Comparing equivalences of polynomials

An addendum to the talk of K. Győry on reduction theory of integral polynomials

László Remete

Joint work with M. Bhargava, J.-H. Evertse, K. Győry and A. Swaminathan

University of Debrecen

2023. 12. 01.

Introduction

The purpose of this talk is to compare the $\mathbb{Z}$, the $GL_2(\mathbb{Z})$ and the Hermite equivalences following the paper *Hermite equivalence of polynomials* (B.E.Gy.R.S. 2023)

Basic results:

- Lagrange 1773: There are only finitely many $GL_2(\mathbb{Z})$-equivalence classes of **quadratic** polynomials in $\mathbb{Z}[X]$ with given non-zero discriminant. (effective)
- Hermite 1851: There are only finitely many $GL_2(\mathbb{Z})$-equivalence classes of **cubic** polynomials in $\mathbb{Z}[X]$ with given non-zero discriminant. (effective)
- Delone, Nagell 1930: There are only finitely many $\mathbb{Z}$-equivalence classes of **cubic monic** polynomials in $\mathbb{Z}[X]$ with given non-zero discriminant. (ineffective)

Hermite's attempt to extend his results

Hermite attempted to extend his theorem (1851) on cubic polynomials to the case of arbitrary degree $n \geq 4$, but without success. Instead, he proved a theorem with a weaker equivalence.

- Hermite 1857: There are only finitely many Hermite equivalence classes of polynomials of degree $n \geq 2$ in $\mathbb{Z}[X]$ with given non-zero discriminant.

Hermite's original objective was finally achieved more than a century later.

- Birch and Merriman 1972: There are only finitely many $GL_2(\mathbb{Z})$-equivalence classes of polynomials of degree $n \geq 2$ in $\mathbb{Z}[X]$ with given non-zero discriminant. (ineffective)
- Independently: Győry 1973: There are only finitely many $\mathbb{Z}$-equivalence classes of monic polynomials of degree $n \geq 2$ in $\mathbb{Z}[X]$ with given non-zero discriminant. (effective)

$\mathbb{Z}$-equivalence

Two **monic** polynomials $f, g \in \mathbb{Z}[X]$ of degree n are said to be $\mathbb{Z}$-**equivalent**, if

$$g(X) = \varepsilon^n \cdot f(\varepsilon X + z)$$

for some $\varepsilon \in \{1, -1\}$ and $z \in \mathbb{Z}$.

If f and g are $\mathbb{Z}$-equivalent irreducible polynomials, β is a root of g, then $\varepsilon\beta + z$ is a root of f. So, f and g are $\mathbb{Z}$-equivalent, iff there exist α, β with $f(\alpha) = 0 = g(\beta)$ and $\alpha = \varepsilon\beta + z$.

If f and g are $\mathbb{Z}$-equivalent monic irreducible polynomials, and α and β are their corresponding roots, then

- f and g have the same discriminant,
- $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$; $\mathbb{Z}[\alpha] = \mathbb{Z}[\beta]$.

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

Two polynomials $f, g \in \mathbb{Z}[X]$ of degree n are said to be $GL_2(\mathbb{Z})$-**equivalent**, if

$$g(X) = \pm(cX+d)^n \cdot f\left(\frac{aX+b}{cX+d}\right), \text{ for some } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z}).$$

If f and g are $GL_2(\mathbb{Z})$-equivalent irreducible polynomials, $g(\beta) = 0$, then $f\left(\frac{a\beta+b}{c\beta+d}\right) = 0$. So, f and g are $GL_2(\mathbb{Z})$-equivalent, iff there exist α, β with $f(\alpha) = 0 = g(\beta)$ and $\alpha = \frac{a\beta+b}{c\beta+d}$.

If f, g are $GL_2(\mathbb{Z})$-equivalent monic irreducible polynomials, and α and β are their corresponding roots, then

- f and g have the same discriminant,
- $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$; $\mathbb{Z}[\alpha] = \mathbb{Z}[\beta]$.

Hermite equivalence

Let $f(X) = f_0X^n + \ldots + f_n = f_0(X-\alpha_1)\cdots(X-\alpha_n) \in \mathbb{Z}[X]$
Hermite associated the decomposable form below to $f(X)$

$$[f](\underline{X}) = f_0^{n-1}\prod_{i=1}^{n}(\alpha_i^{n-1}X_1 + \alpha_i^{n-2}X_2 + \ldots + X_n),$$

where $\underline{X} = (X_1, X_2, \ldots, X_n)^T$. Two polynomials $f, g \in \mathbb{Z}[X]$ are said to be **Hermite equivalent**, if there is a matrix $U \in GL_n(\mathbb{Z})$, such that

$$[g](\underline{X}) = [f](U\underline{X}).$$

If f and g are irreducible and there exist α, β roots of f and g for which

$$(\beta^{n-1}, \beta^{n-2}, \ldots, 1) = (\alpha^{n-1}, \alpha^{n-2}, \ldots, 1)\cdot U,$$

then f and g are Hermite equivalent. I.e. if f and g are monic and $\mathbb{Z}[\alpha] = \mathbb{Z}[\beta]$, then f and g are Hermite equivalent.

If f and g are Hermite equivalent irreducible polynomials, then

- f and g have the same discriminant,
- $\mathbb{Q}[X]/(f(X))$ is isomorphic to $\mathbb{Q}[X]/(g(X))$

Two monic polynomials $f, g \in \mathbb{Z}[X]$ are Hermite equivalent if and only if $\mathbb{Z}[\alpha] \simeq \mathbb{Z}[\beta]$. So, if $\alpha = p(\beta)$ and $\beta = q(\alpha)$ for some polynomials $p, q \in \mathbb{Z}[X]$, then $f, g \in \mathbb{Z}[X]$ are Hermite equivalent.

Comparing monic equivalences

In general:

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

Degree 2

Separable monic quadratic polynomials in $\mathbb{Z}[X]$ are Hermite equivalent if and only if they are $\mathbb{Z}$-equivalent.

Degree 3

Separable cubic polynomials in $\mathbb{Z}[X]$ are Hermite equivalent if and only if they are $GL_2(\mathbb{Z})$-equivalent. Moreover, every Hermite equivalence class of separable monic cubic polynomials in $\mathbb{Z}[X]$ is a union of at most 10 $\mathbb{Z}$-equivalence classes. (Bennett, 2001)

Degree 4

• Every Hermite equivalence class of separable quartic polynomials in $\mathbb{Z}[X]$ is a union of at most 10 $GL_2(\mathbb{Z})$-equivalence classes, and at most 7, if the discriminant is large enough. (Bhargava, 2022)

• Every Hermite equivalence class of separable monic quartic polynomials in $\mathbb{Z}[X]$ is a union of at most 2760 $\mathbb{Z}$-equivalence classes, and at most 182, if the discriminant is large enough. (Akhtari, Bhargava, 2022)

Degree ≥ 5

Every Hermite equivalence class of separable monic polynomials of degree $n \geq 5$ in $\mathbb{Z}[X]$ is a union of at most $2^{4(n+5)(n-2)}$ $\mathbb{Z}$-equivalence classes. (Evertse, 2011)

Cubic Hermite equivalence class with many $\mathbb{Z}$-classes

Let $f(X) = X^3 - X^2 - 2X + 1$, then $f(X)$ is Hermite equivalent to $g_i(X)$ $(i = 0, \ldots, 8)$, where

$$\begin{array}{l|l}
g_0(X) = X^3 - X^2 - 2X + 1 & \alpha \\
g_1(X) = X^3 - 3X^2 - 4X - 1 & \alpha^2 - 2\alpha \\
g_2(X) = X^3 - 4X^2 + 3X + 1 & \alpha^2 - \alpha \\
g_3(X) = X^3 - 5X^2 + 6X - 1 & \alpha^2 \\
g_4(X) = X^3 - 6X^2 + 5X - 1 & \alpha^2 + \alpha \\
g_5(X) = X^3 - 9X^2 + 20X + 1 & 2\alpha^2 - \alpha \\
g_6(X) = X^3 - 11X^2 - 102X - 181 & 4\alpha^2 - 9\alpha \\
g_7(X) = X^3 - 29X^2 + 138X - 181 & 5\alpha^2 + 4\alpha \\
g_8(X) = X^3 - 40X^2 + 391X + 181 & 9\alpha^2 - 5\alpha
\end{array}$$

These nine polynomials belong to nine distinct $\mathbb{Z}$-equivalence classes. (Ljunggren, 1942 and Baulin, 1960)

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

Let α and β be roots of the irreducible monic Hermite equivalent polynomials f and g, respectively, with $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$. Then there exists $p \in \mathbb{Z}[X]$, such that $\beta = p(\alpha)$.

Assume that the action of the Galois group of $f(X)$ on the set of the roots of $f(X)$ is doubly transitive, then f and g are $GL_2(\mathbb{Z})$ equivalent if and only if there exist $a, b, c, d \in \mathbb{Z}$ integers, such that $ad - bc = \pm 1$ and

$$\frac{a\alpha + b}{c\alpha + d} = p(\alpha).$$

Remark

If the Galois group of $g(X)$ is not 2-transitive, then theoretically it may happen that there is a solution of the above equation only if there are two different conjugates of α in the equation.

Big quartic Hermite equivalence class

Let $f(X) = X^4 - X^3 - 4X^2 + 2X + 1$ and α be a root of $f(X)$, then there are 10 $\mathbb{Z}$-inequivalent generators of $\mathbb{Z}[\alpha]$. (Gaál, 2019, p.300)

$$\begin{aligned}
\beta_1 &= \alpha^3 - 4\alpha \\
\beta_2 &= \alpha^2 - 2\alpha \\
\beta_3 &= 2\alpha^2 - \alpha \\
\beta_4 &= \alpha^3 - \alpha^2 \\
\beta_5 &= \alpha \\
\beta_6 &= \alpha^2 + \alpha \\
\beta_7 &= \alpha^3 - \alpha^2 - 3\alpha \\
\beta_8 &= \alpha^3 - \alpha^2 - 4\alpha \\
\beta_9 &= 4\alpha^3 - 4\alpha^2 - 15\alpha \\
\beta_{10} &= 5\alpha^3 - \alpha^2 - 21\alpha
\end{aligned}$$

The Galois group of f is S_4, so by solving the equations

$$\frac{a\beta_i + b}{c\beta_i + d} = \beta_j$$

for $a, b, c, d \in \mathbb{Z}$, with $ad - bc = \pm 1$, and for all pairs $i, j = 1, \dots, 10$, we conclude that the Hermite equivalence class of α splits into three $GL_2(\mathbb{Z})$ equivalence classes:

$$\{\beta_1, \beta_5, \beta_8\}, \{\beta_2, \beta_6, \beta_7, \beta_{10}\}, \{\beta_3, \beta_4, \beta_9\}.$$

Big quintic and sextic Hermite equivalence classes

Quintic Hermite equivalence class (Gaál, Győry, 1999)

Let

$$f(X) = X^5 - 5X^3 + X^2 + 3X - 1,$$

then the Galois group of f is S_5 and the Hermite equivalence class of $f(X)$ consists of 39 $\mathbb{Z}$-equivalence classes which form 10 $GL_2(\mathbb{Z})$-equivalence classes.

Sextic Hermite equivalence class (Bilu, Gaál, Győry, 2004)

Let

$$f(X) = X^6 - 5X^5 + 2X^4 + 18X^3 - 11X^2 - 19X + 1,$$

then the Galois group of f is S_6 and the Hermite equivalence class of $f(X)$ consists of 45 $\mathbb{Z}$-equivalence classes which form 11 $GL_2(\mathbb{Z})$-equivalence classes.

Infinite families

The defining polynomials f and g of the algebraic integers α and β are Hermite equivalent, if there exist $p, q \in \mathbb{Z}[X]$, such that $\beta = p(\alpha)$ and $\alpha = q(\beta)$.

This means that $f(X) \mid q(p(X)) - X$. I.e. $f(X) \cdot h(X) + X$ must be a polynomial of $p(X)$ for some $h \in \mathbb{Z}[X]$. If we can guarantee that the Galois group of $f(X)$ is doubly transitive, and we can find the polynomials above with $\deg p \leq \deg f - 2$, then α and β can not be in the same $GL_2(\mathbb{Z})$-equivalence class, since the equation

$$\frac{a\alpha + b}{c\alpha + d} = p(\alpha)$$

clearly has no solution with $ad - bc = \pm 1$ as the degree of α in $(c\alpha + d) \cdot p(\alpha) - (a\alpha + b)$ is less than the degree of f.

Infinite quartic examples

Let $p(X) = X^2 - r$ and $q(X) = X^2 - s$, where $r, s \in \mathbb{Z}$. Then let

$$f(X) = q(p(X)) - X = (X^2 - r)^2 - X - s$$

• There exist infinitely many $r, s \in \mathbb{Z}$, for which $f(X)$ is irreducible and has Galois group S_4. (Kappe, Warren, 1989). Lets consider such parameters r, s.

• Let α be a root of $f(X)$, then $\beta = p(\alpha) = \alpha^2 - r$ is a root of $g(X) = (X^2 - s)^2 - X - r$. The polynomials $f(X)$ and $g(X)$ are clearly Hermite equivalent, but not $GL_2(\mathbb{Z})$-equivalent, since $\deg p \leq \deg f - 2$. Indeed, if there would be a solution $(a, b, c, d) \in \mathbb{Z}^4$, with $ad - bc = \pm 1$, of

$$\frac{a\alpha + b}{c\alpha + d} = \alpha^2 - r,$$

then there would be a nonzero cubic polynomial in $\mathbb{Z}[X]$ with root α, which is not possible. (Bérczes, Evertse, Győry, 2013)

Infinite examples of arbitrary degree $n \geq 4$

Let us fix $p(X) = X - X^2$. Our aim is to find $f, h \in \mathbb{Z}[X]$, for which $f(X) \cdot h(X) + X$ is a polynomial of $X - X^2$.

$p(X) = X - X^2$ is not the simplest choice in the monic case, but it can easily be extended to the nonmonic case. With $p(X) = X^2$, it is easier to find monic examples, but it can not be extended to the nonmonic case.

We will assume that

$$f^{(n)}(X) = X^n - t \cdot h^{(n)}(1 - X),$$

where t is a prime. This form is useful, since f is automatically irreducible and $h^{(n)}(X) \cdot h^{(n)}(1 - X)$ is a polynomial of $X - X^2$. So we only have to find $h^{(n)}(X)$, such that

$$X^n \cdot h^{(n)}(X) = r^{(n)}(X - X^2) - X.$$

$$X^n \cdot h^{(n)}(X) = r^{(n)}(X - X^2) - X.$$

On the left hand side the constant term is 0, so $r^{(n)}(0)$ is also 0. Therefore we can write

$$X^n \cdot h^{(n)}(X) = (X - X^2) \cdot a^{(n)}(X - X^2) - X$$

$$X^{n-1} \cdot h^{(n)}(X) = (1 - X) \cdot a^{(n)}(X - X^2) - 1$$

We want to create an example for any n, so $a^{(n)}(X)$ has to be a partial sum of a power series $C(X)$, for which

$$(1 - X) \cdot C(X - X^2) - 1 = 0.$$

It is true for the well known generating function $C(X)$ of the Catalan numbers:

$$C(X) = \sum_{j=0}^{\infty} \frac{1}{j+1} \binom{2j}{j} \cdot X^j$$

Let $a^{(n)}(X)$ be the $n-2$-nd partial sum of the generating function $C(X)$ of the Catalan numbers, and let

$$h^{(n)}(X) = \frac{(1-X)\cdot a^{(n)}(X-X^2)-1}{X^{n-1}},$$

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

$$f^{(n)}(X) = X^n - t\cdot h^{(n)}(1-X) = X^n + t\cdot k^{(n)}(X).$$

Then

$$f^{(n)}(X)\cdot h^{(n)}(X) + X = q(X-X^2),$$

where

$$q(X) = X\cdot a^{(n)}(X) - t\cdot \frac{X\cdot a^{(n)}(X)^2 - a^{(n)}(X)+1}{X^{n-1}}$$

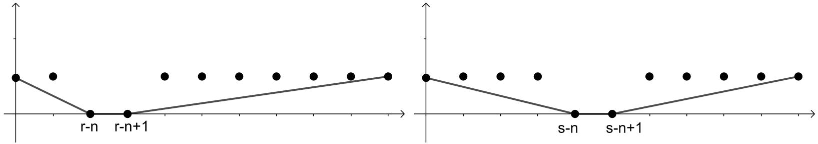
Fortunately, $C(X)$ satisfies $X\cdot C(X)^2 - C(X) + 1 = 0$, so $q(X)$ is also an integer polynomial and therefore $\mathbb{Z}[\alpha] = \mathbb{Z}[\alpha-\alpha^2]$.

Prooving irreducibility of $k^{(n)}(X)$

One can show that

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

Let $n < r < 6n/5$ and $6n/5 < s < 36n/25$ be primes. If $n > 24$, then there exist such primes (Nagura, 1952). Furthermore, it is easy to construct the $r-$ and $s-$Newton polygons of $h^{(n)}(-X)$:



These polygons consist of three primitive edges of length $r-n,\ 1,\ 2n-r-3$ and $s-n,\ 1,\ 2n-s-3$ respectively.

Dumas's irreducibility criterion (1906)

The degree of any nontrivial factor of $f(X) \in \mathbb{Z}[X]$ must be the sum of lengths of the primitive edges of the Newton polygons of $f(X)$ with respect to any prime.

• In our case an irreducible factor of $h^{(n)}(-X)$ must be the sum of some of the numbers $r-n$, 1, $2n-r-3$ and also the sum of some of the numbers $s-n$, 1, $2n-s-3$.

• This implies that if $h^{(n)}(-X) \in \mathbb{Q}[X]$ is reducible, then it has a rational root. But it can be shown that $h^{(n)}(-X)$ does not have a rational root, so it is irreducible for any $n \geq 4$ and so is $k^{(n)}(X)$.

Prooving $GL_2(\mathbb{Z})$-inequivalence of α and $p(\alpha) = \alpha - \alpha^2$

- By the Frobenius's or the Chebotarev's density theorem, there are infinitely many primes p, such that $k^{(n)}(X)$ has no root modulo p.
- Finally let t be a prime with $t \equiv -C_{n-1}^{-1} \pmod{p}$, where p is a prime for which $k^{(n+1)}(X)$ has no root modulo p.
- If the Galois group of $f^{(n)}(X)$ would not be 2-transitive, then there would be a root of $k^{(n+1)}(X)$ modulo p, which is a contradiction. Therefore, α and $\alpha - \alpha^2$ are not $GL_2(\mathbb{Z})$-equivalent.

$$\begin{aligned}
f^{(4)}(X) &= X^4 + t \cdot (2X^2 + 2X + 1) \\
f^{(5)}(X) &= X^5 + t \cdot (5X^3 + 5X^2 + 3X + 1) \\
f^{(6)}(X) &= X^6 + t \cdot (14X^4 + 14X^3 + 9X^2 + 4X + 1) \\
f^{(7)}(X) &= X^7 + t \cdot (42X^5 + 42X^4 + 28X^3 + 14X^2 + 5X + 1) \\
&\vdots
\end{aligned}$$

Nonmonic equivalences

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

Two polynomials $f, g \in \mathbb{Z}[X]$ of degree n are said to be $GL_2(\mathbb{Z})$-**equivalent**, if

$$g(X) = \pm(cX+d)^n \cdot f\left(\frac{aX+b}{cX+d}\right), \text{ for some } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z}).$$

A polynomial is called properly nonmonic, if it is not $GL_2(\mathbb{Z})$ equivalent to a monic polynomial.

Hermite equivalence

Two polynomials $f, g \in \mathbb{Z}[X]$ are said to be **Hermite equivalent**, if there is a matrix $U \in GL_n(\mathbb{Z})$, such that

$$[g](\underline{X}) = [f](U\underline{X}).$$

If f and g are irreducible and there exist α, β roots of f and g for which

$$(\beta^{n-1}, \beta^{n-2}, \ldots, 1) = (\alpha^{n-1}, \alpha^{n-2}, \ldots, 1) \cdot U,$$

then f and g are Hermite equivalent. I.e. if the $\mathbb{Z}$-modules

$$\mathbb{Z}\left\langle 1, \alpha, \ldots, \alpha^{n-1} \right\rangle \text{ and } \mathbb{Z}\left\langle 1, \beta, \ldots, \beta^{n-1} \right\rangle$$

are equal, then f and g are Hermite equivalent. (The converse is not true in general.)

If $\beta = p(\alpha)$ for some $p \in \mathbb{Z}[X]$, then it is not necessarily true, that

$$p(\alpha)^k \in \mathbb{Z}\left\langle 1, \alpha, \ldots, \alpha^{n-1} \right\rangle.$$

Lemma

If the leading coefficient of $f(X)$ is c and $p(X) = X \cdot s(cX)$ for some $s \in \mathbb{Z}[X]$, then $p(\alpha)^k \in \mathbb{Z}\langle 1, \alpha, \ldots, \alpha^{n-1}\rangle$ for each $k = 0, 1, \ldots, n-1$.

Infinite examples

Compared to the monic case, the only difference is that now we want to find $p, q \in \mathbb{Z}[X]$ polynomials of the form $p(X) = X \cdot s(f_0 X)$ and $q(X) = X \cdot r(g_0 X)$, where f_0 and g_0 are the leading coefficients of f and g and $r, s \in \mathbb{Z}[X]$.
For these p, q polynomials we have to find $h \in \mathbb{Z}[X]$, such that

$$f(X) \cdot h(X) = q(p(X)) - X.$$

By the previous lemma, in this case f and g are Hermite equivalent, but if we can choose $p(X)$ such that $\deg p \leq \deg(f) - 2$, then f and g are not $GL_2(\mathbb{Z})$-equivalent. In this way, we can create infinite examples for Hermite equivalence classes that split into at least two $GL_2(\mathbb{Z})$-equivalence classes.

Example of degree 4

Let $s \in \mathbb{Z}$ be an integer such that $s \equiv 1 \pmod{15}$ and let

$$f(X) = 2X^4 + 8X^2 + 2sX - 2s^2 + 9.$$

$$\left.\begin{array}{ll} f(X) \equiv 2(X+1)(X^3+2X^2+2X+2) & \pmod 3 \\ f(X) \equiv 2(X^2+X+2)(X+1)(X+3) & \pmod 5 \end{array}\right\} Gal(f) \simeq S_4.$$

Let α be a root of $f(X)$, and $\beta = \alpha + 2\alpha^2$. Then

$$1, \beta, \beta^2, \beta^3 \in \mathbb{Z}\left\langle 1, \alpha, \alpha^2, \alpha^3 \right\rangle.$$

The integer defining polynomial $g(X)$ of β also has a leading coefficient 2, and $q(X)$ is also of the form $X \cdot r(2X)$. Therefore

$$1, \alpha, \alpha^2, \alpha^3 \in \mathbb{Z}\left\langle 1, \beta, \beta^2, \beta^3 \right\rangle,$$

so α and β are Hermite equivalent, but not $GL_2(\mathbb{Z})$-equivalent, since $\deg p \leq \deg f - 2$.

Example of degree 5

Let $s \in \mathbb{Z}$ be an integer such that $s \equiv 71 \pmod{110}$ and let

$$2X^5 + (-800s^2 - 278s - 24)X + 800s^2 + 253s + 20.$$

$$\left.\begin{array}{l} f(X) \equiv 2X^5 + 3X + 3 \pmod{5} \\ f(X) \equiv 2X(X^2+9)(X+3)(X+8) \pmod{11} \end{array}\right\} Gal(f) \simeq S_5.$$

Let α be a root of $f(X)$, and $\beta = \alpha + 2\alpha^2$. Then

$$1, \beta, \beta^2, \beta^3, \beta^4 \in \mathbb{Z}\left\langle 1, \alpha, \alpha^2, \alpha^3, \alpha^4 \right\rangle.$$

The integer defining polynomial $g(X)$ of β also has a leading coefficient 2, and $q(X)$ is also of the form $X \cdot r(2X)$. Therefore

$$1, \alpha, \alpha^2, \alpha^3, \alpha^4 \in \mathbb{Z}\left\langle 1, \beta, \beta^2, \beta^3, \beta^4 \right\rangle,$$

so α and β are Hermite equivalent, but not $GL_2(\mathbb{Z})$-equivalent.

Infinite examples of arbitrary degree $n \geq 4$

We could generalize the infinite monic examples based on the generating function of the Catalan numbers to the (properly) nonmonic case. Let again $a^{(n)}(X)$ be the $n-2$-nd partial sum of the generating function $C(X)$ of the Catalan numbers, t and c be prime numbers, and let

$$h^{(n)}(X) = \frac{(1-X)\cdot a^{(n)}(X-X^2)-1}{X^{n-1}}, \qquad k^{(n)}(X) = -h^{(n)}(1-X),$$

$$f^{(n)}(X) = cX^n + t\cdot k^{(n)}(cX).$$

Then we have

$$f^{(n)}(X)\cdot h^{(n)}(cX) + X = q(X-cX^2),$$

where

$$q(X) = X\cdot a^{(n)}(cX) - c^{n-2}t\cdot \frac{cX\cdot a^{(n)}(cX)^2 - a^{(n)}(cX)+1}{(cX)^{n-1}}$$

$$f^{(n)}(X) = cX^n + t \cdot k^{(n)}(cX)$$

• If $c = 1$, then we get back the family of monic examples. But if c is a prime, then

$$f^{(n)}(X) \equiv t \pmod{c},$$

so if t is chosen to be a non $n-$th power remainder modulo c, then there is no integer solution to $F^{(n)}(X, Y) = Y^n \cdot f^{(n)}(X/Y) = \pm 1$, hence $f^{(n)}(X)$ is properly nonmonic and primitive.

• Let α be a root of $f^{(n)}(X)$, then α and $\alpha - c\alpha^2$ are Hermite equivalent but not $GL_2(\mathbb{Z})$-equivalent algebraic numbers.

•This family of examples is infinite for every degree $n \geq 4$ and for every leading coefficient c, since there are infinitely many possible choices for t, and the discriminant of $f^{(n)}(X) \to \infty$ as $t \to \infty$.

Conclusion

For $n \geq 4$, the notions of Hermite and $GL_2(\mathbb{Z})$-equivalence of polynomials of degree n are different in general. More precisely:

- For every integer $n \geq 4$, there exists an infinite collection of Hermite equivalence classes, each containing two monic polynomials f and g that are not $GL_2(\mathbb{Z})$-equivalent.
- For every integer $n \geq 4$, there exists an infinite collection of Hermite equivalence classes, each containing two primitive polynomials f and g that are properly nonmonic and not $GL_2(\mathbb{Z})$-equivalent.

References

- Bhargava M., Evertse J.-H., Győry K., R. L., Swaminathan. A.A. (2023), *Hermite equivalence of polynomials*, Acta Arith. **209**, 17–58.
- Bennett M.A. (2001), *On the representation of unity by binary cubic forms,* Trans. Amer. Math. Soc. **353**, 1507–1534.
- Bérczes A., Evertse J.-H. and Győry K. (2013), *Multiply monogenic orders*, Ann. Sc. Norm. Super. Pisa, Cl. Sci. (5) **12**, No. 2, 467–497.
- Bilu Y., Gaál I. and Győry K. (2004), *Index form equations in sextic fields: a hard computation*, Acta Arith. **115**, No. 1, 85–96.
- Birch B.J. and Merriman J.R. (1972), *Finiteness theorems for binary forms with given discriminant*, Proc. Lond. Math. Soc. (3) **24**, 385–394.

- Delaunay B. (1930), *Über die Darstellung der Zahlen durch die binären kubischen Formen von negativer Diskriminante*, Math. Z. **31**, 1–26.
- Evertse J.-H. (2011), *A survey on monogenic orders*, Publ. Math. **79**, No. 3–4, 411–422.
- Evertse J.-H. and Győry K. (2017), *Discriminant equations in Diophantine number theory*, Cambridge University Press, 2017.
- Gaál I. (2019), *Diophantine equations and power integral bases. Theory and algorithms* 2nd edition, BirkhÃ¤user, 2019.
- Gaál I. and Győry K. (1999), *Index form equations in quintic fields*, Acta Arith. **89**, No. 4, 379–396.
- Győry K. (1973), *Sur les polynômes à coefficients entiers et de discriminant donné*, Acta Arith. **23**, 419–426.

- Hermite C. (1851), *Sur l'introduction des variables continues dans la théorie des nombres*, J. Reine Angew. Math. **41**, 191–216.
- Hermite C. (1857), *Extrait d'une lettre de M. C. Hermite à M. Borchardt sur le nombre limité d'irrationalités auxquelles se réduisent les racines des équations à coefficients entiers complexes d'un degré et d'un discriminant donnés*, J. Reine Angew. Math. **53**, 182–192.
- Kappe L.-C. and Warren B. (1989), *An elementary test for the Galois group of a quartic polynomial*, Amer. Math. Monthly, **96**, 133–137.
- Lagrange J.L. (1773), *Recherches d'arithmétiques*, Nonv. Mém. Acad. Berlin, 265–312; Oeuvres **III**, 693–758.
- Nagell T. (1930), *Zur Theorie der kubischen Irrationalitäten*, Acta Math. **55**, 33–65.