is an algebraic integer. We choose the first coefficient: $\operatorname{Tr}_{\text{abs}} \gamma^2 = \frac{1}{16}(a^2 + b^2 p + c^2 q + d^2 r)$. Checking that this is in $\frac{\mathbb{Z}}{4}$ but not in $\frac{\mathbb{Z}}{2}$ is equivalent to proving that $a^2 + b^2 p + c^2 q + d^2 r \equiv 4 \pmod 8$. And since $\text{odd}^2 \equiv 1 \pmod 8$, we actually want

$$1 + p + q + r \equiv 4 \pmod 8,$$

which is readily checked. □

2.4.2 The use of computers

While it is very difficult to find an upper bound for the Pythagoras number of an order and while this paper is mostly about finding lower bounds for *infinite families* of number field orders, the task of finding some lower bound for one given order is easily algorithmically solved. Here we explain the ideas behind such an algorithm and in the next subsection we list some results obtained by using it. The algorithm has a reasonable running time only for elements with small traces, so it becomes hardly usable if we adjoin square roots of large numbers m, s; luckily, to fill the gaps in our proofs, we mostly needed to deal with fields where $m, s < 100$. Implementation in Python is available at https://github.com/raskama/number-theory/tree/main/biquadratic.

While we describe the algorithm specifically for full rings of integers, it works for non-maximal orders as well, as long as one knows their integral basis.

Given an $\alpha \in \mathcal{O}_K$, we want to determine whether it is a sum of squares in $\mathcal{O}_K$, and if so, then how many squares are needed. It is in fact possible to find all representations of α as a sum of squares as follows:

1. If α is not totally positive, then it is not a sum of squares.
2. If x^2 occurs in a representation of α as a sum of squares, then $\alpha \succcurlyeq x^2$; in particular, $\operatorname{Tr}_{\text{abs}} \alpha \geq \operatorname{Tr}_{\text{abs}} x^2$. Therefore we identify all possible summands x^2 as follows:
   (a) Suppose $x = \frac{a+b\sqrt{m}+c\sqrt{s}+d\sqrt{t}}{4}$ and bear in mind that depending on the integral basis, there are congruence conditions imposed on the integers a, b, c, d. Find all quadruples which respect these conditions and satisfy
   $$\frac{1}{16}(a^2 + b^2 m + c^2 s + d^2 t) \leq \operatorname{Tr}_{\text{abs}} \alpha;$$
   clearly there are only finitely many of them since $\operatorname{Tr}_{\text{abs}} \alpha$ is a given constant.
   (b) From the thus obtained list of possible x^2, omit those which do not satisfy $\alpha \succcurlyeq x^2$. In this way, the following finite set is obtained:
   $$S_\alpha = \{x^2 : x \in \mathcal{O}_K, \alpha \succcurlyeq x^2\}.$$
3. Now it remains to check whether α can be written as a sum of any number of elements of the finite set S_α. This can be done straightforwardly in many ways, e.g. by recursion: Try one element $x^2 \in S_\alpha$ and then check whether there are any elements $y^2 \in S_\alpha$ satisfying $\alpha - x^2 \succcurlyeq y^2$; if there are, go over them one by one, etc.

This algorithm is very useful if one has a guess about an element which will require many squares in its representation. If one wants to get an idea about the probable value of $\mathcal{P}(\mathcal{O}_K)$, one can use the following modification, which determines the lengths of all elements up to a given trace:

1. Choose a constant T and find the set

$$S^{(1)} = \{x^2 : x \in \mathcal{O}_K, \mathrm{Tr}_{\mathrm{abs}}\, x^2 \leq T\}.$$

   This is done similarly as in the first algorithm.

2. Compute all sums of two elements of $S^{(1)}$ and reject those whose absolute trace exceeds T, thus forming the set

$$S^{(2)} = \{x_1^2 + x_2^2 : x_1, x_2 \in \mathcal{O}_K, \mathrm{Tr}_{\mathrm{abs}}(x_1^2 + x_2^2) \leq T\}.$$

3. By iteratively adding all elements of $S^{(1)}$, compute the sequence of sets

$$S^{(n)} = \{x_1^2 + \cdots + x_n^2 : x_i \in \mathcal{O}_K, \mathrm{Tr}_{\mathrm{abs}}(x_1^2 + \cdots + x_n^2) \leq T\}.$$

4. Stop as soon as $S^{(n+1)} = S^{(n)}$. Then $\mathcal{P}(\mathcal{O}_K) \geq n$; in particular, any element of $S^{(n)} \setminus S^{(n-1)}$ has length n.

As $S^{(1)}$ has $O(T^2)$ elements, the time and space complexity of this algorithm is $O(T^{2(n+1)})$, where n is the expected $\mathcal{P}(\mathcal{O}_K)$ as above. To reduce the space complexity, it is e.g. possible to restrict ourselves to finding all sums of n squares with a specific trace (and do this for every trace up to T).

Checking whether certain element α is sum of n squares can be done with time complexity $O(T^{2\lceil n/2 \rceil})$, where $T = \mathrm{Tr}_{\mathrm{abs}}\, \alpha$, since one can construct $S^{(\lfloor n/2 \rfloor)}$, $S^{(\lceil n/2 \rceil)}$ and for every element in $S^{(\lfloor n/2 \rfloor)}$ check whether its complementary element is in $S^{(\lceil n/2 \rceil)}$.

These time restrictions proved to be sufficient for our needs and also for producing hypotheses about infinite families of $\mathcal{O}_K$. In particular, the results of Subsection 2.6.5 were observed after running this algorithm over several hundreds of fields of similar type.

2.4.3 The computed data

Here we collected those lemmata needed in later proofs which were checked by an algorithm explained in the previous subsection. Of course, in principle they could be verified by a straightforward but very tedious computation with pen and paper.

Lemma 2.4.3. *Let $K = \mathbb{Q}(\sqrt{m}, \sqrt{s})$ be a totally real biquadratic field with the usual Convention 2.2.1 that $m < s < t$ are square-free. To simplify the notation, put*

$$\alpha_0 = \begin{cases} 7 + (1 + \sqrt{m})^2 & \text{if } m \not\equiv 1 \pmod 4, \\ 7 + \left(\frac{1+\sqrt{m}}{2}\right)^2 & \text{if } m \equiv 1 \pmod 4. \end{cases}$$

Then:

1. *If (m, s) is one of $(17, 19)$, $(17, 21)$, $(17, 22)$, $(21, 22)$ and $(21, 23)$, then $\ell(\alpha_0) = 5$.*

2. *If (m, s) is one of $(10, 11)$, $(10, 17)$, $(10, 19)$, $(11, 14)$, $(11, 17)$, $(11, 21)$; $(14, 15)$, $(14, 17)$, $(14, 19)$, $(15, 17)$, $(15, 21)$, $(15, 22)$, $(19, 21)$, $(19, 22)$, $(22, 23)$, $(23, 26)$ – i.e. if K lies in $\mathcal{K}_1 \cup \mathcal{K}_2 \cup \mathcal{K}_3$ in the notation of Subsection 2.6.2 and $(m, s) \neq (10, 13)$, $(11, 13)$, $(30, 35)$ – then $\ell(\alpha_0) = 5$.*

3. *If (m, s) is $(10, 13)$ or $(11, 13)$, then $3 + (\frac{1+\sqrt{13}}{2})^2 + (1 + \frac{1+\sqrt{13}}{2})^2$ has length 5; if $(m, s) = (30, 35)$, the same holds for $7 + (1 + \sqrt{42})^2$.*

4. *If (m, s) is one of $(22, 26)$, $(26, 30)$, $(19, 23)$, then $15 + (1 + \sqrt{m})^2$ has length 5.*

5. *If* (m,s) *is one of* $(30,38)$, $(34,42)$, $(38,46)$, $(31,39)$, $(35,43)$, $(39,47)$, $(43,51)$, $(47,55)$; $(34,46)$, $(31,43)$, $(35,47)$, $(39,51)$, $(43,55)$, *then* $28+(1+\sqrt{m})^2$ *has length* 5.

6. *If* (m,s) *is one of* $(10,14)$, $(11,15)$, $(15,19)$; $(14,22)$, $(22,30)$, $(26,34)$, $(11,19)$, $(15,23)$, $(23,31)$; $(10,22)$, $(14,26)$, $(22,34)$, $(26,38)$, $(11,23)$, $(19,31)$, $(23,35)$, *then* $7+\left(\frac{\sqrt{m}+\sqrt{s}}{2}\right)^2$ *has length* 5.

7. *If* $m=6$ *and* s *is one of* 13, 17, 29, 37, 41; 7, 11, 19; 26, 34; 14, 22, 38, 46, 62, 70, 86, *then the* α *defined in Proposition 2.6.7 has length* 5.

8. *If* $m=6$ *and* $s=10$, *then* $3+\left(\sqrt{6}-\frac{\sqrt{6}+\sqrt{10}}{2}\right)^2+\left(2+\frac{\sqrt{6}+\sqrt{10}}{2}\right)^2$ *has length* 5.

9. *If* $m=7$ *and* s *is one of* 13, 17, 29, 33, 37, 41; 10; 15, 19, 23, 31, 39, 43, 47, 51, *then the* α *defined in Proposition 2.6.6 has length* 5.

10. *If* $m=7$ *and* $s=11$, *then* $3+\left(\frac{\sqrt{7}+\sqrt{11}}{2}\right)^2+\left(1+\frac{\sqrt{7}+\sqrt{11}}{2}\right)^2$ *has length* 5.

11. *If* $m=2$ *and* s *is one of* 11, 15, 17, 21, 29, *then the* α *defined in Proposition 2.6.9 has length* 5.

12. *If* $m=2$ *and* $s=13$, *then* $3+(1+\sqrt{2})^2+\left(\sqrt{2}+\frac{1+\sqrt{13}}{2}\right)^2+\left(2+\frac{1+\sqrt{13}}{2}+\frac{\sqrt{2}+\sqrt{26}}{2}\right)^2$ *has length* 5.

13. *If* $m=3$ *and* s *is one of* 13, 17, 29, 37, 41; 10; 11, 19, 23, 31, 35, 43, *then the* α *defined in Proposition 2.6.10 has length* 5.

14. *If* $m=5$ *and* $s=13$ *or* $s=17$, *then the* α *defined in Proposition 2.6.8 has length* 5.

15. *If* $m=5$ *and* $s\not\equiv 1 \pmod 4$, $7<s\leq 3253$, *then the* α *defined in Proposition 2.7.1 has length* 5.

16. *If* $m=13$ *and* s *is one of* 17, 21, 29, 33, 37, 41, *then the* α *defined in Proposition 2.8.3 has length* 6.

17. *In fields* $\mathbb{Q}(\sqrt{13},\sqrt{n})$ *with* $n=6,7,10,11$, *the element* $12+2\sqrt{13}+(1+\sqrt{n})^2$ *has length* 6.

Proof. As we pointed out, proving that an element α is not a sum of n squares in a given field is just a straightforward computational task. Therefore, we proved this lemma by implementing the above-described algorithm in Python.

One small exception is part (15), but only for technical reasons: To reduce computation time, we verified the statement by computer only for $7<s\leq 499$, while the remaining cases were handled by refining the proof of Proposition 2.7.3 – see Observation 2.7.4. □

During our computations, only seven fields stood out as possible candidates for $\mathcal{P}(\mathcal{O}_K)<5$ (for all other fields, we were able to find an element of length 5 with a relatively small trace). Especially, for $K=\mathbb{Q}(\sqrt{2},\sqrt{3}),\mathbb{Q}(\sqrt{2},\sqrt{5}),\mathbb{Q}(\sqrt{3},\sqrt{5})$ we suspect $\mathcal{P}(\mathcal{O}_K)=3$ and for $K=\mathbb{Q}(\sqrt{2},\sqrt{7}),\mathbb{Q}(\sqrt{3},\sqrt{7}),\mathbb{Q}(\sqrt{5},\sqrt{6}),\mathbb{Q}(\sqrt{5},\sqrt{7})$ we suspect $\mathcal{P}(\mathcal{O}_K)=4$.

The following proposition collects our results about these seven fields: We present an element of the suspected maximal length as well as bounds up to which the computation was completed. The example elements α_0 are chosen with the lowest possible trace (many elements with the desired length can be found).

Proposition 2.4.4. *If* K, l *and* α_0 *is one of the triples specified below then* $\ell(\alpha_0)=l$ *and* $\ell(\alpha)\leq l$ *for all* $\alpha\in\sum\mathcal{O}_K^2$ *such that* $\operatorname{Tr}\alpha\leq 500$.

1. $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, $l = 3$, $\alpha_0 = 6 + \sqrt{2} + \sqrt{6}$;
2. $K = \mathbb{Q}(\sqrt{2}, \sqrt{5})$, $l = 3$, $\alpha_0 = 6 + \sqrt{5}$;
3. $K = \mathbb{Q}(\sqrt{3}, \sqrt{5})$, $l = 3$, $\alpha_0 = 3 + \frac{1+\sqrt{5}}{2}$;
4. $K = \mathbb{Q}(\sqrt{2}, \sqrt{7})$, $l = 4$, $\alpha_0 = 10 + 2\sqrt{2} + \sqrt{7}$;
5. $K = \mathbb{Q}(\sqrt{3}, \sqrt{7})$, $l = 4$, $\alpha_0 = 8 + \sqrt{3} + \sqrt{7}$;
6. $K = \mathbb{Q}(\sqrt{5}, \sqrt{6})$, $l = 4$, $\alpha_0 = 10 + 2\sqrt{6} + \frac{1+\sqrt{5}}{2}$;
7. $K = \mathbb{Q}(\sqrt{5}, \sqrt{7})$, $l = 4$, $\alpha_0 = 11 + 2\sqrt{7} + \frac{1+\sqrt{5}}{2}$.

Note that a nontrivial upper bound shall be proven only for fields containing $\sqrt{5}$, and in general, obtaining an upper bound even for a single field is difficult: Therefore, although we are convinced that e.g. $\mathcal{P}(\mathcal{O}_K) = 3$ for $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, we know only $3 \leq \mathcal{P}(\mathcal{O}_K) \leq 7$.

The following proposition collects some of our computed data for fields containing $\sqrt{3}$. Based on it, we conjecture that there are only finitely many fields $K = \mathbb{Q}(\sqrt{3}, \sqrt{s})$ with $\mathcal{P}(\mathcal{O}_K) \leq 5$; this is in sharp contrast with the situation in fields containing $\sqrt{2}$ or $\sqrt{5}$ (see the conjecture in Subsection 2.8.3 and compare this with the situation in quadratic fields, described in Section 2.3).

Proposition 2.4.5. *For $K = \mathbb{Q}(\sqrt{3}, \sqrt{s})$ where $s = 17$, $s = 22$ or $26 \leq s \leq 55$, we have $\mathcal{P}(\mathcal{O}_K) \geq 6$. If s is odd, the same holds also for $55 < s \leq 79$.*

In all these cases, there exists $\alpha \in \mathcal{O}_K$ with $\ell(\alpha) = 6$ and $\mathrm{Tr}(\alpha) \leq 1000$. For example, the following elements have length 6:

$$87 + 18\sqrt{3} - 20\sqrt{17} - 4\sqrt{51}; \quad 150 + 45\sqrt{3} - 14\sqrt{26}; \quad \frac{1}{2}(199 - 50\sqrt{3} + 14\sqrt{31} - 19\sqrt{93}).$$

Although our program showed that for $s = 58, 62, 70$ or 74, elements with $\mathrm{Tr}(\alpha) \leq 1100$ have length at most five, we believe that $\mathcal{P}(\mathcal{O}_K) \geq 6$ holds even in those fields (and in fact for all $K \ni \sqrt{3}$ with $s \geq 26$). A hint towards this is also the fact that for $s = 46$, all elements with $\mathrm{Tr}(\alpha) \leq 900$ have $\ell(\alpha) \leq 5$. The computer we used is not a particularly strong one, since numerical experiments were not our priority.

2.5 Results for fields with coprime m, s

In this section we examine the specific fields $K = \mathbb{Q}(\sqrt{m}, \sqrt{s})$ where m and s are coprime, i.e. $t = ms$. They are easier to work with than the general case (and therefore also often occur in works of other authors); in particular, if we restrict to the fields of type (B1), we were able to prove that the Pythagoras number of $\mathcal{O}_K$ is 7 (with a few exceptions); see Theorem 2.5.3. This proves one of the main results of this paper, Theorem 2.1.1. The other results of this section can be put neatly together as follows:

Proposition 2.5.1. *Let $p, q \notin \{2, 3, 5, 6, 7, 13\}$ be two coprime square-free positive integers which are not both congruent to 3 modulo 4. Then $\mathcal{P}(\mathcal{O}_K) \geq 6$ for $K = \mathbb{Q}(\sqrt{p}, \sqrt{q})$.*

Proof. This is just a combination of Propositions 2.5.2, 2.5.4 and 2.5.5. □

As a side remark, the inequalities for p, q in all the following propositions are optimal in the sense that if they are violated, then the given α has length less than 6. To see this, observe that the inequalities only exclude fields containing square roots of 2, 3, 5, 6, 7 or 13, and in these

fields $\ell(7) < 4$, see Section 2.3. On the other hand, at least for fields containing $\sqrt{13}$ another element of length 6 can be found, see Proposition 2.8.3.

We start with a result for fields of type (B1); besides being one third of the above proposition, it will also serve as a lemma for the upcoming Theorem 2.5.3.

Proposition 2.5.2 (Type (B1))**.** *Let $K = \mathbb{Q}(\sqrt{p}, \sqrt{q})$ where $p \equiv 2$ and $q \equiv 3 \pmod 4$ are coprime square-free integers such that $p, q \geq 10$. Then $\mathcal{P}(\mathcal{O}_K) \geq 6$.*

In particular, the following element has length 6:

$$\alpha = 7 + (1 + \sqrt{p})^2 + (1 + \sqrt{q})^2.$$

Proof. In this case, the integral basis is given by $\mathcal{O}_K = \mathrm{Span}_{\mathbb{Z}}\{1, \sqrt{p}, \sqrt{q}, \frac{\sqrt{p}+\sqrt{pq}}{2}\}$. Suppose

$$\alpha = \sum \Big(a_i + b_i\sqrt{p} + c_i\sqrt{q} + d_i\frac{\sqrt{p}+\sqrt{pq}}{2}\Big)^2.$$

This means

$$\begin{aligned} 9 + p + q + 2\sqrt{p} + 2\sqrt{q} = \sum \Big(&(a_i^2 + b_i^2 p + c_i^2 q + d_i^2\frac{p+pq}{4} + b_i d_i p) \\ &+ (2a_i b_i + a_i d_i + c_i d_i q)\sqrt{p} + (2a_i c_i + b_i d_i p + d_i^2\frac{p}{2})\sqrt{q} \\ &+ (2b_i c_i + c_i d_i + a_i d_i)\sqrt{pq}\Big). \end{aligned}$$

By comparing coefficients, one gets the following conditions:

$$9 + p + q = \sum a_i^2 + q\sum c_i^2 + p\sum \Big(\Big(b_i + \frac{d_i}{2}\Big)^2 + q\frac{d_i^2}{4}\Big), \tag{2.5.1}$$

$$2 = 2\sum a_i b_i + \sum a_i d_i + q\sum c_i d_i, \tag{2.5.2}$$

$$2 = 2\sum a_i c_i + p\sum b_i d_i + \frac{p}{2}\sum d_i^2, \tag{2.5.3}$$

$$0 = 2\sum b_i c_i + \sum c_i d_i + \sum a_i d_i. \tag{2.5.4}$$

Without loss of generality $a_i \geq 0$ and we will prove the following statements:

(i) There is a nonzero b_i and a nonzero c_j.

(ii) All the coefficients d_i are zero.

(iii) There is exactly one nonzero coefficient $|b_i| = 1$ and one nonzero coefficient $|c_j| = 1$.

(iv) If $c_i \neq 0$, then $b_i = 0$ and vice versa.

(v) If c_i is nonzero, then $a_i = c_i = 1$, the same for b_i.

The proofs follow:

(i) Suppose $b_i = 0$ for all i. Then from (2.5.4) we get $\sum c_i d_i = -\sum a_i d_i$. Together with (2.5.2), this yields

$$2 = q\sum c_i d_i - \sum c_i d_i = (q-1)\sum c_i d_i,$$

which is impossible as $q \geq 10$ and $\sum c_i d_i$ is rational integer.

If $c_i = 0$ for all i, we proceed similarly: From (2.5.3) follows $2 = \frac{p}{2}\sum(2b_i d_i + d_i^2)$, which is again impossible as $p \geq 10$ and $\sum 2b_i d_i + d_i^2$ is rational integer.

(ii) Suppose there is some $|d_i| > 0$. Since there is also some nonzero c_i, from (2.5.1) we get $9 + p + q \geq q + \frac{pq}{4}$. This is not possible for $p, q \geq 10$.

(iii) We already know that there is at least one nonzero c_j and b_i. On the other hand, equation (2.5.1) now yields

$$9 + p + q \geq q \sum c_i^2 + p \sum b_i^2.$$

If $\sum c_i^2 > 1$ or $\sum b_i^2 > 1$ this is clearly impossible as $p, q \geq 10$.

(iv) This is an easy consequence of $0 = 2\sum b_i c_i$ (2.5.4) and the previous statement.

(v) These are again direct consequences of $1 = \sum a_i b_i$ (2.5.2) and $1 = \sum a_i c_i$ (2.5.3) and our assumption that $a_i \geq 0$.

From the previous statements, it can be seen that the only way how to write α as a sum of squares is $\alpha = (1 + \sqrt{p})^2 + (1 + \sqrt{q})^2 + \sum x_i^2$, where $x_i \in \mathbb{Z}$. This concludes the proof as 7 is not a sum of three squares over rational integers. □

Exploiting the previous proposition, we are able to prove one of our main results. Observe that it covers *all* fields with coprime $m, s \geq 10$ of type (B1), since if m, s are coprime, they cannot both be 2 modulo 4.

Theorem 2.5.3 (Type (B1))**.** *Let $K = \mathbb{Q}(\sqrt{p}, \sqrt{q})$ where $p \equiv 2$ and $q \equiv 3 \pmod 4$ are coprime square-free integers such that $p, q \geq 10$. Then $\mathcal{P}(\mathcal{O}_K) = 7$.*

In particular, the following element has length 7:

$$\alpha = 7 + (1 + \sqrt{p})^2 + (1 + \sqrt{q})^2 + \Big(\frac{\sqrt{p} + \sqrt{pq}}{2}\Big)^2.$$

Proof. It suffices to prove that $\ell(\alpha) = 7$; the rest is clear since 7 is an upper bound on the Pythagoras number for every order of degree 4. For a field of type (B1), we have $\mathcal{O}_K = \mathrm{Span}_{\mathbb{Z}}\{1, \sqrt{p}, \sqrt{q}, \frac{\sqrt{p}+\sqrt{pq}}{2}\}$. Suppose that $\alpha = 9 + p + q + \frac{p+pq}{4} + 2\sqrt{p} + \left(2 + \frac{p}{2}\right)\sqrt{q}$ is a sum of an arbitrary number of squares.

Analogously to the proof of Proposition 2.5.2, we denote the squares as $(a_i + b_i\sqrt{p} + c_i\sqrt{q} + d_i\frac{\sqrt{p}+\sqrt{pq}}{2})^2$. By comparing coefficients, one gets the following conditions:

$$9 + p + q + \frac{p + pq}{4} = \sum a_i^2 + q\sum c_i^2 + p\sum\left(\Big(b_i + \frac{d_i}{2}\Big)^2 + \frac{d_i^2 q}{4}\right), \tag{2.5.5}$$

$$2 = 2\sum a_i b_i + \sum a_i d_i + q\sum c_i d_i, \tag{2.5.6}$$

$$2 + \frac{p}{2} = 2\sum a_i c_i + p\sum b_i d_i + \frac{p}{2}\sum d_i^2, \tag{2.5.7}$$

$$0 = 2\sum b_i c_i + \sum c_i d_i + \sum a_i d_i. \tag{2.5.8}$$

Without loss of generality all $d_i \geq 0$ and we will step by step prove the following lemmata:

(i) There exists a nonzero b_i and a nonzero c_j.

(ii) There is exactly one nonzero d_i, let us say d_1. This $d_1 = 1$ and $b_1 \in \{-1, 0\}$.

(iii) There exists a nonzero b_i for $i > 1$.

(iv) There is exactly one j such that c_j is nonzero, and exactly one $k > 1$ such that b_k is nonzero. For these indices, $|c_j| = 1$ and $|b_k| = 1$. Also $\sum a_i^2 = 9$.

(v) $a_1 = b_1 = c_1 = 0$. Thus, the first summand is $(\frac{\sqrt{p}+\sqrt{pq}}{2})^2$.

The last lemma implies that $\ell(\alpha) = 7$ since $7 + (1 + \sqrt{p})^2 + (1 + \sqrt{q})^2$ has length 6 by Proposition 2.5.2.

Now let us present the proofs of the lemmata:

(i) This can be proven in the same way as the first part of the proof of 2.5.2.

(ii) If $d_i^2 \geq 4$ for some i or there are at least two $d_i = 1$, the RHS of (2.5.5) is at least $q + \frac{pq}{2}$ (since there is a nonzero c_i); however, $q + \frac{pq}{2} > 9 + p + q + \frac{p+pq}{4}$ for $p, q \geq 10$. On the other hand, comparing parities of LHS and RHS of (2.5.7), there must exist at least one odd d_i, implying there is exactly one nonzero d_i, without loss of generality $d_1 = 1$.

Now if $b_1 \notin \{-1, 0\}$, then $p(b_1 + \frac{d_1}{2})^2 \geq \frac{9}{4}p$, which, taken together with the other known estimates (nonzero c_i and $d_1 = 1$), makes (2.5.5) impossible for $p \geq 10$.

(iii) If $b_1 = 0$, it is clear from **(i)**, so assume $b_1 = -1$ and $b_i = 0$ for $i > 1$.

Then from (2.5.6) we get $2 = -2a_1 + a_1 + c_1 q$, from (2.5.8) also $0 = -2c_1 + c_1 + a_1$. By adding these two equalities, we get $2 = c_1(q-1)$, which is impossible.

(iv) This almost immediately follows from earlier results and (2.5.5): With our knowledge, the equality can be rewritten as

$$9 + p + q + \frac{p+pq}{4} = \sum a_i^2 + q \sum c_i^2 + p \frac{1+q}{4} + p \sum_{i \geq 2} b_i^2.$$

Since there is at least one nonzero c_i, we know $\sum c_i^2 \geq 1$, and similarly $\sum_{i \geq 2} b_i^2 \geq 1$. Thus the RHS is at least $p + q + \frac{pq+p}{4}$, which is LHS minus 9. From this it is clear that both aforementioned sums must be exactly 1 (implying that exactly one summand in each of them is 1) and $\sum a_i^2 = 9$.

(v) From (2.5.7) we get $2 - pb_1 = \sum 2a_i c_i$. This is impossible for $b_1 \neq 0$, as one easily deduces from $p \geq 10$ and the fact that there is exactly one nonzero $|c_i| = 1$ and that $\sum a_i^2 = 9$.

If $c_1 \neq 0$, from (2.5.6) we get $2 - c_1 q - a_1 = \sum_{i>1} 2a_i b_i$. Since $\sum a_i^2 = 9$ and $q \geq 10$, this is again impossible as there is only one nonzero b_i for $i > 1$, equal to ± 1. Thus $c_1 = 0$.

From (2.5.8) we get $a_1 = -\sum_{i>1} 2b_i c_i$, so the only other possibility besides $a_1 = 0$ is $a_1 = \pm 2$.

If $a_1 = -2$, equations (2.5.6), (2.5.7), (2.5.8) read as $2 = \sum_{i>1} a_i b_i$, $1 = \sum_{i>1} a_i c_i$, $1 = \sum_{i>1} b_i c_i$. The last one shows that $b_i \neq 0$ and $c_j \neq 0$ must happen for $i = j$, but then the first two equations imply different values of a_i, which is a contradiction.

If $a_1 = 2$, we get $0 = \sum_{i>1} a_i b_i$, $1 = \sum_{i>1} a_i c_i$, $-1 = \sum_{i>1} b_i c_i$, which leads to the same contradiction. □

The following propositions handle the fields of type (B2,3) and (B4). They can be proved using the exact same five steps as in the proof of Proposition 2.5.2, each of these steps analogously requiring either straightforward inequalities concerning trace or a simple parity argument. As all these ideas were already illustrated, we omit these proofs.

One thing to mention is that instead of using the integral basis explicitly, one can work with elements of the form $\frac{a_i}{4} + \frac{b_i}{4}\sqrt{p} + \frac{c_i}{4}\sqrt{q} + \frac{d_i}{4}\sqrt{pq}$ and impose congruence relations upon the coefficients. The structure of the proofs would remain unchanged and it can perhaps be clearer, especially for fields of type (B4). This other approach is often used throughout the rest of the paper.

Proposition 2.5.4 (Type (B2,3)). *Let $K = \mathbb{Q}(\sqrt{p}, \sqrt{q})$ where $p \equiv 2, 3$ and $q \equiv 1 \pmod 4$ are coprime square-free integers such that $p \geq 10$, $q \geq 17$. Then $\mathcal{P}(\mathcal{O}_K) \geq 6$.*

In particular, the following element has length 6:

$$\alpha = 7 + (1 + \sqrt{p})^2 + \Big(\frac{1+\sqrt{q}}{2}\Big)^2.$$

Proposition 2.5.5 (Type (B4)). *Let $K = \mathbb{Q}(\sqrt{p}, \sqrt{q})$ where $p \equiv q \equiv 1 \pmod 4$ are coprime square-free integers such that $p, q \geq 17$. Then $\mathcal{P}(\mathcal{O}_K) \geq 6$.*

In particular, the following element has length 6:

$$\alpha = 7 + \Big(\frac{1+\sqrt{p}}{2}\Big)^2 + \Big(\frac{1+\sqrt{q}}{2}\Big)^2.$$

Note that in the last proposition, the field is in fact always of type (B4a) since $\gcd(p, q) \equiv 1 \pmod 4$. Let us also remark that the omitted case $p \equiv q \equiv 3$ (see Proposition 2.5.1) seems to be somewhat harder, but we believe that $\mathcal{P}(\mathcal{O}_K) \geq 6$ holds even in that situation.

2.6 Pythagoras number is at least 5 (up to seven exceptions)

In this section we prove the first half of Theorem 2.1.2, i.e. that $\mathcal{P}(\mathcal{O}_K) \geq 5$ unless $K = \mathbb{Q}(\sqrt{2},\sqrt{3})$, $\mathbb{Q}(\sqrt{2},\sqrt{5})$, $\mathbb{Q}(\sqrt{3},\sqrt{5})$ (where we expect $\mathcal{P}(\mathcal{O}_K) = 3$) or $K = \mathbb{Q}(\sqrt{3},\sqrt{7})$, $\mathbb{Q}(\sqrt{2},\sqrt{7})$, $\mathbb{Q}(\sqrt{5},\sqrt{6})$, $\mathbb{Q}(\sqrt{5},\sqrt{7})$ (where we expect $\mathcal{P}(\mathcal{O}_K) = 4$).

The structure of the proof is as follows: The fields which contain $\sqrt{2}$, $\sqrt{3}$ or $\sqrt{5}$ are handled in Subsection 2.6.5, with the most difficult case postponed until Subsection 2.7.1; the fields containing $\sqrt{6}$ or $\sqrt{7}$ are discussed in Subsection 2.6.4. The fields containing $\sqrt{13}$ are postponed until Proposition 2.8.3, where we prove that the Pythagoras number is in fact at least 6. For the fields which contain none of these six numbers, the easier case of $m \equiv 1 \pmod 4$ is solved in Subsection 2.6.1, while Subsection 2.6.2 solves a majority of the fields where $m \not\equiv 1 \pmod 4$. Among these, the fields with $s = m+4$, $s = m+8$ or $s = m+12$ turn out to be the most problematic; a solution for them is provided in Subsection 2.6.3. A formal proof of the whole Theorem 2.1.2 (1), including references to specific propositions rather than subsections, is situated at the very end of Section 2.6.

Since the proof is a bit lengthy, we first provide a hint how to easily obtain the weaker estimate $\mathcal{P}(\mathcal{O}_K) \geq 4$: By trace considerations, it is simple to show that if $\ell(7) < 4$, then K must contain $\sqrt{2}$, $\sqrt{3}$, $\sqrt{5}$, $\sqrt{6}$, $\sqrt{7}$ or $\sqrt{13}$. For fields with $m = 6$, the element $10 + 2\sqrt{6} = 1+1+1+(1+\sqrt{6})^2$ is a sum of less than four squares only in $\mathbb{Q}(\sqrt{6},\sqrt{10})$, and here one easily finds another counterexample. For fields with $m = 7$ or $m = 13$, one obtains similar results for $11 + 2\sqrt{7} = 1+1+1+(1+\sqrt{7})^2$ and $\frac{13}{2} + \frac{1}{2}\sqrt{13} = 1+1+1+\left(\frac{1+\sqrt{13}}{2}\right)^2$, respectively; only the field $\mathbb{Q}(\sqrt{7},\sqrt{11})$ has to be handled separately. It then remains to find a proof for fields containing $\sqrt{2}$, $\sqrt{3}$ or $\sqrt{5}$. This is easily done by the same method which we use in Subsection 2.6.4 for proving $\mathcal{P}(\mathcal{O}_K) \geq 5$ for $m = 6, 7$; a more general explanation of this strategy is provided later in Subsection 2.8.1.

The rest of the section is spent solely by proving the result advertised in its title. Remember that we keep the notation $1 < m < s < t$ for the three square-free integers whose square roots belong to K.

2.6.1 The cases where $m \equiv 1 \pmod 4$

The following proposition shows that for $m \equiv 1 \pmod 4$, the simplest element of length 5 in $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$ has length 5 also in $\mathcal{O}_K$:

Proposition 2.6.1. *Let $K = \mathbb{Q}(\sqrt{m},\sqrt{s})$ be a totally real biquadratic field with $m \equiv 1 \pmod 4$ where $m \neq 5, 13$. Then $\mathcal{P}(\mathcal{O}_K) \geq 5$.*

In particular, $\ell(\alpha_0) = 5$ holds for

$$\alpha_0 = 7 + \left(\frac{1+\sqrt{m}}{2}\right)^2 = 7 + \frac{1+m}{4} + \frac{\sqrt{m}}{2}.$$

Proof. Peters [Pe2] proved that α_0 cannot be expressed as a sum of four squares in $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$, see Theorem 2.3.1. Therefore, if $\alpha_0 = \sum_{i=1}^4 x_i^2$ in $\mathcal{O}_K$, we can assume $x_1 \notin \mathbb{Q}(\sqrt{m})$.

First suppose that $x_i \in \mathbb{Q}(\sqrt{m})$ for $i \neq 1$. Then $x_1^2 \in \mathbb{Q}(\sqrt{m})$, hence by Lemma 2.4.1 x_1 has the form $k\sqrt{s} + l\sqrt{t}$ for $k, l \in \mathbb{Q}$. However, these elements have a big trace: To minimise the trace of x_1^2, one has to choose either $x_1 = \sqrt{s}$ or $x_1 = \frac{\sqrt{s}\pm\sqrt{t}}{2}$. Therefore, by comparing traces of α_0 and x_1^2, we obtain one of the inequalities

$$7 + \frac{1+m}{4} \geq s \quad \text{or} \quad 7 + \frac{1+m}{4} \geq \frac{s+t}{4}.$$

The first inequality is nonsense since $s \geq m+1$. As for the second, it clearly implies $t \leq 28$ which holds only for finitely many biquadratic fields; and none of them satisfies $m \equiv 1 \pmod 4$.

Therefore we can assume $x_1, x_2 \notin \mathbb{Q}(\sqrt{m})$. We distinguish two cases. In the first, both x_1 and x_2 are of the form $\frac{a+b\sqrt{m}+c\sqrt{s}+d\sqrt{t}}{2}$ for $a, b, c, d \in \mathbb{Z}$, i.e. "no quarter-integers are involved". Then $\mathrm{Tr}_{\mathrm{abs}}(x_1^2 + x_2^2) \geq 2\,\mathrm{Tr}_{\mathrm{abs}}\left(\frac{1+\sqrt{s}}{2}\right)^2$, yielding

$$7 + \frac{1+m}{4} \geq 2\frac{1+s}{4},$$

i.e. $27 + m \geq 2s$. This, together with our conditions on m, holds only for the five fields $\mathbb{Q}(\sqrt{17}, \sqrt{19})$, $\mathbb{Q}(\sqrt{17}, \sqrt{21})$, $\mathbb{Q}(\sqrt{17}, \sqrt{22})$, $\mathbb{Q}(\sqrt{21}, \sqrt{22})$, $\mathbb{Q}(\sqrt{21}, \sqrt{23})$; these fields were handled by our computer program, see Lemma 2.4.3 (1).

In the other case, one of x_i is of the form $\frac{a+b\sqrt{m}+c\sqrt{s}+d\sqrt{t}}{4}$ with a, b, c, d odd. Then, by Lemma 2.4.2, x_i^2 is of the same form; hence, to get α_0, at least one other summand must take the same form. Comparing traces, this yields

$$7 + \frac{1+m}{4} \geq 2\frac{1+m+s+t}{16},$$

i.e. $57 + m \geq s + t$, implying $56 \geq t$. This is impossible, since quarter-integers can only occur for fields of type (B4), and the smallest value of t in such a field is 65. □

2.6.2 The cases where $m \not\equiv 1 \pmod 4$

If we consider the fields where $m \not\equiv 1 \pmod 4$, it is natural to ask whether $\alpha_0 = 7 + (1+\sqrt{m})^2$ satisfies $\ell(\alpha_0) = 5$. Usually, the answer is positive. However, in contrast with the analogous question for $m \equiv 1$, there are infinitely many fields where this is not the case:

Observation 2.6.2. In a field $\mathbb{Q}(\sqrt{m}, \sqrt{s})$ where $s = m + 4$, $s = m + 8$ or $s = m + 12$, four squares suffice to represent $\alpha_0 = 7 + (1+\sqrt{m})^2 = (8+m) + 2\sqrt{m}$. More specifically, denote $y_1 = 1 + \frac{\sqrt{m}+\sqrt{s}}{2}$ and $y_2 = 1 + \frac{\sqrt{m}-\sqrt{s}}{2}$. Then

$$\alpha_0 = \begin{cases} y_1^2 + y_2^2 + 2^2 & \text{if } s = m+4, \\ y_1^2 + y_2^2 + 1^2 + 1^2 & \text{if } s = m+8, \\ y_1^2 + y_2^2 & \text{if } s = m+12, \end{cases}$$

as one easily sees from the general identity $y_1^2 + y_2^2 = 2 + \frac{m+s}{2} + 2\sqrt{m}$.

The three families of fields which were shown to be problematic in Observation 2.6.2 will be handled in the next subsection. The aim of this subsection is to prove that when one excludes these three families (and of course supposes $m \neq 2, 3, 6, 7$), then five squares are indeed needed for α_0 in all but three fields.

Proposition 2.6.3. *Let $K = \mathbb{Q}(\sqrt{m}, \sqrt{s})$ be a totally real biquadratic field with $m \not\equiv 1 \pmod 4$ such that $\mathcal{P}(\mathcal{O}_F) = 5$ for $F = \mathbb{Q}(\sqrt{m})$. (Namely $m \neq 2, 3, 6, 7$.) Assume further that $s \neq m+4, m+8, m+12$. Then $\mathcal{P}(\mathcal{O}_K) \geq 5$.*

In particular, the length of

$$\alpha_0 = 7 + (1+\sqrt{m})^2 = (8+m) + 2\sqrt{m}$$

is 5 unless $K = \mathbb{Q}(\sqrt{10}, \sqrt{13})$, $\mathbb{Q}(\sqrt{11}, \sqrt{13})$ or $\mathbb{Q}(\sqrt{30}, \sqrt{35})$. In the first two of these three fields, $\ell\left(3 + (\frac{1+\sqrt{13}}{2})^2 + (1 + \frac{1+\sqrt{13}}{2})^2\right) = 5$; in the last, $\ell\left(7 + (1+\sqrt{42})^2\right) = 5$.

Proof. We start by defining three sets of exceptional fields for which the following proof does not work and they must be handled separately. For convenience, denote by $\mathcal{K}$ the set of all fields for which we aim to prove the theorem, i.e. fields where $m \not\equiv 1 \pmod 4$, $m \neq 2, 3, 6, 7$

and $s \neq m+4, m+8, m+12$. Now, the problematic fields will be defined by the following inequalities:

$$\begin{aligned}\mathcal{K}_1 &= \{K \in \mathcal{K} : 31 + 3m \geq 4s\},\\ \mathcal{K}_2 &= \{K \in \mathcal{K} : 31 + 2m \geq s + t\},\\ \mathcal{K}_3 &= \{K \in \mathcal{K} : 31 + m \geq 2s\}.\end{aligned}$$

Clearly $\mathcal{K}_1 \subset \mathcal{K}_3$. It is also not very difficult to see that all these sets are finite; this is done in Lemma 2.6.4. Once the lists are proven to be finite, a computer program can be applied to solve them; this was done in Lemma 2.4.3 (2) and (3). (Note that the three specific fields listed in the statement of Proposition 2.6.3 belong to $\mathcal{K}_2$ or $\mathcal{K}_3$.) Having gotten this out of the way, let us now proceed with the general proof:

There are several possibilities regarding the integral basis; however, we shall perform the proof for all of them simultaneously. We assume $\alpha_0 = \sum x_i^2$, where

$$x_i = \frac{a_i + b_i\sqrt{m} + c_i\sqrt{s} + d_i\sqrt{t}}{2}, \qquad \text{with } a_i + b_i + c_i + d_i \equiv 0 \pmod 2.$$

Depending on the integral basis, further conditions are imposed on the coefficients, but we shall repeat those directly when using them. As usual, the core of the proof is comparing of traces; however, in this case, it will not give us enough information. Therefore we start with another observation, which will then make the comparing of traces more efficient.

Since α_0 is not a sum of four squares in $\mathbb{Z}[\sqrt{m}]$, we can assume that at least one of x_i is not in $\mathbb{Z}[\sqrt{m}]$. Now we proceed to prove a sequence of claims which further restrict the possible values of all the coefficients b_i, c_i, d_i:

(i) At least one product $a_k b_k \neq 0$. In particular, $\sum a_i^2 + m\sum b_i^2 \geq 1 + m$.

(ii) With the exception of fields $K \in \mathcal{K}_1$, we have $\sum c_i^2 + \sum d_i^2 \leq 3$. In particular, c_i and d_i only take the values $0, \pm 1$.

(iii) With the same fields $K \in \mathcal{K}_1$ excluded, there are at least two $x_i \notin \mathbb{Z}[\sqrt{m}]$. This also means $\sum c_i^2 + \sum d_i^2 \geq 2$.

(iv) If $K \notin \mathcal{K}_1 \cup \mathcal{K}_2$, the following holds: Either all $d_i = 0$, or $\sum b_i^2 + \sum c_i^2 + \sum d_i^2 \leq 3$.

(v) If $K \notin \mathcal{K}_1 \cup \mathcal{K}_3$, we have $\sum b_i^2 + \sum c_i^2 + \sum d_i^2 \leq 4$. In particular, $\sum b_i^2 \leq 2$, so b_i can only take values $0, \pm 1$.

The proofs follow:

(i) Comparing the coefficients in front of $\sqrt{m}$ yields the equality $2 = 2(\sum \frac{a_i b_i}{4} + m_0 \sum \frac{c_i d_i}{4})$. Assuming that $a_i b_i = 0$ for all indices, we get $4 = m_0 \sum c_i d_i$, implying $m_0 \mid 4$. Since m_0 is square-free and at least 3, this is impossible.

(ii) By comparing traces, exploiting the previous claim, we get

$$32 + 4m = 4\,\mathrm{Tr}_{\mathrm{abs}}\,\alpha = \sum a_i^2 + m\sum b_i^2 + s\sum c_i^2 + t\sum d_i^2 \geq 1 + m + s\Big(\sum c_i^2 + \sum d_i^2\Big).$$

For the sake of contradiction, assume $\sum c_i^2 + \sum d_i^2 \geq 4$. This yields $31 + 3m \geq 4s$, which is the definition of $K \in \mathcal{K}_1$.

(iii) We already know that at least one $x_i \notin \mathbb{Z}[\sqrt{m}]$. Suppose it were the only one – say, x_1. Then $x_1^2 \in \mathbb{Z}[\sqrt{m}]$, which, by Lemma 2.4.1, means $x_1 = \frac{c_1\sqrt{s} + d_1\sqrt{t}}{2}$.

Combining the previous claim with $c_1 \equiv d_1 \pmod 2$, we get $|c_1| = |d_1| = 1$. Thus there are only two possibilities: $x_1^2 = \frac{s+t}{4} \pm \frac{m_0}{2}\sqrt{m}$. Although for $m_0 \equiv 2 \pmod 4$ this indeed belongs to

$\mathbb{Z}[\sqrt{m}]$, it can never belong to $\mathbb{Z}[2\sqrt{m}]$. Thus $\alpha_0 - x_1^2$ cannot be a sum of squares in $\mathbb{Z}[\sqrt{m}]$, a contradiction.

(iv) To arrive at a contradiction, assume that $\sum b_i^2 + \sum c_i^2 + \sum d_i^2 \geq 4$ where at least one d_i is nonzero. Since $K \notin \mathcal{K}_1$, by the previous claim we also know $\sum c_i^2 + \sum d_i^2 \geq 2$. Putting these pieces of information together, we have $m\sum b_i^2 + s\sum c_i^2 + t\sum d_i^2 \geq 2m + s + t$. Thus

$$32 + 4m \geq 1 + m\sum b_i^2 + s\sum c_i^2 + t\sum d_i^2 \geq 1 + 2m + s + t,$$

i.e. $31 + 2m \geq s + t$. This is the definition of $K \in \mathcal{K}_2$.

(v) For the sake of contradiction, assume $\sum b_i^2 + \sum c_i^2 + \sum d_i^2 \geq 5$. By (iii) we also know $\sum c_i^2 + \sum d_i^2 \geq 2$. Putting these pieces of information together, we have $m\sum b_i^2 + s\sum c_i^2 + t\sum d_i^2 \geq 3m + 2s$. Thus

$$32 + 4m \geq 1 + m\sum b_i^2 + s\sum c_i^2 + t\sum d_i^2 \geq 1 + 3m + 2s,$$

i.e. $31 + m \geq 2s$. This is the definition of $K \in \mathcal{K}_3$. Now $\sum b_i^2 \leq 2$ follows using claim (iii).

Now, assuming $K \notin \mathcal{K}_1 \cup \mathcal{K}_2 \cup \mathcal{K}_3$, the five proven claims provide very strong restrictions for the possible values of $|b_i|, |c_i|, |d_i|$. One sees that all of them are only zeros or ones. To simplify the following discussion, denote by B, C, D the number of nonzero b_i, c_i, d_i. If $D \neq 0$, then by claim (iv) $B + C + D \leq 3$ and by claims (i) and (iii) $B \geq 1$ and $C + D \geq 2$. This gives rise to two possibilities: $B = C = D = 1$ or $B = 1, C = 0, D = 2$. On the other hand, if $D = 0$, then claims (i) and (v) give $1 \leq B \leq 2$ and claims (ii) and (iii) yield $2 \leq C \leq 3$. These are four more possibilities.

Of these latter four possibilities, three can be excluded based on examining the integral bases: Since $D = 0$, all d_i are zero, hence even. Since $B, C \neq 0$, there are odd values of b_i and of c_i. Unless $B = C = 2$, the values of B and C are different, so there is some index i where exactly one of b_i and c_i is odd; therefore a_i is odd as well. Hence a_i, b_i, c_i all attain odd values in our summands, while d_i does not. However, this requires at least two of the elements $\frac{1+\sqrt{m}}{2}$, $\frac{1+\sqrt{s}}{2}$, $\frac{\sqrt{m}+\sqrt{s}}{2}$ to be algebraic integers, and this is impossible (it holds only for fields of type (B4), but there $m \equiv 1 \pmod 4$).

So of the cases where $D = 0$, only $B = C = 2$ remains to be solved. Here all d_i are even, while b_i and c_i attain also odd values. In order not to get a contradiction as in the last paragraph, they must attain these values simultaneously, so the integral basis must contain $\frac{\sqrt{m}+\sqrt{s}}{2}$. This happens if and only if $m \equiv s \pmod 4$. Now we compare traces one last time, using also the existence of $a_k \neq 0$:

$$32 + 4m = \sum a_i^2 + 2m + 2s \geq 1 + 2m + 2s,$$

which can be rewritten as $s - m \leq \frac{31}{2} < 16$. The condition $m \equiv s \pmod 4$ now yields $s = m + 4, m + 8$ or $m + 12$, in which cases nontrivial decompositions indeed exist.

The last two cases to be handled are $B = C = D = 1$ and $B = 1, C = 0, D = 2$. Let us tackle the latter. There are two odd d_i, while only one b_i is odd and all c_i are even. To satisfy the parity condition $a_i + b_i + c_i + d_i \equiv 0 \pmod 2$ for both indices where $d_i \neq 0$, at least one a_i must also be odd. This leads to a contradiction similar to one we already saw: For $m \not\equiv 1$, at most one of the elements $\frac{1+\sqrt{m}}{2}$, $\frac{1+\sqrt{t}}{2}$, $\frac{\sqrt{m}+\sqrt{t}}{2}$ can be an algebraic integer.

The last remaining case is $B = C = D = 1$. (Here the parity condition is easily satisfied: Either one or three of a_i are odd.) By claim (iii) there are two different summands $x_i \notin \mathbb{Z}[\sqrt{m}]$, so we can assume $c_1 = 1$, $d_2 = 1$ (and all the other $c_i, d_i = 0$). There is exactly one nonzero b_i, let us denote it by $b_k = \pm 1$. First we realise that $k = 1$ or $k = 2$: If not, then to satisfy the parity condition, all of a_1, a_2, a_k are odd and all the elements $\frac{1+\sqrt{m}}{2}$, $\frac{1+\sqrt{s}}{2}$, $\frac{1+\sqrt{t}}{2}$ are integral; this is nonsense. So indeed $k = 1$ or $k = 2$. To conclude, let us consider three of the four

equations obtained by comparing α_0 with $\sum x_i^2$ coefficient by coefficient:

$$\begin{aligned} 4 &= \sum a_i b_i + m_0 \sum c_i d_i = \pm a_k \\ 0 &= \sum a_i c_i + s_0 \sum b_i d_i = a_1 + s_0 b_2 \\ 0 &= \sum a_i d_i + t_0 \sum b_i c_i = a_2 + t_0 b_1. \end{aligned}$$

If $k = 2$, then $b_1 = 0$, so the last equation gives $a_k = a_2 = 0$, which contradicts the first equation. Similarly, if $k = 1$, then the second equation contradicts the first.

Thus the proof is concluded (except for the cases $\mathcal{K}_1$, $\mathcal{K}_2$, $\mathcal{K}_3$, which are handled below). □

Now we handle the exceptional cases for which the inequalities in the previous proof were not good enough, thus completing the proof.

Lemma 2.6.4. *Denote by $\mathcal{K}$ the set of all biquadratic fields where $m \not\equiv 1 \pmod 4$, $m \neq 2, 3, 6, 7$ and $s \neq m+4, m+8, m+12$. Then the following sets are finite:*

$$\begin{aligned} \mathcal{K}_1 &= \{K \in \mathcal{K} : 31 + 3m \geq 4s\}, \\ \mathcal{K}_2 &= \{K \in \mathcal{K} : 31 + 2m \geq s + t\}, \\ \mathcal{K}_3 &= \{K \in \mathcal{K} : 31 + m \geq 2s\} \end{aligned}$$

and for each $K \in \mathcal{K}_1 \cup \mathcal{K}_2 \cup \mathcal{K}_3$, the claim of the previous proposition holds: Namely, $\alpha_0 = 7 + (1 + \sqrt{m})^2$ has length 5 in $\mathcal{O}_K$ unless K is one of the three exceptional fields; these three fields contain another element of length 5, defined in the previous proposition.

Proof. Clearly $\mathcal{K}_1 \subset \mathcal{K}_3$, so it suffices to consider the larger sets $\mathcal{K}_2$ and $\mathcal{K}_3$. We already explained in Subsection 2.4.2 that in a *fixed* order $\mathcal{O}_K$, computing the length of a given element is just a computational task. Thus to prove our result, it suffices to provide a full list of fields in $\mathcal{K}_2$ and $\mathcal{K}_3$; the rest of the proof can be handled by a simple computer program (or a very patient student). The results of this computation are already prepared in Lemma 2.4.3 (2) and (3).

We start with $\mathcal{K}_3$. The defining inequality implies $30 \geq s$, so we have $10 \leq m \leq 29$. It suffices to go through all square-free $m \not\equiv 1 \pmod 4$ in this interval and for each of them to list all square-free s satisfying $m < s \leq \frac{31+m}{2}$. We also omit cases where $s = m+4, m+8, m+12$. The full list of the eighteen pairs (m, s) such that $\mathbb{Q}(\sqrt{m}, \sqrt{s}) \in \mathcal{K}_3$ follows:

$$\begin{aligned} &(10,11), (10,13), (10,17), (10,19); (11,13), (11,14), (11,17), (11,21); (14,15), (14,17), \\ &(14,19); (15,17), (15,21), (15,22); (19,21), (19,22); (22,23); (23,26). \end{aligned}$$

We omitted the fields $(10, 15)$ and $(14, 21)$, since we require t to be the largest of the three number m, s, t, while these fields contain $\sqrt{6}$. Therefore, they do not belong to $\mathcal{K}$ and are handled in Subsection 2.6.4.

The finiteness of $\mathcal{K}_2$ is less obvious. However, using the notation with $t_0 < s_0 < m_0$, one can write

$$31 \geq s + t - 2m = m_0 t_0 + m_0 s_0 - 2 s_0 t_0 \geq m_0 t_0 + m_0(t_0 + 1) - 2(m_0 - 1)t_0 = m_0 + 2t_0,$$

so the values of m_0 and hence also s_0 and t_0 are bounded. With a little care, it is quite fast and simple to find a complete list by hand.

It turns out that, due to the restriction $m \geq 10$, the set $\mathcal{K}_2$ contains only two fields:

$$\mathcal{K}_2 = \{\mathbb{Q}(\sqrt{15}, \sqrt{21}), \mathbb{Q}(\sqrt{30}, \sqrt{35})\}.$$

Once we have made the lists explicit, we can apply our computer program. This was successfully done, see Lemma 2.4.3 (2) and (3). In the three fields given by $(10, 13)$, $(11, 13)$ and $(30, 35)$, the original α_0 turns out to be a sum of four or even three squares, hence we had to find another element of length 5. □

2.6.3 The exceptional cases $s = m + 4, m + 8, m + 12$

In this subsection we want to prove $\mathcal{P}(\mathcal{O}_K) \geq 5$ for the three families of fields given by $s = m+4$, $s = m + 8$ and $s = m + 12$ (keeping the conditions $m \not\equiv 1 \pmod 4$, $m \neq 2, 3, 6, 7$). For these fields, the proof from the previous subsection cannot be used, since $\alpha_0 = 7 + (1 + \sqrt{m})^2$ can be written as a sum of four or less squares, see Observation 2.6.2. To find a solution of this problem, let us first examine why the main proof failed in these cases.

The problem lies in the identity

$$\begin{aligned}\alpha_0 - \left(1 + \frac{\sqrt{m} + \sqrt{s}}{2}\right)^2 - \left(1 + \frac{\sqrt{m} - \sqrt{s}}{2}\right)^2 &= (7 + 1 + m + 2\sqrt{m}) - (2 + \frac{m+s}{2} + 2\sqrt{m}) \\ &= 7 - 1 - \frac{s-m}{2},\end{aligned}$$

where $7 - 1 - \frac{s-m}{2}$ is either $7 - 3 = 4$, $7 - 5 = 2$ or $7 - 7 = 0$, depending on the concrete family. All the three values, 4, 2 and 0, are sums of at most two squares in $\mathbb{Z}$.

In this, we were actually rather unlucky: Most positive numbers require three or even four squares! So one solution which suggests itself is to replace 7 by another number n which shares the crucial property of 7 (namely, it is not a sum of three squares in $\mathbb{Z}$), but also solves the previous problem since $n - 3$, $n - 5$ or $n - 7$ (again depending on the family we are examining) is not a sum of two squares.

The next number after 7 which is not a sum of three squares is 15; and while $15 - 5 = 1^2 + 3^2$ and $15 - 7 = 2^2 + 2^2$ are sums of two squares, $15 - 3$ is not. Therefore the first family, $s = m + 4$, could be solved using the element $15 + (1 + \sqrt{m})^2$. The next number which is not a sum of three squares, 23, does not help, but for 28 one sees that both $28 - 5 = 23$ and $28 - 7 = 21$ can not be represented by two squares. Thus, in the following proposition, we solve the remaining two families thanks to the element $28 + (1 + \sqrt{m})^2$.

Proposition 2.6.5. *Let $K = \mathbb{Q}(\sqrt{m}, \sqrt{s})$ where $m \not\equiv 1 \pmod 4$, $m \neq 2, 3, 6, 7$, and $s = m + 4$, $s = m + 8$ or $s = m + 12$. Then $\mathcal{P}(\mathcal{O}_K) \geq 5$.*

In particular,

$$\alpha = \begin{cases} 15 + (1 + \sqrt{m})^2 & \text{if } s = m + 4, \\ 28 + (1 + \sqrt{m})^2 & \text{if } s = m + 8 \text{ or } m + 12 \end{cases}$$

has length 5 unless K is one of the following 16 fields: $m = 10, 11, 15$ and $s = m + 4$; $m = 14, 22, 26, 11, 15, 23$ and $s = m + 8$; $m = 10, 14, 22, 26, 11, 19, 23$ and $s = m + 12$. In these exceptional fields, $7 + (\frac{\sqrt{m}+\sqrt{s}}{2})^2$ has length 5.

Proof. The proof goes along the same lines as that of Proposition 2.6.3, only at the end one must prove that it is impossible to have two summands of the form $x_i = \frac{a_1 + b_1\sqrt{m} + \sqrt{s} \pm \sqrt{t}}{2}$. We just go through the claims which have to be proven on the way, to see which exceptional fields must be handled separately. (See Lemma 2.4.3, not only for the 16 exceptional fields listed in (6) but also the fields included in (4) and (5), for which the statement holds but the following proof breaks down.)

As always, we suppose $\alpha = \sum x_i^2$ with $x_i = \frac{a_i + b_i\sqrt{m} + c_i\sqrt{s} + d_i\sqrt{t}}{2}$; since $m \equiv s \not\equiv 1 \pmod 4$, the conditions are $a_i \equiv d_i$ and $b_i \equiv c_i \pmod 2$ (and in the cases where $t \equiv 3$, a_i and d_i must both be even). It is important to note $t = \frac{ms}{t_0^2}$, where t_0, as the greatest common divisor of m and s, divides 4, 8 or 12, respectively. Together with t_0 being square-free, one sees that if m and s are even, then $t_0 = 2$ or 6, the latter case occurring only if $s = m + 12$ and $3 \mid m$. Similarly, if m and s are odd (thus 3 modulo 4), then $t_0 = 1$ or 3, the latter case again occurring only if $s = m + 12$ and $3 \mid m$. From this, it is easy to see whether $t \equiv 1$ or $t \equiv 3 \pmod 4$, determining the integral basis.

(A) $s = m + 4$: The three fields with $m \leq 15$ must have been handled separately (Lemma 2.4.3 (6)) since α is a sum of less than five squares already in $\mathbb{Z}[\sqrt{m}]$. From now on suppose

$m > 15$. Then at least one x_i is not in $\mathbb{Z}[\sqrt{m}]$. Also, by comparing coefficients in front of $\sqrt{m}$, we see that at least one $a_i b_i \neq 0$. Suppose now that there is a nonzero d_i. For odd m we have $\frac{d_i^2 t}{4} = \frac{d_i^2}{4} m(m+4) \geq \frac{1}{4} m(22+4) = \frac{13}{2} m$, while for even m we use the fact that $t = \frac{m(m+4)}{4} \equiv 3 \pmod 4$ to deduce $\frac{d_i^2 t}{4} \geq \frac{2^2}{4} \frac{m(m+4)}{4} \geq m \frac{19+4}{4}$. Either way, $\frac{d_i^2 t}{4}$ is larger than $\mathrm{Tr}_{\mathrm{abs}}\, \alpha = 16 + m$, which is a contradiction. Hence, all d_i are zero.

Now this implies that all a_i must be even, and one can forget about the integral basis since t plays no more role. If there were only one summand with $c_i \neq 0$, its square would have to belong to $\mathbb{Z}[\sqrt{m}]$, so by Lemma 2.4.1, it would be $\frac{c_i}{2}\sqrt{s}$ with c_i even; we also know that at least one b_j is nonzero, and since $c_j = 0$, this b_j is even. Putting this together, if there is only one summand with $c_i \neq 0$, comparing traces yields $16 + m \geq \frac{b_j^2}{4} m + \frac{c_i^2}{4} s \geq m + s = 2m + 4$, which is impossible.

Therefore there are at least two summands with $c_i \neq 0$. This also means $\sum c_i^2 \geq 2$, and due to the congruence conditions $\sum b_i^2 + \sum c_i^2 \geq 4$. The next step is to show that $\sum b_i^2 + \sum c_i^2 > 4$ is impossible; and indeed, comparing traces and exploiting $\sum b_i^2 + \sum c_i^2 \geq 6$ and $\sum c_i^2 \geq 2$ leads to a contradiction for $m > 26$ (leaving a few cases to be checked separately, see Lemma 2.4.3 (4)).

Now, finally, we know $\sum b_i^2 + \sum c_i^2 = 4$, which together with the existence of nonzero b_i and nonzero c_j implies that one can assume $c_1 = c_2 = 1$, $|b_1| = |b_2| = 1$, and all other b_i, c_i, d_i are zeros. As a result of this, the equations obtained by comparing coefficients of α and $\sum x_i^2$ take the simple form (with the notation $A_i = \frac{a_i}{2} \in \mathbb{Z}$):

$$\begin{aligned} 16 + m &= \sum A_i^2 + m\Big(\frac{1}{4} + \frac{1}{4}\Big) + s\Big(\frac{1}{4} + \frac{1}{4}\Big) = \sum A_i^2 + m + 2, \\ 2 &= 2 \sum \frac{A_i b_i}{2} = A_1 b_1 + A_2 b_2, \\ 0 &= \sum A_i c_i = A_1 + A_2, \\ 0 &= \sum b_i c_i = b_1 + b_2. \end{aligned}$$

The last three equations together with $|b_1| = 1$ show that (after possibly switching x_1 and x_2) $A_1 = b_1 = 1$, $A_2 = b_2 = -1$, which turns the first equation into

$$12 = \sum_{i \geq 3} A_i^2.$$

From this, we see that it is necessary (and sufficient) that there are at least three more summands A_3, A_4, A_5. We have proven that α is not a sum of less than five squares.

(B) $s = m + 8$: For the cases where $m \leq 28$, another choice of α had to be made (Lemma 2.4.3 (6)), since this α is a sum of less than five squares in $\mathbb{Z}[\sqrt{m}]$. Otherwise the proof is just the same as for $s = m + 4$. Proving that all d_i must be zero is slightly complicated by the fact that both for odd and even m, we get $t \equiv 1$; but since in the even case we have $m \geq 30$, one still gets a contradiction if $d_{i_0} \neq 0$:

$$29 + m \geq \frac{{d_{i_0}}^2}{4} t \geq \frac{1}{4} \frac{m(m+8)}{4} \geq m \frac{38}{16} \geq m + \frac{11}{8} m > m + m \geq m + 30.$$

After that, one goes through the same steps as for $s = m + 4$, so we omit most of them. The inequality $\sum b_i^2 + \sum c_i^2 > 4$ gives a contradiction for $m > 48$, so the cases with $m \leq 48$ must be handled separately (Lemma 2.4.3 (5)). For $m > 48$, we eventually come to the conclusion that there must be the summands $x_1^2 = \left(1 + \frac{\sqrt{m}+\sqrt{s}}{2}\right)^2$ and $x_2^2 = \left(-1 + \frac{-\sqrt{m}+\sqrt{s}}{2}\right)^2$, and the other summands are squares of rational integers A_i satisfying $\sum_{i \geq 3} A_i^2 = \alpha - x_1^2 - x_2^2 = 23$. Thus there are at least four such summands – so any representation of α as a sum of squares which uses $x_1 \notin \mathbb{Z}[\sqrt{m}]$ actually needs at least *six* squares.

(C) $s = m + 12$: Here the proof is absolutely the same as in the previous case (even including the fact that for $m \leq 28$ there is a representation of α as a sum of less than five squares in $\mathbb{Z}[\sqrt{m}]$).

The only step where we have to be careful is showing that all d_i are zero. If $s = m+12$, then t_0 can take the values $1, 2, 3, 6$, and especially in the last case, $t = \frac{m(m+12)}{36}$ is not *much larger* then m, which is what the estimates make use of. However, if t_0 is 2 or 6, then $t \equiv 3 \pmod 4$, so $\frac{d_i^2}{4} t \geq t$; and since for $m > 29$ the first field with $s = m + 12$ and $t_0 = 6$ is actually $m = 66$, $s = 78$ (due to 54 not being square-free and the field $\mathbb{Q}(\sqrt{30}, \sqrt{42})$ satisfying $t = m + 12$, since $s = 35$), one gets the following contradiction:

$$29 + m \geq \frac{d_i^2}{4} t \geq t = \frac{m(m+12)}{36} \geq m \frac{78}{36} > 2m,$$

implying $29 > m$. For $t_0 = 1, 2, 3$ one also gets the inequality $\frac{d_i^2}{4} t > 2m$, leading to the same contradiction, so all d_i must indeed be zeros.

To disprove $\sum b_i^2 + \sum c_i^2 > 4$, one must assume $m > 44$ (the remaining cases being handled in Lemma 2.4.3 (5)). With this assumption, one again concludes that one of the summands is $x_1^2 = \left(1 + \frac{\sqrt{m}+\sqrt{s}}{2}\right)^2$, another is $x_2^2 = \left(-1 + \frac{-\sqrt{m}+\sqrt{s}}{2}\right)^2$, and the other summands are squares of rational integers A_i. They must satisfy $\sum_{i \geq 3} A_i^2 = \alpha - x_1^2 - x_2^2 = 21$, so there must be at least three of them. Any representation of α as a sum of squares therefore needs at least five squares. □

2.6.4 Fields containing $\sqrt{6}$ or $\sqrt{7}$

In this section we prove that, save a few exceptions, rings of integers containing $\sqrt{6}$ or $\sqrt{7}$ have Pythagoras number at least 5. More specifically, we prove Propositions 2.6.6 and 2.6.7. In these statements, the meaning of s is fixed by Convention 2.2.1: We have $m = 7$ ($m = 6$, resp.), $s > m$ square-free, and the condition $t > s$ translates into $7 \nmid s$ ($3 \nmid s$, resp.).

Proposition 2.6.6. *Let $K = \mathbb{Q}(\sqrt{7}, \sqrt{s})$. Then $\mathcal{P}(\mathcal{O}_K) \geq 5$.*

In particular, if $s \neq 11$, then $\ell(\alpha) = 5$ holds for $\alpha = \alpha_0 + w^2$, where $\alpha_0 = 1^2 + 1^2 + 1^2 + (1 + \sqrt{7})^2 = 11 + 2\sqrt{7}$ and

$$w = \begin{cases} \frac{1+\sqrt{s}}{2} & \text{if } s \equiv 1 \pmod 4, \\ 1 + \sqrt{s} & \text{if } s \equiv 2 \pmod 4, \\ \frac{\sqrt{7}+\sqrt{s}}{2} & \text{if } s \equiv 3 \pmod 4. \end{cases}$$

For $s = 11$, the element $3 + (\frac{\sqrt{7}+\sqrt{11}}{2})^2 + (1 + \frac{\sqrt{7}+\sqrt{11}}{2})^2$ has length 5.

Proof. Suppose that $\alpha = \sum x_i^2$; since $\alpha \notin \mathbb{Q}(\sqrt{7})$, we can assume $x_1^2 \notin \mathbb{Q}(\sqrt{7})$. It is known (and easy to check) that $\ell(\alpha_0) = 4$ in $\mathbb{Z}[\sqrt{7}]$, see Theorem 2.3.1. Therefore, it suffices to prove that $x_1 = \pm w$ and $x_i \in \mathbb{Z}[\sqrt{7}]$ for $i \neq 1$; indeed, in such a case $\alpha_0 = \sum_{i \neq 1} x_i^2$ requires at least four summands.

To achieve this, denote $x_i = \frac{a_i + b_i\sqrt{7} + c_i\sqrt{s} + d_i\sqrt{7s}}{2}$; there are congruence conditions imposed on the coefficients, but these depend on the type of the field and we do not need them just yet. Comparing traces yields

$$11 + \operatorname{Tr}_{\text{abs}} w^2 = \operatorname{Tr}_{\text{abs}} \alpha = \sum \frac{a_i^2 + 7b_i^2 + sc_i^2 + 7sd_i^2}{4} \geq \frac{s}{4}\Big(\sum c_i^2 + 7 \sum d_i^2\Big). \tag{2.6.1}$$

Since $x_1 \notin \mathbb{Z}[\sqrt{7}]$, the value of $\sum c_i^2 + 7 \sum d_i^2$ is nonzero. To examine this quantity further, we must distinguish the three possible types of fields:

(A) $s \equiv 1$: The field is of type (B2,3) with $q = s$, which means that $a_i \equiv c_i$ and $b_i \equiv d_i \pmod 2$. Therefore the smallest nonzero value of $\sum c_i^2 + 7\sum d_i^2$ is 1. Suppose first, for the sake of contradiction, that $\sum c_i^2 + 7\sum d_i^2 > 1$. Then we have at least $\sum c_i^2 + 7\sum d_i^2 \geq 2$. Plugging this, together with $\operatorname{Tr}_{\text{abs}} w^2 = \frac{1+s}{4}$, into the inequality (2.6.1), yields

$$11 + \frac{1+s}{4} \geq \frac{s}{4} 2,$$

i.e. $45 \geq s$. This holds only for six fields, handled separately in Lemma 2.4.3 (9); otherwise we get a contradiction.

Thus we proved $\sum c_i^2 + 7\sum d_i^2 = 1$; together with $x_1 \notin \mathbb{Q}(\sqrt{7})$ this means $|c_1| = 1$ and all other $c_i, d_i = 0$. In particular, $x_i \in \mathbb{Z}[\sqrt{7}]$ for $i \neq 1$. By choosing the sign, we may assume $x_1 = \frac{a_1 + b_1\sqrt{7} + \sqrt{s}}{2}$. This yields

$$\alpha = x_1^2 + \underbrace{\cdots\cdots}_{\in \mathbb{Q}(\sqrt{7})} = \underbrace{\cdots\cdots}_{\in \mathbb{Q}(\sqrt{7})} + \frac{a_1}{2}\sqrt{s} + \frac{b_1}{2}\sqrt{7s}.$$

Comparing this with $\alpha = (11 + \frac{1+s}{4}) + 2\sqrt{7} + \frac{\sqrt{s}}{2}$, we conclude $a_1 = 1$, $b_1 = 0$. Thus indeed $x_1 = \frac{1+\sqrt{s}}{2} = w$.

(B) $s \equiv 2$: The proof is the same as in the previous case, only with different congruence conditions: The field is of type (B1) with $q = 7$, which means that a_i, b_i are even and $c_i \equiv d_i \pmod 2$. Therefore the smallest nonzero value of $\sum c_i^2 + 7\sum d_i^2$ is 4. Suppose first, for the sake of contradiction, that $\sum c_i^2 + 7\sum d_i^2 > 4$. Then we have at least $\sum c_i^2 + 7\sum d_i^2 \geq 8$, since either some d_j is nonzero, giving $c_j^2 + 7d_j^2 \geq 1 + 7$, or there are at least two nonzero even c_i. Plugging this, together with $\operatorname{Tr}_{\text{abs}} w^2 = 1 + s$, into the inequality (2.6.1), yields

$$11 + (1+s) \geq \frac{s}{4} 8,$$

i.e. $12 \geq s$. This holds only for $s = 10$, handled separately in Lemma 2.4.3 (9); otherwise we get a contradiction.

Thus $\sum c_i^2 + 7\sum d_i^2 = 4$; as before, this means that $x_i \in \mathbb{Z}[\sqrt{7}]$ for $i \neq 1$ and (after possibly changing the sign) $x_1 = \frac{a_1 + b_1\sqrt{7}}{2} + \sqrt{s}$. Hence

$$\alpha = x_1^2 + \underbrace{\cdots\cdots}_{\in \mathbb{Q}(\sqrt{7})} = \underbrace{\cdots\cdots}_{\in \mathbb{Q}(\sqrt{7})} + a_1\sqrt{s} + b_1\sqrt{7s}.$$

Comparing this with $\alpha = (11 + 1 + s) + 2\sqrt{7} + 2\sqrt{s}$, we conclude $a_1 = 2$, $b_1 = 0$. Thus indeed $x_1 = 1 + \sqrt{s} = w$.

(C) $s \equiv 3$: This is analogous to the previous two cases, so we provide only stepping stones. This time the field is of type (B2,3) with $q = 7s$, so $a_i \equiv d_i$ and $b_i \equiv c_i \pmod 2$; as in the first case, the minimal nonzero value of $\sum c_i^2 + 7\sum d_i^2$ is 1. The assumption $\sum c_i^2 + 7\sum d_i^2 \geq 2$ leads to $51 \geq s$; this holds only for nine fields, of which eight are handled in Lemma 2.4.3 (9) and $s = 11$ in Lemma 2.4.3 (10). Thus $\sum c_i^2 + 7\sum d_i^2 = 1$, which straightforwardly leads to $x_i \in \mathbb{Z}[\sqrt{7}]$ for $i \neq 1$ and $\pm x_1 = \frac{a_1 + b_1\sqrt{7} + \sqrt{s}}{2}$; comparing coefficients then yields $\pm x_1 = \frac{\sqrt{7} + \sqrt{s}}{2} = w$ as needed. □

By straightforwardly applying the same method, we can prove the analogous result for $\sqrt{6}$. The only difference is that there are more cases to handle due to the fact that s is not necessarily coprime with 6. However, once the case distinction is made and the integral basis fixed, the proofs are complete analogies to the one above. Note that we had to include $m = 6$ explicitly in the statement to exclude the one possibility $t = 6$, $s = 3$, $m = 2$.

Proposition 2.6.7. *Let $K = \mathbb{Q}(\sqrt{6}, \sqrt{s})$ with $m = 6$. Then $\mathcal{P}(\mathcal{O}_K) \geq 5$.*

In particular, if $s \neq 10$, then $\ell(\alpha) = 5$ holds for $\alpha = \alpha_0 + w^2$, where $\alpha_0 = 1^2 + 1^2 + 1^2 + (1 + \sqrt{6})^2 = 10 + 2\sqrt{6}$ and

$$w = \begin{cases} \frac{1+\sqrt{s}}{2} & \text{if } s \equiv 1 \pmod 4, \\ \frac{\sqrt{6}+\sqrt{s}}{2} & \text{if } s \equiv 2 \pmod 4, \\ 1 + \sqrt{s} & \text{if } s \equiv 3 \pmod 4. \end{cases}$$

For $s = 10$, the element $3 + (\sqrt{6} - \frac{\sqrt{6}+\sqrt{10}}{2})^2 + (2 + \frac{\sqrt{6}+\sqrt{10}}{2})^2$ has length 5.

Proof. Direct analogy of the previous proof. If $s \equiv 1, 3 \pmod 4$, then $\gcd(6, s) = 1$, so there is nothing new and one gets the inequalities $s \leq 41$ and $s \leq 22$, respectively, which leaves $5 + 3$ fields to be checked separately in Lemma 2.4.3 (7). If $s \equiv 2$, one has $\gcd(6, s) = 2$ and $s = 2m_0$, which makes the estimates slightly less efficient; moreover, one must distinguish between fields with $m_0 \equiv 1 \pmod 4$, which are of type (B1), and fields with $m_0 \equiv 3 \pmod 4$, which are of type (B2,3). The case $s = 10$ is dealt with in Lemma 2.4.3 (8), while the $2 + 7$ fields which are not excluded by the analogously obtainable inequalities $s \leq 2 \cdot 23$ in the former and $s \leq 2 \cdot 46$ in the latter case, are again solved in Lemma 2.4.3 (7). □

2.6.5 Fields containing $\sqrt{2}$, $\sqrt{3}$ or $\sqrt{5}$

Finally, we shall handle the fields with $m = 2, 3, 5$. Here we find the result quite surprising; the Pythagoras number of $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ is only three, but it still turns out that save a few exceptions, the Pythagoras number of $\mathcal{O}_K$ where K contains $\mathbb{Q}(\sqrt{m})$ is at least five. This is in contrast with the situation in $\mathbb{Z}$: $\mathcal{P}(\mathbb{Z}) = 4$, while in orders of quadratic extensions of $\mathbb{Z}$ the Pythagoras number grows only by (at most) one. Let us also remark that for $m = 5$, the Pythagoras number is actually *at most* five, and for $m = 2$ we conjecture the same, while for $m = 3$ it seems that usually $\mathcal{P}(\mathcal{O}_K) = 6$ – see Theorem 2.1.3 and Conjecture 2.1.6.

The proofs in this subsection are reasonably straightforward (although some tricks like using Lemmata 2.4.1 and 2.4.2 are required) and not even very lengthy; only guessing the appropriate choice of α would be difficult. We used data from our computer programs (see Subsection 2.4.2) to observe which choice might be the right one. In the case of $K = \mathbb{Q}(\sqrt{5}, \sqrt{s})$ with $s \not\equiv 1 \pmod 4$, we were unable to find such a suitable α; therefore we had to develop stronger tools – the proof of this case is given in Subsection 2.7.1.

Proposition 2.6.8. *Let $K = \mathbb{Q}(\sqrt{5}, \sqrt{s})$ for $s \equiv 1 \pmod 4$. Then $\mathcal{P}(\mathcal{O}_K) \geq 5$.*

In particular, the following element has length 5:

$$\alpha = 1^2 + 1^2 + \left(\frac{1 + \sqrt{5}}{2}\right)^2 + \left(\frac{1 + \sqrt{s}}{2}\right)^2 + \left(\frac{-\sqrt{5} + \sqrt{s}}{2}\right)^2.$$

Proof. Let us suppose that

$$\alpha = \left(5 + \frac{s}{2}\right) + \frac{\sqrt{5}}{2} + \frac{\sqrt{s}}{2} - \frac{\sqrt{5s}}{2} = \sum x_i^2.$$

First assume that at least one of x_i is of the form $\frac{a_i + b_i\sqrt{5} + c_i\sqrt{s} + d_i\sqrt{5s}}{4}$ for a_i, b_i, c_i, d_i odd. Then, by Lemma 2.4.2, x_i^2 is of the same form, which implies that at least one other x_j must have the same property as well. Then by comparing traces we obtain

$$5 + \frac{s}{2} \geq \mathrm{Tr}_{\mathrm{abs}}(x_i^2 + x_j^2) \geq 2 \cdot \frac{1 + 5 + s + 5s}{16} = \frac{3 + 3s}{4},$$

i.e. $17 \geq s$. This is a contradiction unless $s = 13$ or $s = 17$, which cases are handled in Lemma 2.4.3 (14).

So we have shown that all summands are in fact of the form

$$x_i = \frac{a_i + b_i\sqrt{5} + c_i\sqrt{s} + d_i\sqrt{5s}}{2} \qquad \text{where } a_i + b_i + c_i + d_i \text{ is even.}$$

Our next aim is to prove that $d_i = 0$ for each i. Again, this is achieved by comparing traces: If at least one d_i is nonzero, we get

$$5 + \frac{s}{2} \geq 5s \sum \frac{1}{4} d_i^2 \geq \frac{5s}{4};$$

this holds only for $s < 7$, so in our situation all d_i must indeed be zero.

What can be the value of $\sum c_i^2$? It cannot be zero, since $\alpha \notin \mathbb{Q}(\sqrt{5})$. The cases $\sum c_i^2 = 1$ and $\sum c_i^2 = 2$ require the most care; now we shall prove that $\sum c_i^2 \geq 3$ is impossible (for $s > 10$). Indeed, it would yield

$$5 + \frac{s}{2} \geq s\frac{1}{4} \sum c_i^2 \geq \frac{3s}{4}.$$

Next we exclude the case $\sum c_i^2 = 1$. Without loss of generality we assume $x_1 = \frac{a_1 + b_1\sqrt{5} + \sqrt{s}}{2}$; $a_1 \not\equiv b_1 \pmod 2$. All the other summands belong to $\mathbb{Q}(\sqrt{5})$, so we must have $\alpha - x_1^2 \in \mathbb{Q}(\sqrt{5})$. After comparing the third and fouth coefficient of

$$x_1^2 = \frac{a_1^2 + 5b_1^2 + s}{4} + \frac{a_1 b_1}{2}\sqrt{5} + \frac{a_1}{2}\sqrt{s} + \frac{b_1}{2}\sqrt{5s}$$

with those of α, we see $a_1 = 1$, $b_1 = -1$. This is a contradiction, since one of them must be even.

So we have proven that $\sum c_i^2 = 2$ is necessary. Without loss of generality we write $x_1 = \frac{a_1 + b_1\sqrt{5} + \sqrt{s}}{2}$ and $x_2 = \frac{a_2 + b_2\sqrt{5} + \sqrt{s}}{2}$ with $a_1 \not\equiv b_1$ and $a_2 \not\equiv b_2 \pmod 2$; the remaining x_i are in $\mathbb{Q}(\sqrt{5})$. Comparing traces, we get the equality

$$5 + \frac{s}{2} = \frac{1}{4}\Big(\sum a_i^2 + 5\sum b_i^2 + s \cdot 2\Big),$$

i.e. $20 = \sum a_i^2 + 5\sum b_i^2$. This yields a short list of possible combinations of x_i, and it is a simple matter to check by hand that the only one which indeed gives α is the one by which α was defined:

Since $\alpha - (x_1^2 + x_2^2) \in \mathbb{Q}(\sqrt{5})$, we compare coefficients:

$$x_1^2 + x_2^2 = \underbrace{\cdots\cdots}_{\in\mathbb{Q}(\sqrt{5})} + \frac{a_1 + a_2}{2}\sqrt{s} + \frac{b_1 + b_2}{2}\sqrt{5s},$$

so $a_1 + a_2 = 1$ and $b_1 + b_2 = -1$. The latter equality together with $\sum b_i^2 \leq 4$ clearly gives only one solution: $b_1 = -1, b_2 = 0$ (or vice versa). Then a_1 is even, and $a_2 = 1 - a_1$ is odd.

To satisfy the inequality $a_1^2 + a_2^2 \leq 20 - 5b_1^2 = 15$, the only options are $a_1 = -2, 0, 2$. Thus there are only three possibilities:

- $x_1 = \frac{-2 - \sqrt{5} + \sqrt{s}}{2}$, $x_2 = \frac{3 + \sqrt{s}}{2}$,
- $x_1 = \frac{-\sqrt{5} + \sqrt{s}}{2}$, $x_2 = \frac{1 + \sqrt{s}}{2}$,
- $x_1 = \frac{2 - \sqrt{5} + \sqrt{s}}{2}$, $x_2 = \frac{-1 + \sqrt{s}}{2}$.

In the first case, $\alpha - x_1^2 - x_2^2 = \frac{1}{2} - \frac{\sqrt{5}}{2}$, which is not totally positive, hence cannot be a sum of squares – a contradiction. Similarly, in the third case $\alpha - x_1^2 - x_2^2 = \frac{5}{2} + \frac{2\sqrt{5}}{2}$, which is also not totally positive.

Hence we have proven that $x_1 = \frac{-\sqrt{5} + \sqrt{s}}{2}$, $x_2 = \frac{1 + \sqrt{s}}{2}$, which gives $\sum_{i \geq 3} x_i^2 = \frac{7 + \sqrt{5}}{2}$. We already know that $x_i \in \mathbb{Q}(\sqrt{5})$ for $i \geq 3$, so there must be at least three more summands since $\ell\big(\frac{7+\sqrt{5}}{2}\big) = 3$ in $\mathbb{Z}\big[\frac{1+\sqrt{5}}{2}\big]$ by Theorem 2.3.1. This concludes the proof. □

Now we solve both types of biquadratic fields containing $\sqrt{2}$.

Proposition 2.6.9. *If $K = \mathbb{Q}(\sqrt{2}, \sqrt{s})$ for $s \neq 3, 5, 7$, then $\mathcal{P}(\mathcal{O}_K) \geq 5$.*
In particular, depending on the value of s modulo 4, the following element has length 5:

$$\alpha = \begin{cases} 1^2 + (1-\sqrt{2})^2 + (2-\sqrt{2})^2 + \left(\frac{1}{2} + \sqrt{2} + \frac{\sqrt{s}}{2}\right)^2 + \left(\frac{-1+\sqrt{2}-\sqrt{s}+\sqrt{2s}}{2}\right)^2 & \text{if } 13 \neq s \equiv 1; \\ 1^2 + \sqrt{2}^2 + (1-\sqrt{2})^2 + \left(1 + \frac{-\sqrt{2}-\sqrt{2s}}{2}\right)^2 + \left(\frac{\sqrt{2}}{2} - \sqrt{s} + \frac{\sqrt{2s}}{2}\right)^2 & \text{if } s \equiv 3; \\ 1 + \sqrt{2}^2 + (1+\sqrt{2})^2 + \left(\sqrt{2} + \frac{1+\sqrt{13}}{2}\right)^2 + \left(2 + \frac{1+\sqrt{13}}{2} + \frac{\sqrt{2}+\sqrt{26}}{2}\right)^2 & \text{if } s = 13. \end{cases}$$

Proof. The proof is analogous to that of Proposition 2.6.8. One handles the cases $s \equiv 1$ and $s \equiv 3$ separately and arrives at inequalities $s \leq 30$ and $s \leq 16$, respectively; thus, to get a full contradiction, one needs to cover the cases $s = 13, 17, 21, 29$ and $s = 11, 15$, which is done in Lemma 2.4.3 (11) and (12). □

Finally, we turn our attention to fields containing $\sqrt{3}$. As a side note, remember that, unlike with $\sqrt{2}$ and $\sqrt{5}$, the lower bound 5 is known not to always be optimal – see Proposition 2.4.5.

Proposition 2.6.10. *If $K = \mathbb{Q}(\sqrt{3}, \sqrt{s})$ for $s \neq 5, 7$, then $\mathcal{P}(\mathcal{O}_K) \geq 5$.*
In particular, the following element has length 5:

$$\alpha = \begin{cases} 1^2 + 1^2 + (2+\sqrt{3})^2 + \left(\frac{1+\sqrt{s}}{2}\right)^2 + \left(1 + \frac{1+\sqrt{s}}{2}\right)^2 & \text{if } s \equiv 1 \pmod 4; \\ 1^2 + 1^2 + (2+\sqrt{3})^2 + \left(\frac{\sqrt{s}+\sqrt{3s}}{2}\right)^2 + \left(1 + \frac{\sqrt{s}+\sqrt{3s}}{2}\right)^2 & \text{if } s \equiv 2 \pmod 4; \\ 1^2 + 1^2 + (2+\sqrt{3})^2 + \left(\frac{\sqrt{3}+\sqrt{s}}{2}\right)^2 + \left(1 + \frac{\sqrt{3}+\sqrt{s}}{2}\right)^2 & \text{if } s \equiv 3 \pmod 4. \end{cases}$$

Proof. Again, the proof is analogous to that of Proposition 2.6.8. Each of the three cases must be done separately. In the first and in the third, one arrives at the inequality $s \leq 46$, while the second yields $s \leq 10$. These $5 + 1 + 6$ fields must be examined separately, see Lemma 2.4.3 (13). □

It is interesting that while the used element $1^2 + 1^2 + (2+\sqrt{3})^2$ is not a sum of two squares, it has another representation as a sum of three squares: $1^2 + (1+\sqrt{3})^2 + (1+\sqrt{3})^2$.

Now we have (almost) all the pieces needed to prove the main result of Section 2.6. The structure of the proof should be clear from the structure of this section, but for clarity, we repeat it here:

Proof of Theorem 2.1.2 (1). First suppose that K contains none of $\sqrt{2}$, $\sqrt{3}$, $\sqrt{5}$, $\sqrt{6}$, $\sqrt{7}$ and $\sqrt{13}$. If $m \equiv 1 \pmod 4$, we use Proposition 2.6.1. If $m \not\equiv 1 \pmod 4$, most fields are covered in Proposition 2.6.3, and the exceptional cases where s is equal to $m+4$, $m+8$ or $m+12$ are handled in Proposition 2.6.5.

On the other hand, suppose that $m \in \{2, 3, 5, 6, 7, 13\}$ and K is not one of the seven exceptional fields. The cases $m = 2$ and $m = 3$ are covered in Proposition 2.6.9 and Proposition 2.6.10, respectively. If $m = 5$ and $s \equiv 1 \pmod 4$, Proposition 2.6.8 is used, while for $s \not\equiv 1$, Proposition 2.7.1 applies. Finally, for $m = 6$ (7 or 13, resp.) one exploits Proposition 2.6.7 (2.6.6 or 2.8.3, resp.). □

2.7 Fields containing $\sqrt{5}$

In this section, we take a closer look at fields containing $\sqrt{5}$. They are special since for most of them, we were able to determine the exact value of the Pythagoras number, namely 5. (The four exceptional fields are $\mathbb{Q}(\sqrt{2}, \sqrt{5})$, $\mathbb{Q}(\sqrt{3}, \sqrt{5})$, $\mathbb{Q}(\sqrt{5}, \sqrt{6})$ and $\mathbb{Q}(\sqrt{5}, \sqrt{7})$; for the first two we expect $\mathcal{P}(\mathcal{O}_K) = 3$, while for the latter two $\mathcal{P}(\mathcal{O}_K) = 4$.)

In Subsection 2.7.1, we continue where we left off in the previous section by proving that $\mathcal{P}(\mathcal{O}_K) \geq 5$ for all but finitely many fields $K = \mathbb{Q}(\sqrt{5}, \sqrt{s})$ where $s \equiv 2, 3 \pmod 4$. This turned out to be much more involved than the seemingly analogous cases handled in Subsection 2.6.5; the method which we developed for proving Proposition 2.7.2 deserves further investigation and can be employed in many other situations.

Subsection 2.7.2 is untypical for this text as it is the only part where we prove an upper bound on the Pythagoras number. To achieve that, we first introduce the reader to the so-called g-invariants $g_R(n)$ of a ring R and then explain how they, in general, provide upper bounds for Pythagoras numbers in field extensions, generalising a result by Kala and Yatsyna [KY2]. Finally, we prove that $g_{\mathcal{O}_F}(2) = 5$ holds for $F = \mathbb{Q}(\sqrt{5})$, a result published in [Sa2].

2.7.1 Lower bound in the most difficult case

The aim of this subsection is to show that with finitely many exceptions, $\mathcal{P}(\mathcal{O}_K) \geq 5$ holds for all biquadratic fields $K = \mathbb{Q}(\sqrt{5}, \sqrt{s})$. Recall the notation $1 < m < s < t$, which in this case means $s \neq 2, 3$, s is square-free, $5 \nmid s$. Since the case $s \equiv 1 \pmod 4$ was already handled in Proposition 2.6.8, we achieve our goal by proving the following:

Proposition 2.7.1. *Let $K = \mathbb{Q}(\sqrt{5}, \sqrt{s})$ where $s \not\equiv 1 \pmod 4$, $s \neq 6, 7$. Then $\mathcal{P}(\mathcal{O}_K) \geq 5$.*
In particular, $\ell(\alpha) = 5$ holds for

$$\alpha = 1^2 + \Big(\frac{1+\sqrt{5}}{2}\Big)^2 + \Big(\frac{1+\sqrt{5}}{2}\Big)^2 + (\lfloor\sqrt{s}\rfloor + \sqrt{s})^2 + (\lceil\sqrt{s}\rceil + \sqrt{s})^2.$$

The symbols $\lfloor x \rfloor$ and $\lceil x \rceil$ denote the largest integer satisfying $n \leq x$ and the smallest integer satisfying $x \leq n$, respectively.

Proof. The core of the proof is contained in Proposition 2.7.3. Once that result is proven, two tasks remain: First, one has to take care of the fields with $s \leq 3253$ where the proposition does not apply; as usual, this was done by our computer program, see Lemma 2.4.3 (15).

Second, one has to exploit that for $s \geq 3254$, Proposition 2.7.3 allows only the following type of decomposition:

$$\alpha = x_1^2 + x_2^2 + \beta = \Big(\frac{a_1 + b_1\sqrt{5}}{2} + \sqrt{s}\Big)^2 + \Big(\frac{a_2 + b_2\sqrt{5}}{2} + \sqrt{s}\Big)^2 + \beta, \quad \text{where } \beta \in \sum \mathcal{O}^2_{\mathbb{Q}(\sqrt{5})}.$$

We shall show that $b_1 = b_2 = 0$ and $\frac{1}{2}a_1 = \lfloor\sqrt{s}\rfloor$ and $\frac{1}{2}a_2 = \lceil\sqrt{s}\rceil$ (or vice versa). This suffices since then $\beta = 1^2 + (\frac{1+\sqrt{5}}{2})^2 + (\frac{1+\sqrt{5}}{2})^2$ which has length 3 in $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ (remember that by Proposition 2.7.3 we can only use summands from this subfield).

To achieve this, we expand brackets:

$$\Big(\frac{a_1 + b_1\sqrt{5}}{2} + \sqrt{s}\Big)^2 + \Big(\frac{a_2 + b_2\sqrt{5}}{2} + \sqrt{s}\Big)^2 = \underbrace{\cdots\cdots}_{\in\mathbb{Q}(\sqrt{5})} + (a_1 + a_2)\sqrt{s} + (b_1 + b_2)\sqrt{5s};$$

comparing this with $\alpha = \underbrace{\cdots\cdots}_{\in\mathbb{Q}(\sqrt{5})} + 2(\lfloor\sqrt{s}\rfloor + \lceil\sqrt{s}\rceil)\sqrt{s}$, one sees that $a_1 + a_2 = 2(\lfloor\sqrt{s}\rfloor + \lceil\sqrt{s}\rceil)$ and $b_1 + b_2 = 0$.

To conclude the proof, one has to compare traces. As we explain below, the assumption $\mathrm{Tr}_{\mathrm{abs}}\,\alpha \geq \mathrm{Tr}_{\mathrm{abs}}(x_1^2 + x_2^2)$ together with the equalities $a_1 + a_2 = 2(\lfloor\sqrt{s}\rfloor + \lceil\sqrt{s}\rceil)$ and $b_1 + b_2 = 0$ and parity conditions $a_1 \equiv b_1$ and $a_2 \equiv b_2 \pmod 2$ leaves only five possible choices (if we fix that either $a_1 > a_2$, or $a_1 = a_2$ and $b_1 \geq b_2$); namely, (a_1, a_2, b_1, b_2) can either take the correct value $(2\lceil\sqrt{s}\rceil, 2\lfloor\sqrt{s}\rfloor, 0, 0)$, or one of the following four:

$$(2\lceil\sqrt{s}\rceil + 2, 2\lfloor\sqrt{s}\rfloor - 2, 0, 0); \qquad (\lceil\sqrt{s}\rceil + \lfloor\sqrt{s}\rfloor, \lceil\sqrt{s}\rceil + \lfloor\sqrt{s}\rfloor, 1, -1);$$
$$(\lceil\sqrt{s}\rceil + \lfloor\sqrt{s}\rfloor + 2, \lceil\sqrt{s}\rceil + \lfloor\sqrt{s}\rfloor - 2, \pm 1, \mp 1).$$

For the four incorrect possibilities, one indeed gets $\beta = \alpha - (x_1^2 + x_2^2) \in \mathbb{Q}(\sqrt{5})$ with nonnegative trace, but in none of the cases is β totally nonnegative. This concludes the proof.

To help the reader, we explain how to compare the traces efficiently. By evaluating the traces, one gets

$$2s + \lfloor\sqrt{s}\rfloor^2 + \lceil\sqrt{s}\rceil^2 + 4 \geq \frac{a_1^2 + a_2^2 + 5(b_1^2 + b_2^2)}{4} + 2s;$$

on the right-hand side we use the general identity $2x^2 + 2y^2 = (x+y)^2 + (x-y)^2$ together with the known values of $a_1 + a_2$ and $b_1 + b_2$ to obtain

$$\lfloor\sqrt{s}\rfloor^2 + \lceil\sqrt{s}\rceil^2 + 4 \geq \frac{(a_1 - a_2)^2 + 5(b_1 - b_2)^2}{8} + \frac{(\lfloor\sqrt{s}\rfloor + \lceil\sqrt{s}\rceil)^2}{2}.$$

Surprisingly, this is can be rewritten (for $\sqrt{s} \notin \mathbb{Z}$) as $36 \geq (a_1 - a_2)^2 + 5(b_1 - b_2)^2$, which, together with the parity conditions, leaves only the five possibilities listed above. □

Before proving Proposition 2.7.3, we start with a general result which provides very strong information about the possible decompositions of a whole family of elements; this family contains also α. Results of this type could be proved for extensions of fields other than $\mathbb{Q}(\sqrt{5})$, but in no other case were we forced to use them. Avoiding them was practical, since counterexamples of this type lead to a rather large number of exceptional fields (compare part (15) of Lemma 2.4.3 with other parts of the same lemma).

Proposition 2.7.2. *Let $\alpha_0, A_1, A_2 \in \mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ and $n \in \mathbb{N}$. Then there exists a bound $S(n)$ such that for $s > S(n)$, $s \not\equiv 1 \pmod 4$, (square-free, $5 \nmid s$), the following holds:*

Denote $K = \mathbb{Q}(\sqrt{5}, \sqrt{s})$. Whenever the number

$$\alpha = \alpha_0 + \left(\lfloor\sqrt{s}\rfloor + A_1 + \sqrt{s}\right)^2 + \left(\lfloor\sqrt{s}\rfloor + A_2 + \sqrt{s}\right)^2$$

is represented as a sum of at most n squares in $\mathcal{O}_K$, then exactly two of the squares belong to $(\mathcal{O}_{\mathbb{Q}(\sqrt{5})} + \sqrt{s})^2$ and the remaining lie in $(\mathcal{O}_{\mathbb{Q}(\sqrt{5})})^2$.

Proof. First we observe that absolute values of two of the conjugates of α are bounded by a constant $k = k(\alpha_0, A_1, A_2)$ independent on s; this is clearly true for the two automorphisms of K sending $\sqrt{s} \mapsto -\sqrt{s}$, since the conjugates of α_0, A_1 and A_2 are only constants and $\lfloor\sqrt{s}\rfloor - \sqrt{s}$ is bounded. From this one easily sees that if $\alpha = \sum x_i^2$ with $x_i = a_i + b_i\sqrt{5} + c_i\sqrt{s} + d_i\sqrt{5s}$ **(where the coefficients belong to $\mathbb{Q}$, not necessarily $\mathbb{Z}$)**, then

$$|a_i - b_i\sqrt{5} - c_i\sqrt{s} + d_i\sqrt{5s}| < \sqrt{k},$$
$$|a_i + b_i\sqrt{5} - c_i\sqrt{s} - d_i\sqrt{5s}| < \sqrt{k}.$$

Triangle inequality then yields

$$|a_i - c_i\sqrt{s}| < \sqrt{k} \qquad \text{and} \qquad |b_i\sqrt{5} - d_i\sqrt{5s}| < \sqrt{k}. \tag{2.7.1}$$

We shall exploit this later. Now we need to find any constants $C, D \in \mathbb{Q}$ and $S_1 \in \mathbb{N}$ such that for $s > S_1$, we have $|c_i| \leq C$ and $|d_i| \leq D$. This is easily done by comparing traces, since $\operatorname{Tr}_{\text{abs}} \alpha$ is $4s + O(\sqrt{s})$ while $\operatorname{Tr}_{\text{abs}} x_i^2 \geq c_i^2 s$ and $\operatorname{Tr}_{\text{abs}} x_i^2 \geq d_i^2 5s$; thus by choosing a large enough S_1 we can even deduce $c_i^2 \leq 4$ and $5d_i^2 \leq 4$. (Since $c_i, d_i \in \frac{\mathbb{Z}}{2}$, we have $C = 2$ and $D = \frac{1}{2}$; but the exact value of these constants is not important.)

From now on consider only $s > S_1$. Our plan is to compare the asymptotic behaviour of $\operatorname{Tr}_{\text{abs}} \alpha$ and $\sum \operatorname{Tr}_{\text{abs}} x_i^2$. We already mentioned that $\operatorname{Tr}_{\text{abs}} \alpha$ can be written as $4s + x(s)$, where $|x(s)| \leq k_1\sqrt{s} + k_2$; here k_1 and k_2 are explicit constants depending only on α_0, A_1, A_2.

So it remains to analyse $\sum \operatorname{Tr}_{\text{abs}} x_i^2$, where $\operatorname{Tr}_{\text{abs}} x_i^2 = a_i^2 + 5b_i^2 + sc_i^2 + 5sd_i^2$. Thanks to (2.7.1) we can replace the first two terms: There is a $\delta \in (-\sqrt{k}, \sqrt{k})$ such that

$$a_i^2 = (c_i\sqrt{s} + \delta)^2 = sc_i^2 + 2\delta c_i\sqrt{s} + \delta^2 = sc_i^2 + y,$$

where $|y| \leq (2 \cdot \sqrt{k}C)\sqrt{s} + (\sqrt{k})^2$. Similarly $5b_i^2 = 5sd_i^2 + z$ where $|z| \leq (2 \cdot \sqrt{k}D\sqrt{5})\sqrt{s} + (\sqrt{k})^2$. All in all,

$$\mathrm{Tr}_{\mathrm{abs}}\, x_i^2 = (sc_i^2 + y) + (5sd_i^2 + z) + sc_i^2 + 5sd_i^2 = 2(c_i^2 + 5d_i^2)s + (y + z) = 2(c_i^2 + 5d_i^2)s + O(\sqrt{s}).$$

So far the number of squares in the decomposition played no role; what we have proved actually holds for any $x_i^2 \preccurlyeq \alpha$. Now, in the last step, the constants start depending on n:

$$\begin{aligned}\sum_{i=1}^{n} \mathrm{Tr}_{\mathrm{abs}}\, x_i^2 = \sum_{i=1}^{n}\Big(2(c_i^2 + 5d_i^2)s + O(\sqrt{s})\Big) &= 2\Big(\sum_{i=1}^{n} c_i^2 + 5d_i^2\Big)s + nO(\sqrt{s}) \\ &= 2\Big(\sum_{i=1}^{n} c_i^2 + 5d_i^2\Big)s + O(\sqrt{s}).\end{aligned}$$

Since this also has to be equal to $\mathrm{Tr}_{\mathrm{abs}}\, \alpha = 4s + O(\sqrt{s})$, we finally conclude that for $s > S(n)$ the coefficients in front of s are equal:

$$2 = \sum_{i=1}^{n}(c_i^2 + 5d_i^2).$$

Since c_i, d_i are either both in $\frac{\mathbb{Z}}{2} \setminus \mathbb{Z}$ or both in $\mathbb{Z}$, one easily sees that each nonzero summand in this sum is either $1^2 + 0 = 1$ or $\left(\frac{1}{2}\right)^2 + 5\left(\frac{1}{2}\right)^2 = \frac{3}{2}$. However, to obtain 2 as a sum of these numbers, the only choice is $1 + 1$. Therefore for each i we have either $c_i = d_i = 0$, or $|c_i| = 1$, $d_i = 0$, and the latter case happens for exactly two indices i_1, i_2. Since $x_i^2 = (-x_i)^2$, we can choose $c_{i_1} = c_{i_2} = 1$, which concludes the proof. □

The result we need to complete the proof of Proposition 2.7.1 is just the previous Proposition with concrete choices $\alpha_0 = 1 + \left(\frac{1+\sqrt{5}}{2}\right)^2 + \left(\frac{1+\sqrt{5}}{2}\right)^2 = 4 + \sqrt{5}$, $A_1 = 0$, $A_2 = 1$, and with the effectively computed bound $S(4)$. The main reason for proving first the general version was to make the proof easier to read. Now, going through the previous proof step by step, computing the bounds explicitly (and being slightly more careful in order to get reasonably small values) yields the following:

Proposition 2.7.3. *Denote $K = \mathbb{Q}(\sqrt{5}, \sqrt{s})$ for $s \geq 3254$, $s \not\equiv 1 \pmod 4$, (square-free, $5 \nmid s$). Then the following holds:*

Whenever the number

$$\alpha = 1^2 + \Big(\frac{1+\sqrt{5}}{2}\Big)^2 + \Big(\frac{1+\sqrt{5}}{2}\Big)^2 + \left(\lfloor\sqrt{s}\rfloor + \sqrt{s}\right)^2 + \left(\lceil\sqrt{s}\rceil + \sqrt{s}\right)^2$$

is represented as a sum of four squares in $\mathcal{O}_K$, then exactly two of the squares belong to $(\mathcal{O}_{\mathbb{Q}(\sqrt{5})} + \sqrt{s})^2$ and the remaining two lie in $(\mathcal{O}_{\mathbb{Q}(\sqrt{5})})^2$.

Proof. The reader has already seen the general version of this proof in Proposition 2.7.2. Thus we only include concrete values of some bounds as stepping stones.

To avoid fractions, we denote $\varphi = \frac{1+\sqrt{5}}{2}$ and $\overline{\varphi} = \frac{1-\sqrt{5}}{2}$.

If α' is the image of α in the automorphism of K sending $\sqrt{5} \mapsto -\sqrt{5}$, $\sqrt{s} \mapsto -\sqrt{s}$ and α'' in the automorphism $\sqrt{5} \mapsto \sqrt{5}$, $\sqrt{s} \mapsto -\sqrt{s}$, then clearly

$$\alpha' = 1 + 2\overline{\varphi}^2 + \left(\lfloor\sqrt{s}\rfloor - \sqrt{s}\right)^2 + \left(\lceil\sqrt{s}\rceil - \sqrt{s}\right)^2 < 1 + 2\overline{\varphi}^2 + 1 = 5 - \sqrt{5}$$

and similarly

$$\alpha'' < 2 + 2\varphi^2 = 5 + \sqrt{5}.$$

Thus

$$|a_i - b_i\sqrt{5} - c_i\sqrt{s} + d_i\sqrt{5s}| < \sqrt{5-\sqrt{5}},$$
$$|a_i + b_i\sqrt{5} - c_i\sqrt{s} - d_i\sqrt{5s}| < \sqrt{5+\sqrt{5}}.$$

By triangle inequality

$$|a_i - c_i\sqrt{s}| < \kappa \qquad \text{and} \qquad |b_i\sqrt{5} - d_i\sqrt{5s}| < \kappa, \tag{2.7.2}$$

where $\kappa = \frac{1}{2}\Big(\sqrt{5-\sqrt{5}} + \sqrt{5+\sqrt{5}}\Big)$.

Now we shall express the asymptotic behaviour of $\mathrm{Tr}_{\mathrm{abs}}\,\alpha$. Denote $\{s\} = \sqrt{s} - \lfloor\sqrt{s}\rfloor$. Then

$$\begin{aligned}
\mathrm{Tr}_{\mathrm{abs}}\,\alpha &= 1 + 2\cdot\frac{3}{2} + \lfloor\sqrt{s}\rfloor^2 + s + \lceil\sqrt{s}\rceil^2 + s \\
&= 4 + 2s + (\sqrt{s} - \{s\})^2 + (\sqrt{s} + (1 - \{s\}))^2 \\
&= 4 + 4s - 2\{s\}\sqrt{s} + 2(1-\{s\})\sqrt{s} + \{s\}^2 + (1-\{s\})^2 \\
&= 4 + 4s + \lambda\sqrt{s} + \mu \\
&= 4s + \lambda\sqrt{s} + (4+\mu),
\end{aligned}$$

where $\lambda \in (-2, 2)$ and $\mu \in (\frac{1}{2}, 1)$. Thus we got

$$|\mathrm{Tr}_{\mathrm{abs}}\,\alpha - 4s| < 2\sqrt{s} + 5. \tag{2.7.3}$$

We first use this inequality together with $\mathrm{Tr}_{\mathrm{abs}}\,\alpha \geq s(c_i^2 + 5d_i^2)$ to find S_1 such that for $s > S_1$ we have $|c_i| \leq 2$ and $|d_i| \leq \frac{1}{2}$. Suppose that one of these inequalities does not hold, i.e. either $|c_i| \geq \frac{5}{2}$ or $|d_i| \geq 1$. Then $\mathrm{Tr}_{\mathrm{abs}}\,\alpha \geq 5s$, giving $s < 2\sqrt{s} + 5$, which is a contradiction already for $s \geq 12$.

From now on consider only $s \geq 12$. From (2.7.2) we know that there exists $\delta_i \in (-\kappa, \kappa)$ such that

$$a_i^2 = (c_i\sqrt{s} + \delta_i)^2 = sc_i^2 + 2\delta_i c_i\sqrt{s} + \delta_i^2 = sc_i^2 + y_i,$$

where $|y_i| \leq (2\kappa C)\sqrt{s} + \kappa^2$. Similarly $5b_i^2 = 5sd_i^2 + z_i$ where $|z_i| \leq (2\kappa D\sqrt{5})\sqrt{s} + \kappa^2$. All in all,

$$\mathrm{Tr}_{\mathrm{abs}}\,x_i^2 = (sc_i^2 + y_i) + (5sd_i^2 + z_i) + sc_i^2 + 5sd_i^2 = 2(c_i^2 + 5d_i^2)s + w_i,$$

where $|w_i| = |y_i + z_i| < \kappa(4+\sqrt{5})\sqrt{s} + 2\kappa^2$.

Now, assuming that there are only four summands, and summing over all i, this yields

$$\sum_{i=1}^{4}\mathrm{Tr}_{\mathrm{abs}}\,x_i^2 = 2\Big(\sum_{i=1}^{4} c_i^2 + 5d_i^2\Big)s + \sum_{i=1}^{4} w_i,$$

hence, since the left-hand side is equal to $\mathrm{Tr}_{\mathrm{abs}}\,\alpha$, we conclude

$$\Big|\mathrm{Tr}_{\mathrm{abs}}\,\alpha - 2\Big(\sum_{i=1}^{4} c_i^2 + 5d_i^2\Big)s\Big| < 4\big(\kappa(4+\sqrt{5})\sqrt{s} + 2\kappa^2\big).$$

Finally we can draw conclusions about the value of $\Sigma := \sum_{i=1}^{4}(c_i^2 + 5d_i^2)$: Comparing the last inequality with (2.7.3), we obtain

$$|s(4 - 2\Sigma)| < \big(2 + 4\kappa(4+\sqrt{5})\big)\sqrt{s} + (5 + 8\kappa^2).$$

One easily sees that Σ can only take values from $\frac{\mathbb{Z}}{2}$, since the same is true for each of the four summands. Therefore $\Sigma \neq 2$ would mean $|s(4-2\Sigma)| \geq s$. Hence if $\Sigma \neq 2$, then the previous inequality implies

$$s < \big(2 + \kappa(16 + 4\sqrt{5})\big)\sqrt{s} + (5 + 8\kappa^2) \approx 56.29\sqrt{s} + 42.89.$$

This inequality holds only for $s \leq 3253$.

Thus for $s \geq 3254$, it is necessary that $\Sigma = \sum_{i=1}^{4}(c_i^2 + 5d_i^2) = 2$. Drawing the conclusion that without loss of generality $c_1 = c_2 = 1$ and the other coefficients c_i, d_i are zero is easy (and was done in the previous proof already). □

There are many ways how to improve the bound 3254 significantly. In our presentation, we preferred the simplicity of the proof over the optimality of the result. However, in order to spare computation time in proving Lemma 2.4.3 (15), it is better to use the following stronger bound, for which we only provide a sketch of the proof:

Observation 2.7.4. The condition $s \geq 3254$ in Proposition 2.7.3 can be relaxed to $s \geq 500$.

To see this, one must go over the corresponding proof slower and more carefully. First show independently by comparing traces that $\Sigma = \sum_{i=1}^{4}(c_i^2 + 5d_i^2) \leq 4$ unless $s \leq 32$. From this inequality deduce all possible values of $(c_1, d_1, \ldots, c_4, d_4)$. Use this to observe that $\sum(|c_i| + \sqrt{5}|d_i|) \leq 2 + \sqrt{5}$. This enables to avoid the rough estimates $|c_i| \leq 2$, $|d_i| \leq \frac{1}{2}$ and get a stronger inequality then the one listed in the proof:

$$\Big|\mathrm{Tr}_{\mathrm{abs}}\,\alpha - 2\Big(\sum_{i=1}^{4} c_i^2 + 5d_i^2\Big)s\Big| < 2\kappa(2+\sqrt{5})\sqrt{s} + 4\cdot 2\kappa^2,$$

leading directly to

$$|s(4-2\Sigma)| < (2 + 2\kappa(2+\sqrt{5}))\sqrt{s} + (5 + 8\kappa^2).$$

This implies $\Sigma = 2$ unless $s < 499.8$.

2.7.2 Upper bound

Before stating a general result (Proposition 2.7.5) which provides an upper bound for Pythagoras numbers, we must introduce a generalisation of the Pythagoras number, the so-called *g-invariants* of a ring. For $\mathbb{Z}$, they were introduced by Mordell, see [Mo], their study being called "quadratic Waring's problem". For recent results on them, see e.g. [CI, KrY].

Let R be a commutative ring. A homogeneous polynomial in n variables over R of degree two is called an n-ary *quadratic form*; if it is of degree one, we call it a *linear form*. A quadratic form Q *represents* $\alpha \in R$ if there exists a nonzero $\vec{x} = (x_1, \ldots, x_n) \in R^n$ such that $\alpha = Q(x_1, \ldots, x_n) = Q(\vec{x})$. If a form represents only totally positive elements, it is *totally positive definite*; a *totally positive semidefinite* form may also represent zero. The simplest totally positive definite n-ary quadratic form, sum of n squares, is traditionally denoted by I_n. Thus, the fact that a number $\alpha \in R$ is a sum of, say, five squares can be rephrased as "α is represented by I_5 over R". More generally, let Q be an n-ary quadratic form and A a k-ary quadratic form, $1 \leq k \leq n$. We say that A is *represented* by Q (or Q *represents* A) if there exist linear forms $\mathcal{L}_1, \ldots, \mathcal{L}_n : R^k \to R$ such that

$$Q(\mathcal{L}_1(\vec{x}), \ldots, \mathcal{L}_n(\vec{x})) = A(\vec{x}).$$

Clearly, Q represents $\alpha \in R$ if and only if it represents the unary form αx^2. Two quadratic forms are *equivalent* if one can be obtained from the other by an invertible substitution.

Let us now consider the set Sq_k of all k-ary quadratic forms which can be written as a sum of squares of linear forms, i.e. which are represented by I_n for some, possibly large, n. Then, similarly to the definition of the Pythagoras number, we put

$$g_R(k) = \min\{n : I_n \text{ represents all forms in } \mathrm{Sq}_k\}.$$

If no such n exists, we put $g_R(k) = \infty$; however, if R is an order in a number field, then $g_R(k)$ is finite for every k. (For maximal orders, see [Ic2]; the general statement is [KrY], Corollary 1.3.) In particular, $g_R(1) = \mathcal{P}(R)$.

Very few exact values of $g_R(k)$ are known. Mordell and Ko proved that $g_{\mathbb{Z}}(k) = k+3$ for $2 \leq k \leq 5$, see e.g. [Ko]; much later, Kim and Oh showed $g_{\mathbb{Z}}(6) = 10$ in [KO]. In Theorem 2.7.7, we prove $g_{\mathcal{O}_F}(2) = 5$ for $F = \mathbb{Q}(\sqrt{5})$; this was probably proven by Sasaki and published in [Sa2]. For discussion of values of $g_R(k)$ where R is a global field, local ring or a nonreal maximal order, see the introduction of [Ic2].

The g-invariants provide upper bounds on the Pythagoras number. Kala and Yatsyna showed in [KY2], Corollary 3.3, that $g_{\mathbb{Z}}(k)$ is an upper bound for $\mathcal{P}(\mathcal{O})$ where $\mathcal{O}$ is any order of degree k; this is the upper bound $\mathcal{P}(\mathcal{O}) \leq 7$ which holds for all biquadratic orders. We exploit their idea to prove the following generalisation:

Proposition 2.7.5. *Let $R \supset S$ be commutative rings such that R is a free module over S of rank k. Then*

$$\mathcal{P}(R) \leq g_S(k).$$

Proof. To simplify the notation, we assume $k = 2$ (which is the case we shall need); the general proof is entirely analogous. Let $\beta_1, \beta_2 \in R$ be an integral basis of R over S. Now take any $\alpha \in R$ and assume it is a sum of $N_\alpha \in \mathbb{N}$ squares; we show that it can be rewritten as a sum of $g = g_S(2)$ squares. We have

$$\alpha = \sum_{i=1}^{N_\alpha} (a_i\beta_1 + b_i\beta_2)^2.$$

Define a binary quadratic form Q_α over S by

$$Q_\alpha(X, Y) = \sum_{i=1}^{N_\alpha} (a_iX + b_iY)^2;$$

since it is a sum of squares of linear forms over S, it can be written as

$$Q_\alpha(X, Y) = \sum_{i=1}^{g} (c_iX + d_iY)^2.$$

This is an equality of two polynomials, so it is valid after replacing X, Y by elements of any commutative ring containing S. In particular, we can plug in the integral basis of R:

$$\alpha = \sum_{i=1}^{N_\alpha} (a_i\beta_1 + b_i\beta_2)^2 = \sum_{i=1}^{g} (c_i\beta_1 + d_i\beta_2)^2.$$

This is the desired representation of α as a sum of g squares. □

Remark. The condition that R is free as an S-module is not necessary; it suffices that it is generated by k elements. Since any torsion-free module of rank r over a Dedekind domain is generated by $r+1$ elements, one gets the weaker estimate $\mathcal{P}(\mathcal{O}) \leq g_{\mathcal{O}_F}(r+1)$ for any field extension L/F and any order $\mathcal{O}_F \subset \mathcal{O} \subset \mathcal{O}_L$. An interesting question is whether $r+1$ can be replaced by r (as in the case where $\mathcal{O}_F$ is a PID).[2]

For the rest of this section, denote $F = \mathbb{Q}(\sqrt{5})$. With the previous proposition, in order to obtain an upper bound $\mathcal{P}(\mathcal{O}) \leq 5$ for $\mathcal{O} \supset \mathcal{O}_F$, it remains to prove $g_{\mathcal{O}_F}(2) = 5$. This is Theorem 2.7.7. To prove it, we need a lemma from Sasaki's paper [Sa3]:

Lemma 2.7.6 ([Sa3], Lemma 12)**.** *Let $F = \mathbb{Q}(\sqrt{5})$ and let Q be a binary quadratic form over $\mathcal{O}_F$. Then Q is a sum of four squares of linear forms if and only if Q is*

[2] This question was one of the starting points for the recent preprint [KrY]. There, it is resolved as follows: If $\mathcal{O}_F$ is not a PID, it is more natural to use another version of the g-invariant (there denoted as $G_{\mathcal{O}_F}$) which is defined in terms of general quadratic lattices instead of just quadratic forms. In this setting, the inequality $\mathcal{P}(\mathcal{O}) \leq G_{\mathcal{O}_F}(r)$ indeed holds, and one also gets several other interesting inequalities for both versions of the invariant, vastly generalising our Proposition 2.7.5.

1. *totally positive semidefinite,*

2. *classical (i.e. the coefficient in front of XY is in $2\mathcal{O}_F$),*

3. *not equivalent to the form $G(X,Y) = 2X^2 + 2XY + 2\frac{1+\sqrt{5}}{2}Y^2$ over the completion $(\mathcal{O}_F)_{(2)}$, where (2) is the dyadic place.*

Its proof is based on the fact that the genus of I_4 in F contains only one class, so it suffices to determine which binary forms are represented locally. Let us note that the conditions of Q being positive semidefinite and classical are implicit in Sasaki's formulation, and instead of G, he uses the form $2X^2 + 2(\frac{1+\sqrt{5}}{2})XY + 2Y^2$ equivalent to G over $(\mathcal{O}_F)_{(2)}$.

Remark. Due to 93:11 of [O'M], the form G from the previous statement can be characterised as the unique (up to equivalence) unimodular binary form over $(\mathcal{O}_F)_{(2)}$ which is anisotropic and takes only values from $2(\mathcal{O}_F)_{(2)}$.

Since the following necessary result by Sasaki is, to our best knowledge, only available in Japanese in [Sa2], we provide both its full statement and proof.

Theorem 2.7.7 (Sasaki)**.** *Let $F = \mathbb{Q}(\sqrt{5})$. Then*

$$g_{\mathcal{O}_F}(2) = 5.$$

Proof. The easier inequality $g_{\mathcal{O}_F}(2) \geq 5$ can be proven either directly or using Lemma 2.7.6 by exhibiting any binary form which is a sum of squares and is equivalent to G over the dyadic place. One such form is $2X^2 + 2XY + (2\frac{1+\sqrt{5}}{2} + 16)Y^2 = (X+Y)^2 + X^2 + (2\frac{1+\sqrt{5}}{2} + 15)Y^2$; it is a sum of (five) squares since $2\frac{1+\sqrt{5}}{2} + 15$, as a totally positive element of $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$, is a sum of (three) squares, and its equivalence to G over the dyadic place follows e.g. from the previous remark.

Now we shall take any binary quadratic form $Q(X,Y) = \sum_i \mathcal{L}_i^2(X,Y) = \sum_i (a_iX + b_iY)^2$ where $a_i, b_i \in \mathcal{O}_F$ and prove that it can be rewritten as a sum of five squares. Clearly, any form which is a sum of squares is totally positive semidefinite and classical; therefore, if Q is not equivalent to G over $(\mathcal{O}_F)_{(2)}$, even four squares suffice by Lemma 2.7.6. Thus we may assume that Q is equivalent to G over $(\mathcal{O}_F)_{(2)}$. This means that Q represents only elements of $2\mathcal{O}_F$.

If one of $\mathcal{L}_i^2$ represents an element outside $2\mathcal{O}_F$, then so does $Q - \mathcal{L}_i^2$; therefore $Q - \mathcal{L}_i^2$ satisfies the conditions of Lemma 2.7.6 and can be represented by four squares, showing that Q is a sum of five squares. It remains to show that it is absurd for all $\mathcal{L}_i^2$ to represent only elements of $2\mathcal{O}_F$: By plugging in $(X,Y) = (1,0)$ and $(0,1)$, one sees that both a_i and b_i lie in $2\mathcal{O}_F$; thus $\mathcal{L}_i^2$ takes only values from $4\mathcal{O}_F$. This contradicts the fact that $\sum \mathcal{L}_i^2$ represents 2 over $(\mathcal{O}_F)_{(2)}$. □

Finally we can put the pieces together:

Theorem 2.7.8. *Let K be a quadratic extension of $\mathbb{Q}(\sqrt{5})$ and $\mathcal{O}$ any order in K containing $\frac{1+\sqrt{5}}{2}$. Then $\mathcal{P}(\mathcal{O}) \leq 5$.*

Proof. By combining Proposition 2.7.5 and Theorem 2.7.7, one sees that $\mathcal{P}(R) \leq 5$ holds for any commutative ring R which is a free module over $\mathcal{O}_{\mathbb{Q}(\sqrt{5})} = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ of rank 2.

Since the class number of $\mathbb{Q}(\sqrt{5})$ is 1, any finitely generated torsion-free module over $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ is free. In particular, any ring which is a free $\mathbb{Z}$-module of rank r and contains $\frac{1+\sqrt{5}}{2}$ is a free $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$-module of rank $\frac{r}{2}$. This concludes the proof. □

We reiterate that for biquadratic fields, the result is not only applicable to maximal orders; it also holds for any order of the form $\mathbb{Z}[\frac{1+\sqrt{5}}{2}, \alpha]$ where $\alpha \notin \mathbb{Q}(\sqrt{5})$ is an algebraic integer of degree 2:

Corollary 2.7.9. *For any biquadratic number field K containing $\sqrt{5}$, there are infinitely many orders $\mathcal{O} \subset K$ satisfying $\mathcal{P}(\mathcal{O}) \leq 5$.*

Moreover, Theorem 2.7.8 does not only apply to biquadratic fields. For fields which are not totally real, it gives nothing new (recall that any order which is not totally real has $\mathcal{P}(\mathcal{O}) \leq 5$ by [Pf]); but it can be applied to other totally real quartic orders. Notably, it includes the maximal order $\mathbb{Z}\left[\sqrt{\frac{5+\sqrt{5}}{2}}\right]$, which, along with $\mathbb{Z}[\sqrt{2}, \frac{1+\sqrt{5}}{2}]$, is the only totally real quartic order where the local-global principle for sums of squares is satisfied (by Scharlau's dissertation [Sch]).

2.8 Six is almost always a lower bound

In this section, we follow up the previous results by showing that $\mathcal{P}(\mathcal{O}_K) = 5$ is still not the typical behaviour. We prove the second part of Theorem 2.1.2, namely:

Theorem 2.8.1. *Let $F = \mathbb{Q}(\sqrt{m})$ be a real quadratic field with $\mathcal{P}(\mathcal{O}_F) = 5$, i.e. $m \neq 2, 3, 5, 6, 7$. Then there are only finitely many totally real biquadratic fields $K \supset F$ with $\mathcal{P}(\mathcal{O}_K) \leq 5$.*

Proof. For $m \neq 13$, it is a direct consequence of Proposition 2.8.2 which also contains the appropriate definition of the element α with length 6. The case $m = 13$ is handled separately (but using the same idea) in Proposition 2.8.3. □

The proof is concluded in Subsection 2.8.2, while Subsection 2.8.1 explains the underlying main idea which may be exploited in many other situations besides biquadratic fields with a given quadratic subfield.

The case $m = 13$ is handled separately since $\mathbb{Q}(\sqrt{13})$ has very few elements of length 5 (see Theorem 2.3.1); also, the obtained Proposition 2.8.3 is used in Section 2.6. However, it should be noted that the main idea of the proof remains the same as in the other cases.

Now we provide an important part of the proof – for each biquadratic field with $m \neq 2, 3, 5, 6, 7, 13$, we define the appropriate α which usually has length 6. We always have $\alpha = \alpha_0 + w^2$ with α_0 as in Section 2.6; however, to find the appropriate definition of w, we must distinguish 12 families of fields. The simple method by which this terrifyingly looking case distinction was constructed is explained in the next two subsections.

The list of all the mutually disjoint families, and for each of them the appropriate choice of α_0 and w, follows. To be concise, we write only e.g. "Type (B1)" to mean "The field K is of type (B1)". The letter q has the same meaning as in Subsection 2.2.1, i.e. in (B1) it just means $q \equiv 3 \pmod 4$ and in (B2,3) it means $q \equiv 1 \pmod 4$.

1. If $m \not\equiv 1 \pmod 4$, we put $\alpha_0 = 7 + (1 + \sqrt{m})^2$ and:
   - (a) Type (B1):
     - i. $q = m$, i.e. $m \equiv 3 \pmod 4$
       - A. $s_0 > 3t_0$: Put $w = 1 + \sqrt{s}$.
       - B. $s_0 < 3t_0$: Put $w = 1 + \frac{\sqrt{s}+\sqrt{t}}{2}$.
     - ii. $q = s$, i.e. $s \equiv 3 \pmod 4$
       - A. $s_0 > 4t_0$: Put $w = 1 + \sqrt{s}$.
       - B. $s_0 < 4t_0$: Put $w = \frac{\sqrt{m}+\sqrt{t}}{2}$.
     - iii. $q = t$, i.e. $t \equiv 3 \pmod 4$: Put $w = \frac{\sqrt{m}+\sqrt{s}}{2}$.
   - (b) Type (B2,3):
     - i. $q = s$, i.e. $s \equiv 1 \pmod 4$: Put $w = \frac{1+\sqrt{s}}{2}$.
     - ii. $q = t$, i.e. $t \equiv 1 \pmod 4$: Put $w = \frac{\sqrt{m}+\sqrt{s}}{2}$.

2. If $m \equiv 1 \pmod 4$, we put $\alpha_0 = 7 + (\frac{1+\sqrt{m}}{2})^2$ and:
   (a) Type (B2,3):
      i. $s_0 > 3t_0$: Put $w = 1 + \sqrt{s}$.
      ii. $s_0 < 3t_0$: Put $w = 1 + \frac{\sqrt{s}+\sqrt{t}}{2}$.
   (b) Type (B4):
      i. $s_0 > 3t_0$: Put $w = \frac{1+\sqrt{s}}{2}$.
      ii. $s_0 < 3t_0$:
         A. Type (B4a): Put $w = \frac{1+\sqrt{m}+\sqrt{s}+\sqrt{t}}{4}$.
         B. Type (B4b): Put $w = \frac{1+\sqrt{m}+\sqrt{s}-\sqrt{t}}{4}$.

Let us note that these families indeed cover all possibilities, since $s_0 = 4t_0$ cannot happen for s_0 square-free and $s_0 = 3t_0$ is possible only for $s_0 = 3$, $t_0 = 1$, leading to $m = 3$ which violates the assumption $\mathcal{P}(\mathcal{O}_{\mathbb{Q}(\sqrt{m})}) = 5$.

We conclude this part by formulating what remains to be proven.

Proposition 2.8.2. *Let $F = \mathbb{Q}(\sqrt{m})$ be a given field as in Theorem 2.8.1, with $m \neq 13$, and for each totally real biquadratic field $K \supset F$ define $\alpha = \alpha_0 + w^2$ as above. Then, with finitely many exceptions, $\ell(\alpha) = 6$ in $\mathcal{O}_K$.*

Proof. For a given m, there are only finitely many biquadratic fields K where m is not the smallest of the three square-free integers whose square roots lie in K; disregarding them, we may assume that the usual Convention 2.2.1 holds. Clearly, every m corresponds to only finitely many choices of (t_0, s_0).

After realising this, it suffices to prove twelve separate lemmata, where for example the first of them, with code name (1(a)iA), claims: "Let $s_0 > t_0 \geq 1$ be two coprime square-free numbers such that $s_0 t_0 \equiv 3 \pmod 4$ and $s_0 > 3t_0$. Put $\alpha_0 = 7 + (1 + \sqrt{s_0 t_0})^2$. If we take any large enough square-free m_0 coprime with $s_0 t_0$, and then denote $K = \mathbb{Q}(\sqrt{s_0 t_0}, \sqrt{m_0 t_0})$ and put $w = 1 + \sqrt{m_0 t_0}$, then $\ell(\alpha_0 + w^2) = 6$ in $\mathcal{O}_K$."

Another of these twelve statements, Lemma 2.8.4, is formulated and proven in Subsection 2.8.2. The others are omitted, since all the twelve proofs are very similar, and after understanding one of them, it is not difficult to write any of the others. □

2.8.1 The idea

Here we suggest a general strategy which applies in many situations when one examines $\mathcal{P}(\mathcal{O}_K)$ where K runs over extensions of a given field F with an already known Pythagoras number $\mathcal{P}(\mathcal{O}_F)$. This strategy was applied to obtain the appropriate definition of α for the situation of Theorem 2.8.1, but it can be tried for any field, not just the biquadratic ones. The aim is to find conditions under which $\mathcal{P}(\mathcal{O}_K) \geq \mathcal{P}(\mathcal{O}_F) + 1$ can be proven: For example, $\mathcal{P}(\mathbb{Z}) = 4$, and indeed, $\mathcal{P}(\mathcal{O}_{\mathbb{Q}(\sqrt{n})}) = 5$ holds for almost all positive n. Or, as we have already seen in Subsection 2.6.4: For $F = \mathbb{Q}(\sqrt{6})$ or $\mathbb{Q}(\sqrt{7})$, where $\mathcal{P}(\mathcal{O}_F) = 4$, almost all biquadratic fields $K \supset F$ have $\mathcal{P}(\mathcal{O}_K) \geq 5$.

The way of constructing the "witness" $\alpha \in \mathcal{O}_K$ which probably has length $P(\mathcal{O}_F) + 1$, follows: First, one takes $\alpha_0 \in \mathcal{O}_F$ of length $\mathcal{P}(\mathcal{O}_F)$ in $\mathcal{O}_F$. (It is convenient to use one with the minimal trace, but any α_0 can work.) It is reasonable to hope that in most extensions $K \supset F$, α_0 will also require $\mathcal{P}(\mathcal{O}_F)$ squares. For example, the only real quadratic fields where 7 can be written as a sum of less than four integral squares are those generated by $\sqrt{2}$, $\sqrt{3}$, $\sqrt{5}$, $\sqrt{6}$, $\sqrt{7}$ and $\sqrt{13}$; and a similar statement for our situation where F is quadratic and K biquadratic was proven in Subsections 2.6.1 and 2.6.2. However, we need to find an element with length $\mathcal{P}(\mathcal{O}_F) + 1$. This is often achieved by choosing $w^2 \in \mathcal{O}_K \setminus \mathcal{O}_F$ where the trace of w^2 is the

minimal possible among such elements. Then one defines $\alpha = \alpha_0 + w^2$ and hopes to prove that any representation of α as a sum of squares uses w^2 as one of the summands. This has a good chance of success if $\operatorname{Tr}\alpha_0$ is much smaller than $\operatorname{Tr} w^2$: In such a case, w^2 will be one of the very few squares totally smaller or equal to α and not belonging to $\mathcal{O}_F$.

This strategy was very successful in Peters' examination of quadratic fields as extensions of $\mathbb{Z}$: The choice $\alpha_0 = 7$ and $w = (1 + \sqrt{m})$ or $w = (\frac{1+\sqrt{m}}{2})$, see Theorem 2.3.1, led to an element of length 5 in all but six maximal orders, and the analogy for non-maximal orders succeeded every time except of $\mathbb{Z}[\sqrt{5}]$, see also Observation 2.3.2.

Let us note, however, that there is no guarantee that this strategy will indeed work – as we have seen in Subsection 2.6.3, there are infinitely many biquadratic fields where even the weaker statement $\ell(\alpha_0) = 5$ fails. This is also why the proof in the next subsection had to be carefully divided into twelve different branches depending on the integral basis and on m, and why it was necessary to perform the proof separately for each of these twelve families. The most troublesome situation occurs if the choice of w^2 is not unique: In such a case it might be difficult to show that the rejected candidates for w^2 cannot be used in the decomposition of α instead of w^2. But the strategy turned out to be successful in all twelve families.

We conclude this subsection by illustrating how it applies in the exceptional case $m = 13$.

Proposition 2.8.3. *Let $K = \mathbb{Q}(\sqrt{13}, \sqrt{s})$. Then $\mathcal{P}(\mathcal{O}_K) \geq 6$.*

In particular, $\ell(\alpha) = 6$ holds for $\alpha = \alpha_0 + w^2$, where $\alpha_0 = 3 + (\frac{1+\sqrt{13}}{2})^2 + (1 + \frac{1+\sqrt{13}}{2})^2 = 12 + 2\sqrt{13}$ and

$$w = \begin{cases} \frac{1+\sqrt{s}}{2} & \text{if } s \equiv 1 \pmod 4, \\ 1 + \sqrt{s} & \text{if } s \equiv 2, 3 \pmod 4. \end{cases}$$

Proof. The proof is an incarnation of the above explained strategy: Since $\ell(\alpha_0) = 5$ in $\mathcal{O}_{\mathbb{Q}(\sqrt{13})}$, see Theorem 2.3.1, it suffices to show by trace considerations that w^2 must be one of the summands and all the others must belong to $\mathbb{Q}(\sqrt{13})$. See also the analogous proofs in Subsection 2.6.4.

More specifically: If $s \not\equiv 1$ and we assume a decomposition of α which is not of the form $w^2 + \cdots$ where the remaining summands are squares in $\mathbb{Q}(\sqrt{13})$, we arrive at $s \leq 13$, an immediate contradiction. For $s \equiv 1$, the obtained inequality is $s \leq 49$, which left only six fields; these were solved in Lemma 2.4.3 (16). □

Note that the statement of the proposition actually holds even for fields $\mathbb{Q}(\sqrt{13}, \sqrt{n})$ for $n = 6, 7, 10, 11$, see Lemma 2.4.3 (17); the element $\alpha_0 + (1 + \sqrt{n})^2$ has length 6. This is interesting, especially for fields containing $\sqrt{6}$ and $\sqrt{7}$, for which we in general know only $\mathcal{P}(\mathcal{O}_K) \geq 5$; it is further evidence that fields with Pythagoras number less than 6 are very rare, see Conjecture 2.1.6.

2.8.2 The proof

In this subsection we provide the proof of Theorem 2.8.1. The general idea was explained at length in the previous subsection: One starts with $\alpha_0 \in \mathbb{Q}(\sqrt{m})$ which has the minimal trace among elements of length 5, namely $\alpha_0 = 7 + (\frac{1+\sqrt{m}}{2})^2$ if $m \equiv 1 \pmod 4$ and $7 + (1 + \sqrt{m})^2$ otherwise. Then one takes $w^2 \in \mathcal{O}_K \setminus \mathbb{Q}(\sqrt{m})$ which has minimal trace, to define $\alpha = \alpha_0 + w^2$, as the table above Proposition 2.8.2 shows. This w depends not only on the integral basis and on whether $m = q$ or $m \neq q$, but sometimes also on (in)validity of inequalities like $3s > t$.

To solve this last problem, one had to consider all the finitely many decompositions $m = s_0 t_0$ for the given m. Clearly, if we prove that for each fixed choice of t_0 and s_0 there are only finitely many m_0 such that the biquadratic field K given by $m = t_0 s_0, s = t_0 m_0, t = s_0 m_0$ has $\mathcal{P}(\mathcal{O}_K) \leq 5$, then we are done.

Since the proofs are really the same in all twelve families, we provide proof only in one of them. We have chosen the most difficult branch where some small additional tricks were needed.

Lemma 2.8.4 (Branch (2(b)iiA)). *If the field $K = \mathbb{Q}(\sqrt{m}, \sqrt{s})$ is of type (B4a), $m \neq 5, 13$ and $s_0 < 3t_0$ holds, and m_0 is large enough, then the following element has length 6:*

$$\begin{aligned}\alpha = \alpha_0 + w^2 &= 7 + \frac{1+m}{4} + \frac{\sqrt{m}}{2} + \Big(\frac{1+\sqrt{m}+\sqrt{s}+\sqrt{t}}{4}\Big)^2 \\ &= \Big(7 + \frac{5+5m+s+t}{16}\Big) + \frac{5+m_0}{8}\sqrt{m} + \frac{1+s_0}{8}\sqrt{s} + \frac{1+t_0}{8}\sqrt{t}.\end{aligned}$$

Remark. In this family, the condition is $m_0 > \frac{117+5m}{3t_0-s_0}$, as one sees from the proof.

Proof. Suppose $\alpha = \sum x_i^2$. Since α_0 cannot be written as a sum of less than five squares in $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$, it suffices to prove that one of the x_i^2 must be equal to w^2 and all other $x_i \in \mathbb{Q}(\sqrt{m})$.

Write $x_i = \frac{a_i+b_i\sqrt{m}+c_i\sqrt{s}+d_i\sqrt{t}}{4}$; since K is of type (B4a), we see that a_i, b_i, c_i, d_i are either all even or all odd, and $a_i + b_i + c_i + d_i \equiv 0 \pmod 4$. Since $\alpha \notin \mathbb{Q}(\sqrt{m})$, at least one of the summands is not in $\mathbb{Q}(\sqrt{m})$, hence at least one of all the coefficients c_i, d_i is nonzero. Due to the parity condition, either $\max\{\sum c_i^2, \sum d_i^2\} \geq 4$, or $\sum c_i^2 \geq 1$ and $\sum d_i^2 \geq 1$.

Comparing traces of α and $\sum x_i^2$, one gets

$$7 + \frac{5+5m+s+t}{16} = \frac{1}{16}\Big(\sum a_i^2 + m\sum b_i^2 + s\sum c_i^2 + t\sum d_i^2\Big) \geq \frac{1}{16}\Big(s\sum c_i^2 + t\sum d_i^2\Big),$$

which can be rewritten as

$$\frac{117+5m}{16} + m_0\frac{t_0+s_0}{16} \geq m_0\frac{1}{16}(t_0\sum c_i^2 + s_0\sum d_i^2).$$

If $(t_0\sum c_i^2 + s_0\sum d_i^2) > t_0 + s_0$, then by choosing m_0 large enough we obtain a contradiction. Therefore the expression must be at most $t_0 + s_0$. Hence $\sum c_i^2 \geq 4$ or $\sum d_i^2 \geq 4$ is impossible because of our assumption on s_0 and t_0, since then $(t_0\sum c_i^2 + s_0\sum d_i^2) \geq 4t_0 > t_0 + s_0$. Thus necessarily $\sum c_i^2 = \sum d_i^2 = 1$. Therefore we may assume $|c_1| = |d_1| = 1$ and $c_i, d_i = 0$ otherwise.

We have just proven $x_i \in \mathbb{Q}(\sqrt{m})$ for $i \neq 1$. Since $(-x_1)^2 = x_1^2$, we may assume $c_1 = 1$; hence there are two possibilities: Either $x_1 = \frac{a_1+b_1\sqrt{m}+\sqrt{s}+\sqrt{t}}{4}$, or $x_1 = \frac{a_1+b_1\sqrt{m}+\sqrt{s}-\sqrt{t}}{4}$. In both cases, we will use the fact that $\alpha - x_1^2 \in \mathbb{Q}(\sqrt{m})$ to determine the values of a_1 and b_1.

In the first case,

$$x_1^2 = \Big(\frac{a_1 + b_1\sqrt{m} + \sqrt{s} + \sqrt{t}}{4}\Big)^2 \in \mathbb{Q}(\sqrt{m}) + \frac{a_1 + b_1 s_0}{8}\sqrt{s} + \frac{a_1 + b_1 t_0}{8}\sqrt{t};$$

by comparing the coefficients in front of $\sqrt{s}$ and $\sqrt{t}$ with those of α, we obtain two equations $a_1 + b_1 s_0 = 1 + s_0$ and $a_1 + b_1 t_0 = 1 + t_0$. Since $t_0 \neq s_0$, there is a unique solution: $a_1 = b_1 = 1$. Therefore we indeed arrived at $x_1 = \frac{1+\sqrt{m}+\sqrt{s}+\sqrt{t}}{4}$, which is what we needed.

It remains to be shown that the other case is impossible. Again we write

$$x_1^2 = \Big(\frac{a_1 + b_1\sqrt{m} + \sqrt{s} - \sqrt{t}}{4}\Big)^2 \in \mathbb{Q}(\sqrt{m}) + \frac{a_1 - b_1 s_0}{8}\sqrt{s} + \frac{-a_1 + b_1 t_0}{8}\sqrt{t};$$

this time we obtain the equations $a_1 - b_1 s_0 = 1 + s_0$ and $-a_1 + b_1 t_0 = 1 + t_0$. Again, the solution is unique: $a_1 = \frac{t_0+s_0+2s_0t_0}{t_0-s_0}$, $b_1 = \frac{t_0+s_0+2}{t_0-s_0}$. However, in order that $x_1 \in \mathcal{O}_K$, it is necessary that a_1 and b_1 are odd integers. But it is easy to check that if $s_0 \equiv t_0 \equiv 1 \pmod 4$, which are the conditions of (B4a), then $b_1 = \frac{t_0+s_0+2}{t_0-s_0} = 1 + 2\frac{s_0+1}{t_0-s_0}$ is either even, or not an integer. This concludes the proof. □

2.8.3 A conjecture

We suspect that it is in fact possible to prove a stronger result, listed already in the Introduction as the first part of Conjecture 2.1.6. However, we did not try proving it in order not to make this paper longer than it already is. Moreover, the potential proof would not only have many branches, but probably some of them would require new ideas. As the last part of this paper, let us repeat the Conjecture 2.1.6 and list some evidence towards it:

Conjecture. Let K be a totally real biquadratic field.

1. If K contains none of $\sqrt{2}$ and $\sqrt{5}$, then $\mathcal{P}(\mathcal{O}_K) \geq 6$ holds with finitely many exceptions.
2. If K contains $\sqrt{2}$ or $\sqrt{5}$, then $\mathcal{P}(\mathcal{O}_K) \leq 5$.
3. The inequality $\mathcal{P}(\mathcal{O}_K) < 5$ holds precisely for the following seven fields:
   For $K = \mathbb{Q}(\sqrt{2},\sqrt{3}), \mathbb{Q}(\sqrt{2},\sqrt{5}), \mathbb{Q}(\sqrt{3},\sqrt{5})$, where $\mathcal{P}(\mathcal{O}_K) = 3$, and
   for $K = \mathbb{Q}(\sqrt{2},\sqrt{7}), \mathbb{Q}(\sqrt{3},\sqrt{7}), \mathbb{Q}(\sqrt{5},\sqrt{6}), \mathbb{Q}(\sqrt{5},\sqrt{7})$, where $\mathcal{P}(\mathcal{O}_K) = 4$.

Part (2) was already proven for $\sqrt{5}$; for $\sqrt{2}$, it is an observation based on computer calculations: Our program never found an element with length 6 or 7. Of course we do not have a proof for even one concrete field, let alone for all extensions of $F = \mathbb{Q}(\sqrt{2})$. We suggest that in analogy with Theorem 2.7.7, one should try to prove $g_{\mathcal{O}_{\mathbb{Q}(\sqrt{2})}}(2) = 5$. This seems feasible, since the crucial point in the proof of Lemma 2.7.6, namely that the genus of I_4 contains only one class, remains valid for $\mathbb{Q}(\sqrt{2})$.[3]

Let us turn to (3). The fact that these seven are the only possible exceptional fields is proven as Theorem 2.1.2 (1), and an element of the suspected maximal length in each of them was already given in Proposition 2.4.4. Thus, it only remains to prove a stronger upper bound for these seven fields. Proposition 2.4.4 also contains some numerical evidence – namely, the conjecture is valid for elements with trace up to 500.

A further point in favour of this part of the conjecture is that it holds locally – by the result [Sch], Kapitel 0, Lemma 1, already mentioned in the Introduction, four integral squares are sufficient in all completions $K_\mathfrak{p}$, and three squares suffice unless $\mathfrak{p}$ is dyadic and $[K_\mathfrak{p} : \mathbb{Q}_2]$ is odd. Since biquadratic fields are Galois extensions of $\mathbb{Q}$ of even degree, one can show that such a problematic dyadic place can exist only for fields of type (B4), where 2 does not ramify. None of the seven listed fields are of this type.

Regarding part (1), again it is based on computer experiments. There would be two separate tasks in proving it. First, one has to handle the cases not included in Theorem 2.8.1, namely fields containing $\sqrt{3}$, $\sqrt{6}$ or $\sqrt{7}$. Here we observed from our data that even for quite small values of s, the corresponding $\mathcal{O}_K$ usually contained an element of length 6. (For instance, for $K \ni \sqrt{3}$, Proposition 2.4.5 suggests that $\mathcal{P}(\mathcal{O}_K) \geq 6$ holds for all $s \geq 26$ as well as for $s = 17$ and $s = 22$, leaving only nine exceptions.) To prove this, one would either have to find in the computed data a family of such elements (as in Subsection 2.6.5 for length 5 and $K \ni \sqrt{2}, \sqrt{3}$ or $\sqrt{5}$); or alternatively, if no such family could be found, one could prove an analogy of Proposition 2.7.2 and construct a family of counterexamples in this way.

And the second task would be to prove a stronger version of Theorem 2.8.1: If m is chosen large enough, then there are no exceptional fields. It would be ideal to show that the corresponding $\alpha = \alpha_0 + w^2$ *always* requires six squares. However, this is not true; at least some infinite families of exceptional fields *can* be found: $s = m + 4$, $s = m + 8$ and $s = m + 12$. Possibly they can be handled similarly as in Subsection 2.6.3. However, it is clear that solving all cases would be a tedious task requiring both patience and clever ideas.

[3] This strategy of the proof was successfully carried out by He and Hu in [HH] before the present paper was published. Thus, part (2) of the Conjecture in now in fact a theorem.

A further indication that the inequality $\mathcal{P}(\mathcal{O}_K) \geq 6$ indeed holds for all but finitely many fields (excluding $m = 2$ or 5) is that it is almost true in the case of m, s coprime (see Proposition 2.5.1). As a final piece of evidence we list a result which was shown to us by M. Tinková (including a proof) and will be part of an upcoming paper of hers. Since it contains no phrase "up to finitely many exceptions", it is a stronger version of Theorem 2.8.1 for two of the twelve families, namely those coded by (1(a)iA) and (1(a)iiA), as well as an alternative for a third family, (1(a)iiB).

Theorem 2.8.5 (Tinková)**.** *Let $K = \mathbb{Q}(\sqrt{p}, \sqrt{q})$ where p, q are square-free positive integers such that $p \equiv 2$ and $q \equiv 3 \pmod 4$. Moreover, let $q_0 > r_0 \geq 3$ and $p_0 > 3r_0$. Then $\mathcal{P}(\mathcal{O}_K) \geq 6$.*

In particular, $\alpha = 7 + (1 + \sqrt{p})^2 + (1 + \sqrt{q})^2$ has length 6.

3. A cubic ring of integers with the smallest Pythagoras number

This chapter contains the paper [Kr] J. Krásenský, *A cubic ring of integers with the smallest Pythagoras number*, Arch. Math. (Basel) 118, 39–48 (2022).

3.1 Introduction

In this note, we shall study sums of integral squares in the cubic field $K^{(49)} = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$, which can be characterised e.g. as the unique number field of discriminant 49 or as the maximal totally real subfield of the seventh cyclotomic field. In the main Theorem 3.2.2, we show that any sum of integral squares can in fact be written as a sum of four such squares – in the terminology introduced below, the Pythagoras number of $\mathcal{O}_{K^{(49)}}$ is 4. In Theorem 3.1.1 we recall the generally known fact that this is the smallest possible value among totally real fields of odd degree. Moreover, with the information gained during the proof of the main theorem, it is fairly simple to fully characterise the numbers which are sums of integral squares in $K^{(49)}$ (Theorem 3.2.3) and to use this to construct a diagonal universal quadratic form in five variables (Corollary 3.2.4).

Let us start by summarising the known results. For standard definitions and notation, in particular regarding number fields, local fields and quadratic forms, we refer the reader to [Mi] and [O'M].

When R is a commutative ring, $\sum R^2$ denotes the set of all elements of R which can be written as a sum of squares, and for $\alpha \in \sum R^2$, its *length* $\ell(\alpha)$ is the smallest integer n such that α can be written as a sum of n squares. The *Pythagoras number* of R is then defined as the largest length occurring in $\sum R^2$, i.e.

$$\mathcal{P}(R) = \sup\{\ell(\alpha) : \alpha \in \textstyle\sum R^2\}.$$

In this notation, Lagrange's four square theorem can be written as $\mathcal{P}(\mathbb{Z}) = 4$. The Pythagoras number is primarily studied for fields [Ho, TVY, BV, BL, BGV, Hu], as this is arguably the easier case, but there are several results about the Pythagoras number of rings of integers $\mathcal{O}_K$ of a number field K as well. In fact, if K is not totally real, then $\mathcal{P}(\mathcal{O}_K) \leq 4$ [Pf]. For totally real fields, the situation is dramatically different: By Scharlau [Sch2], there are number fields K with arbitrarily large $\mathcal{P}(\mathcal{O}_K)$. On the other hand, $\mathcal{P}(\mathcal{O}_K)$ is bounded by a constant depending only on the degree $d = [K : \mathbb{Q}]$, as shown by Kala and Yatsyna [KY2]. This constant is the so-called g-invariant $g_{\mathbb{Z}}(d)$, see e.g. [KO2]; thus for $1 \leq d \leq 5$, this bound is $d+3$, and for $d = 6$, its value is 10.

For a given number field K, it is fairly simple to obtain lower bounds for $\mathcal{P}(\mathcal{O}_K)$, since finding the length of any given α is only a computational task; the main content of several recent papers [Ti, KRS, Kr2] is finding good lower bounds for infinite families of fields. Obtaining tight upper bounds is much more difficult. The result of Kala and Yatsyna was generalised in [KRS] to include g-invariants of any subfield of K, which in particular yielded $\mathcal{P}(\mathcal{O}_K) \leq 5$ for quadratic extensions of $\mathbb{Q}(\sqrt{5})$; however, very few values of g-invariants of totally real orders are known, so this generalisation is of limited use.

Since cubic fields have no subfields besides $\mathbb{Q}$, the only easily available upper bound for their Pythagoras number is $\mathcal{P}(\mathcal{O}_K) \leq g_{\mathbb{Z}}(3) = 6$. Recently, Tinková [Ti] showed that this upper bound is attained in infinitely many totally real cubic fields K. More precisely, she studied the family of so-called *simplest cubic fields* $\mathbb{Q}(\rho_a)$, introduced by Shanks [Sh], where ρ_a is a root of the polynomial $x^3 - ax^2 - (a+3)x - 1$, $a \geq -1$, and proved that $\mathcal{P}(\mathbb{Z}[\rho_a]) = 6$ for $a \geq 3$. (This order is the full ring of integers for a positive proportion of a.)

For $a = 0, 1, 2$, Tinková exhibits elements of length 5, and for $a = -1$ she only gives $\ell(7) = 4$, noting that using a computer program, she checked that no element with a reasonably small trace has bigger length. Therefore, it is natural to conjecture that $\mathcal{P}(\mathbb{Z}[\rho_{-1}]) = 4$. Our Theorem 3.2.2 confirms this hypothesis, since $\mathbb{Q}(\rho_{-1}) = K^{(49)}$. Among totally real cubic fields, our result provides the first one where $\mathcal{P}(\mathcal{O}_K) \leq 4$, and by Tinková's result we know that it is the only simplest cubic field where the order $\mathbb{Z}[\rho_a]$ has Pythagoras number less than 5.

In total, very few totally real fields K with $\mathcal{P}(\mathcal{O}_K) \leq 4$ are known: For $K = \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{5})$ one has $\mathcal{P}(\mathcal{O}_K) = 3$, while for $K = \mathbb{Q}, \mathbb{Q}(\sqrt{6})$ and $\mathbb{Q}(\sqrt{7})$ it is known that $\mathcal{P}(\mathcal{O}_K) = 4$. For all other real quadratic fields, the maximal possible value $5 = g_{\mathbb{Z}}(2)$ is attained. The paper [KRS] proves that there are at most seven real biquadratic fields with $\mathcal{P}(\mathcal{O}_K) \leq 4$, conjecturing that these seven fields indeed satisfy the inequality. This weak evidence may lead one to conjecture that in fact, there are only finitely many totally real K with $\mathcal{P}(\mathcal{O}_K) \leq 4$.

We conclude this section by combining two well-known facts in order to show $\mathcal{P}(\mathcal{O}_K) \geq 4$ for every totally real number field of odd degree. The result is stated for general orders:

Theorem 3.1.1. *Let K be a totally real number field with $[K : \mathbb{Q}]$ odd. Then $\mathcal{P}(K) = 4$. If $\mathcal{O}$ is an order in K, then $\mathcal{P}(\mathcal{O}) \geq 4$.*

Proof. The fact that $\mathcal{P}(K) = 4$ can be found in [La, Ex. XI.5.9(2)]. It is an application of the local-global principle, and the core of the argument is as follows: Since there is an odd number of real embeddings, by Hilbert's reciprocity law there exists at least one finite place where the form $x^2 + y^2 + z^2$ is anisotropic.

It is also well known that if R is any integral domain and F its field of fractions, then $\mathcal{P}(R) \geq \mathcal{P}(F)$. Indeed, if $\frac{\alpha}{\beta}$ is not a sum of n squares in F, then the same holds for $\alpha\beta$ in F and thus also in R. Now the proof is concluded since the field of fractions of $\mathcal{O}$ is K. □

3.2 Preliminaries and results

We have already defined the Pythagoras number, the set $\sum R^2$ and the length $\ell(\,\cdot\,)$. By I_n we mean the quadratic form $x_1^2 + \cdots + x_n^2$. For brevity, we sometimes denote squares simply by $\square$. The symbol $h(\varphi)$ stands for the class number of the quadratic form φ. For its definition, as well as for other standard terminology and notation, we refer the reader to O'Meara's book [O'M]. The starting point of this paper is the following result, proven by analytical methods in [Pe4]:

Theorem 3.2.1 (Peters, 1977)**.** *There are only six totally real number fields where $h(I_3) = 1$; $K^{(49)}$ is one of them. (The other fields in question are $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{17})$ and the cubic field $K^{(148)}$ with discriminant 148.)*

From now on, we will leave general number fields and focus only on the field with discriminant 49. Let $\zeta_7 = \exp(\frac{2\pi \mathrm{i}}{7})$ be the primitive seventh root of unity and let $K^{(49)}$ stand for the totally real cubic field $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$. Usually we denote its ring of integers $\mathbb{Z}[\zeta_7 + \zeta_7^{-1}]$ simply by $\mathcal{O}$. Later, we will also use the element $\rho = \zeta_7 + \zeta_7^{-1}$ which generates $\mathcal{O}$; its minimal polynomial is $x^3 + x^2 - 2x - 1$. Our main theorem is the following:

Theorem 3.2.2. $\mathcal{P}\big(\mathbb{Z}[\zeta_7 + \zeta_7^{-1}]\big) = 4$.

There are many remarkable properties of $K^{(49)}$; for example, it has class number 1, it is a Galois extension of $\mathbb{Q}$, and every other cubic Galois extension of $\mathbb{Q}$ has larger discriminant (in absolute value).

Thanks to Theorem 3.2.1, sums of three integral squares in $\mathcal{O}$ satisfy the local-global principle; hence, our main tools are the completions $\mathcal{O}_{\mathfrak{p}}$ of the ring of integers $\mathcal{O}$ at places $\mathfrak{p}$. In particular, we will examine the only dyadic place of $\mathcal{O}$, corresponding to the prime ideal (2). (The fact that 2 is indeed a prime of $\mathcal{O} = \mathbb{Z}[\zeta_7 + \zeta_7^{-1}]$ is easily checked using [Mi, Th. 3.41].)

In general, local conditions do not suffice to describe the set $\sum \mathcal{O}_K^2$; usually there are elements which are not a sum of squares ("globally") despite being a sum of integral squares at all completions. Scharlau calls them "Ausnahmeelemente" (i.e. *exceptional elements*) and examines them in depth in [Sch] – for example, he shows that up to multiplication by squares of units, there are always only finitely many of them; on the other hand, he proves that in every cubic order there is at least one such element. As the discriminant of $K^{(49)}$ is odd, the only local condition for a sum of squares is total positivity [Sch, Kap. 0]. In our second result, we characterise the set of sums of squares, showing that up to multiplication by units there is only one exceptional element, namely $1+\rho+\rho^2$. (Remember that $\rho = \zeta_7 + \zeta_7^{-1}$.)

Theorem 3.2.3. *Let $\alpha \in \mathcal{O}$ be totally positive. Then the following statements are equivalent:*

(1a) $\alpha \notin \sum \mathcal{O}^2$.

(1b) α *is not a sum of four integral squares.*

(2a) The norm of α *is* 7.

(2b) $\alpha = u^2(1+\rho+\rho^2)$ *for a unit* $u \in \mathcal{O}$.

(2c) α *is an indecomposable element and not a square.*

The proof of this result, as well as the therein contained notion of *indecomposable elements*, is to be found in Section 3.5. Note that while a full characterisation of $\sum \mathcal{O}_K^2$ is not usually known, for real quadratic fields the problem is solved in [Pe2, Satz 2].

We can immediately state a simple corollary of our characterisation of $\sum \mathcal{O}^2$. Remember that a totally positive definite quadratic form is called *universal* if it represents all totally positive integers. In [KY2], it is proven that $K^{(49)}$ has the very rare property of admitting a universal quadratic form with rational integral coefficients (the form in question has four variables: $x^2+y^2+z^2+w^2+xw+yw+zw$). With our knowledge, one easily constructs a universal quadratic form in five variables:

Corollary 3.2.4. *The totally positive definite quadratic form $x_1^2+x_2^2+x_3^2+x_4^2+(1+\rho+\rho^2)x_5^2$ is universal over $\mathcal{O}$.*

While the form given in [KY2] has less variables, their form is *non-classical*, i.e. the corresponding symmetric matrix contains non-integral entries. Our form is not only classical, but even diagonal. For monogenic simplest cubic fields, [KT, Th. 1.1] provides a construction of a diagonal universal quadratic form, which for $\mathcal{O}_{K^{(49)}}$ requires 12 variables, so our form is much simpler. To the best of our knowledge, no classical universal form in five or less variables in a totally real field of odd degree has been previously known. (By a well-known argument involving Hilbert reciprocity, at least four variables are necessary for fields of odd degree [EK].)

3.3 Sums of three squares

It is well known [O'M, 102:5] that every quadratic form with class number 1 satisfies the local-global principle. This means that a number is represented over $\mathcal{O}$ if and only if it is represented over $\mathcal{O}_\mathfrak{p}$ for all places $\mathfrak{p}$. While the sum of four squares I_4 does not have this property (we will later prove that $1+\rho+\rho^2$ is not a sum of any number of squares, while being a sum of four squares everywhere locally), we shall exploit that I_3 satisfies the local-global principle to fully determine which numbers are a sum of three integral squares in $K^{(49)}$:

Proposition 3.3.1. *In $\mathcal{O} = \mathbb{Z}[\zeta_7+\zeta_7^{-1}]$, the quadratic form I_3 represents a nonzero number α if and only if α satisfies both the following conditions:*

1. *α is totally positive;*

2. *at the dyadic place $\mathcal{O}_{(2)}$, $\alpha \neq -t^2$ for all $t \in \mathcal{O}_{(2)}$.*

The proof is given at the end of this section. To prepare for it, we need to examine the dyadic completion $\mathcal{O}_{(2)}$. We state our results more generally for the ring of integers $\mathfrak{O}$ in a dyadic local field L with a few additional properties, since this generality makes the proofs clearer. We start with a useful observation:

Observation 3.3.2. Let $\mathfrak{O}$ be any commutative ring where 2 is a prime element. Then the following statements are equivalent for $x, y \in \mathfrak{O}$:

1. $x \equiv y \pmod 2$;

2. $x^2 \equiv y^2 \pmod 4$;

3. $x^2 \equiv y^2 \pmod 2$.

Indeed, the implications (1) $\Rightarrow$ (2) $\Rightarrow$ (3) are trivial. For (3) $\Rightarrow$ (1), one rewrites the condition (3) as $2 \mid (x-y)^2$ and uses the fact that 2 is a prime.

This observation can further be exploited to get the following lemma:

Lemma 3.3.3. *Let $\mathfrak{O}$ be the ring of integers of a dyadic local field L where 2 is a prime element and the degree $[L : \mathbb{Q}_2]$ is odd. Let $u, v \in \mathfrak{O}$ be units. Then:*

1. *$u^2 + v^2 \neq \square$;*

2. *there are no $y, z \in \mathcal{O}$ such that $u^2 + y^2 + z^2 \equiv 0 \pmod 4$.*

Proof. Assume that, contrary to the first statement, $u^2 + v^2 = w^2$ for some $w \in \mathfrak{O}$. Then $w^2 \equiv (u+v)^2 \pmod 2$, so the previous observation yields $w^2 \equiv (u+v)^2 \pmod 4$.

Plugging this into $u^2 + v^2 = w^2$ gives $2uv \equiv 0 \pmod 4$. This is equivalent to $uv \equiv 0 \pmod 2$, which cannot happen since u, v are units. Thus the first part is proven.

Similarly, if the second statement is violated, we write $z^2 \equiv (u+y)^2 \pmod 2$, so the above observation yields $z^2 \equiv (u+y)^2 \pmod 4$. Plugging in, we get $2u^2 + 2y^2 + 2uy \equiv 0 \pmod 4$. This is equivalent to $u^2 + uy + y^2 \equiv 0 \pmod 2$; as u is a unit, it follows that there exists a root of $t^2 + t + 1$ modulo 2, i.e. in $\mathfrak{O}/(2)$.

Since 2 is the prime element, $\mathfrak{O}/(2)$ is the residue field. It is isomorphic to $\mathbb{F}_{2^d}$, where $d = [L : \mathbb{Q}_2]$ is by assumption an odd number. However, this is a contradiction – no root of an irreducible quadratic polynomial over $\mathbb{F}_2$ can be contained in an extension of odd degree. $\square$

We were building towards the following characterisation of sums of three squares in $\mathcal{O}_{(2)}$ and more generally in the ring of integers in any unramified dyadic local field of odd degree:

Lemma 3.3.4. *Let L be any dyadic local field where 2 is a prime element and the degree $[L : \mathbb{Q}_2]$ is odd. Then, over its ring of integers $\mathfrak{O}$, the form I_3 represents exactly those nonzero elements which are not equal to $-t^2$ for any $t \in \mathfrak{O}$.*

Proof. Bear in mind that a square is integral if and only if the squared number is integral. Now, the proof has two parts. First we show that if a number in $\mathfrak{O}$ is a sum of three squares in L, then these squares are necessarily integral. Afterwards we use the known results about representations over a local field.

Let us examine whether a sum of three non-integral squares can belong to $\mathfrak{O}$. We use the fact that 2 is the prime element, and multiply the equality by a suitable power of 2, to reformulate the question as follows: Is it possible to find $x, y, z \in \mathfrak{O}$, with x being a unit, so that $x^2 + y^2 + z^2 \equiv 0 \pmod 4$? By Lemma 3.3.3 (2), the answer is no.

We have just shown that if the sum of three squares is integral, then the squared numbers are integral as well (which, as a corollary, also yields that 0 is not non-trivially represented, i.e. I_3 is anisotropic). Therefore, we now only have to examine the numbers represented by I_3 over the field L instead of over the ring $\mathfrak{O}$. Since I_3 is anisotropic and its determinant is a square, [O'M, 63:21] yields that the only not-represented elements are minus squares. □

With this dyadic preparation, we are ready to characterise sums of three squares in $\mathcal{O}$.

Proof of Proposition 3.3.1. By Theorem 3.2.1, the form I_3 has class number 1, so it satisfies the local-global principle. Thus, it suffices to check which numbers are represented locally.

In the real embeddings, every positive number is already a square, while negative numbers cannot be written as any number of squares. In a non-dyadic completion, every ternary unimodular form is universal [O'M, 92:1b]. Thus it remains to examine the only dyadic place $\mathcal{O}_{(2)}$. This was done in Lemma 3.3.4 – this lemma applies since (2) is inert, so $[K^{(49)}_{(2)} : \mathbb{Q}_2]$ is equal to $[K^{(49)} : \mathbb{Q}]$, which is odd. □

3.4 The main proof

Now we fully understand sums of three integral squares. To complete the proof that every sum of squares in $\mathbb{Z}[\zeta_7 + \zeta_7^{-1}]$ is already a sum of four squares, one has to examine two types of problematic elements: Those which are equal to minus square of a unit in $\mathcal{O}_{(2)}$, and those which are minus square of a number divisible by 2 in $\mathcal{O}_{(2)}$. To deal with the latter type, one simple trick suffices:

Observation 3.4.1. Let $\alpha \in \mathcal{O}$ be totally positive and let it be equal to $-(2t)^2$ at the dyadic place. Then $\ell(\alpha) = 4$, i.e. it is a sum of four but not of three squares.

Indeed, the number $\alpha/2$ is totally positive and it is clearly not equal to $-\square$ at the dyadic place, hence by Proposition 3.3.1 we have $\alpha/2 = x^2+y^2+z^2$ in $\mathcal{O}$. Then $\alpha = (x+y)^2+(x-y)^2+z^2+z^2$. On the other hand, by the same proposition, α is not a sum of three squares.

As a side note, one could also use the universality of the quadratic form $x^2 + y^2 + z^2 + w^2 + xw + yw + zw$ to deduce that every totally positive number in $2\mathcal{O}$ is a sum of four squares, since $2(x^2 + y^2 + z^2 + w^2 + xw + yw + zw) = (x + y + w)^2 + (x - y)^2 + (z + w)^2 + z^2$. Either way, combining Proposition 3.3.1 with the above observation, we obtain the following neat statement, which is the basis of the proofs of Theorems 3.2.2 and 3.2.3:

Corollary 3.4.2. *If a totally positive number in $\mathcal{O}$ is not a sum of four integral squares, then in $\mathcal{O}_{(2)}$ it is equal to $-u^2$ where u is a unit.*

Finally, we are ready to prove that the Pythagoras number of $\mathcal{O}$ is 4:

Proof of Theorem 3.2.2. Let $\alpha \in \sum \mathcal{O}^2$. Clearly, α is totally non-negative, so in most cases Corollary 3.4.2 applies and α is a sum of four squares. It remains to deal with the case when at the dyadic place, $\alpha = -u^2$ with u a unit. In this case, the condition that α is totally positive is not enough for its being a sum of squares (compare Theorem 3.2.3). However, we know that $\alpha = \sum x_i^2$ for some $x_i \in \mathcal{O}$. We shall show that if x_j is a dyadic unit, then $\alpha - x_j^2$ is a sum of three squares in $\mathcal{O}$, implying that α is a sum of four squares. This will conclude the proof, since at least one of the summands must be a unit.

For the sake of contradiction, suppose that $\sum_{i\neq j} x_i^2$ is not a sum of three squares in $\mathcal{O}$. It is totally positive, so by Proposition 3.3.1 it must be $-\square$ in $\mathcal{O}_{(2)}$. However, the equality $-u^2 = x_j^2 - \square$ in $\mathcal{O}_{(2)}$ is impossible by Lemma 3.3.3 (1) since u and x_j are units. □

3.5 Characterisation of sums of squares

In this section we are going to determine which numbers can be written as a sum of squares (by Theorem 3.2.2 they can in fact be represented as a sum of *four* squares). To achieve this, we shall need the following notion: A totally positive number in $\mathcal{O}$ is called *indecomposable* if it cannot be written as a sum of two totally positive elements of $\mathcal{O}$.

The indecomposable elements are quite difficult to study; it is a significant success that [KT, Th. 1.2] fully characterises them for the order $\mathbb{Z}[\rho_a]$ in the simplest cubic fields. For our case, their result reads as follows (recall that $\rho = \zeta_7 + \zeta_7^{-1}$):

Lemma 3.5.1 (Kala, Tinková)**.** *Up to multiplication by squares of units, the only indecomposables of $\mathcal{O}$ are 1 and $1 + \rho + \rho^2$.*

We use this lemma to provide a very explicit description of the set $\sum \mathcal{O}^2$, namely: a totally positive α is an exceptional element if and only if it satisfies the simple condition (2a) or equivalently (2b). However, note that the core of the proof does not use the indecomposable elements explicitly – without the lemma, we would still have the equivalence of (1a) (and (1b)) with (2c).

Theorem 3.2.3. *Let $\alpha \in \mathcal{O}$ be totally positive. Then the following statements are equivalent:*

(1a) $\alpha \notin \sum \mathcal{O}^2$.

(1b) α *is not a sum of four integral squares.*

(2a) The norm of α *is* 7.

(2b) $\alpha = u^2(1 + \rho + \rho^2)$ *for a unit* $u \in \mathcal{O}$.

(2c) α *is an indecomposable element and not a square.*

Proof. The new input in this proof will be the equivalence between (1a) and (2c). Most of the other implications are clear by now:

By Theorem 3.2.2, (1a) and (1b) are equivalent. Statements (2b) and (2c) are equivalent by the previous lemma. The equivalence of (2a) and (2b) is elementary: On the one hand, one easily checks (or looks up in [KT]) that $1 + \rho + \rho^2$ has norm 7; on the other hand, since (7) ramifies, any two (totally positive) elements of norm 7 generate the same ideal, hence differ only by multiplication by a (totally positive) unit. It is well known [Ti] that in simplest cubic fields, a unit is totally positive if and only if it is a square.

The implication from (2c) to (1a) is also immediate: An indecomposable element is either a square or not a sum of squares. Hence our task is to prove the converse: If α is decomposable, then α is a sum of squares. In the following, we will repeatedly exploit Corollary 3.4.2: If a totally positive number is not a sum of squares, then in $\mathcal{O}_{(2)}$ it must be equal to $-u^2$ where u is a unit.

Assume that $\alpha = \beta + \gamma$. If both β and γ are sums of squares, then so is α. If neither of them is a sum of squares, then at the dyadic place, α is $-(u_1^2 + u_2^2)$ where u_1, u_2 are units. However, by Lemma 3.3.3 (1) the sum of two unit squares is not a square in $\mathcal{O}_{(2)}$, hence α is a sum of squares in $\mathcal{O}$.

Hence we may assume that $\beta = \sum x_i^2$ and γ is not a sum of squares. We also may assume that x_1 is a unit in $\mathcal{O}_{(2)}$; if not, we use the equality $(2x)^2 = x^2 + x^2 + x^2 + x^2$. Clearly it suffices to show that $\tilde{\gamma} = x_1^2 + \gamma$ is a sum of squares. And this is easy, since Lemma 3.3.3 (1) gives a contradiction if both γ and $\tilde{\gamma}$ are minus squares of units in $\mathcal{O}_{(2)}$. □

The key idea behind the above proof is that while not every indecomposable element is a sum of squares, the sum of two indecomposables in $\mathcal{O}$ can always be rewritten as a sum of

squares. With the just proven theorem, one immediately gets Corollary 3.2.4: The quadratic form $x_1^2 + x_2^2 + x_3^2 + x_4^2$ represents all totally positive elements except for those of the form $u^2(1 + \rho + \rho^2)$, and these are represented by $(1 + \rho + \rho^2)x_5^2$.

3.6 Final notes

The crucial ingredient of our proofs was the fact that the sum of three squares I_3 satisfies the local-global principle. The same arguments in fact prove that $\mathcal{P}(\mathcal{O}_K) = 4$ for every totally real field K of odd degree where (2) is inert, *provided that I_3 integrally represents all numbers which it integrally represents everywhere locally*, but the only straightforward way to prove this integral local-global principle is proving $h(I_3) = 1$.

Therefore, the only totally real fields where it is reasonably simple to show that $\mathcal{P}(\mathcal{O}_K)$ is small are the six fields listed in Theorem 3.2.1 as the only fields with $h(I_3) = 1$. Let us discuss them briefly:

For $\mathbb{Q}$, we have $\mathcal{P}(\mathbb{Z}) = 4$ by Lagrange's four square theorem. For $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$ it is well known [Dz, Ma] that $\mathcal{P}(\mathcal{O}_K) = 3$; the proofs are based on the local-global principle. For $\mathbb{Q}(\sqrt{17})$, the situation is different: $\mathcal{P}(\mathbb{Z}[\frac{1+\sqrt{17}}{2}]) = 5$, which is the largest value allowed for quadratic orders by the bound $g_{\mathbb{Z}}(2)$; this is easily proven by checking that $7 + (\frac{1+\sqrt{17}}{2})^2$ is not a sum of four squares. Actually, by [CP, Th. 5"], there are many different elements of length 5 in $\mathbb{Z}[\frac{1+\sqrt{17}}{2}]$: Any totally positive element of the norm $128 \cdot 4^k$ has length 5.

The only remaining field is $K^{(148)}$, the cubic field with discriminant 148. There, the same strategy as in this paper might be applied – first, one proves an analogy of Proposition 3.3.1, characterising sums of three squares, and then hopefully exploits this result to prove $\mathcal{P}(\mathcal{O}_{K^{(148)}}) = 4$ or $\mathcal{P}(\mathcal{O}_{K^{(148)}}) = 5$. It should not be too difficult, but the situation is slightly complicated by the fact that (2) ramifies, so the behaviour at the dyadic place is less simple than in our Lemma 3.3.4. For example, total positivity is no longer the only local condition for a sum of squares.

4. On quadratic Waring's problem in totally real number fields

This chapter contains the paper [KrY] J. Krásenský and P. Yatsyna, *On quadratic Waring's problem in totally real number fields*, Proc. Amer. Math. Soc. 151, 1471–1485 (2023).

4.1 Introduction

The *quadratic Waring's problem* or a *new Waring's problem with squares of linear forms* (eponymous with the title of Mordell's paper [Mo] that initiated the problem around 1930) asks what is the smallest number of squares needed to represent all admissible quadratic forms. For positive semidefinite quadratic forms in r variables over $\mathbb{Z}$, where $r \leq 5$, Mordell and Ko [Ko, Mo, Mo2] proved that $r+3$ squares of linear forms suffice. Observe that quadratic forms that are sums of squares of linear forms are necessary positive semidefinite. However, there exists a (unique) positive definite quadratic form in 6 variables which is not a sum of squares [Mo3].

Let $\Sigma_{\mathbb{Z}}(r)$ be the set of quadratic forms in r variables representable by a sum of squares of linear forms over $\mathbb{Z}$. The *g-invariant* $g_{\mathbb{Z}}(r)$ is the smallest natural number such that every form in $\Sigma_{\mathbb{Z}}(r)$ is, in fact, a sum of $g_{\mathbb{Z}}(r)$ squares. The above results now read as $g_{\mathbb{Z}}(r) = r+3$, for $1 \leq r \leq 5$. This is a generalisation of Lagrange's four-square theorem, i.e. that $g_{\mathbb{Z}}(1) = 4$.

The only remaining known value, $g_{\mathbb{Z}}(6) = 10$, was determined just in 1997 by Kim and Oh [KO]. Much effort went into obtaining upper and lower bounds for $g_{\mathbb{Z}}(r)$. For $7 \leq r \leq 20$, explicit bounds are known [KO2, Sa]. The upper bounds valid for all r improved gradually: from functions growing faster than exponentially [Ic2] through an exponential [KO3] to the currently best $g_{\mathbb{Z}}(r) = O(\mathrm{e}^{(4+2\sqrt{2}+\varepsilon)\sqrt{r}})$ due to Beli, Chan, Icaza and Liu [BCIL].

The g-invariant can be generalised to $g_R(\,\cdot\,)$ of an arbitrary ring R by replacing forms over $\mathbb{Z}$ by forms over R. In particular, the value $\mathcal{P}(R) = g_R(1)$ is the *Pythagoras number* of R, much examined both for arbitrary fields (see, for example, [Le]) and for orders of number fields [HH, Kr, KRS, Pe2, Ti, Sch2], and, in an influential paper [CDLR], for affine and local algebras.

For any number field K and $r \geq 3$, we have $g_K(r) = r+3$ [BLOP, Prop. 3.2]. The exact values of $g_{\mathbb{Z}}(r)$ for $1 \leq r \leq 5$, given above, derive as a straightforward consequence of the fact that every positive definite form of rank r is represented by a form that is in the genus of I_{r+3} (the sum of $r+3$ squares form): Up to rank eight, this genus contains only one equivalence class [Kn].

For orders $\mathcal{O}$ in number fields which are not totally real, one has $\mathcal{P}(\mathcal{O}) \leq 5$ [Pf] and for maximal orders even $\mathcal{P}(\mathcal{O}_K) \leq 4$ and more generally $g_{\mathcal{O}_K}(r) \leq r+3$ [Ic2, Sec. 1] thanks to the theory of spinor genera, but the totally real case exhibits radically different behaviour. For totally real number field K, $\mathcal{P}(\mathcal{O}_K)$ can be arbitrarily large [Sch2], but it is bounded by a function depending only on the degree $d = [K : \mathbb{Q}]$ [KY2], namely $\mathcal{P}(\mathcal{O}) \leq g_{\mathbb{Z}}(d)$ for any order $\mathcal{O}$ of degree d (the related bound $\mathcal{P}(K) \leq g_F([K : F])$ for fields has already appeared in [CDLR]).

The fact that $g_{\mathcal{O}_K}(r)$ is finite was given together with an upper bound in [Ic, Ic2]. Chan and Icaza have shown that $g_{\mathcal{O}_K}(r) \leq D\mathrm{e}^{\kappa\sqrt{r}}$ for totally real number fields K of class number 1, where constants κ and D depend only on K [CI, Thm. 1.1]. We improved this bound as follows:

Theorem 4.1.1. *Let $\mathcal{O}$ be an order in a number field K of degree d. Then*

$$g_{\mathcal{O}}(r) \leq g_{\mathbb{Z}}(rd).$$

In particular, for every $\varepsilon > 0$, there exists a constant D, depending only on ε, such that

$$g_{\mathcal{O}}(r) \leq D\mathrm{e}^{(4+2\sqrt{2}+\varepsilon)\sqrt{dr}}.$$

The first inequality directly follows from Theorem 4.1.2 (1) below. The latter is a consequence of [BCIL, Thm. 1.1], that is, the bound $g_{\mathbb{Z}}(r) = O(\mathrm{e}^{(4+2\sqrt{2}+\varepsilon)\sqrt{r}})$.

For number fields with a class number larger than 1, the g-invariant is still well-defined. However, there is a natural alternative: Let $G_{\mathcal{O}_K}(r)$ be obtained by replacing quadratic forms with quadratic lattices and suitably rephrasing the condition about a sum of squares of linear forms. (The precise formulation is in Definition 4.2.1; note that the analogous definition for Hermitian lattices is used in [BCIL, Li2, Li].) A more encompassing result of this paper is the following:

Theorem 4.1.2. *Let $K \supset F$ be number fields, $[K : F] = d$, and $\mathcal{O}$ any order in K which contains $\mathcal{O}_F$.*

1. *If $\mathcal{O}$ is a free $\mathcal{O}_F$-module, then $g_{\mathcal{O}}(r) \leq g_{\mathcal{O}_F}(rd)$. In general, $g_{\mathcal{O}}(r) \leq g_{\mathcal{O}_F}(rd+1)$.*
2. *$G_{\mathcal{O}_K}(r) \leq G_{\mathcal{O}_F}(rd)$. In particular, $\mathcal{P}(\mathcal{O}_K) \leq G_{\mathcal{O}_K}(1) \leq G_{\mathcal{O}_F}(d)$.*
3. *$g_{\mathcal{O}}(r) \leq G_{\mathcal{O}_F}(rd)$. In particular, $\mathcal{P}(\mathcal{O}) \leq G_{\mathcal{O}_F}(d)$.*

The proof is a direct consequence of the general Theorem 4.4.1 (the only exception is the second part of (1), which is precisely Corollary 4.3.3). In fact, we show that $g_R(r) \leq g_S(dr)$ for a ring extension R/S generated as an S-module by d elements.

Let us compare the statements: If $\mathcal{O} = \mathcal{O}_K$, (3) follows from (2), whereas (1) and (2) are independent. For non-maximal orders, (2) cannot be applied, and (1) and (3) are independent. Finally, the simplest situation when (1) can be applied is if F has the class number 1; in that case $G_{\mathcal{O}_F} = g_{\mathcal{O}_F}$, so (3) gives exactly the same.

Let us point out that, aside from providing a first inequality of this type for the g-invariants where $r > 1$, our Theorem 4.1.2 also provides a new upper bound for the Pythagoras number in the case when $\mathcal{O}_K$ is not a free $\mathcal{O}_F$-module, thus essentially resolving a question posed in a remark after [KRS, Prop. 7.5]. This is also evidence that the lattice version of the invariant is important. Further evidence towards its significance is that this invariant is necessary in the proof of $g_{\mathcal{O}}(r) \leq g_{\mathcal{O}_F}(rd+1)$, see Corollary 4.3.3. Also, note that in Theorem 4.1.1, if $\mathcal{O} = \mathcal{O}_K$, then $g_{\mathcal{O}_K}(r)$ can be replaced by $G_{\mathcal{O}_K}(r)$. For that, one applies Theorem 4.1.2 (2) instead of (1).

Some explicit upper bounds for $g_{\mathcal{O}_F}(r)$ for $r > 1$ and a totally real field $F \neq \mathbb{Q}$ were given by Sasaki [Sa2]. For $F = \mathbb{Q}(\sqrt{5})$ he proved $g_{\mathcal{O}_F}(2) = 5$ (see also [KRS, Thm. 7.7]), and also showed $g_{\mathcal{O}_F}(3) \leq 70$, $g_{\mathcal{O}_F}(4) \leq 776$ and $g_{\mathcal{O}_F}(5) \leq 3080$. Our results improve these latter bounds to 10, 37 and 68, respectively, since $g_{\mathbb{Z}}(6) = 10$, while $g_{\mathbb{Z}}(8) \leq 37$ and $g_{\mathbb{Z}}(10) \leq 68$ [KO2].

Another immediate consequence of Theorem 4.1.2 is that $g_{\mathcal{O}}(r)$ is always finite.

Corollary 4.1.3. *All g-invariants of an order in a number field are finite.*

Even for rings of integers, this corollary is of interest – the original proof of finiteness of $g_{\mathcal{O}_K}(r)$ for every r is due to Icaza [Ic, Ic2] and depends on the results from [HKK] about $\mathcal{O}_K$-lattices, while our approach only relies on [HKK] for the finiteness of $g_{\mathbb{Z}}(\,\cdot\,)$.

It seems that Theorem 4.1.2 provides optimal upper bounds for most of the cases that we can check. In the case of Pythagoras number ($r = 1$), this was illustrated for quadratic fields [Pe2], simplest cubic fields [Ti] and biquadratic fields [KRS]. In this paper, we show that for all but three quadratic fields K, the inequality $G_{\mathcal{O}_K}(2) \leq g_{\mathbb{Z}}(4) = 7$ is, in fact, equality.

Theorem 4.1.4. *Let K be a real quadratic field other than $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{5})$. Then $G_{\mathcal{O}_K}(2) = 7$.*

For $\mathbb{Q}(\sqrt{5})$, the correct value is 5, as shown by Sasaki [Sa2]. The same was recently proven for $\mathbb{Q}(\sqrt{2})$ by He and Hu [HH]; both papers are based on the local-global principle for sums of four integral squares. For the only remaining field $\mathbb{Q}(\sqrt{3})$ we expect $G(2) = 6$, but it can be very difficult to prove, since already for the form $x^2 + y^2 + z^2$ it is not clear whether the local-global principle holds (for representation of integral binary forms).

The proof of Theorem 4.1.4 is contained in Section 4.5. The upper bound is already clear. For the lower bound in cases $\mathbb{Q}(\sqrt{n})$ with $n \equiv 1 \pmod 4$, we explicitly produce a quadratic form which is not a sum of 6 squares of linear forms (Proposition 4.5.3), in fact proving the stronger result $g_{\mathcal{O}_K}(2) = 7$. If $n \not\equiv 1 \pmod 4$, we use the inequality between G-invariants in the other direction, exploiting the results on the Pythagoras numbers of orders in biquadratic number fields from [KRS].

From the definition, it is clear that $g_{\mathcal{O}_K}(r) \leq G_{\mathcal{O}_K}(r)$, and in Proposition 4.3.2, we shall see $G_{\mathcal{O}_K}(r) \leq g_{\mathcal{O}_K}(r+1)$. It is natural to ask: Can $g_{\mathcal{O}_K}(r) < G_{\mathcal{O}_K}(r)$ happen for some number field K and some $r \in \mathbb{N}$, or does equality always hold? Guessing the answer is difficult since the exact values of the invariants are rarely known. However, we fully solve it at least for the "lattice Pythagoras number" $G_{\mathcal{O}_F}(1)$ of a quadratic ring of integers:

Theorem 4.1.5. *Let F be a real quadratic field. Then $\mathcal{P}(\mathcal{O}_F) = G_{\mathcal{O}_F}(1)$. This value is five except for $F = \mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{5})$, where it is three, and for $F = \mathbb{Q}(\sqrt{6})$ and $\mathbb{Q}(\sqrt{7})$, where it is four.*

Proof. All the values $\mathcal{P}(\mathcal{O}_F)$ for a real quadratic field F are known thanks to Peters, Maaß, Dzewas, Cohn and Pall and an unpublished result by Kneser (contained in Scharlau's dissertation) [Pe2, Ma, Dz, CP, Sch]; an overview of these results can be found in Section 3 of [KRS]. It remains to determine $G_{\mathcal{O}_F}(1)$. All the five exceptional cases have class number 1, so there is no difference between $\mathcal{P}(\mathcal{O}_F)$ and $G_{\mathcal{O}_F}(1)$. For the other cases, we get $5 = \mathcal{P}(\mathcal{O}_F) \leq G_{\mathcal{O}_F}(1) \leq g_{\mathbb{Z}}(2) = 5$. □

4.2 Preliminaries

We use [Na] as a reference for everything related to number fields and [KnS] for quadratic forms and lattices. In order to be able to conduct all proofs in the more geometric language of quadratic lattices instead of switching back and forth between lattices and polynomials, we define quadratic lattices over any integral domain (and free lattices even over any commutative ring) instead just over a Dedekind domain.

4.2.1 Quadratic forms, g-invariants

Let R be any commutative ring with unity. A *quadratic* (*linear*, resp.) *form* over R in r variables is a homogeneous polynomial in $R[X_1, \ldots, X_r]$ of degree 2 (1, resp.). A form in r variables is also called r-ary: unary, binary, ternary, etc. If for quadratic forms φ and ψ in r and s variables, $r \geq s$, it is possible to find linear forms $L_1, \ldots, L_r$ such that

$$\varphi(L_1(X_1, \ldots, X_s), \ldots, L_r(X_1, \ldots, X_s)) = \psi(X_1, \ldots, X_s),$$

we say that φ *represents* ψ. Two forms in the same number of variables which represent each other are called *equivalent*.

Consider the set $\Sigma_R(r)$ of all r-ary quadratic forms over R which can be written as a sum of squares of linear forms over R, i.e. which are represented by the quadratic form $X_1^2 + \cdots + X_N^2$ for some $N \in \mathbb{N}$. Then we put

$$g_R(r) = \min\{n : X_1^2 + \cdots + X_n^2 \text{ represents all forms in } \Sigma_R(r)\}.$$

If no such n exists, we put $g_R(r) = \infty$; however, if R is the ring of integers in a number field, then $g_R(r)$ is finite for every r [Ic2]. (Our Corollary 4.1.3 extends this result to non-maximal

orders.) Note that $g_R(1) = \mathcal{P}(R)$ is the *Pythagoras number*: The smallest number P such that, if $\alpha \in R$ is a sum of squares, then it can be written as a sum of at most P squares.

By *length* we mean the minimal number of squares which is necessary to represent a form φ (or a number α). The length is denoted by $\ell(\,\cdot\,)$ or $\ell_R(\,\cdot\,)$. Hence, $g_R(r)$ is the biggest finite length of an r-ary form over R.

4.2.2 Quadratic spaces and modules

Let R be a commutative ring with unity. A *quadratic module* over R is a pair (M, Q), where M is an R-module and $Q : M \to R$ is a *quadratic map*, i.e. a map such that $Q(a\mathbf{x}) = a^2 Q(\mathbf{x})$ for every $a \in R$ and $\mathbf{x} \in M$, and that the induced map $B_Q(\mathbf{x}, \mathbf{y}) = Q(\mathbf{x} + \mathbf{y}) - Q(\mathbf{x}) - Q(\mathbf{y})$ is bilinear. If R is a field, then M is a vector space and (M, Q) is called a *quadratic space*.

Consider two quadratic modules (M, Q_M) and (N, Q_N) over R. An *isometry* is an injective R-linear map $\iota : M \to N$ which respects the quadratic maps, i.e. $Q_N(\iota(\mathbf{x})) = Q_M(\mathbf{x})$ for every $\mathbf{x} \in M$. If this map is bijective, then the corresponding quadratic modules are *isometric*; this is an equivalence relation denoted by $\simeq$. By omitting the condition of injectivity, we get the notion of *representation*: M is represented by N if there exists any R-linear map $\iota : M \to N$ such that $Q_N(\iota(\mathbf{x})) = Q_M(\mathbf{x})$ for $\mathbf{x} \in M$. This is denoted by $M \to N$ (and by $M \not\to N$ if such an R-linear map for M to N does not exist, i.e. N does not represent M).

The *orthogonal sum* $M \perp N$ of the quadratic modules M, N is the direct sum of R-modules $M \oplus N$ equipped with the quadratic map $Q(\mathbf{x} + \mathbf{y}) = Q_M(\mathbf{x}) + Q_N(\mathbf{y})$ for $\mathbf{x} \in M, \mathbf{y} \in N$.

4.2.3 Free lattices

If L is a finitely generated free module of rank r (i.e. isomorphic to R^r as an R-module) equipped with any quadratic map Q, we call (L, Q) a *free quadratic lattice* of *rank* r. A lattice of rank r is also called r-ary: unary, binary, etc. The free unary lattice $R\mathbf{e}$ where $Q(\mathbf{e}) = a$ is denoted by $\langle a \rangle$; it is unique up to isometry. The basic quadratic module defined over any commutative ring R is I_n, which is the free lattice R^n equipped with the "sum-of-squares" form $Q(\mathbf{x}) = \mathbf{x}^{\mathrm{T}}\mathbf{x}$. One can also write $I_n \simeq \underbrace{\langle 1 \rangle \perp \cdots \perp \langle 1 \rangle}_{n\text{-times}}$.

For a quadratic form $\varphi(X_1, \ldots, X_r)$ over R, one can construct the corresponding free quadratic lattice L_φ as the R-module R^r (with standard basis vectors $\mathbf{e_1}, \ldots, \mathbf{e}_r$) equipped with the quadratic map Q defined as $Q(\alpha_1\mathbf{e}_1 + \cdots + \alpha_r\mathbf{e}_r) = \varphi(\alpha_1, \ldots, \alpha_r)$. On the other hand, if a free quadratic lattice (or in fact any quadratic module) is generated by $\mathbf{x}_1, \ldots, \mathbf{x}_k$ as an R-module, then they can be used to define a quadratic form $\varphi(X_1, \ldots, X_k) = Q(X_1\mathbf{x}_1 + \cdots + X_k\mathbf{x}_k)$. In particular, there is a bijection between quadratic forms over R in r variables (up to equivalence) and *free* quadratic lattices of rank r (up to isometry). Also, note that φ represents ψ if and only if the corresponding lattice L_φ represents L_ψ. Especially, φ can be written as a sum of n squares of linear forms if and only if L_φ is represented by I_n.

4.2.4 Quadratic lattices

Assume now that R is an integral domain with the quotient field F. We will define quadratic lattices over R as a particularly well-behaved class of quadratic modules. Note that if R is not an integral domain, we only have the notion of a *free* quadratic lattice. Also, for Dedekind domains we will use the much nicer description of lattices given in the next subsection.

Consider a finite-dimensional vector space V over F. An *R-lattice* in V is any R-submodule $L \subset V$ which satisfies $L \subset R\mathbf{v}_1 + \cdots + R\mathbf{v}_r$ for some basis $(\mathbf{v}_1, \ldots, \mathbf{v}_r)$ of V. The *rank* of L is the dimension of the vector space FL. If (V, Q) is a finite-dimensional quadratic space over F, then a *quadratic lattice* is (L, Q') where L is an R-lattice in V and the quadratic map Q' is the restriction of Q to L.

Often we do not make a distinction between a quadratic lattice and its underlying R-lattice; e.g. the *rank* of a quadratic lattice is simply the rank of the corresponding R-module. From now on, a lattice usually means a quadratic lattice. Also, we sometimes denote the quadratic maps corresponding to different lattices by Q, since it is always clear what the underlying lattice is.

Note that free lattices (over an integral domain) are indeed lattices in this more general sense, since they can be embedded in a quadratic space by tensoring with the quotient field F. On the other hand, while lattices (and thus also the lattice version of the g-invariants) can be defined over any integral domain, it is much easier to work with them over Dedekind domains, see the next subsection.

Finally, we are ready to define the lattice version of the g-invariant:

Definition 4.2.1. For any integral domain R, consider the family $\Sigma_R^{\text{lat}}(r)$ of all quadratic lattices of rank r which are represented (over R) by I_N for some $N \in \mathbb{N}$. Then we put

$$G_R(r) = \min\{n : I_n \text{ represents all lattices in } \Sigma_R^{\text{lat}}(r)\}.$$

If no such n exists, we put $G_R(r) = \infty$.

To compare, it is clear that

$$g_R(r) = \min\{n : I_n \text{ represents all } \textit{free} \text{ lattices in } \Sigma_R^{\text{lat}}(r)\};$$

therefore, $g_R(r) \leq G_R(r)$. If R is a PID we have an equality as all lattices are free.

The following simple lemma is useful since it allows us to work with a smaller family of lattices than the whole $\Sigma_R^{\text{lat}}(r)$.

Lemma 4.2.2. *For a quadratic lattice Λ over an integral domain R, the following are equivalent:*

1. *Λ represents every lattice L of rank r such that $L \to I_N$ for some $N \in \mathbb{N}$.*
2. *Λ represents every sublattice of I_N of rank at most r for every $N \in \mathbb{N}$.*
3. *Λ represents every sublattice of I_N of rank r for every $N \in \mathbb{N}$.*

Subsequently, Definition 4.2.1 has the following formulation:

$$G_R(r) = \min\{n : I_n \textit{ represents all sublattices of } I_N \textit{ of rank } r \textit{ for every } N \in \mathbb{N}\}.$$

Proof. (3) $\implies$ (2): Let $L \subset I_N$ be of rank $s \leq r$. Then $L \perp I_{r-s} \subset I_{N+r-s}$ has rank r and is therefore represented by Λ. By restricting to L, we obtain the required representation.

(2) $\implies$ (1): Let L be a lattice of rank r with a representation $\iota : L \to I_N$. Then $\iota(L)$ is a sublattice of I_N of rank at most r, and is therefore represented by Λ. Thus $L \to \iota(L) \to \Lambda$.

(1) $\implies$ (3): Every sublattice of I_N is represented by I_N and thus by Λ. □

Our definitions are valid even for rings of characteristic 2. However, in that situation the questions considered in this paper are trivial because of the following observation.

Observation 4.2.3. Let $2 = 0$ in an integral domain R. Then $G_R(r) = g_R(r) = 1$ for every r. (If R contains zero divisors, we still have $g_R(r) = 1$ while $G_R(r)$ is not defined.) This follows from the fact that in characteristic two, $I_n \to I_1$ for every n, so every lattice represented by I_n is represented by I_1 as well. The representation $\iota : I_n \to I_1$ is $\iota(\sum \alpha_i \mathbf{e}_i) = (\sum \alpha_i)\mathbf{e}$ where $\mathbf{e_1}, \ldots, \mathbf{e}_n$ and $\mathbf{e}$ are the standard bases.

4.2.5 Number fields, orders, Dedekind domains

Let K be a number field with the ring of integers $\mathcal{O}_K$. Its degree over any subfield F is denoted by $[K : F]$. If $[K : \mathbb{Q}] = d$, then $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank d, and any basis of this module is called *integral basis* of $\mathcal{O}_K$. An *order* in K is any subring $\mathcal{O} \subset \mathcal{O}_K$ which is also a $\mathbb{Z}$-module of rank d. In particular, $\mathcal{O}_K$ is the maximal order with respect to inclusion.

A number field K is called *totally real* if all its embeddings into $\mathbb{C}$ actually map it into $\mathbb{R}$. With one exception, our results and proofs work for all number fields, but they are only interesting for the totally real ones, since $g_{\mathcal{O}_K}(r) \leq r + 3$ for every K which is not totally real.

Most of the time, the only property of the ring of integers $\mathcal{O}_K$ which we need is the fact that it is a *Dedekind domain*. If R is a Dedekind domain, then R-lattices are nothing else than finitely generated torsion-free R-modules. By the structure theorem [Na, Ch. 1, Thm. 1.32], any R-lattice L of rank d can be written as a direct sum $\mathfrak{a}_1\mathbf{x}_1 \oplus \cdots \oplus \mathfrak{a}_d\mathbf{x}_d$ where $\mathfrak{a}_i$ are fractional ideals and $\mathbf{x}_i \in L$ (although sometimes it is useful to take them in the vector space $F \cdot L$ where F is the quotient field of R).

We shall need the following properties, which follow from the structure theorem:

Lemma 4.2.4. *Let R be a Dedekind domain.*

1. *Every lattice L of rank r over R can be written in the form $L = R\mathbf{x}_1 + \cdots + R\mathbf{x}_{r-1} + \mathfrak{A}^{-1}\mathbf{x}_r$, where $\mathbf{x}_j \in L$ and $\mathfrak{A}$ is an integral ideal in R.*

2. *Let $S \subset R$ be another Dedekind domain such that R is a torsion-free S-module of rank d. Then: Any ideal $\mathfrak{A}$ in R can be written as $S\gamma_1 + \cdots + S\gamma_{d-1} + \mathfrak{b}^{-1}\gamma_d$ for $\gamma_i \in \mathfrak{A}$ and $\mathfrak{b}$ an integral ideal in S. In particular, $R = S\beta_1 + \cdots + S\beta_{d-1} + \mathfrak{a}^{-1}\beta_d$ for $\beta_i \in R$ and an integral ideal $\mathfrak{a}$ in S.*

The most typical situation when (2) applies is if $K \supset F$ are number fields with $d = [K : F]$ and $R = \mathcal{O}_K$, $S = \mathcal{O}_F$. It is important to note that if $\mathcal{O}_F \neq \mathbb{Z}$, there is not necessarily an integral basis of $\mathcal{O}_K$ over $\mathcal{O}_F$ (this happens if and only if $\mathfrak{a} = \mathcal{O}_F$), but there still exists the above *pseudo-basis* $(\beta_1, \ldots, \beta_d)$.

As mentioned, over a Dedekind domain, R-lattices of rank r are exactly the R-modules of the form $L = \mathfrak{a}_1\mathbf{x}_1 + \cdots + \mathfrak{a}_r\mathbf{x}_r$ where $\mathfrak{a}_i$ are fractional ideals in R and $\mathbf{x}_i \in L$ are linearly independent in the vector space $F \otimes_R L$ where F is the quotient field. A quadratic lattice is then any quadratic module on such an R-lattice. It is beneficial to consider this the definition of a quadratic lattice since the original definition from Subsection 4.2.4 is more difficult to work with. This lattice is free if and only if $\mathfrak{a}_1 \cdots \mathfrak{a}_r$ is a principal ideal [Na, Ch. 1, Thm. 1.32].

If $S \subset R$ are two Dedekind domains and $L = \mathfrak{a}_1 x_1 + \cdots + \mathfrak{a}_r x_r$ is a quadratic S-lattice (with quadratic map Q), we can (and often will) "extend the scalars" by taking the tensor product: $R \otimes_S L$ is the quadratic R-lattice $R\mathfrak{a}_1 x_1 + \cdots + R\mathfrak{a}_r x_r$ (where the quadratic map Q_R extends Q).

Note that a non-maximal order $\mathcal{O}$ is never a Dedekind domain. In particular, although we defined $G_{\mathcal{O}}(r)$, we will prove almost nothing nontrivial about it (only Proposition 4.3.1) since the theory of lattices over non-maximal orders is much more involved than over Dedekind domains.

4.3 Observations about G

One simple property of the classical g-invariant is $g_{\mathcal{O}}(r+1) \geq g_{\mathcal{O}}(r) + 1$ over any totally real order $\mathcal{O}$ (see below and compare to [BLOP, Cor. 2.4]). We show that the same holds for the lattice version $G_{\mathcal{O}}$ as well.

Proposition 4.3.1. *Let K be a totally real number field and $\mathcal{O} \subset \mathcal{O}_K$ any order. Then:*

1. $G_{\mathcal{O}}(r) > G_{\mathcal{O}}(s)$ *for* $r > s$.

2. $G_{\mathcal{O}}(r) - r \geq G_{\mathcal{O}}(s) - s$ *for* $r \geq s$.

3. $G_{\mathcal{O}}(r) \geq G_{\mathcal{O}}(1) + r - 1$ *for all* $r \geq 1$.

The same is true if we replace $G_{\mathcal{O}}$ *by* $g_{\mathcal{O}}$.

Proof. We show the claims about $G_{\mathcal{O}}$. The proofs for $g_{\mathcal{O}}$ are verbatim the same, except that every occurrence of "lattice" is replaced by "free lattice".

Now we explain that it is enough to show $G_{\mathcal{O}}(r+1) \geq G_{\mathcal{O}}(r) + 1$ for every r. This inequality immediately gives (1). Further, $G_{\mathcal{O}}(r+1) \geq G_{\mathcal{O}}(r) + 1$ can be rearranged as $G_{\mathcal{O}}(r+1) - (r+1) \geq G_{\mathcal{O}}(r) - r$, and recursively, we get (2). Finally, letting $s = 1$ in (2) gives us (3).

To show $G_{\mathcal{O}}(r+1) \geq G_{\mathcal{O}}(r) + 1$, we shall use the fact that the only way to express 1 as a sum of squares in $\mathcal{O}$ is $1 = (\pm 1)^2$. (Generally, 1 can never be written as a sum of two totally positive algebraic integers.)

Let $G = G_{\mathcal{O}}(r)$ and take any lattice L (with quadratic map Q) of rank r such that $L \to I_N$ for some $N \in \mathbb{N}$, but $L \not\to I_{G-1}$. Consider now the lattice $L \perp \langle 1 \rangle$ of rank $r+1$. Clearly $L \perp \langle 1 \rangle \to I_{N+1}$. We claim that $L \perp \langle 1 \rangle \not\to I_G$.

Consider any representation $\iota : L \perp \langle 1 \rangle \to I_G$. Denote by $\mathbf{f}$ a generating vector of $\langle 1 \rangle$. Then $\iota(\mathbf{f})$ is a vector in I_G such that $Q(\iota(\mathbf{f})) = 1$. The only such vectors are $\pm$ vectors of the standard basis, as $1 = (\pm 1)^2$ is the only way to write 1 as a sum of squares. Let us say $\iota(\mathbf{f}) = \mathbf{e}_G$. Then ι maps L into the orthogonal complement of $\mathbf{e}_G$. This is a representation $L \to I_{G-1}$ and thus a contradiction. □

The following proposition may not be true for non-maximal orders, since it significantly uses the properties of lattices over Dedekind domains.

Proposition 4.3.2. *For any Dedekind domain* R *we have* $g_R(r) \leq G_R(r) \leq g_R(r+1)$.

Proof. The first inequality is obvious from the definition. For the second, denote $g = g_R(r+1)$ and consider any L of rank r which is a sublattice of I_N for some $N \in \mathbb{N}$. By Lemma 4.2.2, it is enough to show that $L \to I_g$.

By assumption, L is a sublattice of I_N of rank r:

$$L = R\mathbf{x}_1 + \cdots + R\mathbf{x}_{r-1} + \mathfrak{a}^{-1}\mathbf{x}_r$$

with $\mathbf{x}_j \in I_N$ and $\mathfrak{a}$ an integral ideal in R.

Denote $A = \mathfrak{a}I_1$; clearly it is a unary sublattice of I_1. Put $L_1 = L \perp A$; this is a quadratic sublattice of I_{N+1}. It is a free lattice of rank $r+1$, so by the definition of g we have $L_1 \to I_g$. Restriction to L yields a representation $L \to I_g$. □

Assuming Theorem 4.1.2 (3), i.e. the inequality $g_{\mathcal{O}}(r) \leq G_{\mathcal{O}_F}(rd)$, this yields the second part of Theorem 4.1.2 (1) as a simple corollary:

Corollary 4.3.3. *Let* $K \supset F$ *be number fields,* $[K : F] = d$*, and* $\mathcal{O}$ *be any order in* K *containing* $\mathcal{O}_F$*. Then* $g_{\mathcal{O}}(r) \leq g_{\mathcal{O}_F}(rd+1)$.

Proof. Theorem 4.1.2 (3) together with the previous proposition implies $g_{\mathcal{O}}(r) \leq G_{\mathcal{O}_F}(rd) \leq g_{\mathcal{O}_F}(rd+1)$. □

Let us stress once again that in most extensions K/F, this is the best (to our knowledge) available inequality between $g_{\mathcal{O}_K}(\,\cdot\,)$ and $g_{\mathcal{O}_F}(\,\cdot\,)$ since $\mathcal{O}_K$ usually does not have an integral basis over $\mathcal{O}_F$, which makes it impossible to use the first part of Theorem 4.1.2 (1).

4.4 The main proof

In this section we prove the key result of this paper – the inequalities between the g-, resp. G-invariants of a ring and its subring. This theorem implies most of the other contents of this article. Since the proof does not use any number theoretic properties, we formulate it more generally for commutative rings with unity and for Dedekind domains. Namely, we prove the following:

Theorem 4.4.1. *Let $R \supset S$ be commutative rings with unity.*

1. *If R is generated by d elements as an S-module, then $g_R(r) \leq g_S(rd)$.*
2. *If R, S are Dedekind domains and R is a torsion-free S-module of rank d, then $G_R(r) \leq G_S(rd)$.*
3. *If S is a Dedekind domain and R is a torsion-free S-module of rank d, then $g_R(r) \leq G_S(rd)$.*

Although we formulate it as one theorem and the main idea behind the proofs is the same, the three statements are independent and neither of them implies any of the others. If we replace Dedekind domains by $\mathcal{O}_K$ for a number field K and rings by (not necessarily maximal) orders $\mathcal{O}$, we obtain precisely the main Theorem 4.1.2, almost word for word.

We start with part (1); its proof could be written purely in terms of polynomials, but we instead choose the equivalent language of free quadratic lattices.

Proof of Theorem 4.4.1 (1). By assumption, we have $R = S\beta_1 + \cdots + S\beta_d$ for some $\beta_i \in R$. We let $g = g_S(rd)$. Consider a free lattice L over R of rank r for which there is a representation $\iota : L \to I_N$; our aim is to prove that $L \to I_g$.

Denote the basis vectors of L by $\mathbf{x}_1, \ldots, \mathbf{x}_r$. Now, $\iota(L) = \sum_{j \leq r} R\iota(\mathbf{x}_j)$ is a submodule of I_N over R. Every $\iota(\mathbf{x}_j)$ is an element of R^N, so by assumption we can write $\iota(\mathbf{x}_j) = \mathbf{f}_1^{(j)}\beta_1 + \cdots + \mathbf{f}_d^{(j)}\beta_d$ with $\mathbf{f}_i^{(j)} \in S^N$. (Since R is not necessarily a free S-module, these "vectors of coefficients" $\mathbf{f}_i^{(j)}$ are not unique, but they do exist.)

Consider now the quadratic S-module

$$M = \sum_{i \leq d} \sum_{j \leq r} S\mathbf{f}_i^{(j)},$$

which is a quadratic submodule of I_N over S generated by rd elements. If it were free, then by definition of g it is represented by I_g over S; however, this is in general not the case. Thus, let us consider the following auxiliary free quadratic S-lattice $\widetilde{M}$ of rank rd: The underlying S-module is S^{rd} and we denote its basis by $\mathbf{e}_{ij}$. The quadratic map $\widetilde{Q}$ is defined as follows:

$$\widetilde{Q}\Big(\sum_{i,j} \alpha_{ij}\mathbf{e}_{ij}\Big) = Q_M\Big(\sum_{i,j} \alpha_{ij}\mathbf{f}_i^{(j)}\Big),$$

where Q_M is the quadratic map on M. Not only is $\widetilde{Q}$ a well-defined quadratic map; it was defined in such a way that the linear map $\widetilde{M} \to M$ given by $\mathbf{e}_{ij} \mapsto \mathbf{f}_i^{(j)}$ is a representation. Since M is a subset of I_N, this yields a representation $\widetilde{M} \to I_N$ over S. Thus, by the definition of g, $\widetilde{M} \to I_g$ over S. If we extend scalars by taking the tensor product, we get $R \otimes_S \widetilde{M} \to R \otimes_S I_g$, which is usually written as "$R \otimes_S \widetilde{M} \to I_g$ over R".

In the lattice $R \otimes_S \widetilde{M}$ one can find the vectors $\mathbf{y}_j = \mathbf{e}_{1j}\beta_1 + \cdots + \mathbf{e}_{dj}\beta_d$. Consider now the R-linear map $L \to R \otimes_S \widetilde{M}$ given by $\mathbf{x}_j \mapsto \mathbf{y}_j$. One easily sees that it respects the quadratic map and thus it is a representation. Hence we have $L \to R \otimes_S \widetilde{M} \to I_g$, which concludes the proof. □

We note that the proof does not require the quadratic structure on the modules; it would work just as well for modules equipped with a different map type. In particular, a statement analogous to Theorem 4.4.1 holds for representing cubic forms by sums of cubes, etc.

The quadratic structure does not play the main role in the proofs of the second and third parts of Theorem 4.4.1, either. Instead, most of the work consists of handling the underlying S-modules and R-modules seen as subsets of $(\mathrm{Quot}(S))^n$ or $(\mathrm{Quot}(S)\cdot R)^n$ (where $\mathrm{Quot}(\cdot)$ means the quotient field) and showing that they are in fact subsets of S^n or R^n. Note that for an ideal $\mathfrak{a}\subset S$ we write $(\mathfrak{a}S)^n$ to mean n-dimensional vectors with coordinates in $\mathfrak{a}$; this is to avoid confusion with powers of ideals.

The definitions of lattices in part (2) are more complicated than in (1) since one has to work with non-principal ideals. On the other hand, we can avoid using the auxiliary lattice $\widetilde{M}$ thanks to Lemma 4.2.2.

Proof of Theorem 4.4.1 (2). Consider a quadratic R-lattice L of rank r which is a sublattice of I_N for some $N\in\mathbb{N}$. By Lemma 4.2.2, it is enough to show $L\to I_G$ over R, where $G=G_S(rd)$. By Lemma 4.2.4 (1), $L=R\mathbf{x}_1+\dots+R\mathbf{x}_{r-1}+\mathfrak{A}^{-1}\mathbf{x}_r$, where each $\mathbf{x}_i$ is an element of R^N and $\mathfrak{A}$ is an integral ideal. Observe that $\mathfrak{A}^{-1}\mathbf{x}_r\subset L$ implies $\mathbf{x}_r\in(\mathfrak{A}R)^N$.

Lemma 4.2.4 (2) provides us with the pseudo-bases $(\beta_i)_{i\le d}$ of R and $(\gamma_i)_{i\le d}$ of $\mathfrak{A}$, together with integral ideals $\mathfrak{a}$ and $\mathfrak{b}$ in S, such that

$$\begin{aligned} R &= S\beta_1+\dots+S\beta_{d-1}+\mathfrak{a}^{-1}\beta_d \qquad \text{with } \beta_i\in R,\\ \mathfrak{A} &= S\gamma_1+\dots+S\gamma_{d-1}+\mathfrak{b}^{-1}\gamma_d \qquad \text{with } \gamma_i\in\mathfrak{A}. \end{aligned}$$

Now define the vectors $\mathbf{f}_i^{(j)}\in(\mathrm{Quot}(S))^N$ as the coordinates of $\mathbf{x}_j$ with respect to these pseudo-bases:

$$\begin{aligned} \mathbf{x}_j &= \mathbf{f}_1^{(j)}\beta_1+\dots+\mathbf{f}_d^{(j)}\beta_d \qquad \text{for } 1\le j\le r-1;\\ \mathbf{x}_r &= \mathbf{f}_1^{(r)}\gamma_1+\dots+\mathbf{f}_d^{(r)}\gamma_d. \end{aligned}$$

If $i\ne d$, then $\mathbf{f}_i^{(j)}\in S^N$. For $j\ne r$ one has $\mathbf{f}_d^{(j)}\in(\mathfrak{a}^{-1}S)^N$ and in the last case $\mathbf{f}_d^{(r)}\in(\mathfrak{b}^{-1}S)^N$. Therefore $M=\sum_{i<d,j\le r}S\mathbf{f}_i^{(j)}+\sum_{j<r}\mathfrak{a}\mathbf{f}_d^{(j)}+\mathfrak{b}\mathbf{f}_d^{(r)}$ is a well-defined sublattice of S^N of rank at most rd. We can also understand it as a quadratic sublattice of I_N over S. By the definition of $G=G_S(rd)$ (or, strictly speaking, by Lemma 4.2.2), it is represented by I_G over S.

Since $M\to I_G$ over S, we get $R\otimes_S M\to I_G$ over R. On the other hand, one can explicitly write

$$R\otimes_S M=\sum_{i<d,\,j\le r}R\mathbf{f}_i^{(j)}+\sum_{j<r}(R\mathfrak{a})\mathbf{f}_d^{(j)}+(R\mathfrak{b})\mathbf{f}_d^{(r)}.$$

That is, M was defined in such a way that $\mathbf{x}_j\in R\otimes_S M$ for $j\le r-1$ and $\mathfrak{A}^{-1}\mathbf{x}_r\subset R\otimes_S M$ – to see this, observe $\beta_d\in R\mathfrak{a}$, $\mathfrak{A}^{-1}\gamma_i\subset R$ and $\mathfrak{A}^{-1}\gamma_d\subset R\mathfrak{b}$. In particular, L is a sublattice of (and thus represented by) $R\otimes_S M$. Composition of these two representations yields $L\to R\otimes_S M\to I_G$ over R. This is the desired representation $L\to I_G$. □

The proof of part (3) is almost the same as for (2) and the technical details are in fact slightly simpler. Therefore our explanations will be less detailed.

Proof of Theorem 4.4.1 (3). By assumption, we have $R=S\beta_1+\dots+S\beta_{d-1}+\mathfrak{a}^{-1}\beta_d$, where each $\beta_i\in R$ and $\mathfrak{a}$ is an integral ideal in S. Clearly, $\mathfrak{a}^{-1}\beta_d\subset R$.

Denote $G=G_S(rd)$. Consider any free R-lattice L in r variables which is represented by I_N. We need to show that L is represented by I_G over R. Denote by L' the quadratic R-submodule of I_N which is the image of L under the representation $L\to I_N$. It is generated by r vectors, say $L'=R\mathbf{x}_1+\dots+R\mathbf{x}_r$, where all $\mathbf{x}_j\in R^N$. Since $L\to L'$, it suffices to show that $L'\to I_G$.

Denote $\mathbf{x}_j = \mathbf{f}_1^{(j)}\beta_1 + \cdots + \mathbf{f}_{d-1}^{(j)}\beta_{d-1} + \mathbf{f}_d^{(j)}\beta_d$. It is important to note that while $\mathbf{f}_i^{(j)} \in S^N$ for $1 \le i \le d-1$ (and $1 \le j \le r$), one only gets $\mathbf{f}_d^{(j)} \in (\mathfrak{a}^{-1}S)^N$.

Define the S-lattice $M = \sum_{j\le r}\left(S\mathbf{f}_1^{(j)} + \cdots + S\mathbf{f}_{d-1}^{(j)} + \mathfrak{a}\mathbf{f}_d^{(j)}\right)$ of rank at most rd. We claim that it is a sublattice of I_N over S; that is, it contains only vectors from S^N. This only has to be checked for the last summand from each bracket; and there, indeed, $\mathfrak{a}\cdot\mathbf{f}_d^{(j)} \subset \mathfrak{a}\cdot(\mathfrak{a}^{-1}S)^N \subset S^N$. Therefore, M is a well-defined quadratic sublattice of I_N. By the definition of $G = G_S(rd)$ (or more precisely by Lemma 4.2.2), it is represented by I_G over S.

Since $M \to I_G$ over S, we get $R\otimes_S M \to I_G$ over R. We also claim $\mathbf{x}_j \in R\otimes_S M$ for every j; to see this, remember $\beta_d \in R\mathfrak{a}$. So, L' is a sublattice of (and thus represented by) $R\otimes_S M$. Composition of these two representations yields $L' \to R\otimes_S M \to I_G$ over R. This is the desired representation $L' \to I_G$. □

4.5 $G(2)$ for quadratic rings of integers

While the definition of $g(r)$ may seem more straightforward than the definition of $G(r)$, we consider the latter to be the more useful and natural invariant. Perhaps it is not found in the literature simply because almost nothing nontrivial was known for any field of a class number other than 1 (see [Li2] for an example for Hermitian lattices). Now we can partly remedy this by deciding the $G(2)$-invariant of most real quadratic fields – that is, we prove Theorem 4.1.4.

Combining our inequalities, we are able to get not only an upper bound but in more than half cases also the lower bound:

Lemma 4.5.1. *Let $F = \mathbb{Q}(\sqrt{n})$ be a quadratic field, $n > 1$ square-free. Then:*

1. $G_{\mathcal{O}_F}(2) \le 7$.
2. *If $n \not\equiv 1 \pmod 4$, $n \ge 10$, then $G_{\mathcal{O}_F}(2) = 7$.*

Proof. The first statement is just the inequality $G_{\mathcal{O}_F}(2) \le g_{\mathbb{Z}}(4) = 7$.

For the second, we need $7 \le G_{\mathcal{O}_F}(2)$. Pick any square-free $n_2 \ge 10$ coprime to n such that one of n, n_2 is 2 and the other 3 modulo 4. By [KRS, Thm. 5.3], the biquadratic field $K = \mathbb{Q}(\sqrt{n}, \sqrt{n_2})$ has $\mathcal{P}(\mathcal{O}_K) = 7$. The extension K/F is of degree 2, so Theorem 4.1.2 applies: $7 = \mathcal{P}(\mathcal{O}_K) \le G_{\mathcal{O}_F}(2)$. □

To prove Theorem 4.1.4, it remains to treat the fields $\mathbb{Q}(\sqrt{n})$ for $n = 6$, $n = 7$ and most importantly for $n \equiv 1 \pmod 4$. By a direct computation we get the following:

Lemma 4.5.2. *Biquadratic fields $K_1 = \mathbb{Q}(\sqrt{6}, \sqrt{7})$ and $K_2 = \mathbb{Q}(\sqrt{13}, \sqrt{15})$ have $\mathcal{P}(\mathcal{O}_{K_i}) = 7$. More specifically, the following elements are sums of seven but not of six squares in $\mathcal{O}_{K_i}$:*

- $\alpha_1 = 43 + \sqrt{6} - 8\sqrt{7} + \sqrt{7\cdot 6}$;
- $\alpha_2 = 114 + 15\sqrt{13} + 20\sqrt{15} + 6\sqrt{13\cdot 15}$.

Thus $G_{\mathcal{O}_F}(2) = g_{\mathcal{O}_F}(2) = 7$ for $F = \mathbb{Q}(\sqrt{n})$, $n = 6, 7, 13$.

Proof. As soon as we check that α_i is a sum of six but not seven squares (i.e. its length is 7), the rest is easy: $\mathcal{P}(\mathcal{O}_{K_i}) = 7$ will follow from the just obtained $\mathcal{P}(\mathcal{O}_{K_i}) \ge \ell(\alpha_i) = 7$ combined with the inequality $\mathcal{P}(\mathcal{O}_{K_i}) \le g_{\mathbb{Z}}(4) = 7$. After this, we also get $\mathcal{P}(\mathcal{O}_{K_i}) \le G_{\mathcal{O}_F}(2) \le g_{\mathbb{Z}}(4)$ for $[K_i : F] = 2$, so $G_{\mathcal{O}_F}(2) = 7$; and since all three quadratic fields have class number 1, we also have $g_{\mathcal{O}_F} = G_{\mathcal{O}_F}$.

So it remains to explain that α_i is a sum of seven but not of six squares in $\mathcal{O}_{K_i}$, which we computed using Magma [BCP]. □

On a side note, the lemma also yields $g_{\mathcal{O}_F}(2) = 7$ for $F = \mathbb{Q}(\sqrt{15})$: Although the class number is 2 and therefore the equality $g_{\mathcal{O}_F}(2) = G_{\mathcal{O}_F}(2)$ is not immediate, we have $\mathcal{O}_K = \mathbb{Z}[\sqrt{15}]\cdot 1 + \mathbb{Z}[\sqrt{15}]\cdot\frac{1+\sqrt{13}}{2}$, so $\mathcal{O}_K$ is a free $\mathcal{O}_F$-module, implying $7 = \mathcal{P}(\mathcal{O}_K) \le g_{\mathcal{O}_F}(2)$.

4.5.1 The case 1 mod 4

For $F = \mathbb{Q}(\sqrt{n})$, $n = 5$ we have Sasaki's result $G_{\mathcal{O}_F} = g_{\mathcal{O}_F}(2) = 5$. The case $n = 13$ was handled separately in Lemma 4.5.2. In this subsection we treat all the remaining real quadratic fields $\mathbb{Q}(\sqrt{n})$ with $n \equiv 1 \pmod 4$.

It is worth mentioning that the form φ in the following theorem was discovered by examining elements of length seven in real biquadratic fields $\mathbb{Q}(\sqrt{p}, \sqrt{n})$ for the first few values of n and for $p \not\equiv 1 \pmod 4$ coprime with n. Quite probably there are other forms with the same property.

Proposition 4.5.3. *If $F = \mathbb{Q}(\sqrt{n})$ for $n \geq 17$ square-free, $n \equiv 1 \pmod 4$, then $g_{\mathcal{O}_F}(2) \geq 7$. In particular, denote*

$$\begin{aligned}\varphi(X,Y) &= \left(7 + \left(\tfrac{1+\sqrt{n}}{2}\right)^2\right)X^2 + \left(\tfrac{5+\sqrt{n}}{2}X + Y\right)^2 + \left((5+\sqrt{n})X + \tfrac{1+\sqrt{n}}{2}Y\right)^2 \\ &= \frac{3n+77+26\sqrt{n}}{2}X^2 + (10+n+7\sqrt{n})XY + \frac{n+5+2\sqrt{n}}{4}Y^2.\end{aligned}$$

Then $\ell(\varphi) = 7$, i.e. φ is a sum of 7, but not of 6 squares of binary linear forms.

Proof. The fact that φ is a sum of seven squares is clear from the first representation, since $7 + \left(\frac{1+\sqrt{n}}{2}\right)^2$ is a sum of five squares. So it remains to show that φ is never a sum of six or less squares.

First we solve the cases $n \leq 53$. We define the biquadratic field $K = \mathbb{Q}(\sqrt{10}, \sqrt{n})$. One integral basis of K is $(1, \sqrt{10}, \frac{1+\sqrt{n}}{2}, \sqrt{10}\frac{1+\sqrt{n}}{2})$, so $\mathcal{O}_K = \mathcal{O}_F \cdot 1 + \mathcal{O}_F \cdot \sqrt{10}$. Instead of directly applying the inequality $\mathcal{P}(\mathcal{O}_K) \leq g_{\mathcal{O}_F}(2)$, we use the simple idea from its proof: Put $\alpha_{10} = \varphi(1, \sqrt{10})$. By definition, this is a sum of seven squares in $\mathcal{O}_K$; in fact, it is clear that $\ell_{\mathcal{O}_K}(\alpha_{10}) \leq \ell_{\mathcal{O}_F}(\varphi)$. By a direct computation (e.g. in Magma) as in Lemma 4.5.2, we easily check that $\ell_{\mathcal{O}_K}(\alpha_{10}) = 7$ for $n = 17$, 21, 29, 33, 37, 41 and 53. This means that $\ell_{\mathcal{O}_F}(\varphi) \geq 7$ in these cases.

Now we solve the cases $53 < n \leq 65$. The previous approach fails, since $\ell(\alpha_{10})$ turns out to be 5 for all three n in question. However, we can use the same trick with 10 replaced by 11: By the same direct computation we check that $\alpha_{11} = \varphi(1, \sqrt{11})$ has length 7 for $n = 57$, 61 and 65. (While for $n = 73$, this trick again fails, and, surprisingly, even replacing 11 by 14, 15, 19, 22, 23, 26, 30 or 31 is useless.)

Now comes the main part of the proof, for $n \geq 73$. Consider a representation of φ as a sum of squares of linear forms, i.e. $\varphi(X,Y) = \sum_i (x_i X + y_i Y)^2$ with $x_i, y_i \in \mathcal{O}_F$. By comparing the coefficients of Y^2 one gets $\sum y_i^2 = \frac{5+n}{4} + \frac{\sqrt{n}}{2}$. The number on the right decomposes uniquely as a sum of squares, namely as $(\pm 1)^2 + \left(\pm\frac{1+\sqrt{n}}{2}\right)^2$; therefore, after possibly transferring the signs to the x_i and reordering the terms, the decomposition must be of the form

$$\varphi(X,Y) = (x_1 X + Y)^2 + \left(x_2 X + \tfrac{1+\sqrt{n}}{2}Y\right)^2 + \sum_{i>2}(x_i X)^2.$$

Before we proceed, observe that it suffices to show that $x_1 = \frac{5+\sqrt{n}}{2}$ and $x_2 = 5 + \sqrt{n}$: Once this is proven, one has $\sum_{i>2} x_i^2 = 7 + \left(\frac{1+\sqrt{n}}{2}\right)^2$, which requires at least five squares in $\mathcal{O}_F$, see [Pe2, p. 161].

Comparing the coefficients of XY yields $x_1 + x_2\frac{1+\sqrt{n}}{2} = \frac{10+n+7\sqrt{n}}{2}$, which we rearrange as

$$x_1 = \frac{10+n+7\sqrt{n}}{2} - \frac{1+\sqrt{n}}{2}x_2. \tag{4.5.1}$$

This means that it only remains to show $x_2 = 5 + \sqrt{n}$.

Let us now focus on the equality $\frac{3n+77+26\sqrt{n}}{2} = \sum x_i^2 = \sum \left(\frac{a_i+b_i\sqrt{n}}{2}\right)^2$ where $a_i \equiv b_i \pmod 2$. It can equivalently be rewritten as a system of two Diophantine equations (with the above parity condition):

$$\sum a_i^2 + n\sum b_i^2 = 154 + 6n, \tag{4.5.2}$$

$$\sum a_i b_i = 26. \tag{4.5.3}$$

Looking at (4.5.3) modulo 4, we see that there must be a nonzero even number of indices i such that $a_i \equiv b_i \equiv 1 \pmod 2$. In particular, $\sum b_i^2$ is an even number. Also, $\sum a_i^2 \geq 2$.

We shall now prove that $\sum b_i^2 \leq 6$. If not, then $\sum b_i^2 \geq 8$, so (4.5.2) gives $2 + 8n \leq 154 + 6n$, a contradiction for $n \geq 77$. It remains to deal with $n = 73$. In this case, $\sum b_i^2 \geq 10$ is impossible, so we have $\sum b_i^2 = 8$; then $\sum a_i^2 = 8$ by (4.5.2). By Cauchy–Schwarz inequality, $|\sum a_i b_i| \leq \sqrt{8 \cdot 8} = 8$, which contradicts (4.5.3).

So we indeed have $\sum b_i^2 \leq 6$ for $n \geq 73$. In particular, $|b_i| \leq 2$ for every i.

Rewrite now (4.5.1) explicitly as $x_1 = (5 - \frac{a_2}{4} + n\frac{2-b_2}{4}) + \sqrt{n}(\frac{7}{2} - \frac{a_2+b_2}{4})$, i.e. $a_1 = 10 - \frac{a_2}{2} + n\frac{2-b_2}{2}$ and $b_1 = 7 - \frac{a_2+b_2}{2}$. Since $|b_1|, |b_2| \leq 2$, triangle inequality applied to the second equation gives $|a_2| \leq 14 + |b_2| + |2b_1| \leq 20$. Therefore, the first equation yields $a_1 \geq n\frac{2-b_2}{2}$.

We now show that $b_2 = 2$: If not, then $b_2 < 2$, so $a_1 \geq \frac{n}{2}$. However, plugging this in (4.5.2) yields $\frac{1}{4}n^2 \leq 154 + 6n$, which is a contradiction for $n \geq 40$.

Having proven $b_2 = 2$, we are almost done. It only remains to determine the even number a_2. Combining $\sum b_i^2 \leq 6$ with the fact that there are at least two indices i such that b_i is odd, one sees that necessarily $\sum b_i^2 = 6$. We have $b_1 = 6 - \frac{a_2}{2}$. Since $|b_1| \leq 1$ and a_2 is even, there are only three possibilities for a_2.

First assume $a_2 = 14$. Plugging $\sum b_i^2 = 6$ into (4.5.2), we get $\sum a_i^2 = 154$, so our value of a_2 is impossible.

The second option is $a_2 = 12$. In this case, $a_1 = 10 - \frac{12}{2} + n\frac{2-2}{2} = 4$, so $a_1^2 + a_2^2 = 16 + 144 = 160$, which again contradicts the equality $\sum a_i^2 = 154$.

The only remaining case is $a_2 = 10$. This means $x_2 = \frac{a_2+b_2\sqrt{n}}{2} = 5 + \sqrt{n}$, and we get $x_1 = \frac{5+\sqrt{n}}{2}$. Thus $(x_1X + y_1Y)^2$ and $(x_2X + y_2Y)^2$ are exactly the second and third term in the original definition of φ, and we already explained that the first term requires at least five more squares. □

Proof of Theorem 4.1.4. The upper bound $G_{\mathcal{O}_F}(2) \leq 7$ is in Lemma 4.5.1 (1). Part (2) of the same Lemma gives the lower bound $G_{\mathcal{O}_F}(2) \geq 7$ for $n \not\equiv 1 \pmod 4$, $n \geq 10$. For $n = 6, 7, 13$, the lower bound is contained in Lemma 4.5.2, and for the remaining $n \equiv 1 \pmod 4$ in Proposition 4.5.3. □

5. Pythagoras number of non-maximal orders in biquadratic fields

This chapter differs from the other parts of this thesis in the respect that it is not a separate paper. (It will form the basis of the planned paper [Kr2].) For this reason, it does not need a separate introduction, but instead uses the terminology and basic facts from Chapter 2.

In particular, bear in mind that by *biquadratic field* we automatically mean a totally real one, and that every biquadratic field K contains three square-free rational integers $t > s > m > 1$ which are squares in K. Further, remember that it can also be uniquely and conveniently described by the triple (m_0, s_0, t_0), where $m_0 = \gcd(s,t)$ etc.; then we have $m = s_0 t_0$ etc., $m_0 > s_0 > t_0$, and these three numbers are coprime and square-free (but t_0 can be 1; this happens exactly if m and s are coprime).

While the second chapter focused on $\mathcal{P}(\mathcal{O}_K)$ where K is a biquadratic field, in this chapter we study $\mathcal{P}(\mathcal{O})$ where $\mathcal{O} \subset \mathcal{O}_K$ is a non-maximal order. Recall that an order in K is any subring $\mathcal{O} \subset \mathcal{O}_K$ which has K as its field of fractions; this latter condition is equivalent to $\mathcal{O}$ being a free $\mathbb{Z}$-module of rank 4. Remember that the bound from [KY2] gives $\mathcal{P}(\mathcal{O}) \leq 7$, and although in this chapter we mostly aim to exhibit examples where this upper bound is attained, we also already know about infinitely many non-maximal biquadratic orders where the Pythagoras number is much lower:

Theorem. *Let $\mathcal{O}$ be a quartic order containing $\sqrt{2}$ or $\frac{1+\sqrt{5}}{2}$. Then $\mathcal{P}(\mathcal{O}) \leq 5$.*

To see this, observe that such an order contains either $S = \mathbb{Z}[\sqrt{2}]$ or $S = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$, and as these rings are principal ideal domains, $\mathcal{O}$ is a free S-module of rank 2. Thus the inequality is Proposition 2.7.5 combined with the facts that $g(2) = 5$ for both these rings [Sa2, HH].

Although part (2) of Theorem 4.1.2 generalises the inequality from Proposition 2.7.5 by no longer requiring that $\mathcal{O}$ be a free module, it is not useful in our particular case since by Theorem 4.1.4, even the improved upper bound is equal to 7 in all remaining cases with the possible exception of $\mathbb{Z}[\sqrt{3}]$. Thanks to the conjecture that $g_{\mathbb{Z}[\sqrt{3}]}(2) = 6$, it is safe to expect $\mathcal{P}(\mathcal{O}) \leq 6$ for all quartic orders containing $\sqrt{3}$.

This having been said, let us present the main result of this text, which was already announced in the second chapter:

Theorem 5.0.1. *Take three rational integers $M_0 > S_0 > T_0 \geq 5$ such that none of the products $T = M_0 S_0$, $S = M_0 T_0$ and $M = S_0 T_0$ is a square. Then $\mathcal{O} = \mathbb{Z}\,1 + \mathbb{Z}\sqrt{M} + \mathbb{Z}\sqrt{S} + \mathbb{Z}\sqrt{T}$ is a biquadratic order and $\mathcal{P}(\mathcal{O}) = 7$.*

In particular, if we put $\alpha = 7 + (1+\sqrt{M})^2 + (1+\sqrt{S})^2 + (1+\sqrt{T})^2$, then $\ell(\alpha) = 7$.

This will indeed prove Theorem 2.1.5 (which states that every biquadratic field contains infinitely many orders with Pythagoras number 7) since by the results of the next section, every biquadratic order contains a proper suborder of the required form. (A formal proof of Theorem 2.1.5 is given at the end of Section 5.2.)

Theorem 5.0.1 may be the simplest of our results about non-maximal orders, yet it is not the only one. The next section explains that every quartic order of the shape $\mathbb{Z} + \mathbb{Z}\sqrt{n_1} + \mathbb{Z}\sqrt{n_2} + \mathbb{Z}\sqrt{n_3}$ corresponds to the construction above. Such orders shall be called *basic*. Proposition 5.2.1 shows that if the condition $T_0 \geq 5$ is violated, then actually $\ell(\alpha) \leq 4$; thus, we have fully determined the basic orders $\mathcal{O}$ in which this specific α has length 7. However, $\mathcal{P}(\mathcal{O}) = 7$ can often be proved for basic orders even when $T_0 \leq 4$. In particular, if $T_0 \neq 1$ and we replace α by

$\alpha' = 7 + (2+\sqrt{M})^2 + (1+\sqrt{S})^2 + (1+\sqrt{T})^2$, we usually still get $\ell(\alpha') = 7$ and thus $\mathcal{P}(\mathcal{O}) = 7$, see Theorem 5.4.2. A more general result, Theorem 5.3.5, shows that in basic orders, there are often many other elements of length 7; it introduces a family of such likely elements, where α and α' are only two of the infinitely many members.

We also get the following strengthening of Theorem 2.1.5:

Corollary 5.0.2. *For every $k \in \mathbb{N}$, every real biquadratic field contains infinitely many orders $\mathcal{O}$ where there are at least k elements of length 7, distinct as elements of $\mathcal{O}^\times/(\mathcal{O}^\times)^2$.*

This may be surprising, as at least for maximal orders, [HKK] shows that there are only finitely many elements with $\ell(\,\cdot\,) > 5$. However, while we expect this result to carry over to non-maximal orders as well, there is probably no reason why in a fixed $\mathcal{O}_K$, the number of elements of large length in $\mathcal{O}$ should not grow with the index $[\mathcal{O}_K : \mathcal{O}]$.

In fact, this Corollary 5.0.2 follows from Theorem 5.3.7 which claims even more: Among all basic orders, the orders with less than k elements of length 7 have in a certain specific sense density 0.

5.1 Basic properties of basic orders

Handling general non-maximal orders is quite difficult; indeed, it is not even so easy to describe all orders which lie in a given number field. In this text we treat almost exclusively a particularly well-behaved family of non-maximal orders in biquadratic fields which are in some respects easier to work with than the full rings of integers. Because their main property is the fact that they have a nice integral basis, we shall call them *basic orders* for the purpose of this text. Although they are quite special, it is still a rich family – we shall see that every biquadratic field and even every biquadratic order contains infinitely many basic orders.

Let $\mathcal{O}$ be an order in a biquadratic field K. We say that $\mathcal{O}$ is *basic* if it is of the form

$$\mathcal{O} = \mathbb{Z}\,1 + \mathbb{Z}\sqrt{M} + \mathbb{Z}\sqrt{S} + \mathbb{Z}\sqrt{T}$$

for some rational integers $T > S > M > 1$. Be careful, by far not every set of the given form is closed under multiplication; in Proposition 5.1.5 we shall see exactly which condition must be imposed upon M, S, T to ensure that the resulting set is indeed an order. Also, to obtain an order, the $\mathbb{Z}$-module must have rank 4; in other words, $1, \sqrt{M}, \sqrt{S}, \sqrt{T}$ must be linearly independent over $\mathbb{Q}$.

Observation 5.1.1. Let $M, S, T > 1$ be three distinct rational integers and K a biquadratic field, with m, s, t bearing the usual meaning. Then the following are equivalent:

1. The elements $1, \sqrt{M}, \sqrt{S}, \sqrt{T}$ lie in K and are linearly independent over $\mathbb{Q}$.
2. There exist positive integers a, b, c so that $\{M, S, T\} = \{a^2 m, b^2 s, c^2 t\}$.

Proof. This statement is just a variation on the well-known fact that m, s, t are the only square-free integers which are squares in K, and that $1, \sqrt{m}, \sqrt{s}, \sqrt{t}$ is a basis of K over $\mathbb{Q}$. □

So now we see that a basic order has an integral basis of the form $1, a\sqrt{m}, b\sqrt{s}, c\sqrt{t}$. If we put $a = b = c = 1$, we clearly get an order, since $\sqrt{m}\sqrt{s} = t_0\sqrt{t}$ is a multiple of $\sqrt{t}$ etc. This is the maximal basic order contained in $\mathcal{O}_K$; it has index 2, 4 or 16 in $\mathcal{O}_K$ depending on whether K is of type (B1), (B2,3), or (B4). To prove that in fact, every order contains a maximal basic order, a small observation is needed:

Lemma 5.1.2. *Let $\mathcal{O} \subset K = \mathbb{Q}(\sqrt{m}, \sqrt{s})$ be any order. There exists a unique positive integer k_m such that $k_m\sqrt{m} \in \mathcal{O}$ and if $n\sqrt{m} \in \mathcal{O}$, then $k_m \mid n$. Analogously we can define k_s and k_t.*

Proof. It suffices to prove that $\mathcal{O}$ contains some multiple of $\sqrt{m}$, $\sqrt{s}$, $\sqrt{t}$; the existence of a minimal choice is then due to the fact that $\mathbb{Z}$ is a PID. But this is clear: If we denote $n = [\mathcal{O}_K : \mathcal{O}]$, then $n\sqrt{m}, n\sqrt{s}, n\sqrt{t} \in \mathcal{O}$. Indeed, $n\mathcal{O}_K \subset \mathcal{O}$, since n is the order of the factorgroup. □

Proposition 5.1.3. *Let $\mathcal{O}$ be any order in a biquadratic field K and k_m, k_s, k_t be as in the previous lemma. Then*

$$\mathcal{O}_{\mathrm{b}} := \mathbb{Z}\,1 + \mathbb{Z}\sqrt{k_m^2 m} + \mathbb{Z}\sqrt{k_s^2 s} + \mathbb{Z}\sqrt{k_t^2 t} \subset \mathcal{O}$$

is a basic order; moreover, it contains every basic order contained in $\mathcal{O}$.

Proof. From Observation 5.1.1 it is clear that $\mathcal{O}_{\mathrm{b}}$ has rank 4 as a $\mathbb{Z}$-module. To check that it is closed under multiplication, it suffices to look at the integral basis. We exploit the previous statement: For example, $\sqrt{k_m^2 m}\sqrt{k_s^2 s} = k_m k_s t_0 \sqrt{t}$ lies in $\mathcal{O} \cdot \mathcal{O} \subset \mathcal{O}$, hence k_t divides $k_m k_s t_0$ and the product belongs to $\mathcal{O}_{\mathrm{b}}$. Thus $\mathcal{O}_{\mathrm{b}}$ is indeed an order. The facts that it is basic and that it contains every other basic suborder of $\mathcal{O}$ are immediate. □

Let us fix the notation $1, \sqrt{M}, \sqrt{S}, \sqrt{T}$ for the integral basis of a basic order such that $M < S < T$. (Note that we may have e.g. $M = t$, $S = 20^2 s$, $T = 20^2 m$, see also Example 5.1.6.) We shall see that the triple (M, S, T) has very similar properties to (m, s, t) with the exception that M, S, T are not square-free and their decomposition into M_0, S_0, T_0 is neither square-free nor coprime:

Proposition 5.1.4. *Let $\mathcal{O} = \mathbb{Z}\,1 + \mathbb{Z}\sqrt{M} + \mathbb{Z}\sqrt{S} + \mathbb{Z}\sqrt{T}$ be a basic order. Then we can write*

$$M = S_0 T_0, \quad S = M_0 T_0, \quad T = M_0 S_0$$

for unique $M_0, S_0, T_0 \in \mathbb{N}$; furthermore it holds that

$$\sqrt{M}\sqrt{S} = T_0\sqrt{T}, \quad \sqrt{M}\sqrt{T} = S_0\sqrt{S}, \quad \sqrt{S}\sqrt{T} = T_0\sqrt{M}.$$

Proof. The latter three equalities follow immediately from the earlier ones. But more surprisingly, we can obtain the earlier from the latter: By multiplying the fouth and fifth equality, we get $M\sqrt{ST} = S_0 T_0 \sqrt{ST}$, which yields $M = S_0 T_0$. Analogously we obtain $S = M_0 T_0$ and $T = S_0 T_0$.

Thus it suffices to prove that $\sqrt{M}\sqrt{S}$ is an integral multiple of $\sqrt{T}$ etc.; this will provide the definition of M_0, S_0, T_0 and ensure that the latter equalities hold, proving the proposition. Now, we have $\sqrt{M}\sqrt{S} \in \mathbb{Q}\sqrt{T}$ owing to the fact that $\sqrt{M}, \sqrt{S}, \sqrt{T}$ are in some order rational multiples of $\sqrt{m}, \sqrt{s}, \sqrt{t}$ (where a product of two elements gives a rational multiple of the remaining one). As $\mathbb{Q}\sqrt{T} \cap \mathcal{O} = \mathbb{Z}\sqrt{T}$, we see that $\sqrt{M}\sqrt{S}$ is indeed an integral multiple of $\sqrt{T}$. □

In fact, we can forget about the field K and the maximal order $\mathcal{O}_K$ and define a basic order directly as a ring:

Proposition 5.1.5. *Let $1 < T_0 < S_0 < M_0$ be such that none of the products $M_0 S_0, M_0 T_0, S_0 T_0$ is a square. Then we can put $M = S_0 T_0$, $S = M_0 T_0$, $T = M_0 S_0$ and obtain a basic biquadratic order*

$$\mathcal{O} = \mathbb{Z}\,1 + \mathbb{Z}\sqrt{M} + \mathbb{Z}\sqrt{S} + \mathbb{Z}\sqrt{T}.$$

Vice versa, every basic order in any biquadratic field corresponds to such a triple (T_0, S_0, M_0).

Proof. The 'vice versa' direction is contained in Proposition 5.1.4. As for the other, one routinely checks that $\mathcal{O}$ is closed under multiplication, thus a ring. Further, the field $K = \mathbb{Q}(\sqrt{M}, \sqrt{S})$ is biquadratic since $\sqrt{M}$ and $\sqrt{S}$ are linearly independent over $\mathbb{Q}$ (as $MS = T_0^2 M_0 S_0$ is not a square). Finally, $\sqrt{T} \in K$ since $\sqrt{T} = \sqrt{M_0 S_0} = \frac{1}{T_0}\sqrt{M_0 T_0}\sqrt{S_0 T_0} \in K$. Hence $\mathcal{O} \subset K$. □

Notice that the numbers M_0, S_0, T_0 need not be square-free, neither are they necessarily coprime; one of them may be 1 or a square.

Example 5.1.6. If we put

$$\begin{aligned} M_0 &= 2^4 \cdot 3 \cdot 5^2 \cdot 7^3 \cdot 11^7, \\ S_0 &= 2 \cdot 3^4 \cdot 5^3 \cdot 7 \cdot 11^7, \\ T_0 &= 3^2 \cdot 5 \cdot 7^4 \cdot 11^7, \end{aligned}$$

we obtain

$$\begin{aligned} M &= 2 \cdot 3^6 \cdot 5^4 \cdot 7^5 \cdot 11^{14}, \\ S &= 2^4 \cdot 3^3 \cdot 5^3 \cdot 7^7 \cdot 11^{14}, \\ T &= 2^5 \cdot 3^5 \cdot 5^5 \cdot 7^4 \cdot 11^{14}. \end{aligned}$$

The respective square-free parts of M, S, T are $m = 2 \cdot 7$, $t = 3 \cdot 5 \cdot 7$, $s = 2 \cdot 3 \cdot 5$, so the basic order with integral basis $(1, \sqrt{M}, \sqrt{S}, \sqrt{T})$ lies in $\mathbb{Q}(\sqrt{14}, \sqrt{30})$.

To summarise the results of this section: We have introduced basic orders as sets of the form $\mathbb{Z} + \mathbb{Z}\sqrt{M} + \mathbb{Z}\sqrt{S} + \mathbb{Z}\sqrt{T}$ which are closed under multiplication and have rank 4 as $\mathbb{Z}$-modules; in Proposition 5.1.5 we have shown that these conditions are equivalent to the fact that M, S, T can be decomposed as $M = S_0 T_0$ etc. and none of them is a square; by Proposition 5.1.4 this is the same as saying that $\sqrt{M}\sqrt{S} \in \mathbb{N}\sqrt{T}$ etc. and none of M, S, T is a square. Also, as we assume $T > S > M > 1$, we have $M_0 > S_0 > T_0 \geq 1$. Proposition 5.1.3 ensures that every biquadratic order contains a basic order which is maximal with respect to inclusion.

5.2 The first theorem

The aim of this section is proving Theorem 5.0.1, namely: In a basic order where $T_0 \geq 5$, the element $\alpha = 7 + (1 + \sqrt{M})^2 + (1 + \sqrt{S})^2 + (1 + \sqrt{T})^2$ has $\ell(\alpha) = 7$. Before we prove this result, we shall first see that this is the limit of this approach:

Proposition 5.2.1. *Suppose that $\mathcal{O}$ is a basic order with $T_0 \leq 4$. Then the α defined above is a sum of at most four squares, namely*

$$\alpha = \left(1 + \sqrt{M} + \sqrt{S}\right)^2 + \left((1 - T_0) + \sqrt{T}\right)^2 + \underbrace{9 - (1 - T_0)^2}_{\square + \square},$$

where $9 - (1 - T_0)^2$ is equal to $9 = 3^2$, $8 = 2^2 + 2^2$, $5 = 1^2 + 2^2$ or 0.

Proof. It is obvious after remembering that $\sqrt{MS} = T_0\sqrt{T}$:

$$\begin{aligned} \text{RHS} &= 1 + M + S + 2\sqrt{M} + 2\sqrt{S} + 2\sqrt{MS} + (1 - T_0)^2 + 2(1 - T_0)\sqrt{T} + T + 9 - (1 - T_0)^2 \\ &= 1 + M + S + 2\sqrt{M} + 2\sqrt{S} + 2T_0\sqrt{T} + 2\sqrt{T} - 2T_0\sqrt{T} + T + 9 \\ &= 10 + M + S + T + 2\sqrt{M} + 2\sqrt{S} + 2\sqrt{T} \\ &= \alpha. \end{aligned}$$

□

Now that we have seen the limitations, we will spend this section proving Theorem 5.0.1 which covers all the remaining cases. First note that 7 is a sum of four squares, so $\ell(\alpha) \leq 7$. As usual, the main task is to show that it is impossible to use less than seven squares. Throughout the section, let us suppose that $\alpha = \sum_{i=1}^{n} x_i^2$ for an as yet unknown number of squares n, and denote $x_i = a_i + b_i\sqrt{M} + c_i\sqrt{S} + d_i\sqrt{T}$. Then

$$x_i^2 = (a_i^2 + b_i^2 M + c_i^2 S + d_i^2 T) + 2(a_i b_i + c_i d_i M_0)\sqrt{M} + 2(a_i c_i + b_i d_i S_0)\sqrt{S} + 2(a_i d_i + b_i c_i T_0)\sqrt{T}.$$

Comparing this with α, we obtain the following equalities:

$$\begin{aligned} 10 + M + S + T &= \sum_{i=1}^{n} (a_i^2 + b_i^2 M + c_i^2 S + d_i^2 T) \\ 1 &= \sum_{i=1}^{n} a_i b_i + M_0 \sum_{i=1}^{n} c_i d_i \\ 1 &= \sum_{i=1}^{n} a_i c_i + S_0 \sum_{i=1}^{n} b_i d_i \\ 1 &= \sum_{i=1}^{n} a_i d_i + T_0 \sum_{i=1}^{n} b_i c_i \end{aligned}$$

Let us focus on the second equality. The crucial point of the whole proof is:

$$1 \equiv \sum_{i=1}^{n} a_i b_i \pmod{M_0} \quad \text{and } M_0 \neq 1,$$

hence at least one pair of (a_i, b_i) is simultaneously nonzero. By applying the same to the third and fourth equation, respectively, we arrive at the following:

Observation 5.2.2. There are indices (unfortunately not necessarily different) j, k, l such that $a_j b_j \neq 0$, $a_k c_k \neq 0$ and $a_l d_l \neq 0$. Thus e.g. $a_j^2 + b_j^2 M \geq 1 + M$.

If we knew that j, k, l are pairwise different, the rest would be immediate, as one easily checks. As it is, the proof still requires a bit of effort:

We already know that $b_j^2 \geq 1$, $c_k^2 \geq 1$, $d_l^2 \geq 1$ and $a_j^2 \geq 1$ (this may or may not be the same coefficient as a_k and a_l). Thus, step by step, the first equality yields:

$$\begin{aligned} 10 + M + S + T &= a_j^2 + b_j^2 M + c_k^2 S + d_l^2 T + \sum_{i \neq j} a_i^2 + \sum_{i \neq j} b_i^2 M + \sum_{i \neq k} c_i^2 S + \sum_{i \neq l} d_i^2 T \\ 10 + M + S + T &\geq 1 + M + S + T + \sum_{i \neq j} a_i^2 + \sum_{i \neq j} b_i^2 M + \sum_{i \neq k} c_i^2 S + \sum_{i \neq l} d_i^2 T \\ 9 &\geq \sum_{i \neq j} a_i^2 + \sum_{i \neq j} b_i^2 M + \sum_{i \neq k} c_i^2 S + \sum_{i \neq l} d_i^2 T \end{aligned}$$

This is almost the goal. Since $T > S > M = S_0 T_0 \geq 6 \cdot 5 > 9$, the last inequality immediately proves that the last three sums must be zero, i.e. $b_i = 0$ for $i \neq j$, $c_i = 0$ for $i \neq k$ and $d_i = 0$ for $i \neq l$. So, in fact, all the summands except for x_j, x_k and x_l are squares of natural integers, i.e. only numbers $1, 4$ and 9.

Also, it is obvious that $|b_j| = |c_k| = |d_l| = 1$. Let us summarise what we have so far: For each i we have $|a_i| \leq 3$. Among the b_i's, there is exactly one nonzero element and it is $b_j = \pm 1$; similarly the only nonzero c_i is $c_k = \pm 1$ and the only nonzero d_i is $d_l = \pm 1$.

From this we draw two conclusions: All the products $a_i b_i$ are 0 except for $a_j b_j = \pm a_j$. Similarly, among the products $c_i d_i$, there is at most one nonzero value; this value is $c_k d_k$ and it is nonzero if and only if $d_k \neq 0$, i.e. $k = l$. With these two pieces of information in mind, the second equality turns into

$$\begin{aligned} 1 &= \sum_{i=1}^{n} a_i b_i + M_0 \sum_{i=1}^{n} c_i d_i \\ 1 &= a_j b_j + M_0 c_k d_k \\ 1 &= \pm a_j + M_0 c_k d_k \\ |1 \mp a_j| &= M_0 |c_k d_k|. \end{aligned}$$

Suppose now that $c_k d_k \neq 0$ (which is equivalent to $l = k$). Then the right-hand side is at least $M_0 \geq 5$. However, this is a contradiction since the left-hand side is at most $|1 + 3| = 4$.

Thus we have proved that $k \neq l$ and $a_j b_j = 1$. By symmetry, j, k, l are pairwise different and $a_j b_j = a_k c_k = a_l d_l = 1$, which means

$$x_j = \pm(1 + \sqrt{M}), \quad x_k = \pm(1 + \sqrt{S}), \quad x_l = (1 + \sqrt{T}).$$

Thus

$$\alpha = 7 + x_j^2 + x_k^2 + x_l^2,$$

and we have already shown that the remaining squares x_i^2, $i \notin \{j, k, l\}$, can only be squares of rational integers. Thus at least four of them are needed to represent 7. This concludes the proof of Theorem 5.0.1. □

Finally, although it should be clear, we explicitly show how the just proven result easily yields the fact about infinitely many orders with $\mathcal{P}(\mathcal{O}) = 7$ in every biquadratic field.

Proof of Theorem 2.1.5. Clearly it suffices to show that every order $\mathcal{O}_0$ contains a proper suborder with $\mathcal{P}(\,\cdot\,) = 7$. Consider the maximal basic suborder $\mathcal{O}_\mathrm{b}$ of $\mathcal{O}_0$, which exists thanks to Proposition 5.1.3. Take the corresponding M_0, S_0 and T_0, and if necessary, multiply them all by 5 and use them to define a new basic order $\mathcal{O}'$. Then M, S, T from $\mathcal{O}_\mathrm{b}$ changed by 25, so $\mathcal{O}'$ is a proper subset of $\mathcal{O}_\mathrm{b}$ and hence of $\mathcal{O}_0$; the multiplication by 5 could not influence the fact that the products $M_0 S_0$, $M_0 T_0$ and $S_0 T_0$ are not squares, so $\mathcal{O}'$ is indeed an order, see Section 5.1; and finally, $T_0 \geq 5$, so $\mathcal{P}(\mathcal{O}) = 7$ by Theorem 5.0.1. □

5.3 A more general result

This section generalises the ideas from the proof of Theorem 5.0.1. This serves two purposes: On the one hand, we are able to exploit these results later to prove $\mathcal{P}(\mathcal{O}) = 7$ even for most basic orders with $2 \leq T_0 \leq 4$. On the other hand, particularly in orders where T_0 is huge, we prove that there are many elements of length 7 – see Theorems 5.3.5 and 5.3.7. Let us note that Theorem 5.0.1 is a simple corollary of the newer Theorem 5.3.5; however, we first wanted to present the direct proof to illustrate the ideas.

Throughout the section, we continue to study the basic order $\mathcal{O} = \mathbb{Z} + \mathbb{Z}\sqrt{M} + \mathbb{Z}\sqrt{S} + \mathbb{Z}\sqrt{T}$ with $T > S > M > 1$; further, $M = S_0 T_0$, $S = M_0 T_0$, $T = M_0 S_0$ and clearly $T_0 < S_0 < M_0$. We shall examine a simple family of numbers, each of which is evidently a sum of seven squares:

For a given triple $(A, B, C) \in \mathbb{Z}$, in the fixed order $\mathcal{O}$, we define

$$\alpha(A, B, C) := 7 + (A + \sqrt{M})^2 + (B + \sqrt{S})^2 + (C + \sqrt{T})^2.$$

Our aim is prove that with a few exceptions, it is possible to choose $A, B, C \in \mathbb{Z}$ so that $\ell(\alpha(A, B, C)) = 7$ in $\mathcal{O}$. In these cases, we shall in fact prove a stronger claim: The representation of this suitable $\alpha(A, B, C)$ as a sum of nonzero squares is essentially unique, namely it must contain the three summands $(A+\sqrt{M})^2$, $(B+\sqrt{S})^2$, $(C+\sqrt{T})^2$ and then either $7 = 4+1+1+1$ or $7 = 1 + \cdots + 1$.

Observation 5.3.1. The equality $\alpha(A, B, C) = \sum_{i=1}^{n} x_i^2$ with $x_i = a + b\sqrt{M} + c\sqrt{S} + d\sqrt{T}$ is

equivalent to the following system of Diophantine equations over $\mathbb{Z}$:

$$7 + A^2 + B^2 + C^2 + M + S + T = \sum_{i=1}^{n} (a_i^2 + b_i^2 M + c_i^2 S + d_i^2 T) \tag{I}$$

$$A = \sum_{i=1}^{n} a_i b_i + M_0 \sum_{i=1}^{n} c_i d_i \tag{II}$$

$$B = \sum_{i=1}^{n} a_i c_i + S_0 \sum_{i=1}^{n} b_i d_i \tag{III}$$

$$C = \sum_{i=1}^{n} a_i d_i + T_0 \sum_{i=1}^{n} b_i c_i \tag{IV}$$

Since $\pm x_i$ have the same square, we can without loss of generality require $a_i \geq 0$ for all i.

We start with a simple yet powerful observation which uses congruences modulo M_0, S_0, T_0 to examine possible solutions of the equations.

Lemma 5.3.2. *Consider a solution of the system of equations (I)–(IV).*

- *If $M_0 \nmid A$, then there exists at least one index j such that $a_j b_j \neq 0$.*
- *If $S_0 \nmid B$, then there exists at least one index k such that $a_k c_k \neq 0$.*
- *If $T_0 \nmid C$, then there exists at least one index l such that $a_l d_l \neq 0$.*

Moreover, if all three conditions hold and the inequality

$$M \geq 7 + A^2 + B^2 + C^2$$

is satisfied, then $|b_j| = |c_k| = |d_l| = 1$, and all other b_i, c_i and d_i are zero.

Proof. Supposing that $a_i b_i = 0$ for each i, the first sum in (II) would be zero, which would imply $M_0 \mid A$; that contradicts our assumption. Similarly we prove the second and third claim using equations (III) and (IV), respectively.

As for the last statement, from the previous claims we know that at least one of the a_i, one of the b_i, one of the c_i and one of the d_i is nonzero. We shall prove that (I) implies $\sum b_i^2 = \sum c_i^2 = \sum d_i^2 = 1$ (which immediately gives the assertion): If at least one of the sums was larger, then

$$\sum_{i=1}^{n} (a_i^2 + b_i^2 M + c_i^2 S + d_i^2 T) \geq 1 + M + S + T + M \geq 1 + M + S + T + 7 + A^2 + B^2 + C^2,$$

which clearly contradicts (I). This concludes the proof. □

It might seem natural to say that without loss of generality $j = 1$, $k = 2$ and $l = 3$. However, the problem is that j, k, l are not necessarily different indices. In fact, the next important step is the proof that under some further conditions they must be distinct. But first let us rewrite the equations with our current knowledge:

Observation 5.3.3. Under the conditions of Lemma 5.3.2, the system of equations can be reformulated as follows: $|b_j| = |c_k| = |d_l| = 1$ and all other b_i, c_i, d_i are zero;

$$7 + A^2 + B^2 + C^2 = \sum_{i=1}^{n} a_i^2 \tag{I}$$

$$A = a_j b_j + M_0 c_k d_k \tag{II}$$

$$B = a_k c_k + S_0 b_l d_l \tag{III}$$

$$C = a_l d_l + T_0 b_j c_j. \tag{IV}$$

Remember that we already proved that a_j, a_k, a_l are nonzero. Observe that the second summand in (II) is nonzero if and only if $k \neq l$, and in such case it is $\pm M_0$. Similar observations can be made about (III) and (IV).

Suppose still that the conditions of Lemma 5.3.2 are satisfied, so that the previous observation applies. Now we observe the following: To prove that $\alpha(A,B,C)$ can only be represented as $7+(A+\sqrt{M})^2+(B+\sqrt{S})^2+(C+\sqrt{T})^2$, it suffices to show that j,k,l are pairwise different. Indeed, if (II) loses its second summand, it directly yields $x_j = a_j + b_j\sqrt{M} + 0 + 0 = \pm(A+\sqrt{M})$; similarly for (III) and (IV). And with this information, (I) simplifies as

$$7 = \sum_{i\neq j,k,l} a_i^2,$$

and it is clear that 7 is not a sum of three squares in $\mathbb{Z}$.

So let us now supply this last piece of the jigsaw puzzle:

Lemma 5.3.4. *Suppose that the assumptions of Lemma 5.3.2 hold. Then:*

- *If $M_0 > |A| + \sqrt{7+A^2+B^2+C^2}$, then $k \neq l$.*
- *If $S_0 > |B| + \sqrt{7+A^2+B^2+C^2}$, then $j \neq l$.*
- *If $T_0 > |C| + \sqrt{7+A^2+B^2+C^2}$, then $j \neq k$.*
- *If the first* two *conditions hold and $|A| \neq |B|$, then $j \neq k$.*

Proof. From (I) it follows that $|a_i| \leq \sqrt{7+A^2+B^2+C^2}$ for each index i.

Now, $k = l$ is equivalent to $c_k d_k \neq 0$ (and then in fact it is ± 1). Thus if $k = l$, (II) gives

$$M_0 = |M_0 c_k d_k| = |A - a_j b_j| \leq |a_j b_j| + |A| = |a_j| + |A| \leq |A| + \sqrt{7+A^2+B^2+C^2}.$$

This proves the first implication. The second and third are obtained analogously.

As for the fourth, suppose that the first two claims can be applied. Then (II) and (III) give $|A| = |a_j b_j| = |a_j|$ and $|B| = |a_k c_k| = |a_k|$. Thus our assumption $|A| \neq |B|$ yields $|a_j| \neq |a_k|$, which clearly implies $j \neq k$. □

Now finally we can summarise our result:

Theorem 5.3.5. *For any triple (A,B,C) of nonzero integers, consider the element*

$$\alpha(A,B,C) = 7 + (A+\sqrt{M})^2 + (B+\sqrt{S})^2 + (C+\sqrt{T})^2$$

in the basic order $\mathbb{Z} + \mathbb{Z}\sqrt{M} + \mathbb{Z}\sqrt{S} + \mathbb{Z}\sqrt{T}$, with the usual meaning of M_0, S_0, T_0.

There exists a constant N such that if $M_0 > S_0 > T_0 > N$, then $\ell(\alpha(A,B,C)) = 7$, and even more, the only two representations of $\alpha = \alpha(A,B,C)$ as a sum of nonzero squares in $\mathcal{O}$ are

$$\alpha = 2^2 + 1^2 + 1^2 + 1^2 + (A+\sqrt{M})^2 + (B+\sqrt{S})^2 + (C+\sqrt{T})^2$$

and

$$\alpha = \underbrace{1^2 + \cdots + 1^2}_{7\times} + (A+\sqrt{M})^2 + (B+\sqrt{S})^2 + (C+\sqrt{T})^2.$$

In fact, $N = \max\{|A|,|B|,|C|\} + \sqrt{7+A^2+B^2+C^2}$.

Proof. It suffices to check the assumptions of the next proposition. Since $C \neq 0$ and $T_0 > |C|$, the first condition holds. The remaining four follow directly from $M_0 > S_0 > T_0 > \max\{|A|,|B|,|C|\} + \sqrt{7+A^2+B^2+C^2}$. □

We have weakened the statement of the theorem in order to make it shorter. However, often we need the following form which requires weaker conditions:

Proposition 5.3.6. *The claim of the previous theorem about the length and representations of $\alpha(A,B,C)$ holds for a triple of nonzero integers (A,B,C) as soon as all the following conditions are satisfied in $\mathcal{O}$:*

- $T_0 \nmid C$.
- $M = T_0 S_0 \geq 7 + A^2 + B^2 + C^2$.
- $M_0 > |A| + \sqrt{7 + A^2 + B^2 + C^2}$.
- $S_0 > |B| + \sqrt{7 + A^2 + B^2 + C^2}$.
- *Either* $T_0 > |C| + \sqrt{7 + A^2 + B^2 + C^2}$ *or* $|A| \neq |B|$.

Proof. We start by observing that the third and fourth conditions together with $A, B \neq 0$ imply $M_0 \nmid A$, $S_0 \nmid B$. After that, there is nothing to prove – all the work has been done throughout the section. However, let us summarise to achieve clarity:

The representations of $\alpha(A,B,C)$ as a sum of squares correspond to solutions of equations (I)–(IV) from Observation 5.3.1. The conditions of Lemma 5.3.2 are satisfied. Thus the equations can be simplified as stated in the Observation 5.3.3. In the paragraph following that observation, it is explained that the only case when nontrivial solutions exist is when j,k,l are not pairwise different. However, that is excluded by Lemma 5.3.4. □

Observe that Theorem 5.3.5 yields Theorem 5.0.1 as a direct corollary, since $5 > 1 + \sqrt{10}$. Another interesting corollary follows:

Theorem 5.3.7. *For any $k \in \mathbb{N}$, there exists a constant N_k such in each basic order $\mathcal{O}$ with $T_0 > N_k$, there are at least k elements of length 7, pairwise different modulo $(\mathcal{O}^\times)^2$.*

Proof. Indeed, N_k can easily be chosen so that there are enough triples (A,B,C) satisfying conditions of Theorem 5.3.5, namely $T_0 > N_k > \max\{|A|,|B|,|C|\} + \sqrt{7 + A^2 + B^2 + C^2}$.

It only remains to be seen that all these $\alpha(A,B,C)$ are different numbers in $\mathcal{O}^\times/(\mathcal{O}^\times)^2$. There is a funny way of proving this: We know that if T_0 is large enough (which we assume), then every relevant $\alpha(A,B,C)$ can uniquely be represented as a sum of ten nonzero squares – in particular, in such a representation, seven of the summands are equal to 1. On the other hand, for any $\beta \in \mathcal{O}$, the number $\beta^2\alpha(A,B,C)$ can be represented as a sum of ten nonzero squares, seven of which are equal to β^2. However, this cannot be true for any number $\alpha(A',B',C')$ unless $\beta^2 = 1$; thus $\alpha(A',B',C') \neq \beta^2\alpha(A,B,C)$. □

This directly yields the advertised Corollary 5.0.2. Moreover, if we arrange all basic biquadratic orders e.g. based on the sum $M_0 + S_0 + T_0$ or on the value M_0, then the orders with less then k elements of length 7 will have zero density for any given k.

5.4 The remaining 'non-coprime' cases

In this section we prove that in basic orders $\mathcal{O}$, we have $\mathcal{P}(\mathcal{O}) = 7$ except when $T_0 = 1$ (which in the mind of a reader of Chapter 2 means that M and S are coprime, although it is no longer the case; it is simply the case when $T = MS$) or M is particularly small. Most of the work was already done in the previous section.

The following proposition shows that using $\alpha(2,1,1)$ instead of $\alpha(1,1,1)$, one can fully solve the case $T_0 = 4$.

Proposition 5.4.1. *Let $\mathcal{O}$ be a basic order with $T_0 \geq 4$. Then $\mathcal{P}(\mathcal{O}) = 7$, as $\ell(\alpha(2,1,1) = 7$.*

Proof. This follows directly from Proposition 5.3.6; one has $S_0 \geq 5$ and $M_0 \geq 6$, so all conditions are readily checked. (Note that the same proof would apply for the other elements $\alpha(A,B,C)$ with $|A| = 2$, $|B| = |C| = 1$ as well.) □

On the other hand, note that if $T_0 = 1$, i.e. $T = MS$, then the results from previous section cannot be used, as the first condition from Proposition 5.3.6 is always violated. However, this is almost the only problem:

Theorem 5.4.2. *Let $\mathcal{O}$ be a basic order where $T \neq MS$ are not coprime and M is different from 6, 8, 10 and 12. Then $\mathcal{P}(\mathcal{O}) = 7$. In particular, $\ell(\alpha(2,1,1) = 7$.*

Proof. The case of $T_0 \geq 4$ is handled in the previous proposition. Observe that the conditions of Propositon 5.3.6 hold if and only if $T_0 > 1$ (which we assume), $M = T_0 S_0 \geq 13$ (which is satisfied as we have excluded all composite nonsquares under 13), $M_0 > 2 + \sqrt{13}$ and $S_0 > 1 + \sqrt{13}$. Thanks to $M_0 > S_0 > T_0 > 1$, these last two conditions only fail if $T_0 = 3$ and $S_0 = 4$ (giving $M = 12$) or $T_0 = 2$ and $S_0 = 3, 4, 5$ (giving $M = 6, 8, 10$). □

Note that if $M = 6$, then $\ell(7) = 2$, so using elements of the form $\alpha(A,B,C)$ is hopeless. If $M = 8, 10$ or 12, then we cannot use Proposition 5.3.6 directly, but if one examined its proof carefully, one could probably prove $\ell(\alpha(A,B,C)) = 7$ for a suitable choice of A, B, C. However, it is curious that by far the most difficult case turned out to be the one where $T = MS$: This is in sharp contrast with the case of maximal orders, where we obtained the strongest results exactly under this assumption (see Section 2.5).

We conclude the chapter by a cheap result which is about non-basic non-maximal orders.

Theorem 5.4.3. *Let $P, Q \geq 10$ be odd integers such that P is even, Q is odd, and neither one of them nor PQ is a square. Then $\mathcal{O} = \mathbb{Z} + \mathbb{Z}\sqrt{P} + \mathbb{Z}\sqrt{Q} + \mathbb{Z}\frac{\sqrt{P}+\sqrt{Q}}{2}$ is a biqudratic order and $\mathcal{P}(\mathcal{O}) = 7$.*

In particular, we have $\ell(\alpha) = 7$ for $\alpha = 7 + (1+\sqrt{P})^2 + (1+\sqrt{Q})^2 + \left(\frac{\sqrt{P}+\sqrt{PQ}}{2}\right)^2$

Proof. The only thing to be checked is that under the given conditions, $\mathcal{O}$ is indeed a biquadratic order. Otherwise, the proof is entirely the same as the proof of Theorem 2.5.3; we intentionally chose the integral basis of $\mathcal{O}$ in such a way that the shape of $\mathcal{O}$ is the same as the shape of $\mathcal{O}_K$ for a biquadratic field of type (B1) with coprime p, q. □

Bibliography

[BCIL] C. N. Beli, W. K. Chan, M. I. Icaza and J. Liu, *On a Waring's problem for integral quadratic and Hermitian forms*, Trans. Amer. Math. Soc. 371, 5505–5527 (2019).

[BCP] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput., 24, 235—265 (1997).

[BGV] K. J. Becher, D. Grimm and J. Van Geel, *Sums of squares in algebraic function fields over a complete discretely valued field*. Pacific J. Math. 276 (2), 257–276 (2014).

[BH] M. Bhargava and J. Hanke, *Universal quadratic forms and the 290-theorem*, Invent. Math., to appear.

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

[BK2] V. Blomer and V. Kala, *On the rank of universal quadratic forms over real quadratic fields*, Doc. Math. 23, 15–34 (2018).

[BL] K. J. Becher and D. B. Leep, *The length and other invariants of a real field*. Math. Z. 269, 235–252 (2011).

[BLOP] R. Baeza, D. Leep, M. O'Ryan and M. J. P. Prieto, *Sums of squares of linear forms*, Math. Z. 193, no. 2, 297–306 (1986).

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

[BV] K. J. Becher and J. Van Geel, *Sums of squares in function fields of hyperelliptic curves*, Math. Z. 261, 829–844 (2009).

[CDLR] M. D. Choi, Z. D. Dai, T. Y. Lam and B. Reznick, *The Pythagoras number of some affine algebras and local algebras*, J. Reine Angew. Math. 336, 45–82 (1982).

[CI] W. K. Chan and M. I. Icaza, *Hermite reduction and a Waring's problem for integral quadratic forms over number fields*, Trans. Amer. Math. Soc. 374, 2967–2985 (2021).

[CKR] W. K. Chan, M.-H. Kim and S. Raghavan, *Ternary universal integral quadratic forms over real quadratic fields*, Japan. J. Math. 22, 263–273 (1996).

[Co] G. Collinet, *Sums of squares in rings of integers with 2 inverted*, Acta Arith. 173, 27–37 (2016).

[CP] H. Cohn and G. Pall, *Sums of four squares in a quadratic ring*, Trans. Amer. Math. Soc. 105, 536–556 (1962).

[Č+] M. Čech, D. Lachman, J. Svoboda, M. Tinková and K. Zemková, *Universal quadratic forms and indecomposables over biquadratic fields*, Math. Nachr. 292, 540–555 (2019).

[De] J. I. Deutsch, *Universality of a non-classical integral quadratic form over* $\mathbb{Q}[\sqrt{5}]$, Acta Arith. 136, 229–242 (2009).

[DS] A. Dress and R. Scharlau, *Indecomposable totally positive numbers in real quadratic orders*, J. Number Theory 14, 292–306 (1982).

[Dz] J. Dzewas, *Quadratsummen in reell-quadratischen Zahlkörpern*, Math. Nachr. 21, 233–284 (1960).

[EH] D. Estes and J. S. Hsia, Sums of three integer squares in complex quadratic fields, Proc. Amer. Math. Soc. 89, 211–214 (1983).

[EK] A. G. Earnest and A. Khosravani. *Universal positive quaternary quadratic lattices over totally real number fields*, Mathematika 44, 342–347 (1997).

[HH] Z. He and Y. Hu, *Pythagoras number of quartic orders containing* $\sqrt{2}$, preprint. Available at arXiv:2204.10468.

[HKK] J. S. Hsia, Y. Kitaoka and M. Kneser, *Representations of positive definite quadratic forms*, J. Reine Angew. Math. 301, 132–141 (1978).

[Ho] D. W. Hoffmann, *Pythagoras numbers of fields*, J. Amer. Math. Soc. 12 (3), 839–848 (1999).

[Hu] Y. Hu, *The Pythagoras number and the u-invariant of Laurent series fields in several variables*, J. Algebra 426, 243–258 (2015).

[Ic] M. I. Icaza, *Effectiveness in representations of positive definite quadratic forms*, PhD thesis at The Ohio State University (1992).

[Ic2] M. I. Icaza, *Sums of squares of integral linear forms*, Acta Arith. 124, 231–241 (1996).

[Ja] F. Jarvis, *Algebraic Number Theory*, Springer (2007).

[JK] S. W. Jang and B. M. Kim, *A refinement of the Dress–Scharlau theorem*, J. Number Theory 158, 234–243 (2016).

[JW] C. Ji and D. Wei, Sums of integral squares in cyclotomic fields, C. R. Math. Acad. Sci. Paris 344, 413–416 (2007).

[JWX] C. Ji, Y. Wang and F. Xu, *Sums of three squares over imaginary quadratic fields*, Forum Math. 18, 585–601 (2006).

[Ka] V. Kala, *Universal quadratic forms and elements of small norm in real quadratic fields*, Bull. Aust. Math. Soc. 94, 7–14 (2016).

[Ka2] V. Kala, *Norms of indecomposable integers in real quadratic fields*, J. Number Theory 166, 193–207 (2016).

[Ka3] V. Kala, *Number fields without universal quadratic forms of small rank exist in most degrees*, Math. Proc. Cambridge Philos. Soc. 174, 225–231 (2023).

[Ki1] B. M. Kim, *Finiteness of real quadratic fields which admit positive integral diagonal septenary universal forms*, Manuscripta Math. 99, 181–184 (1999).

[Ki2] B. M. Kim, *Universal octonary diagonal forms over some real quadratic fields*, Comment. Math. Helv. 75, 410–414 (2000).

[KK] B. M. Kim and J. Y. Kim, *Sums of nonvanishing integral squares in real quadratic fields*, J. Number Theory 177, 497–515 (2017).

[KKP] B. M. Kim, M.-H. Kim and D. Park, *Real quadratic fields admitting universal lattices of rank 7*, J. Number Theory 233, 456–466 (2022).

[Kn] M. Kneser, *Klassenzahlen definiter quadratischer Formen*, Arch. Math. (Basel) 8, 241–250 (1957).

[KnS] M. Kneser and R. Scharlau, *Quadratische Formen*, Springer (2002).

[Ko] C. Ko, *On the representation of a quadratic form as a sum of squares of linear forms*, Q. J. Math. 1, 81–98 (1937).

[KO] M.-H. Kim and B.-K. Oh, *Representations of positive definite senary integral quadratic forms by a sum of squares*, J. Number Theory 63, 89–100 (1997).

[KO2] M.-H. Kim and B.-K. Oh, *Bounds for quadratic Waring's problem*, Acta Arith. 104, 155–164 (2002).

[KO3] M.-H. Kim and B.-K. Oh, *Representations of integral quadratic forms by sums of squares*, Math. Z. 250, 427–442 (2005).

[KP] B. M. Kim and P.-S. Park, *Sums of distinct integral squares in real quadratic fields*, C. R. Math. Acad. Sci. Paris 349, 497–500 (2011).

[Kr] J. Krásenský, *A cubic ring of integers with the smallest Pythagoras number*, Arch. Math. (Basel) 118, 39–48 (2022).

[Kr2] J. Krásenský, *Pythagoras number of non-maximal orders in biquadratic fields*, in preparation.

[KRS] J. Krásenský, M. Raška and E. Sgallová, *Pythagoras numbers of orders in biquadratic fields*, Expo. Math. 40, 1181–1228 (2022).

[KrY] J. Krásenský and P. Yatsyna, *On quadratic Waring's problem in totally real number fields*, Proc. Amer. Math. Soc. 151, 1471–1485 (2023).

[KS] V. Kala and J. Svoboda, *Universal quadratic forms over multiquadratic fields*, Ramanujan J. 48, 151–157 (2019).

[KT] V. Kala and M. Tinková, *Universal quadratic forms, small norms and traces in families of number fields*, Int. Math. Res. Not. IMRN (accepted). Available at arXiv:2005.12312.

[KTZ] J. Krásenský, M. Tinková and K. Zemková, *There are no universal ternary quadratic forms over biquadratic fields*, Proc. Edinburgh Math. Soc. 63(3), 861–912 (2020).

[KY] V. Kala and P. Yatsyna, *Sums of squares in S-integers*, New York J. Math. 26, 1145–1154 (2020).

[KY2] V. Kala and P. Yatsyna, *Lifting problem for universal quadratic forms*, Adv. Math. 377, 24 pp. (2021).

[KY3] V. Kala and P. Yatsyna, *On Kitaoka's conjecture and lifting problem for universal quadratic forms*, Bull. Lond. Math. Soc. 55, 854–864 (2023).

[La] T. Y. Lam, *Introduction to quadratic forms over fields*, Graduate Studies in Mathematics 65, American Mathematical Society (2005).

[Le] D. Leep, *A historical view of the Pythagoras numbers of fields*, In Quadratic forms—algebra, arithmetic, and geometry, 493 of Contemp. Math., pp. 271–288. Amer. Math. Soc., Providence, RI (2009).

[Li] J. Liu, *On a Waring's problem for Hermitian lattices*, Bull. Sci. Math. 174 (2021).

[Li2] J. Liu, *g-invariant on unary Hermitian lattices over imaginary quadratic fields with class number 2 or 3*, J. Algebra 622, 636–675 (2023).

[Ma] H. Maaß, *Über die Darstellung total positiver Zahlen des Körpers $R(\sqrt{5})$ als Summe von drei Quadraten*, Abh. Math. Sem. Univ. Hamburg 14, 185–191 (1941).

[Mi] J. S. Milne, *Algebraic Number Theory* (v3.08), 2020, Available at www.jmilne.org/math/.

[Mo] L. J. Mordell, *A new Waring's problem with squares of linear forms*, Q. J. Math. 1, 276–288 (1930).

[Mo2] L. J. Mordell, *On the representation of a binary quadratic form as a sum of squares of linear forms*, Math. Z. 35, 1–15 (1932).

[Mo3] L. J. Mordell, *The Representation of a Definite Quadratic Form as a Sum of Two Others*, Ann. of Math. 38(4), 751–757 (1937).

[Mos] C. Moser, *Représentation de -1 par une somme de carrés dans certains corps locaux et globaux, et dans certains anneaux d'entiers algébriques*, C. R. Math. Acad. Sci. Paris 271, 1200–1203 (1970).

[MU] M. Mazur and S. V. Ullom. *Galois module structure of units in real biquadratic number fields*, Acta Arith. 111, 105–124 (2004).

[Na] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Springer (1990).

[O'M] O. T. O'Meara, *Introduction to Quadratic Forms*, Springer-Verlag (1973).

[Pe] M. Peters, *Die Stufe von Ordnungen ganzer Zahlen in algebraischen Zahlkörpern*. Math. Ann. 195, 309–314 (1971).

[Pe2] M. Peters, *Quadratische Formen über Zahlringen*, Acta Arith. 24, 157–164 (1973).

[Pe3] M. Peters, *Summen von Quadraten in Zahlringen*, J. Reine Angew. Math. 268/269, 318–323 (1974).

[Pe4] M. Peters, *Einklassige Geschlechter von Einheitsformen in totalreellen algebraischen Zahlkörpern*. Math. Ann. 226, 117–120 (1977).

[Per] O. Perron, *Die Lehre von den Kettenbrüchen*, B. G. Teubner (1913).

[Pf] A. Pfister, *Quadratic forms with applications to algebraic geometry and topology*, London Math. Soc. Lect. Notes 217, Cambridge University Press (1995).

[Ra] M. Raška, *Representing multiples of m in real quadratic fields as sums of squares*, J. Number Theory 244, 24–41 (2023).

[Ram] S. Ramanujan, *On the expression of a number in the form* $ax^2 + by^2 + cz^2 + du^2$, Proc. Cambridge Philos. Soc 19, 11–21 (1917).

[Ro] A. E. Ross, *On representation of integers by quadratic forms*, Proc. Nat. Acad. Sci. 18, 600–608 (1932).

[Sa] H. Sasaki, *Sums of squares of integral linear forms*, J. Austral. Math. Soc. Ser. A 69, 298–302 (2000).

[Sa2] H. Sasaki, *Sums of squares of totally positive definite quadratic forms over real quadratic field* $\mathbb{Q}(\sqrt{5})$ (in Japanese), Otemae Junior College Research bulletin 25, 407–412 (2005).

[Sa3] H. Sasaki, *2-universal O-lattices over real quadratic fields*, Manuscripta Math. 119, 97–106 (2006).

[Sa4] H. Sasaki, *Quaternary universal forms over* $\mathbb{Q}[\sqrt{13}]$, Ramanujan J. 18, 73–80 (2009).

[Sch] R. Scharlau, *Zur Darstellbarkeit von totalreellen ganzen algebraischen Zahlen durch Summen von Quadraten*, PhD thesis at Universität Bielefeld (1979).

[Sch2] R. Scharlau, *On the Pythagoras number of orders in totally real number fields*, J. Reine Angew. Math. 316, 208–210 (1980).

[Sh] D. Shanks, *The simplest cubic number fields*, Math. Comp. 28, 1137–1152 (1974).

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

[Ti] M. Tinková, *On the Pythagoras number of the simplest cubic fields*, submitted. Available at arXiv:2101.11384.

[TV] M. Tinková and P. Voutier, *Indecomposable integers in real quadratic fields*, J. Number Theory 212, 458–482 (2020).

[TVY] S. V. Tikhonov, J. Van Geel and V. I. Yanchevskii, *Pythagoras numbers of function fields of hyperelliptic curves with good reduction*, Manuscripta Math. 119, 305–322 (2006).

[Wi] K. S. Williams, *Integers of biquadratic fields*, Canad. Math. Bull. Vol. 13, 519–526 (1970).

[Ya] P. Yatsyna, *A lower bound for the rank of a universal quadratic form with integer coefficients in a totally real number field*, Comment. Math. Helv. 94(2), 221–239 (2019).

List of publications

- J. Krásenský, M. Tinková and K. Zemková, *There are no universal ternary quadratic forms over biquadratic fields*, Proc. Edinburgh Math. Soc. 63(3), 861–912 (2020).
- J. Krásenský, M. Raška and E. Sgallová, *Pythagoras numbers of orders in biquadratic fields*, Expo. Math. 40, 1181–1228 (2022).
- J. Krásenský, *A cubic ring of integers with the smallest Pythagoras number*, Arch. Math. (Basel) 118, 39–48 (2022).
- J. Krásenský and P. Yatsyna, *On quadratic Waring's problem in totally real number fields*, Proc. Amer. Math. Soc. 151, 1471–1485 (2023).