Mathematical Proceedings of the Cambridge Philosophical Society

VOL. 174 MARCH 2023 PART 2

Math. Proc. Camb. Phil. Soc. (2023), **174**, 225–231

doi: 10.1017/S0305004122000214

First published online 6 May 2022

Number fields without universal quadratic forms of small rank exist in most degrees

BY VÍTĚZSLAV KALA†

Charles University, Faculty of Mathematics and Physics, Department of Algebra, Sokolovská 49/83, 18675 *Praha* 8, *Czech Republic.*

e-mails: kala@karlin.mff.cuni.cz, vita.kala@gmail.com

(*Received* 01 *February* 2021*; revised* 14 *April* 2022*; accepted* 11 *April* 2022)

Abstract

We prove that in each degree divisible by 2 or 3, there are infinitely many totally real number fields that require universal quadratic forms to have arbitrarily large rank.

2020 Mathematics Subject Classification: 11E12 (Primary); 11E20, 11R21, 11R80 (Secondary)

1. *Introduction*

In 1770 Lagrange proved that every positive integer is the sum of four squares, opening up the study of universal quadratic forms. These were then first investigated over the integers $\mathbb{Z}$, leading to the celebrated 15- and 290-Theorems [**Bh, BH**], and also over number fields, starting with Maaß [**Ma**] and Siegel [**Si**] in the 1940s. To be precise, let $\mathcal{O}_F$ be the ring of integers in a totally real number field F. A totally positive quadratic form Q with $\mathcal{O}_F$-coefficients is *universal* over F if it represents all the totally positive elements of $\mathcal{O}_F$.

Universal forms exist over every F thanks to the asymptotic local-global principle [**HKK**]. Of particular interest is thus the smallest possible rank $m'(F)$ of a universal form over F. For example, we have $m'(\mathbb{Q})=4$ by the Four-Square Theorem. Among real quadratic fields, $m'(\mathbb{Q}(\sqrt{D}))=3$ for $D=2,3,5$, and these are the only real quadratic fields that admit a

† The author was supported by Czech Science Foundation GAČR, grant 21-00420M, and by Charles University, projects PRIMUS/20/SCI/002 and UNCE/SCI/022.

ternary universal form that is moreover classical (i.e., has all its cross-terms divisible by 2) [CKR]. This provides interesting evidence towards Kitaoka's Conjecture that there are only finitely many number fields F with $m'(F)=3$.

Further, the ranks $m'(\mathbb{Q}(\sqrt{D}))$ can be arbitrarily large [BK1], [Ka], ditto for multiquadratic fields of a given degree [KS]. Despite a number of other exciting results obtained in the last 25 years [BK2, CL+, EK, KT, KY, Ki, KKP, KTZ, Ya], ranks of universal forms over number fields, especially of higher degree, remain mysterious.

The aim of this short paper is to extend the previous special results on unbounded ranks $m'(F)$ to number fields of most degrees:

THEOREM 1. *Let d and m be positive integers such that d is divisible by 2 or 3. Then there are infinitely many totally real number fields F of degree $[F:\mathbb{Q}]=d$ over which every universal quadratic form has rank at least m.*

If $d=2$, this was proved by the author [Ka, Theorem 1·1]. The key idea was to use continued fractions to construct quadratic fields that have many indecomposable elements, which are hard to represent by a quadratic form. Constructing such elements in higher degrees is more difficult, nevertheless, the author and Svoboda [KS, Theorem 1] extended the result to all degrees $d=2^h$. In the cubic case $d=3$, this theorem was proved by Yatsyna [Ya, Theorem 5] using interlacing polynomials and elements of trace one.

Our argument will use Schur's trace bound [Sch] to show a general Theorem 4: in certain cases, suitable elements from a cyclic number field L force a quadratic form that represents them to have many variables, even in an overfield. We will then prove Theorem 1 by choosing L to be a real quadratic, or simplest cubic [Sh] number field.

Theorem 1 also holds for quadratic lattices that are not necessarily free; in fact, we will formulate the rest of the paper in lattice-theoretic language. Also note that we do not assume the quadratic forms to be classical, although this is a very common assumption and there are only very few results available without it (e.g., [De]).

2. *Preliminaries*

Let F be a totally real number field of degree $[F:\mathbb{Q}]=N$ over $\mathbb{Q}$, i.e., there are N real embeddings $\sigma_1,\ldots,\sigma_N : F\to\mathbb{R}$. We denote $\mathcal{O}_F$ the ring of algebraic integers. An element $\alpha\in F$ is *totally positive* (denoted $\alpha\succ 0$) if $\sigma_i(\alpha)>0$ for all $1\le i\le N$. Further, $\alpha\succeq\beta$ if $\alpha-\beta\succ 0$ or $\alpha=\beta$. The set of all totally positive algebraic integers is $\mathcal{O}_F^+$.

For $\alpha\in F$ we have its *trace* $\mathrm{Tr}_{F/\mathbb{Q}}(\alpha)=\sum_{1\le i\le N}\sigma_i(\alpha)$ and *discriminant* $\Delta_{F/\mathbb{Q}}(\alpha)$, which is the square of the determinant of the matrix $(\sigma_i(\alpha^{j-1}))_{1\le i,j\le N}$. The *discriminant of* F, i.e., the discriminant of an integral basis for $\mathcal{O}_F$, will be denoted disc_F. We have $\mathrm{disc}_F \mid \Delta_{F/\mathbb{Q}}(\alpha)$ for each $\alpha\in\mathcal{O}_F$.

A *totally positive quadratic $\mathcal{O}_F$-lattice of rank r* (an *$\mathcal{O}_F$-lattice* for short) is a pair (Λ, Q), where Λ is a finitely generated $\mathcal{O}_F$-submodule of F^r such that $\Lambda F=F^r$, $Q:F^r\to F$ is a quadratic form, and $Q(v)\in\mathcal{O}_F^+$ for all $v\in\Lambda, v\ne 0$. We also have the attached symmetric bilinear form $B(v,w)=(Q(v+w)-Q(v)-Q(w))/2$. An $\mathcal{O}_F$-lattice (Λ, Q) is *universal* (over F) if for each $\alpha\in\mathcal{O}_F^+$ there is $v\in\Lambda$ with $Q(v)=\alpha$.

Let $m(F)$ denote the minimal rank of a universal $\mathcal{O}_F$-lattice. Note that to each quadratic form Q (as considered in the Introduction) corresponds the $\mathcal{O}_F$-lattice $(\mathcal{O}_F^r, Q)$, and so $m(F)\le m'(F)$ (it is interesting to note that no example of strict inequality is known here).

https://doi.org/10.1017/S0305004122000214 Published online by Cambridge University Press

Take non-zero vectors $v_1, \ldots, v_n \in \Lambda$. The corresponding *Gram matrix* is the $n \times n$ matrix $A = (B(v_i, v_j))_{1 \le i,j \le n}$. Note that we have $B(v_i, v_i) = Q(v_i) = a_i$ and $B(v_i, v_j) = b_{ij}/2$ for all $i \neq j$ and suitable $a_i, b_{ij} \in \mathcal{O}_F$. As the lattice Λ is totally positive, $a_i \succ 0$ and we have a version of the *Cauchy–Schwarz inequality* $4a_ia_j \succeq b_{ij}^2$ for all $i \neq j$, equivalently, $Q(v_i)Q(v_j) \succeq B(v_i, v_j)^2$ (this quickly follows from the positive-definiteness of the quadratic form $\sigma_h(Q)$ on $\mathbb{R}^r$ for $h = 1, \ldots, N$).

Also note that the rank of A (as a matrix over the field F) is at most the rank r of the lattice Λ (for the rank of A equals the rank of the $\mathcal{O}_F$-sublattice of Λ spanned by $v_1, \ldots, v_n$). For more background on quadratic lattices, see [**OM**].

Further, we will crucially use the following lower bound due to Schur.

PROPOSITION 2. *([**Sch**, Section 2·II.]). Let F be a totally real number field of degree $[F : \mathbb{Q}] = N$.*

If $\beta \in \mathcal{O}_F$, then

$$\mathrm{Tr}_{F/\mathbb{Q}}\beta^2 \ge c_N \Delta_{F/\mathbb{Q}}(\beta)^{2/(N^2-N)} \text{ with } c_N = \frac{N^2 - N}{\left(2^2 \cdot 3^3 \cdot 4^4 \cdots (N-1)^{N-1} \cdot N^N\right)^{2/(N^2-N)}}.$$

Proof. Schur's bound [**Sch**, Section 2·II.] states that if $x_1, \ldots, x_N$ are real numbers such that $x_1^2 + \cdots + x_N^2 \le 1$, then the discriminant $\prod_{1 \le i < j \le N} (x_i - x_j)^2 \le c_N^{-(N^2-N)/2}$. Setting $x_i = \sigma_i(\beta)/(\mathrm{Tr}_{F/\mathbb{Q}}\beta^2)^{1/2}$ gives the inequality we need.

For an integer $k \ge 2$, we will denote S_k and A_k the symmetric and alternating groups on the set $\{1, 2, \ldots, k\}$. The cyclic group of order k is denoted C_k (considered multiplicatively).

We will work with extensions of a given number field by an S_k-number field, whose existence is given by the following proposition.

PROPOSITION 3. *Let $D, X, k \ge 2$. There are infinitely many totally real number fields K of degree $[K : \mathbb{Q}] = k$ whose discriminant $\mathrm{disc}_K > X$ is coprime with D and whose Galois closure $\widetilde{K}$ has Galois group $\mathrm{Gal}(\widetilde{K}/\mathbb{Q}) \simeq S_k$.*

Proof. This is well known. The most straightforward proof is probably using Hilbert's irreducibility theorem (see, e.g., [**Kal**, Theorem 4·2·3]).

Much more strongly, Kedlaya [**Ke**, Theorem 1·1] proved that one can even impose the additional condition that the disc_K is squarefree. Further, Bhargava, Shankar and Wang [**BSW**] proved that the polynomials $f(x) = x^k + a_1x^{k-1} + \cdots + a_{k-1}x + a_k$, whose rupture fields K have the required properties (including squarefree disc_K), have positive density when ordered by $\max\{|a_i|^{1/i} \mid 1 \le i \le k\}$.

3. *The proof*

To prove Theorem 1, we will use the following general theorem that we will then apply to suitable fields L (of degrees $\ell = 2, 3$).

THEOREM 4. *Let k, ℓ, m, n be positive integers such that $k = 3$ or $k \ge 5$.*

Assume that there is a totally real Galois number field L of degree $[L : \mathbb{Q}] = \ell$ whose Galois group is $\mathrm{Gal}(L/\mathbb{Q}) \simeq C_\ell$ and that contains elements $a_1, \ldots, a_n \in \mathcal{O}_L^+$ such that if an $\mathcal{O}_L$-lattice represents $a_1, \ldots, a_n$, then it has rank $\ge m$.

https://doi.org/10.1017/S0305004122000214 Published online by Cambridge University Press

There is $B>0$ (depending on k,ℓ,L,a_i) with the following property: for every totally real number field K of degree $[K:\mathbb{Q}]=k$ whose discriminant $\mathrm{disc}_K>B$ is coprime with disc_L and whose Galois closure $\widetilde{K}$ has Galois group $\mathrm{Gal}(\widetilde{K}/\mathbb{Q})\simeq S_k$, we have $[KL:\mathbb{Q}]=k\ell$ and

$$m(KL)\geq m.$$

Proof. Let $L,K,\widetilde{K}$ be as in the statement (with B to be specified later).

As disc_K and disc_L are coprime, we have $K\cap L=\mathbb{Q}$ (for $\mathrm{disc}_{K\cap L}$ is a common divisor of disc_K and disc_L by the formula for the discriminant of a tower of number fields [**Neu**, Corollary III·2·10]). Thus $[KL:\mathbb{Q}]=k\ell$. Let us use Galois theory to describe all subfields $\mathbb{Q}\subset M\subset KL$ (without giving references for all the theorems that we use – see any good textbook on Abstract Algebra).

First, consider $H=\widetilde{K}\cap L$. Since H is a subfield of L, we have $\mathrm{Gal}(H/\mathbb{Q})\simeq C_t$ for some $t\mid\ell$, and $\mathrm{Gal}(\widetilde{K}/H)$ is a normal subgroup of $\mathrm{Gal}(\widetilde{K}/\mathbb{Q})\simeq S_k$. The only such subgroups are S_k and A_k (as $k\neq 4$), and so correspondingly, $H=\mathbb{Q}$ or $H=\mathbb{Q}(\sqrt{\mathrm{disc}_K})$. But the latter case is impossible, as disc_K and disc_L are coprime, and so $\sqrt{\mathrm{disc}_K}\notin L$.

Thus $\widetilde{K}\cap L=\mathbb{Q}$, and so $\widetilde{K}L$ is Galois with

$$\mathrm{Gal}(\widetilde{K}L/\mathbb{Q})\simeq S_k\times C_\ell.$$

Further,

$$\mathrm{Gal}(\widetilde{K}L/KL)\simeq S_{k-1}\times\{1\}$$

(on the right-hand side, we will view S_{k-1} as the subgroup of S_k that consists of permutations fixing the element k).

Thus by Galois correspondence, the fields $\mathbb{Q}\subset M\subset KL$ correspond to subgroups

$$S_k\times C_\ell\supset G\supset S_{k-1}\times\{1\}.$$

We claim that for each such subgroup, we have $G\subset S_{k-1}\times C_\ell$ or $G\supset S_k\times\{1\}$.

For if $G\not\subset S_{k-1}\times C_\ell$, then there is an element $(\sigma,u)\in G$ with $\sigma\notin S_{k-1}$. Considering the decomposition of $\sigma\in S_k$ into disjoint cycles, we can write $\sigma=\tau(i_1\cdots i_jk)$ where $\tau\in S_{k-1}, j\geq 1$, and $(i_1\cdots i_jk)$ denotes the cycle of length $j+1$ that permutes $i_1,\cdots,i_j,k$ in the given order. Multiplying $(\sigma,u)\in G$ from the left by $((i_1\cdots i_j)^{-1}\tau^{-1},1)\in S_{k-1}\times\{1\}\subset G$, we obtain $((i_jk),u)\in G$. If we finally conjugate this element by $((1i_j),1)\in S_{k-1}\times\{1\}\subset G$, we get $((1k),u)\in G$.

If the order o of u in C_ℓ is odd, then $((1k),1)=((1k),u)^o\in G$. If o is even, then also

$$\begin{aligned}G\ni((12),1)[((1k),u)((12),1)((1k),u)((1k),u)^{o-2}]((12),1)\\ =((12),1)((2k),1)((12),1)=((1k),1).\end{aligned}$$

Thus $G\supset S_k\times\{1\}$ (as $((1k),1)\in G$ and $G\supset S_{k-1}\times\{1\}$), as we wanted to show.

Correspondingly, each intermediate field $\mathbb{Q}\subset M\subset KL$ satisfies

$$M\supset K \text{ or } M\subset L.$$

Let us finally specify that

$$\mathrm{disc}_K>B \text{ for } B=\max_M\left(\left(\frac{keT}{\ell c_{ke}}\right)^{(k^2e-k)/2}\right),$$

https://doi.org/10.1017/S0305004122000214 Published online by Cambridge University Press

where the maximum is taken over all fields M such that $K \subset M \subset KL$, $e = [M : K]$, $T = 4\max\{\mathrm{Tr}_{L/\mathbb{Q}}(a_i a_j) \mid 1 \le i < j \le n\}$ and c_{ke} are the constants from Proposition 2.

Let (Λ, Q) be a universal $\mathcal{O}_{KL}$-lattice. As $L \subset KL$, the lattice Λ represents all the elements $a_1, \ldots, a_n \in \mathcal{O}_L^+$; fix vectors $v_i \in \Lambda$ such that $Q(v_i) = a_i$. We will show that Λ has rank $\ge m$ by showing that the Gram matrix $(B(v_i, v_j))_{1\le i,j\le n}$ corresponding to the vectors v_i has rank $\ge m$.

We have $B(v_i, v_i) = Q(v_i) = a_i$ and let $B(v_i, v_j) = b_{ij}/2$ for all $i \ne j$ and suitable $b_{ij} \in \mathcal{O}_{KL}$. We will now show that $b_{ij} \in L$ for all $i \ne j$.

Assume that this is not the case for some $i \ne j$ and let $M = \mathbb{Q}(b_{ij})$. By the description of possible fields $\mathbb{Q} \subset M \subset KL$ obtained above, we have that $M \supset K$. Let $[M : K] = e$; then $\mathrm{disc}_M \ge \mathrm{disc}_K^e$ (again by the formula for the discriminant of a tower).

As the $\mathcal{O}_{KL}$-lattice Λ is totally positive, we have the Cauchy–Schwartz inequality $4a_i a_j \succeq b_{ij}^2$ (see Section 2).

Taking traces and applying Proposition 2 for the field M of degree $[M : \mathbb{Q}] = ke$, we get

$$kT \ge \mathrm{Tr}_{KL/\mathbb{Q}}(4a_i a_j) \ge \mathrm{Tr}_{KL/\mathbb{Q}}(b_{ij}^2) = \frac{\ell}{e}\mathrm{Tr}_{M/\mathbb{Q}}(b_{ij}^2) \ge \frac{\ell}{e} c_{ke} \Delta_{M/\mathbb{Q}}(b_{ij})^{2/((ke)^2 - ke)}.$$

As b_{ij} does not lie in a proper subfield of M, we have $\Delta_{M/\mathbb{Q}}(b_{ij}) \ne 0$, and so $\Delta_{M/\mathbb{Q}}(b_{ij}) \ge \mathrm{disc}_M \ge \mathrm{disc}_K^e > B^e$. Thus

$$kT > \frac{\ell}{e} c_{ke} B^{2/(k^2 e - k)},$$

contradicting the choice of B.

We proved that $b_{ij} \in L$ for all $i \ne j$.

Therefore all the entries of the Gram matrix $(B(v_i, v_j))_{1\le i,j\le n}$ lie in L, and so this matrix corresponds to an $\mathcal{O}_L$-lattice Λ' that represents all the elements $a_1, \ldots, a_n$ over L. By the assumption of the theorem, every such lattice has rank $\ge m$.

Accordingly, the Gram matrix $(B(v_i, v_j))_{1\le i,j\le n}$ has rank $\ge m$, which finally implies that the rank of Λ is also $\ge m$.

We can now finally use the preceding result to prove our main theorem.

THEOREM (Theorem 1, lattice-theoretic formulation). *Let d and m be positive integers such that d is divisible by 2 or 3. Then there are infinitely many totally real number fields F of degree $[F : \mathbb{Q}] = d$ over which every totally positive universal quadratic $\mathcal{O}_F$-lattice has rank at least m, i.e., $m(F) \ge m$.*

Proof. For $d = 2, 4, 8$, this was proved by Kala–Svoboda [**KS**, Theorem 1], and for $d = 3$ by Yatsyna [**Ya**, Theorem 5].

If $d = 6$ or $d \ge 10$ is even, choose $\ell = 2$ and $k = d/2$; we have $k = 3$ or $k \ge 5$.

By [**Ka**, Section 4], there are (infinitely many) real quadratic fields $L = \mathbb{Q}(\sqrt{D})$ that contain $n = m$ elements ($\alpha_1, \alpha_3, \ldots, \alpha_{2M+1}$ in the notation of [**Ka**] for $M = m - 1$) such that their corresponding Gram matrix is diagonal by [**Ka**, Proposition 4·1], and so every $\mathcal{O}_K$-lattice that represents these elements has rank $\ge m$.

https://doi.org/10.1017/S0305004122000214 Published online by Cambridge University Press

By Proposition 3, there are infinitely many fields K of degree $k = d/2$ with the properties required by Theorem 4, and so for each of them we have $[KL : \mathbb{Q}] = d$ and $m(KL) \geq m$, as needed.

If $d = 9$ or $d \geq 15$ is divisible by 3, choose $\ell = 3$ and $k = d/3$; again $k = 3$ or $k \geq 5$.

Let $n = \max(9m^2, 240)$ and let us consider Shanks' *simplest cubic fields* [Sh] $L = \mathbb{Q}(\rho)$ (where ρ is a root of the polynomial $x^3 - ax^2 - (a+3)x - 1$ for some $a \in \mathbb{Z}_{\geq -1}$). Each simplest cubic field L is Galois with $\mathrm{Gal}(L/\mathbb{Q}) \simeq C_3$.

Kala–Tinková [KT, Subsection 7·2] proved that there are (infinitely many) such fields L that contain n elements $a_1, a_2, \ldots, a_n \in \mathcal{O}_L^+$ and an element $\delta \succ 0$ in the codifferent $\{\alpha \in L \mid \mathrm{Tr}_{L/\mathbb{Q}}(\alpha\beta) \in \mathbb{Z}$ for all $\beta \in \mathcal{O}_L\}$ with $\mathrm{Tr}_{L/\mathbb{Q}}(\delta a_i) = 1$ for all i. By [KT, Subsection 7·2 and Proof of Proposition 7·4], if an $\mathcal{O}_L$-lattice represents all the elements $a_1, \ldots, a_n$, then it has rank $\geq \sqrt{n}/3 = m$.

It again just remains to use Proposition 3 and Theorem 4.

This covers all the positive integers d that are divisible by 2 or 3, finishing the proof.

In Theorem 4, one can directly claim that $m(KL) \geq m(L)$ instead of assuming the existence of suitable elements $a_1, \ldots, a_n$, for such elements with $m = m(L)$ always exist:

THEOREM 5 ([CO, Corollary 5·8]). *Let F be a totally real number field. There is a finite set $S \subset \mathcal{O}_F^+$ such that if an $\mathcal{O}_F$-lattice represents all the elements of S, then it is universal.*

Over the rationals $\mathcal{O}_F = \mathbb{Z}$ this is just a weak version of the famous 290-theorem [BH]. More generally, Kim–Kim–Oh [KKO] proved a similar result for representations of quadratic forms by quadratic forms (over $\mathbb{Z}$), and remarked that their theorem should also hold over number fields. This was indeed recently established by Chan–Oh [CO] (a similar result was also announced by L. Sun [Su]).

Note that Theorem 4 also holds with different Galois groups than C_ℓ and S_k [Do] (for example, already [KS] dealt with multiquadratic fields F, i.e., $\mathrm{Gal}(F/\mathbb{Q}) \simeq C_2^h$). However, the present formulation is sufficient for the proof of our main Theorem 1, and a more general statement probably would not bring more clarity.

Finally, let us comment that the most direct way of extending Theorem 1 to all degrees $d > 1$ does not work: We would need to know the existence of (infinitely many) totally real cyclic fields L of any prime degree $\ell \geq 5$ that contain suitable elements $a_1, \ldots, a_n$. To ensure the existence of these elements, it is very helpful for L to have a power integral basis and units of all signatures (e.g., for then Yatsyna's "Condition (A)" [Ya] is satisfied). However, Gras [Gr] showed that the only totally real cyclic fields L of prime degree $\ell \geq 5$ with a power integral basis are the maximal real subfields of a cyclotomic field, i.e., there is only one such field in a given degree. Thus one would need to work with fields without power integral basis, or with different Galois structure.

Acknowledgments. I thank Giacomo Cherubini, Jakub Krásenský, Ari Shnidman, Hanson Smith, Bára Tížková, and Pavlo Yatsyna for our interesting discussions and for their helpful suggestions. I also thank the anonymous referee for several useful corrections.

REFERENCES

[Bh] M. BHARGAVA. On the Conway–Schneeberger fifteen theorem. *Contemp. Math.* **272** (1999), 27–37.

[BH] M. BHARGAVA and J. HANKE. Universal quadratic forms and the 290-theorem. Preprint.

[BSW] M. BHARGAVA, A. SHANKAR and X. WANG. Squarefree values of polynomial discriminants I. *Invent. Math.* (to appear), https://arxiv.org/abs/1611.09806.

[BK1] V. BLOMER and V. KALA. Number fields without universal n-ary quadratic forms. *Math. Proc. Camb. Phil. Soc.* **159** (2015), 239–252.

[BK2] V. BLOMER, V. KALA. On the rank of universal quadratic forms over real quadratic fields. *Doc. Math.* **23** (2018), 15–34.

[CL+] M. ČECH, D. LACHMAN, J. SVOBODA, M. TINKOVÁ and K. ZEMKOVÁ. Universal quadratic forms and indecomposables over biquadratic fields. *Math. Nachr.* **292** (2019), 540–555.

[CKR] W. K. CHAN, M.-H. KIM and S. RAGHAVAN. Ternary universal integral quadratic forms. *Japan. J. Math.* **22** (1996), 263–273.

[CO] W. K. CHAN and B.-K. OH. Can we recover an integral quadratic form by representing all its subforms?. Preprint, https://arxiv.org/abs/2201.08957.

[De] J. I. DEUTSCH. Universality of a non-classical integral quadratic form over $\mathbb{Q}(\sqrt{5})$. *Acta Arith.* **136** (2009), 229–242.

[Do] M. DOLEŽÁLEK. Subfields of number field extensions and quadratic forms. *Bachelor's thesis*. Charles University (2022, to appear).

[EK] A. G. EARNEST and A. KHOSRAVANI. Universal positive quaternary quadratic lattices over totally real number fields. *Mathematika* **44** (1997), 342–347.

[Gr] M.-N. GRAS. Non monogénéité de l'anneau des entiers des extensions cycliques de $\mathbb{Q}$ de degré premier $l \geq 5$. *J. Number Theory* **23** (1986), 347–353.

[HKK] J. S. HSIA, Y. KITAOKA and M. KNESER. Representations of positive definite quadratic forms. *J. Reine Angew. Math.* **301** (1978), 132–141.

[Ka] V. KALA. Universal quadratic forms and elements of small norm in real quadratic fields. *Bull. Aust. Math. Soc.* **94** (2016), 7–14.

[KS] V. KALA and J. SVOBODA. Universal quadratic forms over multiquadratic fields. *Ramanujan J.* **48** (2019), 151–157.

[KT] V. KALA and M. TINKOVÁ. Universal quadratic forms, small norms and traces in families of number fields. *Int. Math. Res. Not. IMRN* (to appear), https://arxiv.org/abs/2005.12312.

[KY] V. KALA and P. YATSYNA. Lifting problem for universal quadratic forms. *Adv. Math.* **377** (2021), 107497, 24 pp.

[Kal] S. KALYANSWAMY. Inverse Galois Problem for Totally Real Number Fields. Cornell University Mathematics Department Senior Thesis, 2012. http://pi.math.cornell.edu/files/Research/SeniorTheses/kalyanswamyThesis.pdf.

[Ke] K. S. KEDLAYA. A construction of polynomials with squarefree discriminants. *Proc. Amer. Math. Soc.* **140** (2012), 3025–3033.

[Ki] B. M. KIM. Universal octonary diagonal forms over some real quadratic fields. *Comment. Math. Helv.* **75** (2000), 410–414.

[KKO] B. M. KIM. M.-H. KIM and B.-K. OH. A finiteness theorem for representability of quadratic forms by forms. *J. Reine Angew. Math.* **581** (2005), 23–30.

[KKP] B. M. KIM, M.-H. KIM and D. PARK. Real quadratic fields admitting universal lattices of rank 7. *J. Number Theory* **233** (2022), 456–466.

[KTZ] J. KRÁSENSKÝ, M. TINKOVÁ and K. ZEMKOVÁ. There are no universal ternary quadratic forms over biquadratic fields. *Proc. Edinb. Math. Soc.* **63** (2020), 861–912.

[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** (1941), 185–191.

[Neu] J. NEUKIRCH. *Algebraic Number Theory* (Springer-Verlag, Berlin, 1999).

[OM] O. T. O'MEARA. *Introduction to Quadratic forms* (Springer-Verlag, Berlin, 1973).

[Sch] I. SCHUR. Über die Verteilung der Wurzeln bei gewissen algebraischen Gleichungen mit ganzzahligen Koeffizienten. *Math. Z.* **1** (1918), 377–402.

[Sh] D. SHANKS. The simplest cubic number fields. *Math. Comp.* **28** (1974), 1137–1152.

[Si] C. L. SIEGEL. Sums of m th powers of algebraic integers. *Ann. of Math.* **46** (1945), 313–339.

[Su] L. SUN. A finiteness theorem for quadratic forms. Preprint.

[Ya] P. YATSYNA. A lower bound for the rank of a universal quadratic form with integer coefficients in a totally real field. *Comment. Math. Helv.* **94** (2019), 221–239.

https://doi.org/10.1017/S0305004122000214 Published online by Cambridge University Press