TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 332, Number 2, August 1992

ORBITS IN UNIMODULAR HERMITIAN LATTICES

DONALD G. JAMES

ABSTRACT. Let L be a unimodular indefinite hermitian lattice over the integers $\mathfrak{o}$ of an algebraic number field, and $N(L, c)$ the number of primitive representations of $c \in \mathfrak{o}$ by L that are inequalivant modulo the action of the integral special unitary group $SU(L)$ on L. The value of $N(L, c)$ is determined from the local representations via a product formula.

1. INTRODUCTION

Let F be an algebraic number field and K a quadratic extension of F. Let V be an indefinite hermitian space over K of finite dimension $n \geq 3$ and $f: V \times V \to K$ the associated nondegenerate hermitian form on V with respect to the nontrivial automorphism $*$ of K over F where $f(ax, by) = a^* f(x, y) b$. Assume V supports a unimodular lattice L (in the sense of O'Meara [O'M, 82G] for quadratic spaces). Denote by $U(V)$ the unitary group of V and by $U(L)$ the subgroup of isometries in $U(V)$ that leave L invariant. We study the orbits of primitive elements in L under the action of the special unitary group $SU(L) = U(L) \cap SL(V)$. The problem is first solved locally; the global result is then obtained by applying the strong approximation theorem of Shimura [S, 5.12]. The analogous problem for quadratic lattices was considered in [J4]; earlier work on this integral version of Witt's theorem can be found in [J1, J2, N and W]. Kilhefner [K] gives hermitian analogues for the results in [J1].

Let Ω_F be the set of all nontrivial prime spots on F and S the set of all finite prime spots. Denote by $\mathfrak{o} = \mathfrak{o}_F$ the associated Dedekind ring of algebraic integers. Let $\mathfrak{O}_K$ be the integral closure of $\mathfrak{o}_F$ in K. Although L is an $\mathfrak{O}_K$-module, most of the calculations are done locally at the dyadic primes in S that ramify in K. The localization procedure followed here is essentially that first studied by Shimura [S] (see also [G]). Let $\mathfrak{p}$ be a prime spot of F and $F_\mathfrak{p}$ the corresponding local field. Put $K_\mathfrak{p} = K \otimes_F F_\mathfrak{p}$ and $V_\mathfrak{p} = V \otimes_F F_\mathfrak{p}$. Making the standard identifications, we have $K \subset K_\mathfrak{p}$, $F_\mathfrak{p} \subset K_\mathfrak{p}$ and $V \subset V_\mathfrak{p}$. The hermitian form f on V extends naturally to a hermitian from on $V_\mathfrak{p}$. For

Received by the editors June 18, 1990.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11E39; Secondary 20G25, 20G30.

Key words and phrases. Unimodular hermitian forms, algebraic integers, integral representations, unitary group, orbits, local fields, cyclotomic fields.

This research was partially supported by the National Science Foundation.

each $\mathfrak{p} \in S$, let $\mathfrak{o}_\mathfrak{p}$ be the topological closure of $\mathfrak{o}$ in $F_\mathfrak{p}$, and $\mathfrak{O}_\mathfrak{p}$ the integral closure of $\mathfrak{o}_\mathfrak{p}$ in $K_\mathfrak{p}$. Put $L_\mathfrak{p} = \mathfrak{O}_\mathfrak{p} L \subset V_\mathfrak{p}$. Then $L_\mathfrak{p}$ is locally unimodular so that $f(L_\mathfrak{p}, L_\mathfrak{p}) = \mathfrak{O}_\mathfrak{p}$ and $L_\mathfrak{p}$ has a basis with $\det f(x_i, x_j)$ a unit in $\mathfrak{O}_\mathfrak{p}$. Note when $\mathfrak{p}$ splits in K that $K_\mathfrak{p} = F_\mathfrak{p} \times F_\mathfrak{p}$, $\mathfrak{O}_\mathfrak{p} = \mathfrak{o}_\mathfrak{p} \times \mathfrak{o}_\mathfrak{p}$ and the involution $*$ on K becomes $(a, b)^* = (b, a)$ on $K_\mathfrak{p}$.

An element $x \in L$ is called *primitive* if $f(x, L) = \mathfrak{O}_K$. We say L *represents* $c \in \mathfrak{o}$ if there exists a primitive $x \in L$ with $f(x) = f(x, x) = c$ (all our representations are understood to be primitive). Put

$$L(c) = \{x \in L \mid f(x) = c \text{ and } f(x, L) = \mathfrak{O}_K\}$$

and let $N(L, c)$ be the number of orbits in $L(c)$ under the action of $SU(L)$, that is, the number of primitive representation of c modulo the action of $SU(L)$. Similarly, denote by $N(L_\mathfrak{p}, c)$ the corresponding number of local primitive representations of $c \in \mathfrak{o}_\mathfrak{p}$ modulo the action of $SU(L_\mathfrak{p})$. These representation numbers, $N(L, c)$ and $N(L_\mathfrak{p}, c)$, will be seen in §§4 and 5 to be finite. Representations of c by x and y are called (locally or globally) equivalent when x and y lie in the same orbit.

Theorem 1.1. *Let L be a unimodular lattice on an indefinite hermitian space V with dimension $n \geq 3$. Let c be a nonzero element in $\mathfrak{o}$ represented by L and assume $V \perp \langle -c \rangle$ has local Witt index at least two for some $\mathfrak{q} \notin S$. Then*

$$N(L, c) = \prod_{\mathfrak{p}} N(L_\mathfrak{p}, c)$$

where the product is taken over all dyadic primes $\mathfrak{p} \in S$ that ramify in K.

Note that the Witt index condition on $V \perp \langle -c \rangle$ is always satisfied when there exists a spot $\mathfrak{q} \notin S$ which splits in K. For example, the condition is satisfied if $K \subset \mathbf{R}$, the real field. The values of $N(L, c)$ will be explicitly calculated in some special cases, including $F = \mathbf{Q}$ (see Theorem 6.1), or K a cyclotomic field (see §7). Since the structure of local hermitian lattices is simpler than that of local quadratic lattices, the final results here will be more general than those in [J4].

2. Global orbits

The following result reduces the question of global equivalence of representations of the corresponding local problems.

Theorem 2.1. *Let L be a unimodular lattice on a hermitian space V with dimension $n \geq 3$. Let c be a nonzero element in $\mathfrak{o}_F$ and assume $V \perp \langle -c \rangle$ has local Witt index at least two for some $\mathfrak{q} \notin S$. Let $x, y \in L(c)$ be locally equivalent at each $\mathfrak{p} \in S$. Then there exists $\varphi \in SU(L)$ such that $\varphi(x) = y$.*

Proof. By hypothesis, there exist local $\varphi_\mathfrak{p} \in SU(L_\mathfrak{p})$ such that $\varphi_\mathfrak{p}(x) = y$ for each $\mathfrak{p} \in S$. By Witt's theorem, there exists $\theta \in U(V)$ such that $\theta(x) = y$. Let $\det \theta = \eta$. Then the norm $N_{K/F}(\eta) = 1$. Take $r \in V$ with $f(r) \neq 0$ and $f(r, x) = 0$. Since the quasi-symmetry

$$\Psi(r)\colon z \mapsto z - (1 - \eta) f(r, z) f(r)^{-1} r, \qquad z \in V,$$

fixes x and $\det \theta \Psi(r)^{-1} = 1$, we may assume $\theta \in SU(V)$. Then $\theta_\mathfrak{p}^{-1} \varphi_\mathfrak{p}(x) = x$ for each $\mathfrak{p} \in S$. Let $V = Kx \perp W$. Then $\theta_\mathfrak{p}^{-1} \varphi_\mathfrak{p} \in SU(W_\mathfrak{p})$, $\dim W \geq 2$ and

$W_\mathfrak{q}$ is indefinite for some $\mathfrak{q} \notin S$. By the strong approximation theorem on $SU(W)$ [S, 5.12] (and modifying the norm notation $\| \ \|_\mathfrak{p}$ from [O'M, 101]), there exists $\psi \in SU(W)$ such that $\|\psi - \theta_\mathfrak{p}^{-1}\varphi_\mathfrak{p}\|_\mathfrak{p} < \varepsilon$ for the finite number of $\mathfrak{p}$ in S where $\|\theta\|_\mathfrak{p} \neq 1$, and $\|\psi\|_\mathfrak{p} = 1$ for all remaining $\mathfrak{p}$ in S. Extend ψ by the identity to $SU(V)$ and put $\varphi = \theta\psi \in SU(V)$. Then $\varphi(x) = y$ and $\|\varphi\|_\mathfrak{p} = 1$ for all $\mathfrak{p} \in S$, provided ε was chosen sufficiently small initially. Hence $\varphi \in SU(L)$. □

The proof of Theorem 1.1 is similar to that for the analogous result in quadratic spaces, namely, Theorem 2.3 in [J4]; it will be given after some local results have been developed.

3. Local orbits

The norm and trace mappings from $K_\mathfrak{p}$ to $F_\mathfrak{p}$ are denoted by $N_\mathfrak{p}$ and $T_\mathfrak{p}$, respectively. For each $\mathfrak{p} \in S$, denote by $L'_\mathfrak{p}$ the sublattice of $L_\mathfrak{p}$ generated by the $x \in L_\mathfrak{p}$ with $f(x) \in 2\mathfrak{o}_\mathfrak{p}$. Trivially, $L'_\mathfrak{p} = L_\mathfrak{p}$ for any nondyadic $\mathfrak{p}$. Now suppose $\mathfrak{p}$ splits in K. Then, since the involution on $\mathfrak{O}_\mathfrak{p} = \mathfrak{o}_\mathfrak{p} \times \mathfrak{o}_\mathfrak{p}$ is given by $(a, b)^* = (b, a)$, for any $x \in L_\mathfrak{p}$ we have $f((1, 0)x) = N_\mathfrak{p}(1, 0)f(x) = 0$. Hence $(1, 0)x \in L'_\mathfrak{p}$ and $x = (1, 1)x$ is in $L'_\mathfrak{p}$, therefore $L'_\mathfrak{p} = L_\mathfrak{p}$. When $\mathfrak{p} \in S$ is not split in K, let $\mathfrak{P}$ denote the unique maximal ideal in $\mathfrak{O}_\mathfrak{p}$. Assume $x \in L_\mathfrak{p}$ is primitive. Then $f(x, L'_\mathfrak{p}) = \mathfrak{P}^m$ for some $m \geq 0$. Here $m = m_\mathfrak{p}(x)$ is called the *degree*. Moreover, $m = 0$ when $\mathfrak{p}$ is nondyadic. By convention we set $m = 0$ when $\mathfrak{p}$ is split. Call x *characteristic* when $m_\mathfrak{p}(x) \geq 1$ ($\mathfrak{p}$ must then be dyadic).

Theorem 3.1. *Assume $L_\mathfrak{p}$ is unimodular with $n = \operatorname{rank} L_\mathfrak{p} \geq 3$ and x, y are primitive in $L_\mathfrak{p}$. Then there exists $\varphi \in SU(L_\mathfrak{p})$ such that $\varphi(x) = y$ if and only if*

(i) $f(x) = f(y)$,
(ii) $m_\mathfrak{p}(x) = m_\mathfrak{p}(y) = m$,
(iii) $x - y \in \mathfrak{P}^m L'_\mathfrak{p}$.

This theorem provides the information needed to calculate $N(L_\mathfrak{p}, c)$. To prove the theorem we must first determine the structure of $L'_\mathfrak{p}$ at the dyadic primes and find generators for $SU(L_\mathfrak{p})$. Both of those problems have already been investigated in [J3].

When $\mathfrak{p}$ does not split in K, let $K_\mathfrak{p} = F_\mathfrak{p}(\zeta)$ where $\zeta^2 \in \mathfrak{o}_\mathfrak{p}$ and $\zeta^* = -\zeta$. Fix a prime π in $K_\mathfrak{p}$ and p in $F_\mathfrak{p}$ and let $e = \operatorname{ord}_p 2$. In the nondyadic case $\mathfrak{O}_\mathfrak{p}$ is generated over $\mathfrak{o}_\mathfrak{p}$ by 1 and ζ provided we choose ζ to be a prime or a unit according as the extension is ramified or not. If $\mathfrak{p}$ is dyadic, there are the following three possible types of extension of $K_\mathfrak{p}$ over $F_\mathfrak{p}$ (see [Jc] or [O'M, 63.2 and 63.3] for more details).

(i) $K_\mathfrak{p}$ is an unramified extension of $F_\mathfrak{p}$. Then $\zeta^2 = 1 + 4\delta$ with δ a unit in $\mathfrak{o}_\mathfrak{p}$, and $\mathfrak{O}_\mathfrak{p}$ consists of the elements $(\alpha + \zeta\beta)/2$ with $\alpha, \beta \in \mathfrak{o}_\mathfrak{p}$ and $\alpha \equiv \beta \bmod 2$. Here $2\mathfrak{O}_\mathfrak{p} = \mathfrak{P}^e$.
(ii) $K_\mathfrak{p}$ is a ramified extension of $F_\mathfrak{p}$ and ζ is a prime in $K_\mathfrak{p}$— the ramified prime case. Now we may assume $\pi = \zeta$, $p = \pi\pi^*$ and $\mathfrak{O}_\mathfrak{p}$ is generated over $\mathfrak{o}_\mathfrak{p}$ by 1 and π. Here $2\mathfrak{O}_\mathfrak{p} = \mathfrak{P}^{2e}$.

(iii) $K_\mathfrak{p}$ is a ramified extension of $F_\mathfrak{p}$ and ζ is a unit in $K_\mathfrak{p}$— the ramified unit case. We now have $\zeta^2 = 1 - p^{2h+1}\delta$ for some unit δ in $\mathfrak{o}_\mathfrak{p}$ and some rational integer h with $0 \leq h < e$. Put $\pi = (1+\zeta)p^{-h}$ so that $\pi\pi^* = p\delta$. Here $\mathfrak{O}_\mathfrak{p}$ consists of the elements $(\alpha + \zeta\beta)p^{-h}$ with $\alpha, \beta \in \mathfrak{o}_\mathfrak{p}$ and $\alpha \equiv \beta \bmod p^h$; also $2\mathfrak{O}_\mathfrak{p} = \mathfrak{P}^{2e}$.

In summary, if $K_\mathfrak{p}/F_\mathfrak{p}$ is a quadratic extension of fields, $\mathfrak{O}_\mathfrak{p}$ consists of the elements $(\alpha + \zeta\beta)p^{-h}$ with $\alpha, \beta \in \mathfrak{o}_\mathfrak{p}$ and $\alpha \equiv \beta \bmod p^h$, where we define $h = 0$ in the nondyadic and ramified prime dyadic cases, and $h = e$ in the unramified dyadic case. Note that $T_\mathfrak{p}(\mathfrak{O}_\mathfrak{p}) = 2p^{-h}\mathfrak{o}_\mathfrak{p}$. Let $\mathfrak{U}_\mathfrak{p}$ denote the group of units in $\mathfrak{O}_\mathfrak{p}$, and $\mathfrak{u}_\mathfrak{p}$ the units in $\mathfrak{o}_\mathfrak{p}$. Then $[\mathfrak{u}_\mathfrak{p} : N_\mathfrak{p}(\mathfrak{U}_\mathfrak{p})] = 2$ when $\mathfrak{p}$ is ramified dyadic. Also, let f denote the residue class degree of the local field $F_\mathfrak{p}$.

Lemma 3.2. *Assume $\mathfrak{p}$ is ramified dyadic and $c \in \mathfrak{o}_\mathfrak{p}$. Then there exists $a \in \mathfrak{O}_\mathfrak{p}$ such that $N_\mathfrak{p}(a) \equiv c \bmod 2p^{-h}$.*

Proof. Let $a = \alpha + \pi\beta$ where $\alpha, \beta \in \mathfrak{o}_\mathfrak{p}$. Then $N_\mathfrak{p}(a) \equiv \alpha^2 + p\delta\beta^2 \bmod 2p^{-h}$ (with $\delta = 1$ in the ramified prime case) and $\alpha^2 + p\delta\beta^2 \equiv c \bmod 2p^{-h}$ can be solved for α and β inductively through successive powers of p. □

The following result was established as Proposition 2.1 in [J3].

Lemma 3.3. *Let $F_\mathfrak{p}$ be a dyadic local field with $\mathfrak{p}$ not split in K. Then $L'_\mathfrak{p} = \{r \in L_\mathfrak{p} | p^h f(r) \in 2\mathfrak{o}_\mathfrak{p}\}$. In particular, $L_\mathfrak{p} = L'_\mathfrak{p}$ when $K_\mathfrak{p}$ is an unramified extension of $F_\mathfrak{p}$.*

Corollary 3.4. $0 \leq m_\mathfrak{p}(x) \leq e - h$ *for all primitive $x \in L_\mathfrak{p}$.*

Proof. Let $f(x, z) = 1$ where $z \in L_\mathfrak{p}$. In the nonsplit dyadic cases take $a \in \mathfrak{P}^{e-h}$. Then $az \in L'_\mathfrak{p}$ and consequently $m_\mathfrak{p}(x) \leq e - h$. □

Since $L_\mathfrak{p}$ is a unimodular $\mathfrak{O}_\mathfrak{p}$-lattice with rank at least three, it is split by a hyperbolic plane (if $\mathfrak{p}$ splits in K this can be easily verified, otherwise see [Jc, 7.1, 8.1a, 10.3]). Hence $L_\mathfrak{p} = H_\mathfrak{p} \perp M_\mathfrak{p}$ where $H_\mathfrak{p} = \mathfrak{O}_\mathfrak{p}u + \mathfrak{O}_\mathfrak{p}v$ is a hyperbolic plane with $f(u) = f(v) = 0$ and $f(u, v) = 1$. This choice of u and v will be fixed throughout the local discussion.

Lemma 3.5. *Let $F_\mathfrak{p}$ be a dyadic local field with $\mathfrak{p}$ ramified in K. Then $L_\mathfrak{p} = H_\mathfrak{p} \perp J_\mathfrak{p} \perp B_\mathfrak{p}$ where $J_\mathfrak{p}$ is a sum of hyperbolic planes and rank $B_\mathfrak{p} \leq 2$. If n is odd, $B_\mathfrak{p} = \mathfrak{O}_\mathfrak{p}w$, with $f(w)$ a unit, and*

$$L'_\mathfrak{p} = H_\mathfrak{p} \perp J_\mathfrak{p} \perp \mathfrak{P}^{e-h}w.$$

If n is even, then $B_\mathfrak{p} = \mathfrak{O}_\mathfrak{p}z + \mathfrak{O}_\mathfrak{p}w$ with $f(z, w) = 1$ and $z \in L'_\mathfrak{p}$, and

$$L'_\mathfrak{p} = H_\mathfrak{p} \perp J_\mathfrak{p} \perp (\mathfrak{O}_\mathfrak{p}z + \mathfrak{P}^k w)$$

where $k = \max\{0, e - h - \operatorname{ord}_p f(w)\}$.

Proof. The splitting of $L_\mathfrak{p}$ follows from [Jc, 10.3]. If $B_\mathfrak{p} = \mathfrak{O}_\mathfrak{p}z + \mathfrak{O}_\mathfrak{p}w$ with $f(z, w) = 1$ we can arrange that $z \in L'_\mathfrak{p}$ as follows. Replace z by $z' = z + aw$ with $a \in \mathfrak{O}_\mathfrak{p}$ chosen such that $N_\mathfrak{p}(a) \equiv f(z)f(w)^{-1} \bmod 2p^{-h}$ by Lemma 3.2. Then $p^h f(z') \in 2\mathfrak{o}_\mathfrak{p}$. Multiply z' by a unit to recover $f(z', w) = 1$. The structure of $L'_\mathfrak{p}$ follows from Lemma 3.3. □

We now define the standard isometries needed in the unitary group $U(L_\mathfrak{p})$. Put $\mu = (1, 0)$ when $\mathfrak{p}$ is split. Otherwise, fix $2\mu = 1$ except when $F_\mathfrak{p}$ is dyadic and $K_\mathfrak{p}$ is either an unramified or a ramified unit extension of $F_\mathfrak{p}$; in these exceptional cases fix $2\mu = 1 + \zeta \in p^h\mathfrak{O}_\mathfrak{p}$. Then $T_\mathfrak{p}(\mu) = 1$. For $s \in M'_\mathfrak{p} = M_\mathfrak{p} \cap L'_\mathfrak{p}$, define the *Eichler transformation* $E(u, s)$ by

$$E(u, s)(x) = x - f(u, x)s + f(s, x)u - \mu f(s)f(u, x)u, \qquad x \in L_\mathfrak{p}.$$

Then $E(u, s) \in SU(L_\mathfrak{p})$ (note that $\mu f(s) \in \mathfrak{O}_\mathfrak{p}$ by Lemma 3.3). Let $\mathscr{E}$ denote the subgroup of $SU(L\mathfrak{p})$ generated by the Eichler transformations $E(u, s)$ and $E(v, s)$ with $s \in M'_\mathfrak{p}$.

Let λ in $\mathfrak{O}_\mathfrak{p}$ have $T_\mathfrak{p}(\lambda) = 0$. The *transvection* $T_\lambda(u)$ is defined by

$$T_\lambda(u)(x) = x + \lambda f(u, x)u, \qquad x \in L_\mathfrak{p}.$$

Then $T_\lambda(u)$ and $T_\lambda(v)$ belong to $SU(L_\mathfrak{p})$.

Let $\nu \neq 0$ in $\mathfrak{O}_\mathfrak{p}$ satisfy $T_\mathfrak{p}(\nu) = N_\mathfrak{p}(\nu)$. For $r \in L_\mathfrak{p}$ with $\nu f(r)^{-1}$ in $\mathfrak{O}_\mathfrak{p}$, define the *quasi-symmetry* $\Psi_\nu(r)$ by

$$\Psi_\nu(r)(x) = x - \nu f(r, x)f(r)^{-1}r, \qquad x \in L_\mathfrak{p}.$$

Then $\Psi_\nu(r) \in U(L_\mathfrak{p})$ and $\det \Psi_\nu(r) = 1 - \nu$.

Lemma 3.6. *$U(H_\mathfrak{p})$ is generated by quasi-symmetries and transvections.*

Proof. We will reduce $\varphi \in U(H_\mathfrak{p})$ to the identity using quasi-symmetries and transvections. Let $\varphi(u) = au + bv$. Since $\Psi_2(u - v)$ interchanges u and v, assume $a \in \mathfrak{U}_\mathfrak{p}$. Put $\lambda = -ba^{-1}$. Then $T_\mathfrak{p}(\lambda) = 0$, since $f(au + bv) = 0$, and $T_\lambda(v)\varphi(u) = au$. If $T_\mathfrak{p}(a) \neq 0$, put $r = au - v$ and $\nu a = T_\mathfrak{p}(a) = -f(r)$ so that $T_\mathfrak{p}(\nu) = N_\mathfrak{p}(\nu)$. Then $\Psi_\nu(r)(au) = au - r = v$ and we may assume $\varphi(u) = u$ after applying $\Psi_2(u - v)$. If, however, $T_\mathfrak{p}(a) = 0$, then $T_{a^*}(v)(au) = au + N_\mathfrak{p}(a)v$ with $N_\mathfrak{p}(a) \in \mathfrak{u}_\mathfrak{p}$. After interchanging u and v, it can again be assumed that $\varphi(u) = u$ since $T_\mathfrak{p}(N_\mathfrak{p}(a)) \neq 0$. Now $\varphi(v) = cu + v$ with $T_\mathfrak{p}(c) = 0$ and the proof can be completed with the transvection $T_{-c}(u)$.

Proof of Theorem 3.1 (necessity). Condition (i) is clearly necessary and, except in the ramified dyadic situations, (ii) and (iii) are vacuous since $L_\mathfrak{p} = L'_\mathfrak{p}$. Assume, therefore, $\mathfrak{p}$ is ramified dyadic and there exists $\varphi \in SU(L_\mathfrak{p})$ with $\varphi(x) = y$. Condition (ii) is necessary since $\varphi(L'_\mathfrak{p}) = L'_\mathfrak{p}$. It remains to show that (iii) is satisfied. Let $L_\mathfrak{p} = H_\mathfrak{p} \perp J_\mathfrak{p} \perp B_\mathfrak{p}$ as in Lemma 3.5. By Theorem 4.2 in [J3], $U(L_\mathfrak{p})$ is generated by $\mathscr{E}$, $U(H_\mathfrak{p})$ and at most one symmetry in $U(B_\mathfrak{p})$. Observe first that $\theta(x) \equiv x \bmod \mathfrak{P}^m L'_\mathfrak{p}$ when θ is an Eichler transformation $E(u, s)$ or $E(v, s)$ with $s \in M'_\mathfrak{p}$, or when θ is an element in $U(H_\mathfrak{p})$ (since $f(\theta(x) - x, H_\mathfrak{p}) \subset \mathfrak{P}^m$). Moreover, if $\Psi_\lambda(t) \in U(H_\mathfrak{p})$, then $f(t) \in 2p^{-h}\mathfrak{o}_\mathfrak{p}$ and, consequently, $\lambda \in 2p^{-h}\mathfrak{O}_\mathfrak{p}$. It remains to study the effect of a quasi-symmetry Ψ_ν from $U(B_\mathfrak{p})$ in φ. Since $\det \varphi = 1$ and $\det \Psi_\nu = 1 - \nu$, and since $U(H_\mathfrak{p})$ is generated by transvections and quasi-symmetries, there will also have to be quasi-symmetry from $U(H_\mathfrak{p})$ in φ; consequently $\nu \in 2p^{-h}\mathfrak{O}_\mathfrak{p}$. When $B_\mathfrak{p} = \mathfrak{O}_\mathfrak{p} w$, $f(w)$ is a unit, $\mathfrak{P}^{e-h} w \subset L'_\mathfrak{p}$ and $\Psi_\nu(w)(x) \equiv x \bmod \mathfrak{P}^m L'_\mathfrak{p}$ since $m \leq e - h$. When $\operatorname{rank} B_\mathfrak{p} = 2$, take $B_\mathfrak{p}$ as in Lemma 3.5. If $k = 0$ there is nothing to prove since $L_\mathfrak{p} = L'_\mathfrak{p}$. Finally assume $k \geq 1$. The quasi-symmetry needed is $\Psi_\nu(r)$ with $r = w - f(w)z$ (see [J3, p. 477]). Then $\Psi_\nu(r)(x) \equiv x \bmod \mathfrak{P}^m L'_\mathfrak{p}$ since $\mathfrak{P}^k r \subset L'_\mathfrak{p}$.

Proof of Theorem 3.1 (sufficiency). Assume primitive x, y in $L_\mathfrak{p}$ satisfy the three conditions given in Theorem 3.1. Let $x = au + bv + r$ with $a, b \in \mathfrak{P}^m$ and $r \in M_\mathfrak{p}$. We prove first there exists $\varphi \in SU(L_\mathfrak{p})$ such that $\varphi(x) = \pi^m u + b'v + r'$. Note that when the quasi-symmetry $\Psi_\nu(t)$ lies in $U(H_\mathfrak{p})$, with $t \in H_\mathfrak{p}$, then $\Psi_\nu(t)\Psi_\nu(w)^{-1} \in SU(L_\mathfrak{p})$, where w is as in Lemma 3.5 (since $\operatorname{ord}_p f(w) \leq \operatorname{ord}_p f(t)$). Assume, therefore, $\operatorname{ord}_p a \leq \operatorname{ord}_p b$ (otherwise use $\Psi_2(u - v)$ to interchange u and v). If $\operatorname{ord}_\pi a > m$ there exists $t_1 \in M'_\mathfrak{p}$ such that $\operatorname{ord}_\pi f(t_1, r) = m$. The coefficient of u in $E(u, t_1)(x)$ now has order m and we may assume $a = \pi^m \varepsilon$ with $\varepsilon \in \mathfrak{U}_\mathfrak{p}$. Apply the isometry $u \mapsto \varepsilon^{-1}u$, $v \mapsto \varepsilon^* v$ to x; although this isometry needed not be in $SU(L_\mathfrak{p})$, by Lemma 3.6 it can be multiplied by a quasi-symmetry $\Psi_\nu(w)$ so that the product is in $SU(L_\mathfrak{p})$. We may now assume $a = \pi^m$. Likewise, assume $y = au + cv + s$ with $s \in M_\mathfrak{p}$. By condition (iii), $x - y = (b' - c)v + (r' - s) \in \mathfrak{P}^m L'_\mathfrak{p}$. Hence $t' = a^{-1}(r' - s) \in M'_\mathfrak{p}$ and $E(v, t')(x) = au + c'v + s$. Put $\lambda = a^{-1}(c - c')$. Then $T_\mathfrak{p}(\lambda) = 0$, since $f(x) = f(y)$, and $T_\lambda(v)E(v, t')(x) = y$, completing the proof.

Corollary 3.7. *Assume* $\operatorname{rank} L_\mathfrak{p} = n \geq 3$ *and* $\mathfrak{p}$ *is not ramified dyadic. Then* $N(L_\mathfrak{p}, c) = 1$ *for any* $c \in \mathfrak{o}_\mathfrak{p}$.

Proof. First $N(L_\mathfrak{p}, c) \leq 1$ by Theorem 3.1 since $L_\mathfrak{p} = L'_\mathfrak{p}$. Also, given $c \in \mathfrak{o}_\mathfrak{p}$, there now exists $a \in \mathfrak{O}_\mathfrak{p}$ with $T_\mathfrak{p}(a) = c$. Put $x = u + av$. Then $f(x) = c$ and $N(L_\mathfrak{p}, c) \geq 1$.

Proof of Theorem 1.1. Partition $L(c)$ into orbits under $SU(L)$ and let $O(L, c)$ denote the collection of these orbits. Then $N(L, c) = |O(L, c)|$ and there exists a natural mapping

$$\Gamma\colon O(L, c) \to \prod_{\mathfrak{p}} O(L_\mathfrak{p}, c)$$

into the Cartesian product of the corresponding local orbits $O(L_\mathfrak{p}, c)$. By Corollary 3.7, the product is essentially over the dyadic primes $\mathfrak{p} \in S$ which ramify in K. The map is injective by Theorem 2.1 so it remains to show that Γ is surjective. We are given primitive $x_\mathfrak{p} \in L_\mathfrak{p}$ with $f(x_\mathfrak{p}) = c$ for each dyadic $\mathfrak{p} \in S$ that ramifies. Since $n \geq 3$ there exist similar $x_\mathfrak{p} \in L_\mathfrak{p}$ for all remaining $\mathfrak{p} \in S$. Also, by hypothesis, there exists primitive $r \in L$ with $f(r) = c$. By Witt's theorem, as in the proof of Theorem 2.1, there exist $\theta_\mathfrak{p} \in SU(V_\mathfrak{p})$ such that $\theta_\mathfrak{p}(x_\mathfrak{p}) = r$ for each dyadic $\mathfrak{p} \in S$ that ramifies, and by Theorem 3.1 corresponding $\theta_\mathfrak{p}$ in $SU(L_\mathfrak{p})$ for the remaining $\mathfrak{p} \in S$. There now exists $\psi \in SU(V)$, by strong approximation [S, 5.12], such that $\|\psi - \theta_\mathfrak{p}^{-1}\|_\mathfrak{p}$ is small for all ramifying dyadic primes, while $\|\psi\|_\mathfrak{p} = 1$ at the remaining $\mathfrak{p} \in S$. Put $y = \psi(r)$ so that $f(y) = c$. Then y is close to $x_\mathfrak{p}$, and hence primitive in $L_\mathfrak{p}$, for all ramifying dyadic $\mathfrak{p}$. For the remaining $\mathfrak{p} \in S$, $\psi \in SU(L_\mathfrak{p})$ and hence $y \in L$ is primitive. Moreover, $\psi\theta_\mathfrak{p} \in SU(L_\mathfrak{p})$ and $\psi\theta_\mathfrak{p}(x_\mathfrak{p}) = y$ for all ramifying dyadic primes. Hence the orbit of y in $O(L, c)$ is mapped by Γ onto the product of the orbits of $x_\mathfrak{p}$, for the ramifying dyadic primes.

Remark. Theorem 1.1 is still true if the assumption " L represents c " is replaced by " $V_\mathfrak{q}$ represents c for all $\mathfrak{q} \notin S$." Then there exists $r \in V$ with $f(r) = c$ by the Hasse Minkowski Theorem. Since $r \in L_\mathfrak{p}$ for almost all $\mathfrak{p} \in S$, the above proof is easily modified by including the finite number of exceptions in the approximations $\|\psi - \theta_\mathfrak{p}^{-1}\|_\mathfrak{p}$ small.

4. Local representations: n odd

We now compute $N(L_\mathfrak{p}, c)$ when $n = \operatorname{rank} L_\mathfrak{p}$ is odd and $\mathfrak{p}$ is ramified dyadic. As in Lemma 3.5,

$$L_\mathfrak{p} = H_\mathfrak{p} \perp J_\mathfrak{p} \perp \mathfrak{O}_\mathfrak{p} w \quad \text{and} \quad L'_\mathfrak{p} = H_\mathfrak{p} \perp J_\mathfrak{p} \perp \mathfrak{P}^{e-h} w.$$

The discriminant $dL_\mathfrak{p} = (-1)^{(n-1)/2} f(w) N_\mathfrak{p}(\mathfrak{U}_\mathfrak{p})$ is an invariant of $L_\mathfrak{p}$. The rank and the discriminant determine $L_\mathfrak{p}$ when n is odd by [Jc, 10.4]. Thus for each odd rank n, there exist two classes of unimodular lattices. Define $\delta(L_\mathfrak{p}) = 1$ when $dL_\mathfrak{p} = (-1)^{(n-1)/2} N_\mathfrak{p}(\mathfrak{U}_\mathfrak{p})$, and $\delta(L_\mathfrak{p}) = -1$ otherwise. When $\delta(L_\mathfrak{p}) = 1$ we can assume $f(w) = 1$.

Lemma 4.1. *Assume $n \geq 3$ odd with $\mathfrak{p}$ ramified dyadic. Then*

(i) *$N(L_\mathfrak{p}, c) \geq 1$ for all $c \in \mathfrak{o}_\mathfrak{p}$,*
(ii) *$N(L_\mathfrak{p}, c) = 1$ for all $c \in p\mathfrak{o}_\mathfrak{p}$.*

Proof. Let $c \in \mathfrak{o}_\mathfrak{p}$ and $x = u + bv + aw$ with $a \in \mathfrak{O}_\mathfrak{p}$ chosen by Lemma 3.2 such that $N_\mathfrak{p}(a) f(w) \equiv c \bmod 2p^{-h}$. Take $b \in \mathfrak{O}_\mathfrak{p}$ such that $f(x) = T_\mathfrak{p}(b) + N_\mathfrak{p}(a) f(w) = c$. Thus $N(L_\mathfrak{p}, c) \geq 1$. Now assume characteristic $y \in L_\mathfrak{p}$ represents $c \in p\mathfrak{o}_\mathfrak{p}$. Then $f(y, L'_\mathfrak{p}) \subset \mathfrak{P}$ and $y \equiv aw \bmod \mathfrak{P} L_\mathfrak{p}$ for some unit $a \in \mathfrak{U}_\mathfrak{p}$. But then $c = f(y) \equiv N_\mathfrak{p}(a) f(w) \bmod \mathfrak{P}$ and c must be a unit. It follows that $N(L_\mathfrak{p}, c) \leq 1$, since all noncharacteristic representations are equivalent by Theorem 3.1.

Lemma 4.2. *Assume $n \geq 3$ is odd with $\mathfrak{p}$ ramified prime. Then*

$$N(L_\mathfrak{p}, c) = 1 + e \quad \textit{for all units } c \in \mathfrak{u}_\mathfrak{p}.$$

Proof. Let $x = \zeta^m (u + bv) + aw$ with $0 \leq m \leq e$, $b \in \mathfrak{o}_\mathfrak{p}$ and $a \in \mathfrak{U}_\mathfrak{p}$. Then $f(x, L'_\mathfrak{p}) = \mathfrak{P}^m$ so that $m_\mathfrak{p}(x) = m$. Also, $f(x) = 2p^m b + N_\mathfrak{p}(a) f(w) = c$ provided the congruence $N_\mathfrak{p}(a) f(w) \equiv c \bmod 2p^m$ can be solved for $a = \alpha + \zeta\beta \in \mathfrak{O}_\mathfrak{p}$ Since $m \leq e$, the congruence

$$N_\mathfrak{p}(a) f(w) = (\alpha^2 - p\beta^2) f(w) \equiv c \mod 2p^m$$

can be solved for $\alpha, \beta \in \mathfrak{o}_\mathfrak{p}$ inductively through successive powers of p. Hence there exist $1 + e$ inequivalent representations of c, one for each value of m. Moreover, if y is a second representation of c with $m_\mathfrak{p}(y) = m$, then $y = \zeta^m r + a'w$ for some $r \in H_\mathfrak{p} \perp J_\mathfrak{p}$ and $a' \in \mathfrak{U}_\mathfrak{p}$. Take x as above. Since $f(r) \in T_\mathfrak{p}(\mathfrak{O}_\mathfrak{p}) = 2\mathfrak{o}_\mathfrak{p}$, it follows that $N_\mathfrak{p}(a^{-1}a') \equiv 1 \bmod 2p^m$ and, consequently, $a \equiv a' \bmod \mathfrak{P}^{m+e}$. Thus $x - y \in \mathfrak{P}^m L'_\mathfrak{p}$ and the two representations are equivalent by Theorem 3.1. Hence $N(L_\mathfrak{p}, c) = 1 + e$.

Lemma 4.3. *Assume $n \geq 3$ is odd and $\mathfrak{p}$ is ramified unit. Then there exists a characteristic representation of $c \in \mathfrak{u}_\mathfrak{p}$ with degree m, $1 \leq m \leq e - h$, if and only if there exists $a \in \mathfrak{U}_\mathfrak{p}$ with $N_\mathfrak{p}(a) \equiv c f(w)^{-1} \bmod 2p^{m-h}$.*

Proof. Assume $x = \pi^m r + aw$ represent c, where $r \in H_\mathfrak{p} \perp J_\mathfrak{p}$ and $a \in \mathfrak{U}_\mathfrak{p}$. Then $c = f(x) \equiv N_\mathfrak{p}(a) f(w) \bmod 2p^{m-h}$. Conversely, if $a \in \mathfrak{U}_\mathfrak{p}$ satisfies this congruence, put $x' = \pi^m (u + bv) + aw$ with $b \in \mathfrak{O}_\mathfrak{p}$ chosen such that $f(x') = c$.

Corollary 4.4. *Assume $f = e - h = 1$ with $\mathfrak{p}$ ramified unit. Then $L_\mathfrak{p}$ characteristically represents c if and only if $c \equiv f(w) \bmod p^2$.*

Proof. Let $a = \alpha + \pi\beta \in \mathfrak{U}_\mathfrak{p}$ so that $N_\mathfrak{p}(a) = \alpha^2 + 2p^{-h}\alpha\beta + p\delta\beta^2$. Since $|\mathfrak{o}_\mathfrak{p}/p| = 2$, it follows that $\alpha \equiv \delta \equiv 1 \bmod p$ and, by the lemma there is a characteristic representation if and only if $c \equiv f(w) \bmod p^2$.

Lemma 4.5. *Assume $n \geq 3$ is odd, $h = e - 1$ and $\mathfrak{p}$ is ramified unit. Then $N(L_\mathfrak{p}, c) = 1$ or 3.*

Proof. By Theorem 3.1 and Lemma 4.3, $N(L_\mathfrak{p}, c) = 1$ unless there is an $a = \alpha + \pi\beta \in \mathfrak{U}_\mathfrak{p}$ with $N_\mathfrak{p}(a) = \alpha^2 + 2p^{-h}\alpha\beta + p\delta\beta^2 \equiv cf(w)^{-1} \bmod p^2$. Moreover, when such an $a \in \mathfrak{U}_\mathfrak{p}$ exists, there is a characteristic representation of $c = f(x)$ with $x = \pi(u + bv) + aw$. Let $a' = a + \pi\gamma$ where $\gamma \in \mathfrak{u}_\mathfrak{p}$ and $\gamma\delta \equiv 2p^{-e}\alpha \bmod p$. Then $N_\mathfrak{p}(a') \equiv N_\mathfrak{p}(a) \bmod p^2$ and there exists $b' \in \mathfrak{O}_\mathfrak{p}$ such that $c = f(x')$ with $x' = \pi(u + b'v) + a'w$. Therefore $x - x' \notin \mathfrak{P}L'_\mathfrak{p}$ and $N(L_\mathfrak{p}, c) \geq 3$. Now let $y = \pi r + dw$ be any characteristic representation of c. Then $N_\mathfrak{p}(da^{-1}) \equiv 1 \bmod p^2$ and it follows that $d \equiv a, a' \bmod p$. Hence $y - x \in \mathfrak{P}L'_\mathfrak{p}$ or $y - x' \in \mathfrak{P}L'_\mathfrak{p}$ so that $N(L_\mathfrak{p}, c) \leq 3$ by Theorem 3.1.

5. Local representations: n even

Assume $n = \operatorname{rank} L_\mathfrak{p} \geq 4$ is even and $\mathfrak{p}$ is ramified dyadic. Then, as in Lemma 3.5,

$$L_\mathfrak{p} = H_\mathfrak{p} \perp J_\mathfrak{p} \perp (\mathfrak{O}_\mathfrak{p} z + \mathfrak{O}_\mathfrak{p} w) \quad \text{and} \quad L'_\mathfrak{p} = H_\mathfrak{p} \perp J_\mathfrak{p} \perp (\mathfrak{O}_\mathfrak{p} z + \mathfrak{P}^k w)$$

where $k = \max\{0, e - h - \operatorname{ord}_p f(w)\}$. There are no characteristic representations when $k = 0$ since then $L_\mathfrak{p} = L'_\mathfrak{p}$, that is, $L_\mathfrak{p}$ is an *even* lattice. The discriminant $dL_\mathfrak{p} = (-1)^{(n-2)/2}(f(z)f(w) - 1)N_\mathfrak{p}(\mathfrak{U}_\mathfrak{p})$ is an invariant of $L_\mathfrak{p}$. Define $\delta(L_\mathfrak{p}) = 0$ when $dL_\mathfrak{p} = (-1)^{n/2}N_\mathfrak{p}(\mathfrak{U}_\mathfrak{p})$; in particular, we can assume that $f(z) = 0$ in this case. Otherwise, define $\delta(L_\mathfrak{p}) = 2$. The invariants n, $dL_\mathfrak{p}$ (or $\delta(L_\mathfrak{p})$) and $\operatorname{ord}_p f(w)$ uniquely determine $L_\mathfrak{p}$ by [Jc, 10.4].

Lemma 5.1. *Assume $n \geq 4$ is even and $c \in \mathfrak{o}_\mathfrak{p}$ with $\mathfrak{p}$ ramified dyadic. Then*

(i) *$N(L_\mathfrak{p}, c) \leq 1$ when c is a unit,*
(ii) *$N(L_\mathfrak{p}, c) = 0$ for all $c \in \mathfrak{o}_\mathfrak{p}$ with $\operatorname{ord}_p c < e - h - k$,*
(iii) *$N(L_\mathfrak{p}, c) \geq 1$ for all $c \in \mathfrak{o}_\mathfrak{p}$ with $\operatorname{ord}_p c \geq e - h - k$,*
(iv) *$N(L_\mathfrak{p}, c) = 1$ when $k = 0$ for all $c \in \mathfrak{o}_\mathfrak{p}$ with $\operatorname{ord}_p c \geq e - h$.*

Proof. Assume primitive $x \in L_\mathfrak{p}$ represents $c \in \mathfrak{o}_\mathfrak{p}$. If x is characteristic, then $f(x, L'_\mathfrak{p}) \subset \mathfrak{P}$ and $x \equiv az \bmod \mathfrak{P}L_\mathfrak{p}$ for some unit $a \in \mathfrak{U}_\mathfrak{p}$. Then $c = f(x) \equiv N_\mathfrak{p}(a)f(z) \equiv 0 \bmod \mathfrak{P}$, since $f(z) \in 2p^{-h}\mathfrak{o}_\mathfrak{p}$ by Lemma 3.3. This proves (i) since there is at most one noncharacteristic representation (up to equivalence). Since $\operatorname{ord}_p f(w) \geq e - h - k$, the lattice $L_\mathfrak{p}$ cannot represent any element c with $\operatorname{ord}_p c < e - h - k$; this proves (ii). As in Lemma 4.1, there is a noncharacteristic representation of each $c \in \mathfrak{o}_\mathfrak{p}$ with $\operatorname{ord}_p c \geq e - h - k$. When $k = 0$ this is the only representation (up to equivalence).

Lemma 5.2. *Assume $n \geq 4$ is even, $e = 1$, $k > 0$ and $\mathfrak{p}$ ramified prime. Then $N(L_\mathfrak{p}, c) = 2^f$ for $c \in 2\mathfrak{o}_\mathfrak{p}$.*

Proof. Since $k > 0$ and $e = 1$ it follows that $k = 1$ and $f(w)$ is a unit. Also $f(z) \in 2\mathfrak{o}_\mathfrak{p}$ by Lemma 3.3. Put $x = \zeta(u + bv) + dz + a\zeta w$ with $a, b \in \mathfrak{o}_\mathfrak{p}$ and $d \in \mathfrak{u}_\mathfrak{p}$. Then $f(x) = 2pb + d^2f(z) + pa^2f(w)$. For fixed d, choose $a \in \mathfrak{o}_\mathfrak{p}$ such that $pa^2f(w) \equiv c - d^2f(z) \bmod 4$, and then b such that $f(x) = c$. Varying d, this gives $2^f - 1$ inequivalent characteristic representations of c. Hence $N(L_\mathfrak{p}, c) \geq 2^f$, since there also exists a noncharacteristic representation of c

from Lemma 5.1. Let $y = \zeta r + d'z + a'\zeta w$ be a characteristic representation of c, where r lies in $H_{\mathfrak{p}} \perp J_{\mathfrak{p}}$. Then $d \equiv d' \bmod \mathfrak{P}$ for one of the x's above and $y - x \equiv (a' - a)\zeta w \bmod \mathfrak{P}L'_{\mathfrak{p}}$. Since $f(y) = c = f(x)$, it follows that $N_{\mathfrak{p}}(a') \equiv a^2 \bmod 2$ and hence $a' \equiv a \bmod \mathfrak{P}$. Thus x and y are equivalent representations, and $N(L_{\mathfrak{p}}, c) \le 2^f$.

Lemma 5.3. *Assume $n \geq 4$ is even, with $\mathfrak{p}$ ramified unit, $h = e - 1$, $k > 0$ and $\delta(L_{\mathfrak{p}}) = 0$. Then*

(i) $N(L_{\mathfrak{p}}, c) = 2^{f+1} - 1$ *when* $\operatorname{ord}_p c \geq 2$,

(ii) $N(L_{\mathfrak{p}}, c) = 2^f - 1$ *when* $\operatorname{ord}_p c = 1$.

Proof. Since $k > 0$ and $h = e - 1$, it follows that $k = 1$ and $f(w)$ is a unit. Since $dL_{\mathfrak{p}} = (-1)^{n/2}N_{\mathfrak{p}}(\mathfrak{U}_{\mathfrak{p}})$ and $\operatorname{ord}_p f(w)$ determine $L_{\mathfrak{p}}$, we may assume $f(z) = 0$ and $f(w) = 1$. Put $x = \pi(u + bv) + dz + a\pi w$ with $a \in \mathfrak{o}_{\mathfrak{p}}$, $b \in \mathfrak{O}_{\mathfrak{p}}$ and $d \in \mathfrak{u}_{\mathfrak{p}}$. Then $f(x) = p\delta T_{\mathfrak{p}}(b) + ad2p^{-h} + p\delta a^2$.

Assume first $\operatorname{ord}_p c \geq 2$. Fix $d \in \mathfrak{u}_{\mathfrak{p}}$ and put $a = 0$ or $a = -2p^{-e}d\delta^{-1} \in \mathfrak{u}_{\mathfrak{p}}$, and choose $b \in \mathfrak{O}_{\mathfrak{p}}$ such that $f(x) = c$. Since there are $2^f - 1$ choices for $d \bmod p$, this gives $2(2^f - 1)$ inequivalent characteristic representations of c, and hence $N(L_{\mathfrak{p}}, c) \geq 2^{f+1} - 1$. Conversely, if $y = \pi r + d'z + a'\pi w$ represents c, then $d' \equiv d \bmod \mathfrak{P}$ for one of the x's constructed above. It follows that $a' \equiv 0 \bmod \mathfrak{P}$ or $a' \equiv 2p^{-e}d\delta^{-1} \bmod \mathfrak{P}$, and hence y is equivalent to one of these x's. Thus $N(L_{\mathfrak{p}}, c) = 2^{f+1} - 1$.

Now assume $p^{-1}c$ is a unit. Put $b = 0$ and choose $a \in u_p$ such that $a^2\delta \not\equiv p^{-1}c \bmod P$. Then choose $d \in u_p$ so that $f(x) = c$. Since there are $2^f - 2$ choices for $a \bmod p$, this gives $2^f - 2$ inequivalent characteristic representations of c. Hence $N(L_p, c) \geq 2^f - 1$. Conversely, any characteristic representation of c is equivalent to one of those just constructed, so that $N(L_p, c) = 2^f - 1$.

Lemma 5.4. *Assume $n \geq 4$ is even, with $\mathfrak{p}$ ramified unit, $h = e - 1$, $k > 0$ and $\delta(L_{\mathfrak{p}}) = 2$. Then*

(i) $N(L_{\mathfrak{p}}, c) = 1$ *when* $\operatorname{ord}_p c \geq 2$,

(ii) $N(L_{\mathfrak{p}}, c) = 2^f + 1$ *when* $\operatorname{ord}_p c = 1$.

Proof. Since $\delta(L_{\mathfrak{p}}) = 2$ and $k = 1$, $V_{\mathfrak{p}}$ cannot be hyperbolic so that $f(w)$ is a unit and the binary lattice $\mathfrak{O}_{\mathfrak{p}}z + \mathfrak{O}_{\mathfrak{p}}w$ must be anisotropic. Hence

$$\operatorname{ord}_p f(dz + \pi aw) = 1$$

for all $d \in \mathfrak{U}_{\mathfrak{p}}$ and $a \in \mathfrak{O}_{\mathfrak{p}}$. Therefore, $L_{\mathfrak{p}}$ cannot characteristically represent any $c \in p^2\mathfrak{o}_{\mathfrak{p}}$, proving (i). Now assume $\operatorname{ord}_p c = 1$. Fix $a \in \mathfrak{o}_{\mathfrak{p}}$. Since $f(z + \pi aw) = p\varepsilon$ for some unit ε, there exist $d \in \mathfrak{u}_{\mathfrak{p}}$ and $b \in \mathfrak{O}_{\mathfrak{p}}$ such that $x = \pi(u + bv) + d(z + \pi aw)$ represents c. Hence there exist 2^f inequivalent characteristic representations of c and $N(L_{\mathfrak{p}}, c) \geq 2^f + 1$. Conversely, since $a \bmod \mathfrak{P}$ uniquely determines $d \bmod \mathfrak{P}$, any characteristic representation of c is equivalent to one constructed above. Hence $N(L_{\mathfrak{p}}, c) = 2^f + 1$.

6. Quadratic extensions of $\mathbf{Q}$

Let $F = \mathbf{Q}$, $K = \mathbf{Q}(\sqrt{m})$, with m a square free integer, and $\mathfrak{o}_F = \mathbf{Z}$. Let p be a rational prime. Then p splits in K if either $p = 2$ and $m \equiv 1 \bmod 8$, or p is odd and $\left(\frac{m}{p}\right) = 1$. Otherwise, for $p = 2$, we have an unramified extension if $m \equiv 5 \bmod 8$, a ramified unit extension with $h = 0$ if $m \equiv 3 \bmod 4$, and a ramified prime extension if m is even. Since $-1 \notin N_{\mathfrak{p}}(\mathfrak{U}_{\mathfrak{p}})$ at the dyadic prime when $m \equiv 3 \bmod 4$, we may assume $f(w) = \delta(L_{\mathfrak{p}})$ in $L_{\mathfrak{p}}$ when n is odd, and $f(z) = \delta(L_{\mathfrak{p}})$ and $f(w) = 1$ when n is even and $L_{\mathfrak{p}}$ is not even, in this situation.

Theorem 6.1. *Let L be a unimodular lattice on an indefinite hermitian space V of dimension $n \geq 3$ over $K = \mathbf{Q}(\sqrt{m})$. Let $c \neq 0$ be a rational integer represented by L, and assume the local Witt index of $V \perp \langle -c \rangle$ at the real prime is at least two when $m < 0$. Then*

(i) *$N(L, c) = 3$ when $m \equiv 3 \bmod 4$, $c \equiv \delta(L_{\mathfrak{p}}) \bmod 4$ and $L_{\mathfrak{p}}$ is not even,*
(ii) *$N(L, c) = 2$ when $m \equiv 2 \bmod 4$, $n \equiv c \bmod 2$ and $L_{\mathfrak{p}}$ is not even,*
(iii) *$N(L, c) = 1$ otherwise.*

Proof. This follows from Theorem 1.1 and the local results in the two previous sections since $e = f = 1$ for any ramifying dyadic prime.

Remark. This theorem also provides information about the orbits in $L(c)$ under the action of the group $U(L)$. Clearly, when $N(L, c) = 1$ there is also only one orbit under the action of $U(L)$. However, when $N(L, c) > 1$ there will also be at least two orbits under $U(L)$, for no locally characteristic vector in $L(c)$ can be mapped by $U(L)$ into a locally noncharacteristic vector.

Example. Assume $m \equiv 3 \bmod 4$ and L is a free $\mathfrak{O}_K$-module with orthogonal basis $x_1, \ldots, x_n$, where $f(x_i) = -1$ for $1 \leq i \leq r$ and $f(x_i) = 1$ for $r+1 \leq i \leq n$. Then $dL_2 = (-1)^r \in N_2(\mathfrak{U}_2)$ if and only if r is even (and then $\delta(L_2) = 0$ or 1). Assume $1 \leq r < n$ where $m < 0$ so that L is indefinite. Let $c \in \mathbf{Z}$ be nonzero. When $m < 0$, assume $r \geq 2$ if $c < 0$, and $r \leq n-2$ if $c > 0$, so that the index condition on $V \perp \langle -c \rangle$ is satisfied. Then $N(L, c) = 3$ if either n is even and $c \equiv 2r \bmod 4$, or n is odd and $c \equiv 2r + 1 \bmod 4$; otherwise $N(L, c) = 1$.

7. Cyclotomics fields

We now consider hermitian forms over the cyclotomic field $K = \mathbf{Q}(\omega)$, with ω a primitive mth root of unity, and $F = \mathbf{Q}(\omega) \cap \mathbf{R} = \mathbf{Q}(\omega + \omega^*)$ the maximal real subfield of K. The involution $*$ on K is complex conjugation. Let $\mathfrak{o} = \mathfrak{o}_F$ be the ring of algebraic integers in F.

Theorem 7.1. *Let L be a unimodular lattice on an hermitian space V of dimension $n \geq 3$ over $K = \mathbf{Q}(\omega)$ where ω is a primitive mth root of unity and $m \geq 3$ is odd. Assume L represents $c \in \mathfrak{o}_F$, $c \neq 0$, and the local Witt index of $V \perp \langle -c \rangle$ is at least two for some archimedean prime spot. Then $N(L, c) = 1$.*

Proof. When $m \geq 3$ is odd, the prime 2 is unramified in K and, consequently, $N(L, c) \leq 1$ for any nonzero $c \in \mathfrak{o}_F$, by Theorem 1.1. □

When $m = 2^k \geq 4$, it follows that $\imath \in K$ where $\imath^2 = -1$, and hence $K = F(\imath)$. Moreover, 2 totally ramifies in K. When $\mathfrak{p} \in S$ is the unique dyadic prime spot, $K_\mathfrak{p}/F_\mathfrak{p}$ is a dyadic ramified unit extension with $e = \operatorname{ord}_2 p = \frac{1}{2}\phi(2^k) = 2^{k-2}$. Since $\imath^2 = 1 - p^e\varepsilon$ with ε a unit in $\mathfrak{o}_\mathfrak{p}$, it follows that $h = 0$ when $e = 1$, and $e > h \geq \frac{1}{2}(e-1)$, in general. Therefore, $e = 2$ and $h = 1$ when $m = 8$.

Lemma 7.2. *Let $K = \mathbf{Q}(\omega)$ where ω is a primitive mth root of unity with $m = 2^k \geq 4$. If $\mathfrak{p}$ is the unique prime spot over 2, then $K_\mathfrak{p}/F_\mathfrak{p}$ is a ramified unit extension with $e = m/4$ and $h = e - 1$.*

Proof. It remains to show $h = e - 1$ when $m \geq 16$. Put $p = \omega + \omega^* \in \mathfrak{o}_\mathfrak{p}$. Since e is a 2-power, $\binom{e}{e/2} \equiv 2 \bmod 4$, and $\binom{e}{i} \equiv 0 \bmod 4$ for $1 \leq i < e/2$. Hence $\omega^e = \imath$ and $p^e = (\omega + \omega^*)^e \equiv 2 \bmod 4$, so that p is prime in $F_\mathfrak{p}$. Put

$$a = 1 + p^{e/2} + p^{3e/4} + p^{7e/8} + \cdots + p^{(e-1)e/e}.$$

Then $a \in \mathfrak{o}_\mathfrak{p}$ and $(a\imath)^2 \equiv 1 - p^{2e-1} \bmod 4$. Since $K_\mathfrak{p} = F_\mathfrak{p}(a\imath)$ it follows that $h = e - 1$. □

Now return to the general cyclotomic field $K = \mathbf{Q}(\omega)$ where $m = 2^k m'$ with $k \geq 2$ and m' odd. Let $\mathfrak{p}$ be a dyadic prime spot in S. Denote by g the number of dyadic spots in S. Each $\mathfrak{p}$ will now ramify in K. As before, let $e = \operatorname{ord}_p 2$ be the ramification index in $F_\mathfrak{p}$ and hence also in F. Then $e = 2^{k-2}$, since 2 is unramified in $\mathbf{Q}(\omega')$ where ω' is a primitive m'th root of unity. Let f denote the residue class degree of p in F (and hence also in $K = F(\imath)$). Then $f \geq 1$ is minimal such that $2^f \equiv 1 \bmod m'$ (with $f = 1$ when $m' = 1$) and $2efg = \phi(m)$. Hence $fg = \phi(m')$. Define $g' = g'(L)$ ($\leq g$) to be the number of dyadic primes $\mathfrak{p}$ where $\delta(L_\mathfrak{p}) = 1$ when n is odd, and where $\delta(L_\mathfrak{p}) = 0$ and $L_\mathfrak{p}$ is not an even lattice when n is even. Define g'' ($\leq g - g'$) to be the number of dyadic primes where $\delta(L_\mathfrak{p}) = 2$ and $L_\mathfrak{p}$ is not even.

Theorem 7.3. *Let L be a unimodular lattice on an hermitian space V of dimension $n \geq 3$ over $K = \mathbf{Q}(\omega)$, where ω is a primitive mth root of unity. Assume L represents the nonzero integer $c \in \mathbf{Z}$ and that the local Witt index of $V \perp \langle -c \rangle$ is at least two at some archimedean prime spot. Then, when $m \equiv 0$* mod 8,

(i) $N(L, c) = (2^{f+1} - 1)^{g'}$ *when* $n \equiv c \equiv 0 \bmod 2$,
(ii) $N(L, c) = 3^{g'}$ *when* $n \equiv c \equiv 1 \bmod 2$,
(iii) $N(L, c) = 1$ *otherwise;*

and when $m \equiv 4 \bmod 8$,

(iv) $N(L, c) = (2^{f+1} - 1)^{g'}$ *when* $2n \equiv c \equiv 0 \bmod 4$,
(v) $N(L, c) = (2^f - 1)^{g'}(2^f + 1)^{g''}$ *when* $n \equiv 0 \bmod 2$ *and* $c \equiv 2 \bmod 4$,
(vi) $N(L, c) = 3^{g'}$ *when* $n \equiv c \equiv 1 \bmod 2$, *provided f is even when* $c \equiv 3 \bmod 4$,
(vii) $N(L, c) = 3^{g-g'}$ *where n and f are odd, and* $c \equiv 3 \bmod 4$,
(viii) $N(L, c) = 1$ *otherwise.*

Proof. Apply Theorem 1.1 and the local results in §§4 and 5. The condition $m \equiv 0 \bmod 8$ ensures that locally $e \geq 2$ with $e - h = 1$ for any dyadic prime, so that $c \equiv 0, 1 \bmod p^2$. However, $e = 1$ and $p = 2$ when $m \equiv 4 \bmod 8$. Parts (i), (iv) and (v) then follow from Lemmas 5.3 and 5.4.

Now assume n is odd. As in Lemma 7.2, take $p^e \equiv 2 \bmod 4$ and $\zeta^2 \equiv 1 - p^{2e-1} \bmod 4$. Consider first $\delta(L_\mathfrak{p}) = -1$. Choose $b \in \mathfrak{u}_\mathfrak{p}$ such that $X^2 + X \equiv b \bmod p$ has no roots; in particular, take $b = 1$ when f is odd. Put $f(w) = 1 + pb \notin N_\mathfrak{p}(\mathfrak{U}_\mathfrak{p})$. When $e \geq 2$, the congruence in Lemma 4.3 has no solutions for c odd, and hence there are no characteristic representations of c. When $e = 1$, so that $p = 2$ and $\pi = 1 + \imath$, the congruence has a solution if and only if $c \equiv 3 \bmod 4$ and f is odd (that is when $b = 1$). Finally let $\delta(L_\mathfrak{p}) = 1 = f(w)$. If c is odd, the congruence in Lemma 4.3 can always be solved when $e \geq 2$, or when $c \equiv 1 \bmod 4$. However, if $e = 1$ and $c \equiv 3 \bmod 4$, the congruence can only be solved when f is even, since it reduces to solving $X^2 + X \equiv 1 \bmod 2$. The remaining parts of the theorem now follow from Lemma 4.5.

Remarks. The value of $N(L, c)$ can be computed when $c \notin \mathbf{Z}$, but it now also depends on the varying values of $\operatorname{ord}_p c$ at the dyadic primes. The comment following Theorem 6.1 also applies here.

Acknowledgment

The author thanks the referee for suggesting a number of improvements in the presentation.

References

[G] L. J. Gerstein, *Integral decomposition of hermitian forms*, Amer. J. Math. **92** (1970), 398–418.

[Jc] R. Jacobowitz, *Hermitian forms over local fields*, Amer. J. Math. **84** (1962), 441–465.

[J1] D. G. James, *On Witt's theorem for unimodular quadratic forms*, Pacific J. Math. **26** (1968), 303–316 and **33** (1970), 645–652.

[J2] ——, *Representations by integral quadratic forms*, J. Number Theory **4** (1972), 321–329.

[J3] ——, *Invariant submodules of unimodular hermitian forms*, Pacific J. Math. **72** (1977), 471–482.

[J4] ——, *Integral sums of squares in algebraic number fields*, Amer. J. Math. **113** (1991), 129–146.

[K] D. Z. Kilhefner, *Integral extensions of isometries of unimodular hermitian forms*, Ph. D. Thesis, Pennsylvania State Univ., 1971.

[N] V. V. Nikulin, *Integral symmetric bilinear forms and some of their applications*, Math. USSR-Izv. **14** (1980), 103–167.

[O'M] O. T. O'Meara, *Introduction to quadratic forms*, Springer-Verlag, New York, 1963.

[S] G. Shimura, *Arithmetic of unitary groups*, Ann. of Math. **79** (1964), 369–409.

[W] C. T. C. Wall, *On the orthogonal groups of unimodular quadratic forms*, Math. Ann. **147** (1962), 328–338.

Department of Mathematics, Pennsylvania State University, University Park, Pennsylvania 16802

E-mail address: james@math.psu.edu