Can. J. Math., Vol. XXIX, No. 5, 1977, pp. 928–936

WITTS THEOREM FOR QUADRATIC FORMS OVER NON-DYADIC DISCRETE VALUATION RINGS

DAVID MORDECAI COHEN

Introduction. Let R be a discrete valuation ring, with maximal ideal pR, such that $\frac{1}{2} \in R$. Let L be a finitely generated R-module and $B : L \times L \rightarrow R$ a non-degenerate symmetric bilinear form. The module L is called a *quadratic module*. For notational convenience we shall write $xy = B(x, y)$. Let $O(L)$ be the group of isometries, i.e. all R-linear isomorphisms $\varphi : L \rightarrow L$ such that $B(\varphi(x), \varphi(y)) = B(x, y)$. Given two submodules M and N of L and an isometry $\tau : M \rightarrow N$ defined on M, we shall find necessary and sufficient conditions for τ to extend to L, i.e. there exists $\varphi \in O(L)$ such that $\varphi \restriction M = \tau$.

Our starting point is the observation that when L is unimodular (i.e. the form $B : L \times L \rightarrow R$ induces an isomorphism $L \simeq \mathrm{Hom}_R(L, R)$), our theorem can be proved by imitating the proof of Witt's theorem for L/pL over the field R/pR. We are therefore led to define, for an arbitrary quadratic module L, a family of invariant submodules L_j such that $L = \lim_{\leftarrow} L/L_j$, and the induced bilinear forms $\bar{B} : L/L_j \times L/L_j \rightarrow R/p^j$ are non-degenerate. Since the "forms" L/L_j are non-degenerate, the submodules L_j are in some sense more "natural" for the study of quadratic forms than the usual filtration, p^jL. Using the L_j we define a family of normal subgroups $O_j(L)$ which form a neighborhood system of the identity of $O(L)$ in the usual topology.

For L/L_j we show that if $M + L_{j-1} = N + L_{j-1}$ then only a length and a primality condition are needed to give an isometry $\varphi \in O(L)$ such that $\varphi(M) + L_j = N + L_j$. Since $L = \lim L/L_j$ we use a limit argument to prove our theorem for L.

To illustrate the techniques involved we first prove the theorem for the case of two vectors x and y with $x^2 = y^2$. This case is originally due to James and Rosenzweig [**1**]. The main theorem generalizes a theorem of Band [**2**].

We will first assume that R is complete. The non complete case follows by an easy argument (cf. [**1**] and [**5**]).

Section I. In this section we discuss the topologies on L and $O(L)$ which are induced by the valuation on R.

Definition. For $x \in L$, we define $\mathrm{ord}\,(x) = \min\,\{\mathrm{ord}_R\,(xy) |$ for all $y \in L\}$.

Clearly,

Received August 10, 1976 and in revised form, April 20, 1977.

i) ord (ax) = ord (a) + ord (x) for any $a \in R$
ii) ord $(x + y) \geqq \min \{\text{ord}(x), \text{ord}(y)\}$
iii) ord $(x) \leqq$ ord (x^2)
iv) If $L = L_1 \perp L_2$ and $x = x_1 + x_2, x_i \in L_i$, then ord $(x) = \min \{\text{ord}_{L_i}(x_i)\}$

By selecting a vector x_1, such that ord (x_1) is a minimum, we can decompose $L = \langle x_1 \rangle \perp L_1$. By induction, we can prove that L is an orthogonal sum of lines. Therefore by property iv) above it follows that for a large integer N, if ord $(x) > N$, then $x \in pL$.

We now define the submodules L_j.

Definition. $L_j = \{x \in L | \text{ord}(x) \geqq j\}$

Clearly then,
(1.1) $L_j \supset L_{j+1} \supset pL$ for all j,
(1.2) $L_j \subset pL$ for all $j > N$,
(1.3) $L_{j+1} = pL_j \quad j > N$.

From properties (1.1) and (1.3) it follows that the topology on L induced by the L_j agrees with the p-adic topology. Therefore $L = \lim_{\leftarrow} L/L_j$. Since for any isometry $\varphi \in O(L)$, ord (x) = ord $(\varphi(x))$, the submodule L_j is invariant, i.e. $\varphi(L_j) = L_j$. Clearly the induced forms $B : L/L_j \times L/L_j \rightarrow R/p^j$ are non-degenerate.

The orthogonal group $O(L)$ has a natural p-adic topology inherited from R in which it is complete.

Definition. $O_j(L) = \{\varphi \in O(L) |$ for all $x \in L, \varphi(x) \equiv x (\text{mod } L_j)\}$.

Since the L_j are invariant under the action of $O(L)$, the $O_j(L)$ are normal subgroups. Since $L = \lim_{\leftarrow} L/L_j$, the $O_j(L)$ satisfy
(1.4) $O_j(L) \supset O_{j+1}(L)$
(1.5) $\bigcap O_j(L) = \{1\}$.
The $O_j(L)$ therefore form a neighborhood of the identity in $O(L)$.

We now define some special types of vectors.

Definition. $v \in \mathscr{L}$ is *orthogonal* if ord (v) = ord (v^2), or equivalently if $L = \{v\} \perp K$.

If v is orthogonal of order j, then for any $x \in L$, ord $(xv) \geqq$ ord (v^2) and so $(^{vx}/v^2)v \in L_j$. Therefore the reflection about v, defined as usual by setting $\sigma_v(x) = x - 2\ (^{vx}/v^2)v$ [**4**], is an isometry of L. Since $\sigma_v{}^2 = 1$, if $v \equiv w (\text{mod } L_k)$ and w is also orthogonal then $\sigma_w(x) \equiv \sigma_v(v)$ (mod L_k), $\sigma_v\sigma_w(x) \equiv x$ (mod L_k) and $\sigma_v\sigma_w \in O_k(L)$.

Definition. A vector $v \in L$ is called *simple* if there exists a vector w, necessarily also simple, such that ord (v) = ord (vw) = ord (w).

Since ord $(pwv) >$ ord $(wv) \geqq$ ord (w), a simple vector v is primitive (i.e. $v \notin pL$). If v is simple, and ord $(z) >$ ord (v), then ord $((v + z)w) =$ ord (vw) $=$ ord $(w) =$ ord $(v + z)$ and $v + z$ is also simple. If v is orthogonal then ord $(v) =$ ord (v^2) and v is simple. Therefore simple vectors are a generalization of orthogonal vectors. Our interest in them is further explained by the following lemma.

LEMMA 1. *Let $x \in L$ be primitive. Then there exists v and $z \in L$ such that $x = pz + v$ and either v is orthogonal, or v is simple and isotropic* (i.e. $v^2 = 0$).

Proof. Using an orthogonal basis of L, we can write $x = pz_1 + u$ where u is the sum of mutually perpendicular orthogonal vectors. Such a vector is simple. If u is orthogonal then set $v = u$.

If ord $(u^2) >$ ord (u) then choose $w \in L$ such that ord $(u) =$ ord $(wu) =$ ord (w). Using Hensel's lemma we can find an $a \in R$ such that $(apw + u)^2 = 0$. Since ord $(apw) >$ ord $(w) =$ ord (u), $apw + u$ is simple. Then set $z = z_1 - apw$ and $v = apw + u$.

If v is a simple vector for which ord $(v^2) >$ ord (v) then using Hensel's lemma we can find a simple isotropic vector v^* such that ord $(v) =$ ord $(vv^*) =$ ord (v^*). Therefore we have an isotropic vector v^* such that $L = \{v, v^*\} \perp K$.

Definition. The *exponent* of a vector x modulo L_k will denote the greatest integer t for which there is a $z \in L$ such that

$$x \equiv p^t z \pmod{L_k}.$$

If $x \notin pL + L_k$ then x has exponent zero modulo L_k and is called *primitive* modulo L_k.

Note that if t_k is the exponent of x modulo L_k then $t_k \geqq t_{k+1}$. Suppose that $x \in p^t L$ and $x \notin p^{t+1}L$, i.e. x has exponent t in L. Suppose that N is sufficiently large so that for all $j > N$, $L_j \subset pL$. Then $L_{j+t} \subset p^{t+1}L$ and $x \notin p^{t+1}L + L_{j+t}$. Therefore for all $k > N + t$ the exponent of x modulo L_k equals t. In particular if x is primitive in L and k is large, then x is primitive modulo L_k. Conversely if x is primitive modulo L_k, for any k, then $x \notin pL + L_k$ and x is primitive in L. If v is simple and ord $(v) < k$, then v is primitive modulo L_k.

LEMMA 2. *If* ord $(x) = k$ *and x is primitive modulo L_{k+1}, then x is simple.*

Proof. Write $x = pz + v$ for some simple vector v. Since x is primitive modulo L_{k+1}, ord $(v) \leqq k$. Choose a simple vector w such that ord $(v) =$ ord $(vw) =$ ord (w). Then

$$k \leqq \text{ord } (xw) = \text{ord } (pzw + vw) = \text{ord } (vw) = \text{ord } (v) \leqq k$$

Therefore ord $(xw) =$ ord $(w) = k$, and x is simple.

COROLLARY. *If v is simple,* ord $(v) \leqq k$, $v \equiv w \pmod{L_k}$ *and w is primitive modulo L_{k+1}, then w is simple and* ord $(v) =$ ord (w).

https://doi.org/10.4153/CJM-1977-093-7 Published online by Cambridge University Press

Proof. If ord $(v) < k$, then $w = v + z$ where ord $(z) \geqq k >$ ord (v). Then it is clear that w is simple and that ord $(w) =$ ord (v). If ord $(v) = k$, then ord $(w) = k$ and the lemma applies.

If $x \equiv p^t x_1 \equiv p^t x_2 \pmod{L_k}$ then $p^t(x_1 - x_2) \in L_k$, $x_1 \equiv x_2 \pmod{L_{k-t}}$ and $x_1^2 \equiv x_2^2 \pmod{p^{k-t}}$. Therefore even though the vector x_1 is not unique its length modulo p^{k-t} is an invariant of x. Thus we make the following definition.

Definition. For x and $y \in L$, we shall write $x \approx y \pmod{L_k}$ if

1) x and y have the same exponent t modulo L_k, and

2) given any x_1 and y_1 such that $x \equiv p^t x_1$ and $y \equiv p^t y_1 \pmod{L_k}$ then $x_1^2 \equiv y_1^2 \pmod{p^{k-t}}$.

Remark 1. $x \approx y \pmod{L_k}$ does not necessarily imply that $x \approx y \pmod{L_{k-1}}$. However if the exponent of x and y modulo L_k equals the exponent of x and y modulo L_{k-1} then a fortiori $x \approx y \pmod{L_k}$ does imply that $x \approx y \pmod{L_{k-1}}$. Since for large enough k, the exponent of x and y modulo L_k equals the exponent of x and y in L, if $x^2 = y^2$ then for all sufficiently large k, $x \approx y \pmod{L_k}$.

LEMMA 3. *The congruence relation* $x \approx y \pmod{L_k}$ *satisfies the following properties.*

1) *If* $\varphi \in O(L)$, *then for all* k, $x \approx \varphi(x) \pmod{L_k}$.

2) *If* $x \equiv y \pmod{L_k}$, *then* $x \approx y \pmod{L_k}$

3) *If* $px \approx py \pmod{L_k}$, *then* $x \approx y \pmod{L_{k-1}}$

4) *If* v *is simple,* ord $(v) \leqq k$, *and* $v \equiv w \pmod{L_k}$ *then* $pz + v \approx pz + w \pmod{L_{k+1}}$ *implies that* w *is simple and that* $v \approx w \pmod{L_{k+1}}$.

Proof. Only (4) is not immediate. Since ord $(v) \leqq k$, $pz + v$ and $pz + w$, and therefore w are all primitive modulo L_{k+1}. By the corollary to Lemma 2, since $v \equiv w \pmod{L_k}$, w is simple. Finally

$$\begin{aligned} 0 \equiv (pz + w)^2 - (pz + v)^2 &\equiv 2pz(v - w) + (w^2 - v^2) \\ &\equiv w^2 - v^2 \pmod{p^{k+1}}. \end{aligned}$$

In Section 2 we shall prove that if $x \approx y \pmod{L_k}$ for all k, then there is an isometry $\varphi \in O(L)$ such that $\varphi(x) = y$. By Remark 1, if $x^2 = y^2$ and x and y have the same exponent in L, then for all large k, $x \approx y \pmod{L_k}$. Therefore the theorem will involve only a finite number of k. In particular if L is unimodular, then $L_k = p^k L$ and for primitive vectors x and y we will get Witt's original theorem, i.e. $x^2 = y^2$ if and only if there exists $\varphi \in O(L)$, $\varphi(x) = y$.

Section 2. We now prove that if $x \approx y \pmod{L_k}$ for all k, then there is an isometry $\varphi \in O(L)$ such that $\varphi(x) = y$. We prove this first for simple vectors and then use the properties of Lemma 3 to extend it to all x and y in L.

LEMMA 4. *Let* v *be a simple vector such that* ord $(v) \leqq k$ *and either* v *is orthogonal or* v *is isotropic. Then for any* $w \in L$ *such that*

i) $v \equiv w \pmod{L_k}$
ii) $v \approx w \pmod{L_{k+1}}$
there exists an isometry $\varphi \in O(L)$ *such that* $\varphi(v) \equiv w \pmod{L_{k+1}}$.

Proof. By Lemma 3, we already know that w is simple. Let $u = v - u$. Then $u \in L_k$. If u were orthogonal, then $\sigma_u \in O_k(L)$.

Since $u = v - w$, and $v^2 \equiv w^2 \pmod{p^{k+1}}$,

$$\sigma_u(v) = v - [{}^{2(v-w)v/}(v - w)^2](v - w) \equiv v - (v - w) \equiv w \pmod{L_{k+1}}.$$

Then $\varphi = \sigma_u$ is the desired isometry.

Therefore we may assume that $\text{ord}\,(u^2) > \text{ord}\,(u) \geqq k$. Since $v^2 = (w + u)^2 \equiv w^2 + 2wu \pmod{p^{k+1}}$,

$$(2.1)\quad wu \equiv vu \equiv u^2 \equiv 0 \pmod{p^{k+1}}.$$

If v is orthogonal, then $\text{ord}\,(w) = \text{ord}\,(v) = \text{ord}\,(v^2) = \text{ord}\,(w^2)$ and w is orthogonal. Similarly it follows from (2.1) that $v + w = 2w + u$ is also orthogonal. Following the proof of Witt's theorem for a field, $\sigma_{v+w}(v) \equiv -w \pmod{L_{k+1}}$ and $\sigma_w\sigma_{v+w}(v) \equiv w \pmod{L_{k+1}}$. Since $2w \equiv v + w \pmod{L_k}$, $\sigma_{2w}\sigma_{v+w} \in O_k(L)$. Then let $\varphi = \sigma_w\sigma_{v+w}$.

Therefore we may assume that v is isotropic. Then neither w nor $v + w$ is orthogonal and there are no reflections σ_w or σ_{v+w}. Assume though that there is a simple isotropic vector v^* such that

$$(2.2)\quad L = \{v, v^*\} \perp K \quad \text{and} \quad L = \{w, v^*\} \perp K'.$$

Then $v - v^*$, and $w - v^*$ are both orthogonal and $\sigma_{v-v^*}(v) \equiv v^* \pmod{L_{k+1}}$ and $\sigma_{w-v^*}(v^*) \equiv w \pmod{L_{k+1}}$. Since $v - v^* \equiv w - v^* \pmod{L_k}$, $\varphi = \sigma_{v-v^*}\sigma_{w-v^*} \in O_k(L)$ and $\varphi(v) \equiv w \pmod{L_{k+1}}$.

We shall now show that such a v^* exists. Choose any simple isotropic vector $\tilde{v}$ such that $L = \{v, \tilde{v}\} \perp K$. If $\text{ord}\,(\tilde{v}w) \leqq k$, then $\text{ord}\,(\tilde{v}w) = \text{ord}\,(\tilde{v}v + \tilde{v}u) = \text{ord}\,(\tilde{v}v) = \text{ord}\,(v) = \text{ord}\,(w)$ and $v^* = \tilde{v}$ is the desired vector. If $\text{ord}\,(\tilde{v}w) > k$, then find $a, b \in R$ and $w_1 \in K$ so that $w = av + b\tilde{v} + w_1$. Since $\text{ord}\,(vw) > k$, and $\text{ord}\,(\tilde{v}w) > k$, $av + b\tilde{v} \in L_{k+1}$. Therefore $w \equiv w_1 \pmod{L_{k+1}}$ and w_1 is thus a simple vector of order k in K. Choose a simple isotropic vector $\tilde{w}$ in K such that $K = \{w_1, \tilde{w}\} \perp K''$. Then let $v^* = \tilde{v} + \tilde{w}$. Since $\text{ord}\,(v^*w) = \text{ord}\,(\tilde{w}w_1) = k$, v^* is the desired vector.

COROLLARY. *Let x and $y \in L$. If*
1) $x \equiv y \pmod{L_k}$, *and*
2) $x \approx y \pmod{L_{k+1}}$
then there exists $\varphi \in O(L)$, *such that* $\varphi(x) \equiv y \pmod{L_{k+1}}$.
Moreover, if x is primitive modulo L_{k+1}, we can choose $\varphi \in O_k(L)$.

Proof. By (3) of Lemma 3, we may assume that x is primitive modulo L_{k+1}. Write $x = pz + v$ where v is simple, $\text{ord}\,(v) \leqq k$, and v is either orthogonal or isotropic. If $w = v + y - x$, then $y = pz + w$. Since $x \equiv y \pmod{L_k}$, $v \equiv w$

(mod L_k). By Lemma 3, $v \approx w$ (mod L_{k+1}). By Lemma 4, there is an isometry $\varphi \in O_k(L)$, such that $\varphi(v) \equiv w$ (mod L_{k+1}). Since $\varphi \in O_k(L)$, $\varphi(pz) \equiv pz$ (mod L_{k+1}) and is the desired isometry.

For $x, y \in L$ we shall write $x \approx y$ if there is $\varphi \in O(L)$ such that $\varphi(x) = y$.

THEOREM 1. *Given $x, y \in L$. Then $x \approx y$ if and only if*

(2.3) $x \approx y$ (mod L_k) *for all k.*

Proof. By dividing x by p, we may assume that x and y are both primitive in L. We shall construct a convergent sequence of isometries φ_k, such that $\varphi_k(x) \equiv y$ (mod L_k). Then for $\varphi = \lim_{\rightarrow} \varphi_k$, $\varphi(x) = y$.

The classical Witt's theorem for fields gives φ_1 such that $\varphi_1(x) = y$ (mod L_1).

Assume that we have φ_k, such that $\varphi_k(x) \equiv y$ (mod L_k). Since φ_k is an isometry, by Lemma 3, $\varphi_k(x) \approx y$ (mod L_{k+1}). By the above corollary, there is a $\chi \in O(L)$, such that $\chi\varphi_k(x) \equiv y$ (mod L_{k+1}). Let $\varphi_{k+1} = \chi\varphi_k$. For large k, x is primitive modulo L_k, and we can choose $\chi \in O_k(L)$, and, thus, the sequence converges.

Remark 2. If $x^2 = y^2$ and $x \approx y$ (mod L_k), for large enough k, then automatically $x \approx y$ (mod L_j) for all $j > k$. So if we add the to theorem the hypothesis that $x^2 = y^2$, we need (2.3) for only a finite number of k. Also, by Remark 1, we would then need (2.3) for only those k for which the primality of x or y changes in passing from L_{k-1} to L_k. This theorem gives Rosenzweig's Theorem.

Section 3. We now extend the results of Section 2 to arbitrary submodules. We first generalize Lemma 1.

Definition. A set of simple vectors $v_1, \ldots, v_n$ will be called *completely orthogonal* if

1) each v_i is either orthogonal or isotropic, and

2) $L = \{v_1\} \perp \ldots \perp \{v_r\} \perp \{v_{r+1}, v^*_{r+1}\} \perp \ldots \perp \{v_n, v_n^*\} \perp K$ for some simple isotropic vectors v_i^*.

Note. ord $(a_1v_1 + \ldots + a_nv_n) = \min\{\text{ord}(a_iv_i)\}$.

For convenience we shall extend the definition of simple vector to allow some of the v_i to be the zero vector.

LEMMA 5. *Every submodule M has a basis $pz_1 + v_1, \ldots, pz_n + v_n$ where the v_i are completely orthogonal simple vectors.*

Proof. If M contains any vector $y = pz + v$ where v is orthogonal, then ord (yv) = ord $(pzv + v^2)$ = ord (v^2) = ord (v). Thus for any $x \in M$, $x - (xv/yv)y \in M$. We can then write $L = \{v\} \perp K$, and $M = \{pz + v\} \oplus M'$ where $M' \subset K$, and can then proceed by induction. Therefore assume that M contains no $y = pz + v$ with v orthogonal.

Choose a simple vector $w \in M + pL$ whose order is maximal, i.e. if v_j is simple and $v_j \in M + pL$ then ord $(w) \geqq$ ord (v_j). Then $M = \{pz + w\} \oplus M'$ for some $z \in L$.

By induction on the dimension of M we have a basis $pz + w, pz_2 + v_2, \ldots, pz_n + v_n$. of M where the v_j are simple vectors completely orthogonal. Then ord $(wv_j) >$ ord (v_j). Otherwise, ord $(w) \geqq$ ord $(v_j) =$ ord $(wv_j) \geqq$ ord (w), and $w + v_j$ would be orthogonal.

Since $v_2, \ldots, v_n$ are completely orthogonal we can write

$$L = \{v_2, v_2^*\} \perp \ldots \perp \{v_n, v_n^*\} \perp K, \quad v_i^* \text{ isotropic}$$

and

$$w = a_2v_2 + \ldots + a_nv_n + b_2v_2^* + \ldots + b_nv_n^* + v', \quad v' \in K.$$

Since ord $(wv_j) >$ ord (v_j), p divides b_j. Therefore

$$pz + w - a_2(pz_2 + v_2) - \ldots - a_n(pz_n + v_n) = pz' + v'.$$

LEMMA 6. *If $v_1, \ldots, v_n$ are simple isotropic vectors, completely orthogonal,* ord $(v_i) \leqq k$, *and* ord $(a_2v_2 + \ldots + a_nv_n) \geqq k$ $a_i \in R$, *then there exists* $\varphi \in O_k(L)$ *such that*

$$\varphi(v_1) = v_1 + a_2v_2 + \ldots + a_nv_n$$
$$\varphi(v_j) = v_j \quad \text{for } j \neq 1.$$

Proof. Choose simple isotropic vectors v_i^* such that $L = \{v_1, v_1^*\} \perp \ldots \perp \{v_n, v_n^*\} \perp K$. Then define $\varphi \in O(L)$ by $\varphi(v_1^*) = v_1^*$ and $\varphi(v_j^*) = v_j^* - (a_jv_jv_j^*/v_1v_1^*)v_1^*$ and $\varphi|K =$ identity. Since $(a_jv_jv_j^*/v_1v_1^*)v_1^* \in L_k$, $\varphi \in O_k(L)$.

LEMMA 7. *Let $v_1, \ldots, v_n$ be simple vectors completely orthogonal,* ord $(v_i) \leqq k$. *Let w_j be simple vectors such that*

1) $v_j \equiv w_j \pmod{L_k}$.

2) *For any* $a_j \in R$, $\sum_1^n a_jv_j \approx \sum_j^n a_jw_j \pmod{L_{k+1}}$.

Then there is an isometry $\varphi \in O_k(L)$ *such that* $\varphi(v_j) \equiv w_j \pmod{L_{k+1}}$.

Proof. Suppose that v_1 is orthogonal. By Lemma 4 there is an isometry $\psi \in O_k(L)$ such that $\psi(v_1) \equiv w_1 \pmod{L_{k+1}}$. By properties (1) and (2) of Lemma 2,

$$\textstyle\sum_1^n a_j\psi(v_j) \approx \sum_1^n a_jv_j \approx \sum_1^n a_jw_j \approx a_1\psi(v_1) + \sum_2^n a_jw_j \pmod{L_{k+1}}.$$

Since $\psi \in O_k(L)$, we may assume that $v_1 = w_1$.

Write $L = \{v_1\} \perp K$. Let $w_j' = w_j - (w_jv_1/v_1^2)v_1$. Then $w_j' \in K$, and $w_j \equiv w_j' \pmod{L_{k+1}}$. By property (2) of Lemma 3 we can complete the proof by induction.

Suppose that all the v_i are isotropic. By induction assume that $v_2 = w_2$, $\ldots, v_n = w_n$. Choose simple isotropic v_i^* such that

$$L = \{v_2, v_2^*\} \perp \ldots \perp \{v_n, v_n^*\} \perp K$$

https://doi.org/10.4153/CJM-1977-093-7 Published online by Cambridge University Press

and

$$w_1 = a_2v_2 + b_2v_2^* + \ldots + a_nv_n + b_nv_n^* + w,\ w \in K.$$

By Condition 2 above $w_1v_j \equiv v_1v_j \equiv 0 \pmod{p^{k+1}}$. Thus $b_jv_j^* \in L_{k+1}$, and $w_1 \equiv a_2v_2 + \ldots + a_nv_n + w \pmod{L_{k+1}}$. Since $w_1 \equiv v_1 \pmod{L_k}$ and the v_i are completely orthogonal each $a_jv_j \in L_k$, and $w \equiv v_1 \pmod{L_k}$.

By Lemma 3, Condition 2, and Lemma 6,

$$w \approx w_1 - a_2v_2 - \ldots - a_nv_n \approx v_1 - a_2v_2 - \ldots - a_nv_n \approx v_1 \pmod{L_{k+1}}.$$

Therefore by Lemma 4 applied to w and v_1 and K, there is an isometry $\psi \in O_k(L)$ such that $\psi(w) \equiv v_1 \pmod{L_{k+1}}$ and such that $\psi(w_1) \equiv a_2v_2 + \ldots + a_nv_n + v_1 \pmod{L_{k+1}}$. Now Lemma 6 completes the proof.

COROLLARY. *Let M and N be submodules of L. Let $\chi : M \rightarrow N$ be a linear transformation such that for all $x \in M$,*

1) $\chi(x) \equiv x \quad \pmod{L_k}$

2) $\chi(x) \approx x \quad \pmod{L_{k+1}}$.

Suppose that M has a basis $x_1, \ldots, x_n$ such that each x_j is primitive modulo L_{k+1}. Then there is an isometry $\varphi \in O_K(L)$ such that

$$\varphi(x) \equiv \chi(x) \quad \pmod{L_{k+1}}.$$

Proof. Let $x_i = pz_i + v_i$ be a basis of M such that ord $(v_i) \leqq k$. Let $w_i = \chi(x_i) - pz_i$. Then $w_i \equiv v_i \pmod{L_k}$.

For any $x = pz + v \in M$, if $w = \chi(x) - pz$, then $v \equiv w \pmod{L_k}$. Since $pz + v \approx pz + w \pmod{L_{k+1}}$, by Lemma 3, $v \approx w \pmod{L_{k+1}}$.

Therefore the v_i and w_i satisfy the conditions of the lemma, and there is an isometry $\varphi \in O_k(L)$ such that $\varphi(v_i) \equiv w_i \pmod{L_{k+1}}$. Therefore $\varphi(x_i) \equiv \varphi(pz_i + v_i) \equiv pz_i + w_i \equiv \chi(x_i) \pmod{L_{k+1}}$.

LEMMA 8. *Let M and N be submodules of L and $\chi : M \rightarrow N$ a linear transformation such that for all $x \in M$,*

1) $\chi(x) \equiv x \quad \pmod{L_k}$

2) $\chi(x) \approx x \quad \pmod{L_{k+1}}$.

Then there is an isometry $\varphi \in O(L)$ such that

$$\varphi(x) \equiv \chi(x) \quad \pmod{L_{k+1}}.$$

Proof. We shall show that there is an isometry $\psi \in O(L)$ such that if $x \in M$ is imprimitive modulo L_{k+1}, then

$$\psi(x) \equiv \chi(x) \pmod{L_{k+1}}.$$

We can then apply the corollary to Lemma 7 to find an isometry $\psi' \in O_k(L)$ such that $\psi'\psi(x) \equiv \chi(x) \pmod{L_{k+1}}$ for all $x \in M$ primitive modulo L_{k+1}. Since $\psi' \in O_k(L)$, if x is imprimitive modulo L_{k+1}, then $\psi'\psi(x) \equiv \chi(x) \pmod{L_{k+1}}$, and the lemma would be proved.

We shall use induction to construct ψ. Assume that the lemma is true for $k - 1$.

https://doi.org/10.4153/CJM-1977-093-7 Published online by Cambridge University Press

Using Lemma 5, choose a basis $x_1, \ldots, x_n$ of M. Suppose that for $i \leqq s$, $x_i = pz_i + v_i$ and ord $(v_i) \leqq k$, and that for $i > s$, $x_i \equiv pz_i \pmod{L_{k+1}}$.

Let M' be the submodule of L generated by $x_1, \ldots, x_s, z_{s+1}, \ldots, z_n$. Choose a basis $x_1', \ldots, x_r'$ of M'. For each x_i' choose a vector u_i in M such that $px_i' \equiv u_i \pmod{L_{k+1}}$. Since $\chi(u_i) \approx px_i' \pmod{L_{k+1}}$, there is a y_i' in L such that $\chi(u_i) \approx py_i' \pmod{L_{k+1}}$. Now define a linear transformation χ' on M' by setting, for each x_i', $\chi'(x_i') = y_i'$. Then for any $x' \in M'$ if $px' \equiv x$ (mod L_{k+1}) then $p\chi'(x') \equiv \chi(x) \pmod{L_{k+1}}$. The key fact is that although χ is not an isometry, if $x \equiv u \pmod{L_{k+1}}$ where x and u are elements of M, then $\chi(x) \equiv \chi(u) \pmod{L_{k+1}}$. Therefore for any $x' \in M'$, $p\chi'(x') \approx \chi(x) \approx x \approx px'$ (mod L_{k+1}), and so $\chi'(x') \approx x' \pmod{L_k}$.

Thus M' and χ' satisfy the hypotheses of the lemma for $k - 1$. By induction there is an isometry $\psi \in O(L)$ such that $\psi(x') \equiv \chi'(x') \pmod{L_k}$. If $x \in M$ is imprimitive, choose $x' \in M'$ such that $px' \equiv x \pmod{L_{k+1}}$. Then $\psi(x) \equiv \psi(px') \equiv p\psi(x') \equiv p\chi'(x') \equiv \chi(x) \pmod{L_{k+1}}$. Thus ψ is desired isometry and the lemma is proved.

THEOREM. *Let M and N be submodules of L, and $\tau : M \to N$ an isometry defined on M. Then τ extends to an isometry of L if and only if $\tau(x) \approx x$ for all $x \in M$.*

Proof. By Theorem 1, that condition is equivalent to $\tau(x) \approx x \pmod{L_k}$ for all k.

We shall construct a convergent sequence of isometries $\varphi_k \in O(L)$ such that $\varphi_k(x) \equiv \tau(x) \pmod{L_k}$. Then for $\varphi = \lim \varphi_k$, $\varphi(x) = \tau(x)$.

By the classical Witt's theorem for fields there is an isometry $\varphi_1 \in O(L)$ such that $\varphi_1(x) \equiv \tau(x) \pmod{L_1}$.

Assume that we have an isometry φ_k such that $\varphi_k(x) \equiv \tau(x) \pmod{L_k}$. Then $\varphi_k(x) \approx x \approx \tau(x) \pmod{L_{k+1}}$ by Lemma 3. Therefore by Lemma 8, we have $\psi \in O(L)$ such that $\psi\varphi_k(x) \equiv \chi(x) \pmod{L_{k+1}}$. Let $\varphi_{k+1} = \psi\, \varphi_k$.

For large enough k, M will satisfy the conditions of the corollary to Lemma 7. Thus for large enough k, $\varphi_{k+1} \in \varphi_k O_k(L)$, and so the sequence φ_k converges.

I would like to thank Professor N. C. Ankeny for the encouragement and guidence he has given me while writing this paper.

REFERENCES

1. D. G. James and S. Rosenzweig, *Associated vectors in lattices over valuation rings*, Amer. J. Math. *90* (1968), 295–307.
2. M. Band, *On the integral extension of quadratic forms over local fields*, Can. J. Math. *22* (1970), 297–307.
3. Allen Trojan, *The integral extension of isometries of quadratic forms*, Can. J. Math. *18* (1966), 920–942.
4. O. T. O'Meara, *Introduction to quadratic forms* (Springer-Verlag, 1971).
5. C. L. Siegel, *Equivalence of quadratic forms*, Amer. J. Math. *63* (1941), 658–680.

University of California,
Irvine, California