PACIFIC JOURNAL OF MATHEMATICS
Vol. 80, No. 2, 1979

A WITT'S THEOREM FOR UNIMODULAR LATTICES

Y. C. LEE

Let K be a dyadic local field, $\mathfrak{o}$ its ring of integers, L a regular unimodular lattice over $\mathfrak{o}$. If x and y are vectors in L, we ask for necessary and sufficient conditions to map x isometrically to y. Trojan and James obtain conditions via a T-invariant when $\mathfrak{o}$ is 2-adic. Hsia uses characteristic sets and G-invariants for vectors and he solves the problem when $\mathfrak{o}$ is dyadic in general. We define here a new numerical invariant, the degree of a vector, which reflects more on the structure of L and the relationship between x, y and L. The Witt conditions will be stated in terms of this degree invariant.

1. Introduction. Let π be a prime element generating the maximal ideal of $\mathfrak{o}$ and let e be such that $2\mathfrak{o} = \pi^e\mathfrak{o}$. Let Q be a quadratic form on L, B its associated symmetric bilinear form. Then Q and B are connected by

$$Q(x + y) = Q(x) + Q(y) - B(x, y) .$$

The lattice L is unimodular simply means $B(L, L) = \mathfrak{o}$ and det L is a unit. The structure of unimodular lattices is well-known and can be found in O'Meara [7]. A vector v is primitive if $v \notin \pi L$. Hence v is primitive if and only if $B(v, L) = \mathfrak{o}$.

PROPOSITION 1. *Let v be a vector in a unimodular lattice L. Then $v \in \pi^k L$ if and only if $B(v, L) \subseteqq \pi^k\mathfrak{o}$.*

Proof. The necessity is trivial. Assume $B(v, L) \subseteqq \pi^k\mathfrak{o}$ and h is the highest power of π that divides v, that is, $v = \pi^h w$ for some primitive vector w. Hence $B(w, L) = \mathfrak{o}$ and $B(v, L) = B(\pi^h w, L) = \pi^h\mathfrak{o}$ and $h \geqq k$.

If $z \in L$ satisfies $\operatorname{ord} Q(z) \leqq \operatorname{ord} B(z, L)$, then the map σ_z given by

$$\sigma_z(v) = v - B(v, z)z/Q(z)$$

is an integral isometry known as the reflection of z. The group of integral isometries is denoted by $O(L)$. O'Meara and Pollak [8], [9] have shown that $O(L)$ is generated by reflections except in a few cases when the residue field $\mathfrak{o}/\pi\mathfrak{o}$ contains only two elements, and that in the exceptional cases one extra generator given by an

Eichler transform is needed. If i is a nonzero isotropic vector and z satisfies $B(i, z) = 0$ then an Eichler transform E_z^i is defined by:

$$E_z^i(v) = v + B(v, i)z - B(v, z)i - Q(z)B(v, i)i \, .$$

We say two vectors x and y are associated, denoted $x \sim y$ if there is a $\phi \in O(L)$ such that $\phi(x) = y$. For each k such that $e \geqq k \geqq 0$, let

$$L^{(-k)} = \{v \in L \colon Q(v) \in \pi^{-k}\mathfrak{o}\} \, .$$

Each $L^{(-k)}$ is invariant under the action of $O(L)$ and

$$L = L^{(-e)} \supseteqq \cdots \supseteqq L^{(-1)} \supseteqq L^{(0)} \, .$$

DEFINITION. The lattice L is said to have degree k if

$$L = \cdots = L^{(-k)} \neq L^{(-k+1)} \, .$$

The sublattice $L^{(0)}$ is called the even sublattice of L. A degree 0 lattice is simply called an even lattice.

2. The degree invariant.

DEFINITION. Let v be a primitive vector. The degree of v, $m(v)$, is given by $m(v) = \operatorname{ord} B(v, L^{(0)})$.

If d is the degree of L, then clearly $\pi^{[d/2]}L \subseteqq L^{(0)}$, where $[d/2]$ denotes the smallest integer greater than $d/2$. Consequently, $m(v) \leqq [d/2]$.

Furthermore, if v is a primitive vector with degree m and w is another primitive vector with $w - v \in \pi^m L$, then the degree of w is also m. For we have $w = v + \pi^m z$ and

$$\begin{aligned} B(w, L^{(0)}) &= B(v + \pi^m z, L^{(0)}) \\ &= B(v, L^{(0)}) + \pi^m B(z, L^{(0)}) \\ &= \pi^m \mathfrak{o} \, . \end{aligned}$$

3. Witt's theorem.

THEOREM. *Let x and y be primitive vectors such that $Q(x) = Q(y)$. Then x is associated to y if and only if $m(x) = m(y) = m$ and $y - x \in \pi^m L$.*

We remark that the condition $y - x \in \pi^m L$ expresses how close the vectors x and y must be. With the upperbounds calculated for m, this condition becomes quite appealing. Before proving the theorem we first set up an invariant which has its own importance.

DEFINITION. If a is an element of K, the quotient field of $\mathfrak{o}$, let

$$S_a = \{u \in L: Q(u) \equiv a \mod \mathfrak{o}\} .$$

DEFINITION. If v is a primitive vector of degree m, let

$$S_a(v) = B(v, u) \mod \pi^m \mathfrak{o}$$

where u is a vector in S_a.

Since $Q(\phi(u)) = Q(u)$ for any isometry ϕ, it is clear that S_a is invariant under $O(L)$. To show that $S_a(v)$ is well-defined, let u, u' be vectors in S_a. Then $Q(u) \equiv Q(u') \equiv a \mod \mathfrak{o}$, and

$$\begin{aligned} Q(u - u') &= Q(u) - Q(u') - B(u', u - u') \\ &\equiv 0 \mod \mathfrak{o} . \end{aligned}$$

Hence $u - u' \in L^{(0)}$ and

$$\begin{aligned} B(v, u) - B(v, u') &= B(v, u - u') \\ &\equiv 0 \mod \pi^m \mathfrak{o} . \end{aligned}$$

Since S_a is invariant under $O(L)$, we immediately obtain that if x and y are associated, then $S_a(x) = S_a(y)$.

Proof of theorem. Let x and y be associated vectors. Clearly $m(x) = m(y)$. For each nonempty S_a, we have

$$S_a(x) \equiv S_a(y) \mod \pi^m \mathfrak{o} .$$

Therefore,

$$B(y - x, u) \equiv 0 \mod \pi^m \mathfrak{o}$$

for any $u \in S_a$. Since the collection $\{S_a\}$ partitions L, this means

$$B(y - x, u) \equiv 0 \mod \pi^m \mathfrak{o}$$

for all $u \in L$. Proposition 1 shows that $y - x \in \pi^m L$.

It is convenient to collect that following two results.

PROPOSITION 2. *Let x and y be primitive vectors such that $Q(x) = Q(y)$ and $m(x) = m(y) = 0$. Then $x \sim y$.*

Proof. This is a direct application of Kneser's theorem [6].

PROPOSITION 3. *Let x and y be primitive vectors such that $Q(x) = Q(y)$ and $m(x) = m(y) = m$. Then $x \sim y$ provided one of the following holds*:

(i) $y - x \in \pi^m L$ *and* $\operatorname{ord} Q(y - x) = 2m$;

(ii) $y - x \in \pi^m L$ *and there is a vector* $u \in L^{(0)}$ *with* $\operatorname{ord} Q(u) = 0$ *and* $\operatorname{ord} B(x, u) = \operatorname{ord} B(y, u) = m$;

(iii) $y - x \in \pi^{m+1} L$ *and there is a vector* $u \in L^{(-1)} - L^{(0)}$ *with* $\operatorname{ord} B(x, u) = \operatorname{ord} B(y, u) = m$.

Proof. Let $z = \pi^{-m}(y - x)$.

(i) Since $Q(z)$ is a unit, the reflection σ_z is integral and sends x to y.

(ii) We may assume $\operatorname{ord} Q(z) > 0$. Let

$$z' = z + B(x, u)u/\pi^m Q(u) .$$

Then it is easily shown that $Q(z')$ is a unit. Hence $\sigma_{z'}$ and σ_u are integral reflections and $\sigma_{z'}, \sigma_u(x) = y$.

(iii) Again assume $\operatorname{ord} Q(z) > 0$. Let

$$z' = z + B(x, u)u/\pi^{m+1} Q(u) .$$

Then $\operatorname{ord} Q(z') = -1$. Hence $\sigma_{z'}$ is integral and $\sigma_{z'}\sigma_u(x) = y$.

Proof of theorem (continued). Let x and y be primitive vectors satisfying the conditions $Q(x) = Q(y)$, $m(x) = m(y) = m$ and $y - x \in \pi^m L$.

If $m = 0$, Proposition 2 settles the problem. Let $m \geqq 1$. We may further assume that $\operatorname{ord} Q(y - x) > 2m$, otherwise Proposition 3 (ii) already provides the necessary isometry. We proceed with the proof in a series of lemmas.

LEMMA 1. *If* $B(x, L^{(-1)}) = B(y, L^{(-1)}) = \pi^{m-1}\mathfrak{o}$, *then* $x \sim y$.

Proof. Since $B(x, L^{(0)}) = B(y, L^{(0)}) = \pi^m \mathfrak{o}$, we know that $L^{(-1)} - L^{(0)}$ is a nonempty set. Choose v and w from this set so that $\operatorname{ord} B(x, v) = \operatorname{ord} B(y, w) = m - 1$. Then one of the vectors $v, w, v + w$, which we denote by u, will satisfy $\operatorname{ord} B(x, u) = \operatorname{ord} B(y, u) = m - 1$. This vector u also lies in $L^{(-1)} - L^{(0)}$. Let $z = \pi^{-m}(y - x)$ and $z' = z + B(x, u)u/\pi^{m-1}Q(u)$. Then $\sigma_{z'}$ is an integral isometry and $\sigma_{z'}\sigma_u(x) = y$.

LEMMA 2. *If* $B(x, L^{(-2)}) = B(y, L^{(-2)}) = \pi^{m-1}\mathfrak{o}$ *and* $B(x, L^{(-1)}) = B(y, L^{(-1)}) = \pi^m \mathfrak{o}$, *then* $x \sim y$.

Proof. As in Lemma 1, we can choose a vector z from $L^{(-2)} -$

$L^{(-1)}$ such that $\operatorname{ord} B(x, z) = \operatorname{ord} B(y, z) = m - 1$. Then Proposition 3 (ii) can be applied with $u = \pi z$.

LEMMA 3. *Assume $B(x, L^{(-2)}) = B(y, L^{(-2)}) = \pi^m\mathfrak{o}$. If there is a vector $z \in L^{(-2)} - L^{(-1)}$, then $x \sim y$.*

Proof. There are vectors v and w in $L^{(0)}$ such that $\operatorname{ord} B(x, v) = \operatorname{ord} B(y, w) = m$. One of the three vectors $v, w, v + w$, which will be denoted by u, must satisfy $\operatorname{ord} B(x, u) = \operatorname{ord} B(y, u) = m$. If $\operatorname{ord} Q(u) = 0$, Proposition 3 (ii) can be used. Otherwise let $u' = u + \pi z$. Then $\operatorname{ord} Q(u') = 0$ and $\operatorname{ord} B(x, u') = \operatorname{ord} B(y, u') = m$. Hence Proposition 3 (ii) can again be used.

From here on we may assume that $B(x, L^{(-2)}) = B(y, L^{(-2)}) = \pi^m\mathfrak{o}$, and that there are no vectors u in L with $\operatorname{ord} Q(u) = -2$. This further means that there are no vectors u in L with $Q(u)$ having negative even orders. Hence the degree of L equals $-2h + 1$ for some positive integer h. By an earlier remark and Proposition 2, we may assume that $h > m > 1$.

LEMMA 4. *Under the above assumptions, the lattice L has one of the following decompositions*:

(i) $L = \mathfrak{o}v \perp M$ *if L is odd-dimensional,*

(ii) $L = (\mathfrak{o}v \oplus \mathfrak{o}w) \perp M$ *if L is even-dimensional,*

where $\operatorname{ord} Q(v) = -2h + 1$, $\operatorname{ord} Q(w) \geqq 1$, $B(v, w) = 1$ *and M is an even sublattice.*

Proof. (i) We can write $L = \mathfrak{o}v_1 \perp M_1$, where $\operatorname{ord} Q(v_1) = -2h + 1$. If M_1 is not even, then M_1 contains vectors u with $\operatorname{ord} Q(u)$ being some negative odd integer. By adding appropriate vectors av_1, $a \in \mathfrak{o}$, to these vectors, we can form a new decomposition $L = \mathfrak{o}v_2 \perp M_2$ with the degree of M_2 less than the degree of M_1. By induction we can obtain the desired decomposition.

(ii) Starting with a decomposition $L = (\mathfrak{o}v_1 \oplus \mathfrak{o}w_1) \perp M_1$, we can use v_1 to change M_1 until $L = (\mathfrak{o}v_2 \oplus \mathfrak{o}w_2) \perp M$, where M is even. Finally, since $\operatorname{ord} Q(w_2)$ is odd or greater than 0, we can use v_2 to change w_2 to obtain the desired decomposition.

LEMMA 5. *Let L be odd-dimensional. Then there exists an isometry ϕ such that $\phi(x) - y \in \pi^{m+1}L$. Hence $x \sim y$.*

Proof. Let $L = \mathfrak{o}v \perp M$ be given by Lemma 4. Write

$$x = av + \pi^m z, \quad y = bv + \pi^m z'$$

where z, z' are primitive vectors of M. Since

$$Q(x) - Q(y) = (a^2 - b^2)Q(v) + \pi^{2m}(Q(z) - Q(z')) = 0 ,$$

we have

$$(a^2 - b^2)Q(v) \equiv 0 \bmod \pi^{2m}\mathfrak{o}$$

so that

$$a^2 - b^2 \equiv 0 \bmod \pi^{2m+2h-1}\mathfrak{o} ,$$

and

$$a - b \equiv 0 \bmod \pi^{m+h}\mathfrak{o} .$$

Hence $\pi^{2m}(Q(z) - Q(z')) \equiv 0 \bmod \pi^{2m+1}\mathfrak{o}$ and

$$Q(z) - Q(z') \equiv 0 \bmod \pi\mathfrak{o} .$$

There exists a vector $w \in M$ with $B(w, z') = 1$. Let $u = z' + c\pi w$, so that $Q(u) = Q(z') + c\pi + c^2\pi^2 Q(w)$. The equation

$$Q(z') + c\pi + c^2\pi^2 Q(w) = Q(z)$$

can be solved for c by Hensel's lemma. Since $Q(u) = Q(z)$, $m(u) = m(z) = 0$, by Proposition 2 there is an isometry ϕ in $O(M)$ such that $\phi(z) = u$. Now $z - u \in \pi^{m+1}L$. By Proposition 3 (iii), $\phi(x) \sim y$ and so $x \sim y$.

LEMMA 6. *Let L be even-dimensional. Then $x \sim y$.*

Proof. Let $L = (\mathfrak{o}v \oplus \mathfrak{o}w) \perp M$ be given by Lemma 4. Write

$$x = \pi^m av + w + \pi^m z$$
$$y = \pi^m bv + \varepsilon w + \pi^m z' ,$$

where z and z' are in M and ε is a unit. Then

$$0 = Q(x) - Q(y) = \pi^{2m}(a^2 - b^2)Q(v) + \pi^m(a - b\varepsilon) + (1 - \varepsilon^2)Q(w) + \pi^{2m}(Q(z) - Q(z')) .$$

Using an argument similar to that used in Lemma 5, we show that $a - b \in \pi^h\mathfrak{o}$ and $1 - \varepsilon \in \pi^m\mathfrak{o}$. Hence for some $c \in \mathfrak{o}$,

$$\pi^m(a - b\varepsilon) = \pi^m(a - (a + \pi^h c)\varepsilon) \equiv \pi^m a(1 - \varepsilon) \bmod \pi^{2m+1}\mathfrak{o} .$$

If $\operatorname{ord}(1 - \varepsilon) \geqq m + 1$, then $\pi^m a(1 - \varepsilon) \equiv 0 \bmod \pi^{2m+1}\mathfrak{o}$. Hence $Q(z) - Q(z') = 0 \bmod \pi\mathfrak{o}$ and there is an isometry $\phi \in O(M)$ such that $\phi(z) - z \in \pi M$. Hence $\phi(x) - y \in \pi^{m+1}L$ and $\phi(x) \sim y$ by Proposition 3 (iii).

If $\operatorname{ord}(1-\varepsilon)=m$ we note that a and b must be simultaneously units or nonunits.

(1) Both a and b are units. Then $\operatorname{ord}\pi^m(a-b\varepsilon)=2m$. Hence $\operatorname{ord}(Q(z)-Q(z'))=0$, and at least one of $Q(z)$, $Q(z')$ is a unit. Without loss of generality, let $Q(z)$ be a unit. If $\operatorname{ord}B(z,z')\geqq 1$, then the vector $u=z+w$ fulfills the hypothesis of Proposition 3 (ii), hence $x\sim y$. Now let $\operatorname{ord}B(z,z')=0$.

(i) $\operatorname{ord}Q(z')\geqq 1$. There exists a vector $z''=z+\zeta z'$ such that ζ is a unit and $Q(z'')=Q(z')$. For this z'', we have $B(z'',M)=B(z',M)=\mathfrak{o}$. Hence there is an isometry $\phi\in O(M)$ with $\phi(z')=z''$. Proposition 3 (ii) can now be used on $\phi(x)$ and y, with $u=z$.

(ii) $\operatorname{ord}Q(z)=\operatorname{ord}Q(z')=0$. Since $Q(z)-Q(z')$ is not zero, the residue field $\mathfrak{o}/\pi\mathfrak{o}$ must possess more than two elements. And since $\operatorname{ord}B(x,w+\zeta z)=0$ for all units ζ, we can choose a unit ζ such that $\operatorname{ord}B(y,w+\zeta z)=0$ as well. Now Proposition 3 (ii) can be used with $u=w+\zeta z$.

(2) Both a and b are nonunits. Then $\operatorname{ord}a(1-\varepsilon)\geqq 2m+1$. Here $Q(z)-Q(z')\equiv 0 \bmod \pi\mathfrak{o}$. Hence there is an isometry $\phi\in O(M)$ such that $\phi(z)\equiv z' \bmod \pi M$. Now we can rewrite

$$x=\pi^{m+1}a'v+w+\pi^m z$$
$$y=\pi^{m+1}b'v+\varepsilon w+\pi^m z+\pi^{m+1}\bar{z}\ ,$$

where $\bar{z}\in M$. Since x and y are primitive, z must also be primitive. Hence there exists a primitive vector $z''\in M$ which decomposes M as:

$$M=(\mathfrak{o}z\oplus\mathfrak{o}z'')\perp M'\ .$$

If $\operatorname{ord}Q(z)\geqq 1$, we may choose z'' so that $\operatorname{ord}Q(z'')=0$. Hence the hypothesis of Proposition 3 (ii) is satisfied with $u=z''+w$. Assume now $\operatorname{ord}Q(z)=0$. If we can choose a vector z'' with $\operatorname{ord}Q(z'')=0$, we are again done. Otherwise we can choose a vector z'' with $Q(z'')=0$. Let $\gamma=(\varepsilon-1)/\pi^m$. Consider the Eichler transform $E^{z''}_{\gamma w}$ on x:

$$E^{z''}_{\gamma w}(x)=x+B(x,z'')\gamma w-B(x,\gamma w)z''-Q(\gamma w)B(x,z'')z''\ .$$

An easy calculation shows that

$$x-E^{z''}_{\gamma w}(x)\equiv \varepsilon w \bmod \pi^{m+1}L\ .$$

Hence

$$y-E^{z''}_{\gamma w}(x)\equiv 0 \bmod \pi^{m+1}L\ .$$

Proposition 3 (iii) can be applied to y and $E^{z''}_{\gamma w}(x)$, with $u=\pi^h v$.

REFERENCES

1. J. S. Hsia, *An invariant for integral equivalence*, Amer. J. Math., **93** (1971), 867–871.

2. ———, *Integral equivalence of vectors over depleted modular lattices on dyadic local fields*, Amer. J. Math., **90** (1968), 285–294.

3. ———, *Integral equivalence of vectors over local modular lattices*, Pacific J. Math., **23** (1967), 527–542.

4. ———, *Integral equivalence of vectors over local modular lattice, II*, Pacific J. Math., **31** (1969), 47–59.

5. D. G. James, *On Witt's theorem for unimodular quadratic forms, II*, Pacific J. Math., **33** (1970), 645–652.

6. M. Kneser, *Witt's Satz für quadratische Formen über lokalen Ringen*, Nach. der Akad. Wiss. Göttingen, II, Math-Phys. Klasse, Heft, **9** (1972), 195–205.

7. O. T. O'Meara, *Introduction to Quadratic Forms*, Springer Verlag, 1962.

8. O. T. O'Meara and B. Pollak, *Generation of local integral orthogonal groups*, Math. Zeit., **87** (1965), 385–400.

9. ———, *Generation of local integral orthogonal groups, II*, Math. Zeit., **93** (1966), 171–188.

10. A. Trojan, *The integral extension of isometries of quadratic forms over local fields*, Canad. J. Math., **18** (1966), 920–942.

Received August 31, 1977.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY
CAMBRIDGE, MA 02139