

FAILURES OF INTEGRAL SPRINGER'S THEOREM

NICOLAS DAANS, VÍTĚZSLAV KALA, JAKUB KRÁSENSKÝ, AND PAVLO YATSYNA

ABSTRACT. We discuss the phenomenon where an element in a number field is not integrally represented by a given positive definite quadratic form, but becomes integrally represented by this form over a totally real extension of odd degree. We prove that this phenomenon happens infinitely often, and, conversely, establish finiteness results about the situation when the quadratic form is fixed.

1. INTRODUCTION

A famous theorem of Springer says that, given a quadratic form defined over a field K and a field extension L/K of odd degree, the form is isotropic over K if and only if it is so over L , see, for example, [EKM08, Corollary 18.5] for a modern proof. By standard (de)homogenisation arguments, this theorem can be rephrased alternatively as a statement about representation by quadratic forms:

Theorem (Springer, 1952 [Spr52]). *Let K be a field, $Q \in K[X_1, \dots, X_n]$ a quadratic form over K , L/K a field extension of odd degree, $a \in K$.*

If $a \in Q(L)$, then $a \in Q(K)$.

For a commutative ring R and a quadratic form $Q \in R[X_1, \dots, X_n]$, we say that $a \in R$ is *represented by Q over R* if $a = Q(x_1, \dots, x_n)$ for some $x_1, \dots, x_n \in R$, and we denote by $Q(R)$ the subset of R of all represented elements.

In number theory, one is often concerned with *integral* representations of quadratic forms, and it is natural to ask whether the analogue of the above theorem holds in this context. More precisely, let K be a number field (respectively a local field of characteristic 0), and denote by $\mathcal{O}_K$ its ring of integers (respectively its discrete valuation ring). We ask:

Question (“Integral Springer’s Theorem for representations”, ISTR). *Let K be a number field or a local field of characteristic 0. Let $Q \in \mathcal{O}_K[X_1, \dots, X_n]$ be a quadratic form over $\mathcal{O}_K$, L/K a field extension of odd degree, $a \in \mathcal{O}_K$.*

If $a \in Q(\mathcal{O}_L)$, does it necessarily follow that also $a \in Q(\mathcal{O}_K)$?

A positive answer has been obtained in the case where K is a local field, or K is a number field and Q is an indefinite quadratic form; see Theorem 2.1 and Theorem 2.2 below and the discussion that follows. In particular, this applies whenever K is not totally real.

This leaves just one case to consider: when K is a totally real number field and Q is a definite form. We shall consider in particular the case where Q is positive definite, i.e. represents only totally positive elements of K . Although some of the existing literature on this topic has correctly insinuated that the ISTR should in this case fail (i.e. the above Question

Date: Monday 22nd April, 2024.

2020 *Mathematics Subject Classification.* 11E12, 11H55, 11R80.

The research was supported by Czech Science Foundation grant 21-00420M (N. D., V. K.), and by Charles University programmes PRIMUS/24/SCI/010 (N. D., P. Y.) and UNCE/24/SCI/022 (P. Y.).

has a negative answer), to the best of the authors' knowledge, no concrete examples thereof have so far been provided or discussed in the literature, at least not when also the extension L is assumed to be totally real. This is the goal of the present note.

After introducing some basic concepts and notations, we start in Section 2 by briefly discussing the cases where a positive answer to ISTR is known for number fields and local fields. These provide sufficient (local) conditions for ISTR to hold or fail in certain contexts, also for positive definite quadratic forms. In Section 3, we use these conditions and established facts from the theory of integral quadratic forms, to derive general finiteness results which bound the potential failure of ISTR for positive definite quadratic forms. In particular, we show:

Theorem (see Corollary 3.3 and Proposition 3.2). *Let K be a totally real number field, d a positive integer, $n \geq 5$, and $Q \in \mathcal{O}_K[X_1, \dots, X_n]$ be a positive definite quadratic form. There exist only finitely many $a \in \mathcal{O}_K \setminus Q(\mathcal{O}_K)$ (up to multiplication by squares of units) and finitely many minimal totally real extensions L/K of degree $2d+1$ such that $a \in Q(\mathcal{O}_L)$.*

Similar statements exist for positive quadratic forms in 3 or 4 variables under more technical assumptions, see Remark 3.4. Moreover, a version of this statement for fixed element a actually holds without the assumption that the degree of L/K is odd, see Theorem 3.1.

In Section 4 we provide several classes of examples: we show that ISTR fails for quadratic forms over $\mathbb{Z}$ of all ranks ≥ 2 , even when restricting to totally real cubic Galois extensions, and for ranks ≥ 4 we provide an infinite parametrised family of examples:

Theorem (see Theorem 4.2). *Let $k \in \mathbb{Z}^+$, $k \geq 4$ and let $K = \mathbb{Q}(\omega)$ where ω is a root of the irreducible polynomial $T^3 + T^2 - 2T - 1$. Let $Q(X_1, X_2, X_3, X_4) = X_1^2 + X_2^2 + X_3^2 + (8k+5)X_4^2$. Then there exists a natural number n such that $n \in Q(\mathcal{O}_K)$, but $n \notin Q(\mathbb{Z})$.*

On the other hand, we give an example showing that the local conditions which guarantee that ISTR holds, as established in Section 2, are not necessary, see Theorem 4.8.

Acknowledgements. We would like to thank Zilong He for a friendly email exchange when we were exploring the topic of this paper.

2. BACKGROUND

For a number field K , we denote by $\mathcal{O}_K^+$ the subset of $\mathcal{O}_K$ of *totally positive elements* (i.e. of those that are positive in all real embeddings; however, we impose no restrictions in complex embeddings), by $\mathcal{O}_K^\times$ the set of units of $\mathcal{O}_K$, and by $\mathcal{O}_K^{\times 2}$ the set of squares of units. Note that $0 \notin \mathcal{O}_K^+$. In particular, we denote by $\mathbb{Z}^+$ the set of (non-zero) natural numbers. For subsets $S_1, S_2 \subseteq K$ we write $S_1 S_2 = \{xy \mid x \in S_1, y \in S_2\}$. For $x, y \in K$, we write $x \succ y$ or $y \prec x$ if $x - y$ is totally positive.

Given an integral domain R with field of fractions K , by a *quadratic R -lattice* we shall mean a pair (Λ, Q) where Λ is a finitely generated R -submodule of a finite-dimensional K -vector space, and $Q : \Lambda \rightarrow R$ is a quadratic map, i.e. a map satisfying $Q(av) = a^2 Q(v)$ for $a \in R$ and $v \in \Lambda$, and such that the associated map

$$\mathfrak{b}_Q : \Lambda \times \Lambda \rightarrow R : (v, w) \mapsto Q(v + w) - Q(v) - Q(w)$$

is bilinear.

Given a quadratic lattice (Λ, Q) , the K -dimension of $K\Lambda$ is called the *rank* of (Λ, Q) . We call a quadratic lattice (Λ, Q) *degenerate* if there exists $v \in \Lambda$ such that $Q(v + w) = Q(w)$ for all $w \in \Lambda$, *nondegenerate* otherwise.

When (Λ, Q) is a quadratic lattice and Λ is a free R -module, then we may identify Λ with R^n for some $n \in \mathbb{Z}^+$, and there exists a homogeneous quadratic polynomial $f \in R[X_1, \dots, X_n]$ such that $Q((x_1, \dots, x_n)) = f(x_1, \dots, x_n)$ for all $(x_1, \dots, x_n) \in R^n$. In this case, we also call Q a *quadratic form*. Note that all quadratic lattices over a field are free, so in this case, the study of quadratic lattices reduces to that of quadratic forms.

Given a quadratic lattice (Λ, Q) and $a \in R$, we say that Q *represents* a if $a = Q(v)$ for some $v \in \Lambda$. We denote by $Q(R)$ the set of elements of R represented by Q . (It is more common to denote this by $Q(\Lambda)$, but we chose a more convenient notation for the purposes of this paper, as we are interested in extensions of scalars.)

Given an extension S/R of integral domains, and a quadratic lattice (Λ, Q) over R , there exists a unique quadratic map $Q_S : \Lambda \otimes_R S \rightarrow S$ that extends Q ; we call $(\Lambda \otimes_R S, Q_S)$ the *extension of scalars* of (Λ, Q) from R to S , and also denote $\Lambda_S = \Lambda \otimes_R S$. We might simply write $Q(S)$ instead of $Q_S(S)$. Clearly, we have $Q(R) \subseteq Q(S) \cap R$, and in general, the inclusion might be strict. Springer's Theorem implies that, if L/K is a field extension of odd degree and Q a quadratic form over K , then $Q(K) = Q(L) \cap K$.

Given a number field K , we call a quadratic lattice (Λ, Q) over $\mathcal{O}_K$ *indefinite* if K is not totally real or there is an embedding $\sigma : K \rightarrow \mathbb{R}$ such that $\sigma(Q(\mathcal{O}_K)) \subset \mathbb{R}$ contains both positive and negative elements. If K is totally real, we call Λ *positive definite* if $Q(v)$ is totally positive for all $v \in \Lambda \setminus \{0\}$. Note that a positive definite quadratic lattice is in particular nondegenerate.

For a discrete prime $\mathfrak{p}$ of K , denote by $\mathcal{O}_{\mathfrak{p}}$ the completion of $\mathcal{O}_K$ with respect to $\mathfrak{p}$. When $\mathfrak{p}$ is archimedean, then $\mathcal{O}_{\mathfrak{p}}$ is the completion of K with respect to $\mathfrak{p}$, i.e. it is $\mathbb{R}$ or $\mathbb{C}$. If (Λ, Q) is a quadratic $\mathcal{O}_K$ -lattice and $a \in \mathcal{O}_K$, we say that a is *locally represented by Q over $\mathcal{O}_K$* if $a \in Q(\mathcal{O}_{\mathfrak{p}})$ for all primes $\mathfrak{p}$ of K (both discrete and archimedean). In general, this is not sufficient to conclude that $a \in Q(\mathcal{O}_K)$, but in some cases it is; a quadratic $\mathcal{O}_K$ -lattice (Λ, Q) such that every element of $\mathcal{O}_K$ which is locally represented by Q lies in $Q(\mathcal{O}_K)$, is called *regular*.

We now discuss briefly the known results regarding ISTR which are relevant to our setup, without attempting to give a complete account of the history or of related results in the literature.

Theorem 2.1 (Local Integral Springer's Theorem for representations, [Xu99, He23]). *Let K be a local field of characteristic 0 and L/K be a field extension of odd degree. Let (Λ, Q) be a quadratic $\mathcal{O}_K$ -lattice. Then $Q(\mathcal{O}_K) = Q(\mathcal{O}_L) \cap \mathcal{O}_K$.*

The above was first observed in the case where K is either non-dyadic or 2 is unramified in K in [Xu99], using the local integral quadratic form theory developed by Riehm and O'Meara. The missing case where K is dyadic and 2 is ramified was very recently solved in [He23].

The following globalisation of Theorem 2.1 was proven for the case $K = \mathbb{Q}$ in [Xu99] and also conjectured there to hold in general; the general case was then proven recently in [He23] using the theory of base of norm generators ("BONGs") as developed by Beli in among others [Bel03, Bel06, Bel10, Bel22]. The proofs rely on a combination of local Theorem 2.1 with delicate computations of integral spinor norms.

Theorem 2.2 (Integral Springer’s Theorem for representations by indefinite forms, [Xu99, He23]). *Let K be a number field and L/K a field extension of odd degree. Let (Λ, Q) be an indefinite quadratic $\mathcal{O}_K$ -lattice. Then $Q(\mathcal{O}_K) = Q(\mathcal{O}_L) \cap \mathcal{O}_K$.*

We note that the results of [Xu99, He23] are actually more general than what we address in the above two theorems, since they consider not just representation of elements by quadratic lattices, but also representations of quadratic lattices by other quadratic lattices. In fact, for quadratic lattices of rank at least 4, Theorem 2.2 can be deduced directly from Theorem 2.1 via the following well-known local-global principle; see, for example, [Hsi76] for an algebraic proof.

Theorem 2.3 (Local-global principle for integral representation by indefinite forms). *Let K be a number field, (Λ, Q) a nondegenerate indefinite quadratic $\mathcal{O}_K$ -lattice of rank at least 4, $a \in \mathcal{O}_K$. Then $a \in Q(\mathcal{O}_K)$ if and only if a is locally represented by Q over $\mathcal{O}_K$.*

We now turn our attention to the positive definite case. We shall provide evidence in Section 4 via several examples that no obvious version of Theorem 2.2 (ISTR) can hold when replacing indefinite quadratic lattices by positive definite quadratic lattices, and in fact we suspect that failure of ISTR for positive definite quadratic forms happens often.

These results on ISTR should be viewed alongside the *lifting problem* for universal quadratic forms. Briefly, for a number field K , a quadratic $\mathcal{O}_K$ -lattice is *universal* if it represents all elements of $\mathcal{O}_K^+$; the existence and properties of universal lattices have been widely studied, see e.g. the surveys [Kal23b, Kim04]. The lifting problem then asks if it is possible for an $\mathcal{O}_K$ -lattice to be universal over a larger field $L \supset K$. Analogously to our expectations concerning ISTR, when the lattice is indefinite, then a version of local-global principle holds and the extension of scalars is universal quite often [HHX23, XZ22]. However, in the positive definite case, this seems to happen very rarely [KL24, KY21, KY23, KY24].

We conclude this section by pointing out that ISTR can only fail for elements which are locally represented over the base field.

Proposition 2.4. *Let L/K be an odd-degree extension of number fields, (Λ, Q) a quadratic $\mathcal{O}_K$ -lattice. If $a \in Q(\mathcal{O}_L) \cap \mathcal{O}_K$, then a is locally represented by Q over $\mathcal{O}_K$.*

In particular, if (Λ, Q) is a regular $\mathcal{O}_K$ -lattice (e.g. if its class number is 1), then ISTR holds for all odd-degree extensions of K .

Proof. Assume that, on the contrary, there exists a prime $\mathfrak{p}$ of K with $a \notin Q(\mathcal{O}_{\mathfrak{p}})$. There exists a prime $\mathfrak{q}$ of L of odd degree over $\mathfrak{p}$ (as the global degree is the sum of the local degrees, see e.g. [O’M00, 15:3(1)]); note that this argument works both for archimedean and discrete primes $\mathfrak{p}$. Thus, by Theorem 2.1, we get $a \notin Q(\mathcal{O}_{\mathfrak{q}})$. Hence, in particular, $a \notin Q(\mathcal{O}_L)$, which is a contradiction.

The second part of the statement is clear. □

3. FINITENESS RESULTS

Theorem 3.1. *Let $d \in \mathbb{Z}^+$, K a totally real number field, (Λ, Q) a positive definite quadratic $\mathcal{O}_K$ -lattice, $a \in \mathcal{O}_K$. There exist only finitely many totally real number fields L of degree d over K such that $a \in Q(\mathcal{O}_L)$ but $a \notin Q(\mathcal{O}_{L'})$ for every proper subfield L' of L containing K .*

In the proof we shall use the concept of the *house* of a totally real algebraic integer α , denoted by $|\overline{\alpha}|$ and defined as $\max_{i=1}^t |\alpha_i|$, where $\alpha_1, \dots, \alpha_t$ are all the conjugates of α .

Proof. Let n be the rank of Λ . There is a basis $(v_1, \dots, v_n)$ of $K\Lambda$ such that $\Lambda \subseteq \mathcal{O}_K v_1 + \dots + \mathcal{O}_K v_n$. It follows that, for any number field extension L/K , $\Lambda_{\mathcal{O}_L} \subseteq \mathcal{O}_L v_1 + \dots + \mathcal{O}_L v_n$.

By [KY23, Lemma 4] there exists a fixed constant C such that, for every totally real number field extension L/K and for every $\beta_1, \dots, \beta_n \in \mathcal{O}_L$, one has $C \cdot \overline{Q(\beta_1 v_1 + \dots + \beta_n v_n)} > \max_{i=1}^n \overline{\beta_i}^2$.

If now L is a totally real number field containing K such that $a \in Q(\mathcal{O}_L)$, then there exist $\beta_1, \dots, \beta_n \in \mathcal{O}_L$ such that $a = Q(\beta_1 v_1 + \dots + \beta_n v_n)$; and if additionally $a \notin Q(\mathcal{O}_{L'})$ for every proper subfield L' , then L must be generated by $\beta_1, \dots, \beta_n$ over K . By the previous paragraph, $\beta_1, \dots, \beta_n$ satisfy $\overline{\beta_i}^2 < C\overline{a}$. As there are only finitely many totally real algebraic integers β of degree at most $d \cdot [K : \mathbb{Q}]$ and with $\overline{\beta}^2 < C\overline{a}$ (see, for example, Northcott's Theorem [Nor49, Theorem 1]), we conclude that only finitely many such fields L may exist. $\square$

In Proposition 2.4, we have seen that the only elements for which ISTR can fail are those which are represented locally but not globally. The following proposition combines this with the almost local-global principle of Hsia, Kitaoka and Kneser to get a finiteness result:

Proposition 3.2. *Let K be a totally real number field, (Λ, Q) a positive definite quadratic $\mathcal{O}_K$ -lattice of rank at least 5. There exists a finite set $S \subseteq \mathcal{O}_K^+ \setminus Q(\mathcal{O}_K)$ with the property that, for every field extension L/K of odd degree, we have $Q(\mathcal{O}_L) \cap \mathcal{O}_K^+ \subseteq Q(\mathcal{O}_K) \cup S\mathcal{O}_K^{\times 2}$, and if L is not totally real, then we additionally have $(Q(\mathcal{O}_L) \cap \mathcal{O}_K^+) \cup \{0\} = Q(\mathcal{O}_K) \cup S\mathcal{O}_K^{\times 2}$.*

Proof. Let S be a set which consists of exactly one representative from each set of the form $\alpha\mathcal{O}_K^{\times 2}$ where $\alpha \in \mathcal{O}_K^+ \setminus Q(\mathcal{O}_K)$ is locally represented by Q over $\mathcal{O}_K$. The local-global principle established in [HKK78, Theorem 3] implies that S is finite. We check that such S satisfies the statement: First, clearly $S \subseteq \mathcal{O}_K^+ \setminus Q(\mathcal{O}_K)$. Further, by Proposition 2.4, every element of $Q(\mathcal{O}_L) \cap \mathcal{O}_K^+$ is locally represented by Q over K ; thus it either belongs to $Q(\mathcal{O}_K)$, or it is not globally represented and hence it lies in $S\mathcal{O}_K^{\times 2}$. This shows that $Q(\mathcal{O}_L) \cap \mathcal{O}_K^+ \subseteq Q(\mathcal{O}_K) \cup S\mathcal{O}_K^{\times 2}$.

Now assume additionally that L is not totally real, and pick $a \in S$. By the choice of S , we have $a \in Q(\mathcal{O}_{\mathfrak{p}})$ for every prime $\mathfrak{p}$ of K , and thus also for every prime of L . Since Q is indefinite over $\mathcal{O}_L$, Theorem 2.3 implies that $a \in Q(\mathcal{O}_L)$. From this, it follows that $S\mathcal{O}_K^{\times 2} \subseteq Q(\mathcal{O}_L)$. $\square$

Corollary 3.3. *Let K be a totally real number field, (Λ, Q) a positive definite quadratic $\mathcal{O}_K$ -lattice of rank at least 5, $d \in \mathbb{Z}^+$. There exist only finitely many totally real field extensions L/K of degree $2d+1$ such that $Q(\mathcal{O}_L) \cap \mathcal{O}_K \neq Q(\mathcal{O}_K)$, but $Q(\mathcal{O}_{L'}) \cap \mathcal{O}_K = Q(\mathcal{O}_K)$ for every proper subfield L' of L containing K .*

Proof. This follows by combining Proposition 3.2 and Theorem 3.1: Proposition 3.2 gives the finite set S of elements for which ISTR may fail and Theorem 3.1 states that the desired finiteness result holds for each of them separately. $\square$

Remark 3.4. If K is a totally real number field, then for positive definite quadratic lattices over $\mathcal{O}_K$ of rank 3 or 4, a similar local-global principle as the one used in the proof of Proposition 3.2 exists for the representation of *square-free* totally positive elements, see, for example, Section 5 in [SP04]. Using this, one can state a variation of Proposition 3.2 and Corollary 3.3 also for lattices of rank 3 or 4.

4. FAILURES OF ISTR

We shall first construct an infinite family of quadratic forms over $\mathbb{Z}$ which represent a certain natural number over the ring of integers in a totally real cubic field, but not over $\mathbb{Z}$.

For an integral domain R , $n \in \mathbb{Z}^+$, and $a_1, \dots, a_n \in R$, we shall denote by $\langle a_1, \dots, a_n \rangle$ the *diagonal quadratic form* given by $R^n \rightarrow R : (x_1, \dots, x_n) \mapsto \sum_{i=1}^n a_i x_i^2$. In particular, $\langle a_1, \dots, a_n \rangle(R)$ denotes the set $Q(R)$ when $Q = \langle a_1, \dots, a_n \rangle$. We denote by $\perp$ the orthogonal sum of quadratic lattices.

Let us denote by K_{49} the number field of discriminant 49. This is a cyclic cubic extension of $\mathbb{Q}$, in particular, it is totally real. It can be defined alternatively as the splitting field of the polynomial $T^3 + T^2 - 2T - 1$ over $\mathbb{Q}$, or as the maximal totally real subfield of the seventh cyclotomic field, i.e. the field generated over the rationals by $\omega = \zeta_7 + \zeta_7^{-1}$, where ζ_7 is a primitive 7th root of 1.

Proposition 4.1. *Let $n, m \in \mathbb{Z}^+$ such that $n \equiv 28 \pmod{32}$, $m \equiv 5 \pmod{8}$, and $3.25m < n < 4m$. Then*

- (1) $n \notin \langle 1, 1, 1, m \rangle(\mathbb{Z})$, but
- (2) $n - m\omega^2 \in \langle 1, 1, 1 \rangle(\mathcal{O}_{K_{49}})$; in particular $n \in \langle 1, 1, 1, m \rangle(\mathcal{O}_{K_{49}})$.

Proof. First, assume that $n \in \langle 1, 1, 1, m \rangle(\mathbb{Z})$, i.e. $n = w^2 + x^2 + y^2 + mz^2$ for certain $w, x, y, z \in \mathbb{Z}$. By the assumption that $n < 4m$, this is possible only if $z^2 \in \{0, 1\}$, since otherwise $n - mz^2$ would be negative. But this means either $n = w^2 + x^2 + y^2$ or $n - m = w^2 + x^2 + y^2$, and by reducing modulo 32 (respectively, 8) one sees that neither option is possible. We conclude that $n \notin \langle 1, 1, 1, m \rangle(\mathbb{Z})$.

We now show that $n - m\omega^2 \in \langle 1, 1, 1 \rangle(\mathcal{O}_{K_{49}})$. Note that $\omega^2 \prec 3.25$, which implies that $n - m\omega^2$ is totally positive. By [Kr 22, Proposition 3.1] it now suffices to show that $-(n - m\omega^2)$ is not a square in $\mathbb{Z}_2[\omega]$. One can see that indeed $m\omega^2 - n$ is not a square modulo 8: if it were, it would modulo 8 be of the form $(\omega + 2b)^2 = \omega^2 + 4(b^2 + \omega b)$ for some $b \in \{0, 1, \omega, \omega^2, 1 + \omega, 1 + \omega^2, \omega + \omega^2, 1 + \omega + \omega^2\}$, which yields $b^2 + \omega b \equiv 1 + \omega^2 \pmod{2}$, and one verifies exhaustively that such b cannot exist. $\square$

Theorem 4.2. *Let $k \in \mathbb{Z}^+$, $k \geq 4$. Then there exists $n \in \mathbb{Z}^+$ such that $\langle 1, 1, 1, 8k + 5 \rangle$ represents n over $\mathcal{O}_{K_{49}}$ but not over $\mathbb{Z}$. In particular, there exist infinitely many quadratic forms of rank 4 over $\mathbb{Z}$ which are pairwise non-isometric over $\mathbb{Q}$ and for which ISTR fails.*

Proof. For the first part, observe that, for $k = 4$ and thus $m = 8k + 5 = 37$, one can choose $n = 124$ and conclude with Proposition 4.1. For $k > 4$, there are more than 32 natural numbers between $3.25m$ and $4m$, hence in particular some element $n \equiv 28 \pmod{32}$; as such one can again apply Proposition 4.1.

For the second part, observe, by comparing determinants, that the forms $\langle 1, 1, 1, 8k + 5 \rangle$ and $\langle 1, 1, 1, 8l + 5 \rangle$ are not isometric over $\mathbb{Q}$ if $(8k + 5)(8l + 5)$ is not a square, i.e. there cannot be a linear change of variables over $\mathbb{Q}$ transforming one form into the other. And clearly, one can find infinitely many positive integers $k_1, k_2, k_3, \dots$ such that $(8k_i + 5)(8k_j + 5)$ is never a square for $i \neq j$. $\square$

Remark 4.3. Theorem 4.2 implies that, for every $D \in \mathbb{Z}^+$ with $D \geq 4$, there exist infinitely many quadratic forms over $\mathbb{Z}$ of rank D which are pairwise non-isometric over $\mathbb{Q}$ and for which ISTR fails. It suffices to observe that, if Q is a positive definite form over $\mathbb{Z}$ and $a \in Q(\mathcal{O}_K) \setminus Q(\mathbb{Z})$, then also for $Q' = Q \perp \langle a + 1 \rangle$ we have $a \in Q'(\mathcal{O}_K) \setminus Q'(\mathbb{Z})$.

Example 4.4. Consider the setup of Proposition 4.1 but replace the form $\langle 1, 1, 1, m \rangle$ by $\langle 1, 1, m \rangle$. Numerical data suggests that a similar result should hold: for many $m \geq 7$, there seems to be some n slightly larger than $3.25m$ such that $n \notin \langle 1, 1, m \rangle(\mathbb{Z})$ but $n - m\omega^2 \in \langle 1, 1 \rangle(\mathcal{O}_{K_{49}})$. For $m = 2p$ and $m = 4k + 2$, we verified this numerically for the first 200 primes p greater than three and natural numbers $k \leq 200$.

Presumably analytical techniques could be used to show that this happens infinitely often.

Example 4.5. We note that ISTR can even fail for binary quadratic forms: the form $\langle 1, 71 \rangle$ does not represent 232 over $\mathbb{Z}$, but in $\mathcal{O}_{K_{49}}$ we have $(4\omega^2 - \omega - 16)^2 + 71\omega^2 = 232$ for $\omega = \zeta_7 + \zeta_7^{-1}$.

Furthermore, observe that, when α, β are any totally real algebraic integers with $\alpha^2 + 71\beta^2 = 232$, then $\frac{232}{71} \succ \beta^2$. As $\frac{232}{71} < 4$, it follows from Kronecker's Theorem [Kro57] that, up to conjugation, $\beta^2 = 2 + 2\cos(\frac{2\pi}{n})$ for some $n \in \mathbb{Z}^+$. Since $2 + 2\cos(\frac{2\pi}{n}) < \frac{232}{71}$ if and only if $n \leq 7$, one obtains that this forces $\beta^2 \in \{0, 1, 2, \frac{3+\sqrt{5}}{2}, 3, \omega^2\}$. Thus, up to conjugation and switching signs, the only possibilities for the pair (α, β) are $(\sqrt{232}, 0)$, $(\sqrt{161}, 1)$, $(\sqrt{90}, \sqrt{2})$, $(\sqrt{\frac{1}{2}(251-71\sqrt{5})}, \frac{1+\sqrt{5}}{2})$, $(\sqrt{19}, \sqrt{3})$, and $(4\omega^2 - \omega - 16, \omega)$. In particular, K_{49} is the unique minimal totally real number field of odd degree in which the equation $x^2 + 71y^2 = 232$ has an integral solution.

Further, we show that ISTR fails fairly often: For a (quite arbitrarily chosen) quadratic form over $\mathbb{Q}$, it fails for the majority of cubic fields with small discriminant.

Example 4.6. Consider the form $Q = \langle 1, 1, 14 \rangle$ over $\mathbb{Z}$ and the first 100 totally real cubic fields, ordered by discriminant. One can compute that if K is one of these fields and $\text{disc}(K) \neq 43^2$, then ISTR fails for Q over the extension $K/\mathbb{Q}$. For K with discriminant 43^2 , we do not know whether ISTR fails for Q .

More precisely: There are 54 natural numbers under 1500 which are locally but not globally represented by Q over $\mathbb{Z}$; the smallest is 3, the largest is 1428. These are all represented by $\langle 1, 2, 7 \rangle$, which is everywhere locally isometric to $\langle 1, 1, 14 \rangle$. One verifies numerically that, for every totally real cubic extension $K/\mathbb{Q}$ where $\text{disc}(K) \leq 3132$ and $\text{disc}(K) \neq 43^2$, there is at least one of these 54 exceptional numbers which becomes represented by Q over $\mathcal{O}_K$. (For the field with $\text{disc}(K) = 43^2$, there is no natural number under 3500 which becomes represented over $\mathcal{O}_K$.) In particular, ISTR fails for Q in these 99 cubic extensions.

The following is an illustration for a failure of ISTR over a base field other than $\mathbb{Q}$.

Example 4.7. Let $K = \mathbb{Q}(\sqrt{21})$ and let $L = \mathbb{Q}(\vartheta)$, where $\vartheta = \zeta_{21} + \zeta_{21}^{-1}$, i.e. L is the maximal totally real subfield of the 21st cyclotomic field. It is of degree 6 as ϑ has minimal polynomial $T^6 - T^5 - 6T^4 + 6T^3 + 8T^2 - 8T + 1$ over $\mathbb{Q}$. Then $\sqrt{21} = 2\vartheta^5 + 2\vartheta^4 - 10\vartheta^3 - 8\vartheta^2 + 12\vartheta + 3 \in L$, and L/K is an extension of degree 3.

One verifies that the element $7 + (\frac{1+\sqrt{21}}{2})^2$ is not a sum of 4 squares in $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{21}}{2}]$, but it is a sum of 4 squares in $\mathcal{O}_L = \mathbb{Z}[\vartheta]$, since it is equal to

$$1^2 + (\vartheta - 1)^2 + (\vartheta^2 + \vartheta - 2)^2 + (\vartheta^5 - \vartheta^4 - 7\vartheta^3 + 5\vartheta^2 + 12\vartheta - 5)^2.$$

Many other examples could be produced. For example, one can check that for $\alpha = 12 + 2\sqrt{13}$ and the degree 3 field extension $\mathbb{Q}(\zeta_{13} + \zeta_{13}^{-1})/\mathbb{Q}(\sqrt{13})$, one gets $\alpha \notin \langle 1, 1, 1, 1 \rangle(\mathbb{Z}[\frac{1+\sqrt{13}}{2}])$ but $\alpha \in \langle 1, 1, 1, 1 \rangle(\mathbb{Z}[\zeta_{13} + \zeta_{13}^{-1}])$.

We conclude with an example illustrating that the fact that a positive definite quadratic form over $\mathbb{Z}$ is not regular (i.e. there exist elements in $\mathbb{Z}^+$ represented by the form everywhere locally but not over $\mathbb{Z}$) does not imply a failure of ISTR for this form. In other words, the second part of Proposition 2.4 cannot be turned in an equivalence.

Consider the form $Q = \langle 1, 2, 5, 5 \rangle$. It is well known that $Q(\mathbb{Z}) = \mathbb{Z}_{\geq 0} \setminus \{15\}$, see e.g. [Bha99], in particular, Q represents all natural numbers everywhere locally and thus over $\mathbb{Q}$.

Theorem 4.8. *Let K be a number field such that $[K : \mathbb{Q}]$ is odd. Then $15 \in \langle 1, 2, 5, 5 \rangle(\mathcal{O}_K)$ if and only if K is not totally real.*

Proof. First assume that K is totally real, and assume that $15 = w^2 + 2x^2 + 5y^2 + 5z^2$ for $w, x, y, z \in \mathcal{O}_K$. We first argue why, in this case, one must have $y, z \notin \mathbb{Z}$. Suppose on the contrary that $z \in \mathbb{Z}$. We must then have $z^2 \in \{0, 1\}$, otherwise $15 - 5z^2$ would be negative. In other words, either $15 = w^2 + 2x^2 + 5y^2$ or $10 = w^2 + 2x^2 + 5y^2$. However, neither 10 nor 15 is represented by $\langle 1, 2, 5 \rangle$ over the field $\mathbb{Q}_5$, hence in particular they are not represented by $\langle 1, 2, 5 \rangle$ over $\mathbb{Q}$. By the classical Springer's Theorem, they cannot be represented over K either. We obtain a contradiction and conclude that $z \notin \mathbb{Z}$; by symmetry, also $y \notin \mathbb{Z}$.

Now set $d = [K : \mathbb{Q}]$ and recall Siegel's result that, for any $\alpha \in \mathcal{O}_K^+$ different from 1 or $\frac{3 \pm \sqrt{5}}{2}$ we have that $\text{Tr}_{K/\mathbb{Q}}(\alpha) > \frac{3d}{2}$ [Sie45, Theorem III], where $\text{Tr}_{K/\mathbb{Q}}$ denotes the trace in the extension $K/\mathbb{Q}$. Since we excluded the possibility that $y^2, z^2 \in \{0, 1\}$ in the previous paragraph, and $\frac{3 \pm \sqrt{5}}{2}$ does not lie in K since d is odd, we must have $\text{Tr}_{K/\mathbb{Q}}(y^2), \text{Tr}_{K/\mathbb{Q}}(z^2) > \frac{3d}{2}$. We compute that

$$\begin{aligned} 15d &= \text{Tr}_{K/\mathbb{Q}}(w^2 + 2x^2 + 5y^2 + 5z^2) = \text{Tr}_{K/\mathbb{Q}}(w^2) + 2 \text{Tr}_{K/\mathbb{Q}}(x^2) + 5 \text{Tr}_{K/\mathbb{Q}}(y^2) + 5 \text{Tr}_{K/\mathbb{Q}}(z^2) \\ &< 0 + 0 + 5d \frac{3}{2} + 5d \frac{3}{2} = 15d, \end{aligned}$$

which is impossible.

Now, assume that K is not totally real. Since 15 is everywhere locally represented by $\langle 1, 2, 5, 5 \rangle$, and $Q_{\mathcal{O}_K}$ is indefinite, by Theorem 2.3 we have $15 \in \langle 1, 2, 5, 5 \rangle(\mathcal{O}_K)$. $\square$

The following example is in similar spirit: We show that sometimes the failure of ISTR for a given element and a given quadratic form is rare. Note that the exceptional cubic field in this case is not K_{49} which served us in many of our previous examples; it is not even a Galois extension of $\mathbb{Q}$:

Example 4.9. Consider the form $Q(W, X, Y, Z) = 29W^2 + X^2 + 2Y^2 + 4Z^2 + XZ + YZ$. One has $145 \notin Q(\mathbb{Z})$; in fact, it is one of the “escalator lattices” occurring in the proof of the 290-Theorem of Bhargava and Hanke [BH11]. For a totally real cubic field K , we show that $145 \in Q(\mathcal{O}_K)$ if and only if K is the field with discriminant 229.

First of all, let β be a root of $T^3 - 4T - 1$. Then $\mathbb{Q}(\beta)$ has discriminant 229 and one can check that $145 \in Q(\mathbb{Z}[\beta])$ by plugging in

$$W = \beta, \quad X = \beta^2 + 2\beta - 5, \quad Y = 2\beta^2 - 8, \quad Z = -\beta + 1.$$

On the other hand, assume now that K is a totally real cubic field and $145 = 29w^2 + x^2 + 2y^2 + 4z^2 + xz + yz$. This immediately yields $\text{Tr}_{K/\mathbb{Q}}(w^2) \leq 3 \cdot \frac{145}{29} = 15$. First, just as in the previous theorem, we show that $w^2 \notin \mathbb{Z}$: If it were, then $w^2 \in \{0, 1, 4\}$, so the ternary form $X^2 + 2Y^2 + 4Z^2 + XZ + YZ$ would represent one of the numbers 145, $145 - 29 = 4 \cdot 29$ and $145 - 4 \cdot 29 = 29$ over K and thus, by the classical Springer's theorem, over $\mathbb{Q}$. However, this is impossible as none of them is represented over $\mathbb{Q}_{29}$.

Thus, $w \notin \mathbb{Q}$, so we have $K = \mathbb{Q}(w)$. This in particular means that for the discriminant $\Delta(w)$ of $\mathbb{Z}[w]$ we have $\text{disc}(K) \leq \Delta(w)$. On the other hand, the inequality [Kal23a, Prop. 2], which is a corollary of Schur's bound, yields for cubic fields $\Delta(w) \leq \frac{1}{2}(\text{Tr}_{K/\mathbb{Q}}(w^2))^3$. Putting all the inequalities together, we get

$$\text{disc}(K) \leq \Delta(w) \leq \frac{1}{2}(\text{Tr}_{K/\mathbb{Q}}(w^2))^3 \leq \frac{15^3}{2} = 1687.5.$$

There are only 50 totally real cubic fields that satisfy this bound, and for them we checked the representation numerically.

We leave open several questions for further investigation.

Questions 4.10.

- (1) Do there exist a number field K , a quadratic form Q over $\mathcal{O}_K$, $a \in \mathcal{O}_K$, and an infinite collection of totally real number field extensions L/K of odd degree such that $a \in Q(\mathcal{O}_L)$, but $a \notin Q(\mathcal{O}_{L'})$ for every proper subfield L' of L containing K ?
- (2) Given an odd-degree extension L/K of totally real fields, does there always exist a quadratic form Q over $\mathcal{O}_K$ and $a \in \mathcal{O}_K \cap Q(\mathcal{O}_L) \setminus Q(\mathcal{O}_K)$?

REFERENCES

- [Bel03] C.N. Beli. Integral spinor norm groups over dyadic local fields. *J. Number Theory*, 102(1):125–182, 2003.
- [Bel06] C. N. Beli. Representations of integral quadratic forms over dyadic local fields. *Electron. Res. Announc. Amer. Math. Soc.*, 12:100–112, 2006.
- [Bel10] C.N. Beli. A new approach to classification of integral quadratic forms over dyadic local fields. *Trans. Amer. Math. Soc.*, 362(3):1599–1617, 2010.
- [Bel22] C.N. Beli. Representations of quadratic lattices over dyadic local fields. Available as arXiv:1905.04552v2, 2022.
- [BH11] M. Bhargava and J. Hanke. Universal quadratic forms and the 290-theorem. Preprint, 2011.
- [Bha99] M. Bhargava. On the Conway-Schneeberger fifteen theorem. In *Quadratic Forms and Their Applications*, volume 272 of *Contemporary Mathematics*, pages 27–37. Amer. Math. Soc., 1999.
- [EKM08] R. Elman, N. Karpenko, and A. Merkurjev. *The Algebraic and Geometric Theory of Quadratic Forms*, volume 56 of *Colloquium Publications*. Amer. Math. Soc., 2008.
- [He23] Z. He. Arithmetic Springer theorem and n -universality under field extensions. Available as arXiv:2312.09560, 2023.
- [HHX23] Z. He, Y. Hu, and F. Xu. On indefinite k -universal integral quadratic forms over number fields. *Math. Z.*, 304(20), 2023.
- [HKK78] J.S. Hsia, Y. Kitaoka, and M. Kneser. Representations of positive definite quadratic forms. *J. Reine Angew. Math.*, 301:132–141, 1978.
- [Hsi76] J.S. Hsia. Representations by spinor genera. *Pacific J. Math.*, 63(1), 1976.
- [Kal23a] V. Kala. Number fields without universal quadratic forms of small rank exist in most degrees. *Proc. Cambridge Philos. Soc.*, 174:225–231, 2023.
- [Kal23b] V. Kala. Universal quadratic forms and indecomposables in number fields: a survey. *Commun. Math.*, 31(2):81–114, 2023.
- [Kim04] M.-H. Kim. Recent developments on universal forms. In *Algebraic and arithmetic theory of quadratic forms*, volume 344 of *Contemporary Mathematics*, pages 215–228. Amer. Math. Soc., Providence, RI, 2004.
- [KL24] D. Kim and S. H. Lee. Lifting problem for universal quadratic forms over totally real cubic number fields. *Bull. Lond. Math. Soc.*, 56:1192–1206, 2024.
- [Krás22] J. Krásenský. A cubic ring of integers with the smallest Pythagoras number. *Arch. Math.*, 118:39–48, 2022.

- [Kro57] L. Kronecker. Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten. *J. Reine Angew. Math.*, 53:173–175, 1857.
- [KY21] V. Kala and P. Yatsyna. Lifting problem for universal quadratic forms. *Adv. Math.*, 377:107497, 2021.
- [KY23] V. Kala and P. Yatsyna. On Kitaoka’s conjecture and lifting problem for universal quadratic forms. *Bull. Lond. Math. Soc.*, 55(2):854–864, 2023.
- [KY24] V. Kala and P. Yatsyna. Even better sums of squares over quintic and cyclotomic fields, 2024. Available as arxiv:2402.03850.
- [Nor49] D.G. Northcott. An inequality in the theory of arithmetic and algebraic varieties. *Proc. Cambridge Philos. Soc.*, 45(4):502–509, 1949.
- [O’M00] T. O’Meara. *Introduction to quadratic forms*. Springer, 2000.
- [Sie45] C.L. Siegel. The trace of totally positive and real algebraic integers. *Ann. of Math.*, 46(2):302–312, 1945.
- [SP04] R. Schulze-Pillot. Representation by integral quadratic forms—a survey. In *Algebraic and arithmetic theory of quadratic forms*, volume 344 of *Contemp. Math.*, pages 303–321. Amer. Math. Soc., Providence, RI, 2004.
- [Spr52] T.A. Springer. Sur les formes quadratiques d’indice zéro. *C. R. Acad. Sci. Paris*, 234:1517–1519, 1952.
- [Xu99] F. Xu. Arithmetic Springer theorem on quadratic forms under field extensions of odd degree. In *Integral Quadratic Forms and Lattices*, volume 249 of *Contemporary Mathematics*, pages 175–197. Amer. Math. Soc., 1999.
- [XZ22] F. Xu and Y. Zhang. On indefinite and potentially universal quadratic forms over number fields. *Trans. Amer. Math. Soc.*, 375:2459–2480, 2022.

CHARLES UNIVERSITY, FACULTY OF MATHEMATICS AND PHYSICS, DEPARTMENT OF ALGEBRA, SOKOLOVSKÁ 83, 186 75 PRAHA 8, CZECH REPUBLIC

Email address, N. Daans: `nicolas.daans@matfyz.cuni.cz`

Email address, V. Kala: `vitezslav.kala@matfyz.cuni.cz`

Email address, P. Yatsyna: `p.yatsyna@matfyz.cuni.cz`

CZECH TECHNICAL UNIVERSITY IN PRAGUE, FACULTY OF INFORMATION TECHNOLOGY, DEPARTMENT OF APPLIED MATHEMATICS, THÁKUROVA 9, 160 00 PRAHA 6, CZECH REPUBLIC

Email address, J. Krásenský: `jakub.krasensky@fit.cvut.cz`