INTEGRAL AND RATIONAL REPRESENTATIONS OF FORMS

W. DUKE

Abstract. Criteria are given for the integral representation of a binary quartic form by certain integral ternary quadratic forms and its rational representation by some discriminant forms. These conditions depend on integral or rational solutions of a Weierstrass equation associated to the forms.

To Wolfgang Schmidt, on the occasion of his ninetieth birthday

1. Introduction

A form is a homogeneous polynomial. Let R be a ring containing $\mathbb{Z}$. Suppose that F and f are fixed forms in m and n variables, respectively, with coefficients in R. A basic and very general problem is to determine whether or not m forms $(\varphi_1, \dots, \varphi_m)$ exist, each in the variables of f and with coefficients in R, so that

$$F(\varphi) = F(\varphi_1, \dots, \varphi_m) = f \tag{1.1}$$

holds identically.

In this paper I will say that F *represents* f *over* R (or that (1.1) is *solvable over* R) if, in addition to (1.1), we assume that $m \geq n$, $\deg F | \deg f$ and each φ_j has degree $\frac{\deg f}{\deg F}$. If F and f represent each other over R then they are *equivalent* over R, in which case $m = n$, the degrees are equal and $\varphi \in \mathrm{GL}_m(R)$.

When $R = \mathbb{C}$ or $\mathbb{R}$, whether or not F represents f over R is a problem of classical algebraic geometry or invariant theory. Suppose, for example, that

$$F(\varphi) = \varphi_1^2 + \varphi_2^2 + \varphi_3^2.$$

It is familiar that F represents any nonsingular ternary quadratic form f with nonzero complex linear φ_j, which are real if f is real and positive definite. It is less well-known, but follows from old work of Hesse [9], that F represents any nonsingular ternary *quartic* form f over $\mathbb{C}$. Hilbert showed in [11] that this can be done over $\mathbb{R}$ if f is also real and positive definite (see also [12], [27] and [16]).

When $R = \mathbb{Q}$ or $\mathbb{Z}$, the question of the solvability of (1.1) is a problem of arithmetic geometry or number theory. It amounts to solving a special system of generally inhomogeneous polynomial equations in rational numbers or the integers. Unless we restrict F and f, it is usually intractable, the case $R = \mathbb{Z}$ being especially difficult. Over $\mathbb{Z}$, a motivating special case is to determine which integers are represented by F. Clearly, if F represents f over $\mathbb{Z}$ then F represents every integer represented by f. In particular, if F and f are equivalent over $\mathbb{Z}$, then they represent the same integers.

It is trivial that solvability of (1.1) over $\mathbb{Q}$ (over $\mathbb{Z}$) implies solvability over $\mathbb{Q}_p$ (over $\mathbb{Z}_p$) for all primes p (including $p = \infty$, where $\mathbb{Q}_\infty = \mathbb{Z}_\infty = \mathbb{R}$). In short, global solvability implies local solvability. When F and f are quadratic forms (so that the φ_j are linear), Hasse [8] showed that the converse holds over $\mathbb{Q}$: local solvability implies global solvability.

Provided that we make various additional assumptions, Siegel's main theorem on quadratic forms implies that the converse also holds over $\mathbb{Z}$, i.e. an integral local to global result holds when F and f are integral and quadratic.[1] For example, by [20],[21] (see also [22]) it is enough to assume that F and f come from symmetric integral matrices with nonzero determinants $\Delta = \Delta_F$ and $D = D_f$ and that the genus of F contains only one class.[2] Although the local conditions involve all primes p, here local solvability is always possible for all but possibly finitely many primes. Furthermore, the problem reduces to solving a finite system of congruences. Thus for quadratic forms where an integral local to global result holds, it is possible to determine solvability of (1.1) over $\mathbb{Z}$ in a finite number of steps, at least in principle.

In this paper I am interested in characterizing the integral representability of *binary quartic* forms by an integral ternary quadratic form and their rational representability by a discriminant form of degree two or four. In particular, this problem includes the representation over $\mathbb{Z}$ of a binary quartic form at the sum of three squares.[3] The goal is to give easily formulated and, if possible, finitely verifiable solvability conditions. In addition to Siegel's main theorem, I apply results of Mordell/Thue and Nagell. Otherwise the methods used are elementary. Usually I give explicit constructions of solutions when they exist. Some computations are lengthy and were discovered, and are best verified, with the assistance of software, in particular PARI/GP.

Remarks. When F is a sum of squares, $n = 2$ and R is any field of characteristic not two, solving (1.1) is a well-known problem in the algebraic theory of quadratic forms. See for instance [13] and [17].

A well studied analytic technique for treating Diophantine systems over $\mathbb{Q}$ or $\mathbb{Z}$ is to count asymptotically all solutions in a growing box, or show that none exist, via the Hardy-Littlewood method or one of its nonabelian variations. When applied to general systems over $\mathbb{Z}$, these methods are usually only effective when the number of variables is large compared to the number of equations and the associated system is homogeneous. The literature here is too large to effectively summarize, but two highly influential papers are those of Birch [1] and Schmidt [19].

2. Integral representations by a ternary quadratic form

Let F be a nonsingular integral ternary quadratic form. The problem of representing binary quadratic forms by F over $\mathbb{Z}$ was introduced by Gauss in his Disquisitiones [7, Art. 266–300].[4] In addition to anticipating aspects of integral local to global solvability by F, he made a number of arithmetic applications using the relationship between the discriminants of the binary quadratics represented by F and the integers represented by $-(\det F)F^{-1}$. Among these applications are his formula for the number of representations of an integer as the sum of three squares in terms of class numbers of binary quadratic forms.

In this section I will give a finite set of criteria for the representation of a binary quartic form f over $\mathbb{Z}$ by a nonsingular integral ternary quadratic form F, assuming that the genus of F contains only one class. Let

$$f(x,y) = (a,b,c,d,e) = ax^4 + 4bx^3y + 6cx^2y^2 + 4dxy^3 + ey^4 \quad \text{with } a,b,c,d,e \in \mathbb{Z}. \tag{2.1}$$

[1] Unless otherwise stated, an *integral* quadratic form will be supposed to come from an integral symmetric matrix. I will not distinguish a quadratic form from its associated symmetric matrix.

[2] Here the notions of genus and class are defined with respect to $\mathrm{GL}_m(\mathbb{Z}_p)$ for all p and $\mathrm{GL}_m(\mathbb{Z})$. To apply Siegel's result we must assume that $-\Delta$ and $-\Delta D$ are not squares in case m=2 or m=n+2, respectively. For a direct proof that the one class per genus condition suffices in case $n = 1$ see e.g. [2]. For results without the one class genus condition see [23].

[3] The problem of deciding which ternary quartic forms are the sum of three squares of integral quadratic forms seems to be open and difficult.

[4] A useful supplement for the study of this part of [7] is [26, Chap. 4].

The usual invariants of f in (2.1) are[5]

$$I = I_f = ae - 4bd + 3c^2 \quad \text{and} \quad J = J_f = \det \left[\begin{smallmatrix} a & b & c \\ b & c & d \\ c & d & e \end{smallmatrix}\right] = ace + 2bcd - ad^2 - eb^2 - c^3.$$

The discriminant of f is

$$D = D_f = I^3 - 27J^2. \tag{2.2}$$

Associated to F and f from (2.1) is the Weierstrass equation

$$\tfrac{\Delta}{2} Y^2 = X^3 - IX + 2J, \tag{2.3}$$

where $\Delta = \det F \neq 0$. Assuming that $D \neq 0$ for D from (2.2), this defines an elliptic curve E_Δ over the rationals, which is the Jacobian of the curve of genus one over $\mathbb{Q}$ determined by

$$Y^2 = 2\Delta f(X, 1)$$

(c.f. [28]). By a theorem of Mordell [14], itself reliant upon a well-known result of Thue [25], the equation (2.3) has at most finitely many solutions (X, Y) where X is integral.[6] Define for $\lambda \in \mathbb{Q}$

$$Q_\lambda = \begin{bmatrix} a & 2b & c+\lambda \\ 2b & 4c - 2\lambda & 2d \\ c+\lambda & 2d & e \end{bmatrix}. \tag{2.4}$$

Our first result reduces the binary quartic representation problem to a ternary quadratic one with an extra condition that involves equation (2.3). Since I need the rational case later, here I work over either $\mathbb{Z}$ or $\mathbb{Q}$.

Theorem 1. *Choose R to be either $\mathbb{Q}$ or $\mathbb{Z}$. Let F be an integral ternary quadratic form with $\Delta = \det F \neq 0$ and let f as in (2.1) be a Gaussian binary quartic form with invariants I, J and with $D \neq 0$. Then F represents f over R if and only if F represents the ternary quadratic form Q_X from (2.4) over R for some $X \in R$. In this case, we have that (X, Y) satisfies the equation (2.3) for some $Y \in R$.*

Proof. That F represents f over R means that there exists $\varphi = (\varphi_1, \varphi_2, \varphi_3)$ with binary quadratic forms having coefficients in R:

$$\varphi_j(x, y) = a_j x^2 + b_j xy + c_j y^2 \tag{2.5}$$

such that

$$f(x, y) = F\big(\varphi_1(x, y), \varphi_2(x, y), \varphi_3(x, y)\big). \tag{2.6}$$

Next note that for

$$V = (x^2, xy, y^2) \quad \text{and} \quad U = \left[\begin{smallmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{smallmatrix}\right] \in R^{3\times 3} \tag{2.7}$$

we have $UV^t = \varphi^t$ and (2.6) is equivalent to $\varphi F \varphi^t = f(x, y)$ and also

$$f(x, y) = V(U^t F U)V^t.$$

A calculation using (2.4) shows that *for any* λ

$$VQ_\lambda V^t = f(x, y). \tag{2.8}$$

Therefore (2.6) is equivalent to

$$V(U^t F U)V^t = VQ_\lambda V^t. \tag{2.9}$$

[5] See [18, §199] for the basic invariant theory of binary quartic forms. I am using I, J in place of his S, T.

[6] Although Thue's result is non-effective, the finiteness statement can be made effective, albeit with huge constants. See [24, Chap. IX] for a discussion and references.

Now

$$Q_\lambda = \begin{bmatrix} a & 2b & c \\ 2b & 4c & 2d \\ c & 2d & e \end{bmatrix} + \lambda J_0, \quad \text{where} \;\; J_0 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & -2 & 0 \\ 1 & 0 & 0 \end{bmatrix}.$$

It is easy to show that if A is a 3×3 symmetric complex matrix such that

$$VAV^t = 0$$

identically, then A is a multiple of J_0. It follows from this and a look at the $c + \lambda$ entries of Q_λ from (2.4) that, if (2.9) holds for some $\lambda = X \in R$, we must have

$$U^t F U = Q_X. \tag{2.10}$$

The "only if" part of the first statement of the Theorem now follows. The "if" part is a direct consequence of (2.9) and (2.8).

Now observe that if (2.10) holds then $\det Q_X = \Delta Y^2$ for some $Y \in R$. Explicitly,

$$Y = \det U. \tag{2.11}$$

Finally, from (2.4) a calculation shows that

$$\det Q_X = 2X^3 - 2IX + 4J$$

so we get the second statement. □

Say that φ with φ_j from (2.5) is *non-degenerate* if $\det U \neq 0$ for U from (2.7). The condition of $\varphi(x, y)$ being non-degenerate is invariant under $(x, y) \mapsto (x, y)A$ for $A \in \mathrm{GL}_2(\mathbb{Q})$.

Using Siegel's integral local to global result we can deduce from Theorem 1 the following finite set of criteria for the non-degenerate solvability over integers of f by a form F with one class in its genus.

Theorem 2. *Let F be a nonsingular integral ternary quadratic form that belongs to a genus that contains one class and let $f = (a, b, c, d, e)$ be a Gaussian binary quartic form with invariants I, J and with $D \neq 0$. Then F represents f over $\mathbb{Z}$ with a non-degenerate φ if and only if the following holds: for some solution (X, Y) to*

$$\tfrac{\Delta}{2} Y^2 = X^3 - IX + 2J,$$

with $X \in \mathbb{Z}$ and (X, Y) not of order two in the associated elliptic curve, we have that for any prime p (including $p = \infty$)

$$U^t F U = Q_X$$

has a solution $U \in \mathrm{Mat}_{3,3}(\mathbb{Z}_p)$, where Q_X is from (2.4).

Example 1. Suppose that $F(\varphi) = \varphi_1^2 + \varphi_2^2 + \varphi_3^2$, which is in a genus of one class. Let

$$f(x, y) = (2, -1, 3, -2, 3) = 2x^4 - 4x^3y + 18x^2y^2 - 8xy^3 + 3y^4,$$

for which $I = 25$ and $J = -8$. The elliptic curve with Weierstrass equation

$$\tfrac{1}{2}Y^2 = X^3 - 25X - 16$$

has no rational points of order two. The equation has four integral solutions (X, Y) with $Y > 0$: $(-1, 4), (-3, 8), (6, 10)$ and $(22, 142)$. We have

$$Q_{-1} = \begin{bmatrix} 2 & -2 & 2 \\ -2 & 14 & -4 \\ 2 & -4 & 3 \end{bmatrix}, \quad Q_{-3} = \begin{bmatrix} 2 & -2 & 0 \\ -2 & 18 & -4 \\ 0 & -4 & 3 \end{bmatrix}, \quad Q_6 = \begin{bmatrix} 2 & -2 & 9 \\ -2 & 0 & -4 \\ 9 & -4 & 3 \end{bmatrix}, \quad Q_{22} = \begin{bmatrix} 2 & -2 & 14 \\ -2 & -10 & -4 \\ 14 & -4 & 3 \end{bmatrix}.$$

It can be checked that

$$Q_{-1} = U^t U, \;\; U = \begin{bmatrix} 0 & -2 & 1 \\ 1 & -3 & 1 \\ 1 & 1 & 1 \end{bmatrix} \;\text{ gives }\; f(x, y) = (-2xy + y^2)^2 + (x^2 - 3xy + y^2)^2 + (x^2 + xy + y^2)^2$$

and

$$Q_{-3} = U^t U, \quad U = \begin{bmatrix} -1 & 1 & -1 \\ -1 & 1 & 1 \\ 0 & 4 & -1 \end{bmatrix} \;\text{ gives }\; f(x, y) = (-x^2 + xy - y^2)^2 + (-x^2 + xy + y^2)^2 + (4xy - y^2)^2.$$

On the other hand, $U^t U \equiv Q_6 \pmod 4$ and $U^t U \equiv Q_{22} \pmod 4$ have no solutions.

Remarks. The focus of this paper is the basic question of the solvability over $\mathbb{Z}$ or $\mathbb{Q}$ of (1.1) for certain F and binary quartic f and, when possible, to explicitly find some solutions. For the more refined problems of finding all solutions, or counting them with weights, it is natural to consider equivalence classes of solutions, with equivalence appropriately defined. Two solutions of the general equation (1.1) can be said to be equivalent if they can be transformed into each other in the obvious way by either an automorph of F or of f, defined over R. In Example 1 above, the automorphs of F consist of all sign changes and permutations of $(\varphi_1, \varphi_2, \varphi_3)$ while the only nontrivial automorph of f is given by $(x, y) \leftrightarrow (-x, -y)$. It is clear that the two solutions given are inequivalent in this sense. It is likely that they represent all classes. To prove this we would need to show that no other inequivalent solutions to either quadratic system $Q_{-1} = U^tU$ or $Q_{-3} = U^tU$ exist as well as that no other integral points on the elliptic curve exist.

3. Rational representations by discriminant forms

In this section I will consider the representation of binary quartics by certain discriminant forms, and now only over $\mathbb{Q}$.

Representation by a symmetric 2×2 *determinant.* Four times

$$F(\varphi_1, \varphi_2, \varphi_3) = \varphi_2^2 - \varphi_1\varphi_3 = -\det \begin{bmatrix} \varphi_1 & \varphi_2 \\ \varphi_2 & \varphi_3 \end{bmatrix}, \tag{3.1}$$

is the usual discriminant of the binary quadratic form

$$\varphi_1 x^2 + 2\varphi_2 xy + \varphi_3 y^2.$$

The following genus zero result is easy to prove.

A nonsingular integral binary quadratic form $f(x, y) = ax^2 + 2bxy + cy^2$ *is represented by* F *from (3.1) over* $\mathbb{Q}$ *with linear forms* φ_j *if, and only if, the conic determined by*

$$f(X, Y) - Z^2 = 0$$

contains nontrivial rational points.

For a binary quartic form f, we have a genus one version of this result.

Theorem 3. *Let* f *be a Gaussian binary quartic form with invariants* I, J *and with* $D \neq 0$ *and* E *be the elliptic curve over* $\mathbb{Q}$ *defined by*

$$Y^2 = X^3 - 4IX - 16J. \tag{3.2}$$

If f *is represented by* F *from (3.1) over* $\mathbb{Q}$ *then* E *contains nontrivial rational points. If* E *contains nontrivial rational points not of order* 2 *then* f *is represented by* F *over* $\mathbb{Q}$ *by a triple* $\varphi = (\varphi_1, \varphi_2, \varphi_3)$ *of binary quadratic forms* $\varphi_j(x, y) = a_j x^2 + b_j xy + c_j y^2$ *with*

$$b_1 = 2a_2, \quad c_1 = a_3, \quad \text{and} \quad 2c_2 = b_3. \tag{3.3}$$

Proof. The first statement follows from the last statement of Theorem 1 applied to

$$F_1(\varphi) = 2(\varphi_2^2 - \varphi_1\varphi_3), \tag{3.4}$$

for which $\Delta_{F_1} = -2$, and with f replaced by $2f$. Note that $I_{2f} = 4I_f$ and $J_{2f} = 8J_f$.

For the second statement, let (X, Y) solve $Y^2 = X^3 - 4IX - 16J$ with $Y \neq 0$. This is possible by our assumption that E has a nontrivial point, not order 2. Define[7]

$$B = \frac{1}{Y} \begin{bmatrix} 8b^2-8ac-2aX & 8bc-8ad-4bX & 2c^2-2ae-2cX+\frac{1}{2}X^2 \\ 4bc-4ad-2bX & 10c^2-8bd-2ae-4cX-\frac{1}{2}X^2 & 4cd-4be-2dX \\ 2c^2-2ae-2cX+\frac{1}{2}X^2 & 8dc-8be-4dX & 8d^2-8ce-2eX \end{bmatrix}. \tag{3.5}$$

[7] One method to derive the matrix B will be indicated at the end of the paper.

Then for F from (3.1) and V from (2.7), a (software assisted) calculation verifies that

$$F(BV^t) = f(x,y),$$

where $BV^t = \varphi^t$. The last statement follows from this and (3.5). □

Example 2. Let

$$f(x,y) = (1,1,3,1,2) = x^4 + 4x^3y + 18x^2y^2 + 4xy^3 + 2y^4,$$

for which $I = 25$ and $J = -18$. By using the method of the previous section, we can see that f is represented over $\mathbb{Z}$ by F from (3.1). Here we use that the Weierstrass equation

$$Y^2 = X^3 - 100X + 288$$

has three integral solutions: $(8,0), (-8,\pm 24)$. The first corresponds to a point of order two. Using $(-8,24)$, it is easy to get the explicit integral solution:

$$f(x,y) = (x^2 + 2xy - 16y^2)^2 - (y^2)(-46x^2 - 68xy + 254y^2).$$

On the other hand, the matrix B from Theorem 3 with $(X,Y) = (-8,24)$ yields the non-integral representation over $\mathbb{Q}$

$$f(x,y) = (x^2 + \tfrac{71}{12}xy + \tfrac{5}{6}y^2)^2 - (2xy + \tfrac{47}{12}y^2)(\tfrac{47}{12}x^2 + \tfrac{5}{3}xy - \tfrac{1}{3}y^2),$$

but with the symmetry condition given in (3.3).

Representation by a symmetric hyperdeterminant. Consider now the quartic form

$$F(\varphi) = F(\varphi_1,\varphi_2,\varphi_3,\varphi_4) = \varphi_1^2\varphi_4^2 - 3\varphi_2^2\varphi_3^2 + 4\varphi_1\varphi_3^3 + 4\varphi_4\varphi_2^3 - 6\varphi_1\varphi_2\varphi_3\varphi_4, \tag{3.6}$$

which gives the discriminant of the binary cubic form

$$\varphi_1 x^3 + 3\varphi_2 x^2 y + 3\varphi_3 xy^2 + \varphi_4 y^3.$$

It is also the symmetric Cayley hyperdeterminant [3]. Eisenstein [5] introduced this discriminant in his study of integral binary cubic forms. It is invariant under the simultaneous transpositions $\varphi_1 \leftrightarrow \varphi_4$ and $\varphi_2 \leftrightarrow \varphi_3$. In addition to being homogeneous of degree four, it satisfies for $k \neq 0$

$$F(k^3\varphi_1, k^2\varphi_2, k\varphi_3, \varphi_4) = k^6 F(\varphi_1,\varphi_2,\varphi_3,\varphi_4). \tag{3.7}$$

In particular,

$$F(\varphi_1,\varphi_2,\varphi_3,\varphi_4) = F(-\varphi_1,\varphi_2,-\varphi_3,\varphi_4) = F(\varphi_1,-\varphi_2,\varphi_3,-\varphi_4).$$

Other special properties are the composition formula [6]

$$F(F_1, \tfrac{1}{3}F_2, \tfrac{1}{3}F_3, F_4) = 16F^3,$$

where $F_j = \frac{\partial F}{\partial \varphi_j}$ and the Hessian identity [4]

$$\det[F_{i,j}] = 432F^2.$$

Our next aim is to characterize those binary quartic forms that can be represented over $\mathbb{Q}$ by this discriminant form evaluated at linear forms

$$\varphi = (a_1x + a_2y, b_1x + b_2y, c_1x + c_2y, d_1x + d_2y).$$

Now the associated system of equations is quartic, not quadratic, but the solvability criterion now only depends on whether or not the elliptic curve over $\mathbb{Q}$ defined by (3.2) contains nontrivial rational points of order three.

Theorem 4. *Let $f = (a, b, c, d, e)$ be a (Gaussian) binary quartic form with invariants I, J such that $D \neq 0$. Then f is represented by F from (3.6) over*
$\mathbb{Q}$ by linear forms φ_j if, and only if, the elliptic curve E defined over $\mathbb{Q}$ by

$$Y^2 = X^3 - 4IX - 16J$$

contains rational points of order three.

Proof. The proof of Theorem 4 makes use of the basic invariant theory of pairs of binary Gaussian cubic forms, [18, p.204–218].

Our problem is to determine when $(a_1, b_1, c_1, d_1) \in \mathbb{Q}^4$ and $(a_2, b_2, c_2, d_2) \in \mathbb{Q}^4$ exist so that for F from (3.6) and f from (2.1) we have

$$F(a_1x + a_2y, b_1x + b_2y, c_1x + c_2y, d_1x + d_2y) = f(x, y). \tag{3.8}$$

For the pair of binary cubic forms

$$f_j = (a_j, b_j, c_j, d_j) = a_ju^3 + 3b_ju^2v + 3c_juv^2 + d_jv^3, \quad j = 1, 2, \tag{3.9}$$

(3.8) can also be written

$$\mathrm{disc}_{u,v}(xf_1 + yf_2) = f(x, y).$$

The coefficients a, b, c, d, e of f are invariants of the pair (f_1, f_2). There are two other such invariants that make the resulting set of seven complete and independent over $\mathbb{C}$. These are given by

$$P = P_{f_1,f_2} = a_1d_2 - a_2d_1 - 3(b_1c_2 - b_2c_1) \tag{3.10}$$

$$Q = Q_{f_1,f_2} = \det \begin{bmatrix} a_1c_1 - b_1^2 & a_1c_2 + c_1a_2 - 2b_1b_2 & a_2c_2 - b_2^2 \\ a_1d_1 - b_1c_1 & a_1d_2 + d_1a_2 - b_1c_2 - c_1b_2 & a_2d_2 - b_2c_2 \\ b_1d_1 - c_1^2 & b_1d_2 + d_1b_2 - 2c_1c_2 & b_2d_2 - c_2^2 \end{bmatrix}. \tag{3.11}$$

Now a computation (using software) shows that for the coefficients of f coming from the assumption (3.8),

$$\begin{aligned} 12I &= P(P^3 - 24Q) \\ 216J &= -P^6 + 36P^3Q - 216Q^2. \end{aligned} \tag{3.12}$$

In addition,

$$D = (P^3 - 27Q)Q^3.$$

The equations of (3.12) are equivalent to the conditions given by Nagell in [15, Thm.1][8] for E from (3.2) to have rational points of order three. In this case, the points are given by

$$(X, Y) = (\tfrac{1}{3}P^2, \pm 4Q).$$

This shows that if we have a representation of f by F over $\mathbb{Q}$ then E has points of order three.

For the converse, given that points (X, Y) of order three exist on E, we must produce φ that represents f. By Nagell's criteria we can assume that we have $P, Q \in \mathbb{Q}$ with $Q > 0$ that satisfy the equations of (3.12). Define the matrix

$$C = \begin{bmatrix} \frac{12acP+aP^3-12aQ-12b^2P}{12Q^3} & \frac{6adP-6bcP+bP^3-12bQ}{12Q^2} & \frac{2aeP+4bdP-6c^2P+cP^3-12cQ}{12Q} & \frac{6beP-6cdP+dP^3-12dQ}{12} \\ \frac{6adP-6bcP+bP^3-12bQ}{12Q^3} & \frac{2aeP+4bdP-6c^2P+cP^3-12cQ}{12Q^2} & \frac{6beP-6cdP+dP^3-12dQ}{12Q} & \frac{12ceP-12d^2P+eP^3-12eQ}{12} \end{bmatrix}. \tag{3.13}$$

Using (3.12), one can check by (software assisted) computation that for F from (3.6)

$$F\big((x, y)C\big) = f(x, y).$$

□

[8] If $P = 0$ then $I = 0$ and $J = -Q^2 \neq 0$. If $P \neq 0$, in his notation use $3c = P$ and $P^2d = 36Q$.

Example 3. Let

$$f(x,y)=5x^4-4x^3y-48x^2y^2+12xy^3+12y^4,$$

for which $I=264$ and $J=23$. The elliptic curve given by

$$Y^2=X^3-1056X-368$$

has rank zero with points of order three: (3.12) gives $P=12$ and $Q=61$. Computation of C yields the representation over $\mathbb{Q}$:

$$f(x,y)=F\big(-\tfrac{77}{226981}x-\tfrac{41}{226981}y,-\tfrac{41}{3721}x-\tfrac{940}{3721}y,-\tfrac{940}{61}x+\tfrac{321}{61}y,321x-264y\big).$$

Derivation of matrices C and B. Although the proof of Theorem 4 is complete as given, the origin of the matrix C in (3.13) likely seems mysterious. To clarify this, and since it has generalizations, I will sketch its derivation. Note that if the result of Theorem 4 holds then so does the second statement of Theorem 3. One way to derive the other mysterious matrix B given in (3.5) is to use C to give it in this special case and then verify that it works in general. I will show how at the end.

We need the basic invariant theory of binary quartic forms. Again, a good reference is [18]. The Hessian of a quartic $f=(a,b,c,d,e)$ is the covariant given by

$$H_f(x,y)=(ac-b^2)x^4+2(ad-bc)x^3y+(ae+2bd-3c^2)x^2y^2+2(be-cd)xy^3+(ce-d^2)y^4. \tag{3.14}$$

We must produce φ by which F represents f or, what is the same, a suitable pair of binary cubic forms (3.9) so that

$$f(x,y)=\mathrm{disc}_{u,v}(xf_1+yf_2)=F\big((x,y)C\big). \tag{3.15}$$

The idea, which over $\mathbb{C}$ was utilized by Hilbert in [10], is to find a binary quartic g with the property that

$$g_u=\tfrac{\partial g}{\partial u}=4f_1 \quad\text{and}\quad g_v=\tfrac{\partial g}{\partial v}=4f_2. \tag{3.16}$$

We have the following readily checked identity:

$$\mathrm{disc}_{u,v}\big(\tfrac{1}{4}(xg_u+yg_v)\big)=-J_gg+I_gH_g. \tag{3.17}$$

We will proceed under the assumption that $P\neq 0$ and $Q>0$ and make the ansatz

$$g=\alpha f+6H_f. \tag{3.18}$$

Then by (3.17) we are led to solve the equation

$$-J_{\alpha f+6H_f}(\alpha f+6H_f)+I_{\alpha f+6H_f}H_{\alpha f+6H_f}=\beta f \tag{3.19}$$

in α,β. For this we apply the well-known formulas (see e.g. [18, p. 201])

$$\begin{aligned}I_{\alpha f+6H_f}&=I\alpha^2+18J\alpha+3I^2\\ J_{\alpha f+6H_f}&=J\alpha^3+I^2\alpha^2+9IJ\alpha+(54J^2-I^3)+3I^2\\ H_{\alpha f+6H_f}&=(\alpha I+9J)f+(\alpha^2-3I)H_f.\end{aligned}$$

Upon using the Nagell criteria, a solution of (3.19) is shown to be

$$\alpha=\tfrac{P^3-12Q}{2P}\quad\text{and}\quad\beta=\tfrac{6^4Q^6}{P^4}.$$

Therefore, (3.17) and (3.18) yield

$$f=\tfrac{P^4}{6^4Q^6}\,\mathrm{disc}_{u,v}\big(\tfrac{1}{4}(xg_u+yg_v)\big)\quad\text{where}\quad g=\tfrac{P^3-12Q}{2P}f+6H_f.$$

Next, apply (3.14), homogeneity of F and (3.7) to get f_1,f_2 from (3.16). Finally, we get C from (3.15).

Turning to the matrix B in (3.5), one way to derive it from C is to compute the (binary cubic) Hessian of $xf_1 + yf_2$ using C. The discriminant of this Hessian equals that of $xf_1 + yf_2$, which is f.

References

1. Birch, B. J. Homogeneous forms of odd degree in a large number of variables. Mathematika 4 (1957), 102–105.
2. Cassels, J. W. S. Rational quadratic forms, Academic Press, Inc., London-New York, 1978, xvi+413 pp.
3. Cayley, A. On the Theory of Linear Transformations, Cambridge Math. J. 4 (1845), 193–209, # 13 in Collected Papers.
4. Cayley, A. Note sur les hyperdéterminants, J. Reine Angew. Math. 34 (1847), 148–152, # 54 in Collected Papers.
5. Eisenstein, G. Untersuchungen über die cubischen Formen mit zwei Variabeln, J. Reine Angew. Math. 27 (1844), 89–104, # 4 in Math. Werke.
6. Eisenstein, G. Über eine merkwürdige identische Gleichung, ibid, 105–106, #5 in Math. Werke.
7. Gauss, C.F. Disquisitiones arithmeticae. (1801) Translated by Arthur A. Clarke. Springer-Verlag, New York, (1986). xx+472 pp. Original in Bd. I of Werke.
8. Hasse, H. Symmetrische Matrizen im Körper der rationalen Zahlen J. Reine Angew. Math. 153 (1924), 12–43. #3 in Math. Abhandlungen.
9. Hesse, O. Über die Doppeltangenten der Curven vierter Ordnung. J. Reine Angew. Math. 49 (1858), 279–332. #25 in Gesammelte Werke
10. Hilbert, D. Über binäre Formen mit vorgeschriebener Discriminante Math. Ann. 31 (1888), no. 4, 482–492. #7 in Gesammelte Abhandlungen.
11. Hilbert, D. Über die Darstellung definiter Formen als Summe von Formenquadraten Math. Ann. 32 (1888), no. 3, 342–350. #10 in Gesammelte Abhandlungen.
12. Hilbert, D. Über ternäre definite Formen Acta Math. 17 (1893), no. 1, 169–197. #20 in Gesammelte Abhandlungen.
13. Lam, T. Y. Introduction to quadratic forms over fields. Grad. Stud. Math., 67 American Mathematical Society, Providence, RI, 2005. xxii+550 pp.
14. Mordell, L. On the integer solutions of the equations $ey^2 = ax^3 + bx^2 + cx + d$, Proc. London Math. Soc. 21 (1923), 415–419.
15. Nagell,T. Recherches sur l'arithmétique des cubiques planes du premier genre dans un domaine de rationalité quelconque, Nova Acta Soc. Sci. Ups. (4) 15 (1952), no. 6, 66 pp., #90 in Collected Papers.
16. Pfister, A.; Scheiderer, C. An elementary proof of Hilbert's theorem on ternary quartics. J. Algebra 371 (2012), 1–25.
17. Rajwade, A. R. Squares. Cambridge University Press, Cambridge, 1993. xii+286 pp.
18. Salmon, G. Lessons introductory to the modern higher algebra, 5th ed. Chelsea, N.Y.
19. Schmidt, W. M. The density of integer points on homogeneous varieties. Acta Math.154 (1985), no.3-4, 243–296.
20. Siegel, C.L. Über die analytische Theorie der quadratischen Formen. Ann. of Math. (2) 36 (1935), no. 3, 527–606, # 20 in Gesammelte Abhandlungen.
21. Siegel, C.L. Über die analytische Theorie der quadratischen Formen. II. Ann. of Math. (2) 37 (1936), no. 1, 230–263, # 22 in Gesammelte Abhhandlungen.
22. Siegel, C.L. Lectures on the analytical theory of quadratic forms. Notes by Morgan Ward of course at IAS (1934/35), Fourth revised edition (1995)
23. Siegel, C.L. On the theory of indefinite quadratic forms. Ann. of Math. (2) 45 (1944), 577–622, # 45 in Gesammelte Abhhandlungen.
24. Silverman, J. H. The arithmetic of elliptic curves Grad. Texts in Math., 106 Springer, Dordrecht, 2009, xx+513 pp.
25. Thue, A. Über Annäherungswerte algebraischer Zahlen. J. Reine Angew. Math. 135 (1909), 284–305.
26. Venkov, B. A. Elementary number theory. Translated from the Russian by H. Alderson Wolters-Noordhoff Pub., Groningen 1970 ix+249 pp.
27. Wall, C. T. C. Is every quartic a conic of conics? Math. Proc. Cambridge Philos. Soc. 109 (1991), no.3, 419–424.
28. Weil, A. Remarques sur un mémoire d'Hermite. Arch. Math. (Basel) 5 (1954), 197–202. in Oeuvres II, 111–116.

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