Divisibility of Discriminants of Homogeneous Polynomials

by

Andrej Vuković

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Pure Mathematics

Waterloo, Ontario, Canada, 2023

Examining Committee Membership

The following served on the Examining Committee for this thesis. The decision of the Examining Committee is by majority vote.

External Examiner:	Jacob Tsimerman Professor, Dept. of Mathematics, University of Toronto
Supervisor(s):	Xiaoheng Jerry Wang Associate Professor, Dept. of Pure Mathematics, University of Waterloo David McKinnon Professor, Dept. of Pure Mathematics, University of Waterloo
Internal Member:	Yu-Ru Liu Professor, Dept. of Pure Mathematics, University of Waterloo
Internal Member:	Matthew Satriano Associate Professor, Dept. of Pure Mathematics, University of Waterloo
Internal-External Member:	David Jao Professor, Dept. of C&O, University of Waterloo

Author’s Declaration

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

We prove several square-divisibility results about the discriminant of homogeneous polynomials of arbitrary degree and number of variables, when certain coefficients vanish, and give characterizations for when the discriminant is divisible by p^2 for p prime.

We also prove several formulas about a certain polynomial Δ'_d, first introduced in [8], which behaves like an average over the partial derivatives of Δ_d, the discriminant of degree d polynomials. In particular, we prove that Δ'_d is irreducible when $d \geq 5$.

Acknowledgements

I would like to thank my advisors, Jerry Wang and David McKinnon, for their patience and support. Particular thanks go to Jerry, my primary advisor, for introducing me to this subject and guiding me through it in weekly meetings. I would also like to thank Matthew Satriano, Jason Bell, and Cameron Stewart for helpful discussions.

This research was supported by the Natural Sciences and Engineering Research Council of Canada (NSERC) [grant number PGSD3-535032-2019, promoted to CGSD-535001-2019 in April 2021].

Dedication

To my parents.

Table of Contents

List of Figures

Chapter 1

Introduction

A classical question in analytic number theory is, "Given a multivariate polynomial with integer coefficients, what is the probability that when evaluating the polynomial at random integers, the resulting integer is squarefree, i.e., is not divisible by the square of a prime?" The simplest case of one variable and degree one asks for the probability that a random integer is squarefree, which is well-known to be $6/\pi^2$. The one variable degree two case can also be solved by elementary methods. The one variable degree three case was solved by Hooley [17]. For homogeneous polynomials of two variables, the question is known up to degree 6 by Greaves [16]. Conditional on the *abc* conjecture, Granville [15] proved it in general in the one variable case, and Poonen [25] proved it in the multivariate case, albeit using a different ordering.

The difficulty of the squarefree counting problem lies in obtaining a good upper bound for a “tail estimate” of the form

$$\# \bigcup_{p>M} \{(a_1, \dots, a_n) \colon |a_i| < X, p^2 \mid F(a_1, \dots, a_n)\}.$$

There are two “reasons” for p^2 to divide $F(a_1, \dots, a_n)$: mod p or mod p^2. We say $p^2 \mid F(a_1, \dots, a_n)$ *strongly* if $p^2 \mid F(b_1, \dots, b_n)$ for any $b_i \equiv a_i \pmod p$. Otherwise, we say it divides $F(a_1, \dots, a_N)$ *weakly.* The strongly divisible case can be handled in general by the quantitative Ekedahl sieve [3]. The weakly divisible case is the hardest step. This has been done for many situations in recent years by Manjul Bhargava and his many collaborators: for various invariant polynomials that arise from representations used to count number fields and Selmer group averages in [1, 2, 6, 7, 4, 5]; for the discriminant of monic polynomials and general polynomials in [9, 10]; and for the polynomial $x_1^4 + x_2^3$ in [30]. A key step in understanding the weakly divisible case is to understand where the “hidden” p^2 is. In this thesis, we focus on the discriminant polynomial $\Delta_{d,k}$ of homogeneous polynomials in $k+1$ variables $x_0, \dots, x_k$ and degree d. Such an f has $\binom{k+d}{d}$ coefficients, and the discriminant $\Delta_{d,k}$ is an integral irreducible polynomial in the coefficients of f of degree $(k+1)(d-1)^k$ with relatively prime coefficients. Over an algebraically closed field L, the discriminant $\Delta_{d,k}(f)$ vanishes whenever the variety $V(f) \subseteq \mathbb{P}^k$ cut out by f has a singular point over L, and in fact it is defined uniquely up to sign over an algebraically closed field by this requirement along with the fact that it is integral, irreducible, and primitive. We prove:

Theorem 1. Let $f(x_0, \dots, x_k) \in \mathbb{Z}[x_0, \dots, x_k]$ be a homogeneous polynomial of degree $d \geq 2$. Let p be a prime such that $p^2 \mid \Delta_{d,k}(f)$ weakly. Then there exists a linear change of variables such that the coefficients of $x_0^d, x_0^{d-1}x_1, x_0^{d-1}x_2, \ldots, x_0^{d-1}x_{k-1}$ are all divisible by p^2 and the coefficient of $x_0^{d-1}x_k$ is divisible by p.

To prove this, we consider the divisibility of $\Delta_{d,k}(f)$ when the coefficients of $x_0^{d-1}x_i$ for $i = 0, \ldots, k-1$ all vanish, and we prove:

Theorem 2. Let $f(x_0, \ldots, x_k) \in \mathbb{Z}[a_0, \ldots, a_N][x_0, \ldots, x_k]$, where $N = \binom{k+d}{d} - 1$, be a generic homogeneous polynomial of degree $d \geq 2$. Let a_i denote the coefficient of $x_0^{d-1}x_i$ for $i = 0, \ldots, k$. Then $a_k^2 \mid \Delta_{d,k}(f)$ in the quotient ring $\mathbb{Z}[a_0, \ldots, a_N]/(a_0, \ldots, a_{k-1})$.

In the case $k = 1$, this is consistent with the formula

$$\Delta_{d,1}(a_1 x^{d-1} y + \cdots + a_d y^d) = a_1^2 \Delta_{d-1,1}(a_1 x^{d-1} + \cdots + a_d y^{d-1}),$$

which can be obtained directly from the Sylvester matrix for the resultant.

It then follows by symmetry that:

Corollary 3. Let $a_0, \ldots, a_N$ denote the coefficients of a generic homogeneous polynomial in $x_0, \ldots, x_k$ of degree $d \geq 2$, where $N = \binom{k+d}{d} - 1$, such that a_i is the coefficient of $x_0^{d-1}x_i$ for $i = 0, \ldots, k$. Then

$$\Delta_{d,k} \equiv a_0 D_0 \pmod{(a_0, \ldots, a_k)^2}$$

for some polynomial $D_0 \in \mathbb{Z}[a_{k+1}, \ldots, a_N]$.

In the case $k = 1$, this is consistent with the formula

$$\Delta_{d,1}(a_0 x^d + \cdots + a_d y^d) \equiv -4 a_0 a_2^3 \Delta_{d-2,1}(a_2 x^{d-2} + \cdots + a_d y^{d-2}) \pmod{(a_0, a_1)^2}. \quad (1.1)$$

To obtain this formula, first note that by setting $a_0 = 0$ in the Sylvester matrix for the discriminant of $f(x,y) = a_0x^d + \cdots + a_dy^d$, we can conclude that $\Delta_{d,1}(f) = a_0F + a_1^2\Delta_{d-1,1}(a_1x^{d-1} + \cdots + a_{d-1}y^{d-1})$ for some $F \in \mathbb{Z}[a_0,\ldots,a_d]$, so working modulo $(a_0,a_1)^2$ is equivalent to working modulo (a_0^2, a_1). Equation (1.1) then follows by another Sylvester matrix calculation by setting $a_1 = 0$.

Let $f(x_0,\ldots,x_k) \in \mathbb{Z}[x_0,\ldots,x_k]$ with coefficients $a_i(f)$ for $i = 0,\ldots,N$, where $N = \binom{k+d}{d} - 1$, d is the degree of f, and the coefficients have the same ordering as in Corollary 3. Observe now that if $a_0(f),\ldots,a_d(f)$ are all divisible by a prime p, then we have

$$\frac{\partial\Delta_{d,k}}{\partial a_0}(f) \equiv D_0(f) \pmod{p}.$$

Hence, if we know that $p \mid D_0(f)$, then we have $p^2 \mid \Delta_{d,k}(f)$. As a result, we also have the following application to the strongly divisible case.

Theorem 4. Let $f(x_0,\ldots,x_k) \in \mathbb{Z}[x_0,\ldots,x_k]$ be a homogeneous polynomial of degree $d \geq 2$. Let p be a prime. Denote all the coefficients of f by $a_0(f),\ldots,a_N(f)$, where $N = \binom{k+d}{d} - 1$. Suppose

$$p \mid \Delta_{d,k}(f), \qquad \text{and} \qquad p \mid \frac{\partial\Delta_{d,k}}{\partial a_i}(f) \quad \text{for all } i = 0,\ldots,N.$$

Then $p^2 \mid \Delta_{d,k}(f)$ strongly.

We conjecture that the same behaviour happens to any polynomial.

Conjecture 5. Let $F(x_0,\ldots,x_N) \in \mathbb{Z}[x_0,\ldots,x_N]$ be any polynomial. Then for sufficiently large primes p, depending on F, whenever $a_0, \ldots, a_N \in \mathbb{Z}$ are such that

$$p \mid F(a_0, \ldots, a_N), \qquad \text{and} \qquad p \mid \frac{\partial F}{\partial a_i}(a_0, \ldots, a_N) \quad \text{for all} \;\; i = 0, \ldots, N, \tag{1.2}$$

we also have $p^2 \mid F(a_0, \ldots, a_N)$.

It is easy to see that Conjecture 5 reduces to the case where F is a squarefree homogeneous polynomial. When F is a squarefree binary form in x_0, x_1 of degree d, we see that $\Delta_{d,1}(F) \neq 0$ and if $p \nmid \Delta_{d,1}(F)$, then (1.2) can only happen when $d \geq 2$ and $p \mid a_0(f)$ and $p \mid a_1(f)$, which imply that $p^2 \mid F(a_0, a_1)$. This argument fails when there are at least three variables because a squarefree polynomial can have vanishing discriminant. For example the polynomial $F(x_0, x_1, x_2) = x_0 x_1^2 + x_2^3$ is squarefree (even irreducible) but has discriminant zero.

We can give an explicit formula for D_0 in the case of ternary cubic forms. We write

$$f(x_0, x_1, x_2) = a_0 x_0^3 + x_0^2(a_1 x_1 + a_2 x_2) + x_0 Q(x_1, x_2) + C(x_1, x_2),$$

where Q is a binary quadratic form and C is a binary cubic form. Then we have, by the explicit formula of $\Delta_{3,2}$ in [7, (1)-(3)],

$$\Delta_{3,2}(f) \equiv a_0\, \Delta_{2,1}(Q)^3 \operatorname{Res}(Q, C) \pmod{(a_0, a_1, a_2)^2}, \tag{1.3}$$

where $\operatorname{Res}(Q, C)$ is the resultant of Q and C. In light of (1.1) and (1.3), we suspect in general that if

$$f(x_0, x_1, \dots, x_k) = a_0 x_0^d + x_0^{d-1}(a_1x_1 + \cdots + a_kx_k) + x_0^{d-2}Q(x_1, \dots, x_k) + \cdots ,$$

then $\Delta_{2,k-1}(Q)^3 \mid D_0$. We can prove the weaker result that $\Delta_{2,k-1}(Q) \mid D_0$.

Theorem 6. Let $f(x_0, \dots, x_k) \in \mathbb{Z}[a_0, \dots, a_N][x_0, \dots, x_k]$ be a generic homogeneous polynomial of degree $d \geq 2$, where $N = \binom{k+d}{d} - 1$, expressed as

$$f(x_0, x_1, \dots, x_k) = a_0 x_0^d + x_0^{d-1}(a_1x_1 + \cdots + a_kx_k) + x_0^{d-2}Q(x_1, \dots, x_k) + \cdots$$

where $Q(x_1, \dots, x_k)$ is a quadratic form. Then, in the ring $\mathbb{Z}[a_0, \dots, a_N]/(a_1, \dots, a_k, \Delta_{2,k-1}(Q))$, $a_0^2 \mid \Delta_{d,k}(f)$.

Our final results concern a certain polynomial $\Delta'_d(f)$ first defined in [8]. Given a polynomial $f(x) = a_0x^d + \cdots + a_d$ with degree $d \geq 3$ (so $a_0 \neq 0$) and roots $r_1, \dots, r_d$, we define

$$\Delta'_d(f) = \sum_{i<j} \frac{\Delta_d(f)}{(r_i - r_j)^2},$$

where $\Delta_d(f)$ denotes the usual polynomial discriminant of $f(x)$. Since Δ'_d is a symmetric integer polynomial in the roots $r_1, \dots, r_d$, it can be written as an integer polynomial in the coefficients of f. In [8], this polynomial is used to generalize the notions of strong and weak divisibility when a high power of p divides $\Delta_d(f)$.

Notice that if $p \mid \Delta_d(f)$ and $p \mid \Delta'_d(f)$, then modulo p, the polynomial $f(x)$ either has a triple root or two pairs of double roots, implying that $p^2 \mid \Delta_d(f)$ strongly. When $d = 3$

and $d = 4$, we have the factorizations

$$\begin{aligned}
\Delta_3' &= (a_1^2 - 3a_0a_2)^2 \\
\Delta_4' &= (-a_2^2 + 3a_1a_3 - 12a_0a_4) \\
&\times \ (-a_1^2a_2^2 + 4a_0a_2^3 + 3a_1^3a_3 - 14a_0a_1a_2a_3 + 18a_0^2a_3^2 + 6a_0a_1^2a_4 - 16a_0^2a_2a_4)
\end{aligned}$$

The polynomial Δ_3' is the cube root of the discriminant of Δ_3 as a polynomial in a_3. When $\Delta_4 = 0$, the first factor of Δ_4' corresponds to when f has a triple root, and the second factor of Δ_4' corresponds to when f has a pair of double roots. It is then natural to ask whether a similar factorization exists in any degree. The answer is negative.

Theorem 7. For all $d \geq 5$, Δ_d' is irreducible in $\mathbb{C}[a_0, \ldots, a_d]$.

We suspect this is related to the insolubility of quintics!

We will give two proofs for the main divisibility result, Theorem 2. We note first that when $d = 2$, the discriminant is given by

$$\Delta_{2,k}(f) = (-1)^{k(k+1)/2} \det(A_f),$$

where A_f is the $(k+1) \times (k+1)$ matrix of the second partial derivatives of the quadratic form f. Theorem 2 then follows immediately. So we may assume $d \geq 3$. We will also assume that $k \geq 2$ since the case $k = 1$ is simply the case of binary forms and the result is known by (1.1). We will give one proof in Chapter 2 using the theory of A-discriminants from [13]. They are generalizations of the usual discriminant, characterizing whether $V(f)$ has a singular point when certain monomials do not appear in f. We use the degree formula of Matsui–Takeuchi [24] to compute the degree of the A-discriminant when the monomials $x_0^d, x_0^{d-1}x_1, \ldots, x_0^{d-1}x_{k-1}$ do not appear, and we prove that it is exactly $\deg(\Delta_{d,k}) - 2$. A little bit of algebraic geometry is then used to show that $\Delta_{d,k}$ is exactly the square of the coefficient of $x_0^{d-1}x_k$ multiplied by the A-discriminant, up to scaling.

We will give a second proof of Theorem 2 in Chapter 3 using a result of Poonen–Stoll [26]. Suppose $f \in R[x_0, \ldots, x_k]$ is homogeneous of degree d where R is a discrete valuation ring with residue field ℓ. Let $H = \mathrm{Proj}(R[x_0, \ldots, x_k]/(f))$ with special fibre H_ℓ and singular subscheme $(H_\ell)_{\mathrm{sing}}$. Then [26, Theorem 1.1] states that $\Delta_{d,k}(f)$ is a uniformizer if and only if H is regular and $(H_\ell)_{\mathrm{sing}}$ consists of a non-degenerate double point in $H(\ell)$. (We recall the definitions of "regular" and "non-degenerate double point" in Chapter 3.) Suppose now that

$$f(x_0, \ldots, x_k) = a_k x_0^{d-1}x_k + a_{k+1}x_0^{d-2}x_1^2 + \cdots + a_N x_k^d,$$

as in the setting of Theorem 2. Let $K = \mathbb{C}(a_{k+1}, \ldots, a_N)$ and $R = K[[a_k]]$ with residue field K. We prove that H is not regular in this case, which implies that $a_k^2 \mid \Delta_{d,k}(f)$ in R, since we already know $a_k \mid \Delta_{d,k}(f)$.

We also prove Theorem 6 using the same method. In this case, we have

$$f(x_0, \ldots, x_k) = a_0 x_0^d + x_0^{d-2}Q(x_1, \ldots, x_k) + \cdots .$$

Then $\Delta_{2,k-1}(Q) = 0$ if and only if Q is singular, over any field of characteristic not 2. Let K be the algebraic closure of the field of fractions of $\mathbb{C}[a_{k+1}, \ldots, a_N]/(\Delta_{2,k-1}(Q))$. We take $R = K[[a_0]]$. The special fibre H_K has $[1 : 0 : \cdots : 0]$ as a singular point, and we prove that it is not a non-degenerate double point, implying that $a_0^2 \mid \Delta_{d,k}(f)$ in R. Here the algebraic closure is taken so that we have a simpler criterion ([26, Remark 4.3]) for non-degenerate double points.

We prove Theorem 7 in Chapter 4. We prove first a formula for Δ'_d in terms of the partial derivatives of Δ_d.

Theorem 8. Let $f(x) = a_0x^d + a_1x^{d-1} + \cdots + a_d \in \mathbb{Z}[a_0, \ldots, a_d][x]$ with $d \geq 3$. Then as polynomials in $a_0, \ldots, a_d$, we have

$$-4\Delta'_d = \sum_{i=0}^{d-2} \binom{d-i}{2} a_i \frac{\partial \Delta_d}{\partial a_{i+2}}.$$

From this, we have a recursive formula of the form

$$\Delta'_d(a_0x^d + \cdots + a_d) = a_0F_n + a_1^2\Delta'_{d-1}(a_1x^{d-1} + \cdots + a_d)$$

for some polynomial $F_n \in \mathbb{Z}[a_0, \ldots, a_d]$. Using this formula, we prove that if Δ'_{d-1} is irreducible, then so is Δ'_d. Theorem 7 then follows because Δ'_5 is irreducible, by direct calculation.

As another application of Theorem 8, we also prove the following formula:

$$\Delta'_d(a_0x^d + a_{d-1}x + a_d) = (-1)^{d(d-1)/2-1} \frac{d^{d-1}(d-1)^3}{8} a_0^{d-1}a_{d-1}^2a_d^{d-3}.$$

Chapter 2

A-Discriminants

The A-discriminant is a generalization of ordinary discriminants, resultants, and hyperdeterminants, which is discussed in [13]. In this chapter, we will use A-discriminants to give our first proof of Theorem 2. We recall some facts about toric varieties, introduce A-discriminants, and discuss the degree formula for A-discriminants due to Matsui and Takeuchi [24], a crucial tool in our proof. The details on toric varieties are largely drawn from [11], [12], [13, Chapter 5], and [22]. The information on Euler obstructions is mainly from [24].

2.1 Definition of the A-discriminant

We start with some preliminary definitions.

Definition 2.1. An *algebraic torus* T over $\mathbb{C}$ is an affine algebraic group isomorphic to

$(\mathbb{C}^{\times})^n$ for some $n \geq 1$.

Definition 2.2. A *toric variety* over $\mathbb{C}$ is an irreducible variety V over $\mathbb{C}$ containing an algebraic torus T as a Zariski open subvariety such that the action of the torus on itself extends to an action on V.

For any $\omega = (m_0, \ldots, m_k) \in \mathbb{Z}^{k+1}$ and $x = (x_0, \ldots, x_k) \in (\mathbb{C}^{\times})^{k+1}$, we define

$$x^{\omega} = x_0^{m_0} \cdots x_k^{m_k}.$$

The maps $x \to x^{\omega}$ for $\omega \in \mathbb{Z}^{k+1}$ are the characters of $(\mathbb{C}^{\times})^{k+1}$.

Following [13, p. 166], we define the variety $X_A \subseteq \mathbb{P}^{r-1}(\mathbb{C})$ associated to a subset $A = \{\omega_1, \ldots, \omega_r\} \subseteq \mathbb{Z}^{k+1}$, as the Zariski closure in $\mathbb{P}^{r-1}(\mathbb{C})$ of the set

$$\{[x^{\omega_1} : \cdots : x^{\omega_r}] \mid x = (x_0, \ldots, x_k) \in (\mathbb{C}^{\times})^{k+1}\}.$$

Proposition 2.3 ([12], Props. 1.1.8 and 2.1.2)**.** *The variety X_A is a projective toric variety with torus $(\mathbb{C}^{\times})^{k+1}$.*

Indeed, consider the action of $(\mathbb{C}^{\times})^{k+1}$ on $\mathbb{P}^{r-1}(\mathbb{C})$ by

$$x \cdot [z_1 : \cdots : z_r] = [x^{\omega_1} z_1 : \cdots : x^{\omega_r} z_r].$$

Then X_A is the closure of $[1 : \cdots : 1]$ under this action, and this action naturally extends to an action on X_A.

The next result is a special case of the orbit-cone correspondence for toric varieties.

Proposition 2.4 ([13], Ch. 5, Props. 1.9 and 2.5.)**.** Let $A = \{\omega_1, \ldots, \omega_r\} \subseteq \mathbb{Z}^{k+1}$. Let P be the convex hull of A. The set of torus orbits in X_A is in bijection with the set of non-empty faces of the polytope P. The orbit $X^0(\sigma)$ corresponding to a face σ of P is cut out inside X_A by points with homogeneous coordinates $[z_1 : \cdots : z_r]$ satisfying $z_i = 0$ for $\omega_i \notin \sigma$ and $z_i \neq 0$ for $\omega_i \in \sigma$. Write $X(\sigma)$ for the closure of $X^0(\sigma)$. Then $X(\sigma)$ is isomorphic to $X_{A\cap\sigma}$. Furthermore, $X(\sigma)$ is cut out inside X_A by the equations $z_i = 0$ for $\omega_i \notin \sigma$. If σ_1 and σ_2 are two faces of Q, then $X(\sigma_1) \subseteq X(\sigma_2)$ if and only if $\sigma_1 \subseteq \sigma_2$.

Definition 2.5 ([13], p. 271)**.** Let $A = \{\omega_1, \ldots, \omega_r\} \subseteq \mathbb{Z}^{k+1}$. Let

$$\mathbb{C}^A = \Big\{ \sum_{\omega \in A} a_\omega x^\omega \colon a_\omega \in \mathbb{C} \Big\}.$$

Let $\nabla_0 \subseteq \mathbb{C}^A$ denote the set of all f for which there exists $x^{(0)} \in (\mathbb{C}^\times)^{k+1}$ such that

$$f(x^{(0)}) = \frac{\partial f}{\partial x_i}(x^{(0)}) = 0 \text{ for all } i = 0, \ldots, k.$$

Let ∇_A be the Zariski closure of ∇_0 in $\mathbb{C}^A$.

Proposition 2.6 ([13], Ch. 9, Prop. 1.1)**.** The variety ∇_A is invariant under scalar multiplication, and its projectivization $\mathbb{P}(\nabla_A)$ is projectively dual to X_A.

The previous proposition allowed Gelfand, Kapranov, and Zelevinsky to define the A-discriminant as follows.

Definition 2.7 ([13], Ch. 9, Def. 1.2)**.** If A is such that ∇_A is a subvariety of $\mathbb{C}^A$ of codimension 1, then the A-*discriminant* is an irreducible primitive integral polynomial Δ_A in the coefficients a_ω of f that vanishes on ∇_A. If codim $\nabla_A > 1$, we set $\Delta_A = 1$.

Although the A-discriminant is only uniquely defined up to sign, we conventionally refer to it using the definite article, following [13]. This does not affect any of the proofs.

With this notation, Δ_A satisfies the following properties.

Proposition 2.8 ([13], Ch. 9, Props. 1.3 and 1.4)**.** The A-discriminant Δ_A is homogeneous, and in addition, for every monomial $\prod a_\omega^{m(\omega)}$ in Δ_A, the vector $\sum m(\omega) \cdot \omega \in \mathbb{Z}^{k+1}$ is the same. In other words, Δ_A is weighted homogeneous if each a_ω is given weight ω.

Remark 2.9. If the set $A \subseteq \mathbb{Z}^{k+1}$ is *homogeneous of degree* d in the sense that A is contained in the affine hyperplane $x_0 + \cdots + x_k = d$, then we may dehomogenize by taking $A' = T(A)$ where $T : \mathbb{Z}^{k+1} \to \mathbb{Z}^k$ is the linear map $(x_0, \ldots, x_k) \mapsto (x_1, \ldots, x_k)$. It is then easy to see that $X_A = X_{A'}$, $\nabla_A = \nabla_{A'}$ and $\Delta_A = \Delta_{A'}$.

2.2 Degree of the A-discriminant

In this section, we present Matsui–Takeuchi's formula for the degree of the A-discriminant and compute it in our case of interest. This formula involves the calculation of certain Euler obstructions. Many of these ideas were first introduced by MacPherson in [21].

To calculate Euler obstructions, we will use normalized relative sub-diagram volumes, which we first define.

Definition 2.10 ([24], Def. 1.2)**.** Given a subset $S \subseteq \mathbb{R}^n$, we define the *affine subspace* of $\mathbb{R}^n$ generated by S as

$$\mathbb{L}(S) = \bigcup_{m \geq 0} \Big\{ \sum_{i=1}^{m} c_i s_i \mid s_i \in S, c_i \in \mathbb{R}, c_1 + \cdots + c_m = 1 \Big\}.$$

Given a subset $A \subseteq \mathbb{Z}^n$, we similarly define the *affine lattice* generated by A contained in $\mathbb{L}(A)$ as

$$M(A) = \bigcup_{m \geq 0} \Big\{ \sum_{i=1}^{m} c_i s_i \mid s_i \in A, c_i \in \mathbb{Z}, c_1 + \cdots + c_m = 1 \Big\}.$$

We then define the *normalized volume with respect to an affine lattice* $M(A)$, denoted by

$$\mathrm{Vol}(\quad; A),$$

as the $(\dim \mathbb{L}(A))$-dimensional volume on the affine space $\mathbb{L}(A)$ normalized so that $(\dim \mathbb{L}(A))!$ is the covolume of the lattice $M(A)$, i.e., the volume of the quotient $\mathbb{R}^n/M(A)$. In other words, the smallest full-dimensional simplex with vertices in $M(A)$ has volume 1.

Definition 2.11 ([24], Def. 4.2)**.** Let P be a polytope in $\mathbb{Z}^n$, σ a face of P, and $\Delta_\beta \subseteq \Delta_\alpha$ faces of σ. If $\Delta_\beta = \Delta_\alpha$, then we set $\mathrm{RSV}_{\mathbb{Z}}(\Delta_\alpha, \Delta_\beta) = 1$. Suppose now $\Delta_\beta \subsetneq \Delta_\alpha$. Let $\mathbb{L}(\Delta_\beta)' = \mathbb{R}^n/\mathbb{L}(\Delta_\beta)$ and let $p_\beta : \mathbb{R}^n \to \mathbb{L}(\Delta_\beta)'$ be the natural projection. Let

$$\begin{aligned} K_{\alpha,\beta} &= p_\beta(\Delta_\alpha), \\ \Theta_{\alpha,\beta} &= \text{convex hull of } \Big(K_{\alpha,\beta} \cap (p_\beta(\mathbb{Z}^n) \setminus \{0\}) \Big). \end{aligned}$$

Define the *normalized relative sub-diagram volume* $\mathrm{RSV}_{\mathbb{Z}}(\Delta_\alpha, \Delta_\beta)$ by

$$\mathrm{RSV}_{\mathbb{Z}}(\Delta_\alpha, \Delta_\beta) = \mathrm{Vol}(K_{\alpha,\beta} \setminus \Theta_{\alpha,\beta}\,;\, p_\beta(\mathbb{Z}^n) \cap \mathbb{L}(K_{\alpha,\beta})),$$

where $K_{\alpha,\beta} \setminus \Theta_{\alpha,\beta}$ is the set difference.

In what follows, we will be considering the set $A \subseteq \mathbb{Z}^k$ defined by

$$A = \{(0, \ldots, 0, 1)\} \cup \{(\omega_1, \ldots, \omega_k) \in \mathbb{Z}^k : \omega_i \geq 0, 2 \leq \omega_1 + \cdots + \omega_k \leq d\},$$

where $k \geq 2$ and $d \geq 3$. Let P be the convex hull of A. The vertices of P are $\mathcal{A}$, $\mathcal{B}_1, \ldots, \mathcal{B}_{k-1}$, $\mathcal{C}_1, \ldots, \mathcal{C}_k$ where

$$\begin{aligned} \mathcal{A} &= (0, \ldots, 0, 1), \\ \mathcal{B}_i &= (\omega_1, \ldots, \omega_k),\ \text{where } \omega_i = 2,\ \text{and } \omega_j = 0 \text{ for } j \neq i, \\ \mathcal{C}_i &= (\omega_1, \ldots, \omega_k),\ \text{where } \omega_i = d,\ \text{and } \omega_j = 0 \text{ for } j \neq i. \end{aligned} \tag{2.1}$$

(See Figure 2.1 at the end of the chapter for the case of $d = 3$ and $k = 3$.) The m-simplices of P, for $m = 0, \ldots, k$, are of the following five types:

(i) $\mathcal{A}\mathcal{C}_k\mathcal{B}_{i_1}\mathcal{C}_{i_1} \ldots \mathcal{B}_{i_{m-1}}\mathcal{C}_{i_{m-1}}$

(ii) $\mathcal{A}\mathcal{B}_{i_1} \ldots \mathcal{B}_{i_m}$

(iii) $\mathcal{B}_{i_1} \ldots \mathcal{B}_{i_{m+1}}$

(iv) $\mathcal{C}_{i_1} \ldots \mathcal{C}_{i_{m+1}}$

(v) $\mathcal{B}_{i_1}\mathcal{C}_{i_1}\dots\mathcal{B}_{i_m}\mathcal{C}_{i_m}$.

Only the simplices of types (i) and (ii) contain $\mathcal{A}$. We compute their RSV.

Lemma 2.12. With notation as above, we have

$$\mathrm{RSV}_{\mathbb{Z}}(\mathcal{A}\mathcal{C}_k\mathcal{B}_{i_1}\mathcal{C}_{i_1}\dots\mathcal{B}_{i_{m-1}}\mathcal{C}_{i_{m-1}},\mathcal{A}) = \mathrm{RSV}_{\mathbb{Z}}(\mathcal{A}\mathcal{B}_{i_1}\dots\mathcal{B}_{i_m},\mathcal{A}) = 2^{m-1}.$$

Proof. Let $\mathcal{B}_k = (0,\dots,0,2)$. Let Δ_β be the 0-dimensional simplex $\mathcal{A}$. The map p_β is simply translation by $\mathcal{A}$ so that $\mathcal{A}$ maps to 0. Let Δ_α be the m-dimensional simplex $\mathcal{A}\mathcal{C}_k\mathcal{B}_{i_1}\mathcal{C}_{i_1}\dots\mathcal{B}_{i_{m-1}}\mathcal{C}_{i_{m-1}}$. Then $\Theta_{\alpha,\beta}$ is the simplex $\mathcal{B}_k\mathcal{C}_k\mathcal{B}_{i_1}\mathcal{C}_{i_1}\dots\mathcal{B}_{i_{m-1}}\mathcal{C}_{i_{m-1}}$ and $\mathrm{RSV}_{\mathbb{Z}}(\mathcal{A}\mathcal{C}_k\mathcal{B}_{i_1}\mathcal{C}_{i_1}\dots\mathcal{B}_{i_{m-1}}\mathcal{C}_{i_{m-1}},\mathcal{A})$ is the normalized m-dimensional volume of $\mathcal{A}\mathcal{B}_k\mathcal{B}_{i_1}\dots\mathcal{B}_{i_{m-1}}$, which is 2^{m-1}.

Similarly, $\mathrm{RSV}_{\mathbb{Z}}(\mathcal{A}\mathcal{B}_{i_1}\dots\mathcal{B}_{i_m},\mathcal{A})$ is the normalized m-dimensional volume of $\mathcal{A}\mathcal{B}_{i_1}\dots\mathcal{B}_{i_m}$, since $\Theta_{\alpha,\beta}$ in this case is the $(m-1)$-dimensional simplex $\mathcal{B}_{i_1}\dots\mathcal{B}_{i_m}$. The normalized m-dimensional volume of $\mathcal{A}\mathcal{B}_{i_1}\dots\mathcal{B}_{i_m}$ equals the normalized $(m-1)$-dimensional volume of $\mathcal{B}_{i_1}\dots\mathcal{B}_{i_m}$, which is 2^{m-1}. □

Definition 2.13. Let $A \subseteq \mathbb{Z}^{k+1}$, and let P be the polytope obtained by taking the convex hull of A. Let σ be a face of P. The *Euler obstruction* Eu is inductively defined on faces Δ_β of P by:

(i) $\mathrm{Eu}(P) = 1$,

(ii) $\mathrm{Eu}(\Delta_\beta) = \sum_{\Delta_\beta \subsetneq \Delta_\alpha} (-1)^{\dim\Delta_\alpha - \dim\Delta_\beta - 1}\,\mathrm{RSV}_{\mathbb{Z}}(\Delta_\alpha,\Delta_\beta)\,\mathrm{Eu}(\Delta_\alpha)$.

In [24], the authors used a different definition of Euler obstruction and proved that the above definition is equivalent to it ([24, Theorem 4.3, Corollary 4.4]).

By Proposition 2.4, any face σ of Q corresponds to an orbit $X^0(\sigma)$ of the torus action in X_A. We say a face σ is *smooth* in X_A if every point (or equivalently one point) of $X^0(\sigma)$ is in the smooth locus of X_A. Then we have:

Theorem 9 ([24], Thm. 4.3, Cor. 4.4)**.** The Euler obstruction Eu is equal to 1 on faces that are smooth in X_A.

Since smoothness is an open condition, we see that if $\mathcal{B}$ is a vertex of P that is smooth in X_A, then the Euler obstruction of any face that contains $\mathcal{B}$ is equal to 1. Indeed, the singular locus of X_A is closed under the torus action since multiplying by x^ω does not affect Jacobian rank on an affine chart. The singular locus is also Zariski-closed, and $X^0(\tau)$ is in the closure of $X^0(\sigma)$ if τ is in the boundary of σ.

Proposition 2.14. Let $k \geq 2$ and $d \geq 3$ be integers. Let

$$A = \{(0, \ldots, 0, 1)\} \cup \{(\omega_1, \ldots, \omega_k) \in \mathbb{Z}^k \colon \omega_i \geq 0, 2 \leq \omega_1 + \cdots + \omega_k \leq d\}.$$

With the notations $\mathcal{A}, \mathcal{B}_i, \mathcal{C}_i$ as in (2.1), the vertices $\mathcal{B}_1, \ldots, \mathcal{B}_{k-1}, \mathcal{C}_1, \ldots, \mathcal{C}_k$ are smooth in X_A. As a result, the Euler obstruction of every simplex except for the point $\mathcal{A}$ is equal to 1.

Proof. The variety X_A is the Zariski closure of the set

$$\{[x_k : x_1^2 : \cdots : x_k^d] \mid x_1, \ldots, x_k \in \mathbb{C}^\times\},$$

where we include all monomials of non-negative degree $\leq d$ in $x_1, \ldots, x_k$ except $1, x_1, \ldots, x_{k-1}$. The monomial corresponding to $\mathcal{B}_i$ for $1 \leq i \leq k-1$ is x_i^2, and the monomial corresponding to $\mathcal{C}_i$ for $1 \leq i \leq k$ is x_i^d. By symmetry of $x_1, \ldots, x_{k-1}$, it suffices to check that $\mathcal{B}_1$, $\mathcal{C}_1$, and $\mathcal{C}_k$ are smooth in X_A. The point corresponding to $\mathcal{B}_1$ is $[0 : 1 : 0 : \cdots : 0]$ and the affine chart containing this point has affine coordinates

$$\frac{x_k}{x_1^2}, \quad \text{and} \quad \frac{x_1^{\omega_1} \cdots x_k^{\omega_k}}{x_1^2}, \text{ where } \omega_i \geq 0, 2 \leq \omega_1 + \cdots + \omega_k \leq d.$$

We note that all of these affine coordinates are products of

$$\frac{x_k}{x_1^2}, \frac{x_2}{x_1}, \ldots, \frac{x_k}{x_1}, x_1, \ldots, x_k.$$

Since $x_i = (x_i/x_1)x_1$ for $i = 2, \ldots, k$, we may shorten this list to

$$S_0 = \left\{ \frac{x_k}{x_1^2}, \frac{x_2}{x_1}, \ldots, \frac{x_{k-1}}{x_1}, x_1 \right\}.$$

Because the monomials in S_0 all appear as affine coordinates and are algebraically independent, we conclude that the intersection of X_A with the affine chart containing $[0 : 1 : 0 : \cdots : 0]$ is isomorphic to $\mathbb{A}^k$, which implies smoothness at $[0 : 1 : 0 : \cdots : 0]$.

The smoothness of X_A at $\mathcal{C}_1$ and $\mathcal{C}_k$ follows by a similar argument. The affine coordinates for the affine chart containing the point corresponding to $\mathcal{C}_i$, for $i = 1$ or k, are

$$\frac{x_k}{x_i^d}, \quad \text{and} \quad \frac{x_1^{\omega_1} \cdots x_k^{\omega_k}}{x_i^d}, \text{ where } \omega_i \geq 0, 2 \leq \omega_1 + \cdots + \omega_k \leq d.$$

All of these affine coordinates are products of

$$\frac{1}{x_i}, \frac{x_1}{x_i}, \dots \frac{x_k}{x_i}.$$

We take

$$S_1 = \left\{\frac{1}{x_1}, \frac{x_2}{x_1}, \dots, \frac{x_k}{x_1}\right\} \qquad \text{and} \qquad S_k = \left\{\frac{1}{x_k}, \frac{x_1}{x_k}, \dots, \frac{x_{k-1}}{x_k}\right\}$$

to be the algebraically independent generating sets of affine coordinates for the affine charts containing the points corresponding to $\mathcal{C}_1$ and $\mathcal{C}_k$, respectively. This proves that both points are smooth in X_A. $\square$

Proposition 2.15. With notation as in Proposition 2.14, the Euler obstruction of the point $\mathcal{A}$ is $\frac{1}{2}(1-(-1)^k)$.

Proof. The vertex $\mathcal{A}$ is contained in $\binom{k-1}{m-1}$ m-simplices of type (i), $\binom{k-1}{m}$ m-simplices of type (ii), and no m-simplices of types (iii)–(v). Therefore, by Proposition 2.14 on the Euler obstruction for all the other simplices and Lemma 2.12 on the RSV values, we have

$$\begin{aligned}
\mathrm{Eu}(\mathcal{A}) &= (\mathrm{RSV}(\mathcal{A}\mathcal{C}_k, \mathcal{A}) + \mathrm{RSV}(\mathcal{A}\mathcal{B}_1, \mathcal{A}) + \cdots + \mathrm{RSV}(\mathcal{A}\mathcal{B}_{k-1}, \mathcal{A})) \\
&\quad - (\mathrm{RSV}(\mathcal{A}\mathcal{C}_k\mathcal{B}_1\mathcal{C}_1, \mathcal{A}) + \mathrm{RSV}(\mathcal{A}\mathcal{C}_k\mathcal{B}_2\mathcal{C}_2, \mathcal{A}) + \cdots + \mathrm{RSV}(\mathcal{A}\mathcal{C}_k\mathcal{B}_{k-1}\mathcal{C}_{k-1}, \mathcal{A})) + \cdots \\
&= \sum_{m=1}^{k} (-1)^{m+1} \left(\binom{k-1}{m-1} 2^{m-1} + \binom{k-1}{m} 2^{m-1} \right) \\
&= (-1)^{k+1} + (1/2)((-1)^k + 1) \\
&= \frac{1}{2}(1-(-1)^k),
\end{aligned}$$

as desired. $\square$

Note that the local ring of X_A at an affine chart containing the point corresponding to $\mathcal{A}$ when $k = 3$ and $d = 2$ is not isomorphic to affine space, so by Proposition 2.15, the converse of Theorem 9 does not hold.

We can now state Matsui–Takeuchi's degree formula.

Theorem 10 ([24], Thm. 1.4)**.** Let $A \subseteq \mathbb{Z}^{k+1}$ be a finite set and let P be its convex hull. Let $m = \#A - 1$. For $1 \leq i \leq m$, set

$$\delta_i = \sum_{\Delta \text{ a face of } P} (-1)^{\operatorname{codim} \Delta} \left(\left(\binom{\dim \Delta - 1}{i} + (-1)^{i-1}(i+1) \right) \operatorname{Vol}(\Delta; A \cap \Delta) \operatorname{Eu}(\Delta) \right),$$

where $\operatorname{Vol}(\Delta; A \cap \Delta)$ is the normalized volume from Definition 2.11. Let $X_A^* = \mathbb{P}(\nabla_A)$ be the projective dual of X_A. Let $r = \operatorname{codim} X_A^* = m - \dim X_A^*$. Then

$$r = \min\{i \mid \delta_i \neq 0\} \qquad \text{and} \qquad \deg X_A^* = \delta_r.$$

The special case of Theorem 10 when X_A is smooth has already been proved in [13, Chapter 9, Theorem 2.8].

Corollary 11 ([24], Cor. 1.6)**.** With notations as in Theorem 10, if $\delta_1 \neq 0$, then $\mathbb{P}(\nabla_A)$ is a hypersurface and the degree of the A-discriminant is

$$\deg \Delta_A = \sum_{\Delta \text{ a face of } P} (-1)^{\operatorname{codim} \Delta} (\dim \Delta + 1) \operatorname{Vol}(\Delta; A \cap \Delta) \operatorname{Eu}(\Delta). \tag{2.2}$$

We can now compute the degree of the A-discriminant in our example.

Theorem 12. Let $k \geq 2$ and $d \geq 3$ be integers. Let

$$A = \{(0, \dots, 0, 1)\} \cup \{(\omega_1, \dots, \omega_k) \in \mathbb{Z}^k \colon \omega_i \geq 0, 2 \leq \omega_1 + \cdots + \omega_k \leq d\}.$$

Then $\mathbb{P}(\nabla_A)$ is a hypersurface and

$$\deg(\Delta_A) = (k+1)(d-1)^k - 2.$$

Proof. With the notations of (2.1), we find that the normalized volumes of each of the five types of simplices are given by: (i) $d^m - 2^{m-1}$, (ii) 2^{m-1}, (iii) 2^m, (iv) d^m, and (v) $d^m - 2^m$. By Proposition 2.15, we find that the contribution to (2.2) where $m = 0$ is

$$(-1)^k(2k-1) + \frac{(-1)^k}{2} - \frac{1}{2} = (-1)^k\left(2k - \frac{1}{2}\right) - \frac{1}{2}.$$

The $m > 0$ contribution is

$$\begin{aligned}
&\sum_{m=1}^{k}\binom{k-1}{m-1}(-1)^{k-m}(m+1)(d^m - 2^{m-1}) + \sum_{m=1}^{k}\binom{k-1}{m}(-1)^{k-m}(m+1)2^{m-1} \\
&+ \sum_{m=1}^{k}\binom{k-1}{m+1}(-1)^{k-m}(m+1)2^m + \sum_{m=1}^{k}\binom{k}{m+1}(-1)^{k-m}(m+1)d^m \\
&+ \sum_{m=1}^{k}\binom{k-1}{m}(-1)^{k-m}(m+1)(d^m - 2^m) \\
&= \sum_{m=1}^{k}\binom{k+1}{m+1}(-1)^{k-m}(m+1)d^m + \sum_{m=1}^{k}\left(2\binom{k-1}{m+1} - \binom{k}{m}\right)(-1)^{k-m}(m+1)2^{m-1} \\
&= (-1)^k(k+1)((1-d)^k - 1) - \frac{1}{2}(-1)^k(2k + 3(-1)^k - 3) \\
&= (k+1)(d-1)^k - 2(-1)^k k + \frac{1}{2}(-1)^k - \frac{3}{2}.
\end{aligned}$$

Adding the $m = 0$ term gives

$$\deg(\Delta_A) = (k+1)(d-1)^k - 2,$$

as desired. $\square$

We now recall and prove Theorem 2.

Theorem 2. Let $f(x_0, \ldots, x_k) \in \mathbb{C}[a_0, \ldots, a_N][x_0, \ldots, x_k]$, where $N = \binom{k+d}{d} - 1$, be a generic homogeneous polynomial of degree $d \geq 2$. Let a_i denote the coefficient of $x_0^{d-1}x_i$ for $i = 0, \ldots, k$. Then $a_k^2 \mid \Delta_{d,k}(f)$ in the ring $\mathbb{C}[a_0, \ldots, a_N]/(a_0, \ldots, a_{k-1})$.

Proof. The $k = 1$ case and the $d = 2$ case are already dealt with in the Introduction (in the paragraph following Theorem 7). We may therefore assume that $k \geq 2$ and $d \geq 3$.

We set $a_0 = \cdots = a_{k-1} = 0$ so that

$$f(x_0, \ldots, x_k) = a_k x_0^{d-1} x_k + \text{lower degree terms in } x_0.$$

We note that if $a_k = 0$, then the point $[1 : 0 : \cdots : 0]$ is a singular point of $V(f)$ and so $\Delta_{d,k}(f) = 0$. Our goal is to prove that $a_k^2 \mid \Delta_{d,k}$ in $\mathbb{C}[a_k, \ldots, a_N]$. Define the set $A \subseteq \mathbb{Z}^{k+1}$ by

$$A = \{(d-1, 0, \ldots, 0, 1)\} \cup \{(\omega_0, \ldots, \omega_k) \in \mathbb{Z}^{k+1} \mid \omega_i \geq 0,\, \omega_0 \leq d-2,\, \omega_0 + \cdots + \omega_k = d\}.$$

Then x^ω for $\omega \in A$ are exactly the monomials that appear in $f(x_0, \ldots, x_k)$. Recall the affine space $\mathbb{C}^A$ consisting of $\mathbb{C}$-linear combinations of monomials x^ω for $\omega \in A$. We have the subset $\nabla_0 \subseteq \mathbb{C}^A$ consisting of $g \in \mathbb{C}^A$ for which there exists $(\beta_0, \dots, \beta_k) \in (\mathbb{C}^\times)^{k+1}$ such that

$$g(\beta_0, \dots, \beta_k) = \frac{\partial g}{\partial x_i}(\beta_0, \dots, \beta_k) = 0 \text{ for all } i = 0, \dots, k.$$

We call such a point $(\beta_0, \dots, \beta_k)$ a singular point of g. The Zariski closure of ∇_0 is denoted by ∇_A.

Lemma 2.16. If $g \in \mathbb{C}^A$ is such that $(\beta_0, \dots, \beta_k) \in \mathbb{C}^{k+1}$ with $\beta_k \neq 0$ is a singular point of g, then $g \in \nabla_A$.

Proof. Since $\beta_k \neq 0$, we see that for $\epsilon_0, \dots, \epsilon_{k-1} \in \mathbb{C}^\times$ having small enough absolute value, the polynomial

$$g(x_0 - \epsilon_0 x_k, \dots, x_{k-1} - \epsilon_{k-1} x_k, x_k) \in \nabla_0$$

since it has $(\beta_0 + \epsilon_0 \beta_k, \dots, \beta_{k-1} + \epsilon_{k-1}\beta_k, \beta_k) \in (\mathbb{C}^\times)^{k+1}$ as a singular point and belongs to $\mathbb{C}^A$. Taking closure gives $g \in \nabla_A$. $\square$

For any homogeneous polynomial $F(a_0, \dots, a_N)$ in the coefficients of homogeneous polynomials of degree d in $k+1$ variables, we write

$$V(F)^A = V(F, a_0, a_1, \dots, a_{k-1}) \subseteq \mathbb{P}^N.$$

Suppose $g \in V(\Delta_{d,k})^A(\mathbb{C})$. Then $V(g)$ has a singular point $[\beta_0 : \cdots : \beta_k] \in \mathbb{P}^k(\mathbb{C})$. If $\beta_k \neq 0$, then we have by Lemma 2.16 that $g \in \mathbb{P}(\nabla_A)$.

Proposition 2.17. We have that

$$V(\Delta_{d,k})^A(\mathbb{C}) = \mathbb{P}(\nabla_A) \cup V(a_k)^A(\mathbb{C}).$$

Proof: The inclusion $V(\Delta_{d,k})^A(\mathbb{C}) \supseteq \mathbb{P}(\nabla_A) \cup V(a_k)^A(\mathbb{C})$ is clear. For the other inclusion, it remains to handle the case where $V(g)$ has a singular point $[\beta_0 : \cdots : \beta_k] \in \mathbb{P}^k(\mathbb{C})$ with $\beta_k = 0$.

Lemma 2.18. Suppose $g(x_0, \ldots, x_k) \in V(\Delta_{d,k})^A(\mathbb{C})$ has a singular point $[\beta_0 : \cdots : \beta_k] \in \mathbb{P}^k(\mathbb{C})$ with $\beta_0 = \beta_k = 0$. Then $g \in \mathbb{P}(\nabla_A)$.

Proof. We fix a lift $\tilde{g}$ of g in $\mathbb{C}^A$ and write

$$\tilde{g}(x_0, \ldots, x_k) = x_0^{d-1} h_1(x_1, \ldots, x_k) + \cdots + h_d(x_1, \ldots, x_k) \in \mathbb{C}^A,$$

Then we see that $(\beta_1, \ldots, \beta_k)$ is a singular point of $h_d(x_1, \ldots, x_k)$ and at least one of $\beta_1, \ldots, \beta_{k-1}$ is nonzero. Suppose without loss of generality that $\beta_1 \neq 0$. Then for any $\epsilon \in \mathbb{C}^\times$, we see that $(\beta_1, \ldots, \beta_{k-1}, \beta_k - \epsilon\beta_1)$ is a singular point of $h_d(x_1, \ldots, x_{k-1}, x_k + \epsilon x_1)$, and so $(0, \beta_1, \ldots, \beta_{k-1}, \beta_k - \epsilon\beta_1)$ is a singular point of

$$g_\epsilon(x_0, \ldots, x_k) = x_0^{d-1} h_1(x_1, \ldots, x_k) + \cdots + x_0 h_{d-1}(x_1, \ldots, x_k) + h_d(x_1, \ldots, x_{k-1}, x_k + \epsilon x_1).$$

For ϵ small enough, we have $\beta_k - \epsilon\beta_1 \neq 0$ and so by Lemma 2.16, we have $g_\epsilon \in \nabla_A$. Taking closure gives $\tilde{g} \in \nabla_A$ and so $g \in \mathbb{P}(\nabla_A)$. $\square$

Lemma 2.19. Suppose $g(x_0, \ldots, x_k) \in \nabla_A$. Then for any $i = 1, \ldots, k-1$ and any $b_i \in \mathbb{C}$, we have $h := g(x_0, \ldots, x_{i-1}, x_i - b_i x_0, x_{i+1}, \ldots, x_k) \in \nabla_A$.

Proof. Suppose g is the limit of a sequence $g_n \in \nabla_0$, each having a singular point with nonzero coordinates. Let $h_n = g_n(x_0, \ldots, x_{i-1}, x_i - b_i x_0, x_{i+1}, \ldots, x_k)$. Then each h_n has a singular point with nonzero x_k-coordinate. So by Lemma 2.16, each $h_n \in \nabla_A$. Taking closure gives $h \in \nabla_A$. $\square$

Proof of Proposition 2.17: Suppose $g(x_0, \ldots, x_k) \in V(\Delta_{d,k})^A(\mathbb{C})$ has a singular point $[\beta_0 : \cdots : \beta_k] \in \mathbb{P}^k(\mathbb{C})$ with $\beta_k = 0$. If $\beta_0 = 0$, then we are done by Lemma 2.18. Suppose $\beta_0 \neq 0$. If all of $\beta_1 = \cdots = \beta_{k-1} = 0$, then by taking the x_k-partial derivative, we find that $a_k = 0$. Suppose without loss of generality that $\beta_1 \neq 0$. Fix any lift $\tilde{g}$ of g in $\mathbb{C}^A$. Then $h(x_0, \ldots, x_k) = \tilde{g}(x_0 + (\beta_0/\beta_1)x_1, x_1, \ldots, x_k)$ has $(0, \beta_1, \ldots, \beta_k)$ as a singular point. By Lemma 2.18, we have $h \in \nabla_A$. By Lemma 2.19, we have $\tilde{g} \in \nabla_A$ and so $g \in \mathbb{P}(\nabla_A)$. $\square$

It now follows from the Nullstellensatz that if $\mathbb{P}(\nabla_A) = V(\Delta_A)$ is a hypersurface cut out by an A-discriminant Δ_A, then we have

$$\Delta_{d,k}\,|_{\mathbb{C}^A} = c\, a_k^{k_1}\, \Delta_A^{k_2}$$

for some non-negative integers k_1, k_2 and some nonzero constant $c \in \mathbb{C}^\times$. It is therefore sufficient to prove that

$$\deg \Delta_A = \deg \Delta_{d,k} - 2 > 2, \tag{2.3}$$

which also implies that $\mathbb{P}(\nabla_A) = V(\Delta_A)$.

To find the degree of Δ_A, we dehomogenize and work with the set $A \subseteq \mathbb{Z}^k$ defined by

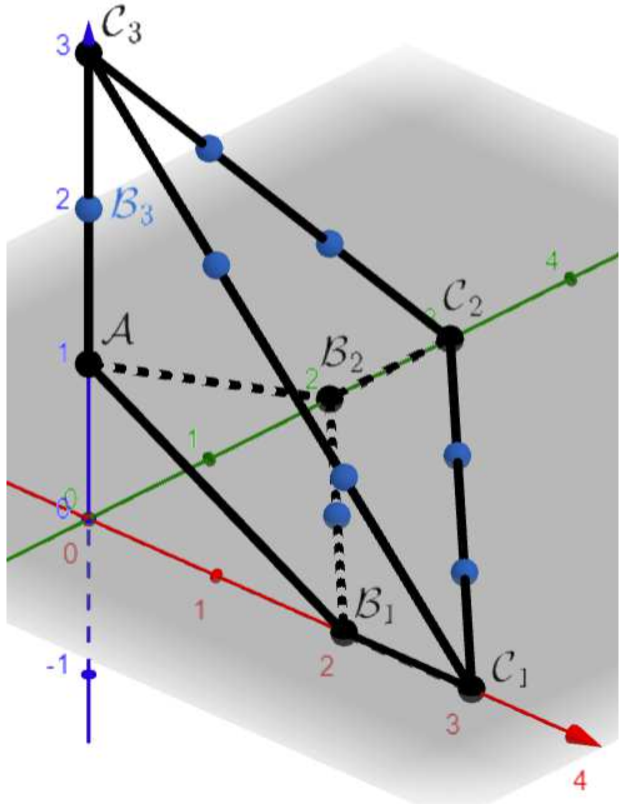
$$A = \{(0, \dots, 0, 1)\} \cup \{(\omega_1, \dots, \omega_k) \in \mathbb{Z}^k \colon \omega_i \geq 0, 2 \leq \omega_1 + \cdots + \omega_k \leq d\}.$$

This is exactly the set we studied in the previous section when we proved in Theorem 12 that

$$\deg \Delta_A = (k+1)(d-1)^k - 2 = \deg \Delta_{d,k} - 2,$$

which is greater than 2 since $k \geq 2$ and $d \geq 3$. This completes the proof of Theorem 2. $\square$

Figure 2.1: The polytope corresponding to the case $k = 3$ and $d = 3$, dehomogenized by setting $x_0 = 1$. Additional points on the exterior edges are shown to give a clearer picture of the simplicial structure.



Chapter 3

Square-divisibility of Discriminants

In this chapter, we will use techniques in algebraic geometry and a result of Poonen–Stoll [26] to give a second proof of Theorem 2 and proofs of Theorems 1, 4, and 6. We restate the result of Poonen–Stoll in our notation.

Note that a locally Noetherian scheme is said to be *regular* if all of its local rings are regular local rings. Following [26], if X is a scheme of finite type over a field k, a k-point $Q \in X$ is a *non-degenerate double point* if there exist $n \geq 1$ and $f \in k[[x_0, \dots, x_n]]$ such that there is an isomorphism of complete k-algebras $\hat{\mathcal{O}}_{X,Q} \simeq k[[x_0, \dots, x_n]]/(f)$ and an equality of ideals $(\partial f/\partial x_0, \dots, \partial f/\partial x_n) = (x_0, \dots, x_n)$.

Theorem 13 ([26], Thm. 1.1)**.** Let R be a discrete valuation ring with valuation $v : R \twoheadrightarrow \mathbb{Z} \cup \{\infty\}$ and residue field ℓ. Let $f \in R[x_0, \dots, x_k]$ be a homogeneous polynomial of degree d with discriminant $\Delta_{d,k}(f)$. Let $H = \operatorname{Proj}\left(R[x_0, ..., x_k]/(f)\right)$, let H_ℓ denote its special fibre, and let $(H_\ell)_{\text{sing}}$ denote the singular subscheme of its special fibre. Then the following are equivalent:

(a) $v(\Delta_{d,k}(f)) = 1$;

(b) H is regular, and $(H_\ell)_{\text{sing}}$ consists of a non-degenerate double point in $H(\ell)$.

We now give a second proof of Theorem 2.

Theorem 2. Let $f(x_0, \ldots, x_k) \in \mathbb{Z}[a_0, \ldots, a_N][x_0, \ldots, x_k]$, where $N = \binom{k+d}{d} - 1$, be a generic homogeneous polynomial of degree $d \geq 2$. Let a_i denote the coefficient of $x_0^{d-1}x_i$ for $i = 0, \ldots, k$. Then $a_k^2 \mid \Delta_{d,k}(f)$ in the ring $\mathbb{Z}[a_0, \ldots, a_N]/(a_0, \ldots, a_{k-1})$.

Second proof. Let $K = \mathbb{C}(a_{k+1}, \ldots, a_N)$ and let $R = K[[a_k]]$, equipped with the a_k-adic valuation and residue field K. Consider

$$f(x_0, \ldots, x_k) = a_k x_0^{d-1} x_k + \text{lower degree terms in } x_0.$$

By Theorem 13, it suffices to prove that

$$H = \operatorname{Proj}\Big(R[x_0, ..., x_k]/(f)\Big)$$

is not regular, i.e., that there exists a local ring of H that is not regular. The affine open $D(x_0)$ has coordinate ring

$$\begin{aligned} \mathcal{O}_H(D(x_0)) &\simeq R[x_1/x_0, ..., x_k/x_0]/(f(1, x_1/x_0, ..., x_k/x_0)) \\ &\simeq R[x_1, ..., x_k]/(f(1, x_1, ..., x_k)). \end{aligned}$$

The ideal $\mathfrak{m} = (a_k, x_1, ..., x_k)$ in $R[x_1, ..., x_k]$ is maximal and contains $f(1, x_1, \ldots, x_k)$. Moreover,

$$\mathcal{O}_{H,\mathfrak{m}} \simeq R[x_1, ..., x_k]_{(a_k,x_1,...,x_k)}/(f(1, x_1, \ldots, x_k)).$$

We observe first that the ring $R[x_1, ..., x_k]_{(a_k,x_1,...,x_k)}$ is a regular local ring. Indeed, as a localization of $R[x_1, \ldots, x_k]$, it has Krull dimension at most $k + 1$, and the images of $a_k, x_1, \ldots, x_k$ in $\mathfrak{m}/\mathfrak{m}^2$ are linearly independent over K.

We know that if $(S, \mathfrak{m})$ is a regular local ring and $0 \neq x \in \mathfrak{m}$, then $S/(x)$ is regular if and only if $x \notin \mathfrak{m}^2$. In our case, since $\deg(f) = d \geq 2$, we have

$$f(1, x_1, ..., x_k) = a_k x_k + \text{degree at least 2 terms} \in \mathfrak{m}^2.$$

Therefore, the local ring $\mathcal{O}_{H,\mathfrak{m}}$ is not regular. By Theorem 13, we have that $a_k^2 \mid \Delta_{d,k}(f)$ in R. This completes the second proof of Theorem 2. □

We can now prove Theorem 1.

Theorem 1. Let $f(x_0, \ldots, x_k) \in \mathbb{Z}[x_0, \ldots, x_k]$ be a homogeneous polynomial of degree $d \geq 2$. Let p be a prime such that $p^2 \mid \Delta_{d,k}(f)$ weakly. Then there exists a linear change of variables such that the coefficients of $x_0^d, x_0^{d-1}x_1, x_0^{d-1}x_2, \ldots, x_0^{d-1}x_{k-1}$ are all divisible by p^2 and the coefficient of $x_0^{d-1}x_k$ is divisible by p.

Proof. Recall that if p is a prime such that $p^2 \mid \Delta_{d,k}(f)$ weakly, this means there exists some $g \in \mathbb{Z}[x_0, \ldots, x_k]$ homogeneous of degree d such that $g \equiv f \pmod{p}$ and $p^2 \nmid \Delta_{d,k}(g)$. The special fibres $H_{\mathbb{F}_p}$ for $\operatorname{Proj}\left(\mathbb{Z}_p[x_0, \ldots, x_n]/(f)\right)$ and $\operatorname{Proj}\left(\mathbb{Z}_p[x_0, \ldots, x_n]/(g)\right)$ are isomorphic. It then follows from Theorem 13 using g that $(H_{\mathbb{F}_p})_{\text{sing}}$ consists of a single point, which is defined over $\mathbb{F}_p$. By applying a linear change of variables over $\mathbb{Z}$, we may assume that this singular point modulo p is at $[1 : 0 : \cdots : 0]$. In other words, we may assume that

$$p \mid a_i \qquad \text{for } i = 0, \ldots, k.$$

By Corollary 3, we have

$$\Delta_{d,k} \equiv a_0 D_0 \pmod{(a_0, \ldots, a_k)^2}$$

for some polynomial D_0 in the coefficients of f. If $p^2 \nmid a_0$, then from $p^2 \mid \Delta_{d,k}(f)$, we have $p \mid D_0(f)$. But then $p \mid D_0(g)$ since g and f are congruent mod p, which implies that $p^2 \mid \Delta_{d,k}(g)$, a contradiction. Hence, we have $p^2 \mid a_0$.

It is now easy to arrange for p^2 to divide $a_1, \ldots, a_{k-1}$. If p^2 divides all of $a_1, \ldots, a_k$, then we are done. Suppose p^2 does not divide at least one of them. Then by swapping the variables, we may assume that $p^2 \nmid a_k$. We can then perform a change of variables of the form

$$x_i \mapsto x_i, \text{ for } i = 0, \ldots, k-1, \qquad x_k \mapsto \beta_1 x_1 + \cdots + \beta_{k-1} x_{k-1} + x_k$$

to arrange for $p^2 \mid a_i$ for $i = 1, \ldots, k-1$. (For example, when $f(x, y, z, w) = \sum_{i,j,k,\ell} a_{ijkl} x^i y^j z^k w^\ell$ is a quaternary quadratic form, this change of variables will send $a_{1100} \mapsto a_{1100} + \beta_1 a_{1001}$ and $a_{1010} \mapsto a_{1010} + \beta_2 a_{1001}$ while leaving the leading coefficient a_{2000} fixed.) This completes the proof of Theorem 1. $\square$

Theorem 2, or more precisely Corollary 3, can be used to deal with not only the weakly divisible case (Theorem 1), but also the strongly divisible case (Theorem 4).

Theorem 4. Let $f(x_0, \ldots, x_k) \in \mathbb{Z}[x_0, \ldots, x_k]$ be a homogeneous polynomial of degree $d \geq 2$. Let p be a prime. Denote all the coefficients of f by $a_0(f), \ldots, a_N(f)$, where $N = \binom{k+d}{d} - 1$. Suppose

$$p \mid \Delta_{d,k}(f), \qquad \text{and} \qquad p \mid \frac{\partial \Delta_{d,k}}{\partial a_i}(f) \quad \text{for all } i = 0, \ldots, N.$$

Then $p^2 \mid \Delta_{d,k}(f)$ strongly.

Proof. We prove that $p^2 \mid \Delta_{d,k}(f)$. Since the divisibility conditions above are mod-p conditions, we will automatically have that p^2 strongly divides $\Delta_{d,k}(f)$.

Since $p \mid \Delta_{d,k}(f)$, we know that f mod p has a singular point $[r_0 : \cdots : r_k] \in \mathbb{P}^k(\ell)$, where ℓ is some finite extension of $\mathbb{F}_p$. Let L be an unramified extension of $\mathbb{Q}_p$ with residue field ℓ, and let $[s_0 : \cdots : s_k] \in \mathbb{P}^k(\mathcal{O}_L)$ be a lift of $[r_0 : \cdots : r_k]$. Without loss of generality, we may assume at least one of the s_i is a unit. Then there exists a matrix $\gamma \in \mathrm{SL}_{k+1}(\mathcal{O}_L)$ such that

$$(1, 0, \ldots, 0) = (s_0, \ldots, s_k)\gamma.$$

Note that if we were to assume $p^2 \nmid \Delta_{d,k}(f)$ for a contradiction and use Theorem 13 as in the previous section, we could take $\ell = \mathbb{F}_p$ and $L = \mathbb{Q}_p$. We define

$$g(x_0, \ldots, x_k) = f((x_0, \ldots, x_k)\gamma^{-1}) \in \mathcal{O}_L[x_0, \ldots, x_k].$$

Then $\Delta_{d,k}(g) = \Delta_{d,k}(f)$, and it is enough to prove that $p^2 \mid \Delta_{d,k}(g)$.

Write $b_i = a_i(f)$ and $c_i = a_i(g)$ for the coefficients of f and g. Then since $[1 : 0 : \cdots : 0]$ is a singular point of g mod p, we know that $p \mid c_i$ for $i = 0, \ldots, k$. Again from Corollary 3, we have

$$\Delta_{d,k} \equiv a_0 D_0 \pmod{(a_0, \ldots, a_k)^2}.$$

So it suffices to prove that $p \mid D_0(g)$. We note that

$$D_0 \equiv \frac{\partial \Delta_{d,k}}{\partial a_0} \pmod{(a_0, \ldots, a_k)}.$$

We know that p divides all the partial derivatives of $\Delta_{d,k}$ when evaluated at f. It remains to prove the same is true when they are evaluated at g.

Fix any generic $g_0(x_0, \ldots, x_k) \in \mathbb{Z}[a_0, \ldots, a_N][x_0, \ldots, x_k]$ and any generic $\gamma_0 \in \mathrm{SL}_{k+1}$. Write also $\Delta_{d,k}(a_0, \ldots, a_N)$ for $\Delta_{d,k}(g_0)$. Let

$$f_0(x_0, \ldots, x_{k+1}) = g_0((x_0, \ldots, x_{k+1})\gamma_0).$$

Then there exist polynomials $L_0, \ldots, L_N \in \mathbb{Z}[a_0, \ldots, a_N][\mathrm{SL}_{k+1}]$ such that

$$a_i(f_0) = L_i(a_0, \ldots, a_N, \gamma_0) \quad \text{for all } i = 0, \ldots, N.$$

Since $\Delta_{d,k}$ is an SL_{k+1}-invariant, we have

$$\Delta_{d,k}(a_0, \ldots, a_N) = \Delta_{d,k}(L_0(a_0, \ldots, a_N, \gamma_0), \ldots, L_N(a_0, \ldots, a_N, \gamma_0)).$$

For any $i = 0, \ldots, N$, differentiating with respect to a_i gives

$$\frac{\partial \Delta_{d,k}}{\partial a_i}(a_0, \ldots, a_N) = \sum_{j=0}^{N} \frac{\partial \Delta_{d,k}}{\partial a_j}(L_0, \ldots, L_N) \frac{\partial L_j}{a_i}(a_0, \ldots, a_N, \gamma_0).$$

Specializing to $a_0 = c_0, \ldots, a_{k+1} = c_{k+1}$ and $\gamma_0 = \gamma$ gives

$$\frac{\partial \Delta_{d,k}}{\partial a_i}(g) = \sum_{j=0}^{N} \frac{\partial \Delta_{d,k}}{\partial a_j}(f)\, c_{ij}$$

for some $c_{ij} \in \mathcal{O}_L$. Since $p \mid \dfrac{\partial \Delta_{d,k}}{\partial a_i}(f)$ for all $i = 0, \ldots, N$, we have $p \mid \dfrac{\partial \Delta_{d,k}}{\partial a_i}(g)$ for all $i = 0, \ldots, N$. This concludes the proof of Theorem 4. □

We end this chapter with the proof of Theorem 6.

Theorem 6. Let $f(x_0, \ldots, x_k) \in \mathbb{Z}[a_0, \ldots, a_N][x_0, \ldots, x_k]$ be a generic homogeneous polynomial of degree $d \geq 2$, where $N = \binom{k+d}{d} - 1$, expressed as

$$f(x_0, x_1, \ldots, x_k) = a_0 x_0^d + x_0^{d-1}(a_1 x_1 + \cdots + a_k x_k) + x_0^{d-2} Q(x_1, \ldots, x_k) + \cdots$$

where $Q(x_1, \ldots, x_k)$ is a quadratic form. Let K be the algebraic closure of the field of fractions of $\mathbb{Z}[a_{k+1}, \ldots, a_N]/(a_1, \ldots, a_k, \Delta_{2,k-1}(Q))$ and let $R = K[[a_0]]$. Then $a_0^2 \mid \Delta_{d,k}(f)$ in R.

Proof. We note that on writing

$$2Q(x_1, \ldots, x_k) = (x_1, \ldots, x_k) A_Q (x_1, \ldots, x_k)^{\top}$$

for some symmetric $k \times k$ matrix A_Q with coefficients in K, we have

$$\Delta_{2,k-1}(Q) = (-1)^{k(k-1)/2} \det(A_Q).$$

Alternatively, A_Q is the matrix of second partial derivatives of Q. In particular, A_Q is a singular matrix if and only if Q is singular over K.

The special fibre H_K is cut out by $x_0^{d-2} Q(x_1, \ldots, x_n) + \cdots$, which has a singular point at $[1 : 0 : \cdots : 0]$. The completed local ring of H_K at the point $P = [1 : 0 : \cdots : 0]$ is

$$\hat{\mathcal{O}}_{H_K,P} = K[[x_1, \ldots, x_k]]/(Q(x_1, \ldots, x_k) + C(x_1, \ldots, x_k))$$

where $C(x_1, \ldots, x_k)$ consists of the terms in $f(1, x_1, \ldots, x_k)$ of degree at least 3. We claim that P is not a non-degenerate double point. Suppose otherwise. Then by [26, Remark 4.3], there is an isomorphism

$$\varphi : K[[x_1, \ldots, x_k]]/(Q(x_1, \ldots, x_k) + C(x_1, \ldots, x_k)) \xrightarrow{\sim} K[[x_1, \ldots, x_k]]/(x_1^2 + \cdots + x_k^2).$$

Let $L_1, \ldots, L_k \in K[x_1, \ldots, x_k]$ be linear forms such that for any $i = 1, \ldots, k$,

$$\varphi(x_i) \equiv L_i(x_1, \ldots, x_k) \pmod{(x_1, \ldots, x_k)^2}.$$

Then, by comparing the lowest degree terms, we have

$$x_1^2 + \cdots + x_k^2 \mid Q(L_1, \ldots, L_k) \quad \text{in } K[[x_1, \ldots, x_k]].$$

Since φ is an isomorphism, we see that the map $(x_1, \dots, x_k) \mapsto (L_1, \dots, L_k)$ is a linear isomorphism. Hence, since Q is singular and $x_1^2 + \cdots + x_k^2$ is a non-singular quadratic form, we must have $Q(L_1, \dots, L_k) = 0$ and so $Q = 0$ in order for $x_1^2 + \cdots + x_k^2$ to divide $Q(L_1, \dots, L_k)$. However, Q is nonzero in the field K. Therefore, we have by Theorem 13 that $a_0^2 \mid \Delta_{d,k}(f)$ in R. This completes the proof of Theorem 6. $\square$

Chapter 4

On Δ_d'

In this chapter, we consider the polynomial Δ_d' and prove Theorem 7 and Theorem 8. We first recall the definition of Δ_d', introduced in [8], which one can think of as a derivative of the discriminant with respect to all of the coefficients.

Given a polynomial $f(x) = a_0x^d + \cdots + a_d$ with degree $d \geq 3$ (so $a_0 \neq 0$) and roots $r_1, \ldots, r_d$, we define

$$\Delta_d'(f) = \sum_{i<j} \frac{\Delta_d(f)}{(r_i - r_j)^2},$$

where in this chapter, we drop the subscript k and use $\Delta_d(f)$ to denote the usual polynomial discriminant of $f(x)$. Since Δ_d' is a symmetric polynomial in the roots $\{r_i\}$ with integer coefficients, it can be written as a polynomial $\Delta_d'(a_0, \ldots, a_d) \in \mathbb{Z}[a_0, \ldots, a_d]$ in the coefficients of f. We then extend the definition of $\Delta_d'(f)$ to where $a_0 = 0$ using $\Delta_d'(0, a_1, \ldots, a_d)$. We will also write $\Delta_d(a_0, \ldots, a_d)$ for $\Delta_d(a_0x^d + \cdots + a_d)$.

The polynomial $\Delta_d'(a_0, \ldots, a_d)$ is homogeneous of degree $2d - 2$, and weighted homogeneous of degree $d(d-1)-2$ if we give each a_i weight i. Since $d \nmid d(d-1)-2$ when $d \geq 3$, we see that $\Delta_d'(a_0, \dots, a_d)$ does not contain a monomial of the form $a_0^{m_1} a_d^{m_2}$. This immediately gives

$$\Delta_d'(a_0 x^d + a_d) = 0.$$

It is worth noting that $\Delta_d(a_0 x^d + a_d) = (-1)^{d(d-1)/2} d^d a_0^{d-1} a_d^{d-1}$ is not necessarily zero. Similarly, we note that

$$d(d-1)-2 = 2(d-1) + (d-3)d$$

is the unique way to express $d(d-1)-2$ as a non-negative integer combination of $d-1$ and d. As a result, we have

$$\Delta_d'(a_0 x^d + a_{d-1} x + a_d) = C_d a_0^{d-1} a_{d-1}^2 a_d^{d-3},$$

for some integer C_d. In light of Theorem 8, we see that C_d is the coefficient of $a_0^{d-2} a_2 a_{d-1}^2 a_d^{d-3}$ in Δ_d multiplied by $\binom{d}{2}/(-4)$. We will compute this coefficient in Theorem 16.

Theorem 8. Let $f(x) = a_0 x^d + a_1 x^{d-1} + \cdots + a_d \in \mathbb{Z}[a_0, \dots, a_d][x]$ with $d \geq 3$. Then as polynomials in $a_0, \dots, a_d$, we have

$$-4\Delta_d' = \sum_{i=0}^{d-2} \binom{d-i}{2} a_i \frac{\partial \Delta_d}{\partial a_{i+2}}. \tag{4.1}$$

Proof. It suffices to prove the equation holds over $\mathbb{C}$. Suppose first that $f \in \mathbb{C}[x]$ is a polynomial of degree d with a double root at 0, so that $a_{d-1}(f) = a_d(f) = 0$. Let

$g(x) = f(x)/x^2$. From the formula

$$\Delta_d(a_0x^d + \cdots + a_d) \equiv -4a_d a_{d-2}^3 \Delta_{d-2}(a_0x^{d-2} + \cdots + a_{d-2}) \pmod{(a_d, a_{d-1})^2}, \tag{4.2}$$

for the discriminant of a polynomial, we see that

$$\frac{\partial \Delta_d}{\partial a_d}(f) = -4a_{d-2}^3 \Delta_{d-2}(g)$$

and

$$\frac{\partial \Delta_d}{\partial a_i}(f) = 0, \text{ for } i = 0, \ldots, d-1.$$

Let $r_1, \ldots, r_{d-2}$ denote the roots of $g(x)$. Then

$$\Delta_d'(f) = a_0^{2d-2} \left(\prod_{i=1}^{d-2} (r_i - 0)^2 \right)^2 \prod_{1 \le i < j \le d-2} (r_i - r_j)^2 = a_{d-2}^4 \Delta_{d-2}(g). \tag{4.3}$$

Hence we see that (4.1) holds when f has a double root at 0.

We claim that both sides of (4.1) are invariant under shifts of the form $f(x) \mapsto f(x+r)$ for any $r \in \mathbb{C}$. This is true for Δ_d' by definition. For the right-hand side, we have

$$a_j(f(x+r)) = \sum_{i=0}^{j} \binom{d-i}{d-j} a_i r^{j-i} = a_j + (d-j+1)a_{j-1}r + \cdots. \tag{4.4}$$

From

$$\Delta_d(a_0, \ldots, a_d) = \Delta_d(a_0(f(x+r)), \ldots, a_d(f(x+r))),$$

we have

$$\frac{\partial \Delta_d}{\partial a_i}(f) = \sum_{j=i}^{d} \frac{\partial \Delta_d}{\partial a_j}(f(x+r)) \binom{d-i}{d-j} r^{j-i}$$

and solving for the partial derivatives evaluated at $f(x+r)$ gives

$$\frac{\partial \Delta_d}{\partial a_j}(f(x+r)) = \sum_{\ell=j}^{d} \frac{\partial \Delta_d}{\partial a_\ell}(f) \binom{d-j}{\ell-j} (-r)^{\ell-j}. \tag{4.5}$$

We observe that $a_j(f(x+r))$ is expressed in terms of a_i for $i \le j$, while the partial derivative $\frac{\partial \Delta_d}{\partial a_j}(f(x+r))$ is expressed in terms of the partial derivatives $\frac{\partial \Delta_d}{\partial a_i}(f)$ for $i \ge j$; both with coefficients 1 when $i = j$. It suffices to prove that when $\ell \ge i+3$, the coefficient of

$$a_i \frac{\partial \Delta_d}{\partial a_\ell}(f) \quad \text{in} \quad \sum_{j=0}^{d-2} \binom{d-j}{2} a_j(f(x+r)) \frac{\partial \Delta_d}{\partial a_{j+2}}(f(x+r)) \quad \text{is} \quad 0.$$

Expanding using (4.4) and (4.5) shows that this coefficient equals

$$\frac{(d-i)!}{(d-\ell)!(\ell-i-2)!} r^{\ell-i-2} \sum_{i \le j \le \ell-2} \binom{\ell-i-2}{\ell-j-2} (-1)^{\ell-j-2} = 0$$

since $\ell - i - 2 \ge 1$.

We have shown that the difference H of the two sides in the desired equation (4.1) vanishes on the subset U of $\mathbb{P}^d(\mathbb{C})$ consisting of $[a_0 : \cdots : a_d]$ such that the binary form $a_0x^d + \cdots + a_dy^d$ has a factor of the form $(x+ry)^2$ for some $r \in \mathbb{C}$. The Zariski closure of U in $\mathbb{P}^d(\mathbb{C})$ has dimension at least $d-1$ and is contained in the irreducible variety $V(\Delta_d)$. Hence they are the same, and so H vanishes on $V(\Delta_d)$. It then follows from the Nullstellensatz and the irreducibility of Δ_d that $\Delta_d \mid H$ in $\mathbb{C}[a_0, \ldots, a_d]$. Comparing homogeneous degrees gives $H = \lambda\Delta_d$ for some $\lambda \in \mathbb{C}$. Comparing weighted homogeneous degrees then gives $\lambda = 0$. Therefore, $H = 0$ and this completes the proof of Theorem 8. $\square$

Corollary 14. For $d \geq 4$, we have the recursive formula

$$\Delta'_d(a_0, \ldots, a_d) \equiv a_1^2 \Delta'_{d-1}(a_1, \ldots, a_d) \pmod{a_0}.$$

Proof. We know that

$$\Delta_d(a_0x^d + \cdots + a_d) \equiv a_1^2 \Delta_{d-1}(a_1x^{d-1} + \cdots + a_d) \pmod{a_0}.$$

Hence, by Theorem 8, we have that modulo a_0

$$\begin{aligned} -4\Delta'_d &\equiv \sum_{i=1}^{d-2} \binom{d-i}{2} a_i \frac{\partial \Delta_d(a_0x^d + \cdots + a_d)}{\partial a_{i+2}} \\ &\equiv a_1^2 \sum_{j=0}^{d-3} \binom{d-1-j}{2} a_{j+1} \frac{\partial \Delta_{d-1}(a_1x^{d-1} + \cdots + a_d)}{\partial a_{j+3}} \\ &\equiv -4a_1^2 \Delta'_{d-1}(a_1, \ldots, a_d) \pmod{a_0}, \end{aligned}$$

as desired. $\square$

We note that Corollary 14 implies that if $a_0, \ldots, a_d \in \mathbb{Z}$ and p is a prime dividing a_0 and a_1, then $p \mid \Delta'_d(a_0, \ldots, a_d)$ and $p \mid \Delta_d(a_0, \ldots, a_d)$, but we do not necessarily have $p^2 \mid \Delta_d(a_0, \ldots, a_d)$. For example, if $g(x) \in \mathbb{Z}[x]$ is a monic polynomial of degree $d-2$ such that $p \nmid \Delta_{d-2}(g)$, then by (1.1),

$$\Delta_d(px^d + px^{d-1} + g(x)) \equiv -4p\,\Delta_{d-2}(g) \pmod{p^2},$$

which is not divisible by p^2 if $p > 2$. We now prove that if p does not divide the leading coefficient, then $p \mid \Delta'_d$ and $p \mid \Delta_d$ imply $p^2 \mid \Delta_d$.

Corollary 15. Suppose $f(x) = a_0x^d + \cdots + a_d \in \mathbb{Z}[x]$ is a polynomial of degree $d \geq 3$. Let p be an odd prime such that $p \nmid a_0$. Then $p \mid \Delta'_d(f)$ and $p \mid \Delta_d(f)$ if and only if $p^2 \mid \Delta_d(f)$ strongly.

Proof. The backward direction follows because $p^2 \mid \Delta_d(f)$ strongly implies that p divides all the partial derivatives of Δ_d evaluated at f, and so $p \mid 4\Delta'_d(f)$ since $4\Delta'_d$ is in the ideal generated by the partial derivatives of Δ_d in $\mathbb{Z}[a_0, \ldots, a_d]$. We then have $p \mid \Delta'_d(f)$ since $p \neq 2$.

We now prove the forward direction. Since $p \mid \Delta'_d(f)$ and $p \mid \Delta_d(f)$ are mod-p conditions, it suffices to prove that $p^2 \mid \Delta_d(f)$; in other words, the "strongly" part is automatic. Suppose for a contradiction that $p^2 \nmid \Delta_d(f)$. Then f mod p has a simple double root defined over $\mathbb{F}_p$. By moving this root mod p to 0, we may assume that $p \mid a_{d-1}$ and $p \mid a_d$. We also have $p \nmid a_{d-2}$ since f mod p has no triple root. Let $g(x) = a_0x^{d-2} + \cdots + a_{d-2}$. By (4.2) and (4.3), we have

$$\begin{aligned}
\Delta_d(f) &\equiv -4a_d a_{d-2}^3 \Delta_{d-2}(g) \pmod{p^2} \\
\Delta'_d(f) &\equiv a_{d-2}^4 \Delta_{d-2}(g) \pmod{p},
\end{aligned}$$

where the second congruence follows because (4.3) is an equality mod a_{d-1} and a_d, both of which are divisible by p. It now follows that $p \mid \Delta_{d-2}(g)$ and then the first congruence gives $p^2 \mid \Delta_d(f)$. $\square$

We give another application of Theorem 8.

Theorem 16. Suppose $d \geq 3$. Then

$$\Delta'_d(a_0x^d + a_{d-1}x + a_d) = (-1)^{d(d-1)/2-1}\frac{d^{d-1}(d-1)^3}{8}a_0^{d-1}a_{d-1}^2a_d^{d-3}.$$

Proof. When $d = 3$, we check using the explicit formula that

$$\Delta'_3(a_0x^3 + a_2x + a_3) = (-3a_0a_2)^2 = \frac{3^22^3}{8}a_0^2a_2^2a_3^0.$$

Suppose now $d \geq 4$. By Theorem 8, we see that it suffices to prove that

$$\text{the coefficient of } a_0^{d-2}a_2a_{d-1}^2a_d^{d-3} \text{ in } \Delta_d \text{ is } (-1)^{d(d-1)/2}d^{d-2}(d-1)^2,$$

since $\binom{d}{2}a_0\frac{\partial\Delta_d}{\partial a_2}$ is the only nonzero term. Let M denote the $(2d-1)\times(2d-1)$ Sylvester matrix (used to calculate the resultant of f and f' for a degree d polynomial f) whose determinant is $(-1)^{d(d-1)/2}a_0\Delta_d$. For any $(2d-1)\times(2d-1)$ matrix B whose coordinates are linear forms in $a_0,\ldots,a_d$, let $c(B)$ denote the coefficient of $a_0^{d-1}a_2a_{d-1}^2a_d^{d-3}$ in $\det(B)$. Then it remains to prove that

$$c(M) = d^{d-2}(d-1)^2.$$

We note that a_2 appears in exactly one coordinate in every row in M. For $i = 1, \dots, 2d-1$, let M_i be the matrix obtained from M by keeping the a_2 in the i-th row and replacing all other a_2's by 0. Then we see that

$$c(M) = c(M_1) + c(M_2) + \cdots + c(M_{2d-1}). \tag{4.6}$$

This can be seen using the Leibniz formula for the determinant:

$$\det(B) = \sum_{\sigma \in S_{2d-1}} \operatorname{sign}(\sigma) P(B, \sigma), \quad \text{where} \quad P(B, \sigma) = \prod_{i=1}^{2d-1} (i, \sigma(i))\text{-entry of } B.$$

Indeed, for a fixed $\sigma \in S_{2d-1}$, if the $(j, \sigma(j))$-entry of M is a nonzero multiple of a_2 for some $j = 1, \dots, 2d-1$, then

$$P(M, \sigma) = P(M_j, \sigma), \quad \text{and} \quad P(M_\ell, \sigma) = 0 \text{ for } \ell \neq j.$$

Summing over σ gives (4.6).

Each $c(M_i)$ can be computed explicitly. We have

$$c(M_i) = \begin{cases} d^{d-2}(d-1) & \text{if } 1 \leq i \leq d-1 \\ -d^{d-3}(d-1)(d-2) & \text{if } d \leq i \leq 2d-2 \\ d^{d-3}(d-1)^2(d-2) & \text{if } i = 2d-1. \end{cases}$$

We will state the key results only. We write $c(B, \sigma)$ for the coefficient of $a_0^{d-1} a_2 a_{d-1}^2 a_d^{d-3}$ in $P(B, \sigma)$. It turns out that for $c(M_i, \sigma)$ to be nonzero, σ contains a cycle of length $2d-4$

if $1 \leq i \leq d-1$ or a cycle of length $2d-5$ if $d \leq i \leq 2d-1$. More precisely:

(a) Suppose $i = 1, \ldots, d-2$. If $c(M_i, \sigma) \neq 0$, then σ contains the $(2d-4)$-cycle

$$(i \quad i+2 \quad d+i+2 \quad i+3 \quad \cdots \quad 2d-1 \quad d \quad 1 \quad d+1 \quad 2 \quad \cdots \quad i-1 \quad d+i-1)$$

and fixes $d+i+1$. The 2×2 matrix formed from the remaining two indices $i+1$ and $d+i$ is

$$N = \begin{pmatrix} a_0 & a_{d-1} \\ da_0 & a_{d-1} \end{pmatrix}.$$

In this case, we have

$$c(M_i) = d^{d-2}(d-1).$$

(b) Suppose $i = d-1$. If $c(M_i, \sigma) \neq 0$, then σ contains the $(2d-4)$-cycle

$$(d-1 \quad d+1 \quad 2 \quad d+2 \quad \cdots \quad d-2 \quad 2d-2)$$

and fixes $2d-1$. The 2×2 matrix formed from the remaining two indices 1 and d is also N. In this case, we have

$$c(M_i) = d^{d-2}(d-1).$$

(c) Suppose $i = d, \ldots, 2d-4$. If $c(M_i, \sigma) \neq 0$, then σ contains the $(2d-5)$-cycle

$$(i \quad i-d+3 \quad i+3 \quad i-d+4 \quad \cdots \quad 2d-1 \quad d \quad 1 \quad d+1 \quad 2 \quad \cdots \quad i-1 \quad i-d)$$

and fixes $i-d+1$ and $i+2$. The 2×2 matrix formed from the remaining two indices $i-d+2$ and $i+1$ is also N. In this case, we have

$$c(M_i) = -d^{d-3}(d-1)(d-2).$$

(d) Suppose $i = 2d-3$. If $c(M_i, \sigma) \neq 0$, then σ contains the $(2d-5)$-cycle

$$(2d-3 \quad d \quad 1 \quad d+1 \quad 2 \quad \cdots \quad 2d-4 \quad d-3)$$

and fixes $d-2$ and $2d-1$. The 2×2 matrix formed from the remaining two indices $d-1$ and $2d-2$ is also N. In this case, we have

$$c(M_i) = -d^{d-3}(d-1)(d-2).$$

(e) Suppose $i = 2d-2$. If $c(M_i, \sigma) \neq 0$, then σ contains the $(2d-5)$-cycle

$$(2d-2 \quad d+1 \quad 2 \quad d+2 \quad 3 \quad \cdots \quad 2d-3 \quad d-2)$$

and fixes $d-1$ and $2d-1$. The 2×2 matrix formed from the remaining two indices 1 and d is also N. In this case, we have

$$c(M_i) = -d^{d-3}(d-1)(d-2).$$

(f) Suppose $i = 2d-1$. If $c(M_i, \sigma) \neq 0$, then σ contains the $(2d-5)$-cycle

$$(2d-1 \quad d+2 \quad 3 \quad d+3 \quad 4 \quad \cdots \quad 2d-2 \quad d-1).$$

The 4×4 matrix formed from the remaining four indices 1, 2, d, $d+1$ is

$$N' = \begin{pmatrix} a_0 & 0 & a_{d-1} & a_d \\ 0 & a_0 & 0 & a_{d-1} \\ da_0 & 0 & a_{d-1} & 0 \\ 0 & da_0 & 0 & a_{d-1} \end{pmatrix}.$$

In this case, we have

$$c(M_i) = d^{d-3}(d-1)^2(d-2).$$

Note that we have

$$\sum_{i=1}^{d-1} c(M_i) = d^{d-2}(d-1)^2, \qquad \sum_{i=d}^{2d-1} c(M_i) = 0.$$

Summing these two equations gives the desired result. □

We conclude by proving Theorem 7. One can check directly that $\Delta_5'(a_0, \ldots, a_5)$ is irreducible in $\mathbb{C}[a_0, \ldots, a_5]$. Therefore, Theorem 7 follows from:

Theorem 17. Let $d \geq 6$ be an integer. If Δ_{d-1}' is irreducible in $\mathbb{C}[a_0, \ldots, a_{d-1}]$, then Δ_d' is irreducible in $\mathbb{C}[a_0, \ldots, a_d]$.

Proof. Suppose for a contradiction that Δ_d' is not irreducible. Any factorization of Δ_d' gives a factorization of $a_1^2\Delta'_{d-1}(a_1,\ldots,a_d)$ in $\mathbb{Z}[a_1,\ldots,a_d]$ via Corollary 14 by setting $a_0 = 0$. Since Δ'_{d-1} is irreducible, we see that there are three possibilities for a factorization of Δ'_d:

$$\begin{aligned}
\Delta'_d(a_0,\ldots,a_d) &= (a_0G+1)(a_0H+a_1^2\Delta'_{d-1}(a_1,\ldots,a_d)) \\
\Delta'_d(a_0,\ldots,a_d) &= (a_0G+a_1)(a_0H+a_1\Delta'_{d-1}(a_1,\ldots,a_d)) \\
\Delta'_d(a_0,\ldots,a_d) &= (a_0G+a_1^2)(a_0H+\Delta'_{d-1}(a_1,\ldots,a_d)),
\end{aligned}$$

where $G, H \in \mathbb{C}[a_0,\ldots,a_d]$. Since any factor of a homogeneous and weighted homogeneous polynomial is also homogeneous and weighted homogeneous, we see that only the third type of factorization is possible and that, moreover, $a_0G + a_1^2$ must be of the form $c\,a_0\,a_2 + a_1^2$ for some $c \in \mathbb{C}$ in order to be weighted homogeneous. This means that if $a_1 = a_2 = 0$, then $\Delta'_d = 0$. Consider now the polynomial $f(x) = x^2(x^{d-2}+1)$. We know from (4.3) that

$$\Delta'_d(f) = \Delta_{d-2}(x^{d-2}+1) \neq 0,$$

but $a_1(f) = a_2(f) = 0$, which is a contradiction. $\square$

References

[1] M. Bhargava. The density of discriminants of quartic rings and fields. *Annals of Mathematics*, pages 1031–1063, 2005.

[2] M. Bhargava. The density of discriminants of quintic rings and fields. *Annals of mathematics*, pages 1559–1591, 2010.

[3] M. Bhargava. The geometric sieve and the density of squarefree values of invariant polynomials. *arXiv preprint arXiv:1402.0031*, 2014.

[4] M. Bhargava and A. Shankar. The average number of elements in the 4-selmer groups of elliptic curves is 7. *arXiv preprint arXiv:1312.7333*, 2013.

[5] M. Bhargava and A. Shankar. The average size of the 5-selmer group of elliptic curves is 6, and the average rank is less than 1. *arXiv preprint arXiv:1312.7859*, 2013.

[6] M. Bhargava and A. Shankar. Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves. *Annals of Mathematics*, pages 191–242, 2015.

[7] M. Bhargava and A. Shankar. Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0. *Annals of Mathematics*, pages 587–621, 2015.

[8] M. Bhargava, A. Shankar, and X. Wang. An improvement on Schmidt's bound on the number of number fields of bounded discriminant and small degree. *Forum of Mathematics, Sigma*, 10(e86):1–13, 2022.

[9] M. Bhargava, A. Shankar, and X. Wang. Squarefree values of polynomial discriminants i. *Inventiones mathematicae*, 228(3):1037–1073, 2022.

[10] M. Bhargava, A. Shankar, and X. Wang. Squarefree values of polynomial discriminants ii. *arXiv preprint arXiv:2207.05592*, 2022.

[11] D. Cox. What is a toric variety? *Contemporary Mathematics*, 334:203–224, 2003.

[12] D. Cox, J. Little, and H. Schenck. *Toric varieties*, volume 124. American Mathematical Soc., 2011.

[13] I. Gelfand, M. Kapranov, and A. Zelevinsky. *Discriminants, resultants, and multidimensional determinants.* Modern Birkhäuser classics. Birkhäuser, Boston, 2008.

[14] G. González-Sprinberg. L'obstruction locale d'euler et le théoreme de macpherson. *Astérisque*, 82(83):7–32, 1981.

[15] A. Granville. ABC allows us to count squarefrees. *International Mathematics Research Notices*, 1998(19):991–1009, 01 1998.

[16] G. Greaves. Power-free values of binary forms. *Quart. J. Math. Oxford Ser. (2)*, 43(1):45–65, 1992.

[17] C. Hooley. On the square-free values of cubic polynomials. *J. Reine Angew. Math.*, 229:147–154, 1968.

[18] Y. Jiang. Note on macpherson's local euler obstruction. *Michigan Mathematical Journal*, 68(2):227–250, 2019.

[19] J. Kowalski. On the proportion of squarefree numbers among sums of cubic polynomials. *The Ramanujan Journal*, 54:343–354, 2021.

[20] A. Landesman. Notes on counting extensions of degrees 2 and 3, following Bhargava. https://people.math.harvard.edu/~landesman/assets/bhargavology-seminar-notes.pdf. [Online; accessed 23 August, 2023].

[21] R. MacPherson. Chern classes for singular algebraic varieties. *Annals of Mathematics*, 100(2):423–432, 1974.

[22] T. Mandel. Introduction to toric varieties and algebraic geometry. https://math.ou.edu/~tmandel/Toric_Varieties_Notes.pdf, 2022. [Online; accessed 23 August, 2023].

[23] J. Mather. Notes on topological stability. *Bulletin of the American Mathematical Society*, 49(4):475–506, 2012.

[24] Y. Matsui and K. Takeuchi. A geometric degree formula for A-discriminants and Euler obstructions of toric varieties. *Advances in Mathematics*, 226(2):2040–2064, January 2011.

[25] B. Poonen. Squarefree values of multivariable polynomials. *Duke Mathematical Journal*, 118(2):353–373, 2003.

[26] B. Poonen and M. Stoll. The valuation of the discriminant of a hypersurface. *Preprint*, 2020. [Online; accessed 23 August, 2023 at https://math.mit.edu/~poonen/papers/discriminant.pdf].

[27] F. Rohrer. On toric schemes. *Proceedings of the 32nd Symposium and 6th Japan-Vietnam Joint Seminar on Commutative Algebra*, pages 182–188, 2010.

[28] F. Rohrer. The geometry of toric schemes. *Journal of Pure and Applied Algebra*, 217(4):700–708, apr 2013.

[29] T. Saito. The discriminant and the determinant of a hypersurface of even dimension. *Mathematical Research Letters*, 19(04):855–871, 2012.

[30] G. Sanjaya and X. Wang. On the squarefree values of a^4+b^3. *Mathematische Annalen*, pages 1–29, 2022.

[31] The Stacks Project Authors. *Stacks Project*. https://stacks.math.columbia.edu, 2018.

[32] S. Venkatesh. Constructible sheaves and stratified spaces. https://math.mit.edu/~sidnv/Constructible_Sheaves_on_Stratified_Spaces.pdf, 2015. [Online; accessed 23 August, 2023].

[33] H. Whitney. Tangents to an analytic variety. *Annals of Mathematics*, 81(3):496–549, 1965.