PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 135, Number 12, December 2007, Pages 3765–3770
S 0002-9939(07)08895-8
Article electronically published on August 30, 2007

REPRESENTED VALUE SETS FOR INTEGRAL BINARY QUADRATIC FORMS AND LATTICES

A. G. EARNEST AND ROBERT W. FITZGERALD

(Communicated by Ken Ono)

ABSTRACT. A characterization is given for the integral binary quadratic forms for which the set of represented values is closed under products. It is also proved that for an integral binary quadratic lattice over a Dedekind domain, the product of three values represented by the form is again a value represented by the form. This generalizes the trigroup property observed by V. Arnold in the case of integral binary quadratic forms.

1. INTRODUCTION

For an integral binary quadratic form f, let $D(f)$ denote the set of integers represented by f (i.e., $a \in D(f)$ if and only if there exists $(x, y) \in \mathbb{Z}^2$ such that $f(x, y) = a$). V. Arnold [2] posed the problem of characterizing the forms f for which $D(f)$ is closed under products. Following [1], we will say that such a form f has the semigroup property. For example, if $f(x, y) = x^2 + dy^2$, then f has the semigroup property, as can be seen from the classical composition identity

$$(u^2 + dv^2)(z^2 + dw^2) = (uz + dvw)^2 + d(uw - vz)^2.$$

On the other hand, the form $f(x, y) = 3x^2 + 3y^2$ does not have the semigroup property, since f represents 3 but not 9.

While the set $D(f)$ is not always closed under products, Arnold observed that it is always true that products of three elements of $D(f)$ again lie in $D(f)$. This he termed the "trigroup property". One interesting consequence of the trigroup property is that mf has the semigroup property whenever the integer m lies in $D(f)$. It will be seen (Corollary 2.5) that the diagonal forms f with the semigroup property are those of the type mf_0 with $m \in D(f_0)$, where m is the greatest common divisor of the coefficients of f. In particular, the primitive diagonal forms with the semigroup property are precisely those that represent 1. This characterization no longer holds for non-diagonal forms, as can be seen by considering the primitive form $f(x, y) = 2x^2 + 3xy + 4y^2$, which has the semigroup property (see Corollary 2.6) but does not represent 1.

The present paper has two primary goals. The first is to give a complete solution to the problem posed by Arnold by giving a characterization of all integral binary quadratic forms having the semigroup property (see Theorem 2.3). The second is to use the multiplicative structure present on a binary quadratic space to show

Received by the editors June 14, 2006 and, in revised form, September 5, 2006.
2000 *Mathematics Subject Classification.* Primary 11E16; Secondary 11E12, 11E25, 11R29.

©2007 American Mathematical Society
Reverts to public domain 28 years from publication

that the trigroup property holds quite generally for binary quadratic lattices over a Dedekind domain (see Theorem 3.1).

2. Integral binary quadratic forms with the semigroup property

In this section, we consider integral binary quadratic forms; that is, forms of the type $f(x,y) = ax^2 + bxy + cy^2$ where $a, b, c \in \mathbb{Z}$. For convenience, we refer to such an f simply as a "form" and denote it by the shorthand notation (a,b,c). The discriminant of $f = (a,b,c)$ is $\Delta_f = b^2 - 4ac$. It will be assumed here that all forms under consideration are either positive definite (if $\Delta_f < 0$) or indefinite (if $\Delta_f > 0$). A form (a,b,c) is said to be primitive if g.c.d.$(a,b,c) = 1$. When f is not primitive, we will write $f = c_f f_0$, where $c_f = $ g.c.d.(a,b,c) and f_0 is primitive.

Two forms f and g are equivalent, denoted $f \sim g$, if there is an integral transformation of determinant $+1$ taking one form to the other. For a form f, $[f]$ will denote the set of all forms equivalent to f. Composition of forms induces a binary operation on the set of equivalence classes of primitive forms of a fixed discriminant. Adopting the approach of Dirichlet, we now briefly summarize the basic properties of this operation; details can be found, for example, in [3]. Let f and g be two primitive forms of the same discriminant. Then there exist $a, a', B, C \in \mathbb{Z}$ such that $f \sim (a, B, a'C)$ and $g \sim (a', B, aC)$. Moreover, for any prescribed integer n, a and a' can be chosen so that a, a' and n are pairwise relatively prime. For forms of this special type, there is a composition identity

$$(au^2 + Buv + a'Cv^2)(a'z^2 + Bzw + aCw^2) = aa'X^2 + BXY + CY^2, \tag{2.1}$$

where

$$X = uz - Cvw \qquad \text{and} \qquad Y = auw + a'vz + Bvw. \tag{2.2}$$

The set of equivalence classes of primitive forms of a fixed discriminant Δ has the structure of a finite abelian group, which will be denoted by $\mathfrak{F}_\Delta$, under the operation defined by $[f][g] = [(aa', B, C)]$. The identity element of $\mathfrak{F}_\Delta$ is the class id_Δ consisting of the forms that represent 1. If $f = (a,b,c)$, then $[f]^{-1} = [f^{op}]$, where $f^{op} = (a, -b, c)$.

As all equivalent forms represent the same integers, the notation $D([f])$ will be used to denote the set $D(g)$ for any $g \in [f]$. It follows from the composition identity (2.1) that if f and g represent the integers m and n, respectively, then the forms in the equivalence class $[f][g]$ represent the product mn; that is, $D(f)D(g) \subset D([f][g])$. Note also that $D(f^{op}) = D(f)$ since $f^{op}(x,y) = f(x,-y)$.

The above properties lead to an immediate proof of the trigroup property (as was observed in [1]).

Proposition 2.1. *Let f be an integral binary quadratic form. If $a, b, c \in D(f)$, then $abc \in D(f)$.*

Proof. Write $a = c_f a_0$, $b = c_f b_0$ and $c = c_f c_0$, where $a_0, b_0, c_0 \in D(f_0) = D(f_0^{op})$. Then

$$a_0 b_0 c_0 \in D(f_0)D(f_0)D(f_0^{op}) \subset D([f_0][f_0][f_0]^{-1}) = D([f_0]) = D(f_0).$$

Consequently, $c_f a_0 b_0 c_0 \in D(c_f f_0) = D(f)$. So there exists $(x,y) \in \mathbb{Z}^2$ such that $f(x,y) = c_f a_0 b_0 c_0$. Then $f(c_f x, c_f y) = abc$. □

Remark. The assumption of integrality is essential for the trigroup property to hold. For example, consider the form $f = \frac{1}{2}x^2 + 2y^2$. Then f represents $\frac{1}{2}$, $\frac{5}{2}$ and 4, but f does not represent 5.

In order to characterize forms with the semigroup property, we will need the following preliminary result.

Lemma 2.2. *Let g and h be primitive integral binary quadratic forms of the same discriminant Δ, and let p be an odd prime and n an integer. If $p \in D(g)$ and $np \in D(h)$, then either $n \in D([g][h])$ or $n \in D([g^{op}][h])$.*

Proof. Without loss of generality, it can be assumed that $g = (a, b, a'c)$ and $h = (a', b, ac)$, where a, a' and p are pairwise relatively prime. Let $u, v, z, w \in \mathbb{Z}$ be such that $g(u, v) = p$ and $h(z, w) = np$. Completing squares gives $4ap = (2au+bv)^2-\Delta v^2$ and $4a'np = (2a'z + bw)^2 - \Delta w^2$. From the first of these equations, note that p does not divide v; otherwise, we would also have $p \mid u$, leading to the contradiction $p^2 \mid p$. Suppose that p does not divide w. Then, solving for Δ in each of the previous equations leads to

$$\frac{(2au + bv)^2}{v^2} \equiv \frac{(2a'z + bw)^2}{w^2} \pmod{p}.$$

Hence, there exists $\epsilon = \pm 1$ such that

$$(2au + bv)w \equiv \epsilon(2a'z + bw)v \pmod{p}. \tag{2.3}$$

If $p \mid w$, then $p \mid z$ and (2.3) still holds.

First consider the case when $\epsilon = -1$. Then (2.3) implies

$$2auw + bvw \equiv -2a'vz - bvw \pmod{p}$$

and hence

$$auw + bvw + a'vz \equiv 0 \pmod{p}. \tag{2.4}$$

From the composition identity (2.1), we have

$$np^2 = aa'X^2 + bXY + cY^2, \tag{2.5}$$

where $p \mid Y$ by (2.2). It follows that $p \mid X$ and, upon cancelling p^2 from both sides of (2.5), that $n \in D([g][h])$.

Now consider the case when $\epsilon = +1$. Then (2.3) implies that $auw \equiv a'vz \pmod{p}$. Since g.c.d.$(a, a') = 1$, there exist $l, k \in \mathbb{Z}$ such that $al - a'k = b$. Set $B = 2al - b = 2a'k+b$ and $C = c+lk$. Let $g'(x, y) = g(x+ly, -y)$ and $h'(x, y) = h(x+ky, y)$. Then $g' \sim g^{op}$, $h' \sim h$, $g'(x, y) = ax^2 + Bxy + a'Cy^2$ and $h'(x, y) = a'x^2 + Bxy + aCy^2$. Now set $u' = u+lv$, $v' = -v$, $z' = z-kw$ and $w' = w$. Then $g'(u', v') = g(u, v) = p$ and $h'(z', w') = h(z, w) = np$. From (2.1) and (2.2), it follows that

$$np^2 = aa'X^2 + BXY + CY^2, \tag{2.6}$$

where

$$Y = au'w' + a'v'z' + Bv'w' = auw - a'vz + vw(a'k - al + b).$$

Here $a'k - al + b = 0$ by the choice of l, k, and $p \mid (auw - a'vz)$ from (2.3). Hence, $p \mid Y$. It follows that $p \mid X$ and, upon cancelling p^2 from both sides of (2.6), that $n \in D([g^{op}][h])$. This completes the proof of the lemma. □

Theorem 2.3. *Let f be an integral binary quadratic form. Then f has the semigroup property if and only if $c_f \in D(f_0) \cup D([f_0]^3)$.*

Proof. ($\Longleftarrow$) Let $A, B \in D(f)$. Then $A = c_f a$ and $B = c_f b$, where $a, b \in D(f_0)$. Then $ab \in D([f_0]^2) = D([f_0^{op}]^2)$. If $c_f \in D([f_0])$, then $c_f ab = c_f(ab) \in D([f_0][f_0^{op}]^2) = D([f_0][f_0]^{-2}) = D([f_0]^{-1}) = D(f_0^{op}) = D(f_0)$. On the other hand, if $c_f \in D([f_0]^3)$, then $c_f ab = c_f(ab) \in D([f_0]^3[f_0^{op}]^2) = D([f_0]^3[f_0]^{-2}) = D([f_0]) = D(f_0)$. So, in either case, $c_f ab \in D(f_0)$, and it follows that $AB = c_f(c_f ab) \in D(f)$, as required.

($\Longrightarrow$) By a classical theorem due to Weber [6], there exists an odd prime p such that $p \in D(f_0)$. Then $c_f p \in D(f)$, and so $c_f^2 p^2 \in D(f)$ by the semigroup property. Hence, $c_f p^2 \in D(f_0)$. It then follows from the lemma, with $g = h = f_0$ and $n = c_f p$, that either $c_f p \in D(id_\Delta)$ or $c_f p \in D([f_0]^2)$. In the first case, Lemma 2.2 (with $g = f_0$, $h = id_\Delta$ and $n = c_f$) implies that $c_f \in D(f_0)$. In the second case, Lemma 2.2 (with $g = f_0$, $[h] = [f_0]^2$ and $n = c_f$) implies that either $c_f \in D(f_0)$ or $c_f \in D([f_0]^3)$. □

Corollary 2.4. *Let f be a primitive integral binary quadratic form of discriminant Δ. The following are equivalent:*

(a) *f has the semigroup property.*
(b) *There is an odd prime p such that f represents both p and p^2.*
(c) *f or $[f]^3$ represents 1.*
(d) *$[f]$ has order 1 or 3 in $\mathfrak{F}_\Delta$.*

Remark. Forms which admit certain types of integer normed pairings are seen in [1] to give rise to elements of order 3 in the corresponding class group.

Corollary 2.5. *Let f be a diagonal integral binary quadratic form. Then f has the semigroup property if and only if f_0 represents c_f.*

Proof. Since f_0 is diagonal, $[f_0]^2$ is the identity and $[f_0]^3 = [f_0]$. □

Corollary 2.6. *For any $a, b \in \mathbb{Z}$, the form (a, b, a^2) has the semigroup property.*

Proof. Let $f = (a, b, a^2)$. Then $c_f = \text{g.c.d.}(a, b)$ and $f_0 = (a_0, b_0, c_f a_0^2)$, where $a = c_f a_0$ and $b = c_f b_0$. Since $\text{g.c.d.}(a_0, b_0) = 1$, identity (2.1) with $B = b_0$ and $C = c_f a_0$ gives $[f_0]^2 = [(a_0^2, b_0, c_f a_0)]$. Then applying (2.1) with $B = b_0$ and $C = c_f$ to the forms $(a_0, b_0, c_f a_0^2)$ and $(a_0^2, b_0, c_f a_0)$ gives $[f_0]^3 = [(a_0^3, b_0, c_f)]$. Hence, $c_f \in D([f_0]^3)$, and it follows from Theorem 2.3 that f has the semigroup property. □

3. The trigroup property for binary quadratic lattices

Throughout this section, $\mathfrak{o}$ will denote a Dedekind domain for which the quotient field F has characteristic different from 2. Let (V, Q) be a nondegenerate quadratic space over F of dimension 2, and let B be the symmetric bilinear form on V such that $B(v, v) = Q(v)$ for all $v \in V$. Let E be an extension of the field F such that $(\hat{V}, \hat{Q})$ represents 1 over E, where $(\hat{V}, \hat{Q})$ denotes the space obtained from (V, Q) via extension of scalars to E. Then $\hat{V}$ can be given the structure of a commutative E-algebra with involution $^-$ (for example, see [4]). Let $1_{\hat{V}}$ be the identity element of this algebra. The multiplication on $\hat{V}$ is related to the quadratic mapping $\hat{Q}$ by the identity

$$x\bar{x} = \hat{Q}(x)1_{\hat{V}}, \text{ for all } x \in \hat{V},$$

from which follow the identities

$$x\bar{y} + \bar{x}y = 2\hat{B}(x,y)1_{\hat{V}}$$

and

$$\hat{Q}(x)\hat{Q}(y) = \hat{Q}(xy)$$

for all $x, y \in \hat{V}$.

For the remaining discussion, the notation and terminology of O'Meara's book [5] will be adopted. Let L be an $\mathfrak{o}$-lattice on V, and let $\{v_1, v_2\}$ be a basis for V over F that is adapted to L. That is, $L = \mathfrak{a}_1 v_1 + \mathfrak{a}_2 v_2$ for some fractional ideals $\mathfrak{a}_1, \mathfrak{a}_2$ of F. Then, by 82:8 of [5], the scale and norm ideals of L are given by the equations

$$\mathfrak{s}L = \sum_{i,j} \mathfrak{a}_i \mathfrak{a}_j B(v_i, v_j), \quad \mathfrak{n}L = \sum_i \mathfrak{a}_i^2 Q(v_i) + 2\mathfrak{s}L.$$

Theorem 3.1. *Assume that* $\mathfrak{n}L \subseteq \mathfrak{o}$. *If* $a, b, c \in Q(L)$, *then* $abc \in Q(L)$.

Proof. Let $x, y, z \in L$. It suffices to show that $xy\bar{z} \in L$, since then $Q(xy\bar{z}) = \hat{Q}(xy\bar{z}) = \hat{Q}(x)\hat{Q}(y)\hat{Q}(z) = Q(x)Q(y)Q(z)$.

To establish this, write $x = x_1v_1 + x_2v_2$, $y = y_1v_1 + y_2v_2$ and $z = z_1v_1 + z_2v_2$ with $x_i, y_i, z_i \in \mathfrak{a}_i$ for $i = 1, 2$. Consider the expansion

$$xy\bar{z} = \sum_{i,j,k \in \{1,2\}} x_i y_j z_k v_i v_j \bar{v}_k. \tag{3.1}$$

Consider first the terms in (3.1) for which $i = k$. Such a term has the form

$$x_i y_j z_i v_i v_j \bar{v}_i = x_i y_j z_i Q(v_i) 1_{\hat{V}} v_j = (x_i z_i Q(v_i)) y_j v_j.$$

Now

$$x_i z_i Q(v_i) \in \mathfrak{a}_i^2 Q(v_i) \subseteq \mathfrak{n}L \subseteq \mathfrak{o}.$$

So

$$(x_i z_i Q(v_i)) y_j \in \mathfrak{a}_j$$

and

$$(x_i z_i Q(v_i)) y_j v_j \in \mathfrak{a}_j v_j \subseteq L$$

since $\mathfrak{a}_j$ is a fractional ideal of F.

The terms in the expansion (3.1) with $j = k$ are similarly in L. The only other terms in the expansion are those involving $v_i^2 \bar{v}_k$ with $i \neq k$. From the identity $v_i\bar{v}_k + \bar{v}_i v_k = 2B(v_i, v_k)1_{\hat{V}}$, it follows that

$$v_i^2 \bar{v}_k = v_i(v_i\bar{v}_k) = v_i(2B(v_i, v_k)1_{\hat{V}} - \bar{v}_i v_k) = 2B(v_i, v_k)v_i - Q(v_i)v_k.$$

The corresponding term in (3.1) can thus be expressed as

$$x_i y_i z_k v_i^2 \bar{v}_k = (2y_i z_k B(v_i, v_k)) x_i v_i - (x_i y_i Q(v_i)) z_k v_k.$$

Here $(x_i y_i Q(v_i)) z_k v_k \in L$ follows as in the previous paragraph. For the other term, note that

$$2y_i z_k B(v_i, v_k) \in 2\mathfrak{s}L \subseteq \mathfrak{n}L \subseteq \mathfrak{o},$$

from which it follows that

$$(2y_i z_k B(v_i, v_k)) x_i v_i \in \mathfrak{a}_i v_i \subseteq L.$$

It now follows that $xy\bar{z} \in L$, and the proof is complete. □

References

[1] F. Aicardi and V. Timorin, *On binary quadratic forms with semigroup property*, preprint.
[2] V. I. Arnold, *Arithmetics of binary quadratic forms, symmetry of their continued fractions and geometry of their de Sitter world*, Bull. Braz. Math. Soc. **34** (2003), 1-41. MR1991436 (2004h:11030)
[3] D. A. Cox, *Primes of the form x^2+ny^2. Fermat, class field theory and complex multiplication*, John Wiley & Sons, New York, 1989. MR1028322 (90m:11016)
[4] A. G. Earnest and D. R. Estes, *Class groups in the genus and spinor genus of binary quadratic lattices*, Proc. London Math. Soc. **40** (1980), 40-52. MR560994 (81i:10025)
[5] O. T. O'Meara, *Introduction to Quadratic Forms*, Springer-Verlag, Berlin, 1963.
[6] H. Weber, *Beweis des Satzes, dass jede eigentlich primitive quadratische Form unendlich viele Primzahlen darzustellen fähig ist*, Math. Ann. **20** (1882), 301-329. MR1510171

Department of Mathematics, Southern Illinois University, Carbondale, Illinois 62901
E-mail address: aearnest@math.siu.edu

Department of Mathematics, Southern Illinois University, Carbondale, Illinois 62901
E-mail address: rfitzg@math.siu.edu