# Orders with few rational monogenizations

**Jan-Hendrik Evertse**
**Universiteit Leiden**

Analytic Number Theory Seminar

Utrecht, October 18, 2024

# Contents

We discuss part of

J.-H. Evertse, *Orders with few rational monogenizations,*
Acta Arithmetica 210 (2023), 307–335.

**Organization of the lecture:**

1. **Some results on monogenic orders**
2. **Introduction of rationally monogenic orders**
   (generalization of monogenic orders, special case of so-called invariant rings of polynomials, introduced and studied by Birch and Merriman (1972), Nakagawa (1989), Simon (2001), Del Corso, Dvornicich and Simon (2005), Wood (2011))
3. **Analogues of results in 1) for rationally monogenic orders**
4. **Brief outline of the proof of the main new result**

# Monogenic orders

Let $K$ be a number field of degree $n$, and denote by $O_K$ its ring of integers.
An *order* of $K$ is a subring of $O_K$ which has quotient field $K$.

An order $O$ of $K$ is called *monogenic* if there is $\alpha \in O_K$ such that

$$O = \mathbb{Z}[\alpha] = \{f(\alpha) : f \in \mathbb{Z}[X]\}.$$

Then $O$ has $\mathbb{Z}$-module basis $1, \alpha, \ldots, \alpha^{n-1}$.
Such an $\alpha$ is called a *monogenic generator* of $O$.

Given an order $O$, we are interested in the set of $\alpha$ such that $O = \mathbb{Z}[\alpha]$.

# Monogenic orders

Let $K$ be a number field of degree $n$, and denote by $O_K$ its ring of integers.
An *order* of $K$ is a subring of $O_K$ which has quotient field $K$.

An order $O$ of $K$ is called *monogenic* if there is $\alpha \in O_K$ such that

$$O = \mathbb{Z}[\alpha] = \{f(\alpha) : f \in \mathbb{Z}[X]\}.$$

Then $O$ has $\mathbb{Z}$-module basis $1, \alpha, \ldots, \alpha^{n-1}$.
Such an $\alpha$ is called a *monogenic generator* of $O$.

Given an order $O$, we are interested in the set of $\alpha$ such that $O = \mathbb{Z}[\alpha]$.

Two algebraic integers $\alpha, \beta$ are called *$\mathbb{Z}$-equivalent* if $\beta = \pm\alpha + a$ for some $a \in \mathbb{Z}$. For such $\alpha, \beta$ we have $\mathbb{Z}[\alpha] = \mathbb{Z}[\beta]$.

Thus, the set of $\alpha$ with $O = \mathbb{Z}[\alpha]$ can be partitioned into $\mathbb{Z}$-equivalence classes. Such a $\mathbb{Z}$-equivalence class is called a *monogenization* of $O$.

# A finiteness result

Every order of a quadratic number field $K$ has precisely one monogenization, i.e., for every order $O$ of $K$ there is $\alpha$ with $O = \mathbb{Z}[\alpha]$ and up to $\mathbb{Z}$-equivalence it is unique.

But orders of number fields of degree $\geq 3$ may have more than one monogenization, or no monogenization at all.

# A finiteness result

Every order of a quadratic number field $K$ has precisely one monogenization, i.e., for every order $O$ of $K$ there is $\alpha$ with $O = \mathbb{Z}[\alpha]$ and up to $\mathbb{Z}$-equivalence it is unique.

But orders of number fields of degree $\geq 3$ may have more than one monogenization, or no monogenization at all.

**Theorem (Győry, 1973)**

*Let $K$ be a number field of degree $\geq 3$. Then every order of $K$ has at most finitely many monogenizations, i.e., for every such order $O$ there are up to $\mathbb{Z}$-equivalence at most finitely many $\alpha$ with $O = \mathbb{Z}[\alpha]$.*

Győry gave in fact an *effective* proof, this means that his proof provides an algorithm that decides in principle whether $O$ is monogenic and if so, to find all monogenizations. In various situations, there are practical algorithms to find all monogenizations.

We go into another direction, and consider upper bounds for the *number* of monogenizations of an order.

# Number of monogenizations

**Theorem (Ev., Győry, 1985)**

*Let $K$ be a number field of degree $n \geq 3$. Then every order of $K$ has at most $C(n) = (4 \times 7^{3n \times n!})^{n-2}$ monogenizations.*

**Improvements:**

$C(3) = 10$ (Bennett, 2001)

$C(4) = 2760$ (Bhargava, Akhtari, 2021)

$C(n) = 2^{4(n+5)(n-2)}$ for $n \geq 5$ (Ev., 2011)

# Number of monogenizations

**Theorem (Ev., Győry, 1985)**

*Let $K$ be a number field of degree $n \geq 3$. Then every order of $K$ has at most $C(n) = (4 \times 7^{3n \times n!})^{n-2}$ monogenizations.*

**Improvements:**

$C(3) = 10$ (Bennett, 2001)

$C(4) = 2760$ (Bhargava, Akhtari, 2021)

$C(n) = 2^{4(n+5)(n-2)}$ for $n \geq 5$ (Ev., 2011)

For $n = 3$ there is an order with 9 monogenizations, namely the ring of integers of $\mathbb{Q}(\cos 2\pi/7)$.
For $n \geq 4$ the present bounds for $C(n)$ are probably far too large.

There are examples of orders of number fields of arbitrarily large degree $n$ with $\gg n$ monogenizations (e.g., rings of integers of cyclotomic or real cyclotomic fields).

But most orders have much fewer monogenizations.

# Almost all orders in a given number field have only few monogenizations

**Theorem (Bérczes, Ev., Győry, 2013)**

*Let $K$ be a number field of degree $\geq 3$.*
*Then $K$ has at most finitely many orders with more than two monogenizations.*

This is best possible.

# Almost all orders in a given number field have only few monogenizations

**Theorem (Bérczes, Ev., Győry, 2013)**

*Let $K$ be a number field of degree $\geq 3$.*
*Then $K$ has at most finitely many orders with more than two monogenizations.*

This is best possible.

**Example 1.** Suppose $O_K$ has infinitely many units $\varepsilon$ such that $\mathbb{Q}(\varepsilon) = K$. Then $\mathbb{Z}[\varepsilon] = \mathbb{Z}[\varepsilon^{-1}]$ give infinitely many orders of $K$ with two monogenizations (for there is no $a \in \mathbb{Z}$ with $\varepsilon^{-1} = \pm\varepsilon + a$).

# Almost all orders in a given number field have only few monogenizations

**Theorem (Bérczes, Ev., Győry, 2013)**

*Let $K$ be a number field of degree $\geq 3$.*
*Then $K$ has at most finitely many orders with more than two monogenizations.*

This is best possible.

**Example 1.** Suppose $O_K$ has infinitely many units $\varepsilon$ such that $\mathbb{Q}(\varepsilon) = K$. Then $\mathbb{Z}[\varepsilon] = \mathbb{Z}[\varepsilon^{-1}]$ give infinitely many orders of $K$ with two monogenizations (for there is no $a \in \mathbb{Z}$ with $\varepsilon^{-1} = \pm\varepsilon + a$).

**Example 2.** Let $\alpha, \beta \in O_K$ with $K = \mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$ be *$GL_2(\mathbb{Z})$-equivalent*, i.e., $\beta = \frac{a\alpha+b}{c\alpha+d}$ for some $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z})$ (i.e., $a, b, c, d \in \mathbb{Z}$ and $ad - bc = \pm 1$). Suppose $c \neq 0$.
Then $\mathbb{Z}[\alpha] = \mathbb{Z}[\beta]$ is an order of $K$ with two monogenizations.

# Almost all orders in a given number field have only few monogenizations

**Theorem (Bérczes, Ev., Győry, 2013)**

*Let $K$ be a number field of degree $\geq 3$.*
*Then $K$ has at most finitely many orders with more than two monogenizations.*

This is best possible.

**Example 1.** Suppose $O_K$ has infinitely many units $\varepsilon$ such that $\mathbb{Q}(\varepsilon) = K$. Then $\mathbb{Z}[\varepsilon] = \mathbb{Z}[\varepsilon^{-1}]$ give infinitely many orders of $K$ with two monogenizations (for there is no $a \in \mathbb{Z}$ with $\varepsilon^{-1} = \pm\varepsilon + a$).

**Example 2.** Let $\alpha, \beta \in O_K$ with $K = \mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$ be *$GL_2(\mathbb{Z})$-equivalent*, i.e., $\beta = \frac{a\alpha+b}{c\alpha+d}$ for some $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z})$ (i.e., $a, b, c, d \in \mathbb{Z}$ and $ad - bc = \pm 1$). Suppose $c \neq 0$.
Then $\mathbb{Z}[\alpha] = \mathbb{Z}[\beta]$ is an order of $K$ with two monogenizations.

The examples suggest, that for a given order $O$ one should consider the $GL_2(\mathbb{Z})$-equivalence classes of $\alpha$ with $O = \mathbb{Z}[\alpha]$.

# $GL_2(\mathbb{Z})$-equivalence classes

Recall that $\alpha, \beta$ are called $GL_2(\mathbb{Z})$-equivalent if $\beta = \frac{a\alpha+b}{c\alpha+d}$ for some $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z})$.

**Theorem (Bérczes, Ev., Győry, 2013)**

*Let $K$ be a number field of degree $n \geq 5$ whose Galois closure has Galois group $S_n$ (the permutation group on $n$ elements).*

*Then for all orders $O$ of $K$ with at most finitely many exceptions, the set of $\alpha$ with $O = \mathbb{Z}[\alpha]$ is contained in at most one $GL_2(\mathbb{Z})$-equivalence class.*

# $GL_2(\mathbb{Z})$-equivalence classes

Recall that $\alpha, \beta$ are called $GL_2(\mathbb{Z})$-equivalent if $\beta = \frac{a\alpha+b}{c\alpha+d}$ for some $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{Z})$.

**Theorem (Bérczes, Ev., Győry, 2013)**

*Let $K$ be a number field of degree $n \geq 5$ whose Galois closure has Galois group $S_n$ (the permutation group on $n$ elements).*

*Then for all orders $O$ of $K$ with at most finitely many exceptions, the set of $\alpha$ with $O = \mathbb{Z}[\alpha]$ is contained in at most one $GL_2(\mathbb{Z})$-equivalence class.*

The condition on the Galois group of the Galois closure of $K$ is technical; it can be weakened somewhat, but we do not know whether it can be removed completely.

If $K$ has degree 3 then the assertion of the theorem holds true for all orders of $K$, without exceptions (elementary fact).

For number fields of degree 4 the theorem is false.

# $GL_2(\mathbb{Z})$-equivalence classes, degree 4

**Theorem (Bérczes, Ev., Győry, 2013)**

*Let $r, s$ be integers such that $f(X) = (X^2 - r)^2 - X - s$ is irreducible, and let $K = \mathbb{Q}(\alpha)$, where $\alpha$ is a root of $f$.*

*Then $K$ has infinitely many orders $O_m$ $(m = 1, 2, \ldots)$ with the following property: $O_m = \mathbb{Z}[\alpha_m] = \mathbb{Z}[\beta_m]$, where $\beta_m = \alpha_m^2 - r_m$, $\alpha_m = \beta_m^2 - s_m$ for certain integers $r_m, s_m$.*

Clearly, $\alpha_m, \beta_m$ are not $GL_2(\mathbb{Z})$-equivalent. For otherwise, $\beta_m = \frac{a\alpha_m + b}{c\alpha_m + d}$ with $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z})$ and $\alpha_m$ would have degree 3.

Our aim is to generalize the previous results from monogenic orders $\mathbb{Z}[\alpha]$ to so-called rationally monogenic orders $\mathbb{Z}_\alpha$, attached to not necessarily integral algebraic numbers $\alpha$.

# Rationally monogenic orders

Let $\alpha$ be a not necessarily integral algebraic number of degree $n$. Let $f_\alpha(X) := a_0X^n + \cdots + a_n \in \mathbb{Z}[X]$ be its minimal polynomial, with $a_0 > 0$, $\gcd(a_0, \ldots, a_n) = 1$.

**Definition.** Write $f_\alpha(X) = (X - \alpha)(a_0X^{n-1} + \omega_1 X^{n-2} + \cdots + \omega_{n-1})$.
Then $\mathbb{Z}_\alpha$ is the $\mathbb{Z}$-module with basis $1, \omega_1, \ldots, \omega_{n-1}$.

This module was introduced by Birch and Merriman (1972).
Nakagawa (1989) showed that it is an order of $\mathbb{Q}(\alpha)$, i.e., contained in the ring of integers of $\mathbb{Q}(\alpha)$ and closed under multiplication.

# Rationally monogenic orders

Let $\alpha$ be a not necessarily integral algebraic number of degree $n$. Let $f_\alpha(X) := a_0X^n + \cdots + a_n \in \mathbb{Z}[X]$ be its minimal polynomial, with $a_0 > 0$, $\gcd(a_0, \ldots, a_n) = 1$.

**Definition.** Write $f_\alpha(X) = (X - \alpha)(a_0X^{n-1} + \omega_1X^{n-2} + \cdots + \omega_{n-1})$. Then $\mathbb{Z}_\alpha$ is the $\mathbb{Z}$-module with basis $1, \omega_1, \ldots, \omega_{n-1}$.

This module was introduced by Birch and Merriman (1972). Nakagawa (1989) showed that it is an order of $\mathbb{Q}(\alpha)$, i.e., contained in the ring of integers of $\mathbb{Q}(\alpha)$ and closed under multiplication.

**Equivalent definitions:**

**1.** $\mathbb{Z}_\alpha = \mathbb{Z}[\alpha] \cap \mathbb{Z}[\alpha^{-1}]$ (Del Corso, Dvornicich, Simon, 2005).

**2.** Let $\mathcal{M}_\alpha := \{x_0 + x_1\alpha + \cdots + x_{n-1}\alpha^{n-1} : x_0, \ldots, x_{n-1} \in \mathbb{Z}\}$. Then $\mathbb{Z}_\alpha = \{\xi \in \mathbb{Q}(\alpha) : \xi\mathcal{M}_\alpha \subseteq \mathcal{M}_\alpha\} = \{\xi \in \mathbb{Q}(\alpha) : \xi\mu \in \mathcal{M}_\alpha \ \forall \mu \in \mathcal{M}_\alpha\}$.

We call orders of the shape $\mathbb{Z}_\alpha$ *rationally monogenic orders*.

# $\{$Monogenic orders$\}$ $\subsetneq$ $\{$Rationally monogenic orders$\}$

For a non-zero algebraic number $\alpha$ of degree $n$ define

$$\begin{aligned} \mathcal{M}_\alpha &= \{x_0 + x_1\alpha + \cdots + x_{n-1}\alpha^{n-1} : x_0, \ldots, x_{n-1} \in \mathbb{Z}\}, \\ \mathbb{Z}_\alpha &= \{\xi \in \mathbb{Q}(\alpha) : \xi\mathcal{M}_\alpha \subseteq \mathcal{M}_\alpha\}. \end{aligned}$$

Orders of the shape $\mathbb{Z}_\alpha$ are called rationally monogenic orders.

If $\alpha$ is an algebraic integer, then $\mathbb{Z}_\alpha = \mathcal{M}_\alpha = \mathbb{Z}[\alpha]$.
So monogenic orders are rationally monogenic.

The following was probably known before:

**Theorem 1 (Ev., 2023)**

*Every number field of degree $\geq 3$ has infinitely many orders that are rationally monogenic but not monogenic.*

# Rational monogenizations

Let $\alpha$ be a non-zero algebraic number of degree $n$. Recall

$$\begin{aligned}\mathcal{M}_\alpha &= \{x_0 + x_1\alpha + \cdots + x_{n-1}\alpha^{n-1} : x_0, \ldots, x_{n-1} \in \mathbb{Z}\},\\ \mathbb{Z}_\alpha &= \{\xi \in \mathbb{Q}(\alpha) : \xi\mathcal{M}_\alpha \subseteq \mathcal{M}_\alpha\}.\end{aligned}$$

**Lemma**

*Let $\alpha, \beta$ be two $GL_2(\mathbb{Z})$-equivalent algebraic numbers, i.e., $\beta = \frac{a\alpha+b}{c\alpha+d}$ for some $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{Z})$. Then $\mathbb{Z}_\alpha = \mathbb{Z}_\beta$.*

**Proof.**

Suppose $\alpha, \beta$ have degree $n$. Then $\mathcal{M}_\beta = (c\alpha + d)^{1-n}\mathcal{M}_\alpha$. Hence $\mathbb{Z}_\beta = \mathbb{Z}_\alpha$. □

Given an order $O$ of a number field $K$, a *rational monogenization* of $O$ is a $GL_2(\mathbb{Z})$-equivalence class of $\alpha$ such that $\mathbb{Z}_\alpha = O$.

# Finiteness results

Every order of a cubic number field has at most one rational monogenization, that is, for every such order $O$ there is up to $GL_2(\mathbb{Z})$-equivalence at most one $\alpha$ with $O = \mathbb{Z}_\alpha$.

Orders of number fields of degree $\geq 4$ may not be rationally monogenic, or have more than one rational monogenization.

# Finiteness results

Every order of a cubic number field has at most one rational monogenization, that is, for every such order $O$ there is up to $GL_2(\mathbb{Z})$-equivalence at most one $\alpha$ with $O = \mathbb{Z}_\alpha$.

Orders of number fields of degree $\geq 4$ may not be rationally monogenic, or have more than one rational monogenization.

Work of Birch and Merriman (1972) implies the following:

**Theorem**

*Let $K$ be a number field of degree $\geq 4$. Then every order of $K$ has at most finitely many rational monogenizations, i.e., for every such order $O$ there are up to $GL_2(\mathbb{Z})$-equivalence at most finitely many $\alpha$ such that $\mathbb{Z}_\alpha = O$.*

The original proof of Birch and Merriman is ineffective. Ev. and Győry (1991) gave an effective proof, i.e., it allows to determine the rational monogenizations in principle.

# Number of rational monogenizations

**Theorem (Bérczes, Ev., Győry, 2004)**

*Let $K$ be a number field of degree $n \geq 4$. Then every order of $K$ has at most $C'(n) := n \times 2^{24n^3}$ rational monogenizations.*

**Improvements:**

$C'(4) = 40$ (Bhargava, 2021)

$C'(n) = 2^{5n^2}$ for $n \geq 5$ (Ev., Győry, 2017)

Similarly as in the monogenic case, for most orders the actual number of rational monogenizations is much smaller.

# Almost all orders in a given number field have only few rational monogenizations

**Theorem 2 (Ev., 2023)**

**(i)** *Let $K$ be a number field of degree $4$. Then $K$ has at most finitely many orders with more than two rational monogenizations.*

**(ii)** *Let $K$ be a number field of degree $n \geq 5$ whose Galois closure has Galois group $S_n$. Then $K$ has at most finitely many orders with more than one rational monogenization.*

# Almost all orders in a given number field have only few rational monogenizations

**Theorem 2 (Ev., 2023)**

**(i)** *Let $K$ be a number field of degree 4. Then $K$ has at most finitely many orders with more than two rational monogenizations.*

**(ii)** *Let $K$ be a number field of degree $n \geq 5$ whose Galois closure has Galois group $S_n$. Then $K$ has at most finitely many orders with more than one rational monogenization.*

We saw that there are quartic number fields with infinitely many orders $\mathbb{Z}[\alpha_m] = \mathbb{Z}[\beta_m]$ such that $\alpha_m$, $\beta_m$ are not $GL_2(\mathbb{Z})$-equivalent.
Hence (i) is best possible.

For number fields of degree $\geq 5$, the condition on the Galois group of the Galois closure of $K$ is technical; it can be weakened somewhat but we don't know whether it can be removed completely.

# Almost all orders in a given number field have only few rational monogenizations

**Theorem 2 (Ev., 2023)**

**(i)** *Let $K$ be a number field of degree 4. Then $K$ has at most finitely many orders with more than two rational monogenizations.*

**(ii)** *Let $K$ be a number field of degree $n \geq 5$ whose Galois closure has Galois group $S_n$. Then $K$ has at most finitely many orders with more than one rational monogenization.*

We saw that there are quartic number fields with infinitely many orders $\mathbb{Z}[\alpha_m] = \mathbb{Z}[\beta_m]$ such that $\alpha_m$, $\beta_m$ are not $GL_2(\mathbb{Z})$-equivalent.
Hence (i) is best possible.

For number fields of degree $\geq 5$, the condition on the Galois group of the Galois closure of $K$ is technical; it can be weakened somewhat but we don't know whether it can be removed completely.

The proofs of (i) and (ii) are different. We briefly outline the proof of (ii).

# Cross ratios and units

Let $K$ be a number field of degree $n \geq 5$.

We consider the orders $O = \mathbb{Z}_\alpha = \mathbb{Z}_\beta$ of $K$ with $\alpha$, $\beta$ not $GL_2(\mathbb{Z})$-equivalent and want to prove that there are only finitely many such orders.
The proof uses cross ratios.

Let $L$ be the Galois closure of $K$, and $x \mapsto x^{(i)}$ $(i = 1, \ldots, n)$ the embeddings $K \hookrightarrow L$.
Denote by $O_L$ the ring of integers of $L$, and by $O_L^*$ the unit group of $O_L$.

Define the *cross ratios* $\mathrm{cr}_{ijkl}(\alpha) := \dfrac{(\alpha^{(i)} - \alpha^{(j)})(\alpha^{(k)} - \alpha^{(l)})}{(\alpha^{(i)} - \alpha^{(k)})(\alpha^{(j)} - \alpha^{(l)})}$
for $\alpha \in K$ and distinct $i, j, k, l \in \{1, \ldots, n\}$.

# Cross ratios and units

Let $K$ be a number field of degree $n \geq 5$.

We consider the orders $O = \mathbb{Z}_\alpha = \mathbb{Z}_\beta$ of $K$ with $\alpha$, $\beta$ not $GL_2(\mathbb{Z})$-equivalent and want to prove that there are only finitely many such orders.
The proof uses cross ratios.

Let $L$ be the Galois closure of $K$, and $x \mapsto x^{(i)}$ ($i = 1, \ldots, n$) the embeddings $K \hookrightarrow L$.
Denote by $O_L$ the ring of integers of $L$, and by $O_L^*$ the unit group of $O_L$.

Define the *cross ratios* $\mathrm{cr}_{ijkl}(\alpha) := \dfrac{(\alpha^{(i)} - \alpha^{(j)})(\alpha^{(k)} - \alpha^{(l)})}{(\alpha^{(i)} - \alpha^{(k)})(\alpha^{(j)} - \alpha^{(l)})}$
for $\alpha \in K$ and distinct $i, j, k, l \in \{1, \ldots, n\}$.

**Proposition**

*Let $\alpha, \beta$ be such that $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta) = K$ and $\mathbb{Z}_\alpha = \mathbb{Z}_\beta$.*
*Then for all distinct $i, j, k, l$ we have $\mathrm{cr}_{ijkl}(\alpha)/\mathrm{cr}_{ijkl}(\beta) \in O_L^*$.*

# Outline of the proof of Theorem 2 (ii)

Let $K$ be a number field of degree $n \geq 5$ and $L$ its Galois closure. Assume that $L$ has Galois group $S_n$.

There are results from Diophantine geometry, giving precise information on the structure of the set of solutions of polynomial unit equations

$$f(x_1, \ldots, x_m) = 0 \text{ in } x_1, \ldots, x_m \in O_L^*, \text{ where } f \in L[X_1, \ldots, X_m]$$

(Ev., van der Poorten and Schlickewei, Laurent, 1980-s).

# Outline of the proof of Theorem 2 (ii)

Let $K$ be a number field of degree $n \geq 5$ and $L$ its Galois closure. Assume that $L$ has Galois group $S_n$.

There are results from Diophantine geometry, giving precise information on the structure of the set of solutions of polynomial unit equations

$$f(x_1, \ldots, x_m) = 0 \quad \text{in } x_1, \ldots, x_m \in O_L^*, \quad \text{where } f \in L[X_1, \ldots, X_m]$$

(Ev., van der Poorten and Schlickewei, Laurent, 1980-s).

The quantities $\varepsilon_{ijkl} := \mathrm{cr}_{ijkl}(\alpha)/\mathrm{cr}_{ijkl}(\beta)$ with $\mathbb{Z}_\alpha = \mathbb{Z}_\beta$ belong to $O_L^*$ and satisfy polynomial relations, e.g., for any five distinct $i, j, k, l, m$,

$$(\varepsilon_{jklm} - 1)(\varepsilon_{imkj} - 1)(\varepsilon_{iljk} - 1) = (\varepsilon_{jkml} - 1)(\varepsilon_{imjk} - 1)(\varepsilon_{ilkj} - 1).$$

An application of the general result on polynomial unit equations gives that the tuple $\varepsilon = (\varepsilon_{ijkl})_{i,j,k,l}$ belongs to a finite set depending only on $K$.

# Outline of the proof of Theorem 2 (ii)

Let $K$ be a number field of degree $n \geq 5$ and $L$ its Galois closure. Assume that $L$ has Galois group $S_n$.

There are results from Diophantine geometry, giving precise information on the structure of the set of solutions of polynomial unit equations

$$f(x_1, \ldots, x_m) = 0 \text{ in } x_1, \ldots, x_m \in O_L^*, \quad \text{where } f \in L[X_1, \ldots, X_m]$$

(Ev., van der Poorten and Schlickewei, Laurent, 1980-s).

The quantities $\varepsilon_{ijkl} := \mathrm{cr}_{ijkl}(\alpha)/\mathrm{cr}_{ijkl}(\beta)$ with $\mathbb{Z}_\alpha = \mathbb{Z}_\beta$ belong to $O_L^*$ and satisfy polynomial relations, e.g., for any five distinct $i, j, k, l, m$,

$$(\varepsilon_{jklm} - 1)(\varepsilon_{imkj} - 1)(\varepsilon_{iljk} - 1) = (\varepsilon_{jkml} - 1)(\varepsilon_{imjk} - 1)(\varepsilon_{ilkj} - 1).$$

An application of the general result on polynomial unit equations gives that the tuple $\varepsilon = (\varepsilon_{ijkl})_{i,j,k,l}$ belongs to a finite set depending only on $K$.

An elementary (but somewhat complicated) argument shows that each tuple $\varepsilon$ gives rise to at most finitely many orders of $K$. **QED**

# Thank you for your attention.