Qatar Univ. Sci. J. (1991), 11: 11 - 17

DIAGONALIZABLE INDEFINITE INTEGRAL QUADRATIC FORMS

By

LAILA E. M. RASHID
Mathematics Department, Faculty of Education,
Kafer El-Sheikh, Tanta Univerrsity, Kafer El-Sheikh, Egypt

ABSTRACT

This paper deals with some special cases on Hasse's principle about the diagonalization of Z-lattices L of indefinite regular guadratic forms over Q. It is asserted that for some specific values of a certain set D of discriminants of L, that the local condition of L_2 diagonalization is equivalent to the global condition that L is an odd lattice.

INTRODUCTION

Let L be a Z-lattice on an indefinite regular quadratic Q-space V, of finite dimension $n \geqslant 3$, with associated symmetric bilinear form f: $V \times V \rightarrow Q$. Assume, for convenience, that f(L,L) = Z, namely the scale of L is Z. Let $x_1, \ldots, x_n$ be a Z-basis for L and put $d = dL = \det f(x_i, x_j)$, the discriminant of the lettice L. We study a Hasse principle for diagonalization, that is, we investigate the set D of discriminants with the property that all indefinite lattices with discriminant in D, which diagonalize locally at all primes, also diagonalize globally over Z. Since all lattices diagonalize locally at the odd primes (see O'Meare [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 $\pm 1 \in D$. It is also shown in James [3] that $\pm 2\,q \in D$ for all primes $q \equiv 3 \bmod 4$, but $2.41 \notin D$. We prove here the following.

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

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

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 D appears very difficult. In fact we will exhibit $d \in D$ with d containing arbitrarily many prime factors (see proposition 2).

Let $i = i(L) = i(V)$ be the Witt index of V. Then D(i) denotes the set of discriminants of Lattices L on spaces V with Witt index at least i which diagonalize over Z whenever the localization L_2 diagonalizes. It is also useful to introduce the stable version $D(\infty)$ of discriminants where $dL \in D(\infty)$ means the lattice $L \perp H^m$ diagonalizes for m sufficiently large, assuming L_2 diagonalizes, where H^m is the orthogonal sum of m integral hyperbolic planes H corresponding to the matrix

$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ Trivially,

$$D = D(1) \subseteq D(2) \subseteq \ldots \subseteq D(\infty).$$

We also establish some results for the sets D(i). For example, $\pm qq'$ is in D(2) for primes $q \equiv q' \equiv 3 \bmod 4$, but $\pm qq'$ is not in D(1). Thus $D(1) \neq D(2)$. On the other hand, the discriminants p, 4p, p^2, $p\ell$ and $4p\ell$ are not in $D(\infty)$ for any primes p, l with $p \equiv 1 \bmod 4$ and $\left(\frac{\ell}{p}\right) = 1$.

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

PRELIMINARIES

It is convenient to adopt the convention that p is always a prime with $p \equiv 1 \bmod 4$, while q is a prime with $q = 3 \bmod 4$. Let $< a_1, \ldots, a_n >$ denote the Z-lattice $Zx_1 \perp \ldots \perp Zx_n$ with an orthogonal basis where $f(x_i, x_i) = a_i$, $1 \leqslant i \leqslant n$. 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 $e \geqslant \frac{1}{2} n(n-1)$, nor by 2^7 (see Earnest and Hsia [2], Kneser [4]).

We also need to know when two 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_ℓ and M_ℓ have the same Jordan type. We will use the following special cases.

(i) If L_ℓ and M_ℓ are unimodular, then $L_\ell \cong M_\ell$.

(ii) Let $L_\ell = J_\ell \perp < \ell b >$ and $M_\ell = K_\ell \perp < \ell c >$

with J_ℓ and K_ℓ unimodular, of the same rank, and b, c ℓ-adic units. Assume ℓ an odd prime. Then $L_\ell \cong M_\ell$ if and only if $S_\ell L_\ell = S_\ell M_\ell$ that is, if and only if the Hilbert symbol $(\frac{bc,\ \ell}{\ell}) = 1$.

(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).

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 $q \equiv 3 \bmod 4$. Then

(i) $\pm 1, \pm 2, \pm 4 \in D$,

(ii) $d, 2d \in D(g)$,

(iii) $2d \in D(g-1)$, provided $g \geqslant 2$ and there exists a prime $q' \equiv 3 \bmod 8$ dividing d.

Proof: Let L be an odd lattice with $d = dL$, rank $n \geqslant 3$ and index $i(L) \geqslant g \geqslant 1$. Let q be a prime dividing d. Consider the two Z-lattices $N = J \perp < q >$ and $N' = K \perp < -q >$

where J and K are diagonalized lattices and $dN = dN' = bq$, where $(b, q) = 1$. Since $q \equiv 3 \bmod 4$, we have

$$S_q N = (\frac{q,\ qb}{q}) = (\frac{q,\ -b}{q}) = -(\frac{b}{q})$$

and

$$S_q N' = (\frac{-q,\ qb}{q}) = (\frac{-q,\ b}{q}) = (\frac{b}{q}).$$

Hence we can choose M equal to N or N' such that $S_q M = S_q L$. In fact, more generally, since $i(L) \geqslant g$, we can choose

$$M = < \pm q_1, \pm q_2, \ldots, \pm q_g, \pm 1, \ldots, \pm 1 >$$

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 $S_\infty M = S_\infty L$ and $S_\ell M = M = S_\ell L$ for all odd primes ℓ. By Hilbert reciprocity, $S_2 M = S_2 L$ 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 $d \in D(g)$. A slight modification of the above, introducing a ± 2 term into M, shows that $2d \in D(g)$. This proves (ii). The above argument also holds, with minor modifications, when $g = 0$ and $d = \pm 1$, ± 2 or ± 4. In the case $d = \pm 4$, the sign of $< \pm 2^2 >$ in M must be chosen to ensure $M_2 \cong L_2$ if L_2 has a 4-modular component. This proves (i).

Now assume $dL = 2d$ and there exists a prime $q \equiv 3 \bmod 8$ dividing d. Consider $N = J \perp < q >$ and $N' = K \perp < 2q >$ with J and K as before. Since $(\frac{2}{q}) = -1$, it follows that $S_q N = -S_q N'$. A similar conclusion holds for the pair $J \perp < -q >$ and $K \perp <-2q >$. 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 $i(L) \geqslant g - 1 \geqslant 1$, proving (iii).

Remark: Proposition 1 establishes $\pm qq' \in D(2)$ for primes $q \equiv q' \equiv 3 \bmod 4$. However, $\pm qq'$ is not in D(1). We may assume $(\frac{q}{q'}) = 1$. By Dirichlet's Theorem there exists a prime $\ell \equiv 3 \bmod 4$ with $-(\frac{\ell}{q'}) = (\frac{\ell}{q}) = 1$. Then $(\frac{-qq'}{\ell}) = 1$ and there exists $c \in N$ with $c^2 \equiv -qq' \bmod \ell$. Put $a = (c^2 + qq')\,\ell^{-1} \in N$ and let B be the binary Z-lattice corresponding to the symmetric matrix $\begin{bmatrix} \ell & c \\ c & a \end{bmatrix}$. Put $L = < 1, 1, \ldots, 1, -1 > \perp B$. Then L has index $i(L) = 1$ and $dL = -qq'$. Also $S_q L = (\frac{\ell}{q}) = 1$ and $S_q L = -1$. If L diagonalizes, then $L = U \perp J$ where $U = < 1, 1, \ldots, 1 >$ and J is one of the five lattices $< 1, 1, -qq' >$, $< 1, -1, qq' >$, $< 1, q, -q' >$, $< 1, -q, q' >$ or $< -1, q, q' >$. 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 D(1). The lattice obtained from L by scaling by -1 also does not diagonalize. Hence $qq' \notin D(1)$.

Proposition 2: Let $p_i \equiv 5 \bmod 8$, $1 \leqslant i \leqslant m$, be distinct primes with $(\frac{p_i}{p_j}) = 1$, $1 \leqslant i \neq j \leqslant m$, and $d = \pm 2\, p_1 p_2 \ldots p_m$. Then d and d_q are in D for any prime $q \equiv 3 \bmod 4$.

Proof: Consider the binary Z-lattice $B = < -p_1 \ldots p_r, 2p_{r+1} \ldots p_m >$ where $o \leqslant r \leqslant m$. By varying r and permuting the primes p_i, there are 2^m distinct choices for B. Since, for $1 \leqslant i \leqslant r$,

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

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

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

the values of the Hasse symbols $S_p B$ are distinct for each of these 2^m choices of B. Let L be an odd indefinite Z-lattice with $dL = d$. Then we can find $M = U \perp B$ with

$U = < \pm 1, \ldots, \pm 1 >$ and rank M = rank L such that $s(M) = s(L)$ and $S_\ell M = S_\ell L$ 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 $d \in D$.

Next consider $< q > \perp B_1$ and $< -q > \perp B_2$ where B_1 and B_2 are variants of B with $dB_1 = -dB_2$ achieved by changing a sign in the coefficients (since $(\frac{-1}{p}) = 1$, this has no effect on $S_p B$). 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 $dq \in D$.

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 D for any prime $q \equiv 3 \bmod 4$.

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

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

Proof: By Diriclet's theorem there exists a prime $q \equiv 3 \bmod 4$ with $(\frac{p}{q}) = -1$. Hence there exists $c \in N$ such that $c^2 p \equiv -1 \bmod q$. Put $a = (1+c^2p)q^{-1} \in N$ and let $B = Zx_1 + Zx_2$ be the binary lattice where $f(x_1, x_1) = a$, $f(x_1, x_2) = pc$ and $f(x_2, x_2) = pq$. Then $dB = p$. Let $L = U \perp < -DE^2 > \perp B$ where $U = < \pm 1, \ldots, \pm >$ is unimodular. Then L is an indefinite lattice with $dL = \pm pDE^2$ and the localization L_2 diagonalizes. If L diagonalizes, then $L = Z x \perp N$ with $\mathrm{ord}_p f(x, x) = 1$. Hence $f(x,L) \subseteq pZ$ and consequently $x = pu + v + w$ where $u \in U$, $v = \propto x_1 + \beta x_2 \in B$ and $w \in < -DE^2 >$ with $f(w,w) \equiv 0 \bmod p^2$. Hence

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

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

Corollary: If $p \equiv 1 \bmod 4$ and ℓ are primes with $(\frac{\ell}{p}) = 1$, then $\pm d \notin D(\infty)$ for $d = p$, $4p$, $p\ell$ and $4p\ell$.

Remark: By varying the choice of B in the proof of proposition 3, it is possible to

produce more discriminants $d \notin D(\infty)$. We give three further examples.
Let $D, E \in N$.

(i) Let $p \equiv p' \equiv 1 \bmod 4$ be primes with $\left(\frac{p'}{p}\right) = -1$.

then

$\pm pp'E^2 \notin D(\infty)$.

(ii) Let $p \equiv p' \equiv 1 \bmod 8$ be primes with $\left(\frac{p'}{p}\right) = -1$.

then

$\pm 2pp'E^2 \notin D(\infty)$.

(iii) Let $p \equiv 1 \bmod 4$ be a prime with $\left(\frac{\ell}{p}\right) = 1$ for all primes ℓ dividing D. Then

$\pm p^2DE^2 \in D(\infty)$.

REFERENCES

[1] **Cassels, J.W.S. 1978.** Rational Quadratic Forms, Academic Press, London.

[2] **Earnest, A.G.** and **J.S. Hsia, 1975.** Spinor norms of local integral rotations II, Pacific J. Math. 61, pp. 71-86.

[3] **James, D.G. 1969.** Indefinite quadratic forms of determinant ±2p, Proc. Amer. Math. Soc. 21, 214-218.

[4] **Kneser, M. 1956.** Klassenzahlen indefiniter quadratischer Formen in drei oder mehr Varanderlichen, Arch. Math. 7, 323-332.

[5] **O'Meara, O.T. 1963.** Introduction to Quadratic Forms, Springer-Verlag, New York.

[6] **Serre, J.P. 1973.** A Course in Arithmetic, Springer-Verlag, New York.

[7] **Wall, C.T.C. 1962.** On the orthogonal groups of unimodular quadratic forms, Math. Ann. 147, 328-338.

الصيغ التربيعيــة التكاملية غير المحددة
والقابلــة للتحويل للصــورة القطريــة

ليلــى رشـــيد

هذا البحث يتعلق ببعض الحالات الخاصة « لقاعدة هاسة » عن التحويل للصورة القطرية للشبكيات (L) فوق (Z) ، الناتجة عن الصيغ الثنائية المنتظمة غير المحدودة ، فوق (Q) ؛ حيث تتوصل الباحثة إلى أنه بالنسبة لبعض القيم الخاصة المنتمية للمجموعة المعيَّنة (D) من مميزات (L) ، فإن الشرط الموضعي عن التحويل للصورة القطرية لـ (L_2) ، يكافئ الشرط الشمولي أن (L) شبكية فردية النوع .