Sums of integral squares in number fields

Jakub Krásenský

Based on joint works with M. Raška, E. Sgallová, P. Yatsyna and R. Scharlau

Charles University (Prague)

June 2, 2023

QFs in number theory – what can we study?

- General question: Given a quadratic form Q over a ring R, determine which elements of R it represents.
  - Very hard even for $R = \mathbb{Z}$.
  - For $\mathbb{Q}$ (and number fields in general) solved by the Hasse–Minkowski theorem = local–global principle.
- Lagrange, 1770: Every nonnegative element of $\mathbb{Z}$ can be written as a sum of four squares.
- Two types of generalisations:
  - Replacing $x^2 + y^2 + z^2 + w^2$ by another quadratic form $\rightarrow$ *universal forms*.
  - If we replace $\mathbb{Z}$ by R, what should replace "nonnegative element" and "four"? $\rightarrow$ this talk.

- Maaß, 1941: Every totally nonnegative element of $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ can be written as a sum of three squares.
- Can $\frac{1+\sqrt{5}}{2}$ be written as a sum of squares?
- Suppose that $\sum(a_i + b_i\sqrt{5})^2 = \frac{1+\sqrt{5}}{2}$ for $a_i, b_i \in \mathbb{Q}$.
- Then $\sum(a_i - b_i\sqrt{5})^2 = \frac{1-\sqrt{5}}{2} < 0$.
- We call $a + b\sqrt{5} \in \mathbb{Q}(\sqrt{5})$ *totally nonnegative* if $a + b\sqrt{5} \geq 0$ and $a - b\sqrt{5} \geq 0$.
- But: $\frac{1+\sqrt{5}}{2} = \left(\frac{1+\sqrt{5}}{2}\right)^2 + \mathrm{i}^2$ is a sum of squares in $\mathbb{Q}(\frac{1+\sqrt{5}}{2}, \mathrm{i})$.

Number fields

- A *number field* is a field K with $[K : \mathbb{Q}]$ is finite. (We can always write $K = \mathbb{Q}(\alpha)$ for an algebraic number α.)
- We call K *totally real* if all embeddings $K \hookrightarrow \mathbb{C}$ actually map $K \hookrightarrow \mathbb{R}$. ($\mathbb{Q}(\alpha)$ is totally real if all conjugates of α are real.)
  - Examples: $\mathbb{Q}$, $\mathbb{Q}(\sqrt{3})$; non-examples: $\mathbb{Q}(\mathrm{i})$, $\mathbb{Q}(\sqrt[3]{2})$
- If in all embeddings $\sigma : K \hookrightarrow \mathbb{R}$ we have $\sigma(\alpha) > 0$, then α is *totally positive*, denoted by $\alpha \succ 0$.
  - Sums of squares are totally positive.
  - The set K^+ of tot. positive elements is closed under addition and multiplication.
- The ring of integers of K is
  $\mathcal{O}_K = \{\alpha \in K \mid \alpha \text{ is a root of a monic } \mathbb{Z}\text{-polynomial}\}$.
- An *order* is any subring $\mathcal{O} \subseteq \mathcal{O}_K$ with fraction field K. Every order has an *integral basis* – it is a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$.

- In $\mathbb{Z} = \mathcal{O}_{\mathbb{Q}}$, every (totally) positive integer is a sum of four squares.
- In $\mathbb{Z}[\frac{1+\sqrt{5}}{2}] = \mathcal{O}_{\mathbb{Q}(\sqrt{5})}$, every totally positive integer is a sum of three squares.
- Siegel, 1945: For a totally real number field $K \neq \mathbb{Q}, \mathbb{Q}(\sqrt{5})$, not all totally positive integers are sums of integral squares.
    - Hence, universal forms and sums of squares are distinct topics.

Definitions

- For a ring R, we put $\sum R^2 = \left\{\sum_{i=1}^N \alpha_i^2 \mid N \in \mathbb{N}, \alpha_i \in R\right\}$.
- The *length* of an element:
  $\ell(\alpha) =$ “smallest N such that $\alpha = \sum_{i=1}^N \alpha_i^2$”.
  - $\ell(7) = 4$ in $\mathbb{Z}$,
  - $\ell(-1) = \infty$ in $\mathbb{Z}$,
  - $\ell(-1) = 1$ in $\mathbb{Z}[\mathrm{i}]$.
- The *Pythagoras number*: $\mathcal{P}(R) = \sup_{\alpha \in \sum R^2} \ell(\alpha)$.
- $\mathcal{P}(\mathbb{Z}) = 4, \mathcal{P}(\mathbb{Z}[\frac{1+\sqrt{5}}{2}]) = 3$.
- $\mathcal{P}(\mathbb{C}) = 1, \mathcal{P}(\mathbb{R}) = 1, \mathcal{P}(\mathbb{Q}) = 4$.
- $\mathcal{P}(\mathbb{Z}[x]) = \infty$.

Local conditions

- To determine whether a quadratic form (over a number field or an order) represents a given element, we can use certain necessary conditions called "local conditions". Examples:
  - Over $\mathbb{Q}$, $x^2 + y^2$ is always positive. (A "real condition".)
  - Over $\mathbb{Q}$, $v_3(x^2 + y^2)$ is always even. (Condition "modulo p".)
- For $\mathbb{Q}$, they are expressed in terms of the embedding $\mathbb{Q} \hookrightarrow \mathbb{R}$ and the embeddings $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ for all primes p.
- For a number field K, the local conditions use all completions of K, i.e. all embeddings $K \hookrightarrow \mathbb{C}$ and all completions $K_{\mathfrak{p}}$, where $\mathfrak{p}$ is a prime ideal.
- They may seem scary, but in fact the local work is quite easy.
- A quadratic form "satisfies the local–global principle" if these local conditions are sufficient.
- For example, over $\mathbb{Z}$, this holds for the forms $x^2 + y^2$ (two-squares theorem), $x^2 + y^2 + z^2$ (three-squares theorem) and $x^2 + y^2 + z^2 + w^2$ (four-squares theorem).

The simple cases

- Hasse–Minkowski theorem: Over a number **field**, the local–global principle holds for every quadratic form.
- Corollary: $\mathcal{P}(K) \leq 4$ (and explicit values are known).
  - This is just because the same is true for every local field: $K_{\mathfrak{p}}, \mathbb{R}, \mathbb{C}$.
- Theory of spinor genera: If K is not tot. real, then local–global principle holds for forms over $\mathcal{O}_K$ in at least four variables.
- Corollary: $\mathcal{P}(\mathcal{O}_K) \leq 4$ unless K is totally real.
- Similarly: $\mathcal{P}(\mathcal{O}) \leq 5$ unless K is totally real.
- But what about $\mathcal{P}(\mathcal{O}_K)$ for totally real K?
- Also, the local–global principle provides a simple description of $\sum K^2$ resp. $\sum \mathcal{O}^2$. What can be said about it if local–global principle fails?

Two partial converses:

Theorem (Hsia–Kitaoka–Kneser, 1978)

Let Q be a quadratic form over $\mathcal{O}_K$ in at least five variables. There is a bound $c(Q, K)$ such that the local–global principle holds for representations of all α with $\mathrm{N}(\alpha) > c(Q, K)$.

- Corollary: $\mathcal{P}(\mathcal{O}_K)$ is finite even when K totally real.
- Corollary: In every $\mathcal{O}_K$ there is a universal quadratic form.
- Unfortunately, the bound is very impractical.

Two partial converses:

Theorem

Let Q be a quadratic form over $\mathcal{O}_K$. If $h(Q) = 1$ (the class number), then the local–global principle holds for Q.

- The computation of $h(Q)$ can be done in Magma, OSCAR, ...
- This lies behind the 2-, 3- and 4-square theorems over $\mathbb{Z}$ and behind $\mathcal{P}(\mathcal{O}_{\mathbb{Q}(\sqrt{5})}) = 3$.
- Dzewas(?): $h(I_3) = h(x^2 + y^2 + z^2) = 1$ over $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$. Thus $\mathcal{P}(\mathcal{O}_K) = 3$ and $\sum \mathcal{O}_K^2$ is described by local conditions. *(Why is $2 + \sqrt{2}$ not a sum of squares?)*
- Unfortunately, $h(I_3) = 1$ only for six totally real fields.

Theorem (K., 2022)

Let $K = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$. Then:

- $\mathcal{P}(\mathcal{O}_K) = 4$.
- $\sum \mathcal{O}_K^2 = \{\alpha \in \mathcal{O}_K \mid \alpha \succcurlyeq 0, \mathrm{N}(\alpha) \neq 7\}$.

Theorem (K., 2022)

Let $K = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$*. Then:*

- $\mathcal{P}(\mathcal{O}_K) = 4$.
- $\sum \mathcal{O}_K^2 = \{\alpha \in \mathcal{O}_K \mid \alpha \succcurlyeq 0, \mathrm{N}(\alpha) \neq 7\}$.

Steps of the proof:

- $h(I_3) = 1$. Check local conditions for representations as sums of three squares.
  - These are total positivity and a condition in $(\mathcal{O}_K)_{(2)}$.
- If $\alpha = \sum_{i=1}^{N} \alpha_i^2$, show that either α or $\alpha - \alpha_i^2$ satisfies these conditions for some i.
- Hence this $\alpha - \alpha_i^2$ is a sum of three squares.
- The second claim exploits the characterisation of *additively indecomposable integers* in *simplest cubic fields* by Magda Tinková and Víťa Kala.

About the set $\sum \mathcal{O}^2$

- In any ring R, a sum of squares is a square modulo $2R$.
  - Thus $2+\sqrt{2} \notin \sum \mathcal{O}^2_{\mathbb{Q}(\sqrt{2})}$.
- The only local conditions for $\alpha \in \mathcal{O}$ to be a sum of squares are $\alpha \succcurlyeq 0$ and $\alpha = \square \pmod{2\mathcal{O}}$.
- Under these conditions, α is locally a sum of four squares.
- Conjecture (R. Scharlau, 1979): There are only finitely many tot. real orders where $\sum \mathcal{O}^2$ contains *all* such numbers.
  - Only six such orders are known: $\mathcal{O}_K$ for $K = \mathbb{Q}; \mathbb{Q}(\sqrt{n})$ for $n = 2, 3, 5$; $\mathbb{Q}(\sqrt{2}, \sqrt{5})$; $\mathbb{Q}(\zeta_{20}+\zeta_{20}^{-1})$.
  - Local–global principle fails spectacularly. (Not even tons of variables rescue the situation!)
  - On the other hand, there are only finitely many exceptions up to multiplication by units. *(You have already heard the core of the argument.)*

Theorem (Peters; Cohn and Pall; Dzewas; Kneser; Maaß)

Let $\mathcal{O}$ be an order in a real quadratic number field. Then

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

The maximal length is attained for example by:

- *Length 3:* $1+\sqrt{2}^2+(1+\sqrt{2})^2$, $2+(2+\sqrt{3})^2$, $2+\left(\frac{1+\sqrt{5}}{2}\right)^2$;
- *Length 4:* $3+(1+\sqrt{6})^2$, $3+(1+\sqrt{7})^2$, $3+(1+\sqrt{5})^2$;
- *Length 5:* $3+\left(\frac{1+\sqrt{13}}{2}\right)^2+\left(1+\frac{1+\sqrt{13}}{2}\right)^2$ *in* $\mathbb{Z}\left[\frac{1+\sqrt{13}}{2}\right]$; *in all the remaining cases* $7+(1+f\sqrt{n})^2$ *or* $7+\left(f\frac{1+\sqrt{n}}{2}\right)^2$.

Together with $\mathcal{P}(\mathcal{O}) \leq 5$ for not-totally-real orders, this lead Peters to conjecture $\mathcal{P}(\mathcal{O}) \leq 5$ for all number field orders.

Theorem (R. Scharlau, 1980)

There are totally real number fields with arbitrarily large $\mathcal{P}(\mathcal{O}_K)$.

The proof uses multiquadratic fields $\mathbb{Q}(\sqrt{n_1}, \sqrt{n_2}, \ldots, \sqrt{n_k})$ for pairwise coprime square-free n_j.

Theorem (Kala–Yatsyna, 2021)

There exists a function $g(d)$ *such that for every field* K *with* $d = [K : \mathbb{Q}]$ *and every order* $\mathcal{O} \subseteq \mathcal{O}_K$ *one has*

$$\mathcal{P}(\mathcal{O}) \leq g(d).$$

- In particular, $\mathcal{P}(\mathcal{O}) \leq 5$ for quadratic, ≤ 6 for cubic and ≤ 7 for quartic orders.
- It seems that typically, this upper bound is the correct value:
  - For real quadratic orders, there are only six exceptions.
  - And there is the next slide.

Let ρ_a be a root of $x^3 - ax^2 - (a+3)x - 1$ for an integer $a \geq -1$. Then $K(\rho_a)$ is called a *simplest cubic field*.

Theorem (Tinková, 2023+)

Let $K = \mathbb{Q}(\rho_a)$ *for* $a \geq 2$. *Then* $\mathcal{P}(\mathbb{Z}[\rho_a]) = 6$.

Theorem (K.–Raška–Sgallová, 2022)

There are infinitely many biquadratic fields K *with* $\mathcal{P}(\mathcal{O}_K) = 7$*: In particular, it holds for every* $K = \mathbb{Q}(\sqrt{p}, \sqrt{q})$ *where* $p, q > 7$ *are coprime square-free integers,* $p \equiv 2, q \equiv 3 \pmod 4$.

Theorem (K., 2023+)

Every real biquadratic field K *contains infinitely many orders* $\mathcal{O}$ *with* $\mathcal{P}(\mathcal{O}) = 7$.

Lower bounds

- $\mathcal{P}(\mathcal{O}) \geq \mathcal{P}(K) = 4$ for any order $\mathcal{O}$ in number field K of odd degree. (By Springer's theorem, $7 \neq \square + \square + \square$ in K.)
- For a given totally real order $\mathcal{O}$, one can just pick any $\alpha \in \sum \mathcal{O}^2$; $\ell(\alpha)$ is a lower bound on $\mathcal{P}(\mathcal{O})$.
  E.g. $\mathcal{P}(\mathbb{Z}) \geq \ell(7) = 4$.
- Computing the length of a given α is straightforward.
- For real biquadratic fields K, Raška implemented a systematic search for elements of large length in $\mathcal{O}_K$: `https://github.com/raskama/number-theory/tree/main/biquadratic`
- The mentioned results on quadratic, cubic and biquadratic fields depend on finding a suitable α in *every* such order.

Theorem (K.–Raška–Sgallová, 2022)

- *Let K be a real biquadratic field. Then $\mathcal{P}(\mathcal{O}_K) \geq 5$ unless K is one of at most seven exceptions.*
- *Fix a square-free positive $n > 7$. Then $\mathcal{P}(\mathcal{O}_K) \geq 6$ for all but finitely many real biquadratic fields $K \ni \sqrt{n}$.*
- *But: Let K be a biquadratic field containing $\sqrt{5}$. Then $\mathcal{P}(\mathcal{O}_K) \leq 5$.*

Conjecture

Let K be a real biquadratic field.

1. If K contains $\sqrt{2}$ or $\sqrt{5}$, then $\mathcal{P}(\mathcal{O}_K) \leq 5$.
   (Proof completed by He and Hu, 2022+.)
2. If K contains none of $\sqrt{2}$ and $\sqrt{5}$, then $\mathcal{P}(\mathcal{O}_K) \geq 6$ holds with finitely many exceptions.
3. "There are indeed exceptions.": Among the real biq. fields, there are three with $\mathcal{P}(\mathcal{O}_K) = 3$ and four with $\mathcal{P}(\mathcal{O}_K) = 4$.

Theorem (K.–Scharlau, 2023+)

Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{5})$ *and* $L = \mathbb{Q}(\zeta_{20} + \zeta_{20}^{-1}) = \mathbb{Q}\left(\sqrt{\frac{5+\sqrt{5}}{2}}\right)$. *Then*

$$\mathcal{P}(\mathcal{O}_K) = \mathcal{P}(\mathcal{O}_L) = 3.$$

The proof is based on examining the other forms in the genus of I_3, see next slide.

Conjecture

There are precisely three other totally real quartic fields K with $\mathcal{P}(\mathcal{O}_K) = 3$, namely $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ and $\mathbb{Q}(\zeta_{16} + \zeta_{16}^{-1})$.

Sketch of the proof

The genus of I_3 over $K = \mathbb{Q}(\sqrt{2}, \sqrt{5})$ consists of two equivalence classes, with representatives I_3 and Q_3, where

$$Q_3(x, y, z) = 2x^2 + 2y^2 + 3z^2 + 2\overline{\varphi}xy - 2\sqrt{2}xz + 2\sqrt{2}\varphi yz$$

$(\varphi = \frac{1+\sqrt{5}}{2}$ and $\overline{\varphi} = \frac{1-\sqrt{5}}{2})$. Thus:

Proposition

If $\alpha \in \mathcal{O}_K$ is locally a sum of squares, then it is represented either by I_3 or by Q_3.

It remains to show the following:

Lemma

If $\alpha \in \mathcal{O}_K$ is represented by Q_3, then it is also represented by I_3.

Sketch of the proof

Proof.

$$
\begin{aligned}
&Q_3(a,b,c) = \\
&= \left(\tfrac{1}{\sqrt{2}}a\right)^2 + \left(\tfrac{\varphi}{\sqrt{2}}a + \overline{\varphi}c\right)^2 + \left(\tfrac{\overline{\varphi}}{\sqrt{2}}a + \sqrt{2}b + \varphi c\right)^2 \\
&= \left(\tfrac{1}{\sqrt{2}}b + c\right)^2 + \left(\tfrac{\varphi}{\sqrt{2}}b + c\right)^2 + \left(\sqrt{2}a + \tfrac{\overline{\varphi}}{\sqrt{2}}b - c\right)^2 \\
&= \left(\tfrac{1}{\sqrt{2}}(a+b) - \overline{\varphi}c\right)^2 + \left(\tfrac{\varphi}{\sqrt{2}}(a-b) - \varphi c\right)^2 + \left(\tfrac{\overline{\varphi}}{\sqrt{2}}(a+b)\right)^2 \\
&= \left(\tfrac{1}{\sqrt{2}}(a-\varphi b) - \varphi c\right)^2 + \left(\tfrac{1}{\sqrt{2}}(-\varphi a + \overline{\varphi}b)\right)^2 + \left(\tfrac{1}{\sqrt{2}}(\overline{\varphi}a + b) - \overline{\varphi}c\right)^2 \\
&= \left(\tfrac{1}{\sqrt{2}}(a+\overline{\varphi}b) - c\right)^2 + \left(\tfrac{1}{\sqrt{2}}(\varphi a - b) - c\right)^2 + \left(\tfrac{1}{\sqrt{2}}(\overline{\varphi}a - \varphi b) - c\right)^2.
\end{aligned}
$$

The squares in the first equality are integral iff $a \equiv 0$ (all the congruences are modulo $\sqrt{2}$), in the second iff $b \equiv 0$, in the third iff $a \equiv b$, in the fourth iff $a \equiv \varphi b$ and in the fifth iff $a \equiv \overline{\varphi}b$. □

The proof for the other field $\mathbb{Q}(\zeta_{20} + \zeta_{20}^{-1})$ is similar.

A proper list of references can be found in the following two papers:

- J. Krásenský, M. Raška and E. Sgallová, *Pythagoras numbers of orders in biquadratic fields*, Expo. Math. 40, 1181–1228 (2022). Available at arXiv:2105.08860.
- J. Krásenský and P. Yatsyna, *On quadratic Waring's problem in totally real number fields*, Proc. Amer. Math. Soc. 151, 1471–1485 (2023). Available at arXiv:2112.15243.

If you're interested, I encourage you to read the introductions.
Or contact me at **krasensky(at)seznam(dot)cz**.

Thank you for your attention (and for all your questions)!

Representation of QFs by QFs – informally

- A quadratic form φ is *represented* by a quadratic form Q over the same ring if we obtain φ from Q by plugging in suitable linear forms.
- Example: $\varphi(x, y) = 3x^2 + 4xy + 4y^2$ is represented by the sum-of-three-squares form I_3: $x^2 + x^2 + (x + 2y)^2$.
- Most definitions and some theorems from previous slides (for repr. of numbers by forms) can be adapted to this setting.
- Mordell, 1930s: Every binary QF over $\mathbb{Z}$ which is a sum of squares of linear forms (i.e. represented by some I_N) is already a sum of 5 squares.
- *New Waring's problem* studies precisely these *g-invariants*:

Definition

Let R be a ring. Denote by Σ_R^k the set of all k-ary quadratic forms which are represented by I_N for some (possibly large) N. We put

$$g_R(k) = \min\{n \in \mathbb{N} \mid \text{Every form in } \Sigma_R^k \text{ is represented by } I_n\}.$$

- THE upper bound: For $\mathcal{O} \subset K$ with $d = [K : \mathbb{Q}]$ we have

$$\mathcal{P}(\mathcal{O}) \leq g_{\mathbb{Z}}(d).$$

- $\mathcal{P}(R) = g_R(1)$.
- The values are known for R number field and (almost) for R not-totally-real order.
- Otherwise only:
  - $g_{\mathbb{Z}}(k) = k + 3$ for $k = 1, \ldots, 5$ (Mordell, Ko, 1930s) but $g_{\mathbb{Z}}(6) = 10$ (Kim, Oh 1997).
  - $g_{\mathcal{O}_{\mathbb{Q}(\sqrt{5})}}(2) = 5$ (Sasaki, 1993), $g_{\mathcal{O}_{\mathbb{Q}(\sqrt{2})}} = 5$ (He, Hu, 2022+).
  - $G_{\mathcal{O}_K}(2) = 7$ for all other real quadratic fields K other than $\mathbb{Q}(\sqrt{3})$ (K., Yatsyna, 2022).
    (Here G_R is the "correctly defined" g_R. It matches g_R if R is a UFD.)
- $\mathcal{P}(\mathcal{O}_K) \leq G_{\mathcal{O}_F}(d)$ for $[K : F] = d$ (K., Yatsyna, 2022).

Application for construction of universal forms

1) Via indecomposables

There are only finitely many indecomposable elements up to multiplication by squares. Let's say that every indecomposable element of $\mathcal{O}_K$ is $\gamma\square$, where $\gamma \in \{\gamma_1, \dots, \gamma_n\}$.

Proposition

There exists a universal quadratic form over K with $n\mathcal{P}(\mathcal{O}_K)$ elements.

Proof.

Every totally positive element can be written as a finite sum

$$\gamma_1\square + \gamma_1\square \cdots + \gamma_1\square + \gamma_2\square + \cdots ,$$

so it can be represented by the form

$$\gamma_1 I_{\mathcal{P}(\mathcal{O}_K)} \perp \dots \perp \gamma_n I_{\mathcal{P}(\mathcal{O}_K)}.$$

□

2) Via geometry of numbers

Theorem (Kala–Yatsyna)

Let K be a totally real number field with discriminant Δ. If $\alpha \in \mathcal{O}_K$ is totally positive element $\mathrm{N}(\alpha) > \Delta$, then there exists $\beta \in \mathcal{O}_K$ such that $\alpha - \beta^2$ is totally positive. (In particular, α is not indecomposable.)

This leads to a simple construction of a universal form:

Proposition

Let Q be a quadratic form which represents all totally positive elements of norm at most Δ. Then $Q \perp I_{\mathcal{P}(\mathcal{O}_K)}$ is universal.