# Equivalence relations for polynomials

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

**Joint work with Manjul Bhargava, Kálmán Győry, László Remete, Ashvin Swaminathan**

Number Theory Conference 2022
in honour of Kálmán Győry, János Pintz and András Sárközy
July 4, 2022

Preprint: arXiv:2109.02932v2
Slides: https://pub.math.leidenuniv.nl/∼evertsejh/lectures.shtml

# Aim of the lecture

In the 1850-s, Hermite introduced an equivalence relation for univariate polynomials with integer coefficients, henceforth called 'Hermite equivalence', which was largely unnoticed.

We compare this with better known equivalence relations for polynomials, i.e., $GL_2(\mathbb{Z})$-equivalence and order equivalence (invariant orders of the polynomials being isomorphic).

# Aim of the lecture

In the 1850-s, Hermite introduced an equivalence relation for univariate polynomials with integer coefficients, henceforth called 'Hermite equivalence', which was largely unnoticed.

We compare this with better known equivalence relations for polynomials, i.e., $GL_2(\mathbb{Z})$-equivalence and order equivalence (invariant orders of the polynomials being isomorphic).

It will turn out that
$GL_2(\mathbb{Z})$-equivalence $\Rightarrow$ Hermite equivalence $\Rightarrow$ order equivalence.

Our aim is the following:

- show that the implication arrows cannot be reversed, i.e., to give examples of Hermite equivalent polynomials that are not $GL_2(\mathbb{Z})$-equivalent, and order equivalent polynomials that are not Hermite equivalent.

# $GL_n(\mathbb{Z})$-equivalence of decomposable forms

Hermite equivalence of univariate polynomials is defined by means of decomposable forms associated to these polynomials.

# $GL_n(\mathbb{Z})$-equivalence of decomposable forms

Consider decomposable forms of degree $n \geq 2$ in $n$ variables

$$F(\underline{X}) = c \prod_{i=1}^{n} (\alpha_{i,1} X_1 + \cdots + \alpha_{i,n} X_n) \in \mathbb{Z}[X_1, \ldots, X_n],$$

where $c \in \mathbb{Q}^*$ and $\alpha_{i,j} \in \overline{\mathbb{Q}}$ for $i, j = 1, \ldots, n$.

The *discriminant* of $F$ is given by $D(F) := c^2 \big( \det(\alpha_{i,j})_{1 \leq i,j \leq n} \big)^2$.
We have $D(F) \in \mathbb{Z}$.

# $GL_n(\mathbb{Z})$-equivalence of decomposable forms

Consider decomposable forms of degree $n \geq 2$ in $n$ variables

$$F(\underline{X}) = c \prod_{i=1}^{n} (\alpha_{i,1}X_1 + \cdots + \alpha_{i,n}X_n) \in \mathbb{Z}[X_1, \ldots, X_n],$$

where $c \in \mathbb{Q}^*$ and $\alpha_{i,j} \in \overline{\mathbb{Q}}$ for $i, j = 1, \ldots, n$.

The *discriminant* of $F$ is given by $D(F) := c^2 \big( \det(\alpha_{i,j})_{1 \leq i,j \leq n} \big)^2$.
We have $D(F) \in \mathbb{Z}$.

Two decomposable forms $F, G$ as above are called *$GL_n(\mathbb{Z})$-equivalent* if

$$G(\underline{X}) = \pm F(U\underline{X}) \quad \text{for some } U \in GL_n(\mathbb{Z})$$

(here $\underline{X} = (X_1, \ldots, X_n)^T$ is a column vector).

Two $GL_n(\mathbb{Z})$-equivalent decomposable forms have the same discriminant.

# $GL_n(\mathbb{Z})$-equivalence of decomposable forms

Consider decomposable forms of degree $n \geq 2$ in $n$ variables

$$F(\underline{X}) = c\prod_{i=1}^{n}(\alpha_{i,1}X_1 + \cdots + \alpha_{i,n}X_n) \in \mathbb{Z}[X_1, \ldots, X_n],$$

where $c \in \mathbb{Q}^*$ and $\alpha_{i,j} \in \overline{\mathbb{Q}}$ for $i, j = 1, \ldots, n$.

The *discriminant* of $F$ is given by $D(F) := c^2\big(\det(\alpha_{i,j})_{1\leq i,j\leq n}\big)^2$.
We have $D(F) \in \mathbb{Z}$.

Two decomposable forms $F, G$ as above are called *$GL_n(\mathbb{Z})$-equivalent* if

$$G(\underline{X}) = \pm F(U\underline{X}) \quad \text{for some } U \in GL_n(\mathbb{Z})$$

(here $\underline{X} = (X_1, \ldots, X_n)^T$ is a column vector).

Two $GL_n(\mathbb{Z})$-equivalent decomposable forms have the same discriminant.

**Theorem (Hermite, 1850)**

*Let $n \geq 2$, $D \neq 0$. Then the decomposable forms in $\mathbb{Z}[X_1, \ldots, X_n]$ of degree $n$ and discriminant $D$ lie in finitely many $GL_n(\mathbb{Z})$-equivalence classes.*

# Hermite equivalence of univariate polynomials

Let $f = c(X - \alpha_1)\cdots(X - \alpha_n) \in \mathbb{Z}[X]$ (with $c \in \mathbb{Z}_{\neq 0}$, $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}$).

Define the discriminant of $f$ by $D(f) := c^{2n-2} \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2$.

# Hermite equivalence of univariate polynomials

Let $f = c(X-\alpha_1)\cdots(X-\alpha_n) \in \mathbb{Z}[X]$ (with $c \in \mathbb{Z}_{\neq 0}$, $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}$).

Define the discriminant of $f$ by $D(f) := c^{2n-2}\prod_{1\le i<j\le n}(\alpha_i-\alpha_j)^2$.

To $f$ we associate the decomposable form

$$[f](\underline{X}) := c^{n-1}\prod_{i=1}^{n}(X_1+\alpha_i X_2+\cdots+\alpha_i^{n-1}X_n) \in \mathbb{Z}[X_1,\ldots,X_n].$$

**Fact.** $D(f) = D([f])$ (Vandermonde).

# Hermite equivalence of univariate polynomials

Let $f = c(X-\alpha_1)\cdots(X-\alpha_n) \in \mathbb{Z}[X]$ (with $c \in \mathbb{Z}_{\neq 0}$, $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}$).

Define the discriminant of $f$ by $D(f) := c^{2n-2} \prod_{1\leq i<j\leq n}(\alpha_i - \alpha_j)^2$.

To $f$ we associate the decomposable form

$$[f](\underline{X}) := c^{n-1} \prod_{i=1}^{n} (X_1 + \alpha_i X_2 + \cdots + \alpha_i^{n-1} X_n) \in \mathbb{Z}[X_1, \ldots, X_n].$$

**Fact.** $D(f) = D([f])$ (Vandermonde).

Hermite introduced in 1857 the following equivalence relation:

Two polynomials $f, g \in \mathbb{Z}[X]$ of degree $n$ are called *Hermite equivalent* if the associated decomposable forms $[f]$ and $[g]$ are $GL_n(\mathbb{Z})$-equivalent, i.e., $[g](\underline{X}) = \pm[f](U\underline{X})$ for some $U \in GL_n(\mathbb{Z})$.

# Hermite equivalence of univariate polynomials

Let $f = c(X-\alpha_1)\cdots(X-\alpha_n) \in \mathbb{Z}[X]$ (with $c \in \mathbb{Z}_{\neq 0}$, $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}$).

Define the discriminant of $f$ by $D(f) := c^{2n-2} \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2$.

To $f$ we associate the decomposable form

$$[f](\underline{X}) := c^{n-1} \prod_{i=1}^{n} (X_1 + \alpha_i X_2 + \cdots + \alpha_i^{n-1} X_n) \in \mathbb{Z}[X_1, \ldots, X_n].$$

**Fact.** $D(f) = D([f])$ (Vandermonde).

Hermite introduced in 1857 the following equivalence relation:

Two polynomials $f, g \in \mathbb{Z}[X]$ of degree $n$ are called *Hermite equivalent* if the associated decomposable forms $[f]$ and $[g]$ are $GL_n(\mathbb{Z})$-equivalent, i.e., $[g](\underline{X}) = \pm [f](U\underline{X})$ for some $U \in GL_n(\mathbb{Z})$.

Hermite's theorem on decomposable forms and the above fact imply:

**Theorem (Hermite, 1857)**

*Let $n \ge 2$, $D \neq 0$. Then the polynomials $f \in \mathbb{Z}[X]$ of degree $n$ and of discriminant $D$ lie in finitely many Hermite equivalence classes.*

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

We want to compare Hermite equivalence with $GL_2(\mathbb{Z})$-equivalence.

Two polynomials $f, g \in \mathbb{Z}[X]$ of degree $n$ are called *$GL_2(\mathbb{Z})$-equivalent* if there is $\begin{pmatrix} a & b \\ d & e \end{pmatrix} \in GL_2(\mathbb{Z})$ such that

$$g(X) = \pm(dX + e)^n f\left(\frac{aX+b}{dX+e}\right).$$

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

We want to compare Hermite equivalence with $GL_2(\mathbb{Z})$-equivalence.

Two polynomials $f, g \in \mathbb{Z}[X]$ of degree $n$ are called *$GL_2(\mathbb{Z})$-equivalent* if there is $\left(\begin{smallmatrix} a & b \\ d & e \end{smallmatrix}\right) \in GL_2(\mathbb{Z})$ such that

$$g(X) = \pm(dX+e)^n f\left(\frac{aX+b}{dX+e}\right).$$

**Lemma**

*Let $f, g \in \mathbb{Z}[X]$ be two $GL_2(\mathbb{Z})$-equivalent polynomials of equal degree. Then they are Hermite equivalent.*

The converse is in general not true.

# Proof of Lemma

We have to prove that any two $GL_2(\mathbb{Z})$-equivalent polynomials $f, g$ in $\mathbb{Z}[X]$ are Hermite equivalent.

# Proof of Lemma

We have to prove that any two $GL_2(\mathbb{Z})$-equivalent polynomials $f, g$ in $\mathbb{Z}[X]$ are Hermite equivalent.

Let $f(X) = c\prod_{i=1}^{n}(X - \alpha_i) \in \mathbb{Z}[X]$ and $g(X) = \pm(dX + e)^n f\left(\frac{aX+b}{dX+e}\right)$, where $A := \left(\begin{smallmatrix} a & b \\ d & e \end{smallmatrix}\right) \in GL_2(\mathbb{Z})$.

Then $g(X) = \pm c\prod_{i=1}^{n}(\beta_i X - \gamma_i), \quad \beta_i = d - a\alpha_i, \ \gamma_i = -e + b\alpha_i.$

# Proof of Lemma

We have to prove that any two $GL_2(\mathbb{Z})$-equivalent polynomials $f, g$ in $\mathbb{Z}[X]$ are Hermite equivalent.

Let $f(X) = c\prod_{i=1}^{n}(X - \alpha_i) \in \mathbb{Z}[X]$ and $g(X) = \pm(dX + e)^n f\left(\frac{aX+b}{dX+e}\right)$, where $A := \left(\begin{smallmatrix} a & b \\ d & e \end{smallmatrix}\right) \in GL_2(\mathbb{Z})$.

Then $g(X) = \pm c\prod_{i=1}^{n}(\beta_i X - \gamma_i), \quad \beta_i = d - a\alpha_i, \ \gamma_i = -e + b\alpha_i.$

Define the inner product of two column vectors $\underline{x} = (x_1, \dots, x_n)^T$, $\underline{y} = (y_1, \dots, y_n)^T$ by $\langle \underline{x}, \underline{y} \rangle := x_1 y_1 + \cdots + x_n y_n$.
Let as before $\underline{X} = (X_1, \dots, X_n)^T$. Thus,

$$[f](\underline{X}) = c^{n-1}\prod_{i=1}^{n}\langle \underline{a}_i, \underline{X}\rangle, \text{ where } \underline{a}_i = (1, \alpha_i, \dots, , \alpha_i^{n-1})^T,$$

$$[g](\underline{X}) = \pm c^{n-1}\prod_{i=1}^{n}\langle \underline{b}_i, \underline{X}\rangle, \text{ where } \underline{b}_i = (\beta_i^{n-1}, \beta_i^{n-2}\gamma_i, \dots, \gamma_i^{n-1})^T.$$

# Proof of Lemma

We have to prove that any two $GL_2(\mathbb{Z})$-equivalent polynomials $f, g$ in $\mathbb{Z}[X]$ are Hermite equivalent.

Let $f(X) = c\prod_{i=1}^{n}(X - \alpha_i) \in \mathbb{Z}[X]$ and $g(X) = \pm(dX + e)^n f\left(\frac{aX+b}{dX+e}\right)$, where $A := \left(\begin{smallmatrix} a & b \\ d & e \end{smallmatrix}\right) \in GL_2(\mathbb{Z})$.

Then $g(X) = \pm c\prod_{i=1}^{n}(\beta_i X - \gamma_i)$, $\beta_i = d - a\alpha_i$, $\gamma_i = -e + b\alpha_i$.

Define the inner product of two column vectors $\underline{x} = (x_1, \ldots, x_n)^T$, $\underline{y} = (y_1, \ldots, y_n)^T$ by $\langle \underline{x}, \underline{y} \rangle := x_1 y_1 + \cdots + x_n y_n$.
Let as before $\underline{X} = (X_1, \ldots, X_n)^T$. Thus,

$$[f](\underline{X}) = c^{n-1}\prod_{i=1}^{n}\langle \underline{a}_i, \underline{X} \rangle, \text{ where } \underline{a}_i = (1, \alpha_i, \ldots, , \alpha_i^{n-1})^T,$$

$$[g](\underline{X}) = \pm c^{n-1}\prod_{i=1}^{n}\langle \underline{b}_i, \underline{X} \rangle, \text{ where } \underline{b}_i = (\beta_i^{n-1}, \beta_i^{n-2}\gamma_i, \ldots, \gamma_i^{n-1})^T.$$

Then $\underline{b}_i = t(A)\underline{a}_i$ with $t(A) \in GL_n(\mathbb{Z})$ for $i = 1, \ldots, n$. So

$$[g](\underline{X}) = \pm c^{n-1}\prod_{i=1}^{n}\langle t(A)\underline{a}_i, \underline{X} \rangle = \pm c^{n-1}\prod_{i=1}^{n}\langle \underline{a}_i, t(A)^T\underline{X} \rangle = \pm [f](t(A)^T\underline{X}). \quad \square$$

# Finiteness results for $GL_2(\mathbb{Z})$-equivalence

Recall that two polynomials $f, g \in \mathbb{Z}[X]$ of the same degree are $GL_2(\mathbb{Z})$-equivalent if $g(X) = \pm(dX+e)^{\deg f} f\left(\frac{aX+b}{dX+e}\right)$ for some $\left(\begin{smallmatrix} a & b \\ d & e \end{smallmatrix}\right) \in GL_2(\mathbb{Z})$.

**Theorem (Birch and Merriman, 1972)**

*Let $n \geq 2$, $D \neq 0$. Then there are only finitely many $GL_2(\mathbb{Z})$-equivalence classes of polynomials $f \in \mathbb{Z}[X]$ of degree $n$ and discriminant $D$.*

The proof of Birch and Merriman is ineffective.

# Finiteness results for $GL_2(\mathbb{Z})$-equivalence

Recall that two polynomials $f, g \in \mathbb{Z}[X]$ of the same degree are $GL_2(\mathbb{Z})$-equivalent if $g(X) = \pm(dX+e)^{\deg f} f\left(\frac{aX+b}{dX+e}\right)$ for some $\left(\begin{smallmatrix} a & b \\ d & e \end{smallmatrix}\right) \in GL_2(\mathbb{Z})$.

**Theorem (Ev. and Győry, 1991)**

*Let $n \geq 2$, $D \neq 0$. Then there is an effective $C = C(n, D)$ such that every $f \in \mathbb{Z}[X]$ of degree $n$ and discriminant $D$ is $GL_2(\mathbb{Z})$-equivalent to a polynomial $f^*$ with $H(f^*) := \max|\text{coeff. } f^*| \leq C$.*

In 2017, Ev. and Győry proved this with $C = \exp\left((16n^3)^{25n^2}|D|^{5n-3}\right)$.

This extends work of Győry from the late 1970-s on monic polynomials.

The theorems of Birch and Merriman and Ev. and Győry on $GL_2(\mathbb{Z})$-equivalence use finiteness results for unit equations and Baker's theory on logarithmic forms, and thus are much deeper than Hermite's.

# An algebraic criterion for Hermite equivalence

In what follows, we restrict ourselves to polynomials in $\mathbb{Z}[X]$ that are irreducible and primitive, i.e., with coefficients having gcd 1.

For an algebraic number $\alpha$ of degree $n$ define the free $\mathbb{Z}$-module generated by $1, \alpha, \dots, \alpha^{n-1}$,

$$\mathcal{M}_\alpha := \{x_1 + x_2\alpha + \cdots + x_n\alpha^{n-1} : x_1, \dots, x_n \in \mathbb{Z}\}$$

**Lemma**

*Let $f, g \in \mathbb{Z}[X]$ be primitive, irreducible polynomials of degree $\geq 2$. Then $f, g$ are Hermite equivalent if and only if there are $\lambda \neq 0$, a root $\alpha$ of $f$ and a root $\beta$ of $g$ such that $\mathcal{M}_\beta = \lambda\mathcal{M}_\alpha = \{\lambda\xi : \xi \in \mathcal{M}_\alpha\}$.*

# Connection with invariant orders

Let $\mathcal{M}_\alpha := \left\{x_1 + x_2\alpha + \cdots + x_n\alpha^{n-1} : x_1, \ldots, x_n \in \mathbb{Z}\right\}$ for $\alpha$ of degree $n$,

$\mathbb{Z}_\alpha := \{\xi \in \mathbb{Q}(\alpha) : \xi\mathcal{M}_\alpha \subseteq \mathcal{M}_\alpha\}$, the ring of scalars of $\mathcal{M}_\alpha$.

It can be shown that $\mathbb{Z}_\alpha = \mathbb{Z}[\alpha] \cap \mathbb{Z}[\alpha^{-1}]$. It is an order in $\mathbb{Q}(\alpha)$.

Let $f \in \mathbb{Z}[X]$ be a primitive, irreducible polynomial and $\alpha$ a root of $f$. Then $\mathbb{Z}_\alpha$ is called the *invariant order* of $f$; it is up to isomorphism uniquely determined.
The discriminant of $\mathbb{Z}_\alpha$ is equal to $D(f)$.

# Connection with invariant orders

Let $\mathcal{M}_\alpha := \{x_1 + x_2\alpha + \cdots + x_n\alpha^{n-1} : x_1, \ldots, x_n \in \mathbb{Z}\}$ for $\alpha$ of degree $n$,

$\mathbb{Z}_\alpha := \{\xi \in \mathbb{Q}(\alpha) : \xi\mathcal{M}_\alpha \subseteq \mathcal{M}_\alpha\}$, the ring of scalars of $\mathcal{M}_\alpha$.

It can be shown that $\mathbb{Z}_\alpha = \mathbb{Z}[\alpha] \cap \mathbb{Z}[\alpha^{-1}]$. It is an order in $\mathbb{Q}(\alpha)$.

Let $f \in \mathbb{Z}[X]$ be a primitive, irreducible polynomial and $\alpha$ a root of $f$. Then $\mathbb{Z}_\alpha$ is called the *invariant order* of $f$; it is up to isomorphism uniquely determined.
The discriminant of $\mathbb{Z}_\alpha$ is equal to $D(f)$.

We saw that if $f, g$ are primitive, irreducible, Hermite equivalent polynomials then there are $\lambda \neq 0$, a root $\alpha$ of $f$ and a root $\beta$ of $g$ such that $\mathcal{M}_\beta = \lambda\mathcal{M}_\alpha$. This implies $\mathbb{Z}_\alpha = \mathbb{Z}_\beta$.

**Corollary**

*If $f, g$ are irreducible, primitive, Hermite equivalent polynomials in $\mathbb{Z}[X]$, then $f$ has a root $\alpha$ and $g$ a root $\beta$ such that $\mathbb{Z}_\alpha = \mathbb{Z}_\beta$, i.e., $f$ and $g$ have isomorphic invariant orders.*

# Summary

Let $f, g \in \mathbb{Z}[X]$ be two primitive, irreducible polynomials.
Then $f, g$ are $GL_2(\mathbb{Z})$-equivalent
$\Rightarrow$ $f, g$ are Hermite equivalent
$\Rightarrow$ $f, g$ are order equivalent (have isomorphic invariant orders)
$\Rightarrow$ $f, g$ have equal discriminant.

There are only finitely many $GL_2(\mathbb{Z})$-equivalence classes of polynomials of given degree and discriminant.

So each order equivalence class, resp. Hermite equivalence class is the union of finitely many $GL_2(\mathbb{Z})$-equivalence classes.

# The monic case

We are interested in the problem whether or not two polynomials with isomorphic invariant orders are Hermite equivalent.
We first consider monic polynomials.

Let $f \in \mathbb{Z}[X]$ be irreducible and monic and $\alpha$ a root of $f$. Let $\deg f = n$. Recall that

$$\mathcal{M}_\alpha = \{ \sum_{i=1}^{n} x_i \alpha^{i-1} : x_i \in \mathbb{Z} \},\ \mathbb{Z}_\alpha = \{ \xi \in \mathbb{Q}(\alpha) : \xi \mathcal{M}_\alpha \subseteq \mathcal{M}_\alpha \}.$$

Since $f$ is monic, $\alpha^n, \alpha^{n+1}, \ldots \in \mathcal{M}_\alpha$. Hence $\mathcal{M}_\alpha = \mathbb{Z}_\alpha = \mathbb{Z}[\alpha]$.

**Corollary**

*Let $f, g \in \mathbb{Z}[X]$ be irreducible and monic. Then $f, g$ are Hermite equivalent if and only if $f$ has a root $\alpha$ and $g$ a root $\beta$ such that $\mathbb{Z}[\alpha] = \mathbb{Z}[\beta]$, i.e., if and only if $f$ and $g$ have isomorphic invariant orders.*

# The non-monic case

If $f, g \in \mathbb{Z}[X]$ are irreducible and monic, then
$f, g$ are Hermite equivalent $\iff$ $f, g$ have isomorphic invariant orders.

If $f, g \in \mathbb{Z}[X]$ are irreducible, primitive and not both monic, then
$f, g$ are Hermite equivalent $\implies$ $f, g$ have isomorphic invariant orders.

What about $\impliedby$?

# The non-monic case

If $f, g \in \mathbb{Z}[X]$ are irreducible and monic, then
$f, g$ are Hermite equivalent $\Longleftrightarrow$ $f, g$ have isomorphic invariant orders.

If $f, g \in \mathbb{Z}[X]$ are irreducible, primitive and not both monic, then
$f, g$ are Hermite equivalent $\Longrightarrow$ $f, g$ have isomorphic invariant orders.

What about $\Longleftarrow$?

**Theorem (Delone and Faddeev, The theory of irrationalities of the third degree, 1940)**

*Let $f, g \in \mathbb{Z}[X]$ be two irreducible, primitive polynomials of degree 3. If $f, g$ have isomorphic invariant orders then they are $GL_2(\mathbb{Z})$-equivalent, hence Hermite equivalent.*
*So for primitive, irreducible, cubic polynomials, $GL_2(\mathbb{Z})$-equivalence, Hermite equivalence and order equivalence coincide.*

# The non-monic case

If $f, g \in \mathbb{Z}[X]$ are irreducible and monic, then
$f, g$ are Hermite equivalent $\iff$ $f, g$ have isomorphic invariant orders.

If $f, g \in \mathbb{Z}[X]$ are irreducible, primitive and not both monic, then
$f, g$ are Hermite equivalent $\implies$ $f, g$ have isomorphic invariant orders.

What about $\impliedby$?

**Theorem (Delone and Faddeev, The theory of irrationalities of the third degree, 1940)**

*Let $f, g \in \mathbb{Z}[X]$ be two irreducible, primitive polynomials of degree 3. If $f, g$ have isomorphic invariant orders then they are $GL_2(\mathbb{Z})$-equivalent, hence Hermite equivalent.*
*So for primitive, irreducible, cubic polynomials, $GL_2(\mathbb{Z})$-equivalence, Hermite equivalence and order equivalence coincide.*

There are Hermite inequivalent polynomials of degree 4 with isomorphic invariant orders.

Likely, this is true for degree $\geq 5$ as well, but we haven't been able to produce any counterexamples in this case yet.

# Isomorphic invariant orders $\not\Rightarrow$ Hermite equivalence

Let $f \in \mathbb{Z}[X]$ be irreducible and primitive and $\alpha$ a root of $f$. Let $\deg f = n$. Recall that

$$\mathcal{M}_\alpha = \{ \sum_{i=1}^{n} x_i \alpha^{i-1} : x_i \in \mathbb{Z} \}, \ \mathbb{Z}_\alpha = \{ \xi \in \mathbb{Q}(\alpha) : \xi \mathcal{M}_\alpha \subseteq \mathcal{M}_\alpha \}.$$

Define $I_\alpha := \mathbb{Z}_\alpha + \alpha \mathbb{Z}_\alpha$ to be the fractional ideal of $\mathbb{Z}_\alpha$ generated by 1 and $\alpha$.

**Theorem (BEGRS, 2022)**

*Let $f, g \in \mathbb{Z}[X]$ be irreducible and primitive. Then $f, g$ are Hermite equivalent if and only if $f$ has a root $\alpha$ and $g$ a root $\beta$ such that $\mathbb{Z}_\alpha = \mathbb{Z}_\beta$ and the fractional ideals $I_\alpha$ and $I_\beta$ belong to the same ideal class.*

# Isomorphic invariant orders $\not\Rightarrow$ Hermite equivalence

Let $f \in \mathbb{Z}[X]$ be irreducible and primitive and $\alpha$ a root of $f$. Let $\deg f = n$. Recall that

$$\mathcal{M}_\alpha = \{ \sum_{i=1}^{n} x_i \alpha^{i-1} : x_i \in \mathbb{Z} \}, \; \mathbb{Z}_\alpha = \{\xi \in \mathbb{Q}(\alpha) : \xi \mathcal{M}_\alpha \subseteq \mathcal{M}_\alpha\}.$$

Define $I_\alpha := \mathbb{Z}_\alpha + \alpha \mathbb{Z}_\alpha$ to be the fractional ideal of $\mathbb{Z}_\alpha$ generated by 1 and $\alpha$.

**Theorem (BEGRS, 2022)**

*Let $f, g \in \mathbb{Z}[X]$ be irreducible and primitive. Then $f, g$ are Hermite equivalent if and only if $f$ has a root $\alpha$ and $g$ a root $\beta$ such that $\mathbb{Z}_\alpha = \mathbb{Z}_\beta$ and the fractional ideals $I_\alpha$ and $I_\beta$ belong to the same ideal class.*

**Example**

Let $f = 4X^4 - X^3 - 62X^2 + 13X + 255$, $g = 5X^4 - X^3 - 2X^2 - 7X - 6$. Then $f$ and $g$ are irreducible, $f$ has a root $\alpha$ and $g$ a root $\beta$ such that $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$ and $\mathbb{Z}_\alpha = \mathbb{Z}_\beta$ is the maximal order of $\mathbb{Q}(\alpha)$.

But $I_\alpha$ is principal and $I_\beta$ is not. So $f$ and $g$ are not Hermite equivalent.

# Hermite equivalence $\not\Rightarrow$ $GL_2(\mathbb{Z})$-inequivalence

For polynomials of degree 2 (trivial) and of degree 3 (Delone and Faddeev) Hermite equivalence and $GL_2(\mathbb{Z})$-equivalence coincide.

# Hermite equivalence $\not\Rightarrow$ $GL_2(\mathbb{Z})$-inequivalence

For polynomials of degree 2 (trivial) and of degree 3 (Delone and Faddeev) Hermite equivalence and $GL_2(\mathbb{Z})$-equivalence coincide.

**Theorem (BEGRS, 2021)**

*For every $n \geq 4$ there are infinitely many pairs $(f, g)$ of irreducible, primitive polynomials in $\mathbb{Z}[X]$ of degree $n$ such that $f, g$ are Hermite equivalent but $GL_2(\mathbb{Z})$-inequivalent.*
*These pairs lie in different Hermite equivalence classes.*

The proof is by means of an explicit construction.

# The construction (I)

Consider the formal power series $C(X) := \dfrac{1-\sqrt{1-4X}}{2X} = \sum_{i=0}^{\infty} C_i X^i$,

with $C_i = \frac{1}{i+1}\binom{2i}{i} \in \mathbb{Z}$ the $i$-th Catalan number.

# The construction (I)

Consider the formal power series $C(X) := \frac{1-\sqrt{1-4X}}{2X} = \sum_{i=0}^{\infty} C_i X^i$,

with $C_i = \frac{1}{i+1}\binom{2i}{i} \in \mathbb{Z}$ the $i$-th Catalan number.

Let $n \geq 4$, and

$$a^{(n)}(X) := \sum_{i=0}^{n-2} C_i X^i,$$

$$b^{(n)}(X) := \frac{X(a^{(n)}(X))^2 - a^{(n)}(X) + 1}{X^{n-1}},$$

$$k^{(n)}(X) := \frac{1 - X \cdot a^{(n)}(X - X^2)}{(1-X)^{n-1}}.$$

# The construction (I)

Consider the formal power series $C(X) := \frac{1-\sqrt{1-4X}}{2X} = \sum_{i=0}^{\infty} C_i X^i$,

with $C_i = \frac{1}{i+1}\binom{2i}{i} \in \mathbb{Z}$ the $i$-th Catalan number.

Let $n \geq 4$, and

$$a^{(n)}(X) := \sum_{i=0}^{n-2} C_i X^i,$$

$$b^{(n)}(X) := \frac{X(a^{(n)}(X))^2 - a^{(n)}(X) + 1}{X^{n-1}},$$

$$k^{(n)}(X) := \frac{1 - X \cdot a^{(n)}(X - X^2)}{(1-X)^{n-1}}.$$

Note $X^{n-1} | Xa^{(n)}(X)^2 - a^{(n)}(X) + 1$ since $XC(X)^2 - C(X) + 1 = 0$,

$X^{n-1} | 1 - (1-X)a^{(n)}(X - X^2)$ since $C(X - X^2) = \frac{1}{1-X}$,

$(1-X)^{n-1} | 1 - X \cdot a^{(n)}(X - X^2)$.

So $a^{(n)}(X)$, $b^{(n)}(X)$, $k^{(n)}(X)$ are polynomials in $\mathbb{Z}[X]$ of degree $n-2$.

# The construction (II)

Let $a^{(n)}(X)$, $b^{(n)}(X)$, $k^{(n)}(X)$ be the polynomials from the previous slide, let $c$ be either 1 or a prime and $t$ a prime different from $c$, and put

$$f_{t,c}^{(n)}(X) := cX^n + tk^{(n)}(cX),$$
$$g_{t,c}^{(n)}(X) := cX^n + t(1 - 2cX \cdot a^{(n)}(X)) - c^{n-1}t^2b^{(n)}(cX).$$

Note that both $f_{t,c}^{(n)}(X)$, $g_{t,c}^{(n)}(X)$ are polynomials in $\mathbb{Z}[X]$ of degree $n$ with leading coefficient $c$.
They are both primitive, and by Eisenstein's criterion, both irreducible.

# The construction (II)

Let $a^{(n)}(X)$, $b^{(n)}(X)$, $k^{(n)}(X)$ be the polynomials from the previous slide, let $c$ be either 1 or a prime and $t$ a prime different from $c$, and put

$$f_{t,c}^{(n)}(X) := cX^n + tk^{(n)}(cX),$$
$$g_{t,c}^{(n)}(X) := cX^n + t(1 - 2cX \cdot a^{(n)}(X)) - c^{n-1}t^2 b^{(n)}(cX).$$

**Theorem**

*Let $n \geq 4$. Then there are infinitely many pairs $(c, t)$ as above such that $f_{t,c}^{(n)}(X)$, $g_{t,c}^{(n)}(X)$ have the following properties:*

- **(i)** *$f_{t,c}^{(n)}(X)$, $g_{t,c}^{(n)}(X)$ are irreducible, primitive polynomials in $\mathbb{Z}[X]$ of degree $n$ with leading coefficient $c$;*
- **(ii)** *$f_{t,c}^{(n)}(X)$, $g_{t,c}^{(n)}(X)$ are Hermite equivalent;*
- **(iii)** *$f_{t,c}^{(n)}(X)$, $g_{t,c}^{(n)}(X)$ are not $GL_2(\mathbb{Z})$-equivalent.*

*Moreover, the pairs $(f_{t,c}^{(n)}, g_{t,c}^{(n)})$ lie in different Hermite equivalence classes.*

# Special polynomials

A polynomial $f \in \mathbb{Z}[X]$ is called *special* if there is $g \in \mathbb{Z}[X]$ such that $g$ is Hermite equivalent to $f$ but $GL_2(\mathbb{Z})$-inequivalent to $f$.

All polynomials in $\mathbb{Z}[X]$ of degree 2 and 3 are non-special (trivial for $n = 2$, Delone and Faddeev for $n = 3$).

For every $n \geq 4$ we have constructed infinitely many primitive, irreducible special polynomials of degree $n$ that lie in different Hermite equivalence classes (the polynomials $f_{t,c}^{(n)}$ from the previous slide).

**Vague belief**

Most polynomials are non-special.

# Special polynomials

A polynomial $f \in \mathbb{Z}[X]$ is called *special* if there is $g \in \mathbb{Z}[X]$ such that $g$ is Hermite equivalent to $f$ but $GL_2(\mathbb{Z})$-inequivalent to $f$.

All polynomials in $\mathbb{Z}[X]$ of degree 2 and 3 are non-special (trivial for $n = 2$, Delone and Faddeev for $n = 3$).

For every $n \geq 4$ we have constructed infinitely many primitive, irreducible special polynomials of degree $n$ that lie in different Hermite equivalence classes (the polynomials $f_{t,c}^{(n)}$ from the previous slide).

**Question**

*Let $K$ be a given number field. Consider the primitive, irreducible, special polynomials $f \in \mathbb{Z}[X]$ such that a root of $f$ generates $K$. Do these polynomials lie in only finitely Hermite equivalence classes?*

# Special polynomials

A polynomial $f \in \mathbb{Z}[X]$ is called *special* if there is $g \in \mathbb{Z}[X]$ such that $g$ is Hermite equivalent to $f$ but $GL_2(\mathbb{Z})$-inequivalent to $f$.

All polynomials in $\mathbb{Z}[X]$ of degree 2 and 3 are non-special (trivial for $n = 2$, Delone and Faddeev for $n = 3$).

For every $n \geq 4$ we have constructed infinitely many primitive, irreducible special polynomials of degree $n$ that lie in different Hermite equivalence classes (the polynomials $f_{t,c}^{(n)}$ from the previous slide).

**Question**

*Let $K$ be a given number field. Consider the primitive, irreducible, special polynomials $f \in \mathbb{Z}[X]$ such that a root of $f$ generates $K$. Do these polynomials lie in only finitely Hermite equivalence classes?*

There are number fields $K$ of degree 4 for which this is false.

But we do not exclude that for number fields of degree $\geq 5$ this is true.

# A weaker result

For a number field $K$, let $\mathcal{PI}(K)$ denote the set of primitive, irreducible polynomials $f \in \mathbb{Z}[X]$ such that $K$ is generated by a root of $f$.

Recall that $f \in \mathcal{PI}(K)$ is special if there is $g \in \mathbb{Z}[X]$ such that $g$ and $f$ are Hermite equivalent but $GL_2(\mathbb{Z})$-inequivalent.

Call two polynomials $f, g \in \mathbb{Z}[X]$ $GL_2(\mathbb{Q})$-equivalent if they have the same degree, say $n$, and $g(X) = u(dX + e)^n f\left(\frac{aX+b}{dX+e}\right)$ for some $u \in \mathbb{Q}^*$ and $\left(\begin{smallmatrix} a & b \\ d & e \end{smallmatrix}\right) \in GL_2(\mathbb{Q})$.

# A weaker result

For a number field $K$, let $\mathcal{PI}(K)$ denote the set of primitive, irreducible polynomials $f \in \mathbb{Z}[X]$ such that $K$ is generated by a root of $f$.

Recall that $f \in \mathcal{PI}(K)$ is special if there is $g \in \mathbb{Z}[X]$ such that $g$ and $f$ are Hermite equivalent but $GL_2(\mathbb{Z})$-inequivalent.

Call two polynomials $f, g \in \mathbb{Z}[X]$ $GL_2(\mathbb{Q})$-equivalent if they have the same degree, say $n$, and $g(X) = u(dX+e)^n f\left(\frac{aX+b}{dX+e}\right)$ for some $u \in \mathbb{Q}^*$ and $\left(\begin{smallmatrix} a & b \\ d & e \end{smallmatrix}\right) \in GL_2(\mathbb{Q})$.

**Theorem (E.)**

*Let $K$ be a number field of degree $n \geq 5$ whose normal closure has as Galois group the full symmetric group $S_n$.*

*Then the special polynomials in $\mathcal{PI}(K)$ lie in finitely many $GL_2(\mathbb{Q})$-equivalence classes.*

There are number fields $K$ of degree 4 for which this is false.

# Outline of the proof

Assume $[K : \mathbb{Q}] = n \geq 5$ and its normal closure $L$ has Galois group $S_n$.

Let $f \in \mathcal{PI}(K)$ be special. Choose $g \in \mathcal{PI}(K)$ such that $g$ and $f$ are Hermite equivalent but $GL_2(\mathbb{Z})$-inequivalent.

Then $\exists\ \alpha, \beta$ such that $f(\alpha) = g(\beta) = 0$, $K = \mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$.

# Outline of the proof

Assume $[K:\mathbb{Q}] = n \geq 5$ and its normal closure $L$ has Galois group $S_n$.

Let $f \in \mathcal{PI}(K)$ be special. Choose $g \in \mathcal{PI}(K)$ such that $g$ and $f$ are Hermite equivalent but $GL_2(\mathbb{Z})$-inequivalent.

Then $\exists\ \alpha, \beta$ such that $f(\alpha) = g(\beta) = 0$, $K = \mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$.

Let $\xi \mapsto \xi^{(i)}$ $(i = 1, \ldots, n)$ be the embeddings $K \hookrightarrow \mathbb{C}$ and define the *cross ratios* of $\xi$,

$$cr_{ijkl}(\xi) = \frac{(\xi^{(i)} - \xi^{(j)})(\xi^{(k)} - \xi^{(l)})}{(\xi^{(i)} - \xi^{(k)})(\xi^{(j)} - \xi^{(l)})}.$$

**Lemma ($\Leftarrow$ Hermite equivalence of $f$ and $g$)**

$\frac{cr_{ijkl}(\alpha)}{cr_{ijkl}(\beta)} \in \mathcal{O}_L^*$ *for all distinct* $i, j, k, l \in \{1, \ldots, n\}$.

# Outline of the proof

Assume $[K:\mathbb{Q}] = n \geq 5$ and its normal closure $L$ has Galois group $S_n$.

Let $f \in \mathcal{PI}(K)$ be special. Choose $g \in \mathcal{PI}(K)$ such that $g$ and $f$ are Hermite equivalent but $GL_2(\mathbb{Z})$-inequivalent.

Then $\exists\ \alpha, \beta$ such that $f(\alpha) = g(\beta) = 0$, $K = \mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$.

Let $\xi \mapsto \xi^{(i)}$ $(i = 1, \ldots, n)$ be the embeddings $K \hookrightarrow \mathbb{C}$ and define the *cross ratios* of $\xi$,

$$cr_{ijkl}(\xi) = \frac{(\xi^{(i)} - \xi^{(j)})(\xi^{(k)} - \xi^{(l)})}{(\xi^{(i)} - \xi^{(k)})(\xi^{(j)} - \xi^{(l)})}.$$

**Lemma ($\Leftarrow$ Hermite equivalence of $f$ and $g$)**

$\dfrac{cr_{ijkl}(\alpha)}{cr_{ijkl}(\beta)} \in \mathcal{O}_L^*$ *for all distinct* $i, j, k, l \in \{1, \ldots, n\}$.

Using algebraic relations between the cross ratios and finiteness results for unit equations, one shows that there are only finitely many possibilities for the $cr_{ijkl}(\alpha)$.
Any given set of values for the $cr_{ijkl}(\alpha)$ fixes the $GL_2(\mathbb{Q})$-equivalence class of $f$. □

# Quantitative results

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

*Let $n \geq 3$, and let $\mathcal{O}$ be any order of a number field of degree $n$. Then the primitive, irreducible polynomials $f \in \mathbb{Z}[X]$ with invariant order $\mathcal{O}$ lie in at most $C(n)$ $GL_2(\mathbb{Z})$-equivalence classes.*

# Quantitative results

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

*Let $n \geq 3$, and let $\mathcal{O}$ be any order of a number field of degree $n$. Then the primitive, irreducible polynomials $f \in \mathbb{Z}[X]$ with invariant order $\mathcal{O}$ lie in at most $C(n)$ $GL_2(\mathbb{Z})$-equivalence classes.*

The best bounds for $C(n)$ obtained so far:

| $n$ | $C(n)$ | |
|---|---|---|
| 3 | 1 | (Delone, Faddeev, 1940) |
| 4 | 10 | (Bhargava, 2021) |
| $\geq 5$ | $2^{5n^2}$ | (Ev., Győry, 2017) |

# Quantitative results

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

*Let $n \geq 3$, and let $\mathcal{O}$ be any order of a number field of degree $n$. Then the primitive, irreducible polynomials $f \in \mathbb{Z}[X]$ with invariant order $\mathcal{O}$ lie in at most $C(n)$ $GL_2(\mathbb{Z})$-equivalence classes.*

The best bounds for $C(n)$ obtained so far:

| $n$ | $C(n)$ | |
|---|---|---|
| 3 | 1 | (Delone, Faddeev, 1940) |
| 4 | 10 | (Bhargava, 2021) |
| $\geq 5$ | $2^{5n^2}$ | (Ev., Győry, 2017) |

In the case $n = 4$, Bhargava used an injection from the $GL_2(\mathbb{Z})$-equiv. classes of quartic polynomials $f$ with invariant order $\mathcal{O}$ to sols. of a cubic Thue equation $F(x, y) = 1$ and used Bennett's upper bound 10 for the number of sols. of the latter.

# Quantitative results

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

*Let $n \geq 3$, and let $\mathcal{O}$ be any order of a number field of degree $n$. Then the primitive, irreducible polynomials $f \in \mathbb{Z}[X]$ with invariant order $\mathcal{O}$ lie in at most $C(n)$ $GL_2(\mathbb{Z})$-equivalence classes.*

The best bounds for $C(n)$ obtained so far:

| $n$ | $C(n)$ | |
|---|---|---|
| 3 | 1 | (Delone, Faddeev, 1940) |
| 4 | 10 | (Bhargava, 2021) |
| $\geq 5$ | $2^{5n^2}$ | (Ev., Győry, 2017) |

In the case $n = 4$, Bhargava used an injection from the $GL_2(\mathbb{Z})$-equiv. classes of quartic polynomials $f$ with invariant order $\mathcal{O}$ to sols. of a cubic Thue equation $F(x, y) = 1$ and used Bennett's upper bound 10 for the number of sols. of the latter.

The case $n \geq 5$ was deduced from Beukers' and Schlickewei's upper bound $2^{16r+8}$ for the number of solutions of $x + y = 1$ in $x, y \in \Gamma$, with $\Gamma$ a multiplicative group of rank $r$.

# Quantitative results

## Theorem

*Let $n \geq 3$, and let $\mathcal{O}$ be any order of a number field of degree $n$. Then the primitive, irreducible polynomials $f \in \mathbb{Z}[X]$ with invariant order $\mathcal{O}$ lie in at most $C(n)$ $GL_2(\mathbb{Z})$-equivalence classes.*

| $n$ | $C(n)$ | |
|---|---|---|
| 3 | 1 | *(Delone, Faddeev, 1940)* |
| 4 | 10 | *(Bhargava, 2021)* |
| $\geq 5$ | $2^{5n^2}$ | *(Ev., Győry, 2017)* |

## Open problems

- Improve $C(n)$ (to something polynomial in $n$?)
- Lower bounds growing to infinity with $n$.

# Quantitative results

**Theorem**

*Let $n \geq 3$, and let $\mathcal{O}$ be any order of a number field of degree $n$. Then the primitive, irreducible polynomials $f \in \mathbb{Z}[X]$ with invariant order $\mathcal{O}$ lie in at most $C(n)$ $GL_2(\mathbb{Z})$-equivalence classes.*

| $n$ | $C(n)$ | |
|---|---|---|
| 3 | 1 | *(Delone, Faddeev, 1940)* |
| 4 | 10 | *(Bhargava, 2021)* |
| $\geq 5$ | $2^{5n^2}$ | *(Ev., Győry, 2017)* |

**Corollary**

*The primitive, irreducible polynomials $f \in \mathbb{Z}[X]$ of degree $n$ in a given Hermite equivalence class lie in at most $C(n)$ $GL_2(\mathbb{Z})$-equivalence classes.*

# Congratulations, Kálmán, János, András.