Duke Math. J. 40 (1973), 533-539.

REPRESENTABILITY OF BINARY QUADRATIC FORMS OVER A BÈZOUT DOMAIN

PHILIP A. LEONARD AND KENNETH S. WILLIAMS

1. **Introduction.** By a form we shall mean a binary quadratic form in indeterminates X and Y with coefficients in a Bézout domain R, that is, an integral domain in which every finitely-generated ideal is principal. Such a form $lX^2 + mXY + nY^2$ will be called primitive if $(l, m, n) = R$. Δ will denote a nonsquare element of R which is the discriminant of some binary quadratic form in R. If the characteristic of R is 2, no such Δ exists; so we assume throughout that char $(R) \neq 2$.

If $f(X, Y) = aX^2 + bXY + cY^2$ is a given form and $g(X, Y)$ is a form of discriminant Δ, we say that $f(X, Y)$ is representable by $g(X, Y)$ if there exist elements $p, q, r, s \in R$ with $ps - qr \neq 0$ such that $f(X, Y) = g(pX + qY, rX + sY)$. If such elements p, q, r and s exist, we call (p, q, r, s) a representation of f by g. Clearly a necessary condition for the representability of f by g is

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

where k is a nonzero element of R. From now on we assume that $f(X, Y) = aX^2 + bXY + cY^2$ is a given form of discriminant Δk^2, where k is a fixed nonzero element of R, and that $g(X, Y) = lX^2 + mXY + nY^2$ denotes an arbitrary primitive form of discriminant Δ. A representation (p, q, r, s) of $f(X, Y)$ by the form $g(X, Y)$ will be called proper if $ps - qr = k$ and improper if $ps - qr = -k$.

In the classical case $R = Z$ (the domain of rational integers) for discriminants given by

$$-\Delta = 3, 4, 7, 8, 11, 19, 43, 67, 163$$

one of us [7], extending results of Mordell [4] (see also [5]) and Pall [6] (see also [8]), has determined necessary and sufficient conditions for a positive-definite form of discriminant Δk^2 to be representable by a positive-definite form of discriminant Δ, as well as the number of such representations. Later the authors of this paper extended these results to all field discriminants Δ, replacing the use of unique factorization in the ring of integers of $Q(\sqrt{\Delta})$ by a relationship between certain ideals of this ring and representations of $f(X, Y)$ by forms of discriminant Δ. In the present paper we replace the use of these ideals by

Received January 13, 1973. The second author's research was supported under National Research Council of Canada Grant A-7233.

using the concept of a pair introduced by Kaplansky [3]. We let d denote a fixed element of R such that $(a, b, c) = (d)$, and our main result (Theorem 4.2) shows that when $d \mid k$ there is a one-to-one correspondence between equivalence classes of proper representations of the form $aX^2 + bXY + cY^2$ of discriminant Δk^2 by a representative set of inequivalent primitive forms $g_i(X, Y)$, $i \in I$, of discriminant Δ and classes of associate solutions (as defined in Section 2) of $d = g_i(x, y)$, $i \in I$.

2. Notation and preliminary remarks. Throughout this paper K denotes the quotient field of R and $L = K(\sqrt{\Delta})$, where $\sqrt{\Delta}$ is arbitrarily fixed once and for all. For any element $z = x + y\sqrt{\Delta}$ of L we let $z' = x - y\sqrt{\Delta}$ denote its conjugate and $\mathrm{N}(z) = zz'$ its norm. Let A be a two-dimensional free R-submodule of L. We define the norm of A, written $\mathrm{N}(A)$, to be the fractional ideal of R generated by the elements $\mathrm{N}(z)$, where $z \in A$. For a basis $\{x, y\}$ of A we define the discriminant of A (relative to this basis) to be $\mathrm{D}(A) = (xy' - x'y)^2 \in K$. A change of basis will affect $\mathrm{D}(A)$ only by multiplying it by the square of a unit in R. A pair $[A, \alpha]$ consists of a two-dimensional free R-submodule A of L and a nonzero element α of K, with norm and discriminant defined by

$$\mathrm{N}[A, \alpha] = \mathrm{N}(A)/\alpha, \qquad \mathrm{D}[A, \alpha] = \mathrm{D}(A)/\alpha^2.$$

A pair $[A, \alpha]$ is called primitive if its norm is R. Two pairs $[A, \alpha]$ and $[B, \beta]$ are said to be equivalent if there exists a nonzero element $z \in L$ with $B = zA$, $\beta = \alpha\,\mathrm{N}(z)$. One easily checks that primitivity, norms and discriminants (the last up to the square of units in R) are well-defined on equivalence classes of pairs.

We shall be concerned with pairs $[A, \alpha]$ of discriminant Δ and binary quadratic forms of the same discriminant. An admissible basis for such a pair $[A, \alpha]$ is a basis $\{x, y\}$ of A such that $xy' - x'y = \alpha\sqrt{\Delta}$. (Such a basis always exists [3; §5].) Any two admissible bases are related by a strictly unimodular transformation. Relative to a given admissible basis $\{x, y\}$ the pair $[A, \alpha]$ gives rise to the binary quadratic form $(xX + yY)(x'X + y'Y)/\alpha \in K[X, Y]$ of discriminant Δ. If $lX^2 + mXY + nY^2$ is of discriminant Δ, we note that the pair $[\langle l, (m - \sqrt{\Delta})/2\rangle, l]$ gives rise to this form in the above manner. Kaplansky [3] has proved the following result [3; Theorem 1 and remarks at beginning of §6].

THEOREM 2.1. *The above procedure gives a one-to-one correspondence between all equivalence classes of primitive pairs with discriminant Δ and all proper equivalence classes of primitive binary quadratic forms with discriminant Δ.*

If $[A, \alpha]$ and $[B, \beta]$ are pairs, we define their product by $[A, \alpha]\,[B, \beta] = [AB, \alpha\beta]$, where AB is the product R-submodule of L (It is two-dimensional free as R is a Bézout domain.). Of fundamental importance is the fact that primitive pairs with discriminant Δ form a group under this operation. Moreover, the notion of product is also well-defined on equivalence classes of pairs, and this induces a group structure on the primitive classes of discriminant Δ.

It will be important to relate pairs with representations of f by primitive forms of discriminant Δ and also with representations of d by primitive forms of discriminant Δ. The first is done in Lemma 3.1 and the second is achieved by adapting portions of [1; Chapter 2] to our more general situation. It is convenient to introduce P, the unique order in L having discriminant Δ, and to call two solutions $(x_1, y_1), (x_2, y_2) \in R \times R$ of $d = lx^2 + mxt + ny^2$ associate if u is a unit in P where u is given by

$$lx_1 + \frac{m - \sqrt{\Delta}}{2}\, y_1 = u\left[lx_2 + \frac{m - \sqrt{\Delta}}{2}\, y_2\right].$$

With these definitions we have the following analog of [1; p. 143, Theorem 5].

THEOREM 2.2. *There is a one-to-one correspondence between classes of associate solutions of $d = g(x, y) = lx^2 + mxy + ny^2$ and pairs $[M, d] \in C^{-1}$ with $M \subseteq P$, where C denotes the class of pairs equivalent to the pair*

$$\left[\left\langle l, \frac{m - \sqrt{\Delta}}{2}\right\rangle, l\right].$$

3. The main lemma. In this section we consider proper representations of $f(X, Y) = aX^2 + bXY + cY^2$ by a fixed form $g(X, Y) = lX^2 + mXY + nY^2$ of discriminant Δ. Two such representations, (p, q, r, s) and $(p', q', r', s',)$, are said to be equivalent if there is a proper automorph $\mathfrak{A}$ of g such that

$$\begin{bmatrix} p' & q' \\ r' & s' \end{bmatrix} = \mathfrak{A} \begin{bmatrix} p & q \\ r & s \end{bmatrix}.$$

Equivalence classes of proper representations of f by g are related to pairs by the following result.

LEMMA 3.1. *There is a one-to-one correspondence between equivalence classes of proper representations of f by g and pairs $[A, a]$ of discriminant Δ satisfying*

(i) *$\langle a, h\rangle \subseteq A$ where $h = (b - k\sqrt{\Delta})/2$ and*

(ii) *$[A, a]$ gives rise (relative to some admissible basis) to the form $g(X, Y)$.*

Proof. (a) If (p, q, r, s) is a proper representation of f by g, let $A = \langle \alpha_1, \alpha_1\rangle$, where $\alpha_1 = lp + (r/2)(m + \sqrt{\Delta})$ and $\alpha_2 = nr + (p/2)(m - \sqrt{\Delta})$. Then $\alpha_1\alpha_2' - \alpha_1'\alpha_2 = a\sqrt{\Delta}$ so that the pair $[A, a]$ has discriminant Δ and $\{\alpha_1, \alpha_2\}$ as an admissible basis. It is easy to verify that, relative to $\{\alpha_1, \alpha_2\}$, the pair $[A, a]$ gives rise to $g(X, Y) = lX^2 + mXY + nY^2$. Since $a = p\alpha_1 + r\alpha_2$ and $h = q\alpha_1 + s\alpha_2$, the pair $[A, a]$ has all the indicated properties.

(b) On the other hand, suppose that $[A, a]$ is a pair of the kind described in the statement of the lemma, giving rise to $g(X, Y)$ relative to the admissible basis $\{\alpha_1, \alpha_2\}$. From (i) we have $a, h \in A$ and so, as $\{\alpha_1, \alpha_2\}$ is a basis for A, there exist unique elements p, q, r and s of R such that $a = p\alpha_1 + r\alpha_2$ and $h = q\alpha_1 + s\alpha_2$. We note that $ps - qr \neq 0$, since otherwise $rh = as$, which is impossible as $k \neq 0$. Using these representations for a and h, together with the equations $\alpha_1\alpha_1' = la$, $\alpha_1\alpha_2' + \alpha_1'\alpha_2 = ma$ and $\alpha_2\alpha_2' = na$, we obtain $a = (1/a)(p\alpha_1 + r\alpha_2)(p\alpha_1' + r\alpha_2') = lp^2 + mpr + nr^2$, $b = h + h' = (1/a)((p\alpha_1 + r\alpha_2)(q\alpha_1' + s\alpha_2') + (p\alpha_1' + r\alpha_2')(q\alpha_1 + s\alpha_2)) = 2lpq + m(ps + qr) + 2nrs$, and $c = hh'/a = (1/a)(q\alpha_1 + s\alpha_2)(q\alpha_1' + s\alpha_2') = lq^2 + mqs + ns^2$. Therefore $aX^2 + bXY + nY^2 = l(pX + qY)^2 + m(pX + qY)(rX + sY) + n(rX + sY)^2$. Furthermore, $(ps - qr)\alpha_1 = sa - rh$ and $(ps - qr)\alpha_2 = -qa + ph$, and so

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

that is, $ps - qr = k$. Thus the admissible basis $\{\alpha_1, \alpha_2\}$ for the pair $[A, a]$ leads to a proper representation (p, q, r, s) of f by g.

(c) The representation (p, q, r, s) determined in (b) clearly depends on the choice of basis $\{\alpha_1, \alpha_2\}$; on the other hand, its equivalence class does not. For let $\{\beta_1, \beta_2\}$ be a different admissible basis for $[A, a]$, relative to which this pair also gives rise to the form g, and let (p', q', r', s') be the proper representation of f by g derived from this basis as in (b). Then, on the one hand, $\beta_1 = t\alpha_1 + v\alpha_1$ and $\beta_2 = u\alpha_1 + w\alpha_2$ for t, u, v and w in R, with $tw - uv = 1$, so that

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

that is, $\begin{pmatrix} t & u \\ v & w \end{pmatrix}$ is a proper automorph of g. On the other hand,

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

and since $\{\alpha_1, \alpha_2\}$ is a basis, (p, q, r, s) and (p', q', r', s') are equivalent.

(d) Using (b) and (c) we define a function ϕ from pairs $[A, a]$ of the prescribed type to classes of proper representations of f by g, and we note that ϕ is surjective by (a). The function ϕ is also injective, for suppose $[A_1, a]$ and $[A_2, a]$ are pairs of the stated kind, giving rise via bases $\{\alpha_1, \alpha_2\}$ and $\{\beta_1, \beta_2\}$ respectively, to proper representations (p, q, r, s) and (p', q', r', s') in the same class, say

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

where $\begin{pmatrix} t & u \\ v & w \end{pmatrix}$ is a proper automorph of g. This means

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

Thus $(\beta_1 \quad \beta_2) = (\alpha_1 \quad \alpha_2) \begin{pmatrix} t & u \\ v & w \end{pmatrix}$ and the two bases, being related by a strictly unimodular transformation, must belong to the same module, and so $[A_1, a] = [A_2, a]$. This completes the proof.

4. Main result. In order to arrive at the principal result of this paper, we relate the one-to-one correspondences discussed in Sections 2 and 3 by means of the group structure enjoyed by the primitive pairs of discriminant Δ. This is done by means of the equation $[A, a][M, d] = [\langle a, h\rangle P, ad]$. Unfortunately, we require an extra hypothesis to ensure that the pair on the right-hand side of this equation is of the right kind.

LEMMA 4.1. *The pair* $[\langle a, h\rangle P, ad]$ *is primitive. Its discriminant is* Δ *if and only if* $d \mid k$.

Proof. We use [3; p. 527, Theorem 2], some of the computations contained in its proof, and the relationship between norms and discriminants expressed by [1; p. 125, Equation (6.3)] which also holds in the more general situation considered here. The module $\langle a, h\rangle P$ has norm (ad), and thus the pair $[\langle a, h\rangle P, ad]$ is indeed primitive.

Let Q be the order corresponding to the module $\langle a, h\rangle$ so that QP is the order corresponding to the module $\langle a, h\rangle P$. Let Δ_0 denote the discriminant of QP so that $D(\langle a, h\rangle P) = \Delta_0(ad)^2$, which equals (up to the square of a unit in R) $\Delta(ad)^2$ if and only if $\Delta_0 = \Delta$, that is, if and only if $QP = P$ [3; p. 527, Theorem 2(a)].

Thus the pair $[\langle a, h\rangle P, ad]$ has discriminant Δ if and only if $QP = P$, that is, if and only if $Q \subseteq P$ (as P is an order). By the computations in [3], $Q = \langle 1, h/d\rangle$ and $P = \langle 1, (m - \sqrt{\Delta})/2\rangle$. Clearly, then, $Q \subseteq P$ if and only if

$h/d = r + s(m - \sqrt{\Delta})/2$ for some $r, s \in R$. This is equivalent to the conditions $b/2d = r + sm/2$ and $k/2d = s/2$, and we conclude that $Q \subseteq P$ implies $d \mid k$.

On the other hand, suppose $d \mid k$ so that $k/d = s$ for s in R. Since $m^2s^2 - 4lns^2 = \Delta s^2 = (b/d)^2 - 4\cdot(a/d)(c/d)$, we have $(b/d)^2 \equiv m^2s^2 \pmod 4$ and therefore $b/d \equiv ms \pmod 2$ [2; p. 234, Lemma 2.12]. Thus there is an element r in R such that $b/2d = r + sm/2$, and since $k/2d = s/2$ we have $Q \subseteq P$ as required.

Let $\mathcal{C} = \{C_i \mid i \in I\}$ denote the collection of equivalence classes of primitive pairs of discriminant Δ. By a representative set of primitive forms of discriminant Δ we mean a collection of forms $g_i(X, Y)$, one for each i in I, such that the equivalence class of $g_i(X, Y)$ corresponds (in the sense of Section 2) to the pair-class C_i. It is convenient, under the assumption $d \mid k$, to let C_0 denote the class of the primitive pair $[\langle a, h\rangle P, ad]$ and use the group structure on $\mathcal{C}$ to define, for each i in I, a class $C_{\pi(i)}$ by the equation $C_0 C_{\pi(i)} = C_i$. Note that π is just a permutation of the index set I. The principal result of the paper can now be established.

THEOREM 4.2. *Let $\{g_i(X, Y) \mid i \in I\}$ be a representative set of primitive forms of discriminant Δ, and let $f = f(X, Y) = aX^2 + bXY + cY^2$ be given a form of discriminant Δk^2, with $d \mid k$. For each i in I there is a one-to-one correspondence between classes of proper representations of f by $g_i(X, Y)$ and classes of associate solutions of $d = g_{\pi(i)}(x, y)$.*

Proof. Let i in I be given. For each equivalence class of proper representations of f by g_i there is exactly one pair $[A, a]$, in the class C_i, with properties as given in Lemma 3.1. As the primitive pairs of discriminant Δ form a group, such a pair $[A, a]$ gives rise to a pair $[M, d]$, defined by

$$[A, a][M, d] = [\langle a, h\rangle P, ad], \tag{4.1}$$

belonging in the class $C_{\pi(i)}^{-1}$ and thus (by Theorem 2.2) to a class of associate solutions of $d = g_{\pi(i)}(x, y)$. This provides the indicated one-to-one correspondence as Theorem 2.2 and Lemma 3.1 concern one-to-one correspondences, and (4.1) shows that pairs $[A, a]$ and $[M, d]$ of the required types are also in one-to-one correspondence.

5. Final remarks. We remark that when Δ is such that P (the unique order with discriminant Δ) is maximal, then this ensures that $d \mid k$. This occurs in the classical case $R = Z$, $K = Q$ and $L = Q(\sqrt{\Delta})$ if discrim $L = \Delta$. Moreover, in this case every form of discriminant Δ is primitive and the number of classes of inequivalent forms of discriminant Δ is finite so that our main result Theorem 4.2 becomes in this case the following theorem.

THEOREM 5.1. *The number of classes of proper representations of the form $aX^2 + bXY + cY^2$ of discriminant Δk^2 by a representative set of inequivalent forms of discriminant Δ is equal to the number of classes of representations of d by a representative set of inequivalent forms of discriminant Δ.*

References

1. Z. I. Borevich and I. R. Shafarevich. *Number Theory*, New York, Academic Press, 1966.
2. Bill J. Dulin and H. S. Butts, *Composition of binary quadratic forms over integral domains*, Acta Arith., vol. 20(1972), pp. 223–251.
3. Irving Kaplansky, *Composition of binary quadratic forms*, Studia Math., vol. 31(1968), pp. 523–530.
4. L. J. Mordell, *On the representation of a binary quadratic form as a sum of squares of linear forms*, Math. Z., vol. 35(1932), pp. 1–15.
5. Ivan Niven, *Integers of quadratic fields as sums of squares*, Trans. Amer. Math. Soc., vol. 48(1940), pp. 405–417.
6. Gordon Pall, *Sums of two squares in a quadratic field*, Duke Math. J., vol. 18(1951), pp. 399–409.
7. Kenneth S. Williams, *Forms representable by an integral positive-definite binary quadratic form*, Math. Scand., vol. 29(1971), pp. 73–86.
8. ———, *Note on a theorem of Pall*, Proc. Amer. Math. Soc., vol. 28(1971), pp. 315–316.

Leonard: Department of Mathematics, Arizona State University, Tempe, Arizona 85281

Williams: Department of Mathematics, Carleton University, Ottawa, Ontario, Canada