PACIFIC JOURNAL OF MATHEMATICS
Vol. 15, No. 3, 1965

INTEGRAL INVARIANTS FOR VECTORS OVER LOCAL FIELDS

D. G. JAMES

This paper considers isometric invariants of vectors in lattices (quadratic forms) over the ring of integers in a local field for the prime 2. By extending the notion of order to vectors in the lattice we obtain a set of invariants which enable the general vector to be decomposed into a sum of simple vectors. The lengths of these simple vectors are invariant modulo certain powers of 2 and these lengths together with the original invariants form a complete set for the 2-adic integers. In the special case where there are no one dimensional, orthogonal sublattices (improper quadratic forms) the invariants form a complete set for all local fields.

Let F be a local field, that is a field complete with respect to a discrete, non-archimedean valuation with a finite residue class field, and R the ring of integers in F. Denote by $\nu(x)$ the order of the element x in F and by π a fixed prime in R; we may assume that $\nu(\pi) = 1$. Let V be a nonsingular lattice over R, i.e. a finite dimensional, torsion-free R-module with scalar product $\alpha \cdot \beta \in R$. An isometry φ of V is a one-to-one, linear transformation of V satisfying $\varphi(\alpha) \cdot \varphi(\beta) = \alpha \cdot \beta$. We investigate the isometric invariants of vectors $\alpha \in V$ in the unramified dyadic case, $\nu(2) = 1$. The p-adic case (p odd) has been considered by Rosenzweig [7] and an alternative approach by Ankeny (on the following lines) is included in the author's Ph. D. thesis [1].

In § 1 we develop the necessary structure theorems for V, much of which will also be found in [4], [5] and [6]; § 2 gives a complete set of invariants in the improper case; while § 3 treats the general case, but here we restrict ourselves to the 2-adic numbers, the results being more complex.

Frequent use is made of the following generalization of Hensel's lemma (see [3, p. 29]): if $f(x)$ is a polynomial with coefficients in R and $x_0 \in R$ is such that $\nu(f(x_0)) > 2\nu(f'(x_0))$, then $f(x)$ has a root $x \in R$ with $\nu(x - x_0) \geqq 1$.

1. We extend the notion of order to $\alpha \in V$ by defining $\nu(\alpha) = \min \nu(\alpha \cdot \beta)$, the minimum being taken over all $\beta \in V$. For each $r = 0, 1, 2, \cdots$ we denote by $V(r)$ the sublattice $\{\alpha \in V \mid \nu(\alpha) \geqq r\}$ and define $\nu_r(\alpha) = \min \nu(\alpha \cdot \beta)$, then minimum now being taken over all

Received August 20, 1964.

$\beta \in V(r)$. Then

$$\nu_r(\alpha) \leqq \nu_{r+1}(\alpha) \leqq \nu_r(\alpha) + 1 .$$

We write $V = U \oplus W$ if U and W are orthogonal sublattices together spanning V. Denote by $(\xi_1, \cdots, \xi_s)$ the sublattice spanned by $\xi_1, \cdots, \xi_s \in V$ and by U' the orthogonal complement of the sublattice U.

LEMMA 1. *Let $\xi \in V$. Then $V = (\xi) \oplus (\xi)'$ if and only if $\nu(\xi^2) = \nu(\xi)$.*

Proof. Clearly $(\xi) \oplus (\xi)' \subseteqq V$. Take $\alpha \in V$. Then

$$\alpha = (\alpha \cdot \xi / \xi^2)\xi + (\alpha - (\alpha \cdot \xi/\xi^2)\xi) \in (\xi) \oplus (\xi)' .$$

This gives the reverse inclusion. Notice that $\alpha \cdot \xi / \xi^2 \in R$ since $\nu(\alpha \cdot \xi) \geqq \nu(\xi) = \nu(\xi^2)$.

LEMMA 2. *If $\lambda, \mu \in V$ satisfy $\nu(\lambda) = \nu(\mu) = \nu(\lambda \cdot \mu) < \nu(\lambda^2)$ then $V = (\lambda, \mu) \oplus (\lambda, \mu)'$.*

Proof. Let $\alpha \in V$ and write $\alpha = (k_1\lambda + k_2\mu) + (\alpha - k_1\lambda - k_2\mu)$ where $k_1 = ((\alpha \cdot \mu)(\lambda \cdot \mu) - (\alpha \cdot \lambda)\mu^2)k_3^{-1}$, $k_2 = ((\alpha \cdot \lambda)(\lambda \cdot \mu) - (\alpha \cdot \mu)\lambda^2)k_3^{-1}$ and $k_3 = (\lambda \cdot \mu)^2 - \lambda^2\mu^2$. Since $\nu(k_3) = 2\nu(\lambda)$ it follows that $k_1, k_2 \in R$. From $\lambda \cdot (\alpha - k_1\lambda - k_2\mu) = \mu \cdot (\alpha - k_1\lambda - k_2\mu) = 0$ we have $\alpha \in (\lambda, \mu) \oplus (\lambda, \mu)'$.

LEMMA 3. *If $V = (\xi) \oplus (\lambda, \mu)$ where $\nu(\xi) = \nu(\lambda) = \nu(\mu) = \nu(\lambda \cdot \mu)$ then there exist $\alpha, \beta, \gamma \in V$ such that $V = (\alpha) \oplus (\beta) \oplus (\gamma)$.*

Proof. We may assume by Lemma 1 that $\nu(\lambda^2) > \nu(\lambda)$ and $\nu(\mu^2) > \nu(\mu)$. Let $\alpha = \xi + \lambda$, $\beta = \xi - (\xi^2/\lambda \cdot \mu)\mu$ so that $\alpha \cdot \beta = 0$. Since $\nu(\alpha^2) = \nu(\alpha)$ and $\nu(\beta^2) = \nu(\beta)$ we are finished by Lemma 1.

We can now establish the main result on the structure of V. Let H_e denote a hyperbolic plane of the form (λ, μ) where $\lambda \cdot \mu = \pi^e$, $\nu(\lambda^2) > \nu(\lambda) = e$ and $\nu(\mu^2) > \nu(\mu) = e$. We call a sublattice of the form $V_e = H_e \oplus \cdots \oplus H_e$ *improper* and a sublattice of the form $V_e = (\xi_1) \oplus \cdots \oplus (\xi_t)$ with $\nu(\xi_i^2) = \nu(\xi_i) = e$, *proper*.

PROPOSITION 1. (O'Meara [5]) Let V be a nonsingular lattice over a local field. Then

$$V = V_{e_1} \oplus V_{e_2} \oplus \cdots \oplus V_{e_m} \qquad e_1 < e_2 < \cdots < e_m$$

with the sublattices V_{e_i}, $1 \leqq i \leqq m$, either proper or improper. Furthermore, e_i, dim V_{e_i} and the forms of the V_{e_i}, $1 \leqq i \leqq m$, are invariants of V.

Proof. Choose $\alpha \in V$ to minimize $\nu(\alpha)$. Since the valuation is discrete there exists $\beta \in V$ such that $\nu(\alpha) = \nu(\beta) = \nu(\alpha \cdot \beta)$. If $\nu(\alpha^2) = \nu(\alpha)$ we split off the vector α using Lemma 1 and if $\nu(\alpha^2) > \nu(\alpha)$ we split off the plane (α, β). Proceeding in this manner we obtain the stated structure for V, after using Lemma 3 to get the correct form for the sublattices V_{e_i}.

We now establish the invariance of e_i and $\dim V_{e_i}$, $1 \leqq i \leqq m$. Let $\xi_1, \cdots, \xi_n$ and $\eta_1, \cdots, \eta_n$ be two bases of V arranged so that $\nu(\xi_i) \leqq \nu(\xi_{i+1})$ and $\nu(\eta_i) \leqq \nu(\eta_{i+1})$, $1 \leqq i \leqq n-1$. It suffices to show that $\nu(\xi_i) = \nu(\eta_i)$, $1 \leqq i \leqq n$. Let d be the first discrepancy and suppose that $\nu(\xi_d) > \nu(\eta_d) = f$. Then expressing η_i in terms of the ξ_i we see that

$$\eta_1 = a_{11}\xi_1 + \cdots + a_{1d-1}\xi_{d-1} + \alpha_1$$
$$\cdot \quad \cdot \quad \cdot$$
$$\eta_d = a_{d1}\xi_1 + \cdots + a_{dd-1}\xi_{d-1} + \alpha_d \ .$$

In these equations $a_{ij} \in R$ and $\nu(\alpha_i) > f$. Eliminating the ξ_i we see that there exist $c_i \in R$, with at least one c_i a unit, such that $\sum_{i=1}^{d} c_i\eta_i = \sum_{i=1}^{d} c_i\alpha_i$. But $\nu(\Sigma c_i\eta_i) \leqq f$ and $\nu(\Sigma c_i\alpha_i) > f$ gives the required contradiction.

Finally we show that the form of V_{e_i} is invariant. Let

$$V = V_{e_1} \oplus \cdots \oplus V_{e_m} = V_{e_1}^* \oplus \cdots \oplus V_{e_m}^*$$

be two decompositions satisfying the conditions of the proposition and $\xi_1, \cdots, \xi_n$ the basis in the first case and $\eta_1, \cdots, \eta_n$ in the second. Suppose that $V_e = (\xi_h) \oplus \cdots \oplus (\xi_k)$ is proper. To prove that V_e^* is proper it is sufficient to show the existence of a vector λ orthogonal to $\eta_1, \cdots, \eta_{h-1}$ with $\nu(\lambda^2) = \nu(\lambda) = e$. If $\xi_h = \sum_{i=1}^{n} a_i\eta_i$ take $\lambda = \sum_{i=h}^{n} a_i\eta_i$; the required properties of λ follow from those of ξ_h.

Lattices with the same invariants above are said to be of the same *type*. A basis splitting V into the sum of lines and planes, as in Proposition 1, is called a *canonical basis*.

PROPOSITION 2. If $\alpha, \beta \in V$ satisfy $\nu(\alpha) = \nu(\beta) = \nu(\alpha \cdot \beta) = r$, $\nu(\alpha^2) \geqq r+2$ and $\nu(\beta^2) \geqq r+1$ then there exist $\lambda, \mu \in V$ such that $V = (\lambda, \mu) \oplus (\lambda, \mu)'$ where $\lambda^2 = \mu^2 = 0$, $\lambda \cdot \mu = \pi^r$ and $\alpha = \frac{1}{2}\pi^{-r}\alpha^2\lambda + \mu$.

Proof. Put $\lambda = x\alpha + \beta$ where x is a root of the equation $\alpha^2x^2 + 2\alpha \cdot \beta x + \beta^2 = 0$ (a root congruent to $x_0 = -\beta^2/2\alpha \cdot \beta$ exists by

Hensel's lemma). Then $\lambda^2 = 0$ and, multiplying by a unit if necessary, $\alpha\cdot\lambda = \pi^r$. Put $\mu = -\frac{1}{2}\pi^{-r}\alpha^2\lambda + \alpha$.

A hyperbolic plane (λ, μ) as in Proposition 2 is called *totally isotropic.*

PROPOSITION 3. (O'Meara [6]) Let $H_i = (\lambda_i, \mu_i)$, $i = 1, 2$, be two totally isotropic hyperbolic planes with $\nu(\lambda_1) = \nu(\lambda_2) = r$. Then an isometry $\varphi: H_1 \rightarrow H_2$ extends to an isometry of V.

Proof. It is sufficient to show that the orthogonal complements of H_1 and H_2 are isometric. Assume first that $\lambda_1 = \lambda_2$. Let $\eta_1, \cdots, \eta_{n-2}$ be a basis of H_1'. Let $\zeta_i = \eta_i - \pi^{-r}(\eta_i\cdot\mu_2)\lambda_1$, $1 \leqq i \leqq n-2$, so that we have $\zeta_i\cdot\zeta_j = \eta_i\cdot\eta_j$, $\zeta_i\cdot\lambda_2 = \zeta_i\cdot\mu_2 = 0$, $1 \leqq i, j \leqq n-2$. Since $\zeta_1, \cdots, \zeta_{n-2}$ is a basis of H_2' this case is finished. Now we assume there exist $\alpha \in H_1$, $\beta \in H_2$ such that $\nu(\alpha\cdot\beta) = r$. From symmetry we may take $\nu(\lambda_1\cdot\lambda_2) = r$ and then the sublattice (λ_1, λ_2) is totally isotropic by Proposition 2. By the first part we now have that H_1' and H_2' are both isometric to $(\lambda_1, \lambda_2)'$. Finally we assume that $\nu(\alpha\cdot\beta) > r$ for all $\alpha \in H_1$, $\beta \in H_2$. The sublattice $(\lambda_1, \mu_1 + \mu_2)$ is now totally isotropic and its orthogonal complement is isometric to H_1' and H_2' by the second part of the proof.

For $\alpha \in V$ with $\nu(\alpha^2) = \nu(\alpha) = r$ we define $N_r(\alpha)$ to be 0 if there exists $\beta \in V(r)$ such that $\alpha\cdot\beta = 0$ and $\nu(\beta^2) = r$, and to be 1 otherwise. A vector $\alpha \in V$ is called *imprimitive* if $\alpha = \pi\beta$ with $\beta \in V$, otherwise it is *primitive.*

PROPOSION 4. Let $V = (\xi) \oplus (\xi)' = (\eta) \oplus (\eta)'$. Then there exists an isometry φ of V such that $\varphi(\xi) = \eta$ if and only if $\xi^2 = \eta^2$, $\nu(\xi) = \nu(\eta) = r$ and $N_r(\xi) = N_r(\eta)$.

Proof. For the general case see O'Meara [5, Theorems 5.1, 5.2]. See also Jones [2] for a discussion of related results in the 2-adic case.

The rest of this section will be devoted to constructing isometric invariants of vectors.

We call $r(\neq 0)$ a *critical index* of $\alpha \in V$ if

$$\nu_{r-1}(\alpha) = \nu_r(\alpha) < \nu_{r+1}(\alpha) ;$$

0 is a *critical index* of $\alpha \in V$ if

$$\nu(\alpha) < \nu_1(\alpha) .$$

The critical indices can only be the orders of basis vectors (the e_i of

Proposition 1) and hence a vector has only a finite number of critical indices. They are isometric invariants.

We say that the vectors $\lambda_1, \cdots, \lambda_m$ are *fully orthogonal* if $V = V_1 \oplus \cdots \oplus V_m$ where $\lambda_i \in V_i$, $1 \leqq i \leqq m$.

PROPOSITION 5. Let α have critical indices at $r_1, r_2, \cdots, r_s$ where $r_1 < r_2 < \cdots < r_s$ and let $\nu_{r_j}(\alpha) = r_j + b_j$. Then

$$r_1 + b_1 < r_2 + b_2 < \cdots < r_s + b_s, \quad b_1 > b_2 > \cdots > b_s$$

and $\alpha = \sum_{j=1}^{s} \pi^{b_j}\lambda_j$ where λ_j are fully orthogonal, primitive vectors. Each λ_j has only one critical index and

$$\nu(\lambda_j) = \nu_{r_j}(\lambda_j) = r_j \, , \qquad 1 \leqq j \leqq s \, .$$

Proof. Let $\xi_1, \cdots, \xi_n$ be a canonical basis of V, so that $\alpha = \sum_{i=1}^{n} a_i\xi_i$. We will use induction on the number of critical indices. Let $\lambda_1 = \pi^{-b_1} \sum' a_i\xi_i \in V$, the sum being over those ξ_i for which either $\nu(\xi_i) \leqq r_1$, or $\nu(\xi_i^2) = \nu(\xi_i)$ and $\nu(a_i) \geqq b_1$, or $\nu(\xi_i^2) > \nu(\xi_i) = \nu(\xi_i \cdot \xi_{i+1})$ and $\nu(a_i) \geqq b_1$, $\nu(a_{i+1}) \geqq b_1$. λ_1 now satisfies the conditions stated and the rest of α is a vector with critical indices at $r_2, \cdots, r_s$.

COROLLARY. *There exist* $\beta_i \in V$, $1 \leqq i \leqq s$, *such that* $\beta_i \cdot \lambda_j = 0$ $(i \neq j)$ *and* $\nu(\lambda_i) = \nu(\beta_i) = \nu(\beta_i \cdot \lambda_i)$.

The λ_j are called *critical components* of α. In general they are not uniquely determined. However, the r_j and b_j are invariant and the lengths of the λ_j are invariant modulo certain powers of π.

PROPOSITION 6. Suppose $\alpha = \sum_{j=1}^{s} \pi^{b_j}\lambda_j = \sum_{j=1}^{s} \pi^{b_j}\mu_j$ are two decompositions as in Proposion 5 with $\nu(\lambda_j) = \nu(\mu_j) = r_j$. Then

$$\left(\pi^{-b_t} \sum_{j=1}^{t} \pi^{b_j}\mu_j\right)^2 \equiv \left(\pi^{-b_t} \sum_{j=1}^{t} \pi^{b_j}\lambda_j\right)^2 (\operatorname{mod} \pi^{r_{t+1}+b_{t+1}-b_t}) \, ,$$
$$1 \leqq t \leqq s-1 \, .$$

Proof. Fix t, $1 \leqq t \leqq s-1$. By Corollary to Proposition 5 there exist β_i such that $\nu(\beta_i \cdot \lambda_i) = \nu(\beta_i) = r_i$, $\beta_i \cdot \lambda_j = 0$ $(i \neq j)$. Then

$$\alpha \cdot \beta_i = \pi^{b_i}\lambda_i \cdot \beta_i \equiv \sum_{j=1}^{t} \pi^{b_j}\mu_j \cdot \beta_i (\operatorname{mod} \pi^{r_{t+1}+b_{t+1}}) \, , \qquad 1 \leqq i \leqq t \, .$$

We can therefore find $x_i \in R$ such that $\nu(x_i - 1) \geqq r_{t+1} + b_{t+1} - r_i - b_i$ and $x_i\lambda_i \cdot \beta_i = \pi^{-b_i} \sum_{j=1}^{t} \pi^{b_j}\mu_j \cdot \beta_i$. This shows that the vector $\eta = \sum_{j=1}^{t} \pi^{b_j}(\mu_j - x_j\lambda_j)$ is orthogonal to all the vectors $\beta_1, \cdots, \beta_t$. Furthermore

$$(1)\qquad \sum_{j=1}^{t} x_j\pi^{b_j}\lambda_j + \eta = \sum_{j=1}^{t} \pi^{b_j}\mu_j\ .$$

We now have

$$\alpha = \sum_{j=1}^{t} \pi^{b_j}\lambda_j + \sum_{j=t+1}^{s} \pi^{b_j}\lambda_j = \eta + \sum_{j=1}^{t} x_j\pi^{b_j}\lambda_j + \sum_{j=t+1}^{s} \pi^{b_j}\mu_j\ .$$

Since $\nu((x_j - 1)\pi^{b_j}\lambda_j) \geqq r_{t+1} + b_{t+1}$ for $1 \leqq j \leqq t$, we have

$$\pi^{-b_t}\eta \in V(r_{t+1} + b_{t+1} - b_t)\ .$$

The result is now obtained by squaring (1).

Notice that it is not necessary to assume that the μ_j are orthogonal. Let $D_t(\alpha) = (\pi^{-b_t} \sum_{j=1}^{t} \pi^{b_j}\lambda_j)^2$ and $d_t(\alpha) = r_{t+1} + b_{t+1} - b_t$ for $1 \leqq t \leqq s-1$. We have established that $D_t(\alpha)(\operatorname{mod} \pi^{d_t(\alpha)})$, $1 \leqq t \leqq s-1$, are invariants of the vector α and hence also isometric invariants.

COROLLARY. *If V does not contain any vectors ξ such that $\nu(\xi^2) = \nu(\xi) = d_t(\alpha)$ then $D_t(\alpha)$ modulo $\pi^{d_t(\alpha)+1}$ is actually invariant.*

Under certain conditions an even stronger condition can be established.

Let $\alpha = \sum_{j=1}^{s} \pi^{b_j}\lambda_j$ be as in Proposition 5. Define $N_{r_j}(\alpha)$ to be 0 if there exists a $\beta \in V(r_j)$ such that $\beta\cdot\lambda_j = 0$ and $\nu(\beta^2) = r_j$, otherwise let $N_{r_j}(\alpha)$ be 1. $N_{r_j}(\alpha)$, $1 \leqq j \leqq s$, are independent of the choice of the critical components (left to the reader) and hence are isometric invariants.

We will show that in certain cases the above isometric invariants form a complete set.

We conclude this section with a simple observation. Let $W_i \subseteqq V = (\xi_1, \cdots, \xi_n)$ and $\dim W_i = \dim V$, $i = 1, 2$. Then for some $k \geqq 0$ we have $\pi^k V = (\pi^k\xi_1, \cdots, \pi^k\xi_n) \subseteqq W_1$. Let $\varphi\colon W_1 \rightarrow W_2$ be an isometry. Let $\alpha \in W_1$ be primitive in W_1 but imprimitive in V, i.e. $\alpha = \pi\beta$ where $\beta \notin W_1$, $\beta \in V$. Then if φ is to extend to an isometry of V, $\varphi(\alpha)$ must be imprimitive in V, $\varphi(\alpha) = \pi\beta'$ say, and then we must have $\varphi(\beta) = \beta'$. Thus by considering $\pi^k\xi_i \in W_1$ we can determine whether φ extends to an isometry of V or not.

2. We now give a complete set of invariants for the improper case. We assume that V contains no vectors ξ such that $\nu(\xi^2) = \nu(\xi)$. Call such a lattice V *fully improper*.

PROPOSITION 7. Let α and β be vectors with one critical index, at r. Then there exists an isometry φ of V such that $\varphi(\alpha) = \beta$ if and only if $\alpha^2 = \beta^2$ and $\nu(\alpha) = \nu(\beta)$.

Proof. We may assume α and β are primitive so that $\nu(\alpha) = \nu(\beta) = r$. If $\nu(\alpha) = \nu(\alpha\cdot\beta)$ then by Lemma 2 $V = (\alpha, \beta) \oplus (\alpha, \beta)'$. Define an isometry φ by $\varphi(\alpha) = \beta$, $\varphi(\beta) = \alpha$ and identity on $(\alpha, \beta)'$. We may therefore assume $\nu(\alpha\cdot\beta) > \nu(\alpha)$. Now choose $\rho \in V(r)$ such that $\nu(\alpha\cdot\rho) = \nu(\beta\cdot\rho) = \nu(\alpha) = \nu(\rho)$. If $\nu(\rho^2) > \nu(\rho) + 1$, then (α, ρ) and (β, ρ) are totally isotropic, and we are finished by Proposition 3. If $\nu(\rho^2) = \nu(\rho) + 1$, put $\gamma = x\rho + \alpha$ where $x\rho^2 + 2\rho\cdot\alpha = 0$, so that $\alpha^2 = \beta^2 = \gamma^2$. Now as above, we can find isometries φ_1, φ_2 such that $\varphi_1(\alpha) = \gamma$, $\varphi_2(\gamma) = \beta$. Put $\varphi = \varphi_2\varphi_1$.

For vectors with more than one critical index we use the invariants of Proposition 6 to adjust the lengths of the critical components and then split them off in orthogonal sublattices. The proof is then complete by induction. We need first another result.

PROPOSITION 8. Let $V = (\lambda_1, \eta) \oplus (\lambda_2, \xi)$ where $\nu(\lambda_1) = \nu(\lambda_1\cdot\eta) = \nu(\eta) = r_1$ and $\nu(\lambda_2) = \nu(\xi) = \nu(\lambda_2\cdot\xi) = r_2$. If $\alpha = \pi^c\lambda_1 + \lambda_2$ where $c \geqq 1$, and if $\nu(y) \geqq r_2 - r_1 - c > 0$, then there exists an isometry φ of V such that

$$\varphi(\alpha) = \beta = \pi^c(\lambda_1 + y\eta) + z\xi - \lambda_2$$

for some $z \in R$.

Proof. Let $z \in R$ be a root of the equation

$$\frac{1}{2}z^2\xi^2 - z\lambda_2\cdot\xi + \pi^{2c}y\Big(\lambda_1\cdot\eta + \frac{y}{2}\eta^2\Big) = 0 .$$

Then $\nu(z) \geqq c$ and $\alpha^2 = \beta^2$. Put

$$\gamma_1 = \pi^c\Big(\lambda_1 + \frac{1}{2}y\eta\Big) + \frac{1}{2}z\xi ,$$

$$\gamma_2 = \frac{1}{2}\pi^c y\eta + \frac{1}{2}z\xi - \lambda_2 ,$$

$$\gamma_3 = \eta - \Big(\frac{\eta^2}{\eta\cdot\lambda_1}\lambda_1\Big)\lambda_1 ,$$

$$\gamma_4 = \xi - \Big(\frac{\xi^2}{\xi\cdot\lambda_2}\lambda_2\Big)\lambda_2 .$$

It follows that $\gamma_1 - \gamma_2 = \alpha, \gamma_1 + \gamma_2 = \beta$ and $\gamma_1\cdot\gamma_2 = \gamma_1\cdot\gamma_4 = \gamma_2\cdot\gamma_3 =$

$\gamma_3 \cdot \gamma_4 = 0$. Define an isometry φ on the sublattice $(\gamma_1, \gamma_2, \gamma_3, \gamma_4)$ of V by

$$\varphi(\gamma_1) = \gamma_1 , \qquad \varphi(\gamma_2) = -\gamma_2 ,$$
$$\varphi(\gamma_3) = \gamma_3 , \qquad \varphi(\gamma_4) = -\gamma_4 .$$

By considering the vectors in this sublattice that are imprimitive in V we see that φ extends uniquely to an isometry of V. Since $\varphi(\alpha) = \beta$ we are finished.

PROPOSITION 9. Let V be a fully improper lattice. Take $\alpha, \beta \in V$. Then there exists an isometry φ of V such that $\varphi(\alpha) = \beta$ if and only if

1. $\alpha^2 = \beta^2$
2. α and β have the same critical indices $r_1, \cdots, r_s$
3. $\nu_{r_i}(\alpha) = \nu_{r_i}(\beta) = r_i + b_i \qquad 1 \leqq i \leqq s$
4. $D_t(\alpha) \equiv D_t(\beta)(\mathrm{mod}\, \pi^{d_t(\alpha)+1}) \qquad 1 \leqq t \leqq s - 1$.

Proof. The necessity of the conditions follows from § 1. Notice that the invariant $N_{r_i}(\alpha)$ is always 1 in this case. For the sufficiency we use induction on s. The case $s = 1$ is Proposition 7. Take $s > 1$. Let $\alpha = \sum_{i=1}^{s} \pi^{b_i}\lambda_i$ and $\beta = \sum_{i=1}^{s} \pi^{b_i}\mu_i$ be decompositions into fully orthogonal critical components. Let η be such that $\nu(\eta) = \nu(\eta \cdot \lambda_1) = \nu(\lambda_1)$ and $\eta \cdot \lambda_i = 0$ $(i \neq 1)$. Then from 4, with $t = 1$, we have

$$\lambda_1^2 \equiv \mu_1^2(\mathrm{mod}\, \pi^{r_2+b_2-b_1+1}) .$$

Take $y \in R$ such that $(\lambda_1 + y\eta)^2 = \mu_1^2$; this equation has a solution y such that $\nu(y) \geqq r_2 + b_2 - r_1 - b_1$. By Proposition 8, taking $c = b_1 - b_2 \geqq 1$, there exists an isometry of V mapping $\pi^{b_1}\lambda_1 + \pi^{b_2}\lambda_2$ into $\pi^{b_1}(\lambda_1 + y\eta) + \pi^{b_2}(z\xi - \lambda_2)$, i.e. mapping α into a vector α_1 whose first critical component has the same length as the first critical component of β. We now split off the first critical component of α_1 into a binary sublattice. We then proceed to adjust the lengths of the remaining critical components of α.

In this way we can map $\alpha = \Sigma\pi^{b_i}\lambda_i$ into a vector $\alpha^* = \Sigma\pi^{b_i}\lambda_i^*$ with $\lambda_i^{*2} = \mu_i^2, 1 \leqq i \leqq s$. Those λ_i^*, μ_i satisfying $\nu(\mu_i^2) \geqq \nu(\mu_i) + 2$ can be imbedded in totally isotropic, binary lattices and mapped into each other using Propositions 2 and 3. We may therefore assume that $\nu(\mu_i^2) = \nu(\mu_i) + 1$ for all i.

We now restrict ourselves to studying $\alpha = \Sigma\pi^{b_i}\lambda_i$ and $\beta = \Sigma\pi^{b_i}\mu_i$ with $\lambda_i^2 = \mu_i^2$ and $\nu(\lambda_i^2) = \nu(\lambda_i) + 1$. By Proposition 7 we may assume $\mu_1 = \lambda_1$ after applying an isometry to α. Take $\rho \in V$ such that $\nu(\mu_1 \cdot \rho) = \nu(\mu_1) = \nu(\rho)$ and $\rho \cdot \mu_i = 0, 2 \leqq i \leqq s$. Using Lemma 2 we can split off (μ_1, ρ). However, we will not have $\rho \cdot \lambda_i = 0$ in general.

We apply a further isometry θ to α keeping λ_1 fixed and mapping λ_i, $2 \leqq i \leqq s$, into vectors orthogonal to ρ. Then splitting off (λ_1, ρ) we are finished by induction.

We construct θ as follows. Let $V = (\lambda_1, \eta_1) \oplus (\lambda_2, \xi_1) \oplus U$ where λ_i, $3 \leqq i \leqq s$, are in the sublattice U. We may assume that $\nu(\eta_1^2) = \nu(\eta_1) + 1$ and $\nu(\xi_1^2) = \nu(\xi_1) + 1$, for otherwise we have totally isotropic, binary lattices and these may be concelled. Thus we may assume $\xi_1^2 = \lambda_2^2$. Let

$$\lambda_2' = x\pi^{r_2 - r_1}\Bigl(\lambda_1 - \Bigl(\frac{\lambda_1^2}{\lambda_1 \cdot \eta_1}\eta_1\Bigr) + y\lambda_2 + \xi_1 ,$$

where x and y are chosen so that $\lambda_2'^2 = \lambda_2^2$ and $\lambda_2' \cdot \rho = 0$ (the equations for x and y have solutions in R). Then $\lambda_2' \cdot \lambda_1 = 0$ and $\nu(\lambda_2' \cdot \lambda_2) = \nu(\lambda_2)$. Thus $V = (\lambda_1, \gamma) \oplus (\lambda_2, \lambda_2') \oplus U$ for some $\gamma \in V$. We now take an isometry mapping λ_2 into λ_2' and acting as the identity on $(\lambda_2, \lambda_2')'$. Similarly we can map λ_i, $3 \leqq i \leqq s$, into vectors orthogonal to ρ.

3. We now consider the general case but restrict ourselves to R being the ring of 2-adic integers.

PROPOSITION 10. Let α and β be vectors with one critical index, at r. Then there exists an isometry φ of V such that $\varphi(\alpha) = \beta$ if and only if $\alpha^2 = \beta^2$, $\nu(\alpha) = \nu(\beta)$ and $N_r(\alpha) = N_r(\beta)$.

Proof. We may assume α and β primitive so that $\nu(\alpha) = \nu(\beta) = r$. If $\nu(\alpha^2) = \nu(\alpha)$ we are finished by Proposition 4. Assume $\nu(\alpha^2) > \nu(\alpha)$. As in Proposition 7 we take $\rho \in V(r)$ such that $\nu(\alpha \cdot \rho) = \nu(\beta \cdot \rho) = \nu(\alpha)$. We need only consider the case $\nu(\rho^2) = \nu(\rho)$. Then we may assume that $\alpha = x\rho + \eta$, $\beta = \rho + \xi$ with $\eta \cdot \rho = \xi \cdot \rho = 0$. We now wish to find $\lambda, \mu \in V$ such that $\alpha = \lambda + \mu$, $\lambda \cdot \mu = 0$ and $\lambda^2 = \rho^2$. The necessary equations can be solved, but only because $\nu(x) = 0$ so that for the 2-adics $\nu(x^2 - 1) \geqq 3$. We then construct an isometry φ such that $\varphi(\lambda) = \rho$ and $\varphi(\mu) = \xi$ using Proposition 4.

This result need not be true if we go beyond the 2-adics; further invariants are necessary as is shown by an example latter.

To treat vectors with more than one critical component we must establish some results analogous to Proposition 8. The situation is now more complex and the particular invariants depend on the structure of V. For there to exist an isometry mapping α into β we need the following invariants:

(i) $\alpha^2 = \beta^2$

(ii) α and β have the same critical indices $r_1, \cdots, r_s$

(iii) $N_{r_i}(\alpha) = N_{r_i}(\beta),\qquad 1 \leqq i \leqq s$
(iv) $\nu_{r_i}(\alpha) = \nu_{r_i}(\beta) = r_i + b_i,\qquad 1 \leqq i \leqq s$
(v) $D_t(\alpha) \equiv D_t(\beta)(\operatorname{mod} \pi^{d_t(\alpha)+f_t}),\qquad 1 \leqq t \leqq s-1$,
where $f_t = 0, 1$ or 2 depending on the structure of V.

These conditions, with $f_t = 2$, are always sufficient, but usually not necessary. The conditions with $f_t = 1$ are necessary, provided there do not exist any $\xi_t \in V$ satisfying $\nu(\xi_t^2) = \nu(\xi_t) = d_t(\alpha)$ for $1 \leqq t \leqq s-1$, and also sufficient provided further that $b_{i-1} \neq b_i + 1$ or $r_{i+1} + b_{i+1} \neq r_i + b_i + 1$ for any i. The proofs of these remarks are similar to the proof of Proposition 9 using results analogous to Proposition 8 to adjust the lengths of the critical components.

PROPOSITION 11. Let $V = (\lambda_1) \oplus (\lambda_2)$ where $\nu(\lambda_1) = r_1$, $\nu(\lambda_2) = r_2$ and let $c \geqq 1$ and $r_2 - r_1 - c \geqq 1$. If $\alpha = \pi^c\lambda_1 + \lambda_2$ then there exists an isometry φ of V such that

$$\varphi(\alpha) = \beta = \pi^c x\lambda_1 - y\lambda_2$$

for some $y \in R$, provided either
(a) $\nu(x-1) \geqq r_2 - r_1 - c + 1$,
or
(b) $\nu(x-1) \geqq r_2 - r_1 - c \geqq 2, c \geqq 2$.

Proof. Let y be a root of the equation

$$y^2 = 1 + \pi^{2c}(1 - x^2)\frac{\lambda_1^2}{\lambda_2^2}, \qquad y \equiv 1 (\operatorname{mod} 4) .$$

This equation has a root $y \in R$ by (a) or (b) using Hensel's lemma. Put

$$\gamma_1 = \frac{1}{2}\pi^c(1 + x)\lambda_1 + \frac{1}{2}(1 - y)\lambda_2$$

and

$$\gamma_2 = \frac{1}{2}\pi^c(1 - x)\lambda_1 + \frac{1}{2}(1 + y)\lambda_2 .$$

Then $\gamma_1 + \gamma_2 = \alpha$, $\gamma_1 - \gamma_2 = \beta$ and $\gamma_1 \cdot \gamma_2 = 0$. For (a) we have $\nu(\gamma_2^2) = \nu(\gamma_2)$, so that $V = (\gamma_2) \oplus (\gamma_2)'$ and we take φ such that $\varphi(\gamma_2) = -\gamma_2$ and φ is the identity on $(\gamma_2)'$. Then $\varphi(\alpha) = \beta$. For (b) we take the isometry on (γ_1, γ_2) defined by $\varphi(\gamma_1) = \gamma_1$, $\varphi(\gamma_2) = -\gamma_2$ and extend this to V through the imprimitive vectors as in Proposition 8.

PROPOSITION 12. Let $V = (\lambda_1) \oplus (\lambda_2, \xi)$ where $\nu(\lambda_1) = r_1$, $\nu(\lambda_2) = \nu(\xi) = \nu(\lambda_2 \cdot \xi) = r_2$, $\nu(\lambda_2^2) > \nu(\lambda_2)$ and $\nu(\xi^2) > \nu(\xi)$. If $\alpha = \pi^c\lambda_1 + \lambda_2$ with

$c \geqq 1$, then there exists an isometry φ of V such that

$$\varphi(\alpha) = \beta = \pi^c x \lambda_1 + y\xi - \lambda_2$$

for some $y \in R$, provided either $\nu(x-1) \geqq r_2 - r_1 - c + 1$ or $\nu(x-1) \geqq r_2 - r_1 - c \geqq 2$.

PROPOSITION 13. Let $V = (\lambda_1, \eta) \oplus (\lambda_2)$ where $\nu(\lambda_1) = \nu(\eta) = \nu(\lambda_1 \cdot \eta) = r_1$, $\nu(\lambda_1^2) > \nu(\lambda_1)$, $\nu(\eta^2) > \nu(\eta)$ and $\nu(\lambda_2) = r_2$. If $\alpha = \pi^c \lambda_1 + \lambda_2$ with $c \geqq 1$ and $r_2 - r_1 - c > 0$, then there exists an isometry φ of V such that

$$\varphi(\alpha) = \beta = \pi^c(\lambda_1 + y\eta) - z\lambda_2$$

for some $z \in R$, provided that either $\nu(y) \geqq r_2 - r_1 - c + 1$ or $\nu(y) \geqq r_2 - r_1 - c$ and $c \geqq 2$.

The proofs of Propositions 12 and 13 are similar to those of Propositions 8 and 11. These results now enable us to establish the results stated for isometric invariants in the 2-adic case above.

Suppose that $\alpha = \sum_{i=1}^{s} \pi^{b_i} \lambda_i$ and $\beta = \sum_{i=1}^{s} \pi^{b_i} \mu_i$ satisfy conditions (i)–(v) above (in some case of f_t). If $\nu(\lambda_1^2) = \nu(\lambda_1)$, then from (v) $\lambda_1^2 \equiv \mu_1^2 (\operatorname{mod} \pi^{d_1(\alpha)+f_1})$ so that $\lambda_1^2 = x\mu_1^2$ with $\nu(x-1) \geqq d_1(\alpha) + f_1 - r_1$. Provided that $d_1(\alpha) + f_1 - r_1 \geqq 3$, we may take $\lambda_1^2 = x^2\mu_1^2$ with $\nu(x-1) \geqq d_1(\alpha) + f_1 - r_1 - 1$. Then, applying an isometry as in Proposition 11 or 12, we may assume that $\lambda_1 = \mu_1$, etc. Likewise, if $\nu(\lambda_1^2) > \nu(\lambda_1)$, we use suitable combinations of the methods given above.

The presence of vectors satisfying $\nu(\xi_t^2) = \nu(\xi_t) = d_t(\alpha)$ for certain t enable us to use the weakest form of (v) with $f_t = 0$, but because of the proliferation of cases we proceed no further with this.

To extend the above beyond the 2-adics requires further invariants as is shown by the following example:

$$V = (\xi_1) \oplus (\xi_2) \oplus (\xi_3)$$

$$\xi_1^2 = \xi_2^2 = 1\,, \qquad \xi_3^2 = 2$$

$$\alpha = \xi_1 + \xi_2\,, \qquad \beta = a\xi_1 + a\xi_2 + b\xi_3$$

where the residue class field has four elements (i.e. $ab = 1$, $a^2 = b$, $b^2 = a$ and $a + b = 1$). Although (i)–(v) are satisfied no isometry of V maps α into β. To show this look at the conditions imposed upon the image of ξ_3 modulo 4.

References

1. D. G. James, *The extension of isometries of sublattices over local fields*, M.I.T. Ph. D. Thesis, 1963.

2. B. W. Jones, *The arithmetic theory of quadratic forms*, Carus Monographs, No. 10, Mathematical Association of America, 1950.

3. S. Lang, *Algebraic Numbers*, Addison-Wesley, 1964.

4. O. T. O'Meara, *Introduction to quadratic forms*, Springer-Verlag, 1963.

5. ———, *Quadratic forms over local fields*, Amer. J. Math. **77** (1955), 87-116.

6. ———, *Witt's theorem and the isometry of lattices*, Proc. Am. Math. Soc. **7** (1956), 9-22.

7. S. Rosenzweig, *An analogy of Witt's theorem for modules over the ring of p-adic integers*, M.I.T. Ph. D. Thesis, 1958.

University of Auckland