THE INTEGRAL EXTENSION OF ISOMETRIES OF QUADRATIC FORMS OVER LOCAL FIELDS

ALLAN TROJAN

Let F be a local field with ring of integers $\mathfrak{o}$ and prime ideal $\pi\mathfrak{o}$. If V is a vector space over F, a lattice L in V is defined as an $\mathfrak{o}$-module in the vector space V with the property that the elements of L have bounded denominators in the basis for V. If V is, in addition, a quadratic space, the lattice L then has a quadratic structure superimposed on it. Two lattices on V are then said to be isometric if there is an isometry of V that maps one onto the other.

In this paper, we consider the following problem: given two elements, v and w, of the lattice L over the regular quadratic space V, find necessary and sufficient conditions for the existence of an isometry on L that maps v onto w. Rosenzweig **(3)** has settled this problem for the case where F is a local field in which 2 is a unit. We extend the results to local fields in which 2 is a prime element.

We remark that if $v^2 = w^2$ and char $F \neq 2$, the existence of an isometry of V that maps v onto w is given by Witt's theorem. Therefore the results obtained constitute a partial generalization of Witt's theorem to lattices over local fields.

1. Notation and basic concepts. O. T. O'Meara's book **(1)** contains an extensive discussion of the local theory of quadratic forms. We shall assume that the reader is familiar with the notation and results contained there. We do, however, wish to emphasize a few important facts.

V will always stand for a regular n-dimensional quadratic space over a local field F, and L an n-dimensional lattice over V. If L is non-empty, there is a basis $\{x_1, \dots, x_n\}$ for V which is also a basis for L. We write

$$L = x_1\,\mathfrak{o} + x_2\,\mathfrak{o} + \dots + x_n\,\mathfrak{o}.$$

If $\alpha \in F$, then we write $\mathfrak{d}(\alpha)$, to indicate the quadratic defect of α **(1**, p. 160**)**. ρ will always signify a unit of $\mathfrak{o}$ such that $\mathfrak{d}(1 + 4\rho) = 4\mathfrak{o}$.

Now let M and N be lattices over V, v an element of V, and $\mathfrak{A}$ an ideal in F. We then make the following definitions: $s(M)$ is the ideal generated by $(M.M)$; $n(M)$ the ideal generated by M^2; $M\# = \{x: (x.M) \subseteq \mathfrak{o}\}$;

$$M^{\mathfrak{A}} = \{x: (x\,.\,M) \subseteq \mathfrak{A}\}; \qquad M^{\perp} = \{x: x \in L \text{ and } x\,.\,M = \{0\}\};$$

FM is the vector space spanned by M. A modular lattice is then said to be proper if $n(M) = s(M)$ and is otherwise said to be improper. Zero lattices will be considered improper.

Received March 29, 1965.

https://doi.org/10.4153/CJM-1966-092-x Published online by Cambridge University Press

We shall use the notation $L \oplus M$ to stand for the orthogonal sum of the lattices L and M. $\langle v \rangle$ will be used to denote the lattice generated by a given vector v. We shall sometimes represent lattices by their matrix representation, so that $\begin{vmatrix} \epsilon & \delta \\ \delta & \sigma \end{vmatrix}$ would indicate that lattice generated by two vectors, v and w, such that $v^2 = \epsilon$, $v \cdot w = \delta$, $w^2 = \sigma$.

The lattice L admits of a decomposition (called the Jordan Decomposition),

$$L = L_1 \oplus \ldots \oplus L_t$$

into modular sublattices such that

$$s(L_1) \supset s(L_2) \supset \ldots \supset s(L_t).$$

If 2 is a prime element of F, then dim L_i, $s_i = s(L_i)$, $n_i = n(L_i)$, t are called the Jordan invariants of the decomposition and are, in fact, independent of the decomposition chosen **(1**, Chapter 9**)**.

There is a somewhat similar decomposition of vectors in L into critical components. This was developed by Rosenzweig **(3)** in the following manner.

If K is a lattice with Jordan form $K = K_1 \oplus K_2$ and v is a vector in K with the decomposition $v = v_1 + \pi^r v_2$ with $v_i \in K_i (i = 1, 2)$ both maximal vectors (that is $\pi^{-1} v_i \notin K$) and $r \geqslant 0$, then there is a Jordan decomposition $K = M_1 \oplus M_2$ such that $v \in M_1$. Similarly, if $k = \text{ord}\, s(K_2) - \text{ord}\, s(K_1)$ and $v = \pi^{k+r} v_1 + v_2$ with v_i maximal in K_i $(i = 1, 2)$ and $r \geqslant 0$, then there is a second Jordan decomposition $K = N_1 \oplus N_2$ with $v \in N_2$.

Now let v be an element of the lattice L. From the previous two facts it easily follows that there is some decomposition of L of the form

$$L = \sum_{l}^{m}{}_{\oplus} L_i$$

with L_i empty or π^i-modular in which the unique representation

$$v = \sum_{1}^{p}{}_{\oplus} \pi^{f_i} v_{\lambda_i} \qquad (v_{\lambda_i} \text{ maximal in } L_{\lambda_i}, v_{\lambda_i} \neq 0)$$

has the following two properties:

1. $f_1 > f_2 > \ldots > f_p$.
2. $f_1 + \lambda_1 < f_2 + \lambda_2 < \ldots < f_p + \lambda_p$.

The λ_i are called the critical indices of v and the f_i, the critical exponents. Their uniqueness follows from the following observation:

Let $L^{(i)} = L^{\mathfrak{A}_i}$ where $\mathfrak{A}_i = \pi^i \mathfrak{o}$. We note that

$$L^{(i)} = L_l + \ldots + L_i + \pi L_{i+1} + \ldots + \pi^{m-i} L_m.$$

Then, upon letting

$$e_i = \min_{y \in L^{(i)}} \text{ord}\, (v . y),$$

it is easily shown that λ is a critical index of v if and only if $e_{\lambda-1} = e_\lambda = e_{\lambda+1} - 1$.

https://doi.org/10.4153/CJM-1966-092-x Published online by Cambridge University Press

This, of course, implies the uniqueness of the critical indices (and hence the critical exponents) of v. It is also clear that if v and w are isometrically equivalent vectors in L, then they have the same critical indices and exponents.

We make the further definition: $s_i = \lambda_{i+1} + f_{i+1} - \lambda_i - f_i$. Now let

$$L = \sum_{l}^{m}{}_{\oplus} M_i$$

(with M_i π^i-modular or zero) be any other Jordan decomposition for L. Let

$$v = \sum_{l}^{m}{}_{\oplus} 2^{h_i} w_i$$

(where $w_i \in M_i$, w_i maximal or zero). Then we have the following facts concerning the critical indices and exponents of v:

1. If $k = \lambda_j$, then $h_k = f_k$.
2. If $k < \lambda_1$, then $h_k \geqslant f_1 + \lambda_1 - k$.
3. If $\lambda_j < k < \lambda_{j+1}$, then $h_k \geqslant f_j$ when $\lambda_j < k \leqslant \lambda_j + s_j$ and $h_k + k \geqslant f_{j+1} + \lambda_{j+1}$ when $\lambda_j + s_j \leqslant k < \lambda_{j+1}$.
4. $\sum_{l}^{\lambda_i + s_i} 2^{h_j} w_j$ has as its critical indices $\{\lambda_1, \ldots, \lambda_i\}$.

From this point on, we shall assume that 2 is a prime element of F unless otherwise stated. Let $v, w \in L$. We say that v is equivalent to w (written $v \sim w$) if there is an isometry, ϕ, on L that $\phi(v) = w$. We shall develop necessary and sufficient conditions for the equivalence of vectors, first over modular lattices, then for vectors with one critical index, and finally for the general case.

2. Equivalence of vectors over modular lattices. In this section we shall assume that L is a modular lattice. If L is proper it has an orthogonal basis; if improper it is an orthogonal sum of two-dimensional sublattices (**1**, Theorem 93.15). This leads us to the following important definition:

Definition. Let L be 2^k-modular and $\{x_i\}$ a basis for L which is orthogonal if L is proper. We define a mapping T with domain, the elements of L, and range, a subset of the residue class field of F. Write $x = 2^{-m} \sum \alpha_i x_i$ where $\alpha_i \in \mathfrak{o}$ and at least one of the α_i is a unit. Then $T(x)$ is defined in the following manner:

(a) If L is improper, $T(x) = 0$.

(b) If L is proper and there exist integers $i, j \leqslant n$ such that

$$2^{-k}(\alpha_i^2 x_i^2 - \alpha_j^2 x_j^2) \not\equiv 0 \pmod 2,$$

then $T(x) = 0$.

(c) If L is proper and

$$2^{-k}(\alpha_i^2 x_i^2 - \alpha_j^2 x_j^2) \equiv 0 \pmod 2$$

for all pairs of integers $i, j \leqslant n$, then

$$T(x) \equiv 2^{-k}\alpha_1{}^2 x_1{}^2 \pmod 2.$$

Our definition of T appears to be dependent on the orthogonal basis $\{x_i\}$. However, the following proposition shows that the original choice of basis is, in fact, immaterial to the definition of T.

PROPOSITION 2.1. *The following statements are true for any two maximal elements, v and w, of a unimodular lattice L:*

1. $T(v) \not\equiv 0 \pmod 2$ *if and only if* $n(\langle v\rangle^{\perp}) \subset n(L)$.
2. *If* $y \in L$, $\operatorname{ord} y^2 = 0$, *and* $T(v) \neq 0$, *then* $$(v\cdot y)^2/y^2 \equiv T(v) \pmod 2.$$
3. *If* $v \sim w$, *then* $T(v) = T(w)$.

Before proceeding to the question of equivalence of vectors over modular lattices, we state some important facts concerning the structure of these lattices.

PROPOSITION 2.2. *Every two-dimensional unimodular lattice over an unramified dyadic local field is isometric to one of the following lattices:*

$$H(0) = \begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix}, \qquad B(0) = \begin{vmatrix} 1 & 1 \\ 1 & 0 \end{vmatrix}, \qquad H(\rho) = \begin{vmatrix} 2\rho & 1 \\ 1 & 2 \end{vmatrix},$$

$$B(\rho) = \begin{vmatrix} 4\rho & 1 \\ 1 & 1 \end{vmatrix}, \qquad E(\epsilon, \delta) = \begin{vmatrix} \epsilon & 1 \\ 1 & 2\delta \end{vmatrix},$$

where ϵ, δ are units of $\mathfrak{o}$.

PROPOSITION 2.3. *We have the following facts concerning unimodular lattices:*

1. $B(\rho) \oplus H(\rho)$ *is not isometric to* $B(0) \oplus H(0)$.
2. $B(\rho) \oplus H(0)$ *is not isometric to* $B(0) \oplus H(\rho)$.
3. $H(\rho) \oplus \langle\epsilon\rangle$ *is not isometric to* $H(0) \oplus \langle\epsilon(1 + 4\rho)\rangle$.
4. $H(\rho) \oplus \langle\epsilon\rangle$ *is anisotropic.*
5. $H(\rho) \oplus B(\rho)$ *is anisotropic.*

Here ϵ is some unit of $\mathfrak{o}$.

For a proof of the previous two propositions, see **(2)**.

PROPOSITION 2.4. *Let v, w be maximal vectors in the two-dimensional modular lattice L. Then $v \sim w$ if and only if $v^2 = w^2$ and $T(v) = T(w)$.*

Proof. In view of Proposition 2.1, we need only prove the sufficiency of the conditions. There are three cases here to consider.

Case 1. $\operatorname{ord} v^2 = 0$. In this case, there are vectors v_1, w_1 such that

$$L = \langle v\rangle \oplus \langle v_1\rangle = \langle w\rangle \oplus \langle w_1\rangle$$

and $v_1{}^2 = w_1{}^2$. The required isometry ϕ is defined by the conditions $\phi(v) = w$ and $\phi(v_1) = w_1$.

Case 2. ord $v^2 \geqslant 1$, $v^2 \not\equiv 0$. Here, there is a vector $v_1 \in L$ such that $v \cdot v_1 = 1$. Let $v_1^2 = \alpha$ and $v^2 = \delta$. Clearly $L = v\mathfrak{o} + v_1\mathfrak{o}$.

We first show that there exists a vector $w_1 \in L$ such that $w \cdot w_1 = 1$ and $w_1^2 \equiv v_1^2 \pmod 2$. This fact is obvious if L is improper; so we may assume that L is proper, in which case $T(v) \not\equiv 0$. Now $2^{-1}(v - w) \in L$ (because $T(v) = T(w)$) and thus $w \cdot v_1 \equiv v \cdot v_1 \equiv 1 \pmod 2$. Let $w \cdot v_1 = 1 + 2\mu$ where $\mu \in \mathfrak{o}$. Then the required w_1 is $w_1 = (1 + 2\mu)^{-1}v_1$.

So, now we have two representations for L,

$$L = v\mathfrak{o} + v_1\mathfrak{o} = w\mathfrak{o} + w_1\mathfrak{o}$$

where $v^2 = w^2 = \delta$, $v \cdot v_1 = w \cdot w_1 = 1$, $v_1^2 = \alpha$, $w_1^2 = \beta$, and $\alpha \equiv \beta \pmod 2$. Furthermore $(1 - \delta\alpha)$ and $(1 - \delta\beta)$ both represent det L, and therefore the equation

$$(1 - \alpha\delta)/(1 - \beta\delta) = x^2$$

has solutions in F. But

$$(1 - \alpha\delta)/(1 - \beta\delta) \equiv 1 + \delta(\alpha - \beta) \equiv 1 \pmod{2\delta}.$$

But if $x^2 \equiv 1 \pmod{2\delta}$, then $x \equiv \pm 1 \pmod{\delta}$. Consequently there is a unit γ such that $\gamma \equiv 1 \pmod{\delta}$ and $\gamma^2 = (1 - \alpha\delta)/(1 - \beta\delta)$.

We note that

$$FL \simeq \langle v \rangle \oplus \langle v - \delta v_1 \rangle \simeq \langle w \rangle \oplus \langle w - \delta w_1 \rangle$$

and that $(v - \delta v_1)^2 = \gamma^2(w - \delta w_1)^2$, so that there is an isometry ϕ on FL such that $\phi(v) = w$ and

$$\phi(v - \delta v_1) = \gamma(w - \delta w_1).$$

We show that ϕ is the required isometry on L, that is, $\phi(L) \subset L$. It is sufficient to prove that $\phi(v_1) \in L$. But

$$\begin{aligned}\phi(v_1) &= \delta^{-1}\phi(v - (v - \delta v_1)) = \delta^{-1}(w - \gamma(w - \delta w_1)) \\ &= \gamma w_1 + (1 - \gamma)\delta^{-1}w.\end{aligned}$$

Since γ, $(1 - \gamma)/\delta \in \mathfrak{o}$, $\phi(v_1) \in L$.

Case 3. $v^2 = 0$. Here we have $L \simeq B(0)$ or $L \simeq H(0)$. If $L \simeq B(0)$, there is a basis $\{x, y\}$ for L such that $x^2 = 1$, $x \cdot y = 1$, $y^2 = 0$. Also, there are units ϵ_1, ϵ_2 such that $v = \epsilon_1 y$ or $v = \epsilon_1(2x - y)$ and $w = \epsilon_2 y$ or $\epsilon_2(2x - y)$. Furthermore, $\epsilon_1/\epsilon_2 \equiv 1 \pmod 2$ by Proposition 2.1 (2).

Now let μ be a unit such that $\mu \equiv 1 \pmod 2$. We define an isometry, ϕ_μ, on FL by the maps

$$\phi_\mu(y) = \mu y, \qquad \phi_\mu(2x - y) = (2x - y)\mu^{-1}.$$

It is easily checked that ϕ_μ is an isometry on L (since $\phi_\mu(x) \in L$). We let ψ be a second isometry on L defined by the maps $\psi(y) = 2x - y$ and

$$\psi(2x - y) = y.$$

If we let $\alpha = \epsilon_1/\epsilon_2$ and $\beta = \epsilon_2/\epsilon_1$, it is clear that one of the following isometries will map v onto w: $\phi_\alpha, \phi_\beta, \phi_\alpha \psi, \phi_\beta \psi$.

The case where $L \simeq H(0)$ is settled in a similar manner.

PROPOSITION 2.5. *Let v be a maximal element of the unimodular lattice L. Then if* $\operatorname{ord} v^2 \geqslant 1$, *there is a decomposition $L = R \oplus S$ with $v \in R$,* $\dim R = 2$ *and the additional conditions:*

1. *S is improper if $T(v) \neq 0$.*
2. *R is improper if $T(v) = 0$.*

Proof. There are three cases to consider.

Case 1. L is improper. Here we may write $L = \sum_\oplus L_i$ where

$$L_i = x_i \mathfrak{o} + y_i \mathfrak{o}$$

and $x_i \cdot y_i = 1$. If we let $v = \sum \alpha_i x_i + \sum \beta_j y_j$, then since v is maximal, there is an integer k such that $\operatorname{ord} \alpha_k = 0$ or $\operatorname{ord} \beta_k = 0$. By symmetry, we may assume that $\operatorname{ord} \alpha_k = 0$. We then let $R = v\mathfrak{o} + y_k \mathfrak{o}$. Since R is a unimodular lattice, it splits L and we may therefore write $L = R \oplus S$. Clearly $n(S) \subset \mathfrak{o}$.

Case 2. L is proper, $T(v) = 0$. Let $\{x_i\}$ be an orthogonal basis for L. If we write $v = \sum \alpha_i x_i$, it is clear that there are integers j, k such that α_j, α_k are units and $\alpha_j^2 x_j^2 \not\equiv \alpha_k^2 x_k^2 \pmod 2$. Now every unit of F is a square (mod 2). Let β be a unit such that $\beta^2 \equiv x_k^2/x_j^2 \pmod 2$. If $y = \beta x_j + x_k$, then $y^2 \equiv 0 \pmod 2$ and $v \cdot y \not\equiv 0 \pmod 2$. If $R = v\mathfrak{o} + y\mathfrak{o}$, then R is an improper and unimodular lattice which splits L.

Case 3. $T(v) \neq 0$. Let x be an element of L such that $\operatorname{ord} x^2 = 0$. Then the lattice $R = x\mathfrak{o} + v\mathfrak{o}$ is unimodular, so we can write $L = R \oplus S$. By Proposition 2.1(1), S is improper.

This brings us to the main result of this section.

THEOREM 2.1. *Let v, w be maximal elements of the unimodular lattice L. Then $v \sim w$ if and only if $v^2 = w^2$ and $T(v) = T(w)$.*

Proof. The necessity has already been proved. We shall prove the sufficiency. There are three cases.

Case 1. $\operatorname{ord} v^2 = 0$. We may write $L = \langle v \rangle \oplus \langle v \rangle^\perp = \langle w \rangle \oplus \langle w \rangle^\perp$. We wish to prove $\langle v \rangle^\perp \simeq \langle w \rangle^\perp$. Now $F\langle v \rangle^\perp \simeq F\langle w \rangle^\perp$ by Witt's theorem. Now

$$n(\langle v \rangle^\perp) = n(\langle w \rangle^\perp)$$

by Proposition 2.1(1), so the unimodular lattices $\langle v \rangle^\perp$ and $\langle w \rangle^\perp$ have the same Jordan invariants. By (**1**, Theorem 93.29), $\langle v \rangle^\perp \simeq \langle w \rangle^\perp$.

Case 2. $\operatorname{ord} v^2 \geqslant 1$, $T(v) = 0$. We first show the existence of improper, unimodular lattices R, S such that $v \in R, w \in S, R, S \subset L, \dim R = \dim S = 2$, and $R \simeq S$. By Proposition 2.5 there exist improper, unimodular lattices

P_1, P_2 such that $v \in P_1$, $w \in P_2$, $P_i \subset L$, $\dim P_i = 2$. If $P_1 \simeq P_2$, the result follows if we let $R = P_1$, $S = P_2$. Now if $\dim L = 3$, then $P_1 \simeq P_2$ by Proposition 2.3(3). If $\operatorname{ord} v^2 \geqslant 2$, then $P_1 \simeq P_2 \simeq H(0)$ since the lattice $H(\rho)$ cannot represent an element of order $\geqslant 2$ by a maximal vector. So we may assume $\dim L \geqslant 4$, $P_1 \simeq H(0)$, $P_2 \simeq H(\rho)$, $\operatorname{ord} v^2 = 1$. (The case where $P_2 \simeq H(0)$ is, of course, the same by symmetry.) We may choose vectors y_1, y_2 such that $P_1 = v\mathfrak{o} + y_1\mathfrak{o}$ with $v \cdot y_1 = 0$, $y_1^2 = 0$, and $P_2 = w\mathfrak{o} + y_2\mathfrak{o}$ with $w \cdot y_2 = 1$, $y_2^2 = 2\eta$ where η is a unit. Now $P_1^\perp$ is not isometric to $B(0)$, for otherwise $P_2^\perp \simeq B(\rho)$ and this violates Proposition 2.3(1). Similarly $P_1^\perp$ is not isometric to $B(\rho)$. Thus $P_1^\perp$ represents 2η (mod 4). (This may be verified by inspection if $\dim P_1^\perp = 2$. If $\dim P_1^\perp \geqslant 3$, we use the fact that $P_1^\perp$ is split by a lattice isomorphic to either $H(0)$ or $H(\rho)$.) Choose $x \in P_1^\perp$ such that $x^2 \equiv 2\eta$ (mod 4). Let $R = v\mathfrak{o} + (y_1 + x)\mathfrak{o}$, $S = P_2$. Then

$$\det R \equiv \det S \pmod 8,$$

i.e. $R \simeq S$. The lattices R, S satisfy the required conditions.

So finally we have $L = R \oplus R^\perp = S \oplus S^\perp$ with $R \simeq S$. Now $FR^\perp \simeq FS^\perp$ by Witt's theorem and $n(R^\perp) = n(S^\perp)$ by Proposition 2.1(1). Thus $R^\perp \simeq S^\perp$. The proposition now follows by applying Proposition 2.4 to the two-dimensional lattices R and S.

Case 3. $\operatorname{ord} v^2 \geqslant 1$, $T(v) \neq 0$. By Proposition 2.5, there exist proper unimodular lattices $P_1, P_2 \subset L$ such that $L = P_i \oplus P_i^\perp$ $(i = 1, 2)$, $v \in P_1$, $w \in P_2$, $\dim P_1 = \dim P_2 = 2$ and $P_i^\perp$ improper unimodular. If $P_1 \simeq P_2$ we define R, S by $R = P_1$, $S = P_2$. Now suppose that P_1 is not isometric to P_2. Then $P_1^\perp$ is not isometric to $P_2^\perp$ and we may assume without loss of generality that $P_1^\perp \simeq H(0) \oplus P$, $P_2^\perp \simeq H(\rho) \oplus P$ where P is a direct sum of hyperplanes. By Proposition 2.3(1, 2), P_i is not isometric to $B(0)$ or $B(\rho)$ $(i = 1, 2)$. Thus $\operatorname{ord} v^2 = 1$ (otherwise $\det P_1 \equiv -1 \pmod 4$), so that there are units ϵ_i, δ and vectors $x_i \in P_i$ $(i = 1, 2)$ such that $v^2 = 2\delta$, $x_i^2 = \epsilon_i$ $(i = 1, 2)$, $x_1 \cdot v = 1$, $x_2 \cdot w = 1$. Clearly $P_1 = v\mathfrak{o} + x_1\mathfrak{o}$ and $P_2 = w\mathfrak{o} + x_2\mathfrak{o}$. Now since $\det P_1/\det P_2 \equiv 1 \pmod 4$ and $\det P_i = -1 + 2\epsilon_i\delta_i$, we have $\epsilon_1\delta_1 \equiv \epsilon_2\delta_2$ (mod 2). Now since $P_1^\perp$ is improper and the residue class field is perfect, there is a vector $y \in P_1^\perp$ such that

$$\delta y^2 \equiv (\epsilon_2\delta_2 - \epsilon_1\delta_1) \pmod 4.$$

Let $R = v\mathfrak{o} + (y + x_1)\mathfrak{o}$, $S = P_2$. Now $\det R = \det S$. Furthermore since $v \in R$ and $T(v) \neq 0$, $R^\perp$ is improper unimodular. Similarly $S^\perp$ is improper unimodular. Since $\det R^\perp = \det S^\perp$, we have $R^\perp \simeq S^\perp$ and therefore $R \simeq S$.

So we now have R, S such that $v \in R$, $w \in S$, $L = R \oplus R^\perp = S \oplus S^\perp$, $R \simeq S$, $R^\perp \simeq S^\perp$, $\dim R = \dim S = 2$, $T(v) = T(w)$. The theorem now follows by applying Proposition 2.4 to the lattices R and S.

3. Vectors with one critical index. Suppose the lattice L has the decomposition $L = \sum_\oplus L_i$ where L_i is 2^i-modular or zero. Then, correspondingly,

https://doi.org/10.4153/CJM-1966-092-x Published online by Cambridge University Press

each vector $v \in L$ has the unique decomposition $v = \sum_{\oplus} 2^{h_i} v_i$ where v_i is a maximal element of the lattice L_i. When we use the notation $T(v_i)$, it will be understood that this refers to our previously defined mapping acting on elements of the modular lattice L_i.

THEOREM 3.1. *Let $L = \sum_{\oplus} L_i = \sum_{\oplus} M_i$ be two decompositions of L such that L_i, M_i are 2^i-modular or zero lattices. Let $v, w \in L$ where*

$$v = \sum_{\oplus} 2^{h_i} u_i = \sum_{\oplus} 2^{k_i} v_i, \qquad w = \sum_{\oplus} 2^{l_i} w_i$$

and u_i, w_i are maximal in L_i, v_i are maximal in M_i. If, in addition, $v \sim w$, then

$$T(u_{\lambda_i}) = T(v_{\lambda_i}) = T(w_{\lambda_i})$$

where the λ_i are the critical indices of v and w.

Proof. If L_{λ_i} is improper, the result is trivial. We assume now that L_{λ_i} is proper. Let $\mathfrak{A}_i$ be the fractional ideal $2^i\mathfrak{o}$. Let

$$L_{(i)} = L^{\mathfrak{A}_i} = L_{\lambda_i} \oplus \{2L_{\lambda_{i-1}} + L_{\lambda_{i+1}} + \ldots\}$$

and

$$M = \{x : x \in L^{\mathfrak{A}_i} \text{ and } v \cdot x = 0\}.$$

Then the equalities follow immediately from two facts:
1. $T(v_\lambda) \neq 0$ if and only if for all $x \in M$, ord $x^2 > \lambda_i$.
2. If $y \in L_{(i)}$ and ord $y^2 = y_i$, then $T(v_{\lambda_i}) = 2^{-\lambda_i}(v \cdot y)^2/y^2$.
These two statements are easily proved using the relations between critical indices and exponents established in §1.

We devote the rest of this section to the consideration of vectors with one critical index. We assume that

$$L = \sum_{-\infty}^{\infty}{}_{\oplus} L_i$$

where L_i is 2^i-modular or empty, v and w are maximal elements of L,

$$v = \sum_{-\infty}^{\infty}{}_{\oplus} v_i, \qquad w = \sum_{-\infty}^{\infty}{}_{\oplus} w_i$$

where v_i, $w_i \in L_i$. For simplicity, we assume that 0 is the only critical index of v and w. (Since v, w are maximal, their critical exponent is 0.) We let

$$v' = \sum_{-\infty}^{0}{}_{\oplus} v_i, \qquad w' = \sum_{-\infty}^{0}{}_{\oplus} w_i.$$

All but a finite number of the L_i, v_i, w_i are, of course, zero.

PROPOSITION 3.1. *Suppose $T(v_0) \neq 0$. Let T_0 be any unit that represents $T(v_0)$. Then if*

$$\mathfrak{d}(1 + (v' - v_0)^2/T_0) = \mathfrak{d}(1 + (v - v')^2/T_0) = 0,$$

there is a vector $y \in L_0$ such that $v \sim y$.

Remark. $\mathfrak{d}(1 + (v' - v_0)^2/T_0)$ and $\mathfrak{d}(1 + (v - v')^2/T_0)$ are independent of the choice of T_0. If, for example, $\mathfrak{d}(1 + (v' - v_0)^2/T_0) = 0$, then since $(v' - v_0) \equiv 0 \pmod 2$, we have $(v' - v_0)^2 \equiv 0$ (mod 4 **(1**, Proposition 63.5**)**. So if $T'_0 \equiv T_0 \pmod 2$, then

$$1 + (v' - v_0)^2/T_0 \equiv 1 + (v' - v_0)^2/T'_0 \pmod 8.$$

Therefore $\mathfrak{d}(1 + (v' - v_0)^2/T'_0) = 0$ by **(1**, Proposition 63.2**)**.

Proof. We may write

$$L_0 = \sum_1^m{}_\oplus \langle x_i \rangle$$

where

$$v_0 = \sum_1^m{}_\oplus x_i.$$

Let

$$M_0 = \langle x_i + (v - v') \rangle \oplus \sum_2^m{}_\oplus \langle x_i \rangle.$$

Since $\mathfrak{d}(1 + (v - v')^2/T_0) = 0$, we have $\det L_0 = \det M_0$, i.e. $L_0 \simeq M_0$. Let K be the lattice such that

$$\sum_0^\infty{}_\oplus L_i = M_0 \oplus K.$$

A simple application of **(1**, Theorem 93.29**)** shows that

$$K \simeq \sum_1^\infty{}_\oplus L_i.$$

A second application of this procedure, this time to the "left-hand side" of v, gives us lattices N_0, J such that

$$v \in N_0, \qquad N_0 \simeq M_0, \qquad J \simeq \sum_{-\infty}^{-1}{}_\oplus L_i.$$

Let ϕ be an isometry such that

$$\phi(N_0) = L_0, \qquad \phi\left(\sum_{-\infty}^{-1}{}_\oplus L_i\right) = J, \qquad \text{and } \phi\left(\sum_1^\infty{}_\oplus L_i\right) = K.$$

Then $y = \phi(v)$ is the required vector.

PROPOSITION 3.2. *Let $w_i = 0$ for all $i \leqslant -1$ and $T(v_0) = T(w_0) \neq 0$. Then $v \sim w$ if and only if $\mathfrak{d}(1 + (v' - v_0)^2/T_0) = 0$ where T_0 is any unit representing $T(v_0)$.*

Proof. Necessity: We may, by Proposition 3.1, assume that $v_i = 0$ if $\mathfrak{d}(1 + v_i^2/T_0) = 0$, provided $i \neq 0$. In particular, we assume that $v_{-3-k} = 0$ if $k \geqslant 0$.

Let $\langle v\rangle^\perp = J \oplus \text{rad } \langle v\rangle^\perp$ and $\langle w\rangle^\perp = K \oplus \text{rad } \langle w\rangle^\perp$. Now if v were equivalent to w, we would have $J \simeq K$. We shall prove that if $\mathfrak{d}(1 + (v' - v_0)^2/T_0) \neq 0$, then J is not isometric to K.

There are three cases to be considered.

Case 1. $v_{-1} = 0$, ord $v_{-2}^2 = 2$. Here both L_{-2} and L_0 are proper. We may write

$$L_0 = \sum_1^m \oplus \langle x_i\rangle \qquad \text{where } v_0 = \sum_1^m \oplus x_i.$$

Furthermore, there is a lattice L'_{-2} such that $L_{-2} = \langle 2^{-2}v_{-2}\rangle \oplus L'_{-2}$.

We now construct a new decomposition $L = \sum_\oplus M_i$. If $i \neq -2.0$, let $L_i = M_i$. Let

$$M_0 = \langle x_1 + v_{-2}\rangle \oplus \sum_2^m \oplus \langle x_i\rangle.$$

Now there is a vector y such that $\langle y\rangle \oplus \langle x_1 + v_{-2}\rangle = \langle 2^{-2}v_{-2}\rangle \oplus \langle x_1\rangle$. We let $M_{-2} = \langle y\rangle \oplus L'_{-2}$. Now

$$d(M_{-2})/d(L_{-2}) = d(M_0)/d(L_0) = 1 + (v' - v_0)^2/T_0 = 1 + 4\rho.$$

Also $v \cdot M_i = 0$ if $i < 0$. Therefore the Jordan decompositions of J and K have the following forms:

$$J = \sum_{-\infty}^{-1} \oplus L_i \oplus \sum_0^\infty \oplus N_j, \qquad K = \sum_{-\infty}^{-1} \oplus M_i \oplus \sum_0^\infty \oplus N'_j.$$

If N is the first non-zero N_j, then $n(N) \subseteq 2\mathfrak{o}$ since $T(v_0) \neq 0$.

We wish to show that J is not isometric to K. There are three subcases.

(a) L_{-1} is improper and non-zero. Then $n(L_{-1})n(N)/s(L_{-1})^2 \subseteq 8\mathfrak{o}$. But

$$d\left(\sum_{-\infty}^{-1} \oplus M_i\right) \Big/ d\left(\sum_{-\infty}^{-1} \oplus L_i\right) = 1 + 4\rho.$$

Therefore condition (i) of **(1**, 93.29**)** is violated, i.e. J is not isometric to K.

(b) $L_{-1} = 0$. Here $n(L_{-2})n(N)/s(L_{-2})^2 \subseteq 8\mathfrak{o}$. Once again condition (i) of **(1**, 93.29**)** is violated.

(c) L_{-1} is proper. Then $n(N) \subseteq 4n(L_{-1})$. If J were isomorphic to K, we would have by condition (ii) of **(1**, 93.29**)** that

$$F\left(\sum_{-\infty}^{-1} \oplus L_i\right) \to F\left(\sum_{-\infty}^{-1} \oplus M_i\right) \oplus \langle \tfrac{1}{2}\rangle.$$

By Witt's theorem, this would imply that $\langle 2^{-2}v_{-2}\rangle \to \langle y\rangle \oplus \langle\frac{1}{2}\rangle$, which would mean that $\langle \epsilon(1 + 4\rho)\rangle \oplus \langle 2(1 + 4\rho)\rangle \simeq \langle\epsilon\rangle \oplus \langle 2\rangle$ where $\epsilon = 4y^2$. A calculation with Hasse symbols shows this to be false. Therefore J is not isometric to K.

https://doi.org/10.4153/CJM-1966-092-x Published online by Cambridge University Press

Case 2. ord $v_{-1}^2 = 1$. By means of a procedure similar to that used above we may write

$$J = \sum_{-\infty}^{-1}\oplus L_i \oplus \sum_{0}^{\infty}\oplus N_i \quad \text{and} \quad K = \sum_{-\infty}^{-1}\oplus M_i \oplus \sum_{0}^{\infty}\oplus N'_i,$$

where, if N is the first non-zero N_i, then $n(N) \subseteq 2\mathfrak{o}$. Furthermore, these two decompositions have the following property:

$$d\Big(\sum_{-\infty}^{-1}\oplus L_i\Big) \Big/ d\Big(\sum_{-\infty}^{-1}\oplus M_i\Big) = 1 + 2\epsilon$$

where ϵ is some unit. But here $n(L_{-1})n(N)/s(L_{-1})^2 \subseteq 4\mathfrak{o}$. Thus J is not isometric to K.

Case 3. ord $v_{-1}^2 = 2$. We assume that L_{-1} is proper, since the usual determinantal arguments work when L_{-1} is improper. Since

$$\mathfrak{d}(1 + (v_{-2}^2 + v_{-1}^2)/T_0) = 4\mathfrak{o},$$

we have $\mathfrak{d}(1 + v_{-2}^2/T_0) = 0$ by **(1**, 63.4**)**. Therefore, by Proposition 3.1, we may assume that $v_{-2} = 0$. We construct a new decomposition, $L = \sum_\oplus M_i$. When $i \neq -1, 0$, let $L_i = M_i$. Write

$$L_0 = \sum_{1}^{m}\oplus \langle x_i\rangle \qquad \text{where } v_0 = \sum_{1}^{m}\oplus x_i.$$

Also choose y_1 and y_2 such that $v_{-1} = 2(y_1 + y_2)$ and $L_{-1} = \langle y_1\rangle \oplus \langle y_2\rangle \oplus R$, for some lattice R. Let $2y_i^2 = \epsilon_i (i = 1, 2)$. We choose a vector y'_1 such that

$$\langle x_1\rangle \oplus \langle y_1\rangle = \langle 2y_1 + x_1\rangle \oplus \langle y'_1\rangle$$

and choose also y'_2 such that

$$\langle 2y_1 + 2y_2 + x_1\rangle \oplus \langle y'_2\rangle = \langle y_2\rangle \oplus \langle x_1 + 2y_1\rangle.$$

Note that

$$y'_2\cdot(2y_1 + 2y_2 + x_1) = y'_1\cdot(2y_1 + x_1 + 2y_2) = y'_2\cdot y'_1 = 0.$$

Letting $M_{-1} = \langle y'_2\rangle \oplus \langle y'_1\rangle \oplus R$ and

$$M_0 = \langle x_1 + 2y_1 + 2y_2\rangle \oplus \sum_{2}^{m}\oplus \langle x_i\rangle,$$

we then have

$$L = \sum_{-\infty}^{\infty}\oplus M_i$$

as an alternative decomposition for L.

We remark that

$$(y')^2 = \alpha y_1^2, \qquad (y'_2)^2 = \beta y_2^2, \qquad d(L_{-1})/d(M_{-1}) = \alpha\beta$$

where

$$\alpha = (x_1^2 + 2\epsilon_1)/x_1^2, \qquad \beta = (x_1^2 + 2\epsilon_1 + 2\epsilon_2)/(x_1^2 + 2\epsilon_1),$$

and
$$\alpha\beta = 1 + (v' - v_0)^2/T_0,$$

these last three equalities being taken modulo the units squared.

As before, we have

$$J = \sum_{-\infty}^{-1}{}_{\oplus}\, L_i \oplus \sum_{0}^{\infty}{}_{\oplus}\, N_i \quad \text{and} \quad K = \sum_{-\infty}^{-1}{}_{\oplus}\, M_i \oplus \sum_{0}^{\infty}{}_{\oplus}\, N'_i$$

as Jordan decompositions for J and K. Now $n(N_i) \subseteq 4n(L_{-1})$ for $i \geqslant 0$. By **(1**, 93.29 (ii)**)**, if J were isomorphic to K we would have

$$F\Big(\sum_{-\infty}^{-1}{}_{\oplus}\, L_i\Big) \to F\Big(\sum_{-\infty}^{-1}{}_{\oplus}\, M_i\Big) \oplus \langle \tfrac{1}{2} \rangle.$$

Using Witt's theorem and **(1**, 63.21**)**, we would have

$$\langle \alpha\epsilon_1 \rangle \oplus \langle \beta\epsilon_2 \rangle \oplus \langle \alpha\beta \rangle \simeq \langle \epsilon_1 \rangle \oplus \langle \epsilon_2 \rangle \oplus \langle 1 \rangle.$$

To prove that J is not isometric to K, we need only show that this previous isometry does not hold. A calculation with Hasse symbols (using the fact that $\mathfrak{d}(\alpha\beta) = 4\mathfrak{o}$) reduces the problem to showing that $(\alpha, \alpha\epsilon_1\epsilon_2) = -1$, or equivalently, that the lattice

$$N = \sum_{1}^{3}{}_{\oplus}\, z_i$$

(where $z_1^2 = \alpha$, $z_2^2 = \alpha\epsilon_1\epsilon_2$, $z_3^2 = -1$) is anisotropic. To do this, we prove that N contains a sublattice N' isometric to $H(\rho)$. (This will prove that N is anisotropic by Proposition 2.3(4).)

We let $N' = (\epsilon_1 z_1 + z_2)\mathfrak{o} + \{(z_1 + z_3)/\alpha\epsilon_1\}\mathfrak{o}$. This lattice is represented symbolically by the matrix

$$\begin{vmatrix} \alpha\epsilon_1(\epsilon_1 + \epsilon_2) & 1 \\ 1 & 2/\alpha^2\epsilon_1) \end{vmatrix}.$$

Now $2(\epsilon_1 + \epsilon_2) = (v' - v_0)^2$; hence $\epsilon_1 + \epsilon_2 \equiv 0 \pmod 2$. Therefore N' is improper unimodular. Since $\alpha \equiv 1 \pmod 2$, we have

$$-(\det N') \equiv 1 - 2(\epsilon_1 + \epsilon_2) \equiv 1 + 4\rho \pmod 8.$$

Therefore $N' \simeq H(\rho)$. This proves Case 3.

Sufficiency. We have $\mathfrak{d}(1 + (v' - v_0)^2/T_0) = 0$. Now the fact that

$$T(v_0) = T(w_0) \neq 0$$

implies that $\mathfrak{d}(1 + (v_0^2 - w_0^2)/T_0) = 0$. Since $v^2 = w_0^2$ and

$$\mathfrak{d}(1 + (v' - w_0)^2/T_0) = 0,$$

we then have $\mathfrak{d}(1 + (v - v')^2/T_0) = 0$.

https://doi.org/10.4153/CJM-1966-092-x Published online by Cambridge University Press

Consequently, we may apply Proposition 3.1 to find a vector $x \in L_0$ such that $x \sim v$. Furthermore, $T(x) = T(v_0) = T(w_0)$ in L_0 by Theorem 3.1. By Theorem 2.1, we now have $x \sim w$. This proves the sufficiency.

PROPOSITION 3.3. *Let $v^2 = w^2$, $T(v_0) = T(w_0) \neq 0$. Then $v \sim w$ if and only if $\mathfrak{d}(1 + [(v')^2 - (w')^2]/T_0) = 0$ where T_0 is any unit representing $T(v_0)$.*

Proof. We construct a second decomposition $L = \sum_\oplus M_i$. Let $M_i = L_i$ if $i > 0$. We write

$$L_0 = \sum_1^m{}_\oplus \langle x_i \rangle \qquad \text{where } \sum_1^m{}_\oplus x_i = w_0.$$

Let

$$M_0 = \langle w' - w_0 + x_i \rangle \oplus \sum_2^m{}_\oplus \langle x_i \rangle.$$

When $i < 0$, choose M_i such that

$$\sum_{-\infty}^0 M_i = \sum_{-\infty}^0 L_i.$$

Then if $v = \sum_\oplus y_i$ where $y_i \in M_i$, then

$$\mathfrak{d}\left(1 + \sum_{-\infty}^{-1} y_i^2/T_0\right) = \mathfrak{d}(1 + [(v')^2 - (w')^2 + (w')^2 - y_0^2]/T_0)$$
$$= \mathfrak{d}(1 + [(v')^2 - (w')^2]/T_0).$$

($\mathfrak{d}(1 + [(w')^2 - y^2]/T_0) = 0$ because $T(y_0) = T(w')$ in M_0.) The result now follows from Proposition 3.2 because $w' \in M_0$.

PROPOSITION 3.4. *Let $L = J_1 \oplus K_1 = J_2 \oplus K_2$ where J_1, J_2 are modular improper. Then $J_1 \simeq J_2$ implies that $K_1 \simeq K_2$.*

Proof. We may, by scaling, assume that J_1 and J_2 are unimodular. The result follows from (**1**, 93.14) if $J_1 \simeq J_2 \simeq H(0)$. If $J_1 \simeq H(\rho)$, then

$$H(\rho) \oplus J_1 \oplus K_1 \simeq H(\rho) \oplus J_2 \oplus K_2.$$

But $H(\rho) \oplus H(\rho) \simeq H(0) \oplus H(0)$. Thus

$$H(0) \oplus H(0) \oplus K_1 \simeq H(0) \oplus H(0) \oplus K_2.$$

Therefore $K_1 \simeq K_2$.

PROPOSITION 3.5. *If $v^2 = w^2$ and $T(v_0) = T(w_0) = 0$, then $v \sim w$.*

Proof. Since v has only one critical index, we may assume that $v \in L_0$. There are two cases to consider.

Case 1. ord $v^2 = 0$. Then $L = \langle v \rangle \oplus \langle v \rangle^\perp = \langle w \rangle \oplus \langle w \rangle^\perp$. Furthermore, since $T(v_0) = T(w_0) = 0$, $\langle v \rangle^\perp$ and $\langle w \rangle^\perp$ have proper, unimodular components. Thus, by (**1**, 93.14(a)), $\langle v \rangle^\perp \simeq \langle w \rangle^\perp$.

Case 2. $\operatorname{ord} v^2 \geqslant 1$. Then $\operatorname{ord} w_0^2 \geqslant 1$. First assume that L_0 contains a hyperplane. In this case, there are vectors $x, y \in L_0$ such that $x^2 = w_0^2$, $x \cdot y = 1$, $y^2 = 0$. By Theorem 2.1 there is an isometry ϕ that leaves every element of L_i fixed if $i \neq 0$ and maps w_0 onto x. Let $w'' = \phi(w) = x + w - w_0$. Let $J = (x + w - w_0)\mathfrak{o} + y\mathfrak{o}$. Then $J \simeq H(0)$ and J splits L. Similarly there is a lattice $K \simeq H(0)$ that splits L and a vector $v'' \sim v$ such that $v'' \in K$. Write $L = K \oplus K' = J \oplus J'$. Then by Proposition 3.4, $J' \simeq K'$. Furthermore, by Proposition 2.1, there is an isometry ψ such that $\psi(K) = J$ and $\psi(w'') = v''$. Thus $w'' \sim v''$, which implies $v \sim w$.

Now assume that L_0 contains no hyperplanes. By Proposition 2.5, we may embed w_0 in an improper lattice $L = w_0\mathfrak{o} + x\mathfrak{o}$ which splits L_0. We may assume that $w_0 \cdot x = 1$. Let $w_0^2 = \mu_1$ and $x^2 = \lambda_1$. We may similarly embed v in an improper lattice $H' = v\mathfrak{o} + y\mathfrak{o}$ which splits L_0. We let $v^2 = \mu_2$, $v \cdot y = 1$, $y^2 = \lambda_2$. We have $H \simeq H' \simeq H(\rho)$. Let $H'' = w\mathfrak{o} + x\mathfrak{o}$. If $H'' \simeq H(\rho)$, then there exist lattices R, S such that $L \simeq H'' \oplus R = H' \oplus S$, with $R \simeq S$ by Proposition 3.4. The result then follows by Theorem 2.1. Otherwise $H'' \simeq H(0)$. Here either $\operatorname{ord} w_{-1}^2 = 1$ or $\operatorname{ord} w_1^2 = 1$. Assume that $\operatorname{ord} w_{-1}^2 = 1$. (The other possibility is handled in a similar manner.) Let ϵ be a unit such that $\lambda_2 + \epsilon^2 w_{-1}^2 \equiv 0 \pmod 4$. Let $H''' = v\mathfrak{o} + (y + \epsilon w_{-1})\mathfrak{o}$. Then

$$H''' \simeq H(0) \simeq H''.$$

Also $v \in H'''$, $w \in H''$, and H''' splits L. The result then follows from Proposition 3.4 and Theorem 2.1.

We now have the result for vectors with one critical index. We use the same notation as before.

THEOREM 3.2. *Suppose that v and w are maximal vectors, both with only one critical index $\lambda_1 = 0$. Then $v \sim w$ if and only if:*

1. $T(v_0) = T(w_0)$ *over* L_0.
2. $v^2 = w^2$.
3. $\mathfrak{d}(1 + [(v')^2 - (w')^2]/T_0) = 0$ *if* $T(v_0) \neq 0$

where T_0 is any unit representing $T(v_0)$.

4. Vectors with several critical indices. We now wish to find necessary and sufficient conditions that characterize the equivalence of two vectors, each having several critical indices. We have already shown that if $v \sim w$, then v and w have the same critical indices λ_i and exponents f_i and furthermore $T(v_{\lambda_i}) = T(w_{\lambda_i})$.

We first make a remark about notation. All Jordan decompositions of L will be written in the form $L = \sum_\oplus L_i$, $L = \sum_\oplus L'_i$, etc. where $L_i, L'_i, \ldots$ are 2^i-modular. Correspondingly, if $v \in L$, then $v = \sum_\oplus v_i = \sum_\oplus v'_i$, etc. where $v_i \in L_i$, $v'_i \in L'_i, \ldots$. Recalling that $s_i = \lambda_{i+1} + f_{i+1} - \lambda_i - f_i$, we let

$$v_{(i)} = \sum_{-\infty}^{\lambda_i + s_i}{}_\oplus v_j \quad \text{and} \quad v_{[i]} = \sum_{-\infty}^{\lambda_i}{}_\oplus v_j.$$

$v'_{(i)}$ and $v'_{[i]}$ are similarly defined. For simplicity, we assume that $s(L) = \mathfrak{o}$. This will make no difference to the final result.

PROPOSITION 4.1. *Let $v \sim w$. Then*

$$\text{ord } (v^2_{(i)} - w^2_{(i)}) \geqslant \lambda_{i+1} + f_{i+1} + f_i + \Delta_i$$

where

$$\Delta_i = 0 \qquad \text{if } L_{\lambda_i + s_i} \text{ is proper,}$$

$$\Delta_i = 1 \qquad \text{if } L_{\lambda_i + s_i} \text{ is improper.}$$

Proof. We let $L = M \oplus N$ where

$$M = \sum_0^{\lambda_i + s_i} L_j.$$

We may write $v = r \oplus r'$, $w = s \oplus s'$ where $r, s \in M$ and $r', s' \in N$. Now let ϕ be an isometry on L such that $\phi(v) = w$. We let $\phi(r) = t \oplus t'$,

$$\phi(r') = u \oplus u',$$

where $t, u \in M$ and $t', u' \in N$. Now $\phi(r) = (s - u) + (s' - u')$ and we know from the facts concerning critical indices that $2^{f_i}|r$ (that is, $2^{-f_i}r \in L$) $2^{f_i}|s$, $2^{f_i}|u$. Therefore $2^{f_i}|(s' - u')$. Hence

$$\begin{aligned} \text{ord } \{r^2 - (s-u)^2\} - \text{ord } (s' - u')^2 &\geqslant 2f_i + \lambda_i + s_i + 1 \\ &= f_i + f_{i+1} + \lambda_{i+1} + 1. \end{aligned}$$

Also, the facts that

$$\text{ord } u \cdot L \geqslant \text{ord } r' \cdot L \geqslant \lambda_{i+1} + f_{i+1}$$

and $2^{f_i}|s$ imply that ord $2s \cdot u \geqslant f_i + f_{i+1} + \lambda_{i+1} + 1$. Thus

$$\text{ord } (r^2 - (s^2 + u^2)) \geqslant f_i + f_{i+1} + \lambda_{i+1} + 1.$$

We now prove that ord $u^2 \geqslant f_i + f_{i+1} + \lambda_{i+1} + \Delta_i$. This will prove the proposition since $r = v_{(i)}$ and $s = w_{(i)}$. Note that λ_{i+1} is the smallest critical index of $\phi(r') = u \oplus u'$. This means that we may write

$$u = \sum_0^{\lambda_i + s_i}{}_{\oplus}\, 2^{h_j} u_j$$

where u_j is maximal in L_j and

$$h_j \geqslant f_{i+1} + (\lambda_{i+1} - j) = f_i + (s_i + \lambda_i) - j.$$

Hence

$$\text{ord } (2^{2h_j} u_j^2) \geqslant h_j + \lambda_{i+1} + f_{i+1} + E_j$$

where $E_j = 1$ if L_j is improper, $E_j = 0$ if L_j is proper. But

$$h_i + \lambda_{i+1} + f_{i+1} + E_j \geqslant f_i + \lambda_i + f_{i+1} + \Delta_i$$

for $0 \leqslant j \leqslant \lambda_i + s_i$. This proves the theorem.

We now find a similar relation holding for $v_{[i]}$ and $w_{[i]}$. To do this, we first need a lemma.

LEMMA 4.1. *Let $L = \oplus L_i = \oplus K_i$ be two Jordan decompositions for L in which $L_i \simeq K_i$. Then there is a finite sequence of decompositions*

$$L = \sum_{\oplus} L_i^{(k)} \qquad (k = 0, \ldots, m)$$

with the following properties:

(a) $L_i^{(0)} = L_i$;
(b) $L_i^{(m)} = K_i$;
(c) $L_i^{(k)} \simeq L_i \qquad (k = 0, \ldots, m)$;
(d) *if* $S_k = \{i : L_i^{(k)} \neq L_i^{(k+1)}\}$,

then S_k consists of 2 integers or 3 consecutive integers.

Proof. We show the existence of a chain of decompositions

$$L = \sum_{\oplus} L_i^{(k)}, \qquad (k = 0, \ldots, t)$$

satisfying (a), (c), (d) and such that $L_0^{(t)} = K_0$. The result then follows by induction on the lengths of the decomposition.

$L_i^{(1)}$ is obtained in the following manner: We may write

$$K_0 = x_1\,\mathfrak{o} + \ldots + x_r\,\mathfrak{o}.$$

Furthermore, each x_i has an expansion

$$x_i = \sum_{j=0}^{s}{}_{\oplus}\, v_{ij}.$$

Now let

$$x_i^{(1)} = \sum_{j=0}^{2}{}_{\oplus}\, v_{ij} \quad \text{and} \quad L_0^{(1)} = x_1^{(1)}\mathfrak{o} + \ldots + x_r^{(1)}\mathfrak{o}.$$

Then $L_0^{(1)} \simeq L_0$ since $x_i \cdot x_j \equiv x_i^{(1)} \cdot x_j^{(1)} \pmod 8$. Furthermore, there are lattices $L_1^{(1)}$, $L_2^{(1)}$ such that $L_0 \oplus L_1 \oplus L_2 = L_0^{(1)} \oplus L_1^{(1)} \oplus L_2^{(1)}$. Now if we let $L_j^{(1)} = L_j$ when $j > 2$, the decomposition $L = \oplus L_i^{(1)}$ satisfies (a), (c), (d).

Now, if $k > 1$, we let

$$x_i^{(k)} = \sum_{j=0}^{k+1}{}_{\oplus}\, v_{ij} \quad \text{and} \quad L_0^{(k)} = \sum x_i^{(k)}\mathfrak{o}.$$

Then $L_0^{(k)} \simeq L_0$. We define $L_i^{(k)}$ inductively by the relations

$$L_0^{(k-1)} \oplus L_{k+1}^{(k-1)} = L_0^{(k)} \oplus L_{k+1}^{(k)}$$

and $L_i^{(k)} = L_i^{(k-1)}$ if $i \neq 0$, $k + 1$. Clearly $L_0^{(r-1)} = K_0$ and the sequence $L_0^{(k)}$ possesses properties (a), (c), (d). This proves the theorem.

PROPOSITION 4.2. *If $v \sim w$ and $T(v_{\lambda_i}) \neq 0$, then*

$$\mathfrak{d}(1 + \{(v_{[i]}^2 - w_{[i]}^2)/2^{2f_i+\lambda_i} \cdot T_i\}) = 0$$

where T_i is any unit representing $T(v_{\lambda_i})$.

Proof. We establish the following equivalent result: If $L = \sum_{\oplus} L_j = \sum_{\oplus} L'_j$ where $L_j \simeq L'_j$ and if $T(v_{\lambda_i}) \neq 0$, then

$$\mathfrak{d}\{1 + [v_{[i]}{}^2 - (v_{[i]}')^2]/2^{2f_i+\lambda_i} \cdot T_i\} = 0.$$

By Lemma 4.1, we may assume that there exists an integer r or a pair of integers s, t such that $L_j \simeq L'_j$ when either (a) $j \neq s, t$ or (b) $j \neq r, r+1, r+2$. We do these cases separately.

Case (a). The result is easily obtained except when $s < \lambda_i < t$ or $t < \lambda_i < s$. Assume $s < t$. Letting $x = v_s \oplus v_t$ and $y = v'_s \oplus v'_t$, we see that x and y have the same critical indices and exponents. There are three possibilities. The critical indices of x may be (1) s and t, (2) s, (3) t. In the first case we have by Proposition 4.1 that

$$\text{ord } ((v_s)^2 - (v'_s)^2 \geqslant g_s + g_t + t + 1$$

where g_s, g_t are the critical exponents of x. But $g_t + t \geqslant f_i + \lambda_i + 1$ and $g_s \geqslant f_i + 1$. Therefore

$$\{(v_s)^2 - (v'_s)^2\} \div \{2^{2f_i+\lambda_i} T_i\} \equiv 0 \pmod 8,$$

hence the result.

Now if s is the only critical index of x, we have $2^{f_i+1}|v_s$ since λ_i is a critical index of v and $s < \lambda_i$. Therefore $2^{f_i+1}|v_t$ since s is the only critical index of x. Thus

$$\text{ord } v_t{}^2 \geqslant 2(f_i + 1) + t \geqslant 2(f_i + 1) + \lambda_i + 1.$$

The same inequality holds for ord $(v'_t)^2$. Since $x^2 = y^2$, we again obtain (x).

If t is the only critical index, the result is obtained in a similar manner to that of the above case.

Case (b). The result follows easily except when $r + 1 = \lambda_i$. But here if we let $x = v_r + v_{r+1} + v_{r+2}$, $y = v'_r + v'_{r+1} + v'_{r+2}$, then r is the only critical index of x and y. Here the result follows directly from Theorem 3.1.

We have now obtained several necessary conditions for equivalence. The rest of this section will be devoted to showing that these conditions are also sufficient.

THEOREM 4.1. *Using the notation previously defined, we have* $v \sim w$ *if and only if:*

1. $v^2 = w^2$,
2. v, w *have the same critical indices* λ_i, *and exponents* f_i,
3. $T(v_{\lambda_i}) = T(w_{\lambda_i})$,
4. ord $(v_{(i)}{}^2 - w_{(i)}{}^2 \geqslant \lambda_{i+1} + f_{i+1} + f_i + \Delta_i$,
5. $\mathfrak{d}(1 + \{(v_{[i]}{}^2 - w_{[i]}{}^2)/2^{2f_i+\lambda_i} \cdot T_i\}) = 0$,

where

$$\Delta_i = 1 \qquad \text{if } L_{\lambda_i+s_i} \text{ is improper},$$

$$\Delta_i = 0 \qquad \text{if } L_{\lambda_i+s_i} \text{ is proper}$$

and T_i *is any unit representing* $T(v_{\lambda_i})$.

The sufficiency of the conditions will be proved in several stages. The necessity, of course, has already been shown. We shall assume from here on that 1–5 are satisfied for v and w.

PROPOSITION 4.3. *Let* x *be a maximal element of a unimodular lattice* L. *Then if* α *is any integer, there is a vector* $y \in L$ *such that* y *is maximal*, $T(x) = T(y)$, *and* $y^2 = x^2 + 4\alpha$ *provided* $\mathfrak{d}(1 + 4\alpha/T_0) = 0$ *when* $T(x) = 0$ *and* T_0 *is any unit representing* $T(x)$.

Proof. Let $x^2 = \eta$. We first assume $T(x) = 0$. Then if ord $\eta = 0$ there is a vector $x' \in L$ such that the lattice $\langle x \rangle \oplus \langle x' \rangle$ splits L. Choose any integer β such that $(x')^2\beta^2 \equiv \alpha \pmod 2$. Then $\langle x + 2\beta x' \rangle \simeq \langle \eta + 4\alpha \rangle$ and furthermore $T(x + 2\epsilon x') = 0$; hence the result. Now if ord $\eta \geqslant 1$, there is a two-dimensional, improper lattice K, containing x, that splits L. Choose an integer μ such that

$$K \simeq \begin{vmatrix} \eta & 1 \\ 1 & \mu \end{vmatrix}.$$

Then the result follows from the fact that

$$K \simeq \begin{vmatrix} n + 4\alpha & 1 \\ 1 & \mu \end{vmatrix}.$$

If $T(x) \neq 0$, we may choose an orthogonal basis for $L = \sum_\oplus \langle x_i \rangle$ such that $x = \sum x_i$. The result follows from the fact that $\langle x_1^2 \rangle \simeq \langle T_0 \rangle \simeq \langle x_1^2 + 4\alpha \rangle$.

PROPOSITION 4.4. *There is a decomposition* $L = \sum_\oplus L'_i$ *with* $L_i \simeq L'_i$ *such that one of the following two congruence relations holds:*

1. ord $((v'_{(1)})^2 - (w_{(1)})^2) \geqslant f_1 + f_2 + \lambda_2 + 1$.
2. ord $((w_{(1)} - w_{\lambda_1+s_1})^2 - (v'_{(1)} - v_{\lambda_1+s_1})^2) \geqslant f_1 + f_2 + \lambda_2 + 1$.

Proof. If $L_{\lambda_1+s_1}$ is improper, the result is trivial by condition 4 of Theorem 4.1. If $T(v_{\lambda_1}) \neq 0$ and $s_1 = 1$, then $v_{(1)} - v_{\lambda_1+s_1} = v_{[1]}$ and $w_{[1]} = w_{(1)} - w_{\lambda_1+s_1}$. Here the result is an outcome of condition 5 since

$$\text{ord } (v_{(1)}{}^2 - w_{[1]}{}^2) \geqslant 2f_1 + \lambda_1 + 2 = \lambda_2 + f_1 + f_2 + 1.$$

We now assume that $L_{\lambda_1+s_1}$ is proper and $s_1 \neq 1$ if $T(v_\lambda) \neq 0$. Let

$$x = v_{(1)} - v_{\lambda_1+s_1}$$

and $y = w_{(1)} - w_{\lambda_1+s_1}$. We may assume that ord $(x^2 - y^2) = f_1 + f_2 + \lambda_2$.

There is a vector $z \in L_{\lambda_1+s_1}$ such that

$$\operatorname{ord}\,(y^2 + z^2 - v_{(1)}{}^2) \geqslant \lambda_2 + f_2 + f_1 + 1.$$

We apply Proposition 4.3 to find a vector $\mu_{\lambda_1} \in L_{\lambda_1}$ such that $T(\mu_{\lambda_1}) = T(w_{\lambda_1})$, $\exp \mu_{\lambda_1} = f_1$, and

$$\mu_{\lambda_1}{}^2 = w_1{}^2 + v_{(1)}{}^2 - y^2 - z^2.$$

We now let $u_j = w_j$ when $j \leqslant \lambda_1 - 1$ or $\lambda_1 + 1 \leqslant j \leqslant \lambda_1 + s_1 - 1$, and $u_{\lambda_1+s_1} = z$. We also define

$$u = \sum_0^{\lambda_i+s_i}{}_{\oplus}\, u_j.$$

Of course, $u_j \in L_j$. Also $u^2 = u_{(1)}{}^2 = v_{(1)}{}^2$. The requirements for Theorem 3.1 are satisfied for the vectors $u_{(1)}$ and $v_{(1)}$. Hence there is an isometry ϕ on L such that $\phi(u_{(1)}) = v_{(1)}$. Let $L'_i = \phi(L_i)$. The decomposition $L = \sum_\oplus L'_i$ satisfies condition 2 of the proposition since

$$\begin{aligned}\operatorname{ord}\,[(v'_{(1)} - v'_{\lambda_1+s_1})^2 - (w_{(1)} - w_{\lambda_1+s_1})^2] &= \operatorname{ord}\,[(v_{(1)}{}^2 - z^2 - y^2] \\ &\geqslant \lambda_2 + f_2 + f_1 + 1.\end{aligned}$$

PROPOSITION 4.5. *Suppose $L = L_j \oplus L_m$ where L_j is 2^j-modular and L_m is 2^m-modular. Assume that $v = v_j \oplus v_m$ has critical indices $\lambda_1 = j$, $\lambda_2 = m$, exponents f_1, f_2, and $T(v_j) = 0$. Let η be an integer such that*

$$\operatorname{ord}\,(\eta - v_j{}^2) \geqslant f_1 + f_2 + \lambda_2 + 1.$$

Then there is a decomposition $L = L''_j \oplus L''_m$ such that $v''_j{}^2 = \eta$ and $L''_j \simeq L_j$, $L''_m \simeq L_m$ provided

$$\mathfrak{d}\{1 + (v^2{}_j - \eta)/T_2.\, 2^{2f_2+\lambda_2}\} = 0$$

when $T_2 \neq 0$ and $f_1 - f_2 = 1$.

Proof. We may assume by scaling that $j = 0, f_2 = 0$. *Let* $f = f_1$.

Our method is the following. We show that if $\operatorname{ord}\,\{v_0{}^2 - \eta\} = f + m + k + 1$ (where $k \geqslant 0$), then there is a splitting $L = L'_0 \oplus L'_m$ such that

$$\operatorname{ord}\,\{v'_0)^2 - \eta\} \geqslant f + m + k + 2.$$

This allows us to construct a sequence of vectors $v \sim v^{(1)} \sim v^{(2)}$ such that

$$\lim_{i\to\infty} \{v_0{}^{(i)}\}^2 = \eta.$$

By the compactness of the unit sphere of F, there exists a vector w such that $v \sim w$ and $w_0{}^2 = \eta$. This fact is equivalent to the result we wish to prove.

Now since v_0 may be embedded in an improper two-dimensional sublattice of L_0, we may assume that L_0 is itself two-dimensional, improper. Choose a basis $\{x, y\}$ for L_0 such that $x^2 = y^2 = \delta$, $x \cdot y = 1$ where $\delta = 0$ or $\delta^2 \equiv 4\rho$ (mod 8). Then there are units ϵ, ϵ', and an integer $t \geqslant 0$, such that

$$v = 2^f(\epsilon x - 2^t \epsilon' y).$$

https://doi.org/10.4153/CJM-1966-092-x Published online by Cambridge University Press

Now let α be any unit. Then there is a vector $u_m \in L_m$ such that

$$v_m \cdot u_m = 2^m \alpha$$

and ord $u_m^2 \geqslant m + 1$ if $T(v_m) = 0$. Let $u_m^2 = 2^{m+i}\beta$ where β is a unit.

We let $x' = x + 2^k u_m$ and $L'_0 = x'\mathfrak{o} + y\mathfrak{o}$. Since $d(L_0) = d(L'_0)$, we have $L_0 \simeq L'_0$. Choose L'_m such that $L'_0 \oplus L'_m = L_0 \oplus L_m$. Now let $v'_0 = \mu x' + \gamma y$. We have

$$\mu\{\delta + 2^{2k+m+i}\beta\} + \gamma = 2^f\epsilon\delta + 2^{f+t}\epsilon' + 2^{k+m}\alpha,$$

$$\mu + \delta\gamma = 2^f\epsilon + 2^{f+t}\epsilon'\delta,$$

as a result of the relations $v'_0 \cdot x' = v \cdot x'$ and $v'_0 \cdot y = v_0 \cdot y$.

We solve the above equations for μ and γ and then calculate $(v'_0)^2$. Using the facts that $n > f > 0$ and ord $\delta \geqslant 1$, we arrive at the congruence

$$\{v_0^2 - (v'_0)^2\} \equiv 2^{f+m+k+1}\epsilon\alpha + 2^{2f+2k+m+i}\epsilon^2\beta \pmod{2^{f+m+k+2}}.$$

Now $f + m + k + 1 < 2f + 2k + m + i$ provided $T(v_m) = 0$, or $f \neq 1$ or $k > 0$. In this case we choose u_m such that $2^{f+m+k+1}\epsilon\alpha = v_0^2 - \eta$. Now if $T(v_m) \neq 0, f = 1$, and $k = 0$, then

$$f + m + k + 1 = 2f + 2k + m + i = m + 2.$$

Therefore

$$v_0^2 = (v'_0)^2 \equiv 2^{m+2}(\epsilon\alpha + \epsilon^2\beta) \pmod{2^{m+3}}.$$

But the hypothesis implies that there is an integer γ such that

$$v_0^2 - n = 2^{m+2}T_2(\gamma + \gamma^2).$$

If we choose u_m such that $\alpha = \gamma T_2/\epsilon$, it is easily seen that $\beta \equiv \gamma^2 T_0/\epsilon^2 \pmod 2$. Thus

$$v_0^2 - (v'_0)^2 \equiv 2^{m+2}T_2(\gamma + \gamma^2) \equiv v_0^2 - \eta \pmod{2^{m+3}}.$$

This proves the proposition.

PROPOSITION 4.6. *Let $v \in L = L_0 \oplus L_m$. If the critical indices of v are $\lambda_1 = 0$, $\lambda_2 = n$, and the critical exponents are $f_1 = f, f_2 = 0$, and if η is an integer such that* ord $(v_0^2 - \eta) \geqslant f + m + 1$, *then there is a second decomposition*

$$L = L'_0 \oplus L'_m$$

such that $L_0 \simeq L'_0$, $L_m \simeq L'm$, and $(v'_0)^2 = \eta$ provided:

1. $\mathfrak{d}(1 + 2^{-m}(v^2_0 - \eta)/T_2) = 0$ *when* $T(v_m) \neq 0$, $s_1 = m - 1$.
2. $\mathfrak{d}(1 + 2^{-m}(v^2_0 - \eta)/T_1) = 0$ *when* $T(v_0) \neq 0$, $s_1 = 1$.

Proof. If $T(v_0) = 0$, the proposition follows from Proposition 4.5. If $T(v_n) = 0$, the result follows by applying Proposition 4.5 to $L\# = 2^{-m}L_m \oplus L_0$.

We now assume that $T(v_0) \neq 0$, $T(v_m) \neq 0$ and use the same method as in Proposition 4.5. We assume that $v_0^2 - \eta = \delta 2^{m+f+k+1}$, where $k \geqslant 0$, and δ is a unit. We find $L'_0 \simeq L_0$ such that ord $\{(v'_0)^2 - \delta\} \geqslant m + f + k + 2$.

We choose $y_i \in L_0$ such that

$$L_0 = \sum_1^r {}_{\oplus} \langle y_j \rangle \oplus M$$

where $r = 1$ or 2, and

$$v_0 = \sum_1^r {}_{\oplus} 2^f y_j.$$

Given any unit α, there is a vector $u_m \in L_m$ such that $w_m \cdot u_m = 2^m \alpha$. If we let $2^m \beta = u_m^2$, then $\beta \equiv \alpha^2/T_2 \pmod 2$. We define

$$L'_0 = \sum_1^r {}_{\oplus} \langle y'_j \rangle \oplus M$$

where $y'_1 = y_1 \oplus 2^k u_m$ and $y'_2 = y_2$ if $r = 2$. We have

$$(v'_0)^2 - v^2_0 \equiv \beta 2^{2f+2k+m} + \alpha 2^{f+k+m+1} + \alpha^2 T_1^{-1} 2^{2k+2m} \pmod{2^{f+k+m+2}}.$$

We first assume that $m > 2$. Then $\langle y_1 \rangle \simeq \langle y'_1 \rangle$ and therefore $L'_0 \simeq L_0$. Since $2k + 2m > f + m + k + 1$, the above congruence is the same as the relation obtained in Proposition 4.5. The relation ord $\{(v'_0)^2 - \eta)\} \geqslant f + m + k + 2$ can thus be solved.

Suppose now that $m = 2$. Then $f = 1$, $s_1 = 1$. The proposition follows if we can show the existence of an α such that $\langle y'_1 \rangle \simeq \langle y_1 \rangle$ and

$$\alpha^2 (T_1^{-1} + T_2^{-1}) 2^{4+2k} + \alpha \cdot 2^{4+k} \equiv (\eta - v_0^2) \pmod{2^{4+k+1}}.$$

If $k > 0$, this is easily done. We assume $k = 0$. Now $\eta - v_0^2 = 2^4 \delta$. A solution to the equation $(T_1^{-1} + T_2^{-1}) x^2 + x - \delta = 0$ exists because the hypotheses (1, 2) imply $\mathfrak{d}(1 + 4\delta/T_1) = \mathfrak{d}(1 + 4\delta/T_2) = 0$, which in turn implies $\mathfrak{d}(1 + 4\delta(T_1^{-1} + T_2^{-1})) = 0$. Let α be an integral solution to the equation. We need only show that $\langle y_1 \rangle \simeq \langle y'_1 \rangle$. Let $v'_0 \cdot y'_1 = 2\gamma (y'_1)^2$. We have $v_0 \cdot y_1 = 2 y_1^2$. Then $(v'_0)^2 - v_0^2 = 4(\gamma^2 (y'_1)^2 - y_1^2)$. Since we may choose $T_1 = y_1^2$, there is a unit μ such that $\gamma^2 (y'_1)^2 / y_1^2 - 1 = 4(\mu + \mu^2)$ (by hypothesis 2). Therefore $(y'_1)^2 / y_1^2 = (1 + 2\mu)^2 \gamma^{-2}$, i.e. $\langle y_1 \rangle \simeq \langle y'_1 \rangle$.

PROPOSITION 4.7. *There is a decomposition $L = \sum_{\oplus} L''_i$ such that $L_i \simeq L''_i$ and either $(v''_{(1)})^2 = w^2_{(1)}$ or $(v''_{(1)} - v_{\lambda_1 + s_1})^2 = (w_{(1)} - w_{\lambda_1 + s_1})^2$.*

Proof. Let $L = \sum_{\oplus} L'_i$ be a decomposition satisfying Proposition 4.4. Let

$$\alpha_1 = (v'_{(1)})^2 - w^2_{(1)} \quad \text{and} \quad \alpha_2 = (v'_{(1)} - v'_{\lambda_1 + s_1})^2 - (w_{(1)} - w_{\lambda_1 + s_1})^2.$$

Then either

(1) ord $\alpha_1 \geqslant \lambda_2 + f_1 + f_2 + 1$ or

(2) ord $\alpha_2 \geqslant \lambda_2 + f_2 + f_1 + 1$.

We also have (1) if $s_1 = \lambda_2 - \lambda_1 - 1$ and (2) if $s_1 = 1$. The proposition will be true if we can find L''_{λ_1}, L''_{λ_2} such that $L'_{\lambda_1} \simeq L''_{\lambda_1}$ and

$$L''_{\lambda_1} \oplus L''_{\lambda_2} = L'_{\lambda_1} \oplus L'_{\lambda_2},$$

and $(v''_{\lambda_1})^2 - (v'_{\lambda_1})^2 + \alpha_j = 0$ for $j = 1$ or 2. We let $m = \lambda_2$, $f = f_1$. Then, the existence of such L'_{λ_1} is a direct outcome of Proposition 4.6, provided that

(A) $\mathfrak{d}(1 + 2^{-m-2f}\alpha_j/T_2) = 0$ if $T(v_m) \neq 0$ and $s_1 = \lambda_2 - \lambda_1 - 1$; and

(B) $\mathfrak{d}(1 + 2^{-m-2f}\alpha_j/T_1) = 0$ when $T(v_0) \neq 0$ and $s_1 = 1$.

Both these conditions must be satisfied for $j = 1$, if (1) is satisfied, or else for $j = 2$ if (2) is satisfied. Now (A) is a consequence of hypothesis 5 of Theorem 4.1 (taking $i = 2$) because if $s_1 = m - 1$, then $v'_{[2]} = v'_{(1)} + v'_{\lambda 2}$ and

$$\mathfrak{d}(1 + 2^{-m-2f}\{(v'_{\lambda 2})^2 - (w'_{\lambda 2})^2\}/T_2) = 0,$$

if $T_2 \not\equiv 0 \pmod 2$. Now if $s_1 = 1$ and $s_1 \neq \lambda_2 - \lambda_1 - 1$, (2) is satisfied and (B) follows from (5) of Theorem 4.1 (taking $i = 1$). The only remaining case is where $s_1 = 1, f_1 - f_2 = 1$, but here it is not difficult to find a decomposition $L = \sum_\oplus L'_i$ such that both (A) and (B) are satisfied.

The proof of the Theorem is now quite easy. By Proposition 4.7, there is a decomposition $L = \sum_\oplus L'_i$ with $L_i \simeq L'_i$ and an integer $k = 0$ or 1 such that if

$$x = \sum_{0}^{\lambda_i + s_1 - k}{}_\oplus\, v'_i \quad \text{and} \quad y = \sum_{0}^{\lambda_1 + s_1 - k}{}_\oplus\, w_i,$$

then $x^2 = y^2$. But both x and y have only one critical index, λ_1, and satisfy the conditions of Theorem 3.2. Thus there is an isometry ϕ on L such that $\phi(L'_i) = L_i$ and $\phi(x) = y$. Furthermore, both $(v - x)$ and $w(-y)$ have one less critical index than v and w, and in addition they satisfy Theorem 4.1, 1–5. The proof now follows by induction.

We quote the corresponding result of Rosenzweig **(3)** obtained for the non-dyadic case. The procedure in this case is greatly simplified by the fact that non-zero modular lattices are proper, and the Jordan decomposition is unique up to an isometry between the components.

THEOREM 4.2. *Let F be a local field in which 2 is a unit. Then if $v, w \in L$, we have $v \sim w$ if and only if:*

1. $v^2 = w^2$.
2. *v, w have the same critical indices λ_i and exponents f_i.*
3. ord $(v_{(i)}^2 - w_{(i)}^2 \geqslant f_i + f_{i+1} + \lambda_{i+1}$.

The following result is also proved in **(3)**, again for non-dyadic fields.

THEOREM 4.3. *Let M, M' be isometric sublattices of L. Then if $\phi(M) = M'$ is an isometry, there is an isometry ψ on L such that $\psi|M = \phi$ if and only if $x \sim \phi(x)$ over L for all $x \in M$.*

No such result is known for the dyadic case.

References

1. O. T. O'Meara, *Introduction to quadratic forms* (New York, 1963).
2. ——— *The integral representations of quadratic forms over local fields*, Amer. J. Math., *80* (1958), 843–878.
3. S. Rosenzweig, *An analogy of Witt's theorem for modules over the ring of p-adic integers*, Doctoral thesis, Mass. Inst. Techn., 1958 (unpublished).

Massachusetts Institute of Technology and
McGill University