EVEN QUADRATIC FORMS WITH CUBE-FREE DISCRIMINANT

DONALD G. JAMES

(Communicated by W. J. Wong)

ABSTRACT. A formula is given for the number of genera of even lattices with rank n , signature s , and discriminant $(-1)^{(n-s)/2}d^2D$, when dD is odd and square-free. In the indefinite case, an orthogonal splitting of these lattices into simple components is also determined.

1. INTRODUCTION

Let L be a $\mathbf{Z}$ -lattice on a regular quadratic space V of finite dimension $n \geq 4$ with associated symmetric bilinear form $f: V \times V \rightarrow \mathbf{Q}$. Assume, for convenience, that $f(L, L) = \mathbf{Z}$ and the signature $s = \text{sig } L$ is nonnegative. Let $x_1, \dots, x_n$ be a $\mathbf{Z}$ -basis for L and put $dL = \det f(x_i, x_j)$, the discriminant of the lattice. The lattice is called *even* if $f(x, x) \in 2\mathbf{Z}$ for all $x \in L$ (otherwise L is *odd*). In this note we will only consider nonunimodular even lattices L with odd cube-free discriminant; thus $dL = \Delta$ where $\Delta = (-1)^{(n-s)/2}d^2D$ with $dD > 1$ square-free and odd. By Chang [2; Satz 2], L exists if and only if n is even and $D \equiv (-1)^{s/2} \pmod{4}$ (note that Chang includes an extra factor $(-1)^{n(n-1)/2}$ in the discriminant); in particular, if L exists, s must be even, and also divisible by 4 when $D \equiv 1 \pmod{4}$.

Denote by $G(n, s, \Delta)$ the number of genera of even lattices with even rank n , (compatible) signature s , and discriminant Δ . For general discriminants, the local invariants can be very complicated, especially for $p = 2$, and a simple formula for the number of genera is unlikely. However, in our case (see Theorem 3),

$$G(n, s, \Delta) = \begin{cases} 2^{e-1}(2^e + (-1)^{s/4}) & \text{if } f = 0 \\ 2^{2e+f-1} & \text{if } f > 0, \end{cases}$$

where e and f are the number of primes dividing d and D , respectively.

When L is indefinite, under our assumptions, the class and genus coincide. Then L can be decomposed into an orthogonal sum of simpler components

Received by the editors July 19, 1988, and in revised form August 26, 1988.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11E12.

This research was partially supported by the National Science Foundation.

using hyperbolic planes, even definite unimodular lattices of rank 8, and a component of small rank (Theorem 4 and the following remarks).

2. LOCAL STRUCTURE AND GENERA

The local structure of quadratic forms and lattices is well understood (see [1] and [7]). In general, we follow the notation in O'Meara [7]. Since dD is odd and L is even, there will be no trouble with the prime 2. When $D \equiv (-1)^{s/2} \pmod{8}$, the localization L_2 must be an orthogonal sum of hyperbolic planes H ; thus the Hasse symbol $S_2 V = (-1)^{n(n+2)/8}$. When $D \equiv 5(-1)^{s/2} \pmod{8}$, L_2 also has one binary anisotropic plane B_2 , with local discriminant 3, and the Hasse symbol changes sign. Hence, in general, $S_2 V = (-1)^{b+n(n+2)/8}$ where $b = (D^2 - 1)/8$. Also, at the infinite prime, $S_\infty V = (-1)^{i(i+1)/2}$, where $i = (n - s)/2$ denotes the Witt index of V .

Now consider the local integral structure L_p at odd primes. If $(p, dD) = 1$, then L_p is unimodular with local discriminant $(-1)^{(n-s)/2} D$; hence $S_p V = 1$. If p divides D , then L_p is almost modular, that is, L_p is an orthogonal sum of a unimodular and a p -modular component. Thus

$$L_p = \langle 1, \dots, 1, \varepsilon, (-1)^{(n-s)/2} \varepsilon D \rangle$$

where ε is a local unit (the notation indicates the lengths of vectors in an integral orthogonal basis); here $S_p V = (\frac{-\varepsilon}{p})$ (Legendre) and hence the Hasse symbol determines the local invariant of L_p (essentially the square class of ε). If p divides d there are two possible Jordan types: either

$$L_p = \langle 1, \dots, 1, \varepsilon, p, p\eta \rangle$$

or

$$L_p = \langle 1, \dots, 1, \varepsilon, p^2 \eta \rangle$$

where ε and η are local units with $\varepsilon\eta = (-1)^{(n-s)/2} D$. In the first case, L_p is again almost modular; here $S_p V = (\frac{-\eta}{p})$ and hence the Hasse symbol $S_p V$ determines the local Jordan invariant of L_p , namely, the discriminant of the unimodular component of L_p . In the second case, where L_p has a p^2 -component, necessarily $S_p V = 1$.

Define $r = \#\{p : p|d \text{ and } S_p V = -1\}$ and $t = \#\{p : p|D \text{ and } S_p V = -1\}$. Put $c = b + s/4$ when $D \equiv 1 \pmod{4}$, and $c = b + \frac{1}{4}(2n + s - 2)$ when $D \equiv 3 \pmod{4}$. By Hilbert reciprocity,

$$\prod_{p|dD} S_p V = S_2 V S_\infty V = (-1)^c,$$

since $b + \frac{1}{8}n(n+2) + \frac{1}{2}i(i+1) \equiv c \pmod{2}$. Hence $r + t \equiv c \pmod{2}$. This gives another necessary condition for V to support an even lattice L with $dL = \Delta$.

The local invariants above determine the genus of L . Counting the possible values for the local invariants leads to the formula for $G(n, s, \Delta)$ given earlier.

However, we must first establish an existence result for the various possible integral lattices.

Theorem 1. *Let n be even and $0 \leq s \leq n$ with $D \equiv (-1)^{s/2} \pmod{4}$. Partition the primes dividing d into three disjoint sets P , Q , and R , and partition the primes dividing D into two disjoint sets S and T , with $r = |R|$, $t = |T|$, and $r + t \equiv c \pmod{2}$. For each $p \in P$ specify a local unit ε_p . Then there exists a space V and an even lattice M on V with $\dim V = n$, $\text{sig } M = s$, and $dM = \Delta = (-1)^{(n-s)/2} d^2 D$. Moreover,*

- (i) M_p has a p^2 -modular component and an orthogonal unimodular component of discriminant ε_p for all $p \in P$,
- (ii) M_p is almost modular and $S_p V = 1$ for all $p \in Q \cup S$,
- (iii) M_p is almost modular and $S_p V = -1$ for all $p \in R \cup T$.

Proof. For p in Q , R , S , or T choose local units ε_p such that $-\varepsilon_p$ is a local square if $p \in Q \cup S$, and a nonsquare if $p \in R \cup T$. Put $\eta_p = (-1)^{(n-s)/2} \varepsilon_p D$ for p dividing d , and $\eta_p = (-1)^{(n-s)/2} \varepsilon_p D/p$ for p dividing D . Define local lattices M_p of rank n as follows.

$$\begin{aligned}
 M_2 &= H \perp \cdots \perp H && \text{when } D \equiv (-1)^{s/2} \pmod{8}, \\
 &= H \perp \cdots \perp H \perp B_2 && \text{when } D \equiv 5(-1)^{s/2} \pmod{8}, \\
 M_p &= \langle 1, \dots, 1, (-1)^{(n-s)/2} D \rangle && \text{when } (p, 2dD) = 1, \\
 &= \langle 1, \dots, 1, \varepsilon_p, p^2 \eta_p \rangle && \text{for each } p \in P, \\
 &= \langle 1, \dots, 1, \eta_p, p, p \varepsilon_p \rangle && \text{for each } p \in Q \cup R, \\
 &= \langle 1, \dots, 1, \varepsilon_p, p \eta_p \rangle && \text{for each } p \in S \cup T.
 \end{aligned}$$

Define local spaces $V_p = M_p \otimes_{\mathbb{Q}_p}$ at each finite prime and let V_∞ have dimension n and signature s . Then $dV_p = (-1)^{(n-s)/2} D$ at all primes, $S_p V = -1$ for $p \in R \cup T$, and $\prod S_p V = 1$ since $r + t \equiv c \pmod{2}$. By [7; 72:1], there now exists a global $\mathbf{Q}$ -space V with localizations V_p at each prime. By [1; p. 129], there exists a lattice M on V with localizations M_p as specified above. Clearly $dM = (-1)^{(n-s)/2} d^2 D$ and M is even by our local choice for M_2 . This completes the proof.

In general, not all genera counted in $G(n, s, \Delta)$ will lie on the same quadratic space. Let $G_V(\Delta)$ denote the number of genera on the specific space V .

Theorem 2. *Let V be a quadratic space with even dimension n , signature s and discriminant $dV = (-1)^{(n-s)/2} D$ where $D \equiv (-1)^{s/2} \pmod{4}$. Assume $S_p V = 1$ for all primes p with $(p, 2dD) = 1$. Then*

$$G_V(\Delta) = \begin{cases} 3^{e-r} & \text{if } r + t \equiv c \pmod{2} \text{ and } S_2 V = (-1)^{b+n(n+2)/8}, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. As observed earlier, V cannot support an even lattice L with $dL = \Delta = (-1)^{(n-s)/2} d^2 D$ unless $S_2 V = (-1)^{b+n(n+2)/8}$ and $r + t \equiv c \pmod{2}$. Then V has

the same invariants (namely, n , s , discriminant, and Hasse symbols) as one of the spaces constructed in Theorem 1, and hence V supports the corresponding even lattice M . Since V is given, the $r+t$ odd primes where $S_p V = -1$ are fixed; that is, R , S , and T are fixed. However, the remaining $e-r$ primes dividing d can be partitioned into P and Q in many ways, and for each p in P there are two choices for the square class of the unit ε_p . It follows that

$$G_V(\Delta) = \sum_{k=0}^{e-r} \binom{e-r}{k} 2^k = 3^{e-r}.$$

Theorem 3. Assume $n \geq 4$ is even, $D \equiv (-1)^{s/2} \pmod{4}$, and $\Delta = (-1)^{(n-s)/2} d^2 D$. Then

$$G(n, s, \Delta) = \begin{cases} 2^{e-1}(2^e + (-1)^{s/4}) & \text{if } f = 0, \\ 2^{2e+f-1} & \text{if } f > 0. \end{cases}$$

Proof. For fixed r , t with $r+t \equiv c \pmod{2}$, there are $\binom{e}{r} \binom{f}{t}$ possible spaces V on which the lattice L with $dL = \Delta$ can lie, depending on the choice of R and T in Theorem 1. Hence, by Theorem 2,

$$G(n, s, \Delta) = \sum_{r+t \equiv c \pmod{2}} \sum \binom{e}{r} \binom{f}{t} 3^{e-r}.$$

Put $j = \sum_{r \text{ even}} \binom{e}{r} 3^{e-r}$ and $k = \sum_{r \text{ odd}} \binom{e}{r} 3^{e-r}$. Then $j+k = 4^e$ and $j-k = 2^e$; Theorem 3 now follows when $f = 0$ since $c = s/4$. When $f > 0$, the theorem follows by first summing on r and then using $\sum \binom{f}{t} (-1)^t = 0$; or it can be done directly as follows. There are four possible lattices for each of the e primes dividing d , one prime dividing D is needed for parity control in $r+t \equiv c \pmod{2}$, and there are two possible lattices for each of the $f-1$ remaining primes. Hence $G(n, s, \Delta) = 4^e 2^{f-1}$.

Remark. In the indefinite case, where $|s| < n$, the class and genus of L coincide under our assumptions on Δ (by Kneser [6] or O'Meara [7]), and hence Theorem 3 also determines the number of classes of even lattices.

3. INDEFINITE LATTICES

Now assume the underlying space V is indefinite so that the class and genus of L coincide. Let H denote a hyperbolic plane and E_8 the even definite unimodular lattice of rank 8.

Theorem 4. Let L be an even indefinite lattice with discriminant $\Delta = (-1)^{n/2} d^2 D$ where $D \equiv 1 \pmod{4}$. Then

$$L = H \perp \cdots \perp H \perp E_8 \perp \cdots \perp E_8 \perp M_m$$

where $m = \text{rank } M_m = 4$ or 8 . Moreover, if the Witt index of V is at least 2, then $m = 4$.

Proof. Assume first that $s = \text{sig } L > 0$. Then 4 divides s . By Theorem 1, there exists a definite even lattice M_m with discriminant $d^2 D$, $m = 4$ or 8

with $m \equiv s \pmod{8}$, and such that $L_p = U_p \perp (M_m)_p$ for each odd prime p , where $U_p = \langle 1, \dots, 1, (-1)^{n/2} \rangle$ is a unimodular lattice of rank $n - m$. Put

$$N = H \perp \dots \perp H \perp E_8 \perp \dots \perp E_8 \perp M_m$$

where the number of E_8 's is chosen to make $\text{sig } N = \text{sig } L$, and then the number of hyperbolic planes H to make $\text{rank } N = n$. Therefore, N_p and L_p are isometric at all primes and N lies in the genus of L . Hence N and L are isometric. When $s = 0$, construct M_4 as before but with signature 0.

If the Witt index of V is at least 2, then we can arrange that M_m has rank 4 and signature 0 or 4. This follows, since $H \perp H \perp M_8$ must now represent E_8 locally at all primes and hence also globally. Thus

$$H \perp H \perp M_8 = E_8 \perp M_4$$

where M_4 has signature 0. This proves Theorem 4.

Remarks. The values for m in Theorem 4 cannot, in general, be improved (use Theorem 1). There is an analogue of Theorem 4 when $D \equiv 3 \pmod{4}$ with $m = 4$ or 6 (and $m = 2$ or 4 when the Witt index is at least 3). These are sharper forms of more general results on orthogonal splitting given earlier by Watson [8] and Gerstein [3, 4]. We have established similar results for integral quadratic forms with square-free discriminant in [5] (however, the proof is different and does not use an analogue of Theorem 1). Also, if L is an odd indefinite lattice with $\text{rank } L \geq 3$ and $dL = \pm d^2 D$, then $L = \langle \pm 1, \dots, \pm 1 \rangle \perp M_m$ with $m \leq 3$ (with 3 best possible, in general). This can be proved by slightly modifying the argument of Theorem 1 in [5].

Proposition. *Let M_m be an even lattice on the m -dimensional space W with signature s' . Assume $dM_m = d^2 D$, $D \equiv 1 \pmod{4d}$, and $S_p W = 1$ for all primes dividing d . Then*

- (i) $M_4 = H \perp B$ if $s' = 0$,
- (ii) $H \perp M_8 = E_8 \perp B$ if $s' = 8$,

where B is an even indefinite binary plane with $dB = -d^2 D$.

Proof. Assume first $m = 8$. For $p|d$ with $(M_8)_p$ almost modular, $(M_8)_p = \langle 1, \dots, 1, \varepsilon, p, p\varepsilon \rangle$ and $S_p W = (\frac{-\varepsilon}{p}) = 1$. Hence $-\varepsilon$ is a local square and $(H \perp M_8)_p$ represents E_8 . Clearly, $H \perp M_8$ represents E_8 locally at all other primes, and hence $H \perp M_8 = E_8 \perp B$ where B is a binary even indefinite lattice with $dB = -d^2 D$. The argument is similar when $m = 4$.

This proposition can be used to establish stronger forms of Theorem 4 in some situations. Denote by $B(d, a)$ the binary even lattice $\mathbf{Z}u + \mathbf{Z}v$ where $f(u, u) = 0$, $f(u, v) = d$, and $f(v, v) = a \in 2\mathbf{Z}$. Then $B(d, a)$ has discriminant $-d^2$.

Theorem 5. Let L be an even indefinite lattice with signature $s \geq 0$ and discriminant $dL = (-1)^{n/2} p^2$, p an odd prime. Then, for $s \equiv 0 \pmod{8}$,

$$L = H \perp \cdots \perp H \perp E_8 \perp \cdots \perp E_8 \perp B(p, a)$$

and, for $s \equiv 4 \pmod{8}$,

$$L = H \perp \cdots \perp H \perp E_8 \perp \cdots \perp E_8 \perp M_4$$

where M_4 is definite.

Proof. This follows using Theorem 4 and the proposition (since $r = 0$ so that $S_p V = 1$).

Remark. Applying Theorem 3 to the situation in Theorem 5 gives $G(n, s, \Delta) = 2 + (-1)^{s/4}$. Hence L is uniquely determined by n , s , and p when $s \equiv 4 \pmod{8}$. When $s \equiv 0 \pmod{8}$ there are three possible L for each (compatible) n , s , and p ; these correspond to $B(p, a)$ with $a = 0$, and $(\frac{a}{p}) = 1$ or -1 (and hence the square class of $a \pmod{p}$ is an invariant for L).

Example. We conclude by explicitly constructing an even definite lattice M_4 with discriminant d^2 when $d \equiv 3 \pmod{4}$. Let

$$N = \perp \mathbb{Z}x_i = \langle 1, 1, -1, d, d \rangle$$

be the odd rank 5 lattice with orthogonal basis as given. Put

$$w = \frac{1}{2}(d-1)x_1 + x_2 + \frac{1}{2}(d+3)x_3 + x_4 + x_5.$$

Then $f(w, w) = -1$ and there is an orthogonal splitting $N = \mathbb{Z}w \perp M_4$. Since $d \equiv 3 \pmod{4}$, all the coefficients of w are odd. Hence any x in M_4 has $f(x, x) \in 2\mathbb{Z}$. Thus M_4 is an even definite lattice with rank 4 and discriminant d^2 . A symmetric matrix representation for M_4 can be easily obtained. In particular, if $d = p \equiv 3 \pmod{4}$ is prime, this M_4 can be used in Theorem 5. The construction of M_4 is more complicated when $p \equiv 1 \pmod{4}$ since then the odd lattice $M_4 \perp \langle -1 \rangle$ does not diagonalize (compute $S_p V$).

ACKNOWLEDGMENT

I wish to thank the referee for carefully reading the paper and suggesting a number of improvements in the presentation.

REFERENCES

1. J. W. S. Cassels, *Rational quadratic forms*, Academic Press, London, 1978.
2. K. S. Chang, *Diskriminanten und Signaturen gerader quadratischer Formen*, Arch. Math. **21** (1970), 59–65.
3. L. J. Gerstein, *Splitting quadratic forms over integers of global fields*, Amer. J. Math. **91** (1972), 106–134.
4. —, *Orthogonal splitting and class numbers of quadratic forms*, J. Number Theory **5** (1973), 332–338.

5. D. G. James, *Orthogonal decompositions of indefinite quadratic forms*, Rocky Mountain J. Math. (to appear).
6. M. Kneser, *Klassenzahlen indefiniter quadratischer Formen in drei oder mehr Veränderlichen*, Arch. Math. 7 (1956), 323–332.
7. O. T. O'Meara, *Introduction to quadratic forms*, Springer-Verlag, New York, 1963.
8. G. L. Watson, *Integral quadratic forms*, Cambridge University Press, London, 1960.

DEPARTMENT OF MATHEMATICS, PENNSYLVANIA STATE UNIVERSITY, UNIVERSITY PARK,
PENNSYLVANIA 16802