Hermite equivalence of polynomials

Bhargava, M.; Evertse, J.H.; Győry, K.; Remete, L.; Swaminathan, A.

ACTA ARITHMETICA
209 (2023)

Hermite equivalence of polynomials

by

Manjul Bhargava (Princeton, NJ), Jan-Hendrik Evertse (Leiden),
Kálmán Győry (Debrecen), László Remete (Debrecen)
and Ashvin A. Swaminathan (Cambridge, MA)

To the memory of Professor Andrzej Schinzel (1937–2021)

1. Introduction

1.1. Summary. In this paper, we resurrect a long-forgotten notion of equivalence for univariate polynomials with integral coefficients introduced by Hermite in the 1850s. We show that the Hermite equivalence class of a polynomial has a very natural interpretation in terms of the invariant ring and invariant ideal associated with the polynomial. We apply this interpretation to shed light on the relationship between Hermite equivalence and more familiar notions of polynomial equivalence, such as $\mathrm{GL}_2(\mathbb{Z})$- and $\mathbb{Z}$-equivalence. Specifically, we prove that $\mathrm{GL}_2(\mathbb{Z})$-equivalent polynomials are Hermite equivalent and, for polynomials of degree 2 or 3, the converse is also true. On the other hand, for every $n \geq 4$, we give infinite collections of examples of polynomials $f, g \in \mathbb{Z}[X]$ of degree n that are Hermite equivalent but not $\mathrm{GL}_2(\mathbb{Z})$-equivalent.

Using his reduction theory for quadratic forms, Hermite proved (ineffectively) that polynomials in $\mathbb{Z}[X]$ with given discriminant lie in finitely many Hermite equivalence classes (this was in fact the reason why Hermite introduced his notion of equivalence). In this paper, we also compare Hermite's finiteness theorem with the most important results of this area, due to Birch and Merriman [6] (1972), Győry [17, 18] (1973, 1974) and Evertse and Győry [12, 13] (1991, 2017), which imply in a precise and effective

2020 *Mathematics Subject Classification*: Primary 11C08.
Key words and phrases: univariate polynomials, binary forms, discriminant, equivalence, monogeneity.
Received 13 November 2021; revised 10 September 2022.
Published online 28 February 2023.

DOI: 10.4064/aa211113-12-11

form that polynomials in $\mathbb{Z}[X]$ of given discriminant lie in finitely many $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes, and hence in finitely many Hermite equivalence classes.

We point out that these results of Birch and Merriman, Győry, and Evertse and Győry are much more precise than Hermite's theorem and require deeper tools to prove. In particular, we correct a faulty reference occurring in Narkiewicz' excellent book [38] (2019), where $\mathrm{GL}_2(\mathbb{Z})$-equivalence and Hermite equivalence of polynomials were mixed up.

1.2. Background. In the mid-nineteenth century, Hermite [29, 30] introduced a new notion of equivalence—which we call *Hermite equivalence*—for univariate polynomials with integral coefficients. His motivation was to prove a finiteness theorem for equivalence classes of polynomials having given degree and discriminant. Such finiteness theorems had already been proven for $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of quadratic polynomials by Lagrange [33], whose work was later improved by Gauss [16]. Hermite [28] proved the same finiteness statement for $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of cubic polynomials. Although he was unable to extend this result to polynomials of degree greater than 3, Hermite realized that, if one replaces "$\mathrm{GL}_2(\mathbb{Z})$-equivalence" with "Hermite equivalence", the desired finiteness statement would follow from the reduction theory for quadratic forms that he had previously developed in [27].

Using his reduction theory for quadratic forms, Hermite proved (ineffectively) that polynomials in $\mathbb{Z}[X]$ with given discriminant lie in finitely many Hermite equivalence classes. Hermite's original objective—proving that there are finitely many $\mathrm{GL}_2(\mathbb{Z})$-classes of polynomials of given degree and discriminant—was finally achieved more than a century later by Birch and Merriman [6], and independently, for monic polynomials and in a more precise and effective form, by Győry [17]. The result of Birch and Merriman was subsequently made effective by Evertse and Győry [12]. Surprisingly, Hermite's result on finiteness for Hermite equivalence classes was not mentioned in any of these works, or in the related papers of Delone [7], Nagell [35], Győry [18, 19, 20, 21, 22, 23, 24], and Evertse and Győry [12]. In fact, Hermite equivalence of polynomials does not appear to have been studied in the literature in the nearly two centuries since Hermite first introduced the notion.

The purpose of this paper is twofold: (1) to provide a thorough treatment of the notion of Hermite equivalence, and (2) to compare Hermite equivalence with two more familiar notions of equivalence for univariate integral polynomials, namely, $\mathrm{GL}_2(\mathbb{Z})$-equivalence and $\mathbb{Z}$-equivalence. We present theoretical arguments as well as examples to shed light on the relationships between these three different types of polynomial equivalence.

1.3. Notions of equivalence. We now define the three notions of equivalence for polynomials in $\mathbb{Z}[X]$ studied in this paper, namely, Hermite equivalence (§1.3.1), $\mathrm{GL}_2(\mathbb{Z})$-equivalence (§1.3.2), and $\mathbb{Z}$-equivalence (§1.3.3).

1.3.1. *Hermite equivalence.* To a polynomial

$$f(X) = f_0X^n + f_1X^{n-1} + \cdots + f_n = f_0(X-\alpha_1)\cdots(X-\alpha_n) \in \mathbb{Z}[X], \tag{1.1}$$

where $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$, Hermite associated the following decomposable form $[f]$ in n variables:

$$[f](\underline{X}) = f_0^{n-1} \prod_{i=1}^{n} (\alpha_i^{n-1}X_1 + \alpha_i^{n-2}X_2 + \cdots + X_n), \tag{1.2}$$

where $\underline{X}$ denotes the column vector $(X_1, \ldots, X_n)^T$. As we shall show, the form $[f]$ has integer coefficients; it is primitive (i.e., its coefficients have greatest common divisor 1) if and only if f is primitive; and its discriminant is equal to that of the polynomial f.

Using the above construction of the form $[f]$, Hermite introduced the following notion of equivalence, which we call *Hermite equivalence*, for polynomials $f, g \in \mathbb{Z}[X]$ of degree n:

Definition 1.1. Let $f, g \in \mathbb{Z}[X]$ be polynomials of degree n. Then f and g are said to be *Hermite equivalent* if the decomposable forms $[f], [g]$ are $\mathrm{GL}_n(\mathbb{Z})$-equivalent, i.e., if there is a matrix $U \in \mathrm{GL}_n(\mathbb{Z})$ such that

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

Since the action of $\mathrm{GL}_n(\mathbb{Z})$ on homogeneous forms of degree n in n variables is discriminant-preserving, it follows that the discriminants of Hermite equivalent polynomials are equal.

1.3.2. $\mathrm{GL}_2(\mathbb{Z})$*-equivalence.* As far as we know, Hermite did not compare his equivalence with the well-known notion of $\mathrm{GL}_2(\mathbb{Z})$-equivalence. Recall that two binary n-ic forms (i.e., binary forms of degree n) $F, G \in \mathbb{Z}[X, Y]$ are called $\mathrm{GL}_2(\mathbb{Z})$-*equivalent* if $G(X, Y) = \pm F(aX + bY, cX + dY)$ for some $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$. In this case F and G have the same discriminant.

To a binary n-ic form F, we may associate the univariate polynomial $f(X) = F(X, 1)$. The discriminants of F and of f (viewed as a degree n polynomial) coincide. Conversely, if $f \in \mathbb{Z}[X]$ is a polynomial of degree at most n, we can associate to f (viewed as a polynomial of degree n) its homogenization, namely, the binary n-ic form $F(X, Y) = Y^n f(X/Y)$. We then define two polynomials $f, g \in \mathbb{Z}[X]$ of degree n to be $\mathrm{GL}_2(\mathbb{Z})$-equivalent if their homogenizations are $\mathrm{GL}_2(\mathbb{Z})$-equivalent. This means precisely that $g(X) = \pm(cX + d)^n f\left(\frac{aX+b}{cX+d}\right)$ for some $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$.

We shall show in what follows that $\mathrm{GL}_2(\mathbb{Z})$-equivalence implies Hermite equivalence, and further that Hermite equivalence is in general weaker than

$\mathrm{GL}_2(\mathbb{Z})$-equivalence. For the sake of convenience, we shall work mostly with $\mathrm{GL}_2(\mathbb{Z})$-equivalence of univariate polynomials rather than of binary forms.

1.3.3. *$\mathbb{Z}$-equivalence.* Two monic polynomials $f, g \in \mathbb{Z}[X]$ of degree n are said to be *$\mathbb{Z}$-equivalent* if $g(X) = \varepsilon^n f(\varepsilon X + a)$ for some $\varepsilon \in \{\pm 1\}$ and $a \in \mathbb{Z}$.

Clearly, $\mathbb{Z}$-equivalent polynomials have the same discriminant, and $\mathbb{Z}$-equivalence implies $\mathrm{GL}_2(\mathbb{Z})$-equivalence (and hence also Hermite equivalence, as we shall show). Note that $\mathbb{Z}$-equivalence is in general much stronger than $\mathrm{GL}_2(\mathbb{Z})$-equivalence.

1.4. Main theorems. Given a polynomial $f \in \mathbb{Z}[X]$ of degree $n \geq 2$, define the *invariant order* of f to be the ring R_f of global sections of the subscheme of $\mathbb{P}^1_{\mathbb{Z}}$ cut out by the homogenization of f (i.e., the unique binary n-ic form F such that $F(x, 1) = f(x)$). Define the *invariant ideal* of f to be the R_f-module I_f of global sections of the pullback of the line bundle $\mathcal{O}(1)$ from $\mathbb{P}^1_{\mathbb{Z}}$ to $\operatorname{Spec} R_f$.

Explicitly, if $f(X) = f_0 X^n + f_1 X^{n-1} + \cdots + f_n \in \mathbb{Z}[X]$ is a polynomial of degree n with leading coefficient $f_0 \neq 0$, and α is the residue class of X in $K_f := \mathbb{Q}[X]/(f)$, then $R_f \subset K_f$ is isomorphic to the ring with $\mathbb{Z}$-basis

$$1, \quad f_0\alpha, \quad f_0\alpha^2 + f_1\alpha, \ \ldots, \ f_0\alpha^{n-1} + f_1\alpha^{n-2} + \cdots + f_{n-2}\alpha$$

and I_f is isomorphic to the fractional R_f-ideal generated by 1 and α. (See Birch–Merriman [6], Nakagawa [37], and Wood [44].)

Then we have the following theoretical results:

THEOREM 1.2. *Let $n \geq 2$ be an integer.*

(i) (Corollary 3.11) *Two polynomials $f, g \in \mathbb{Z}[X]$ of nonzero discriminant and degree n are Hermite equivalent if and only if their invariant orders R_f and R_g are isomorphic, and under such an isomorphism, the $(n-1)$st powers of their invariant ideals I_f and I_g belong to the same ideal class.*

(ii) (Corollary 3.16) *Two monic polynomials $f, g \in \mathbb{Z}[X]$ of nonzero discriminant and degree n are Hermite equivalent if and only if their invariant orders R_f and R_g are isomorphic.*

(iii) (Corollary 2.4) *If two polynomials $f, g \in \mathbb{Z}[X]$ of degree n are $\mathrm{GL}_2(\mathbb{Z})$-equivalent, then they are Hermite equivalent. In particular, if f and g are monic and $\mathbb{Z}$-equivalent, then they are Hermite equivalent.*

An important consequence of Theorem 1.2(iii) is that the effective finiteness theorems due to Evertse and Győry [12, 13] and Győry [17, 18] for $\mathrm{GL}_2(\mathbb{Z})$-equivalence or $\mathbb{Z}$-equivalence classes of polynomials of given discriminant (see Theorems C–F in §4 below) apply just as well to Hermite equivalence classes. We also have effective bounds, due to Lagrange [33] (for $n = 2$), Levi–Delone–Faddeev [8] and Bennett [1] (for $n = 3$), Akhtari and

Bhargava [4] (for $n = 4$), and Evertse and Győry [13] and Evertse [11] (for general $n \geq 5$), for the number of ways in which a ring arises as the invariant order of a $\mathrm{GL}_2(\mathbb{Z})$- or $\mathbb{Z}$-equivalence class of polynomials. We thus obtain the following finiteness results. We use the notation $\log^* x := \max(1, \log x)$ for $x > 0$.

THEOREM 1.3. *Let $n \geq 2$ be an integer.*

(i) (Theorems C and F) *The number of Hermite equivalence classes of polynomials in $\mathbb{Z}[X]$ of given discriminant $D \neq 0$ is effectively bounded in a way that depends only on D. More specifically, every Hermite equivalence class of polynomials in $\mathbb{Z}[X]$ with degree n and discriminant $D \neq 0$ has a representative with coefficients not exceeding*

$$\exp\{(4^2 n^3)^{25n^2} |D|^{5n-3}\}$$

in absolute value, and $n \leq 3 + 2\log|D|/\log 3$.

(ii) (Theorems E and F) *Every Hermite equivalence class of monic polynomials in $\mathbb{Z}[X]$ with degree n and discriminant $D \neq 0$ has a representative with coefficients not exceeding*

$$\exp\{n^{20} 8^{n^2+19} (|D|(\log^* |D|)^n)^{n-1}\}$$

in absolute value, and $n \leq 2 + 2\log|D|/\log 3$.

(iii) (Theorem 4.1(i, iii, v, vii)) *The number of $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of separable polynomials in $\mathbb{Z}[X]$ of degree n in a Hermite equivalence class is 1 if $n = 2$ or 3, at most 10 if $n = 4$, and at most 2^{5n^2} if $n \geq 5$.*

(iv) (Theorem 4.1(ii, iv, vi, viii)) *The number of $\mathbb{Z}$-equivalence classes of monic separable polynomials in $\mathbb{Z}[X]$ of degree n in a Hermite equivalence class is 1 if $n = 2$, at most 10 if $n = 3$, at most 2760 if $n = 4$, and at most 2^{5n^2} if $n \geq 5$.*

Finally, by constructing explicit examples, we prove the following existence theorems concerning the relationship between the aforementioned notions of polynomial equivalence:

THEOREM 1.4.

(i) (Theorem 3.20) *There exist quartic polynomials $f, g \in \mathbb{Z}[X]$ of squarefree discriminant that have isomorphic invariant orders R_f and R_g but f and g are not Hermite equivalent.*

(ii) (§§5.1–5.3) *For each $n \geq 4$, there exist infinitely many Hermite equivalence classes of properly nonmonic ([1]) irreducible polynomials, of monic irreducible polynomials, and of monic reducible polynomials having degree n, that split into more than one $\mathrm{GL}_2(\mathbb{Z})$-equivalence class.*

([1]) That is, not $\mathrm{GL}_2(\mathbb{Z})$-equivalent to a monic polynomial.

Part (i) of Theorem 1.4 shows that the condition that the $(n-1)$st powers of I_f and I_g belong to the same ideal class cannot in general be dropped from Theorem 1.2(i). Part (ii) shows that in all degrees $n \geq 4$, the notion of Hermite equivalence is strictly weaker than $\mathrm{GL}_2(\mathbb{Z})$-equivalence.

Remark 1.5. In the recent book of Narkiewicz [38], on pp. 36–37, there is a misleading reference, which suggests that Hermite proved that the polynomials with given discriminant lie in finitely many $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes, when in fact he had only proven this for Hermite equivalence classes. While Hermite could prove his finiteness result using his reduction theory of quadratic forms, the corresponding result for $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes requires much deeper tools not available to Hermite, namely, finiteness results for unit equations. One of our motivations in writing this article was to correct this reference in Narkiewicz's book [38] and to illustrate by concrete examples that Hermite equivalence is in general weaker than the $\mathrm{GL}_2(\mathbb{Z})$-equivalence and $\mathbb{Z}$-equivalence of polynomials.

1.5. Organization. The rest of this paper is organized as follows. In §2, we prove a number of fundamental properties about Hermite equivalence of polynomials. In §3, we give an interpretation of Hermite equivalence in terms of invariant orders and ideals, thus proving Theorem 1.2. We also use this intepretation to prove Theorem 1.4(i). In §4, we survey the literature on finiteness theorems for polynomial equivalence and observe that these theorems also apply to Hermite equivalence, thus proving Theorem 1.3. We finish in §5 by constructing the infinite collections of examples described in Theorem 1.4(ii).

2. Elementary considerations. In this section, we use elementary arguments to establish several important properties related to Hermite equivalence of polynomials. In §3, we demonstrate that these properties are straightforward consequences of our characterization of Hermite equivalence in terms of invariant orders and ideals.

2.1. Content and primitivity. Recall that the *content* of a polynomial with integer coefficients is the positive greatest common divisor of its coefficients. A polynomial with integer coefficients is called *primitive* if its content is equal to 1.

Theorem 2.1. *Let $f \in \mathbb{Z}[X]$ be a polynomial of degree n with content c. Then $[f]$ has integer coefficients, and its content is c^{n-1}.*

Proof. Let K denote the splitting field of f. Denote by $(\alpha_1, \ldots, \alpha_s)$ the fractional ideal of $\mathcal{O}_K$ generated by $\alpha_1, \ldots, \alpha_s \in K$. Given a polynomial F with coefficients in K, denote by (F) the fractional ideal with respect to $\mathcal{O}_K$ generated by the coefficients of F. Then by Gauss' Lemma

for Dedekind domains, we have $(FG) = (F) \cdot (G)$ for any two polynomials $F, G \in K[X_1, \ldots, X_r]$.

Now write $f = f_0(X - \alpha_1) \cdots (X - \alpha_n)$ with $\alpha_1, \ldots, \alpha_n \in K$ and $f_0 \in \mathbb{Z}$. Then Gauss' Lemma implies that $(f) = (f_0)(1, \alpha_1) \cdots (1, \alpha_n)$ and $([f]) = (f_0)^{n-1}(1, \alpha_1)^{n-1} \cdots (1, \alpha_n)^{n-1} = (f)^{n-1}$. ∎

REMARK 2.2. Theorem 2.1 may also be proven quite explicitly, without relying on Gauss' Lemma. Indeed, if we write $\phi_{\underline{X}}(Y) = X_1 Y^{n-1} + X_2 Y^{n-2} + \cdots + X_n$, then one verifies that $[f]$ is simply the resultant of $\phi_{\underline{X}}(Y)$ and $f(Y)$; i.e.,

$$[f](\underline{X}) = \mathrm{Res}(\phi_{\underline{X}}, f) = \begin{vmatrix} X_1 & \ldots & X_n & & & \\ & \ddots & & \ddots & & \\ & & \ddots & & \ddots & \\ & & & X_1 & \ldots & X_n \\ f_0 & \ldots & f_{n-1} & f_n & & \\ & \ddots & & & \ddots & \\ & & f_0 & \ldots & f_{n-1} & f_n \end{vmatrix},$$

where the first n rows consist of $X_1, \ldots, X_n$ and the last $n-1$ rows of $f_0, \ldots, f_{n-1}, f_n$. It follows that $[f]$ has integral coefficients. First assume that f is primitive. If $[f]$ is not primitive, then there is a prime p such that $\mathrm{Res}(\phi_{\underline{X}}, f) \equiv 0 \pmod{p}$. But then $\phi_{\underline{X}}$ and f, viewed as polynomials over $\mathbb{F}_p[X_1, \ldots, X_n]$, share a common factor. This happens if and only if $f \equiv 0 \pmod{p}$, which is impossible because f is primitive. Hence $[f]$ is primitive as well. Next, assume that f has content c. Write $f' = f/c$. Then f' is primitive and $[f] = c^{n-1}[f']$, which implies that $[f]$ has content c^{n-1}.

COROLLARY 2.3. *Let $f, g \in \mathbb{Z}[X]$ be nonzero polynomials with contents c_f, c_g respectively, and let $f' := c_f^{-1} f$, $g' := c_g^{-1} g$ be the corresponding primitive polynomials. Then f and g are Hermite equivalent if and only if f' and g' are Hermite equivalent and $c_g = c_f$.*

Proof. First assume that f and g are Hermite equivalent. So $[g](X) = \pm[f](UX)$ for some matrix $U \in \mathrm{GL}_n(\mathbb{Z})$. By Theorem 2.1, $[f]$ has content c_f^{n-1}, and $[f](UX)$ has the same content as $[f]$. Further, $[g]$ has content c_g^{n-1}. So $c_g = c_f$.

Since $[f] = c_f^{n-1}[f']$ and $[g] = c_g^{n-1}[g']$ it follows that $[g'](X) = \pm[f'](UX)$. Hence f' and g' are Hermite equivalent. The proof of the "if" part is left to the reader. ∎

2.2. Hermite equivalence and $\mathrm{GL}_2(\mathbb{Z})$-equivalence. We now give an elementary and explicit proof that $\mathrm{GL}_2(\mathbb{Z})$-equivalence implies Hermite equivalence:

THEOREM 2.4. *Let $f, g \in \mathbb{Z}[X]$ be $\mathrm{GL}_2(\mathbb{Z})$-equivalent polynomials. Then f and g are Hermite equivalent. In particular, if f and g are monic and $\mathbb{Z}$-equivalent, then they are Hermite equivalent.*

Proof. Write $f(X) = \prod_{i=1}^{n}(\alpha_{i,1}X - \alpha_{i,2})$. Then

$$[f](\underline{X}) = \prod_{i=1}^{n}(\alpha_{i,2}^{n-1}X_1 + \alpha_{i,2}^{n-2}\alpha_{i,1}X_2 + \cdots + \alpha_{i,1}^{n-1}X_n) = \prod_{i=1}^{n}\langle \underline{a}_i, \underline{X}\rangle,$$

where $\underline{a}_i = (\alpha_{i,2}^{n-1}, \ldots, \alpha_{i,1}^{n-1})^T$ and $\langle \cdot, \cdot \rangle$ denotes the standard inner product. For $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ write

$$\gamma f(X) = (cX + d)^n f\left(\frac{aX + b}{cX + d}\right) = \prod_{i=1}^{n}(\beta_{i,1}X - \beta_{i,2}),$$

where $\beta_{i,1} = \alpha_{i,1}a - \alpha_{i,2}c$ and $\beta_{i,2} = -(-\alpha_{i,1}b + \alpha_{i,2}d)$. Then

$$\begin{aligned}[\gamma f](\underline{X}) &= \prod_{i=1}^{n}(\beta_{i,2}^{n-1}X_1 + \beta_{i,2}^{n-2}\beta_{i,1}X_2 + \cdots + \beta_{i,1}^{n-1}X_n) \\ &= \prod_{i=1}^{n}\langle t(\gamma)\underline{a}_i, \underline{X}\rangle = \prod_{i=1}^{n}\langle \underline{a}_i, t(\gamma)^T\underline{X}\rangle = [f](t(\gamma)^T\underline{X}),\end{aligned}$$

where $t(\gamma)$ is an $n \times n$ matrix whose entries are polynomials in $\mathbb{Z}[a, b, c, d]$. One easily verifies that for any 2×2 matrices γ_1, γ_2 one has $t(\gamma_1\gamma_2) = t(\gamma_2)t(\gamma_1)$, and that $t(I_2) = I_n$, where I_m is the $m \times m$ identity matrix. In particular, if $g = \pm\gamma f$ with $\gamma \in \mathrm{GL}_2(\mathbb{Z})$, then $[g](\underline{X}) = \pm[f](t(\gamma)^T\underline{X})$, $t(\gamma)^T \in \mathrm{GL}_n(\mathbb{Z})$, so f and g are Hermite equivalent. ∎

As mentioned in Remark 3.13, the converse of Theorem 2.4 holds when $n = 2$. Combining the result of Levi–Delone–Faddeev stated in Remark 3.14 with Corollary 3.15 (to follow), we deduce that the converse also holds when $n = 3$. See §5.5 for examples of polynomials in every degree $n \geq 4$ for which the converse fails.

2.3. Discriminant equalities. The *discriminant* of a decomposable form of degree n in n variables

$$F(\underline{X}) = \prod_{i=1}^{n}(\gamma_{i,1}X_1 + \cdots + \gamma_{i,n}X_n)$$

is defined as

$$D(F) := \left(\det\left(\gamma_{i,j}\right)_{i,j=1,\ldots,n}\right)^2.$$

Note that if F, G are two decomposable forms of degree n in n variables with $G(\underline{X}) = \pm F(U\underline{X})$ for some $U \in \mathrm{GL}_n(\mathbb{Z})$, then $D(G) = D(F)$.

THEOREM 2.5. *Let $f \in \mathbb{Z}[X]$ be a polynomial of degree n. Then $D([f])$ $= D(f)$.*

Proof. The discriminant of f is given by

$$D(f) := f_0^{2n-2} \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2,$$

and an easy application of Vandermonde's identity gives the desired equality $D(f) = D([f])$. ∎

Since the action of $\mathrm{GL}_n(\mathbb{Z})$ on decomposable forms in n variables is discriminant-preserving, we obtain the following immediate consequence of Theorem 2.5:

COROLLARY 2.6. *Hermite equivalent polynomials have the same discriminant.*

3. Interpretation of Hermite equivalence. The purpose of this section is to give an interpretation of Hermite equivalence of integer polynomials f and g in terms of the invariant orders and ideals associated to f and g, which we review in §3.1. We use this interpretation to prove Theorem 1.2.

3.1. Rings and ideals associated to polynomials in $\mathbb{Z}[X]$. Let $f \in \mathbb{Z}[X]$ be a polynomial of degree n as in (1.1) with $D(f) \neq 0$ and $f_0 \neq 0$. Consider the étale $\mathbb{Q}$-algebra $K_f := \mathbb{Q}[X]/(f(X))$, and let α be the image of X in K_f. For $k \in \{0, \dots, n-1\}$, we define the free $\mathbb{Z}$-module $I_f(k) \subset K_f$ with basis

(3.1)
$$\langle 1, \alpha, \dots, \alpha^k, \zeta_{k+1}, \dots, \zeta_{n-1} \rangle, \quad \text{where} \quad \zeta_i = f_0\alpha^i + f_1\alpha^{i-1} + \cdots + f_{i-1}\alpha,$$

and we write $R_f := I_f(0)$ and $I_f := I_f(1)$. Before we describe the basic properties of the $\mathbb{Z}$-modules R_f and $I_f(k)$, we require the following definition of the norm of a fractional ideal of an order in an étale algebra:

DEFINITION 3.1. For a given order $\mathcal{O}$ in an étale $\mathbb{Q}$-algebra K and fractional ideal $I \subset K$ of $\mathcal{O}$, we define the norm $N_{\mathcal{O}}(I)$ of I with respect to $\mathcal{O}$ to be the absolute value of the determinant of the $\mathbb{Z}$-linear transformation taking a $\mathbb{Z}$-basis of $\mathcal{O}$ to a $\mathbb{Z}$-basis of I.

REMARK 3.2. Note in particular that if $\alpha \in K$, then the norm of the fractional ideal $\alpha\mathcal{O}$ is just the absolute value of the determinant of the $\mathbb{Q}$-linear map $x \mapsto \alpha x$, and thus $N_{\mathcal{O}}(\alpha\mathcal{O}) = |N_{\mathbb{Q}}^K(\alpha)|$.

The following theorem summarizes the basic properties of the $\mathbb{Z}$-modules R_f and $I_f(k)$:

THEOREM 3.3.

(i) *R_f is a ring of rank n over $\mathbb{Z}$ and thus an order in K_f.*
(ii) *$D(f) = D(R_f)$.*

(iii) *For each $k \in \{0, \dots, n-1\}$, the $\mathbb{Z}$-module $I_f(k)$ is an R_f-submodule of K_f and hence a fractional ideal of R_f. Moreover, $I_f(k)$ is invertible if and only if f is primitive.*

(iv) *$I_f(k) = I_f^k$ and $N_{R_f}(I_f(k)) = |f_0|^{-k}$.*

(v) *$I_f(n-2)$ is an explicit representative of the ideal class of the "inverse different" or the "dualizing module" of R_f.*

(vi) *If $f' \in \mathbb{Z}[X]$ is primitive of degree n such that $f' \mid f$, then the ring of R_f-module endomorphisms of $I_f(n-1)$ is isomorphic to $R_{f'}$ (i.e., $R_{f'} = \{\xi \in K_f : \xi I_f(n-1) \subseteq I_f(n-1)\}$).*

(vii) *R_f is isomorphic to the ring of global functions on the subscheme of $\mathbb{P}^1_{\mathbb{Z}}$ cut out by the homogenization of f, and $I_f(k)$, as an R_f-module, consists of the sections of the pullback of $\mathcal{O}(k)$ from $\mathbb{P}^1_{\mathbb{Z}}$. Hence if g is the translate of f by some $\gamma \in \mathrm{GL}_2(\mathbb{Z})$, then the action of γ on $\mathbb{P}^1_{\mathbb{Z}}$ induces an isomorphism between R_f and R_g, and this isomorphism identifies the ideal classes I_f and I_g. Explicitly, if $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, then $I_g(k) = (-b\alpha + a)^{-k} I_f(k)$.*

Proof. Points (i) and (ii) are results of Birch and Merriman [6, proof of Lemma 3]) and Nakagawa [37, Proposition 1.1]. Points (iii) and (vii) are results of Wood [44, §2.1 and Appendix A] (see also Simon [40, §3]), and (iv) is an elementary calculation. Point (v) is a result of Simon [41, Proposition 14], and (vi) follows upon observing that $I_f(n-1) = I_{f'}(n-1)$ is an invertible fractional ideal for $R_{f'}$ by (iii). ∎

In what follows, we call the ring R_f the *invariant order* of f, and we call the fractional ideal I_f the *invariant* (*fractional*) *ideal* of f.

Remark 3.4. Although this paper is largely concerned with polynomials of nonzero discriminant, the construction of R_f and its associated fractional ideals $I_f(k)$ can also be carried out canonically for polynomials having discriminant zero, and even for the zero polynomial; see Wood [44, §§2.3–2.4].

Remark 3.5. Note that when $f_0 = 1$, the ring R_f is simply the monogenic order $\mathbb{Z}[\alpha]$ generated by α, and the ideals $I_f(k)$ are all equal to the unit ideal (in particular, they are all principal).

3.2. Interpretation of $[f]$ as the norm form of $I_f(n-1)$. Let K be an étale $\mathbb{Q}$-algebra of degree n. Then we can write $K = \prod_{j=1}^m K_j$, where $K_1, \dots, K_m$ are number fields. Letting $\pi_j : K \to K_j$ be the projection onto the jth factor, and $\sigma_{j,k}$ ($k = 1, \dots, n_j := [K_j : \mathbb{Q}]$) the embeddings of K_j in $\overline{\mathbb{Q}}$, the trace and norm over $\mathbb{Q}$ of $\alpha \in K$ are equal to

$$\mathrm{Tr}_{\mathbb{Q}}^K(\alpha) = \sum_{j=1}^m \mathrm{Tr}_{\mathbb{Q}}^{K_j}(\pi_j(\alpha)) = \sum_{j=1}^m \sum_{k=1}^{n_j} \sigma_{j,k}\pi_j(\alpha),$$

and

$$N_{\mathbb{Q}}^{K}(\alpha) = \prod_{j=1}^{m} N_{\mathbb{Q}}^{K_j}(\pi_j(\alpha)) = \prod_{j=1}^{m}\prod_{k=1}^{n_j} \sigma_{j,k}\pi_j(\alpha).$$

The norm can be naturally extended to polynomials in $K[X_1,\dots,X_n]$. Thus, the norm over $\mathbb{Q}$ of such a polynomial has its coefficients in $\mathbb{Q}$.

Let $\mathcal{O}$ be an order in K, and let $I \subset K$ be a (not necessarily invertible) fractional ideal of $\mathcal{O}$ having $\mathbb{Z}$-rank n. Then the *norm form* of I with respect to $\mathcal{O}$ and the $\mathbb{Z}$-basis $\langle\alpha_1,\dots,\alpha_n\rangle$ of I is the decomposable integral form of degree n in n variables defined by

$$N_{I,\mathcal{O}}(X_1,\dots,X_n) := \frac{N_{\mathbb{Q}}^{K}(\alpha_1X_1+\cdots+\alpha_nX_n)}{N_{\mathcal{O}}(I)}.$$

This depends on the choice of a $\mathbb{Z}$-basis for I, but the $\mathrm{GL}_n(\mathbb{Z})$-equivalence class of $N_{I,\mathcal{O}}$ is clearly independent of the choice of a basis.

The following lemma determines the discriminant of the norm form of a fractional ideal:

LEMMA 3.6. *With notation as above, we have* $D(N_{I,\mathcal{O}}) = D(\mathcal{O})$.

Proof. Choose a $\mathbb{Z}$-basis $\langle\omega_1,\dots,\omega_n\rangle$ of $\mathcal{O}$, and let $\gamma \in \mathrm{GL}_n(\mathbb{Q})$ be the $\mathbb{Q}$-linear transformation taking $\omega_1,\dots,\omega_n$ to $\alpha_1,\dots,\alpha_n$. From the definition of discriminant of a decomposable form and the expression for the trace mentioned above, it follows that the discriminant of $N_{\mathbb{Q}}^{K}(\alpha_1X_1+\cdots+\alpha_nX_n)$ is precisely the discriminant $D(\alpha_1,\dots,\alpha_n)$ of the basis $\langle\alpha_1,\dots,\alpha_n\rangle$. Thus,

$$\begin{aligned} D(N_{I,\mathcal{O}}) &= N_{\mathcal{O}}(I)^{-2}D(\alpha_1,\dots,\alpha_n) = |\det\gamma|^{-2}D(\alpha_1,\dots,\alpha_n)\\ &= D(\omega_1,\dots,\omega_n) = D(\mathcal{O}). \ \blacksquare \end{aligned}$$

The significance of the norm form of an ideal class is revealed in the following theorem.

THEOREM 3.7. *For each* $i \in \{1,2\}$, *let* I_i *be a fractional ideal of* $\mathbb{Z}$*-rank* n *for an order* $\mathcal{O}_i$ *in an étale* $\mathbb{Q}$*-algebra* K_i *of degree* n. *If the norm forms* $N_{I_1,\mathcal{O}_1}(X_1,\dots,X_n)$ *and* $N_{I_2,\mathcal{O}_2}(X_1,\dots,X_n)$ *are* $\mathrm{GL}_n(\mathbb{Z})$*-equivalent, then* K_1 *and* K_2 *are isomorphic, and under such an isomorphism,* I_1 *is identified with* κI_2 *for some* $\kappa \in K_2^{\times}$. *Conversely, if there is an isomorphism* $\varphi\colon K_1 \to K_2$ *that identifies* $\mathcal{O}_1$ *with* $\mathcal{O}_2$ *and* I_1 *with* κI_2 *for some* $\kappa \in K_2^{\times}$, *then* $N_{I_1,\mathcal{O}_1}(X_1,\dots,X_n)$ *and* $N_{I_2,\mathcal{O}_2}(X_1,\dots,X_n)$ *are* $\mathrm{GL}_n(\mathbb{Z})$*-equivalent.*

Proof. We prove only the first part of the statement; the second is left to the reader. Choose a $\mathbb{Z}$-basis $\langle\alpha_1^{(i)},\dots,\alpha_n^{(i)}\rangle$ of I_i for each i so that, with respect to these bases, we have

$$N_{I_1,\mathcal{O}_1}(X_1,\dots,X_n) = \pm N_{I_2,\mathcal{O}_2}(X_1,\dots,X_n).$$

For each $i \in \{1,2\}$, write $K^{(i)} = \prod_{j=1}^{m_i} K_j^{(i)}$, where $K_j^{(i)}$ is a number field for each j, and let $\pi_j^{(i)}\colon K^{(i)} \to K_j^{(i)}$ denote the projection map onto the jth factor. Then, using the symbol "$\propto$" to denote "equal up to multiplication by an element of $\mathbb{Q}^\times$," we find that

$$\prod_{j=1}^{m_1} N_{\mathbb{Q}}^{K_j^{(1)}}(\pi_j^{(1)}(\alpha_1^{(1)})X_1 + \cdots + \pi_j^{(1)}(\alpha_n^{(1)})X_n) \propto \prod_{j=1}^{m_2} N_{\mathbb{Q}}^{K_j^{(2)}}(\pi_j^{(2)}(\alpha_1^{(2)})X_1 + \cdots + \pi_j^{(2)}(\alpha_n^{(2)})X_n). \tag{3.2}$$

Since $\alpha_1^{(i)}, \ldots, \alpha_n^{(i)}$ is a $\mathbb{Q}$-basis of K_i, we see that $\pi_j^{(i)}(\alpha_1^{(i)}), \ldots, \pi_j^{(i)}(\alpha_n^{(i)})$ is a $\mathbb{Q}$-spanning set of $K_j^{(i)}$ for each $j \in \{1, \ldots, m_i\}$. Consequently, we have an equality $\{K_j^{(1)} : j \in \{1, \ldots, m_1\}\} = \{K_j^{(2)} : j \in \{1, \ldots, m_2\}\}$ of multisets, and so we can take $K^{(1)} = K^{(2)} =: K$, $m_1 = m_2 =: m$, $K_j^{(1)} = K_j^{(2)} =: K_j$, and $\pi_j^{(1)} = \pi_j^{(2)} =: \pi_j$.

Now, by permuting isomorphic factors among the fields $K_1, \ldots, K_m$ if necessary, we find that, for each j,

$$N_{\mathbb{Q}}^{K_j}(\pi_j(\alpha_1^{(1)})X_1 + \cdots + \pi_j(\alpha_n^{(1)})X_n) \propto N_{\mathbb{Q}}^{K_j}(\pi_j(\alpha_1^{(2)})X_1 + \cdots + \pi_j(\alpha_n^{(2)})X_n). \tag{3.3}$$

Note that the constant of proportionality in (3.3) must be a norm from K_j, as can be seen by specializing $X_1, \ldots, X_n$ to values in $\mathbb{Q}$. Then, since $\pi_j(\alpha_1^{(1)})X_1 + \cdots + \pi_j(\alpha_n^{(1)})X_n$ and $\pi_j(\alpha_1^{(2)})X_1 + \cdots + \pi_j(\alpha_n^{(2)})X_n$ respectively divide the left- and right-hand sides of (3.3) (as polynomials over K_j), there must be some $\kappa_j \in K_j^\times$ and some automorphism σ_j of K_j such that $\pi_j(\alpha_k^{(1)}) = \kappa_j\sigma_j(\pi_j(\alpha_k^{(2)}))$ for each $j = 1, \ldots, m$, $k = 1, \ldots, n$. Taking $\kappa = \prod_{j=1}^m \kappa_j$ and $\sigma = \prod_{j=1}^m \sigma_j$, we deduce that $\alpha_k^{(1)} = \kappa\sigma(\alpha_k^{(2)})$ for each k. Thus, $I_1 = \kappa\sigma(I_2)$, as desired. ∎

Our next theorem states that when $f \in \mathbb{Z}[X]$ is a polynomial of degree n, the form $[f]$, as defined in (1.2), may be interpreted as a norm form of a fractional ideal, namely, $I_f(n-1)$.

THEOREM 3.8. *Let $f \in \mathbb{Z}[X]$ be a polynomial of degree n. Then $[f]$ is, up to sign, the norm form of $I_f(n-1)$ with respect to R_f and the power basis* (3.1).

Proof. This follows from the definition of $[f]$ upon noting that $I_f(n-1)$ has $\mathbb{Z}$-basis $\langle 1, \alpha, \ldots, \alpha^{n-1}\rangle$ and that the norm of $I_f(n-1)$ with respect to R_f is equal to $|f_0|^{1-n}$. ∎

REMARK 3.9. Theorem 2.5 may also be proven using Theorem 3.8. When $D(f) \neq 0$ and f is primitive, combining Theorem 3.8 with Lemma 3.6 and Theorem 3.3(iii, iv) yields $D([f]) = D(N_{I_f(n-1),R_f}) = D(R_f) = D(f)$. In order to include the case $D(f) = 0$ and/or f imprimitive, we observe that $D([f]) - D(f)$, viewed as a polynomial in the coefficients of f, must be identically zero since it vanishes already if $D(f) \neq 0$ and f is primitive.

3.3. Interpretation of Hermite equivalence in terms of invariant orders and ideals. We may now prove the following necessary and sufficient criterion for Hermite equivalence:

THEOREM 3.10. *Let $f, g \in \mathbb{Z}[X]$ be polynomials of degree n and nonzero discriminant. If f and g are Hermite equivalent, then there is a $\mathbb{Q}$-algebra isomorphism from K_f to K_g that maps $I_f(n-1)$ to $\kappa I_g(n-1)$ for some $\kappa \in K_g^\times$, and any such isomorphism maps R_f to R_g.*

Conversely, if there is a $\mathbb{Q}$-algebra isomorphism from K_f to K_g that maps R_f to R_g and $I_f(n-1)$ to $\kappa I_g(n-1)$ for some $\kappa \in K_g^\times$, then f and g are Hermite equivalent.

Proof. Assume that f, g are Hermite equivalent and write $f = c_f f'$, $g = c_g g'$, where $f', g' \in \mathbb{Z}[X]$ are primitive polynomials and c_f, c_g positive integers. Theorems 3.7 and 3.8 imply that there is a $\mathbb{Q}$-algebra isomorphism from K_f to K_g that maps $I_f(n-1)$ to $\kappa I_g(n-1)$ for some $\kappa \in K_g^\times$. By Theorem 3.3(vi), the endomorphism rings of $I_f(n-1)$ and $I_g(n-1)$ are respectively isomorphic to $R_{f'}$ and $R_{g'}$. It follows that the isomorphism $K_f \xrightarrow{\sim} K_g$ restricts to an isomorphism $R_{f'} \xrightarrow{\sim} R_{g'}$.

Now Theorem 2.1 implies that $c_f = c_g$. Thus, since $R_f = \mathbb{Z} + c_f R_{f'}$ and $R_g = \mathbb{Z} + c_g R_{g'}$, the isomorphism $R_{f'} \xrightarrow{\sim} R_{g'}$ restricts to an isomorphism $R_f \xrightarrow{\sim} R_g$.

The second statement follows directly from Theorems 3.7 and 3.8. ∎

We have the following pithy rephrasing of Theorem 3.10 in terms of ideal classes of invariant orders:

COROLLARY 3.11. *Let $f, g \in \mathbb{Z}[X]$ be polynomials of degree n and nonzero discriminant. Then f and g are Hermite equivalent if and only if their invariant orders R_f and R_g are isomorphic, and under such an isomorphism, $I_f(n-1)$ and $I_g(n-1)$ belong to the same ideal class.*

Retain the setting of Corollary 3.11, and suppose further that f and g are primitive. Applying Theorem 3.3(v), we see that the ideal classes of I_f^{n-2} and I_f^{n-1} are carried under this isomorphism to those of I_g^{n-2} and I_g^{n-1}, respectively; hence this isomorphism carries the class of I_f to that of I_g. Thus, for primitive polynomials, we obtain the following variant of Corollary 3.11:

COROLLARY 3.12. *Let $f, g \in \mathbb{Z}[X]$ be primitive polynomials of nonzero discriminant. Then f and g are Hermite equivalent if and only if their invariant orders R_f and R_g are isomorphic, and under such an isomorphism, I_f and I_g belong to the same ideal class.*

REMARK 3.13. When $n = 2$, Theorem 3.10 is well-known. Indeed, if f is a binary quadratic form, then $[f](\underline{X}) = f(X_2, -X_1)$, and so Hermite equivalence and $\mathrm{GL}_2(\mathbb{Z})$-equivalence are the same notion; since it is known (by the ideal class interpretation of Gauss composition) that $\mathrm{GL}_2(\mathbb{Z})$-classes of integral binary quadratic forms f are in bijection with isomorphism classes of pairs (R, I), where R is the invariant order of f and I is the invariant ideal of f, the result follows.

REMARK 3.14. When $n = 3$, the condition that the invariant ideals I_f and I_g lie in the same ideal class can be dropped: by the Levi–Delone–Faddeev correspondence [8], binary cubic forms define isomorphic rings if and only if they are $\mathrm{GL}_2(\mathbb{Z})$-equivalent. In §3.5, we will show that, in contrast to the case $n = 3$, the condition in Theorem 3.10 that the invariant ideals I_f and I_g lie in the same ideal class cannot be dropped when $n > 3$.

3.4. Consequences for Hermite equivalence. In this subsection, we present several corollaries of Theorem 3.10 concerning Hermite equivalence. First, by dropping the condition on the invariant ideals in Theorem 3.10, we obtain the following consequence:

COROLLARY 3.15. *Let $f, g \in \mathbb{Z}[X]$ be Hermite equivalent polynomials of nonzero discriminant. Then their invariant orders R_f and R_g are isomorphic.*

The converse of Corollary 3.15 holds in certain special situations. For example, when f and g are both monic, their invariant ideals I_f and I_g are both principal (in fact, as stated in Remark 3.5, they are both equal to the unit ideal), and applying Theorem 3.10 yields the following consequence:

COROLLARY 3.16. *Let $f, g \in \mathbb{Z}[X]$ be monic polynomials of nonzero discriminant. Then f and g are Hermite equivalent if and only if their invariant orders R_f and R_g are isomorphic.*

REMARK 3.17. Recall that the map sending the $\mathbb{Z}$-equivalence class of a monic quadratic polynomial $f \in \mathbb{Z}[X]$ to the unique quadratic ring with discriminant $D(f)$ is a bijection. Combining this fact with Corollary 3.16, we see that two monic quadratic polynomials $f, g \in \mathbb{Z}[x]$ are Hermite equivalent if and only if they are $\mathbb{Z}$-equivalent.

From the discussion in Remarks 3.13–3.14, we see that the converse to Corollary 3.15 does *not necessarily* hold when $n = 2$, but that it *does* hold

when $n = 3$. In light of this, we pose the following question concerning the converse of Corollary 3.15:

QUESTION 3.18. *Let $n \geq 4$. Do there exist (reducible or irreducible) polynomials $f, g \in \mathbb{Z}[X]$ of degree n and nonzero discriminant that have isomorphic invariant orders but are not Hermite equivalent, and if so, can such polynomials be exhibited?*

Corollary 3.16 implies that, in Question 3.18, if such polynomials f, g exist they necessarily have to be nonmonic. See §3.5 for an explicit example in the quartic case.

REMARK 3.19. Theorem 2.4 can also be proven using Theorem 3.10. Indeed, observe that by Theorem 3.3(vii), if f and g are $\mathrm{GL}_2(\mathbb{Z})$-equivalent, then the invariant orders R_f and R_g are naturally isomorphic and the invariant ideals I_f and I_g lie in the same ideal class under this isomorphism. By Theorem 3.10, we conclude that if f and g have nonzero discriminant and are $\mathrm{GL}_2(\mathbb{Z})$-equivalent, then they are Hermite equivalent. In particular, if f and g are monic and $\mathbb{Z}$-equivalent, then they are Hermite equivalent.

3.5. Necessity of the condition on invariant ideals when $n = 4$. In this section, we give an answer to Question 3.18 by showing that, in contrast to the case $n = 3$, the condition in Theorem 3.10 that the invariant ideals I_f and I_g lie in the same ideal class cannot always be dropped when $n > 3$. Specifically, we consider the case $n = 4$, and show the existence of two quartic polynomials $f, g \in \mathbb{Z}[X]$ such that R_f is isomorphic to R_g but I_f and I_g do not lie in the same ideal class under any isomorphism between R_f and R_g. We prove the following theorem, which implies Theorem 1.3(i):

THEOREM 3.20. *Let*

$$f(X) = 4X^4 - X^3 - 62X^2 + 13X + 255 \text{ and } g(X) = 5X^4 - X^3 - 2X^2 - 7X - 6.$$

Then R_f and R_g are isomorphic, but there is no isomorphism between R_f and R_g under which the ideal classes of I_f and I_g are identified. In fact, I_f is principal, whereas I_g is not.

Proof. We first prove that R_f and R_g are isomorphic. Consider the map $\iota\colon \mathrm{Sym}_4 \mathbb{Z}^2 \to \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}^2 \mathbb{Z}^3$ sending a binary quartic form f as in (1.1) to the pair

$$(A_0, B_f) := \left(\begin{pmatrix} 0 & 0 & 1/2 \\ 0 & -1 & 0 \\ 1/2 & 0 & 0 \end{pmatrix}, \begin{pmatrix} f_0 & f_1/2 & 0 \\ f_1/2 & f_2 & f_3/2 \\ 0 & f_3/2 & f_4 \end{pmatrix} \right).$$

The group $\mathrm{GL}_3(\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z})$ acts on the space $\mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}^2 \mathbb{Z}^3$ via

$$\left(\gamma, \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)\right) \cdot (A, B) = (r \times \gamma A \gamma^T + s \times \gamma B \gamma^T, t \times \gamma A \gamma^T + u \times \gamma B \gamma^T),$$

so we may think of the polynomial f as giving rise to an orbit of $\mathrm{GL}_3(\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z})$ on $\mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}^2 \mathbb{Z}^3$ via the map ι. We then have the following result, which translates properties of invariant orders of univariate quartic polynomials into properties of the corresponding orbits of $\mathrm{GL}_3(\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z})$ on $\mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}^2 \mathbb{Z}^3$:

PROPOSITION 3.21. *Let $f, g \in \mathbb{Z}[X]$ be quartic polynomials such that $\iota(f)$ and $\iota(g)$ are equivalent under the action of $\mathrm{GL}_3(\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z})$. Then R_f and R_g are isomorphic. If f and g are $\mathrm{GL}_2(\mathbb{Z})$-equivalent, then $\iota(f)$ and $\iota(g)$ are equivalent under the action of $\mathrm{GL}_3(\mathbb{Z}) \subset \mathrm{GL}_3(\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z})$.*

Proof. This is an immediate consequence of the parametrization of quartic rings given in [3, Theorem 2] together with [45, Lemma 2.2], which explains how the invariant orders of univariate quartic polynomials fit into this parametrization. ∎

In order to prove that R_f and R_g are isomorphic, it suffices by Proposition 3.21 to exhibit the pair $\left(\gamma, \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)\right) \in \mathrm{GL}_3(\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z})$ such that $\left(\gamma, \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)\right) \cdot (A_0, B_g) = (A_0, B_f)$. A calculation reveals that taking

$$\gamma = \begin{pmatrix} 0 & 2 & -1 \\ -1 & 0 & 1 \\ -3 & -15 & 10 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} r & s \\ t & u \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 63 \end{pmatrix}$$

does the job. Upon observing that $D(f) = D(R_f) = D(R_g) = D(g)$ is squarefree, which implies that $R_f \simeq R_g$ is the maximal order in its field of fractions, verifying that I_f is principal and that I_g is not can be achieved in `sage` using the following code:

```
R.<x> = PolynomialRing(QQ)
K.<a> = NumberField(4*x^4-x^3-62*x^2+13*x+255)
K.ideal(1,a,4*a^2-a,4*a^3-a^2-62*a).is_principal(proof = True)
L.<b> = NumberField(5*x^4-x^3-2*x^2-7*x-6)
L.ideal(1,b,5*b^2-b,5*b^3-b^2-2*b).is_principal(proof = True)
```

In fact, one can use `sage` to verify that the class group of $R_f = R_g$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, so I_g represents the nontrivial class, which squares to the class of I_f. This completes the proof of Theorem 3.20. ∎

We now briefly explain how to search for examples such as the one presented in Theorem 3.20. For simplicity, we restrict our search to irreducible quartic polynomials $f \in \mathbb{Z}[X]$ of squarefree discriminant (so that, in particular, R_f is maximal order in its field of fractions K_f). We claim that we can impose the following condition without loss of generality:

PROPERTY (i). *The fractional ideal I_f is not principal, and the ideal class group of R_f has a nontrivial 2-torsion element.*

To prove the first part of the claim, observe that if the desired form g exists, then at least one of I_f or I_g is not principal. As for the second part,

recall from §3.1 that $I_f(2)$ represents the ideal class of the inverse different of R_f. In particular, if R_f is isomorphic to R_g for some integral binary quartic form g, then the ideal classes of I_f and I_g square to the same element of the class group of R_f. Thus, if I_f and I_g do not lie in the same ideal class, then the class group of R_f has a nontrivial 2-torsion element, namely the one represented by $I_f I_g^{-1}$.

Note that it is not *a priori* obvious that a polynomial f satisfying Property (i) exists, but a computer search reveals many examples.

Having narrowed our search to polynomials f satisfying Property (i), we now explain how to construct a quartic polynomial $g \in \mathbb{Z}[X]$ such that R_f and R_g are isomorphic but such that f and g are not $\mathrm{GL}_2(\mathbb{Z})$-equivalent (note that, by Theorem 3.3(vii), f and g must be $\mathrm{GL}_2(\mathbb{Z})$-inequivalent for $I_f I_g^{-1}$ to be nonprincipal). To construct such a g, we claim that it suffices to impose the following condition:

PROPERTY (ii). $\det B_f = 1$ *and* B_f *is isotropic over* $\mathbb{Q}$.

Suppose Property (ii) is satisfied. Then it follows from the classification of integral ternary quadratic forms that there exists a transformation $\gamma \in \mathrm{GL}_3(\mathbb{Z})$ such that $\gamma B_f \gamma^T = A_0$. Let $B = \gamma A_0 \gamma^T$, and let b denote the row-1, column-3 entry of B. Acting on the pair $\gamma \cdot (A_0, B_f) = (B, A_0)$ via $\left(\begin{smallmatrix} 0 & 1 \\ 1 & -b \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$, we obtain a pair of the shape $(A_0, \iota(g))$, where g is an integral binary quartic form. By Proposition 3.21, R_f and R_g are isomorphic.

Now, if f and g are $\mathrm{GL}_2(\mathbb{Z})$-equivalent, then the stabilizer of the pair (A_0, B_f) in $\mathrm{GL}_3(\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z})$ would contain a nontrivial element. But this is impossible: the stabilizer of (A_0, B_f) is simply the group of automorphisms of the ring R_f, but because R_f has squarefree discriminant, it has no nontrivial automorphisms. Thus, we have the claim.

One can then generate quartic polynomials $f \in \mathbb{Z}[X]$ satisfying Properties (i) and (ii), apply the above procedure to obtain the form g, and check whether $I_f I_g^{-1}$ is principal.

REMARK 3.22. Let $\mathcal{O}$ be the ring of integers of a number field. It is a well-known result of Hecke that the ideal class of the different of $\mathcal{O}$ is a perfect square (see [26, Theorem 176]). In the discussion [10], Emerton asks whether, among all such square roots, there exists a canonical choice. As part of that discussion, the following observation of Wood is mentioned: when $\mathcal{O} = R_f$ for a polynomial $f \in \mathbb{Z}[X]$ of even degree n, it is easy to pick out a "distinguished" square root, namely the ideal class of $I_f\left(\frac{n-2}{2}\right)$. Nevertheless, Theorem 3.20 implies that at least when $n = 4$, this "distinguished" square root is not particularly canonical, because it depends on the choice of a form f such that $\mathcal{O} = R_f$.

3.6. k-Hermite equivalence. Given Theorem 3.8, which establishes that $[f]$ is simply the norm form of $I_f(n-1)$, it is natural to define the following family of generalizations of Hermite equivalence:

DEFINITION 3.23. Let $f, g \in \mathbb{Z}[X]$ be primitive polynomials of degree n and nonzero discriminant, and let $k \in \{0, \dots, n-1\}$. Then f and g are *k-Hermite equivalent* if the norm form of $I_f(k)$ with respect to R_f is $\mathrm{GL}_n(\mathbb{Z})$-equivalent to the norm form of $I_g(k)$ with respect to R_g.

Thus the notion of $(n-1)$-Hermite equivalence coincides with Hermite equivalence. In addition, we see that k-Hermite equivalence and k'-Hermite equivalence together imply $(k+k')$-Hermite equivalence. The converse is not in general true—see Theorem 3.20 for a counterexample with $n = 4$, $k = 1$, and $k' = 2$. It is easy to verify that, as long as $k \notin \{0, n-2\}$ (in which case k-Hermite equivalence simply amounts to having isomorphic invariant orders), every claim made in Theorems 1.2–1.4 holds with "Hermite equivalence" replaced by "k-Hermite equivalence", where the occurrences of $n-1$ are replaced by k.

For primitive polynomials, we can define k-Hermite equivalence for any $k \in \mathbb{Z}$. It follows from Theorem 3.3(iii, v) that the notions of k-Hermite equivalence and $(k+n-2)$-Hermite equivalence coincide.

4. Finiteness theorems. The purpose of this section is to prove Theorem 1.3. In §4.1, we recall several results from the literature concerning finiteness for $\mathrm{GL}_2(\mathbb{Z})$-equivalence (resp., $\mathbb{Z}$-equivalence) classes of polynomials in $\mathbb{Z}[X]$ (resp., monic polynomials in $\mathbb{Z}[X]$), and we observe that, on account of Theorem 2.4, all of these results hold with "$\mathrm{GL}_2(\mathbb{Z})$-equivalence" (resp., "$\mathbb{Z}$-equivalence") replaced by "Hermite equivalence". In §4.2, we discuss the extent to which Hermite equivalence classes fall apart into $\mathrm{GL}_2(\mathbb{Z})$-equivalence and $\mathbb{Z}$-equivalence classes.

4.1. Finiteness for $\mathrm{GL}_2(\mathbb{Z})$- and $\mathbb{Z}$-equivalence classes. Lagrange [33] was the first to develop a reduction theory for quadratic polynomials in $\mathbb{Z}[X]$. His theory was made more precise by Gauss [16]. The theories of Lagrange and Gauss imply in an effective way that there are only finitely many $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of quadratic polynomials in $\mathbb{Z}[X]$ with a given nonzero discriminant. Hermite [28] proved the same finiteness statement for the $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of cubic polynomials in $\mathbb{Z}[X]$. Furthermore, for polynomials of general degree n, Hermite obtained a finiteness result for a suitable, less natural invariant Ψ in place of the discriminant; his theory was made more precise by Julia [31].

For polynomials of larger degree, Birch and Merriman [6] proved the following result:

THEOREM A (Birch and Merriman, [6]). *There are only finitely many* $\mathrm{GL}_2(\mathbb{Z})$*-equivalence classes of polynomials in* $\mathbb{Z}[X]$ *of given degree* $n \geq 2$ *and given discriminant* $D \neq 0$.

An immediate consequence of Theorem A and Theorem 2.4 is the following theorem of Hermite:

THEOREM B (Hermite, [29, 30]). *There are only finitely many Hermite equivalence classes of polynomials in* $\mathbb{Z}[X]$ *of given degree* $n \geq 2$ *and given discriminant* $D \neq 0$.

Hermite deduced Theorem B from a reduction theory that he developed for decomposable forms, which in turn he derived from what is now considered an elementary reduction theory for positive definite quadratic forms.

As it happens, Birch and Merriman's proof of Theorem A was *ineffective*. On the other hand, a consequence of the theory of Hermite [28] and Julia [31] referenced above is that every polynomial $f \in \mathbb{Z}[X]$ of degree $n \geq 4$ is $\mathrm{GL}_2(\mathbb{Z})$-equivalent to a polynomial f^* whose height $H(f^*)$ (i.e., maximum absolute value of the coefficients) is effectively bounded above in terms of the aforementioned invariant $\Psi(f)$. In [12], Evertse and Győry finally proved an *effective* version of Theorem A, and in [13], they improved this result and made it completely explicit. This improved result of Evertse and Győry is stated as follows:

THEOREM C (Evertse and Győry [13, Theorem 14.1.1]). *Let* $f \in \mathbb{Z}[X]$ *be a polynomial of degree* $n \geq 2$ *and discriminant* $D \neq 0$. *Then* f *is* $\mathrm{GL}_2(\mathbb{Z})$*-equivalent to a polynomial* $f^* \in \mathbb{Z}[X]$ *for which*

$$H(f^*) \leq \exp\{(4^2 n^3)^{25n^2} |D|^{5n-3}\}.$$

In light of Theorem 2.4, Theorem C implies a more precise, effective and quantitative variant of Hermite's result in Theorem B. Theorem C also provides a method to effectively determine in principle all polynomials $f \in \mathbb{Z}[X]$ of given degree $n \geq 2$ and given discriminant $D \neq 0$, up to $\mathrm{GL}_2(\mathbb{Z})$-equivalence.

For monic polynomials there are finiteness results for $\mathbb{Z}$-equivalence which do not follow directly from the results on the weaker $\mathrm{GL}_2(\mathbb{Z})$-equivalence for arbitrary polynomials mentioned above. In the case $n = 3$, Delone (= Delaunay) [7] and Nagell (= Nagel) [35] proved that there are only finitely many $\mathbb{Z}$-equivalence classes of irreducible monic cubic polynomials in $\mathbb{Z}[X]$ with given nonzero discriminant. The first general *effective* result for monic polynomials was proved by Győry [17] for monic polynomials of given nonzero discriminant, where the degree need *not* be fixed:

THEOREM D (Győry [17]). *There are only finitely many* $\mathbb{Z}$*-equivalence classes of monic polynomials in* $\mathbb{Z}[X]$ *with given discriminant* $D \neq 0$, *and a full set of representatives of these classes can be effectively determined.*

We also mention the following theorem, which is an improved version of a quantitative result of Győry [18] on monic polynomials with given degree and given nonzero discriminant.

THEOREM E (Evertse and Győry, [13, Theorem 6.6.2]). *Let $f \in \mathbb{Z}[X]$ be a monic polynomial of degree $n \geq 2$ and discriminant $D \neq 0$. Then f is $\mathbb{Z}$-equivalent to a polynomial f^* for which*

$$H(f^*) \leq \exp\{n^{20}8^{n^2+19}(|D|(\log^* |D|)^n)^{n-1}\}.$$

In both Theorems C and E, the degree n of f can also be estimated from above in terms of $|D(f)|$.

THEOREM F (Győry, [18]). *Every polynomial $f \in \mathbb{Z}[X]$ with nonzero discriminant D has degree*

$$n \leq 3 + 2\log|D|/\log 3.$$

Furthermore, in [18] it is established when equality holds in Theorem F. For monic polynomials $f \in \mathbb{Z}[X]$, the upper bound is slightly improved in [18] to $2 + 2\log|D|/\log 3$.

Clearly, Theorem D is a consequence of Theorem E and the subsequent estimate for the degree of a polynomial in terms of its discriminant. Likewise, Theorems C and F imply that the polynomials in $\mathbb{Z}[X]$ of given discriminant lie in only finitely many $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes, a full system of representatives of which can be determined effectively.

For generalizations of Theorems A, C, D, and E (e.g., for polynomials with S-integral coefficients over number fields) we refer respectively to Birch and Merriman [6], Győry [20, 21, 24], and Evertse and Győry [12, 13]. Theorem D and its consequences, quantitative versions and generalizations provided effective finiteness results for monogeneity and power integral bases of number fields; cf. Győry [18, 19, 20, 21, 22, 25] and Evertse and Győry [13].

Because Hermite equivalence is a weaker notion than $\mathrm{GL}_2(\mathbb{Z})$-equivalence, which is in turn strictly weaker than $\mathbb{Z}$-equivalence, Theorems A, C, D, and E are more precise than Theorem B. Finiteness theorems concerning unit equations played an important role in the proofs of Theorems A, C, D, and E, but such finiteness results were not available to Hermite.

4.2. Comparison of Hermite, $\mathrm{GL}_2(\mathbb{Z})$-, and $\mathbb{Z}$-equivalence. Theorems A–E imply in particular that any Hermite equivalence class of separable polynomials (resp., separable monic polynomials) in $\mathbb{Z}[X]$ is a union of at most finitely many $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes (resp., $\mathbb{Z}$-equivalence classes). In the next theorem, we have collected some upper bounds for the number of $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes (resp., $\mathbb{Z}$-equivalence classes) going into an Hermite equivalence class, which are easily derived from the existing literature.

THEOREM 4.1.

(i) *Separable quadratic polynomials in* $\mathbb{Z}[X]$ *are Hermite equivalent if and only if they are* $\mathrm{GL}_2(\mathbb{Z})$*-equivalent.*

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

(iii) *Separable cubic polynomials in* $\mathbb{Z}[X]$ *are Hermite equivalent if and only if they are* $\mathrm{GL}_2(\mathbb{Z})$*-equivalent.*

(iv) *Every Hermite equivalence class of separable monic cubic polynomials in* $\mathbb{Z}[X]$ *is a union of at most* 10 $\mathbb{Z}$*-equivalence classes.*

(v) *Every Hermite equivalence class of separable quartic polynomials in* $\mathbb{Z}[X]$ *is a union of at most* 10 $\mathrm{GL}_2(\mathbb{Z})$*-equivalence classes* (*and at most* 7 *if the discriminant is sufficiently large*).

(vi) *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 sufficiently large*).

(vii) *Let* $n \geq 5$*. Then every Hermite equivalence class of separable degree-*n *polynomials in* $\mathbb{Z}[X]$ *is a union of at most* 2^{5n^2} $\mathrm{GL}_2(\mathbb{Z})$*-equivalence classes.*

(viii) *Let* $n \geq 5$*. Then every Hermite equivalence class of separable monic degree-*n *polynomials in* $\mathbb{Z}[X]$ *is a union of at most* 2^{5n^2} $\mathbb{Z}$*-equivalence classes.*

Proof. (i)–(iii). These points respectively follow from Remarks 3.13, 3.17, and 3.14.

(iv) By Theorem 2.4 (and its converse, which holds when $n = 3$), it suffices to show that every $\mathrm{GL}_2(\mathbb{Z})$-equivalence class of separable cubic polynomials in $\mathbb{Z}[X]$ is a union of at most 10 $\mathbb{Z}$-equivalence classes. Let f be such a cubic, and let g be the translate of f by an element $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$. Writing $F(X, Y)$ for the homogenization of f, we see that $F(a, c) = 1$, so we obtain a map from monic $\mathrm{GL}_2(\mathbb{Z})$-translates of f to solutions of the cubic Thue equation $F(x, y) = 1$. It is easy to verify that, under this map, two translates g and g' are sent to the same solution if and only if g and g' are $\mathbb{Z}$-equivalent. The result then follows from a theorem of Bennett [1], which states that the equation $F(X, Y) = 1$ has at most 10 solutions.

(v) By a result of Bhargava [4, Theorem 1.2], if $\mathcal{O}$ is an order in a quartic number field, then there are at most 10 $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of quartic polynomials $f \in \mathbb{Z}[X]$ such that $\mathcal{O} = R_f$ (and at most 7 if $D(\mathcal{O}) \gg 1$). While the work [4] treats only the case of irreducible quartic polynomials, it is well-known that the bound only gets better in the reducible case. The result then follows from Corollary 3.15.

(vi) By a result of Akhtari and Bhargava [4, Theorem 1.1], if $\mathcal{O}$ is an order in a quartic number field, then there are at most 2760 $\mathbb{Z}$-equivalence

classes of elements $\alpha \in \mathcal{O}$ such that $\mathcal{O} = \mathbb{Z}[\alpha]$ (and at most 182 if $D(\mathcal{O}) \gg 1$). In the reducible case, we get a bound of 10 from (iv). The result then follows from Corollary 3.16.

(vii) By a result of Evertse and Győry [13, Theorem 17.1.1], there are at most 2^{5n^2} $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of separable degree-n polynomials in $\mathbb{Z}[X]$ having the same invariant order. The result then follows from Corollary 3.15.

(viii) This point follows from [13, Theorem 9.1.4]. When the Hermite equivalence class under consideration consists of irreducible polynomials of degree n, [11, Theorem 1.1] obtained the slightly better bound $2^{4(n+5)(n-2)}$. ∎

In §5.3–5.5, we give various examples of pairs of polynomials (f, g) of degree $n \geq 4$ that are Hermite equivalent but not $\mathrm{GL}_2(\mathbb{Z})$-equivalent. On the other hand, we conjecture that for $n \geq 5$, "most" Hermite equivalence classes consist of only one $\mathrm{GL}_2(\mathbb{Z})$-equivalence class. To state our conjecture precisely, and for the sake of convenience in the rest of the paper, we introduce the following notation:

NOTATION. For an integer $n \geq 1$, let $\mathcal{PI}(n)$ denote the set of primitive irreducible polynomials in $\mathbb{Z}[X]$ of degree n, and let $\mathcal{MI}(n) \subset \mathcal{PI}(n)$ denote the subset of monic polynomials. For a number field K, let $\mathcal{PI}(K) \subset \mathcal{PI}(n)$ denote the subset of polynomials f with $K_f = K$, and let $\mathcal{MI}(K) \subset \mathcal{MI}(n)$ denote the subset of polynomials f with $K_f = K$.

CONJECTURE 4.2. *Let K be a number field of degree ≥ 5. Then among the Hermite equivalence classes of polynomials in $\mathcal{PI}(K)$, there are only finitely many that split into more than one $\mathrm{GL}_2(\mathbb{Z})$-equivalence class.*

Conjecture 4.2 has already been proved if we restrict our consideration to monic polynomials and impose some condition on the number field K. Indeed, we have the following result, which is a direct consequence of a result of Bérczes, Evertse, and Győry [2, Theorem 1.2(iii)]:

THEOREM G. *Let K be a number field of degree $n \geq 5$, whose normal closure has Galois group S_n. Then among the Hermite equivalence classes of polynomials in $\mathcal{MI}(K)$, there are only finitely many that split into more than one $\mathrm{GL}_2(\mathbb{Z})$-equivalence class.*

We note that the method of proof of Theorem G used by Bérczes et al. is ineffective—i.e., it does not provide a method to compute the exceptional Hermite equivalence classes.

5. Examples. In this section, we prove Theorem 1.4(ii)–(v) by constructing the relevant infinite collections of polynomials that are Hermite equivalent but not $\mathrm{GL}_2(\mathbb{Z})$-equivalent.

5.1. Infinite sequence of monic examples in degree 4. The conclusion of Theorem G, and hence Conjecture 4.2, is false for $n = 4$. Indeed, consider the polynomials $f_{r,s}(X) = (X^2 - r)^2 - X - s$ with $r, s \in \mathbb{Z}$ such that $f_{r,s}$ is irreducible and the Galois group of the splitting field of $f_{r,s}$ is S_4. Let $K_{r,s}$ be the field generated by a zero of $f_{r,s}$. Kappe and Warren [32] showed that such pairs (r, s) exist, and that there are infinitely many distinct ones among the fields $K_{r,s}$. Bérczes, Evertse, and Győry [2] showed that every field $K_{r,s}$ as above has the following properties:

(i) There are infinitely many pairs of algebraic integers (α_m, β_m) $(m = 1, 2, \ldots)$ in $K_{r,s}$ such that $\mathbb{Q}(\alpha_m) = \mathbb{Q}(\beta_m) = K_{r,s}$, $\beta_m = \alpha_m^2 + r_m$, $\alpha_m = \beta_m^2 + s_m$ for certain $r_m, s_m \in \mathbb{Z}$.
(ii) There are infinitely many distinct orders among the $\mathbb{Z}[\alpha_m]$ $(m = 1, 2, \ldots)$.

Let f_m be the (monic integral) minimal polynomial of α_m and g_m that of β_m. Then we have the following result on Hermite equivalence of the polynomials f_m and g_m:

THEOREM 5.1. *The polynomials f_m lie in infinitely many distinct Hermite equivalence classes. Moreover, for each m, the polynomials f_m and g_m are Hermite equivalent but not* $\mathrm{GL}_2(\mathbb{Z})$*-equivalent.*

Proof. The first claim follows from (ii) above in conjunction with Corollary 3.15. As for the second claim, (i) above implies that $\mathbb{Z}[\alpha_m] = \mathbb{Z}[\beta_m]$, so by Corollary 3.16, the polynomials f_m and g_m are Hermite equivalent for each m. If g_m is the translate of f_m by $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$, then there exists a conjugate β'_m of β_m such that $\beta'_m = \frac{a\alpha_m + b}{c\alpha_m + d} \in \mathbb{Q}(\alpha_m) = K_{r,s} = \mathbb{Q}(\beta_m)$. But since the normal closure of $\mathbb{Q}(\beta_m)$ has Galois group S_4, we must have $\beta'_m = \beta_m$. Consequently,

$$\alpha_m^2 + r_m = \beta_m = \frac{a\alpha_m + b}{c\alpha_m + d}, \quad \text{so} \quad (c\alpha + d)(\alpha_m^2 + r_m) - a\alpha_m - b = 0,$$

but this is impossible because α_m is of degree 4 and a, b, c, d are not all 0. ∎

The argument in the proof of Theorem 5.1 above can be used to produce other pairs (f, g) of primitive irreducible polynomials that are Hermite equivalent but not $\mathrm{GL}_2(\mathbb{Z})$-equivalent. In the next subsection, we construct such pairs of polynomials in degrees 4 and 5. The examples we construct are in fact nonmonic, unlike the example treated in Theorem 5.1.

5.2. Infinite sequences of nonmonic examples in degrees 4 and 5. We start with polynomials of degree 4. Let $s, t \in \mathbb{Z}$ be such that $s \equiv 1 \pmod{15}$ and $t \equiv 21 \pmod{30}$, let

$$f(X) = 2X^4 + 8tX^2 + 2sX - 2s^2 + 8t^2 + t,$$

and observe that $f(X) \equiv 2X^4 + 2X + 1 \pmod 3$, $f(X) \equiv 2(X+1)(X+3) \cdot (X^2 + X + 2) \pmod 5$ and f is primitive. These observations imply that f is irreducible in $\mathbb{Z}[X]$ and that the Galois group of f (as a subgroup of S_4) contains a transposition and a 4-cycle and is thus S_4.

Now, let α be a zero of f, and let $\beta = \alpha + 2\alpha^2$. Then the minimal polynomial of β is

$$\begin{aligned} g(X) = {} & 2X^4 + 32X^3 t + (-16s^2 + 192t^2 + 12s + 16t)X^2 \\ & + (-128s^2 t + 512t^3 - 32s^2 + 32st + 128t^2 + 2s + 8t)X \\ & + (2s^2 - 8t^2 - t)(16s^2 - 64t^2 + 8s - 24t - 1). \end{aligned}$$

A computation shows that

$$\begin{pmatrix} \beta^3 \\ \beta^2 \\ \beta \\ 1 \end{pmatrix} = U \cdot \begin{pmatrix} \alpha^3 \\ \alpha^2 \\ \alpha \\ 1 \end{pmatrix},$$

where U is

$$\begin{pmatrix} 1 - 8s - 48t & 8s^2 + 96t^2 - 12s - 28t & 12s^2 + 32st - 48t^2 - 6s - 6t & -32s^2 t + 128t^3 + 6s^2 - 8t^2 - 3t \\ 4 & -16t + 1 & -4s & 4s^2 - 16t^2 - 2t \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

For any $s, t \in \mathbb{Z}$, we have $\det U = 1$, i.e., $U \in \mathrm{GL}_4(\mathbb{Z})$. This means that $I_f(3) = I_g(3)$, so by Theorem 3.10, the polynomials f and g are Hermite equivalent. One readily verifies using the argument at the end of the proof of Theorem 5.1 that f and g are not $\mathrm{GL}_2(\mathbb{Z})$-equivalent.

We next consider polynomials of degree 5. Let $s \in \mathbb{Z}$ be such that $s \equiv 71 \pmod{110}$, and let

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

Then observe that $f(X) \equiv 2X^5 + 3X + 3 \pmod 5$, $f(X) \equiv 2X(X+8) \cdot (X+3)(X^2+9) \pmod{11}$, and f is primitive. These observations imply that f is irreducible in $\mathbb{Z}[X]$ and the Galois group of f (as a subgroup of S_5) contains a transposition and a 5-cycle and is thus S_5.

Now, let α be a zero of f, and let $\beta = \alpha + 2\alpha^2$. Then the minimal polynomial of β is

$$\begin{aligned} g(X) = {} & 2X^5 - 32(16s+3)(25s+4)X^3 + 4(25s+4)(96s+13)X^2 \\ & + 4(25s+4)(51200s^3 + 27392s^2 + 4944s + 299)X \\ & - (32s+5)(25s+4)(19200s^2 + 6272s + 511). \end{aligned}$$

A computation shows that

$$\begin{pmatrix} \beta^4 \\ \beta^3 \\ \beta^2 \\ \beta \\ 1 \end{pmatrix} = U \cdot \begin{pmatrix} \alpha^4 \\ \alpha^3 \\ \alpha^2 \\ \alpha \\ 1 \end{pmatrix},$$

where U is

$$\begin{pmatrix} 6400s^2+2224s+193 & 6400s^2+2424s+224 & -3200s^2-712s-32 & -6400s^2-1924s-144 & -3200s^2-1012s-80 \\ 6 & 1 & 3200s^2+1112s+96 & 1600s^2+656s+64 & -4800s^2-1518s-120 \\ 4 & 4 & 1 & 0 & 0 \\ 0 & 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

For any $s \in \mathbb{Z}$, we have $\det U = 1$, i.e., $U \in \mathrm{GL}_5(\mathbb{Z})$. This means that $I_f(4) = I_g(4)$, so by Theorem 3.10, the polynomials f and g are Hermite equivalent. Again, one readily verifies using the argument at the end of the proof of Theorem 5.1 that f and g are not $\mathrm{GL}_2(\mathbb{Z})$-equivalent.

5.3. Further monic examples in degrees 4, 5, and 6. We start by describing a general strategy by which one can construct examples of Hermite equivalence classes of polynomials that split into multiple $\mathrm{GL}_2(\mathbb{Z})$-equivalence or $\mathbb{Z}$-equivalence classes. For this, we require the following notation:

NOTATION. Given an algebraic number α, we denote by $f_\alpha \in \mathbb{Z}[X]$ the primitive irreducible polynomial with positive leading coefficient having α as a zero.

Recall that a number field K is called *monogenic* if its ring of integers $\mathcal{O}_K$ can be expressed as $\mathcal{O}_K = \mathbb{Z}[\alpha] = R_{f_\alpha}$. In this case, letting $n = [K : \mathbb{Q}]$, the elements $1, \alpha, \dots, \alpha^{n-1}$ form a $\mathbb{Z}$-module basis of $\mathcal{O}_K$, and we call this basis a *power integral basis* of K. The elements $\alpha \in K$ with $\mathcal{O}_K = \mathbb{Z}[\alpha]$ are precisely those of discriminant $D(\mathcal{O}_K)$. By Corollary 3.16, the minimal polynomials f_α of these elements α form a Hermite equivalence class.

Let α be an algebraic integer of degree $n \geq 4$, and let $f_\alpha(X) = X^n + a_1X^{n-1} + \cdots + a_n \in \mathbb{Z}[X]$ be its minimal polynomial. Consider an element β of $\mathbb{Z}[\alpha]$ such that $\mathbb{Z}[\alpha] = \mathbb{Z}[\beta]$. We want to decide whether α and β are $\mathrm{GL}_2(\mathbb{Z})$-equivalent, in the sense that $\beta = \frac{a\alpha+b}{c\alpha+d}$ for some $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$ ([2]). To do this, we write β in the form

$$\beta = b_1 + b_2\alpha + \cdots + b_n\alpha^{n-1} \quad \text{with } b_1, \dots, b_n \in \mathbb{Z}. \tag{5.1}$$

([2]) Observe that two primitive irreducible polynomials $f, g \in \mathbb{Z}[X]$ are $\mathrm{GL}_2(\mathbb{Z})$-equivalent if and only if there are a zero α of f and a zero β of g such that α and β are $\mathrm{GL}_2(\mathbb{Z})$-equivalent.

Since $\mathbb{Z}[\beta - b_1] = \mathbb{Z}[\beta]$ and $\beta - b_1$ is $\mathrm{GL}_2(\mathbb{Z})$-equivalent to α if and only if β is, we may assume that $b_1 = 0$. Then β is $\mathrm{GL}_2(\mathbb{Z})$-equivalent to α if and only if

$$(c\alpha + d)(b_2\alpha + \cdots + b_n\alpha^{n-1}) - (a\alpha + b) = 0 \tag{5.2}$$

for some $a, b, c, d \in \mathbb{Z}$ with $ad - bc = \pm 1$. Representing the left-hand side of (5.2) as a linear combination of $1, \alpha, \ldots, \alpha^n$ and substituting in the relation $\alpha^n = -(a_1\alpha^{n-1} + \cdots + a_n)$, the coefficients of $1, \alpha, \ldots \alpha^{n-1}$ in the resulting expression must all be 0. We therefore obtain the following system of linear equations in a, b, c, d:

$$\begin{array}{rrrr} & & -cb_na_n & = b, \\ & db_2 & -cb_na_{n-1} & = a, \\ cb_2 & +db_3 & -cb_na_{n-2} & = 0, \\ cb_3 & +db_4 & -cb_na_{n-3} & = 0, \\ \vdots & \vdots & \vdots & \vdots \\ cb_{n-2} & +db_{n-1} & -cb_na_2 & = 0, \\ cb_{n-1} & +db_n & -cb_na_1 & = 0. \end{array} \tag{5.3}$$

We conclude that β is $\mathrm{GL}_2(\mathbb{Z})$-equivalent to α if and only if the system (5.3) has a nonzero solution (a, b, c, d) with $ad - bc = \pm 1$.

To determine how the Hermite equivalence class of f_α falls apart into $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes, it now remains to determine the $\mathbb{Z}$-equivalence classes of elements $\beta \in \mathbb{Z}[\alpha]$ such that $\mathbb{Z}[\alpha] = \mathbb{Z}[\beta]$. This amounts to determining all power integral bases of $\mathbb{Z}[\alpha]$. As it happens, all such bases are explicitly known in several number fields K of degrees $n = 4$, 5, and 6. Owing to this fact, we can determine how the Hermite equivalence class of polynomials $f \in \mathcal{MI}(K)$ with $R_f = \mathcal{O}_K$ splits into $\mathbb{Z}$-equivalence classes and into $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes. In the rest of this subsection, we will illustrate this using three concrete examples in degrees 4, 5, and 6.

We start with a polynomial of degree 4. Let α be a zero of the irreducible polynomial

$$f(X) = X^4 - X^3 - 4X^2 + 2X + 1.$$

Then $D(f) = 3981$, which is squarefree, so R_f is the maximal order in K_f. A full set of pairwise $\mathbb{Z}$-inequivalent β with $R_f = \mathbb{Z}[\beta]$ is given by $\beta = b_2\alpha + b_3\alpha^2 + b_4\alpha^3$, where (b_2, b_3, b_4) are listed in Table 1 below; see Gaál [14, p. 300, last line]. Then, by solving the system of linear equations (5.3) for all pairs β_i, β_j, with $i, j = 1, \ldots, 10$, we conclude that $\{\beta_1, \ldots, \beta_{10}\}$ splits into 3 $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes:

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

Since the Galois group of f is S_4, this implies that the Hermite equivalence class of f splits into 10 $\mathbb{Z}$-equivalence classes, represented by $f_{\beta_1}, \ldots, f_{\beta_{10}}$, and 3 $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes, represented by f_{β_i} for $i = 1, 2, 3$.

We next consider a polynomial of degree 5. Let α be a zero of the irreducible polynomial

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

Then $D(f) = 24217$, which is squarefree, so R_f is the maximal order in K_f. A full set of pairwise $\mathbb{Z}$-inequivalent β with $R_f = \mathbb{Z}[\beta]$ is given by $\beta =$

Table 1. The set of β with $\mathbb{Z}[\beta] = \mathcal{O}_K$ is the union of the $\mathbb{Z}$-equivalence classes represented by the ten $\mathbb{Z}$-inequivalent elements $\{\beta_1, \ldots, \beta_{10}\}$, with $\beta_5 = \alpha$.

	b_2	b_3	b_4
β_1	-4	0	1
β_2	-2	1	0
β_3	-1	2	0
β_4	0	-1	1
β_5	1	0	0
β_6	1	1	0
β_7	3	1	-1
β_8	4	1	-1
β_9	15	4	-4
β_{10}	21	1	-5

Table 2. The set of β with $\mathbb{Z}[\beta] = \mathcal{O}_K$ is the union of the $\mathbb{Z}$-equivalence classes represented by the 39 $\mathbb{Z}$-inequivalent elements $\{\beta_1, \ldots, \beta_{39}\}$, with $\beta_8 = \alpha$.

	b_2	b_3	b_4	b_5
β_1	0	1	0	0
β_2	0	2	1	-1
β_3	0	4	0	-1
β_4	0	5	0	-1
β_5	1	-5	0	1
β_6	1	-4	0	1
β_7	1	-1	0	0
β_8	1	0	0	0
β_9	1	1	-2	-1
β_{10}	1	4	0	-1
β_{11}	2	-1	-1	0
β_{12}	2	4	-1	-1
β_{13}	2	9	-1	-2

	b_2	b_3	b_4	b_5
β_{14}	2	15	-1	-3
β_{15}	2	10	-1	-2
β_{16}	3	4	-1	-1
β_{17}	3	5	-1	-1
β_{18}	3	9	-1	-2
β_{19}	3	10	-1	-2
β_{20}	3	14	-1	-3
β_{21}	3	18	-2	-4
β_{22}	4	-1	-1	0
β_{23}	4	0	-1	0
β_{24}	4	5	-1	-1
β_{25}	4	24	-2	-5
β_{26}	4	29	-2	-6

	b_2	b_3	b_4	b_5
β_{27}	5	-4	-1	1
β_{28}	5	8	-2	-2
β_{29}	5	33	-2	-7
β_{30}	7	5	-2	-1
β_{31}	7	9	-2	-2
β_{32}	7	14	-2	-3
β_{33}	9	18	-3	-4
β_{34}	11	-13	-2	3
β_{35}	12	27	-4	-6
β_{36}	17	28	-6	-6
β_{37}	33	30	-51	-26
β_{38}	83	170	-25	-39
β_{39}	124	246	-40	-55

$b_2\alpha + b_3\alpha^2 + b_4\alpha^3 + b_5\alpha^4$, where (b_2, b_3, b_4, b_5) are listed in Table 2; see Gaál and Győry [15, Example 1].

Then, by solving the system of linear equations (5.3) for all pairs β_i, β_j with $i, j = 1, \ldots, 10$, we find that $\{\beta_1, \ldots, \beta_{39}\}$ splits into 10 $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes:

$$\{\beta_1, \beta_6, \beta_{14}, \beta_{35}\}, \quad \{\beta_2, \beta_{12}, \beta_{17}, \beta_{19}, \beta_{33}, \beta_{37}\}, \quad \{\beta_3, \beta_{13}, \beta_{25}, \beta_{31}\},$$
$$\{\beta_4, \beta_{15}, \beta_{18}, \beta_{23}\}, \quad \{\beta_5, \beta_8, \beta_9, \beta_{16}, \beta_{27}\}, \quad \{\beta_7, \beta_{11}, \beta_{22}, \beta_{39}\},$$
$$\{\beta_{10}, \beta_{24}, \beta_{26}, \beta_{32}\}, \quad \{\beta_{20}, \beta_{28}, \beta_{29}, \beta_{34}\}, \quad \{\beta_{21}, \beta_{30}\}, \quad \{\beta_{36}, \beta_{38}\}.$$

Since the Galois group of f is S_5, this implies that the Hermite equivalence class of f splits into 39 $\mathbb{Z}$-equivalence classes, represented by $f_{\beta_1}, \ldots, f_{\beta_{39}}$, and 10 $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes, represented by f_{β_i} for $i = 1, 2, 3, 4, 5, 7, 10, 20, 21, 36$.

Table 3. The set of β with $\mathbb{Z}[\beta] = \mathcal{O}_K$ is the union of the $\mathbb{Z}$-equivalence classes represented by the 45 $\mathbb{Z}$-inequivalent elements $\{\beta_1, \ldots, \beta_{45}\}$, with $\beta_1 = \alpha$.

	b_2	b_3	b_4	b_5	b_6
β_1	1	0	0	0	0
β_2	−1	1	0	0	0
β_3	−2	−2	1	0	0
β_4	2	7	−2	−3	1
β_5	4	9	−3	−3	1
β_6	−4	12	0	−4	1
β_7	5	−1	−3	1	0
β_8	−5	−5	4	2	−1
β_9	5	6	−2	−3	1
β_{10}	−5	9	1	−4	1
β_{11}	5	9	−3	−3	1
β_{12}	−6	2	3	−1	0
β_{13}	6	−5	−2	1	0
β_{14}	6	8	−3	−3	1
β_{15}	7	1	−4	1	0
β_{16}	−7	6	2	−1	0
β_{17}	−7	−6	5	2	−1
β_{18}	8	10	−4	−3	1
β_{19}	9	10	−4	−3	1
β_{20}	10	0	−4	1	0
β_{21}	10	8	−6	−2	1
β_{22}	−10	−17	6	6	−2
β_{23}	11	3	−8	2	0
β_{24}	−11	−7	6	2	−1
β_{25}	−11	−13	7	5	−2
β_{26}	−11	18	2	−5	1
β_{27}	12	7	−6	−2	1
β_{28}	−13	−6	6	2	−1
β_{29}	13	15	−8	−5	2
β_{30}	−14	−14	8	5	−2
β_{31}	16	16	−9	−5	2
β_{32}	17	16	−9	−5	2
β_{33}	18	11	−10	−4	2
β_{34}	20	22	−11	−8	3
β_{35}	21	−10	−8	6	−1
β_{36}	22	24	−12	−8	3
β_{37}	23	14	−12	−4	2
β_{38}	−26	−20	14	7	−3
β_{39}	43	45	−21	−14	5
β_{40}	−46	−45	26	15	−6
β_{41}	108	106	−63	−36	15
β_{42}	−119	−118	68	40	−16
β_{43}	153	−26	−126	75	−12
β_{44}	173	167	−105	−58	25
β_{45}	−590	−585	336	198	−79

We finally consider a polynomial of degree 6. Let α be a zero of the irreducible polynomial

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

Then $D(f) = 592661$, which is squarefree, so R_f is the maximal order in K_f. A full set of pairwise $\mathbb{Z}$-inequivalent β with $R_f = \mathbb{Z}[\beta]$ is given by $\beta = b_2\alpha + b_3\alpha^2 + b_4\alpha^3 + b_5\alpha^4 + b_6\alpha^5$, where $(b_2, b_3, b_4, b_5, b_6)$ are listed in Table 3; see Bilu, Gaál, and Győry [5, Example].

Then, by solving the system of linear equations (5.3) for all pairs β_i, β_j with $i, j = 1, \dots, 45$, we deduce that $\{\beta_1, \dots, \beta_{45}\}$ splits into 11 $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes:

$$\{\beta_1, \beta_{19}, \beta_{26}, \beta_{35}, \beta_{42}\}, \quad \{\beta_2, \beta_{14}, \beta_{20}, \beta_{23}, \beta_{30}\}, \quad \{\beta_3, \beta_4, \beta_{13}, \beta_{40}\},$$
$$\{\beta_5, \beta_{15}, \beta_{18}, \beta_{29}, \beta_{38}\}, \quad \{\beta_6, \beta_{21}, \beta_{31}, \beta_{39}, \beta_{44}\}, \quad \{\beta_7, \beta_{22}, \beta_{33}\},$$
$$\{\beta_8, \beta_{11}, \beta_{24}, \beta_{27}, \beta_{45}\}, \quad \{\beta_9, \beta_{28}, \beta_{37}\}, \quad \{\beta_{10}, \beta_{12}, \beta_{36}\},$$
$$\{\beta_{16}, \beta_{32}, \beta_{34}, \beta_{41}, \beta_{43}\}, \quad \{\beta_{17}, \beta_{15}\}.$$

Since the Galois group of f is S_6, this implies that the Hermite equivalence class of f splits into 45 $\mathbb{Z}$-equivalence classes, represented by $f_{\beta_1}, \dots, f_{\beta_{45}}$, and 11 $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes, represented by f_{β_i} for $i = 1, 2, 3, 5, 6, 7, 8, 9, 10, 16, 17$.

5.4. Reducible monic examples in arbitrary degree. In this subsection, we prove the following theorem, which shows that it is easy to construct examples of reducible monic polynomials that are Hermite equivalent but not $\mathrm{GL}_2(\mathbb{Z})$-equivalent:

THEOREM 5.2. *Let $n \geq 3$ be an integer, and let $f \in \mathcal{MI}(n)$ be such that $f(0) = 1$ and f has trivial stabilizer in $\mathrm{GL}_2(\mathbb{Z})$. Then the monic reducible polynomials $Xf(X) \in \mathbb{Z}[X]$ and $X^{n+1}f(1/X) \in \mathbb{Z}[X]$ are Hermite equivalent but not $\mathrm{GL}_2(\mathbb{Z})$-equivalent.*

Proof. Let $g(X) = Xf(X)$ and $h(X) = X^{n+1}f(1/X)$. To prove that g and h are Hermite equivalent, it suffices by Corollary 3.16 to prove that R_g and R_h are isomorphic. But since both the leading and constant coefficients of f are equal to 1, we have $\mathrm{Res}(X, f(X)) = \mathrm{Res}(X, X^n f(1/X)) = 1$. It follows that R_g and R_h are both isomorphic to $\mathbb{Z} \times R_f$, as desired.

Now, if g and h are $\mathrm{GL}_2(\mathbb{Z})$-equivalent, then the fact that f has no rational roots implies that h is the translate of g by an element $\gamma \in \mathrm{GL}_2(\mathbb{Z})$ such that γ sends X to X and $f(X)$ to $X^n f(1/X)$. But any γ stabilizing X is upper-triangular, so $\gamma \cdot \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ is a nontrivial transformation stabilizing f, which is a contradiction. ∎

5.5. Irreducible monic and nonmonic examples in arbitrary degree. In the previous subsections, we gave examples of polynomials of degree

4, 5, and 6 that are Hermite equivalent but not $\mathrm{GL}_2(\mathbb{Z})$-equivalent. In this subsection, we extend this to every degree ≥ 4. Our result is as follows:

THEOREM 5.3.

(i) *For every integer $n \geq 4$, there exists an infinite collection of Hermite equivalence classes, each containing two polynomials $f, g \in \mathcal{PI}(n)$ that are properly nonmonic (i.e., not $\mathrm{GL}_2(\mathbb{Z})$-equivalent to monic polynomials) and not $\mathrm{GL}_2(\mathbb{Z})$-equivalent.*

(ii) *For every integer $n \geq 4$, there exists an infinite collection of Hermite equivalence classes, each containing two polynomials $f, g \in \mathcal{MI}(n)$ that are not $\mathrm{GL}_2(\mathbb{Z})$-equivalent.*

More precisely, we give, for every integer $n \geq 4$, an infinite parametric family of pairs of polynomials $(f_{t,c}^{(n)}, g_{t,c}^{(n)})$ in $\mathcal{PI}(n)$ where c runs through 1 and an infinite set of primes and t runs through an infinite set of primes, with the following properties:

(5.4)
$$\begin{cases} f_{t,c}^{(n)}, g_{t,c}^{(n)} \text{ have leading coefficient } c \text{ and are properly nonmonic if } c > 1; \\ f_{t,c}^{(n)}, g_{t,c}^{(n)} \text{ are Hermite equivalent but not } \mathrm{GL}_2(\mathbb{Z})\text{-equivalent.} \end{cases}$$

In fact, the polynomials $f_{t,c}^{(n)}$ and $g_{t,c}^{(n)}$ will be such that if we fix n and c and let $t \to \infty$ then the absolute values of the discriminants of $f_{t,c}^{(n)}$ and $g_{t,c}^{(n)}$ tend to ∞. Since Hermite equivalent polynomials have the same discriminant by Corollary 2.6, the pairs $(f_{t,c}^{(n)}, g_{t,c}^{(n)})$ lie in infinitely many different Hermite equivalence classes.

5.5.1. *Construction of the polynomials $f_{t,c}^{(n)}$ and $g_{t,c}^{(n)}$.* Consider the formal power series in X,

$$C(X) = \frac{1-\sqrt{1-4X}}{2X} = (2X)^{-1}\left(1 - \sum_{i=0}^{\infty} \binom{1/2}{i}(-4X)^i\right) = \sum_{i=0}^{\infty} C_i X^i \tag{5.5}$$

where

$$C_i = \frac{1}{i+1} \cdot \binom{2i}{i}.$$

Recall that C_i is the ith *Catalan number* and is an integer for each i (see, e.g., Stanley [42]). Next, let $n \geq 4$ be an integer, and let $a^{(n)}(X)$ the $(n-2)$th partial sum of $C(X)$, i.e., let

$$a^{(n)}(X) = \sum_{i=0}^{n-2} C_i \cdot X^i \in \mathbb{Z}[X].$$

Since $C(X)$ satisfies the equation

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

the coefficients of X^k $(k = 0, \dots, n-2)$ in $X \cdot (a^{(n)}(X))^2$ and in $a^{(n)}(X) - 1$ are the same. Thus, as polynomials in $\mathbb{Z}[X]$,

$$X^{n-1} \mid X \cdot (a^{(n)}(X))^2 - a^{(n)}(X) + 1. \tag{5.6}$$

Let

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

By (5.6), $b^{(n)}(X)$ is a polynomial in $\mathbb{Z}[X]$ of degree $n-2$. Then, substituting $X - X^2$ for X in (5.5) we obtain

$$C(X - X^2) = \frac{1 - \sqrt{(1-2X)^2}}{2(X - X^2)} = \frac{1}{1 - X}.$$

Using again the fact that the coefficients of X^k $(k = 0, \dots, n-2)$ in $(1-X) \cdot a^{(n)}(X - X^2)$ and in $(1-X) \cdot C(X - X^2) = 1$ are the same, we find that

$$X^{n-1} \mid (1 - X) \cdot a^{(n)}(X - X^2) - 1. \tag{5.7}$$

Let

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

By (5.7), $h^{(n)}(X)$ and $k^{(n)}(X)$ are polynomials in $\mathbb{Z}[X]$ of degree $n-2$. It is easy to check that

$$(X - X^2) \cdot a^{(n)}(X - X^2) = X + h^{(n)}(X) \cdot X^n, \tag{5.8}$$

$$b^{(n)}(X - X^2) = -h^{(n)}(X) \cdot k^{(n)}(X). \tag{5.9}$$

Now, let c be either 1 or a prime, and let t be a prime different from c. Define the polynomials

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

Notice that, by (5.8) and (5.9),

$$\widetilde{g_{t,c}^{(n)}}(X - X^2) = \widetilde{f_{t,c}^{(n)}}(X) \cdot \widetilde{f_{t,c}^{(n)}}(1 - X). \tag{5.10}$$

Subsequently, define the polynomials

$$f_{t,c}^{(n)}(X) := c^{1-n}\widetilde{f_{t,c}^{(n)}}(cX) = cX^n + t \cdot k^{(n)}(cX), \tag{5.11}$$

$$g_{t,c}^{(n)}(X) := c^{1-n}\widetilde{g_{t,c}^{(n)}}(cX) = cX^n + t(1 - 2cXa^{(n)}(cX)) + c^{n-1}t^2 \cdot b^{(n)}(cX). \tag{5.12}$$

5.5.2. *Verifying primitivity and irreducibility.* From the definitions it is clear that both $f_{t,c}^{(n)}$, $g_{t,c}^{(n)}$ are polynomials in $\mathbb{Z}[X]$ of degree n and leading coefficient c. Next, since $k^{(n)}(0) = 1$, the constant term of $f_{t,c}^{(n)}$ is t. So $f_{t,c}^{(n)}$ is primitive. Furthermore, by Eisenstein's criterion applied at the prime t, we see that $f_{t,c}^{(n)}$ is irreducible. The constant term of $g_{t,c}^{(n)}$ is t mod $c^{n-1}t^2$, so $g_{t,c}^{(n)}$ is also primitive, and once again Eisenstein's criterion implies that it is also irreducible.

LEMMA 5.4. *The polynomials $f_{t,c}^{(n)}$ and $g_{t,c}^{(n)}$ are the minimal polynomials of algebraic numbers α and β, respectively, such that $\beta = \alpha - c\alpha^2$. Further, $p_{t,c}^{(n)}(\beta) = \alpha$, where*

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

Proof. The polynomials $f_{t,c}^{(n)}$ and $g_{t,c}^{(n)}$ are primitive and irreducible, so they are the minimal polynomials of certain algebraic numbers. Choose a zero α of $f_{t,c}^{(n)}$, and put $\beta := \alpha - c\alpha^2$. Note that $\widetilde{f_{t,c}^{(n)}}(c\alpha) = 0$, so by (5.10) we have $\widetilde{g_{t,c}^{(n)}}(c\alpha - (c\alpha)^2) = 0$. This implies $g_{t,c}^{(n)}(\beta) = 0$. This proves the first claim.

As for the second claim, by (5.8), (5.9), and (5.11) we have

$$\begin{aligned} p_{t,c}^{(n)}(X - cX^2) &= c^{-1}(cX - (cX)^2)a^{(n)}(cX - (cX)^2) - c^{n-2}tb^{(n)}(cX - (cX)^2) \\ &= X + c^{n-1}h^{(n)}(cX)X^n + c^{n-2}th^{(n)}(cX) \cdot k^{(n)}(cX) \\ &= X + c^{n-2}h^{(n)}(cX)f_{t,c}^{(n)}(X), \end{aligned}$$

and by substituting $X = \alpha$ we get $p_{t,c}^{(n)}(\beta) = \alpha$. ∎

We note that the discriminants of $f_{t,c}^{(n)}$ and $g_{t,c}^{(n)}$ are polynomials in t and c that for any fixed value of c tend to ∞ with t.

5.5.3. *Verifying Hermite equivalence.* We next show that $f_{t,c}^{(n)}$ and $g_{t,c}^{(n)}$ are Hermite equivalent. We first prove a preparatory lemma.

LEMMA 5.5. *Take $f \in \mathcal{PI}(n)$ with leading coefficient c, and let $\gamma \in K_f$ be a root of f. Further, take $s \in \mathbb{Z}[X]$, and let $p(X) = Xs(cX)$. Then $p(\gamma)^k \in I_f(n-1) = \mathbb{Z}\langle 1, \gamma, \ldots, \gamma^{n-1}\rangle$ for each $k = 0, \ldots, n-1$.*

Proof. Let $\widetilde{f}(X) := c^{n-1}f(c^{-1}X)$. Then $\widetilde{f}$ is monic and in $\mathbb{Z}[X]$. Let $i \geq n$. Then there exist polynomials $\widetilde{q}, \widetilde{r} \in \mathbb{Z}[X]$ such that $X^i = \widetilde{q}(X)\widetilde{f}(X) + \widetilde{r}(X)$, where the degree of $\widetilde{r}$ is less than n. By substituting cX for X and then dividing by c^{n-1} we find that there exist $q, r \in \mathbb{Z}[X]$ such that $c^{i-n+1}X^i = q(X) \cdot f(X) + r(X)$, where the degree of r is less than n. This implies that $c^{i-n+1}\gamma^i \in I_f(n-1)$ for every integer $i \geq n$.

Let $k \in \{0, \ldots, n-1\}$. Observe that c^i divides the coefficient of X^i in $(c \cdot p(X))^k$. Therefore if $k < n$ and $i \geq n$, then c^{i-k} divides the coefficient of X^i in $p(X)^k$. It follows that $p(\gamma)^k$ is a $\mathbb{Z}$-linear combination of $1, \gamma, \ldots, \gamma^{n-1}$ and $c^{i-n+1}\gamma^i$ for $i \geq n$. Hence $p(\gamma)^k \in I_f(n-1)$. ∎

PROPOSITION 5.6. *Let $n \geq 3$. Then $f_{t,c}^{(n)}$ and $g_{t,c}^{(n)}$ are Hermite equivalent.*

Proof. For short, we write $f = f_{t,c}^{(n)}$ and $g = g_{t,c}^{(n)}$. By Lemma 5.4, $\beta = \alpha - c\alpha^2$ is a zero of g. In view of Theorem 3.10, it suffices to show that the $\mathbb{Z}$-modules $I_f(n-1) = \mathbb{Z}\langle 1, \alpha, \ldots, \alpha^{n-1}\rangle$ and $I_g(n-1) = \mathbb{Z}\langle 1, \beta, \ldots, \beta^{n-1}\rangle$ coincide.

From Lemma 5.5 with $p(X) = X - cX^2 = X(1-cX)$, it follows that $1, \beta, \ldots, \beta^{n-1} \in I_f(n-1)$, so $I_g(n-1) \subseteq I_f(n-1)$. For the other direction, we apply Lemma 5.5 with f replaced by g and with $p = p_{t,c}^{(n)} + c^{n-2}tb^{(n)}(0)$. Notice that $p(X)/X$ is of the form $s(cX)$ with $s \in \mathbb{Z}[X]$. It follows that $p(\beta)^k \in I_g(n-1)$ for $k = 0, \ldots, n-1$. By Lemma 5.4 we have $p(\beta) = \alpha + c^{n-2}tb^{(n)}(0)$. Thus, $\alpha^k \in I_g(n-1)$ for $k = 0, \ldots, n-1$, so $I_f(n-1) \subseteq I_g(n-1)$. ∎

5.5.4. *Verifying (proper non)monicity.* Clearly, if $c = 1$, then both $f_{t,c}^{(n)}$ and $g_{t,c}^{(n)}$ are monic. We now show that if $c \neq 1$ and $n \geq 4$, then for an appropriate choice of t and c, $f_{t,c}^{(n)}$ and $g_{t,c}^{(n)}$ are properly nonmonic.

Take c to be prime with $c \equiv 1 \pmod{n}$, and consider the subgroup of $\mathbb{F}_c^* = (\mathbb{Z}/c\mathbb{Z})^*$ given by

$$S_{n,c} = \{\pm r^n : r \in \mathbb{F}_c^*\}.$$

Since $c \equiv 1 \pmod{n}$ and $n \geq 4$, the order of $S_{n,c}$ is at most $2(c-1)/n < c-1$ (it contains up to sign all powers of g^n, where g is a primitive root modulo c), so it is a proper subgroup of $\mathbb{F}_c^*$.

LEMMA 5.7. *Assume that $n \geq 4$, let c be a prime with $c \equiv 1 \pmod{n}$, and let t be a prime different from c with $t \pmod{c} \notin S_{n,c}$. Then $f_{t,c}^{(n)}$ and $g_{t,c}^{(n)}$ are properly nonmonic.*

Proof. Let $\left(\begin{smallmatrix} a & b \\ d & e \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$ be any element, and consider the polynomial $\pm(dX+e)^n f_{t,c}^{(n)}\left(\frac{aX+b}{dX+e}\right)$ given by translating $f_{t,c}^{(n)}$ by $\left(\begin{smallmatrix} a & b \\ d & e \end{smallmatrix}\right)$ (up to sign). The leading coefficient of this polynomial is $\pm F(a,d)$, where $F(X,Y) =$

$Y^n f_{t,c}^{(n)}(X/Y)$ is the homogenization of f. We have

$$F(a,d) \equiv t \cdot d^n \not\equiv \pm 1 \pmod{c}.$$

Hence $f_{t,c}^{(n)}$ is properly nonmonic. The same argument shows that $g_{t,c}^{(n)}$ is properly nonmonic. ∎

5.5.5. *Verifying* $\mathrm{GL}_2(\mathbb{Z})$*-inequivalence.* We now prove that, for every integer $n \geq 4$, there exist infinitely many parameters c, t satisfying the conditions from Lemma 5.7 such that $f_{t,c}^{(n)}$ and $g_{t,c}^{(n)}$ are not $\mathrm{GL}_2(\mathbb{Z})$-equivalent. We need some preparatory lemmas.

LEMMA 5.8. *Let $n \geq 4$ be an integer. Then the polynomial $k^{(n)}$ is irreducible.*

Proof. We checked by computer the irreducibility of $k^{(n)}$ for $4 \leq n \leq 38$, so in the course of the proof we may assume that $n \geq 39$. The proof consists of two steps: we first show that either $k^{(n)}$ is irreducible or it has a rational root, and second that $k^{(n)}$ cannot have a rational root.

STEP 1. In this step, we use an argument based on Newton polygons. To set up this argument, we first show that the polynomials $k^{(n)}$ satisfy the recursive equation

$$(X-1) \cdot k^{(n+1)}(X) + k^{(n)}(X) = C_{n-1} \cdot X^n. \tag{5.13}$$

To prove (5.13), let $n \geq 2$, and recall that $k^{(n)}(X) = -h^{(n)}(1-X)$. It therefore suffices to prove the recursive equation

$$X \cdot h^{(n+1)}(X) - h^{(n)}(X) = C_{n-1} \cdot (1-X)^n. \tag{5.14}$$

By the definition of $h^{(n)}(X)$ we have

$$\begin{aligned} &X \cdot h^{(n+1)}(X) - h^{(n)}(X) \\ &\quad = X \cdot \frac{(X-X^2) \cdot a^{(n+1)}(X-X^2) - X}{X^{n+1}} - \frac{(X-X^2) \cdot a^{(n)}(X-X^2) - X}{X^n} \\ &\quad = \frac{(X-X^2) \cdot (a^{(n+1)}(X-X^2) - a^{(n)}(X-X^2))}{X^n} \\ &\quad = \frac{(X-X^2) \cdot C_{n-1} \cdot (X-X^2)^{n-1}}{X^n} = C_{n-1} \cdot (1-X)^n, \end{aligned}$$

so (5.14) holds. Now, let

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

We claim that

$$K^{(n)}(X) = k^{(n)}(X+1) \quad \text{for } n \geq 2. \tag{5.15}$$

It is straightforward to check that $K^{(2)}(X) = k^{(2)}(X+1) = 1$, $K^{(3)}(X) = k^{(3)}(X+1) = X+2$. By comparing the coefficients of X^i $(i = 0, \dots, n)$ on the left- and right-hand sides, we deduce the recursive equation

$$X \cdot K^{(n+1)}(X) + K^{(n)}(X) = C_{n-1} \cdot (X+1)^n \quad \text{for } n \geq 2.$$

Together with (5.13), this implies (5.15).

Henceforth we assume that $n \geq 39$. We now show that either $k^{(n)}$ is irreducible or it has a rational root. Of course it suffices to prove this for $K^{(n)}(X)$ instead of $k^{(n)}(X)$. We apply a theorem of Dumas (see Dumas [9, pp. 236–237] or Mott [34, Proposition 3.2]) which for convenience of the reader we recall here.

For a prime number l and an integer a, let $v_l(a)$ denote the largest integer m such that l^m divides a. Given a polynomial $f(X) = a_0X^s + a_1X^{s-1} + \cdots + a_s \in \mathbb{Z}[X]$ and a prime l, the Newton polygon $N_{f,l}$ is the lower convex hull of the points $(i, v_l(a_i))$ $(i = 0, \dots, s)$. Let $i_0 = 0 < i_1 < \cdots < i_u = s$ be the indices such that $(i_j, v_l(a_{i_j}))$ $(j = 0, \dots, u)$ are the vertices of $N_{f,l}$ and put $n_j := i_j - i_{j-1}$, $m_j := v_l(a_{i_j}) - v_l(a_{i_{j-1}})$, $d_j := \gcd(m_j, n_j)$, $w_j := n_j/d_j$ for $j = 1, \dots, u$.

Proposition 5.9 (Dumas' Irreducibility Theorem). *The degree of any nontrivial factor in $\mathbb{Z}[X]$ of $f(X)$ must be a sum of the form $\sum_{j=1}^{u} t_j w_j$, where $t_j \in \mathbb{Z}$ and $0 \leq t_j \leq d_j$, for $j = 1, \dots, u$.*

Let p and q be prime numbers for which $n < p < \frac{6n}{5}$ and $\frac{6n}{5} < q < \frac{36n}{25}$. By the results of Nagura [36], such primes exist for $n > 24$. Let a_i denote the coefficient of X^i in $K^{(n)}$. It is easy to calculate the l-adic valuation $v_l(a_i)$ of a_i for $l \in \{p, q\}$. The properties of p and q imply that for $l \in \{p, q\}$ we have

$$v_l(C_{n-1}) = 1, \quad v_l\left(\binom{n}{i} \cdot (n-1-i) \cdot (n-i)\right) = 0 \quad \text{for } i = 0, \dots, n-2.$$

Thus, for $l \in \{p, q\}$ we have $v_l(a_i) = 0$ if $n - 1 + i = l$ or $n + i = l$, and $v_l(a_i) = 1$ otherwise. With these observations, one easily verifies that the Newton polygon $N_{K^{(n)},l}$ consists of three edges connecting the points

$$(0, 1), \qquad (l-n, 0), \qquad (l-n+1, 0), \qquad (n-2, 1).$$

Proposition 5.9 now implies that for $l = p$ as well as $l = q$, the following holds: if $K^{(n)}$ factors over $\mathbb{Q}$, then it must have at most three irreducible factors of degrees which are sums of the numbers $l - n$, 1 and $2n - l - 3$. For $l = p$, we obtain the following five possibilities:

- $K^{(n)}(X)$ is irreducible;
- $K^{(n)}(X) = K_1(X) \cdot K_2(X)$, where $\deg(K_1) = p - n$ and $\deg(K_2) = 2n - p - 2$;
- $K^{(n)}(X) = K_1(X) \cdot K_2(X)$, where $\deg(K_1) = p - n + 1$ and $\deg(K_2) = 2n - p - 3$;

- $K^{(n)}(X) = K_1(X) \cdot K_2(X)$, where $\deg(K_1) = n-3$ and $\deg(K_2) = 1$;
- $K^{(n)}(X) = K_1(X) \cdot K_2(X) \cdot K_3(X)$, where $\deg(K_1) = p-n$, $\deg(K_2) = 1$, and $\deg(K_3) = 2n-p-3$.

We can conclude something similar for $l = q$, obtaining the following five possibilities:

- $K^{(n)}(X)$ is irreducible;
- $K^{(n)}(X) = K_1^*(X) \cdot K_2^*(X)$, where $\deg(K_1^*) = q-n$ and $\deg(K_2^*) = 2n-q-2$;
- $K^{(n)}(X) = K_1^*(X) \cdot K_2^*(X)$, where $\deg(K_1^*) = q-n+1$ and $\deg(K_2^*) = 2n-q-3$;
- $K^{(n)}(X) = K_1(X) \cdot K_2(X)$, where $\deg(K_1) = n-3$ and $\deg(K_2) = 1$;
- $K^{(n)}(X) = K_1^*(X) \cdot K_2^*(X) \cdot K_3^*(X)$, where $\deg(K_1^*) = q-n$, $\deg(K_2^*) = 1$, and $\deg(K_3^*) = 2n-q-3$.

Since $p < q$ and $p+q < \frac{6n}{5} + \frac{36n}{25} < 3n-4$ for $n \geq 39$, we see that

$$p-n \neq 2n-q-2, \quad p-n+1 \neq 2n-q-2,$$
$$p-n \neq 2n-q-3, \quad p-n+1 \neq 2n-q-3.$$

Therefore, the second and the third possibilities above cannot be true, which means that $K^{(n)}(X)$, and so $k^{(n)}(X)$, either is irreducible or has a rational root.

Step 2. In this step, we prove that $k^{(n)}$ does not have a rational root; consequently, by the result of Step 1, it is irreducible.

We keep our assumption $n \geq 39$. Applying the recursive equation (5.13) twice in succession, we obtain the following identity relating $k^{(n+2)}$ and $k^{(n)}$:

$$(X-1)^2 \cdot k^{(n+2)}(X) = k^{(n)}(X) + C_n \cdot X^n \cdot \left(X^2 - X - \frac{C_{n-1}}{C_n} \right). \tag{5.16}$$

By the definition of the Catalan numbers, we have $\frac{C_{n-1}}{C_n} = \frac{n+1}{4n-2}$, so the roots of $X^2 - X - \frac{C_{n-1}}{C_n}$ are given by

$$\alpha_1 = \frac{1 - \sqrt{2 + \frac{3}{2n-1}}}{2} \quad \text{and} \quad \alpha_2 = \frac{1 + \sqrt{2 + \frac{3}{2n-1}}}{2}.$$

Furthermore, since $n \geq 39$, we have

$$-\frac{1}{4} < \alpha_1 < -\frac{1}{5} \quad \text{and} \quad \frac{6}{5} < \alpha_2 < \frac{5}{4}.$$

Therefore,

- if $x \leq -\frac{1}{4}$ and n is odd, then

$$C_n \cdot x^n \cdot \left(x^2 - x - \frac{C_{n-1}}{C_n} \right) < 0; \tag{5.17}$$

- if $x \leq -\frac{1}{4}$ and n is even, then

$$C_n \cdot x^n \cdot \left(x^2 - x - \frac{C_{n-1}}{C_n} \right) > 0; \tag{5.18}$$

- if $-\frac{1}{5} \leq x < 0$ and n is odd then

$$C_n \cdot x^n \cdot \left(x^2 - x - \frac{C_{n-1}}{C_n} \right) > 0; \tag{5.19}$$

- if $x > 0$ then

$$k^{(n)}(x) > 0, \tag{5.20}$$

because the coefficients of $k^{(n)}$ are all positive. This fact about the coefficients of $k^{(n)}$ is easily proven by induction: one simply divides the recursive equation (5.13) through by $X - 1$, applies the formal power series expansion $\frac{1}{1-X} = 1 + X + X^2 + \cdots$, and verifies that the coefficients of $k^{(n+1)}$ are positive if the same holds for the coefficients of $k^{(n)}$.

It is easy to check by computer that the first derivative of $k^{(39)}$ is strictly positive (e.g., its absolute minimum is strictly positive), so $k^{(39)}$ is monotonically increasing. Since $k^{(39)}(-1/4) < 0$ and $k^{(39)}(-1/5) > 0$, we deduce that

- if $x \leq -1/4$, then $k^{(39)}(x) < 0$;
- if $-1/5 \leq x$, then $k^{(39)}(x) > 0$.

Therefore, by (5.16), (5.17), (5.19) and (5.20) the same is true for every odd integer $n > 39$:

- if $x \leq -1/4$ and n is odd, then $k^{(n)}(x) < 0$;
- if $-1/5 \leq x$ and n is odd, then $k^{(n)}(x) > 0$.

On the other hand, it is easy to check that $k^{(4)}(x)$ is strictly positive, so by (5.16),(5.18), and (5.20):

- if $x \leq -1/4$ and n is even, then $k^{(n)}(x) > 0$;
- if $0 \leq x$ and n is even, then $k^{(n)}(x) > 0$.

It remains to handle the interval $-1/5 \leq x < 0$. For this, we can use the fact that if n is even, then $k^{(n+1)}(x) > 0$ and so by (5.13), we have

$$k^{(n)}(x) = C_{n-1} \cdot x^n + (1 - x) \cdot k^{(n+1)}(x) > 0.$$

It follows that if $n \geq 39$, then all real roots of $k^{(n)}$ are strictly between $-1/4$ and $-1/5$. However, the coefficients of $k^{(n)}$ are all positive integers, and its constant term is 1, so all rational roots are of the form $-1/d$, where d divides the leading coefficient. As there are no such numbers strictly between $-1/4$ and $-1/5$, $k^{(n)}$ has no rational roots. Therefore, $k^{(n)}$ is irreducible for any $n \geq 4$. ∎

LEMMA 5.10. *Let $n \geq 4$ be an integer. Then there exist infinitely many primes p such that $k^{(n)}$ has no root modulo p.*

Proof. A well-known consequence of Chebotarev's density theorem or Frobenius' density theorem for primes asserts that if $f \in \mathbb{Z}[X]$ is irreducible, then there are infinitely many primes p modulo which f has no roots; see for instance Lenstra and Stevenhagen [43] and Serre [39]. ∎

PROPOSITION 5.11. *Let $n \geq 4$ be an integer, let $p > C_{n-1}$ be a prime such that $k^{(n+1)}$ has no root modulo p, and let c be either 1 or a prime and t a prime such that*

$$c \equiv 1 \pmod{p} \quad \text{and} \quad t \equiv -C_{n-1}^{-1} \pmod{p}. \tag{5.21}$$

Then $f_{t,c}^{(n)}$ and $g_{t,c}^{(n)}$ are not $\mathrm{GL}_2(\mathbb{Z})$-equivalent.

Proof. By Lemma 5.4 we may write

$$\begin{aligned} f_{t,c}^{(n)}(X) &= c\prod_{i=1}^{n}(X-\alpha_i), \\ g_{t,c}^{(n)}(X) &= c\prod_{i=1}^{n}(X-\beta_i), \qquad \text{where } \beta_i = \alpha_i - c\alpha_i^2 \text{ for } i = 1,\dots,n. \end{aligned} \tag{5.22}$$

Assume that $f_{t,c}^{(n)}$ and $g_{t,c}^{(n)}$ are $\mathrm{GL}_2(\mathbb{Z})$-equivalent. Then there is $\left(\begin{smallmatrix} a & b \\ d & e \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$ such that

$$\begin{aligned} g_{t,c}^{(n)}(X) &= \pm(dX+e)^n f_{t,c}^{(n)}\left(\frac{aX+b}{dX+e}\right) \\ &= \pm c\prod_{i=1}^{n}(a-\alpha_i d)\cdot\prod_{i=1}^{n}\left(X+\frac{b-\alpha_i e}{a-\alpha_i d}\right). \end{aligned}$$

This implies that $\pm\prod_{i=1}^{n}(a-\alpha_i d) = 1$ and that the sets

$$\{\beta_1,\beta_2,\dots,\beta_n\} \quad \text{and} \quad \left\{-\frac{b-\alpha_1 e}{a-\alpha_1 d}, -\frac{b-\alpha_2 e}{a-\alpha_2 d},\dots,-\frac{b-\alpha_n e}{a-\alpha_n d}\right\},$$

both of which have order n, coincide.

We now split into two cases. The first case is

$$\beta_1 = \alpha_1 - c\alpha_1^2 = -\frac{b-\alpha_1 e}{a-\alpha_1 d},$$

and the other case is that

$$\beta_1 = \alpha_1 - c\alpha_1^2 = -\frac{b-\alpha_j e}{a-\alpha_j d}$$

for some $j \neq 1$. In the first case, we have

$$-cd\alpha_1^3 + (ac+d)\alpha_1^2 + (-a+e)\alpha_1 - b = 0.$$

But α_1 is of degree $n > 3$, so the coefficients of $1, \alpha_1, \alpha_1^2, \alpha_1^3$ above are 0. This implies that $a = b = d = e = 0$, which is a contradiction, so this case is not possible.

The second case is more complicated. In this case, we have

$$(\alpha_1 - c\alpha_1^2) \cdot (a - \alpha_j d) = \alpha_j e - b \tag{5.23}$$

for some $j \neq 1$. By using identity (5.13) and the conditions (5.21), we obtain

$$f_{t,c}^{(n)}(X) \equiv X^n - \frac{1}{C_{n-1}} \cdot k^{(n)}(X) \equiv \frac{X-1}{C_{n-1}} \cdot k^{(n+1)}(X) \pmod{p} \tag{5.24}$$

So 1 is a root of $f_{t,c}^{(n)}(X)$ modulo p. But then from (5.22) it follows that

$$\prod_{i=1}^{n}(1 - \alpha_i) \equiv 0 \pmod{p}. \tag{5.25}$$

Let $\mathfrak{p}$ be an arbitrary prime ideal divisor of p in the splitting field L of $f_{t,c}^{(n)}$. It follows from (5.25) that $1 - \alpha_k \equiv 0 \pmod{\mathfrak{p}}$ for some k with $1 \leq k \leq n$. There exists $\varphi \in \mathrm{Gal}(L/\mathbb{Q})$ for which $\varphi(\alpha_k) = \alpha_1$; let $\mathfrak{p}_1 = \varphi(\mathfrak{p})$ be the corresponding prime ideal of L. Then $1 - \alpha_1 \equiv 0 \pmod{\mathfrak{p}_1}$, and combining this with (5.24) and (5.22) yields

$$k^{(n+1)}(X) \equiv C_{n-1} \cdot c \prod_{i=2}^{n}(X - \alpha_i) \pmod{\mathfrak{p}_1}. \tag{5.26}$$

However, $c \equiv 1 \pmod{\mathfrak{p}_1}$, so by (5.23) we know that

$$\alpha_j e - b \equiv 0 \pmod{\mathfrak{p}_1}. \tag{5.27}$$

Now, $\mathfrak{p}_1 \nmid e$, for otherwise $\mathfrak{p}_1 \mid b$, which would contradict $ae - bd = \pm 1$. Thus $p \nmid e$; let e^{-1} denote the inverse of e in $\mathbb{Z}/p\mathbb{Z}$. Then (5.27) gives $\alpha_j \equiv e^{-1}b \pmod{\mathfrak{p}_1}$, and by substituting this into (5.26) we find that $k^{(n+1)}(e^{-1}b) \equiv 0 \pmod{\mathfrak{p}_1}$. Taking norms with respect to $L/\mathbb{Q}$, we infer that $k^{(n+1)}(e^{-1}b) \equiv 0 \pmod{p}$, contradicting the choice of p. Therefore, the second case is not possible either, and we conclude that $f_{t,c}^{(n)}$ and $g_{t,c}^{(n)}$ are not $\mathrm{GL}_2(\mathbb{Z})$-equivalent. ∎

Finally, upon combining Lemma 5.7, Proposition 5.6, and Proposition 5.11, we obtain the following result:

THEOREM 5.12. *Let $n \geq 4$ be an integer, and let p be a prime with $p > C_{n-1} = \frac{1}{n} \cdot \binom{2n-2}{n-1}$ such that $k^{(n+1)}$ has no root modulo p. Further, let c be either 1 or a prime, and let t be any prime with*

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

Then the polynomials $f_{t,c}^{(n)}$ and $g_{t,c}^{(n)}$ given respectively by (5.11) *and* (5.12) *lie in $\mathcal{PI}(n)$ and satisfy the following properties:*

(i) $f_{t,c}^{(n)}$, $g_{t,c}^{(n)}$ *have leading coefficient* c *and are properly nonmonic if* $c > 1$*;*
(ii) $f_{t,c}^{(n)}$, $g_{t,c}^{(n)}$ *are Hermite equivalent but not* $\mathrm{GL}_2(\mathbb{Z})$*-equivalent.*

REMARK 5.13. Note that, by Dirichlet's theorem on primes in arithmetic progressions, for given n there are infinitely many choices for c as in the statement of Theorem 5.12, and further that for given n, c there are infinitely many choices for t.

If we fix n, c and let $t \to \infty$, then the absolute value of the discriminant of $f_{t,c}^{(n)}$ tends to ∞, and thus the pairs $f_{t,c}^{(n)}$, $g_{t,c}^{(n)}$ run through infinitely many different Hermite equivalence classes.

Acknowledgements. We are very grateful to the anonymous referee, who very carefully scrutinized our paper and corrected some errors.

The research of the first-named author was supported by a Simons Investigator Grant and NSF grant DMS-1001828. The research of the third-named author was supported in part by Grants K115479 and K128088 from the Hungarian National Foundation for Scientific Research (OTKA) and from the Austrian-Hungarian joint project ANN130909 (FWF-NKFIH). The research of the fourth named author was supported in part by the project EFOP-3.6.1-16-2016-00022 co-financed by the European Union and the European Social Fund. The research of the fifth-named author was supported by the NSF Graduate Research Fellowship.

References

[1] M. A. Bennett, *On the representation of unity by binary cubic forms*, Trans. Amer. Math. Soc. 353 (2001), 1507–1534.
[2] A. Bérczes, J.-H. Evertse, and K. Győry, *Multiply monogenic orders*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (5) 12 (2013), 467–497.
[3] M. Bhargava, *Higher composition laws. III. The parametrization of quartic rings*, Ann. of Math. (2) 159 (2004), 1329–1360.
[4] M. Bhargava, *On the number of monogenizations of a quartic order* (with an appendix by S. Akhtari), Publ. Math. Debrecen 100 (2022), 513–531.
[5] Y. Bilu, I. Gaál, and K. Győry, *Index form equations in sextic fields: a hard computation* Acta Arith. 115 (2004), 85–96.
[6] B. J. Birch and J. R. Merriman, *Finiteness theorems for binary forms with given discriminant*, Proc. London Math. Soc. (3), 24 (1972), 385–394.
[7] B. Delaunay, *Über die Darstellung der Zahlen durch die binären kubischen Formen von negativer Diskriminante*, Math. Z. 31 (1930), 1–26.
[8] B. N. Delone and D. K. Faddeev, *The Theory of Irrationalities of the Third Degree*, Transl. Math. Monogr. 10, Amer. Math. Soc., Providence, R.I., 1964.
[9] G. Dumas, *Sur quelques cas d'irreductibilité des polynomes à coefficients rationnels*, J. Math. Pures Appl. (6), 2 (1906), 191–258.
[10] M. Emerton, *Does (the ideal class of) the different of a number field have a canonical square root?* https://mathoverflow.net/q/52815 (2011).

[11] J.-H. Evertse, *A survey on monogenic orders*, Publ. Math. Debrecen 79 (2011), 411–422.

[12] J.-H. Evertse and K. Győry, *Effective finiteness results for binary forms with given discriminant*, Compos. Math. 79 (1991), 169–204.

[13] J.-H. Evertse and K. Győry, *Discriminant Equations in Diophantine Number Theory*, New Math. Monogr. 32, Cambridge Univ. Press, Cambridge, 2017.

[14] I. Gaál, *Diophantine Equations and Power Integral Bases, Theory and Algorithms*, Birkhäuser/Springer, Cham, 2019, 2nd ed. of [MR1896601].

[15] I. Gaál and K. Győry, *Index form equations in quintic fields*, Acta Arith. 89 (1999), 379–396.

[16] C. F. Gauss, *Disquisitiones arithmeticae*, Yale Univ. Press, New Haven, CN, 1966; translated into English by A. A. Clarke, SJ.

[17] K. Győry, *Sur les polynômes à coefficients entiers et de discriminant donné*, Acta Arith. 23 (1973), 419–426.

[18] K. Győry, *Sur les polynômes à coefficients entiers et de discriminant donné. II*, Publ. Math. Debrecen 21 (1974), 125–144.

[19] K. Győry, *Sur les polynômes à coefficients entiers et de discriminant donné. III*, Publ. Math. Debrecen 23 (1976), 141–165.

[20] K. Győry, *On polynomials with integer coefficients and given discriminant. IV*, Publ. Math. Debrecen 25 (1978), 155–167.

[21] K. Győry, *On polynomials with integer coefficients and given discriminant. V,* $\mathfrak{p}$*-adic generalizations*, Acta Math. Acad. Sci. Hungar. 32 (1978), 175–190.

[22] K. Győry, *Corps de nombres algébriques d'anneau d'entiers monogène*, in: Séminaire Delange–Pisot–Poitou, 20e année: 1978/1979, Théorie des nombres, Fasc. 2, exp. 26, 7 pp., Secrétariat Math., Paris, 1980.

[23] K. Győry, *Upper bounds for the degrees of decomposable forms of given discriminant*, Acta Arith. 66 (1994), 261–268.

[24] K. Győry, *Bounds for the solutions of decomposable form equations*, Publ. Math. Debrecen 52 (1998), 1–31.

[25] K. Győry, *Discriminant form and index form equations*, in: Algebraic Number Theory and Diophantine Analysis (Graz, 1998), de Gruyter, Berlin, 2000, 191–214.

[26] E. Hecke, *Lectures on the Theory of Algebraic Numbers*, Grad. Texts in Math. 77, Springer, New York, 1981.

[27] C. Hermite, *Note sur la réduction des fonctions homogènes à coefficients entiers et à deux indéterminées*, J. Reine Angew. Math. 36 (1848), 357–364.

[28] C. Hermite, *Sur l'introduction des variables continues dans la théorie des nombres*, J. Reine Angew. Math. 41 (1851), 191–216.

[29] C. Hermite, *Sur la théorie des formes quadratiques. Premier mémoire*, J. Reine Angew. Math. 47 (1854), 313–342.

[30] C. Hermite, *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 (1857), 182–192.

[31] G. Julia, *Étude sur les formes binaires non quadratiques à indéterminées réelles, ou complexes, ou à indéterminées conjuguées*. Thèse, Faculté des Sciences de Paris, 1917, 300 pp.

[32] L.-C. Kappe and B. Warren, *An elementary test for the Galois group of a quartic polynomial*, Amer. Math. Monthly 96 (1989), 133–137.

[33] J.-L. Lagrange, *Recherches d'arithmétique*, Nouv. Mém. Acad. Berlin 1773 et 1775; Oeuvres III (1773), 695–758.

[34] J. L. Mott, *Eisenstein-type irreducibility criteria*, in: Zero-Dimensional Commutative Rings (Knoxville, TN, 1994), Lecture Notes in Pure Appl. Math. 171, Dekker, New York, 1995, 307–329.
[35] T. Nagell, *Zur Theorie der kubischen Irrationalitäten*, Acta Math. 55 (1930), 33–65.
[36] J. Nagura, *On the interval containing at least one prime number*, Proc. Japan Acad. 28 (1952), 177–181.
[37] J. Nakagawa, *Binary forms and orders of algebraic number fields*, Invent. Math. 97 (1989), 219–235.
[38] W. Narkiewicz, *The Story of Algebraic Numbers in the First Half of the 20th Century: From Hilbert to Tate*, Springer Monogr. Math., Springer, Cham, 2018.
[39] J.-P. Serre, *On a theorem of Jordan*, Bull. Amer. Math. Soc. (N.S.) 40 (2003), 429–440.
[40] D. Simon, *La classe invariante d'une forme binaire*, C. R. Math. Acad. Sci. Paris 336 (2003), 7–10.
[41] D. Simon, *A "class group" obstruction for the equation* $Cy^d = F(x, z)$, J. Théor. Nombres Bordeaux 20 (2008), 811–828.
[42] R. P. Stanley, *Catalan Numbers*, Cambridge Univ. Press, New York, 2015.
[43] P. Stevenhagen and H. W. Lenstra, Jr. *Chebotarëv and his density theorem*, Math. Intelligencer 18 (1996), 26–37.
[44] M. M. Wood, *Rings and ideals parameterized by binary n-ic forms*, J. London Math. Soc. (2), 83 (2011), 208–231.
[45] M. M. Wood, *Quartic rings associated to binary quartic forms*, Int. Math. Res. Notices 2012, 1300–1320.

Manjul Bhargava
Department of Mathematics
Princeton University
Princeton, NJ 08540, USA
E-mail: bhargava@math.princeton.edu

Kálmán Győry, László Remete
Institute of Mathematics
University of Debrecen
H-4002 Debrecen, Hungary
E-mail: gyory@science.unideb.hu
remete.laszlo@science.unideb.hu

Jan-Hendrik Evertse
Department of Mathematics
Leiden University
Leiden, the Netherlands
E-mail: evertse@math.leidenuniv.nl

Ashvin A. Swaminathan
Department of Mathematics
Harvard University
Cambridge, MA 02138, USA
E-mail: ashvins@alumni.princeton.edu