Hermite equivalence of polynomials

Jan-Hendrik Evertse
Universiteit Leiden

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

Oberwolfach workshop 'Diophantische Approximationen'
April 22, 2022

Preprint: arXiv:2109.02932v2
Slides: https://pub.math.leidenuniv.nl/$\sim$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 a better known equivalence relation, i.e., $GL_2(\mathbb{Z})$-equivalence.

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 a better known equivalence relation, i.e., $GL_2(\mathbb{Z})$-equivalence.

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

Our aims are the following:

- show that Hermite equivalence is weaker than $GL_2(\mathbb{Z})$-equivalence, i.e., to give examples of Hermite equivalent polynomials that are not $GL_2(\mathbb{Z})$-equivalent;
- say something about the number of $GL_2(\mathbb{Z})$-equivalence classes going into a Hermite equivalence class.

$GL_n(\mathbb{Z})$-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 $D(f) := c^{2n-2} \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2$.

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

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 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 $n \geq 2$, $D \neq 0$. 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 $\left(\begin{smallmatrix} a & b \\ d & e \end{smallmatrix}\right) \in GL_2(\mathbb{Z})$ such that

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

$GL_2(\mathbb{Z})$-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 $\underline{x} = (x_1, \ldots, x_n)^T$, $\underline{y} = (y_1, \ldots, y_n)^T$ 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,

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

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

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 $\underline{x} = (x_1, \ldots, x_n)^T$, $\underline{y} = (y_1, \ldots, y_n)^T$ 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 $C = \exp\left((16n^3)^{25n^2}|D|^{5n-3}\right)$.

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 α of degree n define the free $\mathbb{Z}$-module generated by $1, \alpha, \ldots, \alpha^{n-1}$,

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

Lemma

Let $f, g \in \mathbb{Z}[X]$ be primitive, irreducible polynomials of degree ≥ 2. Then f, g are Hermite equivalent if and only if there are $\lambda \neq 0$, a root α of f and a root β 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 α 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 α a root of f. Then $\mathbb{Z}_\alpha$ is called the *invariant order* of f; it is up to isomorphism uniquely determined.

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 α of degree n,

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

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 α a root of f. Then $\mathbb{Z}_\alpha$ is called the *invariant order* of f; it is up to isomorphism uniquely determined.

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

Corollary 1

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

The monic case

Let $f \in \mathbb{Z}[X]$ be irreducible and monic and α 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 2

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 α and g a root β 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 $\iff$ 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 $\impliedby$?

Any two irreducible, primitive polynomials of degree 3 with isomorphic invariant orders are $GL_2(\mathbb{Z})$-equivalent (Delone and Faddeev, The theory of irrationalities of the third degree, 1940).

Hence any two irreducible, primitive, Hermite equivalent polynomials of degree 3 are $GL_2(\mathbb{Z})$-equivalent.

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 $\impliedby$?

Any two irreducible, primitive polynomials of degree 3 with isomorphic invariant orders are $GL_2(\mathbb{Z})$-equivalent (Delone and Faddeev, The theory of irrationalities of the third degree, 1940).

Hence any two irreducible, primitive, Hermite equivalent polynomials of degree 3 are $GL_2(\mathbb{Z})$-equivalent.

For degree 4 this is no longer true (and very likely neither for degree ≥ 5 but we haven't been able to produce any counterexamples in this case yet).

The non-monic case

Let $f \in \mathbb{Z}[X]$ be irreducible and primitive and α 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 α.

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 α and g a root β such that $\mathbb{Z}_\alpha = \mathbb{Z}_\beta$ and the fractional ideals I_α and I_β belong to the same ideal class.

The non-monic case

Let $f \in \mathbb{Z}[X]$ be irreducible and primitive and α 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 α.

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 α and g a root β such that $\mathbb{Z}_\alpha = \mathbb{Z}_\beta$ and the fractional ideals I_α and I_β 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 α and g a root β 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_α is principal and I_β is not. So f and g are not Hermite equivalent.

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)
≥ 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)
≥ 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)
≥ 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 Γ 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)*
≥ 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)*
≥ 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.

Hermite equivalent but $GL_2(\mathbb{Z})$-inequivalent polynomials

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

Hermite equivalent but $GL_2(\mathbb{Z})$-inequivalent polynomials

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

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

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

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

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 $\quad X^{n-1} | Xa^{(n)}(X)^2 - a^{(n)}(X) + 1$ 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

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

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

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

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.

Lemma

Let α be a root of $f_{t,c}^{(n)}(X)$. Then $\beta := \alpha - c\alpha^2$ is a root of $g_{t,c}^{(n)}(X)$ and moreover, $\alpha = p_{t,c}^{(n)}(\beta)$, where

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

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

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

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.

Lemma

Let α be a root of $f_{t,c}^{(n)}(X)$. Then $\beta := \alpha - c\alpha^2$ is a root of $g_{t,c}^{(n)}(X)$ and moreover, $\alpha = p_{t,c}^{(n)}(\beta)$, where

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

Proposition

$\mathcal{M}_\alpha = \mathcal{M}_\beta$, so $f_{t,c}^{(n)}(X)$ and $g_{t,c}^{(n)}(X)$ are Hermite equivalent.

The final result

Theorem (BEGRS, 2021)

Let $n \geq 4$, and let $p > C_{n-1} = n^{-1}\binom{2n-2}{n-1}$ be a prime such that $k^{(n+1)}(X)$ has no zeros modulo p.
Further, let c be either 1 or a prime, and t a prime, such that

$$(*) \qquad c \equiv 1 \pmod{np}, \quad C_{n-1}t \equiv 1 \pmod{p}, \quad t \neq c.$$

Then the polynomials $f_{t,c}^{(n)}(X)$, $g_{t,c}^{(n)}(X)$ 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.*

The final result

Theorem (BEGRS, 2021)

Let $n \geq 4$, and let $p > C_{n-1} = n^{-1}\binom{2n-2}{n-1}$ be a prime such that $k^{(n+1)}(X)$ has no zeros modulo p.
Further, let c be either 1 or a prime, and t a prime, such that

$$(*) \qquad c \equiv 1 \pmod{np}, \quad C_{n-1}t \equiv 1 \pmod{p}, \quad t \neq c.$$

Then the polynomials $f_{t,c}^{(n)}(X)$, $g_{t,c}^{(n)}(X)$ 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.*

Using Newton polygons with various primes one shows that the polynomials $k^{(n+1)}(X)$ ($n \geq 4$) are irreducible.

Then by Chebotarev's density theorem there are infinitely many primes p such that $k^{(n+1)}(X)$ has no zeros modulo p.

The final result

Theorem (BEGRS, 2021)

Let $n \geq 4$, and let $p > C_{n-1} = n^{-1}\binom{2n-2}{n-1}$ be a prime such that $k^{(n+1)}(X)$ has no zeros modulo p.
Further, let c be either 1 or a prime, and t a prime, such that

$$(*) \qquad c \equiv 1 \,(\mathrm{mod}\, np), \quad C_{n-1}t \equiv 1 \,(\mathrm{mod}\, p), \quad t \neq c.$$

Then the polynomials $f_{t,c}^{(n)}(X)$, $g_{t,c}^{(n)}(X)$ 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.*

By Dirichlet's theorem on primes in arithmetic progressions, there are infinitely many pairs (c, t) with (*).

This gives for every $n \geq 4$, infinitely many pairs (f, g) of irreducible, primitive polynomials of degree n that are Hermite equivalent but not $GL_2(\mathbb{Z})$-equivalent. By making a further selection, we get infinitely many pairs lying in different Hermite equivalence classes.

Special polynomials

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

For every $n \geq 4$ there are infinitely many primitive, irreducible, special polynomials $f \in \mathbb{Z}[X]$ of degree n that are pairwise Hermite inequivalent.

Vague belief

For a given number field K, let $\mathcal{PI}(K)$ denote the set of primitive, irreducible polynomials that have a root that generates K.

Then 'most' polynomials in $\mathcal{PI}(K)$ are non-special.

Perhaps they lie in only finitely many $GL_2(\mathbb{Z})$-equivalence classes?

A result on special polynomials (work in progress)

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

For a given number field K, we denote by $\mathcal{PI}(K)$ the set of primitive, irreducible polynomials $f \in \mathbb{Z}[X]$ with $\mathbb{Q}[X]/(f) \cong K$.

We call two polynomials $f, g \in \mathbb{Z}[X]$ of degree n *$GL_2(\mathbb{Q})$-equivalent* if $g(X) = \lambda(dx+e)^n f\left(\frac{aX+b}{dX+e}\right)$ for some $\lambda \in \mathbb{Q}^*$ and $\left(\begin{smallmatrix} a & b \\ d & e \end{smallmatrix}\right) \in GL_2(\mathbb{Q})$.

A result on special polynomials (work in progress)

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

For a given number field K, we denote by $\mathcal{PI}(K)$ the set of primitive, irreducible polynomials $f \in \mathbb{Z}[X]$ with $\mathbb{Q}[X]/(f) \cong K$.

We call two polynomials $f, g \in \mathbb{Z}[X]$ of degree n *$GL_2(\mathbb{Q})$-equivalent* if $g(X) = \lambda(dx+e)^n f\left(\frac{aX+b}{dX+e}\right)$ for some $\lambda \in \mathbb{Q}^*$ and $\left(\begin{smallmatrix} a & b \\ d & e \end{smallmatrix}\right) \in GL_2(\mathbb{Q})$.

Theorem

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.

A result on special polynomials (work in progress)

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

For a given number field K, we denote by $\mathcal{PI}(K)$ the set of primitive, irreducible polynomials $f \in \mathbb{Z}[X]$ with $\mathbb{Q}[X]/(f) \cong K$.

We call two polynomials $f, g \in \mathbb{Z}[X]$ of degree n *$GL_2(\mathbb{Q})$-equivalent* if $g(X) = \lambda(dx+e)^n f\left(\frac{aX+b}{dX+e}\right)$ for some $\lambda \in \mathbb{Q}^*$ and $\left(\begin{smallmatrix} a & b \\ d & e \end{smallmatrix}\right) \in GL_2(\mathbb{Q})$.

Theorem

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.

For number fields of degree 4 this is in general not true.

The proof uses finiteness results for unit equations.

A result on special polynomials (work in progress)

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

For a given number field K, we denote by $\mathcal{PI}(K)$ the set of primitive, irreducible polynomials $f \in \mathbb{Z}[X]$ with $\mathbb{Q}[X]/(f) \cong K$.

We call two polynomials $f, g \in \mathbb{Z}[X]$ of degree n *$GL_2(\mathbb{Q})$-equivalent* if $g(X) = \lambda(dx + e)^n f\left(\frac{aX+b}{dX+e}\right)$ for some $\lambda \in \mathbb{Q}^*$ and $\left(\begin{smallmatrix} a & b \\ d & e \end{smallmatrix}\right) \in GL_2(\mathbb{Q})$.

Theorem

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.

Question

In the above theorem, can $GL_2(\mathbb{Q})$-equivalence be replaced by $GL_2(\mathbb{Z})$-equivalence?

Thank you for your attention.