WITT'S THEOREM AND THE ISOMETRY OF LATTICES

O. T. O'MEARA

1. Introduction. The cancellation law for quadratic forms as originally proved by Witt [10] states that if $\mathcal{J}+\mathcal{G}$ and $\mathcal{J}+\mathcal{K}$ are field equivalent then so are $\mathcal{G}$ and $\mathcal{K}$. In general this result is not valid under ring equivalence but some work has been done in this direction, notably by Jones and Durfee in the local theory and by Eichler and Kneser in the ring of rational integers. Although the integral formulation of Witt's theorem holds over any local field in which 2 is a unit [2; 5], it is not true over the 2-adic integers [2]; but in that case it is known [6] that $\mathcal{G} \cong \mathcal{K}$ provided that $\mathcal{J}$ is of unit determinant, $\mathcal{G} = 2\mathcal{G}'$ and $\mathcal{K} = 2\mathcal{K}'$. The author [9] has extended this result to any local field in which 2 is a prime; also to the ramified case, but with the restriction that $\mathcal{J}$ be a form of one variable only. Our first aim in this paper is to remove this restriction. Secondly, to prove that $\mathcal{G}$ and $\mathcal{K}$ are equivalent provided that $\mathcal{J}$ is the orthogonal sum of totally isotropic binary forms, that is forms of the type

$$\begin{pmatrix} 0 & \pi^{\lambda(i)} \\ \pi^{\lambda(i)} & 0 \end{pmatrix},$$

where the $\lambda(i)$ are arbitrary integers.

2. Notation. The scalars will be taken from a field F of characteristic unequal to 2, provided with a non-Archimedean, complete and discrete valuation [1] and having a perfect residue class field; $\mathfrak{o}$ will be the ring of integers and π a prime element in F; since the cancellation law has been shown to hold for any local field in which 2 is a unit [2; 5], we shall assume throughout that $|2| < 1$ holds in F; the letter e will be used to denote the ordinal of 2, i.e. $|\pi^e| = |2|$; then our assumption can be expressed by the relation $e = \text{ord } 2 \geqq 1$. A specific element $a\pi^t$ will sometimes be written as $[\pi^t]$ if $|a| = 1$ and as $\{\pi^t\}$ if $a \in \mathfrak{o}$; thus $\alpha = [\pi^t], \beta = [\pi^t], \gamma = \{\pi^t\}$ implies that $|\alpha| = |\beta| \geqq |\gamma|$.

All proofs will be geometrical. The notation will be similar to that in [9]. If V is an n-dimensional F-space with scalar product $X \cdot Y$

and if L is a lattice $[3;9]$ in V, we say that $\xi_1, \cdots, \xi_n$ is a (minimal) basis for L if $L = \mathfrak{o}\xi_1 + \cdots + \mathfrak{o}\xi_n$. If $\mathcal{L}$ is the quadratic form associated with this basis and if Λ is the corresponding matrix, we write $\mathcal{L} \cong \Lambda \cong L$. If K is another lattice in V and if there exists an isometry carrying L onto K, we write $L \cong K$, $\Lambda \cong K$ and $\mathcal{L} \cong \mathcal{K}$. The determinant of L is defined to be the determinant of the matrix Λ; we assume that $\det L \neq 0$.

The ideal generated by X^2, $X \in L$, is called the norm of L and will be written $N(L)$; if $N(L) \subseteq \mathfrak{o}$ we say that L is integral. If $X \in L$, we define $\mathfrak{a}_L(X)$, or simply $\mathfrak{a}(X)$, as the ideal generated by $X \cdot Z$ as Z runs through L; the ideal generated by $\mathfrak{a}(X)$, $X \in L$, will be written $\mathfrak{a}(L)$; if $\mathfrak{a}(L) \subseteq \mathfrak{o}$ we say that L is totally integral.

If L is a totally integral lattice of unit determinant it has a canonical basis, i.e. a basis (ξ_λ) such that (i) if $N(L) = \mathfrak{o}$, then $\xi_\lambda \xi_\mu = 0$ for all $\lambda \neq \mu$; (ii) if $N(L) \subseteq (\pi)\mathfrak{o}$, then n is even and $\xi_{2r-1}\xi_{2r} = 1$, $\xi_{2r-1}\xi_\lambda = 0 = \xi_{2r}\xi_\lambda$ for $\lambda \neq 2r-1$, $2r$ and for all r, $1 \leq r \leq n/2$. In the first case we say that L is proper; in the second, improper. If L is arbitrary, it has an orthogonal decomposition

$$(2.1) \qquad L = L_1(\pi^{s(1)}) \oplus \cdots \oplus L_r(\pi^{s(r)})$$

where $s(1) < s(2) < \cdots < s(r)$ and the forms $\pi^{-s(\lambda)}\mathcal{L}_\lambda(\pi^{s(\lambda)})$ are totally integral, of unit determinant. The basis derived from the canonical bases of the $L_\lambda(\pi^{s(\lambda)})$ in the obvious way, is called a canonical basis for L. If L has another decomposition

$$L = K_1(\pi^{t(1)}) \oplus \cdots \oplus K_q(\pi^{t(q)}),$$

then

$$(2.2) \qquad s(\lambda) = t(\lambda), \qquad \dim L_\lambda = \dim K_\lambda,$$

$$(2.2a) \qquad L_\lambda \text{ proper} \Leftrightarrow K_\lambda \text{ proper}.$$

Let (ξ_λ) be canonical; we say that ξ_i is a proper basis element if $\xi_i \xi_\lambda = 0$ for all $\lambda \neq i$; otherwise it is improper. Note that $\mathfrak{a}(\xi_i) = (\xi_i^2)\mathfrak{o}$ if and only if ξ_i is proper.

The proof that L has a canonical basis and of the equations (2.2) can be found in $[9]$; it is rather well known for the rational 2-adic integers $[7]$. If two lattices (not necessarily isometric) have the same invariants (2.2) and (2.2a) we say that they are of the same type.

Some of our proofs will rely on the following "one-dimensional" result, already proved in $[9, \text{Theorem } 5.1]$:

THEOREM 2.1. *Let the lattice L have two decompositions* $\mathfrak{o}\xi \oplus L_1 = L = \mathfrak{o}\eta \oplus K_1$ *with* $\xi^2 = \epsilon = \eta^2$ *and* $|\epsilon| = 1$. *If* $\mathfrak{a}(L_1) \subseteq (2)\mathfrak{o}$, *then* $L_1 \cong K_1$.

3. **The derived canonical basis.** Let (ξ_λ) be a canonical basis for L. Starting with two fixed, distinct and orthogonal basis elements ξ_i, ξ_j and with a given integer α, we shall derive a new canonical basis (Ξ_λ) from the old one (ξ_λ). The operation of passing from the one basis to the other will be denoted by the symbol

$$\text{op } (\xi_i \to \xi_i + \alpha\xi_j);$$

the value of Ξ_i will be given by the equation $\Xi_i = \xi_i + \alpha\xi_j$; thus

$$(3.1) \qquad \Xi_i^2 = \xi_i^2 + \alpha^2\xi_j^2;$$

we define $\Xi_\lambda = \xi_\lambda$ at those values of λ for which $\lambda \neq i, j$ and $\xi_\lambda\xi_j = 0$. Most of the Ξ_λ are now settled; to complete the definition of the basis (Ξ_λ) we must specify the vector Ξ_j and (when ξ_j is improper with $\xi_j\xi_{j+1} \neq 0$, say) the vector Ξ_{j+1}. To ensure that the constructions involved in defining the remaining Ξ_λ yield a canonical basis, we must assume that

$$(3.2) \qquad \alpha \in \mathfrak{o}, \qquad \alpha\mathfrak{a}(\xi_j)/\mathfrak{a}(\xi_i) \subseteq \mathfrak{o},$$

$$(3.3) \quad \left|\Xi_i^2\right| = \left|\mathfrak{a}(\xi_i)\right| \text{ if } \xi_i \text{ proper}, \quad \left|\Xi_i^2\right| < \left|\mathfrak{a}(\xi_i)\right| \text{ if } \xi_i \text{ improper}.$$

CASE 1. ξ_i, ξ_j proper. Then $\alpha\xi_j^2/\Xi_i^2 \in \mathfrak{o}$ by (3.2) and (3.3); define $\Xi_j = \xi_j - (\alpha\xi_j^2/\Xi_i^2)\Xi_i$; then (Ξ_λ) is canonical and

$$(3.4) \qquad \Xi_j^2 = \xi_j^2 - \alpha^2(\xi_j^2)^2/\Xi_i^2.$$

CASE 2. ξ_i improper, ξ_j proper. Let $\xi_{i\pm1} = \Xi_{i\pm1}$ be the basis vector that is not orthogonal to ξ_i. Put

$$A = -\alpha\xi_j^2\Xi_{i\pm1}^2/(\Xi_i^2\Xi_{i\pm1}^2 - (\Xi_i\Xi_{i\pm1})^2) \in \mathfrak{o},$$

$$B = \alpha\xi_j^2(\Xi_i\Xi_{i\pm1})/(\Xi_i^2\Xi_{i\pm1}^2 - (\Xi_i\Xi_{i\pm1})^2) \in \mathfrak{o}$$

and define $\Xi_j = \xi_j + A\Xi_i + B\Xi_{i\pm1}$; then $\Xi_j\Xi_i = 0 = \Xi_j\Xi_{i\pm1}$ by choice of A and B; and (Ξ_λ) is canonical in virtue of (2.2) and (2.2a). Direct computation shows that

$$(3.5) \qquad \Xi_j^2 = \xi_j^2 + [\alpha^2(\xi_j^2)^2\Xi_{i\pm1}^2/(\Xi_i\Xi_{i\pm1})^2].$$

CASE 3. ξ_i proper, $\xi_j\xi_{j+1} \neq 0$. Define $\Xi_j = \xi_j - (\alpha\xi_j^2/\Xi_i^2)\Xi_i$ and $\Xi'_{j+1} = \xi_{j+1} - (\alpha\xi_j\xi_{j+1}/\Xi_i^2)\Xi_i$; then $\Xi_j\Xi'_{j+1} = \xi_j\xi_{j+1}(1 - \alpha^2\xi_j^2/\Xi_i^2)$; put $\Xi_{j+1} = \Xi'_{j+1}(\xi_j\xi_{j+1}/\Xi_j\Xi'_{j+1})$. Then (Ξ_λ) is canonical and direct computation yields $\Xi_j\Xi_{j+1} = \xi_j\xi_{j+1}$ and

$$(3.6) \quad \Xi_j^2 = \xi_j^2 - \alpha^2(\xi_j^2)^2/\Xi_i^2, \qquad \Xi_{j+1}^2 = \xi_{j+1}^2 + [\alpha^2(\xi_j\xi_{j+1})^2/\Xi_i^2].$$

CASE 4. ξ_i improper, $\xi_i\xi_{j+1}\neq 0$. Define Ξ_j as in Case 2 and put $\Xi'_{j+1}=\xi_{j+1}+A'\Xi_i+B'\Xi_{i\pm1}$ where

$$A' = -\alpha(\xi_i\xi_{j+1})\Xi_{i\pm1}^2/(\Xi_i^2\Xi_{i\pm1}^2 - (\Xi_i\Xi_{i\pm1})^2) \in \mathfrak{o},$$

$$B' = \alpha(\xi_i\xi_{j+1})(\Xi_i\Xi_{i\pm1})/(\Xi_i^2\Xi_{i\pm1}^2 - (\Xi_i\Xi_{i\pm1})^2) \in \mathfrak{o}.$$

The fact that A' and B' are integers follows from (3.2) and (3.3). Then Ξ_j and Ξ'_{j+1} are orthogonal to $\mathfrak{o}\Xi_i+\mathfrak{o}\Xi_{i\pm1}$. Also $\Xi'_{j+1}\Xi_j=\xi_{j+1}\xi_j$ $\cdot(1+\{\alpha^2\xi_j^2\Xi_{i\pm1}^2/(\Xi_i\Xi_{i\pm1})^2\})$. Define $\Xi_{j+1}=\Xi'_{j+1}(\xi_{j+1}\xi_j/\Xi'_{j+1}\Xi_j)$. Then (Ξ_λ) is canonical and direct computation shows that $\Xi_j\Xi_{j+1}=\xi_j\xi_{j+1}$ and

$$(3.7) \qquad \Xi_j^2 = \xi_j^2 + [\alpha^2(\xi_j^2)^2\Xi_{i\pm1}^2/(\Xi_i\Xi_{i\pm1})^2],$$

$$(3.7\text{a}) \qquad \Xi_{j+1}^2 = \xi_{j+1}^2 + [\alpha^2(\xi_j\xi_{j+1})^2\Xi_{i\pm1}^2/(\Xi_i\Xi_{i\pm1})^2].$$

This completes the definition of the basis (Ξ_λ).

In the definition of op $(\xi_i\rightarrow\xi_i+\alpha\xi_j)$ we have assumed that $i\neq j$ and that $\xi_i\xi_j=0$. We now define op $(\xi_i\rightarrow\xi_i+\alpha\xi_i)$ in a similar manner:

CASE 5. $i=j$, $|1+\alpha|=1$. Define $\Xi_i=\xi_i+\alpha\xi_i$; if $\xi_{i\pm1}\xi_i\neq 0$, put $\Xi_{i\pm1}=(1+\alpha)^{-1}\xi_{i\pm1}$; set the remaining $\Xi_\lambda=\xi_\lambda$. Note that

$$(3.8) \qquad |\alpha| > |2| \Rightarrow \Xi_i^2 = \xi_i^2 + \alpha^2\xi_i^2 + \{\pi\alpha^2\xi_i^2\}.$$

Finally we define the symbol op $(\xi_{i+1}\rightarrow\xi_{i+1}+\alpha\xi_i)$ when $\xi_i\xi_{i+1}\neq 0$. Note that in this case neither Ξ_i nor Ξ_{i+1} will be defined in the usual way.

CASE 6. $\xi_i\xi_{i+1}\neq 0$, $\alpha\in\mathfrak{o}$. Define $\Xi_i=\xi_i$ and $\Xi'_{i+1}=\xi_{i+1}+\alpha\xi_i$; we then have $\Xi_i\Xi'_{i+1}=\xi_i\xi_{i+1}(1+\alpha\xi_i^2/\xi_i\xi_{i+1})$ and we put

$$\Xi_{i+1} = \Xi'_{i+1}(\xi_i\xi_{i+1}/\Xi_i\Xi'_{i+1}).$$

Set the remaining $\Xi_\lambda=\xi_\lambda$. Note that

$$(3.9) \quad |\alpha| > |2\xi_i\xi_{i+1}/\xi_i^2| \Rightarrow \Xi_{i+1}^2 = \xi_{i+1}^2 + \alpha^2\xi_i^2 + \{\pi\alpha^2\xi_i^2\},$$

$$(3.10) \quad |\alpha| < |2\xi_i\xi_{i+1}/\xi_i^2| \Rightarrow \Xi_{i+1}^2 = \xi_{i+1}^2 + 2\alpha\xi_i\xi_{i+1} + \{2\pi\alpha\xi_i\xi_{i+1}\}.$$

We conclude this section with some lemmas.

LEMMA 3.1. *If $\xi^2=a+\{4\pi\}$ where a is a unit, then $\mathfrak{o}\xi\cong a$.*

PROOF. Apply Hensel's lemma [1].

The next lemma is a necessary modification of a result of the author [9] and a slight sharpening of the binary formulation of Theorem 2 in [2]. Its corollary is weaker than Theorem 14.3 in [9] but will meet the requirements of this paper.

LEMMA 3.2. *Let* $L = \mathfrak{o}\xi_1 + \mathfrak{o}\xi_2$ *be an improper lattice of norm* $(\pi^\nu)\mathfrak{o}$ *such that* $\xi_1\xi_2 = 1$ *and* $\xi_2^2 = a + [\pi^\Delta]$. *Suppose that either* (1) $|\xi_1^2| = |\pi^\nu|$ *and* $\Delta \geqq 2e - \nu + 1$; *or* (2) $\Delta \geqq 2e + 1$; *then there is an* X *in* L *such that* $L = \mathfrak{o}\xi_1 + \mathfrak{o}X$, $\xi_1 X = 1$ *and* $X^2 = a$.

PROOF. The quadratic equation

$$\alpha^2(\xi_1^2 - a(\xi_1^2)^2) + 2\alpha(1 - a\xi_1^2) + (\xi_2^2 - a) = 0$$

can be written in the form $\alpha^2 + [2\pi^{-\nu}]\alpha + \{\pi^{2e-2\nu+1}\} = 0$ which has an integral solution α_0 by Hensel's lemma [1]. Then

$$X = (\xi_2 + \alpha_0\xi_1)/(1 + \alpha_0\xi_1^2)$$

is the vector required.

The second part of the lemma is proved in the same way.

COROLLARY 3.2. *Let* $L = \mathfrak{o}\xi_1 + \mathfrak{o}\xi_2$ *and* $K = \mathfrak{o}\eta_1 + \mathfrak{o}\eta_2$ *be improper lattices of the same norm* $(\pi^\nu)\mathfrak{o}$ *and of the same determinant, such that* $\xi_1^2 = \eta_1^2 = [\pi^\nu]$, $\xi_1\xi_2 = 1 = \eta_1\eta_2$ *and* $\xi_2^2 = \eta_2^2 + \{\pi^{2e-\nu}\}$. *Then* $L \cong K$.

PROOF. Since L and K are evidently field equivalent we can assume that they are in the same metric space V. Define $f = e$ or $f = e + 1$ in such a way that $f + \nu$ is even and put $L' = \mathfrak{o}\xi_0 \oplus L$, $K' = \mathfrak{o}\xi_0 \oplus K$, where $\xi_0^2 = \pi^{-f}$. Applying op $(\eta_2 \to \eta_2 + \alpha\xi_0)$ with a suitable α for which $\eta_2^2 + \alpha^2\xi_0^2 \equiv \xi_2^2 \pmod{\pi^{2e-\nu+1}}$, we see that $L' \cong K'$ by the lemma and so $L \cong K$ by Theorem 2.1.

4. In this section we shall make use of the Hasse invariant $S(\mathcal{L}) = \sum_{\lambda \leqq \mu} (a_\lambda, a_\mu)$ of a (diagonal) quadratic form $\mathcal{L} = \sum a_\lambda x_\lambda^2$; this symbol is fully discussed by Witt in [10]. An easy computation [9] shows that if ϵ is a unit and if $\alpha \in \mathfrak{o}$, then

(4.1) $(1 + 4\alpha, \epsilon) = 1,$

(4.2) $(1 + 4\alpha, \epsilon\pi) = 1 \Leftrightarrow 1 + 4\alpha = a^2,$ $a \in F.$

Durfee [2] has shown that two lattices L and K are equivalent if they are congruent modulo $4\pi\mathfrak{a}(\xi_n)$ where ξ_n is the last basis element in any canonical representation of L. The next theorem is designed to improve the degree of approximation but it will be necessary to make the additional assumption that L and K are in the same metric space V.

THEOREM 4.1. *Let* $L = \sum \mathfrak{o}\xi_\lambda$ *and* $K = \sum \mathfrak{o}\zeta_\lambda$ *be two lattices in the same space* V, *both of the same type and such that* $\mathfrak{a}(K) = \mathfrak{a}(L) \subseteq (2)\mathfrak{o}$. *If* (ζ_λ) *is canonical and has the properties* (i) $(\zeta_1^2)\mathfrak{o} = N(K)$, (ii) $\xi_\lambda\xi_\mu = \zeta_\lambda\zeta_\mu + \{\mathfrak{a}(\zeta_\lambda) \cdot \mathfrak{a}(\zeta_\mu)\}$, *then* $L \cong K$.

PROOF. First let us prove the following contention: $L \cong K$ if (ξ_λ) is also canonical.

PROOF OF CONTENTION. We have $\xi_\lambda \xi_\mu = \zeta_\lambda \zeta_\mu$ if $\lambda \neq \mu$; $\xi_\lambda^2 = \zeta_\lambda^2 + \{\mathfrak{a}(\zeta_\lambda)^2\}$. Put $\zeta_\lambda^2 = a_\lambda$. There is no loss of generality in assuming that $\mathfrak{a}(K) = \mathfrak{a}(L) = (2)\mathfrak{o}$.

CASE 1. ξ_1 and ζ_1 proper. Then $(\xi_1^2)\mathfrak{o} = \mathfrak{a}(\xi_1) = (2)\mathfrak{o} = \mathfrak{a}(\zeta_1) = (a_1)\mathfrak{o}$. Define $f = 0$ or $f = 1$, the choice being such that $f + e$ is odd; define $\xi_0^2 = \pi^{-f}$ and put $L' = \mathfrak{o}\xi_0 \oplus L$, $K' = \mathfrak{o}\xi_0 \oplus K$; by Theorem 2.1 it suffices to prove that $L' \cong K'$.

Suppose that we have constructed a new canonical basis

$$(4.3) \qquad X_0, X_1, \Xi_2, \cdots, \Xi_{i-1}, \xi_i, \cdots, \xi_n, \qquad 2 \leq i \leq n,$$

for L' with the property

$$(4.4) \qquad \Xi_\lambda^2 = a_\lambda, \qquad 1 < \lambda < i.$$

We now show how to construct Ξ_i, that is another basis X_0, X_1, $\Xi_2, \cdots, \Xi_{i-1}, \Xi_i, \xi_{i+1}, \cdots, \xi_n$ in which the property (4.4) is valid for all $1 < \lambda \leq i$: the vectors X_0, X_1 will be variables in this construction.

By varying X_0, X_1, and ξ_i alone, suppose that we obtain another canonical basis (which we continue to write in the form (4.3)) such that $\xi_i^2 = a_i + \epsilon \pi^\Delta$. Then Δ is unbounded. For if not, we can suppose that Δ is maximal; then $\Delta \geq 2$ ord $\mathfrak{a}(\xi_i)$. (a) Let $\Delta + e$ be even. If we define α so that $\alpha^2 X_1^2 \equiv \epsilon \pi^\Delta \pmod{\pi^{\Delta+1}}$, then $|\alpha^2| = |\pi^\Delta/2| \leq 1$ and $|\alpha\mathfrak{a}(X_1)/\mathfrak{a}(\xi_i)|^2 \leq |2|$; hence (3.2) is satisfied and we can apply op $(\xi_i \to \xi_i + \alpha X_1)$ to obtain a greater Δ. Hence (b) $\Delta + e$ must be odd; then $\Delta + f$ is even and in virtue of the perfectness of the residue class field we can define α so that $\alpha^2 X_0^2 \equiv \epsilon \pi^\Delta \pmod{\pi^{\Delta+1}}$; then $|\alpha^2| = |\pi^{\Delta+f}| \leq 1$ and $|\alpha\mathfrak{a}(X_0)/\mathfrak{a}(\xi_i)|^2 = |\pi^{\Delta-f}/\mathfrak{a}(\xi_i)^2|$ which is integral when $f = 0$; if $f = 1$, $|\pi^\Delta| \neq |\mathfrak{a}(\xi_i)|^2$ since $\Delta + e$ odd implies Δ odd; hence

$$\pi^{\Delta-f}/\mathfrak{a}(\xi_i)^2$$

is still integral; (3.2) is therefore satisfied for general f and we can apply op $(\xi_i \to \xi_i + \alpha X_0)$ to reduce $|\pi^\Delta|$. Hence Δ is unbounded.

By choosing a ξ_i with a sufficiently high Δ, e.g. $\Delta \geq$ ord $(4\pi\mathfrak{a}(\xi_i))$, we can construct a Ξ_i such that

$$(4.5) \qquad \Xi_i^2 = a_i$$

in virtue of Lemmas 3.1 and 3.2. This is the Ξ_i required by the construction.

Proceeding in this way we arrive at a basis $X_0, X_1, \Xi_2, \cdots, \Xi_n$ for

L' such that $\sum_2^n \mathfrak{o}\Xi_\lambda \cong \sum_2^n \mathfrak{o}\zeta_\lambda$. Then $\mathfrak{o}X_0 \oplus \mathfrak{o}X_1$ and $\mathfrak{o}\xi_0 \oplus \mathfrak{o}\zeta_1$ are fractionally equivalent by Witt's theorem. Now X_0^2 must represent π^{-f} (mod 2) and in virtue of (3.2) and (3.8) we can therefore apply op $(X_0 \to X_0 + \alpha X_1)$ and op $(X_0 \to X_0 + \alpha X_0)$ in succession to reduce $\mathfrak{o}X_0 \oplus \mathfrak{o}X_1$ to the form $X_0^2 = \pi^{-f}\delta$ and $X_1^2 = a_1\delta$ where $\delta \equiv 1$ (mod 4). Applying Hasse symbols to $\mathfrak{o}X_0 \oplus \mathfrak{o}X_1$ and $\mathfrak{o}\xi_0 \oplus \mathfrak{o}\zeta_1$ we get $(\pi^{-f}\delta, -1)$ $\cdot (a_1\delta, a_1\pi^{-f}) = (\pi^{-f}, -1)(a_1, a_1\pi^{-f})$. Hence $(\delta, -a_1\pi^f) = 1$; but ord $a_1\pi^f$ $= e + f$ is odd, by choice of f; hence δ is a square by (4.2). This completes the proof of the first case.

CASE 2. ξ_1 and ζ_1 improper. Since $N(L) = (\zeta_1^2)\mathfrak{o} = (2\pi^\nu)\mathfrak{o}$ where $0 < \nu \leqq e$, we can suppose that $(\xi_1^2)\mathfrak{o} = N(L)$. Define $f = 0$ or $f = 1$, in such a way that $f + \nu + e$ is odd. Define L' and K' as in Case 1. We must prove that $L' \cong K'$.

Suppose that we have constructed a canonical basis

$$(4.6) \qquad X_0, X_1, X_2, \Xi_3, \cdots, \Xi_{i-1}, \xi_i, \cdots, \xi_n, \qquad 3 \leqq i \leqq n;$$

for L', having the following properties

$$(4.7) \qquad X_1^2 \equiv \xi_1^2 \pmod{4\pi}, \qquad \Xi_\lambda^2 = a_\lambda \text{ for } 2 < \lambda < i,$$

$$(4.8) \qquad N(L) = N(\mathfrak{o}X_1 + \mathfrak{o}X_2 + \mathfrak{o}\Xi_3 + \cdots + \mathfrak{o}\xi_n).$$

We now give the construction for Ξ_i: that is, we produce another basis $X_0, X_1, X_2, \Xi_3, \cdots, \Xi_{i-1}, \Xi_i, \xi_{i+1}, \cdots, \xi_n$ for L', having the properties (4.7) and (4.8) for all $2 < \lambda \leqq i$; X_0, X_1, X_2 will be variable vectors in this construction. Note that (4.7) and (4.8) together imply that $(X_1^2)\mathfrak{o} = N(\mathfrak{o}X_1 + \mathfrak{o}X_2 + \mathfrak{o}\Xi_3 + \cdots + \mathfrak{o}\xi_n)$ and hence

$$(4.9) \qquad |X_2^2| \leqq |X_1^2|.$$

By varying X_0, X_1, X_2 and ξ_i alone, suppose that we obtain another canonical basis (which we continue to write in the form (4.6)) with $\xi_i^2 = a_i + \epsilon\pi^\Delta$ and such that the new basis continues to satisfy equations (4.7) and (4.8). Then Δ is unbounded. For if not, we can choose a Δ that is maximal; then $\Delta \geqq 2$ ord $(\mathfrak{a}(\xi_i))$. (a) Let $\Delta + e + \nu$ be even. In virtue of the perfectness of the residue class field we can define α so that $\alpha^2 X_1^2 \equiv \epsilon\pi^\Delta \pmod{\pi^{\Delta+1}}$; then $|\alpha^2| = |\pi^\Delta/2\pi^\nu| \leqq 1$; and

$$| \alpha\mathfrak{a}(X_1)/\mathfrak{a}(\xi_i) |^2 \leqq 1;$$

hence (3.2) is satisfied and we can apply op $(\xi_i \to \xi_i + \alpha X_1)$; under this change of basis the new value of X_1 satisfies (4.7) in virtue of (3.6) and (3.7), (4.8) is obviously true, and $\xi_i + \alpha X_1$ has a greater Δ, denying the maximality of Δ. Hence (b) $\Delta + e + \nu$ must be odd and so

$\Delta + f$ is even. As in case 1(b) we see that this is also impossible. Hence Δ is unbounded.

We now define Ξ_i as in (4.5). Proceeding in this way we obtain a basis X_0, X_1, X_2, Ξ_3, $\cdots$, Ξ_n for L', which satisfies (4.7) and (4.8) and is such that $\sum_3^n \mathfrak{o}\Xi_\lambda \cong \sum_3^n \mathfrak{o}\zeta_\lambda$. By Witt's theorem, $L'' = \mathfrak{o}X_0 \oplus (\mathfrak{o}X_1 + \mathfrak{o}X_2)$ and $K'' = \mathfrak{o}\xi_0 \oplus (\mathfrak{o}\zeta_1 + \mathfrak{o}\zeta_2)$ are field equivalent; the rest of the proof is devoted to proving that they are in fact integrally equivalent.

Let $L'' = \mathfrak{o}X_0 \oplus (\mathfrak{o}X_1 + \mathfrak{o}X_2)$ be a canonical basis for L'' that satisfies (4.9) and write $X_1^2 = a_1 + \epsilon\pi^\Delta$. Then Δ is unbounded. For if not, we can choose a Δ that is maximal; then $\Delta \geq 2e$ by (4.7); and we can assume that $(X_1^2)\mathfrak{o} = N(L)$. (a) Let $\Delta + e + \nu$ be even. If $\Delta < 3e + \nu$, by the perfectness of the residue class field and by (3.8) there is an α such that $(1 + \alpha)^2 X_1^2 \equiv a_1 \pmod{\pi^{\Delta+1}}$; applying op $(X_1 \rightarrow X_1 + \alpha X_1)$ with this α leads to a contradiction. By Lemma 3.2 we see that $\Delta \geq 3e + \nu$ is also impossible. Hence (b) $\Delta + e + \nu$ is odd and so $\Delta + f$ is even. This is again impossible as in case 1(b). Hence Δ is unbounded and we can take $\Delta = \infty$ by Lemma 3.2. We fix this vector for which $X_1^2 = a_1$. Now let $X_2^2 = a_2 + \epsilon\pi^\Delta$; if Δ is unbounded as X_0 and X_2 vary, we are through; if not, let X_2 be chosen so that Δ is maximal; if $\Delta < 3e - \nu$, then $\Delta \geq e + \nu$ by (4.9), and so $\Delta + e + \nu$ must be odd by (3.9); hence $\Delta + f$ must be even; now $X_0^2 \cong \pi^{-f}(1 + \{2\pi^{\nu+f}\})$ and a determinantal consideration therefore shows that $\Delta \geq 2e + f$; applying op $(X_2 \rightarrow X_2 + \alpha X_0)$ with $\alpha^2 X_0^2 \equiv \epsilon\pi^\Delta \pmod{\pi^{\Delta+1}}$ shows that this is impossible. Hence $\Delta \geq 3e - \nu$.

We therefore have a basis $\mathfrak{o}X_0 \oplus (\mathfrak{o}X_1 + \mathfrak{o}X_2)$ for L'' such that $X_1^2 = a_1$, $X_2^2 = a_2 + \{\pi^{3e-\nu}\}$, $\dot{X}_1 X_2 = \pi^e$ and therefore $X_0^2 = \pi^{-f}\delta$ where $\delta \equiv 1 \pmod 4$. Applying Hasse symbols to L'' and K'' we get

$$(\pi^{-f}\delta, \; -1)(a_1, \; a_1\pi^{-f}\delta)(a_1 d\delta, \; d\pi^{-f}) = (\pi^{-f}, \; -1)(a_1, \; a_1\pi^{-f})(a_1 d, \; d\pi^{-f})$$

where d denotes the determinant of $\mathfrak{o}\zeta_1 + \mathfrak{o}\zeta_2$. Hence $(\delta, \pi) = 1$ and so δ is a square by (4.2). Hence $L'' \cong K''$ by Corollary 3.2. Q.E.D.

PROOF OF THEOREM. First we show how to construct a canonical basis (Ξ_λ) for L from the given basis (ξ_λ). Suppose that $\Xi_\lambda = \xi_\lambda + \alpha_\lambda X_\lambda$ has already been defined for $0 < \lambda < i$ where $1 \leq i \leq n$, and such that $\alpha_\lambda \in \mathfrak{a}(\zeta_\lambda)$, $X_\lambda \in L$, $\zeta_{i-1}\zeta_i = 0$, $L = \sum_1^{i-1} \mathfrak{o}\Xi_\lambda + \sum_i^n \mathfrak{o}\xi_\lambda$ where $\mathfrak{o}\Xi_1 + \cdots + \mathfrak{o}\Xi_{i-1}$ is canonical with the same type as $\mathfrak{o}\zeta_1 + \cdots + \mathfrak{o}\zeta_{i-1}$. We now define Ξ_i.

CASE 1. ζ_i is proper. Consider the vector $Y = \xi_i + A_1\Xi_1 + \cdots + A_{i-1}\Xi_{i-1}$. An easy computation shows that $A_j \in \mathfrak{a}(\zeta_i)$ exist such that $Y\Xi_\lambda = 0$, $\lambda < i$; the Y corresponding to these A_j is defined to be Ξ_i.

CASE 2. ζ_i improper. Define Ξ_i and Ξ'_{i+1} as in Case 1. Then $\Xi_i\Xi'_{i+1}$ $=\zeta_i\zeta_{i+1}(1+\{\mathfrak{a}(\zeta_i)\})$ and we put $\Xi_{i+1}=\Xi'_{i+1}(\zeta_i\zeta_{i+1}/\Xi_i\Xi'_{i+1})$.

Proceeding in this manner we arrive at a canonical basis (Ξ_λ) for L such that $\Xi_\lambda^2=(\xi_\lambda+\alpha_\lambda X_\lambda)^2=\zeta_\lambda^2+\{\mathfrak{a}(\zeta_\lambda)^2\}$. The conditions of the theorem are therefore satisfied by the canonical basis (Ξ_λ) and so L is isometric to K.

THEOREM 4.2. *Let $L=L_1\oplus L_2=K_1\oplus K_2$ be two decompositions of the totally integral lattice L such that L_1 and K_1 are of unit determinant and $\mathfrak{a}(L_2)=\mathfrak{a}(K_2)\subseteq(2)\mathfrak{o}$. If $L_1\cong K_1$, then $L_2\cong K_2$.*

PROOF. First we assume that L_1 and K_1 are proper. Write $L_1=\mathfrak{o}\xi_1$ $\oplus\cdots\oplus\mathfrak{o}\xi_{r-1}$; $L_2=\mathfrak{o}\xi_r+\cdots+\mathfrak{o}\xi_n$; $K_1=\mathfrak{o}\eta_1\oplus\cdots\oplus\mathfrak{o}\eta_{r-1}$; $K_2=\mathfrak{o}\eta_r$ $+\cdots+\mathfrak{o}\eta_n$; all these bases are canonical and such that $(\xi_r^2)\mathfrak{o}=N(L_2)$. Define

$$\Xi_\lambda = \xi_\lambda - (\xi_\lambda\eta_1/\overset{2}{\eta_1})\eta_1 - \cdots - (\xi_\lambda\eta_{r-1}/\overset{2}{\eta_{r-1}})\eta_{r-1}$$

for $r\leq\lambda\leq n$. Then $\Xi_\lambda=\xi_\lambda+\{\mathfrak{a}(\xi_\lambda)\}X_\lambda$ where $X_\lambda\in L$; and $L=L_1$ $+\sum_r^n\mathfrak{o}\Xi_\lambda$ since $\mathfrak{a}(\xi_\lambda)\subseteq(2)\mathfrak{o}$; and $\sum_r^n\mathfrak{o}\Xi_\lambda\subseteq K_2$ since $\Xi_\lambda\eta_\mu=0$ for $1\leq\mu\leq r-1$; now in general the change of basis in a lattice is effected by a unimodular transformation and a determinantal consideration of the matrix connecting $\eta_1,\cdots,\eta_n$ and $\xi_1,\cdots,\xi_{r-1},\Xi_r,\cdots,\Xi_n$ therefore shows that $\sum_r^n\mathfrak{o}\Xi_\lambda=K_2$. But L_2 and $\sum_r^n\mathfrak{o}\Xi_\lambda$ are field equivalent by Witt's theorem; and $\Xi_\lambda\Xi_\mu=\xi_\lambda\xi_\mu+\{\mathfrak{a}(\xi_\lambda)\mathfrak{a}(\xi_\mu)\}$; hence $L_2\cong K_2$ by Theorem 4.1.

If L_1 and K_1 are improper, define $\xi_0^2=1$ and put $L'=\mathfrak{o}\xi_0\oplus L$ $=L_1'\oplus L_2=K_1'\oplus K_2$. Then L_1' and K_1' are proper and so $L_2\cong K_2$.

5. We shall call a vector $X\in V$ *isotropic* if $X^2=0$; a binary lattice L will be called *totally isotropic* if it has a basis $L=\mathfrak{o}X+\mathfrak{o}Y$ for which $X^2=0=Y^2$.

LEMMA 5.1. *Let L be any (not necessarily integral) lattice in V and ξ_1,ξ isotropic vectors in L such that $L=(\mathfrak{o}\xi_1+\mathfrak{o}\xi)\oplus L_1$ and $|\xi_1\xi|=1$. If η is an isotropic vector in L such that $|\xi\eta|=1$ and $\mathfrak{a}(\eta)=\mathfrak{o}$, then $L=(\mathfrak{o}\eta+\mathfrak{o}\xi)\oplus L_1'$ and L_1' is isometric to L_1.*

PROOF. We have $\eta=\alpha\xi_1+\beta\xi+X$ with $X\in L_1$; in virtue of the assumption $|\xi\eta|=1$, α must be a unit. Hence we can write $L=(\mathfrak{o}\xi_1$ $+\mathfrak{o}\xi)\oplus\sum\mathfrak{o}\xi_\lambda=(\mathfrak{o}\eta+\mathfrak{o}\xi)+\sum\mathfrak{o}\xi_\lambda=(\mathfrak{o}\eta+\mathfrak{o}\xi)\oplus\sum\mathfrak{o}\Xi_\lambda$ where $\Xi_\lambda=(\xi_\lambda$ $-(\eta\xi_\lambda/\eta\xi)\xi)$, since $\eta\xi_\lambda/\eta\xi\in\mathfrak{o}$. Put $L_1'=\sum\mathfrak{o}\Xi_\lambda$; this proves the first part of the lemma.

Now $\Xi_\lambda\Xi_\mu=(\xi_\lambda-(\eta\xi_\lambda/\eta\xi)\xi)\cdot(\xi_\mu-(\eta\xi_\mu/\eta\xi)\xi)=\xi_\lambda\xi_\mu$ since ξ is isotropic and orthogonal to both ξ_λ and ξ_μ. Hence $L_1'\cong L_1$. Q.E.D.

If L is a totally integral lattice of unit determinant and of dimension $\geqq 3$, there is a decomposition

$$(5.1) \qquad\qquad L = \sum N_\lambda \oplus L_1 \oplus L_2$$

where the N_λ are totally isotropic binary lattices of unit determinant and where L_1, L_2 satisfy the following conditions: if L is proper, $L_2 \cong [1] \oplus [1]$ or $L_2 \cong [1]$, while if L is improper,

$$L_2 \cong \begin{pmatrix} [\pi^\nu] & 1 \\ 1 & \{\pi^\nu\} \end{pmatrix}, \qquad\qquad \nu > 0;$$

and

$$L_1 \cong \begin{pmatrix} [\pi^\mu] & 1 \\ 1 & \{2\} \end{pmatrix}, \qquad\qquad \text{with } \mu > 0$$

for L proper, and with $\mu > \nu > 0$ for L improper. Note that in this decomposition L_1 is totally isotropic if $\mu > e$.

In the decomposition (5.1) the term $\sum N_\lambda$ is omitted when dim L is either 3 or 4, in other words we then have $L = L_1 \oplus L_2$. We extend this decomposition to lattices of lower dimension by writing

$$(5.1a) \qquad\qquad L \cong L_2 \qquad\qquad \text{if dim } L \leqq 2;$$

the value $\mu = \infty$ is associated with such a lattice.

The proof that a decomposition (5.1) does in fact exist is a simple application of the operations op $(\xi_i \to \xi_i + \alpha\xi_j)$ of §3 and is left to the reader. Compare the result in [9].

THEOREM 5.2. *Let $L_1 \oplus (\mathfrak{o}\xi_j + \mathfrak{o}\xi_{j+1}) \oplus L_2 = L = K_1 \oplus (\mathfrak{o}\eta_j + \mathfrak{o}\eta_{j+1}) \oplus K_2$ be two decompositions of the lattice L such that $\mathfrak{o}\xi_j + \mathfrak{o}\xi_{j+1}$ and $\mathfrak{o}\eta_j + \mathfrak{o}\eta_{j+1}$ are totally isotropic and isometric. Then $L_1 \oplus L_2$ and $K_1 \oplus K_2$ are isometric.*

PROOF. There is no loss of generality in taking $\mathfrak{a}(\xi_j) = \mathfrak{o} = \mathfrak{a}(\eta_j)$. In virtue of the canonical form decomposition theorem and of (5.1) we can write

$$(5.2) \qquad L = \sum_{1}^{j-1} \mathfrak{o}\xi_\lambda \oplus (\mathfrak{o}\xi_j + \mathfrak{o}\xi_{j+1}) \oplus \sum_{j+2}^{k} \mathfrak{o}\xi_\lambda \oplus \sum_{k+1}^{n} \mathfrak{o}\xi_\lambda$$

where (i) $|\mathfrak{a}(\xi_\lambda)| > 1$ for $1 \leqq \lambda \leqq j-1$, $|\mathfrak{a}(\xi_\lambda)| = 1$ for $j \leqq \lambda \leqq k$, and $|\mathfrak{a}(\xi_\lambda)| < 1$ for $k+1 \leqq \lambda \leqq n$; (ii) ξ_λ is canonical for $1 \leqq \lambda \leqq j-1$ and for $k+1 \leqq \lambda \leqq n$; (iii) $\sum_{j+2}^{k} \mathfrak{o}\xi_\lambda$ is expressed in the form (5.1). Since the lattice $\sum_{j+2}^{k} \mathfrak{o}\xi_\lambda$ has the form (5.1), we can define integers ν and μ corresponding to the basis $(\xi_{j+2}, \cdots, \xi_k)$. Of course ν and μ will vary

as we alter the basis $(\xi_1, \cdots, \xi_{j-1}, \xi_{j+2}, \cdots, \xi_n)$: of all such bases for $L_1 \oplus L_2$ which have the properties (i) to (iii), choose one in which first ν and then μ is maximal (ν will be zero when $\mathfrak{a}(\xi_k) = \mathfrak{o}$). Note that ξ_j and ξ_{j+1} are unaltered in this choice of basis. We shall refer to this new basis as (ξ_λ). We can assume that both ξ_λ and $\xi_{\lambda+1}$ are isotropic vectors whenever $\mathfrak{o}\xi_\lambda + \mathfrak{o}\xi_{\lambda+1}$ is totally isotropic.

CONTENTION: there is an isotropic vector ξ_i, $j \leq i \leq k$, such that (a) either $|\xi_i\eta_j| = 1$ or $|\xi_i\eta_{j+1}| = 1$; (b) if $\xi_i\xi_{i+\delta} \neq 0$, then $\xi_{i+\delta}$ is also isotropic.

PROOF OF CONTENTION. Write

$$(5.3) \quad \begin{aligned} \eta_j &= a_{1j}\xi_1 + \cdots + a_{jj}\xi_j + \cdots + a_{kj}\xi_k + \cdots + a_{nj}\xi_n \\ &= X_j + a_{jj}\xi_j + \cdots + a_{kj}\xi_k + Y_j \end{aligned}$$

where $a_{\lambda j} \in \mathfrak{o}$. Similarly

$$(5.4) \quad \eta_{j+1} = X_{j+1} + a_{jj+1}\xi_j + \cdots + a_{kj+1}\xi_k + Y_{j+1}.$$

Let us consider any λ, $1 \leq \lambda \leq j-1$. If ξ_λ is proper, then $|\eta_j\xi_\lambda| \leq 1$ implies that $|a_{\lambda j}\xi_\lambda^2| \leq 1$ and so $|a_{\lambda j}| < 1$; similarly $|a_{\lambda j+1}| < 1$; hence $|a_{\lambda j}^2\xi_\lambda^2| < 1$, $|a_{\lambda j+1}^2\xi_\lambda^2| < 1$ and $|a_{\lambda j}a_{\lambda j+1}\xi_\lambda^2| < 1$. If ξ_λ is improper ($\xi_\lambda\xi_{\lambda+1} \neq 0$, say), then $|\eta_j\xi_\lambda| \leq 1$ implies that $|a_{\lambda j}\xi_\lambda^2 + a_{\lambda+1j}\xi_\lambda\xi_{\lambda+1}| \leq 1$ and so $|a_{\lambda+1j}| < 1$ and by symmetry $|a_{\lambda j}| < 1$; then

$$\left| \eta_j(a_{\lambda j}\pi^{-1}\xi_\lambda + a_{\lambda+1j}\pi^{-1}\xi_{\lambda+1}) \right| \leq 1$$

implies that $(a_{\lambda j}\xi_\lambda + a_{\lambda+1j}\xi_{\lambda+1})^2 \in (\pi)\mathfrak{o}$; similarly

$$(a_{\lambda j+1}\xi_\lambda + a_{\lambda+1j+1}\xi_{\lambda+1})^2 \in (\pi)\mathfrak{o}$$

and

$$(a_{\lambda j}\xi_\lambda + a_{\lambda+1j}\xi_{\lambda+1})(a_{\lambda j+1}\xi_\lambda + a_{\lambda+1j+1}\xi_{\lambda+1}) \in (\pi)\mathfrak{o}.$$

Hence we have

$$(5.5) \quad X_j^2 \in (\pi)\mathfrak{o}, \qquad X_jX_{j+1} \in (\pi)\mathfrak{o}, \qquad X_{j+1}^2 \in (\pi)\mathfrak{o}.$$

It is easy to see that

$$(5.6) \quad Y_j^2 \in (\pi)\mathfrak{o}, \qquad Y_jY_{j+1} \in (\pi)\mathfrak{o}, \qquad Y_{j+1}^2 \in (\pi)\mathfrak{o}.$$

Now let us consider the following cases.

CASE 1. $k - (j+1) = 0$. Then $\eta_j\eta_{j+1}$ is a unit, but $|X_jX_{j+1}| < 1$ and $|Y_jY_{j+1}| < 1$; hence a_{jj} (say) must be a unit and $\xi_i = \xi_{j+1}$ is the vector required.

CASE 2. $k - (j+1) > 0$ is odd. An easy computation shows that $a_{kj} \in (\pi)\mathfrak{o}$. But $|\eta_j\eta_{j+1}| = 1$ and so at least one $a_{\lambda j}$ must be a unit,

$j \leq \lambda \leq k-1$. If $\mu > e$ or if $k = j+2$, we are through. So assume that $k > j+2$ and $\mu \leq e$. Let us suppose (if possible) that $|a_{k-2j}| = 1$ but $|a_{\lambda j}| < 1$ for $j \leq \lambda \leq k-3$. Put $\Xi_{k-2} = a_{1j}\xi_1 + \cdots + a_{j-1j}\xi_{j-1} + a_{k-2j}\xi_{k-2} + \cdots + a_{nj}\xi_n$ and $\Xi_{k-1} = \xi_{k-1}$. Then $\Xi_{k-2}^2 \in (2\pi)\mathfrak{o}$ since $\eta_j^2 = 0$. Define $\Xi_\lambda = \xi_\lambda + A_\lambda\Xi_{k-2} + B_\lambda\Xi_{k-1}$ for $1 \leq \lambda \leq j-1$, $k \leq \lambda \leq n$, where A_λ and B_λ are the integral solutions to

$$\xi_\lambda\Xi_{k-2} + A_\lambda\Xi_{k-2}^2 + B_\lambda\Xi_{k-2}\Xi_{k-1} = 0,$$

(5.7)

$$\xi_\lambda\Xi_{k-1} + A_\lambda\Xi_{k-2}\Xi_{k-1} + B_\lambda\Xi_{k-1}^2 = 0.$$

Then $\sum_1^{j-1} \mathfrak{o}\xi_\lambda \oplus \sum_{k-2}^n \mathfrak{o}\xi_\lambda = \sum_1^{j-1} \mathfrak{o}\Xi_\lambda + (\mathfrak{o}\Xi_{k-2} + \mathfrak{o}\Xi_{k-1}) + \sum_k^n \mathfrak{o}\Xi_\lambda$; if we put $\sum_1^{j-1} \mathfrak{o}\Xi_\lambda + \sum_k^n \mathfrak{o}\Xi_\lambda$ into canonical form and consider the resulting form for L, we see that $\Xi_{k-2}^2 \in (2\pi)\mathfrak{o}$ denies the maximality of μ. Hence $|a_{k-2j}| < 1$ if $|a_{\lambda j}| < 1$ for all $j \leq \lambda \leq k-3$; and similarly $|a_{k-2j+1}| < 1$ if $|a_{\lambda j+1}| < 1$ for $j \leq \lambda \leq k-3$. But these inequalities cannot be satisfied simultaneously since $|\eta_j\eta_{j+1}| = 1$; hence at least one $a_{\lambda j}$ or one $a_{\lambda j+1}$, $j \leq \lambda \leq k-3$, must be a unit and this completes the proof of the second case.

CASE 3. $k - (j+1) > 0$ is even.

(a) $\mathfrak{o}\xi_{k-1} + \mathfrak{o}\xi_k$ proper. Since $\eta_j^2 = 0 = \eta_{j+1}^2$, we must have $a_{k-1j}^2\xi_{k-1}^2 + a_{kj}^2\xi_k^2 \equiv 0 \pmod{\pi}$ and $a_{k-1j+1}^2\xi_{k-1}^2 + a_{kj+1}^2\xi_k^2 \equiv 0 \pmod{\pi}$ from which it follows that

$$a_{k-1j}a_{k-1j+1}\xi_{k-1}^2 + a_{kj}a_{kj+1}\xi_k^2 \equiv 0 \pmod{\pi}.$$

Hence at least one $a_{\lambda j}$, $j \leq \lambda \leq k-2$, must be a unit. If $k = j+3$ or if $\mu > e$ we are through. If $\mu \leq e$ and $k > j+3$ we can employ the argument of Case 2 to show that at least one $a_{\lambda j}$ or one $a_{\lambda j+1}$, $j \leq \lambda \leq k-4$, must be a unit.

(b) $\mathfrak{o}\xi_{k-1} + \mathfrak{o}\xi_k$ improper. If $\nu > e$ we can assume that $\xi_{k-1}^2 = 0 = \xi_k^2$ by (3.10) and Lemma 3.2; hence that $\mu > e$; the result is an immediate consequence of the equation $|\eta_j\eta_{j+1}| = 1$. Now let $\nu = e$ (and so $\mu > e$ again): suppose, if possible, that $|a_{k-1j}| = 1$ but $|a_{\lambda j}| < 1$ for all $i \leq \lambda \leq k-2$. Define

$$\Xi_{k-1} = a_{1j}\xi_1 + \cdots + a_{j-1j}\xi_{j-1} + a_{k-1j}\xi_{k-1} + \cdots + a_{nj}\xi_n.$$

Then $\Xi_{k-1}^2 \in (2\pi)\mathfrak{o}$. Write $\Xi_k = \xi_k$ and define Ξ_λ as in (5.7) for $1 \leq \lambda \leq j-1$, $k+1 \leq \lambda \leq n$. Then $\sum_1^{j-1} \mathfrak{o}\xi_\lambda \oplus \sum_{k-1}^n \mathfrak{o}\xi_\lambda = \sum_1^{j-1} \mathfrak{o}\Xi_\lambda + (\mathfrak{o}\Xi_{k-1} + \mathfrak{o}\Xi_k) + \sum_{k+1}^n \mathfrak{o}\Xi_\lambda$ and this denies the maximality of ν. Hence there is at least one $a_{\lambda j}$ or one $a_{\lambda j+1}$, $j \leq \lambda \leq k-2$, such that $|a_{\lambda j}| = 1$. If $k = j+3$ we are through; if $k > j+3$, $\mathfrak{o}\xi_{k-3} + \mathfrak{o}\xi_{k-2}$ is totally isotropic, and so we are through. Now let $\nu < e$; then we can assume that $|\xi_k^2| < |\pi^\nu|$ by (3.9). Using this fact in an argument similar to the one

just given, we see that $\left|a_{k-1j}\right| < 1$ and $\left|a_{k-1j+1}\right| < 1$ must always hold, no matter what the values of $a_{\lambda j}$ and $a_{\lambda j+1}$, $j \le \lambda \le k-2$, may be. If $k = j+3$ or if $\mu > e$, we are through. So let $k > j+3$ and $\mu \le e$. Suppose, if possible, that $\left|a_{k-3j}\right| = 1$ but $\left|a_{\lambda j}\right| < 1$ for all $j \le \lambda \le k-4$. Define

$$\Xi'_{k-3} = \sum_1^{j-1} a_{\lambda j}\xi_\lambda + a_{k-3j}\xi_{k-3} + a_{k-2j}\xi_{k-2} + \sum_{k+1}^n a_{\lambda j}\xi_\lambda$$

and $\Xi_{k-3} = \Xi'_{k-3} + a_{k-1j}\xi_{k-1} + a_{kj}\xi_k$. Then, as in Case 2, we have

$$\sum_1^{j-1} \mathfrak{o}\xi_\lambda \oplus (\mathfrak{o}\xi_{k-3} + \mathfrak{o}\xi_{k-2}) \oplus (\mathfrak{o}\xi_{k-1} + \mathfrak{o}\xi_k) \oplus \sum_{k+1}^n \mathfrak{o}\xi_\lambda$$

$$= \sum_1^{j-1} \mathfrak{o}\Xi_\lambda + ((\mathfrak{o}\Xi'_{k-3} + \mathfrak{o}\xi_{k-2}) \oplus (\mathfrak{o}\xi_{k-1} + \mathfrak{o}\xi_k)) + \sum_{k+1}^n \mathfrak{o}\Xi_\lambda$$

$$= \sum_1^{j-1} \mathfrak{o}\Xi_\lambda + ((\mathfrak{o}\Xi_{k-3} + \mathfrak{o}\xi_{k-2}) \oplus (\mathfrak{o}\Xi_{k-1} + \mathfrak{o}\Xi_k)) + \sum_{k+1}^n \mathfrak{o}\Xi_\lambda$$

and by considering the norm of the middle blocks it is easy to see that we have $\left|\Xi^2_{k-1}\right| \le \left|\pi^\nu\right|$ and $\left|\Xi^2_k\right| \le \left|\pi^\nu\right|$; but we also have $\left|\Xi^2_{k-3}\right| < \left|2\right|$ $\le \left|\pi^\mu\right|$; this denies the maximality of μ. Hence there is at least one $a_{\lambda j}$ or one $a_{\lambda j+1}$, $j \le \lambda \le k-4$, which is a unit. This completes the proof of the contention.

There is therefore a pair of isotropic vectors ξ_i, $\xi_{i+\delta}$, such that $\left|\eta_i\xi_i\right| = 1$ (say), $\mathfrak{a}(\xi_i) = \mathfrak{o}$ and $\xi_i\xi_{i+\delta} = 1$ where $\delta = \pm 1$. Applying Lemma 5.1 twice we get $L = (\mathfrak{o}\xi_i + \mathfrak{o}\xi_{i+\delta}) \oplus L_3 = (\mathfrak{o}\xi_i + \mathfrak{o}\eta_j) \oplus L_4 = (\mathfrak{o}\eta_j + \mathfrak{o}\eta_{j+1}) \oplus L_5$ with $L_3 \cong L_4 \cong L_5$. If $i = j$ or if $i = j+1$, we are through. If not, $L_3 = (\mathfrak{o}\xi_j + \mathfrak{o}\xi_{j+1}) \oplus L_3'$ and since $L_3 \cong L_5$, we have $L_5 = (\mathfrak{o}X_1 + \mathfrak{o}X_2) \oplus L_5'$ with $(\mathfrak{o}X_1 + \mathfrak{o}X_2) \cong (\mathfrak{o}\xi_j + \mathfrak{o}\xi_{j+1})$ and $L_3' \cong L_5'$. Then $(\mathfrak{o}\xi_i + \mathfrak{o}\xi_{i+\delta}) \oplus L_3' \cong (\mathfrak{o}X_1 + \mathfrak{o}X_2) \oplus L_5'$: that is to say, $L_1 \oplus L_2 \cong K_1 \oplus K_2$. Q.E.D.

This thorem establishes the second result announced in the introduction. For let $L = L' \oplus L^*$ and $K = K' \oplus K^*$ be isometric lattices with $L' \cong \sum N_\lambda \cong K'$ where N_λ is of the form

$$\begin{pmatrix} 0 & \pi^{\nu(\lambda)} \\ \pi^{\nu(\lambda)} & 0 \end{pmatrix}.$$

If $\dim L' = 2 = \dim K'$, then $L^* \cong K^*$ by Theorem 5.2; if $\dim L' = \dim K' > 2$, we apply this result to cancel off two-dimensional totally isotropic lattices, one at a time, until we obtain $L^* \cong K^*$.

REFERENCES

1. E. Artin, *Algebraic numbers and algebraic functions*, Princeton, 1950.

2. W. H. Durfee, *Congruence of quadratic forms over valuation rings*, Duke Math. J vol. 11 (1944) pp. 687–697.

3. M. Eichler, *Quadratische Formen und orthogonale Gruppen*, Berlin, 1952.

4. ———, *Note zur Theorie der Kristallgitter*, Math. Ann. vol. 125 (1952) pp. 51–55.

5. B. W. Jones, *An extension of a theorem of Witt*, Bull. Amer. Math. Soc. vol. 48 (1942) pp. 133–142.

6. B. W. Jones and W. H. Durfee, *A theorem on quadratic forms over the ring of 2-adic integers*, Bull. Amer. Math. Soc. vol. 55 (1949) pp. 758–762.

7. B. W. Jones, *The arithmetic theory of quadratic forms*, Carus Monographs, no. 10, 1950.

8. M. Kneser, *Zur Theorie der Kristallgitter*, Math. Ann. vol. 127 (1954) pp. 105–106.

9. O. T. O'Meara, *Quadratic forms over local fields*, Amer. J. Math. vol. 77 (1955) pp. 87–116.

10. E. Witt, *Theorie der quadratischen Formen in beliebigen Körpern*, J. Reine Angew. Math. vol. 176 (1937) pp. 31–44.

UNIVERSITY OF OTAGO, NEW ZEALAND