# Additive structure of non-monogenic simplest cubic fields

Magdaléna Tinková

Czech Technical University in Prague

Joint work with Daniel Gil-Muñoz.

April 18, 2023

- $K$ algebraic number field
- $d$ degree of $K$ over $\mathbb{Q}$
- $\mathcal{O}_K$ is the ring of algebraic integers in $K$

- $K$ algebraic number field
- $d$ degree of $K$ over $\mathbb{Q}$
- $\mathcal{O}_K$ is the ring of algebraic integers in $K$

### Definition

$K$ is monogenic if $\mathcal{O}_K = \mathbb{Z}[\gamma]$ for some $\gamma \in K$, i.e., every algebraic integer $\alpha \in \mathcal{O}_K$ can be expressed as

$$\alpha = a_0 + a_1\gamma + a_2\gamma^2 + \cdots + a_{d-1}\gamma^{d-1}$$

where $a_i \in \mathbb{Z}$ for all $0 \leq i \leq d-1$.

# Examples

## Example

$K$ real quadratic field $\Rightarrow K = \mathbb{Q}(\sqrt{D})$ where $D > 1$ is square-free

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{D}] & \text{if } D \equiv 2, 3 \pmod 4, \\ \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] & \text{if } D \equiv 1 \pmod 4) \end{cases}$$

$\rightarrow$ They are always monogenic.

# Examples

## Example

$K$ real quadratic field $\Rightarrow K = \mathbb{Q}(\sqrt{D})$ where $D > 1$ is square-free

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{D}] & \text{if } D \equiv 2,3 \pmod 4, \\ \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] & \text{if } D \equiv 1 \pmod 4 \end{cases}$$

$\rightarrow$ They are always monogenic.

## Example

$K = \mathbb{Q}(\eta)$ where $\eta$ is a root of $x^3 - x^2 - 2x - 8$ is not monogenic

# The simplest cubic fields

- introduced by Shanks (1974)
- $K = \mathbb{Q}(\rho)$ where $\rho$ is a root of $x^3 - ax^2 - (a+3)x - 1$ with $a \in \mathbb{Z}$, $a \geq -1$
- they are Galois extensions
- $\mathcal{O}_K = \mathbb{Z}[\rho]$ for infinitely many cases of $a$

# The simplest cubic fields

- introduced by Shanks (1974)
- $K = \mathbb{Q}(\rho)$ where $\rho$ is a root of $x^3 - ax^2 - (a+3)x - 1$ with $a \in \mathbb{Z}$, $a \geq -1$
- they are Galois extensions
- $\mathcal{O}_K = \mathbb{Z}[\rho]$ for infinitely many cases of $a$

## Example

- $\mathcal{O}_K = \mathbb{Z}[\rho]$ if $a^2 + 3a + 9$ is square-free

# The simplest cubic fields

- introduced by Shanks (1974)
- $K = \mathbb{Q}(\rho)$ where $\rho$ is a root of $x^3 - ax^2 - (a+3)x - 1$ with $a \in \mathbb{Z}$, $a \geq -1$
- they are Galois extensions
- $\mathcal{O}_K = \mathbb{Z}[\rho]$ for infinitely many cases of $a$

## Example

- $\mathcal{O}_K = \mathbb{Z}[\rho]$ if $a^2 + 3a + 9$ is square-free
- if $a = 0$, then $a^2 + 3a + 9 = 9$ is not square-free but still $\mathcal{O}_K = \mathbb{Z}[\rho]$

# Monogenic simplest cubic fields

let $\mathfrak{c}$ be the conductor of $K$

**Theorem (Kashio, Sekigawa, 2021)**

*Let $K$ be a simplest cubic fields. Then the following are equivalent:*

1. *The field $K$ is monogenic.*
2. *We have $a \in \{-1, 0, 1, 2, 3, 5, 12, 54, 66, 1259, 2389\}$ or $\frac{a^2+3a+9}{\mathfrak{c}}$ is a cube.*
3. *We have $a \in \{-1, 0, 1, 2, 3, 5, 12, 54, 66, 1259, 2389\}$ or $a \not\equiv 3, 21 \pmod{27}$ and $v_p(a^2+3a+9) \not\equiv 2 \pmod{3}$ for all primes $p \neq 3$.*

# Monogenic simplest cubic fields

let $\mathfrak{c}$ be the conductor of $K$

**Theorem (Kashio, Sekigawa, 2021)**

*Let $K$ be a simplest cubic fields. Then the following are equivalent:*

1. *The field $K$ is monogenic.*
2. *We have $a \in \{-1, 0, 1, 2, 3, 5, 12, 54, 66, 1259, 2389\}$ or $\frac{a^2+3a+9}{\mathfrak{c}}$ is a cube.*
3. *We have $a \in \{-1, 0, 1, 2, 3, 5, 12, 54, 66, 1259, 2389\}$ or $a \not\equiv 3, 21 \pmod{27}$ and $v_p(a^2 + 3a + 9) \not\equiv 2 \pmod 3$ for all primes $p \neq 3$.*

- If $\frac{a^2+3a+9}{\mathfrak{c}} = 1$, then $\mathcal{O}_K = \mathbb{Z}[\rho]$.

## Monogenic simplest cubic fields

let $\mathfrak{c}$ be the conductor of $K$

**Theorem (Kashio, Sekigawa, 2021)**

*Let $K$ be a simplest cubic fields. Then the following are equivalent:*

1. *The field $K$ is monogenic.*
2. *We have $a \in \{-1, 0, 1, 2, 3, 5, 12, 54, 66, 1259, 2389\}$ or $\frac{a^2+3a+9}{\mathfrak{c}}$ is a cube.*
3. *We have $a \in \{-1, 0, 1, 2, 3, 5, 12, 54, 66, 1259, 2389\}$ or $a \not\equiv 3, 21 \pmod{27}$ and $v_p(a^2+3a+9) \not\equiv 2 \pmod{3}$ for all primes $p \neq 3$.*

- If $\frac{a^2+3a+9}{\mathfrak{c}} = 1$, then $\mathcal{O}_K = \mathbb{Z}[\rho]$.
- If $\frac{a^2+3a+9}{\mathfrak{c}} \neq 1$ is a cube, then $\mathcal{O}_K = \mathbb{Z}[\gamma]$ for some $\gamma \neq \rho$.

$B_p(k,l) = \left\{1, \rho, \frac{k+l\rho+\rho^2}{p}\right\}$ where $p$ is a prime and $1 \leq k, l \leq p-1$

$B_p(k,l) = \left\{1, \rho, \frac{k+l\rho+\rho^2}{p}\right\}$ where $p$ is a prime and $1 \leq k, l \leq p-1$

**Proposition**

There exist infinitely many simplest cubic fields with the integral basis $B_p(k,l)$ if and only if $p = 3$ and $(k,l) = (1,1)$, or $p \equiv 1 \pmod 6$ and $(k,l)$ is one of two concrete pairs of $(k_1, l_1)$ and $(k_2, l_2)$ where values of $k_i$ and $l_i$ depend only on $p$.

$B_p(k,l) = \{1, \rho, \frac{k+l\rho+\rho^2}{p}\}$ where $p$ is a prime and $1 \leq k, l \leq p-1$

**Proposition**

There exist infinitely many simplest cubic fields with the integral basis $B_p(k,l)$ if and only if $p = 3$ and $(k,l) = (1,1)$, or $p \equiv 1 \pmod 6$ and $(k,l)$ is one of two concrete pairs of $(k_1, l_1)$ and $(k_2, l_2)$ where values of $k_i$ and $l_i$ depend only on $p$.

- $p = 3$ and $p \equiv 1 \pmod 6$ follows from the solvability of the equation $a^2 + 3a + 9 \equiv 0 \pmod{p^2}$

$B_p(k,l) = \left\{1, \rho, \frac{k+l\rho+\rho^2}{p}\right\}$ where $p$ is a prime and $1 \leq k, l \leq p-1$

**Proposition**

There exist infinitely many simplest cubic fields with the integral basis $B_p(k,l)$ if and only if $p = 3$ and $(k,l) = (1,1)$, or $p \equiv 1 \pmod 6$ and $(k,l)$ is one of two concrete pairs of $(k_1, l_1)$ and $(k_2, l_2)$ where values of $k_i$ and $l_i$ depend only on $p$.

- $p = 3$ and $p \equiv 1 \pmod 6$ follows from the solvability of the equation $a^2 + 3a + 9 \equiv 0 \pmod{p^2}$
- solutions $a_1$ and $a_2$ of $a^2 + 3a + 9 \equiv 0 \pmod{p^2}$ produce concrete values of $(k_1, l_1)$ and $(k_2, l_2)$ for which $\frac{k_i+l_i\rho+\rho^2}{p}$ is an algebraic integer

- $K$ totally real number field
- $\mathcal{O}_K^+$ set of totally positive elements $\alpha \in \mathcal{O}_K$, i.e., all conjugates of $\alpha$ are positive

- $K$ totally real number field
- $\mathcal{O}_K^+$ set of totally positive elements $\alpha \in \mathcal{O}_K$, i.e., all conjugates of $\alpha$ are positive

**Definition**

We say that $\alpha \in \mathcal{O}_K^+$ is indecomposable in $\mathcal{O}_K$ if it cannot be written as $\alpha = \beta + \gamma$ for any $\beta, \gamma \in \mathcal{O}_K^+$.

- only one indecomposable integer in $\mathbb{Z}$, namely $1$

# Results on indecomposable integers

- We know the precise structure of indecomposable integers in quadratic fields $\mathbb{Q}(\sqrt{D})$, where they can be described using the continued fraction of $\sqrt{D}$ or $\frac{\sqrt{D}-1}{2}$ (Perron, 1913; Dress, Scharlau, 1982).

# Results on indecomposable integers

- We know the precise structure of indecomposable integers in quadratic fields $\mathbb{Q}(\sqrt{D})$, where they can be described using the continued fraction of $\sqrt{D}$ or $\frac{\sqrt{D}-1}{2}$ (Perron, 1913; Dress, Scharlau, 1982).
- We also know their structure for several families of cubic fields (Kala, T., 2022; T., 2023+).

# Results on indecomposable integers

- We know the precise structure of indecomposable integers in quadratic fields $\mathbb{Q}(\sqrt{D})$, where they can be described using the continued fraction of $\sqrt{D}$ or $\frac{\sqrt{D}-1}{2}$ (Perron, 1913; Dress, Scharlau, 1982).
- We also know their structure for several families of cubic fields (Kala, T., 2022; T., 2023+).
- some partial results for biquadratic fields (Čech, Lachman, Svoboda, T., Zemková, 2019; Krásenský, T., Zemková, 2020)

**Theorem (Kala, T., 2022)**

*Let $K$ be the simplest cubic field with $a \geq -1$ such that $\mathcal{O}_K = \mathbb{Z}[\rho]$. The elements $1$, $1 + \rho + \rho^2$, and*

$$\alpha(v, w) = -v - w\rho + (v+1)\rho^2$$

*where $0 \leq v \leq a$ and $v(a+2)+1 \leq w \leq (v+1)(a+1)$ are, up to multiplication by totally positive units, all the indecomposable integers in $\mathbb{Q}(\rho)$.*

**Theorem (Kala, T., 2022)**

*Let $K$ be the simplest cubic field with $a \geq -1$ such that $\mathcal{O}_K = \mathbb{Z}[\rho]$. The elements $1$, $1+\rho+\rho^2$, and*

$$\alpha(v,w) = -v - w\rho + (v+1)\rho^2$$

*where $0 \leq v \leq a$ and $v(a+2)+1 \leq w \leq (v+1)(a+1)$ are, up to multiplication by totally positive units, all the indecomposable integers in $\mathbb{Q}(\rho)$.*

We provide analogous results for the simplest cubic fields with the basis $B_3(1,1) = \left\{1, \rho, \frac{1+\rho+\rho^2}{3}\right\}$.

# Universal quadratic forms

Quadratic form $Q(x_1, \ldots, x_n) = \sum_{1 \le i \le j \le n} a_{ij} x_i x_j$ with $a_{ij} \in \mathcal{O}_K$ is

- *classical* if $2 | a_{ij}$ for all $i \neq j$,
- *totally positive definite* if $Q(\gamma_1, \ldots, \gamma_n) \in \mathcal{O}_K^+$ for all $\gamma_i \in \mathcal{O}_K$ not all zero,
- *universal* over $\mathcal{O}_K$ if it represents all elements in $\mathcal{O}_K^+$

# Universal quadratic forms

Quadratic form $Q(x_1,\dots,x_n)=\sum_{1\leq i\leq j\leq n} a_{ij}x_ix_j$ with $a_{ij}\in\mathcal{O}_K$ is

- *classical* if $2|a_{ij}$ for all $i\neq j$,
- *totally positive definite* if $Q(\gamma_1,\dots,\gamma_n)\in\mathcal{O}_K^+$ for all $\gamma_i\in\mathcal{O}_K$ not all zero,
- *universal* over $\mathcal{O}_K$ if it represents all elements in $\mathcal{O}_K^+$

## Theorem

*Let $K$ be a simplest cubic fields with basis $B_3(1,1)$.*

- *There exists a diagonal universal quadratic form over $\mathcal{O}_K$ with $\frac{a^2+3a}{3}+12a+12$ variables.*
- *Every classical universal quadratic form over $\mathcal{O}_K$ has at least $\frac{a^2+3a}{54}$ variables.*

# Pythagoras number

- let $\mathcal{O}$ be a commutative ring
- $\sum \mathcal{O}^2 = \left\{ \sum_{i=1}^{n} \alpha_i^2;\ \alpha_i \in \mathcal{O}, n \in \mathbb{N} \right\}$
- $\sum^m \mathcal{O}^2 = \left\{ \sum_{i=1}^{m} \alpha_i^2;\ \alpha_i \in \mathcal{O} \right\}$
- the Pythagoras number of the ring $\mathcal{O}$ is

$$\mathcal{P}(\mathcal{O}) = \inf \left\{ m \in \mathbb{N} \cup \{\infty\};\ \sum \mathcal{O}^2 = \sum^m \mathcal{O}^2 \right\}.$$

# Pythagoras number

- let $\mathcal{O}$ be a commutative ring
- $\sum \mathcal{O}^2 = \left\{ \sum_{i=1}^{n} \alpha_i^2;\ \alpha_i \in \mathcal{O}, n \in \mathbb{N} \right\}$
- $\sum^m \mathcal{O}^2 = \left\{ \sum_{i=1}^{m} \alpha_i^2;\ \alpha_i \in \mathcal{O} \right\}$
- the Pythagoras number of the ring $\mathcal{O}$ is

$$\mathcal{P}(\mathcal{O}) = \inf \left\{ m \in \mathbb{N} \cup \{\infty\};\ \sum \mathcal{O}^2 = \sum^m \mathcal{O}^2 \right\}.$$

**Theorem**

*Let $K$ be a simplest cubic fields with basis $B_3(1,1)$. Then the Pythagoras number of $\mathcal{O}_K$ is $6$.*

Note that the Pythagoras number of $\mathbb{Z}[\rho]$ is $6$ for $a \geq 3$ (T., 2023+).

Thank you for your attention.