Diagonalizable indefinite integral quadratic forms

by

DONALD G. JAMES* (University Park, Penn.)

1. Introduction. Let \( L \) be a \( \mathbb{Z} \)-lattice on an indefinite regular quadratic \( \mathbb{Q} \)-space \( V \) of finite dimension \( n \geq 3 \), with associated symmetric bilinear form \( f : V \times V \to \mathbb{Q} \). Assume, for convenience, that \( f(L, L) = \mathbb{Z} \), namely the scale of \( L \) is \( \mathbb{Z} \). Let \( x_1, \ldots, x_n \) be a \( \mathbb{Z} \)-basis for \( L \) and put \( d = dL = \det f(x_i, x_j) \), the discriminant of the lattice \( L \). We study a Hasse principle for diagonalization, that is, we investigate the set \( \mathcal{D} \) of discriminants with the property that all indefinite lattices with discriminant in \( \mathcal{D} \), which diagonalize locally at all primes, also diagonalize globally over \( \mathbb{Z} \). Since all lattices diagonalize locally at the odd primes (see O'Meara [5]), the local condition is only significant for the prime 2. A result of J. Milnor states that all odd lattices \( L \) with \( dL = \pm 1 \) have an orthogonal basis (see Serre [6] or Wall [7]). Thus \( \pm 1 \in \mathcal{D} \). It is also shown in James [3] that \( \pm 2q \in \mathcal{D} \) for all primes \( q \equiv 3 \mod 4 \), but \( 2q \notin \mathcal{D} \). We prove here the following

Theorem. Let \( p \equiv 1 \mod 4 \), \( p' \equiv 5 \mod 8 \), \( q \equiv 3 \mod 4 \) and \( q' \equiv 3 \mod 8 \) be primes with Legendre symbols \( \left( \frac{q}{p} \right) = \left( \frac{p'}{q} \right) = -1 \). Then \( \pm d \in \mathcal{D} \) for the following values of \( d \):

\[ 1, 2, 4, q, 2q, q^2, 2q^2, 2qq', 2p', pq, 2pq, 2pp', 2p^2, 2p'q. \]

For each of the discriminants \( d \) considered in the above theorem, except \( d = 4 \), the local condition that \( L_2 \) diagonalizes is equivalent to the global condition that \( L \) is an odd lattice, namely the set \( \{ f(x, x) \mid x \in L \} \) contains at least one odd number. An exact determination of \( \mathcal{D} \) appears very difficult. In fact we will exhibit \( d \in \mathcal{D} \) with \( d \) containing arbitrarily many prime factors (see Proposition 2).

Let \( i = i(L) = i(V) \) be the Witt index of \( V \). Then \( \mathcal{D}(i) \) denotes the set of discriminants of lattices \( L \) on spaces \( V \) with Witt index at least \( i \) which diagonalize over \( \mathbb{Z} \) whenever the localization \( L_i \) diagonalizes. It is also useful to introduce the stable version \( \mathcal{D}(\infty) \) of discriminants where \( dL \in \mathcal{D}(\infty) \)

* This research was partially supported by the National Science Foundation.
means the lattice \( L \perp H^n \) diagonalizes for \( m \) sufficiently large, assuming \( L_2 \) diagonalizes, where \( H^n \) is the orthogonal sum of \( n \) integral hyperbolic planes \( H \) corresponding to the matrix \[
\begin{bmatrix}
0 & 1 \\
1 & 0
\end{bmatrix}
\]. Trivially,
\[
\mathcal{D} = \mathcal{D}(1) \subseteq \mathcal{D}(2) \subseteq \ldots \subseteq \mathcal{D}(\infty).
\]
We also establish some results for the sets \( \mathcal{D}(i) \). For example, \( \pm qf \) is in \( \mathcal{D}(2) \) for primes \( q \equiv q' \equiv 3 \) mod 4, but \( \pm qf \) is not in \( \mathcal{D}(1) \). Thus \( \mathcal{D}(1) \neq \mathcal{D}(2) \). On the other hand, the discriminants \( p, 4p, p^2, pl \) and \( 4pl \) are not in \( \mathcal{D}(\infty) \) for any primes \( p, l \) with \( p \equiv 1 \) mod 4 and \( (\frac{l}{p}) = 1 \).

Although the theorem above only states the existence of a diagonalized form for any lattice with the given discriminant \( d \in \mathcal{D} \), the proofs are constructive and will determine a diagonal matrix for the form (which need not be unique).

2. Preliminaries. It is convenient to adopt the convention that \( p \) is always a prime with \( p \equiv 1 \) mod 4, while \( q \) is a prime with \( q \equiv 3 \) mod 4. Let \( \langle a_1, \ldots, a_n \rangle \) denote the \( \mathbb{Z} \)-lattice \( \mathbb{Z}X_1 \perp \ldots \perp \mathbb{Z}X_n \) with an orthogonal basis where \( f(x_i, x_j) = a_{ij}, 1 \leq i, j \leq n \). Most of our notation follows O'Meara [5]. Thus \( L_p \) is the localization of \( L \) at the prime \( p \), while \( S_p L \) is the Hasse symbol of the local space on which \( L_p \) lies. Let \( s(L) = s(V) \) denote the signature of the space \( V \).

Since we only consider indefinite lattices \( L \), the genus and the class of \( L \) coincide, provided the discriminant \( dL \) is not divisible by any odd prime power \( l^e \) with exponent \( e \geq \frac{1}{2} \) \( n(n-1) \), nor by \( 2^7 \) (see Earnest and Hsiang [2], Kneser [4]).

We also need to know when two \( \mathbb{Z} \)-lattices \( L \) and \( M \) with the same rank \( n \) and discriminant \( d \) are locally isometric. At the infinite prime the spaces must have the same signature. General conditions at the finite primes \( l \) are given in O'Meara ([5], § 92, 93). Assume first, as is necessary, that \( L_1 \) and \( M_1 \) have the same Jordan type. We will use the following special cases.

(i) If \( L_1 \) and \( M_1 \) are unimodular, then \( L_1 \cong M_1 \).

(ii) Let \( L_1 = J_1 \perp \langle b, c \rangle \) and \( M_1 = K_1 \perp \langle c \rangle \) with \( J_1 \) and \( K_1 \) unimodular, of the same rank, and \( b, c \) \( l \)-adic units. Assume \( l \) an odd prime. Then \( L_1 \cong M_1 \) if and only if \( S_1 L_1 = S_1 M_1 \), that is, if and only if the Hilbert symbol
\[
\left( \frac{bc, l}{l} \right) = 1.
\]

(iii) If \( L_2 \) and \( M_2 \) are diagonalizable and have the same Jordan type consisting of a unimodular and a 2-modular component, then \( L_2 \) and \( M_2 \) are isometric by O'Meara ([5], 93:29).

3. Main results. The theorem stated in the Introduction, along with the other comments given there, are consequences of the following more specific results and techniques.

Proposition 1. Let \( \pm d \) be a product of \( g \) distinct primes \( q \equiv 3 \) mod 4. Then

(i) \( \pm 1, \pm 2, \pm 4 \in \mathcal{D} \),

(ii) \( d, 2d \in \mathcal{D}(g) \),

(iii) \( 2d \in \mathcal{D}(g-1) \), provided \( g \geq 2 \), and there exists a prime \( q' \equiv 3 \) mod 8 dividing \( d \).

Proof. Let \( L \) be an odd lattice with \( d = d_L \), rank \( n \geq 3 \) and index \( i(L) \geq g \). Let \( q \) be a prime dividing \( d \). Consider the two \( \mathbb{Z} \)-lattices \( N = J \perp \langle q \rangle \) and \( N' = K \perp \langle -q \rangle \) where \( J \) and \( K \) are diagonalized lattices and \( dN = dN' = bq \), where \( (b, q) = 1 \). Since \( q \equiv 3 \) mod 4, we have
\[
S_q N = \left( \begin{array}{cc}
q & 0 \\
0 & q
\end{array} \right) = \left( \begin{array}{cc}
q & -b \\
0 & q
\end{array} \right) = -\left( \begin{array}{cc}
b & 0 \\
0 & q
\end{array} \right)
\]
and
\[
S_q N' = \left( \begin{array}{cc}
-q & 0 \\
0 & q
\end{array} \right) = \left( \begin{array}{cc}
-q & b \\
0 & q
\end{array} \right) = \left( \begin{array}{cc}
b & 0 \\
0 & q
\end{array} \right).
\]

Hence we can choose \( M \) equal to \( N \) or \( N' \) such that \( S_q M = S_q L \). In fact, more generally, since \( i(L) \geq g \), we can choose
\[
M = \langle \pm q_1, \pm q_2, \ldots, \pm q_g, 1, \ldots, 1 \rangle
\]
such that \( dM = dL = d \), rank \( M = n \), \( s(M) = s(L) \) and \( S_q M = S_q L \) for all primes \( q \) dividing \( d \). Then \( S_{q_1} M = S_{q_1} L \) and \( S_{q_g} M = S_{q_g} L \) for all odd primes \( l \). By Hilbert reciprocity, \( S_{q_1} M = S_{q_2} L \) and hence \( M \) and \( L \) can be viewed as lying on the same quadratic space. By earlier remarks, \( L \) and \( M \) are in the same genus and hence the same class. Thus \( L \) diagonalizes and \( d \in \mathcal{D}(q) \). A slight modification of the above, introducing a \( \pm 2 \) term into \( M \), shows that \( 2d \in \mathcal{D}(g) \). This proves (ii).

The above argument also holds, with minor modifications, when \( g = 0 \) and \( d = \pm 1, \pm 2 \) or \( \pm 4 \). In the case \( d = \pm 4 \), the sign of \( \langle \pm 2^2 \rangle \) in \( M \) must be chosen to ensure \( M \cong L_2 \) if \( L_2 \) has a 4-modular component. This proves (i).

Now assume \( dL = 2d \) and there exists a prime \( q \equiv 3 \) mod 8 dividing \( d \). Consider \( N = J \perp \langle q \rangle \) and \( N' = K \perp \langle -q \rangle \) with \( J \) and \( K \) as before. Since
\[
\left( \frac{2}{q} \right) = -1,
\]
it follows that \( S_q N = -S_q N' \). A similar conclusion holds for the pair \( J \perp \langle -q \rangle \) and \( K \perp \langle -2q \rangle \). Hence we can again arrange that \( S_q L = S_q M \) by using the factor 2 and save one choice of sign. Thus \( L \) now diagonalizes if \( i(L) \geq g - 1 \geq 1 \), proving (iii).
Remark. Proposition 1 establishes $\pm qq' \in \mathcal{O}(2)$ for primes $q \equiv q' \equiv 3 \mod 4$. However, $\pm qq'$ is not in $\mathcal{O}(1)$. We may assume $\left(\frac{q}{q'}\right) = 1$. By Dirichlet's Theorem there exists a prime $l \equiv 3 \mod 4$ with $-\left(\frac{l}{q'}\right) = \left(\frac{l}{q}\right) = 1$. Then $\left(\frac{-qq'}{l}\right) = 1$ and there exists $c \in \mathbb{N}$ with $c^2 \equiv -qq' \mod l$. Put $a = (c^2 + qq')l^{-1} \in \mathbb{N}$ and let $B$ be the binary $\mathbb{Z}$-lattice corresponding to the symmetric matrix $\begin{bmatrix} l & c \\ c & -l \end{bmatrix}$. Put $L = \langle 1, 1, \ldots, 1, -1 \rangle \perp B$. Then $L$ has index $i(L) = 1$ and $dL = -qq'$. Also $S_L \left(\frac{1}{q}\right) = 1$ and $S_{-q} L = -1$. If $L$ diagonalizes, then $L = U \perp J$ where $U = \langle 1, 1, \ldots, 1 \rangle$ and $J$ is one of the five lattices $\langle 1, 1, -qq' \rangle, \langle 1, -1, qq' \rangle, \langle 1, q, -q' \rangle, \langle 1, -q, q' \rangle$ or $\langle -1, 1, 0 \rangle$. But none of these five lattices has the same Hasse symbols as $L$ at $q$ and $q'$. Hence $L$ does not diagonalize and $-qq'$ is not in $\mathcal{O}(1)$. The lattice obtained from $L$ by scaling by $-1$ also does not diagonalize. Hence $qq' \notin \mathcal{O}(1)$.

**Proposition 2.** Let $p_i \equiv 5 \mod 8, 1 \leq i \leq m$, be distinct primes with $\left(\frac{p_i}{p_j}\right) = 1, 1 \leq i \neq j \leq m$, and $d = \pm 2p_1p_2 \ldots p_m$. Then $d$ and $dq$ are in $\mathcal{O}$ for any prime $q \equiv 3 \mod 4$.

**Proof.** Consider the binary $\mathbb{Z}$-lattice $B = \langle -p_1 \ldots p_r, 2p_{r+1} \ldots p_m \rangle$ where $0 \leq r \leq m$. By varying $r$ and permuting the primes $p_i$, there are $2^m$ distinct choices for $B$. Since, for $1 \leq i \leq r$,

$$S_{p_i} B = \left(\frac{-p_1 \ldots p_r}{p_i}, -\frac{-|d|}{p_i}\right) = \left(\frac{2}{p_i}\right) = -1,$$

while for $r+1 \leq j \leq m$,

$$S_{p_j} B = \left(\frac{2p_{r+1} \ldots p_m}{p_j}, -\frac{-|d|}{p_j}\right) = 1,$$

the values of the Hasse symbols $S_B$ are distinct for each of these $2^m$ choices of $B$. Let $L$ be an odd indefinite $\mathbb{Z}$-lattice with $dL = d$. Then we can find $M = U \perp B$ with $U = \langle \pm 1, \ldots, \pm 1 \rangle$ and rank $M = \text{rank } L$ such that $s(M) = s(L)$ and $S_M = S_L$ for all odd primes $l$. Again, by Hilbert reciprocity, $S_2 M = S_2 L$ so that $M$ and $L$ are on the same quadratic space and are isometric. Thus $L$ diagonalizes and $d \in \mathcal{O}$.

Next consider $\langle 1 \rangle \perp B_1$ and $\langle -q \rangle \perp B_2$ where $B_1$ and $B_2$ are variants of $B$ with $dB_1 = -dB_2$ where $B_1$ and $B_2$ are variants of $B$ with $dB_1 = -dB_2$ achieved by changing a sign in the coefficients (since $\left(\frac{-1}{p}\right) = 1$, this has no effect on $S_B$). These two lattices have the same Hasse symbols at all odd primes except $q$ where they have the opposite values. Proceeding as before, we now have $dq \notin \mathcal{O}$.

**Remark.** Many variations of the above two propositions can be established for other combinations of primes. Also the method can be used when $d$ is not square free, although there will now be more Jordan types to consider. For example, as is indicated in the statement of the main theorem, it can be shown that $\pm q^2$ and $\pm 2q^2$ are in $\mathcal{O}$ for any prime $q \equiv 3 \mod 4$.

On the other hand, there are many choices for $d = dL$ of a similar nature where $L$ need not diagonalize.

**Proposition 3.** Let $p \equiv 1 \mod 4$ be prime and $D, E \in \mathbb{N}$ with $\left(\frac{1}{p}\right) = 1$ for any prime $l$ dividing $D$. Then $\pm pDE^2 \notin \mathcal{O}(\infty)$.

**Proof.** By Dirichlet's Theorem there exists a prime $q \equiv 3 \mod 4$ with $\left(\frac{p}{q}\right) = -1$. Hence there exists $e \in \mathbb{N}$ such that $c^2 p \equiv -1 \mod q$. Put $a = 1 + c^2 p^{-1} e \in \mathbb{N}$ and let $B = Zx_1 + Zx_2$ be the binary lattice where $f(x_1, x_1) = 0, f(x_1, x_2) = pc$ and $f(x_2, x_2) = pq$. Then $dB = l$. Let $L = U \perp \langle -DE^2 \rangle \perp B$ where $U = \langle \pm 1, \ldots, \pm 1 \rangle$ is unimodular. Then $L$ is an indefinite lattice with $dL = \pm pDE^2$ and the localization $L_2$ diagonalizes. If $L$ diagonalizes, then $L = Zx_1 \perp \mathbb{N}$ with ord$_2 f(x, x) = 1$. Hence $f(x, L) \subseteq p\mathbb{Z}$ and consequently $x = pu + v + w$ where $u \in U, v = x_1 + x_2 \beta_{x_1} + B, w \in \langle -DE^2 \rangle$ with $f(w, w) \equiv 0 \mod p^2$. Hence

$$f(x, x) = f(v, v) \equiv \alpha^2 a + 2\beta pc + \beta^2 pq \mod p^2.$$ 

Consequently $p$ divides $\alpha$ and $f(x, x) \equiv \beta^2 pq \mod p^2$. Let $f(x, x) = pb$. Then $b$ divides $DE^2$, and $\left(\frac{b}{p}\right) = -1$ by choice of $q$. If $l$ is a prime dividing $b$, then either $l$ divides $D$ and hence $\left(\frac{l}{p}\right) = 1$, or $l$ divides $E$ in which case ord$_l b$ is even (from considering the Jordan type of $L_2$). This leads to the contradiction $\left(\frac{b}{p}\right) = 1$, since $p \equiv 1 \mod 4$. Hence $L$ does not diagonalize and, since $U$ can have arbitrarily large index, necessarily $dL = \pm pDE^2$ is not in $\mathcal{O}(\infty)$.

**Corollary.** If $p \equiv 1 \mod 4$ and $l$ are primes with $\left(\frac{1}{p}\right) = 1$, then $\pm d \notin \mathcal{O}(\infty)$ for $d = p, 4p, pl$ and $4pl$.

**Remark.** By varying the choice of $B$ in the proof of Proposition 3, it is possible to produce more discriminants $d \notin \mathcal{O}(\infty)$. We give three further examples. Let $D, E \in \mathbb{N}$.
(i) Let \( p \equiv p' \equiv 1 \mod 4 \) be primes with \( \left( \frac{p'}{p} \right) = -1 \). Then
\[
\pm pp' E^2 \neq \mathcal{O}(\infty).
\]
(ii) Let \( p \equiv p' \equiv 1 \mod 8 \) be primes with \( \left( \frac{p'}{p} \right) = -1 \). Then
\[
\pm 2pp' E^2 \neq \mathcal{O}(\infty).
\]
(iii) Let \( p \equiv 1 \mod 4 \) be a prime with \( \left( \frac{l}{p} \right) = 1 \) for all primes \( l \) divid
\[
D. \quad \pm p^2 DE^2 \neq \mathcal{O}(\infty).
\]

References


DEPARTMENT OF MATHEMATICS
THE PENNSYLVANIA STATE UNIVERSITY
University Park, PA 16802, USA

Received on 11.4.1986
and in revised form on 31.7.1986

BOOKS PUBLISHED BY THE POLISH ACADEMY OF SCIENCES
INSTITUTE OF MATHEMATICS

K. Kuratowski, Selected papers, in the press.
W. Orlicz, Collected papers, in the press.

MONOGRAFIE MATEMATYCZNE


BANACH CENTER PUBLICATIONS

Vol. 23. Dynamical systems and ergodic theory, in the press.