Can. J. Math., Vol. XXX, No. 3, 1978, pp. 499–511

A WITT THEOREM FOR NON-DEFECTIVE LATTICES

KARL A. MORIN-STROM

In [**10**], Witt laid the foundation for the study of quadratic forms over fields. Suppose Q is a quadratic form defined on a finite dimensional vector space V over a field of characteristic not equal to 2. Witt showed that non-zero vectors x and y in V satisfying $Q(x) = Q(y)$ can be mapped into each other via an isometry of the vector space V. More generally, if $\tau : W \to W'$ is an isometry between subspaces of V, then τ extends to an isometry φ of V. In this paper we are concerned with analogous results for modules over discrete valuation rings. A module with a quadratic form on it is called a *lattice*. Corresponding to Witt's main theorem for spaces, a fundamental problem in the study of lattices is to determine necessary and sufficient conditions for an isometry between two sublattices to extend to an isometry of the whole lattice.

In this paper we use a result of Kneser [**6**] to obtain the general Witt theorem for non-defective lattices over discrete valuation rings. Non-defective lattices include all lattices over non-dyadic rings as well as lattices which are "nice", in a well-defined sense, over dyadic rings and rings of characteristic 2.

1. Introduction. Throughout this paper, $\mathfrak{O}$ is a discrete valuation ring with prime ideal $\mathfrak{p} = \pi\mathfrak{O}$ generated by the element π. $\mathfrak{O}$ is contained in its quotient field, K, and $\mathfrak{O}/\mathfrak{p}$ is the residue field. $\mathfrak{U} = \mathfrak{O} - \mathfrak{p}$ is the multiplicative group of units. An element x in K has *order* k if $x = \pi^k u$ where $u \in \mathfrak{U}$. $\mathfrak{O}$ is *non-dyadic* if $2 \notin \mathfrak{p}$, $\mathfrak{O}$ is *dyadic* if $2 \in \mathfrak{p}$, and $\mathfrak{O}$ is *2-adic* if $\mathfrak{p} = 2\mathfrak{O}$.

L will always be a finitely generated free $\mathfrak{O}$-module. A *quadratic form* on L is a map $Q : L \to K$ such that for all $x \in L$, for all $\alpha \in \mathfrak{O}$, $Q(\alpha x) = \alpha^2 Q(x)$ and such that the associated map

$$B(x, y) = Q(x + y) - Q(x) - Q(y) \tag{1.1}$$

is bilinear. The module L, with Q and B, is called a *lattice*. L is always assumed to be *regular*, meaning for any non-zero vector x, $B(x, L) \neq 0$. An *isometry* of L is an isomorphism $\varphi : L \to L$ such that $Q(x) = Q(\varphi(x))$ for all x. $O(L)$ is the group of isometries of L. x and y are *associated* (written $x \sim y$) if $\varphi(x) = y$ for some φ in $O(L)$. An isometry between lattices is an isomorphism which preserves the quadratic form on them.

If M and N are sublattices of L and x a vector in L, then the ideals $B(x, M)$, $B(M, N)$, and the lattices $\mathfrak{p}^k M = \pi^k M$, $M + N$ are defined in the obvious way. $M \oplus N$ denotes a *direct sum* of lattices (i.e. $M \cap N = \{0\}$) while $M \perp N$

Received January 28, 1977 and in revised form, August 9, 1977. This work was supported in part by Canada Council grant W763898.

means the *orthogonal sum* of lattices, which includes the additional requirement that $B(M, N) = 0$. A vector x is *primitive* in L if $x \in L$, $x \notin \pi L$. The lattice L is $\mathfrak{p}^k$-*modular* if $B(L, L) \subset \mathfrak{p}^k$ and $\det(\pi^{-k}B(x_i, x_j))$ is a unit where $\{x_i\}$ is a basis for L. Equivalently, L is $\mathfrak{p}^k$-modular if for all primitive x in L, $B(x, L) = \mathfrak{p}^k$. A *unimodular* lattice is one which is $\mathfrak{O}$-modular.

O'Meara's text [**7**] is a general source for terminologies and results on the arithmetic theory of quadratic forms, including lattices. Instead of the bilinear form defined in (1.1), O'Meara uses $x \cdot y = \frac{1}{2}B(x, y)$, which has the advantage that $Q(x) = x^2$. However this precludes the possibility of having characteristic 2. We have adopted definition (1.1) so that the characteristic 2 case can be included in a consistent approach.

It is easily shown that a lattice L has an orthogonal splitting

$$L = \perp_k U_k \tag{1.2}$$

where for each k, U_k is a $\mathfrak{p}^k$-modular lattice. This is called a *Jordan decomposition* of L. It is an essential element of traditional approaches to lattices.

Most previous Witt-type results have been done for lattices over the ring of integers in a local number field, requiring $\mathfrak{O}$ be complete and $\mathfrak{O}/\mathfrak{p}$ be finite. For non-dyadic rings, Rosenzweig [**8**] found necessary and sufficient conditions for vectors to be associated, then Band [**1**] completed the Witt theorem for sublattices. In the case of dyadic rings, the conditions for vectors to be associated have been found in a number of special situations by Trojan [**9**] and Hsia [**3**; **4**]. Unfortunately, their invariants and techniques were quite cumbersome because of heavy reliance on the Jordan decomposition of a lattice.

Professor N. C. Ankeny has suggested that rather than the Jordan decomposition, one should look at the invariant sublattices of L given by the following definition:

$$\begin{aligned} L_k &= \{x \in L \mid B(x, L) \subset \mathfrak{p}^k\}, \\ L_k' &= \{x \in L_k \mid Q(x) \in \mathfrak{p}^k\}. \end{aligned} \tag{1.3}$$

These lattices, defined for every integer k, are invariant under isometries of L and satisfy $L_k \supset L_{k+1}$, $\bigcap_k L_k = \{0\}$. Note that if $L = \perp U_j$ is a Jordan decomposition of L, then

$$L_k = \ldots \perp \pi^2 U_{k-2} \perp \pi U_{k-1} \perp U_k \perp U_{k-1} \perp \ldots .$$

If $\mathfrak{O}$ is non-dyadic (2 a unit), then L_k and L_k' are the same lattice because $Q(x) = \frac{1}{2}B(x, x)$. In [**2**], Cohen examines the L_k in the non-dyadic case.

In this paper, we prove the general Witt theorem for any lattice L over a discrete valuation ring which satisfies $L_k = L_k'$ for all k. Such a lattice is called *non-defective*. In the literature, it is also called *totally improper*. For such lattices, we find the necessary and sufficient conditions for an isometry of sublattices to extend to the whole lattice. The proof uses a new simpler tech-

nique based on a recent theorem of M. Kneser [6]. The invariants of vectors turn out to be much simpler when expressed in terms of the L_k than they had been in terms of a Jordan decomposition.

2. Kneser's theorem. L is a lattice, regular as always, over a discrete valuation ring $\mathfrak{O}$, with quadratic form Q and associated bilinear form B. If $u \in L$ satisfies $B(u, L) \subset Q(u)\mathfrak{O}$, then the map $\sigma_u : L \to L$ such that

$$\sigma_u(x) = x - (B(u, x)/Q(u))u, \tag{2.1}$$

is easily verified to be an isometry of L. We call σ_u the *reflection* about u. Such reflections are the main tool for constructing isometries.

LEMMA 2.1. *Suppose H is a sublattice of L such that $H \subset L_0'$. (i.e. for all $x \in H$, $B(x, L) \subset \mathfrak{O}$, $Q(x) \in \mathfrak{O}$.) Let $v, w \in L$ satisfy $Q(v) = Q(w)$ and $h = w - v \in H$.*

(a) *If $Q(h) \in \mathfrak{U}$ $(= \mathfrak{O} - \mathfrak{p})$, then $\sigma_h(v) = w$.*

(b) *If $Q(h) \notin \mathfrak{U}$ and there exists $u \in H$ such that $Q(u)$, $B(u, v)$ and $B(u, w)$ are in $\mathfrak{U}$, then, letting $z = h + (B(u, v)/Q(u))u \in H$, we have $\sigma_z(\sigma_u(v)) = w$.*

In both cases, v and w are associated.

Proof. (a) : $\sigma_h(v) = v - (B(v, h)/Q(h))h = v + h = w$ because $Q(h) = Q(v) + Q(w) - B(v, w) = 2Q(v) - B(v, w) = B(v, v - w) = -B(v, h)$.

(b) : $\sigma_u(v) = v - (B(u, v)/Q(u))u = v + h - z = w - z$. Then $\sigma_z(\sigma_u(v)) = w - z - (B(w - z, z)/Q(z))z = w$ if we can show that $B(\sigma_u(v), z) = -Q(z)$. But $w = z + \sigma_u(v)$ implies that

$$Q(w) = Q(z) + B(z, \sigma_u(v)) + Q(\sigma_u(v)).$$

Since $Q(\sigma_u(v)) = Q(v) = Q(w)$, we get $B(z, \sigma_u(v)) = -Q(z)$.

Definitions. $\mathrm{Hom}(M, K)$ is the group of homomorphisms from the lattice M into the field K. Similarly, we have $\mathrm{Hom}(M, \mathfrak{O})$ and $\mathrm{Hom}(M, \mathfrak{p}^k)$. If M is a sublattice of L, then $\lambda_M : L \to \mathrm{Hom}(M, K)$ is the map such that $\lambda_M(x)\ (y) = B(x, y)$ for all $x \in L$, $y \in M$.

THEOREM 2.2 (M. Kneser). *Assume M, N, and H are sublattices of L such that H is a sublattice of L_0', and M and N satisfy*

$$\lambda_M(H) = \mathrm{Hom}(M, \mathfrak{O}), \quad \lambda_N(H) = \mathrm{Hom}(N, \mathfrak{O}). \tag{2.2}$$

Let $\tau : M \to N$ be an isometry such that

$$\tau(x) \equiv x \pmod{H} \quad \textit{for all } x \in M. \tag{2.3}$$

Then τ can be extended to an isometry $\varphi \in O(L)$ which satisfies

$$\varphi(x) \equiv x \pmod{\mathrm{H}} \quad \textit{for all } x \in L. \tag{2.4}$$

Moreover, φ can be expressed as a product of reflections σ_h, where $h \in H$, provided

https://doi.org/10.4153/CJM-1978-045-5 Published online by Cambridge University Press

either of the following hold:

(2.5) $|\mathfrak{O}/\mathfrak{p}| \neq 2$, *and there exists* $g \in H$ *such that* $Q(g) \in \mathfrak{U}$, *or*

(2.6) $|\mathfrak{O}/\mathfrak{p}| = 2$, *and there exists* $g \in H$ *such that* $Q(g) \in \mathfrak{U}$ *and* $B(g, H) \subset \mathfrak{p}$.

Proof. We prove this theorem via several cases.

Case 1. $\mathrm{Dim}(M) = 1$ and either (2.5) or (2.6) holds.

Suppose $M = \mathfrak{O}v$, $N = \mathfrak{O}w$, where $\tau(v) = w = v + h$, for some $h \in H$. If $Q(h) \in \mathfrak{U}$, we are done by Lemma 2.1 (a). So assume $Q(h) \notin \mathfrak{U}$. Because $Q(v) = Q(w)$, we see that $Q(h) = -B(v, h) = B(w, h) \in \mathfrak{p}$. Let $F = \{f \in H \mid B(v, f) \in \mathfrak{U}, B(w, f) \in \mathfrak{U}\}$. If there exists $f \in F$ such that $Q(f) \in \mathfrak{U}$, we are done by Lemma 2.1 (b).

Otherwise, $Q(F) \subset \mathfrak{p}$. If $|\mathfrak{O}/\mathfrak{p}| \geqq 3$, F contains more elements than any proper sublattice of H, so F must span H. If $f \in F$ and $h = w - v$, then $h + f \in F$ must satisfy $Q(h + f) \in \mathfrak{p}$. Since $Q(h)$ and $Q(f)$ are in $\mathfrak{p}$, $B(h, f)$ must also be in $\mathfrak{p}$, so $B(h, F) \subset \mathfrak{p}$, hence $B(h, H) \subset \mathfrak{p}$ under condition (2.5).

If $f \in F$ and g is given by (2.5) or (2.6), for some $\alpha \in \mathfrak{O}$, the vector $u = g + \alpha f$ will satisfy $u \in F$ and $Q(u) \in \mathfrak{U}$, because $B(w, u) - B(v, u) = B(h, u) \in \mathfrak{p}$. Since this contradicts $Q(F) \subset \mathfrak{p}$, we are done. Condition (2.4) is immediately verified.

Case 2. $\mathrm{Dim}(M) = r > 1$ and either (2.5) or (2.6) holds.

The proof is by induction on r. Let g be given by (2.5) or (2.6). Suppose $\{v_1, \ldots, v_r\}$ is a basis of M over $\mathfrak{O}$. Reordering, we can assume $B(g, v_i) \in B(g, v_1)\mathfrak{O}$ for all i. Changing v_i to $v_i - (B(g, v_i)/B(g, v_1))v_1$, we can assume $B(g, M') = 0$ where $M' = \mathfrak{O}v_2 \oplus \ldots \oplus \mathfrak{O}v_r$. By induction, τ restricted to M' extends to an isometry $\varphi \in O(L)$ which is a product of reflections σ_h, $h \in H$. Because of (2.4), $\varphi(H) = H$ and conditions (2.2) and (2.3) still hold with M replaced by $\varphi(M)$. We can now assume that $\tau(v_i) = v_i$ for all $i > 1$.

By (2.2), there exist h, $h' \in H$ such that $B(v_1, h) = B(\tau(v_1), h') = 1$, $B(v_i, h) = B(v_i, h') = 0$ for all $i > 1$. Define $H'' = \{h \in H | B(h, M') = 0\}$, $M'' = \mathfrak{O}v_1$, $N'' = \mathfrak{O}\tau(v_1)$. We wish to apply Case 1 to the restriction of τ to M''. Conditions (2.2) and either (2.5) or (2.6) hold because g, h, and h' are in H''. (2.3) holds because for all $i > 1$:

$$B(\tau(v_1) - v_1, v_i) = B(\tau(v_1), v_i) - B(v_1, v_i)$$
$$= B(\tau(v_1), \tau(v_i)) - B(v_1, v_i) = 0$$

since τ is an isometry on M. By Case 1, $\tau : v_1 \to \tau(v_1)$ extends to an isometry φ of the lattice L which is a product of reflections σ_h with $h \in H''$. Because $B(M', H'') = 0$, we see from (2.1) that $\varphi(v_i) = v_i = \tau(v_i)$ for all $i > 1$. Hence φ extends τ on all of M.

Case 3. (2.5) and (2.6) do not hold.

We enlarge the lattice L so that (2.5) or (2.6) will hold. Define $L^* = L \perp (\mathfrak{O}\xi \oplus \mathfrak{O}\eta)$ where $Q(\xi) = Q(\eta) = 0$, $B(\xi, \eta) = 1$, and let $M^* =$

$M \perp \mathfrak{O}\eta$, $N^* = N \perp \mathfrak{O}\eta$, $H^* = H \perp (\xi + \eta)$. Define $\tau^* : M^* \to N^*$ to be τ on M and the identity on $\mathfrak{O}\eta$. Let $g = \xi + \eta$. Then $Q(g) = B(\xi, \eta) = 1 \in \mathfrak{U}$. If $|\mathfrak{O}/\mathfrak{p}| = 2$, then $2 \in \mathfrak{p}$, so $B(g, H^*) \subset B(g, g)\mathfrak{O} \subset 2\mathfrak{O} \subset \mathfrak{p}$. So either (2.5) or (2.6) holds. By Case 1 or 2, τ^* extends to an isometry φ^* of L^* which is a product of reflections σ_h with $h \in H^*$.

Since $B(\xi - \eta, H^*) = 0$, we must have $\tau^*(\xi - \eta) = \xi - \eta$. Because $\varphi^*(\eta) = \tau^*(\eta) = \eta$, φ^* is the identity on $\mathfrak{O}\,\xi \oplus \mathfrak{O}\,\eta$. Because L is the orthogonal complement of $\mathfrak{O}\,\xi \oplus \mathfrak{O}\,\eta$, φ^* must satisfy $\varphi^*(L) = L$. Letting φ be the restriction of φ^* to L, φ is an isometry of L which extends τ.

Our use of Kneser's theorem will be via the following corollary to Theorem 2.2.

THEOREM 2.3. *Assume M and N are sublattices of L satisfying*

$$\lambda_M(L_k') = \mathrm{Hom}\,(M, \mathfrak{p}^k), \quad \lambda_N(L_k') = \mathrm{Hom}\,(N, \mathfrak{p}^k), \tag{2.7}$$

where k is fixed. Let $\tau : M \to N$ be an isometry such that

$$\tau(x) \equiv x \ (L_k) \quad \textit{for all } x \in M. \tag{2.8}$$

Then τ extends to an isometry $\varphi \in O(L)$ such that

$$\varphi(x) \equiv x \ (L_k') \quad \textit{for all } x \in L. \tag{2.9}$$

Proof. If $\tau(x) - x = y \in L_k$, then $Q(\tau(x)) = Q(x) + Q(y) + B(x, y)$ implies $Q(y) = -B(x, y) \in \mathfrak{p}^k$, so $y \in L_k'$. Therefore L_k can be changed to L_k' in condition (2.8). With $H = L_k'$, this theorem is a direct corollary to Theorem 2.2 if we scale Q and B by π^{-k}.

3. Modular version of Kneser's results. Here we present modular versions of the results of the last section. They will be derived from the following lemma.

LEMMA 3.1. *Suppose H is a sublattice of L such that $H \subset L_0'$. If $v, w \in L$ satisfy $Q(v) \equiv Q(w)$ $(\mathfrak{p}^r)$ and $h = w - v \in H$, then the following hold.*

(a) *If $Q(h) \in \mathfrak{U}$, then $\sigma_h(v) \equiv w$ $(\pi^r H)$.*

(b) *If $Q(h) \notin \mathfrak{U}$ and there exists $u \in H$ such that $Q(u)$, $B(u, v)$ and $B(u, w)$ are in $\mathfrak{U}$, then $\sigma_z(\sigma_u(v)) \equiv w$ $(\pi^r H)$ where $z = h + (B(u, v)/Q(u))u \in H$.*

Proof. This lemma is proved in exactly the same way as Lemma 2.1.

We say that an isomorphism $\tau : M \to N$ of sublattices of L is an *isometry modulo* $\mathfrak{p}^r$ if

$$Q(\tau(x)) \equiv Q(x) \ (\mathfrak{p}^r) \quad \text{for all } x \in M. \tag{3.1}$$

The following modular version of Kneser's Theorem says that an isometry modulo $\mathfrak{p}^r$ of sublattices satisfying the conditions of Theorem 2.2 can be extended modulo $\pi^r H$ to an isometry of the whole lattice L.

THEOREM 3.2. *Assume M, N, and H are sublattices of L such that H is a sublattice of L_0'. With r a positive integer, assume $\tau : M \to N$ is an isometry modulo $\mathfrak{p}^r$. Suppose M, N and τ satisfy* (2.2) *and* (2.3). *Then there exists an isometry $\varphi \in O(L)$ which satisfies*

(3.2) $\varphi(x) \equiv \tau(x)\ (\pi^r H)$ *for all* $x \in M$, *and*

(3.3) $\varphi(x) \equiv x\ (H)$ *for all* $x \in L$.

In particular, φ extends τ modulo L_r':

(3.4) $\varphi(x) \equiv \tau(x)\ (L_r')$ *for all* $x \in M$.

Moreover, φ can be expressed as a product of reflections σ_h, $h \in H$, provided either (2.5) *or* (2.6) *hold.*

Proof. This theorem can be proved by the same cases as in the proof of Theorem 2.2. Cases 1 and 2 hold identically here remembering that all equations involving Q and B only hold modulo $\mathfrak{p}^r$, while all equations between vectors hold modulo $\pi^r H$. In Case 3 we get an isometry φ^* of L^* which extends τ^* modulo $\pi^r H^*$ and is the identity on $\mathfrak{O}\xi \oplus \mathfrak{O}\eta$ modulo $\pi^r H^*$. Let $M'' = \mathfrak{O}\xi \oplus \mathfrak{O}\eta$, $N'' = \tau^*(M'')$, $H'' = \pi^r M''$, and $\tau'' : M'' \to N''$ be the restriction of φ^*. Applying Theorem 2.2 with Q and B scaled by π^{-r}, there is an isometry φ'' which extends φ^* on M'' and satisfies $\varphi''(x) \equiv x\ (\pi^r M'')$ for all $x \in L$. Then $\varphi''^{-1}\varphi^*$ is an isometry which is the identity on M''. Taking φ to be its restriction to L, φ is an isometry of L which satisfies the requirements of the theorem.

As a direct corollary to Theorem 3.2 we have the following useful theorem.

THEOREM 3.3. *Let $\tau : M \to N$ be an isomorphism of sublattices of L. With k and r fixed integers, $r > 0$, suppose the following conditions hold :*

(3.5) $Q(x) \equiv Q(\tau(x))\ (\mathfrak{p}^{k+r})$ *for all* $x \in M$,

(3.6) $\tau(x) \equiv x\ (L_k)$ *for all* $x \in M$,

(3.7) $\lambda_M(L_k') = \mathrm{Hom}\ (M, \mathfrak{p}^k)$, $\lambda_N(L_k') = \mathrm{Hom}\ (N, \mathfrak{p}^k)$.

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

(3.8) $\varphi(x) \equiv x\ (L_k')$ *for all* $x \in L$

such that φ extends τ modulo L_{k+r}', i.e. the following holds:

(3.9) $\varphi(x) \equiv \tau(x)\ (L_{k+r}')$ *for all* $x \in M$.

4. Some general lemmas on lattices. Recall that a vector $z \in L$ is primitive if $z \notin \pi L$. We say that $z \in L$ is *primitive modulo* L_k if $z \notin \pi L + L_k$.

LEMMA 4.1. *z is primitive* mod L_{j+1} *if and only if* $B(z, L_j) = \mathfrak{p}^j$.

Proof. ($\Rightarrow$) Let k be minimal such that z is primitive mod L_{k+1}. So $k \leqq j$. Consider a modular decomposition of L. The minimality of k implies $z \notin \pi L + L_{k+1}$, $z \in \pi L + L_k$. Then the component of z in the $\mathfrak{p}^k$-modular component of L must be primitive. Therefore $B(z, L_k) = \mathfrak{p}^k$ and $B(z, \pi^{j-k}L_k) = \mathfrak{p}^j$. Since $\pi^{j-k}L_k \subset L_j$, we have $B(z, L_j) = \mathfrak{p}^j$.

($\Leftarrow$) If z is not primitive mod L_{j+1}, then $z \in \pi L + L_{j+1}$, so that $B(z, L_j) \subset \mathfrak{p}^{j+1}$.

The bilinear form $B(x, y)$ via the map $\lambda_M(L_k)$ yields a decomposition of the sublattice M into a direct sum of two lattices, one of which has all the homomorphisms into $\mathfrak{p}^k$, and another which maps into $\mathfrak{p}^{k+1}$, as in the following lemma.

LEMMA 4.2. *Let M be a sublattice of L and k fixed. Then*

(a) *M has a decomposition $M = M_1 \oplus M_2$ such that*

$$\lambda_{M_1}(L_k) = \mathrm{Hom}\ (M_1, \mathfrak{p}^k) \quad \textit{and} \quad B(M_2, L_k) \subset \mathfrak{p}^{k+1}. \tag{4.1}$$

(b) *Given this decomposition, there is a sublattice M_2' of L and a linear transformation γ from M onto $M_1 \oplus \pi M_2'$ such that γ is the identity on M_1 and γ maps M_2 onto $\pi M_2'$ with $\gamma(y) \equiv y$ (L_{k+1}) for all $y \in M$.*

Proof. (a) Assume M_1 is a sublattice of M with maximal dimension such that $\lambda_{M_1}(L_k) = \mathrm{Hom}\ (M_1, \mathfrak{p}^k)$. Say $\{x_1, \ldots, x_m\}$ is a basis of M_1. Then there exist $w_1, \ldots, w_m \in L_k$ which satisfy $B(x_i, w_j) = \delta_{ij}\pi^k$ for all i, j. Then $M = M_1 \oplus M_2$ where M_2 can be adjusted so that $B(M_2, w_i) = 0$ for all i. If $B(M_2, L_k) \not\subset \mathfrak{p}^{k+1}$, choose $y \in M_2$, $w \in L_k$ such that $B(y, w) = \pi^k$. Modifying w by multiples of the w_i, we can assume $B(x_i, w) = 0$ for all i. Also $B(y, w_i) = 0$ for all i because $y \in M_2$. Letting $M_1^* = M_1 \oplus \mathfrak{O}y$, we see that $\lambda_{M_1^*}(L_k) = \mathrm{Hom}\ (M_1^*, \mathfrak{p}^k)$ and $\dim (M_1^*) > \dim (M_1)$, contradicting the maximality of $\dim (M_1)$. Hence $B(M_2, L_k) \subset \mathfrak{p}^{k+1}$.

(b) Let $\{x_1, \ldots, x_m\}$ and $\{y_1, \ldots, y_n\}$ be bases for M_1 and M_2, respectively. Because $B(M_2, L_k) \subset \mathfrak{p}^{k+1}$, Lemma 4.1 implies that the y_i are not primitive mod L_{k+1}. Hence for all i, there exists $z_i \in L$ such that $y_i \equiv \pi z_i$ (L_{k+1}). Changing the z_i by vectors in L_k, we can assure that $\{x_1, \ldots, x_m, z_1, \ldots, z_n\}$ are linearly independent over $\mathfrak{O}$. Define $M_2' = \mathfrak{O}z_1 \oplus \ldots \oplus \mathfrak{O}z_n$ and $\gamma : M \to M_1 \oplus \pi M_2'$ such that $\gamma(x_i) = x_i$, $\gamma(y_j) = \pi z_j$. This is the desired map.

LEMMA 4.3. *If M is a sublattice of L, then $\lambda_M(L_k) = \mathrm{Hom}\ (M, \mathfrak{p}^k)$ if and only if, for any z which is primitive in M, z is primitive* mod L_{k+1}.

Proof. ($\Rightarrow$) Let $\{x_1, \ldots, x_m\}$ be a basis for M and let $w_j \in L_k$ satisfy $B(x_i, w_j) = \delta_{ij}\pi^k$ for all i, j. If $z = \sum \alpha_i x_i$ is primitive in M, then $\alpha_i \notin \mathfrak{p}$ for some i, so $B(z, w_i) = \alpha_i \pi^k \not\equiv 0$ $(\mathfrak{p}^{k+1})$. By Lemma 4.1, z is primitive mod L_{k+1}.

($\Leftarrow$) Consider the decomposition $M = M_1 \oplus M_2$ given by Lemma 4.2. If $M_2 \neq \emptyset$, let z be primitive in M_2. By hypothesis z is primitive mod L_{k+1}, so $B(z, L_k) = \mathfrak{p}^k$, contradicting $B(M_2, L_k) \subset \mathfrak{p}^{k+1}$. Hence $M = M_1$ and we are done.

Definition. The *exponent modulo* L_k of a vector $x \in L$ is the greatest integer $t = t(x, k)$ such that $x \in \pi^t L + L_k$. If $x \in L_r$, we say $t = +\infty$.

Note that the exponent mod L_k of a vector is invariant under isometries of L, i.e. $x \sim y \Rightarrow t(x, k) = t(y, k)$ for all k.

LEMMA 4.4. *Assume $\tau : M \to N$ is a surjective linear transformation of submodules of L which satisfies the following:*

(4.2) *for all $x \in M$, x and $\tau(x)$ have the same exponent* mod L_{k+1},

(4.3) $\lambda_M(L_k) = \text{Hom}\ (M, \mathfrak{p}^k)$.

Then τ is injective and $\lambda_N(L_k) = \text{Hom}\ (N, \mathfrak{p}^k)$.

Proof. Suppose $\tau(x) = 0$ for some non-zero $x \in M$, which we can assume is primitive in M. By Lemma 4.3, x is primitive mod L_{k+1}. Then by (4.2), x and $\tau(x)$ have exponent 0 mod L_{k+1}, contradicting $\tau(x) = 0$. Hence τ is injective.

Assume $\tau(x)$ is primitive in N. Then x must be primitive in M. By Lemma 4.3 and condition (4.2) we see that $\tau(x)$ must be primitive mod L_{k+1}. Then Lemma 4.3 implies $\lambda_N(L_k) = \text{Hom}\ (N, \mathfrak{p}^k)$.

5. Invariants in non-defective lattices. Henceforth L is a non-defective lattice, i.e. $L_k = L_k'$ for all k.

If x is a vector in L, we've seen that its exponent modulo L_k, $t = t(x, k)$, is invariant under isometries of L. Recall that t is the greatest integer such that $x \in \pi^t L + L_k$. Another invariant of x is its length $Q(x)$. A stronger length condition is found by looking at a vector x_k such that $x \equiv \pi^t x_k\ (L_k)$.

Consider two vectors $x_k, x_k' \in L$ which satisfy $x \equiv \pi^t x_k \equiv \pi^t x_k'\ (L_k)$. Then $x_k' - x_k \in L_{k-t}$, so that

$$\begin{aligned} Q(x_k') &= Q(x_k) + Q(x_k' - x_k) + B(x_k, x_k' - x_k) \\ &\equiv Q(x_k)\ (\mathfrak{p}^{k-t}), \end{aligned}$$

where we used the fact that $L_{k-t} = L_{k-t}'$ implies $Q(x_k' - x_k)$ is in $\mathfrak{p}^{k-t}$. Hence $Q(x_k)$ modulo $\mathfrak{p}^{k-t}$ is an invariant of x where x_k is a vector of L satisfying $x \equiv \pi^t x_k\ (L_k)$. For vectors x and y to be associated, they must satisfy the following partial length condition:

(5.1) $x \equiv \pi^t x_k,\ y \equiv \pi^t y_k\ (L_k) \Rightarrow Q(x_k) \equiv Q(y_k)\ (\mathfrak{p}^{k-t})$.

We intend to show that these partial length conditions along with equality of exponents are sufficient for the associativity of vectors in a non-defective lattice.

6. A lifting theorem. The following theorem is the most important step in the proof of the general Witt theorem. Given a map $\tau : M \to N$ of sublattices

of L and an isometry $\varphi \in O(L)$ such that $\varphi \equiv \tau(L_k)$ on M, this theorem will enable us to lift φ to an isometry $\varphi' \in O(L)$ such that $\varphi' \equiv \tau\ (L_{k+1})$.

THEOREM 6.1. *Given a non-defective lattcie L, $k \in \mathbf{Z}$, let $\tau : M \to N$ be a linear transformation of sublattices of L such that for all x in M the following hold:*

(6.1) $\tau(x) \equiv x\ (L_k)$;

(6.2) *x and $\tau(x)$ have the same exponent* mod L_{k+1}, *say t;*

(6.3) $x \equiv \pi^t x',\ \tau(x) \equiv \pi^t y'\ (L_{k+1}) \quad \Rightarrow \quad Q(x') \equiv Q(y')\ (\mathfrak{p}^{k+1-t})$.

Then there is an isometry $\varphi \in O(L)$ such that for all $x \in M$:

(6.4) $\varphi(x) \equiv \tau(x)\ (L_{k+1})$.

Proof. By induction on k. For some sufficiently small k^*, $L = L_{k^*}$, so there is nothing to prove for $k < k^*$. Now assume that the theorem is true for all $k' < k$ and any M, N, and τ.

Let M_1, M_2, M_2', and $\gamma : M \to M_1 \oplus \pi M_2'$ be given by Lemma 4.2. Then $M = M_1 \oplus M_2$ where

(6.5) $\lambda_{M_1}(L_k) = \mathrm{Hom}\ (M_1, \mathfrak{p}^k) \quad$ and $\quad B(M_2, L_k) \subset \mathfrak{p}^{k+1}$.

Also γ is the identity on M_1 and maps M_2 onto $\pi M_2'$ with

(6.6) $\gamma(x) \equiv x\ (L_{k+1}) \quad$ for all $x \in M$.

We lift τ first on M_2, then on M_1.

Let $M' = M_1 \oplus M_2'$. Define a map τ' on M' such that $\tau' = \tau$ on M_1 and for any $z \in M_2'$, $\tau'(z) \in L$ satisfies

(6.7) $\pi\tau'(z) \equiv \tau(\gamma^{-1}(\pi z))\ (L_{k+1})$.

This is possible because $\gamma^{-1}(\pi z) \in M_2$, so $\tau(\gamma^{-1}(\pi z))$ has exponent $\geqq 1$ mod L_{k+1}. After defining τ' on a basis of M_2' to satisfy (6.7), extend it to M_2'. Note that (6.7) holds for any z in M' because γ^{-1} is the identity on M_1.

Claim. $(\tau', M', \tau'(M'))$ satisfies the conditions of the theorem for $k - 1$.

Proof of claim. For any z in M' :

$$\begin{aligned} \pi\tau'(z) &\equiv \tau(\gamma^{-1}(\pi z))\ (L_{k+1}) \quad \text{by (6.7)} \\ &\equiv \gamma^{-1}(\pi z)\ (L_k) \quad \text{by (6.1)} \\ &\equiv \pi z\ (L_{k+1}) \quad \text{by (6.6)}. \end{aligned}$$

Hence $\tau'(z) \equiv z\ (L_{k-1})$ for all $z \in M'$, so (6.1) holds. Proving (6.2) and (6.3) for z and $\tau'(z)$ at $k - 1$ is equivalent to proving them for πz and $\pi\tau'(z)$ at k. Because $\gamma^{-1}(\pi z) \in M$, these conditions hold for $\gamma^{-1}(\pi z)$ and $\tau(\gamma^{-1}(\pi z))$. (6.6) and (6.7) imply $\pi z \equiv \gamma^{-1}(\pi z)$, $\pi\tau'(z) \equiv \tau(\gamma^{-1}(\pi z))\ (L_{k+1})$. Hence (6.2) and (6.3) also hold for πz and $\pi\tau'(z)$, proving the claim.

Applying the induction hypothesis, there exists $\varphi' \in O(L)$ such that

(6.8) $\varphi'(x) \equiv \tau'(x)\ (L_k)$ for all $x \in M'$.

Given $x \in M_2$, suppose $\gamma(x) = \pi z$ where $z \in M_2'$. Then

$$\begin{aligned}\varphi'(x) &\equiv \varphi'(\gamma(x))\ (L_{k+1}) \quad \text{by (6.6)}\\ &= \pi\varphi'(z) \quad \text{because } \gamma(x) = \pi z\\ &\equiv \pi\tau'(z)\ (L_{k+1}) \quad \text{by (6.8)}\\ &\equiv \tau(x)\ (L_{k+1}) \quad \text{by (6.7)}.\end{aligned}$$

For $x \in M_1$, $\tau(x) = \tau'(x) \equiv \varphi'(x)\ (L_k)$ by (6.8). Replacing M by $\varphi'(M)$, conditions (6.1), (6.2), and (6.3) still hold, and we may assume $M = M_1 \oplus M_2$ satisfies (6.5) with

(6.9) $\tau(x) \equiv x\ (L_{k+1})$ for all $x \in M_2$.

By Lemma 4.4, $\tau : M_1 \to \tau(M_1)$ is injective and $\lambda_{\tau(M_1)}(L_k) = \mathrm{Hom}\ (\tau(M_1), \mathfrak{p}_f)$. Since primitive vectors in M_1 have exponent 0 mod L_{k+1}, (6.3) implies

$$Q(\tau(x)) \equiv Q(x)\ (\mathfrak{p}^{k+1}) \quad \text{for all } x \in M_1.$$

Applying Theorem 3.3 with $r = 1$, recalling $L_k = L_k'$, there is an isometry $\varphi \equiv 1\ (L_f)$ such that $\varphi(x) \equiv \tau(x)\ (L_{k+1})$ for all x in M_1. If $x \in M_2$ satisfies $x \equiv \pi z\ (L_{k+1})$ where $z \in L$, then (6.9) and (3.8) imply

$$\varphi(x) \equiv \varphi(\pi z) \equiv \pi z \equiv x \equiv \tau(x)\ (L_{k+1}).$$

Therefore $\varphi(x) \equiv \tau(x)\ (L_{k+1})$ for all $x \in M$, completing the proof.

7. The main theorem. With the lifting of Theorem 6.1, we can now prove the general Witt theorem for non-defective lattices.

THEOREM 7.1. *Let $\tau : M \to N$ be an isomorphism of sublattices of a non-defective lattice L. Then τ extends to an isometry $\varphi \in O(L)$ if and only if the following hold for all $x \in M$ and $y = \tau(x)$:*

(7.1) *x and y have the same exponent* mod L_k, *say $t = t(x, k)$;*

(7.2) $x \equiv \pi^t x_k,\ y \equiv \pi^t y_k\ (L_k) \implies Q(x_k) \equiv Q(y_k)\ (\mathfrak{p}^{k-t})$.

Proof. The necessity of these conditions was shown earlier. If $x = \pi^j x'$ where $x \in M$, $x' \in L$, define $\tau(x') = \pi^{-j}\tau(x)$. Then x and $\tau(x)$ satisfy (7.1) and (7.2) if and only if x' and $\tau(x')$ satisfy them. Hence we can assume that every vector which is primitive in M is also primitive in L.

Claim. For a sufficiently large K, $\lambda_M(L_K) = \mathrm{Hom}\ (M, \mathfrak{p}^K)$.

Proof of claim. Take K to be the order of the highest component of a Jordan decomposition of L. Then $L_{K+i} = \pi^i L_K$ for all $i > 0$. By Lemma 4.2, M has a decomposition $M = M_1 \oplus M_2$ where $\lambda_{M_1}(L_K) = \mathrm{Hom}\ (M_1, \mathfrak{p}^K)$ and

https://doi.org/10.4153/CJM-1978-045-5 Published online by Cambridge University Press

$B(M_2, L_K) \subset \mathfrak{p}^{K+1}$. Suppose x is a primitive vector in M_2. Then Lemma 4.1 implies

$$x \in \pi L + L_{K+1} = \pi L + \pi L_K = \pi L.$$

Since this contradicts our assumption that vectors primitive in M are also primitive in L, we have $M = M_1$, proving the claim.

Given K by the claim, Lemma 4.4 implies τ is injective and $\lambda_N(L_K) = \mathrm{Hom}\ (N, \mathfrak{p}^K)$. If x is primitive in M, its exponent $t(x, k)$ is 0 for all $k > K$, so taking $x_k = x$, $y_k = \tau(x)$ in (7.2), we have $Q(x) \equiv Q(\tau(x))$ $(\mathfrak{p}^k)$. Since $\bigcap_k \mathfrak{p}^k = \{0\}$, we see that $Q(x) = Q(\tau(x))$ for all $x \in M$, so $\tau : M \to N$ is an isometry. If the additional condition:

$$(7.3) \quad \tau(x) \equiv x\ (L_K) \quad \text{for all } x \in M$$

held, then by Theorem 2.3, τ extends to an isometry $\varphi \in O(L)$, and we would be done.

For K' sufficiently small, $\tau(x) \equiv x\ (L_{K'})$ for all $x \in M$. For example, if K' is the order of the lowest component of a Jordan decomposition of L, then $L = L_{K'}$, so this is true trivially. Suppose that for a j such that $K' \leqq j < K$, there is an isometry $\varphi_j \in O(L)$ such that $\varphi_j(x) \equiv \tau(x)\ (L_j)$ for all $x \in M$. Then the map $\varphi_j^{-1}\tau$ satisfies $\varphi_j^{-1}\tau(x) \equiv x\ (L_j)$ for all $x \in M$. Theorem 6.1 gives a lifting $\varphi' \in O(L)$ such that

$$\varphi'(x) \equiv \varphi_j^{-1}\tau(x)\ (L_{j+1}) \quad \text{for all } x \in M.$$

Letting $\varphi_{j+1} = \varphi_j\varphi'$, φ_{j+1} is an isometry satisfying

$$\varphi_{j+1}(x\} \equiv \tau(x)\ (L_{j+1}) \quad \text{for all } x \in M.$$

Taking $\varphi_{K'}$ to be the identity, after at most $K - K'$ such liftings, we obtain an isometry $\varphi_K \in O(L)$ such that (7.3) holds with τ replaced by $\varphi_K^{-1}\tau$. As noted above, there is an isometry φ of L which extends $\varphi_K^{-1}\tau$. Then the isometry $\varphi_K\varphi$ extends τ on M, so the proof is complete.

Letting $M = \mathfrak{O}x$, as an immediate corollary to Theorem 7.1, we can give necessary and sufficient conditions for vectors to be associated in a non-defective lattice.

THEOREM 7.2. *Vectors x and y in a non-defective lattice L are associated if and only if conditions* (7.1) *and* (7.2) *hold for all k.*

8. Remarks. A) Conditions (7.1) and (7.2) of Theorem 7.1 need only be verified for primitive vectors in M in order to assure that τ extends to an isometry of L.

B) The exponents of vectors satisfy $t(x, k) \geqq t(x, k + 1)$ for all x, k. If K' is the order of the lowest component of a Jordan decomposition of L, then

$L = L_{K'}$, so $t(x, K') = +\infty$ for all x. Hence conditions (7.1) and (7.2) need only be considered for $k > K'$.

C) If K is the order of the highest component of a Jordan decomposition of L, then $L_{K+1} = \pi L_K$. If x is primitive in L, then $x \notin \pi L + L_{K+1}$, so $t(x, K+1) = 0$. If one assumes that τ is an isometry, i.e. $Q(x) = Q(\tau(x))$ for all x, then condition (7.2) is only needed when $t(x, k) > 0$. Hence if x and y are primitive with $Q(x) = Q(y)$, then $x \sim y$ if conditions (7.1) and (7.2) hold for k such that $K' < k \leqq K$. This gives an effective method of determining if two vectors are associated.

D) Theorem 7.1 yields an effective method of determining whether an isometry $\tau : M \to N$ extends to an isometry of L. Assume K' and K are as in B) and C), and assume that every vector which is primitive in M is also primitive in L. Then $\lambda_M(L_K) = \mathrm{Hom}\ (M, \mathfrak{p}^K)$ and for $K' \leqq j < K$, M has a decomposition $M = \oplus_{i \geqq 0} M_{ji} \oplus M_j^*$ where $M_j^* \subset L_{j+1}$ and

$$\lambda_{M_{ji}}(L_{j-i}) = \mathrm{Hom}\ (M_{ji}, \mathfrak{p}^j) \quad \text{for all } i. \tag{8.1}$$

The following conditions are necessary and sufficient for τ to extend to an isometry $\varphi \in O(L)$:

$$\lambda_N(L_K) = \mathrm{Hom}\ (N, \mathfrak{p}^K), \tag{8.2}$$

$$\lambda_{\tau(M_{ji})}(L_{j-i}) = \mathrm{Hom}\ (\tau(M_{ji}), \mathfrak{p}^j), \quad \text{and} \tag{8.3}$$

(8.4) if $\{x_{jih} | 1 \leqq h \leqq \dim (M_{ji})\}$ is a basis for M_{ji} and if

$$x_{jih} \equiv \pi^i x_{jih'},\ \tau(x_{jih}) \equiv \pi^i y_{jih'}\ (L_{j+1}), \text{ then for all } i, i' \text{ such}$$

that $i > 0$, $i' \leqq i$, and for all h, h',

$$Q(x_{jih'}) \equiv Q(y_{jih'}),\ B(x_{jih'}, x_{ji'h'}) \equiv B(y_{jih'}, y_{ji'h'})\ (\mathfrak{p}^{j+1-i}).$$

There are only a finite number of conditions in (8.3) and (8.4) because we only consider j such that $K' \leqq j < K$. Conditions (8.2) and (8.3) assure that x and $\tau(x)$ have the same exponent modulo L_{j+1}. Condition (8.4) assures condition (7.2) holds when $t(x, k) > 0$.

References

1. M. Band, *On the integral extensions of quadratic forms over local fields*, Can. J. Math. *22* (1970), 297–307.
2. D. M. Cohen, *Witt's theorem for quadratic forms*, Conference on Quadratic Forms, Queen's Papers in Mathematics, *46* (1977), 406–411.
3. J. S. Hsia, *A note on the integral equivalence of vectors in characteristic 2*, Math. Ann. *179* (1968), 63–69.
4. ——— *One dimensional Witt's theorem over modular lattices*, Bull. Amer. Math. Soc. *76* (1970), 113–115.
5. D. G. James and S. M. Rosenzweig, *Associated vectors in lattices over valuation rings*, Amer. J. Math. *90* (1968), 295–307.
6. M. Kneser, *Witts Satz fur quadratische Formen uber lokalen Ringen*, Nachr. die Akad. der Wiss. Gottingen, Math.-Phys. II Heft *9* (1972), 195–203.

7. O. T. O'Meara, *Introduction to quadratic forms*, Grundlehren der Math. Wiss. (Springer-Verlag, Berlin 1971).
8. S. M. Rosenzweig, *An anology of Witt's theorem for modules over the ring of p-adic integers*, Ph.D. thesis, M.I.T. (1958).
9. A. Trojan, *The integral extension of isometries of quadratic forms over local fields*, Can. J. Math. *18* (1966), 920–942.
10. E. Witt, *Theorie der quadratischen Formen in beliebigen Korpen*, Journal fur die reine und angewandte Math. *176* (1937), 31–44.

Massachusetts Institute of Technology,
Cambridge, Massachusetts;
McGill University,
Montreal, Quebec