Orders with few rational monogenizations

Jan-Hendrik Evertse
Universiteit Leiden

Debrecen On-line Research Seminar "Number Theory"

December 8, 2023

Slides have been posted on
https://pub.math.leidenuniv.nl/∼evertsejh/lectures.shtml

Contents

We discuss part of

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

Organization of the lecture:

1. Overview of results on monogenic orders
2. Introduction of rationally monogenic orders
   (= invariant orders of primitive, irreducible polynomials, introduced by Birch and Merriman (1972), Nakagawa (1989), Simon (2001))
3. Generalizations of results on monogenic orders to rationally monogenic orders
4. Outline of the proof of the main result

Monogenic orders

Let K be a number field, with ring of integers O_K.
An order of K is a subring of O_K with quotient field K.

An order O of K is called *monogenic* if $O = \mathbb{Z}[\alpha]$ for some $\alpha \in O$.
We call such an α a *monogenic generator* of O.

If $O = \mathbb{Z}[\alpha]$ then also $O = \mathbb{Z}[\beta]$ if β is *$\mathbb{Z}$-equivalent* to α, i.e.,
$\beta = \pm\alpha + a$ for some $a \in \mathbb{Z}$.

A *monogenization* of O is a $\mathbb{Z}$-equivalence class of α with $O = \mathbb{Z}[\alpha]$.

Monogenic orders

Let K be a number field, with ring of integers O_K.
An order of K is a subring of O_K with quotient field K.

An order O of K is called *monogenic* if $O = \mathbb{Z}[\alpha]$ for some $\alpha \in O$.
We call such an α a *monogenic generator* of O.

If $O = \mathbb{Z}[\alpha]$ then also $O = \mathbb{Z}[\beta]$ if β is *$\mathbb{Z}$-equivalent* to α, i.e.,
$\beta = \pm\alpha + a$ for some $a \in \mathbb{Z}$.

A *monogenization* of O is a $\mathbb{Z}$-equivalence class of α with $O = \mathbb{Z}[\alpha]$.

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

Monogenic orders

Let K be a number field, with ring of integers O_K.
An order of K is a subring of O_K with quotient field K.

An order O of K is called *monogenic* if $O = \mathbb{Z}[\alpha]$ for some $\alpha \in O$.
We call such an α a *monogenic generator* of O.

If $O = \mathbb{Z}[\alpha]$ then also $O = \mathbb{Z}[\beta]$ if β is *$\mathbb{Z}$-equivalent* to α, i.e.,
$\beta = \pm\alpha + a$ for some $a \in \mathbb{Z}$.

A *monogenization* of O is a $\mathbb{Z}$-equivalence class of α with $O = \mathbb{Z}[\alpha]$.

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

Theorem (Győry, 1973)

Let K be a number field of degree ≥ 3. Then every order O of K has at most finitely many monogenizations, i.e., up to $\mathbb{Z}$-equivalence there are at most finitely many α with $O = \mathbb{Z}[\alpha]$, and these can be determined effectively in principle.

Number of monogenizations

Theorem (Ev., Győry, 1985)

Let K be a number field of degree $n \geq 3$ and $\mathcal{O}$ an order of K. Then $\mathcal{O}$ 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 most orders, these upper bounds are far too large.

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 ≥ 3.
Then K has only 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 ≥ 3.
Then K has only finitely many orders with more than two monogenizations.

This is best possible.

Example 1. Let ε be a unit of O_K with $\mathbb{Q}(\varepsilon) = K$.
Then $\mathbb{Z}[\varepsilon] = \mathbb{Z}[\varepsilon^{-1}]$ is an order of K with two monogenizations (for ε^{-1} cannot be of the shape $\pm\varepsilon + a$ with $a \in \mathbb{Z}$).

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 ≥ 3.
Then K has only finitely many orders with more than two monogenizations.

This is best possible.

Example 1. Let ε be a unit of O_K with $\mathbb{Q}(\varepsilon) = K$.
Then $\mathbb{Z}[\varepsilon] = \mathbb{Z}[\varepsilon^{-1}]$ is an order of K with two monogenizations
(for ε^{-1} cannot be of the shape $\pm\varepsilon + a$ with $a \in \mathbb{Z}$).

Example 2. Let $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{Z})$ (i.e., $a, b, c, d \in \mathbb{Z}$ and $ad - bc = \pm 1$),
let $\alpha \in O_K$ with $\mathbb{Q}(\alpha) = K$ such that $c\alpha + d$ is a unit, and $\beta = \frac{a\alpha+b}{c\alpha+d}$.
Then $\mathbb{Z}[\beta] = \mathbb{Z}[\alpha]$ 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 ≥ 3.
Then K has only finitely many orders with more than two monogenizations.

This is best possible.

Example 1. Let ε be a unit of O_K with $\mathbb{Q}(\varepsilon) = K$.
Then $\mathbb{Z}[\varepsilon] = \mathbb{Z}[\varepsilon^{-1}]$ is an order of K with two monogenizations (for ε^{-1} cannot be of the shape $\pm\varepsilon + a$ with $a \in \mathbb{Z}$).

Example 2. Let $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{Z})$ (i.e., $a, b, c, d \in \mathbb{Z}$ and $ad - bc = \pm 1$), let $\alpha \in O_K$ with $\mathbb{Q}(\alpha) = K$ such that $c\alpha + d$ is a unit, and $\beta = \frac{a\alpha+b}{c\alpha+d}$.
Then $\mathbb{Z}[\beta] = \mathbb{Z}[\alpha]$ is an order of K with two monogenizations.

This suggests that for a given order O it is reasonable to consider $GL_2(\mathbb{Z})$-equivalence classes of α with $O = \mathbb{Z}[\alpha]$, where α, β are called *$GL_2(\mathbb{Z})$-equivalent* if $\beta = \frac{a\alpha+b}{c\alpha+d}$ for some $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{Z})$.

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

Recall that α, β 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 ≥ 5 whose normal closure has 4-transitive Galois group.

Then for all orders O of K with at most finitely many exceptions, the set of α 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 α, β 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 ≥ 5 whose normal closure has 4-transitive Galois group.

Then for all orders O of K with at most finitely many exceptions, the set of α 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 normal closure of K is technical; we do not know whether it can be weakened or removed.

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 α 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, α_m, β_m are not $GL_2(\mathbb{Z})$-equivalent. For otherwise, $\beta_m = \frac{a\alpha_m + b}{c\alpha_m + d}$ with $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{Z})$ and α_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 α.

Rationally monogenic orders

Let α 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 $a_0 > 0$, $\gcd(a_0, \ldots, a_n) = 1$.

Define $\mathbb{Z}_\alpha$ to be the *invariant order* of f_α, introduced by Birch and Merriman (1972), Nakagawa (1989), Simon (2001).

More explicitly, define the $\mathbb{Z}$-module

$$\mathcal{M}_\alpha := \{x_0 + x_1\alpha + \cdots + x_{n-1}\alpha^{n-1} : x_0, \ldots, x_{n-1} \in \mathbb{Z}\}.$$

Then $\mathbb{Z}_\alpha$ is its ring of scalars, i.e.,

$$\mathbb{Z}_\alpha = \{\xi \in \mathbb{Q}(\alpha) : \xi\mathcal{M}_\alpha \subseteq \mathcal{M}_\alpha\} = \{\xi \in \mathbb{Q}(\alpha) : \xi\mu \in \mathcal{M}_\alpha \ \forall \mu \in \mathcal{M}_\alpha\}.$$

This is an order of $\mathbb{Q}(\alpha)$.

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

$\{$Monogenic orders$\}$ $\underset{\neq}{\subset}$ $\{$Rationally monogenic orders$\}$

For a non-zero algebraic number α 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.

If α 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 ≥ 3 has infinitely many orders that are rationally monogenic but not monogenic.

Properties of rationally monogenic orders

Let α be a non-zero algebraic number of degree n. Let $f_\alpha(X) := a_0X^n + a_1X^{n-1} + \cdots + a_n \in \mathbb{Z}[X]$ be its minimal polynomial, with $a_0 > 0$, $\gcd(a_0, \ldots, a_n) = 1$.

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

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

(ii) $\mathbb{Z}_\alpha$ *has* $\mathbb{Z}$*-module basis* $\{1, \omega_1, \ldots, \omega_{n-1}\}$*, where* $f_\alpha(X) = (X - \alpha)(a_0X^{n-1} + \omega_1X^{n-2} + \cdots + \omega_{n-1})$.

(iii) *There is an equality of discriminants* $\mathrm{discr}(\mathbb{Z}_\alpha) = \mathrm{discr}(f_\alpha) = a_0^{2n-2}\prod_{1\le i<j\le n}(\alpha^{(i)} - \alpha^{(j)})^2$.

Rational monogenizations

Let α 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 α, β 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 α, β 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 α such that $\mathbb{Z}_\alpha = O$.

Finiteness results

An order O of a number field K is called *primitive* if there are no order O' and integer $a > 1$ such that $O = \mathbb{Z} + aO'$.

Every rationally monogenic order is primitive.

Theorem (Delone and Faddeev, 1940)

Let O be a primitive order of a cubic number field. Then O has precisely one rational monogenization, i.e., up to $GL_2(\mathbb{Z})$-equivalence there is precisely one α with $\mathbb{Z}_\alpha = O$.

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

Finiteness results

An order O of a number field K is called *primitive* if there are no order O' and integer $a > 1$ such that $O = \mathbb{Z} + aO'$.

Every rationally monogenic order is primitive.

Theorem (Delone and Faddeev, 1940)

Let O be a primitive order of a cubic number field. Then O has precisely one rational monogenization, i.e., up to $GL_2(\mathbb{Z})$-equivalence there is precisely one α with $\mathbb{Z}_\alpha = O$.

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

Theorem (Birch and Merriman, 1972)

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

The original proof of Birch and Merriman is ineffective. Ev. and Győry (1991) gave an effective proof.

Number of rational monogenizations

Theorem (Bérczes, Ev., Győry, 2004)

Let K be a number field of degree $n \geq 4$ and $\mathcal{O}$ an order of K. Then $\mathcal{O}$ 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 only finitely many orders with more than two rational monogenizations.*

(ii) *Let K be a number field of degree ≥ 5 whose normal closure has 5-transitive Galois group. Then K has only 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 only finitely many orders with more than two rational monogenizations.*

(ii) *Let K be a number field of degree ≥ 5 whose normal closure has 5-transitive Galois group. Then K has only 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 α_m, β_m are not $GL_2(\mathbb{Z})$-equivalent.
Hence (i) is best possible.

For number fields of degree ≥ 5, the condition on the Galois group of the normal closure of K is technical; we do not know whether it can be weakened or removed.

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 only finitely many orders with more than two rational monogenizations.*

(ii) *Let K be a number field of degree ≥ 5 whose normal closure has 5-transitive Galois group. Then K has only 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 α_m, β_m are not $GL_2(\mathbb{Z})$-equivalent.
Hence (i) is best possible.

For number fields of degree ≥ 5, the condition on the Galois group of the normal closure of K is technical; we do not know whether it can be weakened or removed.

The proof of Theorem 2 uses ineffective finiteness results for polynomial unit equations, so it does not enable to determine the exceptional orders.

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

Connection with Hermite equivalence

Reference:
M. Bhargava, J.-H. Evertse, K. Győry, L. Remete, A. Swaminathan, *Hermite equivalence of polynomials*, Acta Arithmetica 209 (2023), 17–58.

Let $\mathcal{PI}(n)$ denote the set of primitive, irreducible polynomials in $\mathbb{Z}[X]$ of degree n.
For a number field K, let $\mathcal{PI}(K)$ denote the set of primitive, irreducible polynomials in $\mathbb{Z}[X]$ having a root generating K. So
$\mathcal{PI}(n) = \bigcup_{[K:\mathbb{Q}]=n} \mathcal{PI}(K)$.

Call $f, g \in \mathcal{PI}(n)$ *Hermite equivalent* if f has a root α and g a root β such that $\mathcal{M}_\beta = \lambda \mathcal{M}_\alpha$ for some $\lambda \in \mathbb{Q}(\alpha)$.

This implies $\mathbb{Z}_\alpha = \mathbb{Z}_\beta$ but in general not conversely.

Call $f, g \in \mathcal{PI}(n)$ *$GL_2(\mathbb{Z})$-equivalent* if $g(X) = \pm(cX+d)^n f\left(\frac{aX+b}{cX+d}\right)$ for some $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{Z})$.

$GL_2(\mathbb{Z})$-equivalent polynomials are Hermite equivalent.

Connection with Hermite equivalence (cont'd)

Let $\mathcal{PI}(n)$ denote the set of primitive, irreducible polynomials in $\mathbb{Z}[X]$ of degree n.
For a number field K, let $\mathcal{PI}(K)$ denote the set of primitive, irreducible polynomials in $\mathbb{Z}[X]$ having a root that generates K.

Theorem (Bhargava, Ev., Győry, Remete, Swaminathan, 2023)

For every $n \geq 4$ there are infinitely many Hermite equivalence classes in $\mathcal{PI}(n)$ that fall apart into at least two $GL_2(\mathbb{Z})$-equivalence classes.

Connection with Hermite equivalence (cont'd)

Let $\mathcal{PI}(n)$ denote the set of primitive, irreducible polynomials in $\mathbb{Z}[X]$ of degree n.
For a number field K, let $\mathcal{PI}(K)$ denote the set of primitive, irreducible polynomials in $\mathbb{Z}[X]$ having a root that generates K.

Theorem (Bhargava, Ev., Győry, Remete, Swaminathan, 2023)

For every $n \geq 4$ there are infinitely many Hermite equivalence classes in $\mathcal{PI}(n)$ that fall apart into at least two $GL_2(\mathbb{Z})$-equivalence classes.

Theorem 3 (Ev., 2023)

(i) *Let K be a number field of degree 4. Then $\mathcal{PI}(K)$ has only finitely many Hermite equivalence classes that fall apart into more than two $GL_2(\mathbb{Z})$-equivalence classes.*

(ii) *Let K be a number field of degree ≥ 5 whose normal closure has 5-transitive Galois group. Then $\mathcal{PI}(K)$ has only finitely many Hermite equivalence classes that fall apart into more than one $GL_2(\mathbb{Z})$-equivalence class.*

Special numbers

Let K be a number field of degree ≥ 5 whose normal closure has 5-transitive Galois group.

Aim: Prove that K has only finitely many orders with more than one rational monogenization.

We translate this into a problem on special numbers:
$\alpha \in K$ is called *special* if $\mathbb{Q}(\alpha) = K$ and there is β such that $\mathbb{Z}_\alpha = \mathbb{Z}_\beta$ and β is not $GL_2(\mathbb{Z})$-equivalent to α.

It suffices to prove the following:

The special numbers in K lie in at most finitely many $GL_2(\mathbb{Z})$-equivalence classes.

Special numbers

Let K be a number field of degree ≥ 5 whose normal closure has 5-transitive Galois group.

Aim: Prove that K has only finitely many orders with more than one rational monogenization.

We translate this into a problem on special numbers:
$\alpha \in K$ is called *special* if $\mathbb{Q}(\alpha) = K$ and there is β such that $\mathbb{Z}_\alpha = \mathbb{Z}_\beta$ and β is not $GL_2(\mathbb{Z})$-equivalent to α.

It suffices to prove the following:

The special numbers in K lie in at most finitely many $GL_2(\mathbb{Z})$-equivalence classes.

Indeed, the orders of K with more than one rational monogenization are precisely those of the shape $\mathbb{Z}_\alpha$ with α special.

Once we have shown that the special numbers lie in finitely many $GL_2(\mathbb{Z})$-equivalence classes, it follows that there are only finitely many orders $\mathbb{Z}_\alpha$ with α special.

Reduction to $GL_2(\mathbb{Q})$-equivalence

Let K be a number field of degree ≥ 5 whose normal closure has 5-transitive Galois group.

$\alpha \in K$ is called *special* if $\mathbb{Q}(\alpha) = K$ and there is β such that $\mathbb{Z}_\alpha = \mathbb{Z}_\beta$ and β is not $GL_2(\mathbb{Z})$-equivalent to α.

We say that $\alpha, \beta \in K$ are *$GL_2(\mathbb{Q})$-equivalent* if $\beta = \frac{a\alpha+b}{c\alpha+d}$ for some $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{Q})$ (i.e., $a, b, c, d \in \mathbb{Q}$, $ad - bc \neq 0$).

Proposition 1

Every $GL_2(\mathbb{Q})$-equivalence class of special numbers in K is the union of finitely many $GL_2(\mathbb{Z})$-equivalence classes.

The proof of this proposition uses a finiteness result for unit equations, and a rather complicated elementary argument.

So in order to prove that K has only finitely many orders with more than one rational monogenization, it suffices to prove that the special numbers in K lie in only finitely many $GL_2(\mathbb{Q})$-equivalence classes.

We give the main ideas of the proof of the latter.

Cross ratios

Let K be a number field of degree $n \geq 5$, L the normal closure of K, and $x \mapsto x^{(i)}$ $(i = 1, \ldots, n)$ the embeddings $K \hookrightarrow L$.

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 $i, j, k, l \in \{1, \ldots, n\}$.

Lemma

Let α, β with $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta) = K$.
Then α, β are $GL_2(\mathbb{Q})$-equivalent, i.e., $\beta = \frac{a\alpha+b}{c\alpha+d}$ for some $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{Q})$, if and only if

$$\mathrm{cr}_{ijkl}(\alpha) = \mathrm{cr}_{ijkl}(\beta) \quad \text{for all distinct } i, j, k, l \in \{1, \ldots, n\}.$$

Cross ratios

Let K be a number field of degree $n \geq 5$, L the normal closure of K, and $x \mapsto x^{(i)}$ $(i = 1, \ldots, n)$ the embeddings $K \hookrightarrow L$.

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 $i, j, k, l \in \{1, \ldots, n\}$.

Lemma

Let α, β with $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta) = K$.
Then α, β are $GL_2(\mathbb{Q})$-equivalent, i.e., $\beta = \frac{a\alpha+b}{c\alpha+d}$ for some $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{Q})$, if and only if

$$\mathrm{cr}_{ijkl}(\alpha) = \mathrm{cr}_{ijkl}(\beta) \quad \text{for all distinct } i, j, k, l \in \{1, \ldots, n\}.$$

Proof.

By elementary projective geometry, $\mathrm{cr}_{ijkl}(\alpha) = \mathrm{cr}_{ijkl}(\beta)$ for all i, j, k, l if and only if there is a projective transformation P of $\mathbb{P}^1(L)$ such that $\beta^{(i)} = P\alpha^{(i)}$ for $i = 1, \ldots, n$.
By Galois theory, we can take $P : x \mapsto \frac{ax+b}{cx+d}$ with $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{Q})$. □

Cross ratios

Let K be a number field of degree $n \geq 5$, L the normal closure of K, and $x \mapsto x^{(i)}$ $(i = 1, \ldots, n)$ the embeddings $K \hookrightarrow L$.

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 $i, j, k, l \in \{1, \ldots, n\}$.

Lemma

Let α, β with $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta) = K$.
Then α, β are $GL_2(\mathbb{Q})$-equivalent, i.e., $\beta = \frac{a\alpha+b}{c\alpha+d}$ for some $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{Q})$, if and only if

$$\mathrm{cr}_{ijkl}(\alpha) = \mathrm{cr}_{ijkl}(\beta) \quad \text{for all distinct } i, j, k, l \in \{1, \ldots, n\}.$$

Thus, in order to prove that the special $\alpha \in K$ lie in finitely many $GL_2(\mathbb{Q})$-equivalence classes, it suffices to show that the set of cross ratios

$$\{\mathrm{cr}_{ijkl}(\alpha) : \ \alpha \in K \text{ special}, \ i, j, k, l \in \{1, \ldots, n\} \text{ distinct}\}$$

is finite.

Connection with units

Let K be a number field of degree $n \geq 5$, L the normal closure of K, and $x \mapsto x^{(i)}$ $(i = 1, \ldots, n)$ the embeddings $K \hookrightarrow L$.

Proposition 2

Let α, β with $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta) = K$ and $\mathbb{Z}_\alpha = \mathbb{Z}_\beta$. Then

$$\frac{\mathrm{cr}_{ijkl}(\alpha)}{\mathrm{cr}_{ijkl}(\beta)} \in O_L^* \quad \text{for all distinct } i, j, k, l \in \{1, \ldots, n\}.$$

Combining this with algebraic relations between the cross ratios, this enables us to apply finiteness results for unit equations.

Proof of Proposition 2: Notation

Let K be a number field of degree $n \geq 5$, L the normal closure of K, and $x \mapsto x^{(i)}$ $(i = 1, \ldots, n)$ the embeddings $K \hookrightarrow L$.

For $\gamma_1, \ldots, \gamma_t \in L$, denote by $[\gamma_1, \ldots, \gamma_t]$ the fractional ideal of O_L, i.e., O_L-module, generated by $\gamma_1, \ldots, \gamma_t$.

For $f \in L[X]$, let its *content* $[f]$ be the fractional ideal of O_L generated by the coefficients of f. By Gauss' Lemma, $[fg] = [f] \cdot [g]$ for $f, g \in L[X]$.

Proof of Proposition 2: Notation

Let K be a number field of degree $n \geq 5$, L the normal closure of K, and $x \mapsto x^{(i)}$ $(i = 1, \ldots, n)$ the embeddings $K \hookrightarrow L$.

For $\gamma_1, \ldots, \gamma_t \in L$, denote by $[\gamma_1, \ldots, \gamma_t]$ the fractional ideal of O_L, i.e., O_L-module, generated by $\gamma_1, \ldots, \gamma_t$.

For $f \in L[X]$, let its *content* $[f]$ be the fractional ideal of O_L generated by the coefficients of f. By Gauss' Lemma, $[fg] = [f] \cdot [g]$ for $f, g \in L[X]$.

For a finitely generated $\mathbb{Z}$-submodule $\mathcal{M}$ of K with basis $\{\alpha_1, \ldots, \alpha_m\}$ and indices $i \neq j \in \{1, \ldots, n\}$ define the fractional ideal
$\mathfrak{d}_{ij}(\mathcal{M}) := [\alpha_1^{(i)} - \alpha_1^{(j)}, \ldots, \alpha_m^{(i)} - \alpha_m^{(j)}]$.
This is independent of the choice of a basis of $\mathcal{M}$.

Proof of Proposition 2: Notation

Let K be a number field of degree $n \geq 5$, L the normal closure of K, and $x \mapsto x^{(i)}$ $(i = 1, \ldots, n)$ the embeddings $K \hookrightarrow L$.

For $\gamma_1, \ldots, \gamma_t \in L$, denote by $[\gamma_1, \ldots, \gamma_t]$ the fractional ideal of O_L, i.e., O_L-module, generated by $\gamma_1, \ldots, \gamma_t$.

For $f \in L[X]$, let its *content* $[f]$ be the fractional ideal of O_L generated by the coefficients of f. By Gauss' Lemma, $[fg] = [f] \cdot [g]$ for $f, g \in L[X]$.

For a finitely generated $\mathbb{Z}$-submodule $\mathcal{M}$ of K with basis $\{\alpha_1, \ldots, \alpha_m\}$ and indices $i \neq j \in \{1, \ldots, n\}$ define the fractional ideal
$\mathfrak{d}_{ij}(\mathcal{M}) := [\alpha_1^{(i)} - \alpha_1^{(j)}, \ldots, \alpha_m^{(i)} - \alpha_m^{(j)}]$.
This is independent of the choice of a basis of $\mathcal{M}$.

To prove Proposition 2, it suffices to show that for any $\alpha \in K$ with $\mathbb{Q}(\alpha) = K$, $[\mathrm{cr}_{ijkl}(\alpha)]$ depends only on $\mathbb{Z}_\alpha$.

Indeed then
$\mathbb{Z}_\alpha = \mathbb{Z}_\beta \Rightarrow [\mathrm{cr}_{ijkl}(\alpha)] = [\mathrm{cr}_{ijkl}(\beta)] \Rightarrow \mathrm{cr}_{ijkl}(\alpha)/\mathrm{cr}_{ijkl}(\beta) \in O_L^*$.

Finishing the proof of Proposition 2

Let $\alpha \in K$ with $\mathbb{Q}(\alpha) = K$ and $f_\alpha(X) = a_0X^n + \cdots + a_n \in \mathbb{Z}[X]$ its minimal polynomial with $\gcd(a_0, \ldots, a_n) = 1$.

Recall that $\mathbb{Z}_\alpha$ has basis $\{1, \omega_1, \ldots, \omega_{n-1}\}$ with $f_\alpha(X) = (X - \alpha)(a_0X^{n-1} + \omega_1X^{n-2} + \cdots + \omega_{n-1})$.

Then for all i, j,

$$\begin{aligned}&(\alpha^{(i)} - \alpha^{(j)})f_\alpha(X)\\ &= (X - \alpha^{(i)})(X - \alpha^{(j)})\Big((\omega_1^{(i)} - \omega_1^{(j)})X^{n-2} + \cdots + (\omega_{n-1}^{(i)} - \omega_{n-1}^{(j)})\Big),\end{aligned}$$

Finishing the proof of Proposition 2

Let $\alpha \in K$ with $\mathbb{Q}(\alpha) = K$ and $f_\alpha(X) = a_0X^n + \cdots + a_n \in \mathbb{Z}[X]$ its minimal polynomial with $\gcd(a_0, \ldots, a_n) = 1$.

Recall that $\mathbb{Z}_\alpha$ has basis $\{1, \omega_1, \ldots, \omega_{n-1}\}$ with $f_\alpha(X) = (X - \alpha)(a_0X^{n-1} + \omega_1X^{n-2} + \cdots + \omega_{n-1})$.

Then for all i, j,

$$\begin{aligned}&(\alpha^{(i)} - \alpha^{(j)})f_\alpha(X)\\ &= (X - \alpha^{(i)})(X - \alpha^{(j)})\Big((\omega_1^{(i)} - \omega_1^{(j)})X^{n-2} + \cdots + (\omega_{n-1}^{(i)} - \omega_{n-1}^{(j)})\Big),\end{aligned}$$

and thus, taking contents on the left and right and applying Gauss' Lemma,

$$\begin{aligned}[\alpha^{(i)} - \alpha^{(j)}] &= [1, \alpha^{(i)}] \cdot [1, \alpha^{(j)}] \cdot [\omega_1^{(i)} - \omega_1^{(j)}, \ldots, \omega_{n-1}^{(i)} - \omega_{n-1}^{(j)}]\\ &= [1, \alpha^{(i)}] \cdot [1, \alpha^{(j)}] \cdot \mathfrak{d}_{ij}(\mathbb{Z}_\alpha).\end{aligned}$$

Finishing the proof of Proposition 2

Let $\alpha \in K$ with $\mathbb{Q}(\alpha) = K$ and $f_\alpha(X) = a_0X^n + \cdots + a_n \in \mathbb{Z}[X]$ its minimal polynomial with $\gcd(a_0, \ldots, a_n) = 1$.

Recall that $\mathbb{Z}_\alpha$ has basis $\{1, \omega_1, \ldots, \omega_{n-1}\}$ with $f_\alpha(X) = (X - \alpha)(a_0X^{n-1} + \omega_1X^{n-2} + \cdots + \omega_{n-1})$.

Then for all i, j,

$$\begin{aligned}&(\alpha^{(i)} - \alpha^{(j)})f_\alpha(X)\\ &= (X - \alpha^{(i)})(X - \alpha^{(j)})\Big((\omega_1^{(i)} - \omega_1^{(j)})X^{n-2} + \cdots + (\omega_{n-1}^{(i)} - \omega_{n-1}^{(j)})\Big),\end{aligned}$$

and thus, taking contents on the left and right and applying Gauss' Lemma,

$$\begin{aligned}[\alpha^{(i)} - \alpha^{(j)}] &= [1, \alpha^{(i)}] \cdot [1, \alpha^{(j)}] \cdot [\omega_1^{(i)} - \omega_1^{(j)}, \ldots, \omega_{n-1}^{(i)} - \omega_{n-1}^{(j)}]\\ &= [1, \alpha^{(i)}] \cdot [1, \alpha^{(j)}] \cdot \mathfrak{d}_{ij}(\mathbb{Z}_\alpha).\end{aligned}$$

Hence

$$[\mathrm{cr}_{ijkl}(\alpha)] = \left[\frac{(\alpha^{(i)} - \alpha^{(j)})(\alpha^{(k)} - \alpha^{(l)})}{(\alpha^{(i)} - \alpha^{(k)})(\alpha^{(j)} - \alpha^{(l)})}\right] = \mathfrak{d}_{ij}(\mathbb{Z}_\alpha)\mathfrak{d}_{kl}(\mathbb{Z}_\alpha)\mathfrak{d}_{ik}(\mathbb{Z}_\alpha)^{-1}\mathfrak{d}_{jl}(\mathbb{Z}_\alpha)^{-1}$$

depends indeed only on $\mathbb{Z}_\alpha$. □

Algebraic relations

Let K be a number field of degree $n \geq 5$ whose normal closure L has 5-transitive Galois group.
Let $\alpha \in K$ be special, and choose β such that $\mathbb{Z}_\alpha = \mathbb{Z}_\beta$ and α, β are not $GL_2(\mathbb{Z})$-equivalent. Recall that by Proposition 2,

$$\varepsilon_{ijkl} := \frac{\mathrm{cr}_{ijkl}(\beta)}{\mathrm{cr}_{ijkl}(\alpha)} \in O_L^* \quad \text{for any distinct } i,j,k,l \in \{1,\dots,n\}.$$

We have the relations

$$\mathrm{cr}_{ijkl}(\alpha) + \mathrm{cr}_{ilkj}(\alpha) = 1, \quad \mathrm{cr}_{ijkl}(\alpha)\varepsilon_{ijkl} + \mathrm{cr}_{ilkj}(\alpha)\varepsilon_{ilkj} = 1,$$

which imply

$$\mathrm{cr}_{ijkl}(\alpha) = \frac{\varepsilon_{ilkj} - 1}{\varepsilon_{ilkj} - \varepsilon_{ijkl}}, \quad \mathrm{cr}_{ijkl}(\beta) = \frac{\varepsilon_{ilkj} - 1}{\varepsilon_{iljk} - 1}.$$

Algebraic relations

Let K be a number field of degree $n \geq 5$ whose normal closure L has 5-transitive Galois group.
Let $\alpha \in K$ be special, and choose β such that $\mathbb{Z}_\alpha = \mathbb{Z}_\beta$ and α, β are not $GL_2(\mathbb{Z})$-equivalent. Recall that by Proposition 2,

$$\varepsilon_{ijkl} := \frac{\mathrm{cr}_{ijkl}(\beta)}{\mathrm{cr}_{ijkl}(\alpha)} \in O_L^* \quad \text{for any distinct } i,j,k,l \in \{1,\dots,n\}.$$

We have the relations

$$\mathrm{cr}_{ijkl}(\alpha) + \mathrm{cr}_{ilkj}(\alpha) = 1, \quad \mathrm{cr}_{ijkl}(\alpha)\varepsilon_{ijkl} + \mathrm{cr}_{ilkj}(\alpha)\varepsilon_{ilkj} = 1,$$

which imply

$$\mathrm{cr}_{ijkl}(\alpha) = \frac{\varepsilon_{ilkj} - 1}{\varepsilon_{ilkj} - \varepsilon_{ijkl}}, \quad \mathrm{cr}_{ijkl}(\beta) = \frac{\varepsilon_{ilkj} - 1}{\varepsilon_{iljk} - 1}.$$

Lastly, for any five distinct i,j,k,l,m,

$$1 = \frac{\mathrm{cr}_{jmlk}(\beta)\mathrm{cr}_{ijkm}(\beta)}{\mathrm{cr}_{ijkl}(\beta)} = \frac{\varepsilon_{jklm} - 1}{\varepsilon_{jkml} - 1} \cdot \frac{\varepsilon_{imkj} - 1}{\varepsilon_{imjk} - 1} \cdot \frac{\varepsilon_{iljk} - 1}{\varepsilon_{ilkj} - 1}.$$

Finishing the proof

Recall (*) $\dfrac{\varepsilon_{jklm}-1}{\varepsilon_{jkml}-1}\cdot\dfrac{\varepsilon_{imkj}-1}{\varepsilon_{imjk}-1}\cdot\dfrac{\varepsilon_{iljk}-1}{\varepsilon_{ilkj}-1}=1\ \forall i,j,k,l,m$, all ε-s in O_L^*.

Bérczes, Ev. and Győry (2013) studied the unit equation

$$\frac{x_1-1}{y_1-1}\cdot\frac{x_2-1}{y_2-1}\cdot\frac{x_3-1}{y_3-1}=1 \text{ in } x_1,x_2,x_3,y_1,y_2,y_3\in O_L^*\setminus\{1\}$$

and proved a rather complicated result for the structure of its set of solutions, involving certain infinite families.

This follows from a finiteness result on equations $x_1+\cdots+x_r=1$ in $x_1,\ldots,x_r\in O_L^*$, and so ultimately from Schmidt's Subspace Theorem.

Finishing the proof

Recall (*) $\dfrac{\varepsilon_{jklm}-1}{\varepsilon_{jkml}-1}\cdot\dfrac{\varepsilon_{imkj}-1}{\varepsilon_{imjk}-1}\cdot\dfrac{\varepsilon_{iljk}-1}{\varepsilon_{ilkj}-1}=1\ \forall i,j,k,l,m$, all ε-s in O_L^*.

Bérczes, Ev. and Győry (2013) studied the unit equation

$$\frac{x_1-1}{y_1-1}\cdot\frac{x_2-1}{y_2-1}\cdot\frac{x_3-1}{y_3-1}=1 \text{ in } x_1,x_2,x_3,y_1,y_2,y_3\in O_L^*\setminus\{1\}$$

and proved a rather complicated result for the structure of its set of solutions, involving certain infinite families.

This follows from a finiteness result on equations $x_1+\cdots+x_r=1$ in $x_1,\ldots,x_r\in O_L^*$, and so ultimately from Schmidt's Subspace Theorem.

We apply the result of BEG to (*) for all i,j,k,l,m.

Our assumption that the normal closure L of K has 5-transitive Galois group yields several other relations between the ε-s, which eliminate the infinite families from the BEG-result.

Thus, it follows that the number of possible values for the ε-s is finite.

Finishing the proof (cont'd)

Recall that K is a number field of degree ≥ 5 whose normal closure has 5-transitive Galois group.
We showed that the set

$$\left\{ \varepsilon_{ijkl} = \frac{\mathrm{cr}_{ijkl}(\beta)}{\mathrm{cr}_{ijkl}(\alpha)} : \alpha \in K \text{ special}, \ \mathbb{Z}_\beta = \mathbb{Z}_\alpha, \ i,j,k,l \in \{1,\ldots,n\} \text{ distinct} \right\}$$

is finite.

Using $\mathrm{cr}_{ijkl}(\alpha) = \frac{\varepsilon_{ilkj}-1}{\varepsilon_{ilkj}-\varepsilon_{ijkl}}$, it follows that

$$\{\mathrm{cr}_{ijkl}(\alpha) : \alpha \in K \text{ special}, \ i,j,k,l \in \{1,\ldots,n\} \text{ distinct}\}$$

is finite.

Hence the special $\alpha \in K$ lie in finitely many $GL_2(\mathbb{Q})$-equivalence classes.

This implies that the special $\alpha \in K$ lie in finitely many $GL_2(\mathbb{Z})$-equivalence classes, and thus, that there are only finitely many orders of K with at least two rational monogenizations.

QED

Thank you for your attention.