Krásenský, Jakub; Yatsyna, Pavlo

On quadratic Waring's problem in totally real number fields

Published in:
Proceedings of the American Mathematical Society

DOI:
10.1090/proc/16233

Published: 01/04/2023

Document Version
Peer-reviewed accepted author manuscript, also known as Final accepted manuscript or Post-print

PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 00, Number 0, Pages 000–000
S 0002-9939(XX)0000-0

ON QUADRATIC WARING'S PROBLEM IN TOTALLY REAL NUMBER FIELDS

JAKUB KRÁSENSKÝ AND PAVLO YATSYNA

Abstract. We improve the bound of the g-invariant of the ring of integers of a totally real number field, where the g-invariant $g(r)$ is the smallest number of squares of linear forms in r variables that is required to represent all the quadratic forms of rank r that are representable by the sum of squares. Specifically, we prove that the $g_{\mathcal{O}_K}(r)$ of the ring of integers $\mathcal{O}_K$ of a totally real number field K is at most $g_{\mathbb{Z}}([K:\mathbb{Q}]r)$. Moreover, it can also be bounded by $g_{\mathcal{O}_F}([K:F]r+1)$ for any subfield F of K. This yields a sub-exponential upper bound for $g(r)$ of each ring of integers (even if the class number is not 1). Further, we obtain a more general inequality for the lattice version $G(r)$ of the invariant and apply it to determine the value of $G(2)$ for all but one real quadratic field.

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 [Mo1] 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, Mo1, 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 [KO1]. 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, Sa1]. The upper bounds valid for all r improved gradually: from functions growing faster than exponentially

2020 *Mathematics Subject Classification.* Primary 11E12, 11D85, 11E25, 11E39.

J.K. acknowledges partial support by project PRIMUS/20/SCI/002 from Charles University, by Czech Science Foundation GAČR, grant 21-00420M, by projects UNCE/SCI/022 and GA UK No. 742120 from Charles University, and by SVV-2020-260589.

P.Y. was supported by the project PRIMUS/20/SCI/002 from Charles University and by the Academy of Finland (grants #336005 and #351271, Principal Investigator C. Hollanti).

[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, Pe, Ti, Sch], 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 [Sch], but it is bounded by a function depending only on the degree $d = [K : \mathbb{Q}]$ [KY], 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 [Ic1, 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 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 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 2.1; note that the analogous definition for Hermitian lattices is used in [BCIL, Li1, Li2].) A more encompassing result of this paper is the following:

Theorem 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 4.1 (the only exception is the second part of (1), which is precisely Corollary 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 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 3.3. Also, note that in Theorem 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 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 1.2 is that $g_{\mathcal{O}}(r)$ is always finite.

Corollary 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 [Ic1, 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 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 [Pe], 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 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 1.4 is contained in Section 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 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 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 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) [Pe, Ma, Dz, CP, Sch2]; 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 $5 = \mathcal{P}(\mathcal{O}_F) \leq G_{\mathcal{O}_F}(1) \leq g_{\mathbb{Z}}(2) = 5$. □

2. Preliminaries

We use [Na] as a reference for everything related to number fields and [KS] 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.

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 $R[X_1, \dots, X_r]$ 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 $L_1, \dots, L_r$ such that

$$\varphi\big(L_1(X_1, \dots, X_s), \dots, L_r(X_1, \dots, X_s)\big) = \psi(X_1, \dots, X_s),$$

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 $X_1^2 + \dots + X_N^2$ for some $N \in \mathbb{N}$. Then we put

$$g_R(r) = \min\{n : X_1^2 + \dots + X_n^2 \text{ represents all forms in } \Sigma_R(r)\}.$$

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 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.

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 $M \nrightarrow N$ 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 $\mathbf{x} \in M, \mathbf{y} \in N$.

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.

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 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 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 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 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 $\iota\big(\sum \alpha_i \mathbf{e}_i\big) = \big(\sum \alpha_i\big)\mathbf{e}$ where $\mathbf{e_1}, \dots, \mathbf{e}_n$ and $\mathbf{e}$ are the standard bases.

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 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 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 3.1) since the theory of lattices over non-maximal orders is much more involved than over Dedekind domains.

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 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 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 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 1.2 (3), i.e. the inequality $g_{\mathcal{O}}(r) \leq G_{\mathcal{O}_F}(rd)$, this yields the second part of Theorem 1.2 (1) as a simple corollary:

Corollary 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 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 1.2 (1).

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 4.1. *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 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 4.1 (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 4.1 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 4.1, either. Instead, most of the work consists of handling the underlying S-modules and R-modules seen as subsets of $\big(\mathrm{Quot}(S)\big)^n$ or $\big(\mathrm{Quot}(S)\cdot R\big)^n$ (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 2.2.

Proof of Theorem 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 2.2, it is enough to show $L\to I_G$ over R, where $G = G_S(rd)$. By Lemma 2.4 (1), $L = R\mathbf{x}_1 + \cdots + R\mathbf{x}_{r-1} + \mathfrak{A}^{-1}\mathbf{x}_r$, 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 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

$$\begin{aligned} R &= S\beta_1 + \cdots + S\beta_{d-1} + \mathfrak{a}^{-1}\beta_d \qquad \text{with } \beta_i\in R,\\ \mathfrak{A} &= S\gamma_1 + \cdots + S\gamma_{d-1} + \mathfrak{b}^{-1}\gamma_d \qquad \text{with } \gamma_i\in\mathfrak{A}. \end{aligned}$$

Now define the vectors $\mathbf{f}_i^{(j)}\in\big(\mathrm{Quot}(S)\big)^N$ as the coordinates of $\mathbf{x}_j$ with respect to these pseudo-bases:

$$\begin{aligned} \mathbf{x}_j &= \mathbf{f}_1^{(j)}\beta_1 + \cdots + \mathbf{f}_d^{(j)}\beta_d \qquad \text{for } 1\le j\le r-1;\\ \mathbf{x}_r &= \mathbf{f}_1^{(r)}\gamma_1 + \cdots + \mathbf{f}_d^{(r)}\gamma_d. \end{aligned}$$

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 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 4.1 (3). By assumption, we have $R = S\beta_1 + \cdots + S\beta_{d-1} + \mathfrak{a}^{-1}\beta_d$, 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 $L' = R\mathbf{x}_1 + \cdots + R\mathbf{x}_r$, 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 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 $L' \to I_G$. □

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 [Li1] 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 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 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 1.2 applies: $7 = \mathcal{P}(\mathcal{O}_K) \le G_{\mathcal{O}_F}(2)$. □

To prove Theorem 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 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 $\mathcal{P}(\mathcal{O}_{K_i}) \geq \ell(\alpha_i) = 7$ combined with the inequality $\mathcal{P}(\mathcal{O}_{K_i}) \leq g_{\mathbb{Z}}(4) = 7$. After this, we also get $\mathcal{P}(\mathcal{O}_{K_i}) \leq G_{\mathcal{O}_F}(2) \leq g_{\mathbb{Z}}(4)$ 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 $7 = \mathcal{P}(\mathcal{O}_K) \leq g_{\mathcal{O}_F}(2)$.

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 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 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 $\left(1, \sqrt{10}, \frac{1+\sqrt{n}}{2}, \sqrt{10}\frac{1+\sqrt{n}}{2}\right)$, 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 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 [Pe, 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

$$x_1 = \frac{10+n+7\sqrt{n}}{2} - \frac{1+\sqrt{n}}{2} x_2. \tag{5.1}$$

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):

$$\sum a_i^2 + n \sum b_i^2 = 154 + 6n, \tag{5.2}$$

$$\sum a_i b_i = 26. \tag{5.3}$$

Looking at (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 (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 (5.2). By Cauchy–Schwarz inequality, $|\sum a_i b_i| \leq \sqrt{8 \cdot 8} = 8$, which contradicts (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 (5.1) explicitly as $x_1 = \left(5 - \frac{a_2}{4} + n\frac{2-b_2}{4}\right) + \sqrt{n}\left(\frac{7}{2} - \frac{a_2+b_2}{4}\right)$, 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 (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 (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 1.4. The upper bound $G_{\mathcal{O}_F}(2) \leq 7$ is in Lemma 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 5.2, and for the remaining $n \equiv 1 \pmod 4$ in Proposition 5.3. □

Acknowledgements

We thank the anonymous reviewer for his or her valuable suggestions.

References

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).

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).

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).

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).

CP. H. Cohn and G. Pall, *Sums of four squares in a quadratic ring*, Trans. Amer. Math. Soc. 105, 536–556 (1962).

Dz. J. Dzewas, *Quadratsummen in reell-quadratischen Zahlkörpern*, Math. Nachr. 21, 233–284 (1960).

HH. Z. He and Y. Hu, *Pythagoras number of quartic orders containing* $\sqrt{2}$, 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).

Ic1. M.I. Icaza, *Effectiveness in representations of positive definite quadratic forms*, Thesis (Ph.D.)–The Ohio State University. 1992. 76 pp.

Ic2. M. I. Icaza, *Sums of squares of integral linear forms*, Acta Arith. 124, 231–241 (1996).

Kn. M. Kneser, *Klassenzahlen definiter quadratischer Formen*, Arch. Math. (Basel) 8, 241–250 (1957).

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).

KO1. 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).

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

KRS. J. Krásenský, M. Raška and E. Sgallová, *Pythagoras numbers of orders in biquadratic fields*, Expo. Math. (2022). doi:10.1016/j.exmath.2022.06.002

KS. M. Kneser and R. Scharlau, *Quadratische Formen*, Springer (2002).

KY. V. Kala and P. Yatsyna, *Lifting problem for universal quadratic forms*, Adv. Math. 377, 24 pp. (2021).

Le. D. Leep, *A historical view of the Pythagoras numbers of fields*, In Quadratic forms—algebra, arithmetic, and geometry, **493** of Contemp. Math., pages 271–288. Amer. Math. Soc., Providence, RI (2009).

Li1. J. Liu, *g-invariant on unary Hermitian lattices over imaginary quadratic fields with class number 2 or 3*, arXiv:2111.10825.

Li2. J. Liu, *On a Waring's problem for Hermitian lattices*, Bull. Sci. math. (2021).

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).

Mo1. 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*, Annals of Mathematics 38(4), 751–757 (1937).

Na. W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Springer (1990).

Pe. M. Peters, *Summen von Quadraten in Zahlringen*, J. Reine Angew. Math. 268/269, 318–323 (1974).

Pf. A. Pfister, *Quadratic forms with applications to algebraic geometry and topology*, London Math. Soc. Lect. Notes 217, Cambridge University Press (1995).

Sa1. 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).

Sch. R. Scharlau, *On the Pythagoras number of orders in totally real number fields*, J. Reine Angew. Math. 316, 208–210 (1980).

Sch2. R. Scharlau, *Zur Darstellbarkeit von totalreellen ganzen algebraischen Zahlen durch Summen von Quadraten*, dissertation at Universität Bielefeld (1979).

Ti. M. Tinková, *On the Pythagoras number of the simplest cubic fields*, arXiv:2101.11384.

Charles University, Faculty of Mathematics and Physics, Department of Algebra, Sokolovská 83, 18600 Praha 8, Czech Republic

Email address: krasensky@karlin.mff.cuni.cz

Aalto University, Department of Mathematics and Systems Analysis, P.O. Box 11100, FI-00076, Finland

Email address: pavlo.yatsyna@aalto.fi