Additiv tructur of non-monog nic impl t cubic fi ld

Magdaléna Tinková

Czech Technical University in Prague

Joint work with Daniel Gil-Muñoz.

pril 18, 2023

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

Definition

K is monogenic if $O_K = \mathbb{Z}[\ ]$ for some $\ 2\ K$, i.e., every algebraic integer $\ 2\ O_K$ can be expressed as

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

where $a_i\ 2\ \mathbb{Z}$ for all $0 \leq i \leq d-1$.

Exampl

Example

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

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

! They are always monogenic.

Example

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

Th impl t cubic fi ld

- introduced by Shanks (1974)
- $K = \mathbb{Q}(\ )$ where

Th impl t cubic fi ld

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

Example

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

Th impl t cubic fi ld

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

Example

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

Monogenic imprimitive cubic field

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

Theorem (Kashio, Sekigawa, 2021)

Let K

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

$B_p(k;l) = \quad 1; \quad ; \frac{k+l\rho+\rho^2}{p}$ 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.

$B_p(k;l) = \quad 1; \quad ; \frac{k+l\rho+\rho^2}{p}$ 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 $a^2 + 3a + 9 \equiv 0 \pmod{p^2}$
- 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
- O_K^+ set of totally positive elements $\quad 2\ O_K$, i.e., all conjugates of $\quad$ are positive

- K totally real number field
- O_K^+ set of totally positive elements $\quad 2\ O_K$, i.e., all conjugates of $\quad$ are positive

ult on ind compo abl int g r

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

ult on ind compo abl int g r

- 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; Krásensk , T., Zemková, 2020)

Theorem (Kala, T., 2022)

Let K be the im le t ubi field with $a \geq -1$ u h that $O_K = \mathbb{Z}[\ ]$. The element $1, 1 + \ + \ ^2$, and

$$(v; w) = -v - w \ + (v + 1)^{\ 2}$$

where $0 \leq v \leq a$ and $v(a + 2) + 1 \leq w \leq (v + 1)(a + 1)$ are, u to multi li ation by totally o itive unit , all the inde om o able integer in $\mathbb{Q}(\ )$.

Univ r al quadratic form

Quadratic form $Q($

Pythagora numb r

- let O be a commutative ring
- $\mathrm{P}\ O^2 = \left\{ \sum_{i=1}^{n} x_i^2;\ x_i \in O; n \in \mathbb{N} \right\}$
- $\mathrm{P}_m O^2 = \left\{ \sum_{i=1}^{m} x_i^2;\ x_i \in O \right\}$
- 0G40g0G0g0GT19701Tf2.8830Td-4310.9091Tf7.87912.10g0.240.0-l9

mm

Than you for your att ntion.