[5] M. Waldschmidt, *Nombres transcendents*, LNM 402, Springer, Berlin–Heidelberg New York 1974.
[6] Zhu Yaochen, *On the algebraic independence of certain power series of algebraic numbers*, Chin. Ann. Math. 5B (1) (1984), pp. 109–117.
[7] — *On a criterion of algebraic independence of numbers*, Kexue Tongbao (to appear).

INSTITUTE OF APPLIED MATHEMATICS
ACADEMIA SINICA
Beijing, China
MAX-PLANCK-INSTITUT FÜR MATHEMATIK
Gottfried-Claren-Str. 26
D-5300 Bonn 3

Received on 4.3.1986
and in revised form on 19.8.1986 (1611)

ACTA ARITHMETICA
L (1988)

Diagonalizable indefinite integral quadratic forms

by

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

1. 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 $f: V \times V \to Q$. 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 lattice L. We study a Hasse principle for diagonalization, that is, we investigate the set $\mathscr{D}$ of discriminants with the property that all indefinite lattices with discriminant in $\mathscr{D}$, which diagonalize locally at all primes, also diagonalize globally over 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 $\pm 1 \in \mathscr{D}$. It is also shown in James [3] that $\pm 2q \in \mathscr{D}$ for all primes $q \equiv 3 \bmod 4$, but $2.41 \notin \mathscr{D}$. 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* $\pm d \in \mathscr{D}$ *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 $\{f(x, x) |\ x \in L\}$ contains at least one odd number. An exact determination of $\mathscr{D}$ appears very difficult. In fact we will exhibit $d \in \mathscr{D}$ with d containing arbitrarily many prime factors (see Proposition 2).

Let $i = i(L) = i(V)$ be the Witt index of V. Then $\mathscr{D}(i)$ 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 $\mathscr{D}(\infty)$ of discriminants where $dL \in \mathscr{D}(\infty)$

* This research was partially supported by the National Science Foundation.

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,

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

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

Although the theorem above only states the existence of a diagonalized form for any lattice with the given discriminant $d \in \mathscr{D}$, 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 $p \equiv 1 \bmod 4$, while q is a prime with $q \equiv 3 \bmod 4$. Let $\langle a_1, \ldots, a_n \rangle$ denote the $\mathbf{Z}$-lattice $\mathbf{Z}x_1 \perp \ldots \perp \mathbf{Z}x_n$ 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 $\mathbf{Z}$-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 $L_l \cong M_l$.

(ii) Let $L_l = J_l \perp \langle l\, b \rangle$ and $M_l = K_l \perp \langle l\, c \rangle$ with J_l and K_l unimodular, of the same rank, and b, c l-adic units. Assume l an odd prime. Then $L_l \cong M_l$ if and only if $S_l L_l = S_l M_l$, 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 $q \equiv 3 \bmod 4$. Then*

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

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

(iii) $2d \in \mathscr{D}(g-1)$, *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 $\mathbf{Z}$-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 $q \equiv 3 \bmod 4$, we have

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

and

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

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

$$M = \langle \pm q_1, \pm q_2, \ldots, \pm q_g, \pm 1, \ldots, \pm 1 \rangle$$

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 $S_\infty M = S_\infty L$ and $S_l M = S_l L$ 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 $d \in \mathscr{D}(g)$. A slight modification of the above, introducing a ± 2 term into M, shows that $2d \in \mathscr{D}(g)$. 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 $\langle \pm 2^2 \rangle$ 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 $N = J \perp \langle q \rangle$ and $N' = K \perp \langle 2q \rangle$ 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 $i(L) \geqslant g-1 \geqslant 1$, proving (iii).

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

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

Proof. Consider the binary Z-lattice $B = \langle -p_1 \ldots p_r, 2p_{r+1} \ldots p_m\rangle$ where $0 \leqslant r \leqslant m$. 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 $r+1 \leqslant j \leqslant m$,

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

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 $U = \langle \pm 1, \ldots, \pm 1\rangle$ and rank M = rank L such that $s(M) = s(L)$ and $S_l M = S_l L$ 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 $d \in \mathcal{D}$.

Next consider $\langle q\rangle \perp B_1$ and $\langle -q\rangle \perp B_2$ where B_1 and B_2 are variants of B with $dB_1 = -dB_2$ achieved by changing a sign in the coefficients (since $\left(\frac{-1}{p}\right) = 1$, 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 $dq \in \mathcal{D}$.

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 $\mathcal{D}$ 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 $\left(\frac{l}{p}\right) = 1$ for any prime l dividing D. Then $\pm pDE^2 \notin \mathcal{D}(\infty)$.*

Proof. By Dirichlet's Theorem there exists a prime $q \equiv 3 \bmod 4$ with $\left(\frac{p}{q}\right) = -1$. Hence there exists $c \in N$ such that $c^2 p \equiv -1 \bmod q$. Put $a = (1 + c^2 p)q^{-1} \in N$ 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 $L = U \perp \langle -DE^2\rangle \perp B$ 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 $L = Zx \perp N$ with $\operatorname{ord}_p f(x, x) = 1$. Hence $f(x, L) \subseteq pZ$ and consequently $x = pu + v + w$ where $u \in U$, $v = \alpha x_1 + \beta x_2 \in B$ and $w \in \langle -DE^2\rangle$ with $f(w, w) \equiv 0 \bmod p^2$. Hence

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

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 $\left(\frac{b}{p}\right) = -1$ 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 $\operatorname{ord}_l b$ is even (from considering the Jordan type of L_l). This leads to the contradiction $\left(\frac{b}{p}\right) = 1$, 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 $\mathcal{D}(\infty)$.

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

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

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

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

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

D. Then

$$\pm p^2 DE^2 \notin \mathscr{D}(\infty).$$

References

[1] J. W. S. Cassels, *Rational Quadratic Forms*, Academic Press, London 1978.
[2] A. G. Earnest and J. S. Hsia, *Spinor norms of local integral rotations II*, Pacific J. M 61 (1975), pp. 71–86, 115 (1984), pp. 493–494.
[3] D. G. James, *Indefinite quadratic forms of determinant* $\pm 2p$, Proc. Amer. Math. Soc (1969), pp. 214–218.
[4] M. Kneser, *Klassenzahlen indefiniter quadratischer Formen in drei oder mehr Veranderlic* Arch. Math. 7 (1956), pp. 323–332.
[5] O. T. O'Meara, *Introduction to Quadratic Forms*, Springer-Verlag, New York 1963.
[6] J. P. Serre, *A Course in Arithmetic*, Springer-Verlag, New York 1973.
[7] C. T. C. Wall, *On the orthogonal groups of unimodular quadratic forms*, Math. Ann. (1962), pp. 328–338.

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 (1(