Indecomposable integers and universal quadratic forms

Magdaléna Tinková
(with M. Čech, D. Lachman, J. Svoboda, and K. Zemková)

Department of Algebra, Faculty of Mathematics and Physics,
Charles University, Prague

This work was supported by the Charles University, project GA UK No. 1298218.

May 23, 2018

Outline

- $K = \mathbb{Q}(\beta)$ – totally real number field
- β – root of polynomial of degree d
- $\beta_1 = \beta, \beta_2, \ldots, \beta_d$ – real conjugates of β
- $\alpha \in K \Rightarrow \alpha = a_0 + a_1\beta + a_2\beta^2 + \cdots + a_{d-1}\beta^{d-1}$
- α is totally positive if

$$\begin{aligned} \alpha &= a_0 + a_1\beta + a_2\beta^2 + \cdots + a_{d-1}\beta^{d-1} > 0, \\ \alpha_2 &= a_0 + a_1\beta_2 + a_2\beta_2^2 + \cdots + a_{d-1}\beta_2^{d-1} > 0, \\ &\vdots \\ \alpha_d &= a_0 + a_1\beta_d + a_2\beta_d^2 + \cdots + a_{d-1}\beta_d^{d-1} > 0 \end{aligned}$$

- $\mathcal{O}_K$ – ring of algebraic integers of K
- $\mathcal{O}_K^+$ – totally positive elements of $\mathcal{O}_K$

Quadratic forms

Definition

Quadratic form Q over K with variables $x_1, x_2, \ldots, x_n$ is an expression

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

where $a_{ij} \in \mathcal{O}_K$.

Example

Sum of squares $\sum_{i=1}^{n} x_i^2$.

Our quadratic form is

- *totally positive definite* if $Q(\gamma_1, \dots, \gamma_n)$ is totally positive for all $\gamma_j \in \mathcal{O}_K$, not all zero;
- *classical* if $2|a_{ij}$ for all $i \neq j$;
- *universal* if it represents all elements of $\mathcal{O}_K^+$, i.e., for every $\alpha \in \mathcal{O}_K^+$, there exist $\gamma_1, \dots, \gamma_n \in \mathcal{O}_K$ such that

$$\alpha = \sum_{1 \leq i \leq j \leq n} a_{ij}\gamma_i\gamma_j$$

Assumption: Our forms are totally positive definite and classical.

Question: When are our forms universal?

Theorem (Lagrange, 1770; Maas, 1941)

The sum of four squares is universal over $\mathbb{Q}$. The sum of three squares is universal over $\mathbb{Q}(\sqrt{5})$.

Theorem (Siegel, 1945)

The sum of any number of squares is universal only over $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{5})$.

Conjecture (Kitaoka)

There are only finitely many fields which admit ternary universal quadratic forms.

Theorem (Chan, Kim, Raghavan, 1996)

The only quadratic number fields which admit ternary universal forms are $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, *and* $\mathbb{Q}(\sqrt{5})$.

Theorem (Blomer, Kala, 2015; Kala, 2016)

For each M, *there are infinitely many real quadratic fields that do not admit universal forms with* M *variables.*

Indecomposable integers

Definition

$\alpha \in \mathcal{O}_K^+$ is indecomposable if it cannot be expressed as $\alpha = \beta + \gamma$ where $\beta, \gamma \in \mathcal{O}_K^+$.

- indecomposable integers are difficult to represent by quadratic forms
- we often use them as coefficients of our forms

Quadratic case

- $K = \mathbb{Q}(\sqrt{p})$, p squarefree positive rational integer
- $\mathcal{O}_K = \mathbb{Z}[\sqrt{p}]$ or $\mathcal{O}_K = \mathbb{Z}[\frac{\sqrt{p}+1}{2}]$ for $p \equiv 1 \pmod 4$
- $[u_0, \overline{u_1, \ldots, u_s}]$ = continued fraction of $\sqrt{p}$ or $\frac{\sqrt{p}-1}{2}$
- $p_{-1} = 1, p_0 = u_0, p_{n+1} = p_{n-1} + u_{n+1}p_n$
- $q_{-1} = 0, q_0 = 1, q_{n+1} = q_{n-1} + u_{n+1}q_n$
- $\frac{p_n}{q_n} = [u_0, u_1, \ldots, u_n]$

Definition

Set

$$\alpha_n = p_n + q_n\sqrt{p},$$
$$\alpha_{n,r} = \alpha_n + r\alpha_{n+1}$$

where $0 \leq r \leq u_{n+2}$.

Elements α_n are called *convergents*.

Theorem (Perron, 1913; Dress, Scharlau, 1982)

The elements $\alpha_{n,r}$ where n is odd and $0 \leq r \leq u_{n+2}$ are all indecomposable integers in $\mathbb{Q}(\sqrt{p})$.

We do not have such a characterization of indecomposable integers in fields of higher degrees.

Biquadratic fields

- $K = \mathbb{Q}(\sqrt{p}, \sqrt{q})$, p, q squarefree positive rational integers, $p \neq q$
- $r = \frac{pq}{\gcd(p,q)^2}$
- K has quadratic subfields $\mathbb{Q}(\sqrt{p})$, $\mathbb{Q}(\sqrt{q})$ and $\mathbb{Q}(\sqrt{r})$

Our questions:

1. Which universal quadratic forms have we in biquadratic fields?
2. Do indecomposable integers from quadratic subfields remain indecomposable in our biquadratic field?

Ring of integers of K

Theorem (Williams, 1970)

The only possible integral bases for biquadratic fields are

1. $\left\{1, \sqrt{p}, \sqrt{q}, \frac{\sqrt{p}+\sqrt{r}}{2}\right\}$,
2. $\left\{1, \sqrt{p}, \frac{1+\sqrt{q}}{2}, \frac{\sqrt{p}+\sqrt{r}}{2}\right\}$,
3. $\left\{1, \frac{1+\sqrt{p}}{2}, \frac{1+\sqrt{q}}{2}, \frac{1\pm\sqrt{p}+\sqrt{q}+\sqrt{r}}{2}\right\}$.

Theorem (Čech, Lachman, Svoboda, T., Zemková, 2018)

In cases 1. and 2., indecomposables from $\mathbb{Q}(\sqrt{q})$ *are indecomposable in* $\mathbb{Q}(\sqrt{p}, \sqrt{q})$.

Theorem (Čech, Lachman, Svoboda, T., Zemková, 2018)

If $p < r$, then convergents of $\sqrt{p}$ (resp. $\frac{\sqrt{p}-1}{2}$) remain indecomposable in $\mathbb{Q}(\sqrt{p}, \sqrt{q})$.

Theorem (Čech, Lachman, Svoboda, T., Zemková, 2018)

If $\sqrt{p} < M_p\sqrt{r}$, then indecomposables of $\mathbb{Q}(\sqrt{p})$ remain indecomposable in $\mathbb{Q}(\sqrt{p}, \sqrt{q})$.

Open question: Do indecomposable integers from quadratic subfields always remain indecomposable in our biquadratic field?

Universal forms over biquadratic fields

Theorem (Čech, Lachman, Svoboda, T., Zemková, 2018)

Any universal form over $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ must have at least 5 variables; over $\mathbb{Q}(\sqrt{6}, \sqrt{19})$ it must have at least 6 variables.

Thank you for your attention.