FINITENESS THEOREMS FOR BINARY FORMS WITH GIVEN DISCRIMINANT

By B. J. BIRCH *and* J. R. MERRIMAN

[Received 27 May 1971]

1. Classical invariant theory is concerned with the action of linear groups on spaces of algebraic forms and the algebraic invariants under such actions; in this paper we are concerned with one of the simplest of such spaces, the space of binary forms of given degree, and one of the simplest invariants, the discriminant of the form. We prove in particular that if D_0 is a given integer then there are only finitely many $\mathrm{GL}_2(\mathbf{Z})$-orbits of binary forms f of given degree n with discriminant $D(f) = D_0$.

Before we state our main theorems, we establish our notation and recall some standard definitions. First, suppose that $f(x,y) = \sum_{i=0}^{n} a_i x^{n-i} y^i$ is a binary form of degree n; if $f(x,y)$ factors as $\prod_{j=1}^{n} (\alpha_j x - \beta_j y)$, the *discriminant* of f is

$$D(f) = \prod_{i<j} (\alpha_i \beta_j - \alpha_j \beta_i)^2. \tag{1}$$

Then $D(f) \in \mathbf{Z}[a_0, a_1, \ldots, a_n]$, and $D(f)$ is homogeneous of degree $2(n-1)$ in the sense that $D(\lambda f) = \lambda^{2(n-1)} D(f)$.

If $P = (x,y) \mapsto (ax+by, cx+dy)$ is a linear transformation, $f_P(x,y)$ denotes the transformed form $f(ax+by, cx+dy)$; so

$$D(f_P) = (\det P)^{n(n-1)} D(f).$$

If G is a group of such transformations, and $P \in G$, we say f is G-equivalent to f_P and write $f \underset{G}{\sim} f_P$; the G-orbit of f is the set of g with $g \underset{G}{\sim} f$.

THEOREM 2. *Let K be a number field with ring of integers $\mathfrak{o}_K$. Suppose that we are given a natural number $n \geqslant 2$ and a non-zero $D_0 \in \mathfrak{o}_K$. Then there are only finitely many $\mathrm{GL}_2(\mathfrak{o})$-orbits of binary forms $f \in \mathfrak{o}_K[x,y]$ with $\deg(f) = n$ and $D(f) = D_0$.*

This theorem was proved by Hermite ([**3**]) when $K = \mathbf{Q}$ in the cases $n = 2$ and 3; for general n, Hermite proved a theorem with deceptively similar enunciation, but with a different, less natural, 'determinant' in place of our discriminant; his determinant is skilfully devised so that his theorem is provable by reduction theory. It turns out that Hermite's reduction theory is just what is needed to deduce Theorem 2 from Theorem 1 below—we come back to this in § 5. An easy corollary of

Proc. London Math. Soc. (3) 24 (1972) 385–394

Theorem 2 is that up to the obvious translations by rational integers, there are only finitely many algebraic integers with given discriminant—compare with Nagell's paper [**10**], where this is proved for integers of degree $\leqslant 4$.

Suppose now that S is a finite set of primes of the number field K; $\mathfrak{o}_S$ will always denote the ring of S-integers of K: α is an S-integer if $\alpha = \beta/\gamma$ with $\beta \in \mathfrak{o}_K$ and γ a product of powers of primes from S. The multiplicative group $\mathfrak{o}_S^*$ of units of $\mathfrak{o}_S$ consists accordingly of products of units of $\mathfrak{o}_K$ and of primes from S.

If $f, g \in K[x,y]$ we say that f, g are (K,S)-equivalent and write $f \underset{K,S}{\sim} g$ if there are $\lambda \in \mathfrak{o}_S^*$ and $P \in \mathrm{GL}_2(\mathfrak{o}_S)$ so that $\lambda f = g_P$.

THEOREM 1. *Given K, S as above and a natural number $n \geqslant 3$, there are only finitely many (K,S)-orbits of forms $f \in \mathfrak{o}_K[x,y]$ with* $\deg(f) = n$ *and* $D(f) \in \mathfrak{o}_S^*$.

Theorem 1 may be regarded as the zero-dimensional analogue of Šafarevič's conjecture ([**12**]) that there are only finitely many equivalence classes of curves over K with given genus $g \geqslant 2$ and conductor contained in S; it implies Šafarevič's conjecture for hyperelliptic curves, see [**9**]. We understand from Paršin (conversation and [**11**]) that Šafarevič too has proved his conjecture for hyperelliptic curves, and his proof may well contain something resembling Theorem 1—but of course we have not seen it.

We first prove Theorem 1 for 'split forms', in § 2. Then, in § 3, we deduce that given K, S, n there is a finite extension M of K and a set of primes T of M such that all forms $f \in \mathfrak{o}_K[x,y]$ of degree n with $D(f) \in \mathfrak{o}_S^*$ become split forms of M, so that there are only finitely many (M,T)-orbits of forms satisfying the hypotheses of Theorem 1. In § 4 we complete the proof of Theorem 1 by showing that each (M,T)-orbit is a union of at most finitely many (K,S)-orbits.

In § 5, we use Hermite's method to deduce Theorem 2 from Theorem 1 in the classical case $K = \mathbf{Q}$; and in § 6 we indicate the modifications we need to make to Hermite's theory when K is a number field. We might well have restricted ourselves to the case $K = \mathbf{Q}$, which contains most of the interest; but such laziness could be very annoying to someone who really needed the general result.

NOTATION. As usual, $\mathbf{Q}$, $\mathbf{Z}$, and $\mathbf{N}$ denote the rationals, the rational integers, and the natural numbers; $\mathbf{R}$ is the real and $\mathbf{C}$ the complex field. If f is a form, we always use the notations f_P for a transform of f and $D(f)$ for the discriminant of f defined above. Throughout the paper, K is a fixed algebraic number field with integers $\mathfrak{o}_K$, S is a finite set of primes of K, and $\mathfrak{o}_S$ is the ring of S-integers of K; (K,S)-equivalence has been defined above. Later, we construct a field $M \supseteq K$ with integers $\mathfrak{O}_M$; the set of primes of M above S is T, and $\mathfrak{O}_T$ is the ring of T-integers of M.

2. We say that $f(x,y)$ is a *split form* over $\mathfrak{o}_K$ if

$$f(x,y) = \prod_{j=1}^{n} (\alpha_j x - \beta_j y) \tag{2}$$

with $\alpha_j, \beta_j \in \mathfrak{o}_K$. In this section, we prove

PROPOSITION 1. *There are only finitely many (K,S)-orbits of split forms f over $\mathfrak{o}_K$ with* $\deg(f) \geqslant 3$ *and* $D(f) \in \mathfrak{o}_S^*$.

We need two lemmas.

LEMMA 1. *Every cubic split form $f(x,y)$ over $\mathfrak{o}_K$ with $D(f) \in \mathfrak{o}_S^*$ is (K,S)-equivalent to $xy(x+y)$.*

Proof. Take P so that the corresponding dual projective transformation takes the points $(1,0)$, $(0,1)$, $(1,1)$ of the projective line to $(\alpha_1, -\beta_1)$, $(\alpha_2, -\beta_2)$, $(\alpha_3, -\beta_3)$. Explicitly,

$$P\colon (x,y) \to (ax+by, cx+dy)$$

with $a = \lambda\alpha_1$, $b = -\lambda\beta_1$, $c = \mu\alpha_2$, $d = -\mu\beta_2$, and

$$\lambda = \alpha_2\beta_3 - \beta_2\alpha_3, \quad \mu = \alpha_3\beta_1 - \alpha_1\beta_3.$$

Write $g(x,y) = xy(x+y)$, then $g_P(x,y) = (\det P)f(x,y)$ and

$$(\det P)^2 = D(f) \in \mathfrak{o}_S^*,$$

so $f \underset{K,S}{\sim} g$.

LEMMA 2. *The projective line $x+y = z$ has only finitely many points (x,y,z) with coordinates $x,y,z \in \mathfrak{o}_S^*$.*

The most convenient reference for this lemma, essentially due to Mahler, is Lang ([**7**]). Lang deduces it from Siegel's theorem about the finiteness of the number of integral points on a curve; though this theorem is ineffective, it is possible to deduce an effective version of the lemma from Baker's theorem, cf. Coates ([**2**]).

Proof of Proposition 1. Let $f(x,y) = \prod (\alpha_j x - \beta_j y)$ be a split form over $\mathfrak{o}_K$ with $D(f) \in \mathfrak{o}_S^*$. After Lemma 1, we may suppose $n \geqslant 4$; say $f = gh$ with

$$g(x,y) = \prod_{1}^{3} (\alpha_j x - \beta_j y), \quad h(x,y) = \prod_{4}^{n} (\alpha_j x - \beta_j y).$$

Since all the $\alpha_j, \beta_j \in \mathfrak{o}_K$, $D(g) \in \mathfrak{o}_S^*$, so by Lemma 1 there is a transformation $P \in \mathrm{GL}_2(\mathfrak{o}_K)$ and $\lambda \in \mathfrak{o}_S^*$ so that $g_P(x,y) = \lambda xy(x+y)$. But now

$$f_p(x,y) = xy(x+y)\prod_4^n (\gamma_j x - \delta_j y),$$

with $\gamma_j, \delta_j \in \mathfrak{o}_K$, and

$$D(f_p) = \prod_{4 \leqslant i < j \leqslant n} (\gamma_i\delta_j - \gamma_j\delta_i)^2 \prod_4^n \gamma_j{}^2\delta_j{}^2(\gamma_j+\delta_j)^2 \in \mathfrak{o}_S^*.$$

It follows that $\gamma_j, \delta_j, \gamma_j+\delta_j \in \mathfrak{o}_S^*$ when $4 \leqslant j < n$, so by Lemma 1 there are only finitely many possibilities for γ_j/δ_j, and the proposition follows.

3. Lemma 3. *Suppose that* $f(x,y) \in \mathfrak{o}_K[x,y]$ *and* $D(f) \in \mathfrak{o}_S^*$. *Let* L *be the splitting field of* $f(x,1)$ *and let* $D_{L/K}$ *be the relative discriminant. Then* $D_{L/K} \in \mathfrak{o}_S^*$.

Proof. Let $\theta = \theta_1, \ldots, \theta_n$ be the roots of $f(x,1) = \sum_0^n a_i x^{n-i} = 0$; it will be enough to show that $D_{K(\theta)/K} \in \mathfrak{o}_S^*$, for L is the composite of the $K(\theta_i)$. Since $\sum a_i\theta^{n-i} = 0$, $a_0\theta$ is a root of $\sum (a_i a_0{}^{i-1})x^{n-i} = 0$; so $a_0\theta$ is an algebraic integer. But now

$$(a_0\theta^2 + a_1\theta)^{n-1} + \sum_{j=0}^{n-2} (a_0\theta + a_1)^{n-2-j} a_{n-j}(a_0\theta^2 + a_1\theta)^j = 0,$$

so $a_0\theta^2 + a_1\theta$ is an algebraic integer. We successively deduce that

$$\sum_{i=0}^{r} a_i\theta^{r+1-i} = \eta_r, \quad \text{say},$$

is integral for $r = 0, \ldots, n-2$. Hence $1, \eta_0, \eta_1, \ldots, \eta_{n-2}$ form the basis for a submodule of the integers of $K(\theta)$. The discriminant of this basis is precisely $D(f) \in \mathfrak{o}_S^*$; so the discriminant of $K(\theta)$ over K is in $\mathfrak{o}_S^*$.

Lemma 4. *For given* m, *there are only finitely many extensions* L *of* K *with* $[L:K] = m$ *and* $D_{L/K} \in \mathfrak{o}_S^*$.

Proof. If T is the set of rational primes that either divide $D_{K/\mathbf{Q}}$ or lie below primes of S, then $[L:\mathbf{Q}] \leqslant m[K:\mathbf{Q}]$ and $D_{L/\mathbf{Q}} \in \mathbf{Z}_T^*$; so it is enough to check the lemma for $K = \mathbf{Q}$. If $p \in T$ and e_p is the ramification index of p in L then the power $v_p(D_{L/\mathbf{Q}})$ of p in $D_{L/\mathbf{Q}}$ is bounded by $v_p(e_p) + ep - 1$ (q.v., [**13**]); e_p is bounded by $[L:\mathbf{Q}]$, so $D_{L/\mathbf{Q}}$ is bounded. As is well known ([**4**]), there are only finitely many number fields with given discriminant, so the lemma follows.

Proposition 2. *There is a field* M *with integers* $\mathfrak{D}_M$ *such that all forms* $f(x,y) \in \mathfrak{o}_K[x,y]$ *with* $\deg(f) = n$ *and* $D(f) \in \mathfrak{o}_S^*$ *become split forms over* $\mathfrak{D}_M$.

Proof. In the first place, by Lemmas 3 and 4 there are only finitely many possibilities for the splitting field of $f(x,1)$; take L to be the compositum of these possibilities; then $f(x,y)$ factors as

$$f(x,y) = a_0 \prod_1^n (x-\theta_j y)$$

with $\theta_1, \dots, \theta_n \in L$. Take M as the absolute class field of L and write $\mathfrak{O}_M$ for the ring of integers of M; then every ideal of L becomes principal in M, so we may write $\theta_j = \beta_j/\alpha_j$ where β_j, α_j are coprime integers in $\mathfrak{O}_M$. It follows by Gauss' lemma that

$$f(x,y) = \lambda \prod_1^n (\alpha_j x - \beta_j y)$$

with $\lambda \in \mathfrak{O}_M$; which is what we want.

4. In this section, we complete the proof of Theorem 1. From Propositions 1 and 2, we know that given K, S, n there is a finite extension M of K and a finite set T of primes of M such that there are only finitely many (M,T)-orbits of forms $f \in \mathfrak{o}_K[x,y]$ with $\deg(f) = n$ and $D(f) \in \mathfrak{o}_S^*$. We need to climb down, by showing that if Σ is one of these (M,T)-orbits then Σ is the union of finitely many (K,S)-orbits. Denote by $\mathfrak{O}_M$ the integers of M and by $\mathfrak{O}_T$ the T-integers of M.

Suppose that $f \in \Sigma$; as in Proposition 2, M is a splitting field for f, so every $\sigma \in \mathrm{Gal}(M/K)$ gives a permutation of the roots of f. Suppose that $g \in \Sigma$; then there exist $P \in \mathrm{GL}_2(\mathfrak{O}_M)$ and $\lambda \in \mathfrak{O}_T^*$ so that $f_P = \lambda g$. In particular, P induces a mapping $P^*\colon \theta \mapsto (d\theta - b)/(a - c\theta)$ of the roots of f onto the roots of g; we say that $f \approx g$ if we can find P so that $\sigma^{-1}P^*\sigma(\theta_i) = P^*(\theta_i)$ for all roots θ_i of $f(\theta, 1) = 0$, and for all $\sigma \in \mathrm{Gal}(M/K)$. Clearly $\approx$ is an equivalence relation, and since $\mathrm{Gal}(M/K)$ is finite, Σ is a finite union of $(\approx)$-orbits.

It remains to show that each $(\approx)$-orbit is a finite union of (K,S)-orbits; this will follow from Lemma 6.

Lemma 5. *Suppose that $f \approx g$; then we can number the roots $\theta_1, \dots, \theta_n$ of f and $\varphi_1, \dots, \varphi_n$ of g so that $\varphi_i = \sum_{j=0}^{n-1} b_j \theta_i^j$ $(i = 1, \dots, n)$ with $b_0, \dots, b_{n-1} \in K$.*

Proof. Suppose that f factors as $f_1 \dots f_r$ where $f_1, \dots, f_r$ are irreducible polynomials of $K[x]$, coprime since $D(f) \neq 0$. Suppose that f_1 has degree k, and let its roots be $\theta_1, \dots, \theta_k$. Since $g \approx f$, say $f_P = \lambda g$ with $\sigma^{-1}P^*\sigma\theta = P^*\theta$ for every root θ of f, it follows that g factors as $g_1 \dots g_r$ with the same splitting fields, and if $\varphi_1 = P^*\theta_1$ is the root of g_1 corresponding to the root θ_1 of f_1 then $\varphi_1 \in K(\theta_1)$. It follows that $\varphi_1 = h_1(\theta_1)$ with

$h_1(x) \in K[x]$, $\deg(h_1) < \deg(g_1) = k$, and by conjugacy

$$\varphi_i = h_1(\theta_i) \quad (i = 1, \ldots, k).$$

We choose $h_l(x)$ $(l = 2, \ldots, r)$ similarly, and finish off by using the Chinese remainder theorem to choose $h(x) = \sum_{j=0}^{n-1} b_j x^j \in K[x]$ so that $h(x) \equiv h_l(x)$ modulo $f_l(x)$ $(l = 1, \ldots, r)$.

Lemma 6. *Suppose that T consists precisely of the primes of M above S. Then each $(\approx)$-orbit Ω is a finite union of (K, S)-orbits.*

Proof. Suppose that $f, g \in \Omega$; then the roots of f, g match up as described in Lemma 5, and we may suppose that

$$d\theta_i - b = (a - c\theta_i)\left(\sum_{j=0}^{n-1} b_i \theta_i^j\right) \quad (i = 1, \ldots, n). \tag{3}$$

Regard (3) as n equations in the four unknowns a, b, c, d: by hypothesis, these equations are soluble with $a, b, c, d \in \mathfrak{O}_M$, $ad - bc \in \mathfrak{O}_T^*$. The automorphisms $\sigma \in \mathrm{Gal}(M/K)$ simply permute the equations; so there is a non-trivial solution of (3) with $a_1, b_1, c_1, d_1 \in \mathfrak{o}_K$. For $n \geqslant 3$, the transformation P^* mapping $\theta_1, \ldots, \theta_n$ to $\varphi_1, \ldots, \varphi_n$ is unique; so a_1, b_1, c_1, d_1 are proportional to a, b, c, d. Let $V = \{\mathfrak{a}_1, \ldots, \mathfrak{a}_h\}$ be a set of representatives for the ideal classes of $\mathfrak{o}_K$, including (1) as the representative of the principal class; then we may suppose $(a_1, b_1, c_1, d_1) = \mathfrak{a}_1 \in V$. Write P_1 for the map $(x, y) \mapsto (a_1 x + b_1 y, c_1 x + d_1 y)$, then since $a, b, c, d \in \mathfrak{O}_M$ and $ad - bc \in \mathfrak{O}_T^*$ it follows that $\mathfrak{a}^{-2} \det P_1 \in \mathfrak{o}_S^*$. If we make successive transformations $P_1, \ldots, P_k$ so that the product $\mathfrak{a}_1 \ldots \mathfrak{a}_k$ of the corresponding ideals is principal, then we may remove the common factor β from the elements of the matrix $Q = P_k \ldots P_1$ and so obtain a matrix $\beta^{-1} Q \in \mathrm{GL}_2(\mathfrak{o}_K)$ with $\det(\beta^{-1} Q) \in \mathfrak{o}_S^*$. It follows that the $(\approx)$-orbit Ω may be split as the union of at most h sub-orbits $\Omega_1, \ldots, \Omega_k$ so that, if f, g are in the same sub-orbit Ω_i, there is a matrix $Q \in \mathrm{GL}_2(\mathfrak{o}_K)$ with $\det Q \in \mathfrak{o}_S^*$ and an element $\lambda \in K$ so that $f_Q = \lambda g$. It follows that f, g are (K, S)-equivalent.

This completes the proof of Lemma 6 and hence of Theorem 1.

5. The classical reduction theory devised by Hermite ([**3**]) applies only to the action of $\mathrm{GL}_2(\mathbf{Z})$ on rational forms; it is not particularly difficult to produce the analogous theory for $\mathrm{GL}_2(\mathfrak{o}_K)$, but it is a bit complicated, so in this section we use the classical theory to prove Theorem 2 in the case $K = \mathbf{Q}$, and postpone the modifications necessary for general K to § 6.

If $f(x, y) \in \mathbf{Z}[x, y]$, we may factorize

$$f(x, y) = \prod_{j=1}^{n} (\gamma_j x - \delta_j y) \tag{4}$$

with $\gamma_j, \delta_j \in \mathbf{C}$, in several ways of course. With such a factorization, we associate the definite quadratic form

$$\varphi(X, Y) = \sum |\gamma_j X - \delta_j Y|^2 = AX^2 - 2BXY + CY^2,$$

say, where

$$A = \sum |\gamma_j|^2, \quad 2B = \sum (\bar{\gamma}_j \delta_j + \gamma_j \bar{\delta}_j), \quad C = \sum |\delta_j|^2,$$

with determinant

$$\Delta(\varphi) = 4(AC - B^2) = 2\sum_{i \neq j} |\delta_i \gamma_j - \delta_j \gamma_i|^2.$$

Define

$$\Delta(f) = \min \Delta(\varphi),$$

where the minimum is taken over all factorizations (4). It is easy enough to show that if $D(f) \neq 0$ this minimum is positive and attained. Denote the quadratic form associated with f with $\Delta(\varphi) = \Delta(f)$ by φ_f; say that f is reduced (with respect to $\mathrm{GL}_2(\mathbf{Z})$) if φ_f is reduced, that is,

$$|B| \leqslant A \leqslant C,$$

which implies

$$AC \leqslant \tfrac{1}{3}\Delta(f).$$

If P is a real transformation $P\colon (x, y) \to (ax + by, cx + dy)$, then the form φ_P is associated with the factorization

$$\prod (\gamma_j(ax + by) - \delta_j(cx + dy))$$

of f_P; it follows that if $\lambda \in R^*$ and $P \in \mathrm{GL}_2(R)$, then

$$\Delta(\lambda f_P) = \lambda^{4/n} (\det P)^2 \Delta(f).$$

Lemma 7. *If $f(x, y) = \sum_0^n a_j x^{n-j} y^j \in \mathbf{Z}[x, y]$ is square free then it is $\mathrm{SL}_2(\mathbf{Z})$-equivalent to a reduced form.*

If $f(x, y)$ is reduced, then $|a_r|$ is bounded in terms of $\Delta(f)$ for $r = 1, \ldots, n$.

The first part of the lemma is immediate. To check the second part of the lemma, at any rate for $n > 2$, we note that if f is reduced then

$$(\sum |\gamma_j|^2)^2 \leqslant \sum |\gamma_j|^2 \sum |\delta_j|^2 \ll \Delta(f).$$

On the other hand, a_r is a sum of $\binom{n}{r}$ terms of degree r in the δ's and $(n - r)$ in the γ's; so

$$|a_r|^2 \ll (\sum |\gamma_j|^2)^{n-r} (\sum |\delta_j|^2)^r;$$

and, finally, since $a_0, a_1 \in \mathbf{Z}$ and a_0, a_1 are not both zero,

$$\text{either} \quad |\prod \gamma_j| = |a_0| \geqslant 1 \quad \text{or} \quad |\prod \gamma_j| \, |\sum \delta_j / \gamma_j| = |a_1| \geqslant 1,$$

whence $(\sum |\gamma_j|^2)^{n-1} (\sum |\delta_j|^2) \gg 1$ and $\sum |\delta_j|^2 \ll \Delta^{(n-1)/(n-2)}(f)$.

COROLLARY (Hermite). *Given Δ_0, there are only finitely many* $\mathrm{SL}_2(\mathbf{Z})$-*orbits of binary forms of degree n with* $0 < \Delta(f) \leqslant \Delta_0$.

Proof of Theorem 2 for $K = \mathbf{Q}$. Let D_0 be an integer and S be the set of primes dividing D_0. By Theorem 1, there are only finitely many $(\mathbf{Q}, S)$-orbits of forms f of degree n with $D(f) = D_0$. Suppose now that f, g are in the same $(\mathbf{Q}, S)$-orbit with $D(f) = D(g) = D_0$; then $f_P = g$ for some $P \in \mathrm{GL}_2(\mathbf{R})$, and since $D(f) = D(g)$, $\det P = \pm 1$. Hence $\Delta(f) = \Delta(g)$; so by Lemma 7 there are only finitely many possibilities for g up to $\mathrm{SL}_2(\mathbf{Z})$-equivalence.

COROLLARY OF THEOREM 2. *Up to translations of the type $\alpha \to \alpha + m$ with $m \in \mathbf{Z}$, there are only finitely many algebraic integers $\alpha \in \overline{\mathbf{Q}}$ whose discriminant has a given value $D(\alpha) = D_0 \in \mathbf{Z}$.*

Proof of Corollary. The discriminant of α is the discriminant of the monic polynomial $f(x, 1)$ of which α is the root. If $D(\alpha)$ is bounded, then the degree of α is bounded (by the argument of Lemma 4, since the least discriminant of a number field of degree n tends to infinity with n). There are only finitely many $\mathrm{SL}_2(\mathbf{Z})$-orbits of forms of given degree and discriminant D_0. Let f be a fixed form in one of these orbits; the leading coefficient of $f(ax+by, cx+dy)$ is $f(a,c)$ and, if $\deg(f) \geqslant 3$, $f(a,c) = 1$ has only finitely many solutions in integers (see [**14**], [**2**]). So the number of monic forms in the orbit of f is finite up to the obvious translations $(x,y) \to (x+my, y)$. The corollary is still true for quadratic integers; for, indeed, if $\deg(\alpha) = 2$ and $D(\alpha) = D$ then $\alpha = m + \frac{1}{2}(D + \sqrt{[D]})$, with $m \in \mathbf{Z}$.

6. Finally, we need to describe a reduction theory for binary forms over $\mathfrak{o}_K$, when K is a finite number field. Though such a theory has been worked out (e.g. by Ramanathan), it does not seem to be available in the literature. Suppose that $[K : \mathbf{Q}] = m$, and that there are r independent embeddings of K into $\mathbf{R}$ and s pairs of complex embeddings of K into $\mathbf{C}$, so that $r + 2s = m$. Denote by $\alpha^{(1)}, \ldots, \alpha^{(r)}$ the images of an element $\alpha \in K$ under the r real embeddings $K \to \mathbf{R}$, and denote by $\alpha^{(r+1)}, \ldots, \alpha^{(r+s)}$ the images of α under s complex embeddings $K \to \mathbf{C}$, one embedding from each conjugate pair. Throughout this section, f is square free.

Let $f(x,y) \in \mathfrak{o}_K[x,y]$, and let $f^{(1)}, \ldots, f^{(r+s)}$ be the corresponding images of f in $\mathbf{R}[x,y]$ and $\mathbf{C}[x,y]$. Take factorizations

$$f^{(k)}(x,y) = \prod_j (\gamma_j^{(k)} x - \delta_j^{(k)} y),$$

where the $\gamma_j^{(k)}$ and $\delta_j^{(k)}$, when $1 \leqslant j \leqslant n$ and $1 \leqslant k \leqslant r+s$, are complex numbers, not necessarily conjugates. Define associated forms

$$\varphi^{(k)}(X, Y) = \sum_j |\gamma_j^{(k)}X - \delta_j^{(k)}Y|^2,$$

so that $\varphi^{(k)}$ is a real definite quadratic form for $k = 1, \ldots, r$ and a definite Hermitian form for $k = r+1, \ldots, r+s$; write

$$\varphi^{(k)}(X, Y) = A^{(k)}X\bar{X} - B^{(k)}X\bar{Y} - \bar{B}^{(k)}\bar{X}Y + C^{(k)}Y\bar{Y}$$

so that

$$A^{(k)} = \sum_j \gamma_j^{(k)}\bar{\gamma}_j^{(k)}, \quad B^{(k)} = \sum_j \gamma_j^{(k)}\bar{\delta}_j^{(k)}, \quad C^{(k)} = \sum_j \delta_j^{(k)}\bar{\delta}_j^{(k)};$$

$$\Delta(\varphi^{(k)}) = 4(A^{(k)}C^{(k)} - B^{(k)}\bar{B}^{(k)}) = 2\sum_{i \neq j} |\gamma_j^{(k)}\delta_i^{(k)} - \gamma_i^{(k)}\delta_j^{(k)}|^2.$$

Denote the space of $(r+s)$-tuples φ of forms

$$(\varphi^{(1)}, \ldots, \varphi^{(r)}, \varphi^{(r+1)}, \ldots, \varphi^{(r+s)})$$

with $\varphi^{(1)}, \ldots, \varphi^{(r)}$ real positive quadratic and $\varphi^{(r+1)}, \ldots, \varphi^{(r+s)}$ positive Hermitian forms by $\mathscr{H}$. A transformation P: $(x, y) \mapsto (ax+by, cx+dy)$ of $\mathrm{GL}_2(K)$ acts naturally on $\mathscr{H}$ by

$$P^+ \colon \varphi^{(k)}(x, y) \to \varphi^{(k)}(a^{(k)}x + b^{(k)}y, c^{(k)}x + d^{(k)}y).$$

Humbert ([**5**], [**6**]) shows that there is a finite set W of matrices of $\mathrm{GL}_2(K)$ and a constant Γ (depending only on K) so that every $(r+s)$-tuple $\psi = (\psi^{(1)}, \ldots, \psi^{(r+s)}) \in \mathscr{H}$ is equivalent by $W.\mathrm{GL}_2(\mathfrak{o}_K)$ to an $(r+s)$-tuple $(\varphi^{(1)}, \ldots, \varphi^{(r+s)})$ with

$$|B^{(k)}/A^{(k)}| < \Gamma \quad (k = 1, \ldots, r+s). \tag{5}$$

(This is essentially due to Blumenthal ([**1**]), who asserts that every ψ is equivalent by $\mathrm{GL}_2(\mathfrak{o}_K)$ to a φ satisfying (5). Unfortunately, as Maass pointed out in [**8**], this is true only when $\mathfrak{o}_K$ has class number 1; Blumenthal's argument was rescued by putting in the finite set W. We are grateful to Raghavan, Ramanathan, and Rangachari for giving us these references.) Call an element $\varphi \in \mathscr{H}$ *reduced* if it satisfies (5); so every element of $\mathscr{H}$ is equivalent by $W.\mathrm{SL}_2(\mathfrak{o}_K)$ to a reduced form, but this reduction is by no means unique.

Now let $f(x, y) \in \mathfrak{o}_K[x, y]$. For each k, take the factorization of $f^{(k)}(x, y)$ for which $|\Delta(\varphi^{(k)})|$ is minimal; we thus get a definite element φ_f of $\mathscr{H}$ associated with f. Define

$$\Delta(f) = \max_k |\Delta(\varphi_f^{(k)})|.$$

Say that f is *reduced* if φ_f satisfies (5).

Lemma 8. *Given a positive real number Δ_0, there are only finitely many $\mathrm{GL}_2(\mathfrak{o}_K)$-orbits of forms $f \in \mathfrak{o}_K[x, y]$ with $0 < \Delta(f) < \Delta_0$ and* $\deg(f) = n$.

Proof. Since W is finite and every f is $W.\mathrm{GL}_2(\mathfrak{o}_K)$ equivalent to a reduced form, it is enough to show that there are only finitely many reduced forms with $\Delta(f) < \Delta_0$. But, by (5), if f is reduced,

$$(\sum|\gamma_j^{(k)}|^2)^2 \leqslant \sum|\gamma_j^{(k)}|^2\sum|\delta_j^{(k)}|^2 \ll \Delta_0 \quad (k = 1,\dots,r+s);$$

now

$$|a_t^{(k)}| \leqslant \binom{n}{t}(\sum|\gamma_j^{(k)}|^2)^{\frac{1}{2}(n-t)}(\sum|\delta_j^{(k)}|^2)^{\frac{1}{2}t} \quad (t = 0,\dots,n);$$

hence

$$|a_t^{(k)}| \ll \Delta_0^{\frac{1}{4}n} \quad (2t \leqslant n),$$

so there are only finitely many possibilities for a_t for $2t \leqslant n$; since a_0, a_1 are not both zero, we obtain a lower bound for $\sum|\gamma_j^{(k)}|^2\sum|\delta_j^{(k)}|^2$, so an upper bound for $a_t^{(k)}$ valid for all t, k. So there are only finitely many reduced f with $\Delta(f) \leqslant \Delta_0$.

The general case of Theorem 2 follows from Theorem 1 and Lemma 8 as the particular case $K = \mathbf{Q}$ followed from Theorem 1 and Lemma 7.

REFERENCES

1. O. BLUMENTHAL, 'Über Modulfunktionen von mehreren Verändlichen', *Math. Ann.* 56 (1903) 509–48.
2. J. COATES, 'An effective $\mathfrak{p}$-adic analogue of a theorem of Thue', *Acta Arith.* 15 (1969) 279–305.
3. C. HERMITE, 'Sur l'introduction des variables continues dans la théorie des nombres', *J. reine angew. Math.* 41 (1851) 191–216.
4. —— 'Sur le nombre limité d'irrationalités auxquelles se réduisent les racines des équations à coefficients entiers complexes d'un degré et d'un discriminant donnés', ibid. 53 (1857) 182–92.
5. P. HUMBERT, 'Théorie de la réduction des formes quadratiques définies positives dans un corps algébrique *K* fini', *Comm. Math. Helv.* 12 (1940) 263–306.
6. —— 'Réduction des formes quadratiques dans un corps algébrique fini', ibid. 23 (1949) 50–63.
7. S. LANG, 'Integral points on curves', *Publ. Math. I.H.E.S.* 6 (1960) 27–43.
8. H. MAASS, 'Über Gruppen von hyperabelschen Transformationen', *S.-B. Heidelberger Akad. Wiss. Math.-Natur. Kl.* (1940) 2, 26 pp.
9. J. MERRIMAN, D.Phil. thesis, Oxford, 1970.
10. T. NAGELL, 'Sur les discriminants des nombres algébriques, etc.', *Ark. Mat.* 7 (1967) 265–82, 517–25.
11. A. N. PARŠIN, 'Quelques conjectures de finitude en géométrie diophantienne', *Actes du Congrès International des Mathematiciens* 1970, vol. 1, pp. 467–71 (Gauthier–Villars, Paris, 1971).
12. I. R. ŠAFAREVIČ, 'Algebraic number fields', *Proc. International Congress of Mathematicians, Stockholm,* 1962, pp. 163–76 (in Russian) (Almqvist & Wiksells, Uppsala, 1963).
13. J.-P. SERRE, *Corps locaux,* Actualités sci. et ind. 1296 (Hermann, Paris, 1962).
14. A. THUE, 'Über Annäherungswerte algebraischer Zahlen', *J. reine angew. Math.* 135 (1909) 284–305.

Brasenose College
Oxford

University of Michigan
Present address:
University of Nottingham