

SPINOR NORMS OF LOCAL INTEGRAL ROTATIONS I

J. S. HSIA

The spinor norms of integral rotations on a modular quadratic form over a local field are determined. Whenever possible, these results are expressed in convenient closed forms.

In studying integral quadratic forms over a global field, the obstruction to a Hasse-type local-global principle is measured by the class number of a form in its genus. The spinor genus occupies a vital intermediate level between the class and the genus. Even in the indefinite theory, where the class and the spinor genus should coincide (when there are three or more variables involved), the genus generally is strictly larger than the spinor genus. Thus, it is important that one be able to determine the number of spinor genera in a genus. This number can be computed by means of an idèlic index formula, which requires the knowledge of spinor norms of local integral rotations associated to the given form. Via the Jordan decompositions, the local computations of these spinor norms depend in turn on the modular components. Therefore, it is essential that we know the spinor norms of these local integral "modular" rotations. By scaling, it is sufficient to restrict to the unimodular situation, which is the scope of the present article. We adopt the geometric language of quadratic spaces and lattices instead of the more classical terminology of fractional and integral forms. Our notations used here are those from O'Meara's fundamental text, [1]. Thus, F denotes a local field of characteristic different from 2, \mathfrak{o} the ring of integers in F , $\mathfrak{P} = \pi\mathfrak{o}$ the unique nonzero prime ideal of \mathfrak{o} , \mathfrak{U} the group of units in \mathfrak{o} , $e = \text{ord}(2)$ the ramification index of 2 in the (dyadic) field F , $\mathfrak{D}(\cdot)$ the quadratic defect function, Δ the unique (modulo a unit square) unit of quadratic defect $4\mathfrak{o}$, V a regular quadratic space of dimension n over F , L a unimodular lattice of determinant (discriminant) d on V , $\mathfrak{w}L = b\mathfrak{o}$ the weight ideal of L , $\mathfrak{g}L = a\mathfrak{o}^2 + b\mathfrak{o}$ the norm group of L where a and b denote respectively the norm and weight generators, $O^+(V)$ the group of rotations on V , $O^+(L)$ the corresponding subgroup of units of L , and $\theta(\cdot)$ the spinor norm function.

If $n = 1$, it is clear that $\theta(O^+(L)) = F^{\cdot 2}$. When F is nondyadic, $\theta(O^+(L)) = \mathfrak{U}F^{\cdot 2}$ for $n \geq 2$ (see 92:5, [1]). Thus, we need only be concerned with the dyadic case. So, whenever $n \geq 3$, $\theta(O^+(L))$ contains $\mathfrak{U}F^{\cdot 2}$ by 93:20, [1]. Proposition A below provides the complete

answer for $n \geq 3$. However, we first need a lemma.

LEMMA 1. *For any totally improper unimodular lattice L (i.e., $Q(x) \in 2\mathfrak{o}$ for every $x \in L$), $\theta(0^+(L)) = \mathfrak{u}F^{\cdot 2}$.*

Proof. (i) We first show for $L \cong A(2, 2\rho)$, adapted say to a basis $\{x, y\}$. Any vector v which is primitive in L and such that the symmetry S_v lies in $O(L)$ must satisfy: $Q(v) \neq 0$, and $\text{ord}(Q(v)) = e$. As every integral rotation σ on L is a product of two integral symmetries, $\theta(\sigma) \in \mathfrak{u}F^{\cdot 2}$. On the other hand, given any unit c , there is a primitive vector u in L with $Q(u) = 2c$. So, $\theta(S_x S_u) = cF^{\cdot 2}$. Thus, $\theta(0^+(L)) = \mathfrak{u}F^{\cdot 2}$.

(ii) We next show for L a hyperbolic lattice, i.e., $L \cong m \times A(0, 0)$. Suppose m is either 1 or greater or equal to 3. Then, a theorem of O'Meara-Pollak (see [2]) asserts that $O(L)$ is generated by integral symmetries. Once again, a primitive anisotropic vector v in L gives rise to an integral symmetry S_v if and only if $\text{ord}(Q(v)) = e$. Thus, an even product of these S_v 's will always yield a spinor norm that lies in $\mathfrak{u}F^{\cdot 2}$. Conversely, as L represents all of $2\mathfrak{o}$ primitively, every square class in $\mathfrak{u}F^{\cdot 2}$ will be caught. For $m = 2$, we need only to observe the following trivial inclusions: $0^+(A(0, 0)) \subseteq 0^+(2 \times A(0, 0)) \subseteq 0^+(3 \times A(0, 0))$.

(iii) The general case now follows from the well-known isometry between $A(0, 0) \perp A(0, 0)$ and $A(2, 2\rho) \perp A(2, 2\rho)$.

PROPOSITION A. *Let $n \geq 3$. Then, $\theta(0^+(L)) = \mathfrak{u}F^{\cdot 2}$ if and only if $\text{ord}(a) + \text{ord}(b)$ is even (writ $ab \sim 1$). When $\text{ord}(a) + \text{ord}(b)$ is odd (writ $ab \sim \pi$), $\theta(0^+(L)) = F^{\cdot}$.*

Proof. By the lemma, we may suppose that $\text{ord}(a) < e$. If $ab \sim 1$, then L is equivalent to either $A(0, 0) \perp \cdots \perp A(0, 0) \perp \langle \pm d \rangle$ or $A(0, 0) \perp \cdots \perp A(0, 0) \perp A(a, \alpha)$, $\alpha \in 2\mathfrak{o}$. The generation of $O(L)$ by integral symmetries is again guaranteed by O'Meara-Pollak's theorem. Any primitive vector $v \in L$ with $S_v \in O(L)$ must have $\text{ord}(Q(v)) \leq e$. Should strict inequality prevail, then $Q(v)$ is congruent to either dt^2 or at^2 modulo $2\mathfrak{o}$, for some $t \in \mathfrak{o}$ with $\text{ord}(t^2) < e$, so that $\theta(0^+(L)) \subseteq \mathfrak{u}F^{\cdot 2}$. Containment in the other direction is clear since L always contains $A(0, 0)$. Now, let $ab \sim \pi$. We already know that $\theta(0^+(L))$ contains $\mathfrak{u}F^{\cdot 2}$ as $n \geq 3$. Also, L represents all the weight generators b . Hence, there is a rotation σ on L with spinor norm $\theta(\sigma) = abF^{\cdot 2}$. Thus, $\theta(0^+(L))$ catches all of F^{\cdot} .

In view of this proposition, we shall henceforth be concerned only with binary unimodular lattices. Furthermore, we may suppose

these lattices are not totally improper. In particular, every integral rotation is a product of two integral symmetries, the first or the second of which may be arbitrarily specified (a consequence of the so-called Cartan-Dieudonné theorem). We fix some notations here that will be used throughout the remaining of this article. Write $L \cong A(a, -\delta a^{-1})$, adapted to a basis $\{x, y\}$, where $\mathfrak{D}(1 + \delta) = \delta\mathfrak{o}$ and $-\delta a^{-1}$ belongs to $\mathfrak{m}L = b\mathfrak{o}$. Put $\text{ord}(a) = \nu$ and $\mu = e - \nu$. Also, let $A = \{v \in L \mid v \text{ primitive and } \text{ord}(Q(v)) \leq e\}$, and

$$D = \{Q(v) \mid v \in A\} .$$

Thus, from the remarks made above, it is evident that $\theta(0^+(L)) = aDF^{\cdot 2}$. In most situations, we shall see that the set $aDF^{\cdot 2}$ can be very explicitly determined and the results are expressible in convenient closed forms.

PROPOSITION B. *Let $L \cong A(a, b)$ (i.e., $b = -\delta a^{-1}$) with $ab \sim \pi$. Then, $\theta(0^+(L)) = \theta(0^+(V)) = Q(\langle 1, d \rangle)F^{\cdot 2}$. (Note: $ab \sim \pi$ occurs whenever $\mathfrak{m}L$ exceeds $2\mathfrak{o}$.)*

Proof. Take any $z \in V$ with $Q(z)$ in the norm group $\mathfrak{g}L$. Write $Q(z) = s^2a + 2st + bt^2$, $s, t \in F$. If $s \in \mathfrak{o}$, then t is also integral since $\text{ord}(bt^2) \leq \text{ord}(2st)$ whenever $t \notin \mathfrak{P}$. Similarly, if $t \in \mathfrak{o}$, then $s \in \mathfrak{o}$. If neither s nor t lies in \mathfrak{o} , then one sees from the non-archimedean nature of the valuation together with the hypothesis $\text{ord}(ab)$ being odd that

$$\text{ord}(Q(z)) = \text{Min} \{ \text{ord}(s^2a), \text{ord}(bt^2) \} .$$

Therefore, both s and t belong to \mathfrak{o} , and we have $z \in L$. This means the lattice L is characterized by the set $L = \{z \in V \mid Q(z) \in \mathfrak{g}L\}$. In particular, every fractional isometry on V is in fact an integral isometry on L as well. Thus, $\theta(0^+(L)) = \theta(0^+(V))$. But, $\theta(0^+(V))$ is unaffected by scaling, and the rest is clear.

REMARK (a). From the results obtained so far, the unramified dyadic case follows immediately. L can only assume one of the following five possibilities: $A(0, 0)$, $A(2, 2\rho)$, $A(1, 0)$, $A(1, 4\rho)$, and $A(c, 2f)$, c, f are units. Since both $A(1, 0)$ and $A(1, 4\rho)$ represent all the units, we see that the first four cases all yield $\theta(0^+(L)) = \mathfrak{u}F^{\cdot 2}$, while the last case by Proposition B gives $Q(\langle 1, d \rangle)F^{\cdot 2}$ where

$$d = \det(A(c, 2f)) .$$

We may now further restrict ourselves to the binary “depleted” unimodular case, i.e., when the weight $\mathfrak{m}L = b\mathfrak{o} = 2\mathfrak{o}$ is minimal.

Depletedness implies then $-\delta a^{-1} \in 2\mathfrak{o}$. The next lemma gives both the upper and lower bounds for aDF^{*2} .

LEMMA 2. *Let L be a binary depleted unimodular lattice over F . Assume the defect $\mathfrak{D}(-d) = \delta\mathfrak{o} \neq 2a\mathfrak{o}$. Then,*

$$(1 + \mathfrak{P}^e)F^{*2} \subseteq \theta(0^+(L)) \subseteq \mathfrak{u}F^{*2}.$$

Proof. We may suppose by Lemma 1 that L is not totally improper. So, $\text{ord}(a) = \nu < e$. We also have $\text{ord}(\delta a^{-1}) > e$. If $z \in A$ and $Q(z) = s^2a(1 + 2t/sa - \delta t^2/s^2a^2)$, then surely $aQ(z)F^{*2}$ belongs to $\mathfrak{u}F^{*2}$.

We now show that $(1 + \mathfrak{P}^e)F^{*2} \subseteq aDF^{*2}$. Take any element of the form $1 + h$, $h \in \mathfrak{P}^e$. If $\delta = 0$, the vector $v = x + (ha/2)y$ lies in A , and $\theta(S_x S_y) = (1 + h)F^{*2}$. If $\delta \neq 0$, consider the polynomial

$$f(X) = X^2 - (2a/\delta)X + (ha^2/\delta).$$

As $\text{ord}(f(X)) = \text{ord}(2a/\delta)$, $f(X)$ is reducible by Hensel's lemma (see 13:9, [1]). Write $f(X) = (X - r_1)(X - r_2)$. Since

$$\text{ord}(r_1 + r_2) = \text{ord}(2a/\delta)$$

and $\text{ord}(r_1 r_2) = \text{ord}(ha^2/\delta)$, at least one root, say r_1 , of $f(X)$ is integral. Thus, $\theta(S_x S_{x+r_1 y}) = (1 + h)F^{*2}$.

REMARK (b). All the assumptions imposed on this lemma are necessary for either containment. Suppose the depletedness condition were removed, take an anisotropic space $V \cong \langle 1, d \rangle$ with $d \neq -A$. As the group index $[F^*: \dot{Q}(V)] = 2$, exactly half of the odd-ordered elements and half of the nonzero even-ordered scalars are represented by V . Hence, the containment

$$\theta(0^+(L)) \subseteq \mathfrak{u}F^{*2}$$

surely breaks down. Lemma 3 below will show that the other end of the inclusion will also fail. Next suppose $\delta\mathfrak{o} = 2a\mathfrak{o}$, then $\mathfrak{D}(-d) = \delta\mathfrak{o} \supset 4\mathfrak{o}$ (as $\nu < e$) so that $\text{ord}(\delta)$ is odd which means $ab \sim \pi$, and Proposition B applies. Again, Lemma 3 will show $(1 + \mathfrak{P}^e)F^{*2}$ is not contained in $\theta(0^+(L))$.

LEMMA 3 (Duality). *Let c be a unit of quadratic defect $\mathfrak{D}(c) = \mathfrak{P}^t$, where $1 \leq t < 2e$. Then, there is a unit f such that the Hilbert symbol $(c, f)_{\mathfrak{P}} = -1$, and the defect $\mathfrak{D}(f) = \mathfrak{P}^{2e-t}$.*

Proof. Write $c = s^2(1 + \pi^t r)$ with s, r units. Removing s^2 changes

neither the defect nor the value of the Hilbert symbol, so we may assume $s = 1$. The binary quadratic space $W \cong \langle c, \Delta - c \rangle$ has for its determinant a prime element since t is odd. As W represents Δ , it cannot also represent 1. Hence, the Hilbert symbol $(c, \Delta - c)_{\mathfrak{p}} = -1$. On the other hand, the binary space $\langle c, -\pi r \rangle$ clearly represents 1, so $(c, -\pi r)_{\mathfrak{p}} = 1$. Therefore, $(c, h)_{\mathfrak{p}} = -1$ where $h = r(c - \Delta)/\pi^t$. Put $f = h/r^2 = 1 + 4\rho(\pi^t r)^{-1}$. Manifestedly, $(c, f)_{\mathfrak{p}} = -1$ and $\mathfrak{D}(f) = \mathfrak{P}^{2e-t}$.

REMARK (c). If $cF^{*2} \in \theta(0^+(L))$, c must necessarily be represented by $\langle 1, d \rangle$. Hence, the Hilbert symbol $(-d, c)_{\mathfrak{p}}$ must be 1.

REMARK (d). Let L be as in Lemma 2, and $c = 1 + s + t$, $s \in \mathfrak{P}$, $t \in \mathfrak{P}^{\mu}$. Then, $cF^{*2} \in \theta(0^+(L))$ if and only if $(1 + s)F^{*2} \in \theta(0^+(L))$. This is because by Lemma 2, $1 + (t/1 + s)$ belongs to $\theta(0^+(L))$, and $c = (1 + s)(1 + (t/1 + s))$.

REMARK (e). If $k < e$, then $(1 + \mathfrak{P}^{2k})F^{*2} = (1 + \mathfrak{P}^{2k+1})F^{*2}$. This follows as an immediate consequence of the perfectness of the residue class field of F .

PROPOSITION C. Let $L \cong A(a, -\delta a^{-1})$ with $\delta =$ either 0 or 4ρ , and $\text{ord}(a) < e$. We have:

$$\begin{aligned} \mu \equiv 0, 1 \pmod{4} &\implies \theta(0^+(L)) = (1 + \mathfrak{P}^{[\mu/2]})F^{*2} \\ \mu \equiv 2 \pmod{4} &\implies \theta(0^+(L)) = (1 + \mathfrak{P}^{[\mu/2]-1})F^{*2} \\ \mu \equiv 3 \pmod{4} &\implies \theta(0^+(L)) = (1 + \mathfrak{P}^{[\mu/2]+1})F^{*2}. \end{aligned}$$

(Here $[-]$ denotes the usual greatest integer function.)

Proof. When $\delta = 0$, let $v = sx + ty \in A$. Clearly, $\theta(0^+(L))$ is contained in the respective sets cited above. Conversely, any element of the form $1 + h$, $h \in \mathfrak{P}^{\mu - [\mu/2]}$, can be caught by $\theta(S_x S_{x+(h a/2)y})$ provided $\text{ord}(h) \geq \mu$. If $\text{ord}(h) < \mu$, let $s = 2/ha$. Then, $\text{ord}(s^2 a) = 2e - \nu - 2 \text{ord}(h) \leq e$, $v = sx + y \in A$, and $\theta(S_x S_v) = (1 + h)F^{*2}$. The rest follows from Remark (e).

When $\delta = 4\rho$, again the containment of $\theta(0^+(L))$ in the respective sets is easy to see. Let h, s , and v be as just above. By Lemma 2, we may suppose $\text{ord}(h) < \mu$. $\theta(S_x S_v) = (1 + h - 4\rho/s^2 a^2)F^{*2}$. As $4\rho/s^2 a^2 \in \mathfrak{P}^{\mu}$, Remark (d) applies.

We are now left with $L \cong A(a, -\delta a^{-1})$ where $e < \text{ord}(\delta a^{-1}) < e + \mu$. we break into two classes, the first of which still admits for $\theta(0^+(L))$ to be expressible in closed form — in fact, it extends Proposition C to the cases where $2e > \text{ord}(\delta) > e + \nu + [\mu/2]$, and the

second class does not.

PROPOSITION D. *Let $e + \mu > \text{ord}(\delta a^{-1}) > e + [\mu/2]$. Then, $\theta(0^+(L))$ is given as in Proposition C.*

PROPOSITION E. *Let $e + [\mu/2] \geq \text{ord}(\delta a^{-1}) > e$. Then, we have: $(1 + \mathfrak{P}^{2e - \text{ord}(\delta) + 1})F^{*2} \subseteq \theta(0^+(L))$, while $(1 + \mathfrak{P}^{2e - \text{ord}(\delta)})F^{*2} \not\subseteq \theta(0^+(L))$.*

To handle these two propositions, we need another lemma.

LEMMA 4. *Let $c = 1 + t$ be a unit with defect to , $\mathfrak{P}^u \subset to \subseteq \mathfrak{P}$. Supposing $t\delta \in 4\mathfrak{P}$ and*

$$\text{ord}(t) \geq \begin{cases} [\mu/2] + 1 & \text{if } \mu \equiv 3 \pmod{4} \\ [\mu/2] & \text{if otherwise} \end{cases} .$$

*Then, $cF^{*2} \in \theta(0^+(L))$.*

Proof. Clearly, $\text{ord}(t)$ is odd. Consider the equation:

$$tX^2 - \frac{2}{a}X + \frac{\delta}{a^2} = 0 .$$

The discriminant of the polynomial is $4(1 - \delta t)/a^2$. If we write $-\delta t = 4\pi\alpha$, then Local Square Theorem (see 63:1, [1]) gives it as $4/a^2(1 + 2\pi\beta)^2$ for some $\beta \in \mathfrak{o}$. The roots of the equation are:

$$r_1 = \frac{2(1 + \pi\beta)}{at}, \quad r_2 = \frac{-2\pi\beta}{at}$$

and so $\text{ord}(r_1) < \text{ord}(r_2)$. If μ is even, then $\text{ord}(r_1^2) = 2e - 2\nu - 2\text{ord}(t) \leq \mu$. If $\mu \equiv 1 \pmod{4}$, then the oddness of $\text{ord}(t)$ still implies $\text{ord}(t) \geq [\mu/2] + 1$. So, when μ is odd we also have $\text{ord}(r_1^2) \leq \mu$. Hence, $v = r_1x + y \in A$ and $\theta(S_x S_y) = cF^{*2}$.

Before proving Propositions D and E, we make some remarks below which serve to illustrate why we cannot expect the answer for $\theta(0^+(L))$, in the case when $e + [\mu/2] \geq \text{ord}(\delta a^{-1}) > e$, to be expressible in the convenient closed forms as those given in earlier propositions. For simplicity, we work with the special case when $a = 1$.

REMARKS. (i) Generally, V represents more units than L . In the case at hand, L only represents those units with defect contained in $2\mathfrak{o}$, while V can surely represent units with defect exceeding $2\mathfrak{o}$.

(ii) This example will show why we cannot express $\theta(0^+(L))$ in the closed form as that given in Propositions C and D. Indeed, if

e were even, say $\equiv 0 \pmod{4}$. Take $\delta = 2\pi$ and an s with $\text{ord}(s^2) = e$. Then, the unit $c = 1 + 2/s - \delta/s^2$ lies in $\theta(0^+(L))$ and has defect \mathfrak{P} . Yet, by Lemma 3 there is a unit f with defect $\mathfrak{P}^{2e - \text{ord}(\delta)} = \mathfrak{P}^{e-1}$ that cannot be caught by DF^2 . Next, if e were odd, say $\equiv 3 \pmod{4}$, take an s with $\text{ord}(s) = [e/2]$, and take $\text{ord}(\delta) = e + [e/2] - 1 = e + (e - 3)/2$. We have then $\mathfrak{D}(1 + 2/s - \delta/s^2) = \mathfrak{P}^{[e/2]}$. Again, there is a unit with defect $\mathfrak{P}^{\lfloor e/2 \rfloor + 2}$ not in DF^2 .

(iii) If DF^2 were expressible in a closed form analogous to that in Proposition B, then we might be expecting some answer in the form such as: $\theta(0^+(L)) = (Q(\langle 1, d \rangle) \cap \mathfrak{U})F^2$. But, consider the unit $c = 1 + 2/s - \delta/s^2$ with $cF^2 \in DF^2$. Let $\delta = 4\pi^{-1}$. $V = \langle 1, d \rangle$ represents the unit $f = 1 + 2/m - \delta/m^2$ where $m = 2\pi^{-3}$, and $\mathfrak{D}(f) = \mathfrak{P}^3$. While fF^2 belongs to $(Q(\langle 1, d \rangle) \cap \mathfrak{U})F^2$, it cannot be caught by DF^2 since the latter is contained in $(1 + \mathfrak{P}^{\lfloor e/2 \rfloor})F^2$, which does not contain $(1 + \mathfrak{P}^3)$ when $e \gg 0$.

Our aim now is to determine the *least* power \mathfrak{P}^r such that $(1 + \mathfrak{P}^r)F^2$ lies in $\theta(0^+(L))$. Lemma 3 asserts that $r > 2e - \text{ord}(\delta)$. This inequality turns out to be also sufficient by Proposition E.

Proof of Proposition D. If $v = sx + ty \in A$, let c be the unit $1 + 2t/sa - \delta t^2/s^2 a^2$. If $\text{ord}(s) = 0$, then $c \in 1 + \mathfrak{P}^\mu$. If $\text{ord}(s) > 0$, using the hypothesis on $\text{ord}(\delta)$, one sees that c belongs to $1 + \mathfrak{P}^{\lfloor \mu/2 \rfloor + 1}$ when $\mu \equiv 3 \pmod{4}$ and belongs to $1 + \mathfrak{P}^{\lfloor \mu/2 \rfloor}$ otherwise. Thus, $\theta(0^+(L))$ is contained in the respective sets as required. Conversely, if $c = 1 + t$ is a unit $\text{ord}(t)$ as specified in Lemma 4, then a routine computation shows that $\text{ord}(t\delta) > 2e$, and so Lemma 4 applies. The modification at $\mu \equiv 2 \pmod{4}$ is allowed by Remark (e).

Proof of Proposition E. If $(1 + \mathfrak{P}^{2e - \text{ord}(\delta)})F^2$ also were contained in $\theta(0^+(L))$, then for every unit $c = 1 + t$, $t \in \mathfrak{P}^{2e - \text{ord}(\delta)}$, we have the Hilbert symbol $(c, -d)_{\mathfrak{P}} = 1$ by Remark (c). But, as $\mathfrak{D}(-d) = \mathfrak{P}^{\text{ord}(\delta)}$, Lemma 3 asserts there is a unit f with defect $\mathfrak{P}^{2e - \text{ord}(\delta)}$ such that $(c, f)_{\mathfrak{P}} = -1$. This is impossible!

It now remains to show that if $c = 1 + t$, $t \in \mathfrak{P}^{2e - \text{ord}(\delta) + 1}$, then $cF^2 \in \theta(0^+(L))$. It is sufficient to show that the hypotheses for Lemma 4 is satisfied. $\text{Ord}(t\delta) \geq 2e - \text{ord}(\delta) + 1 - \text{ord}(\delta) > 2e$. Also, $\text{ord}(t) \geq 2e - \text{ord}(\delta) + 1 \geq 2e + 1 - e - \nu - [\mu/2] = \mu - [\mu/2] + 1 \geq [\mu/2] + 1$.

ACKNOWLEDGMENT. I would like to thank the referee for pointing out an error in the original draft of this paper.

REFERENCES

1. O. T. O'Meara, *Introduction to Quadratic Forms*, Berlin-Göttingen-Heidelberg: Springer, 1963.
2. O. T. O'Meara and B. Pollak, *Generation of local integral orthogonal groups. II*, *Math. Zeitschr.*, **93** (1966), 171-188.

Received April 11, 1974 and in revised form July 27, 1974.

OHIO STATE UNIVERSITY