SOME ARITHMETIC APPLICATIONS OF INVARIANT THEORY

W. DUKE

Abstract. The classical invariant theory of binary forms and pairs of binary forms is applied to some problems about the representation of integers by certain binary quartic forms.

1. Introduction

A venerable problem in number theory is to describe the integers that are represented by an integral binary form. Much more is known here in the quadratic case than in higher degree cases, as is reflected in the well-known relationship between binary quadratic forms and (proper) ideals in orders of quadratic fields. A general tool that may be applied to this problem is the arithmetic invariant theory of forms and pairs of forms. In this paper I will provide illustrations where invariant theory yields results about binary quartic forms that are parallel to the some classical results about binary quadratic forms.

The following results were discovered early in the study of representations by the integral binary quadratic form

$$F(x,y) = ax^2 + bxy + cy^2$$

with discriminant $D_F = b^2 - 4ac$.

Theorem 1. *Suppose that $F(x,y)$ is primitive with $D_F \neq 0$.*

i) There exists a primitive binary quadratic form G with $D_G = D_F$ that properly represents the square of each integer prime to D_F that F properly represents.

ii) If F can be written in the form

$$F(x,y) = (b^2 - ac)x^2 + (bc - ad)xy + (c^2 - bd)y^2$$

with integers a, b, c, d then in i) we may take $G = F$.

Part i) is a well-known consequence of the composition of quadratic forms. Roughly speaking, part ii) reflects Eisenstein's observation (c.f. [4]) that (negatives of) Hessians of binary cubics are of order three in the class group, using that a binary quadratic form and its inverse with respect to composition represent the same integers.

The simplest example to illustrate Theorem 1 is when

$$F(x,y) = x^2 + y^2$$

with $D_F = -4$, where $G = F$ and the result follows easily from the duplication formula

$$F(2xy, x^2 - y^2) = F^2(x,y). \tag{1.1}$$

Note that $x^2 + y^2$ does not represent 4 properly although $2 = 1^2 + 1^2$; the theorem is not true if we drop the assumption that the represented integer be prime to the discriminant. Part ii) applies here since we can write F in the required form by using $(a,b,c,d) = (1,0,-1,0)$. The general duplication formula for forms of the type in ii) is given in (3.6).

Research supported by NSF grant DMS 1701638 and Simons Foundation Award Number 554649.

Consider now a binary quartic form F with integral coefficients that is *even* in that it has the form

$$F(x,y) = ax^4 + 2bx^3y + cx^2y^2 + 2dxy^3 + ey^4,$$

for integers a, b, c, d, e and is properly primitive, which we will shorten to "primitive", meaning that $\gcd(a, 2b, c, 2d, e) = 1$. The set of primitive even F is preserved under the usual action of $\Gamma = \mathrm{SL}(2,\mathbb{Z})$ and there are two independent integral invariants, namely

$$A_F = 12ae - 12bd + c^2 \quad \text{and} \quad B_F = 36ace + 18bcd - 54b^2e - 54d^2a - c^3. \tag{1.2}$$

The discriminant of F normalized for even forms is defined by

$$D_F = \tfrac{1}{2^2 3^3}(A_F^3 - B_F^2). \tag{1.3}$$

Given such a form F with $D_F \neq 0$, it is not in general possible to find another integral binary quartic form G, even one with a different (non-zero) discriminant, that properly represents the square of every integer that is properly represented by F and is prime to D_F. This can be seen already when

$$F(x,y) = 4x^4 + y^4,$$

which has $D_F = 2^{10}$. It follows from [5, Theorem 1] that the number of odd integers $\leq T^{\frac{1}{2}}$ properly represented by F is $\gg T^{\frac{1}{4}}$ for $T \geq 1$. Here we use symmetry to show that enough odd integers are represented. Suppose that there were a G with $D_G \neq 0$ that represented properly the square of every odd integer $\leq T^{\frac{1}{2}}$ properly represented by F. Then G would properly represent $\gg T^{\frac{1}{4}}$ squares less than T, i.e. the equation

$$z^2 = G(x,y)$$

would have $\gg T^{\frac{1}{4}}$ solutions with $\gcd(x,y) = 1$ and $|z| \leq T$. But it is known by Mordell's theorem for nonsingular curves of genus one defined over $\mathbb{Q}$ that this number is $\ll_\epsilon T^\epsilon$, for any $\epsilon > 0$.

Our first new result shows that a weaker statement does hold for certain F.

Theorem 2. *Suppose that $F(x,y)$ is a primitive even binary quartic form with $A_F = P^2$ for some $P \in \mathbb{Z}$ and with $D_F \neq 0$. There exists a primitive even binary quartic form G with $D_G = m^2 D_F$ for some positive $m \in \mathbb{Q}$ with the following property. The form G properly represents some nonzero multiple of the square of each integer prime to $3D_F$ that F properly represents.*

As an example let

$$F(x,y) = x^4 + x^2y^2 - 6xy^3 + 2y^4,$$

which has $A_F = 5^2$ and $D_F = -2 \cdot 5^2 \cdot 29$. The proof of Theorem 2 shows that we may take

$$G(x,y) = 4x^4 - 28x^3y + 37x^2y^2 - 26xy^3 + 5y^4,$$

for which $A_G = -5^2 \cdot 23$ and $D_G = 2^6 \cdot 5^2\, D_F$. As particular instances of representations of multiples of squares provided by the proof of Theorem 2 we have

$$\begin{aligned} F(0,1) = 1 \quad &\text{and} \quad G(1,1) = -8 \cdot 1^2, \\ F(1,2) = -11 \quad &\text{and} \quad G(13,3) = -188 \cdot (-11)^2, \\ F(5,14) = 37 \quad &\text{and} \quad G(5417,979) = -750668 \cdot 37^2 \\ F(3,-2) = 293 \quad &\text{and} \quad G(33,71) = -508 \cdot 293^2. \end{aligned}$$

Our next result is an analogue of part ii) of Theorem 1.

Theorem 3. *Suppose that $F(x,y)$ is a primitive even binary quartic form that can be written in the form*

$$F(x,y) = (b^2-ac)x^4 + 2(bc-ad)x^3y + (3c^2-ae-2bd)x^2y^2 + 2(cd-be)xy^3 + (d^2-ce)y^4$$

for integers a,b,c,d,e, and that therefore has $A_F = (ae-4bd+3c^2)^2$.

Assume that $A_F = 0$ and $D_F \neq 0$. If a and e are not both even, then we may take for G in Theorem 2 the form

$$G(x,y) = ax^4 + 4bx^3y + 6cx^2y^2 + 4dxy^3 + ey^4, \tag{1.4}$$

for which $D_G^2 = -2^8\,3^3 D_F$. If both a and e are even we may take

$$G(x,y) = \tfrac{1}{2}ax^4 + 2bx^3y + 3cx^2y^2 + 2dxy^3 + \tfrac{1}{2}ey^4,$$

for which $D_G^2 = -2^{-4}\,3^3 D_F$.

We will give a proof of Theorem 1 that serves as a model for those of Theorems 2 and 3, that of Theorem 2 being necessarily more intricate. The proof of Theorem 1 uses what is essentially Gaussian duplication (see Proposition 1), while those of Theorems 2 and 3 use a higher composition law, one that does not amount to the multiplication of norm forms. Here an even binary quartic is composed with itself and with another even binary quartic, a covariant. This composition law is given in Proposition 2.

To illustrate Theorem 3 consider

$$F(x,y) = x^4 + 6x^2y^2 - 3y^4,$$

which has $A_F = 0$ and $D_F = -2^8\,3^3$ and is of the form required when we choose $(a,b,c,d,e) = (1,0,-1,0,-3)$. We may take

$$G(x,y) = x^4 - 6x^2y^2 - 3y^4,$$

which satisfies $D_G = D_F$. These F and G are connected by an elegant quartic analogue of the duplication formula (1.1):

$$G(3x^2y + 3y^3, x^3 - 3xy^2) = -3G(x,y)F^2(x,y).$$

This identity yields the conclusion of Theorem 2 explicitly in this simple case.

We cannot apply Theorem 2 directly to the even binary quartic

$$F(x,y) = (ax^2+bxy+cy^2)^2 = a^2x^4 + 2abx^3y + (b^2+2ac)x^2y^2 + 2bcxy^3 + c^2y^4,$$

for which $A_F = (b^2-4ac)^2$ but $D_F = 0$. Nevertheless, it is possible to modify the proof of Theorem 2 to show that in part i) of Theorem 1 we can replace the word "square" by "cube", at least for forms with a square-free discriminant. In this way we can get a proof of such a result that does not use the class group, at least directly. See the Remark at the end of the paper for a related example.

Of course, much more can be said about such questions in the quadratic case by using the above-mentioned correspondence between classes of forms and ideal classes and applying algebraic number theory. My purpose here is to illustrate the use of tools that are also applicable to basic representation problems by higher degree binary forms.

2. Preliminaries

First we set notation, make some definitions and record some facts from the invariant theory of binary forms and pairs of binary forms. Let

$$F(x,y)=\sum_{n=0}^{m}a_n x^{m-n}y^n$$

where $a_0,\dots,a_m\in\mathbb{Z}$ be an integral binary form of degree m. We will use the abbreviation

$$F(x,y)=[a_0,\dots,a_m]. \tag{2.1}$$

Such an F is acted on by $g=\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\in\Gamma=\mathrm{SL}(2,\mathbb{Z})$ through

$$F\mapsto F|g=F(ax+by,cx+dy). \tag{2.2}$$

For each pair of non-negative integers m,n fix $c_{m,n}\in\mathbb{Z}^+$ such that $c_{m,0}=1$ and $c_{m,n}=c_{m,m-n}$. Define $\mathcal{F}$ to be the set of all F that can be written in the form

$$F(x,y)=\sum_{n=0}^{m}c_{m,n}a_n x^{m-n}y^n\qquad a_0,\dots,a_m\in\mathbb{Z}. \tag{2.3}$$

Say that $\mathcal{F}$ is admissible if it is preserved under (2.2) and if, for $F\in\mathcal{F}$ as given in (2.3), $\gcd(a_0,\dots,a_m)$ is left invariant under (2.2). In addition to the set $\mathcal{F}_1$ of ordinary integral forms where $c_{m,n}=1$ for all m,n, another admissible set is the set of Gaussian forms $\mathcal{F}_3$ with $c_{m,n}=\binom{m}{n}$. We abbreviate a Gaussian form by using open parentheses, e.g.

$$ax^2+2xy+cy^2=(a,b,c).$$

The set $\mathcal{F}_2$ of even forms, with $c_{m,1}=c_{m,m-1}=2$ for m even and $c_{m,n}=1$ otherwise, is also admissible. Note that admissibility is easily checked by expanding $F(x+y,y)$ and $F(-y,x)$. Clearly $\mathcal{F}_3\subset\mathcal{F}_2\subset\mathcal{F}$. For an admissible $\mathcal{F}$ the form $F\in\mathcal{F}$ given by (2.3) is classically called primitive (for $\mathcal{F}$) if $\gcd(a_0,\dots,a_m)=1$ and properly primitive if

$$\gcd(c_{m,0}a_0,\dots,c_{m,m}a_m)=1.$$

As mentioned before, in this paper we will use "primitive" for "properly primitive" unless otherwise specified.

An (arithmetic) covariant for $F\in\mathcal{F}_1$ is a binary form P_F whose coefficients are integral polynomials of the coefficients of F that satisfies

$$P_F|g=P_{F|g}$$

for all $g\in\Gamma$. If $P_F|g=P_F$ for all $g\in\Gamma$ then P_F gives an invariant of F. The discriminant $D_F=\mathrm{disc}_{x,y}(F)$ is an invariant of F. The Hessian of F

$$H_F(x,y)=\det\begin{pmatrix}F_{xx}&F_{xy}\\F_{yx}&F_{yy}\end{pmatrix} \tag{2.4}$$

is a covariant of F. The Jacobian of two forms F,G is given by

$$J_{F,G}(x,y):=\det\begin{pmatrix}F_x&F_y\\G_x&G_y\end{pmatrix}. \tag{2.5}$$

We have that $J_{F,H_F}(x,y)$ is a covariant of F. The *discriminant form* of two forms F,G of the same degree is given by

$$D_{F,G}(x,y)=\mathrm{disc}_{u,v}(xF(u,v)+yG(u,v)).$$

If F and H_F have the same degree, $D_{F,H_F}(x,y)$ is an invariant of F.

A pair (f_1, f_2) of binary forms of the same degree, each in some $\mathcal{F}$, is acted on in two ways by $g \in \Gamma$. One action is through

$$(f_1, f_2) \mapsto (f_1, f_2)|g = (f_1|g, f_2|g) \tag{2.6}$$

and the second through

$$(f_1, f_2) \mapsto (f_1, f_2)g = (af_1 + cf_2, bf_1 + df_2). \tag{2.7}$$

Invariants and covariants of pairs of forms with a given action are defined similarly to the case of a single form.

The Jacobian $J_{f_1,f_2}(x, y)$ is an invariant of (f_1, f_2) with respect to (2.7) and a covariant of (f_1, f_2) with respect to (2.6). The discriminant form $D_{f_1,f_2}(x, y)$ is an invariant of (f_1, f_2) with respect to (2.6) and a covariant of (f_1, f_2) with respect to (2.7).

In what follows we will normalize $D_F, H_F, J_{F,G}$ and $D_{F,G}$ by multiplying each by a constant, depending on the nature of F and G. For simplicity we will retain the notation $D_F, H_F, J_{F,G}$ and $D_{F,G}$ after we specify the normalization.

3. Pairs of binary quadratic forms

The proof of Theorem 1 makes use of the invariant theory of pairs of binary (Gaussian) quadratic forms, whose theory we will now review. For $f_1 = (a_1, b_1, c_1)$ and $f_2 = (a_2, b_2, c_2)$ we have the normalized discriminant form

$$D_{f_1,f_2}(x, y) = [b_1^2 - a_1c_1, 2b_1b_2 - a_1c_2 - a_2c_1, b_2^2 - a_2c_2]. \tag{3.1}$$

The normalized Jacobian is given by

$$J_{f_1,f_2}(x, y) = [(a_1\, b_2), (a_1\, c_2), (b_1\, c_2)], \tag{3.2}$$

where we are using the convenient notation from [10]:

$$(a_i\, b_j) = a_ib_j - a_jb_i. \tag{3.3}$$

A direct calculation verifies the following identity ("syzygy"):

Proposition 1. *For any pair (f_1, f_2) of Gaussian binary quadratic forms with discriminant form D_{f_1,f_2} we have the identity*

$$D_{f_1,f_2}(-f_2(x, y), f_1(x, y)) = J_{f_1,f_2}^2(x, y). \tag{3.4}$$

Proof of Theorem 1. i) Suppose that $F(x, y) = [a, b, c]$ is a primitive binary quadratic form with integer coefficients and non-zero discriminant D_F. First we show that F may be represented as the Jacobian, normalized as in (3.2), of two binary quadratic forms of Gaussian type. This is an immediate consequence of [6, art. 279]. An easy way to see this directly is to complete (a, b, c) to a matrix $A \in \mathrm{SL}(3, \mathbb{Z})$, which is possible since $\gcd(a, b, c) = 1$, and extract the coefficients of $f_1 = (a_1, b_1, c_1)$ and $f_2 = (a_2, b_2, c_2)$ from the entries of A^{-1}. Thus we have

$$F(x, y) = J_{f_1,f_2}(x, y).$$

Now we claim that we may take

$$G(x, y) = D_{f_1,f_2}(x, y) = (b_1^2 - a_1c_1)x^2 + (2b_1b_2 - a_1c_2 - c_1a_2)xy + (b_2^2 - a_2c_2)y^2. \tag{3.5}$$

The discriminant of $G(x, y)$ is given by

$$\begin{aligned} D_G &= (2b_1b_2 - a_1c_2 - c_1a_2)^2 - 4(b_1^2 - a_1c_1)(b_2^2 - a_2c_2) \\ &= (a_1\, c_2)^2 - 4(a_1\, b_2)(b_1\, c_2) = D_F \end{aligned}$$

by (3.2). Now $F(x,y)^2$ is primitive by the Gauss lemma. Thus by (3.4) it follows that G is primitive.

The resultant of f_1 and f_2 is given by

$$\text{result}(f_1,f_2) = (a_1\,c_2)^2 - 4(a_1\,b_2)(b_1\,c_2) = D_F.$$

Thus for a prime p, if $p|f_1(x,y)$ and $p|f_2(x,y)$ for $\gcd(x,y)=1$ then $p|D_F$. Combining this with (3.4) of Proposition 1 proves i) of Theorem 1. □

ii) For F as in ii) the identity (3.4) reduces to

$$F(-b_1x^2 - 2c_1xy - d_1y^2, a_1x^2 + 2b_1xy + c_1y^2) = F^2(x,y), \tag{3.6}$$

from which the result follows as before. □

4. Pairs of binary cubic forms

The proofs of Theorems 2 and 3 make use of the invariant theory of pairs of binary Gaussian cubic forms. We review this next. A good reference for the theory over $\mathbb{C}$ is [10, p.204–218].

A pair (f_1,f_2) of Gaussian binary cubic forms has the normalized discriminant form[1]

$$D_{f_1,f_2}(x,y) = [\delta_0,\delta_1,\delta_2,\delta_3,\delta_4],$$

an invariant binary quartic under (2.6). The normalization is determined by setting for $f_1 = (a_1,b_1,c_1,d_1)$ and $f_2=(a_2,b_2,c_2,d_2)$ the values

$$\begin{aligned}
\delta_0 =& D_{f_1} = -a_1^2d_1^2 + 6a_1b_1c_1d_1 + 3b_1^2c_1^2 - 4a_1c_1^3 - 4d_1b_1^3,\\
\delta_1 =& 2\,(3b_1b_2c_1^2 - 2a_2c_1^3 + 3b_1^2c_1c_2 - 6a_1c_1^2c_2 - 6b_1^2b_2d_1 + 3a_2b_1c_1d_1\\
&+ 3a_1b_2c_1d_1 + 3a_1b_1c_2d_1 - a_1a_2d_1^2 - 2b_1^3d_2 + 3a_1b_1c_1d_2 - a_1^2d_1d_2),\\
\delta_2 =& 3b_2^2c_1^2 + 12b_1b_2c_1c_2 - 12a_2c_1^2c_2 + 3b_1^2c_2^2 - 12a_1c_1c_2^2\\
&- 12b_1b_2^2d_1 + 6a_2b_2c_1d_1 + 6a_2b_1c_2d_1 + 6a_1b_2c_2d_1 - a_2^2d_1^2 - 12b_1^2b_2d_2\\
&+ 6a_2b_1c_1d_2 + 6a_1b_2c_1d_2 + 6a_1b_1c_2d_2 - 4a_1a_2d_1d_2 - a_1^2d_2^2,\\
\delta_3 =& 2\,(3b_2^2c_1c_2 + 3b_1b_2c_2^2 - 6a_2c_1c_2^2 - 2a_1c_2^3 - 2b_2^3d_1 + 3a_2b_2c_2d_1 - 6b_1b_2^2d_2\\
&+ 3a_2b_2c_1d_2 + 3a_2b_1c_2d_2 + 3a_1b_2c_2d_2 - a_2^2d_1d_2 - a_1a_2d_2^2),\\
\delta_4 =& D_{f_2}.
\end{aligned} \tag{4.1}$$

A full set of (scalar) invariants of the pair (f_1,f_2) is provided by $\delta_0,\delta_1,\delta_2,\delta_3,\delta_4$ together with P and Q, which are given by (recall the convention (3.3))

$$P = P_{f_1,f_2} = (a_1\,d_2) - 3(b_1\,c_2) \tag{4.2}$$

$$\begin{aligned}
Q = Q_{f_1,f_2} =& -(b_1\,c_2)^3 - (c_1\,a_2)^2(c_1\,d_2) - (a_1\,b_2)(b_1\,d_2)^2 + (b_1\,c_2)^2(a_1\,d_2)\\
&+ 3(a_1\,b_2)(b_1\,c_2)(c_1\,d_2) + (a_1\,d_2)(a_1\,b_2)(c_1\,d_2).
\end{aligned} \tag{4.3}$$

Note that $D_{f_1,f_2}(x,y)$ is even. It follows by direct calculation[2] that for A_D, B_D from (1.2) we have

$$A_D = P(P^3 - 24Q) \quad \text{and} \quad B_D = P^6 - 36P^3Q + 216Q^2. \tag{4.4}$$

[1] An analysis of the representations of a given binary quartic form as a discriminant form over $\mathbb{C}$ is given in [7]. Such a discriminant form may be interpreted as the Cayley hyperdeterminant of a linear combination of two symmetric $2\times2\times2$ tensors.

[2] Use a computer or, as is done in [10, p. 211], proceed by hand after reducing to canonical forms.

The normalized Jacobian of (f_1, f_2) is the even form given by

$$J_{f_1,f_2}(x,y) = [(a_1\,b_2), 2(a_1\,c_2), (a_1\,d_2) + 3(b_1\,c_2), 2(b_1\,d_2), (c_1\,d_2)]. \tag{4.5}$$

Write

$$F = J_{f_1,f_2} = [a, 2b, c, 2d, e]$$

and let

$$H_F(x,y) = [2ac - 3b^2, 12ad - 2bc, 12ae + 6bd - c^2, 12be - 2cd, 2ce - 3d^2] \tag{4.6}$$

be its normalized Hessian. By another direct calculation we have

$$A_F = P^2 \quad \text{and} \quad B_F = 54Q - P^3. \tag{4.7}$$

Define the covariant quartic

$$L(x,y) = L_{f_1,f_2}(x,y) = -2PF(x,y) - H_F(x,y) = (3a_1^2c_2^2 + \cdots)x^4 + \cdots . \tag{4.8}$$

Once more, a computation justifies the following higher composition law for binary quartic forms.

Proposition 2. *Notation as above, for any pair (f_1, f_2) of Gaussian binary cubic forms with discriminant form D_{f_1,f_2}, we have the syzygy*

$$D_{f_1,f_2}(-f_2(x,y), f_1(x,y)) = L(x,y)F^2(x,y),$$

where F is defined below (4.5) and L is defined in (4.8).

Proof of Theorem 2. For

$$F(x,y) = ax^4 + 2bx^3y + cx^2y^2 + 2dxy^3 + ey^4,$$

where $A_F = P^2$, we first show that there exist $f_1 = (a_1, b_1, c_1, d_1)$ and $f_2 = (a_2, b_2, c_2, d_2)$ such that

$$F(x,y) = J_{f_1,f_2}(x,y) \tag{4.9}$$

as normalized in (4.5). Since by (1.2) we have

$$P^2 = 12ae - 12bd + c^2, \tag{4.10}$$

we may choose the sign of P so that $P \equiv c \pmod 6$. Here we use that $P - c$ and $P + c$ have the same parity. In view of (4.5) we must show that (a_1, b_1, c_1, d_1) and (a_2, b_2, c_2, d_2) exist so that

$$a = (a_1\,b_2),\ \ b = (a_1\,c_2),\ \ \tfrac{1}{2}(c+P) = (a_1\,d_2),\ \ \tfrac{1}{6}(c-P) = (b_1\,c_2),\ \ d = (b_1\,d_2),\ \ e = (c_1\,d_2).$$

We have the necessary condition that $ae - bd + \frac{1}{12}(c^2 - P^2) = 0$ from (4.10). As before, the needed existence is due to Gauss, who proved a similar result in his treatment of the composition of two binary quadratic forms. The exact statement we need was given by Arndt [1]; an English version of his proof appears in [3, p. 65]. A different proof can be found in [11, p. 380].

Since F is primitive, by the Gauss lemma we deduce from Proposition 2 that

$$D^*_{f_1,f_2}(-f_2(x,y), f_1(x,y)) = L_1(x,y)F^2(x,y), \tag{4.11}$$

where L_1 is integral and $D^*_{f_1,f_2}(x,y)$ is the primitive form obtained of dividing $D_{f_1,f_2}(x,y)$ by the gcd of its coefficients. Let

$$G(x,y) = D^*_{f_1,f_2}(x,y).$$

By (1.3) and (4.7) we have

$$D_F = Q(P^3 - 27Q) \tag{4.12}$$

and from (4.4) and (1.3)

$$D_{D_{f_1,f_2}} = (4Q)^2 D_F, \tag{4.13}$$

so we see that G has a nonzero discriminant since F does and that $D_G = m^2 D_F$ for a positive $m \in \mathbb{Q}$.

Now the resultant of f_1 and f_2 is by [10, p. 205] or a direct calculation

$$\text{result}(f_1, f_2) = P^3 - 27Q. \tag{4.14}$$

Suppose that $F(x,y) = n$ for $\gcd(x,y) = 1$ and $\gcd(n, 3D_F) = 1$. If a prime p is such that $p|r$ where $r = \gcd(f_1(x,y), f_2(x,y))$, then by (4.14) and (4.12) we know that $p|D_f$. By (4.11) we must have that $r^4|L_1(x,y)$ since $\gcd(r,n) = 1$ and we get that

$$G(-\tfrac{1}{r}f_2(x,y), \tfrac{1}{r}f_1(x,y)) = \tfrac{1}{r^4}L_1(x,y)n^2,$$

where $\frac{1}{r^4}L_1(x,y) \in \mathbb{Z}$. This gives the desired representation by G of a nonzero multiple of n^2 unless $L_1(x,y) = 0$, hence $L(x,y) = 0$. In that case we need the following lemma.

Lemma 1. *Suppose that $F(x,y) = [a, 2b, c, 2d, e]$ is an even binary quartic form with Hessian $H_F(x,y)$ given by (4.6). If $p|\gcd(F(x,y), H_F(x,y))$ for integers x, y with $\gcd(x,y) = 1$ then $p|3D_F$.*

Proof. Since $\gcd(x,y) = 1$ and H_F is a covariant of F, by (4.6) we may assume that

$$p|\gcd(a, 2ac - 3b^2).$$

The discriminant of F from (1.3) is given in full by

$$\begin{aligned} D_F =& 16a^3e^3 - 48a^2bde^2 - 8a^2c^2e^2 + 36a^2cd^2e - 27a^2d^4 \\ &+ 36ab^2ce^2 - 6ab^2d^2e - 20abc^2de + 18abcd^3 + ac^4e - ac^3d^2 - 27b^4e^2 \\ &+ b^3cde - 16b^3d^3 - b^2c^3e + b^2c^2d^2. \end{aligned}$$

From this we see that $p|3D_F$. □

Assuming that $L(x,y) = 0$, by Lemma 1 we must have $n = \pm 1$ since

$$L(x,y) = -2PF(x,y) - H_F(x,y),$$

and then the conclusion of Theorem 2 is obvious. □

Before proving Theorem 3, it is instructive to see what can be done under the assumption that $-F$ is the (Gaussian normalized) Hessian of G in (1.4), so

$$F(x,y) = (b^2 - ac)x^4 + 2(bc - ad)x^3y + (3c^2 - ae - 2bd)x^2y^2 + 2(cd - be)xy^3 + (d^2 - ce)y^4,$$

but not necessarily that $A_F = 0$. Note that $A_F = (ae - 4bd + 3c^2)^2$. Letting

$$f_1(x,y) = (b_1, c_1, d_1, e_1) \quad \text{and} \quad f_2(x,y) = (a_1, b_1, c_1, d_1), \tag{4.15}$$

a computation using (4.5) shows that

$$F(x,y) = J_{f_1,f_2}(x,y).$$

Using (4.1) another computation yields the identity

$$D_{f_1,f_2}(y,x) = \tfrac{1}{12}A_G F(x,y) + \tfrac{1}{216}B_G G(x,y), \tag{4.16}$$

where you should note the (y,x) in the first term. Also we have for $L(x,y)$ from (4.8)

$$L(x,y) = \tfrac{1}{12}A_G F(x,y) - \tfrac{1}{72}B_G G(x,y). \tag{4.17}$$

Finally, we have the formulas

$$2^4\,3^2 A_F = A_G^2 \quad \text{and} \quad 2^{10}\,3^6 D_F = B_G^2 D_G. \tag{4.18}$$

Thus using (4.16) and (4.17), we can derive a more explicit version of the syzygy of Proposition 2 if we assume that $-F$ is a Hessian.

Proof of Theorem 3. Assume now that in addition to $-F$ being the Hessian of G we have $A_F = 0$. By (4.18) we know that $A_G = 0$ and using (1.3) therefore

$$D_G^2 = -2^8\,3^3 D_F.$$

Note that this identity implies that $3|D_F$. By Proposition 2 we get for f_1, f_2 from (4.15) the identity

$$G(-f_1(x,y), f_2(x,y)) = -3G(x,y)F^2(x,y),$$

for we know that $B_G \neq 0$.

Since we are assuming that F is primitive, from (1.4) we see that either G is primitive, which happens exactly when not both a_1 and e_1 are even, or the gcd of its coefficients is 2. This completes the proof. □

Remark. It is interesting to apply the identity of Proposition 2 to the pair of binary cubic forms (f_1, f_2), where the first form $f_1 = (a, b, c, d)$ has non-zero discriminant $D = D_{f_1}$ (as computed in (4.1)), but otherwise is arbitrary and the second f_2 is the cubic covariant of f_1. Explicitly,

$$f_2 = (-2b^3 + 3abc - a^2 d, -b^2 c + 2ac^2 - abd, bc^2 - 2b^2 d + acd, 2c^3 - 3bcd + ad^2).$$

The Hessian of f_1 is

$$H_{f_1} = [ac - b^2, ad - bc, bd - c^2].$$

The discriminant of H_{f_1} is $-D$. A calculation shows that

$$D_{f_1,f_2}(x,y) = DQ^2(x,y), \tag{4.19}$$

where $Q(x,y) = x^2 + Dy^2$. The Jacobian of (f_1, f_2) is

$$J_{f_1,f_2} = -2H_{f_1}^2.$$

Now Proposition 2 and (4.19) give, after computing the Hessian of $H_{f_1}^2$, the identity

$$Q(-f_2(x,y), f_1(x,y))^2 = 16 H_{f_1}(x,y)^6.$$

By combining this with a single evaluation, we see that the identity of Proposition 2 reduces to the classical identity of Eisenstein [4, §5, eq. 1] and Cayley [2]:

$$f_2^2 + D f_1^2 = -4H_{f_1}^3.$$

This identity was used by Mordell [8] [9] to characterize *all* of the proper representations of cubes by the principal form $x^2 + Dy^2$ when $4|D$.

Acknowledgement: I am grateful to the referee for providing some needed corrections.

References

1. Arndt, F. Mémoire sur la théorie des formes quadratiques, Archiv Math. Phys. 13 (1849) 410–418.
2. Cayley, A. Note sur les covariants d'une fonction quadratique, cubique, ou biquadratique à deux indéterminnées, J. Reine Angew. Math. 50 (1855), 285–287, in Collected Papers Vol. 2. #135.
3. Dickson, Leonard Eugene. History of the theory of numbers. Vol. III: Quadratic and higher forms. With a chapter on the class number by G. H. Cresse, Chelsea Publishing Co., New York 1966 v+313 pp. (1923)
4. Eisenstein, G. Untersuchen über die cubischen Formen mit zwei Variabeln, Crelle 27 (1844) 89-104, also in Werke I, #4.
5. Erdös, P.; Mahler, K. On the number of integers which can be represented by a binary form. J. London Math. Soc. 13 (1938), no. 2, 134–139.
6. Gauss, Carl Friedrich. Disquisitiones arithmeticae. Translated and with a preface by Arthur A. Clarke. Springer-Verlag, New York, 1986. xx+472 pp. (1801)
7. Hilbert, D. Über binäre Formen mit vorgeschreibener Diskriminante, Math. Annalen 31, 482–492 (1888), also #7 in Gesammelte Abhandlungen II.
8. Mordell, L. J. The Diophantine Equation $y^2 - k = x^3$. Proc. London Math. Soc. (2) 13 (1914), 60–80.
9. Mordell, L. J. Diophantine equations. Pure and Applied Mathematics, Vol. 30 Academic Press, London-New York 1969 xi+312 pp.
10. Salmon, G. Lessons introductory to the modern higher algebra, 5th ed. Chelsea. (1885)
11. Speiser, A. Über die Komposition der binären quadratischen Formen, in Festschrift Heinrich Weber, Teubner, Berlin. (1912), 375–395.

UCLA Mathematics Department, Box 951555, Los Angeles, CA 90095-1555
Email address: wdduke@ucla.edu