Number of integers represented by families of binary forms III: fewnomials

Étienne Fouvry & Michel Waldschmidt

To János Pintz for his Seventy Fifth Birthday.

Abstract. In a series of papers we investigated the following question: given a family $\mathcal{F}$ of binary forms having nonzero discriminant and integer coefficients, for each $d \geqslant 3$, we estimate the number of integers m with $|m| \leqslant N$ which are represented by an element in $\mathcal{F}$ of degree $\geqslant d$. Under suitable assumptions, asymptotically as $N \to \infty$, the main term in the estimate is given by the forms in $\mathcal{F}$ having degree d (if any), while the forms of degree $> d$ contribute only to the error term. The present text is devoted to fewnomials

$$a_0 X^{kr} + a_1 X^{k(r-1)} Y^k + \cdots + a_{r-1} X^k Y^{k(r-1)} + a_r Y^{kr}$$

with fixed $r \geqslant 1$ and varying $k, a_0, a_1, \ldots, a_r$.

Mathematics Subject Classification: Primary 11E76; Secondary 11D45 11D85.

Key words and phrases: Representation of integers by fewnomials, Families of Diophantine equations, Linear forms in logarithms.

1 Introduction

This is the fourth text of a series of papers devoted to the study of the set of integers which are represented by some forms belonging to a family. In the first one [FW2020] we investigated the case of the family of cyclotomic forms. In the second and third texts [FW2023, FW2024] we considered in particular families of binomial binary forms $aX^d + bY^d$, with varying a, b, d, such that a and b are of any sign and $d \geqslant 3$. We now are concerned with fewnomials

$$a_0 X^{kr} + a_1 X^{k(r-1)} Y^k + \cdots + a_{r-1} X^k Y^{k(r-1)} + a_r Y^{kr}$$

with fixed $r \geqslant 1$ and varying $k, a_0, a_1, \ldots, a_r$. Let $\mathcal{F}$ be some (suitably defined) family of such fewnomials. When $r = 1$ we recognize a family of binomial forms. Like in [FW2020], [FW2023] and [FW2024], we are interested by the set of integers represented by some form of the family $\mathcal{F}$. Our method rests on a lower bound for linear forms in logarithms (see Proposition 2.3 below), on a study of the group of automorphisms of the forms in $\mathcal{F}$ and on the non existence of isomorphism exchanging two distinct forms of $\mathcal{F}$ (see Propositions 4.11 and 6.1).

The results of the present paper apply to families of trinomial binary forms

$$aX^d + cX^e Y^{d-e} + bY^d,$$

with varying rational integers a, b, c, d, e, $1 \leqslant e < d$, $abc \neq 0$ when the quotients e/d belongs to a finite set depending on the family. We will pursue the study of more general families of trinomial binary forms in a forthcoming paper [FW2026+]. We will see that the famous *Conjecture abc* has a dramatic impact on the qualities of the results. We will consider families of definite positive forms in another one [FW2026].

In order to present our results, we give a list of definitions and notations.

1.1 About general binary forms

Let $d \geqslant 3$ be an integer. For $\mathbb{K} = \mathbb{Z}$, $\mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$, let $\mathrm{Bin}(d, \mathbb{K})$ be the set of binary forms $F = F(X, Y)$ with degree d, with coefficients in $\mathbb{K}$ and with discriminant different from zero. If F belongs to $\mathrm{Bin}(d, \mathbb{K})$ and if

$$\gamma = \begin{pmatrix} u_1 & u_2 \\ u_3 & u_4 \end{pmatrix} \tag{1.1}$$

belongs to $\mathrm{GL}(2, \mathbb{K})$, we denote by $F \circ \gamma$ the binary form defined by $(F \circ \gamma)(X, Y) = F(u_1X + u_2Y, u_3X + u_4Y)$, after the associated linear change of variables. The form $F \circ \gamma$ belongs to $\mathrm{Bin}(d, \mathbb{K})$. Two forms F and G in $\mathrm{Bin}(d, \mathbb{K})$ are called $\mathbb{K}$*–isomorphic* if there exists γ in $\mathrm{GL}(2, \mathbb{K})$ such that $F \circ \gamma = G$.

If γ is such that $F \circ \gamma = F$, we say that γ is an *automorphism of* F. The set of these automorphisms is a group denoted by $\mathrm{Aut}(F, \mathbb{K})$. We have $-\mathrm{Id} \in \mathrm{Aut}(F, \mathbb{K})$ if and only if d is even.

When F belongs to $\mathrm{Bin}(d, \mathbb{Z})$ we denote by C_F the constant

$$C_F := A_F W_F, \tag{1.2}$$

attached to F. It is defined and thoroughly studied in [SX2019, Theorem 1.2]: according to [SX2019, Theorem 1.1], the number of $m \in \mathbb{Z}$ in the interval $[-N, N]$ which are represented by F is equal to

$$C_F N^{2/d} + O_F(N^{(2/d)-\kappa_d}), \tag{1.3}$$

where $\kappa_d > 0$ is an effective constant only depending on d, uniformly for $N \geqslant 1$. The constant A_F is the area of the fundamental domain attached to F:

$$A_F := \iint_{|F(x,y)| \leqslant 1} dx\, dy, \tag{1.4}$$

and W_F is a positive rational number the delicate definition of which is based on the denominators of the entries of the matrices in $\mathrm{Aut}(F, \mathbb{Q})$ (see [SX2019, Theorem 1.2]). For the purpose of our present work, we will only retain the following values of W_F

$$W_F = \begin{cases} 1 & \text{if } \mathrm{Aut}(F, \mathbb{Q}) = \{\mathrm{Id}\}, \\ 1/2 & \text{if } \mathrm{Aut}(F, \mathbb{Q}) = \{\pm \mathrm{Id}\}, \\ 1/4 & \text{if } \mathrm{Aut}(F, \mathbb{Q}) = \mathbf{D}_2, \end{cases} \tag{1.5}$$

where $\mathbf{D}_2 \subset \mathrm{GL}(2, \mathbb{Z})$ is the group with four elements

$$\mathbf{D}_2 = \left\{ \pm \mathrm{Id}, \pm \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\}.$$

Motivated by the example of forms (1.15) with even k (see below), we say that a binary form $F(X, Y)$ is a *binary form with squared arguments* when there exists a binary form H such that $F(X, Y) = H(X^2, Y^2)$. Necessarily $\deg F$ is even and $\mathrm{Aut}(F, \mathbb{Q})$ contains $\mathbf{D}_2$.

The following definitions concerns family of binary forms containing essentially distinct forms.

Definition 1.1. Let $\mathbb{K}$ as above and let $\mathcal{E}$ be a set of binary forms of any degree $d \geqslant 3$ with coefficients in $\mathbb{K}$.

1. We say that $\mathcal{E}$ is $\mathbb{K}$–*dilation–free*, if for any F, G in $\mathcal{E}$ and any u and v in $\mathbb{K}^\times$, the condition $F(uX, vY) = G(X, Y)$ implies $F = G$.

2. We say that $\mathcal{E}$ is $\mathbb{K}$–*homography–free*, if the following condition holds: For any distinct forms F and G in $\mathcal{E}$ we have the equality
$$\{\gamma \in \mathrm{GL}(2, \mathbb{K}) : F = G \circ \gamma\} = \emptyset.$$

3. A form $F \in \mathcal{E}$ is called $\mathbb{K}$–*rigid* if we have the equality
$$\mathrm{Aut}(F, \mathbb{K}) = \begin{cases} \{\lambda\,\mathrm{Id} : \lambda \in \mathbb{K},\ \lambda^{\deg F} = 1\} & \text{if } F \text{ is not a binary form} \\ & \text{with squared arguments,} \\ \displaystyle\bigcup_{\lambda \in \mathbb{K},\quad \lambda^{\deg F} = 1} & \lambda \cdot \mathbf{D}_2 \text{ otherwise.} \end{cases} \tag{1.6}$$

In section §3.3, we give examples of sets $\mathcal{E}$ which are $\mathbb{K}$–homography–free.

A set which is $\mathbb{K}$–homography–free is also $\mathbb{K}$–dilation–free. If $\mathcal{E}$ is a set which is $\mathbb{K}$–homography–free (resp. $\mathbb{K}$–dilation–free), so is any subset of $\mathcal{E}$.

From (1.6) it follows that if $F \in \mathrm{Bin}(d, \mathbb{Q})$ is a $\mathbb{Q}$–rigid form, we then have
$$\mathrm{Aut}(F, \mathbb{Q}) = \begin{cases} \{\mathrm{Id}\} & \text{if } d \text{ is odd,} \\ \{\pm\mathrm{Id}\} & \text{if } d \text{ is even} \end{cases} \text{ if } F \text{ is not a binary form with squared arguments}$$
and $\mathrm{Aut}(F, \mathbb{Q}) = \mathbf{D}_2$ otherwise. Therefore, for a $\mathbb{Q}$–rigid form F, we have
$$W_F = \begin{cases} 1/(2, d) & \text{if } F \text{ is not a binary form with squared arguments} \\ 1/4 & \text{otherwise} \end{cases} \tag{1.7}$$
by (1.5).

1.2 About family of binary forms.

Definition 1.2. Let $\mathbb{K} = \mathbb{Z}$, $\mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$. Let $\mathcal{F}$ be a set of binary forms. We say that $\mathcal{F}$ is a $\mathbb{K}$–*family of binary forms* if the two following conditions hold

- $\mathcal{F} \subset \bigcup_{d \geqslant 3} \mathrm{Bin}(d, \mathbb{K})$
- for every $d \geqslant 3$, the set $\mathcal{F} \cap \mathrm{Bin}(d, \mathbb{K})$ is finite.

For $d \geqslant 3$, set
$$\mathcal{F}_d := \mathcal{F} \cap \mathrm{Bin}(d, \mathbb{K}). \tag{1.8}$$
When the family $\mathcal{F}$ is given and when the integer d is $\geqslant 3$, the integer $d^\dagger$ is defined by the formula
$$d^\dagger := \begin{cases} \inf\{d' : d' > d \text{ such that } \mathcal{F}_{d'} \neq \emptyset\} & \text{if there exists } d' > d \text{ such that } \mathcal{F}_{d'} \neq \emptyset, \\ \infty & \text{if } \mathcal{F}_{d'} = \emptyset \text{ for all } d' > d. \end{cases}$$
When $\mathbb{K} = \mathbb{Z}$ and when $\mathcal{F}$ is fixed, we are interested in describing the value set of $\mathcal{F}$ defined as the union of all the images $F(\mathbb{Z}^2)$ for $F \in \mathcal{F}$. So we introduce the two sets
$$\mathcal{G}_{\geqslant d}(m) = \Big\{(x, y, F) \ \mid m = F(x, y) \ \text{ with } F \in \mathcal{F}, \deg F \geqslant d \\ (x, y) \in \mathbb{Z}^2 \ \text{ and } \ \max\{|x|, |y|\} \geqslant 2\Big\} \tag{1.9}$$

and

$$\mathcal{R}_{\geqslant d} = \{m \in \mathbb{Z} \mid \mathcal{G}_{\geqslant d}(m) \neq \emptyset\}.$$

The assumption $\max\{|x|, |y|\} \geqslant 2$ is natural: the coefficient $a_0 = F(1,0)$ of F is likely to take infinity many values m, some of which may be repeated infinitely often (see Remark 1.2 in [FW2024]), a situation which would yield for the modified $\mathcal{G}_{\geqslant d}(m)$ an infinite set.

For N a positive integer, we introduce

$$\mathcal{R}_{\geqslant d}(N) = \mathcal{R}_{\geqslant d} \cap [-N, N]. \tag{1.10}$$

1.3 About binary fewnomials

We firstly define a family of binary fewnomials.

Definition 1.3. Let $r \geqslant 1$ be an integer. For every $k \geqslant 3/r$ let $\mathcal{E}_k$ be a finite subset of $\mathbb{Z}^{r+1}$ such that, for every $\boldsymbol{a} = (a_0, \dots, a_r) \in \mathcal{E}_k$, one has

1. $a_0 a_r \neq 0$,
2. the discriminant of the polynomial $a_0 T^r + \cdots + a_r$, is different from zero.

For every $k \geqslant 3/r$ and for every $\boldsymbol{a} \in \mathcal{E}_k$, let $F = F_{k,\boldsymbol{a}}(X,Y)$ be the binary form

$$F_{k,\boldsymbol{a}}(X,Y) = a_0 X^{kr} + a_1 X^{k(r-1)} Y^k + \cdots + a_{r-1} X^k Y^{k(r-1)} + a_r Y^{kr}. \tag{1.11}$$

Then the set $\mathcal{F} = \mathcal{F}_{\boldsymbol{\mathcal{D}}}$ defined by

$$\mathcal{F}_{\boldsymbol{\mathcal{D}}} := \{F_{k,\boldsymbol{a}} : k \geqslant 3/r,\, \boldsymbol{a} \in \mathcal{E}_k\},$$

is called the family of *binary fewnomials attached to the data*

$$\boldsymbol{\mathcal{D}} = (r, (\mathcal{E}_k)).$$

Let $\mathcal{F}$ as in Definition 1.3. Then the degree of every $F \in \mathcal{F}$ is divisible by r and greater than 2. The discriminant of F is different from zero. We define the *height of* F by the formula.

$$\mathcal{A}(F) := \max\{|a_0|, |a_1|, \dots, |a_r|\} \tag{1.12}$$

and the modified height

$$\mathcal{A}^\star(F) := \max\{2, \mathcal{A}(F)\}$$

which naturally appears in some formulas (for instance in Corollary 2.5).

By the definition (1.8) we have the decomposition

$$\mathcal{F} = \bigcup_{k \geqslant 3/r} \mathcal{F}_{kr}.$$

The number of elements in $\mathcal{F}_d$ is less than

$$\max_{F \in \mathcal{F}_d} \left(2\,\mathcal{A}^\star(F) + 1\right)^{r+1}. \tag{1.13}$$

If F is given by (1.11), we have the equality

$$F(X,Y) = Y^{kr} h\left((X/Y)^k\right),$$

where $h(T)$ is the polynomial $a_0 T^r + \cdots + a_{r-1} T + a_r$. This point of view will be exploited in the proof of Corollary 2.5.

1.4 Some examples

Let $\mathcal{F} = \mathcal{F}_{\boldsymbol{\mathcal{D}}}$ be the family of binary fewnomials attached to the data $\boldsymbol{\mathcal{D}}$ as in Definition 1.3. The number of monomials appearing in each form $F \in \mathcal{F}_d$ is at most $r+1$. In particular, when $r = 1$, the forms $F \in \mathcal{F}_d$ are binomial binary forms

$$aX^d + bY^d, \tag{1.14}$$

(cf. [SX2019, Corollary 1.3], [FW2024]), while if $r \geqslant 2$ and if there exists s in the interval $1 \leqslant s \leqslant r-1$ such that each $\boldsymbol{a} = (a_0, a_1, \dots, a_r) \in \mathcal{E}_k$ satisfies $a_j = 0$ for $j \notin \{0, s, r\}$, then the forms $F \in \mathcal{F}_d$ are *trinomial binary forms*

$$aX^{kr} + cX^{ks}Y^{k(r-s)} + bY^{kr}.$$

For example with $r = 2$ and $s = 1$ the family that we are considering is the family of *balanced trinomial binary forms*

$$aX^{2k} + cX^kY^k + bY^{2k}. \tag{1.15}$$

These trinomial forms will be studied in [FW2026+].

As in [FW2023], [FW2024] we are interested in the asymptotic description of the set of integers which are represented by some form F of the family of binary fewnomials $\mathcal{F} = \mathcal{F}_{\boldsymbol{\mathcal{D}}}$, with a fixed $r \geqslant 2$, in particular we study the counting function

$$\sharp\mathcal{R}_{\geqslant d}(N),$$

associated to $\mathcal{F}_{\boldsymbol{\mathcal{D}}}$ (see the Definition (1.10)), where as usual $\sharp E$ the number of elements of a finite set E. Our results will require the constant $\vartheta_d\,(< 2/d)$ which is defined in [FW2023, (2.1)] by the formula:

$$\vartheta_d = \begin{cases} \dfrac{24\sqrt{3}+73}{60\sqrt{3}+73} = \dfrac{2628\sqrt{3}-1009}{5471} = 0.6475\dots & \text{for } d = 3, \\ \dfrac{2\sqrt{d}+9}{4d\sqrt{d}-6\sqrt{d}+9} & \text{for } 4 \leqslant d \leqslant 20, \\ \dfrac{1}{d-1} & \text{for } d \geqslant 21. \end{cases}$$

1.5 The main result

Recall the Definitions 1.2 for $d^\dagger$ and 1.3 for $\boldsymbol{\mathcal{D}}$ and $\mathcal{F}_{\boldsymbol{\mathcal{D}}}$, and Notations (1.2) for C_F, (1.4) for $\mathcal{A}(F)$, (1.9) for $\mathcal{G}_{\geqslant d}(m)$, (1.10) for $\mathcal{R}_{\geqslant d}(N)$.

If F is a binary form we put $A_F^* := A_F/2$ if F is a form with squared arguments, and $A_F^* := A_F$ otherwise. The next result will be proved in §2.4.

Theorem 1.4. *Let $\epsilon > 0$ and let $r \geqslant 2$ be an integer. Let $\mathcal{F} = \mathcal{F}_{\boldsymbol{\mathcal{D}}}$ be the family of binary fewnomials attached to the system of data $\boldsymbol{\mathcal{D}} = (r, (\mathcal{E}_k))$. There exists a constant $\eta > 0$ which depends only on ϵ and r with the following property. Assume that there exists $d_0 \geqslant 3$ such that, for all $d \geqslant d_0$,*

$$\max_{F \in \mathcal{F}_d} \mathcal{A}^\star(F) \leqslant \exp(\eta d/\log d). \tag{1.16}$$

Then

(a) For all $m \in \mathbb{Z} \smallsetminus \{-1, 0, 1\}$ and all $d \geqslant 3$ which is a multiple of r, the set $\mathcal{G}_{\geqslant d}(m)$ is finite. Moreover, for all $d \geqslant d_0$ which is a multiple of r and all $\epsilon > 0$, there exists a constant c depending only on r, d, ϵ such that, for $|m| \geqslant 2$,

$$\sharp\mathcal{G}_{\geqslant d}(m) \leqslant c|m|^{(1/d)+\epsilon}.$$

(b) Assume that $\mathcal{F}$ is a $\mathbb{Q}$–homography–free set. Then for all $d \geqslant 3$ which is a multiple of r, we have, for $N \to \infty$,

$$\sharp\mathcal{R}_{\geqslant d}(N) = \left(\sum_{F\in\mathcal{F}_d} C_F\right) N^{2/d} + O_{\epsilon,r,d}\Big(N^{\max\{\vartheta_d+\epsilon, 2/d^\dagger\}}\Big). \tag{1.17}$$

(c) Assume that $\mathcal{F}$ is a $\mathbb{Q}$–homography–free set of $\mathbb{Q}$–rigid forms. Then for all $d \geqslant 3$ which is a multiple of r, we have, for $N \to \infty$,

$$\sharp\mathcal{R}_{\geqslant d}(N) = \frac{1}{(d,2)}\left(\sum_{F\in\mathcal{F}_d} A_F^\star\right) N^{2/d} + O_{\epsilon,r,d}\Big(N^{\max\{\vartheta_d+\epsilon, 2/d^\dagger\}}\Big).$$

We will prove this result with $\eta = \epsilon(2^{80}3^{15}r^{4r})^{-1}$, corresponding to a value for μ given by (2.3) with $\lambda = 2 + \epsilon$.

The proof of Theorem 1.4 is given in §2: we first recall the definition of a regular family [FW2024, Definition 2.2] (Definition 2.1) and the statements of [FW2024, Theorem 2.6] and of [W2000, Corollary 9.22] (Theorems 2.2 and Proposition 2.3 respectively). These tools allow us to prove the asymptotic estimate (Theorem 2.6) which is required for checking the conditions of a regular family.

The rest of the paper is devoted to giving examples of families satisfying the assumptions of Theorem 1.4. These examples are stated in §3, Theorems 3.2 and 3.4. The main purpose of §4 is to study isomorphisms among two binary fewnomials. The technical arguments are the proofs of Propositions 4.11 and 6.1. The proofs of the Corollaries 3.6 and 3.9 are given in §5 and §6 respectively.

2 Proof of Theorem 1.4

2.1 Regular families

The next definition is Definition 2.2 of [FW2024].

Definition 2.1. An infinite family $\mathcal{F}$ of binary forms as in Definition 1.2 with coefficients in $\mathbb{Z}$ is called *regular* if the following properties are satisfied:
(i) Two forms in the family $\mathcal{F}$ are $\mathbb{Q}$–isomorphic if and only if they are equal.
(ii) There exists an integer $A > 0$ such that for all $\epsilon > 0$, there exist two positive integers $N_0 = N_0(\epsilon)$ and $d_0 = d_0(\epsilon)$ such that, for all $N \geqslant N_0$, the number of integers $m \in [-N, N]$ for which there exists $d \in \mathbb{Z}$, $(x, y) \in \mathbb{Z}^2$ and $F \in \mathcal{F}_d$ with

$$d \geqslant d_0, \quad \max\{|x|, |y|\} \geqslant A \quad \text{and} \quad F(x, y) = m$$

is at most N^ϵ.

We also borrow the following notation from [FW2024]:

$$\begin{aligned}\mathcal{R}_{\geqslant d}(\mathcal{F}, N, A) := \sharp\big\{&m : 0 \leqslant |m| \leqslant N, \text{ there is } F \in \mathcal{F} \text{ with } \deg F \geqslant d\\ &\text{and } (x, y) \in \mathbb{Z}^2 \text{ with } \max\{|x|, |y|\} \geqslant A, \text{ such that } F(x, y) = m\big\}.\end{aligned}$$

Here is the statement of [FW2024, Theorem 2.6].

Theorem 2.2. *Let $\mathcal{F}$ be a regular family of distinct binary forms in the meaning of Definition 2.1. Then for every $d \geqslant 3$ and every positive ϵ, the quantity $\mathcal{R}_{\geqslant d}(\mathcal{F}, N, A)$ satisfies*

$$\mathcal{R}_{\geqslant d}(\mathcal{F}, N, A) = \left(\sum_{F \in \mathcal{F}_d} A_F W_F \right) \cdot N^{2/d} + O_{\mathcal{F},A,d,\epsilon}\big(N^{\max\{\vartheta_d+\epsilon, 2/d^\dagger\}}\big),$$

uniformly as $N \to \infty$.

2.2 Diophantine tool

Our main tool for the proof of Theorem 1.4 is an asymptotic estimate (Theorem 2.6) which we are going to deduce from a lower bound (Proposition 2.3) arising from the theory of linear forms in logarithms, namely [W2000, Corollary 9.22].

Using the notations of [FW2024, §5], we denote by H the absolute height, by h the absolute logarithmic height and by M the Mahler's measure; for a rational number written in its irreducible form as p/q, we have

$$\mathrm{H}(p/q) = \mathrm{M}(p/q) = \max\{|p|, q\}, \qquad \mathrm{h}(p/q) = \log \max\{|p|, q\}.$$

Proposition 2.3. *Let K be a number field of degree $\leqslant D$, α_1, α_2 nonzero elements of K, b_1, b_2 positive integers, A_1, A_2, B positive real numbers. Assume, for $j = 1, 2$,*

$$B \geqslant \max\{\mathrm{e},\ b_1,\ b_2\}, \quad \log A_j \geqslant \max\left\{\frac{1}{D},\ \mathrm{h}(\alpha_j)\right\}.$$

If $\alpha_1^{b_1}\alpha_2^{b_2} \neq 1$, then

$$|\alpha_1^{b_1}\alpha_2^{b_2} - 1| \geqslant \exp\left\{-C(\log B)(\log A_1)(\log A_2)D^4 \max\{1, \log D\}\right\}$$

where $C = 2^{79}3^{15}$.

When $D = 1$, we recognize [FW2024, Proposition 5.1].

Proposition 2.3 follows from [W2000, Corollary 9.22 p. 308] with the constant $C(m)$ of [W2000, p. 252].

The next lemma gives an upper bound for the absolute logarithmic height h of an algebraic number in terms of its usual height.

Lemma 2.4. *Let θ be an algebraic number which is root of a nonzero polynomial of degree r having integer coefficients bounded by H. Then*

$$\mathrm{e}^{\mathrm{h}(\theta)} \leqslant \sqrt{r+1}H.$$

Proof. We use the results of [W2000, Chap. 3] (see the proofs and notations of Lemmas 3.10 and 3.11). For $h \in \mathbb{C}[X]$ a polynomial of degree r, the coefficients of which have moduli $\leqslant H$, we have

$$\mathrm{M}(h) \leqslant \sqrt{r+1}H.$$

If $h \in \mathbb{Z}[X]$ and if f is a factor of h in $\mathbb{Z}[X]$, we have $\mathrm{M}(h/f) \geqslant 1$, hence $\mathrm{M}(f) = \mathrm{M}(h)/\mathrm{M}(h/f) \leqslant \mathrm{M}(h)$. Further, is f is irreducible and if θ is a root of f, then

$$\mathrm{h}(\theta) = \frac{1}{[\mathbb{Q}(\theta) : \mathbb{Q}]} \log \mathrm{M}(f) \leqslant \log \mathrm{M}(f).$$

□

We consider a family $\mathcal{F} = \mathcal{F}_{\boldsymbol{\mathcal{D}}}$ of binary fewnomials attached to the data $\boldsymbol{\mathcal{D}} = (r, (\mathcal{E}_k))$ as in Definition 1.3. Let $(a_0, a_1, \dots, a_r) \in \mathcal{E}_k$ and let

$$h(t) = a_0 t^r + a_1 t^{r-1} + \cdots + a_r \in \mathbb{Z}[t]$$

be the polynomial associated with $(a_0, a_1, \dots, a_r)$. We decompose h into irreducible factors in $\mathbb{C}[t]$:

$$h(t) = a_0 \prod_{j=1}^{r} (t - \theta_j).$$

By hypothesis, $\theta_1, \dots, \theta_r$ are pairwise distinct. The degree D of the number field $\mathbb{Q}(\theta_1, \dots, \theta_r)$ satisfies $1 \leqslant D \leqslant r!$.

Let $k \geqslant 1$ and $r \geqslant 1$ be two integers such that the product $d = kr$ is $\geqslant 3$. Let

$$F(X, Y) = a_0 X^{kr} + a_1 X^{k(r-1)} Y^k + \cdots + a_{r-1} X^k Y^{k(r-1)} + a_r Y^{kr} \tag{2.1}$$

be the binary form in $\mathcal{F}_d$ given by (1.11).

Recall the Definition (1.12) of $\mathcal{A}(F)$. Thanks to Lemma 2.4, we have

$$\max_{1 \leqslant j \leqslant r} \mathrm{e}^{\mathrm{h}(\theta_j)} \leqslant \sqrt{r+1}\mathcal{A}(F).$$

The next result follows from Proposition 2.3.

Corollary 2.5. *Let x and y be in $\mathbb{Z}$. Set $\mathcal{X} := \max\{|x|, |y|\}$. Let F be as (2.1). Assume $\mathcal{X} \geqslant 2$ and $F(x, y) \neq 0$. Then*

$$|F(x, y)| \geq \max\{|a_0 x^d|, |a_r y^d|\} \exp\big\{ - C r^{4r} (\log d)(\log \mathcal{X})(\log \mathcal{A}^\star(F))\big\}$$

with the constant C of Proposition 2.3.

Proof. The case $r = 1$, $k \geqslant 3$ is [FW2024, Corollary 5.2].

When $k = 1$ and $d = r \geqslant 3$, the trivial lower bound $|F(x, y)| \geqslant 1$ gives a stronger result, since

$$\max\{|a_0 x^d|, |a_r y^d|\} \leqslant \mathcal{A}^\star(F)\mathcal{X}^d.$$

We now assume $k \geqslant 2$ and $r \geqslant 2$. We may also assume $xy \neq 0$ since the result is trivial when $xy = 0$.

Let us write

$$F(x, y) = a_0 \prod_{j=1}^{r} (x^k - \theta_j y^k).$$

By symmetry, since $a_0 a_r \neq 0$ and since $\mathrm{h}(1/\theta_j) = \mathrm{h}(\theta_j)$, we may assume $|a_0 x^d| \geqslant |a_r y^d|$. Let $j \in \{1, 2, \dots, r\}$. We first use Proposition 2.3 with

$$D = [\mathbb{Q}(\theta_j) : \mathbb{Q}] \leqslant r!, \quad b_1 = k, \quad b_2 = 1, \quad \alpha_1 = \frac{y}{x}, \quad \alpha_2 = \theta_j,$$

$$\log B = \frac{\log k}{\log 2}, \quad \log A_1 = \frac{\log \mathcal{X}}{\log 2}, \quad \log A_2 = r \log \mathcal{A}^\star(F).$$

Using Stirling's formula [Ro1955]

$$r! \leqslant r^r e^{-r} \sqrt{2\pi r}\, \mathrm{e}^{1/12r}$$

together with the upper bound

$$4\pi^2 r^5 \frac{\log r}{(\log 2)^2} \mathrm{e}^{1/3r} \leqslant \mathrm{e}^{4r}$$

for $r \geqslant 2$ we get

$$\frac{1}{(\log 2)^2} r!^4 r \log(r!) \leqslant r^{4r-1}.$$

From Proposition 2.3, we deduce

$$\left| \theta_j \left(\frac{y}{x}\right)^k - 1 \right| \geqslant \exp\big\{ - Cr^{4r-1} (\log k)(\log \mathcal{X})(\log \mathcal{A}^\star(F))\big\}$$

for $1 \leqslant j \leqslant d$. Hence

$$\prod_{j=1}^{r} \left| \theta_j \left(\frac{y}{x}\right)^k - 1 \right| \geqslant \exp\big\{ - Cr^{4r} (\log k)(\log \mathcal{X})(\log \mathcal{A}^\star(F))\big\}$$

and

$$\begin{aligned} |F(x,y)| &= |a_0 x^d| \prod_{j=1}^{r} \left| \theta_j \left(\frac{y}{x}\right)^k - 1 \right| \\ &\geq |a_0 x^d| \exp\big\{ - Cr^{4r} (\log k)(\log \mathcal{X})(\log \mathcal{A}^\star(F))\big\}. \end{aligned}$$

□

From Corollary 2.5 we deduce the lower bound

$$|F(x,y)| \geqslant \mathcal{X}^d \exp\big\{ - Cr^{4r} (\log d)(\log \mathcal{X})(\log \mathcal{A}^\star(F))\big\}$$

which we write as

$$|F(x,y)| \geqslant \mathcal{X}^{d - Cr^{4r} (\log d)(\log \mathcal{A}^\star(F))}. \tag{2.2}$$

2.3 Asymptotic estimate

The next result gives an asymptotic upper bound for the number of integers which are represented by binary forms of large degree in the family $\mathcal{F}$ of binary fewnomials introduced in section 1.3. It also gives an upper bound for the number of representations of such an integer.

Recall the constant $C = 2^{79}3^{15}$ from Proposition 2.3.

Theorem 2.6. *Under the assumptions of Theorem 1.4, let λ and μ be two real numbers satisfying $\lambda > 2$ and*

$$0 < \mu < \frac{\lambda - 2}{Cr^{4r}\lambda}. \tag{2.3}$$

Let $d_0 \geqslant 3$ be an integer. Assume that the condition

$$\mathcal{A}^\star(F) \leqslant \exp(\mu d/\log d) \tag{2.4}$$

is satisfied for all $d \geqslant d_0$ and all $F \in \mathcal{F}_d$. Then

(a) For all $m \in \mathbb{Z} \smallsetminus \{-1, 0, 1\}$ and all $d \geqslant 3$ multiple of r, the set $\mathcal{G}_{\geqslant d}(m)$ is finite. Furthermore, for all (λ, μ, r, d) as above with $d \geqslant d_0$, there exists a constant c_1, only depending on (λ, μ, r, d), such that, for every $|m| \geqslant 2$, one has the inequality

$$\sharp \mathcal{G}_{\geqslant d}(m) \leqslant c_1 |m|^{\lambda/(2d)}.$$

(b) For all (λ, μ, r, d) as above with $d \geqslant d_0$, there exists c_2 depending only on (λ, μ, r, d), such that, for all $N \geqslant 2$, one has the inequality

$$\sharp\mathcal{R}_{\geqslant d}(N) \leqslant c_2 N^{\lambda/d}.$$

Proof. Define λ' by the equality

$$\mu = \frac{\lambda' - 2}{Cr^{4r}\lambda'}.$$

By (2.3), we have the equalities $2 < \lambda' < \lambda$. The number $\theta := \lambda'/2$ satisfies

$$\theta > 1 \text{ and } 1 - \frac{1}{\theta} = \frac{\lambda' - 2}{\lambda'} = Cr^{4r}\mu.$$

Let $d \geqslant 3$ be a multiple of r, written as $d = kr$. Let $m \in \mathbb{Z}$, $|m| \geqslant 2$ be such that $\mathcal{G}_{\geqslant d}(m) \neq \emptyset$: there exists $(x, y, F) \in \mathcal{G}_{\geqslant d}(m)$ such that $m = F(x, y)$, where $F \in \mathcal{F}_{k'r}$ (with $k' \geqslant k$) is the binary form

$$a_0 X^{k'r} + a_1 X^{k'(r-1)} Y^{k'} + \cdots + a_{r-1} X^{k'} Y^{k'(r-1)} + a_r Y^{k'r}.$$

Let $\mathcal{X} = \max\{|x|, |y|\}$. By hypothesis, we have $\mathcal{X} \geqslant 2$. The lower bound (2.2) yields

$$|m| \geqslant \mathcal{X}^{k'r - Cr^{4r}(\log(k'r))(\log \mathcal{A}^\star(F))}.$$

Assume now $d \geqslant d_0$. From (2.4) we deduce the upper bound

$$Cr^{4r}(\log(k'r))(\log \mathcal{A}^\star(F)) \leqslant Cr^{4r+1}\mu k' = k'r\left(1 - \frac{1}{\theta}\right),$$

hence

$$\mathcal{X}^{k'r} \leqslant |m|^\theta.$$

Define

$$M_0 := \left\lfloor \frac{\theta \log |m|}{r \log 2} \right\rfloor.$$

Thanks to the inequalities $\mathcal{X} \geqslant 2$ and $k' \geqslant k$ we deduce $M_0 \geqslant k$ and

$$k' \leqslant M_0 \qquad \text{and} \qquad \mathcal{X} \leqslant |m|^{\theta/(k'r)}. \tag{2.5}$$

Given x and m, the number of $y^{k'}$ such that $F(x, y) = m$ is at most r, hence the number of such y is at most $2r$. This shows that the set $\mathcal{G}_{\geqslant d}(m)$ is finite for all m with $|m| \geqslant 2$ and $d \geqslant d_0$. Since, for all $d \geqslant 3$ all the sets $\mathcal{F}_d$ are finite, we deduce from Thue's Theorem on the finiteness of the number of solutions of Thue's equation that the set $\mathcal{G}_{\geqslant d}(m)$ is finite for any $d \geqslant 3$.

We also deduce for $d \geqslant d_0$ that the number of elements in $\mathcal{G}_{\geqslant d}(m)$ is bounded by

$$\sharp\,\mathcal{G}_{\geqslant d}(m) \leqslant 4r|m|^{\theta/d} \sum_{k'=k}^{M_0} \sharp\mathcal{E}_{k'}. \tag{2.6}$$

Using the inequality (1.13) under the form

$$\sharp\mathcal{E}_{k'} \leqslant 3^{r+1} \max_{F \in \mathcal{F}_{k'r}} (\mathcal{A}^\star(F))^{r+1},$$

together with the hypothesis (2.3) we deduce

$$\sharp\mathcal{E}_{k'} \leqslant 3^{r+1} \exp\left(\mu k' r(r+1)/(\log(k'r))\right).$$

Combining with (2.6) and the upper bound $\theta < \lambda/2$, we deduce the inequality

$$\begin{aligned}\sharp\,\mathcal{G}_{\geqslant d}(m) &\leqslant 4r|m|^{\theta/d}\cdot M_0\cdot 3^{r+1}\,\exp\left(\mu M_0 r(r+1)/(\log(M_0 r))\right)\\ &\leqslant c_1|m|^{\lambda/(2d)}.\end{aligned}$$

This completes the proof of the item (a).

The proof of the item (b) has similarities and works as follows. Write $d = kr$ and let m be an element of $\mathcal{R}_{\geqslant d}(N)$. It satisfies $|m| \leqslant N$ and it can be written as $m = F(x,y)$ for some (x,y) such that $\mathcal{X} \geqslant 2$, for some $k' \geqslant k$ and some $F \in \mathcal{F}_{k'r}$. However the inequalities (2.5) imply

$$k' \leqslant M_1 \quad \text{and} \quad \max\{|x|,|y|\} \leqslant N^{\theta/(kr)} \quad \text{where} \quad M_1 := \left\lfloor \frac{\theta\log N}{r\log 2}\right\rfloor.$$

Thus we have

$$\sharp\mathcal{R}_{\geqslant d}(N) \leqslant \left(1+2N^{\theta/(kr)}\right)^2 \sum_{k'=k}^{M_1}\sharp\mathcal{E}_{k'},$$

and the item (b) follows. □

2.4 Proof of Theorem 1.4

Let $\epsilon > 0$ be fixed, and $\lambda = 2+2\epsilon$. Let

$$\mu_0 := \frac{\lambda-2}{Cr^{4r}\lambda},$$

and as mentioned above let

$$\eta := \epsilon(2Cr^{4r})^{-1}.$$

The inequality $\eta < \mu_0$ allows to apply Theorem 2.6 (a). Since we have $\lambda/(2d) < (1/d)+\epsilon$ we obtain the upper bound of $\mathcal{G}_{\geqslant d}(m)$ for $d \geqslant d_0$ as claimed in Theorem 1.4 (a). This completes the proof of Theorem 1.4 (a).

We now prove the alinea (b) of Theorem 1.4. We separate its proof according to the size of d, compared with d_0 starting from which, the upper bound (1.16) is true.

— Assume $d \geqslant d_0$. Let us check condition (ii) in the Definition 2.1. Let $\epsilon_1 > 0$. For $d' > \lambda/\epsilon_1$ Theorem 2.6 (b) yields

$$\sharp\mathcal{R}_{\geqslant d'}(N) \leqslant c_2 N^{\lambda/d'} < N^{\epsilon_1}$$

for sufficiently large N. Hence, applying Theorem 2.2 above, with $A = 2$, (or [FW2024, Theorem 1.11]) we obtain the alinea (b) in that case.

— Assume $3 \leqslant d < d_0$ we extend the above proof as follows to take into account the contribution of the forms of $\mathcal{F}$ with degree in the interval $[d, d_0-1]$. We start from the equality

$$\sharp\mathcal{R}_{\geqslant d}(N) = X + O(Y), \tag{2.7}$$

with

$$\begin{aligned}X = \sharp\{m : |m| \leqslant N,\ m = F(x,y) &\text{ for some } (x,y,F)\\ &\text{with } \max\{|x|,|y|\} \geqslant 2,\ F\in\mathcal{F} \text{ with } d \leqslant \deg F < d_0\},\end{aligned}$$

and

$$Y = \sharp\mathcal{R}_{\geqslant d_0}(N).$$

Let $d_1 = (d_0 - 1)^\dagger$ We have $d_1 \geqslant d_0$ and $d_1 \geqslant d^\dagger$. We trivially have $Y = \sharp\mathcal{R}_{\geqslant d_1}(N)$. By the above discussion, we have

$$Y = O(N^{2/d_1}) = O(N^{2/d^\dagger}). \tag{2.8}$$

To deal with X, we benefit from the fact that there are finitely many forms in the union $\bigcup_{d\leqslant d'<d_0} \mathcal{F}_{d'}$. Let $d_2 = (d-1)^\dagger$. If $d_2 > d$ the leading coefficient on the right–hand side of (1.17) vanishes. We suppose that $d_2 \leqslant d_0 - 1$ otherwise there is nothing to prove. Let $F \in \mathcal{F}_{d_2}$. Then [SX2019, Theorem 1.1] gives an asymptotic formula for

$$\sharp\{m : |m| \leqslant N,\ m = F(x,y) \text{ for some } (x,y) \text{ with } \max\{|x|,|y|\} \geqslant 2\}. \tag{2.9}$$

(also see (1.3) above). If $G \in \mathcal{F}_{d_2}$, with $G \neq F$ (so G is not $\mathbb{Q}$–isomorphic to F by hypothesis), then [FW2024, Theorem 1.1] gives an upper bound for

$$\sharp\{m : |m| \leqslant N,\ m = F(x,y) = G(u,v) \text{ for some } (x,y,u,v) \text{ with } \max\{|x|,|y|\} \geqslant 2\}. \tag{2.10}$$

We then apply the inclusion–exclusion principle to give an asymptotic formula for

$$\sharp\{m : |m| \leqslant N,\ m = F(x,y) \text{ for some } (x,y) \text{ with } \max\{|x|,|y|\} \geqslant 2 \text{ and some } F \in \mathcal{F}_{d_2}\}.$$

Since each set $\mathcal{F}_d$ is finite, we deduce from (1.3) the bound

$$\sharp\{m : |m| \leqslant N,\ m = F(x,y) \text{ for some } (x,y) \text{ with } \max\{|x|,|y|\} \geqslant 2 \text{ and some } F \in \bigcup_{d_2^\dagger \leqslant \ell < d_0} \mathcal{F}_\ell\} = O(N^{2/d_2^\dagger}). \tag{2.11}$$

By (2.7), (2.8), (2.9), (2.10) and (2.11) we complete the proof of alinea (b) of Theorem 1.4.

The item (c) of Theorem 1.4 directly follows from the item (b) by a combination of the definition (1.2), the equality (1.7) and the definition of $A_F^\star$.

3 Examples of sets of $\mathbb{C}$ and $\mathbb{Q}$–homography–free sets

Our next task is to exhibit examples of families of binary fewnomials suited for an application of Theorem 1.4 (c). Recall that $\mathbb{K} = \mathbb{Z}$, $\mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$.

3.1 Old examples

Such examples were already given in previous papers of the authors through the following natural approach. Let F and G be two binary forms of $\mathrm{Bin}(d, \mathbb{K})$ and suppose that we are interested in the $\gamma \in \mathrm{GL}(2,\mathbb{K})$ such that $F \circ \gamma = G$. The study of these γ is essentially equivalent to the study of the homographies $\mathfrak{h}$ with coefficients in $\mathbb{K}$ which exchange the complex roots ρ of the polynomials $f(t) := F(t,1)$ and $g(z) := G(z,1)$ (see Lemmas 4.1 and 4.5 and Proposition 4.7 below). When $\mathbb{K} = \mathbb{Q}$, we studied the following cases

- F and G are cyclotomic forms with the same degree, then the ρ are primitive roots of unity (see [FW2020, Proposition 4.8 and Corrigendum]),

- F and G are products of distinct irreducible quadratic forms of the shape $X^2+\alpha Y^2$ with $\alpha \in \mathbb{Z}$, then the roots ρ are algebraic irrational numbers with degree two, so necessarily we have $\mathfrak{h}(\mathbb{Q}(\sqrt{-\alpha})) = \mathbb{Q}(\sqrt{-\alpha})$ (see [FW2023, Propositions 4.1 & 5.1] and [FW2024, Proposition 3.1]),

- F and G are products of distinct linear factors of the shape $X - aY$, with $a \in \mathbb{Q}$, then we exploit the fact that $\mathfrak{h}$ preserves the cross ratios of any 4–tuples of distinct ρ (see [FW2023, Proposition 6.1]).

Apart from products of binomial forms $(X^r+\alpha Y^r)$ (for suitable rational integers α), the above examples do not seem to lead to interesting examples of binary fewnomials.

3.2 New examples

The landscape of Theorem 1.4 is different since the information concerning the binary fewnomials is not of algebraic nature but it concerns the indices where the corresponding coefficients of the form vanish. Theorems 3.2 and 3.4 below are written in that sense. The proofs of these results are based on the above homographies $\mathfrak{h}$ and on the symmetric functions of the roots of a polynomial. The number and the indices of these zero coefficients are important. However, one can prove variations of our results by shifting the string of these zeroes. We will not investigate these possible extensions.

To state our result, we introduce the following conventions: Let $F(X,Y)$ be a binary form, not necessarily a binary fewnomial, written as

$$F(X,Y) = a_0X^d + a_1X^{d-1}Y + \cdots + a_dY^d. \tag{3.1}$$

We suppose that $a_0a_d \neq 0$. We define the two functions

$$\begin{cases} \Lambda^+(F) := \max\{\ell : a_i = 0, 0 < i < \ell\}, \\ \Lambda^-(F) := \min\{\ell : a_i = 0, \ell < i < d\}. \end{cases} \tag{3.2}$$

They satisfy the properties

$$a_{\Lambda^\pm(F)} \neq 0,\ 1 \leqslant \Lambda^+(F) \leqslant \Lambda^-(F) \leqslant d$$

and

$$\Lambda^\mp(F) = \Lambda^\pm(F^{\mathrm{rec}}),$$

where $F^{\mathrm{rec}}(X,Y)$ is the *reciprocal binary form* defined by $F^{\mathrm{rec}}(X,Y) := F(Y,X)$. So we restrict ourselves to statements (for instance Theorem 3.2 or 3.4) in terms of $\Lambda^+(F)$ only.

The first result (Theorem 3.2) considers the case of binary forms where, for the very first positive values of i, the coefficients a_i are equal to zero. The following definition is essential.

Definition 3.1. [Reduced set of binary forms] Let $\mathbb{K}$ be as above and let $d \geqslant 3$ be an integer. A set $\mathcal{E}$ of binary forms of degree d with coefficients in $\mathbb{K}$ is called $\mathbb{K}$–*reduced* if it satisfies the three conditions

1. for any F in $\mathcal{E}$, we have $a_0a_d \neq 0$,

2. the set $\mathcal{E}$ is $\mathbb{K}$–dilation–free,

3. there is no pair (F, G) of distinct binary binomial forms (1.14) of $\mathcal{E}$ and no pair $(u, v) \in (\mathbb{C}^\times)^2$ such that $F(vY, uX) = G(X, Y)$.

If the set $\mathcal{E}$ is $\mathbb{K}$–reduced so does every subset of $\mathcal{E}$. The item 3 is satisfied when $\mathcal{E}$ contains one binomial form at most. When $\mathbb{K} = \mathbb{C}$, the condition 3 is satisfied if and only if $\mathcal{E}$ contains at most one binomial form.

We will prove in §5.1:

Theorem 3.2. *Let $d \geqslant 3$ and $\mathbb{K}$ as above. Let $\mathcal{E}$ be a $\mathbb{K}$–reduced set of binary forms. Assume that any $F \in \mathcal{E}$ satisfies*

$$\Lambda^+(F) \geqslant \frac{d+3}{2}.$$

Then the set $\mathcal{E}$ is $\mathbb{K}$–homography–free.

The assumption $\Lambda^+(F) \geqslant (d+3)/2$ implies that when $d \in \{3, 4\}$, the set $\mathcal{E}$ only contains binomial forms.

Theorem 3.2 is quite general and the discussion in §4.5 will show that the lower bound $\Lambda^+(F) \geqslant (d+3)/2$ is optimal.

A different way to see the quasi–optimality of Theorem 3.2 is the following Proposition, where we follow the notations (3.1) and where we use basic concepts of linear algebra. We introduce the subset of 8 matrices in $\mathrm{GL}(2, \mathbb{K})$:

$$\mathcal{G} = \left\{ \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}, \begin{pmatrix} 0 & \pm 1 \\ \pm 1 & 0 \end{pmatrix} \right\}$$

We have

Proposition 3.3. *For every $d \geqslant 3$ there exists a binary form F with degree d and with integer coefficients, such that*

- $a_1 = a_2 = \cdots a_{\lfloor d/2 \rfloor} = 0$,
- *there exists $\gamma \in \mathrm{GL}(2, \mathbb{Z}) \setminus \mathcal{G}$, such that $F \circ \gamma = F$.*

Proof. Let S be the following matrix

$$S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

which is attached to the change of variables $(X, Y) \mapsto (Y, X)$. Let $\mathcal{E}(d, \mathbb{Q})$ be the $\mathbb{Q}$–vector space gathering all the binary forms with degree d, rational coefficients together with the 0–form. It has dimension $d+1$. If ξ belongs to $\mathrm{GL}(2, \mathbb{Z})$ we denote by $\xi^\dagger$ the automorphism of $\mathcal{E}(d, \mathbb{Q})$ defined by

$$\xi^\dagger(F) = F \circ \xi^{-1} \ (F \in \mathcal{E}(d, \mathbb{Q})).$$

In particular we have the equality $(\xi\eta)^\dagger = \xi^\dagger \eta^\dagger$, for any ξ and $\eta \in \mathrm{GL}(2, \mathbb{Z})$. Of particular importance is the vector subspace

$$\mathcal{S}(d, \mathbb{Q}) := \{F \in \mathcal{E}(d, \mathbb{Q}) : a_k = a_{d-k} \, (0 \leqslant 2k \leqslant d)\}.$$

It is the eigenspace (relative to the eigenvalue 1) of the automorphism $S^\dagger$ of $\mathcal{E}(d, \mathbb{Q})$. A basis of $\mathcal{S}(d, \mathbb{Q})$ is given by

$$\{X^k Y^{d-k} + X^{d-k} Y^k : 0 \leqslant 2k \leqslant d\}.$$

We have the equality $\dim \mathcal{S}(d,\mathbb{Q}) = \lfloor d/2 \rfloor + 1$. Let ξ be any element of $\mathrm{SL}(2,\mathbb{Z})$ such that the element

$$\gamma := \xi S \xi^{-1}$$

does not belong to $\mathcal{G}$. Then $\xi^{\dagger}\left(\mathcal{S}(d,\mathbb{Q})\right)$ is the eigenspace of $\gamma^{\dagger}$ relative to the eigenvalue 1. It also has dimension $\lfloor d/2 \rfloor + 1$.

For $1 \leqslant \kappa < d$, let $\mathcal{V}(d,\kappa,\mathbb{Q})$ be the vector subspace

$$\mathcal{V}(d,\kappa,\mathbb{Q}) := \{F : a_1 = \cdots = a_\kappa = 0\}.$$

Its codimension is equal to κ. If one has the inequality

$$(d+1-\kappa) + (\lfloor d/2 \rfloor + 1) > d+1,$$

which is equivalent to the inequality

$$\kappa \leqslant \lfloor d/2 \rfloor,$$

then the intersection of vector spaces $\mathcal{V}(d,\kappa,\mathbb{Q}) \cap \xi^{\dagger}\left(\mathcal{S}(d,\mathbb{Q})\right)$ contains an element F different from 0. Obviously, for this F, we have $a_1 = \cdots = a_\kappa = 0$ and $\gamma^{\dagger}(F) = F \circ \gamma^{-1} = F$.

Note that this construction is too general to ensure that the form F has a discriminant $\neq 0$ and a first coefficient $a_0 \neq 0$ □

3.2.1 Three illustrations.

• We now consider $d = 3$ (so $\lfloor d/2 \rfloor = 1$) with the choices

$$\xi = \begin{pmatrix} 2 & 1 \\ 3 & 1 \end{pmatrix}, \xi^{-1} = \begin{pmatrix} -1 & 1 \\ 3 & -2 \end{pmatrix} \text{ and } \gamma = \xi S \xi^{-1} = \gamma^{-1} = \begin{pmatrix} 5 & -3 \\ 8 & -5 \end{pmatrix}.$$

Let $\phi(X,Y)$ be the cubic symmetric form

$$\phi(X,Y) := 13(X^3+Y^3) + 51(X^2Y + XY^2).$$

Then we have

$$F(X,Y) = \left(\xi^{\dagger}(\phi)\right)(X,Y) = (\phi \circ \xi^{-1})(X,Y) = 32X^3 - 30XY^2 + 11Y^3.$$

We check the equality $\gamma^{\dagger}(F) = F \circ \gamma^{-1} = F$, since we have the equality

$$F(X,Y) = F(5X - 3Y, 8X - 5Y). \tag{3.3}$$

• The same equality (3.3) holds for

$$F(X,Y) = 256X^4 - 240XY^3 + 111Y^4$$

using the quartic symmetric form

$$\phi(X,Y) = 127(X^4+Y^4) + 740(X^3Y + XY^3) + 1338X^2Y^2.$$

• We consider $d = 10$ (so $\lfloor d/2 \rfloor = 5$) and we require the help of a computer. Consider the symmetrical form $\phi(X,Y)$ defined by

$$\begin{aligned}\phi(X,Y) = 76\,210\,176\,793\ \left(X^{10}+Y^{10}\right) + 872\,977\,899\,590\ \left(X^9Y + XY^9\right) \\ +4\,381\,399\,953\,765\left(X^8Y^2 + X^2Y^8\right) + 12\,658\,497\,992\,520\left(X^7Y^3 + X^3Y^7\right) \\ +23\,266\,629\,555\,330\left(X^6Y^4 + X^4Y^6\right) + 28\,385\,698\,168\,548\,X^5Y^5.\end{aligned}$$

Let

$$\xi = \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}, \xi^{-1} = \begin{pmatrix} -5 & 2 \\ 3 & -1 \end{pmatrix} \text{ and } \gamma = \xi S \xi^{-1} = \gamma^{-1} = \begin{pmatrix} -7 & 3 \\ -16 & 7 \end{pmatrix}$$

By a $\mathrm{GL}(2,\mathbb{Z})$ change of variables, we have

$$\begin{aligned} F(X,Y) &= \left(\xi^{\dagger}(\phi)\right)(X,Y) = (\phi \circ \xi^{-1})(X,Y) = \phi(-5X+2Y, 3X-Y) \\ &= -34\,359\,738\,368\,X^{10} + 49\,565\,859\,840\,X^4Y^6 - 74\,095\,902\,720\,X^3Y^7 \\ &\quad +42\,402\,890\,880\,X^2Y^8 - 10\,956\,131\,760\,XY^9 + 1\,074\,852\,609\,Y^{10}. \end{aligned}$$

We check the equality $\gamma^{\dagger}(F) = F \circ \gamma^{-1} = F$, since we have

$$F(X,Y) = F(-7X+3Y, -16X+7Y).$$

With the help of a computer, one checks that the form F has a discriminant different from 0 and that the coefficients are relatively prime.

3.2.2 A variation of Theorem 3.2

Theorem 3.2 has the defect not to cover the case where $\Lambda^+(F)$ is very close from $d/2$ (i.e, $2\Lambda^+(F) = d$, $d+1$ or $d+2$). For instance it does not apply to the balanced trinomial forms appearing in (1.15). In order to circumvent this failure, we introduce the following sets, where we impose to the forms to have a string of (at least) four zero monomials located just after the monomial $a_{\Lambda^+(F)}X^{d-\Lambda^+(F)}Y^{\Lambda^+(F)}$.

We will prove in §6.3 the following analogue of Theorem 3.2.

Theorem 3.4. *Let $d \geqslant 11$ and $\mathbb{K}$ as above. Let $\mathcal{E}$ be a $\mathbb{K}$–reduced subset of $\mathrm{Bin}(d,\mathbb{K})$. Assume that for each $F \in E$ we have*

$$d/2 \leqslant \Lambda^+(F) \leqslant d-4,\ a_k = 0 \text{ for } \Lambda^+(F)+1 \leqslant k \leqslant \Lambda^+(F)+4.$$

and that if d is even, then $\mathcal{E}$ contains no trinomial of the form

$$a_0X^d + a_{d/2}X^{d/2}Y^{d/2} + a_dY^d. \tag{3.4}$$

Then $\mathcal{E}$ is $\mathbb{K}$–homography–free.

The assumption $\Lambda^+(F) \leqslant d-4$ implies that the set $\mathcal{E}$ contains no binomial form.

The set $\mathcal{E}$ does not contain two forms F and G such that $F(vY,uX) = G(X,Y)$ with u and v in $\mathbb{C}^\times$: indeed, if two forms F and G related by such an equation satisfy $\Lambda^+(F) \geqslant d/2$ and $\Lambda^+(G) \geqslant d/2$ and are not binomial forms, then d is even and F and G are trinomials of the form (3.4).

The assumption $d \geqslant 11$ is necessary in view of the other conditions of Theorem 3.4. For $d = 11$ the elements of $\mathcal{E}$ are of the form

$$a_0X^{11} + a_6X^5Y^6 + a_{11}Y^{11}$$

with $a_0a_6a_{11} \neq 0$.

3.3 Examples of homography–free sets of binary forms

We give examples where the assumptions of Theorem 1.4 (b) and (c) are satisfied.

3.3.1 Corollaries to Theorem 3.2

These corollaries concern two sets of binary forms. The first one is:

$$\mathcal{U}_d^{(1)}(\mathbb{K}) := \left\{ F \in \mathrm{Bin}(d,\mathbb{K}) : a_0 \neq 0,\ \Lambda^+(F) \geqslant (d+3)/2,\ a_{d-1} = a_d = 1 \right\}. \tag{3.5}$$

The condition $a_{d-1} \neq 0$ implies $\Lambda^+(F) \leqslant d-1$, hence if $\mathcal{U}_d^{(1)}(\mathbb{K})$ is not empty then $d \geqslant 5$. Conversely, for $d \geqslant 5$, the set $\mathcal{U}_d^{(1)}(\mathbb{K})$ is infinite. This is a consequence of the following lemma with $e = 1$.

Lemma 3.5. *Let a, d and e be integers such that $a \neq 0$, $1 \leqslant e \leqslant d-1$. Then the discriminant of the binary form*

$$F_a(X,Y) := aX^d + X^eY^{d-e} + Y^d$$

is different from zero.

The form F_a has $\Lambda^+(F_a) = d - e$ and $d - 1 \geqslant (d+3)/2$ for $d \geqslant 5$.

Proof. We need to prove that the polynomial

$$f_a(t) = at^d + t^e + 1 \tag{3.6}$$

has no multiple root. Without loss of generality we may assume that e and d are coprime integers. Suppose that such a multiple root, that we call ρ, exists. It would satisfy $f_a(\rho) = a\rho^d + \rho^e + 1 = 0$ and $f_a'(\rho) = ad\rho^{d-1} + e\rho^{e-1} = 0$, from which we deduce that

$$\rho^{d-e} = -\frac{e}{ad} \quad \text{and that} \quad \rho^e = -\frac{d}{d-e}.$$

However the equation

$$a^e = (-1)^d \frac{e^e(d-e)^{d-e}}{d^d}$$

cannot hold with $a \in \mathbb{Z}$ and e and d coprime integers. □

To define the second set we recall a classical definition: let $k \geqslant 2$ be an integer and let $x = a/b$ be a non zero rational number, written in its minimal form with $b > 0$. We say that x is *k–free* if there is no prime p such that p^k divides ab.
We introduce the following subset $\mathcal{U}_d^{(2)}(\mathbb{Z})$ of $\mathrm{Bin}(d,\mathbb{Z})$ containing all the forms F (written as in (3.1)) such that

$$\begin{cases} (a)\ a_0 > 0,\ a_d \neq 0,\ (d+3)/2 \leqslant \Lambda^+(F) \leqslant d-1, \\ (b)\ a_0 \text{ and } a_d \text{ are } d\text{–free}, \\ (c)\ \text{if there is an odd index } k \text{ such that } a_k \neq 0 \\ \qquad \text{then for the smallest such } k \text{ we have } a_k > 0. \end{cases} \tag{3.7}$$

When a_0 is d–free, the form $F_{a_0}(X,Y)$ defined in Lemma 3.5 also belongs to $\mathcal{U}_d^{(2)}(\mathbb{Z})$, thus this set is infinite.

We state the following corollary to Theorem 3.2. The proof is given in §5.2.

Corollary 3.6. *The following properties hold.*

1. *For every $d \geqslant 5$ the infinite set $\mathcal{U}_d^{(1)}(\mathbb{K})$ is a $\mathbb{K}$–homography–free set of binary forms.*
2. *For $d \geqslant 5$ the infinite set $\mathcal{U}_d^{(2)}(\mathbb{Z})$ is a $\mathbb{Q}$–homography–free set of $\mathbb{Q}$–rigid binary forms.*

3.3.2 Corollaries to Theorem 3.4

We give new examples where the assumptions (b) and (c) of Theorem 1.4 are satisfied.

Our next example is the set

$$\mathcal{V}_d^{(1)}(\mathbb{K}) := \big\{F \in \mathrm{Bin}(d,\mathbb{K}) : a_0 \neq 0,\ d/2 \leqslant \Lambda^+(F) \leqslant d-6,\ a_{d-1} = a_d = 1 \\ a_k = 0 \ \text{ for } \ \Lambda^+(F)+1 \leqslant k \leqslant \Lambda^+(F)+4\big\}. \tag{3.8}$$

We introduce the following subset $\mathcal{V}_d^{(2)}(\mathbb{Z})$ of $\mathrm{Bin}(d,\mathbb{Z})$ containing all the forms F (written as in (3.1)) such that

$$\begin{cases} (a)\ a_0 > 0,\ a_d \neq 0,\ , d/2 \leqslant \Lambda^+(F) \leqslant d-5, \\ \qquad a_k = 0 \text{ for } \Lambda^+(F)+1 \leqslant k \leqslant \Lambda^+(F)+4, \\ (b)\ a_0 \text{ and } a_d \text{ are } d\text{–free}, \\ (c) \text{ if there is an odd index } k \text{ such that } a_k \neq 0, \\ \qquad \text{then for the smallest such } k \text{ we have } a_k > 0 \\ (d) \text{ if } d \text{ is even, then } F \text{ is not a trinomial of the form} \\ \qquad a_0X^d + a_{d/2}X^{d/2}Y^{d/2} + a_dY^d. \end{cases} \tag{3.9}$$

It is plain that the set $\mathcal{V}_d^{(1)}(\mathbb{K})$ (resp. $\mathcal{V}_d^{(2)}(\mathbb{Z})$) is empty for $d < 12$ (resp. for $d < 11$). Let us check that for $d \geqslant 12$ (resp. $d \geqslant 11$) this set is infinite.

For $d = 11$ the set $\mathcal{V}_{11}^{(2)}(\mathbb{Z})$ contains the forms

$$aX^{11} + X^6Y^5 + Y^{11}, \qquad a > 0 \quad d\text{–free},$$

as shown by Lemma 3.5.

For $d \geqslant 12$ and $a \in \mathbb{Z} \smallsetminus \{0\}$, consider the binary forms

$$G_a(X,Y) = X^d + aX^{d-\nu}Y^\nu + XY^{d-1} + Y^d,$$

where $\nu = \nu_d = \lfloor (d+1)/2 \rfloor$. The next result shows that for $|a|$ sufficiently large $G_a(X,Y)$ belongs to both $\mathcal{V}_d^{(1)}(\mathbb{K})$ and $\mathcal{V}_d^{(2)}(\mathbb{Z})$.

Lemma 3.7. *For any $d \geqslant 12$, there exists a constant A_d such that*

$$\sharp\{a \in \mathbb{Z} \smallsetminus \{0\} : G_a \notin \mathrm{Bin}(d,\mathbb{Z})\} \leqslant A_d.$$

Proof. The discriminant of the polynomial $G_a(X,1)$ is equal to $D(a)$ where D is a polynomial in $\mathbb{Z}[T]$. The discriminant of the polynomial $f_1(x)$ introduced in (3.6) is $D(0)$ when $e = 1$. Since f_1 has no multiple roots, we have $D(0) \neq 0$ and the polynomial D has only finitely many roots. □

Remark 3.8. One can check that $A_{12} = 0$, hence the sets $\mathcal{V}_{12}^{(1)}(\mathbb{Z})$ and $\mathcal{V}_{12}^{(2)}(\mathbb{Z})$ contain all the quadrinomials which are of the form

$$X^{12} + aX^6Y^6 + XY^{11} + Y^{12} \quad (a \in \mathbb{Z}).$$

Indeed, the discriminant of the polynomial $T^{12} + aT^6 + T + 1$ is a polynomial of degree 12 in a, with integer coefficients; using a computer, we check that it has no integral solution.

Here is a corollary to Theorem 3.4. The proof is given in §6.3.

Corollary 3.9. *For $d \geqslant 12$, we have*

1. *The infinite set $\mathcal{V}_d^{(1)}(\mathbb{K})$ is a $\mathbb{K}$–homography–free set of binary forms.*
2. *The infinite set $\mathcal{V}_d^{(2)}(\mathbb{Z})$ is a $\mathbb{Q}$–homography–free set of $\mathbb{Q}$–rigid binary forms.*

Remark 3.10. The conditions concerning a_{d-1} and a_d (in (3.5) and in (3.8)) and a_0, a_k and a_d (in (3.7) and in (3.9)), may appear artificial. They are introduced to eliminate possible homotheties between forms and can be replaced by other types of conditions.

4 Homographies between two binary forms

For the proofs of Theorems 3.2 (in section 5.1) and 3.4 (in section 6), in order to check the hypotheses arising from Definition 1.1, we need to study the homographies between two binary forms and the automorphisms of a binary form.

4.1 Zeroes of binary forms

4.1.1 Case of one form.

In this section $\mathbb{K}$ is the field $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$. To the element

$$\gamma = \begin{pmatrix} u_1 & u_2 \\ u_3 & u_4 \end{pmatrix} \in \mathrm{GL}(2,\mathbb{K}) \tag{4.1}$$

we associate the *homography* $\tilde{\gamma}$ of $\mathbb{P}^1(\mathbb{K})$ defined by the formula

$$\tilde{\gamma}(x:t) = (u_1x + u_2t : u_3x + u_4t),$$

where we denote by $(x:t)$ the generic element of $\mathbb{P}^1(\mathbb{K})$. Recall that for γ_1 and γ_2 in $\mathrm{GL}(2,\mathbb{K})$ we have the equivalence

$$\tilde{\gamma}_1 = \tilde{\gamma}_2 \iff \big(\text{ there exists } \lambda \in \mathbb{K}^\times \text{ such that } \gamma_1 = \lambda\gamma_2\ \big) \tag{4.2}$$

and the formula

$$\widetilde{\gamma_1\,\gamma_2} = \tilde{\gamma}_1 \circ \tilde{\gamma}_2 \tag{4.3}$$

Let F be a form $\mathrm{Bin}(d,\mathbb{C})$ and $\mathcal{Z}(F)$ the set of zeroes of F in $\mathbb{P}^1(\mathbb{C})$. By definition, it is the set of classes $(x:t)$ of pairs $(x,t) \in \mathbb{C}^2 \smallsetminus \{(0,0)\}$ modulo the homotheties such that $F(x,t) = 0$. By assumption the cardinality of $\mathcal{Z}(F)$ is d and for $\gamma \in \mathrm{GL}(2,\mathbb{K})$ we have the conjugation equality

$$\mathcal{Z}(F\circ\gamma) = \tilde{\gamma}^{-1}\big(\mathcal{Z}(F)\big), \tag{4.4}$$

which follows from the relations

$$(x:t) \in \mathcal{Z}(F\circ\gamma) \iff (F\circ\gamma)(x:t) = 0 \iff \tilde{\gamma}(x:t) \in \mathcal{Z}(F) \iff (x:t) \in \tilde{\gamma}^{-1}\left(\mathcal{Z}(F)\right).$$

In particular for $\gamma \in \mathrm{Aut}(F,\mathbb{K})$, we have

$$\mathcal{Z}(F) = \tilde{\gamma}\big(\mathcal{Z}(F)\big). \tag{4.5}$$

Thus for $\gamma \in \mathrm{Aut}(F,\mathbb{K})$ the restriction of $\tilde{\gamma}$ to $\mathcal{Z}(F)$, denoted by $\tilde{\gamma}_{|\mathcal{Z}(F)}$, is a bijection of $\mathcal{Z}(F)$. If E is a subset of $\mathbb{P}^1(\mathbb{C})$, let $\mathrm{Aut}(E,\mathbb{K})$ be the set of bijections $\phi : E \to E$ such

that there exists $\gamma \in \mathrm{GL}(2,\mathbb{K})$ with the property $\tilde{\gamma}_{|E} = \phi$. In particular for $\gamma \in \mathrm{GL}(2,\mathbb{K})$ one has the equality

$$\mathrm{Aut}(\mathcal{Z}(F\circ\gamma),\mathbb{K}) = (\tilde{\gamma}_{|\mathcal{Z}(F)})^{-1}\mathrm{Aut}\,(\mathcal{Z}(F),\mathbb{K})\,\tilde{\gamma}_{|\mathcal{Z}(F)}.$$

We have

Lemma 4.1. *Let $F \in \mathrm{Bin}(d,\mathbb{K})$ $(d \geqslant 3)$. The $\tilde{}$–map which transforms $\gamma \in \mathrm{GL}(2,\mathbb{K})$ in the homography $\tilde{\gamma}$ on $\mathbb{P}^1(\mathbb{C})$ induces a homomorphism*

$$\begin{array}{rccc} \Psi & : & \mathrm{Aut}(F,\mathbb{K}) & \longrightarrow & \mathrm{Aut}(\mathcal{Z}(F),\mathbb{K}) \\ & & \gamma & \mapsto & \Psi(\gamma) = \tilde{\gamma}_{|\mathcal{Z}(F)}. \end{array}$$

We have

$$\ker\Psi = \{\zeta\,\mathrm{Id} : \zeta \in \mathbb{K},\ \zeta^d = 1\}.$$

Finally when $\mathbb{K} = \mathbb{C}$ the map Ψ is surjective.

Proof. The existence and unicitiy of Ψ follows from (4.5). As a consequence of (4.3), for any γ_1 and $\gamma_2 \in \mathrm{Aut}(F,\mathbb{K})$, we have $\Psi(\gamma_1\gamma_2) = \Psi(\gamma_1)\circ\Psi(\gamma_2)$. The determination of $\ker\Psi$ comes down to finding the matrices $\gamma \in \mathrm{Aut}(F,\mathbb{K})$ such that $\tilde{\gamma}$ fixes every point of $\mathcal{Z}(F)$. Since $\mathcal{Z}(F)$ contains d points and since $d \geqslant 3$, we deduce the equality $\tilde{\gamma} = \mathrm{Id}$. By (4.2), the automorphism γ is a homothety of the shape $\zeta\,\mathrm{Id}$, with $\zeta \in \mathbb{K}^\times$. The equality $F\circ\gamma = \zeta^d F$ restricts the possible values of ζ by the equality $\zeta^d = 1$.

We now suppose that $\mathbb{K} = \mathbb{C}$ to prove that Ψ is surjective. So let $F \in \mathrm{Bin}(d,\mathbb{C})$ and let $\xi \in \mathrm{GL}(2,\mathbb{C})$ such that $\tilde{\xi}_{|\mathcal{Z}(F)}$ belongs to $\mathrm{Aut}(\mathcal{Z}(F),\mathbb{C})$. We want to prove the existence of some $\gamma \in \mathrm{Aut}(F,\mathbb{C})$ such that $\tilde{\gamma} = \xi$. By (4.4), we have the equality $\mathcal{Z}(F) = \mathcal{Z}(F\circ\xi)$. This implies that the forms F and $F\circ\xi$ are proportional since they have the same zeroes with the same multiplicities. For some $\alpha \in \mathbb{C}^\times$ we have $F\circ\xi = \alpha F$. It remains to put $\gamma := \lambda\xi$, where $\lambda \in \mathbb{C}$ satisfies $\lambda^{-d} = \alpha$ to obtain the equalities $\tilde{\gamma} = \tilde{\xi}$ and $F\circ\gamma = F$. □

Remark 4.2. When $\mathbb{K} = \mathbb{Q}$ or $\mathbb{R}$, the morphism Ψ in Lemma 4.1, is not surjective generally speaking as one sees in the following example. Let a and b be two distinct positive real numbers. Let $F(X,Y)$ in $\mathrm{Bin}(4,\mathbb{R})$ defined by

$$F(X,Y) := (X - aY)(X + Y/a)(X - bY)(X + Y/b).$$

We then have

$$\mathcal{Z}(F) = \big\{(a:1),\,(-1/a:1),\,(b:1),\,(-1/b:1)\big\}.$$

Let $\xi : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ be the homography defined by $\xi(z) := -1/z$. We check that $\xi_{|\mathcal{Z}(F)}$ belongs to $\mathrm{Aut}(\mathcal{Z}(F),\mathbb{R})$. Searching for $\gamma \in \mathrm{Aut}(F,\mathbb{R})$ such that $\tilde{\gamma} = \xi$ is equivalent to searching for $\lambda \in \mathbb{R}^\times$ such that

$$\gamma = \begin{pmatrix} 0 & -\lambda \\ \lambda & 0 \end{pmatrix},$$

satisfies $(F\circ\gamma)\,(X,Y) = F(X,Y)$. Such a $\lambda \in \mathbb{R}$ does not exist, since a direct computation leads to the equality $(F\circ\gamma)(X,Y) = -\lambda^4\cdot F(X,Y)$.

Lemma 4.1 has the following consequence.

Lemma 4.3. *Let $d \geqslant 4$ and let $F \in \mathrm{Bin}(d,\mathbb{Q})$. Suppose that $\mathrm{Aut}(\mathcal{Z}(F),\mathbb{C}) = \{\mathrm{Id}\}$. Then we have*

$$\mathrm{Aut}(F,\mathbb{Q}) = \begin{cases} \{\mathrm{Id}\} & \text{if } 2\nmid d \\ \{\pm\mathrm{Id}\} & \text{if } 2 \mid d. \end{cases}$$

Proof. Since $\mathrm{Aut}(\mathcal{Z}(F),\mathbb{C})$ contains one element only, so does $\mathrm{Aut}(\mathcal{Z}(F),\mathbb{Q})$. This element is Id, hence one has the equality

$$\mathrm{Aut}(F,\mathbb{Q}) = \Psi^{-1}(\{\mathrm{Id}\}) = \ker \Psi,$$

and the result follows from Lemma 4.1. □

Lemma 4.3 never applies when $d = 3$, since, in that case, $\mathrm{Aut}(\mathcal{Z}(F),\mathbb{C})$ always has six elements.

We finish this section by some conventions and notations. The results of §3 concern binary forms $F(X,Y)$ having $a_0 \neq 0$ with the notation (3.1). Thus it is natural to identify the roots of the form $F(X,Y)$ in $\mathbb{P}^1(\mathbb{C})$ with the zeroes (on the complex affine line) of the *associated polynomial*

$$f(t) = F(t,1)/a_0. \tag{4.6}$$

By construction, this polynomial is monic and we are led to consider, for $d \geqslant 1$, the following set of polynomials

$$\mathcal{P}_d(\mathbb{K}) := \{f \in \mathbb{K}[t] : f \text{ monic}, \deg f = d, \mathrm{disc} f \neq 0\}, \tag{4.7}$$

with $\mathbb{K} = \mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ or $\mathbb{Z}$. If f and g belong to $\mathcal{P}_d(\mathbb{K})$, we systematically write them as

$$f(t) = t^d + \alpha_1 t^{d-1} + \cdots + \alpha_d, \tag{4.8}$$

and

$$g(z) = z^d + \beta_1 z^{d-1} + \cdots + \beta_d. \tag{4.9}$$

By convention, we put $\alpha_0 = \beta_0 = 1$.

By analogy with (3.2), we define

$$\Lambda^+(f) := \max\{\ell : \alpha_i = 0, 0 < i < \ell\}. \tag{4.10}$$

Since $\mathrm{disc} f \neq 0$, the polynomial $f(t)$ is not the monomial t^d, thus we have

$$1 \leqslant \Lambda^+(f) \leqslant d. \tag{4.11}$$

By analogy with $\mathcal{Z}(F)$, we introduce the set $\mathcal{Z}(f) := \{\rho \in \mathbb{C} : f(\rho) = 0\}$. This set of zeroes has cardinality d.

4.1.2 Case of two forms.

This paragraph generalizes the section 4.1.1 by studying the links between the zeroes of two forms F_1 and F_2.

Since we do not wish to consider multiplicities for the zeroes, we need to assume that the discriminants are not zero: the two binary forms $(X-Y)(X-2Y)^2(X-3Y)^2$ and $(X-Y)(X-2Y)(X-3Y)^3$ have the same degree, the same sets of zeroes (not with the same multiplicities), and they are not isomorphic.

Definition 4.4. Let $\mathbb{K}$ be one of the fields $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$. Let $\mathcal{E}_1$ and $\mathcal{E}_2$ be two subsets of $\mathbb{P}^1(\mathbb{K})$ with equal cardinalities $\geqslant 3$. We call $\mathbb{K}$*–isomorphism between* $\mathcal{E}_1$ *and* $\mathcal{E}_2$ any bijection ϕ from $\mathcal{E}_1$ on $\mathcal{E}_2$ such that there exists $h \in \mathrm{GL}(2,\mathbb{K})$ with the property of restriction

$$\tilde{h}_{|\mathcal{E}_1} = \phi.$$

The set of these isomorphisms is denoted by $\mathrm{Isom}\big(\mathcal{E}_1, \mathcal{E}_2; \mathbb{K}\big)$. If this set is not empty, we say that $\mathcal{E}_1$ and $\mathcal{E}_2$ are $\mathbb{K}$*–isomorphic.*

When $\sharp\mathcal{E}_1 = \sharp\mathcal{E}_2 = 3$, then the sets $\mathcal{E}_1$ and $\mathcal{E}_2$ are K–isomorphic. We will use

Lemma 4.5. *Let $d \geqslant 3$. Let F_1 and F_2 be two forms of $\mathrm{Bin}(d, \mathbb{C})$. We suppose that $\mathcal{Z}(F_1)$ and $\mathcal{Z}(F_2)$ are $\mathbb{C}$–isomorphic and let $\mathfrak{h}$ be an element of $\mathrm{Isom}(\mathcal{Z}(F_1), \mathcal{Z}(F_2); \mathbb{C})$. Then there exists at least one element $\gamma_0 \in \mathrm{GL}(2, \mathbb{C})$ such that*

$$\tilde{\gamma_0}_{|\mathcal{Z}(F_1)} = \mathfrak{h} \text{ and } F_1 = F_2 \circ \gamma_0. \tag{4.12}$$

Finally when one such element γ_0 is fixed, we have the equality

$$\{\gamma \in \mathrm{GL}(2, \mathbb{C}) : \tilde{\gamma}_{|\mathcal{Z}(F_1)} = \mathfrak{h} \text{ and } F_1 = F_2 \circ \gamma\} = \{\lambda\, \gamma_0 : \lambda \in \mathbb{C}, \lambda^d = 1\}. \tag{4.13}$$

It follows that F_1 and F_2 in $\mathrm{Bin}(d, \mathbb{C})$ are $\mathbb{C}$–isomorphic if and only if $\mathcal{Z}(F_1)$ and $\mathcal{Z}(F_2)$ are $\mathbb{C}$–isomorphic.

Remark 4.6. When $\mathfrak{h}$ belongs to $\mathrm{Isom}(\mathcal{Z}(F_1), \mathcal{Z}(F_2); \mathbb{Q})$, we cannot ensure the existence $\gamma_0 \in \mathrm{GL}(2, \mathbb{Q})$ satisfying (4.12). This is the content of Remark 4.2 above, with the choice $F_1 = F_2 = F$ and $\mathfrak{h} = \xi|_{\mathcal{Z}(F)}$.

Proof. By the definition of $\mathfrak{h}$, there exists $\gamma \in \mathrm{GL}(2, \mathbb{C})$ such that $\tilde{\gamma}_{|\mathcal{Z}(F_1)} = \mathfrak{h}$. Write γ as in (4.1) and

$$F_1(X, Y) = \prod_{i=1}^{d} \big(\alpha_i X - \beta_i Y \big).$$

So we have $\mathcal{Z}(F_1) = \big\{(\beta_i : \alpha_i) : 1 \leqslant i \leqslant d\big\}$ and

$$\mathfrak{h}(\beta_i : \alpha_i) = (u_1\beta_i + u_2\alpha_i : u_3\beta_i + u_4\alpha_i).$$

Since $\mathcal{Z}(F_2) = \mathfrak{h}(\mathcal{Z}(F_1))$ we deduce the equality

$$\mathcal{Z}(F_2) = \big\{(u_1\beta_i + u_2\alpha_i : u_3\beta_i + u_4\alpha_i) : 1 \leqslant i \leqslant d\big\},$$

and the existence of some $c \in \mathbb{C}^\times$ such that

$$F_2(X, Y) = c \prod_{i=1}^{d} \left((u_3\beta_i + u_4\alpha_i)X - (u_1\beta_i + u_2\alpha_i)Y\right).$$

From this equality and from the equality

$$(u_3\beta_i + u_4\alpha_i)(u_1X + u_2Y) - (u_1\beta_i + u_2\alpha_i)(u_3X + u_4Y) = (\det\gamma)\,(\alpha_i X - \beta_i Y),$$

we deduce the equality

$$F_2 \circ \gamma = c\,(\det\gamma)^d\, F_1.$$

Define $\gamma_0 := c^{-1/d}(\det\gamma)^{-1}\,\gamma$ where $c^{1/d}$ is any d–th root of c. Then γ_0 satisfies (4.12).

To prove (4.13), we notice that $\tilde{\gamma}$ and $\tilde{\gamma_0}$ coïncide on a set of $d \geqslant 3$ points of $\mathbb{P}^1(\mathbb{C})$. So they are equal. By (4.2), there exists $\lambda \in \mathbb{C}^\times$ such that $\gamma = \lambda\,\gamma_0$. By hypothesis we have $F_1 = F_2 \circ \gamma_0 = F_2 \circ \gamma$. But F_2 is homogeneous with degree d which leads to the condition $\lambda^d = 1$. □

In the same order of ideas as Lemma 4.5 we have

Proposition 4.7. *Let $d \geqslant 3$ and let F and G two distinct forms of* $\mathrm{Bin}(d, \mathbb{C})$ *such that*

$$\mathrm{Isom}(\mathcal{Z}(F), \mathcal{Z}(G); \mathbb{C}) = \emptyset.$$

Then we have the equality

$$\{\gamma \in \mathrm{GL}(2, \mathbb{C}) : F = G \circ \gamma\} = \emptyset.$$

Proof. By contraposition, suppose that there exists $\gamma \in \mathrm{GL}(2, \mathbb{C})$ such that $F = G \circ \gamma$. By (4.4), we have $\tilde{\gamma}^{-1}(\mathcal{Z}(G)) = \mathcal{Z}(F)$. Thus $\tilde{\gamma}$ is an isomorphism between $\mathcal{Z}(F)$ and $\mathcal{Z}(G)$. □

4.1.3 From binary forms to polynomials

We will define the action of the homographies on the set of polynomials in $\mathcal{P}_d(\mathbb{K})$.

Let F and G be two elements in $\mathrm{Bin}(d, \mathbb{K})$ written as

$$\begin{cases} F(X, Y) = a_0 X^d + a_1 X^{d-1} Y + \cdots + a_d Y^d \\ G(X, Y) = b_0 X^d + b_1 X^{d-1} Y + \cdots + b_d Y^d \end{cases} \tag{4.14}$$

and let γ be an element in $\mathrm{GL}(2, \mathbb{K})$ written as in (1.1). Assume $F = G \circ \gamma$:

$$F(X, Y) = G(u_1 X + u_2 Y, u_3 X + u_4 Y). \tag{4.15}$$

Consider the two monic polynomials f and g in $\mathcal{P}_d(\mathbb{K})$ associated with the binary forms F and G respectively (recall the definition (4.6)):

$$f(t) = \frac{1}{a_0} F(t, 1) \text{ and } g(z) = \frac{1}{b_0} G(z, 1).$$

The relation (4.15) gives

$$f(t) = \frac{b_0}{a_0} (u_3 t + u_4)^d g\left(\frac{u_1 t + u_2}{u_3 t + u_4}\right)$$

and

$$\frac{a_0}{b_0} = c(\gamma, g) \text{ where } c(\gamma, g) := \begin{cases} u_3^d g(u_1/u_3) & \text{if } u_3 \neq 0, \\ u_1^d & \text{if } u_3 = 0. \end{cases} \tag{4.16}$$

Definition 4.8. When f and g are two monic polynomials in $\mathcal{P}_d(\mathbb{K})$ and $\mathfrak{h}$ an homography with matrix γ, we write $\mathfrak{h}(f) = g$ if f and g are related by the equation

$$f(t) = \frac{1}{c(\gamma, g)} (u_3 t + u_4)^d g\left(\frac{u_1 t + u_2}{u_3 t + u_4}\right)$$

where $c(\gamma, g)$ is defined in (4.16).

We separate the homographies over $\mathbb{P}^1(\mathbb{K}) = \mathbb{K} \cup \{\infty\}$ into two sorts. Let $\mathfrak{h} = \tilde{\gamma}$ be an homography of $\mathbb{P}^1(\mathbb{K})$ associated with an element γ as in (4.1).

• If the coefficient u_3 of γ is 0, then $u_4 \neq 0$ and we set

$$q = \frac{u_1}{u_4}, \quad r = \frac{u_2}{u_4}.$$

We say that $\mathfrak{h}$ is an *affine homography*. We write it as $\mathfrak{h} = \mathfrak{h}_{q,r}$, and for $t \in \mathbb{P}^1(\mathbb{K})$ we have

$$\mathfrak{h}(t) = \mathfrak{h}_{q,r}(t) = qt + r,$$

with $(q,r)\in\mathbb{K}^\times\times\mathbb{K}$.
• If $u_3\neq 0$, we set

$$q=\frac{u_1}{u_3},\quad r=\frac{u_2u_3-u_1u_4}{u_3^2},\quad s=-\frac{u_4}{u_3}.$$

We say that $\mathfrak{h}$ is a *non affine homography*. We write it as $\mathfrak{h}=\mathfrak{h}_{q,r,s}$, and for $t\in\mathbb{P}^1(\mathbb{K})$ we have

$$\mathfrak{h}(t)=\mathfrak{h}_{q,r,s}(t)=q+\frac{r}{t-s},$$

where $(q,r,s)\in\mathbb{K}\times\mathbb{K}^\times\times\mathbb{K}$.
The formulas for the inverses are:

$$\mathfrak{h}_{q,r}^{-1}=\mathfrak{h}_{q^{-1},-rq^{-1}}\quad\text{and}\quad\mathfrak{h}_{q,r,s}^{-1}=\mathfrak{h}_{s,r,q}. \tag{4.17}$$

From Definition 4.8 we deduce:

Lemma 4.9. *Let $d\geqslant 2$, let $f(t)$ and $g(z)$ two monic polynomials of $\mathcal{P}_d(\mathbb{K})$ written as in (4.8) and (4.9). Let $\mathfrak{h}$ be an homography such that $g=\mathfrak{h}(f)$.*

1. *If $\mathfrak{h}$ is an affine homography written as $\mathfrak{h}=\mathfrak{h}_{q,r}$, then we have*

$$z=\mathfrak{h}_{q,r}(t)=qt+r,\quad t=\mathfrak{h}_{q,r}^{-1}(z)=\frac{1}{q}(z-r),$$

$$f(t)=\frac{1}{q^d}g(qt+r),\quad g(z)=q^df\left(\frac{z-r}{q}\right).$$

2. *If $\mathfrak{h}$ is a non–affine homography written as $\mathfrak{h}=\mathfrak{h}_{q,r,s}$, then we have*

$$z=\mathfrak{h}_{q,r,s}(t)=q+\frac{r}{t-s},\quad t=\mathfrak{h}_{q,r,s}^{-1}(z)=s+\frac{r}{z-q},$$

$$f(t)=\frac{(t-s)^d}{g(q)}g\left(q+\frac{r}{t-s}\right),\quad g(z)=\frac{(z-q)^d}{f(s)}f\left(s+\frac{r}{z-q}\right), \tag{4.18}$$

and

$$f(s)g(q)=r^d. \tag{4.19}$$

When $\mathbb{K}=\mathbb{C}$, given a monic polynomial f in $\mathcal{P}_d(\mathbb{C})$, we can write

$$f(z)=\prod_{\rho\in\mathcal{Z}(f)}(z-\rho).$$

From Definition 4.8 we deduce

$$(\mathfrak{h}(f))(z):=\prod_{\rho\in\mathcal{Z}(f)}(z-\mathfrak{h}(\rho)). \tag{4.20}$$

Since the polynomials of $\mathcal{P}_d(\mathbb{C})$ have exactly d roots which are all distinct, we have, for any homography $\mathfrak{h}$ and for any f and g in $\mathcal{P}_d(\mathbb{C})$ the property

$$\mathfrak{h}(\mathcal{Z}(f))=\mathcal{Z}(g)\iff g=\mathfrak{h}(f).$$

Lemma 4.10. *Let $d\geqslant 3$ and F and G elements of $\mathrm{Bin}(d,\mathbb{K})$, written as in (4.14). We suppose that $a_0a_db_0b_d\neq 0$. Let $f(t)=F(t,1)/a_0$ and $g(z)=G(z,1)/b_0$ be the two polynomials in $\mathcal{P}_d(\mathbb{K})$ associated with F and G. Let $\gamma\in\mathrm{GL}(2,\mathbb{K})$ and let $\tilde{\gamma}=\mathfrak{h}$ be the homography associated with γ. Then the two following conditions are equivalent:*
(i) There exists $\nu\in\mathbb{K}^\times$ such that $G\circ\gamma=\nu F$.
(ii) We have the equality

$$\mathfrak{h}(f)=g.$$

Proof. (i) implies (ii) has been proved in (4.16).
Conversely, assume $\mathfrak{h}(f) = g$. From Definition 4.8 we deduce

$$\begin{aligned} F(t,1) = a_0 f(t) &= \frac{a_0}{c(\gamma,g)}(u_3t+u_4)^d g\left(\frac{u_1t+u_2}{u_3t+u_4}\right) \\ &= \frac{a_0}{b_0 c(\gamma,g)}(u_3t+u_4)^d G\left(\frac{u_1t+u_2}{u_3t+u_4},1\right) \\ &= \frac{a_0}{b_0 c(\gamma,g)} G(u_1t+u_2,u_3t+u_4), \end{aligned}$$

hence the result with $\nu = \frac{b_0}{a_0}c(\gamma,g)$. □

For $\nu \in \mathbb{K}^\times$ and $F \in \mathrm{Bin}(d,\mathbb{K})$, the polynomial f associated to F is the same as the polynomial associated to νF. When $\mathbb{K} = \mathbb{C}$, the two forms F and νF are $\mathbb{C}$–isomorphic; in general, F and νF are $\mathbb{K}$–isomorphic when ν is a d–th power of an element in $\mathbb{K}$. Consider for instance the two forms

$$F(X,Y) = X^4 + 4XY^3 - Y^4 \text{ and } G(X,Y) = 4F(X,Y).$$

There is no $\gamma \in \mathrm{GL}(2,\mathbb{Q})$ such that $\tilde{\gamma} = \mathrm{Id}$ and $F \circ \gamma = G$. Nevertheless the forms F and G are $\mathbb{Q}$–isomorphic, since we have the equality

$$F(X+Y,X-Y) = G(X,Y).$$

4.2 Preparation of the proof of Theorem 3.2

By Lemma 4.3 and Proposition 4.7, we see that a first step in the proof of Theorem 3.2 will be the following proposition

Proposition 4.11. *Let $d \geqslant 3$. Suppose that there exist polynomials f and g in $\mathcal{P}_d(\mathbb{C})$ such that*

$$\Lambda^+(f) + \Lambda^+(g) \geqslant d+3 \tag{4.21}$$

and a homography $\mathfrak{h}$ such that $\mathfrak{h}(f) = g$. Then either

1. *$\mathfrak{h}$ is a homothety $\mathfrak{h}_{q,0}$ with $q \in \mathbb{C}^\times$, or*
2. *$\mathfrak{h}$ is a non affine homography and it is of the form $\mathfrak{h}_{0,r,0}$ with $r \in \mathbb{C}^\times$. In that situation f and g are of the form $t^d + \alpha_d$ and $z^d + \beta_d$, with $\alpha_d\beta_d = r^d$.*
3. *The hypothesis (4.21) is optimal to obtain the conclusions of the case 2: there exist elements f, g of $\mathcal{P}_d(\mathbb{C})$ and a non affine homography of the form $\mathfrak{h} = \mathfrak{h}_{q,r,s}$, with $(q,s) \neq (0,0)$ with $\mathfrak{h}(f) = g$ and $\Lambda^+(f) + \Lambda^+(g) = d+2$.*

Remark 4.12. In the particular case where $d = 3$, the inequality (4.21) implies that f and g are necessarily of the form $f(t) = t^3 + \alpha_3$ and $g(z) = z^3 + \beta_3$ with $\alpha_3\beta_3 \neq 0$. An example of a pair $(f(t), g(z))$ corresponding to the item 3 is the pair (t^3+1, z^3+3z), since we have $\Lambda^+(f) + \Lambda^+(g) = 5$ and

$$f(t) = \frac{(t-1)^3}{g(1)} g\left(1 + \frac{2}{t-1}\right),$$

(see (4.36) below for a more general construction).

4.3 Proof of Proposition 4.11.1, the case of affine homographies.

We are concerned with the following question: let f and g two polynomials in $\mathcal{P}_d(\mathbb{C})$ satisfying (4.21) and written as (4.8) and (4.9). We want information about the pairs $(q,r) \in \mathbb{C}^\times \times \mathbb{C}$, such that

$$\mathfrak{h}_{q,r}(f) = g.$$

The hypothesis (4.21) and the inequalities (4.11) imply the inequalities $\Lambda^+(f) \geqslant 2$ and $\Lambda^+(g) \geqslant 2$. This means $\alpha_1 = \beta_1 = 0$. So the sum of the roots of f and the sum of the roots of g are equal to 0. We write

$$0 = \sum_{\rho \in \mathcal{Z}(f)} \rho = \sum_{\rho' \in \mathcal{Z}(g)} \rho' = \sum_{\rho \in \mathcal{Z}(f)} (q\rho + r) = dr,$$

so we necessarily have $r = 0$. The proof of the item 1 is complete.

4.4 Proof of Proposition 4.11.2, the case of non affine homographies.

The question now is: let f and g be two polynomials in $\mathcal{P}_d(\mathbb{C})$ satisfying (4.21). We want information about the triples $(q,r,s) \in \mathbb{C} \times \mathbb{C}^\times \times \mathbb{C}$, such that

$$\mathfrak{h}_{q,r,s}(f) = g.$$

This question is deeper than the question relative the affine homographies, since the formulas of transformations of the symmetric functions of the roots are more involved.

The case where $f(s) = 0$ corresponds to g having a root sent to infinity. We avoid this fact by considering g to be monic with degree d. Similar consideration applies to the condition $g(q) = 0$. Recall that in the definitions of $\mathcal{U}_d^{(1)}(\mathbb{K})$, $\mathcal{U}_d^{(2)}(\mathbb{Z})$, $\mathcal{V}_d^{(1)}(\mathbb{K})$ and $\mathcal{V}_d^{(2)}(\mathbb{Z})$ (see §3.3), we impose $a_0 \neq 0$, so the associated polynomials (see (4.6)) are monic with degree d.

4.4.1 From the $f^{(i)}(s)$ to the β_j

We now state

Lemma 4.13. *Let $d \geqslant 1$ and let f and g be monic polynomials in $\mathcal{P}_d(\mathbb{C})$, written as in (4.8) and (4.9). Suppose that there exists $(q,r,s) \in \mathbb{C} \times \mathbb{C}^\times \times \mathbb{C}$ such that the non affine homography $\mathfrak{h}_{q,r,s}$ satisfies $g = \mathfrak{h}_{q,r,s}(f)$, and $f(s) \neq 0$.*

Then we have the equalities

$$\beta_j f(s) = (-1)^j \sum_{i=0}^{j} (-1)^i q^{j-i} r^i \binom{d-i}{j-i} \frac{f^{(i)}(s)}{i\,!} \quad (0 \leqslant j \leqslant d)$$

Proof. By the last part of formula (4.18) of Lemma 4.9 and by Taylor expansion, one has the equalities

$$\begin{aligned} g(z) &= \frac{(z-q)^d}{f(s)} \sum_{k=0}^{d} \frac{f^{(k)}(s)}{k\,!} \left(\frac{r}{z-q}\right)^k \\ &= \frac{1}{f(s)} \sum_{k=0}^{d} r^k \frac{f^{(k)}(s)}{k\,!} (z-q)^{d-k}. \end{aligned}$$

Lemma 4.13 follows by identification via the binomial formula to expand $(z-q)^{d-k}$. □

4.4.2 From the β_i to the $f^{(j)}(s)$

Lemma 4.14. *Let $d \geqslant 1$ and let f and g be polynomials in $\mathcal{P}_d(\mathbb{C})$, written as in (4.8) and (4.9). Suppose that there exists $(q, r, s) \in \mathbb{C} \times \mathbb{C}^\times \times \mathbb{C}$ such that the non affine homography $\mathfrak{h}_{q,r,s}$ satisfies the equality $g = \mathfrak{h}_{q,r,s}(f)$, and $f(s) \neq 0$.*
Then we have the equalities

$$\left(\frac{r}{q}\right)^j \cdot \frac{f^{(j)}(s)}{j\,!\,f(s)} = \sum_{i=0}^{j} \binom{d-i}{j-i} \frac{\beta_i}{q^i}, \tag{4.22}$$

for $0 \leqslant j \leqslant d$.

In the case where $q = 0$, this formula has to be interpreted as

$$r^j \cdot \frac{f^{(j)}(s)}{j\,!\,f(s)} = \beta_j. \tag{4.23}$$

Proof. By the first part of formula (4.18) and by (4.19) we have the equalities

$$\begin{aligned}
\frac{f(t)}{f(s)} &= \left(\frac{t-s}{r}\right)^d g\left(q + \frac{r}{t-s}\right) \\
&= \left(\frac{t-s}{r}\right)^d \sum_{i=0}^{d} \beta_i \left(q + \frac{r}{t-s}\right)^{d-i} \\
&= \frac{1}{r^d} \sum_{i=0}^{d} \beta_i (q(t-s) + r)^{d-i} (t-s)^i \\
&= \sum_{i=0}^{d} \beta_i \sum_{\ell=0}^{d-i} \binom{d-i}{\ell} q^\ell \frac{(t-s)^{\ell+i}}{r^{\ell+i}}.
\end{aligned}$$

Hence

$$\frac{f(t)}{f(s)} = \sum_{j=0}^{d} \frac{(t-s)^j}{r^j} \sum_{i=0}^{j} \beta_i \binom{d-i}{j-i} q^{j-i}. \tag{4.24}$$

By Taylor's expansion, we finally get

$$\frac{r^j f^{(j)}(s)}{j! f(s)} = \sum_{i=0}^{j} \beta_i \binom{d-i}{j-i} q^{j-i}.$$

□

Remark 4.15. If we write

$$y_i := \left(\frac{r}{q}\right)^i \cdot \frac{f^{(i)}(s)}{i\,!\,f(s)},$$

and

$$B_j := \frac{\beta_j}{q^j}, \ (0 \leqslant j \leqslant d),$$

then Lemmas 4.13 and 4.14 can be written respectively

$$\begin{pmatrix} B_0 \\ B_1 \\ \vdots \\ B_d \end{pmatrix} = A \begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_d \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_d \end{pmatrix} = A^{-1} \begin{pmatrix} B_0 \\ B_1 \\ \vdots \\ B_d \end{pmatrix} \tag{4.25}$$

where

$$A = \left((-1)^{i+j}\binom{d-i}{j-i}\right)_{0\leqslant i,j\leqslant d} \quad \text{and} \quad A^{-1} = \left(\binom{d-i}{j-i}\right)_{0\leqslant i,j\leqslant d} \tag{4.26}$$

and where we extend the definition of the binomial coefficients by setting $\binom{n}{k} = 0$ for $k < 0$.

The fact that these two matrices are inverse of each other is the simplest example of *inverse relations* (see for instance [Ri1968, p.43–45], where one sign $(-1)^k$ in formula (1) p. 43 should be removed): the inverse of the $(d+1)\times(d+1)$ matrix

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & \cdots & 0 \\ -\binom{d}{1} & 1 & 0 & 0 & \cdots & 0 \\ \binom{d}{2} & -\binom{d-1}{1} & 1 & 0 & \cdots & 0 \\ -\binom{d}{3} & \binom{d-1}{2} & -\binom{d-2}{1} & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ (-1)^d & (-1)^{d-1} & (-1)^{d-2} & (-1)^{d-3} & \cdots & 1 \end{pmatrix}$$

is the lower triangular matrix A^{-1} where, in the expression of A, we replace each entry by its absolute value.

The matrices A^{-1} and A enjoy an obvious interpretation through the automorphisms $P(X) \mapsto P(X+1)$ and $P(X) \mapsto P(X-1)$ of the vector space of polynomials with degree $\leqslant d$, equipped with the basis $\{X^d, X^{d-1}, \dots, X, 1\}$.

Lemma 4.16. *We adopt the notations and hypotheses of Lemma 4.14. Let e' be an integer such that $0 \leqslant e' \leqslant d-1$. Then we have the equalities*

$$\beta_1 = \beta_2 = \cdots = \beta_{e'} = 0,$$

if and only if, we have the equalities

$$\frac{f^{(k)}(s)}{f(s)} = \frac{d\,!}{(d-k)\,!} \cdot \left(\frac{q}{r}\right)^k, \tag{4.27}$$

for $1 \leqslant k \leqslant e'$.

Proof. This follows from the equalities (4.25), from the triangular structure of the matrix A and A^{-1} (defined in (4.26)) and from the equality $\beta_0 = 1$. □

Let us return to the proof of Proposition 4.11.2. In the next application of Lemma 4.16, we exploit the fact that if the integer k is sufficiently large (in terms of $\Lambda^+(f)$) the k–derivative of the polynomial f is a monomial.

Lemma 4.17. *Let $d \geqslant 3$ and let f and g be polynomials of $\mathcal{P}_d(\mathbb{C})$, written as in (4.8) and (4.9). Let $\Lambda^+(f)$ and $\Lambda^+(g)$ be the two integers defined by (4.10). Suppose that they satisfy*

$$\Lambda^+(f) + \Lambda^+(g) \geqslant d+3, \tag{4.28}$$

and suppose there exists a non affine homography $\mathfrak{h}_{q,r,s}$ ($(q,r,s) \in \mathbb{C}\times\mathbb{C}^\times\times\mathbb{C}$) such that $\mathfrak{h}(f) = g$. Then we have

$$q = s = 0$$

and

$$\Lambda^+(f) = \Lambda^+(g) = d.$$

The polynomials f and g have the shapes $f(t) = t^d + \alpha_d$, $g(z) = z^d + \beta_d$ with the relation $\alpha_d\beta_d = r^d$.

Proof. The assumptions imply $f(s) \neq 0$ (see (4.20)). To shorten notations, write $\lambda := \Lambda^+(f)$ and $\lambda' := \Lambda^+(g)$. We know from (4.11) that $1 \leqslant \lambda$, $\lambda' \leqslant d$ and from (4.8) that

$$f^{(k)}(s) = \frac{d\,!}{(d-k)\,!} \cdot s^{d-k},$$

for all $d - \lambda + 1 \leqslant k \leqslant d$. Combining with Lemma 4.16 (with $e' = \lambda' - 1$), we deduce that, for all $d - \lambda + 1 \leqslant k \leqslant \lambda' - 1$, one has the equality

$$s^d = \Big(\frac{qs}{r}\Big)^k \cdot f(s). \tag{4.29}$$

Suppose that the interval $[d - \lambda + 1, \lambda' - 1]$ contains two positive consecutive integers k and $k + 1$ (this assumption is equivalent to the inequality (4.28)). We apply (4.29) for these values k and $k + 1$ and notice that the left–hand side is constant.

• **Case $s \neq 0$.** So we have $q \neq 0$ by (4.29). After division, we have the equality

$$\frac{qs}{r} = 1.$$

This equality simplifies (4.27) into

$$s^k \frac{(d-k)\,!}{d\,!} \cdot \frac{f^{(k)}(s)}{f(s)} = 1,$$

for $k \leqslant \lambda' - 1$. We apply this formula with the choices $k = d - \lambda$ and $k = d - \lambda + 1$ and this is legal, since we have $d - \lambda < d - \lambda + 1 \leqslant \lambda' - 1$ as a consequence of the assumption (4.28). Thus we obtain the equalities

$$1 = \begin{cases} s^{d-\lambda} \cdot \dfrac{\lambda\,!}{d\,!} \cdot \dfrac{f^{(d-\lambda)}(s)}{f(s)} = \dfrac{s^d + \alpha_\lambda s^{d-\lambda}\,\lambda\,!(d-\lambda)\,!/(d\,!)}{f(s)}, \\[2ex] s^{d-\lambda+1} \cdot \dfrac{(\lambda-1)\,!}{d\,!} \cdot \dfrac{f^{(d-\lambda+1)}(s)}{f(s)} = \dfrac{s^d}{f(s)}. \end{cases}$$

Equating these two expressions and recalling that $\alpha_\lambda \neq 0$, we arrive at a contradiction.

• **Case $q \neq 0$.** The hypothesis (4.28) concerning f and g is symmetric. So, by exchanging the rôles, we may study the existence of a non affine homography $\mathfrak{h}_{s,r,q}$ transforming g into f (see (4.17)). By the above alinea, such a homography $\mathfrak{h}_{s,r,q}$ with $q \neq 0$ does not exist. So we are led to study the remaining case $q = s = 0$.

• **Case $q = s = 0$.** In that case we are asking if, for some $r \neq 0$, the homography

$$\mathfrak{h}_{0,r,0}(t) = \frac{r}{t},$$

can satisfy $\mathfrak{h}_{0,r,0}(f) = g$, or in an equivalent form $\mathfrak{h}_{0,r,0}(g) = f$. By definition of λ we have $\alpha_\lambda \neq 0$.

• Suppose that $\lambda \leqslant d-1$. Then the polynomial $g = \mathfrak{h}_{0,r,0}(f)$ has its coefficient $\beta_{d-\lambda} \neq 0$. Since $d - \lambda \geqslant 1$, we deduce the inequality $\lambda' \leqslant d - \lambda$. Such an inequality is incompatible with the hypothesis $\lambda + \lambda' \geqslant d + 3$.
• So we are left with the case $\lambda = d$. Equivalently we have $f(t) = t^d + \alpha_d$, with $\alpha_d \neq 0$. We check that $[\mathfrak{h}_{0,r,0}(f)](z) = z^d + r^d/\alpha_d$ by Lemma 4.9 (4.18). This is the last statement of Lemma 4.17. □

The proof of Proposition 4.11.2 is complete now.

4.5 Proof of Proposition 4.11.3

4.5.1 Heuristic considerations.

Before entering the proof of Proposition 4.11.3 itself, we consider a related general question involving a system of linear non homogeneous equations.

Let $(q, r, s) \in \mathbb{C} \times \mathbb{C}^\times \times \mathbb{C}$, $d \geqslant 3$, a, b with $1 \leqslant a, b \leqslant d-1$, $\mathcal{I}$ and $\mathcal{J}$ two subsets of $\{1, \dots, d\}$ with respectively a and b elements. Let us consider the following problem.

Does there exist monic polynomials f, g of degree d,

$$f(t) = \alpha_0 t^d + \cdots + \alpha_d, \quad g(z) = \beta_0 z^d + \cdots + \beta_d \quad \text{with} \quad \alpha_0 = \beta_0 = 1$$

and discriminants different from zero, which satisfy

$$\alpha_i = 0 \text{ for } i \in \mathcal{I} \text{ and } \beta_j = 0 \text{ for } j \in \mathcal{J} \tag{4.30}$$

and $\mathfrak{h}_{q,r,s}(f) = g$?

Assuming $\mathfrak{h}_{q,r,s}(f) = g$, there exists $\kappa \in \mathbb{C}^\times$ such that

$$\kappa f(t) = (t-s)^d g\left(q + \frac{r}{t-s}\right),$$

(to be compared with (4.18)) that is

$$\kappa f(t) = \sum_{i=0}^{d} \beta_i (t-s)^i (qt + r - qs)^{d-i}.$$

Notice that $\kappa f(s) = r^d$. We write (4.24) as

$$\frac{f(t)}{f(s)} = \frac{1}{r^d}(q(t-s)+r)^d + \sum_{j=0}^{d} \frac{(t-s)^j}{r^j} \sum_{i=1}^{j} \beta_i \binom{d-i}{j-i} q^{j-i}.$$

Hence the coefficient of t^h in $\kappa f(t)$ is

$$\kappa\alpha_{d-h} = \binom{d}{h} q^h (r-qs)^{d-h} + \sum_{i=\Lambda^+(g)}^{d} \beta_i \sum_{j=\max\{i,h\}}^{d} \binom{j}{h}\binom{d-i}{j-i} (-s)^{j-h} r^{d-j} q^{j-i}.$$

For $h = d$, since $\alpha_0 = 1$, this gives $\kappa = g(q)$.

The conditions (4.30) are equivalent to a system of $a+1$ linear non homogeneous equations

$$\kappa = g(q), \quad \alpha_i = 0 \quad (i \in \mathcal{I})$$

with $d-b+1$ unknowns

$$\kappa, \quad \beta_j \quad (1 \leqslant j \leqslant d,\ j \notin \mathcal{J}).$$

Heuristic. According to the above discussion, subject to the non vanishing of some determinants, we may expect that there is a Zariski closed set of (q,r,s) such that, outside this set,

- when $a+b<d$, then there are infinitely many solutions (f,g);
- when $a+b=d$, there is a unique solution;
- for $a+b>d$, there is no solution.

For instance, given integers λ and λ' in the interval $[1,d-1]$, the conditions $\Lambda^+(f) \geqslant \lambda$ and $\Lambda^+(g) \geqslant \lambda'$ are a special case of (4.30) with

$$\mathcal{I} = \{1,\dots,\lambda-1\}, \quad \mathcal{J} = \{1,\dots,\lambda'-1\},$$

$a=\lambda-1$ and $b=\lambda'-1$. When $\lambda+\lambda'=d+2$ we may expect that, outside a Zariski closed set of (q,r,s), there is a unique solution. In this case item 2 of Proposition 4.11 shows that $\lambda=\Lambda^+(f)$ and $\lambda'=\Lambda^+(g)$.

4.5.2 The proof itself.

We are now concerned with the proof of the last item of Proposition 4.11. Actually the proof below gives more information. The first step is

Lemma 4.18. *Let $d \geqslant 3$ and let $(q,r,s) \in (\mathbb{C}^\times)^3$ such that*

$$r \neq qs \text{ and } r \neq (d-1)qs. \tag{4.31}$$

Then there exists a unique pair (f,g) of monic polynomials with complex coefficients and with degree d, such that

$$\Lambda^+(f)=3,\ \Lambda^+(g)=d-1 \text{ and } \mathfrak{h}_{q,r,s}(f)=g. \tag{4.32}$$

Proof. Write f and g as in (4.8) and (4.9). By the second and the third conditions of (4.32) we can write

$$g(z)=z^d+\beta_{d-1}z+\beta_d, \qquad \kappa f(t)=(qt+r-qs)^d+\beta_{d-1}(qt+r-qs)(t-s)^{d-1}+\beta_d(t-s)^d, \tag{4.33}$$

for some complex number $\kappa \neq 0$ (see Lemma 4.9.2). Since f and g are monic, we have $\alpha_0=\beta_0=1$, that is

$$\kappa = q^d + q\beta_{d-1} + \beta_d.$$

The inequality $\Lambda^+(f) \geqslant 3$ is equivalent to the double equality $\alpha_1=\alpha_2=0$. So we are led to consider the system of three non–homogeneous linear equations in three unknowns β_{d-1}, β_d and κ

$$\begin{cases} q\beta_{d-1} & + & \beta_d & - & \kappa & = & -q^d \\ (r-dqs)\beta_{d-1} & - & ds\beta_d & & & = & -dq^{d-1}(r-qs) \\ (dqs-2r)s\beta_{d-1} & + & ds^2\beta_d & & & = & -dq^{d-2}(r-qs)^2. \end{cases} \tag{4.34}$$

The determinant is

$$\det \begin{pmatrix} q & 1 & -1 \\ r-dqs & -ds & 0 \\ (dqs-2r)s & ds^2 & 0 \end{pmatrix} = drs^2.$$

Since $qrs \neq 0$, there is a unique solution

$$\beta_{d-1} = dq^{d-2}\left(\frac{r}{s} - q\right), \quad \beta_d = q^{d-2}\left(\frac{r}{s} - q\right)\left(\frac{r}{s} - (d-1)q\right), \qquad \kappa = q^{d-2}\left(\frac{r}{s}\right)^2.$$

The assumption (4.31) ensures $\beta_{d-1} \neq 0$ and $\beta_d \neq 0$.

Let us check that $\alpha_3 \neq 0$, which means $\Lambda^+(f) = 3$. By considering the coefficient of t^{d-3} on both sides of the last equality of (4.33) and by the above values of β_d and β_{d-1} we obtain

$$\begin{aligned}
\kappa\alpha_3 &= \binom{d}{3} q^{d-3}(r-qs)^3 + \beta_{d-1}\binom{d-1}{2} s^2\left(r - \frac{d}{3}qs\right) - \beta_d\binom{d}{3}s^3 \\
&= \binom{d}{3} q^{d-3}(r-qs)^3 + \binom{d-1}{2} dq^{d-2}s\left(r - \frac{d}{3}qs\right)(r-qs) \\
&\qquad\qquad - \binom{d}{3} sq^{d-2}(r-qs)\big(r-(d-1)qs\big), \\
&= \binom{d}{3} q^{d-3}r^2(r-qs) \neq 0,
\end{aligned}$$

by assumption. □

Here is how to check that the polynomial $g(z)$ as defined in (4.33) with the above values of β_d and β_{d-1} has a discriminant different from zero, which is a necessary condition for $g(z)$ to belong to $\mathcal{P}_d(\mathbb{C})$. Assume there exists $\rho \in \mathbb{C}$ such that $g(\rho) = g'(\rho) = 0$. The condition $g'(\rho) = 0$ is equivalent to

$$\rho^{d-1} = -\frac{\beta_{d-1}}{d}. \tag{4.35}$$

Combining this value with $g(\rho) = 0$ yields

$$0 = g(\rho) = \rho\left(-\frac{\beta_{d-1}}{d}\right) + \beta_{d-1}\rho + \beta_d.$$

Hence, if ρ exists, its value can only be

$$\rho = \frac{d}{1-d}\cdot\frac{\beta_d}{\beta_{d-1}} = \frac{r/s - (d-1)q}{1-d},$$

thanks to the values already computed for β_d and β_{d-1}. From (4.35) we get the condition for the discriminant of g to be nonzero:

$$\left(\frac{r/s - (d-1)q}{1-d}\right)^{d-1} \neq -q^{d-2}(r/s - q).$$

To complete the proof of the item 3 of Proposition 4.11, we produce an instance of two elements f, g, of $\mathcal{P}_d(\mathbb{Q})$ (i.e. with nonzero discriminant) with $\Lambda^+(f) = 3$ and $\Lambda^+(g) = d-1$ and $\mathfrak{h}_{q,r,s}(f) = g$. Thanks to Remark 4.12 we may assume $d \geqslant 4$. Take $q = 1$, $r = 2$, $s = 1$, $\beta_{d-1} = d$, $\beta_d = 3 - d$, $\kappa = 4$, in other words we have

$$\gamma = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad g(z) = z^d + dz - d + 3,$$

so that $g(q) = 4$,

$$f(t) = \frac{(t-1)^d}{g(q)} g\left(\frac{t+1}{t-1}\right) = \frac{1}{4}\Big((t+1)^d + d(t+1)(t-1)^{d-1} + (3-d)(t-1)^d\Big). \tag{4.36}$$

One checks $\alpha_0 = 1$, $\alpha_1 = \alpha_2 = 0$, $\alpha_3 = \binom{d}{3} \neq 0$,

$$f(t) = t^d + \binom{d}{3} t^{d-3} + \alpha_4 t^{d-4} + \cdots + \alpha_d,$$

$f(1) = 2^{d-2}$, $f(s)g(q) = r^d$, $\Lambda^+(f) = 3$.

The derivative of g is $g'(z) = d(z^{d-1} + 1)$. Let ρ be one its roots. It satisfies $\rho^d = -\rho$ so we have the equality

$$g(\rho) = (d-1)\rho - d + 3,$$

and $g(\rho)$ does not vanish, since ρ has modulus one and $d \geqslant 4$. Since $g(z)$ and $g'(z)$ do not vanish simultaneously, the polynomial belongs to $\mathcal{P}_d(\mathbb{C})$. The proof of the item 3 of Proposition 4.11 is complete.

4.5.3 Comments

In Lemma 4.18 we assume $qs \neq 0$. There is no example of pair (f, g) of monic polynomials of degree d satisfying (4.32) with $qs = 0$, $\Lambda^+(f) = 3$ and $\Lambda^+(g) = d-1$. Indeed for $q = 0$ the system (4.34) yields

$$\begin{cases} r\beta_{d-1} - ds\beta_d & = 0 \\ -2rs\beta_{d-1} + ds^2\beta_d & = 0 \end{cases}$$

which has no solution satisfying $r \neq 0$ and $\beta_{d-1} \neq 0$, while for $s = 0$ and $q \neq 0$ this system (4.34) yields $dq^{d-2}r^2 = 0$, which is not allowed.

We now present some examples of pairs (f, g) of monic polynomials of degree d satisfying $\mathfrak{h}_{q,r,s}(f) = g$ and $\Lambda^+(f) + \Lambda^+(g) < d + 2$.

1. Here is an example with $q = 0$, $s \neq 0$, $\Lambda^+(f) = 2$, $\Lambda^+(g) = d - 1$:

$$g(z) = z^d + \frac{ds}{r} z + 1, \qquad f(t) = (t-s)^d g\left(\frac{r}{t-s}\right) = (t-s)^d + ds(t-s)^{d-1} + r^d.$$

2. When $\lambda + \lambda' = d$, explicit solutions (f, g) with $\Lambda^+(f) = \lambda$ and $\Lambda^+(g) = \lambda'$ are given with $q = s = 0$ by trinomial forms

$$f(t) = t^d + \alpha_\lambda t^{d-\lambda} + \alpha_d, \qquad g(z) = z^d + \beta_{d-\lambda} z^\lambda + \beta_d$$

with

$$\alpha_\lambda \beta_d = \beta_{d-\lambda} r^\lambda, \quad \alpha_d \beta_d = r^d.$$

3. When $\lambda + \lambda' < d$, explicit solutions are given with $q = s = 0$ by quadrinomial forms

$$f(t) = t^d + \alpha_\lambda t^{d-\lambda} + \alpha_{d-\lambda'} t^{\lambda'} + \alpha_d, \qquad g(z) = z^d + \beta_{\lambda'} z^{d-\lambda'} + \beta_{d-\lambda} z^\lambda + \beta_d$$

with

$$\alpha_d \beta_{\lambda'} = \alpha_{d-\lambda} r^{\lambda'}, \quad \alpha_d \beta_{d-\lambda} = \alpha_\lambda r^{d-\lambda}, \quad \alpha_d \beta_d = r^d.$$

5 Proofs of Theorem 3.2 and Corollary 3.6

5.1 Proof of Theorem 3.2

Let F and G be two forms of the reduced set $\mathcal{E}$ of $\mathrm{Bin}(d, \mathbb{K})$. We suppose that they are written as in (4.14) with $a_0 a_d b_0 b_d \neq 0$. By assumption we have $\min\{\Lambda^+(F), \Lambda^+(G)\} \geqslant$

$(d+3)/2$. Let f be the monic polynomial associated to F defined by (4.6) and written as in (4.8) with $\alpha_i = a_i/a_0$ for $0 \leqslant i \leqslant d$ and similarly let g be the monic polynomial associated to G written as (4.9) with $\beta_i = b_i/b_0$ for $0 \leqslant i \leqslant d$. They satisfy (4.21). Our aim is to prove that if there exists a matrix γ (written as in (1.1)) such that $F \circ \gamma = G$, then $F = G$. Assume such a γ exists and let $\tilde{\gamma} = \mathfrak{h}$, the homography attached to γ. Replacing γ with γ^{-1} in Lemma 4.10 we deduce $\mathfrak{h}(g) = f$.

Suppose that $u_3 \neq 0$, then $\mathfrak{h}$ is a non affine homography exchanging $\mathcal{Z}(f)$ and $\mathcal{Z}(g)$. By Proposition 4.11.2, we deduce that $\mathfrak{h}$ is of the form $\mathfrak{h}_{0,r,0}$ and that both F and G are binomials. Thus γ satisfies $u_1 = u_4 = 0$. The hypothesis $F \circ \gamma = G$ leads to the equality $F(u_2 Y, u_3 X) = G(X, Y)$. This contradicts the item 3 of Definition 3.1.

Hence $u_3 = 0$ and $\mathfrak{h}$ is an affine homography exchanging $\mathcal{Z}(f)$ and $\mathcal{Z}(g)$. By Proposition 4.11.1, the homography $\mathfrak{h}$ has to be a homothety. The matrix γ satisfies $u_2 = u_3 = 0$. The hypothesis $F \circ \gamma = G$ leads to the equality $F(u_1 X, u_4 Y) = G(X, Y)$. Item 2 of Definition 3.1 implies $F = G$.

This completes the proof of Theorem 3.2.

5.2 Proof of Corollary 3.6

The proof will use two auxiliary results.

Lemma 5.1. *Let $d \geqslant 3$ and $\mathcal{W}_d^{(1)}(\mathbb{K})$ be a subset of $\mathrm{Bin}(d, \mathbb{Z})$ such that for any $F \in \mathcal{W}_d^{(1)}(\mathbb{K})$ we have $a_0 \neq 0$, $a_{d-1} = a_d = 1$. Then the set $\mathcal{W}_d^{(1)}(\mathbb{K})$ is $\mathbb{K}$–dilation free.*

Proof. Let F and G be two elements in $\mathcal{W}_d^{(1)}(\mathbb{K})$ written as in (4.14) and let $\mathfrak{h}_{q,0}$ be a homothety which exchanges the zeroes of the polynomials f and g associated to F and G written as (4.8) and (4.9). By Lemma 4.5, all the $\gamma \in \mathrm{GL}(2, \mathbb{K})$ such that $\tilde{\gamma} = \mathfrak{h}_{q,0}$ and $F \circ \gamma = G$ have the shape

$$\gamma = \begin{pmatrix} u & 0 \\ 0 & v \end{pmatrix}, \tag{5.1}$$

where u and v are complex numbers different from zero. Returning to the explicit expression of F and $G = F \circ \gamma$ we have

$$G(X, Y) = F(uX, vY) = a_0 u^d X^d + a_1 u^{d-1} v X^{d-1} Y + \cdots + a_{d-1} u v^{d-1} X Y^{d-1} + a_d v^d Y^d,$$

hence the equalities $1 = b_d = v^d a_d = v^d$ and $1 = b_{d-1} = u v^{d-1} a_{d-1} = u v^{d-1}$. They imply that $u = v$ and $u^d = 1$. So $G(X, Y) = F(uX, uY) = u^d F(X, Y) = F(X, Y)$. Hence $\mathcal{W}_d^{(1)}(\mathbb{K})$ is $\mathbb{K}$–dilation–free. □

Lemma 5.2. *Let $d \geqslant 3$ and $\mathcal{W}_d^{(2)}(\mathbb{Z})$ be a subset of $\mathrm{Bin}(d, \mathbb{Z})$ such that for any $F \in \mathcal{W}_d^{(2)}(\mathbb{Z})$ written as in (3.1) we have*

1. *$a_0 > 0$, $a_d \neq 0$, a_0 and a_d are d–free,*
2. *if there is an odd index k such that $a_k \neq 0$, then for the smallest such k we have $a_k > 0$.*

Then
(a) The set $\mathcal{W}_d^{(2)}(\mathbb{Z})$ is $\mathbb{Q}$–dilation free.
(b) Let $F \in \mathcal{W}_d^{(2)}(\mathbb{Z})$ and let

$$\gamma = \begin{pmatrix} u & 0 \\ 0 & v \end{pmatrix} \in \mathrm{GL}(2, \mathbb{Q})$$

be such that $F \circ \gamma = F$. *Then*

$$\gamma = \begin{cases} \pm \mathrm{Id} & \text{if } F \text{ is not a binary form with squared arguments,} \\ \pm \mathrm{Id} \quad \text{or} \quad \pm \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} & \text{if } F \text{ is a binary form with squared arguments.} \end{cases}$$

Proof. (a) Let F and G be two elements in $\mathcal{W}_d^{(2)}(\mathbb{Z})$ written as in (4.14) and u, v two nonzero rational numbers such that $F(uX, vY) = G(X, Y)$. Since the coefficients a_0 and b_0 of X^d in F and G respectively are d–free integers, and since $a_0 > 0$ and $b_0 > 0$, the equality $a_0 u^d = b_0$ implies $u^d = 1$, and similarly $v^d = \pm 1$.
– If $u = v\,(= \pm 1)$ then $F = G$.
– If $u = 1$ and $v = -1$, then $F(X, Y)$ and $F(X, -Y)$ belong to $\mathcal{W}_d^{(2)}(\mathbb{Z})$. If there is some odd k such that $a_k \neq 0$, then the least such k satisfies $a_k > 0$. Since $F(X, -Y)$ also belongs to $\mathcal{W}_d^{(2)}(\mathbb{Z})$, we deduce that $(-1)^k a_k$ is also positive. This gives a contradiction. So both F and G have squared arguments. They are equal.
– If $u = -1$ and $v = 1$, then d is even necessarily. Now $F(X, Y)$ and $F(-X, Y)$ both belong to $\mathcal{W}_d^{(2)}(\mathbb{Z})$. If there is some odd k such that $a_k \neq 0$, then the least such k satisfies $a_k > 0$. Since $F(-X, Y)$ also belongs to $\mathcal{W}_d^{(2)}(\mathbb{Z})$, we deduce that $(-1)^{d-k} a_k$ is also positive. The end of the proof is as above. □

Proof of Corollary 3.6 . To prove the first item we are going to use Theorem 3.2. We first check item 3 in the Definition 3.1 of reduced sets. Since for $d \geqslant 3$ a binary form F such that $1 \leqslant \Lambda^+(F) \leqslant d-1$ is not a binomial form, it follows that no binomial binary form belongs to $\mathcal{U}_d^{(1)}(\mathbb{Z})$ nor to $\mathcal{U}_d^{(2)}(\mathbb{Z})$.

Lemma 5.1 shows that the set $\mathcal{U}_d^{(1)}(\mathbb{K})$ is $\mathbb{K}$–dilation free.

From Theorem 3.2 we deduce that the set $\mathcal{U}_d^{(1)}(\mathbb{K})$ is $\mathbb{K}$–homography–free.

Consider the second item of Corollary 3.6. We need to check that the set $\mathcal{U}_d^{(2)}(\mathbb{Z})$ is $\mathbb{Q}$–homography–free, and Theorem 3.2 shows that it suffices to check that it is $\mathbb{Q}$–dilation free. This result follows from the first part (a) of Lemma 5.2.

To complete the proof of the second item of Corollary 3.6 it only remains to be checked that the elements of $\mathcal{U}_d^{(2)}(\mathbb{Z})$ are $\mathbb{Q}$–rigid binary forms, which means that if F belongs to $\mathcal{U}_d^{(2)}(\mathbb{Z})$, then its group of $\mathbb{Q}$–automorphisms satisfies (1.6).

By Proposition 4.11.1, which is also valid for $f = g$, the only affine homographies which permute $\mathcal{Z}(f)$ are $\mathbb{Q}$–homotheties. By the remark made in §5.1, any $\mathbb{Q}$–automorphism γ of F is such that $\tilde{\gamma}$ is a $\mathbb{Q}$–homothety. So γ has the shape (5.1), but with u and v rational numbers different from zero. It only remains to apply part (b) of Lemma 5.2.

The proofs of both items of Corollary 3.6 are complete. □

5.3 Not homothetic pairs of polynomials

The first alinea of Proposition 4.11 gives no information about the existence or not of a homothety $\mathfrak{h}_{q,0}$ exchanging the distinct polynomials f and $g \in \mathcal{P}_d(\mathbb{K})$. Here we give examples (without proofs) of subsets of $\mathcal{P}_d(\mathbb{K})$ (defined in (4.7)) for which such homotheties do not exist.

Example 5.3. For $1 \leqslant k < d$, let

$$\mathcal{P}_{d,k,k+1}(\mathbb{C}) := \{f \in \mathcal{P}_d(\mathbb{C}) : \alpha_k = \alpha_{k+1} \neq 0\}.$$

Then there is no $q \in \mathbb{C} \smallsetminus \{0,1\}$ and no pair (f,g) of (distinct or not) elements of $\mathcal{P}_{d,k,k+1}(\mathbb{C})$, such that

$$\mathfrak{h}_{q,0}(f) = g.$$

Example 5.4. The second example is of arithmetical nature. Notice that since the discriminant of the elements in $\mathcal{P}_d(\mathbb{Z})$ is not 0, one at least of the two coefficients a_d, a_{d-1} is not 0. For $2 \leqslant k \leqslant d$, consider the set

$$\mathcal{P}_{d,k,\mathrm{free}}(\mathbb{Z}) := \{f \in \mathcal{P}_d(\mathbb{Z}) : a_k \neq 0 \text{ and } a_k \text{ is } k-\text{free}\}.$$

Let $d \geqslant 4$. There is no $q \in \mathbb{Q} \smallsetminus \{0,1,-1\}$ and no distinct f and $g \in \mathcal{P}_{d,k,\mathrm{free}}(\mathbb{Z})$ such that

$$\mathfrak{h}_{q,0}(f) = g.$$

Example 5.5. To eliminate the case of symmetry $\mathfrak{h}_{-1,0}$, it is sufficient to consider the following subset of $\mathcal{P}_{d,k,\mathrm{free}}(\mathbb{Z})$ defined by

$$\mathcal{P}^+_{d,k,\mathrm{free}}(\mathbb{Z}) := \{f \in \mathcal{P}_{d,k,\mathrm{free}}(\mathbb{Z}) : \alpha_k > 0\}.$$

Here is the variant of Example 5.4:

Let $d \geqslant 4$, k odd satisfying $2 \leqslant k \leqslant d$. There is no $q \in \mathbb{Q} \smallsetminus \{0,1\}$ and no distinct f and $g \in \mathcal{P}^+_{d,k,\mathrm{free}}(\mathbb{Z})$ such that

$$\mathfrak{h}_{q,0}(f) = g.$$

6 Proof of Theorem 3.4 and Corollary 3.9

We now write F and G as

$$\begin{cases} F(X,Y) = a_0X^d + a_\lambda X^{d-\lambda}Y^\lambda + a_{\lambda+5}X^{d-\lambda-5}Y^{\lambda+5} + a_{\lambda+6}X^{d-\lambda-6}Y^{\lambda+6} + \cdots + a_dY^d, \\ \\ G(X,Y) = b_0X^d + b_{\lambda'}X^{d-\lambda'}Y^{\lambda'} + b_{\lambda'+5}X^{d-\lambda'-5}Y^{\lambda'+5} + b_{\lambda'+6}X^{d-\lambda'-6}Y^{\lambda'+6} + \cdots + b_dY^d, \end{cases}$$

where $\lambda = \Lambda^+(F)$, $\lambda' = \Lambda^+(G)$, $a_0a_db_0b_da_\lambda b_{\lambda'} \neq 0$. By analogy with the above section, we introduce the two associated polynomials (see (4.6))

$$\begin{cases} f(t) = t^d + \alpha_\lambda t^{d-\lambda} + \alpha_{\lambda+5}t^{d-\lambda-5} + \alpha_{\lambda+6}t^{d-\lambda-6} + \cdots + \alpha_d, \ (\alpha_\lambda\alpha_d \neq 0) \\ \\ g(z) = z^d + \beta_{\lambda'}z^{d-\lambda'} + \beta_{\lambda'+5}z^{d-\lambda'-5} + \beta_{\lambda'+6}z^{d-\lambda'-6} + \cdots + \beta_d, \ (\beta_{\lambda'}\beta_d \neq 0), \end{cases} \tag{6.1}$$

with $\alpha_k = a_k/a_0$ and $\beta_k = b_k/b_0$ for $k = 1,\ldots,d$; we also set $\alpha_0 = \beta_0 = 1$. So the polynomials f and g have (at least) four coefficients equal to zero just after the second monomial (the second monomial of f is $\alpha_{\Lambda^+(f)}t^{d-\Lambda^+(f)}$, the first monomial is t^d) and we have

$$\max\{\lambda,\, \lambda'\} \leqslant d-5. \tag{6.2}$$

The analogue of Proposition 4.11 is the following.

Proposition 6.1. *Let $d \geqslant 10$. Consider in $\mathbb{C}[t]$ and $\mathbb{C}[z]$ respectively, two polynomials f and g (distinct or not) as in (6.1), satisfying (6.2) and the inequality*

$$\lambda + \lambda' \geqslant d. \tag{6.3}$$

Suppose that the discriminants of f and g do not vanish and suppose the existence of a homography $\mathfrak{h}$ such that $\mathfrak{h}(f) = g$. Then either

1. $\mathfrak{h}$ *is a homothety* $\mathfrak{h}_{q,0}$ *with* $q \in \mathbb{C}^\times$, *or*

2. $\mathfrak{h}$ *is a non affine homography of the form* $\mathfrak{h}_{0,r,0}$ *with* $r \in \mathbb{C}^\times$. *In that situation we have*

$$\lambda + \lambda' = d \tag{6.4}$$

and f *and* g *are of the form* $t^d + \alpha_\lambda t^{d-\lambda} + \alpha_d$ *and* $z^d + \beta_{\lambda'} z^{d-\lambda'} + \beta_d$, *with* $\alpha_d \beta_d = r^d$, *and* $\alpha_\lambda r^{\lambda'} = \alpha_d \beta_{\lambda'}$.

6.1 Heuristics again

Let $(q, r, s) \in \mathbb{C} \times \mathbb{C}^\times \times \mathbb{C}$ and $d \geqslant 3$, $\lambda, \lambda', \mu, \mu'$ positive integers. We are looking for the existence of two polynomials f, g in $\mathcal{P}_d$ satisfying

$$\kappa f(t) = (t-s)^d g\left(q + \frac{r}{t-s}\right)$$

for some $\kappa \in \mathbb{C}^\times$ and

$$\alpha_1 = \cdots = \alpha_{\lambda-1} = \alpha_{\lambda+1} = \cdots = \alpha_{\lambda+\mu-1} = 0$$
$$\beta_1 = \cdots = \beta_{\lambda'-1} = \beta_{\lambda'+1} = \cdots = \beta_{\lambda'+\mu'-1} = 0,$$

so that

$$f(t) = t^d + \alpha_\lambda t^{d-\lambda} + \sum_{j=\lambda+\mu}^{d} \alpha_j t^{d-j}$$

and

$$g(z) = z^d + \beta_{\lambda'} z^{d-\lambda'} + \sum_{j=\lambda'+\mu'}^{d} \beta_j z^{d-j},$$

(compare with (6.1)). According to the heuristic discussion of §4.5.1 with the two subsets

$$\mathcal{I} = \{1, \ldots, \lambda-1, \lambda+1, \ldots, \lambda+\mu-1\}, \quad \mathcal{J} = \{1, \ldots, \lambda'-1, \lambda'+1, \ldots, \lambda'+\mu'-1\},$$

with $a = \lambda + \mu - 2$ and $b = \lambda' + \mu' - 2$, we may expect that, given $d \geqslant 3$, $\lambda, \lambda', \mu, \mu'$ satisfying $\lambda + \lambda' + \mu + \mu' = d + 4$, outside a Zariski closed set of (q, r, s), there is a unique solution. We work out an example for sufficiently large d with $\lambda = \mu = 2$, $1 \leqslant \lambda' \leqslant d-1$, $\mu' = d - \lambda'$ below (Example 6.2).

When $\lambda + \lambda' + \mu + \mu' > d + 4$, we may expect that there is no solution. The main result of Proposition 6.1 is that this conclusion holds under the stronger assumptions $\mu \geqslant 5$, $\mu' \geqslant 5$, $\lambda + \lambda' \geqslant d$.

Example 6.2. Take $q = 1$, $r = 1$, $s = 2$, $1 \leqslant \lambda' \leqslant d-1$, $\mu' = d - \lambda'$,

$$\gamma = \begin{pmatrix} 1 & -1 \\ 1 & -2 \end{pmatrix}, \quad g(z) = z^d + \beta_{\lambda'} z^{d-\lambda'} + \beta_d,$$

$$\kappa f(t) = (t-1)^d + \beta_{\lambda'}(t-1)^{d-\lambda'}(t-2)^{\lambda'} + \beta_d (t-2)^d.$$

Since f is monic, we have

$$\kappa = 1 + \beta_{\lambda'} + \beta_d.$$

We are searching for $\beta_{\lambda'}$, β_d and κ such that $\alpha_1 = \alpha_3 = 0$, so that

$$f(t) = t^d + \alpha_2 t^{d-2} + \alpha_4 t^{d-4} + \cdots + \alpha_d.$$

We have

$$\kappa\alpha_1 = -d + A\beta_{\lambda'} - 2d\beta_d,$$
$$\kappa\alpha_3 = -\binom{d}{3} + B\beta_{\lambda'} - 8\binom{d}{3}\beta_d$$

with

$$A = -(d+\lambda'),$$
$$B = -8\binom{\lambda'}{3} - 4\binom{\lambda'}{2}(d-\lambda') - 2\lambda'\binom{d-\lambda'}{2} - \binom{d-\lambda'}{3}.$$

The determinant of the system of three equations in thee unknowns $\beta_{\lambda'}$, β_d and κ

$$\begin{cases} \beta_{\lambda'} + \beta_d - \kappa = -1 \\ A\beta_{\lambda'} - 2d\beta_d = d \\ B\beta_{\lambda'} - 8\binom{d}{3}\beta_d = \binom{d}{3}, \end{cases}$$

is

$$\Delta := \begin{vmatrix} 1 & 1 & -1 \\ A & -2d & 0 \\ B & -8\binom{d}{3} & 0 \end{vmatrix} = 8A\binom{d}{3} - 2dB;$$

this is a polynomial in d of degree 4 and which is multiple of d. It vanishes for at most three values of $d \neq 0$. In particular for d sufficiently large it is different from zero, thus this system has unique solution $(\kappa, \beta_{\lambda'}, \beta_d)$. We want to study the potential vanishing of the unknowns, as the parameter d tends to infinity, when the other parameter λ' is a fixed positive integer. Standard computations lead to the equality

$$B = \frac{1}{6}\left(-d^3 - 3d^2(\lambda'-1) + d(-3\lambda'^2 + 12\lambda' - 2) - \lambda'(\lambda'^2 - 9\lambda + 14)\right),$$

which is summarized as

$$B = -\frac{d^3}{6} - \frac{d^2}{2}(\lambda'-1) + O(d).$$

We use the formula

$$\binom{d}{3} = \frac{d^3}{6} - \frac{d^2}{2} + O(d).$$

• To study the value of $\beta_{\lambda'}$, we consider the determinant

$$\Delta = \begin{vmatrix} -1 & 1 & -1 \\ d & -2d & 0 \\ \binom{d}{3} & -8\binom{d}{3} & 0 \end{vmatrix} = d\binom{d}{3}\begin{vmatrix} 1 & 2 \\ 1 & 8 \end{vmatrix} = 6d\binom{d}{3} = d^4 + O(d^3).$$

So we obtain that $\beta_{\lambda'} \longrightarrow -1$ as $d \longrightarrow +\infty$.

• To study the value of β_d, we consider the determinant

$$\begin{vmatrix} 1 & -1 & -1 \\ A & d & 0 \\ B & \binom{d}{3} & 0 \end{vmatrix} = -A\binom{d}{3} + Bd = \frac{\lambda'}{3}d^3 + O(d^2).$$

Using the above value of Δ, we deduce that, for large d, β_d tends to zero, without vanishing.

• To study the value of κ, we already know that κ tends to zero as d tends to infinity: this follows from the first equation of the system. To prove that κ does not vanish for large values of d we compute the determinant

$$\begin{vmatrix} 1 & 1 & -1 \\ A & -2d & d \\ B & -8\binom{d}{3} & \binom{d}{3} \end{vmatrix} = \begin{vmatrix} 0 & 0 & -1 \\ A+d & -d & d \\ B+\binom{d}{3} & -7\binom{d}{3} & \binom{d}{3} \end{vmatrix} = -7(A+d)\binom{d}{3} + d(B + \binom{d}{3}),$$

which is finally equal to

$$\frac{2\lambda'}{3}d^3 + O(d^2).$$

By dividing by the value of Δ, we find that κ tends to zero, without vanishing.

Using

$$\binom{d}{2} - 4\binom{\lambda'}{2} - 2\lambda'(d-\lambda') - \binom{d-\lambda'}{2} = -\frac{\lambda'}{2}(2d+\lambda'-3)$$

we deduce that when d tends to infinity, we have

$$\alpha_2 \to -\frac{\lambda'}{2}(2d+\lambda'-3) \neq 0.$$

Also from

$$\binom{d}{4} - 16\binom{\lambda'}{4} - 8\binom{\lambda'}{3}(d-\lambda') - 4\binom{b}{2}\binom{d-\lambda'}{2} - 2\lambda'\binom{d-\lambda'}{3} - \binom{d-\lambda'}{4} =$$
$$-\frac{1}{24}\lambda'(-90+4d^3+6d^2(-5+\lambda')+83\lambda'-18\lambda'^2+\lambda'^3+d(82-42\lambda'+4\lambda'^2))$$

we conclude that $\alpha_4 \neq 0$ for sufficiently large d.

This completes the claim of Example 6.2 that for $\lambda = \mu = 2$, $1 \leqslant \lambda' \leqslant d-1$ and $\mu = d - \lambda'$, there is an example of a pair of polynomial f, g in $\mathcal{P}_d$ and an homography $\mathfrak{h}$ satisfying $\mathfrak{h}(f) = g$.

6.2 Proof of Proposition 6.1

Assume first that $\mathfrak{h}$ is an affine homography $\mathfrak{h}_{q,r}$ with $q \in \mathbb{C}^\times$. We use the same argument as in the proof given in §4.3. The conditions (6.2) and (6.3) imply that $\lambda \geqslant 2$ and $\lambda' \geqslant 2$, thus the sums of the roots of f and g are equal to zero. Hence $r = 0$ and $\mathfrak{h}$ is a homothety $\mathfrak{h}_{q,0}$.

Now consider the case where $\mathfrak{h}$ is a non affine homography: $\mathfrak{h} = \mathfrak{h}_{q,r,s}$ with $r \in \mathbb{C}^\times$. The proof below works by contradiction. We will show that each of the three cases $\mathfrak{h}_{q,r,s}$ with q and $s \neq 0$, with $q = 0$ and $s \neq 0$ and finally with $q \neq 0$ and $s = 0$ are impossible.

To start with, we consider the general case $(q, r, s) \in \mathbb{C} \times \mathbb{C}^\times \times \mathbb{C}$.

As a consequence of Lemma 4.17, we suppose that λ and λ' satisfy the inequalities

$$d \leqslant \lambda + \lambda' \leqslant d+2. \tag{6.5}$$

Thanks to Lemma 4.14, we again appeal to the equality (4.22). Recall that we have

$$\beta_0 = 1,\ \beta_{\lambda'} \neq 0,\ \beta_\ell = 0 \text{ for } 1 \leqslant \ell \leqslant \lambda'-1 \text{ and for } \lambda'+1 \leqslant \ell \leqslant \lambda'+4.$$

For

$$j \geqslant d - \lambda + 1, \tag{6.6}$$

the derivative $f^{(j)}(t)$ is a monomial, in particular we have the equality

$$f^{(j)}(s) = \frac{d\,!}{(d-j)\,!} \cdot s^{d-j}. \tag{6.7}$$

We apply (4.22) for four consecutive values of j, chosen in order that exactly two non zero β_i are present on the RHS of these equalities. The corresponding indices are necessarily $i = 0$ and $i = \lambda'$. In this case (4.22) becomes

$$\frac{f^{(j)}(s)}{f(s)} = \frac{d\,!}{(d-j)\,!} \cdot \left(\frac{q}{r}\right)^j + \binom{d-\lambda'}{j-\lambda'} \cdot j\,! \cdot \left(\frac{q}{r}\right)^j \cdot \frac{\beta_{\lambda'}}{q^{\lambda'}}. \tag{6.8}$$

Hence the four values of j are either

$$\lambda', \lambda'+1, \lambda'+2, \lambda'+3 \quad \text{or} \quad \lambda'+1, \lambda'+2, \lambda'+3, \lambda'+4.$$

This has to be compatible with (6.5) and (6.6): so we write $j = d - \lambda + \ell$ with

$$\ell = \ell_0 + i,\ (i = 0,1,2,3) \text{ where } \begin{cases} \ell_0 = 1 & \text{if } \lambda + \lambda' = d \text{ and if } \lambda + \lambda' = d+1, \\ \ell_0 = 2 & \text{if } \lambda + \lambda' = d+2. \end{cases} \tag{6.9}$$

We apply the formulas (6.8) with the four values of ℓ given in (6.9).

$$\frac{f^{(d-\lambda+\ell)}(s)}{f(s)} = \frac{d\,!}{(\lambda-\ell)\,!} \cdot \left(\frac{q}{r}\right)^{d-\lambda+\ell} + \binom{d-\lambda'}{d-\lambda-\lambda'+\ell} \cdot (d-\lambda+\ell)\,! \cdot \left(\frac{q}{r}\right)^{d-\lambda+\ell} \cdot \frac{\beta_{\lambda'}}{q^{\lambda'}}. \tag{6.10}$$

By (6.7) the four equations of the system (6.10) become

$$s^d = \left(\left(\frac{qs}{r}\right)^{d-\lambda+\ell} + \frac{(d-\lambda')\,! \cdot (d-\lambda+\ell)\,!}{(d-\lambda-\lambda'+\ell)\,! \cdot d\,!} \cdot \left(\frac{qs}{r}\right)^{d-\lambda+\ell} \cdot \frac{\beta_{\lambda'}}{q^{\lambda'}} \right) f(s). \tag{6.11}$$

• **We now prove that the case $q \neq 0$ and $s \neq 0$ is impossible.**

To shorten notations, set $\nu = \lambda + \lambda' - d$, so that $\nu \in \{0,1,2\}$, and write $\tau = qs/r$, $\kappa = \beta_{\lambda'}/q^{\lambda'}$ (since $q \neq 0$), and

$$A_\ell := \frac{(d-\lambda+\ell)\,!}{(\ell-\nu)\,!} \cdot \frac{(d-\lambda')\,!}{d\,!},$$

for the four values of ℓ given in (6.9). So (6.11) becomes

$$s^d = \tau^{d-\lambda+\ell}\,(1 + \kappa A_\ell)\, f(s). \tag{6.12}$$

We now exploit the fact that $s \neq 0$. We notice that (6.12) implies $\tau \neq 0$ and $f(s) \neq 0$, and also $1 + \kappa A_\ell \neq 0$ for the four values of ℓ given in (6.9). We eliminate the variable s^d among the four equations (6.12) and we obtain the three equalities, which are satisfied by the two unknowns τ and κ, which both are $\neq 0$.

$$\begin{cases} \tau = \dfrac{1 + \kappa A_{\ell_0}}{1 + \kappa A_{\ell_0+1}}, \\[2ex] \tau = \dfrac{1 + \kappa A_{\ell_0+1}}{1 + \kappa A_{\ell_0+2}}, \\[2ex] \tau = \dfrac{1 + \kappa A_{\ell_0+2}}{1 + \kappa A_{\ell_0+3}}. \end{cases}$$

We now write necessary and sufficient conditions to ensure that the two first equations are compatible and that the two last ones are compatible. We obtain the following system of two equations

$$\begin{cases} (1 + \kappa A_{\ell_0})(1 + \kappa A_{\ell_0+2}) = (1 + \kappa A_{\ell_0+1})^2 \\ (1 + \kappa A_{\ell_0+1})(1 + \kappa A_{\ell_0+3}) = (1 + \kappa A_{\ell_0+2})^2 \end{cases}$$

which (since $\kappa \neq 0$) is equivalent to the system

$$\begin{cases} \big(A_{\ell_0+1}^2 - A_{\ell_0} A_{\ell_0+2}\big)\kappa = A_{\ell_0} + A_{\ell_0+2} - 2A_{\ell_0+1}, \\ \big(A_{\ell_0+2}^2 - A_{\ell_0+1} A_{\ell_0+3}\big)\kappa = A_{\ell_0+1} + A_{\ell_0+3} - 2A_{\ell_0+2}. \end{cases} \tag{6.13}$$

If the system (6.13) has a solution then we have

$$(A_{\ell_0+1}^2-A_{\ell_0}A_{\ell_0+2})(A_{\ell_0+1}+A_{\ell_0+3}-2A_{\ell_0+2}) = (A_{\ell_0+2}^2-A_{\ell_0+1}A_{\ell_0+3})(A_{\ell_0}+A_{\ell_0+2}-2A_{\ell_0+1}). \tag{6.14}$$

We factorize each A_ℓ as

$$A_\ell = (d-\lambda+1)\,!\cdot\frac{(d-\lambda')\,!}{d\,!}A_\ell^*,$$

with

$$A_\ell^* := \prod_{i=2}^{\ell}\frac{\lambda'+i-\nu}{(i-\nu)^+}, \tag{6.15}$$

with the convention $x^+ = \max(x,\,1)$.

By homogeneity, the equality (6.14) is equivalent to

$$(A_{\ell_0+1}^{*2}-A_{\ell_0}^*A_{\ell_0+2}^*)(A_{\ell_0+1}^*+A_{\ell_0+3}^*-2A_{\ell_0+2}^*) = (A_{\ell_0+2}^{*2}-A_{\ell_0+1}^*A_{\ell_0+3}^*)(A_{\ell_0}^*+A_{\ell_0+2}^*-2A_{\ell_0+1}^*). \tag{6.16}$$

Actually, the equality (6.16) cannot hold. This is the purpose of the following lemma.

Lemma 6.3. *Let d, λ and λ' be positive integers such that $d \leqslant \lambda+\lambda' \leqslant d+2$ and $\ell_0 \in \{1,2\}$. Let A_ℓ^* $(1 \leqslant \ell \leqslant 5)$ be defined by (6.15) with $\nu = \lambda+\lambda'-d$. Define*

$$Q := \frac{(A_{\ell_0}^*+A_{\ell_0+2}^*-2A_{\ell_0+1}^*)(A_{\ell_0+2}^{*2}-A_{\ell_0+1}^*A_{\ell_0+3}^*)}{(A_{\ell_0+1}^*+A_{\ell_0+3}^*-2A_{\ell_0+2}^*)(A_{\ell_0+1}^{*2}-A_{\ell_0}^*A_{\ell_0+2}^*)}. \tag{6.17}$$

Then have

$$Q = \begin{cases} \dfrac{\lambda'+3}{3(\lambda'+2)} & \text{if } \lambda+\lambda' = d, \\[2ex] \dfrac{\lambda'+2}{2(\lambda'+1)} & \text{if } \lambda+\lambda' = d+1, \\[2ex] \dfrac{1}{2}(\lambda'+2) & \text{if } \lambda+\lambda' = d+2. \end{cases}$$

In these three cases, we have $Q \neq 1$.

Proof of Lemma 6.3. We first suppose that $\lambda+\lambda' = d+2$, that is $\ell_0 = 2$ and $\nu = 2$. We have the equalities

$$A_1^* = 1,\ A_2^* = \lambda',\ A_3^* = \lambda'(\lambda'+1),\ A_4^* = \frac{\lambda'(\lambda'+1)(\lambda'+2)}{2},\ A_5^* = \frac{\lambda'(\lambda'+1)(\lambda'+2)(\lambda'+3)}{6}.$$

With these values, we obtain the equalities

$$A_2^*+A_4^*-2A_3^* = \frac{1}{2}\cdot\lambda'^2(\lambda'-1),$$

$$A_4^{*2}-A_3^*A_5^* = \frac{1}{12}\,\lambda'^3(\lambda'+1)^2(\lambda'+2),$$

$$A_3^*+A_5^*-2A_4^* = \frac{1}{6}\lambda'^2(\lambda'-1)(\lambda'+1)$$

and

$$A_3^{*2}-A_2^*A_4^* = \frac{1}{2}\lambda'^3(\lambda'+1).$$

By (6.17), we finally obtain

$$Q = \frac{(A_2^* + A_4^* - 2A_3^*)(A_4^{*2} - A_3^* A_5^*)}{(A_3^* + A_5^* - 2A_4^*)(A_3^{*2} - A_2^* A_4^*)} = \frac{1}{2}(\lambda' + 2).$$

This completes the proof of Lemma 6.3 in that case $\lambda + \lambda' = d + 2$.

We now suppose that $d \leqslant \lambda + \lambda' \leqslant d + 1$, that is $\ell_0 = 1$ and $\nu \in \{0, 1\}$. In that case, we can forget the symbol $^+$ in the definition (6.15). We have the equalities

$$A_1^* = 1,\ A_2^* = \frac{\lambda' + 2 - \nu}{2 - \nu},\ A_3^* = \frac{(\lambda' + 2 - \nu)(\lambda' + 3 - \nu)}{(2 - \nu)(3 - \nu)},$$
$$A_4^* = \frac{(\lambda' + 2 - \nu)(\lambda' + 3 - \nu)(\lambda' + 4 - \nu)}{(2 - \nu)(3 - \nu)(4 - \nu)}.$$

With these values, we obtain the equalities

$$A_1^* + A_3^* - 2A_2^* = \frac{\lambda'(\lambda' - 1)}{(2 - \nu)(3 - \nu)},$$

$$A_3^{*2} - A_2^* A_4^* = \frac{\lambda'(\lambda' + 2 - \nu)(\lambda' + 3 - \nu)}{(2 - \nu)^2(3 - \nu)^2(4 - \nu)},$$

$$A_2^* + A_4^* - 2A_3^* = \frac{\lambda'(\lambda' - 1)(\lambda' + 2 - \nu)}{(2 - \nu)(3 - \nu)(4 - \nu)}$$

and

$$A_2^{*2} - A_1^* A_3^* = \frac{\lambda'(\lambda' + 2 - \nu)}{(2 - \nu)^2(3 - \nu)}.$$

By (6.17), we finally obtain

$$Q = \frac{(A_1^* + A_3^* - 2A_2^*)(A_3^{*2} - A_2^* A_4^*)}{(A_2^* + A_4^* - 2A_3^*)(A_2^{*2} - A_1^* A_3^*)} = \frac{\lambda' + 3 - \nu}{(3 - \nu)(\lambda' + 2 - \nu)}.$$

Lemma 6.3 is proved also in that case. □

Thanks to Lemma 6.3, this completes the proof that in Proposition 6.1 the case $q \neq 0$ and $s \neq 0$ is impossible.

We continue the proof of Proposition 6.1 in the other cases.

• **We now prove that the case $q = 0$ and $s \neq 0$ is impossible.**

Suppose that $q = 0$. The second equality of (6.1) implies that $\beta_{\lambda'+1} = 0$. The equality (4.23) gives the vanishing of the derivative

$$f^{(\lambda'+1)}(s) = 0. \tag{6.18}$$

By (6.5) we know that

$$d - \lambda + 1 \leqslant \lambda' + 1 < d,$$

where the last inequality comes from the assumption (6.2). This means that the derivative $f^{(\lambda'+1)}(t)$ is a monomial in t with degree $\geqslant 1$. Combining with (6.18) we obtain that $s = 0$. Contradiction.

• **We now prove that the case $q \neq 0$ and $s = 0$ is impossible.**

We benefit from the symmetry of the question to consider the homography $\mathfrak{h}_{s,r,q}$ which transforms g to f. We also take into account the symmetry of the assumptions

(6.2) and (6.5) concerning these two polynomials. By the above alinea, we deduce that the case $q \neq 0$ and $s = 0$ is also impossible.

• **The remaining case is $q = s = 0$.**

We have $\mathfrak{h}_{0,r,0}(t) = r/t$. By Lemma 4.9 we deduce

$$[\mathfrak{h}_{0,r,0}(f)](z) = \frac{1}{f(0)} \cdot z^d f\left(\frac{r}{z}\right) = \frac{1}{\alpha_d} \cdot z^d f\left(\frac{r}{z}\right).$$

This relation gives the list of equalities

$$\alpha_d \beta_j = \alpha_{d-j} r^j \ (0 \leqslant j \leqslant d)$$

after identification of the coefficients. In this relation, we fix $j = d - \lambda$. Since $\alpha_\lambda \neq 0$, we deduce that $\beta_{d-\lambda} \neq 0$, which implies $d - \lambda \geqslant \lambda'$. This condition is compatible with (6.5) if and only if (6.4) holds. By the definition of λ and λ' we deduce that f and g are both the sum of two or three monomials as indicated.

Recalling that $\alpha_0 = \beta_0 = 1$, we obtain the conditions of the second item of Proposition 6.1. This completes the proof of this proposition.

6.3 Proof of Theorem 3.4 and Corollary 3.9

Proof of Theorem 3.4. Let F and G be two forms in $\mathcal{E}$ and γ an homography such that $F \circ \gamma = G$. Our goal is to prove $F = G$.

Like in §5.1, we consider the two monic polynomials f and g associated with F and G and the homography $\mathfrak{h} = \tilde{\gamma}$ and we apply Proposition 6.1. The last assumption (3.4) of Theorem 3.4 imply that $\mathfrak{h}$ is of the form $\mathfrak{h}_{q,0}$ for some $q \in \mathbb{K}^\times$. By assumption $\mathcal{E}$ is $\mathbb{K}$–reduced, hence $\mathbb{K}$–dilation free, and therefore $F = G$. □

Proof of Corollary 3.9. Consider the first item of Corollary 3.9. The assumption $a_{d-1} = 1$ implies that the set $\mathcal{V}_d^{(1)}(\mathbb{K})$ does not contain binomials nor trinomials of the form (3.4). According to Lemma 5.1, the set $\mathcal{V}_d^{(1)}(\mathbb{K})$ is $\mathbb{K}$–dilation free. The first item now follows from Theorem 3.4.

For the proof of the second item, we use Lemma 5.2 together with Theorem 3.4 in the same way as in the proof of the second item of Corollary 3.6 in section 5.2. □

References

[FW2020] Étienne Fouvry & Michel Waldschmidt, *Sur la représentation des entiers par les formes cyclotomiques de grand degré, On the representation of integers by cyclotomic forms of large degree,* Bull. Soc. Math. France **148** (2020), no. 2, 253–282.
Corrigendum, submitted.

[FW2023] Étienne Fouvry & Michel Waldschmidt, *Number of integers represented by families of binary forms I.* Acta Arithmetica, **209** (2023), 219–267.
arXiv: 2206.03733 [math.NT]. Zbl 07768665 MR4665259

[FW2024] Étienne Fouvry & Michel Waldschmidt, *Number of integers represented by families of binary forms II: binomial forms.* Acta Arithmetica, **214** (2024), 271–287.
arXiv:2306.02462 [math.NT]. MR4772287

[FW2026] Étienne Fouvry & Michel Waldschmidt, *Number of integers represented by families of binary forms IV: positive definite forms*. In preparation.

[FW2026+] Étienne Fouvry & Michel Waldschmidt, *Number of integers represented by families of binary forms V: trinomial forms*. In preparation.

[Ri1968] John Riordan. Combinatorial identities. New York-London-Sydney: John Wiley and Sons, 256 p. (1968).
Zbl 0194.00502 MR0554488

[Ro1955] Herbert Robbins. *A remark on Stirling's formula*. Amer. Math. Monthly **62** (1955), 26–29.
MR0069328

[SX2019] Cameron L. Stewart & Stanley Yao Xiao, *On the representation of integers by binary forms*. Math. Ann. **375** (2019), no. 1-2, 133–163.
Zbl 1464.11035 MR4000237

[W2000] Michel Waldschmidt, *Diophantine Approximation on Linear Algebraic Groups*. Grundlehren der Mathematischen Wissenschaften **326**. Springer-Verlag, Berlin-Heidelberg, 2000.
Zbl 0944.11024 MR1756786

Étienne Fouvry
Univ. Paris–Saclay, CNRS
Laboratoire de Mathématiques d'Orsay
91405 Orsay, France
E-mail: Etienne.Fouvry@universite-paris-saclay.fr

Michel Waldschmidt
Sorbonne Université
CNRS, IMJ–PRG
75005 Paris, France
E-mail: michel.waldschmidt@imj-prg.fr