ACTA ARITHMETICA
XXVI (1974)

Forms representable by integral binary quadratic forms

by

PHILIP A. LEONARD and KENNETH S. WILLIAMS* (Ottawa)

In memory of the late Professor L. J. Mordell

1. Introduction. By a *form* we shall mean an integral binary quadratic form in the indeterminates X and Y. This paper concerns the representability of a given form by forms of discriminant D, where D is the discriminant of a quadratic field (in fact, of the field $Q(\sqrt{D})$, where Q denotes the field of rationals).

If $f(X, Y)$ is a given form, and $g(X, Y)$ is a form of discriminant D, we say that $f(X, Y)$ *is representable by* $g(X, Y)$ if there exist rational integers p, q, r, s with $ps-qr \neq 0$ such that

$$f(X, Y) = g(pX+qY, rX+sY). \tag{1.1}$$

If such integers exist, we call (p, q, r, s) a *representation* of f by g.

From (1.1), a necessary condition for the representability of f by some g of discriminant D is

$$\begin{aligned}\operatorname{discrim}(f(X, Y)) &= \operatorname{discrim}(g(pX+qY, rX+sY)) \\ &= (ps-qr)^2 \operatorname{discrim}(g(X, Y)) = Dk^2.\end{aligned}$$

From now on, we fix D and assume that $f(X, Y) = aX^2+bXY+cY^2$ is a given form of discriminant Dk^2, where k is a positive integer. (Note that a and c must be non-zero.)

For those discriminants D given by

$$-D = 3, 4, 7, 8, 11, 19, 43, 67, 163 \tag{1.2}$$

one of us [5], extending results of Mordell [2] (see also [3]) and Pall [4] (see also [6]), has determined necessary and sufficient conditions for a positive-definite form of discriminant Dk^2 to be representable by a positive-definite form of discriminant D, as well as the number of such representations. We extend these results to all field discriminants D, replacing the use of unique factorization in the ring of integers of $Q(\sqrt{D})$ by a rela-

* Research supported under National Research Council of Canada grant A–7233.

tionship between certain ideals of this ring and representations of $f(X, Y)$ by forms of discriminant D. The way in which these ideals arise is given in Lemma 2.2, and their use in counting representations is shown in Lemma 3.1. The main results of the paper are contained in § 4.

We conclude this introduction by giving some notation to be used throughout. Suppose I is an ideal of the ring of integers of $Q(\sqrt{D})$, with norm given by $N(I) = |a|$ (recall $f(X, Y) = aX^2+bXY+cY^2$ is given). An ideal basis $\{\alpha_1, \alpha_2\}$ of I is said to be *a-ordered* if

$$\alpha_1\alpha_2' - \alpha_1'\alpha_2 = a\sqrt{D},$$

where the dash (′) denotes quadratic conjugation. If $\{\alpha_1, \alpha_2\}$ is such a basis for I we write $I = [\alpha_1, \alpha_2]$. For any ideal basis $\{\alpha_1, \alpha_2\}$, either $I = [\alpha_1, \alpha_2]$ or $I = [\alpha_2, \alpha_1]$ (not both). Moreover, applying strictly unimodular transformations to a given a-ordered basis yields all a-ordered bases of I. If $I = [\alpha_1, \alpha_2]$, we associate with this basis the form

$$\frac{1}{a}\{(\alpha_1\alpha_1')X^2+(\alpha_1\alpha_2'+\alpha_1'\alpha_2)XY+(\alpha_2\alpha_2')Y^2\}, \tag{1.3}$$

which is integral because $II' = (a)$, where I' denotes the conjugate ideal of I, and which is of discriminant

$$\frac{(\alpha_1\alpha_2'+\alpha_1'\alpha_2)^2-4\alpha_1\alpha_1'\alpha_2\alpha_2'}{a^2} = D.$$

We say that the a-ordered basis $\{\alpha_1, \alpha_2\}$ of I *leads to* the form (1.3), and write

$$\{\alpha_1, \alpha_2\} \to \frac{1}{a}\{(\alpha_1\alpha_1')X^2+(\alpha_1\alpha_2'+\alpha_1'\alpha_2)XY+(\alpha_2\alpha_2')Y^2\}.$$

In general, given an ideal I of norm $|a|$ and a form $lX^2+mXY+nY^2$ of discriminant D, we say that I *leads to* $lX^2+mXY+nY^2$ (written $I \to lX^2+mXY+nY^2$) if I possesses an a-ordered basis $\{\alpha_1, \alpha_2\}$ such that $\{\alpha_1, \alpha_2\} \to lX^2+mXY+nY^2$. It is easy to show that bases of strictly equivalent ideals of norm $|a|$ lead to (properly) equivalent forms of discriminant D.

A representation (p, q, r, s) of $f(X, Y)$ by a form $g(X, Y)$ of discriminant D will be called *proper* if $ps-qr = k$, and *improper* if $ps-qr = -k$.

If (p, q, r, s) is a given proper representation of f by the form lX_2+ $+mXY+nY^2$, we define a class of proper representations corresponding to (p, q, r, s) by

$$\mathscr{R}(p, q, r, s) = \left\{(p', q', r', s') : \begin{pmatrix} p' & q' \\ r' & s' \end{pmatrix} = A\begin{pmatrix} p & q \\ r & s \end{pmatrix}, \right.$$
$$\left. \text{where } A \text{ is a proper automorph of } lX^2+mXY+nY^2 \right\}.$$

Finally, let $d = \mathrm{GCD}(a, b, c)$. It is also useful to define classes of representations of d by $lX^2+mXY+nY^2$. If (u, v) is such a representation, with

$$d = lu^2+muv+nv^2,$$

we define its *class* by

$$\mathscr{C}(u, v) = \Big\{(u', v'):\ lu'+\frac{m-\sqrt{D}}{2}v' = \theta\Big(lu+\frac{m-\sqrt{D}}{2}v\Big),$$
$$\text{where } \theta \text{ is a unit of the ring of integers of } Q(\sqrt{D})\Big\}.$$

2. Preliminary lemmas. Let $f(X, Y) = aX^2+bXY+cY^2$ be a form of discriminant Dk^2, $k>0$, $d = \mathrm{GCD}(a, b, c)$, and $h = \frac{1}{2}(b-k\sqrt{D})$, so that $hh' = ac$.

LEMMA 2.1. (i). *h/d and h'/d are integers of $Q(\sqrt{D})$.*

(ii). *If $K = (a, h)$, then $N(K) = N(K') = |a|d$.*

Proof. (i). h/d and h'/d lie in $Q(\sqrt{D})$ and satisfy the monic integral quadratic equation

$$t^2-\frac{b}{d}t+\frac{ac}{d^2} = 0.$$

(ii). Using (i), we have

$$KK' = (a^2, ah, ah', hh') = (ad)\Big(\frac{a}{d}, \frac{h}{d}, \frac{h'}{d}, \frac{c}{d}\Big) = (ad),$$

$$\text{as } \mathrm{GCD}\Big(\frac{a}{d}, \frac{b}{d}, \frac{c}{d}\Big) = 1$$

implies the existence of rational integers r, s, and t satisfying

$$1 = r\frac{a}{d}+s\Big(\frac{h}{d}+\frac{h'}{d}\Big)+t\frac{c}{d}.$$

LEMMA 2.2. *Suppose (p, q, r, s) is a proper representation of f by the form $lX^2+mXY+nY^2$ of discriminant D, that is,*

$$(2.1)\qquad aX^2+bXY+cY^2 = l(pX+qY)^2+m(pX+qY)(rX+sY)+n(rX+sY)^2$$

with $ps-qr = k$. Then

$$a_1 = lp+\frac{r}{2}(m+\sqrt{D}) \quad \text{and} \quad a_2 = nr+\frac{p}{2}(m-\sqrt{D})$$

are integers of $Q(\sqrt{D})$ such that

(i) *the ideal $I = (a_1, a_2)$ has $N(I) = |a|$, and $I = [a_1, a_2]$,*

(ii) *$a = pa_1+ra_2$, $h = qa_1+sa_2$ (so $I\,|\,(a, h)$),*

(iii) *$\{a_1, a_2\}\to lX^2+mXY+nY^2$.*

Proof. It is trivial to verify that α_1 and α_2 are indeed integers of $Q(\sqrt{D})$.

(i) As D is a field discriminant, an integral basis for $Q(\sqrt{d})$ is $\{1, \omega\}$, where $\omega = (\varepsilon+\sqrt{D})/2$, with

$$\varepsilon = \begin{cases} 0, & \text{if} \quad D \equiv 0 \pmod 4), \\ 1, & \text{if} \quad D \equiv 1 \pmod 4). \end{cases}$$

Moreover, $m = 2m_1+\varepsilon$ for some integer m_1. It is easily shown that for rational integers x_1, x_2, y_1, y_2,

$$(x_1+y_1\omega)\alpha_1+(x_2+y_2\omega)\alpha_2$$
$$= \big(x_1+(m_1+\varepsilon)y_1+ny_2\big)\alpha_1+(x_2-ly_1-m_1y_2)\alpha_2.$$

Furthermore, appealing to (2.1), we have

$$\alpha_1\alpha_2'-\alpha_1'\alpha_2 = 2\left(\frac{p}{2}\left(lp+\frac{rm}{2}\right)+\frac{r}{2}\left(nr+\frac{pm}{2}\right)\right)\sqrt{D}$$
$$= (lp^2+mpr+nr^2)\sqrt{D} = a\sqrt{D}.$$

Thus I has $\{\alpha_1, \alpha_2\}$ as a basis, $N(I) = |a|$, and $I = [\alpha_1, \alpha_2]$. (ii) and (iii) follow by direct computation.

LEMMA 2.3. *Let N denote the number of ideals I such that $I|(a, h)$ and $N(I) = |a|$, and for a given form $lX^2+mXY+nY^2$ of discriminant D, let $N_{(l,m,n)}$ denote the number of such $I\to(l, m, n)$. Then*

$$N = \sum N_{(l,m,n)},$$

where the sum is taken over a representative set of inequivalent forms lX^2+ $+mXY+nY^2$ of discriminant D.

Proof. Let $\{l_iX^2+m_iXY+n_iY^2\}_{i=1,\dots,e}$ be a representative set of inequivalent forms of discriminant D. Let

$$\mathscr{I} = \{I\colon N(I) = |a|, I|(a, h)\}$$

and for each i $(1\leqslant i\leqslant e)$ let

$$\mathscr{I}_i = \{I\colon N(I) = |a|, I|(a, h), I\to l_iX^2+m_iXY+n_iY^2\}.$$

Let $I = [\alpha_1, \alpha_2]\in\mathscr{I}$ be such that $\{\alpha_1, \alpha_2\}\to lX^2+mXY+nY^2$. This form is equivalent to precisely one form

$$l_iX^2+m_iXY+n_iY^2,$$

say,

$$l_iX^2+m_iXY+n_iY^2$$
$$= l(tX+uY)^2+m(tX+uY)(vX+wY)+n(vX+wY)^2,$$

where t, u, v, w are rational integers with $tw-uv = 1$. Then $\{ta_1+ua_2, va_1+wa_2\}$ is an a-ordered basis of I leading to

$$l_iX^2+m_iXY+n_iY^2,$$

so that

$$I \to l_iX^2+m_iXY+n_iY^2,$$

that is, $I \in \mathscr{I}_i$, and so

$$\mathscr{I} = \bigcup_{i=1}^{e} \mathscr{I}_i.$$

Moreover no ideal $I \in \mathscr{I}$ can belong to two different $\mathscr{I}_i$ as inequivalent forms arise from ideals which are not strictly equivalent, hence certainly distinct. Thus the $\mathscr{I}_i$ are disjoint and we have

$$N = |\mathscr{I}| = \sum_{i=1}^{e} |\mathscr{I}_i| = \sum_{i=1}^{e} N(l_i, m_i, n_i).$$

LEMMA 2.4. *There is a one-to-one correspondence between ideals I such that $I|(a, h)$ and $N(I) = |a|$, and ideals J such that $N(J) = d$.*

Proof. By Lemma 2.1 any such I defines a unique J with $N(J) = d$ by the relation $(a, h) = IJ$. Conversely, if J is an ideal with $N(J) = d$, then $JJ' = (d)$, and thus $J|(a, h)$, since $(d)|(a, h)$ by Lemma 2.1. Setting $(a, h) = IJ$, we see that J defines a unique I with the desired properties.

LEMMA 2.5. *There is a one-to-one correspondence between classes of representations of d by a representative set of inequivalent forms of discriminant D and ideals J with $N(J) = d$.*

Proof. This result follows from Theorem 5, p. 143 in [1].

3. The main lemma. The result of this section makes more precise the connection (from Lemma 2.2) between ideals, and proper representations of $f(X, Y) = aX^2+bXY+cY^2$ (of discriminant Dk^2) by a given $lX^2+mXY+nY^2$ of discriminant D.

LEMMA 3.1. *There is a one-to-one correspondence between ideals I satisfying*

$$N(I) = |a|, \quad I|(a, h), \quad I \to lX^2+mXY+nY^2, \tag{3.1}$$

and classes of proper representations of $aX^2+bXY+cY^2$ by $lX^2+mXY+ nY^2$.

Proof. Let I be an ideal satisfying (3.1), and let $\{a_1, a_2\}$ be an a-ordered basis of I leading to $lX^2+mXY+nY^2$. Now $I|(a, h)$ means $(a, h) \subseteq [a_1, a_2]$, and so there exist unique rational integers p, q, r, s such that

$$a = pa_1+ra_2, \quad h = qa_1+sa_2. \tag{3.2}$$

We note that $ps-qr\neq 0$, for otherwise we have $rh=as$ contradicting that $k\neq 0$. Moreover as $\{\alpha_1,\alpha_2\}\to lX^2+mXY+nY^2$ we have

$$\alpha_1\alpha_1', = la, \qquad \alpha_1\alpha_2'+\alpha_1'\alpha_2 = ma, \qquad \alpha_2\alpha_2' = na,$$

and so

$$a = \frac{1}{a}(p\alpha_1+r\alpha_2)(p\alpha_1'+r\alpha_2') = lp^2+mpr+nr^2,$$

$$\begin{aligned} b &= h+h' = \frac{1}{a}\big((p\alpha_1+r\alpha_2)(q\alpha_1'+s\alpha_2')+(p\alpha_1'+r\alpha_2')(q\alpha_1+s\alpha_2)\big) \\ &= 2lpq+m(ps+qr)+2nrs, \end{aligned}$$

$$c = \frac{hh'}{a} = \frac{1}{a}(q\alpha_1+s\alpha_2)(q\alpha_1'+s\alpha_2') = lq^2+mqs+ns^2.$$

Therefore

$$aX^2+bXY+cY^2 = l(pX+qY)^2+m(pX+qY)(rX+sY)+n(rX+sY)^2.$$

Further, (3.2) implies

$$(ps-qr)\alpha_1 = sa-rh,$$

$$(ps-qr)\alpha_2 = -qa+ph,$$

and so

$$\begin{aligned} (ps-qr)^2a\sqrt{D} &= (ps-qr)^2(\alpha_1\alpha_2'-\alpha_1'\alpha_2) \\ &= (sa-rh)(-qa+ph')-(sa-rh')(-qa+ph) \\ &= a(ps-qr)(h'-h) = a(ps-qr)k\sqrt{D}, \end{aligned}$$

that is,

$$ps-qr = k.$$

Thus the a-ordered basis $\{\alpha_1,\alpha_2\}$ for I gives rise to a proper representation of f by $lX^2+mXY+nY^2$.

Suppose that $\{\beta_1,\beta_2\}\to lX^2+mXY+nY^2$. This is related to $\{\alpha_1,\alpha_2\}$ by $\beta_1 = t\alpha_1+v\alpha_2$, $\beta_2 = u\alpha_1+w\alpha_2$, where t, u, v and w are rational integers with $tw-uv=1$. As these two bases lead to the same form, we have

$$\begin{aligned} &\frac{1}{a}\{(\alpha_1\alpha_1')X^2+(\alpha_1\alpha_2'+\alpha_1'\alpha_2)XY+(\alpha_2\alpha_2')Y^2\} \\ &= \frac{1}{a}\{(\beta_1\beta_1')X^2+(\beta_1\beta_2'+\beta_1'\beta_2)XY+(\beta_2\beta_2')Y^2\} \\ &= \frac{1}{a}\{(\alpha_1\alpha_1')(tX+uY)^2+(\alpha_1\alpha_2'+\alpha_1'\alpha_2)(tX+uY)(vX+wY)+ \\ &\qquad\qquad +(\alpha_2\alpha_2')(vX+wY)^2\}, \end{aligned}$$

that is

$$\begin{pmatrix} t & u \\ v & w \end{pmatrix}$$

is a proper automorph of the form $lX^2+mXY+nY^2$.

Corresponding to (3.2) we have $a = p'\beta_1+r'\beta_2$, $h = q'\beta_1+s'\beta_2$, and (as indicated on previous page) this means that $\{\beta_1, \beta_2\}$ gives rise to the proper representation (p', q', r', s') of f by $lX^2+mXY+nY^2$. Moreover, we have

$$(a \;\; h) = (\alpha_1 \;\; \alpha_2)\begin{pmatrix} p & q \\ r & s \end{pmatrix} = (\beta_1 \;\; \beta_2)\begin{pmatrix} p' & q' \\ r' & s' \end{pmatrix} = (\alpha_1 \;\; \alpha_2)\begin{pmatrix} t & u \\ v & w \end{pmatrix}\begin{pmatrix} p' & q' \\ r' & s' \end{pmatrix}$$

and since $\{\alpha_1, \alpha_2\}$ is a basis

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} t & u \\ v & w \end{pmatrix}\begin{pmatrix} p' & q' \\ r' & s' \end{pmatrix}$$

that is $\mathscr{R}(p', q', r', s') = \mathscr{R}(p, q, r, s)$.

Thus, each ideal I satisfying (3.1) gives rise to proper representations (p, q, r, s) of f by $lX^2+mXY+nY^2$, defined by (3.2), where $\{\alpha_1, \alpha_2\}$ is any a-ordered basis of I which leads to $lX^2+mNY+nY^2$; moreover, two representations arising in this way lie in the same class. The mapping φ given by $\varphi(I) = \mathscr{R}(p, q, r, s)$ is thus a well-defined function from the set of ideals I satisfying (3.1) to the set of classes of proper representations of f by $lX^2+mXY+nY^2$.

The function φ is surjective, for if (p, q, r, s) is any proper representation of f by $lX^2+mXY+nY^2$, then, letting I be defined as in Lemma 2.2, we have $\varphi(I) = \mathscr{R}(p, q, r, s)$.

Finally, we show that φ is injective. Suppose $\varphi(I) = \varphi(J)$, where I and J are ideals satisfying (3.1). Let $I = [\alpha_1, \alpha_2]$ and $J = [\beta_1, \beta_2]$ give rise by (3.2) to the proper representations $(p, q, r, s), (p', q', r', s')$, respectively. As $\varphi(I) = \varphi(J)$,

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} t & u \\ v & w \end{pmatrix}\begin{pmatrix} p' & q' \\ r' & s' \end{pmatrix}$$

for some automorph

$$\begin{pmatrix} t & u \\ v & w \end{pmatrix}$$

of $lX^2+mXY+nY^2$. Therefore we have

$$(a \;\; h) = (\alpha_1 \;\; \alpha_2)\begin{pmatrix} p & q \\ r & s \end{pmatrix} = (\alpha_1 \;\; \alpha_2)\begin{pmatrix} t & u \\ v & w \end{pmatrix}\begin{pmatrix} p' & q' \\ r' & s' \end{pmatrix} = (\beta_1 \;\; \beta_2)\begin{pmatrix} p' & q' \\ r' & s' \end{pmatrix}$$

and so

$$(\beta_1 \ \ \beta_2) = (a_1 \ \ a_2)\begin{pmatrix} t & u \\ v & w \end{pmatrix}.$$

That is, the two bases are related by a strictly unimodular transformation, and therefore must be bases of the same ideal.

4. Number of representations. We are now in a position to prove the main results of this paper.

THEOREM 4.1. *The number of classes of proper representations of the form $aX^2+bXY+cY^2$ of discriminant Dk^2 by a representative set of inequivalent forms of discriminant D is equal to the number of classes of representations of $d = \mathrm{GCD}(a, b, c)$ by a representative set of inequivalent forms of discriminant D.*

Proof. By a fixed form $lX^2+mXY+nY^2$ of discriminant D, the number of classes of proper representations of $aX^2+bXY+cY^2$ is, by Lemma 3.1, equal to the number of ideals I satisfying (3.1). Letting lX^2+ $+mXY+nY^2$ run over a representative set of inequivalent forms and applying Lemma 2.3, we see that the number of classes of proper representations of $aX^2+bXY+cY^2$ by a representative set of inequivalent forms of discriminant D is equal to the number of ideals I such that $I|(a, h)$ and $N(I) = |a|$. By Lemmas 2.4 and 2.5, this is equal to the number of classes of representations of d by a representative set of inequivalent forms of discriminant D.

COROLLARY 4.1. *Let $f(X, Y) = aX^2+bXY+cY^2$ be a form of discriminant Dk^2, and let $d = \mathrm{GCD}(a, b, c)$. The form $f(X, Y)$ is properly representable by some form of discriminant D if and only if d is representable by a form of discriminant D.*

COROLLARY 4.2. (Cf. [5], Theorem 2.) *Let $f(X, Y) = aX^2+bXY+cY^2$ be a form of discriminant Dk^2, with $D < 0$. The number of proper representations of $f(X, Y)$ by a representative set of forms of discriminant D is equal to $r_D(d)$, the number of representations of $d = \mathrm{GCD}(a, b, c)$ by a representative set of inequivalent forms of discriminant D.*

Proof. The result follows immediately from Theorem 4.1, since each form of discriminant D has precisely w_D automorphs, where w_D denotes the number of units in the ring of integers of $Q(\sqrt{D})$. Thus each class of proper representations of f by a given form (and also each class of representations of d by a given form) has w_D members.

Remark. The preceeding results hold, with slight modifications in the proofs, for improper representations of $f(X, Y)$ by forms of discriminant D. Therefore, a doubling occurs when all (that is both proper and improper) representations of $f(X, Y)$ are counted.

Added in proof. The authors have subsequently obtained generalizations of these results; see Duke Mathematical Journal 40 (1973), pp. 533–539.

References

[1] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, London–New York 1966.

[2] L. J. Mordell, *On the representation of a binary quadratic form as a sum of squares of linear forms*, Math. Zeitschr. 35 (1932), pp. 1–15.

[3] I. Niven, *Integers of quadratic fields as sums of squares*, Trans. Amer. Math. Soc. 48 (1940), pp. 405–417.

[4] G. Pall, *Sums of two squares in a quadratic field*, Duke Math. J. 18 (1951), pp. 399–409.

[5] K. S. Williams, *Forms representable by an integral positive-definite binary quadratic form*, Math. Scand. 29 (1971), pp. 73–86.

[6] — *Note on a theorem of Pall*, Proc. Amer. Math. Soc. 28 (1971), pp. 315–316.

ARIZONA STATE UNIVERSITY
Tempe, Arizona, U.S.A.
CARLETON UNIVERSITY
Ottawa, Ontario, Canada

Received on 7. 11. 1972 (344)