Hermite equivalence of polynomials

Jan-Hendrik Evertse
Universiteit Leiden

Joint work with Kálmán Győry and László Remete

Debrecen On-line Research Seminar
“Diophantine Number Theory”

January 7, 2022

Slides have been posted on
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 more established equivalence relations, i.e., $\mathbb{Z}$-equivalence for monic polynomials and $GL_2(\mathbb{Z})$-equivalence for not necessarily monic polynomials.

It will turn out that $\mathbb{Z}$-equivalence and $GL_2(\mathbb{Z})$-equivalence imply Hermite 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 more established equivalence relations, i.e., $\mathbb{Z}$-equivalence for monic polynomials and $GL_2(\mathbb{Z})$-equivalence for not necessarily monic polynomials.

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

We are interested in the following problems:

- to show that Hermite equivalence is weaker than $\mathbb{Z}$-equivalence and $GL_2(\mathbb{Z})$-equivalence, i.e., to give examples of Hermite equivalent polynomials that are not $\mathbb{Z}$-equivalent or $GL_2(\mathbb{Z})$-equivalent;
- say something about the number of $\mathbb{Z}$-equivalence classes or $GL_2(\mathbb{Z})$-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 $D(f) := c^{2n-2} \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2$.

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

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

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'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.

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

We want to compare the Hermite equivalence with other, better known equivalence relations for univariate polynomials.

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

We want to compare the Hermite equivalence with other, better known equivalence relations for univariate polynomials.

Two monic polynomials $f, g \in \mathbb{Z}[X]$ of degree n are called *$\mathbb{Z}$-equivalent* if $g(X) = f(X + a)$ or $g(X) = (-1)^n f(-X + a)$ for some $a \in \mathbb{Z}$.

Two not necessarily monic 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 $g(X) = \pm(dX + e)^n f(\frac{aX+b}{dX+e})$.

$\mathbb{Z}$-equivalent monic polynomials in $\mathbb{Z}[X]$ are clearly $GL_2(\mathbb{Z})$-equivalent.

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

We want to compare the Hermite equivalence with other, better known equivalence relations for univariate polynomials.

Two monic polynomials $f, g \in \mathbb{Z}[X]$ of degree n are called *$\mathbb{Z}$-equivalent* if $g(X) = f(X+a)$ or $g(X) = (-1)^n f(-X+a)$ for some $a \in \mathbb{Z}$.

Two not necessarily monic 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 $g(X) = \pm(dX+e)^n f(\frac{aX+b}{dX+e})$.

$\mathbb{Z}$-equivalent monic polynomials in $\mathbb{Z}[X]$ are clearly $GL_2(\mathbb{Z})$-equivalent.

Lemma

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

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

We want to compare the Hermite equivalence with other, better known equivalence relations for univariate polynomials.

Two monic polynomials $f, g \in \mathbb{Z}[X]$ of degree n are called *$\mathbb{Z}$-equivalent* if $g(X) = f(X + a)$ or $g(X) = (-1)^n f(-X + a)$ for some $a \in \mathbb{Z}$.

Two not necessarily monic 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 $g(X) = \pm(dX + e)^n f(\frac{aX+b}{dX+e})$.

$\mathbb{Z}$-equivalent monic polynomials in $\mathbb{Z}[X]$ are clearly $GL_2(\mathbb{Z})$-equivalent.

Lemma

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

We will give examples showing that the converse is in general not true.

Proof of Lemma

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

Proof of Lemma

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

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

Proof of Lemma

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

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

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

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

A finiteness result for $\mathbb{Z}$-equivalence

Recall that two monic polynomials $f, g \in \mathbb{Z}[X]$ are $\mathbb{Z}$-equivalent if $g(X) = f(X+a)$ or $(-1)^{\deg f} f(-X+a)$ for some $a \in \mathbb{Z}$.

Theorem (Győry, 1973,1974)

Let $D \neq 0$. Then there are only finitely many $\mathbb{Z}$-equivalence classes of monic polynomials $f \in \mathbb{Z}[X]$ of discriminant D, and a full system of representatives of those can be determined effectively.

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

Recall that two polynomials $f, g \in \mathbb{Z}[X]$ 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 $D \neq 0$. Then there are only finitely many $GL_2(\mathbb{Z})$-equivalence classes of polynomials $f \in \mathbb{Z}[X]$ of discriminant D.

The proof of Birch and Merriman is ineffective.

In 1991, Ev. and Győry gave an effective proof of the theorem of Birch and Merriman, implying that a full system of representatives for the $GL_2(\mathbb{Z})$-equivalence classes can be determined effectively.

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

Recall that two polynomials $f, g \in \mathbb{Z}[X]$ 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 $D \neq 0$. Then there are only finitely many $GL_2(\mathbb{Z})$-equivalence classes of polynomials $f \in \mathbb{Z}[X]$ of discriminant D.

The proof of Birch and Merriman is ineffective.

In 1991, Ev. and Győry gave an effective proof of the theorem of Birch and Merriman, implying that a full system of representatives for the $GL_2(\mathbb{Z})$-equivalence classes can be determined effectively.

The theorems of Győry on $\mathbb{Z}$-equivalence and 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 that of Hermite on his equivalence.

An algebraic criterion for Hermite equivalence

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

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

Call a polynomial with integer coefficients *primitive* if its coefficients have gcd 1.

Henceforth, all polynomials will be primitive.

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 $\mathcal{M}_\beta = \lambda\mathcal{M}_\alpha = \{\lambda\xi : \xi \in \mathcal{M}_\alpha\}$.

Proof of Lemma

Let $f = c\prod_{i=1}^{n}(X-\alpha_i)$, $g = c'\prod_{i=1}^{n}(X-\beta_i) \in \mathbb{Z}[X]$ be irreducible, primitive. Then

$$[f](\underline{X}) = c^{n-1}\prod_{i=1}^{n}\langle \underline{a}_i, \underline{X}\rangle, \quad [g](\underline{X}) = c'^{n-1}\prod_{i=1}^{n}\langle \underline{b}_i, \underline{X}\rangle,$$

with $\underline{a}_i = (1, \alpha_i, \ldots, \alpha_i^{n-1})^T$, $\underline{b}_i = (1, \beta_i, \ldots, \beta_i^{n-1})^T$.

Proof of Lemma

Let $f = c\prod_{i=1}^n (X - \alpha_i)$, $g = c'\prod_{i=1}^n (X - \beta_i) \in \mathbb{Z}[X]$ be irreducible, primitive. Then

$$[f](\underline{X}) = c^{n-1}\prod_{i=1}^n \langle \underline{a}_i, \underline{X}\rangle, \quad [g](\underline{X}) = c'^{n-1}\prod_{i=1}^n \langle \underline{b}_i, \underline{X}\rangle,$$

with $\underline{a}_i = (1, \alpha_i, \ldots, \alpha_i^{n-1})^T$, $\underline{b}_i = (1, \beta_i, \ldots, \beta_i^{n-1})^T$.

So f, g are Hermite equivalent

$$\begin{aligned} &\iff \quad \exists U \in GL_n(\mathbb{Z}) \text{ with } [g](\underline{X}) = \pm[f](U\underline{X}) \\ &\iff \quad \exists U \in GL_n(\mathbb{Z}), \lambda_i \neq 0 \text{ with } \langle \underline{b}_i, \underline{X}\rangle = \lambda_i \langle \underline{a}_i, U\underline{X}\rangle \text{ for } i = 1, \ldots, n \\ &\qquad\ \text{(after reindexing, for } \Leftarrow \text{ use that } [g](\underline{X}), [f](U\underline{X}) \text{ are primitive)} \end{aligned}$$

Proof of Lemma

Let $f = c\prod_{i=1}^n (X-\alpha_i)$, $g = c'\prod_{i=1}^n (X-\beta_i) \in \mathbb{Z}[X]$ be irreducible, primitive. Then

$$[f](\underline{X}) = c^{n-1}\prod_{i=1}^n \langle \underline{a}_i, \underline{X}\rangle, \quad [g](\underline{X}) = c'^{n-1}\prod_{i=1}^n \langle \underline{b}_i, \underline{X}\rangle,$$

with $\underline{a}_i = (1, \alpha_i, \ldots, \alpha_i^{n-1})^T$, $\underline{b}_i = (1, \beta_i, \ldots, \beta_i^{n-1})^T$.

So f, g are Hermite equivalent

$\iff$ $\exists U \in GL_n(\mathbb{Z})$ with $[g](\underline{X}) = \pm[f](U\underline{X})$

$\iff$ $\exists U \in GL_n(\mathbb{Z}), \lambda_i \neq 0$ with $\langle \underline{b}_i, \underline{X}\rangle = \lambda_i \langle \underline{a}_i, U\underline{X}\rangle$ for $i = 1, \ldots, n$
(after reindexing, for $\Leftarrow$ use that $[g](\underline{X})$, $[f](U\underline{X})$ are primitive)

$\iff$ $\exists U \in GL_n(\mathbb{Z})$, $\lambda_i \neq 0$ with $\underline{b}_i = \lambda_i U^T \underline{a}_i$ for $i = 1, \ldots, n$

$\iff$ $\exists \lambda_i \neq 0$ with $\mathcal{M}_{\beta_i} = \lambda_i \mathcal{M}_{\alpha_i}$ for $i = 1, \ldots, n$

$\iff$ $\exists \lambda \neq 0$, root α of f, root β of g with $\mathcal{M}_\beta = \lambda \mathcal{M}_\alpha$
(for $\Leftarrow$ take for $\alpha_i, \beta_i, \lambda_i$ the conjugates of α, β, λ). □

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

We saw that if f, g are Hermite equivalent primitive, irreducible 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 Hermite equivalent, irreducible, primitive 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

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

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, hence Hermite equivalent (Delone and Faddeev, 1940).

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, hence Hermite equivalent (Delone and Faddeev, 1940).
- Bhargava and Swaminathan (4/1/2022) gave a method to produce irreducible, primitive polynomials of degree 4 that have isomorphic invariant orders but are not Hermite equivalent.

Example

$f = 4X^4 - X^3 - 62X^2 + 13X + 255$, $g = 5X^4 - X^3 - 2X^2 - 7X - 6$ have isomorphic invariant orders but are not Hermite equivalent.

The non-monic case

In fact, Bhargava and Swaminathan used a more precise criterion to obtain their example.

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 (Bhargava, Swaminathan, 4/1/2022)

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.

Quantitative results

Recall that if $f \in \mathbb{Z}[X]$ is an irreducible, primitive polynomial, then the invariant order of f is $\mathbb{Z}_\alpha = \mathbb{Z}[\alpha] \cap \mathbb{Z}[\alpha^{-1}]$, where α is any root of f. In the case that f is monic, this invariant order is $\mathbb{Z}[\alpha]$.

$f, g \in \mathbb{Z}[X]$ are $\mathbb{Z}$-equivalent if $g(X) = f(X + a)$ or $(-1)^{\deg f} f(-X + a)$ for some $a \in \mathbb{Z}$.

$f, g \in \mathbb{Z}[X]$ are $GL_2(\mathbb{Z})$-equivalent if $g(X) = \pm(dX + e)^{\deg f} f(\frac{aX+b}{dX+e})$ for some $\begin{pmatrix} a & b \\ d & e \end{pmatrix} \in GL_2(\mathbb{Z})$.

Theorem

Let $n \geq 3$, and let $\mathcal{O}$ be any order of a number field of degree n.

(i) *(Ev., Győry, 1985) The monic, irreducible polynomials $f \in \mathbb{Z}[X]$ with invariant order $\mathcal{O}$ lie in at most $C_1(n)$ $\mathbb{Z}$-equivalence classes.*

(ii) *(Bérczes, Ev., Győry, 2004) The primitive, irreducible polynomials $f \in \mathbb{Z}[X]$ with invariant order $\mathcal{O}$ lie in at most $C_2(n)$ $GL_2(\mathbb{Z})$-equivalence classes.*

Here $C_1(n)$, $C_2(n)$ depend on n only.

Quantitative results

Theorem

Let $n \geq 3$, and let $\mathcal{O}$ be any order of a number field of degree n.

(i) *The monic, irreducible polynomials $f \in \mathbb{Z}[X]$ with invariant order $\mathcal{O}$ lie in at most $C_1(n)$ $\mathbb{Z}$-equivalence classes.*

(ii) *The primitive, irreducible polynomials $f \in \mathbb{Z}[X]$ with invariant order $\mathcal{O}$ lie in at most $C_2(n)$ $GL_2(\mathbb{Z})$-equivalence classes.*

The best bounds for $C_1(n)$, $C_2(n)$ obtained so far (ignoring earlier work):

n	$C_1(n)$	$C_2(n)$
3	10 (Bennett, 2001)	1 (Delone, Faddeev, 1940)
4	2760 (Akhtari, Bhargava, 2021)	10 (Bhargava, 2021)
≥ 5	$2^{4(n+5)(n-2)}$ (Ev. 2011)	2^{5n^2} (Ev., Győry, 2017)

Quantitative results

Theorem

Let $n \geq 3$, and let $\mathcal{O}$ be any order of a number field of degree n.

(i) *The monic, irreducible polynomials $f \in \mathbb{Z}[X]$ with invariant order $\mathcal{O}$ lie in at most $C_1(n)$ $\mathbb{Z}$-equivalence classes.*

(ii) *The primitive, irreducible polynomials $f \in \mathbb{Z}[X]$ with invariant order $\mathcal{O}$ lie in at most $C_2(n)$ $GL_2(\mathbb{Z})$-equivalence classes.*

n	$C_1(n)$	$C_2(n)$
3	10 *(Bennett, 2001)*	1 *(Delone, Faddeev, 1940)*
4	2760 *(Akhtari, Bhargava, 2021)*	10 *(Bhargava, 2021)*
≥ 5	$2^{4(n+5)(n-2)}$ *(Ev. 2011)*	2^{5n^2} *(Ev., Győry, 2017)*

There is a uniform bound $T(n)$ such that if $F \in \mathbb{Z}[X, Y]$ is any irreducible binary form of degree $n \geq 3$, then the Thue equation $F(x, y) = 1$, $x, y \in \mathbb{Z}$ has at most $T(n)$ solutions.

- $C_1(3) \leq T(3)$, $T(3) \leq 10$ (Bennett, 2001);
- $C_1(n) \leq C_2(n)T(n)$ for $n \geq 4$, $C_2(4) \leq C_1(3)$ (Bhargava, theory of cubic resolvent orders), $T(4) \leq 276$ (Akhtari, 2021);
- (for $n \geq 5$) reduction to unit equations in two unknowns.

Quantitative results

Theorem

Let $n \geq 3$, and let $\mathcal{O}$ be any order of a number field of degree n.
(i) *The monic, irreducible polynomials $f \in \mathbb{Z}[X]$ with invariant order $\mathcal{O}$ lie in at most $C_1(n)$ $\mathbb{Z}$-equivalence classes.*

(ii) *The primitive, irreducible polynomials $f \in \mathbb{Z}[X]$ with invariant order $\mathcal{O}$ lie in at most $C_2(n)$ $GL_2(\mathbb{Z})$-equivalence classes.*

n	$C_1(n)$	$C_2(n)$
3	10 *(Bennett, 2001)*	1 *(Delone, Faddeev, 1940)*
4	2760 *(Akhtari, Bhargava, 2021)*	10 *(Bhargava, 2021)*
≥ 5	$2^{4(n+5)(n-2)}$ *(Ev. 2011)*	2^{5n^2} *(Ev., Győry, 2017)*

Open problems

- Improve $C_1(n)$, $C_2(n)$ (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.
(i) *The monic, irreducible polynomials $f \in \mathbb{Z}[X]$ with invariant order $\mathcal{O}$ lie in at most $C_1(n)$ $\mathbb{Z}$-equivalence classes.*

(ii) *The primitive, irreducible polynomials $f \in \mathbb{Z}[X]$ with invariant order $\mathcal{O}$ lie in at most $C_2(n)$ $GL_2(\mathbb{Z})$-equivalence classes.*

n	$C_1(n)$	$C_2(n)$
3	10 *(Bennett, 2001)*	1 *(Delone, Faddeev, 1940)*
4	2760 *(Akhtari, Bhargava, 2021)*	10 *(Bhargava, 2021)*
≥ 5	$2^{4(n+5)(n-2)}$ *(Ev. 2011)*	2^{5n^2} *(Ev., Győry, 2017)*

Corollary

(i) *The monic, irreducible polynomials $f \in \mathbb{Z}[X]$ of degree n in a given Hermite equivalence class lie in at most $C_1(n)$ $\mathbb{Z}$-equivalence classes.*

(ii) *The primitive, irreducible polynomials $f \in \mathbb{Z}[X]$ of degree n in a given Hermite equivalence class lie in at most $C_2(n)$ $GL_2(\mathbb{Z})$-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.

For polynomials of degree ≥ 4 this is not the case.

Theorem

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 equivalent classes.

We give Remete's 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 $C(X) := \frac{1-\sqrt{1-4X}}{2X} = \sum_{i=0}^{\infty} C_i X^i$,

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

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

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 1

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

$GL_2(\mathbb{Z})$-inequivalence

We want to prove that $f_{t,c}^{(n)}(X)$ and $g_{t,c}^{(n)}(X)$ are not $GL_2(\mathbb{Z})$-equivalent. An important ingredient is the following:

Lemma

Let $n \geq 4$. Then the polynomial $k^{(n)}(X)$ is irreducible.

The involved proof uses a theorem of Dumas (1906), which gives, for a given $f \in \mathbb{Z}[X]$ and a prime q, a small list of possibilities for the degrees of the irreducible factors of f in $\mathbb{Z}_q[X]$.

This list can be read off from the Newton polygon of f with respect to q.

$GL_2(\mathbb{Z})$-inequivalence

We want to prove that $f_{t,c}^{(n)}(X)$ and $g_{t,c}^{(n)}(X)$ are not $GL_2(\mathbb{Z})$-equivalent. An important ingredient is the following:

Lemma

Let $n \geq 4$. Then the polynomial $k^{(n)}(X)$ is irreducible.

The involved proof uses a theorem of Dumas (1906), which gives, for a given $f \in \mathbb{Z}[X]$ and a prime q, a small list of possibilities for the degrees of the irreducible factors of f in $\mathbb{Z}_q[X]$.

This list can be read off from the Newton polygon of f with respect to q.

By applying Dumas' theorem with a couple of distinct primes to

$$k^{(n)}(1+X) = C_{n-1} \sum_{i=0}^{n-2} \binom{n}{i} \frac{(n-1-i)(n-i)}{(n-1+i)(n+i)} \cdot X^i$$

one obtains that $k^{(n)}(X)$ is either irreducible or has a rational root.

By a separate argument it is excluded that $k^{(n)}(X)$ has a rational root. □

$GL_2(\mathbb{Z})$-inequivalence

Lemma

Let $n \geq 4$. Then the polynomial $k^{(n)}(X)$ is irreducible.

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

Proposition 2

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

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

Then the polynomials $f_{t,c}^{(n)}(X)$, $g_{t,c}^{(n)}(X)$ are $GL_2(\mathbb{Z})$-inequivalent.

Summary

By combining Propositions 1 and 2 one obtains:

Theorem

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

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

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.*

Summary

Theorem

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.

Thank you for your attention

Thank you for your attention

and last but not least

Thank you for your attention

and last but not least

HAPPY NEW YEAR !!!