

## SPINOR GENERA UNDER $\mathbf{Z}_p$ -EXTENSIONS

WAI-KIU CHAN

Let  $L$  be a quadratic lattice over a number field  $F$ . We lift the lattice  $L$  along a  $\mathbf{Z}_p$ -extension of  $F$  and investigate the growth of the number of spinor genera in the genus of  $L$ . Let  $L_n$  be the lattice obtained from  $L$  by extending scalars to the  $n$ -th layer of the  $\mathbf{Z}_p$ -extension. We show that, under various conditions on  $L$  and  $F$ , the number of spinor genera in the genus of  $L_n$  is  $2^{\eta p^n + O(1)}$  where  $\eta$  is some rational number depending on  $L$  and the  $\mathbf{Z}_p$ -extension. The work involves Iwasawa's theory of  $\mathbf{Z}_p$ -extensions and explicit calculation of spinor norm groups of local integral rotations.

### 1. Introduction.

The question of how the genus of a positive definite quadratic form over the rationals behaves when is lifted to a totally real number field was first raised by Ankeny in the sixties (see the introduction in [EH1]). The closely related problem of how the spinor genus behaves upon field extension was then investigated by Earnest and Hsia. In a series of papers [EH1-3], they showed that, modulo some restrictions on the bottom field, the (proper) spinor genera in the genus of the given lattice do not collapse when lifted to an odd degree extension. In particular, the number of spinor genera in the genus will not decrease in this situation. However, there was no quantitative description of the growth of the spinor genera. When the degree of extension is even, examples show that the spinor genera in a given genus may collapse. Constructive methods for determining the amount of collapsing in the case of quadratic extension of  $\mathbf{Q}$  were given in [EH3]. In this paper, we will consider the problem when the lattice is lifted along a  $\mathbf{Z}_p$ -extension. The result presented in this paper will describe the growth of the number of spinor genera asymptotically.

Our work is initiated by a paper of Estes and Hsia [EsH] in which they developed the theory of *spinor class fields*. Let  $f$  be a quadratic form over a number field  $F$ . Via class field theory, Estes and Hsia identify the group of spinor genera in the genus of  $f$  with the Galois group of an abelian extension  $\Sigma/F$ . The field  $\Sigma$  is called the spinor class field of  $f$ . The spinor class field enjoys properties which are similar to those borne by the Hilbert class field.

Powerful machineries had been developed to yield information on the Hilbert class fields and ideal class numbers. An important example is Iwasawa's work on ideal class numbers of fields inside a  $\mathbf{Z}_p$ -extension. He shows that the  $p$ -part of ideal class number of the  $n$ -th layer of a  $\mathbf{Z}_p$ -extension is  $p^{\mu p^n + \lambda n + \nu}$  when  $n$  is sufficiently large. Here  $\mu, \lambda, \nu$  are constants independent of  $n$ . In this paper, we would like to attack the base change problem mentioned in the last paragraph in Iwasawa's setting. More precisely, let  $f_n$  be the form obtained from  $f$  by extending scalars to the  $n$ -th layer of the  $\mathbf{Z}_p$ -extension. Let  $h_s(f_n)$  be the number of spinor genera in the genus of  $f_n$ . We try to seek a formula for  $h_s(f_n)$  which serves as an analog of Iwasawa's class number formula. The formula implies the following interesting result. Under some mild assumption (see the next paragraph)  $h_s(L_n)$  is either bounded or growing exponentially.

The rest of the paper is organized as follows. In Section 2 we will give some necessary background on quadratic forms and  $\mathbf{Z}_p$ -extensions. Since the number of spinor genera in a given genus is always a 2-power, we start our investigation on  $\mathbf{Z}_2$ -extensions. In Section 3 we will handle the case where the form has good reduction (see Definition 3.1) at the dyadic primes of  $F$ . In Section 4, we do not require the form to have good reduction. But we restrict ourselves on cyclotomic  $\mathbf{Z}_2$ -extension of totally real number fields or  $CM$  fields. The results of Section 4 rely heavily on the spinor norms of local integral rotations at the dyadic primes. Because of this, we will assume that 2 is unramified in the bottom field  $F$ . In Section 5, we will consider the problem when the  $\mathbf{Z}_p$ -extension is the cyclotomic one with  $p > 2$ . One of the main ingredients is Washington's theorem which asserts the boundedness of the  $l$ -part of the ideal class groups in a cyclotomic  $\mathbf{Z}_p$ -extension of abelian number field. In Section 6, we will carry out the calculations of the local spinor norms which is needed in Section 4.

## 2. Background Material.

This paper involves two areas of number theory. Namely, the arithmetic theory of quadratic forms and Iwasawa's theory of  $\mathbf{Z}_p$ -extensions. In order to keep the paper in a reasonable length, we will just provide background material on both areas which is necessary for later discussions. For further detail and any unexplained terminology, we refer the reader to O'Meara's book [OM] and Washington's book [Wa]. We also refer the reader to Iwasawa's original papers [I1-4] for more information on  $\mathbf{Z}_p$ -extensions.

From now on,  $F$  is always either a number field or the completion of a number field at one of its prime spot. In the later case, we will simply say that  $F$  is a local field. The ring of integers in  $F$  is denoted by  $\mathcal{O}_F$ . A

local field is called nondyadic if its residue class field has odd characteristic. Otherwise, it is called dyadic. A 2-adic local field is a dyadic local field in which 2 is unramified. If  $F$  is a dyadic local field, we fix a unit  $\rho_F$  (or simply  $\rho$ ) such that  $\Delta = 1 + 4\rho_F$  is a unit of quadratic defect  $4\mathcal{O}_F$ . If  $R$  is a ring, then  $R^\times$  always denotes the group of invertible elements in  $R$ .

Instead of working with quadratic forms, we will follow O’Meara [OM] to use the language of quadratic spaces and lattices. All spaces and lattices are assumed to be endowed with a non-degenerate quadratic form  $Q$ . Let  $L$  be a lattice on a quadratic space  $V$  over  $F$ . For any anisotropic vector  $v$  in  $V$ ,  $S_v$  will be the symmetry with respect to  $v$ . We put  $P(L)$  to be the set  $\{v \in V : S_v \in O(L)\}$ . The spinor norm map on  $O(V)$  is denoted by  $\theta$  and  $\theta(O^+(L))$  will be abbreviated as  $\theta_L$ . Every hyperbolic plane has a basis  $\{x, y\}$  such that both  $x$  and  $y$  are isotropic vectors and the inner product between them is 1. Such a basis is called a hyperbolic pair. As in [OM, 93B],  $A(\alpha, \beta)$  denotes a binary lattice which has  $\begin{pmatrix} \alpha & 1 \\ 1 & \beta \end{pmatrix}$  as an inner product matrix.

Suppose that  $F$  is a number field and  $\wp$  is a prime spot of  $F$ . Let  $J_F$  be the group of idèles of  $F$  and  $\Theta_L$  the subgroup  $\{(i_\wp) \in J_F : i_\wp \in \theta_{L_\wp} \text{ for all } \wp\}$ . We will assume throughout this paper that *the rank of  $L$  is at least three unless stated otherwise*. Under this assumption, the quotient group  $J_F/F^\times\Theta_L$  can be identified with the set of all (proper) spinor genera in  $gen(L)$  (see [EsH] and [Kn]). The spinor class field of  $L$  is the abelian extension  $\Sigma$  of  $F$  which corresponds to the open subgroup  $F^\times\Theta_L$  via class field theory. It follows directly that  $\Sigma/F$  is a multiquadratic extension and  $[\Sigma : F]$  is equal to  $h_s(L)$ , the number of spinor genera in  $gen(L)$ .

Let  $F$  be a number field. A  $\mathbf{Z}_p$ -extension of  $F$  is a Galois extension  $F_\infty/F$  such that  $\text{Gal}(F_\infty/F)$  is isomorphic to the additive group  $\mathbf{Z}_p$ . Let  $F_n$  be the fixed field of the closed subgroup  $p^n\mathbf{Z}_p$ . Then  $F_n \subseteq F_{n+1}$  and  $\text{Gal}(F_{n+1}/F_n)$  is cyclic of order  $p^n$ . It is also known that the ramified primes in  $F_\infty/F$  are lying above  $p$ . Let  $q = p$  or 4 if  $p = 2$ . Let  $\mathbb{B}_n$  be the unique real subfield of the cyclotomic field  $\mathbf{Q}(\zeta_{qp^n})$  of degree  $p^n$  over  $\mathbf{Q}$ . Then  $\mathbb{B}_\infty = \cup \mathbb{B}_n$  is a  $\mathbf{Z}_p$ -extension of  $\mathbf{Q}$ . The cyclotomic  $\mathbf{Z}_p$ -extension of  $F$  is the compositum  $F\mathbb{B}_\infty$ . In the cyclotomic  $\mathbf{Z}_p$ -extension, all primes lying above  $p$  are ramified and the corresponding inertia groups have finite index in  $\text{Gal}(F\mathbb{B}_\infty/F)$ . All other finite primes are finitely decomposed.

As is customary, we write  $\text{Gal}(F_\infty/F)$  multiplicatively and denote it by  $\Gamma$ . The subgroup  $\text{Gal}(F_\infty/F_n)$  is just  $\Gamma^{p^n}$  and we denote it by  $\Gamma_n$ . By a  $\Gamma$ -module we mean a  $p$ -primary abelian group on which  $\Gamma$  acts continuously. Let  $T$  be an indeterminate and  $\Lambda$  the power series ring  $\mathbf{Z}_p[[T]]$ . Let us fix a topological generator  $\gamma_0$  of  $\Gamma$ . For every compact  $\Gamma$ -module  $M$ , we can endow

it with a unique compact  $\Lambda$ -module structure such that  $(1+T)x = \gamma_0 x$  for every  $x \in M$ . Conversely, every compact  $\Lambda$ -module determines a compact  $\Gamma$ -module uniquely.

Given any  $\Lambda$ -modules  $M$  and  $N$ , we say that  $M$  is pseudo-isomorphic to  $N$ , written as  $M \sim N$ , if there is a  $\Lambda$ -module homomorphism  $M \rightarrow N$  with finite kernel and cokernel. A fundamental theorem of structure of  $\Lambda$ -modules says that if  $M$  is finitely generated, then  $M$  is pseudo-isomorphic to  $\Lambda^r \oplus \sum \Lambda/(p^{n_i}) \oplus \sum \Lambda/(f_j^{m_j})$  where  $r, t, n_i, m_j$  are non-negative integers and  $f_j$  is a so-called distinguished irreducible polynomial [Wa, Thm. 13.12]. If  $r = 0$ , then  $M$  is called  $\Lambda$ -torsion. Let  $\mu(M) = \sum n_i$  and  $\lambda(M) = \sum m_j \deg f_j$ . They are called the  $\mu$ -invariant and the  $\lambda$ -invariant of  $M$ . The ideals  $(p^{n_i})$  and  $(f_j^{m_j})$  are called the divisors of  $M$ . For each  $n \geq 0$ , let  $\omega_n = (1+T)^{p^n} - 1$  and  $\nu_{n,m} = \omega_n/\omega_m$ .

**Lemma 2.1** ([I1]). *Suppose that  $M$  is a finitely generated  $\Lambda$ -torsion module. If  $\nu_{n,t}$  is relatively prime to the divisors of  $M$  for any  $n \geq t$ , then  $[M : \nu_{n,t}M] = p^{\mu(M)p^n + \lambda(M)n + O(1)}$ . Same conclusion holds if we replace  $\nu_{n,t}$  by  $\omega_n$  provided that  $\omega_n$  is relatively prime to the divisors of  $M$ .*

**Proposition 2.1.** *Let  $F_\infty/F$  be a  $\mathbf{Z}_2$ -extension and  $K_\infty$  a Galois extension of  $F$  which contains  $F_\infty$ . Suppose  $\text{Gal}(K_\infty/F_\infty)$  is an elementary 2 group finitely generated as a  $\Lambda$ -module. Let  $K_n$  be the maximal elementary 2 extension of  $F_n$  inside  $K_\infty$ . Then there exists a non-negative integer  $\mu$  such that*

$$[K_n : F_n] = 2^{\mu 2^n + O(1)}.$$

*Proof.* Let  $G_n$  be the Galois group of  $K_\infty$  over  $F_n$ . Then,

$$\text{Gal}(K_n/F_n) = \frac{G_n}{\overline{[G_n, G_n]}G_n^2}$$

where  $\overline{[G_n, G_n]}$  is the closure of the commutator subgroup of  $G_n$ . Since  $\Gamma_n$  acts on  $\mathcal{X} := \text{Gal}(K_\infty/F_\infty)$  by conjugation and  $\omega_n \mathcal{X}$  is the smallest submodule of  $\mathcal{X}$  such that  $\Gamma_n$  acts trivially on the quotient,  $\overline{[G_n, G_n]}$  is just  $\omega_n \mathcal{X}$ . Therefore

$$\text{Gal}(K_n/F_n) = \frac{G_n}{\omega_n \mathcal{X} \cdot G_n^2}.$$

Since  $G_n/\mathcal{X} \cong \Gamma_n$ , the index  $[G_n : \mathcal{X} \cdot G_n^2]$  is 2. As  $[K_n : F_n] = [G_n : \mathcal{X}G_n^2] \cdot [\mathcal{X}G_n^2 : \omega_n \mathcal{X} \cdot G_n^2]$ , we have  $[K_n : F_n] = 2[\mathcal{X}G_n^2 : \omega_n \mathcal{X} \cdot G_n^2]$ .

The natural map  $\mathcal{X} \rightarrow \mathcal{X}G_n^2/\omega_n \mathcal{X} \cdot G_n^2$  is clearly surjective. The kernel is  $\mathcal{X} \cap (\omega_n \mathcal{X} \cdot G_n^2)$ . Take an element  $\omega_n x \cdot g^2$  in  $\mathcal{X} \cap (\omega_n \mathcal{X} \cdot G_n^2)$ . Then  $g^2$  is in  $\mathcal{X}$ . However, as  $G_n/\mathcal{X} \cong \Gamma_n$  is torsion free,  $g$  is already in  $\mathcal{X}$ . Therefore

$\omega_n x \cdot g^2 = \omega_n x \in \omega_n \mathcal{X}$  and hence  $\mathcal{X} \cap (\omega_n \mathcal{X} \cdot G_n^2) = \omega_n \mathcal{X}$ . It is clear that the divisors of  $\mathcal{X}$  are powers of the ideal (2) only. Therefore  $\omega_n$  is relatively prime to the divisors of  $\mathcal{X}$ . Let  $\mu$  be the  $\mu$ -invariant of  $\text{Gal}(K_\infty/F_\infty)$ . Then by Lemma 2.1,  $[K_n : F_n] = 2[\mathcal{X} : \omega_n \mathcal{X}] = 2^{\mu 2^n + O(1)}$ .  $\square$

Suppose now that  $F_\infty$  is the cyclotomic  $\mathbf{Z}_2$ -extension of  $F$ . Let  $H_\infty^*$  be the maximal abelian 2-extension of  $F_\infty$  which is unramified outside  $\infty$  and  $H_\infty$  the maximal unramified abelian 2-extension of  $F_\infty$ . The field  $H_\infty$  is a Galois extension of  $F$ . Therefore,  $\Gamma \cong \text{Gal}(F_\infty/F)$  acts on  $\text{Gal}(H_\infty/F_\infty)$  by conjugation. In this case,  $\text{Gal}(H_\infty/F_\infty)$  becomes a finitely generated  $\Lambda$ -module. Let  $\mu(F)$  be the  $\mu$ -invariant of this module. Similarly, we can define  $\mu(F^*)$  by using  $H_\infty^*$ . Obviously, if  $\mu(F^*) = 0$ , then  $\mu(F) = 0$ . Iwasawa conjectured them to be always zero. The full veracity of this conjecture is not yet established. However, it is settled by Ferrero and Washington [FW] when  $F$  is an abelian extension of  $\mathbf{Q}$  (see [Si] for another proof by Sinnott). There are nonabelian extensions  $F/\mathbf{Q}$  such that  $\mu(F) = 0$ . For example, Kida [Ki] proves that if  $F$  is totally real and  $[F : \mathbf{Q}]$  is a 2-power, then  $\mu(F) = \mu(F^*) = 0$ .

Let  $X$  be a finite set of primes of  $F$  containing all the infinite primes. Let  $\mathcal{I}_n^X$  (resp.  $\mathcal{I}_n^{X*}$ ) be the subgroup of the  $X$ -ideal class group (resp. the narrow  $X$ -ideal class group) of  $F_n$  generated by the order 2 elements.

**Corollary 2.1.** *If  $\mu(F^*) = 0$ , then  $|\mathcal{I}_n^X|$  and  $|\mathcal{I}_n^{X*}|$  are bounded as  $n$  tends to infinity.*

*Proof.* By class field theory,  $|\mathcal{I}_n^X| = [H_n^X : F_n]$  where  $H_n^X$  is the maximal unramified elementary 2-extension of  $F_n$  in which all finite primes in  $X$  split completely. Then  $H_n^X \subseteq H_n =$  maximal unramified elementary 2-extension of  $F_n$ . By Proposition 2.1,  $[H_n : F_n]$  is bounded and hence  $[H_n^X : F_n]$  is also bounded. Similarly for  $|\mathcal{I}_n^{X*}|$ .  $\square$

**Proposition 2.2.** *Let  $M_n$  be the maximal elementary 2-extension of  $F_n$  which is unramified outside  $2 \cup \infty$ . If  $\mu(F^*) = 0$ , then  $[M_n : F_n] = 2^{(r_1+r_2)2^n + O(1)}$  where  $r_1$  (resp.  $r_2$ ) is the number of real (resp. complex) primes of  $F$ .*

*Proof.* Let  $T$  be the set of all dyadic and infinite primes of  $F$ . Let  $\mathcal{M}$  be the subgroup of  $F_n^\times/F_n^{\times 2}$  which corresponds to  $M_n$  via Kummer's theory. If  $a \in F_n^\times$  represents an element in  $\mathcal{M}$ , then  $\langle a \rangle = B^2A$  where  $B$  is an ideal prime to  $T$  and  $A$  is supported on  $T$ . Thus we have a surjective homomorphism

$$\begin{aligned} \mathcal{M} &\longrightarrow \mathcal{I}_n^T \\ a &\longmapsto B. \end{aligned}$$

The kernel of the above map is  $E_n/E_n^2$  where  $E_n$  is the  $T$ -units of  $F_n$ . Since all the dyadic primes of  $F$  is totally ramified in  $F_\infty$ , the number of dyadic primes in  $F_n$  is eventually constant. Together with Dirichlet's theorem, we have  $|E_n/E_n^2| = 2^{(r_1+r_2)2^n+O(1)}$ . The proposition now follows by virtue of Corollary 2.1.  $\square$

**Proposition 2.3.** *Suppose  $F$  is totally real. Let  $N_n$  be the maximal elementary 2-extension of  $F_n$  which is unramified outside 2. If  $\mu(F^*) = 0$ , then  $[N_n : F_n]$  is bounded as  $n$  tends to infinity.*

*Proof.* Let  $\mathcal{N}$  be the subgroup of  $F_n^\times/F_n^{\times 2}$  corresponding to  $N_n$ . Like Proposition 2.2, we have an exact sequence

$$1 \longrightarrow E_n^+/E_n^2 \longrightarrow \mathcal{N} \longrightarrow \mathcal{I}_n^{T^*} \longrightarrow 1$$

where  $E_n^+$  contains those  $T$ -units which are positive at the real primes. Let  $P_n$  be the principle ideals of the  $T$ -integers of  $F_n$  and  $P_n^+$  be the subgroup containing principle ideals generated by elements which are positive at all real primes. Then

$$F_n^\times/F_n^{\times+} E_n \cong P_n/P_n^+$$

where  $F_n^{\times+}$  is the set of elements in  $F_n^\times$  which are positive at all real primes. On the other hand, by weak approximation, we have

$$|F_n^\times/F_n^{\times+}| = 2^{d2^n}$$

where  $d = [F : \mathbf{Q}]$ . This shows that  $|P_n/P_n^+| \cdot [E_n : E_n^+] = 2^{d2^n}$ .

Now,  $|P_n/P_n^+|$  is a subgroup of  $\mathcal{I}_n^{T^*}$ . Since  $\mu(F^*) = 0$ ,  $|\mathcal{I}_n^{T^*}|$  is bounded as  $n \rightarrow \infty$  and hence  $|P_n/P_n^+|$  is also bounded. Therefore,  $[E_n : E_n^+] = 2^{d2^n+O(1)}$ . From the proof of Proposition 2.2, we see that  $[E_n : E_n^2] = 2^{d2^n+O(1)}$ . Consequently,  $[E_n^+ : E_n^2] = O(1)$  and we are done.  $\square$

### 3. Lattice with Good Reduction.

Let  $F_\infty/F$  be an arbitrary  $\mathbf{Z}_2$ -extension. For each  $n$ , we let  $\mathcal{O}_n$  be the ring of integers of  $F_n$ . Let  $L$  be a lattice on a quadratic space  $V$  over  $F$ . The "lifted" lattice  $L \otimes \mathcal{O}_n$  is denoted by  $L_n$ . If  $\mathfrak{P}$  is a prime of  $F_n$ , we use  $\theta_{n\mathfrak{P}}$  instead of  $\theta_{L_n\mathfrak{P}}$  for the sake of brevity.

**Definition 3.1.** *Let  $\wp$  be a dyadic prime of  $F$ .*

(I) *A lattice  $L$  has Type I reduction at  $\wp$  if a Jordan splitting of  $L_\wp$  has a component of rank  $\geq 3$  or a binary component which is isometric to  $\pi^r A(0, 0)$  of  $\pi^r A(2, 2\rho)$  where  $\pi$  is a prime element in  $F_\wp$ .*

(II) A lattice  $L$  has Type II reduction at  $\wp$  if  $L_\wp \cong \langle a_1 \rangle \perp \cdots \perp \langle a_m \rangle$  and  $\text{ord}_\wp(a_{i+1}) - \text{ord}_\wp(a_i) \geq 4e$  for all  $i$  where  $e$  is the absolute ramification index of  $\wp$ .

The lattice  $L$  has good reduction at  $\wp$  if it has either Type I or Type II reduction at  $\wp$ .

It is clear that if  $L$  has Type I reduction at  $\wp$ , then  $L_n$  also has Type I reduction at all  $\mathfrak{P}|\wp$ . By [OM, 93:20] and [H, Lemma 1], we know that  $\theta_{n\mathfrak{P}}$  contains all units of  $\mathcal{O}_{n\mathfrak{P}}$ . We recall that  $P(L)$  is the set of vectors in  $V$  which give rise to symmetries in  $O(L)$ .

**Lemma 3.1.** *If  $L$  has Type II reduction at  $\wp$ , then for any prime divisor  $\mathfrak{P}$  of  $\wp$  in  $F_n$ , the index  $[\theta_{n\mathfrak{P}} : F_{n\mathfrak{P}}^{\times 2}]$  is bounded as  $n$  tends to infinity.*

*Proof.* Suppose  $L_\wp \cong \langle a_1 \rangle \perp \cdots \perp \langle a_m \rangle$ . For simplicity, let  $L_{nj} = \langle a_j \rangle \perp \langle a_{j+1} \rangle$ . If  $\text{ord}_\wp(a_{j+1}) - \text{ord}_\wp(a_j) > 4e$ , then by [EsH, Prop. 1]  $\theta_{n\mathfrak{P}}$  is the subgroup generated by  $a_i a_j F_{n\mathfrak{P}}^{\times 2}$ . Therefore,  $[\theta_{L_{nj}} : F_{n\mathfrak{P}}^{\times 2}] \leq 2^{m(m-1)/2}$ , which is independent of  $n$ .

Now suppose  $\min\{\text{ord}_\wp(a_{j+1}) - \text{ord}_\wp(a_j)\} = 4e$ . For each  $i = 1, \dots, m$ , let  $a_i = \pi^i \epsilon_i$  where  $\epsilon_i \in \mathcal{O}_{F_\wp}^\times$ . By the corollary to Lemma 1 in [EsH], we know that  $O(L_{n\mathfrak{P}})$  is generated by symmetries and Eichler transformations. Also,  $L_{n\mathfrak{P}}$  is not of  $E$  type (see [EH2]). Therefore,  $\theta_{n\mathfrak{P}}$  contains precisely all the even products of  $Q(v)$  where  $v \in P(L_{ni})$  for all  $1 \leq i \leq m - 1$ . We suffice to show that  $Q(P(L_{ni}))$  contains at most four cosets of  $F_{n\mathfrak{P}}^{\times 2}$  in  $F_{n\mathfrak{P}}^\times$  for each  $i$ .

If  $r_{i+1} - r_i > 4e$ , then by [Xu, Prop. 2.1], it is easy to see that  $Q(P(L_{ni}))$  contains at most two cosets. If  $r_{j+1} - r_j = 4e$ , then [Xu, Prop. 2.2 (iii)] implies that  $Q(P(L_{ni}))$  contains at most four cosets. The lemma is now proved.  $\square$

**Theorem 3.1.** *Suppose that the lattice  $L$  has good reduction at all dyadic primes of  $F$  which do not split completely in  $F_\infty$ . Then there exists a non-negative constant  $\mu$  such that  $h_s(L_n) = 2^{\mu 2^n + O(1)}$ .*

*Proof.* Let  $v(L)$  be the volume of the lattice  $L$ . We define five finite subsets of primes of  $F$  as follows:

- $D^r$  = set of all dyadic primes which are ramified in  $F_\infty$
- $D^s$  = set of all dyadic primes which split completely in  $F_\infty$
- $D^d$  = set of all dyadic primes which are finitely decomposed in  $F_\infty$
- $S$  = set of all nondyadic primes which divide  $v(L)$  and split completely in  $F_\infty$
- $T = S \cup D^r \cup D^s \cup D^d \cup \infty$ .

For any set of primes  $X$  of  $F$ ,  $X_n$  denotes the set containing primes of  $F_n$  which lie above some elements in  $X$ . We first make some modification on the local components of  $\Theta_{L_n}$ .

At  $\wp \notin T$ : This  $\wp$  must be non-dyadic. If  $\wp$  does not divide  $v(L)$ , then  $\theta_{n\mathcal{P}} = \mathcal{O}_{n\mathcal{P}}^\times F_{n\mathcal{P}}^{\times 2}$  for any  $\mathcal{P}|\wp$ . If  $\wp|v(L)$ , then  $\wp$  is finitely decomposed in  $F_\infty$ . Therefore, for large enough  $n$ , the number of primes in  $F_n$  dividing  $\wp$  is constant. Therefore, changing  $\theta_{n\mathcal{P}}$  to  $\mathcal{O}_{n\mathcal{P}}^\times F_{n\mathcal{P}}^{\times 2}$  at these  $\mathcal{P}$  will only cause a bounded effect on  $h_s(L_n)$ . Consequently, we may assume that

$$\theta_{n\mathcal{P}} = \mathcal{O}_{n\mathcal{P}}^\times F_{n\mathcal{P}}^{\times 2} \quad \forall \mathcal{P} \notin T_n.$$

At  $\wp \in D^r \cup D^d$ : If  $L$  has Type I reduction at  $\wp$ , then  $[F_{n\mathcal{P}}^\times : \theta_{n\mathcal{P}}] \leq 2$ . If  $L$  has Type II reduction at  $\wp$ , then  $[\theta_{n\mathcal{P}} : F_{n\mathcal{P}}^{\times 2}]$  is bounded as  $n$  tends to infinity. Any  $\wp$  in this case is either ramified or finitely decomposed. Therefore  $|D_n^r \cup D_n^d|$  is eventually constant and so we may assume for any  $\mathcal{P} \in D_n^r \cup D_n^d$ ,

$$\theta_{n\mathcal{P}} = \begin{cases} \mathcal{O}_{n\mathcal{P}}^\times F_{n\mathcal{P}}^{\times 2} & \text{if } L \text{ has Type I reduction at } \wp \\ F_{n\mathcal{P}}^{\times 2} & \text{if } L \text{ has Type II reduction at } \wp. \end{cases}$$

Now, let  $\Sigma_n$  be the spinor class field of  $L_n$  and  $\mathbb{N}_n$  the norm from  $F_n$  to  $F_{n-1}$ . After we modified  $\Theta_{L_n}$ , we have  $\mathbb{N}_{n+1}(\Theta_{L_{n+1}}) \subseteq \Theta_{L_n}$  and hence  $\Sigma_n \subseteq \Sigma_{n+1}$ . Let  $\Sigma_\infty$  be the union of the  $\Sigma_n$ 's. It is not hard to see that  $\Sigma_\infty$  is a Galois extension of  $F$ . Therefore,  $\text{Gal}(\Sigma_\infty/F_\infty)$  is a  $\Lambda$ -module. As  $\Sigma_\infty/F_\infty$  is unramified outside  $T$ ,  $\text{Gal}(\Sigma_\infty/F_\infty)$  is a finitely generated  $\Lambda$ -module (see [Wa] or [I4]).

Let us first assume that  $L$  has Type II reduction at all  $\wp \in D^r$ . We claim that  $\Sigma_n$  is the maximal elementary 2-extension of  $F_n$  inside  $\Sigma_\infty$ . Let  $M_n$  be the maximal elementary 2-extension of  $F_n$  inside  $\Sigma_\infty$ . Then  $\Sigma_n \subseteq M_n$ . If we let  $\mathcal{V}_n$  be the open subgroup in  $J_{F_n}$  corresponding to  $M_n$  via class field theory, then obviously  $F_n^\times \Theta_{L_n} \supseteq \mathcal{V}_n$  and  $F_{n\mathcal{P}}^{\times 2} \subseteq \mathcal{V}_n$  for all  $\mathcal{P}$ . By the modification we made on  $\Theta_{L_n}$ , we know that  $\Sigma_\infty/F$  is unramified outside  $T$ . Therefore  $M_n/F_n$  is unramified outside  $T$  and so

$$\mathcal{O}_{n\mathcal{P}}^\times F_{n\mathcal{P}}^{\times 2} \subseteq \mathcal{V}_n \quad \forall \mathcal{P} \notin T_n.$$

Suppose  $\wp \in D^d$ . If  $L$  has Type II reduction at  $\wp$ , then  $\theta_{n\mathcal{P}} = F_{n\mathcal{P}}^{\times 2} \subseteq \mathcal{V}_n$ . If  $L$  has Type I reduction at  $\wp$ , then  $\theta_{n\mathcal{P}} = \mathcal{O}_{n\mathcal{P}}^\times F_{n\mathcal{P}}^{\times 2}$ . This implies that  $\Sigma_n/F_n$  is unramified at  $\mathcal{P}$ . Since  $F_n/F$  is unramified at  $\wp$ , therefore  $\Sigma_n/F$  is unramified at  $\wp$  and hence so is  $\Sigma_\infty/F$ . Consequently,  $M_n/F_n$  is unramified at  $\mathcal{P}$  and we have

$$\theta_{n\mathcal{P}} = \mathcal{O}_{n\mathcal{P}}^\times F_{n\mathcal{P}}^{\times 2} \subseteq \mathcal{V}_n \quad \forall \mathcal{P} \in D_n^d.$$



Take a sufficiently large integer  $t$  such that  $M_n \subseteq \Sigma_t$ . Then  $M_n F_t \subseteq \Sigma_t$ . This implies that  $\mathbb{N}_{F_t/F_n}(\Theta_{L_t}) \subseteq \mathcal{V}_n$  and

$$\theta_{n\mathcal{P}} \subseteq \mathbb{N}_{F_t/F_n}(\Theta_{L_t}) \subseteq \mathcal{V}_n \quad \forall \mathcal{P} \in D_n^r \cup S_n.$$

Certainly, since  $L$  has Type II reduction at  $\wp \in D^r$ , we also have

$$\theta_{n\mathcal{P}} \subseteq \mathcal{V}_n \quad \forall \mathcal{P} \in D_n^r.$$

It is easy to see that  $\theta_{n\mathcal{P}} = \theta_\wp$  if  $\mathcal{P}|\wp \in \infty$ . Combining everything together, we have  $F_n^\times \Theta_{L_n} \subseteq \mathcal{V}_n$  and hence  $M_n = \Sigma_n$ .

For any  $\sigma \in \text{Gal}(\Sigma_\infty/F_\infty)$  and for any  $n$ ,  $\sigma|_{\Sigma_n} \in \text{Gal}(\Sigma_n/F_\infty \cap \Sigma_n) \subseteq \text{Gal}(\Sigma_n/F_n)$ . Therefore,  $\sigma$  has order 2 and the  $\Lambda$ -module  $\text{Gal}(\Sigma_\infty/F_\infty)$  is pseudo-isomorphic to a direct sum of copies of  $\Lambda/(2)$ . Let  $\mu$  be the  $\mu$ -invariant of  $\text{Gal}(\Sigma_\infty/F_\infty)$ . By Proposition 2.1, we can conclude that  $h_s(L_n) = [\Sigma_n : F_n] = 2^{\mu 2^n + O(1)}$ .

Now, let us assume that  $L$  has Type I reduction at  $P = \{\wp_1, \dots, \wp_r\} \subseteq D^r$ . In this case, we can use a similar argument as before to show that  $\Sigma_n$  is the maximal elementary 2-extension of  $F_n$  inside  $\Sigma_\infty$  which is unramified at all primes in  $P_n$ . The proof now resembles that of Theorem 13.13 in [Wa]. We first assume that all primes in  $D^r$  are totally ramified in  $F_\infty$ . For each  $i = 1, \dots, r$ , let  $\tilde{\wp}_i$  be a prime of  $\Sigma_\infty$  lying over  $\wp_i$ . Let  $I_i$  be the inertia group of  $\tilde{\wp}_i$ . Furthermore, we let  $G = \text{Gal}(\Sigma_\infty/F)$  and  $\mathcal{X} = \text{Gal}(\Sigma_\infty/F_\infty)$ . Then, by our assumption, it is true that  $I_i \cap \mathcal{X} = \emptyset$  and  $G = I_i \mathcal{X} = \mathcal{X} I_i$  for any  $i = 1, \dots, r$ .

Let  $\gamma_0$  be the fixed topological generator of  $\Gamma \cong G/\mathcal{X}$  and let  $\sigma_i \in I_i$  map to  $\sigma_0$  under the natural surjection. Since  $I_i \subseteq \mathcal{X} I_1$ , we can find  $a_i \in \mathcal{X}$  such that  $\sigma_i = a_i \sigma_1$ . Let  $\mathcal{Y}$  be the closed subgroup of  $\mathcal{X}$  generated by  $\{a_2, \dots, a_r\}$  and  $\omega_0 \mathcal{X}$ . Then for any  $n \geq 0$ , one can show that  $\text{Gal}(\Sigma_n/F_n) \cong \mathcal{X}/\mathcal{Y}_n$  where  $\mathcal{Y}_n = \nu_{n,0} \mathcal{Y}$ .

The final step is to remove the assumption that  $F_\infty/F$  is totally ramified at all ramified primes. Let  $t$  be a sufficiently large integer such that all ramified primes in  $F_\infty/F_t$  are totally ramified. Then  $\text{Gal}(\Sigma_n/F_n) \cong \mathcal{X}/\nu_{n,t} \mathcal{Y}_t$  for all  $n \geq t$ . Since  $\mathcal{X}$  and  $\mathcal{Y}_t$  are pseudo-isomorphic, they have the same  $\mu$ -invariant. Let it be  $\mu$ . Then for  $n \geq t$ ,  $h_s(L_n) = |\text{Gal}(\Sigma_n/F_n)| = [\mathcal{X} : \mathcal{Y}_t][\mathcal{Y}_t : \nu_{n,t} \mathcal{Y}_t] = 2^{\mu 2^n + O(1)}$ .  $\square$

#### 4. Cyclotomic $\mathbf{Z}_2$ -Extensions.

In this section, we assume that  $F_\infty/F$  is the cyclotomic  $\mathbf{Z}_2$ -extension and 2 is unramified in  $F$ . For any  $n \geq 1$ ,  $F_n \supseteq \mathbb{B}_n \supseteq \mathbb{B}_1 = \mathbf{Q}(\sqrt{2})$ . Therefore 2 is a square in  $F_n$ . We keep all the notations used in the last section.

We now make some adjustments on the local components of  $\Theta_{L_n}$ . Any nondyadic prime in  $F$  is finitely decomposed in  $F_\infty$ . Therefore the number of prime divisors of  $v(L_n)$  is eventually constant. As a result, we may assume that

$$\theta_{n\mathcal{P}} = \mathcal{O}_{n\mathcal{P}}^\times F_{n\mathcal{P}}^{\times 2}$$

for any nondyadic prime divisor  $\mathcal{P}$  of  $v(L_n)$ . For each  $n$ , the extension  $\Sigma_n/F_n$  is now unramified outside  $2 \cup \infty$ . Let  $M_n$  be the maximal elementary 2-extension of  $F_n$  which is unramified outside  $2 \cup \infty$ . Then  $\Sigma_n \subseteq M_n$ .

**Definition 4.1.** *A lattice  $L$  is called totally indefinite if it is indefinite at all infinite primes of  $F$ .*

**Theorem 4.1.** *Suppose that  $F$  is totally real. If  $\mu(F^*) = 0$  and  $L$  is totally indefinite, then  $h_s(L_n)$  is bounded.*

*Proof.* If  $L$  is totally indefinite, then  $L_n$  is also totally indefinite for all  $n$ . Therefore,  $\theta_{n\mathcal{P}} = F_{n\mathcal{P}}^\times$  for all infinite primes  $\mathcal{P}$ . (Note that all the infinite primes of  $F_n$  are real since infinite primes are not ramified in  $F_\infty$ .) By class field theory and our adjustments on  $\theta_{n\mathcal{P}}$ , the extension  $\Sigma_n/F_n$  is unramified outside 2. In particular,  $\Sigma_n \subseteq N_n =$  the maximal real subfield of  $M_n$ . By Proposition 2.3, we know that  $[N_n : F_n]$  is bounded and hence so is  $h_s(L_n)$ . □

We now present a result on spinor norms of local integral rotations. The proof will be given in Section 6.

**Theorem 4.2.** *Suppose that  $L$  is a lattice on a quadratic space over a 2-adic local field  $F$ . Let  $K/F$  be a totally ramified cyclic extension of degree  $2^n$ ,  $n \geq 4$  and  $\tilde{L}$  the lifted lattice  $L \otimes \mathcal{O}_K$ . Put  $e = 2^n$  to be the ramification index of  $K/F$ . Then:*

- (I) *If a Jordan splitting of  $L$  has a component of rank  $\geq 3$ , then  $\theta_{\tilde{L}} = \mathcal{O}_K^\times K^{\times 2}$ .*
- (II) *Suppose that a Jordan splitting of  $L$  has a component of rank  $\leq 2$  and at least one of them is binary.*
  - (II.1) *If all the components of the Jordan splitting are isometric to  $2^r A(0, 0)$  or  $2^r A(2, 2\rho_F)$ , then  $\theta_{\tilde{L}} = \mathcal{O}_K^\times K^{\times 2}$ .*
  - (II.2) *Assume that 2 is a square in  $K$ . If all the components are of the form  $2^r \epsilon(\langle 1 \rangle \perp \langle \delta \rangle)$  where  $\delta, \epsilon \in \mathcal{O}_F^\times$ , then  $\theta_{\tilde{L}} = (1 + \mathcal{P}^{\frac{e}{2}})K^{\times 2}$ .*
- (III) *Assume that 2 is a square in  $K$  and all the components of a Jordan splitting of  $L$  are of rank 1. In this case, we may assume that  $L \cong \langle 1 \rangle \perp \langle 2^{r_2} \epsilon_2 \rangle \perp \cdots \perp \langle 2^{r_m} \epsilon_m \rangle$  where  $0 = r_1 < r_2 < \cdots < r_m$  and all  $\epsilon_i \in \mathcal{O}_F^\times$ . Then*

$$\theta_{\bar{L}} = \begin{cases} (1 + \mathfrak{P}^{\frac{3e}{4}})K^{\times 2} & \text{if } \min\{r_{i+1} - r_i\} = 1 \quad (\text{III.1}) \\ (1 + \mathfrak{P}^e)K^{\times 2} & \text{if } \min\{r_{i+1} - r_i\} = 2 \quad (\text{III.2}) \\ (1 + \mathfrak{P}^{\frac{3e}{2}})K^{\times 2} & \text{if } \min\{r_{i+1} - r_i\} = 3 \quad (\text{III.3}) \\ \text{subgroup inside } (1 + \mathfrak{P}^{2e-1})K^{\times 2} & \text{if } \min\{r_{i+1} - r_i\} \geq 4 \quad (\text{III.4}). \end{cases}$$

Let  $\varphi$  be a dyadic prime of  $F$ . We define a rational number  $\eta_\varphi$  as follows:

$$\eta_\varphi = \begin{cases} 0 & \text{if } L_\varphi \text{ is in Case (I) or Case (II.1)} \\ \frac{1}{4} & \text{if } L_\varphi \text{ is in Case (II.2)} \\ \frac{3}{8} & \text{if } L_\varphi \text{ is in Case (III.1)} \\ \frac{1}{2} & \text{if } L_\varphi \text{ is in Case (III.2)} \\ \frac{3}{4} & \text{if } L_\varphi \text{ is in Case (III.3)} \\ 1 & \text{if } L_\varphi \text{ is in Case (III.4)}. \end{cases}$$

Let  $f_\varphi$  be the absolute residue degree of  $\varphi$ . Put

$$\eta = \sum_{\varphi|2} \eta_\varphi f_\varphi.$$

If  $L_\varphi$  is in Case (III.4), then  $[\theta_{n\mathfrak{P}} : F_{n\mathfrak{P}}^{\times 2}] \leq 2^{f_\varphi+1}$  which is independent of  $n$ . Therefore, we can assume that for all  $\mathfrak{P}|\varphi$ ,

$$\theta_{n\mathfrak{P}} = F_{n\mathfrak{P}}^{\times 2} \quad \text{if } L_\varphi \text{ is in Case (III.4).}$$

**Lemma 4.1.** *Let  $F$  be a finite extension of  $\mathbf{Q}_2$  and  $\varphi$  the prime ideal of  $\mathcal{O}_F$ . Let  $e$  and  $f$  be the ramification index and the residue degree of  $\varphi$  respectively. Then for any even integer  $i$  satisfying  $0 \leq i \leq 2e - 2$ , we have*

$$[(1 + \varphi^i)F^{\times 2} : (1 + \varphi^{i+2})F^{\times 2}] = 2^f.$$

*Proof.* For any  $i$  between 0 and  $2e - 2$ ,  $(1 + \varphi^i)F^{\times 2} = (1 + \varphi^{i+1})F^{\times 2}$ . Therefore, if  $0 \leq i \leq 2e - 4$ ,

$$\frac{(1 + \varphi^i)F^{\times 2}}{(1 + \varphi^{i+2})F^{\times 2}} \cong \frac{(1 + \varphi^{i+1})F^{\times 2}}{(1 + \varphi^{i+2})F^{\times 2}} \cong \frac{1 + \varphi^{i+1}}{1 + \varphi^{i+2}}.$$

The proof is now finished because  $(1 + \varphi^a)/(1 + \varphi^{a+1})$  has order  $2^f$  for all positive integer  $a$ . □

**Theorem 4.3.** *Suppose that  $F$  is totally real and  $L$  is positive definite. If  $\mu(F^*) = 0$ , then  $h_s(L_n) = 2^{n^2 + O(1)}$ .*

*Proof.* Let  $H_n$  (resp.  $H_n^*$ ) be the maximal unramified (resp. unramified outside  $\infty$ ) elementary 2-extension of  $F_n$ . By the hypothesis, we know that for all  $n$ ,

$$F_n \subseteq H_n^* \subseteq \Sigma_n \subseteq M_n.$$

Using Lemma 4.1 and the fact that the number of dyadic primes in  $F_n$  is constant, we can see that

$$\begin{aligned} [\Sigma_n : H_n^*] &\leq 2^{\eta 2^n} \\ [M_n : \Sigma_n] &\leq 2^{\sum_{\varphi|2} (1-\eta_{\varphi}) f_{\varphi} 2^n + O(1)}. \end{aligned}$$

Let  $d$  be the degree  $[F : \mathbf{Q}]$ . Since  $d = \sum_{\varphi|2} f_{\varphi}$ , therefore,  $[M_n : \Sigma_n] \leq 2^{(d-\eta)2^n + O(1)}$ . The index  $[H_n^* : F_n]$  is bounded as  $\mu(F^*) = 0$ . As a result,

$$\begin{aligned} [M_n : F_n] &= [M_n : \Sigma_n][\Sigma_n : H_n^*][H_n^* : F_n] \\ &\leq 2^{(d-\eta)2^n + O(1)} \cdot 2^{\eta 2^n} \cdot 2^{O(1)} \\ &= 2^{d2^n + O(1)}. \end{aligned}$$

However, Proposition 2.2 says that  $[M_n : F_n] = 2^{d2^n + O(1)}$ . Therefore, we must have  $h_s(L_n) = [\Sigma_n : F_n] = 2^{\eta 2^n + O(1)}$ .  $\square$

Since the theory of  $\mathbf{Z}$ -lattice is of particular interest, we specialize the previous results to the case  $F = \mathbf{Q}$  in the following theorem.

**Theorem 4.4.** *If  $F = \mathbf{Q}$ , then*

- (1) *If  $L$  is indefinite, then  $h_s(L_n)$  is bounded.*
- (2) *If  $L$  is definite, then  $h_s(L_n)$  is bounded if  $L_2$  is in Case (I) or (II.1) and*

$$h_s(L_n) = \begin{cases} 2^{2^{n-2} + O(1)} & \text{if } L_2 \text{ is in Case (II.2)} \\ 2^{3 \cdot 2^{n-3} + O(1)} & \text{if } L_2 \text{ is in Case (III.1)} \\ 2^{2^{n-1} + O(1)} & \text{if } L_2 \text{ is in Case (III.2)} \\ 2^{3 \cdot 2^{n-2} + O(1)} & \text{if } L_2 \text{ is in Case (III.3)} \\ 2^{2^n + O(1)} & \text{if } L_2 \text{ is in Case (III.4)}. \end{cases}$$

We next turn our attention to the case when  $F$  is a  $CM$  field. For each  $n$ , let the maximal real subfield of  $F_n$  be  $E_n$ . Put  $E_{\infty} = \cup E_n$ . It is easy to see that

**Lemma 4.2.**  *$E_{\infty}/E$  is a cyclotomic  $\mathbf{Z}_2$ -extension.*

Let  $\delta_n$  be the discriminant of the field extension  $F_n/E_n$ . By calculating the ramification indices, we can see that the prime divisors of  $\delta_n$  are lying over the prime divisors of the discriminant of  $F/E$ . Since no finite primes in  $E$  split completely in  $E_\infty$ . So we have proved:

**Lemma 4.3.**

- (1) *The prime divisors of  $\delta_n$  are all nondyadic.*
- (2) *The number of distinct prime divisors of  $\delta_n$  is eventually constant.*

Let  $\hat{\wp}$  be a dyadic prime of  $E$ . Define

$$\tau_{\hat{\wp}} = \min\{\eta_{\wp} : \wp \text{ dyadic prime in } F \text{ and } \wp|\hat{\wp}\}$$

where  $\eta_{\wp}$  is defined as before. Let  $f_{\hat{\wp}}$  be the absolute residue degree of  $\hat{\wp}$ . Let

$$\tau = \sum_{\hat{\wp}|2} \tau_{\hat{\wp}} f_{\hat{\wp}}.$$

Let  $J_n$  be the idèle group of  $E_n$ . Via class field theory, we define an elementary 2-extension  $\Omega_n/E_n$  which corresponds to

$$\mathcal{W}_n = E_n^\times \prod_{\hat{\wp}|\infty}^* E_n^{\times 2} \prod_{\hat{\wp} \nmid 2}^* \mathcal{O}_{n\hat{\wp}}^\times E_{n\hat{\wp}}^{\times 2} \prod_{\hat{\wp}|\hat{\wp}}^* \left(1 + \hat{\wp}^{\tau_{\hat{\wp}} 2^{n+1}}\right) E_{n\hat{\wp}}^{\times 2} \subseteq J_n.$$

Here  $\prod^*$  is the restricted product in  $J_n$ .

**Lemma 4.4.** *For any  $n$ ,  $\Sigma_n$  contains  $\Omega_n$ .*

*Proof.* It suffices to show that for each dyadic prime  $\hat{\wp}$  of  $E_n$ , we have

$$\prod_{\mathcal{P}|\hat{\wp}} \mathbb{N}_{F_n\mathcal{P}/E_n\hat{\wp}}(\alpha_{\mathcal{P}}) \in \left(1 + \hat{\wp}^{\tau_{\hat{\wp}} 2^{n+1}}\right)$$

where  $\alpha_{\hat{\wp}} \in (1 + \hat{\wp}^{\eta_{\wp} 2^{n+1}})$ . This is true because  $F_n/E_n$  is unramified at all dyadic primes and hence  $\mathbb{N}_{F_n\mathcal{P}/E_n\hat{\wp}}(1 + \hat{\wp}^a) = (1 + \hat{\wp}^a)$  for any  $a \geq 0$ . The assertion is now clear because  $\tau_{\hat{\wp}} = \min\{\eta_{\wp} : \wp|\hat{\wp}\}$ . □

Let  $M_{E_n}$  (resp.  $M_{F_n}$ ) be the maximal elementary 2-extension of  $E_n$  (resp.  $F_n$ ) which is unramified outside  $2 \cup \infty$ . Obviously,  $\Omega_n \subseteq M_{E_n} \cap \Sigma_n$ .

**Lemma 4.5.** *The degree  $[M_{E_n} \cap \Sigma_n : \Omega_n]$  is bounded as  $n$  tends to infinity.*

*Proof.* Let  $\mathcal{V}_n$  be the subgroup of the idèle group of  $F_n$  which corresponds to the extension  $\Sigma_n/F_n$ . It suffices to show that the index  $[\mathcal{W}_n : E_n^\times \mathbb{N}_{F_n/E_n}(\mathcal{V}_n)]$  is bounded. It is clear that  $E_n^\times \mathbb{N}_{F_n/E_n}(\mathcal{V}_n)$  contains the subgroup

$$E_n^\times \prod_{\hat{\rho} \in \infty}^* E_n^{\times 2} \prod_{\hat{\rho} \mid 2\delta_n}^* \mathcal{O}_{n\hat{\rho}}^\times E_n^{\times 2} \prod_{\hat{\rho} \mid \delta_n}^* E_n^{\times 2} \prod_{\hat{\rho} \mid \hat{\wp}}^* \left(1 + \hat{\rho}^{\tau_{\hat{\wp}} 2^{n+1}}\right) E_n^{\times 2}.$$

Therefore,  $[\mathcal{W}_n : E_n^\times \mathbb{N}_{F_n/E_n}(\mathcal{V}_n)]$  is bounded above by  $\prod_{\hat{\rho} \mid \delta_n} [\mathcal{O}_{n\hat{\rho}}^\times E_n^{\times 2} : E_n^{\times 2}] = \prod_{\hat{\rho} \mid \delta_n} 2$ . It is certainly bounded when  $n$  tends to infinity in view of Lemma 4.3.  $\square$

Let  $K_n$  (resp.  $H_n$ ) be the maximal elementary 2-extension of  $E_n$  (resp.  $F_n$ ) which is unramified outside  $\infty$ .

**Lemma 4.6.** *For any  $n$ ,  $\Omega_n \cap H_n = K_n$ .*

*Proof.* It is clear that  $K_n \subseteq \Omega_n \cap H_n$ . For equality, we suffice to demonstrate that  $\Omega_n \cap H_n/E_n$  is unramified outside  $\infty$ . First of all, as a subextension of  $H_n/E_n$ ,  $\Omega_n \cap H_n/E_n$  is ramified only at the prime dividing  $\delta_n$  and  $\infty$ . On the other hand, since  $\Omega_n \subseteq M_{E_n}$ ,  $\Omega_n \cap H_n/E_n$  is unramified outside  $2 \cup \infty$ . By Lemma 4.3, all prime divisors of  $\delta_n$  is non-dyadic. The assertion is now proved.  $\square$

**Theorem 4.5.** *Let  $F$  be a CM field. If  $\mu(F) = 0$ , then  $h_s(L_n) = 2^{\tau 2^n + O(1)}$ .*

*Proof.* First of all, we note that  $[M_{E_n} : \Omega_n] = 2^{(\frac{d}{2} - \tau)2^n + O(1)}$  and  $[\Omega_n : E_n] = 2^{\tau 2^n + O(1)}$ . They can be proved similarly as in Theorem 4.3. Now,

$$\begin{aligned} [M_{F_n} : \Sigma_n] &\geq [\Sigma_n M_{E_n} : \Sigma_n] \\ &= [M_{E_n} : M_{E_n} \cap \Sigma_n] \\ &= \frac{[M_{E_n} : \Omega_n]}{[M_{E_n} \cap \Sigma_n : \Omega_n]} \\ &= 2^{(\frac{d}{2} - \tau)2^n + O(1)}. \end{aligned}$$

Since  $\mu(F) = 0$ ,  $\mu(E^*) = 0$  also. Therefore,

$$\begin{aligned} [\Sigma_n : H_n] &\geq [\Omega_n H_n : H_n] \\ &= [\Omega_n : \Omega_n \cap H_n] \\ &= [\Omega_n : K_n] \\ &= \frac{[\Omega_n : E_n]}{[K_n : E_n]} \\ &= 2^{\tau 2^n + O(1)}. \end{aligned}$$

Also,  $[H_n : F_n] = 2^{O(1)}$ . So, combining everything together, we have

$$[M_{F_n} : F_n] \geq 2^{(\frac{d}{2}-\tau)2^n+O(1)} \cdot 2^{\tau 2^n+O(1)} \cdot 2^{O(1)} = 2^{\frac{d}{2}2^n+O(1)}.$$

However, Proposition 2.2 shows that the above must be an equality. Consequently,  $h_s(L_n) = [\Sigma_n : F_n] = 2^{\tau 2^n+O(1)}$ . □

### 5. Cyclotomic $\mathbf{Z}_p$ -Extensions, $p > 2$ .

We keep all the notations used in the last section. Let  $F_\infty/F$  be the cyclotomic  $\mathbf{Z}_p$ -extension. Let  $X$  be a finite set of primes of  $F$  containing all the infinite primes. When  $p = 2$ , the assumption  $\mu(F^*) = 0$  implies that  $|\mathcal{I}_n^X|$  and  $|\mathcal{I}_n^{X^*}|$  are bounded as  $n$  tends to infinity (see Corollary 2.1). If  $p > 2$ , the 2-primary modules of the group  $\text{Gal}(F_\infty/F)$  do not behave as well as in the  $p = 2$  case. In particular, we cannot apply Iwasawa’s theory to estimate the 2-part of any class groups of  $F_n$ . However, we do have the following result due to Washington [Wai].

**Theorem 5.1** ([Wai]). *Suppose that  $F$  is an abelian extension of  $\mathbf{Q}$  and  $F_\infty/F$  is the cyclotomic  $\mathbf{Z}_p$ -extension. Then for any prime  $l \neq p$ , the  $l$ -part of the ideal class group of  $F_n$  is bounded as  $n$  tends to infinity.*

**Corollary 5.1.** *Under the hypothesis of Theorem 5.1,  $|\mathcal{I}_n^X|$  and  $|\mathcal{I}_n^{X^*}|$  are bounded as  $n$  tends to infinity.*

In the proofs of Proposition 2.2 and 2.3, we actually only require two conditions satisfied. Firstly,  $|\mathcal{I}_n^X|$  and  $|\mathcal{I}_n^{X^*}|$  are bounded as  $n$  tends to infinity. Secondly, the number of dyadic primes in  $F_n$  is eventually constant. When  $F$  is abelian over  $\mathbf{Q}$ , the first condition is fulfilled by Corollary 5.1. The second one is ensured by the fact that no finite prime split completely in a cyclotomic  $\mathbf{Z}_p$ -extension. Therefore, we have:

**Corollary 5.2.** *Suppose that  $F$  is abelian over  $\mathbf{Q}$ . Let  $M_n$  (resp.  $N_n$ ) be the maximal elementary 2-extension of  $F_n$  which is unramified outside  $2 \cup \infty$  (resp. 2). Then*

- (1)  $[M_n : F_n] = 2^{(r_1+r_2)p^n+O(1)}$ ;
- (2)  $[N_n : F_n] = O(1)$  if  $F$  is real.

From now on,  $F$  is assumed to be an abelian number field in which 2 is unramified. The extension  $F_\infty/F$  is the cyclotomic  $\mathbf{Z}_p$ -extension where  $p$  is an odd prime. Note that 2 is unramified in all  $F_n$ .

**Lemma 5.1.** *If  $L$  does not have Type II reduction at a dyadic prime  $\wp$ , then  $[F_{n\mathcal{P}}^\times : \theta_{n\mathcal{P}}] \leq 2$  for any prime  $\mathcal{P}$  of  $F_n$  dividing  $\wp$ .*

*Proof.* Note that  $L_n$  also does not have Type II reduction at  $\mathfrak{P}$ . Therefore we can just prove the lemma for  $L$ . If a Jordan splitting of  $L_\varphi$  has a component of rank  $\geq 2$ , then it is clear from [H, Prop. A] and [EH, Thm. 3.14]. So, we may assume that  $L \cong \langle 1 \rangle \perp \langle 2^{r_2} \epsilon_2 \rangle \perp \cdots \perp \langle 2^{r_m} \epsilon_m \rangle$  where  $0 = r_1 < r_2 < \cdots < r_m$  and  $\epsilon_i \in \mathcal{O}_F^\times$  for all  $i$ . If  $r_{i+1} - r_i \leq 3$ , then it is a consequence of [EH, 1.9]. The lemma is now proved since Type II reduction means that  $r_{i+1} - r_i \geq 4$  for all  $i$ .  $\square$

Let  $\mathfrak{P}$  be a nondyadic prime of  $F_n$ . If  $\mathfrak{P}$  does not divide  $v(L)$ , then  $\theta_{n\mathfrak{P}} = \mathcal{O}_{n\mathfrak{P}}^\times F_n^{\times 2}$ . Suppose that  $\mathfrak{P} | v(L)$ . Since any finite prime of  $F$  is finitely decomposed in  $F_\infty$  or totally ramified, we may assume that  $\theta_{n\mathfrak{P}} = \mathcal{O}_{n\mathfrak{P}}^\times F_n^{\times 2}$ .

Let  $\varphi$  be a dyadic prime of  $F$  and  $\mathfrak{P}$  a prime of  $F_n$  lying over  $\varphi$ . By Lemma 3.1 and 5.1, we may assume that

$$\theta_{n\mathfrak{P}} = \begin{cases} F_n^{\times 2} & \text{if } L_\varphi \text{ has Type II reduction} \\ \mathcal{O}_{n\mathfrak{P}}^\times F_n^{\times 2} & \text{otherwise.} \end{cases}$$

**Theorem 5.2.** *Suppose that  $F_\infty/F$  is the cyclotomic  $\mathbf{Z}_p$ -extension of a real abelian number field  $F$ . If  $L$  is totally indefinite, then  $h_s(L_n)$  is eventually constant.*

*Proof.* The proof is the same as the one given for Theorem 4.1. We just need to replace Proposition 2.3 by Corollary 5.2. Moreover, the sequence  $h_s(L_n)$  is nondecreasing by [EH2].  $\square$

**Theorem 5.3.** *Suppose that  $F_\infty/F$  is the cyclotomic  $\mathbf{Z}_p$ -extension of a real abelian number field  $F$ . If  $L$  is a definite lattice, then there is a constant  $\sigma$  such that  $0 \leq \sigma \leq [F : \mathbf{Q}]$  and  $h_s(L_n) = 2^{\sigma p^n + O(1)}$ .*

*Proof.* Let  $\Sigma_n$  be the spinor class field of  $L_n$ . By our modification on the local spinor norms, we can assume that  $\Sigma_n \subseteq M_n$ . Let  $H_n^*$  be the maximal elementary 2-extension of  $F_n$  which is unramified outside  $\infty$ . By Washington’s theorem,  $[H_n^* : F_n]$  is bounded as  $n$  tends to infinity. Let  $D$  be the set of all dyadic primes of  $F$  at which  $L$  has Type II reduction. Then

$$[\Sigma_n : F_n] = [\Sigma_n : H_n^*][H_n^* : F_n] \leq \left( \prod_{\mathfrak{P} \in D_n} 2^{e_{\mathfrak{P}} f_{\mathfrak{P}}} \right) \cdot 2^{O(1)}$$

where  $e_{\mathfrak{P}}$  and  $f_{\mathfrak{P}}$  are the absolute ramification index and absolute residue degree of  $\mathfrak{P}$  respectively. Using Lemma 4.1, we also get

$$[M_n : \Sigma_n] \leq \prod_{\mathfrak{P} \in D_n} 2^{e_{\mathfrak{P}} f_{\mathfrak{P}}} \cdot 2^{O(1)}.$$



As a result,  $[M_n : F_n] \leq 2^{[F:\mathbf{Q}]p^n + O(1)}$ . However, Corollary 5.2 says that it must be an equality. Therefore,  $[\Sigma_n : F_n] = (\prod_{\mathcal{P} \in D_n} 2^{e_{\mathcal{P}} f_{\mathcal{P}}}) \cdot 2^{O(1)}$ .

Now  $e_{\mathcal{P}} = 1$  since 2 is unramified in every  $F_n$ . Let  $f_n$  be the absolute residue degree of a dyadic prime of  $F_n$ . It is independent of the choice of the dyadic prime. Since any dyadic prime of  $F$  is finitely decomposed in  $F_\infty$ , there exists a  $n_0$  such that  $f_{n+1} = pf_n$  and  $|D_n| = |D_{n_0}|$  for all  $n \geq n_0$ . In other words,  $f_n = p^{n-n_0} f_{n_0}$  for all  $n \geq n_0$ . Therefore, for  $n \geq n_0$ ,  $\sum_{\mathcal{P} \in D_n} f_{\mathcal{P}} e_{\mathcal{P}} = p^{n-n_0} f_{n_0} |D_{n_0}|$ . Let  $\sigma = p^{-n_0} f_{n_0} |D_{n_0}|$ . Then  $0 \leq \sigma \leq [F : \mathbf{Q}]$  and  $h_s(L_n) = 2^{\sigma p^n + O(1)}$ .  $\square$

**Remark.** (1) If  $D$  is empty, then  $h_s(L_n)$  is eventually constant as the sequence  $h_s(L_n)$  becomes bounded and nondecreasing.  
 (2) If  $D$  contains all the dyadic primes, then  $\sigma = [F : \mathbf{Q}]$ .

Again, let us summarize the result when  $F = \mathbf{Q}$ .

**Theorem 5.4.** *Let  $L$  be a lattice on a quadratic space over  $\mathbf{Q}$  of dimension at least 3. Then  $h_s(L_n)$  is eventually constant unless  $L$  is definite and has Type II reduction at 2. In the exceptional case,  $h_s(L_n) = 2^{p^n + O(1)}$ .*

We next turn our attention to the case where  $F$  is a complex abelian extension of  $\mathbf{Q}$ . Let  $E_n$  be the maximal real subfield of  $F_n$ . Then  $E_\infty = \cup E_n$  is the cyclotomic  $\mathbf{Z}_p$ -extension of  $E = E_0$ . Define a finite set of primes  $R$  of  $E$  as follows. If  $\hat{\varphi} \in R$ , then  $\hat{\varphi}$  is dyadic and there exists a dyadic prime  $\varphi \in D$  lying above  $\hat{\varphi}$ . Now, for any dyadic prime  $\mathcal{P}$  of  $E_n$ , define a subgroup  $\Theta_{\mathcal{P}}$  of  $E_{n\mathcal{P}}^\times$  by

$$\Theta_{\mathcal{P}} = \begin{cases} E_{n\mathcal{P}}^{\times 2} & \text{if } \mathcal{P} \notin R_n \\ \mathcal{O}_{n\mathcal{P}}^\times E_{n\mathcal{P}}^{\times 2} & \text{otherwise.} \end{cases}$$

Let  $\Omega_n$  be the elementary 2-extension of  $E_n$  corresponding to the following subgroup of idèle group of  $E_n$ :

$$E_n^\times \prod_{\mathcal{P}}^* E_{n\mathcal{P}}^{\times 2} \prod_{\mathcal{P} \notin 2}^* \mathcal{O}_{n\mathcal{P}}^\times E_{n\mathcal{P}}^{\times 2} \prod_{\mathcal{P} \in 2}^* \Theta_{\mathcal{P}}.$$

Using the argument in the proof of Theorem 5.3, one can show that  $[\Omega_n : E_n] = 2^{\tau p^n + O(1)}$  for some constant  $\tau$  between 0 and  $[E : \mathbf{Q}]$ .

**Theorem 5.5.** *Suppose that  $F_\infty/F$  is the cyclotomic  $\mathbf{Z}_p$ -extension of a complex abelian number field  $F$ . For any lattice  $L$ , there is a constant  $\tau$  such that  $0 \leq \tau \leq \frac{1}{2}[F : \mathbf{Q}]$  and  $h_s(L_n) = 2^{\tau p^n + O(1)}$ .*

We skip the proof of the above theorem since it is similar to the proof of Theorem 4.5. We merely remark that the constant  $\tau$  is precisely the one described before the theorem.

### 6. Local Spinor Norms.

The aim of this section is to give the proof of Theorem 4.2. Throughout this section, we assume that  $F$  is a 2-adic local field. Let  $L$  be a lattice on a quadratic space  $V$  over  $F$ . We lift the lattice  $L$  to a totally ramified cyclic extension  $K/F$  of degree  $e = 2^n, n \geq 4$ . The lifted lattice  $\tilde{L} = L \otimes \mathcal{O}_K$  is on the space  $\tilde{V} = V \otimes K$ . We always use  $\pi$  to represent a prime element in  $\mathcal{O}_K$ . The unique prime ideal of  $K$  is denoted by  $\mathfrak{P}$ . The scale and the norm of  $L$  are written as  $s(L)$  and  $n(L)$  respectively.

**Definition 6.1.** *A lattice  $M$  on  $\tilde{V}$  is said to be defined over  $\mathcal{O}_F$  if there is a basis  $\{x_1, \dots, x_m\}$  of  $M$  such that the matrix  $\langle B(x_i, x_j) \rangle$  has entries in  $\mathcal{O}_F$ .*

**Lemma 6.1.** *Suppose a Jordan splitting of  $L$  has a unimodular component of rank  $\geq 3$ . Then  $\tilde{L} \cong A(0, 0) \perp N$  where  $N$  is defined over  $\mathcal{O}_F$ .*

*Proof.* Let  $L = L_1 \perp M$  with  $L_1$  unimodular and  $s(M) \subseteq 2\mathcal{O}_F^\times$ . If the rank of  $L_1$  is at least 5, then  $A(0, 0)$  splits  $L_1$  and we are finished. Therefore, we may assume that the rank of  $L_1$  is 3 or 4.

Suppose that the rank of  $L_1$  is 3. Let  $a$  be a norm generator of  $L$ . Then  $a$  is a norm generator of  $\tilde{L}$  as well. We choose 2 to be the weight generator of  $L$ . By the weight formula in [OM, 94], we see that 2 is also a weight generator of  $\tilde{L}$ . Since  $\text{ord}_K(a) + \text{ord}_K(2)$  is even,  $\tilde{L}_1 \cong A(0, 0) \perp N$  for some lattice  $N$  on  $\tilde{V}$ . By comparing determinants, we see that  $N$  is defined over  $\mathcal{O}_F$ .

Suppose that the rank of  $L_1$  is 4. If  $L_1$  is improper, then  $L_1 \cong A(0, 0) \perp A(2, 2\rho_F)$  or  $A(0, 0) \perp A(0, 0)$ . So, we may assume that  $L_1$  is proper. In this case,  $L_1$  has a rank 3 orthogonal summand  $J$  and  $\tilde{L}_1 \cong \tilde{J} \perp \langle \alpha \rangle$  where  $\alpha \in \mathcal{O}_F^\times$ . As in the last paragraph,  $\tilde{J} \cong A(0, 0) \perp N'$  for some  $N'$  defined over  $\mathcal{O}_F$ . Therefore,  $\tilde{L}_1 \cong A(0, 0) \perp N' \perp \langle \alpha \rangle$  and  $N := N' \perp \langle \alpha \rangle$  is defined over  $\mathcal{O}_F$ . □

**Lemma 6.2.** *Let  $\sigma \in O(L)$  and  $x \in L$ . If  $\sigma x \pm x$  is anisotropic, then  $S_{\sigma x \pm x} \sigma(x) = \mp x$ .*

*Proof.* Direct verification. □

Let  $S(L)$  be the subgroup of  $O(L)$  generated by the symmetries which fix  $L$ . Put  $X(L)$  to be the subgroup of  $O(L)$  generated by  $S(L)$  and the Eichler transformations in  $O(L)$ . If  $s(L) \subseteq \mathcal{O}_F$ , we define another group  $X_h(L)$  as follows (see [OP]). If  $\text{rank } L \leq 2$ ,  $X_h(L)$  is just  $S(L)$ . If  $\text{rank}$

$L > 2$ ,  $X_h(L)$  is defined to be the subgroup of  $X(L)$  generated by  $S(L)$  and Eichler transformation  $E_w^y \in X(L)$  for which there exists a splitting  $L = A(0, 0) \perp M$  with  $y \in A(0, 0)$  and  $w \in M$ .

**Theorem 6.1.**  $O(\tilde{L}) = X(\tilde{L})$ .

*Proof.* We proceed by induction on the rank of  $L$ . By scaling, we may assume that  $L = L_1 \perp M$  with  $L_1$  unimodular and  $s(M) \subseteq 2\mathcal{O}_F$ . The theorem is clear if  $L$  is of rank 1.

Suppose that the rank of  $L_1$  is at least 3. By Lemma 6.1,  $\tilde{L} = A(0, 0) \perp N$  where  $N$  is defined over  $\mathcal{O}_F$ . So we may assume  $N = \tilde{J}$  for some lattice  $J$  on a quadratic space over  $F$ . By [OP, 2.5],  $O(\tilde{L}) = X_h(\tilde{L})O(\tilde{J})$  and we are done by induction.

If  $L_1$  is binary, then we can assume that  $L_1$  is  $A(0, 0)$ ,  $A(2, 2\rho_F)$ ,  $A(1, 2\delta)$  or  $A(1, 4\lambda)$  with  $\delta \in \mathcal{O}_F^\times$  and  $\lambda = 0$  or  $\rho_F$ . The case  $A(0, 0)$  can be done by using [OP, 2.5] again. Suppose  $L_1 = A(2, 2\rho_F)$ . If  $Q(M) \cap 2\mathcal{O}_F^\times \neq \emptyset$ , then there exists a  $z \in M$  such that  $Q(z) = 2\eta \in 2\mathcal{O}_F^\times$ . By [OM, 93:29], we can see that  $A(2, 2\rho_F) \perp \langle 2\eta \rangle \cong A(0, 0) \perp \langle 2\eta(1 - 4\rho_F) \rangle$  and so [OP, 2.5] applies. Therefore, we assume that  $Q(M) \cap 2\mathcal{O}_F^\times = \emptyset$ . Then  $n(M) \subseteq 4\mathcal{O}_F$  and hence  $n(\tilde{M}) \subseteq 4\mathcal{O}_K$ . In other words,  $Q(\tilde{M}) \cap 2\mathcal{O}_K^\times$  is empty also. We apply [OP, 2.1] to conclude that  $O(\tilde{L}) = S(\tilde{L})O(\tilde{M})$ . The assertion follows by induction.

Suppose that  $L_1 = A(1, 2\delta)$ . Let  $\{x, y\}$  be a basis of  $L_1$  adapted to  $A(1, 2\delta)$ . Take  $\sigma \in O(\tilde{L})$  and write  $\sigma x = Ax + Cy + w$  with  $w \in \tilde{M}$ . Then  $1 = Q(\sigma x) = A^2 + 2AC + 2C^2\delta + Q(w)$ . Therefore,  $1 - A^2 \in 2\mathcal{O}_K$  and hence  $A \in \mathcal{O}_K^\times$ . If  $1 - A - C \in \mathcal{O}_K^\times$ , then one can check that  $S_{\sigma x - x} \in O(\tilde{L})$ . Otherwise,  $A/\delta + (1 - A + C) \in \mathcal{O}_K^\times$  and  $S_{S_y\sigma x - x} \in O(\tilde{L})$ . Let  $\phi$  be  $S_{\sigma x - x}$  or  $S_{S_y\sigma x - x}S_y$ . Then  $\phi \in X(\tilde{L})$  and  $\phi\sigma x = x$ . Now  $\mathcal{O}_Kx$  splits  $\tilde{L}$  and  $\phi\sigma \in O(\mathcal{O}_Kx^\perp)$ . Therefore induction applies and we can conclude that  $\sigma \in X(\tilde{L})$ . Similar argument applies when  $L_1 = A(1, 4\lambda)$ . One shows that  $\phi\sigma x = x$  where  $\phi = S_{\sigma x - x}$  or  $S_{S_z\sigma x - x}S_z$  with  $z = \pi^{e/2}x + y$ .

If  $L_1$  is of rank 1, then we may assume that  $L = \mathcal{O}_Fx \perp M$  with  $s(M) \subseteq 2\mathcal{O}_F$  and  $Q(x) = 1$ . Let  $\sigma x = Ax + w$  with  $w \in \tilde{M}$ . Direct computations show that  $A$  must be a unit. We suffice to produce  $\phi \in X(\tilde{L})$  so that  $\phi\sigma x = x$ . If  $1 - A \notin 2\mathcal{P}$ , then  $\text{ord}_K(Q(\sigma x - x)) = e + \text{ord}_K(1 - A) \leq 2e$  and so  $S_{\sigma x - x} \in O(\tilde{L})$ . Otherwise,  $S_{\sigma x + x} \in O(\tilde{L})$ .  $\square$

Since 2 is totally ramified in  $K$ , there is a  $\beta \in \mathcal{O}_K^\times$  such that  $2 = \pi^e\beta$ . In below, the quadratic defect function on  $K$  is denoted by  $\mathcal{D}_K$ .

**Lemma 6.3.** *Let  $\delta$  be a unit in  $\mathcal{O}_F^\times$ . Then  $\mathcal{D}_K(\delta) \subseteq \mathcal{P}^{2e-1}$ .*

*Proof.* The lemma is certainly true when  $e = 2$ . For  $n > 1$ , let  $E$  be the unique subfield of  $K$  with  $[E : F] = 2^{n-1}$ . Let  $\mathfrak{P}_E$  be the prime ideal of  $\mathcal{O}_E$ . Apply induction and we have  $\mathcal{D}_E(\delta) \subseteq \mathfrak{P}_E^{2^n-1}$ . As  $\mathfrak{P}_E \mathcal{O}_K = \mathfrak{P}^2$ , we have  $\mathcal{D}_K(\delta) \subseteq \mathfrak{P}^{2^{n+1}-2}$ . Therefore,  $\mathcal{D}_K(\delta) \subseteq \mathfrak{P}^{2^{n+1}-1} = \mathfrak{P}^{2^e-1}$ .  $\square$

**Lemma 6.4.**  $\mathcal{D}_K(\beta) \subseteq \mathfrak{P}^{e-1}$ .

*Proof.* Let  $M$  be the unique quadratic extension of  $F$  inside  $K$ . Inside  $M$ ,  $2 = \pi_M^2 t$  where  $t \in \mathcal{O}_M^\times$  and  $\text{ord}_M(\pi_M) = 1$ . Therefore,  $\pi^e \mathcal{D}_K(\beta) = \pi^e \mathcal{D}_K(t)$  and thus  $\mathcal{D}_K(\beta) = \mathcal{D}_K(t)$ . Apply Lemma 6.3 to the extension  $K/M$  and we have  $\mathcal{D}_K(t) \subseteq \mathfrak{P}^{e-1}$ .  $\square$

We first compute  $\theta_{\tilde{L}}$  when  $\tilde{L}$  is binary. The results are basically extracted from [H] and [Xu].

**Lemma 6.5.** *Suppose that  $L$  is binary unimodular.*

- (1) *If  $L$  is improper, then  $\theta_{\tilde{L}} = \mathcal{O}_K^\times K^{\times 2}$ .*
- (2) *If  $L$  is proper, then  $\theta_{\tilde{L}} = (1 + \mathfrak{P}^{\frac{e}{2}})K^{\times 2}$ .*

*Proof.* (1) is just [H, Lemma 1]. For (2), we may assume that  $L$  represents 1. If  $\tilde{L} \cong A(1, 0)$  or  $A(1, 4\rho_K)$ , then [H, Prop C] applies. Note that  $e \equiv 0 \pmod{4}$ . So, we are left with the case where  $\tilde{L} = A(1, -\alpha)$ ,  $\text{disc}(\tilde{L}) = -(1 + \alpha)$  and  $\mathcal{D}_K(1 + \alpha) = \alpha \mathcal{O}_K \neq 0$  or  $4\mathcal{O}_K$ . However,  $\text{disc}(\tilde{L}) \in \text{disc}(L)K^{\times 2}$  and hence  $\mathcal{D}_K(1 + \alpha) \subseteq \mathfrak{P}^{2e-1}$  by Lemma 6.3. This shows that  $\mathcal{D}_K(1 + \alpha) = \alpha \mathcal{O}_K = \mathfrak{P}^{2e-1}$ . We now apply [H, Prop. D].  $\square$

**Lemma 6.6.** *Suppose  $L = \langle 1 \rangle \perp \langle 2^r \epsilon \rangle$  where  $r \geq 1$  and  $\epsilon \in \mathcal{O}_F^\times$ . Then*

- (1)  $\theta_{\tilde{L}} = K^{\times 2} \cup \epsilon K^{\times 2}$  if  $r > 4$ .
- (2)  $\theta_{\tilde{L}} = (1 + \mathfrak{P}^{2e})K^{\times 2} \cup \epsilon(1 + \mathfrak{P}^{2e})K^{\times 2}$  if  $r = 4$ .
- (3)  $\theta_{\tilde{L}} = (1 + \mathfrak{P}^{\frac{3e}{2}})K^{\times 2} \cup \beta(1 + \mathfrak{P}^{\frac{3e}{2}})K^{\times 2}$  if  $r = 3$ .
- (4)  $\theta_{\tilde{L}} = (1 + \mathfrak{P}^e)K^{\times 2}$  if  $r = 2$ .
- (5)  $\theta_{\tilde{L}} \subseteq \mathcal{O}_K^\times K^{\times 2}$  if  $r = 1$ . Furthermore, if  $\mathcal{D}_K(2) \subseteq \mathfrak{P}^{3e-1}$ , then  $\theta_{\tilde{L}} = (1 + \mathfrak{P}^{\frac{3e}{4}})K^{\times 2}$ .

*Proof.* (1) is just [Xu, Prop. 2.1]. The lattice  $\tilde{L}$  is isometric to  $\langle 1 \rangle \perp \langle \pi^{re} \beta^r \epsilon \rangle$ . The quadratic defect of  $\beta^r \epsilon$  and  $-\beta^r \epsilon$  are contained in  $\mathfrak{P}^{e-1}$ . Since  $e - 1 > 2e - re/2$  for  $r = 3$  or  $4$ , so (2) and (3) can be deduced from [Xu, Prop. 2.2(iii)]. Note that  $\epsilon \in (1 + \mathfrak{P}^{\frac{3e}{2}})K^{\times 2}$  by Lemma 6.3. If  $r = 2$ , then  $(3e - re/2)/2 = e$  and  $\mathcal{D}_K(-\beta^2 \epsilon) = \mathcal{D}_K(-\epsilon) \subseteq \mathfrak{P}^{2e-1}$ . We can now apply [Xu, Prop. 2.3(iii)]. Note that  $e - [e/2 - e/2] = e$ .

If  $r = 1$ , then  $(3e - re/2)/2 = 3e/4$ . On the other hand,  $\mathcal{D}_K(-\beta\epsilon) \subseteq \mathcal{P}^{e-1}$  and  $5e/4 > e - 1 > e - e/2$ . Therefore, [Xu, Prop. 2.3(ii)] applies and so  $\theta_{\tilde{L}} \subseteq \mathcal{O}_K^\times K^{\times 2}$ . If  $\mathcal{D}_K(2) \subseteq \mathcal{P}^{3e-1}$ , then  $\mathcal{D}_K(\beta) \subseteq \mathcal{P}^{2e-1}$  and so  $\mathcal{D}_K(-\beta\epsilon) \subseteq \mathcal{P}^{2e-1}$ . In this case, apply [Xu, Prop. 2.3(iii)] and the result follows.  $\square$

**Corollary 6.1.** *Suppose that  $L$  is a binary lattice. Then  $Q(v) \in \mathcal{O}_K^\times K^{\times 2}$  for all  $v \in P(\tilde{L})$ . Consequently,  $\theta(O(\tilde{L})) \subseteq \mathcal{O}_K^\times K^{\times 2}$ .*

*Proof.* Let  $u \in L$  so that  $Q(u)$  is a norm generator. Then  $Q(u)$  is a norm generator of  $\tilde{L}$  as well. Let  $v \in P(\tilde{L})$ . Then  $Q(v) \in Q(u)\theta(O(\tilde{L}))$ . By Lemma 6.5 and 6.6, we see that  $\theta_{\tilde{L}} \subseteq \mathcal{O}_K^\times K^{\times 2}$ . However,  $Q(u) \in F^\times \subseteq \mathcal{O}_K^\times K^{\times 2}$ . Therefore,  $Q(v) \in \mathcal{O}_K^\times K^{\times 2}$ . The last assertion is a consequence of Theorem 6.1.  $\square$

**Theorem 6.2.** *For any lattice  $L$  on  $V$ ,  $\theta(O(\tilde{L})) \subseteq \mathcal{O}_K^\times K^{\times 2}$ .*

*Proof.* We prove the theorem by induction on the rank of  $L$ . We already established the theorem when the rank of  $L$  is 2 and it is trivial when the rank is 1. So, we assume in below that the rank of  $L$  is at least 3. Since  $F^\times \subseteq \mathcal{O}_K^\times K^{\times 2}$ , we can scale  $L$  by any scalar in  $F$ . This allows us to assume that  $L = L_1 \perp M$  where  $L_1$  is the unimodular component of a Jordan splitting of  $L$ .

Suppose that  $\tilde{L}$  is split by  $\mathbb{H} = A(0, 0)$ . This is the case when (i) the rank of  $L_1$  is  $\geq 3$  (see Lemma 6.1), (ii)  $L_1 = A(0, 0)$  or (iii)  $L_1 = A(2, 2\rho_F)$  and  $Q(M) \cap 2\mathcal{O}_F^\times \neq \emptyset$ . Let  $\sigma \in O(\tilde{L})$ . Clearly  $\tilde{L} = \sigma\tilde{L} = \sigma\mathbb{H} \perp \sigma\tilde{N}$ . Let  $\{x, y\}$  be a hyperbolic pair for  $\mathbb{H}$ . Then  $\{\sigma x, \sigma y\}$  is a hyperbolic pair for  $\sigma\mathbb{H}$ . By [OP, 2.3], there exists an Eichler transformation  $E \in O(\tilde{L})$  such that  $E(\sigma x) = \epsilon x$  for some  $\epsilon \in \mathcal{O}_K^\times$ . Therefore,  $E(\sigma\mathbb{H}) = \mathcal{O}_K x + \mathcal{O}_K z$  where  $\{x, z\}$  is a hyperbolic pair and  $E(\sigma y) = \epsilon^{-1}z$ . By [OP, 2.4], we can find another Eichler transformation  $E' \in O(\tilde{L})$  such that  $E'(z) = y$  and  $E'(x) = x$ . Let  $\tau = E'E$  and  $\phi = S_{x-y}S_{\epsilon x-y}\tau$ . Since  $\phi(\sigma x) = x$  and  $\phi(\sigma y) = y$ . Hence  $\phi\sigma \in O(\tilde{N})$ . By induction,  $\theta(\phi)\theta(\sigma) \subseteq \mathcal{O}_K^\times K^{\times 2}$ . Now,  $Q(x - y) = -2 \in \mathcal{O}_K^\times K^{\times 2}$  and  $Q(\epsilon x - y) = -2\epsilon \in \mathcal{O}_K^\times K^{\times 2}$ . Therefore  $\theta(\phi) \subseteq \mathcal{O}_K^\times K^{\times 2}$  and so is  $\theta(\sigma)$ .

Suppose that  $L_1$  is binary. If  $L_1$  is proper, then we can assume that  $L_1$  represents 1. Let  $x \in L_1$  be a vector such that  $Q(x) = 1$ . In the proof of Theorem 6.1, we show that for any  $\sigma \in O(\tilde{L})$ , we can find  $\phi \in X(\tilde{L})$  so that  $\phi\sigma \in O(\mathcal{O}_K x^\perp)$ . Direct calculation shows that  $\theta(\phi) \in \mathcal{O}_K^\times K^{\times 2}$ . By induction,  $\theta(\sigma) \in \mathcal{O}_K^\times K^{\times 2}$ .

If  $L_1 = A(2, 2\rho_F)$ , we only need to look at the case when  $Q(M) \cap 2\mathcal{O}_F^\times = \emptyset$ . Let  $\{x, y\}$  be a basis of  $L_1$  adapted to  $A(2, 2\rho_F)$ . Let  $\sigma \in O(\tilde{L})$  and write  $\sigma x = Ax + Cy + w$  with  $w \in \tilde{M}$ . Note that  $Q(w) \in 4\mathcal{O}_K$ . Suppose  $C \in \mathcal{O}_K^\times$ .

Then  $Q(\sigma x - x) = 4 - 2B(\sigma x, x) = 4 - 4A - 2C$  which is in  $2\mathcal{O}_K^\times$ . Then  $S_{\sigma x - x}\sigma \in O(\mathcal{O}_K x^\perp)$  and so  $\theta(\sigma) \subseteq \mathcal{O}_K^\times K^{\times 2}$ . Suppose that  $C$  is in  $\mathcal{P}$ . Since  $2 = Q(\sigma x) = 2A^2 + 2AC + 2\rho_F C^2 + Q(w)$ , therefore,  $A$  must be a unit. As a result, the coefficient of  $y$  in  $S_y \sigma x = Ax + (-A\rho_F^{-1} - C)y + w$  is in  $\mathcal{O}_K^\times$ . This implies that  $S_{S_y \sigma x - x}\sigma \in O(\mathcal{O}_K x^\perp)$  and  $Q(S_y \sigma x - x) = 4 - 4A - 2(-A\rho_F^{-1} - C) \in \mathcal{O}_K^\times K^{\times 2}$  and hence  $\theta(\sigma) \in \mathcal{O}_K^\times K^{\times 2}$ .

Finally, let us assume that  $L_1$  has rank 1. By scaling, we may further assume that there is a vector  $x$  in  $L_1$  with  $Q(x) = 1$ . Take  $\sigma \in O(\tilde{L})$  and write  $\sigma x = Ax + w$  with  $w \in \tilde{M}$ . From the proof of Theorem 6.1, we can see that if  $1 - A \in 2\mathcal{P}$ , then  $1 + A \in 2\mathcal{O}_K^\times$ ,  $S_{\sigma x + x} \in O(\tilde{L})$  and  $Q(\sigma x + x) = 2(1 + A) \in 4\mathcal{O}_K^\times$ . Moreover,  $S_{\sigma x + x}\sigma \in O(\tilde{M})$ . By induction, we have  $\theta(\sigma) \in Q(\sigma x + x)\mathcal{O}_K^\times K^{\times 2} = \mathcal{O}_K^\times K^{\times 2}$ . If  $1 - A$  is not in  $2\mathcal{P}$ , then  $S_{\sigma x - x} \in O(\tilde{L})$ . Therefore,  $\text{ord}_K(1 - A) \leq e$ . Note that if we can show that  $\text{ord}_K(1 - A)$  is even, then we are done. For,  $Q(\sigma x - x) = 2(1 - A)$  and so  $\text{ord}_K(Q(\sigma x - x))$  is also even. By a similar argument as before, we have  $\theta(\sigma) \in Q(\sigma x - x)\mathcal{O}_K^\times K^{\times 2} = \mathcal{O}_K^\times K^{\times 2}$ . If  $s(M) \subseteq 4\mathcal{O}_F$ , then  $\text{ord}_K(Q(w)) \geq 2e$ . However,  $Q(\sigma x - x) = (A - 1)^2 + Q(w)$ . This means that  $\text{ord}_K(1 - A) = e$  which is even. So, we may assume  $s(M) = 2\mathcal{O}_F$  and  $\text{ord}_K(1 - A) < e$ .

Let  $L = \langle 1 \rangle \perp L_2 \perp N$  where  $L_2$  is 2-modular and  $s(N) \subseteq 4\mathcal{O}_F$ . Write  $\sigma x = Ax + y + z$  where  $y \in \tilde{L}_2$  and  $z \in \tilde{N}$ . Since  $Q(z) \in 4\mathcal{O}_K$ , we have  $2e > e + \text{ord}_K(1 - A) = \text{ord}_K(Q(\sigma x - x)) = \text{ord}_K((A - 1)^2 + Q(y))$ . Let  $v = (A - 1)x + y$ . We can see that  $S_v \in O(\langle 1 \rangle \perp \tilde{L}_2)$  since  $2B(v, x) = 2(A - 1)$  and  $2B(v, \tilde{L}_2) = 2B(y, \tilde{L}_2) \subseteq 4\mathcal{O}_K$ . If the rank of  $L_2$  is 1, then  $\langle 1 \rangle \perp L_2$  is binary and hence  $Q(v) \in \mathcal{O}_K^\times K^{\times 2}$  by Corollary 6.1. This shows that  $\text{ord}_K(1 - A)$  is even and we are done. Suppose that the rank of  $L_2$  is at least 2. Let  $T = \langle 1 \rangle \perp \tilde{L}_2$  and  $T^\#$  be the dual of  $T$ . Then  $T^{\#2} = \tilde{L}_2^{\#2} \perp \langle 2 \rangle$ . Now  $T^{\#2}$  is an integral lattice defined over  $\mathcal{O}_F$  and the unimodular component has rank  $\geq 2$ . Therefore  $S_v \in O(T^{\#2})$  has spinor norm  $2Q(v)$  which is inside  $\mathcal{O}_K^\times K^{\times 2}$ . In other words,  $\text{ord}_K(Q(\sigma x - x))$  is even and we are done again.  $\square$

**Corollary 6.2.** *If a Jordan splitting of  $L$  has a component of rank  $\geq 3$  or of the form  $2^r A(0, 0)$  or  $2^r A(2, 2\rho_F)$ , then  $\theta_{\tilde{L}} = \mathcal{O}_K^\times K^{\times 2}$ .*

From now on, we assume that 2 is a square in  $K$ . Therefore,  $2 = \pi^e \beta$  with  $\mathcal{D}_K(\beta) = 0$ . It also implies that  $F^\times \subseteq (1 + \mathcal{P}^{2e-1})K^{\times 2}$ .

**Lemma 6.7.** *If  $\theta_{\tilde{L}} \subseteq (1 + \mathcal{P}^\lambda)K^{\times 2}$  with  $\lambda \leq 2e - 1$ , then  $Q(P(\tilde{L})) \subseteq (1 + \mathcal{P}^\lambda)K^{\times 2}$ .*

*Proof.* Let  $v \in P(\tilde{L})$ . Fix  $u \in P(\tilde{L})$  such that  $Q(u) \in \mathcal{O}_F$  is a norm generator. Then  $S_v S_u \in O^+(\tilde{L})$  and therefore  $Q(u)Q(v) \in (1 + \mathcal{P}^\lambda)K^{\times 2}$ . The lemma follows since  $Q(u) \in \mathcal{O}_F \setminus 0 \subseteq (1 + \mathcal{P}^\lambda)K^{\times 2}$ .  $\square$

**Lemma 6.8.** *Let  $0 < \lambda \leq e$  and  $\alpha_1, \dots, \alpha_n, \beta$  be integers in  $\mathcal{O}_K$  such that  $\alpha_i \in (1 + \mathfrak{P}^\lambda)K^{\times 2}$  and  $\beta \in \mathfrak{P}^\lambda$ . If  $1 + \alpha_1 + \dots + \alpha_n + \beta$  is a unit, then it is inside  $(1 + \mathfrak{P}^\lambda)K^{\times 2}$ .*

*Proof.* For each  $i$ , write  $\alpha_i = \eta_i^2 + \pi^\lambda t_i$  where  $\eta_i, t_i \in \mathcal{O}_K$ . Then  $1 + \alpha_1 + \dots + \alpha_n + \beta \equiv (1 + \sum \eta_i)^2 \pmod{\pi^\lambda}$ . Since  $1 + \alpha_1 + \dots + \alpha_n + \beta$  is a unit and  $\lambda > 0$ ,  $(1 + \sum \eta_i)^2$  is also a unit and the lemma is proved.  $\square$

**Lemma 6.9.** *Suppose  $L \cong \langle 1 \rangle \perp M$  with  $s(M) \subseteq 4\mathcal{O}_F$ . If  $\theta_{\tilde{M}} \subseteq (1 + \mathfrak{P}^\lambda)K^{\times 2}$  where  $0 < \lambda \leq e$ , then  $\theta_{\tilde{L}} \subseteq (1 + \mathfrak{P}^\lambda)K^{\times 2}$ .*

*Proof.* In view of Theorem 6.1, we suffice to show that  $Q(v) \in (1 + \mathfrak{P}^\lambda)K^{\times 2}$  for any  $v \in P(\tilde{L})$ . Write  $v = Ax + z$  where  $Q(x) = 1, A \in \mathcal{O}_K$  and  $z \in \tilde{M}$ . Then  $Q(v) = A^2 + Q(z)$ . In below,  $|\cdot|$  denote the  $\mathfrak{P}$ -adic norm on  $K$ .

Suppose that  $|A^2| < |Q(z)|$ . In this case,  $|Q(v)| = |Q(z)|$ . Therefore,  $z \in P(\tilde{M})$  and hence  $Q(z) \in (1 + \mathfrak{P}^\lambda)K^{\times 2}$  by Lemma 6.7 and hypothesis. Now apply Lemma 6.8 to the unit  $1 + A^2/Q(z)$ , we see that  $Q(v) = Q(z)(1 + A^2/Q(z)) \in (1 + \mathfrak{P}^\lambda)K^{\times 2}$ .

If  $|A^2| = |Q(z)|$ , then  $|A^2|$  and  $|Q(z)|$  are both greater than or equal to  $|Q(v)|$ . Therefore  $z \in P(\tilde{M})$  and so  $Q(z) \in (1 + \mathfrak{P}^\lambda)K^{\times 2}$  by Lemma 6.7. Since  $v \in P(\tilde{L})$ , we must have  $|Q(v)| \geq |2B(x, v)| = |2A|$ . Therefore,  $|A^2| \geq |2A|$  and so  $|A| \geq |2|$ . However,  $|4| \geq |Q(z)|$  since  $s(M) \subseteq 4\mathcal{O}_F$ . Therefore  $|4| = |A^2| = |Q(z)| = |Q(v)|$ . Now  $Q(v) = A^2(1 + Q(z)/A^2)$  and this implies  $(1 + Q(z)/A^2) \in \mathcal{O}_K^\times$ . Apply Lemma 6.7 again and we obtain the assertion.

Finally, let us assume that  $|A^2| > |Q(z)|$ . If  $|Q(z)| \leq |4\pi^\lambda|$ , then  $1 + Q(z)/A^2 \in 1 + \mathfrak{P}^\lambda$  because  $|A^2| \geq |4|$  (see the last paragraph) and hence  $Q(v) \in (1 + \mathfrak{P}^\lambda)K^{\times 2}$ . If we have  $|Q(z)| > |4\pi^\lambda| \geq |8|$ , then  $|Q(z)| > |2B(z, w)|$  for any  $w \in \tilde{M}$ . In other words,  $z \in P(\tilde{M})$  and so  $Q(z) \in (1 + \mathfrak{P}^\lambda)K^{\times 2}$ . Apply Lemma 6.8 again to the unit  $1 + Q(z)/A^2$ , we see that  $Q(v) = A^2(1 + Q(z)/A^2) \in (1 + \mathfrak{P}^\lambda)K^{\times 2}$ .  $\square$

**Proposition 6.1.** *Suppose all the components of a Jordan splitting  $L$  are of rank 1. Then  $\theta_{\tilde{L}} \subseteq (1 + \mathfrak{P}^{\frac{3\epsilon}{4}})K^{\times 2}$ . In particular, if  $L$  is split by  $2^r(\langle 1 \rangle \perp \langle 2\epsilon \rangle)$  with  $\epsilon \in \mathcal{O}_F^\times$ , then  $\theta_{\tilde{L}} = (1 + \mathfrak{P}^{\frac{3\epsilon}{4}})K^{\times 2}$ .*

*Proof.* We will proceed by induction on the rank of  $L$ . The proposition is true when  $L$  is of rank 1 or rank 2 (see Lemma 6.6). In view of Lemma 6.9, we may assume that  $L \cong \langle 1 \rangle \perp \langle 2\delta \rangle \perp N$  where  $s(N) \subseteq 4\mathcal{O}_F$  and  $N \neq 0$ . Let  $\{x, y\}$  be a pair of vectors adapted to the summand  $\langle 1 \rangle \perp \langle 2\delta \rangle$ . For any  $v \in P(\tilde{L})$ , write  $v = Ax + Cy + z$  with  $z \in \tilde{N}$  and  $A, C \in \mathcal{O}_K$ .

Suppose that  $|A^2 + 2\delta C^2| > |Q(z)|$ . In this case,  $\text{Max}(|A^2|, |2\delta C^2|) \geq |Q(v)| = |A^2 + 2\delta C^2| \geq |2A|$ . The last inequality holds because  $|Q(v)| \geq |2B(x, v)|$ .

If  $|2\delta C^2| \leq |A^2|$ , then  $|2| \leq |A|$  and so  $|Q(v)| \geq |4|$ . Moreover,  $A^2 + 2\delta C^2 \in (1 + \mathcal{P}^{\frac{3e}{4}})K^{\times 2}$  because  $Ax + Cy \in P(\langle 1 \rangle \perp \langle 2\delta \rangle)$ . If  $|Q(z)| \leq |4\pi^{\frac{3e}{4}}|$ , then  $|Q(z)(A^2 + 2\delta C^2)^{-1}| \leq |\pi^{\frac{3e}{4}}|$  and so  $Q(v) = (A^2 + 2\delta C^2)(1 + Q(z)(A^2 + 2\delta C^2)^{-1}) \in (1 + \mathcal{P}^{\frac{3e}{4}})K^{\times 2}$ . So we assume  $|Q(z)| > |4\pi^{\frac{3e}{4}}| > |8|$ . Then  $z \in P(\tilde{N})$  and induction hypothesis implies that  $Q(z) \in (1 + \mathcal{P}^{\frac{3e}{4}})K^{\times 2}$ . Apply Lemma 6.8 to the unit  $1 + Q(z)(A^2 + 2\delta C^2)^{-1}$  and we are done.

However, if  $|A^2| < |2\delta C^2|$ , then  $|Q(v)| = |2\delta C^2|$ . Also  $|2\delta C^2| = |2\delta C^2 + A^2| > |Q(z)|$ . Therefore,  $|2\delta C^2 + Q(z)| = |2\delta C^2| = |Q(v)|$ . So,  $Cy + z \in P(\langle 2\delta \rangle \perp \tilde{N})$  and induction hypothesis implies that  $2\delta C^2 + Q(z) \in (1 + \mathcal{P}^{\frac{3e}{4}})K^{\times 2}$ . Therefore,  $Q(v) = (2\delta C^2 + Q(z))(1 + A^2(2\delta C^2 + Q(z))^{-1}) \in (1 + \mathcal{P}^{\frac{3e}{4}})K^{\times 2}$ . Note that  $1 + A^2(2\delta C^2 + Q(z))^{-1}$  is a unit since  $|Q(v)| = |2\delta C^2 + Q(z)|$ .

Suppose that  $|A^2 + 2\delta C^2| = |Q(z)|$ . Here, both  $A^2 + 2\delta C^2$  and  $Q(z)$  are in  $(1 + \mathcal{P}^{\frac{3e}{4}})K^{\times 2}$  since  $Ax + Cy \in P(\langle 1 \rangle \perp \langle 2\delta \rangle)$  and  $z \in P(\tilde{M})$ . If  $|A^2| \geq |2\delta C^2 + Q(z)|$ , then  $|A^2| \geq |Q(v)| \geq |2A|$ . So,  $|A| \geq |2|$  and  $|Q(v)| \geq |4|$ . However,  $|4| \geq |Q(z)| \geq |Q(v)|$ . Hence  $|4| = |Q(v)| = |Q(z)| = |A^2 + 2\delta C^2|$ . Therefore,  $1 + Q(z)(A^2 + 2\delta C^2)^{-1}$  is a unit and Lemma 6.8 shows that it is in  $(1 + \mathcal{P}^{\frac{3e}{4}})K^{\times 2}$  and hence so is  $Q(v)$ .

If  $|A^2| < |2\delta C^2 + Q(z)|$ , then  $|2\delta C^2 + Q(z)| = |Q(v)|$  and induction hypothesis implies that  $2\delta C^2 + Q(z) \in (1 + \mathcal{P}^{\frac{3e}{4}})K^{\times 2}$  as  $Cy + z \in P(\langle 2\delta \rangle \perp \tilde{N})$ . Consequently,  $Q(v) = (2\delta C^2 + Q(z))(1 + A^2(2\delta C^2 + Q(z))^{-1}) \in (1 + \mathcal{P}^{\frac{3e}{4}})K^{\times 2}$ .

At last, suppose that  $|A^2 + 2\delta C^2| < |Q(z)|$ . This implies that  $|Q(z)| = |Q(v)|$ . If  $|A^2| > |Q(z)|$ , then  $|A^2| > |Q(v)| \geq |2A|$ . So,  $|A| > |2|$  and  $|4| \geq |Q(z)| = |Q(v)| > |4|$  which is impossible. So, we must have  $|Q(z)| \geq |A^2|$ . Since  $(A^2 + 2\delta C^2)Q(z)^{-1}$  is an integer,  $A^2Q(z)^{-1}$  and  $2\delta C^2Q(z)^{-1}$  are both inside  $\mathcal{O}_K$ . Induction hypothesis shows that  $Q(z) \in (1 + \mathcal{P}^{\frac{3e}{4}})K^{\times 2}$ . We then have  $A^2Q(z)^{-1}$  and  $2\delta C^2Q(z)^{-1}$  are inside  $(1 + \mathcal{P}^{\frac{3e}{4}})K^{\times 2}$ . Since  $|Q(v)| = |Q(z)|$ ,  $1 + A^2Q(z)^{-1} + 2\delta C^2Q(z)^{-1}$  is a unit. Lemma 6.8 shows that this unit must be inside  $(1 + \mathcal{P}^{\frac{3e}{4}})K^{\times 2}$  and hence so is  $Q(v)$ .  $\square$

**Proposition 6.2.** *Suppose  $L \cong \langle 2^{r_1}\epsilon_1 \rangle \perp \cdots \perp \langle 2^{r_n}\epsilon_n \rangle$  where  $\epsilon_i$ 's  $\in \mathcal{O}_F^\times$  and  $r_1 < r_2 < \cdots < r_n$ . If  $\min\{r_i - r_{i-1}\} = 2$ , then  $\theta_{\tilde{L}} = (1 + \mathcal{P}^e)K^{\times 2}$ .*

*Proof.* Clearly,  $(1 + \mathcal{P}^e)K^{\times 2} \subseteq \theta_{\tilde{L}}$  by Lemma 6.6. The reverse inclusion can be proved by using Lemma 6.9, together with an induction argument. Note that  $\theta_{\tilde{M}} \subseteq (1 + \mathcal{P}^e)K^{\times 2}$  for all non-modular binary lattice  $M \cong 2^t\epsilon(\langle 1 \rangle \perp \langle 2^r\delta \rangle)$  with  $r \geq 2$ .  $\square$



**Proposition 6.3.** *Suppose  $L \cong \langle 2^{r_1}\epsilon_1 \rangle \perp \cdots \perp \langle 2^{r_n}\epsilon_n \rangle$  where all the  $\epsilon_i \in \mathcal{O}_F^\times$  and  $r_i - r_{i-1} \geq 3$  for all  $i$ . Then*

$$\theta_{\tilde{L}} = \{ \text{all even products of } Q(v)K^{\times 2} : v \in P(\langle 2^{r_i}\tilde{\epsilon}_i \rangle \perp \langle 2^{r_{i+1}}\tilde{\epsilon}_{i+1} \rangle) \}.$$

*In particular, if  $\min\{r_i - r_{i-1}\} = 3$ , then  $\theta_{\tilde{L}} = (1 + \mathfrak{P}^{\frac{3e}{2}})K^{\times 2}$ .*

*Proof.* Suppose that  $\{x_1, \dots, x_n\}$  is the basis which gives the Jordan splitting stated in the proposition. For simplicity, we let  $L_i = \mathcal{O}_F x_i \perp \mathcal{O}_F x_{i+1}$  for  $i = 1, \dots, n-1$ . Let  $v = \sum A_i x_i \in P(\tilde{L})$ . Then  $Q(v) = \sum A_i^2 2^{r_i} \epsilon_i$ . Let  $k$  be the largest index for which  $|A_k 2^{r_k}|$  is maximal. Then  $|A_k^2 2^{r_k}| \geq |Q(v)| \geq |2B(v, x_j)| = |2A_j 2^{r_j}|$  for all  $j$ . If  $\exists j < k$  such that  $|A_j^2 2^{r_j}| = |A_k^2 2^{r_k}|$ , then  $|A_j| \geq |2|$  as  $|A_j^2 2^{r_j}| \geq |2A_j 2^{r_j}|$ . However,  $|A_k^2 2^{r_k}| \geq |A_j 2^{r_j+1}|$ . Therefore  $|A_k^2 2^{r_k-r_j-1}| \geq |A_j| \geq |2|$  which is impossible since  $r_k - r_j \geq 3$ . Therefore  $k$  is the unique index for which  $|A_k^2 2^{r_k}|$  is maximal and  $|Q(v)| = |A_k^2 2^{r_k}|$ . Therefore, for any  $j \geq k+2$ ,

$$\left| \frac{A_j^2 2^{r_j}}{A_k^2 2^{r_k}} \right| \leq |2^{r_j-r_k-2}| < |8|$$

and for any  $j \leq k-2$ ,

$$\left| \frac{A_j^2 2^{r_j}}{A_k^2 2^{r_k}} \right| \leq |A_k^2 2^{r_k-r_j-2}| < |8|.$$

By local square theorem [OM, 63:1], we then have

$$Q(v) \in (A_{k-1}^2 2^{r_{k-1}} \epsilon_{k-1} + A_k^2 2^{r_k} \epsilon_k + A_{k+1}^2 2^{r_{k+1}} \epsilon_{k+1}) K^{\times 2}.$$

If  $|A_k^2| > |2|$ , then  $|A_k^2| \geq |\pi^{e-2}|$  and

$$\left| \frac{A_{k+1}^2 2^{r_{k+1}}}{A_k^2 2^{r_k}} \right| = |A_{k+1}^2| \left| \frac{2^{r_{k+1}-r_k}}{A_k^2} \right| < |4\pi|.$$

Therefore,  $Q(v) \in Q(P(\tilde{L}_{k-1}))K^{\times 2}$ . If  $|A_k^2| \leq |\pi^{e+2}|$ , then

$$\begin{aligned} \left| \frac{A_{k-1}^2 2^{r_{k-1}}}{A_k^2 2^{r_k}} \right| &\leq |A_k^2 2^{r_k-r_{k-1}-2}| \\ &\leq |2^{r_k-r_{k-1}-1} \pi^2| < |4\pi| \end{aligned}$$

and so  $Q(v) \in Q(P(\tilde{L}_k))K^{\times 2}$ .

We are left with the case where  $|A_k^2| = |\pi^e|$ . If  $\min\{r_i - r_{i-1}\} \geq 4$ , then the last set of inequalities still holds and we are done with this case also.

Therefore we assume right now that  $\min\{r_i - r_{i-1}\} = 3$ . We may further assume that  $|A_{k+1}| = 1$  and  $r_{k+1} - r_k = 3$  for otherwise  $|A_{k+1}^2 2^{r_{k+1}}| < |4| |A_k^2 2^{r_k}|$  and then  $Q(v) \in Q(P(\tilde{L}_{k-1})) \subseteq (1 + \mathfrak{P}^{\frac{3e}{2}})K^{\times 2}$ . Since  $|A_k^2 2^{r_k}| \geq |2^{r_{k-1}+1} A_{k-1}|$ , we have  $|2^{r_k - r_{k-1}}| \geq |A_{k-1}|$ . If strict inequality holds, then

$$\begin{aligned} \left| \frac{A_{k-1}^2 2^{r_{k-1}}}{A_k^2 2^{r_k}} \right| &\leq |A_{k-1}^2 2^{r_{k-1} - r_k - 1}| \\ &< |2^{r_k - r_{k-1}} \pi^2| < |4\pi|. \end{aligned}$$

Therefore,  $Q(v) \in Q(P(\tilde{L}_k))K^{\times 2}$ . So, we may finally assume that  $r_{k+1} - r_k = 3$ ,  $|A_{k-1}| = |\delta|$ ,  $|A_k^2| = |\pi^e|$  and  $|A_{k+1}| = 1$ . Let  $u = A_{k-1}x_{k-1} + A_k x_k$ . Then  $u \in P(\tilde{L}_{k-1})$  and so  $Q(u) \in (1 + \mathfrak{P}^{\frac{3e}{2}})K^{\times 2}$ . On the other hand  $(1 + A_{k+1}^2 2^{r_{k+1}} \epsilon_{k+1} Q(u)^{-1}) \in 1 + \mathfrak{P}^{2e} \subset 1 + \mathfrak{P}^{\frac{3e}{2}}$  and therefore  $Q(v) \in (1 + \mathfrak{P}^{\frac{3e}{2}})K^{\times 2}$ .  $\square$

**Corollary 6.3.** *Suppose  $L \cong \langle 2^{r_1} \epsilon_1 \rangle \perp \cdots \perp \langle 2^{r_n} \epsilon_n \rangle$  where all the  $\epsilon_i \in \mathcal{O}_F^\times$  and  $r_i - r_{i-1} \geq 4$  for all  $i$ . Then  $\theta_{\tilde{L}} \subseteq (1 + \mathfrak{P}^{2e-1})K^{\times 2}$ .*

*Proof.* By Lemma 6.6 and the fact that  $\mathcal{D}_K(\epsilon) \subseteq (1 + \mathfrak{P}^{2e-1})K^{\times 2}$  for all  $\epsilon \in \mathcal{O}_F^\times$ , we see that  $Q(v) \in (1 + \mathfrak{P}^{2e-1})K^{\times 2}$  for all  $v \in P(\langle 2^{r_i} \epsilon_i \rangle \perp \langle 2^{r_{i+1}} \epsilon_{i+1} \rangle)$ ,  $1 \leq i \leq n - 1$ .  $\square$

Up to now, we have completed the proof of Case (I), (II.1) and (III) of Theorem 4.2. Henceforth, we concentrate on Case (II.2) in which the components of a Jordan splitting of  $L$  are of rank 1 or 2 but at least one of them is of rank 2. Also, the binary components are all proper and hence isometric to  $2^r \epsilon(\langle 1 \rangle \perp \langle \delta \rangle)$  for some units  $\epsilon, \delta \in \mathcal{O}_F^\times$ .

**Lemma 6.10.** *Suppose  $A$  and  $C$  are in  $\mathcal{O}_K$  and  $\delta \in \mathcal{O}_F^\times$  such that  $\text{ord}_K(A^2 + \delta C^2) = h < 2e - 1 + 2 \text{ord}_K(C)$ . Then  $h$  is even and  $A^2 + \delta C^2 \in (1 + \mathfrak{P}^{e-h/2+\text{ord}_K(C)})K^{\times 2} \subseteq \mathcal{O}_K^\times K^{\times 2}$ .*

*Proof.* Since  $\mathcal{D}_K(-\delta) \subseteq \mathfrak{P}^{2e-1}$ , we can write  $-\delta = (1 + \pi^{2e-1}u)t^2$  where  $u \in \mathcal{O}_K$  and  $t \in \mathcal{O}_K^\times$ . Then  $A^2 + \delta C^2 = A^2 - E^2 - \pi^{2e-1}uE^2$  where  $E = tC$ .

Let  $A - E = \pi^b \beta$  and  $A + E = \pi^{b'} \beta'$  where  $\beta, \beta' \in \mathcal{O}_K^\times$ . Without loss of generality, we may assume that  $b' \geq b$ . If  $b' > b$ , then  $b = e + \text{ord}_K(E)$  because  $A + E = A - E + 2E$ . Therefore  $\text{ord}_K(A^2 - E^2) > 2e + 2 \text{ord}_K(E)$  and so  $\text{ord}_K(A^2 + \delta C^2) \geq 2e - 1 + 2 \text{ord}_K(E)$  which is a contradiction.

Therefore, we have  $b' = b$ . Then  $h = 2b < 2e - 1 + 2 \text{ord}_K(E)$  and  $b \leq e + \text{ord}_K(E) - 1$ . Now,  $A^2 - E^2 = \pi^{2b} \beta^2 (1 + 2\pi^{-b} \beta^{-1} E)$  and so  $A^2 + \delta C^2 = \pi^{2b} \beta^2 (1 + 2\pi^{-b} \beta^{-1} E - \pi^{2e-1-2b} \beta^{-2} u E^2)$ . Since  $e - b + \text{ord}_K(E) \geq 1$

and  $2e - 1 - 2b + 2 \operatorname{ord}_K(E) \geq e - b + \operatorname{ord}_K(E)$ , therefore  $A^2 + \delta C^2 \in (1 + \mathfrak{P}^{e-h/2+\operatorname{ord}_K(C)})K^{\times 2} \subseteq \mathcal{O}_K^\times K^{\times 2}$ .  $\square$

**Lemma 6.11.** *Let  $\alpha \in (1 + \mathfrak{P}^{e/2})K^{\times 2}$  with  $|4| \leq |\alpha| \leq |2|$ . Suppose  $D$  and  $E$  are integers in  $K$  and  $\gamma \in \mathcal{O}_F^\times$  such that  $1 + (2D^2 + 2E^2\gamma)\alpha^{-1} \in \mathcal{O}_K^\times$ . Then  $1 + (2D^2 + 2E^2\gamma)\alpha^{-1} \in (1 + \mathfrak{P}^{\frac{e}{2}})K^{\times 2}$ .*

*Proof.* Let  $h = \operatorname{ord}_K(D^2 + E^2\gamma)$ . If  $h \geq \operatorname{ord}_K(\alpha) - e/2$ , then  $2(D^2 + E^2\gamma)\alpha^{-1} \in \mathfrak{P}^{\frac{e}{2}}$  and we are done. Hence we assume that  $h < \operatorname{ord}_K(\alpha) - e/2 \leq 2e - e/2 < 2e - 1 + 2 \operatorname{ord}_K(E)$ . So Lemma 6.10 applies and hence  $h$  is even and  $D^2 + E^2\gamma \in (1 + \mathfrak{P}^{e-h/2+\operatorname{ord}_K(E)})K^{\times 2}$ .

If  $h \leq e$ , then  $e - h/2 + \operatorname{ord}_K(E) \geq e/2$  and hence  $2(D^2 + E^2\gamma) \in (1 + \mathfrak{P}^{e/2})K^{\times 2}$ . We are finished again with the help of Lemma 6.8. So, we assume  $h > e$ . In this case,  $(e+h-\operatorname{ord}_K(\alpha)) + (e-h/2+\operatorname{ord}_K(E)) \geq h/2 + \operatorname{ord}_K(E) > e/2$ . In addition,  $e + h - \operatorname{ord}_K(\alpha) > 0$  is even. Therefore,  $(2D^2 + 2E^2\gamma)\alpha^{-1}$  can be written as  $\beta^2 + \pi^{\frac{e}{2}}t$  with  $\beta \in \mathfrak{P}$  and hence  $1 + (2D^2 + 2E^2\gamma)\alpha^{-1} = (1 + \beta)^2 - 2\beta + \pi^{\frac{e}{2}}t \in (1 + \mathfrak{P}^{\frac{e}{2}})K^{\times 2}$ .  $\square$

**Lemma 6.12.** *Let  $\epsilon$  and  $\delta$  be in  $\mathcal{O}_F^\times$ . Then  $\langle \tilde{\epsilon} \rangle \perp \langle \tilde{\epsilon}\delta \rangle \cong \langle \tilde{1} \rangle \perp \langle \tilde{\delta} \rangle$ .*

*Proof.* Let  $L$  be the lattice  $\langle 1 \rangle \perp \langle \delta \rangle$ . Let  $\operatorname{Hasse}(\tilde{L})$  be the Hasse symbol of the quadratic space spanned by  $\tilde{L}$  and  $(,)_K$  be the Hilbert symbol on  $K$ . Then for any  $\epsilon \in \mathcal{O}_F^\times$ ,  $\operatorname{Hasse}(\tilde{L}^\epsilon) = (\epsilon, \epsilon)_K (\epsilon\delta, \delta)_K$ . By Bender's lifting formula for Hilbert symbols of local fields [Be], we have  $(a, b)_K = (\mathbb{N}_{K/F}(a), b)_F$  for any  $a \in K$  and  $b \in F$ . Thus,  $\operatorname{Hasse}(\tilde{L}^\epsilon) = 1$ . Moreover,  $d(\tilde{L}) = d(\tilde{L}^\epsilon)$ . Therefore  $\tilde{L} \otimes K \cong \tilde{L}^\epsilon \otimes K$ . By [OM, 93:16], we suffice to show that the norm groups of  $\tilde{L}^\epsilon$  and  $\tilde{L}$  are equal. Clearly, the weights of both lattices are  $2\mathcal{O}_K = \mathfrak{P}^e$ . Since  $\epsilon \in \mathcal{O}_F^\times$ ,  $\mathcal{D}_K(\epsilon) \subseteq \mathfrak{P}^{2e-1}$  and so  $\epsilon \equiv \eta^2 \pmod{\mathfrak{P}^e}$  for some unit  $\eta$ . Therefore, 1 is a norm generator for both lattices. Hence, their norm groups are equal.  $\square$

**Proposition 6.4.** *Suppose  $L \cong \langle 1 \rangle \perp M$  where  $M$  is binary proper 2-modular. Then  $\theta_{\tilde{L}} = (1 + \mathfrak{P}^{\frac{e}{2}})K^{\times 2}$ .*

*Proof.* By Lemma 6.12, we may assume  $L \cong \langle 1 \rangle \perp 2(\langle 1 \rangle \perp \langle \delta \rangle)$  in basis  $\{x, y, z\}$ . Let  $v \in P(\tilde{L})$ . Write  $v = Ax + Dy + Ez$  where  $A, D, E \in \mathcal{O}_F$ . Then  $Q(v) = A^2 + 2D^2 + 2\delta E^2$ .

Suppose that  $|A^2| > |2D^2 + 2\delta E^2|$ . If  $|A^2| \geq |2|$ , then both  $2D^2A^{-2}$  and  $2\delta E^2A^{-2}$  are integers in  $(1 + \mathfrak{P}^{\frac{e}{2}})K^{\times 2}$ . Since  $|Q(v)| = |A^2|$ , the integer  $1 + 2D^2A^{-2} + 2\delta E^2A^{-2}$  is a unit. Therefore,  $1 + 2D^2A^{-2} + 2\delta E^2A^{-2} \in (1 + \mathfrak{P}^{e/2})K^{\times 2}$  by Lemma 6.8. So we may assume  $|A^2| < |2|$ . As  $|A^2| = |Q(v)| \geq |2B(v, x)| = |2A|$ , we actually have  $|4| \leq |A^2| < |2|$  and Lemma 6.11 applies.

If  $|A^2| < |2D^2 + 2\delta E^2|$ , then  $|Q(v)| = |2D^2 + 2\delta E^2|$  and this implies  $Dy + Ez \in P(\tilde{M})$ . Therefore,  $2D^2 + 2\delta E^2 \in (1 + \mathcal{P}^{\frac{e}{2}})K^{\times 2}$  by Lemma 6.6 and 6.7. Since  $1 + A^2(2D^2 + 2\delta E^2)^{-1}$  is a unit, therefore Lemma 6.8 implies that  $1 + A^2(2D^2 + 2\delta E^2)^{-1} \in (1 + \mathcal{P}^{\frac{e}{2}})K^{\times 2}$  and so is  $Q(v)$ .

Finally, suppose  $|A^2| = |2D^2 + 2\delta E^2|$ . Here, we also have  $2D^2 + 2\delta E^2 \in (1 + \mathcal{P}^{\frac{e}{2}})K^{\times 2}$ . If  $|Q(v)| = |A^2|$ , then  $1 + (2D^2 + 2\delta E^2)A^{-2}$  is a unit and Lemma 6.8 applies. So,  $Q(v) \in (1 + \mathcal{P}^{\frac{e}{2}})K^{\times 2}$ . Therefore, we may assume that  $|Q(v)| < |A^2| = |2D^2 + 2\delta E^2| \leq |2|$ . Since  $|2A| \leq |Q(v)|$ , we have  $|2A| < |A^2|$ . Then  $|2| < |A|$  and  $|4| < |Q(v)|$ . As a result,  $|D^2 + \delta E^2| > |2|$ . Let  $h = \text{ord}_K(A^2) = \text{ord}_K(2D^2 + 2\delta E^2)$ . Then  $\text{ord}_K(D^2 + \delta E^2) = h - e < e < 2e - 1 + 2\text{ord}_K(E)$ . Therefore Lemma 6.10 applies and we have  $D^2 + \delta E^2 \in (1 + \mathcal{P}^{e+e/2-h/2+\text{ord}_K(E)})K^{\times 2}$ . It shows that  $2(D^2 + \delta E^2)A^{-2} \in (1 + \mathcal{P}^{e+e/2-h/2+\text{ord}_K(E)})K^{\times 2}$ . However,  $e+e/2-h/2+\text{ord}_K(E) > e+e/2-e = e/2$ . Therefore Lemma 6.8 applies and  $Q(v) \in (1 + \mathcal{P}^{\frac{e}{2}})K^{\times 2}$ .  $\square$

**Proposition 6.5.** *Suppose  $L \cong \langle 1 \rangle \perp \langle \delta \rangle \perp M$  where  $M$  is binary proper 2-modular. Then  $\theta_{\tilde{L}} = (1 + \mathcal{P}^{\frac{e}{2}})K^{\times 2}$ .*

*Proof.* By Lemma 6.12, we may assume that  $L \cong \langle 1 \rangle \perp \langle \delta \rangle \perp \langle 2 \rangle \perp \langle 2\gamma \rangle$  in basis  $\{x, y, z, w\}$  where  $\gamma$  and  $\delta$  are units in  $\mathcal{O}_F^\times$ . Let  $v \in P(\tilde{L})$  and write  $v = Ax + Cy + Dz + Ew$ . Then  $Q(v) = A^2 + C^2\delta + 2D^2 + 2E^2\gamma$ . Similar to Proposition 6.4, we divide our discussion into three cases according to  $|A^2 + \delta C^2|$  is (i) bigger than, (ii) less than, (iii) equal to  $|2D^2 + 2\gamma E^2|$ . The proof of cases (i) and (ii) are similar to their counterparts in the proof of Proposition 6.4. Therefore, we just treat case (iii) in below. It is clear that  $v$  can be assumed to be primitive in  $\tilde{L}$ .

Suppose that  $|A^2 + \delta C^2| = |2D^2 + 2\gamma E^2|$ . In this case, both  $A^2 + \delta C^2$  and  $2D^2 + 2\gamma E^2$  are in  $(1 + \mathcal{P}^{\frac{e}{2}})K^{\times 2}$ . If  $|Q(v)| = |A^2 + \delta C^2|$ , then  $1 + (A^2 + \delta C^2)(2D^2 + 2\gamma E^2)^{-1}$  is a unit and Lemma 6.8 applies. Therefore, we assume that  $|Q(v)| < |A^2 + \delta C^2| = |2D^2 + 2\gamma E^2| \leq |2|$ . As  $|Q(v)| \geq |2A|$  and  $|2C|$ ,  $A$  and  $C$  cannot be units and hence  $D$  or  $E$  is a unit. Moreover,  $|Q(v)| \geq |4D|$  and  $|4E|$ . Consequently,

$$|4| \leq |Q(v)| < |A^2 + \delta C^2| = |2D^2 + 2\gamma E^2| \leq |2|.$$

Let  $h = \text{ord}_K(A^2 + \delta C^2)$ . Then  $h$  is even and so  $e \leq h \leq 2e - 2 < 2e - 1 + 2\text{ord}_K(C)$ . Apply Lemma 6.10 and we get

$$A^2 + \delta C^2 \in \pi^h(1 + \mathcal{P}^{e-h/2+\text{ord}_K(C)})\mathcal{O}_K^{\times 2}.$$

Similarly, if  $k = \text{ord}_K(D^2 + \gamma E^2)$ , then

$$D^2 + \gamma E^2 \in \pi^k(1 + \mathcal{P}^{e-k/2+\text{ord}_K(E)})\mathcal{O}_K^{\times 2}.$$

Let  $\eta = (2D^2 + 2\gamma E^2)(A^2 + \delta C^2)^{-1}$ . Then

$$\eta \in (1 + \mathfrak{P}^{e-h/2+\text{ord}_K(C)})(1 + \mathfrak{P}^{e-k/2+\text{ord}_K(E)})\mathcal{O}_K^{\times 2}.$$

Therefore, we can write  $\eta = (1 + \pi^{e-k/2+\text{ord}(E)}t)(1 + \pi^{e-h/2+\text{ord}_K(C)}s)\beta^2$  where  $t, s \in \mathcal{O}_K$  and  $\beta \in \mathcal{O}_K^\times$ . Furthermore,  $1 + \eta = (1 + \beta)^2 - 2\beta + \pi^{e-k/2+\text{ord}_K(E)}t + \pi^{e-h/2+\text{ord}_K(C)}s + \pi^{2e-(h+k)/2+\text{ord}_K(E)+\text{ord}_K(C)}st$ .

Now  $|1 + \eta||A^2 + \delta C^2| \geq |2C|$  and  $|2A|$ . This shows that  $\text{ord}_K(1 + \eta) \leq e + \text{ord}_K(C) - h$  and  $e + \text{ord}_K(A) - h$ . Without loss of generality, we assume  $\text{ord}_K(C) \geq \text{ord}_K(A)$ . Since  $|A^2 + \delta C^2| \leq \text{Max}(|A^2|, |C^2|)$ , we have  $h/2 \geq \text{ord}_K(A)$ .

Let  $\text{ord}_K(1 + \eta) = d$ . Then  $d$  must be even since  $\theta_{\tilde{L}} \subseteq \mathcal{O}_K^\times K^{\times 2}$ . Also,

- (a)  $e - d \geq e - e - \text{ord}_K(A) + h \geq h/2 \geq e/2$ ;
- (b)  $e - h/2 + \text{ord}_K(C) - d \geq e - h/2 - \text{ord}_K(C) - e + \text{ord}_K(C) + h = h/2 \geq e/2$  and
- (c)  $e - k/2 + \text{ord}_K(E) - d \geq e - k/2 + \text{ord}_K(E) - e - \text{ord}_K(A) + h \geq (h - k)/2 \geq e/2$  since  $h = k + e$  and  $h - \text{ord}(A) \geq h/2$ .

By (a), (b), (c) above and the fact that  $d$  is even, we see that  $(1 + \eta)\pi^{-d} = ((1 + \beta)\pi^{-d/2})^2 + \pi^{e/2}r$  for some  $r \in \mathcal{O}_K$ . Therefore  $1 + \eta \in (1 + \mathfrak{P}^{e/2})K^{\times 2}$ . We are now finished since  $Q(v) = (A^2 + \delta C^2)(1 + \eta)$ .  $\square$

**Lemma 6.13.** *Suppose  $L \cong \langle 1 \rangle \perp \langle \delta \rangle \perp N$  where  $s(N) \subseteq 4\mathcal{O}_F$ . If  $\theta_{\tilde{N}} \subseteq (1 + \mathfrak{P}^{\frac{e}{2}})K^{\times 2}$ , then  $\theta_{\tilde{L}} = (1 + \mathfrak{P}^{e/2})K^{\times 2}$ .*

*Proof.* Clearly,  $\theta_{\tilde{L}} \supseteq (1 + \mathfrak{P}^{\frac{e}{2}})K^{\times 2}$ . For the other inclusion, we let  $v \in P(\tilde{L})$ . Then  $Q(v) = A^2 + C^2\delta + Q(z)$  where  $z \in \tilde{N}$ . The cases  $|A^2 + C^2\delta| \leq |Q(z)|$  can be proved similarly as before. Suppose that  $|A^2 + C^2\delta| > |Q(z)|$ . In this case,  $A^2 + C^2\delta \in (1 + \mathfrak{P}^{\frac{e}{2}})K^{\times 2}$ . Without loss of generality, we assume  $|A^2| \geq |C^2|$ . Then  $|A^2| \geq |A^2 + C^2\delta| \geq |2A|$  and so  $|A| \geq |2|$ . As a result,  $|A^2 + C^2\delta| = |Q(v)| \geq |4|$ . Now,  $Q(v) = (A^2 + \delta C^2)(1 + Q(z)(A^2 + \delta C^2)^{-1})$ . The following lemma will show that either  $Q(z) \in (1 + \mathfrak{P}^{\frac{e}{2}})K^{\times 2}$  or  $Q(z)(A^2 + \delta C^2)^{-1} \in \mathfrak{P}^{\frac{e}{2}}$ . We are finished in either case.  $\square$

**Lemma 6.14.** *Let  $M$  be a lattice defined over  $\mathcal{O}_F$  with  $s(M) = 2^r\mathcal{O}_F$ . Let  $x \in Q(\tilde{M})$ . Then either  $\text{ord}_K(x) \geq re + e/2$  or  $x \in (1 + \mathfrak{P}^{\frac{e}{2}})K^{\times 2}$ .*

*Proof.* Scaling by  $2^{-r}$  allows us to assume  $r = 0$ . If  $n(M) \subseteq 2\mathcal{O}_F$ , then we are done. Hence we can assume that  $n(M) = \mathcal{O}_F$ . Let  $a$  be a norm generator of  $M$ . Take  $x \in Q(\tilde{L})$ . There exist  $\alpha, \beta \in \mathcal{O}_K$  such that  $x = a\alpha^2 + 2\beta$ . We may assume that  $\text{ord}_K(a\alpha^2) = \text{ord}_K(\alpha) < \text{ord}_K(2\beta)$  since otherwise  $\text{ord}_K(x) \geq e > e/2$ . Under this assumption,  $\text{ord}_K(x) = \text{ord}_K(\alpha^2)$  and  $x(a\alpha^2)^{-1} = 1 + 2\beta(a\alpha^2)$  is a unit.

If  $\text{ord}_K(x) < e/2$ , then  $\text{ord}_K(a\alpha^2) < e/2$  and so  $1 + 2\beta(a\alpha^2)^{-1} \in 1 + \mathfrak{P}^{\frac{e}{2}}$ . As  $a \in \mathcal{O}_F$ ,  $a \in (1 + \mathfrak{P}^{\frac{e}{2}})K^{\times 2}$ . Therefore,  $x \in (1 + \mathfrak{P}^{\frac{e}{2}})K^{\times 2}$ .  $\square$

The next proposition is Case (II.2) of Theorem 4.2.

**Proposition 6.6.** *Suppose  $L$  is split by  $2^r\epsilon(\langle 1 \rangle \perp \langle \delta \rangle)$ . Then  $\theta_{\tilde{L}} = (1 + \mathfrak{P}^{\frac{e}{2}})K^{\times 2}$ .*

*Proof.* We proceed by induction on the rank of  $L$ . The proposition is true if the rank is 2 or 3 or  $L \cong \langle 1 \rangle \perp \langle \delta \rangle \perp 2\epsilon(\langle 1 \rangle \perp \langle \delta \rangle)$  (after scaling  $L$  suitably). In view of Lemma 6.9 and 6.13, we may assume that the second Jordan component has scale  $2\mathcal{O}_F$ . We have two situations here, namely (A)  $L \cong \langle 1 \rangle \perp L_2 \perp N$  and (B)  $L \cong \langle 1 \rangle \perp \langle \delta \rangle \perp L_2 \perp N$  where  $L_2$  is 2-modular and  $s(N) \subseteq 4\mathcal{O}_F$ . The proof of the proposition will be similar to the proofs for Proposition 6.4 and 6.5 and Lemma 6.13. Therefore, we simply lay out the idea below instead of giving the full version of the proof.

In (A), let  $x$  be the vector which gives the summand  $\langle 1 \rangle$ . Take  $v \in P(\tilde{L})$  and write it as  $v = Ax + y + z$  where  $y \in \tilde{L}_2$  and  $z \in \tilde{N}$ . As usual, we subdivide the discussion into three subcases by comparing  $|A^2 + Q(y)|$  and  $|Q(z)|$ . In (B), let  $\{x, y\}$  be the pair of vectors which gives the summand  $\langle 1 \rangle \perp \langle \delta \rangle$ . Let  $v \in P(\tilde{L})$ . This time,  $v$  can be written as  $Ax + Cy + z + w$  where  $z \in \tilde{L}_2$  and  $w \in \tilde{N}$ . We then compare the norms  $|A^2 + C^2\delta + Q(z)|$  and  $|Q(w)|$ .  $\square$

## References

- [Be] E. Bender, *A lifting formula for the Hilbert symbol*, Proc. Amer. Math. Soc., **40**(1) (1973), 63-65.
- [EH] A. Earnest and J. Hsia, *Spinor norms of local integral rotations*, II, Pacific J. Math., **61**(1) (1975), 71-86.
- [EH1] ———, *Spinor genera under field extensions*, I, Acta Arith., **32** (1977), 115-128.
- [EH2] ———, *Spinor genera under field extensions*, II: 2 unramified in the bottom field, Amer. J. Math., **100** (1978), 523-537.
- [EH3] ———, *Spinor genera under field extensions*, III: Quadratic extensions, Number Theory and Algebra, Academic Press, (1977), 43-62 (Ed. H.J. Zassenhaus).
- [EsH] D. Estes and J. Hsia, *Spinor genera under field extensions IV: Spinor class fields*, Japan. J. Math., **16**(2) (1990), 341-350.
- [FW] B. Ferrero and L. Washington, *The Iwasawa invariant  $\mu_p$  vanishes for abelian number fields*, Ann. of Math., **109** (1979), 377-395.
- [H] J.S. Hsia, *Spinor norms of integral rotations I*, Pacific J. Math., **57**(1) (1975), 199-206.

- [I1] K. Iwasawa, *On  $\Gamma$ -extension of algebraic number fields*, Bull. Amer. Math. Soc., **65** (1959), 183-226.
- [I2] ———, *On some properties of  $\Gamma$  finite modules*, Ann. of Math., **2** (1959), 291-312.
- [I3] ———, *On the  $\mu$ -invariants of  $Z_1$ -extensions*, in 'Number Theory, Algebraic Geometry and Commutative Algebra' (in honor of Y. Akizuki), Kinokuniya, Tokyo, (1973), 1-11.
- [I4] ———, *On  $Z_1$ -extensions of algebraic number fields*, Ann. of Math., **98** (1973), 246-326.
- [Ki] Y. Kida, *Cyclotomic  $Z_2$ -extension of  $J$ -fields*, J. Number Th., **14** (1982), 340-352.
- [Kn] M. Kneser, *Klassenzahlen indefiniter quadratischer Formen in drei oder mehr Veränderlichen*, Arch. Math., (Basel), **7** (1956), 323-332.
- [OM] O.T. O'Meara, *Introduction to quadratic forms*, Springer Verlag, Grundlehren Series, **117** (1963).
- [OP] O.T. O'Meara and B. Pollack, *Generation of local orthogonal groups, II*, Math. Z., **93** (1966), 171-188.
- [Si] W. Sinnott, *On the  $\mu$ -invariant of the  $\Gamma$ -transform of a rational function*, Invent. Math., **75**(2) (1984), 273-282.
- [Wa] L. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Mathematics, Springer Verlag, New York, 1982.
- [Wal] ———, *The non- $p$ -part of the class number in a cyclotomic  $Z_p$  extension*, Invent. Math., **49** (1979), 87-97.
- [Xu] F. Xu, *Integral spinor norms in dyadic local fields I*, Pacific J. Math., **157**(1) (1993), 179-200.

Received March 11, 1997 and revised May 20, 1997.

UNIVERSITY OF SOUTHERN CALIFORNIA  
LOS ANGELES CA 90089  
*E-mail address:* wkchan@math.usc.edu