

# Hecke Eigenvalues for Real Quadratic Fields

Kaoru Okada

## CONTENTS

1. Introduction
2. The Trace Formula for Totally Real Number Fields
3. Computation for Real Quadratic Fields
4. Numerical Examples for  $\mathbb{Q}(\sqrt{257})$  and  $\mathbb{Q}(\sqrt{401})$

Acknowledgments

References

---

We describe an algorithm to compute the trace of Hecke operators acting on the space of Hilbert cusp forms defined relative to a real quadratic field with class number greater than one. Using this algorithm, we obtain numerical data for eigenvalues and characteristic polynomials of the Hecke operators. Within the limit of our computation, the conductors of the orders spanned by the Hecke eigenvalue for any principal split prime ideal contain a nontrivial common factor, which is equal to a Hecke  $L$ -value.

---

## 1. INTRODUCTION

Let  $F$  be a totally real algebraic number field with nontrivial class group. We shall study the space  $\mathcal{S}_k(\mathfrak{c}, \psi)$  of Hilbert cusp forms (relative to  $F$ ) and the Hecke operators  $T(\mathfrak{a})$  acting on it. We shall describe our result using the framework first introduced in [Shimura 78]. Following Shimura's work, the trace formula (whose origin goes back to fundamental work of Eichler, Selberg, and Shimizu) was made more explicit in [Saito 84]. Saito's formula gives us a method for computing Hecke eigenvalues as long as the dimension of the space remains reasonably small. It is then natural to expect Hecke eigenvalues for prime ideals  $\mathfrak{p}$  in a given ideal class to have a new feature specific to the ideal class. Such a new feature can be detected only by computing Hecke eigenvalues for the base field with nonprincipal ideal classes. The purpose of this paper is to compute examples of such Hecke eigenvalues for real quadratic fields with class number greater than 1 and to present a new phenomenon that we have discovered through our numerical examples.

We summarize our observations for the data of Hecke eigenvalues when the weight is parallel  $(k_1, k_1)$ , the level  $\mathfrak{c}$  is the maximal order  $\mathfrak{o}_F$  of  $F$ , and the Hecke character  $\psi$  is the identity 1. Let  $\mathbf{f}$  be a primitive form contained in  $\mathcal{S}_{(k_1, k_1)}(\mathfrak{o}_F, 1)$  that is orthogonal to any base change lift from  $\mathbb{Q}$  (that is,  $\mathbf{f}$  is a primitive form in the “ $F$ -proper” subspace of  $\mathcal{S}_{(k_1, k_1)}(\mathfrak{o}_F, 1)$  as defined in [Doi et al. 98]). We denote by  $C_{\mathbf{f}}(\mathfrak{p})$  the eigenvalue of  $T(\mathfrak{p})$  satisfying  $\mathbf{f}|T(\mathfrak{p}) = C_{\mathbf{f}}(\mathfrak{p})\mathbf{f}$ , by  $K_{\mathbf{f}}^+$  the subfield of the

2000 AMS Subject Classification: Primary 11F41; Secondary 11F60, 11F72, 11R42

Keywords: Hilbert cusp form, Hecke operator, eigenvalue, trace formula  $L$ -value

Hecke field  $K_{\mathbf{f}}$  of  $\mathbf{f}$  generated by  $C_{\mathbf{f}}((p)_F)$  for all *rational* primes  $p$ , and by  $\mathfrak{o}_{K_{\mathbf{f}}^+}$  the maximal order of  $K_{\mathbf{f}}^+$ . For split prime ideals  $\mathfrak{p}$ , we computed the discriminant of the order  $\Lambda_{\mathbf{f}}(\mathfrak{p})$  spanned by the eigenvalue of  $T(\mathfrak{p})$  (that is,  $\Lambda_{\mathbf{f}}(\mathfrak{p}) = \mathfrak{o}_{K_{\mathbf{f}}^+} + C_{\mathbf{f}}(\mathfrak{p})N(\mathfrak{p})^{(k_1-2)/2}\mathfrak{o}_{K_{\mathbf{f}}^+}$ ) to see whether it has extra factors outside the discriminant of the maximal order. Extra factors show up as the conductor of the order (for the definition of the conductor, see just above Lemma 2.3); so, we write  $c(\Lambda_{\mathbf{f}}(\mathfrak{p}))$  for the conductor. Surprisingly enough, *as long as the prime ideals  $\mathfrak{p}$  are principal and split, the conductors  $c(\Lambda_{\mathbf{f}}(\mathfrak{p}))$  contain a nontrivial common factor  $\mathfrak{F}_{\mathbf{f}}$ , at least within the limit of our computations.* (see Sections 4.1 and 4.2).

In Section 2, we recall the space of Hilbert cusp forms for totally real number fields and Hecke operators. We then reformulate Saito's formula into a more computable one. The notion of the conductor of an order plays an important role in this process. In Section 3, we give an algorithm to compute the trace of Hecke operators for a real quadratic field  $F$ . Key points of the computation are the determination of the relative discriminant  $D_{K/F}$ , the character  $(\frac{K}{\mathfrak{p}})$ , and the Hecke  $L$ -value  $L_F(0, \chi_{K/F})$  for any totally imaginary quadratic extension  $K$  over  $F$ . In particular, the computation of the Hecke  $L$ -value by Shintani's method [Shintani 76] has been reduced to that of Hilbert symbols (cf. [Okazaki 91]). In Section 4, we give examples of eigenvalues and characteristic polynomials of Hecke operators restricted to the case where the weight is  $(2, 2)$  and  $F$  is  $\mathbf{Q}(\sqrt{257})$  or  $\mathbf{Q}(\sqrt{401})$ , and we describe our analysis of the data to convince the reader of the conclusion we have already described.

While I was preparing the revision of this paper following the request of the referee to provide a more detailed study of  $\mathfrak{F}_{\mathbf{f}}$ , Professor Haruzo Hida provided the following crucial suggestion:

- (1) Within the limits of the computations carried out, check that  $\mathfrak{F}_{\mathbf{f}}\mathfrak{o}_{K_{\mathbf{f}}}$  is divisible by the common factor of  $1 + N(\mathfrak{p}) - C_{\mathbf{f}}(\mathfrak{p})$  for the principal primes  $\mathfrak{p}$ .
- (2) As is well known, several outstanding mathematicians have worked out the congruence primes between a primitive cusp form and an Eisenstein series, which are essentially given by the value at the weight of a Hecke  $L$ -function of the base field. Notably, A. Wiles studied in depth such an Eisenstein congruence, which is a key step in his proof of the Iwasawa conjecture for totally real fields. Therefore, if (1) is affirmative, his result presumably implies that  $\mathfrak{F}_{\mathbf{f}}$  is divisible by the congruence primes. Here

the congruence prime can be found in the prime factors of the numerator of the algebraic part of the Hecke  $L$ -value  $L_F(2, \chi)$  associated with a nontrivial class character  $\chi$ .

- (3) Moreover, it is expected that the set of the primes of  $\mathfrak{F}_{\mathbf{f}}$  coincides with that of the congruence primes between the  $F$ -proper cusp form  $\mathbf{f}$  and the Eisenstein series of weight  $(k_1, k_1)$  with Mellin transform  $L_F(s, \chi)L_F(s + 1 - k_1, \chi^{-1})$  for a nontrivial class character  $\chi$ .

We shall give affirmative numerical evidence for (1) and (2) in Section 4.3. As for (3), we hope to discuss this property in a subsequent paper.

### Notation

For an associative ring  $R$  with identity element, we denote by  $R^\times$  the group of invertible elements of  $R$ . We write  $M_2(R)$  for the ring of  $2 \times 2$  matrices over  $R$ , and  $1_2$  for the identity element of  $M_2(R)$ .

For an algebraic number field  $F$  of finite degree, we denote by  $\mathfrak{o}_F$ ,  $\mathfrak{d}_F$ , and  $D_F$  the maximal order of  $F$ , the different of  $F$  over  $\mathbf{Q}$ , and the discriminant of  $F$  over  $\mathbf{Q}$ . We write  $I(F)$  for the ideal group of  $F$ , and  $P(F)$ ,  $\text{Cl}(F)$ , and  $h_F$  (respectively  $P^+(F)$ ,  $\text{Cl}^+(F)$ , and  $h_F^+$ ) for the principal ideal group of  $F$ , the ideal class group of  $F$ , and the class number of  $F$  (respectively those in the narrow sense). For  $\alpha \in F^\times$ , we put  $(\alpha)_F = \alpha\mathfrak{o}_F$ . For a prime ideal  $\mathfrak{p}$  of  $F$  and  $\mathfrak{m} \in I(F)$ , we denote by  $\text{ord}_{\mathfrak{p}}(\mathfrak{m})$  the order of  $\mathfrak{m}$  at  $\mathfrak{p}$ . For  $\alpha \in F$ , we set  $\alpha \gg 0$  if  $\alpha$  is totally positive. We define  $\mathfrak{o}_{F^+}^\times = \{a \in \mathfrak{o}_F^\times \mid a \gg 0\}$ . For integral ideals  $\mathfrak{a}, \mathfrak{b}$  of  $F$ , we write  $\mathfrak{a} \mid \mathfrak{b}$  if  $\mathfrak{b}\mathfrak{a}^{-1} \subset \mathfrak{o}_F$ ; for elements  $\alpha (\neq 0), \beta$  of  $\mathfrak{o}_F$ , we write  $\alpha \mid \beta$  if  $\beta\alpha^{-1} \in \mathfrak{o}_F$ . For  $\alpha_1, \dots, \alpha_r \in F$ , we write  $[\alpha_1, \dots, \alpha_r]$  for the  $\mathbf{Z}$ -submodule of  $F$  generated by  $\alpha_1, \dots, \alpha_r$ . We denote by  $\zeta_F$  the Dedekind zeta function of  $F$ .

For an extension  $K$  of  $F$  of finite degree, we denote by  $D_{K/F}$  the relative discriminant of  $K$  over  $F$ . For an element  $\alpha$  of  $K$ , we denote by  $D_{K/F}(\alpha)$ ,  $N_{K/F}(\alpha)$ , and  $\text{Tr}_{K/F}(\alpha)$  the relative discriminant, the norm, and the trace of  $\alpha$  in  $K$  over  $F$ . We denote by  $N(\mathfrak{a})$  the norm of an ideal  $\mathfrak{a}$  of  $F$ . (We also use the symbols  $N_{K/F}(\alpha)$ ,  $\text{Tr}_{K/F}(\alpha)$ , and  $N(\mathfrak{a})$  when  $K$  and  $F$  are local fields.)

For  $a \in \mathbf{R}$ , we denote by  $[a]$  the greatest integer not greater than  $a$ . Let  $(\frac{a}{p})$  be the Legendre symbol for  $a \in \mathbf{Z}$  and a prime number  $p$ . For a set  $X$ , we denote the cardinality of  $X$  by  $|X|$  and also by  $\sharp X$ . For a subgroup  $H$  of a group  $G$ , we write  $[G : H] = |G/H|$ . For a subfield  $F$  of a field  $K$ , the symbol  $[K : F]$  means the degree of  $K$

over  $F$ . The disjoint union of sets  $Y_1, \dots, Y_s$  is denoted by  $\bigsqcup_{i=1}^s Y_i$ .

**2. THE TRACE FORMULA FOR TOTALLY REAL NUMBER FIELDS**

In this section, we first recall the definition of Hecke operators acting on the space of Hilbert cusp forms as given in [Shimura 78, §2]. (Cf. also [Shimura 91].)

**2.1 Hilbert Cusp Forms and Hecke Operators**

Let  $F$  be a totally real algebraic number field of degree  $g$ , and denote by  $\mathfrak{a}$  and  $\mathfrak{h}$  the sets of archimedean primes and nonarchimedean primes of  $F$ . For  $\mathfrak{p} \in \mathfrak{h}$ , we also denote by  $\mathfrak{p}$  the corresponding prime ideal of  $F$ . For any set  $X$ , we write  $X^{\mathfrak{a}}$  for the set of all indexed elements  $(x_v)_{v \in \mathfrak{a}}$  with  $x_v \in X$ . Let  $F_{\mathfrak{A}}$  be the ring of adèles of  $F$ , and  $F_{\mathfrak{A}}^{\times}$  the group of ideles of  $F$ . For  $v \in \mathfrak{a} \cup \mathfrak{h}$  and  $x \in F_{\mathfrak{A}}$ , let  $F_v$  be the  $v$ -completion of  $F$ , and  $x_v$  its  $v$ -component. We write  $F_{\mathfrak{a}}$  and  $F_{\mathfrak{h}}$  for the archimedean and nonarchimedean factors of  $F_{\mathfrak{A}}$ , and identify  $F_{\mathfrak{a}}$  with  $\mathbf{R}^{\mathfrak{a}}$ . For  $\mathfrak{a} \in I(F)$  and  $\mathfrak{p} \in \mathfrak{h}$ , we denote by  $\mathfrak{a}_{\mathfrak{p}}$  the topological closure of  $\mathfrak{a}$  in  $F_{\mathfrak{p}}$ . We abbreviate  $(\mathfrak{o}_F)_{\mathfrak{p}}$  and  $(\mathfrak{d}_F)_{\mathfrak{p}}$  by  $\mathfrak{o}_{\mathfrak{p}}$  and  $\mathfrak{d}_{\mathfrak{p}}$ , for short. We then set  $\mathfrak{o}_{\mathfrak{h}} = \prod_{\mathfrak{p} \in \mathfrak{h}} \mathfrak{o}_{\mathfrak{p}}$  and  $\mathfrak{d}_{\mathfrak{h}} = \prod_{\mathfrak{p} \in \mathfrak{h}} \mathfrak{d}_{\mathfrak{p}}$ . For  $a \in F_{\mathfrak{A}}^{\times}$ , we denote by  $a\mathfrak{o}_F$  the fractional ideal of  $F$  such that  $(a\mathfrak{o}_F)_{\mathfrak{p}} = a_{\mathfrak{p}}\mathfrak{o}_{\mathfrak{p}}$  for every  $\mathfrak{p} \in \mathfrak{h}$  (i.e.,  $a\mathfrak{o}_F = F \cap F_{\mathfrak{A}} \prod_{\mathfrak{p} \in \mathfrak{h}} a_{\mathfrak{p}}\mathfrak{o}_{\mathfrak{p}}$ ). For  $a \in F_{\mathfrak{A}}^{\times}$ , we set  $\text{ord}_{\mathfrak{p}}(a) = \text{ord}_{\mathfrak{p}}(a\mathfrak{o}_F)$ . We denote by  $\pi_{\mathfrak{p}}$  a prime element of  $F_{\mathfrak{p}}$ . By a *Hecke character* of  $F$ , we understand a character of  $F_{\mathfrak{A}}^{\times}$  with values in  $\mathbf{T} = \{z \in \mathbf{C} \mid |z| = 1\}$  that is trivial on  $F^{\times}$ .

Let  $G = \text{GL}_2(F)$ . We set  $G_v = \text{GL}_2(F_v)$  for every  $v \in \mathfrak{a} \cup \mathfrak{h}$ . We consider the adèlization  $G_{\mathfrak{A}}$  of  $G$ , and denote by  $G_{\mathfrak{a}}$  and  $G_{\mathfrak{h}}$  its archimedean and nonarchimedean factors. We set  $G_{\mathfrak{a}+} = \{x \in G_{\mathfrak{a}} \mid \det(x) \gg 0\}$  and  $G_+ = G \cap G_{\mathfrak{a}+}G_{\mathfrak{h}}$ . For an element  $x$  of  $G_{\mathfrak{A}}$ , we denote by  $x_{\mathfrak{a}}$  its  $\mathfrak{a}$ -component. For  $x \in G_{\mathfrak{A}}$ , we set  $x^t = \det(x)x^{-1}$  and  $x^{-t} = (x^t)^{-1}$ . We take an element  $\delta_{\mathfrak{h}}$  of  $F_{\mathfrak{h}}$  such that  $\delta_{\mathfrak{h}}\mathfrak{o}_{\mathfrak{h}} = \mathfrak{d}_{\mathfrak{h}}$ , define subsets  $Y_{\mathfrak{h}}$  and  $W_{\mathfrak{h}}$  of  $G_{\mathfrak{h}}$  by

$$Y_{\mathfrak{h}} = \begin{pmatrix} 1 & 0 \\ 0 & \delta_{\mathfrak{h}} \end{pmatrix} M_2(\mathfrak{o}_{\mathfrak{h}}) \begin{pmatrix} 1 & 0 \\ 0 & \delta_{\mathfrak{h}} \end{pmatrix}^{-1} \cap G_{\mathfrak{h}},$$

$$W_{\mathfrak{h}} = \begin{pmatrix} 1 & 0 \\ 0 & \delta_{\mathfrak{h}} \end{pmatrix} \text{GL}_2(\mathfrak{o}_{\mathfrak{h}}) \begin{pmatrix} 1 & 0 \\ 0 & \delta_{\mathfrak{h}} \end{pmatrix}^{-1},$$

and set

$$Y = G_{\mathfrak{a}+}Y_{\mathfrak{h}}, \quad W = G_{\mathfrak{a}+}W_{\mathfrak{h}}.$$

We denote by  $H$  the complex upper half-plane. For  $\alpha = (\alpha_v)_{v \in \mathfrak{a}} = \left( \begin{pmatrix} a_v & b_v \\ c_v & d_v \end{pmatrix} \right)_{v \in \mathfrak{a}} \in G_{\mathfrak{a}+}$ ,  $z = (z_v)_{v \in \mathfrak{a}} \in H^{\mathfrak{a}}$ ,

$k = (k_v)_{v \in \mathfrak{a}} \in \mathbf{Z}^{\mathfrak{a}}$ , and a  $\mathbf{C}$ -valued function  $f$  on  $H^{\mathfrak{a}}$ , we set

$$\alpha(z) = \left( (a_v z_v + b_v) / (c_v z_v + d_v) \right)_{v \in \mathfrak{a}},$$

$$J_k(\alpha, z) = \prod_{v \in \mathfrak{a}} (\det(\alpha_v))^{-k_v/2} (c_v z_v + d_v)^{k_v},$$

$$(f||_k \alpha)(z) = J_k(\alpha, z)^{-1} f(\alpha(z)),$$

and denote by  $\tilde{\mathcal{S}}_k$  the space of all holomorphic functions  $f$  on  $H^{\mathfrak{a}}$  satisfying the following two conditions:

- (i<sub>a</sub>) There exists  $0 < N \in \mathbf{Z}$  such that  $f||_k \gamma = f$  for all  $\gamma \in \text{SL}_2(\mathfrak{o}_F) \cap (1_2 + N \cdot M_2(\mathfrak{o}_F))$ .
- (i<sub>b</sub>) For every  $\alpha \in G_+$ , one has

$$(f||_k \alpha)(z) = \sum_{0 \ll \xi \in L_{\alpha}} c_{\alpha}(\xi) e_F(\xi z)$$

with a lattice  $L_{\alpha}$  of  $F$  and  $c_{\alpha}(\xi) \in \mathbf{C}$ , where  $e_F(\xi z) = \exp(2\pi\sqrt{-1} \sum_{v \in \mathfrak{a}} \xi_v z_v)$ .

Let  $\psi$  be a Hecke character of  $F$  of finite order such that the nonarchimedean part of its conductor is equal to  $\mathfrak{o}_F$  (i.e.  $\psi(\mathfrak{o}_{\mathfrak{h}}^{\times}) = \{1\}$ ). We denote by  $\mathcal{S}_k(\mathfrak{o}_F, \psi)$  the space of all  $\mathbf{C}$ -valued functions  $\mathbf{f}$  on  $G_{\mathfrak{A}}$  satisfying the following two conditions:

- (ii<sub>a</sub>)  $\mathbf{f}(s\alpha x w) = \psi(s)\mathbf{f}(x)$  for  $s \in F_{\mathfrak{A}}^{\times}$ ,  $\alpha \in G$ , and  $w \in W_{\mathfrak{h}}$  ( $x \in G_{\mathfrak{A}}$ ).
- (ii<sub>b</sub>) For every  $x \in G_{\mathfrak{h}}$ , there exists an element  $f_x$  of  $\tilde{\mathcal{S}}_k$  such that  $\mathbf{f}(x^{-t}u) = (f_x||_k u)(\mathbf{i})$  for all  $u \in G_{\mathfrak{a}+}$ , where  $\mathbf{i} = (\sqrt{-1}, \dots, \sqrt{-1}) \in H^{\mathfrak{a}}$ .

The elements of  $\mathcal{S}_k(\mathfrak{o}_F, \psi)$  are called (adelic) *Hilbert cusp forms of weight  $k$ , level  $\mathfrak{o}_F$ , and character  $\psi$* . We note that if  $\mathcal{S}_k(\mathfrak{o}_F, \psi) \neq \{0\}$ , then  $\psi_v(-1) = (-1)^{k_v}$  for all  $v \in \mathfrak{a}$ ; moreover,  $k_v > 0$  for all  $v \in \mathfrak{a}$  (cf. [Shimura 78, Proposition 1.1]).

Let  $R_{\mathbf{C}}(W, Y)$  be the free  $\mathbf{C}$ -module generated by the double cosets  $W \backslash Y / W$ . For  $WyW, WzW, WwW \in W \backslash Y / W$ , we take coset decompositions  $WyW = \bigsqcup_{i=1}^m Wy_i$  and  $WzW = \bigsqcup_{j=1}^n Wz_j$ , and set

$$m(WyW, WzW; WwW) = \#\{(i, j) \mid Wy_i z_j = Ww\}.$$

We then define the product  $(WyW)(WzW)$  by

$$(WyW)(WzW) = \sum_{WwW \in W \backslash Y / W} m(WyW, WzW; WwW) WwW.$$

Note that the above sum is finite. We extend this product  $\mathbf{C}$ -linearly on  $R_{\mathbf{C}}(W, Y)$ . Then  $R_{\mathbf{C}}(W, Y)$  becomes a  $\mathbf{C}$ -algebra, which is called the *Hecke algebra for  $W$  and  $Y$* .

For every  $y \in Y$ , we may assume that  $WyW = \bigsqcup_{i=1}^m Wy_i$  and  $(y_i)_a = 1$  ( $\in G_a$ ). For  $\mathbf{f} \in \mathcal{S}_k(\mathfrak{o}_F, \psi)$ , we define a function  $\mathbf{f}|WyW$  on  $G_A$  by

$$(\mathbf{f}|WyW)(x) = \sum_{i=1}^m \mathbf{f}(xy_i^t) \quad (x \in G_A).$$

Then, for  $s \in F_A^\times$ ,  $\alpha \in G$ ,  $w \in W_h$ , and  $x \in G_A$ , we have  $(\mathbf{f}|WyW)(s\alpha xw) = \psi(s) \sum_{i=1}^m \mathbf{f}(x(y_i w^t)^\iota) = \psi(s)(\mathbf{f}|WyW)(x)$ ; moreover, for  $x \in G_h$ , we have

$$\begin{aligned} (\mathbf{f}|WyW)(x^{-\iota}u) &= \sum_{i=1}^m \mathbf{f}((xy_i^{-1})^{-\iota}u) \\ &= \left( \sum_{i=1}^m (f_{xy_i^{-1}}) \|k u\right) (\mathbf{i}) \end{aligned}$$

for all  $u \in G_{a+}$ , where  $f_{xy_i^{-1}}$  is as in (ii<sub>b</sub>). Thus  $\mathbf{f}|WyW \in \mathcal{S}_k(\mathfrak{o}_F, \psi)$ . Extending this action  $\mathbf{C}$ -linearly to the whole of  $R_{\mathbf{C}}(W, Y)$ , we have a ring homomorphism  $\phi$  of  $R_{\mathbf{C}}(W, Y)$  into the  $\mathbf{C}$ -linear endomorphism algebra  $\text{End}_{\mathbf{C}}(\mathcal{S}_k(\mathfrak{o}_F, \psi))$ . We call an element of  $\phi(R_{\mathbf{C}}(W, Y))$  a *Hecke operator*.

We now determine the generators of  $R_{\mathbf{C}}(W, Y)$ . For each integral ideal  $\mathfrak{a}$  of  $F$ , we define elements  $T(\mathfrak{a})$  and  $S(\mathfrak{a})$  of  $R_{\mathbf{C}}(W, Y)$  by

$$T(\mathfrak{a}) = \sum_{\substack{WyW \in W \backslash Y / W \\ \det(y)_{\mathfrak{o}_F} = \mathfrak{a}}} WyW, \quad S(\mathfrak{a}) = W \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} W,$$

where  $a = (\pi_{\mathfrak{p}}^{\text{ord}_{\mathfrak{p}}(\mathfrak{a})})_{\mathfrak{p} \in \mathbf{h}} \in F_{\mathbf{h}}^\times$  ( $\subset F_A^\times$ ). Now we set  $T(\pi_{\mathfrak{p}}^l, \pi_{\mathfrak{p}}^{l'}) = W \begin{pmatrix} \pi_{\mathfrak{p}}^l & 0 \\ 0 & \pi_{\mathfrak{p}}^{l'} \end{pmatrix} W$  for  $l, l' \in \mathbf{Z}$ . (Note that  $\pi_{\mathfrak{p}} \in F_{\mathfrak{p}}^\times$  ( $\subset F_A^\times$ )). For  $y, z \in Y$ , we have

$$\begin{aligned} (WyW)(WzW) &= WyzW \\ \text{if } \gcd(\det(y)_{\mathfrak{o}_F}, \det(z)_{\mathfrak{o}_F}) &= \mathfrak{o}_F. \end{aligned} \quad (2-1)$$

Thus we have

$$T(\mathfrak{a}) = \prod_{\mathfrak{p}|\mathfrak{a}} \left( \sum_{l_{\mathfrak{p}}=0}^{[\text{ord}_{\mathfrak{p}}(\mathfrak{a})/2]} T(\pi_{\mathfrak{p}}^{l_{\mathfrak{p}}}, \pi_{\mathfrak{p}}^{\text{ord}_{\mathfrak{p}}(\mathfrak{a})-l_{\mathfrak{p}}}) \right),$$

and hence

$$T(\mathfrak{a}\mathfrak{b}) = T(\mathfrak{a})T(\mathfrak{b}) \quad \text{if } \gcd(\mathfrak{a}, \mathfrak{b}) = \mathfrak{o}_F. \quad (2-2)$$

For any integer  $e \geq 0$ , we have

$$T(1, \pi_{\mathfrak{p}}^e) = \bigsqcup_{f=0}^e \bigsqcup_{\substack{1 \leq j \leq N(\mathfrak{p}^f) \\ \gcd(m_{fj}, \pi_{\mathfrak{p}}^f, \pi_{\mathfrak{p}}^{e-f})=1}} W \begin{pmatrix} \pi_{\mathfrak{p}}^{e-f} & m_{fj} \delta_{\mathfrak{p}}^{-1} \\ 0 & \pi_{\mathfrak{p}}^f \end{pmatrix},$$

where  $\{m_{fj}\}_{j=1}^{N(\mathfrak{p}^f)}$  is a complete set of representatives of  $\mathfrak{o}_{\mathfrak{p}}/\pi_{\mathfrak{p}}^f \mathfrak{o}_{\mathfrak{p}}$ . Moreover, for  $l, m, n \geq 0$ , we have

$$T(\pi_{\mathfrak{p}}^l, \pi_{\mathfrak{p}}^l)T(\pi_{\mathfrak{p}}^m, \pi_{\mathfrak{p}}^n) = T(\pi_{\mathfrak{p}}^{l+m}, \pi_{\mathfrak{p}}^{l+n}). \quad (2-3)$$

Thus

$$\begin{aligned} T(1, \pi_{\mathfrak{p}})T(1, \pi_{\mathfrak{p}}^e) &= \begin{cases} T(1, \pi_{\mathfrak{p}}^{e+1}) + N(\mathfrak{p})T(\pi_{\mathfrak{p}}, \pi_{\mathfrak{p}})T(1, \pi_{\mathfrak{p}})^{e-1} & \text{if } e \geq 2, \\ T(1, \pi_{\mathfrak{p}}^2) + (N(\mathfrak{p}) + 1)T(\pi_{\mathfrak{p}}, \pi_{\mathfrak{p}}) & \text{if } e = 1. \end{cases} \end{aligned} \quad (2-4)$$

Therefore, we have

$$\begin{aligned} T(\mathfrak{p})T(\mathfrak{p}^e) &= T(\mathfrak{p}^{e+1}) \\ &\quad + N(\mathfrak{p})S(\mathfrak{p})T(\mathfrak{p}^{e-1}) \quad \text{for } \mathfrak{p} \in \mathbf{h} \text{ and } e \geq 1. \end{aligned} \quad (2-5)$$

From (2-1), (2-3), and (2-4), we see that  $R_{\mathbf{C}}(W, Y)$  is the commutative  $\mathbf{C}$ -algebra generated by  $T(\mathfrak{p})$  and  $S(\mathfrak{p})$  for all prime ideals  $\mathfrak{p}$  of  $F$ . We also denote by  $T(\mathfrak{a})$  the image  $\phi(T(\mathfrak{a}))$  in  $\text{End}_{\mathbf{C}}(\mathcal{S}_k(\mathfrak{o}_F, \psi))$ .

An element  $\mathbf{f}$  of  $\mathcal{S}_k(\mathfrak{o}_F, \psi)$  is called a *primitive form* if  $\mathbf{f}$  is a normalized common eigenfunction of  $T(\mathfrak{p})$  for all prime ideals  $\mathfrak{p}$ . Here *normalized* means that the coefficient  $c(1)$  of the Fourier expansion  $f_x(z) = \sum_{\xi} c(\xi)e_F(\xi z)$  for  $x = 1_2$  ( $\in G_h$ ) is equal to 1, where  $f_x$  is as in (ii<sub>b</sub>). (Cf. [Shimura 78, p. 650].)

## 2.2 The Trace Formula

It is known that the characteristic polynomial of a Hecke operator can be obtained immediately from traces of Hecke operators by using (2-2), (2-5), and Newton's identities ([Miyake 89, pp. 266-267]). In particular if we take a prime ideal  $\mathfrak{p}$  of  $F$ , we can obtain the characteristic polynomial  $X^r + a_1 X^{r-1} + \dots + a_{r-1} X + a_r$  of  $T(\mathfrak{p})$  as follows:

Let  $c_1, \dots, c_r$  be the eigenvalues of  $T(\mathfrak{p})$ , and set  $b_l = c_1^l + \dots + c_r^l = \text{tr}(T(\mathfrak{p})^l)$ . Then by (2-5), we have

$$\text{tr}(T(\mathfrak{p})^l) = \sum_{i=0}^{[l/2]} \left( \binom{l}{i} - \binom{l}{i-1} \right) N(\mathfrak{p})^i \psi(\pi_{\mathfrak{p}})^i \text{tr} T(\mathfrak{p}^{l-2i})$$

for  $l = 1, \dots, r$ , where  $\binom{l}{-1} = 0$ . Therefore, we can obtain  $b_l$  from  $\text{tr} T(\mathfrak{p}^{l-2i})$  ( $i = 0, \dots, [l/2]$ ). By Newton's formula, we have

$$b_l + b_{l-1}a_1 + b_{l-2}a_2 + \dots + b_1 a_{l-1} + l a_l = 0$$

for  $l = 1, \dots, r$ . Thus we can obtain  $a_1, \dots, a_r$  from  $b_1, \dots, b_r$ .

Now we describe the trace formula of a Hecke operator  $T(\mathfrak{a})$  on  $\mathcal{S}_k(\mathfrak{o}_F, \psi)$  given by [Saito 84, Theorem 2.1]. But first, we introduce the following notation.

Let  $K$  be a quadratic extension of  $F$ . We denote by  $\mathcal{O}_{K/F}$  the set of all orders in  $K$  containing  $\mathfrak{o}_F$ . Let  $\Lambda \in \mathcal{O}_{K/F}$ . Since  $\Lambda$  is an  $F$ -lattice, we can take  $x_1, x_2 \in K$  and  $\mathfrak{a}_1, \mathfrak{a}_2 \in I(F)$  such that  $\Lambda = \mathfrak{a}_1 x_1 + \mathfrak{a}_2 x_2$ . Then we define the integral ideal  $D_{K/F}(\Lambda)$  of  $F$  by

$$D_{K/F}(\Lambda) = (\mathfrak{a}_1 \mathfrak{a}_2)^2 \begin{vmatrix} x_1^{(1)} & x_2^{(1)} \\ x_1^{(2)} & x_2^{(2)} \end{vmatrix}^2,$$

where  $x_j^{(1)}, x_j^{(2)}$  are the conjugates of  $x_j$  over  $F$ . We call  $D_{K/F}(\Lambda)$  the relative discriminant of  $\Lambda$  with respect to  $K/F$ .

**Theorem 2.1.** *Let  $F (\neq \mathbf{Q})$  be a totally real algebraic number field of degree  $g$ ,  $\psi$  a Hecke character of  $F$  of finite order such that the nonarchimedean part of its conductor is equal to  $\mathfrak{o}_F$ , and  $k = (k_1, \dots, k_g) \in \mathbf{Z}^{\mathbf{a}}$  such that  $k_j \geq 2$  and  $\psi_{v_j}(-1) = (-1)^{k_j}$  for each  $v_j \in \mathbf{a}$ . For every element  $\mathfrak{b}P(F) \in \text{Cl}(F)$ , we define a mapping  $\eta$  of  $\text{Cl}(F)$  into  $\text{Cl}^+(F)$  by  $\eta(\mathfrak{b}P(F)) = \mathfrak{b}^2 P^+(F)$ . Then, for any integral ideal  $\mathfrak{a}$  of  $F$ , we have*

$$\begin{aligned} \text{tr } T(\mathfrak{a}) &= \varepsilon(\mathfrak{a}) \delta(\mathfrak{a}) \frac{2\zeta_F(2) |D_F|^{3/2}}{(2\pi)^{2g}} \psi \left( \left( \pi_{\mathfrak{p}}^{\text{ord}_{\mathfrak{p}}(\mathfrak{a})/2} \right)_{\mathfrak{p} \in \mathbf{h}} \right) \\ &\cdot \left( \prod_{j=1}^g (k_j - 1) \right) + \varepsilon(\mathfrak{a}) (-1)^{g-1} \\ &\cdot \sum_{\mathfrak{m} \in M_{\mathfrak{a}}} \psi \left( \left( \pi_{\mathfrak{p}}^{\text{ord}_{\mathfrak{p}}(\mathfrak{m})} \right)_{\mathfrak{p} \in \mathbf{h}} \right)^{-1} \\ &\cdot \sum_{n \in N_{\mathfrak{m}}} \sum_{s \in S_n} \left( \prod_{j=1}^g \Phi(s_j, n_j, k_j) \right) \sum_{\Lambda \in R_{sn}} \frac{h(\Lambda)}{h_F[\Lambda^{\times} : \mathfrak{o}_F^{\times}]} \\ &+ (-1)^{g-1} b(k) \sum_{\lambda \in C(\psi)} \lambda \left( \left( \pi_{\mathfrak{p}}^{\text{ord}_{\mathfrak{p}}(\mathfrak{a})} \right)_{\mathfrak{p} \in \mathbf{h}} \right) \sum_{\substack{\mathfrak{b} | \mathfrak{a} \\ \mathfrak{b} \subset \mathfrak{o}_F \\ \mathfrak{b} \in I(F)}} N(\mathfrak{b}). \end{aligned} \tag{2-6}$$

Here

- $\varepsilon(\mathfrak{a}) = 1$  or  $0$  depending on whether  $\mathfrak{a}P^+(F) \in \eta(\text{Cl}(F))$  or not;
- $\delta(\mathfrak{a}) = 1$  or  $0$  depending on whether  $\mathfrak{a}$  is a square or not;
- $M_{\mathfrak{a}} = \{\mathfrak{m}\}$  is the set of all representatives of  $\{\mathfrak{m}P(F) \in \text{Cl}(F) \mid \mathfrak{m}^2 \mathfrak{a} \in P^+(F)\}$  such that  $\mathfrak{m} \subset \mathfrak{o}_F$  and  $\text{gcd}(\mathfrak{m}, \mathfrak{a}) = \mathfrak{o}_F$ ;

- for every  $\mathfrak{m} \in M_{\mathfrak{a}}$ , we take an element  $n_{\mathfrak{m}}$  of  $\mathfrak{o}_F$  such that  $(n_{\mathfrak{m}})_F = \mathfrak{m}^2 \mathfrak{a}$  and  $n_{\mathfrak{m}} \gg 0$ , and we set  $N_{\mathfrak{m}} = n_{\mathfrak{m}} E_F$ , where  $E_F$  is a complete set of representatives of  $\mathfrak{o}_{F^+}^{\times} / (\mathfrak{o}_F^{\times})^2$ ;
- for  $n \in N_{\mathfrak{m}}$ , we set  $S_n = \{s \in \mathfrak{m} \mid s^2 - 4n \ll 0\}$ ;
- let  $s_j, n_j$  be the  $v_j$ -components of  $s, n$  in  $F_{\mathbf{a}}$ , and  $\alpha_j, \beta_j$  the roots of  $X^2 - s_j X + n_j$ ; then we set 
$$\Phi(s_j, n_j, k_j) = \frac{\alpha_j^{k_j-1} - \beta_j^{k_j-1}}{\alpha_j - \beta_j} n_j^{-(k_j-2)/2};$$
- $K_{sn} = F(\sqrt{s^2 - 4n})$ , and  $R_{sn}$  is the set of all distinct orders  $\Lambda$  in  $\mathcal{O}_{K_{sn}/F}$  satisfying  $D_{K_{sn}/F}(\Lambda) \mid (s^2 - 4n)_F \mathfrak{m}^{-2}$ ;
- $h(\Lambda)$  is the class number of  $\Lambda$ ; that is,  $h(\Lambda) = |(K_{sn} \otimes_F F_{\mathbf{h}})^{\times} / K_{sn}^{\times} \prod_{\mathfrak{p} \in \mathbf{h}} \Lambda_{\mathfrak{p}}^{\times}|$ , where  $\Lambda_{\mathfrak{p}}$  is the topological closure of  $\Lambda$  in  $K_{sn} \otimes_F F_{\mathfrak{p}}$ ;
- $b(k) = 1$  or  $0$  depending on whether  $k = (2, \dots, 2)$  or not;
- $C(\psi)$  is the set of all unramified Hecke characters  $\lambda$  of  $F$  such that  $\lambda^2 = \psi$ .

Note that the second sum of the right-hand side of (2-6) is independent of the choice of  $M_{\mathfrak{a}}$ ,  $n_{\mathfrak{m}}$ , and  $E_F$ . We remark also that (2-6) is shortened and corrected from the original formula which appeared in [Saito 84].

### 2.3 Preliminary Lemmas

We now present five lemmas for transforming (2-6) into a more computable form.

**Lemma 2.2.** *Let  $F$  be an algebraic number field of finite degree, and  $K$  a quadratic extension of  $F$ . For an integral ideal  $\mathfrak{c}$  of  $F$ , we put  $\rho(\mathfrak{c}) = \mathfrak{o}_F + \mathfrak{c} \mathfrak{o}_K$ . Then  $\rho$  is a bijection of the set of all integral ideals of  $F$  onto  $\mathcal{O}_{K/F}$ .*

*Proof:* This result follows immediately from [Shimura 71, Proposition 4.11] when  $F = \mathbf{Q}$ , and we prove our assertion in a similar fashion. It is well known that there exist  $\theta \in K$  and  $\mathfrak{a} \in I(F)$  such that  $\mathfrak{o}_K = \mathfrak{o}_F + \theta \mathfrak{a}$ . Let  $\mathfrak{c}$  be an integral ideal of  $F$ . Since  $\mathfrak{c} \mathfrak{o}_K \subset \mathfrak{o}_F + \mathfrak{c} \mathfrak{o}_K \subset \mathfrak{o}_K$ , we see that  $\mathfrak{o}_F + \mathfrak{c} \mathfrak{o}_K$  is a  $\mathbf{Q}$ -lattice in  $K$ . Moreover,  $\mathfrak{o}_F + \mathfrak{c} \mathfrak{o}_K$  is a subring of  $K$  containing  $\mathfrak{o}_F$ . Thus  $\mathfrak{o}_F + \mathfrak{c} \mathfrak{o}_K \in \mathcal{O}_{K/F}$ , and hence  $\rho$  is a mapping. If  $\mathfrak{o}_F + \mathfrak{c} \mathfrak{o}_K = \mathfrak{o}_F + \mathfrak{c}' \mathfrak{o}_K$  with integral ideals  $\mathfrak{c}, \mathfrak{c}'$  of  $F$ , then  $\mathfrak{o}_F + \theta \mathfrak{a} \mathfrak{c} = \mathfrak{o}_F + \mathfrak{c} \mathfrak{o}_K = \mathfrak{o}_F + \mathfrak{c}' \mathfrak{o}_K = \mathfrak{o}_F + \theta \mathfrak{a} \mathfrak{c}'$ . Since  $\{1, \theta\}$  is a basis of  $K$  over  $F$ , we have  $\mathfrak{c} = \mathfrak{c}'$ . Thus  $\rho$  is injective. Let  $\Lambda$  be any order in  $\mathcal{O}_{K/F}$ . Since  $\mathfrak{o}_K$  is the unique maximal order of  $K$ , we have  $\Lambda \subset \mathfrak{o}_K$ . Set  $\mathfrak{b} = \{\mathfrak{c} \in \mathfrak{a} \mid \theta \mathfrak{c} \in \Lambda\}$ . Since

$\mathfrak{o}_F \subsetneq \Lambda \subset \mathfrak{o}_K = \mathfrak{o}_F + \theta\mathfrak{a}$ , we have  $\{0\} \subsetneq \mathfrak{b} \subset \mathfrak{a}$ . Moreover,  $\mathfrak{b}$  is an  $\mathfrak{o}_F$ -module. Thus  $\mathfrak{b} \in I(F)$ . For any  $x \in \Lambda$ , we have  $x = r + \theta s$  with  $r \in \mathfrak{o}_F$  and  $s \in \mathfrak{a}$ , since  $\Lambda \subset \mathfrak{o}_K$ . Then  $\theta s = x - r \in \Lambda$ , and hence  $s \in \mathfrak{b}$ . Therefore,  $\Lambda = \mathfrak{o}_F + \theta\mathfrak{b}$ . Now we set  $\mathfrak{c} = \mathfrak{b}\mathfrak{a}^{-1}$ . Then  $\mathfrak{c}$  is an integral ideal of  $F$ , and  $\Lambda = \mathfrak{o}_F + \theta\mathfrak{b} = \mathfrak{o}_F + \theta\mathfrak{a}\mathfrak{c} = \mathfrak{o}_F + \mathfrak{c}\mathfrak{o}_K$ . Thus  $\rho$  is surjective.  $\square$

We denote the mapping  $\rho^{-1}$  by  $c$ , and we call  $c(\Lambda)$  the conductor of  $\Lambda$  for  $\Lambda \in \mathcal{O}_{K/F}$ .

**Lemma 2.3.** *Let  $F$  and  $K$  be as in Lemma 2.2. Then for  $\Lambda \in \mathcal{O}_{K/F}$ , we have*

$$D_{K/F}(\Lambda) \cdot D_{K/F}^{-1} = c(\Lambda)^2.$$

*Proof:* By Lemma 2.2, we have  $\mathfrak{o}_K = \mathfrak{o}_F + \theta\mathfrak{a}$  and  $\Lambda = \mathfrak{o}_F + \theta\mathfrak{a}c(\Lambda)$  with  $\theta \in K$  and  $\mathfrak{a} \in I(F)$ . Now let  $\theta^{(1)}, \theta^{(2)}$  be the conjugates of  $\theta$  over  $F$ . Then we have  $D_{K/F} = D_{K/F}(\mathfrak{o}_K) = \mathfrak{a}^2(\theta^{(2)} - \theta^{(1)})^2$  and  $D_{K/F}(\Lambda) = (\mathfrak{a}c(\Lambda))^2(\theta^{(2)} - \theta^{(1)})^2$ .  $\square$

Let  $F$  be an algebraic number field of finite degree, and  $K$  a quadratic extension of  $F$ . For  $\mathfrak{p} \in \mathfrak{h}$ , we define

$$\left(\frac{K}{\mathfrak{p}}\right) = \begin{cases} 1 & \text{if } \mathfrak{p} \text{ splits in } K, \\ -1 & \text{if } \mathfrak{p} \text{ remains prime in } K, \\ 0 & \text{if } \mathfrak{p} \text{ ramifies in } K. \end{cases}$$

**Lemma 2.4.** *Let  $F$  be a totally real algebraic number field of finite degree, and  $K$  a totally imaginary quadratic extension of  $F$ . Then for  $\Lambda \in \mathcal{O}_{K/F}$ , we have*

$$h(\Lambda) = h_K[\mathfrak{o}_K^\times : \Lambda^\times]^{-1} N(c(\Lambda)) \prod_{\substack{\mathfrak{p}|c(\Lambda) \\ \mathfrak{p} \in \mathfrak{h}}} \left(1 - \left(\frac{K}{\mathfrak{p}}\right)N(\mathfrak{p})^{-1}\right).$$

*Proof:* This can be proved in exactly the same way as in [Miyake 89, Theorem 6.7.2], which deals with the case  $F = \mathbf{Q}$ . For any lattice  $L$  in  $K$  and  $\mathfrak{p} \in \mathfrak{h}$ , we write  $L_{\mathfrak{p}}$  for the topological closure of  $L$  in  $K \otimes_F F_{\mathfrak{p}}$ . For  $\Lambda \in \mathcal{O}_{K/F}$ , we have

$$\begin{aligned} h(\Lambda) &= \left| (K \otimes_F F_{\mathfrak{h}})^\times / K^\times \prod_{\mathfrak{p} \in \mathfrak{h}} \Lambda_{\mathfrak{p}}^\times \right| \\ &= \left| (K \otimes_F F_{\mathfrak{h}})^\times / K^\times \prod_{\mathfrak{p} \in \mathfrak{h}} (\mathfrak{o}_K)_{\mathfrak{p}}^\times \right| \\ &\quad \cdot \left| K^\times \prod_{\mathfrak{p} \in \mathfrak{h}} (\mathfrak{o}_K)_{\mathfrak{p}}^\times / K^\times \prod_{\mathfrak{p} \in \mathfrak{h}} \Lambda_{\mathfrak{p}}^\times \right|. \end{aligned}$$

Generally for an abelian group  $G$  and subgroups  $H, I$ , and  $J$  satisfying  $I \supset J$ , the sequence

$$1 \rightarrow (H \cap I)/(H \cap J) \rightarrow I/J \rightarrow HI/HJ \rightarrow 1$$

is exact. Thus

$$\begin{aligned} h(\Lambda) &= h_K \cdot \left| \prod_{\mathfrak{p} \in \mathfrak{h}} (\mathfrak{o}_K)_{\mathfrak{p}}^\times / \prod_{\mathfrak{p} \in \mathfrak{h}} \Lambda_{\mathfrak{p}}^\times \right| \\ &\quad \cdot \left| (K^\times \cap \prod_{\mathfrak{p} \in \mathfrak{h}} (\mathfrak{o}_K)_{\mathfrak{p}}^\times) / (K^\times \cap \prod_{\mathfrak{p} \in \mathfrak{h}} \Lambda_{\mathfrak{p}}^\times) \right|^{-1} \\ &= h_K \cdot \left( \prod_{\mathfrak{p} \in \mathfrak{h}} |(\mathfrak{o}_K)_{\mathfrak{p}}^\times / \Lambda_{\mathfrak{p}}^\times| \right) \cdot |\mathfrak{o}_K^\times / \Lambda^\times|^{-1}. \end{aligned}$$

Since  $(\mathfrak{o}_K)_{\mathfrak{p}} \neq \Lambda_{\mathfrak{p}}$  if and only if  $\mathfrak{p} | c(\Lambda)$ , we need to show only that

$$|(\mathfrak{o}_K)_{\mathfrak{p}}^\times / \Lambda_{\mathfrak{p}}^\times| = N(c(\Lambda)_{\mathfrak{p}}) \left(1 - \left(\frac{K}{\mathfrak{p}}\right)N(\mathfrak{p})^{-1}\right) \quad (2-7)$$

for  $(\mathfrak{o}_K)_{\mathfrak{p}} \neq \Lambda_{\mathfrak{p}}$ . We denote an element  $\alpha \otimes \beta$  of  $K \otimes_F F_{\mathfrak{p}}$  simply by  $\alpha\beta$ . Let  $\mathfrak{p}$  satisfy  $(\mathfrak{o}_K)_{\mathfrak{p}} \neq \Lambda_{\mathfrak{p}}$ . Assume first that  $\mathfrak{p}$  splits in  $K$ . Set  $\mathfrak{o}_K = \mathfrak{o}_F + \theta\mathfrak{a}$  with  $\theta \in K$  and  $\mathfrak{a} \in I(F)$ , and take  $\alpha_{\mathfrak{p}} \in F_{\mathfrak{p}}$  such that  $\alpha_{\mathfrak{p}}\mathfrak{o}_{\mathfrak{p}} = \mathfrak{a}_{\mathfrak{p}}$ . Let  $f$  be the minimal polynomial of  $\theta$  over  $F$ , and let  $\theta_1, \theta_2$  be the two roots of  $f$  in  $F_{\mathfrak{p}}$ . For  $a, b \in F_{\mathfrak{p}}$ , we set  $\tau(a + b\alpha_{\mathfrak{p}}\theta) = (a + b\alpha_{\mathfrak{p}}\theta_1, a + b\alpha_{\mathfrak{p}}\theta_2)$ . Then  $\tau$  is a topological  $F_{\mathfrak{p}}$ -algebra isomorphism of  $K \otimes_F F_{\mathfrak{p}}$  onto  $F_{\mathfrak{p}} \times F_{\mathfrak{p}}$ . (cf. [Weil 67, Chapter III, Theorem 4]). Since  $(\alpha_{\mathfrak{p}}(\theta_2 - \theta_1))^2\mathfrak{o}_{\mathfrak{p}} = (D_{K/F})_{\mathfrak{p}} = \mathfrak{o}_{\mathfrak{p}}$ , we have  $\tau((\mathfrak{o}_K)_{\mathfrak{p}}) = \mathfrak{o}_{\mathfrak{p}} \times \mathfrak{o}_{\mathfrak{p}}$  and  $\tau(\Lambda_{\mathfrak{p}}) = \{(\alpha, \beta) \in \mathfrak{o}_{\mathfrak{p}} \times \mathfrak{o}_{\mathfrak{p}} \mid \alpha - \beta \in c(\Lambda)_{\mathfrak{p}}\}$ . Hence  $\tau(\Lambda_{\mathfrak{p}})^\times = \{(\alpha, \beta) \in \mathfrak{o}_{\mathfrak{p}}^\times \times \mathfrak{o}_{\mathfrak{p}}^\times \mid \alpha - \beta \in c(\Lambda)_{\mathfrak{p}}\}$ . For  $(\alpha, \beta) \in \mathfrak{o}_{\mathfrak{p}}^\times \times \mathfrak{o}_{\mathfrak{p}}^\times$ , we set  $\rho((\alpha, \beta)) = \alpha\beta^{-1}(1 + c(\Lambda)_{\mathfrak{p}})$ . Then  $\rho$  is a group homomorphism of  $\mathfrak{o}_{\mathfrak{p}}^\times \times \mathfrak{o}_{\mathfrak{p}}^\times$  onto  $\mathfrak{o}_{\mathfrak{p}}^\times/(1 + c(\Lambda)_{\mathfrak{p}})$ . Since  $\text{Ker}(\rho) = \tau(\Lambda_{\mathfrak{p}})^\times$ , we have  $\tau((\mathfrak{o}_K)_{\mathfrak{p}}^\times)/\tau(\Lambda_{\mathfrak{p}}^\times) = (\mathfrak{o}_{\mathfrak{p}}^\times \times \mathfrak{o}_{\mathfrak{p}}^\times)/\tau(\Lambda_{\mathfrak{p}})^\times \cong \mathfrak{o}_{\mathfrak{p}}^\times/(1 + c(\Lambda)_{\mathfrak{p}})$ . Therefore,

$$|(\mathfrak{o}_K)_{\mathfrak{p}}^\times / \Lambda_{\mathfrak{p}}^\times| = |\mathfrak{o}_{\mathfrak{p}}^\times / (1 + c(\Lambda)_{\mathfrak{p}})| = N(c(\Lambda)_{\mathfrak{p}})(1 - N(\mathfrak{p})^{-1}).$$

Thus we obtain (2-7) in this case. Now assume that  $\mathfrak{p}$  remains prime or ramifies in  $K$ . Then  $K \otimes_F F_{\mathfrak{p}}$  is a field. For  $\beta \in \mathfrak{o}_{\mathfrak{p}}^\times$  and  $\gamma \in (\mathfrak{o}_K)_{\mathfrak{p}}^\times$ , we set  $\mu_1(\beta(1 + c(\Lambda)_{\mathfrak{p}})) = \beta(1 + c(\Lambda)_{\mathfrak{p}})(\mathfrak{o}_K)_{\mathfrak{p}}$  and  $\mu_2(\gamma(1 + c(\Lambda)_{\mathfrak{p}})(\mathfrak{o}_K)_{\mathfrak{p}}) = \gamma\Lambda_{\mathfrak{p}}^\times$ . Since  $(1 + c(\Lambda)_{\mathfrak{p}})(\mathfrak{o}_K)_{\mathfrak{p}} \cap \mathfrak{o}_{\mathfrak{p}}^\times = (1 + c(\Lambda)_{\mathfrak{p}} + \theta c(\Lambda)_{\mathfrak{p}}\mathfrak{a}_{\mathfrak{p}}) \cap \mathfrak{o}_{\mathfrak{p}}^\times = 1 + c(\Lambda)_{\mathfrak{p}}$  and  $\Lambda_{\mathfrak{p}}^\times = \mathfrak{o}_{\mathfrak{p}}^\times + c(\Lambda)_{\mathfrak{p}}(\mathfrak{o}_K)_{\mathfrak{p}} = \mathfrak{o}_{\mathfrak{p}}^\times(1 + c(\Lambda)_{\mathfrak{p}}(\mathfrak{o}_K)_{\mathfrak{p}})$ , the sequence

$$\begin{aligned} 1 \rightarrow \mathfrak{o}_{\mathfrak{p}}^\times / (1 + c(\Lambda)_{\mathfrak{p}}) &\xrightarrow{\mu_1} (\mathfrak{o}_K)_{\mathfrak{p}}^\times / (1 + c(\Lambda)_{\mathfrak{p}}(\mathfrak{o}_K)_{\mathfrak{p}}) \\ &\xrightarrow{\mu_2} (\mathfrak{o}_K)_{\mathfrak{p}}^\times / \Lambda_{\mathfrak{p}}^\times \rightarrow 1 \end{aligned}$$

is exact. Therefore,

$$|(\mathfrak{o}_K)_{\mathfrak{p}}^\times / \Lambda_{\mathfrak{p}}^\times| = |(\mathfrak{o}_K)_{\mathfrak{p}}^\times / (1 + c(\Lambda)_{\mathfrak{p}}(\mathfrak{o}_K)_{\mathfrak{p}})| \cdot |\mathfrak{o}_{\mathfrak{p}}^\times / (1 + c(\Lambda)_{\mathfrak{p}})|^{-1}.$$

Here we have

$$\begin{aligned} |(\mathfrak{o}_K)_{\mathfrak{p}}^\times / (1 + c(\Lambda)_{\mathfrak{p}}(\mathfrak{o}_K)_{\mathfrak{p}})| &= |((\mathfrak{o}_K)_{\mathfrak{p}}/c(\Lambda)_{\mathfrak{p}}(\mathfrak{o}_K)_{\mathfrak{p}})^\times| \\ &= \begin{cases} N(c(\Lambda)_{\mathfrak{p}})^2(1 - N(\mathfrak{p})^{-2}) & \text{if } \mathfrak{p} \text{ remains prime in } K, \\ N(c(\Lambda)_{\mathfrak{p}})^2(1 - N(\mathfrak{p})^{-1}) & \text{if } \mathfrak{p} \text{ ramifies in } K, \end{cases} \end{aligned}$$

and  $|\mathfrak{o}_{\mathfrak{p}}^{\times}/(1 + c(\Lambda)_{\mathfrak{p}})| = |(\mathfrak{o}_{\mathfrak{p}}/c(\Lambda)_{\mathfrak{p}})^{\times}| = N(c(\Lambda)_{\mathfrak{p}})(1 - N(\mathfrak{p})^{-1})$ , which proves (2-7) in this case.  $\square$

**Lemma 2.5.** *Let  $F$  and  $K$  be as in Lemma 2.4. Let  $g$  be the degree of  $F$  over  $\mathbf{Q}$ . Let  $\chi_{K/F}$  be the ideal character corresponding to the extension  $K/F$  (by means of class field theory). Then*

$$L_F(0, \chi_{K/F}) = 2^{g-1} \frac{h_K}{h_F [\mathfrak{o}_K^{\times} : \mathfrak{o}_F^{\times}]},$$

where  $L_F(s, \chi_{K/F})$  is the Hecke  $L$ -function associated with  $\chi_{K/F}$ .

*Proof:* Let  $W_K$  (respectively  $W_F$ ) be the group of the roots of 1 in  $K$  (respectively  $F$ ), and  $R_K$  (respectively  $R_F$ ) the regulator of  $K$  (respectively  $F$ ). Set  $w_K = |W_K|$  and  $w_F = |W_F|$ . Let  $Z_K(s) = ((2\pi)^{1-s} \Gamma(s))^g \zeta_K(s)$  and  $Z_F(s) = (\pi^{-s/2} \Gamma(s/2))^g \zeta_F(s)$ . Then we have  $\text{Res}_{s=0} Z_K(s) = -(2\pi)^g h_K R_K w_K^{-1}$  and  $\text{Res}_{s=0} Z_F(s) = -2^g h_F R_F w_F^{-1}$ . By  $\zeta_K(s) = \zeta_F(s) L_F(s, \chi_{K/F})$ , we have  $Z_K(s) = \pi^{g(1-s)/2} \Gamma((s+1)/2)^g Z_F(s) L_F(s, \chi_{K/F})$ , and hence  $\text{Res}_{s=0} Z_K(s) = \pi^g \text{Res}_{s=0} Z_F(s) \cdot L_F(0, \chi_{K/F})$ . Therefore,

$$L_F(0, \chi_{K/F}) = \frac{h_K R_K w_K^{-1}}{h_F R_F w_F^{-1}}.$$

Thus we need to show that

$$[\mathfrak{o}_K^{\times} : \mathfrak{o}_F^{\times}] = 2^{g-1} w_K w_F^{-1} R_K^{-1} R_F. \tag{2-8}$$

Let  $l$  be the mapping from  $\mathfrak{o}_K^{\times}$  to  $\mathbf{R}^g$  defined by  $l(\delta) = (\log |\delta^{(1)}|, \dots, \log |\delta^{(g)}|)$ , where  $\delta^{(1)}, \dots, \delta^{(g)}$  are the conjugates of  $\delta$  over  $F$ . Then  $\mathfrak{o}_K^{\times}/W_K \mathfrak{o}_F^{\times} \cong l(\mathfrak{o}_K^{\times})/l(\mathfrak{o}_F^{\times})$ . Since  $[l(\mathfrak{o}_K^{\times}) : l(\mathfrak{o}_F^{\times})] = 2^{g-1} R_K^{-1} R_F$ , we have  $[\mathfrak{o}_K^{\times} : W_K \mathfrak{o}_F^{\times}] = 2^{g-1} R_K^{-1} R_F$ . On the other hand, we have  $[W_K \mathfrak{o}_F^{\times} : \mathfrak{o}_F^{\times}] = w_F^{-1} w_K$ . Thus we obtain (2-8).  $\square$

**Lemma 2.6.** *Let  $F$  and  $K$  be as in Lemma 2.4. Then, for any integral ideal  $\mathfrak{f}$  of  $F$ , we have*

$$\begin{aligned} & \sum_{\substack{c|f \\ c \subset \mathfrak{o}_F \\ c \in I(F)}} \left( N(c) \prod_{\substack{p|c \\ p \in \mathfrak{h}}} \left( 1 - \left(\frac{K}{p}\right) N(p)^{-1} \right) \right) \\ &= \left( \prod_{\substack{p|f \\ \left(\frac{K}{p}\right) = -1 \\ p \in \mathfrak{h}}} \frac{N(p)^{\text{ord}_p(\mathfrak{f})+1} + N(p)^{\text{ord}_p(\mathfrak{f})} - 2}{N(p) - 1} \right) \\ & \cdot \left( \prod_{\substack{p|f \\ \left(\frac{K}{p}\right) = 1 \\ p \in \mathfrak{h}}} N(p)^{\text{ord}_p(\mathfrak{f})} \right) \left( \prod_{\substack{p|f \\ \left(\frac{K}{p}\right) = 0 \\ p \in \mathfrak{h}}} \frac{N(p)^{\text{ord}_p(\mathfrak{f})+1} - 1}{N(p) - 1} \right). \end{aligned}$$

*Proof:* For every prime ideal  $\mathfrak{p}$  of  $F$  and  $0 \leq s \in \mathbf{Z}$ , we set

$$\varphi(\mathfrak{p}^s) = \begin{cases} 1 & \text{if } s = 0, \\ N(\mathfrak{p})^s \left( 1 - \left(\frac{K}{p}\right) N(\mathfrak{p})^{-1} \right) & \text{if } s \geq 1. \end{cases}$$

Now let  $\mathfrak{f} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$  be the factorization of  $\mathfrak{f}$  into prime factors. Then

$$\begin{aligned} & \sum_{c|f} \left( N(c) \prod_{p|c} \left( 1 - \left(\frac{K}{p}\right) N(\mathfrak{p})^{-1} \right) \right) \\ &= \sum_{s_1=0}^{e_1} \cdots \sum_{s_r=0}^{e_r} \left( \varphi(\mathfrak{p}_1^{s_1}) \cdots \varphi(\mathfrak{p}_r^{s_r}) \right) \\ &= \prod_{j=1}^r \left( \sum_{s_j=0}^{e_j} \varphi(\mathfrak{p}_j^{s_j}) \right). \end{aligned}$$

Here we have

$$\sum_{s_j=0}^{e_j} \varphi(\mathfrak{p}_j^{s_j}) = \begin{cases} N(\mathfrak{p}_j)^{e_j} & \text{if } \left(\frac{K}{p_j}\right) = 1, \\ \begin{cases} (N(\mathfrak{p}_j)^{e_j+1} + N(\mathfrak{p}_j)^{e_j} - 2) \\ \cdot (N(\mathfrak{p}_j) - 1)^{-1} \end{cases} & \text{if } \left(\frac{K}{p_j}\right) = -1, \\ (N(\mathfrak{p}_j)^{e_j+1} - 1)(N(\mathfrak{p}_j) - 1)^{-1} & \text{if } \left(\frac{K}{p_j}\right) = 0. \end{cases}$$

Therefore, we obtain our lemma.  $\square$

### 2.4 Formula for Computation

From the above lemmas, we obtain the following result:

**Proposition 2.7.** *With the notation of Theorem 2.1, we have*

$$\begin{aligned} \text{tr } T(\mathfrak{a}) &= \varepsilon(\mathfrak{a}) \delta(\mathfrak{a}) (-1)^g 2^{1-g} \zeta_F(-1) \psi \left( \left( \pi_{\mathfrak{p}}^{\text{ord}_{\mathfrak{p}}(\mathfrak{a})/2} \right)_{\mathfrak{p} \in \mathfrak{h}} \right) \\ & \cdot \left( \prod_{j=1}^g (k_j - 1) \right) + \varepsilon(\mathfrak{a}) (-1)^g 2^{-g} \sum_{\mathfrak{m} \in M_{\mathfrak{a}}} \psi \left( \left( \pi_{\mathfrak{p}}^{\text{ord}_{\mathfrak{p}}(\mathfrak{m})} \right)_{\mathfrak{p} \in \mathfrak{h}} \right)^{-1} \\ & \cdot \sum_{n \in N_{\mathfrak{m}}} \sum_{s \in S_n} \left( \prod_{j=1}^g \Phi(s_j, n_j, k_j) \right) \cdot L_F(0, \chi_{K_{S_n}/F}) \\ & \cdot \left( \prod_{\substack{p|f_{S_n} \\ \left(\frac{K_{S_n}}{p}\right) = -1 \\ p \in \mathfrak{h}}} \frac{N(\mathfrak{p})^{\text{ord}_{\mathfrak{p}}(f_{S_n})+1} + N(\mathfrak{p})^{\text{ord}_{\mathfrak{p}}(f_{S_n})} - 2}{N(\mathfrak{p}) - 1} \right) \\ & \cdot \left( \prod_{\substack{p|f_{S_n} \\ \left(\frac{K_{S_n}}{p}\right) = 1 \\ p \in \mathfrak{h}}} N(\mathfrak{p})^{\text{ord}_{\mathfrak{p}}(f_{S_n})} \right) \left( \prod_{\substack{p|f_{S_n} \\ \left(\frac{K_{S_n}}{p}\right) = 0 \\ p \in \mathfrak{h}}} \frac{N(\mathfrak{p})^{\text{ord}_{\mathfrak{p}}(f_{S_n})+1} - 1}{N(\mathfrak{p}) - 1} \right) \\ & + (-1)^{g-1} b(k) \sum_{\lambda \in C(\psi)} \lambda \left( \left( \pi_{\mathfrak{p}}^{\text{ord}_{\mathfrak{p}}(\mathfrak{a})} \right)_{\mathfrak{p} \in \mathfrak{h}} \right) \sum_{\substack{b|a \\ b \subset \mathfrak{o}_F \\ b \in I(F)}} N(\mathfrak{b}), \end{aligned} \tag{2-9}$$

where  $f_{sn} = c(\mathfrak{o}_F + ((s + \sqrt{s^2 - 4n})/2)\mathfrak{o}_F)\mathfrak{m}^{-1} = ((s^2 - 4n)_F D_{K_{sn}/F}^{-1})^{1/2} \mathfrak{m}^{-1}$ , and  $\chi_{K_{sn}/F}$  is the ideal character corresponding to the extension  $K_{sn}/F$ . (We note that  $(s^2 - 4n)_F D_{K_{sn}/F}^{-1}$  is a square by Lemma 2.3.)

*Proof:* In view of Theorem 2.1, we only need to show that

$$\frac{2\zeta_F(2)|D_F|^{3/2}}{(2\pi)^{2g}} = (-1)^g 2^{1-g} \zeta_F(-1), \tag{2-10}$$

$$\sum_{\Lambda \in R_{sn}} \frac{h(\Lambda)}{h_F[\Lambda^\times : \mathfrak{o}_F^\times]} = 2^{1-g} L_F(0, \chi_{K_{sn}/F}) \cdot \left( \prod_{\substack{\mathfrak{p} | f_{sn} \\ (\frac{K_{sn}}{\mathfrak{p}}) = -1}} \frac{N(\mathfrak{p})^{\text{ord}_{\mathfrak{p}}(f_{sn})+1} + N(\mathfrak{p})^{\text{ord}_{\mathfrak{p}}(f_{sn})} - 2}{N(\mathfrak{p}) - 1} \right) \cdot \left( \prod_{\substack{\mathfrak{p} | f_{sn} \\ (\frac{K_{sn}}{\mathfrak{p}}) = 1}} N(\mathfrak{p})^{\text{ord}_{\mathfrak{p}}(f_{sn})} \right) \left( \prod_{\substack{\mathfrak{p} | f_{sn} \\ (\frac{K_{sn}}{\mathfrak{p}}) = 0}} \frac{N(\mathfrak{p})^{\text{ord}_{\mathfrak{p}}(f_{sn})+1} - 1}{N(\mathfrak{p}) - 1} \right). \tag{2-11}$$

By the functional equation of  $\zeta_F$ , we have  $\zeta_F(2) = |D_F|^{-3/2} (-2\pi^2)^g \zeta_F(-1)$ , and hence we obtain (2-10). Next, by Lemma 2.4 and Lemma 2.5, we have

$$\sum_{\Lambda \in R_{sn}} \frac{h(\Lambda)}{h_F[\Lambda^\times : \mathfrak{o}_F^\times]} = \sum_{\Lambda \in R_{sn}} \frac{h_{K_{sn}}}{h_F[\mathfrak{o}_{K_{sn}}^\times : \mathfrak{o}_F^\times]} N(c(\Lambda)) \prod_{\mathfrak{p} | c(\Lambda)} \left( 1 - \left(\frac{K_{sn}}{\mathfrak{p}}\right) N(\mathfrak{p})^{-1} \right) = 2^{1-g} L_F(0, \chi_{K_{sn}/F}) \sum_{\Lambda \in R_{sn}} N(c(\Lambda)) \cdot \prod_{\mathfrak{p} | c(\Lambda)} \left( 1 - \left(\frac{K_{sn}}{\mathfrak{p}}\right) N(\mathfrak{p})^{-1} \right).$$

Now, from Lemma 2.3, we have

$$R_{sn} = \{ \Lambda \in \mathcal{O}_{K_{sn}/F} \mid D_{K_{sn}/F}(\Lambda) \mid (s^2 - 4n)_F \mathfrak{m}^{-2} \} = \{ \Lambda \in \mathcal{O}_{K_{sn}/F} \mid c(\Lambda)^2 \mid (s^2 - 4n)_F D_{K_{sn}/F}^{-1} \mathfrak{m}^{-2} \} = \{ \Lambda \in \mathcal{O}_{K_{sn}/F} \mid c(\Lambda) \mid f_{sn} \}.$$

Thus we have

$$\sum_{\Lambda \in R_{sn}} N(c(\Lambda)) \prod_{\mathfrak{p} | c(\Lambda)} \left( 1 - \left(\frac{K_{sn}}{\mathfrak{p}}\right) N(\mathfrak{p})^{-1} \right) = \sum_{\substack{c | f_{sn} \\ c \subset \mathfrak{o}_F \\ c \in I(F)}} N(c) \prod_{\mathfrak{p} | c} \left( 1 - \left(\frac{K_{sn}}{\mathfrak{p}}\right) N(\mathfrak{p})^{-1} \right),$$

since the mapping  $c$  is bijective by Lemma 2.2. Therefore we obtain (2-11) by Lemma 2.6.  $\square$

### 3. COMPUTATION FOR REAL QUADRATIC FIELDS

In this section, we give an algorithm to compute Formula (2-9) for a real quadratic field  $F$ . In particular, we assume  $F = \mathbf{Q}(\sqrt{m})$  with a square-free integer  $m$  satisfying  $m \equiv 1 \pmod{4\mathbf{Z}}$  exclusively, though the case  $m \not\equiv 1 \pmod{4\mathbf{Z}}$  can be handled by a similar consideration below. Throughout this section, we let  $\omega = (1 + \sqrt{m})/2$ , and denote by  $\sigma$  the nontrivial automorphism of  $F$ . We note that for every integral ideal  $\mathfrak{a}$  of  $F$  there exist rational integers  $a > 0$  and  $b$  such that  $\mathfrak{a} = [a, b + \omega]$ ; moreover, it is well known how to check whether  $\mathfrak{a} \in P(F)$  (respectively  $\mathfrak{a} \in P^+(F)$ ) and to find an explicit generator of  $\mathfrak{a}$  when  $\mathfrak{a} \in P(F)$  (respectively  $\mathfrak{a} \in P^+(F)$ ) by the theory of continued fractions (cf. [Dirichlet 1894], for example). For  $\mathfrak{p} \in \mathfrak{h}$ , we call  $\mathfrak{p}$  *odd* (respectively *even*) if  $\mathfrak{p} \nmid (2)_F$  (respectively  $\mathfrak{p} \mid (2)_F$ ).

#### 3.1 Preliminaries

We note that  $\zeta_F(-1) = \zeta(-1) \cdot L(-1, \left(\frac{\cdot}{m}\right)) = 24^{-1} B_{2, \left(\frac{\cdot}{m}\right)}$ , where  $B_{2, \left(\frac{\cdot}{m}\right)}$  is the second generalized Bernoulli number associated with  $\left(\frac{\cdot}{m}\right)$ . Here  $\left(\frac{\cdot}{m}\right)$  is the character corresponding to  $\mathbf{Q}(\sqrt{m})/\mathbf{Q}$ . It is known that

$$B_{2, \left(\frac{\cdot}{m}\right)} = (6m)^{-1} \sum_{a=1}^m \left(\frac{a}{m}\right) (6a^2 - 6am + m^2)$$

(cf. [Iwasawa 72, §2]). Hence

$$\zeta_F(-1) = (144m)^{-1} \sum_{a=1}^m \left(\frac{a}{m}\right) (6a^2 - 6am + m^2).$$

Thus the first and third sums of the right-hand side of (2-9) are easily computable.

Hereinafter, we consider the second sum for the case  $\varepsilon(\mathfrak{a}) = 1$ , which implies  $M_{\mathfrak{a}} \neq \emptyset$ . We first explain a method for choosing  $M_{\mathfrak{a}}$ ,  $N_{\mathfrak{m}}$ , and  $S_n$  in (2-9). Choose an arbitrary complete set of integral representatives  $C$  of  $\text{Cl}(F)$ . Take the set of all elements  $\mathfrak{b}_1, \dots, \mathfrak{b}_u$  of  $C$  such that  $\mathfrak{b}_j^2 \mathfrak{a} \in P^+(F)$ . If  $\text{gcd}(\mathfrak{b}_j, \mathfrak{a}) = \mathfrak{o}_F$ , then set  $\mathfrak{m}_j = \mathfrak{b}_j$ ; if  $\text{gcd}(\mathfrak{b}_j, \mathfrak{a}) \neq \mathfrak{o}_F$ , then take a prime ideal  $\mathfrak{p}_j$  of  $F$  satisfying  $\mathfrak{p}_j \nmid \mathfrak{a}$  and  $\mathfrak{p}_j^\sigma \mathfrak{b}_j \in P(F)$  (i.e.,  $\mathfrak{p}_j P(F) = \mathfrak{b}_j P(F)$ ), and set  $\mathfrak{m}_j = \mathfrak{p}_j$ . Then the set  $M_{\mathfrak{a}}$  is given by

$$M_{\mathfrak{a}} = \{\mathfrak{m}_1, \dots, \mathfrak{m}_u\}.$$

We fix  $\mathfrak{m} \in M_{\mathfrak{a}}$ . Then we can take  $n_{\mathfrak{m}}$  satisfying  $0 \ll n_{\mathfrak{m}} \in \mathfrak{o}_F$  and  $(n_{\mathfrak{m}})_F = \mathfrak{m}^2 \mathfrak{a}$ . Now we can choose  $\{1\}$  as  $E_F$  when  $h_F = h_F^+$ , and  $\{1, \varepsilon\}$  as  $E_F$  when  $h_F \neq h_F^+$ , where  $\varepsilon$  is the fundamental unit of  $F$  satisfying  $\varepsilon > 1$ . Thus we can take  $N_{\mathfrak{m}} = n_{\mathfrak{m}} E_F$ . (Note that the choice of

$M_a$  and  $N_m$  has no effect on  $\text{tr} T(a)$ , as remarked after Theorem 2.1.) We also fix  $n \in N_m$ . Now we set  $m = [l_1, l_2 + \omega]$  with  $l_1, l_2 \in \mathbf{Z}$  satisfying  $1 \leq l_1$  and  $0 \leq l_2 < l_1$ . For  $s \in \mathfrak{m}$ , we can set  $s = yl_1 + x(l_2 + \omega)$  with  $y, x \in \mathbf{Z}$ . Then we have

$$\begin{aligned} s^2 \ll 4n &\iff s^2 < 4n, (s^\sigma)^2 < 4n^\sigma \\ &\iff -2\sqrt{n} < s < 2\sqrt{n}, -2\sqrt{n}^\sigma < s^\sigma < 2\sqrt{n}^\sigma \\ &\iff \begin{cases} y < -\frac{2l_2 + 1 + \sqrt{m}}{2l_1}x + \frac{2\sqrt{n}}{l_1}, \\ y > -\frac{2l_2 + 1 + \sqrt{m}}{2l_1}x - \frac{2\sqrt{n}}{l_1}, \\ y < -\frac{2l_2 + 1 - \sqrt{m}}{2l_1}x + \frac{2\sqrt{n}^\sigma}{l_1}, \\ y > -\frac{2l_2 + 1 - \sqrt{m}}{2l_1}x - \frac{2\sqrt{n}^\sigma}{l_1}. \end{cases} \end{aligned} \quad (3-1)$$

Thus we have

$$S_n = \{yl_1 + x(l_2 + \omega) \mid y, x \in \mathbf{Z} \text{ satisfying (3-1)}\}.$$

Set  $K = F(\sqrt{\alpha})$  with  $\alpha \in \mathfrak{o}_F$  satisfying  $\alpha \ll 0$ . Then our study is reduced to the computation of the following :

- (i)  $D_{K/F} = \prod_{\mathfrak{p} \in \mathfrak{h}} D_{\mathfrak{p}}$ ,
- (ii)  $\left(\frac{K}{\mathfrak{p}}\right)$  for  $\mathfrak{p} \in \mathfrak{h}$ ,
- (iii)  $L_F(0, \chi_{K/F})$ ,

where  $\prod_{\mathfrak{p} \in \mathfrak{h}} D_{\mathfrak{p}}$  is the prime factorization of  $D_{K/F}$ .

### 3.2 Determination of $D_{\mathfrak{p}}$ and $\left(\frac{K}{\mathfrak{p}}\right)$ for an Odd Prime $\mathfrak{p}$

First we explain a way to determine  $D_{\mathfrak{p}}$  and  $\left(\frac{K}{\mathfrak{p}}\right)$  for an odd prime ideal  $\mathfrak{p}$  of  $F$ .

**Proposition 3.1.** *Let  $F$  be an algebraic number field of finite degree, and  $K = F(\sqrt{\alpha})$  a quadratic extension of  $F$  with  $\alpha \in \mathfrak{o}_F$ . Let  $\mathfrak{p}$  be an odd prime ideal of  $F$ . Then*

$$D_{\mathfrak{p}} = \begin{cases} \mathfrak{o}_F & \text{if } 2 \mid \text{ord}_{\mathfrak{p}}(\alpha), \\ \mathfrak{p} & \text{otherwise.} \end{cases}$$

*Proof:* If  $2 \mid \text{ord}_{\mathfrak{p}}(\alpha)$ , then we can find  $\alpha_1 \in \mathfrak{o}_F$  such that  $K = F(\sqrt{\alpha_1})$  and  $\text{ord}_{\mathfrak{p}}(\alpha_1) = 0$ . Since  $D_{K/F} \mid D_{K/F}(\sqrt{\alpha_1})$  and  $D_{K/F}(\sqrt{\alpha_1}) = (4\alpha_1)_F$ , we have  $D_{\mathfrak{p}} = \mathfrak{o}_F$ . Now assume  $2 \nmid \text{ord}_{\mathfrak{p}}(\alpha)$ , take a prime ideal  $\mathfrak{P}$  of  $K$  that lies above  $\mathfrak{p}$ , and let  $e$  be the ramification index of  $\mathfrak{P}$  in  $K/F$ . Then  $2 \cdot \text{ord}_{\mathfrak{P}}(\sqrt{\alpha}) = \text{ord}_{\mathfrak{P}}(\alpha) = e \cdot \text{ord}_{\mathfrak{p}}(\alpha)$ , and hence  $e = 2$ . Since  $[K_{\mathfrak{P}} : F_{\mathfrak{p}}] = 2$  and  $\mathfrak{p} \nmid (2)_F$ , we have  $D_{\mathfrak{p}} = \mathfrak{p}^{e-1} = \mathfrak{p}$  (cf. [Weil 67, Chapter VIII, Corollary 3 of Proposition 7]).  $\square$

We can determine  $D_{\mathfrak{p}}$  from this proposition.

Let  $F, K$ , and  $\mathfrak{p}$  be as in Proposition 3.1. By Dedekind's discriminant theorem, we know that

$$\left(\frac{K}{\mathfrak{p}}\right) = 0 \iff \mathfrak{p} \mid D_{K/F}. \quad (3-2)$$

For an explicit determination of  $\left(\frac{K}{\mathfrak{p}}\right)$  for  $\mathfrak{p} \nmid D_{K/F}$ , we start with the following lemma.

**Lemma 3.2.** *Let  $F$  be a Galois extension of  $\mathbf{Q}$  of prime degree, and  $K = F(\sqrt{\alpha})$  a quadratic extension of  $F$  with  $\alpha \in \mathfrak{o}_F$ . Let  $\mathfrak{p}$  be an odd prime ideal of  $F$  satisfying  $\mathfrak{p} \nmid D_{K/F}$ , and  $p$  the prime number in  $\mathbf{Q}$  that lies below  $\mathfrak{p}$  (i.e.,  $\mathfrak{p} \mid (p)_F$ , which means that  $\mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}$ ). If  $p$  remains prime in  $F/\mathbf{Q}$ , then we set  $a = N_{F/\mathbf{Q}}(\alpha p^{-\text{ord}_{\mathfrak{p}}(\alpha)})$ ; if  $p$  ramifies in  $F/\mathbf{Q}$ , then we take  $a \in (\alpha \pi_{\mathfrak{p}}^{-\text{ord}_{\mathfrak{p}}(\alpha)} + \pi_{\mathfrak{p}} \mathfrak{o}_{\mathfrak{p}}) \cap \mathbf{Z}$ ; if  $p$  splits in  $F/\mathbf{Q}$ , then we take  $a_0 \in (\alpha + p^{\text{ord}_{\mathfrak{p}}(\alpha)+1} \mathfrak{o}_{\mathfrak{p}}) \cap \mathbf{Z}$ , and set  $a = a_0 p^{-\text{ord}_{\mathfrak{p}}(\alpha)}$ . Then we have*

$$\left(\frac{K}{\mathfrak{p}}\right) = \left(\frac{a}{p}\right).$$

Note that this criterion does not depend on the choices of  $\alpha$  and  $a$  from the proof below.

*Proof:* Put  $[F : \mathbf{Q}] = g$ . Now,  $\mathfrak{p}$  splits or remains prime in  $K/F$  by (3-2), and  $2 \mid \text{ord}_{\mathfrak{p}}(\alpha)$  by Proposition 3.1. Since  $\mathfrak{p}$  is odd, we have

$$(1 + \pi_{\mathfrak{p}} \mathfrak{o}_{\mathfrak{p}})^2 = 1 + \pi_{\mathfrak{p}} \mathfrak{o}_{\mathfrak{p}};$$

indeed, for any element  $1 + \pi_{\mathfrak{p}} y \in 1 + \pi_{\mathfrak{p}} \mathfrak{o}_{\mathfrak{p}}$ , the polynomial  $\pi_{\mathfrak{p}} X^2 + 2X - y$  has a root  $x \in \mathfrak{o}_{\mathfrak{p}}$  by Hensel's lemma, and thus  $(1 + \pi_{\mathfrak{p}} x)^2 = 1 + \pi_{\mathfrak{p}} y$ . Note that  $\mathfrak{p}$  splits in  $K/F$  if and only if the polynomial  $X^2 - \alpha$  is reducible over  $F_{\mathfrak{p}}$ ; that is,

$$\left(\frac{K}{\mathfrak{p}}\right) = 1 \iff \alpha \in (F_{\mathfrak{p}}^{\times})^2.$$

Assume first that  $p$  remains prime in  $F/\mathbf{Q}$ . Then  $[F_{\mathfrak{p}} : \mathbf{Q}_{\mathfrak{p}}] = g$  and  $\text{ord}_{\mathfrak{p}}(p) = 1$ . Write  $\text{Gal}(F/\mathbf{Q}) = \{\sigma_1, \dots, \sigma_g\}$  and  $\alpha_0 = \alpha p^{-\text{ord}_{\mathfrak{p}}(\alpha)} \in \mathfrak{o}_{\mathfrak{p}}^{\times} \cap \mathfrak{o}_F$ . Then

$\{\alpha_0^{p^j} + \mathfrak{o}_{\mathfrak{p}} \mid j = 0, \dots, g-1\} = \{\alpha_0^{\sigma_j} + \mathfrak{o}_{\mathfrak{p}} \mid j = 1, \dots, g\}$  (cf. [Weil 67, Chapter I, Corollary 2 of Theorem 7]). Thus

$$\begin{aligned} \alpha \in (F_{\mathfrak{p}}^{\times})^2 &\iff \alpha_0 \in (\mathfrak{o}_{\mathfrak{p}}^{\times})^2 \\ &\iff (\alpha_0 \alpha_0^p \cdots \alpha_0^{p^{g-1}})^{(p-1)/2} \\ &= \alpha_0^{(N(\mathfrak{p})-1)/2} \in 1 + \mathfrak{p} \mathfrak{o}_{\mathfrak{p}} \\ &\iff (\alpha_0^{\sigma_1} \alpha_0^{\sigma_2} \cdots \alpha_0^{\sigma_g})^{(p-1)/2} \\ &= N_{F/\mathbf{Q}}(\alpha_0)^{(p-1)/2} \in 1 + \mathfrak{p} \mathfrak{o}_{\mathfrak{p}} \\ &\iff a^{(p-1)/2} = N_{F/\mathbf{Q}}(\alpha_0)^{(p-1)/2} \in 1 + \mathfrak{p} \mathbf{Z} \\ &\iff \left(\frac{a}{p}\right) = 1. \end{aligned}$$

Next assume that  $p$  ramifies in  $F/\mathbf{Q}$ . Since  $\alpha\pi_{\mathfrak{p}}^{-\text{ord}_{\mathfrak{p}}(\alpha)} \in \mathfrak{o}_{\mathfrak{p}}^{\times}$  and  $\mathfrak{o}_{\mathfrak{p}}/\pi_{\mathfrak{p}}\mathfrak{o}_{\mathfrak{p}} \cong \mathbf{Z}/p\mathbf{Z}$ , we can take  $a \in (\alpha\pi_{\mathfrak{p}}^{-\text{ord}_{\mathfrak{p}}(\alpha)} + \pi_{\mathfrak{p}}\mathfrak{o}_{\mathfrak{p}}) \cap \mathbf{Z}$ . Thus

$$\begin{aligned} \alpha \in (F_{\mathfrak{p}}^{\times})^2 &\iff \alpha\pi_{\mathfrak{p}}^{-\text{ord}_{\mathfrak{p}}(\alpha)} \in (\mathfrak{o}_{\mathfrak{p}}^{\times})^2 \\ &\iff a \in (\mathfrak{o}_{\mathfrak{p}}^{\times})^2 \\ &\iff a^{(p-1)/2} \in 1 + \pi_{\mathfrak{p}}\mathfrak{o}_{\mathfrak{p}} \\ &\quad (\text{i.e. } a^{(p-1)/2} \in 1 + p\mathbf{Z}) \\ &\iff \left(\frac{a}{p}\right) = 1. \end{aligned}$$

Finally, assume that  $p$  splits in  $F/\mathbf{Q}$ . Then  $F_{\mathfrak{p}} \cong \mathbf{Q}_{\mathfrak{p}}$  and  $\text{ord}_{\mathfrak{p}}(p) = 1$ . Since  $\mathbf{Z}$  is dense in  $\mathfrak{o}_{\mathfrak{p}}$ , we can take  $a_0 \in (\alpha + p^{\text{ord}_{\mathfrak{p}}(\alpha)+1}\mathfrak{o}_{\mathfrak{p}}) \cap \mathbf{Z}$ . Then  $\alpha(1 + p\mathfrak{o}_{\mathfrak{p}}) = \alpha + p^{\text{ord}_{\mathfrak{p}}(\alpha)+1}\mathfrak{o}_{\mathfrak{p}} = a_0(1 + p\mathfrak{o}_{\mathfrak{p}})$ . Thus

$$\begin{aligned} \alpha \in (F_{\mathfrak{p}}^{\times})^2 &\iff a_0 \in (F_{\mathfrak{p}}^{\times})^2 \\ &\quad (\text{i.e. } a = a_0p^{-\text{ord}_{\mathfrak{p}}(\alpha)} \in (\mathfrak{o}_{\mathfrak{p}}^{\times})^2) \\ &\iff a^{(p-1)/2} \in 1 + \pi_{\mathfrak{p}}\mathfrak{o}_{\mathfrak{p}} \\ &\quad (\text{i.e. } a^{(p-1)/2} \in 1 + p\mathbf{Z}) \\ &\iff \left(\frac{a}{p}\right) = 1. \end{aligned}$$

This completes the proof. □

**Lemma 3.3.** *Let  $F = \mathbf{Q}(\sqrt{m})$  be a real quadratic field with a square-free integer  $m$  satisfying  $m \equiv 1 \pmod{4\mathbf{Z}}$ . Let  $p$  be an odd prime number in  $\mathbf{Q}$  such that  $\left(\frac{m}{p}\right) = 1$ , and  $\mathfrak{p}$  the prime ideal of  $F$  that lies above  $p$ . Let  $r$  be an integer such that  $\mathfrak{p} = [p, r + \omega]$ . Then, for  $u \in \mathbf{Z}$  and  $1 \leq j \in \mathbf{Z}$ ,  $u \equiv \sqrt{m} \pmod{p^j\mathfrak{o}_{\mathfrak{p}}}$  if and only if  $u^2 \equiv m \pmod{p^j\mathbf{Z}}$  and  $u \equiv -2r - 1 \pmod{p\mathbf{Z}}$ .*

*Proof:* We first prove that  $u \equiv \sqrt{m}$  or  $-\sqrt{m} \pmod{p^j\mathfrak{o}_{\mathfrak{p}}}$  if and only if  $u^2 \equiv m \pmod{p^j\mathbf{Z}}$  for  $u \in \mathbf{Z}$  and  $1 \leq j \in \mathbf{Z}$ . If  $u - \sqrt{m} \in p^j\mathfrak{o}_{\mathfrak{p}}$  or  $u + \sqrt{m} \in p^j\mathfrak{o}_{\mathfrak{p}}$ , then  $u^2 - m = (u - \sqrt{m})(u + \sqrt{m}) \in p^j\mathfrak{o}_{\mathfrak{p}}$ , and hence  $u^2 - m \in p^j\mathfrak{o}_{\mathfrak{p}} \cap \mathbf{Z} = p^j\mathbf{Z}$ . Conversely,  $X^2 \equiv m \pmod{p^j\mathbf{Z}}$  has exactly two solutions modulo  $p^j\mathbf{Z}$ , since  $p \neq 2$  and  $\left(\frac{m}{p}\right) = 1$ . Since  $p$  is odd and  $\sqrt{m} \in \mathfrak{o}_{\mathfrak{p}}^{\times}$ , we have  $\sqrt{m} \not\equiv -\sqrt{m} \pmod{p^j\mathfrak{o}_{\mathfrak{p}}}$ . Thus if  $u \in \mathbf{Z}$  satisfies the condition  $u^2 \equiv m \pmod{p^j\mathbf{Z}}$ , then  $u \equiv \sqrt{m}$  or  $-\sqrt{m} \pmod{p^j\mathfrak{o}_{\mathfrak{p}}}$ . Now,  $2^{-1}(2r + 1 + \sqrt{m}) = r + \omega \in \mathfrak{p} \subset p\mathfrak{o}_{\mathfrak{p}}$ . Thus  $2r + 1 + \sqrt{m} \in p\mathfrak{o}_{\mathfrak{p}}$ , that is,  $\sqrt{m} \equiv -2r - 1 \pmod{p\mathfrak{o}_{\mathfrak{p}}}$ . Therefore, we obtain our assertion. □

From the two lemmas above, we obtain the following proposition:

**Proposition 3.4.** *Let  $F$  and  $m$  be as in Lemma 3.3, and  $0 \gg \alpha \in \mathfrak{o}_F$ . Set  $K = F(\sqrt{\alpha})$ , and  $\alpha = a_1 + a_2\omega$  with*

$a_1, a_2 \in \mathbf{Z}$ . Let  $\mathfrak{p}$  be an odd prime ideal of  $F$  satisfying  $\mathfrak{p} \nmid D_{K/F}$ , and  $p$  the prime number in  $\mathbf{Q}$  that lies below  $\mathfrak{p}$ . Put  $t = \text{ord}_{\mathfrak{p}}(\alpha)$ . In particular, if  $p$  splits in  $F/\mathbf{Q}$ , we set  $\mathfrak{p} = [p, r + \omega]$  with  $r \in \mathbf{Z}$ ,  $l = \text{ord}_{\mathfrak{p}}(\gcd(a_1, a_2))$ , and take  $u \in \mathbf{Z}$  such that  $u^2 \equiv m \pmod{p^{t-l+1}\mathbf{Z}}$  and  $u \equiv -2r - 1 \pmod{p\mathbf{Z}}$ . Set

$$a = \begin{cases} p^{-2t}(a_1^2 + a_1a_2 + a_2^2(1 - m)/4) & \text{if } p \text{ remains prime in } F/\mathbf{Q}, \\ (mp^{-2})^{t/2}(a_1 - a_2(p - 1)/2) & \text{if } p \text{ ramifies in } F/\mathbf{Q}, \\ p^{-t}((p + 1)/2)(2a_1 + a_2(1 + u)) & \text{if } p \text{ splits in } F/\mathbf{Q}. \end{cases}$$

Then we have

$$\left(\frac{K}{\mathfrak{p}}\right) = \left(\frac{a}{p}\right).$$

*Proof:* If  $p$  remains prime in  $F/\mathbf{Q}$ , our assertion follows immediately from Lemma 3.2. Next we assume that  $p$  ramifies in  $F/\mathbf{Q}$ . Then  $\mathfrak{p} = [p, (p - 1)/2 + \omega]$ . Since  $\sqrt{mp}^{-1} \in F^{\times}$ ,  $\text{ord}_{\mathfrak{p}}(\sqrt{mp}^{-1}) = -1$ , and  $\text{ord}_{\mathfrak{q}}(\sqrt{mp}^{-1}) \geq 0$  for any  $\mathfrak{q} \in \mathfrak{h} - \{\mathfrak{p}\}$ , we see that  $\pi_{\mathfrak{p}} = \sqrt{m}^{-1}p$  is a prime element of  $F_{\mathfrak{p}}$  and  $\alpha\pi_{\mathfrak{p}}^{-t} = \alpha(mp^{-2})^{t/2} \in \mathfrak{o}_F$ . Thus  $a_1(mp^{-2})^{t/2}, a_2(mp^{-2})^{t/2} \in \mathbf{Z}$ , and hence  $\alpha\pi_{\mathfrak{p}}^{-t} + \pi_{\mathfrak{p}}\mathfrak{o}_{\mathfrak{p}} \supset \alpha(mp^{-2})^{t/2} + \mathfrak{p} \supset (mp^{-2})^{t/2}(a_1 - a_2(p - 1)/2)$ . Therefore, we obtain  $a$  in Lemma 3.2 in this case. Now assume that  $p$  splits in  $F/\mathbf{Q}$ . By Lemma 3.3, we have  $u \equiv \sqrt{m} \pmod{p^{t-l+1}\mathfrak{o}_{\mathfrak{p}}}$ . Since  $p^l \mid a_2$ , we have  $a_2u \equiv a_2\sqrt{m} \pmod{p^{t+1}\mathfrak{o}_{\mathfrak{p}}}$ , and hence

$$\begin{aligned} ((p + 1)/2)(2a_1 + a_2(1 + u)) &\equiv ((p + 1)/2) \\ &\quad \cdot (2a_1 + a_2(1 + \sqrt{m})) \\ &= (p + 1)\alpha \\ &\equiv \alpha \pmod{p^{t+1}\mathfrak{o}_{\mathfrak{p}}}. \end{aligned}$$

Thus  $((p + 1)/2)(2a_1 + a_2(1 + u)) \in (\alpha + p^{t+1}\mathfrak{o}_{\mathfrak{p}}) \cap \mathbf{Z}$ . Therefore, our assertion follows from Lemma 3.2. □

**Remark 3.5.** Note that we can find  $u \in \mathbf{Z}$  satisfying

$$u^2 \equiv m \pmod{p^{t-l+1}\mathbf{Z}} \tag{3-3}$$

when  $\left(\frac{m}{p}\right) = 1$ . Then we have  $u \equiv -2r - 1$  or  $2r + 1 \pmod{p\mathbf{Z}}$ , as we see in the proof of Lemma 3.3. Finding a solution  $u$  of (3-3) can be reduced to mod  $p$  calculation by the following procedure: Let  $u = c_0 + c_1p + \dots + c_{t-l}p^{t-l}$  with  $0 \leq c_j \leq p - 1$ , and set  $u_j = c_0 + c_1p + \dots + c_jp^j$  for  $0 \leq j \leq t - l$ . Since  $m \equiv u_j^2 = (u_{j-1} + c_jp^j)^2 \equiv u_{j-1}^2 + 2u_{j-1}c_jp^j \pmod{p^{j+1}\mathbf{Z}}$ , we have

$$m \equiv c_0^2 \pmod{p\mathbf{Z}}, \tag{3-4a}$$

$$p^{-j}(m - u_{j-1}^2) \equiv 2u_{j-1}c_j \pmod{p\mathbf{Z}} \tag{3-4b}$$

for  $1 \leq j \leq t-l$ . Thus we can determine  $c_0, \dots, c_{t-l}$  inductively by (3-4a, b).

From Proposition 3.4 and Remark 3.5, we can immediately determine  $\left(\frac{K}{\mathfrak{p}}\right)$  for every *odd* prime ideal  $\mathfrak{p}$  satisfying  $\mathfrak{p} \nmid D_{K/F}$ .

### 3.3 Determination of $D_{\mathfrak{p}}$ and $\left(\frac{K}{\mathfrak{p}}\right)$ for an Even Prime $\mathfrak{p}$

Next we give a method for determining  $D_{\mathfrak{p}}$  and  $\left(\frac{K}{\mathfrak{p}}\right)$  for an *even* prime ideal  $\mathfrak{p}$  of  $F$ .

**Proposition 3.6.** *Let  $F, m, \alpha, K, a_1,$  and  $a_2$  be as in Proposition 3.4. Let  $\mathfrak{p}$  be an even prime ideal of  $F$ . Assume  $\mathfrak{p}^2 \nmid (\alpha)_F$ . If  $m \equiv 1 \pmod{8\mathbf{Z}}$ , we set  $l = (m-1)/8$  and  $\mathfrak{p} = [2, r + \omega]$ , where  $r = 0$  or  $1$ ; we also set*

$$A_m = \{(a, b) \in \mathbf{Z}^2 \mid a + b(2l(-1)^r + r) - 1 \in 8\mathbf{Z}\},$$

$$A'_m = \{(a, b) \in \mathbf{Z}^2 \mid a - b(2l - r) - 1 \in 4\mathbf{Z}\}.$$

If  $m \equiv 5 \pmod{8\mathbf{Z}}$ , we set  $l = (m-5)/8$ ,

$$A_m = \{(a, b) \in \mathbf{Z}^2 \mid (a-1, b) \in 4\mathbf{Z} \times 8\mathbf{Z}$$

$$\text{or } (a-2l-2, b-3) \in 8\mathbf{Z} \times 4\mathbf{Z}$$

$$\text{or } (a-2l-1, b-1) \in (8\mathbf{Z})^2$$

$$\text{or } (a-2l-5, b-5) \in (8\mathbf{Z})^2\},$$

$$A'_m = \{(a, b) \in \mathbf{Z}^2 \mid (a-1, b) \in (4\mathbf{Z})^2$$

$$\text{or } (a-2l-2, b-3) \in (4\mathbf{Z})^2$$

$$\text{or } (a-2l-1, b-1) \in (4\mathbf{Z})^2\}.$$

Then we have

$$\left(\frac{K}{\mathfrak{p}}\right) = \begin{cases} 1 & \text{if } \mathfrak{p} \nmid (\alpha)_F \text{ and } (a_1, a_2) \in A_m, \\ -1 & \text{if } \mathfrak{p} \nmid (\alpha)_F, (a_1, a_2) \notin A_m, \\ & \text{and } (a_1, a_2) \in A'_m, \\ 0 & \text{otherwise,} \end{cases}$$

and

$$D_{\mathfrak{p}} = \begin{cases} \mathfrak{o}_F & \text{if } \left(\frac{K}{\mathfrak{p}}\right) \neq 0, \\ \mathfrak{p}^2 & \text{if } \left(\frac{K}{\mathfrak{p}}\right) = 0 \text{ and } \mathfrak{p} \nmid (\alpha)_F, \\ \mathfrak{p}^3 & \text{if } \mathfrak{p} \mid (\alpha)_F. \end{cases}$$

*Proof:* We set

$$f = \max\{j \in \mathbf{Z} \mid 0 \leq j \leq 3, \text{ there exists } \gamma \in \mathfrak{o}_F \text{ such that } \gamma^2 \equiv \alpha \pmod{\mathfrak{p}^j}\}.$$

Then, by [Okazaki 91, Proposition 3], we have

$$\left(\frac{K}{\mathfrak{p}}\right) = \begin{cases} 1 & \text{if } f = 3, \\ -1 & \text{if } f = 2, \\ 0 & \text{if } f \leq 1, \end{cases} \quad D_{\mathfrak{p}} = \begin{cases} \mathfrak{p}^{2-2[f/2]} & \text{if } \mathfrak{p} \nmid (\alpha)_F, \\ \mathfrak{p}^3 & \text{if } \mathfrak{p} \mid (\alpha)_F. \end{cases}$$

When  $\mathfrak{p} \mid (\alpha)_F$ , we have  $\alpha + \mathfrak{p}^2 \subset \pi_{\mathfrak{p}} \mathfrak{o}_{\mathfrak{p}}^{\times}$ , thus  $f = 1$ , and hence  $\left(\frac{K}{\mathfrak{p}}\right) = 0$ ; moreover,  $D_{\mathfrak{p}} = \mathfrak{p}^3$ . Thus our proposition holds in this case. Therefore, we may assume  $\mathfrak{p} \nmid (\alpha)_F$ . To prove our proposition, we need to show only that

$$f = 3 \iff (a_1, a_2) \in A_m,$$

$$f \geq 2 \iff (a_1, a_2) \in A'_m.$$

We first assume that  $m \equiv 1 \pmod{8\mathbf{Z}}$ . Then  $\text{ord}_{\mathfrak{p}}(\alpha) = 0$ , and  $\{t \in \mathbf{Z} \mid 0 \leq t < 2^j, 2 \nmid t\}$  is a complete set of representatives of  $(\mathfrak{o}_F/\mathfrak{p}^j)^{\times}$  for  $j \geq 1$ . Therefore, for  $j \geq 1$ , there exists  $\gamma \in \mathfrak{o}_F$  such that  $\gamma^2 \equiv \alpha \pmod{\mathfrak{p}^j}$  if and only if there exists  $t \in \{t \in \mathbf{Z} \mid 0 \leq t < 2^j, 2 \nmid t\}$  such that  $\alpha - t^2 \in \mathfrak{p}^j$ . Now we have

$$\mathfrak{p}^2 = [4, 2l - r + \omega], \quad \mathfrak{p}^3 = [8, -2l(-1)^r - r + \omega].$$

Since  $\alpha - t^2 = (a_1 + a_2(2l(-1)^r + r) - t^2) + a_2(-2l(-1)^r - r + \omega)$  and  $1 \equiv 1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \pmod{8\mathbf{Z}}$ , we have

$$f = 3 \iff \text{there exists } t \in \{1, 3, 5, 7\}$$

$$\text{such that } \alpha - t^2 \in \mathfrak{p}^3$$

$$\iff (a_1, a_2) \in A_m.$$

Moreover, since  $\alpha - t^2 = (a_1 - a_2(2l - r) - t^2) + a_2(2l - r + \omega)$  and  $1 \equiv 1^2 \equiv 3^2 \pmod{4\mathbf{Z}}$ , we have

$$f \geq 2 \iff \text{there exists } t \in \{1, 3\} \text{ such that } \alpha - t^2 \in \mathfrak{p}^2$$

$$\iff (a_1, a_2) \in A'_m.$$

Thus the assertion is proved in this case. Now assume that  $m \equiv 5 \pmod{8\mathbf{Z}}$ . Then  $\text{ord}_{\mathfrak{p}}(\alpha) = 0$ , and  $\{u + v\omega \mid 0 \leq u, v < 2^j, (u, v) \notin (2\mathbf{Z})^2\}$  is a complete set of representatives of  $(\mathfrak{o}_F/\mathfrak{p}^j)^{\times}$  for  $j \geq 1$ . Thus for  $j \geq 1$ , there exists  $\gamma \in \mathfrak{o}_F$  such that  $\gamma^2 \equiv \alpha \pmod{\mathfrak{p}^j}$  if and only if there exists  $(u, v) \in \{(u, v) \in \mathbf{Z}^2 \mid 0 \leq u, v < 2^j, (u, v) \notin (2\mathbf{Z})^2\}$  such that  $\alpha - (u + v\omega)^2 \in \mathfrak{p}^j = [2^j, 2^j\omega]$ . Since  $\alpha - (u + v\omega)^2 = (a_1 - u^2 - (2l+1)v^2) + (a_2 - 2uv - v^2)\omega$  and

$$(a_1 - u^2 - (2l+1)v^2, a_2 - 2uv - v^2) \equiv \begin{cases} (a_1 - 1, a_2) & \text{if } 2 \nmid u \text{ and } 4 \mid v, \\ (a_1 - 5, a_2) & \text{if } 2 \nmid u, 2 \mid v, \text{ and } 4 \nmid v, \\ (a_1 - 2l - 2, a_2 - 3) & \text{if } 2 \nmid u, 2 \nmid v, \text{ and } 4 \mid u - v, \\ (a_1 - 2l - 2, a_2 - 7) & \text{if } 2 \nmid u, 2 \nmid v, \text{ and } 4 \nmid u - v, \\ (a_1 - 2l - 1, a_2 - 1) & \text{if } 4 \mid u \text{ and } 2 \nmid v, \\ (a_1 - 2l - 5, a_2 - 5) & \text{if } 2 \mid u, 4 \nmid u, \text{ and } 2 \nmid v, \end{cases} \pmod{8\mathbf{Z}},$$

we have

$$f = 3 \iff \text{there exists } (u, v) \in \{(u, v) \mid 0 \leq u, v \leq 7,$$

$$(u, v) \notin (2\mathbf{Z})^2\}$$

$$\text{such that } \alpha - (u + v\omega)^2 \in [8, 8\omega]$$

$$\iff (a_1, a_2) \in A_m.$$

Moreover, since

$$(a_1 - u^2 - (2l + 1)v^2, a_2 - 2uv - v^2) \equiv \begin{cases} (a_1 - 1, a_2) & \text{if } 2 \nmid u \text{ and } 2 \mid v, \\ (a_1 - 2l - 2, a_2 - 3) & \text{if } 2 \nmid u \text{ and } 2 \nmid v, \\ (a_1 - 2l - 1, a_2 - 1) & \text{if } 2 \mid u \text{ and } 2 \nmid v, \end{cases} \pmod{4\mathbf{Z}},$$

we have

$$f \geq 2 \iff \text{there exists } (u, v) \in \{(u, v) \mid 0 \leq u, v \leq 3, (u, v) \notin (2\mathbf{Z})^2\} \text{ such that } \alpha - (u + v\omega)^2 \in [4, 4\omega] \iff (a_1, a_2) \in A'_m.$$

This completes the proof. □

**Remark 3.7.** Let  $F, m, \alpha,$  and  $K$  be as in Proposition 3.4. Let  $\mathfrak{p}$  be an *even* prime ideal of  $F$ . When  $\mathfrak{p}^2 \mid (\alpha)_F$ , we cannot apply this case to Proposition 3.6. However we can take  $\alpha_1$ , instead of  $\alpha$ , satisfying

$$K = F(\sqrt{\alpha_1}), \quad \alpha_1 \in \mathfrak{o}_F, \quad \mathfrak{p}^2 \nmid (\alpha_1)_F \tag{3-5}$$

as follows:

- (i) If  $m \equiv 1 \pmod{8\mathbf{Z}}$ , then we take  $\gamma \in \mathfrak{o}_F$  such that  $(\gamma)_F = (\mathfrak{p}^\sigma)^{h_F} \in P(F)$ , and put

$$\alpha_1 = \alpha(2^{-1}\gamma)^{2[\text{ord}_{\mathfrak{p}}(\alpha)/2]}.$$

Then  $\alpha_1$  satisfies (3-5), since  $(2^{-1}\gamma)_F = \mathfrak{p}^{-1}(\mathfrak{p}^\sigma)^{h_F-1}$ .

- (ii) If  $m \equiv 5 \pmod{8\mathbf{Z}}$ , set

$$\alpha_1 = \alpha \cdot 2^{-2[\text{ord}_{\mathfrak{p}}(\alpha)/2]}.$$

Then  $\alpha_1$  satisfies (3-5), since  $\mathfrak{p} = (2)_F$ .

Thus, by Proposition 3.6 and Remark 3.7, we can immediately determine  $D_{\mathfrak{p}}$  and  $(\frac{K}{\mathfrak{p}})$  for an *even* prime ideal  $\mathfrak{p}$ .

### 3.4 Hecke L-Values

Finally, we explain the method for computing  $L_F(0, \chi_{K/F})$  that was established by [Shintani 76] for totally real algebraic number fields  $F$ . [Okazaki 91] deals with Shintani's formula for the case of real quadratic fields  $F$ , and we observe that the ideal character corresponding to  $K/F$  is expressed by the Legendre symbols and the Hilbert symbols. Applying this result to Shintani's formula, we obtain Formula (3-6) with

simple calculation. We note that the conductor of  $\chi_{K/F}$  is equal to  $D_{K/F}$  (cf. [Weil 67, Chapter XIII, Theorem 9]), and we can determine  $D_{K/F}$  by Proposition 3.1 and Proposition 3.6.

Let  $F, m, \alpha, K, a_1,$  and  $a_2$  be as in Proposition 3.4. Let  $\varepsilon$  be the fundamental unit of  $F$  that is greater than 1, and set

$$\varepsilon_+ = \begin{cases} \varepsilon & \text{if } \varepsilon \gg 0, \\ \varepsilon^2 & \text{otherwise.} \end{cases}$$

We take  $e, e' \in \mathbf{Z}$  such that  $\varepsilon_+ = e + e'\omega$ . Let  $\mathfrak{a}_1, \dots, \mathfrak{a}_{h_F^+}$  be a complete set of representatives of  $\text{Cl}^+(F)$  such that  $\mathfrak{a}_\mu \subset \mathfrak{o}_F$  for all  $\mu$ . For  $1 \leq \mu \leq h_F^+$ , we can determine uniquely integers  $d_\mu, d'_\mu,$  and  $d''_\mu$  such that

$$d_\mu[d'_\mu, d''_\mu + \omega] = \mathfrak{a}_\mu D_{K/F},$$

$d_\mu, d'_\mu > 0,$  and  $0 \leq d''_\mu < d'_\mu$ ; we take integers  $s_\mu, s'_\mu,$  and  $Q_\mu$  as follows:

- (i) If  $\mathfrak{a}_\mu D_{K/F} \in P(F)$ , then take  $s_\mu, s'_\mu$  such that

$$(s_\mu + s'_\mu\omega)_F = \mathfrak{a}_\mu D_{K/F},$$

and set

$$Q_\mu = 1.$$

- (ii) If  $\mathfrak{a}_\mu D_{K/F} \notin P(F)$ , then we can take an odd prime ideal  $\mathfrak{q}_\mu$  of  $F$  such that  $\mathfrak{q}_\mu$  splits in  $F/\mathbf{Q}$ ,  $\text{gcd}(\mathfrak{q}_\mu, (\alpha)_F) = \mathfrak{o}_F,$  and  $\mathfrak{q}_\mu \mathfrak{a}_\mu D_{K/F} \in P(F)$ . Then  $\mathfrak{q}_\mu = [\mathfrak{q}_\mu, r_\mu + \omega]$  with  $\mathfrak{q}_\mu, r_\mu \in \mathbf{Z}$ . We take  $s_\mu, s'_\mu$  such that

$$(s_\mu + s'_\mu\omega)_F = \mathfrak{q}_\mu \mathfrak{a}_\mu D_{K/F},$$

and set

$$Q_\mu = \left(\frac{a_1 - a_2 r_\mu}{\mathfrak{q}_\mu}\right).$$

Moreover, for  $1 \leq i \leq d_\mu$  and  $1 \leq j \leq e'd_\mu d'_\mu,$  we take the integer  $1 \leq r_{\mu ij} \leq e'd_\mu d'_\mu$  such that

$$r_{\mu ij} \equiv e'd'_\mu i - (e + e'(d''_\mu + 1))j \pmod{e'd_\mu d'_\mu \mathbf{Z}},$$

and we set

$$B_{\mu ij} = 4^{-1}(e'd_\mu d'_\mu)^{-2}((2e + e')(r_{\mu ij}^2 + j^2) + 4r_{\mu ij}j) - 4^{-1}(e'd_\mu d'_\mu)^{-1}(2e + e' + 2)(r_{\mu ij} + j) + 12^{-1}(2e + e' + 3),$$

$$u_{\mu ij} = (e'd_\mu d'_\mu)^{-1}\left(r_{\mu ij}s_\mu + j\left(es_\mu + e's'_\mu \frac{m-1}{4}\right)\right),$$

$$v_{\mu ij} = (e'd_\mu d'_\mu)^{-1}\left(r_{\mu ij}s'_\mu + j(es'_\mu + e's_\mu + e's'_\mu)\right).$$

Note that  $u_{\mu ij}, v_{\mu ij} \in \mathbf{Z}$ . Now, for an *odd* prime ideal  $\mathfrak{p}$  of  $F$  and  $u + v\omega \in \mathfrak{o}_F$ , we set

$$\chi_{\mathfrak{p}}(u+v\omega) = \begin{cases} \left(\frac{N_{F/\mathbf{Q}}(u+v\omega)}{p}\right) & \text{if } \mathfrak{p} \text{ remains prime in } F/\mathbf{Q}, \\ \left(\frac{u-vr}{p}\right) & \text{otherwise,} \end{cases}$$

where  $p$  is the prime number in  $\mathbf{Q}$  that lies below  $\mathfrak{p}$ , and  $r$  an integer satisfying  $\mathfrak{p} = [p, r + \omega]$ . For an *even* prime ideal  $\mathfrak{p}$  of  $F$  dividing  $D_{K/F}$  and  $\beta \in \mathfrak{o}_F$ , we set

$$\chi_{\mathfrak{p}}(\beta) = \begin{cases} (\beta, \alpha)_{F_{\mathfrak{p}}} & \text{if } \mathfrak{p} \nmid (\beta)_F, \\ 0 & \text{otherwise,} \end{cases}$$

where  $(\ , \ )_{F_{\mathfrak{p}}}$  is the Hilbert symbol (and  $\alpha$  is retained as in Proposition 3.4). Then we obtain

$$\begin{aligned} L_F(0, \chi_{K/F}) &= \sum_{\mu=1}^{h_F^+} \operatorname{sgn}(N_{F/\mathbf{Q}}(s_{\mu} + s'_{\mu}\omega)) Q_{\mu} \\ &\quad \cdot \left( \sum_{i=1}^{d_{\mu}} \sum_{j=1}^{e' d_{\mu} d'_{\mu}} B_{\mu ij} \prod_{\substack{\mathfrak{p} | D_{K/F} \\ \mathfrak{p} \in \mathfrak{h}}} \chi_{\mathfrak{p}}(u_{\mu ij} + v_{\mu ij}\omega) \right. \\ &\quad \left. + \sum_{l=1}^{d_{\mu}} \frac{2l - d_{\mu}}{2d_{\mu}} \prod_{\substack{\mathfrak{p} | D_{K/F} \\ \mathfrak{p} \in \mathfrak{h}}} \chi_{\mathfrak{p}}(ld_{\mu}^{-1}(s_{\mu} + s'_{\mu}\omega)) \right). \end{aligned} \quad (3-6)$$

Thus, if we can compute the Hilbert symbol  $(\beta, \alpha)_{F_{\mathfrak{p}}}$  for an *even* prime  $\mathfrak{p}$  and  $\alpha, \beta \in \mathfrak{o}_F - \{0\}$  satisfying  $\mathfrak{p} \nmid (\beta)_F$ , we can determine  $L_F(0, \chi_{K/F})$  by (3-6). We note that the Hilbert symbol

$$(\ , \ )_{F_{\mathfrak{p}}} : F_{\mathfrak{p}}^{\times} \times F_{\mathfrak{p}}^{\times} \longrightarrow \{\pm 1\}$$

satisfies

$$(a, b)_{F_{\mathfrak{p}}} = (b, a)_{F_{\mathfrak{p}}}, \quad (3-7a)$$

$$(a, bc)_{F_{\mathfrak{p}}} = (a, b)_{F_{\mathfrak{p}}} (a, c)_{F_{\mathfrak{p}}}, \quad (3-7b)$$

for  $a, b, c \in F_{\mathfrak{p}}^{\times}$  and naturally induces the mapping

$$F_{\mathfrak{p}}^{\times} / (F_{\mathfrak{p}}^{\times})^2 \times F_{\mathfrak{p}}^{\times} / (F_{\mathfrak{p}}^{\times})^2 \longrightarrow \{\pm 1\} \quad (3-8)$$

(for the Hilbert symbol, see [Neukirch 86], for example).

### 3.5 Hilbert Symbol for $m \equiv 1 \pmod{8\mathbf{Z}}$

We first give a method for computing the Hilbert symbol when  $m \equiv 1 \pmod{8\mathbf{Z}}$ .

**Lemma 3.8.** *Let  $\mu \in \mathbf{Z}_2^{\times}$  satisfying  $\mu^2 \in \mathbf{Z}$ . Then  $u \equiv \mu \pmod{2^j \mathbf{Z}_2}$  if and only if  $u^2 \equiv \mu^2 \pmod{2^{j+1} \mathbf{Z}}$  and  $u \equiv \mu \pmod{4\mathbf{Z}_2}$  for  $u \in \mathbf{Z}$  and  $2 \leq j \in \mathbf{Z}$ .*

*Proof:* Suppose  $u \equiv \mu \pmod{2^j \mathbf{Z}_2}$  with  $u \in \mathbf{Z}$  and  $2 \leq j \in \mathbf{Z}$ . Then  $u \equiv \mu \pmod{4\mathbf{Z}_2}$ . Since  $u + \mu \equiv 2\mu \pmod{4\mathbf{Z}_2}$  and  $\mu \in \mathbf{Z}_2^{\times}$ , we have  $2^{-1}(u + \mu) \in \mu + 2\mathbf{Z}_2 = \mathbf{Z}_2^{\times}$ , and hence  $\operatorname{ord}_2(u + \mu) = 1$ . Thus  $u^2 - \mu^2 = (u - \mu)(u + \mu) \in 2^{j+1} \mathbf{Z}_2$ , that is,  $u^2 - \mu^2 \in 2^{j+1} \mathbf{Z}$ . Conversely, if  $u^2 \equiv \mu^2 \pmod{2^{j+1} \mathbf{Z}}$  and  $u \equiv \mu \pmod{4\mathbf{Z}_2}$ , then  $\operatorname{ord}_2(u + \mu) = 1$ , and hence  $u - \mu = (u^2 - \mu^2)(u + \mu)^{-1} \in 2^j \mathbf{Z}_2$ .  $\square$

**Lemma 3.9.** *Let  $F = \mathbf{Q}(\sqrt{m})$  be a real quadratic field with a square-free integer  $m$  satisfying  $m \equiv 1 \pmod{8\mathbf{Z}}$ . Let  $\mathfrak{p} = [2, r + \omega]$  be an even prime ideal of  $F$ , where  $r = 0$  or  $1$ . Then, for  $u \in \mathbf{Z}$  and  $2 \leq j \in \mathbf{Z}$ , it follows that  $u \equiv \sqrt{m} \pmod{2^j \mathfrak{o}_{\mathfrak{p}}}$  if and only if  $u^2 \equiv m \pmod{2^{j+1} \mathbf{Z}}$  and  $u \equiv -2r - 1 \pmod{4\mathbf{Z}}$ .*

*Proof:* Since  $m \equiv 1 \pmod{8\mathbf{Z}}$ , we have  $F_{\mathfrak{p}} \cong \mathbf{Q}_2$ . Thus, by Lemma 3.8, we see that  $u \equiv \sqrt{m} \pmod{2^j \mathfrak{o}_{\mathfrak{p}}}$  if and only if  $u^2 \equiv m \pmod{2^{j+1} \mathbf{Z}}$  and  $u \equiv \sqrt{m} \pmod{4\mathfrak{o}_{\mathfrak{p}}}$  for  $u \in \mathbf{Z}$  and  $2 \leq j \in \mathbf{Z}$ . Since  $2^{-1}(2r + 1 + \sqrt{m}) = r + \omega \in \mathfrak{p} \subset 2\mathfrak{o}_{\mathfrak{p}}$ , we have  $\sqrt{m} \equiv -2r - 1 \pmod{4\mathfrak{o}_{\mathfrak{p}}}$ . Thus  $u \equiv \sqrt{m} \pmod{4\mathfrak{o}_{\mathfrak{p}}}$  if and only if  $u \equiv -2r - 1 \pmod{4\mathbf{Z}}$ . This completes the proof.  $\square$

From the two lemmas above, we obtain the following result:

**Proposition 3.10.** *Let  $F$ ,  $m$ ,  $\mathfrak{p}$ , and  $r$  be as in Lemma 3.9. Let  $\beta_1, \beta_2 \in \mathfrak{o}_F - \{0\}$ , and set  $\beta_j = c_j + d_j\omega$  with  $c_j, d_j \in \mathbf{Z}$ . We take  $u_j \in \mathbf{Z}$  such that  $u_j^2 \equiv m \pmod{2^{\operatorname{ord}_{\mathfrak{p}}(\beta_j) - l_j + 5} \mathbf{Z}}$  and  $u_j \equiv -2r - 1 \pmod{4\mathbf{Z}}$ , where  $l_j = \min\{\operatorname{ord}_2(2c_j + d_j), \operatorname{ord}_2(d_j)\}$ . We set  $t_j = 2^{-\operatorname{ord}_{\mathfrak{p}}(\beta_j)}(c_j + d_j(1 + u_j)/2)$ . Then we have*

$$\begin{aligned} &(\beta_1, \beta_2)_{F_{\mathfrak{p}}} \\ &= (-1)^{(t_1-1)(t_2-1)/4 + \operatorname{ord}_{\mathfrak{p}}(\beta_1)(t_2^2-1)/8 + \operatorname{ord}_{\mathfrak{p}}(\beta_2)(t_1^2-1)/8}. \end{aligned}$$

*Proof:* Since  $\mathfrak{o}_{\mathfrak{p}}^{\times} = (1 + 2^3 \mathfrak{o}_{\mathfrak{p}}) \cup (3 + 2^3 \mathfrak{o}_{\mathfrak{p}}) \cup (5 + 2^3 \mathfrak{o}_{\mathfrak{p}}) \cup (7 + 2^3 \mathfrak{o}_{\mathfrak{p}})$ , we have  $(\mathfrak{o}_{\mathfrak{p}}^{\times})^2 \subset 1 + 2^3 \mathfrak{o}_{\mathfrak{p}}$ . Conversely, for any element  $1 + 2^3 y \in 1 + 2^3 \mathfrak{o}_{\mathfrak{p}}$ , we can take a root  $x \in \mathfrak{o}_{\mathfrak{p}}$  of the polynomial  $2X^2 + X - y$  by Hensel's lemma, then  $1 + 2^3 y = (1 + 2^2 x)^2$ , and hence  $1 + 2^3 \mathfrak{o}_{\mathfrak{p}} \subset (\mathfrak{o}_{\mathfrak{p}}^{\times})^2$ . Therefore,

$$(\mathfrak{o}_{\mathfrak{p}}^{\times})^2 = 1 + 2^3 \mathfrak{o}_{\mathfrak{p}}. \quad (3-9)$$

Now set  $e_j = \operatorname{ord}_{\mathfrak{p}}(\beta_j)$ . Since  $\beta_j = 2^{l_j-1}(2^{-l_j}(2c_j + d_j) + 2^{-l_j}d_j\sqrt{m})$ , we have  $e_j \geq l_j - 1$ . Thus  $u_j \equiv \sqrt{m} \pmod{2^{e_j-l_j+4} \mathfrak{o}_{\mathfrak{p}}}$  by Lemma 3.9, and hence  $d_j(1 + u_j)/2 \equiv d_j\omega \pmod{2^{e_j+3} \mathfrak{o}_{\mathfrak{p}}}$ . Therefore,  $t_j = 2^{-e_j}(c_j + d_j(1 + u_j)/2) \equiv 2^{-e_j}\beta_j \pmod{2^3 \mathfrak{o}_{\mathfrak{p}}}$ , that is,  $t_j(\mathfrak{o}_{\mathfrak{p}}^{\times})^2 =$

$2^{-e_j} \beta_j(\mathfrak{o}_{\mathfrak{p}}^\times)^2$ . It follows that  $(\beta_1, \beta_2)_{F_{\mathfrak{p}}} = (2^{e_1} t_1, 2^{e_2} t_2)_{F_{\mathfrak{p}}}$ . Since  $F_{\mathfrak{p}} \cong \mathbf{Q}_2$ , we have

$$(2^{e_1} t_1, 2^{e_2} t_2)_{F_{\mathfrak{p}}} = (-1)^{(t_1-1)(t_2-1)/4 + e_1(t_2^2-1)/8 + e_2(t_1^2-1)/8}$$

(cf. [Neukirch 86, Chapter III, Theorem 5.6], for example). This completes the proof.  $\square$

**Remark 3.11.** It is well known that  $X^2 \equiv a \pmod{2^j \mathbf{Z}}$  has exactly four solutions modulo  $2^j \mathbf{Z}$  for  $a \in 1 + 8\mathbf{Z}$  and  $3 \leq j \in \mathbf{Z}$ . If  $x_j$  is one of the solutions, then all the solutions are  $x_j, x_j + 2^{j-1}, -x_j$ , and  $-x_j + 2^{j-1}$ , since  $x_j$  is odd. Now we can inductively determine  $x_j$  by

$$x_3 = 1, \\ x_j = \begin{cases} x_{j-1} & \text{if } 2 \mid 2^{-j+1}(x_{j-1}^2 - a), \\ x_{j-1} + 2^{j-2} & \text{otherwise,} \end{cases}$$

for  $4 \leq j \in \mathbf{Z}$ . To prove this, we assume that  $x_{j-1}$  is a solution of  $X^2 \equiv a \pmod{2^{j-1} \mathbf{Z}}$  with  $j \geq 4$ , and set

$$c = \begin{cases} 0 & \text{if } 2 \mid 2^{-j+1}(x_{j-1}^2 - a), \\ 1 & \text{otherwise,} \end{cases}$$

and  $x_j = x_{j-1} + c2^{j-2}$ . Since  $2^{-j+1}(x_{j-1}^2 - a) \equiv c \equiv -x_{j-1}c \pmod{2\mathbf{Z}}$ , we have  $x_{j-1}^2 - a \equiv -x_{j-1}c2^{j-1} \pmod{2^j \mathbf{Z}}$ . Thus

$$x_j^2 = x_{j-1}^2 + x_{j-1}c2^{j-1} + c^22^{j+j-4} \\ \equiv x_{j-1}^2 - (x_{j-1}^2 - a) = a \pmod{2^j \mathbf{Z}}.$$

From this, we can easily find  $u_j$  of Proposition 3.10 and  $u$  of Proposition 3.14 below.

From Proposition 3.10 and Remark 3.11, we can immediately compute the Hilbert symbol when  $m \equiv 1 \pmod{8\mathbf{Z}}$ .

### 3.6 Hilbert Symbol for $m \equiv 5 \pmod{8\mathbf{Z}}$

Now we explain a method for computing the Hilbert symbol when  $m \equiv 5 \pmod{8\mathbf{Z}}$ .

By [Okazaki 91, Proposition 4], we have

**Proposition 3.12.** *Let  $F = \mathbf{Q}(\sqrt{m})$  be a real quadratic field with a square-free integer  $m$  satisfying  $m \equiv 5 \pmod{8\mathbf{Z}}$ . Let  $\mathfrak{p}$  be an even prime ideal of  $F$ . Put  $\tau = 1 + 4\omega$  and  $\xi = (m - 9)/4 + \omega$ . Then  $F_{\mathfrak{p}}^\times / (F_{\mathfrak{p}}^\times)^2$  is generated by  $-1, \tau, \xi, 2$ , and we have*

$$(b, a)_{F_{\mathfrak{p}}} = \begin{cases} 1 & \text{if } (b, a) = (-1, -1) \\ & \text{or } (-1, \tau) \text{ or } (-1, 2) \\ & \text{or } (\tau, \tau) \text{ or } (\tau, \xi) \\ & \text{or } (\xi, 2) \text{ or } (2, 2), \\ -1 & \text{if } (b, a) = (-1, \xi) \text{ or } (\tau, 2) \text{ or } (\xi, \xi). \end{cases}$$

From this proposition, we can take

$$\{(-1)^{i_1} \tau^{i_2} \xi^{i_3} 2^{i_4} \mid i_1, i_2, i_3, i_4 \in \{0, 1\}\}$$

as a complete set of representatives of  $F_{\mathfrak{p}}^\times / (F_{\mathfrak{p}}^\times)^2$ . Thus for any  $\beta_1, \beta_2$  in  $\mathfrak{o}_F - \{0\}$ , we can compute  $(\beta_1, \beta_2)_{F_{\mathfrak{p}}}$  by (3-7a), (3-7b), (3-8), and Proposition 3.12, if we can find  $l_{j1}, l_{j2}, l_{j3}, l_{j4} \in \{0, 1\}$  such that  $\beta_j (F_{\mathfrak{p}}^\times)^2 = (-1)^{l_{j1}} \tau^{l_{j2}} \xi^{l_{j3}} 2^{l_{j4}} (F_{\mathfrak{p}}^\times)^2$  for  $j = 0, 1$ . Now we have  $\beta_j (-1)^{i_{j1}} \tau^{i_{j2}} \xi^{i_{j3}} 2^{-\text{ord}_{\mathfrak{p}}(\beta_j)} \in \mathfrak{o}_F \cap \mathfrak{o}_{\mathfrak{p}}^\times$  for any  $i_{j1}, i_{j2}, i_{j3} \in \{0, 1\}$ , and

$$\beta_j (-1)^{i_{j1}} \tau^{i_{j2}} \xi^{i_{j3}} 2^{-\text{ord}_{\mathfrak{p}}(\beta_j)} \in (\mathfrak{o}_{\mathfrak{p}}^\times)^2 \\ \iff \beta_j (F_{\mathfrak{p}}^\times)^2 = (-1)^{i_{j1}} \tau^{i_{j2}} \xi^{i_{j3}} 2^{i_{j4}} (F_{\mathfrak{p}}^\times)^2,$$

where  $i_{j4} = 0$  or  $1$  according as  $2 \mid \text{ord}_{\mathfrak{p}}(\beta_j)$  or  $2 \nmid \text{ord}_{\mathfrak{p}}(\beta_j)$ . Thus, for an element  $\delta$  of  $\mathfrak{o}_F$ , we wish to give an effective method to see that  $\delta \in (\mathfrak{o}_{\mathfrak{p}}^\times)^2$ . (In fact, this will be given in Proposition 3.14 below.)

For  $\gamma \in (\mathbf{Q}_2)^2$ , we denote by  $\gamma^{1/2}$  the root of  $X^2 - \gamma$  contained in  $(\bigsqcup_{j=-\infty}^{\infty} 2^j(1 + 4\mathbf{Z}_2)) \cup \{0\}$ . Note that  $\gamma_1^{1/2} \gamma_2^{1/2} = (\gamma_1 \gamma_2)^{1/2}$  for  $\gamma_1, \gamma_2 \in (\mathbf{Q}_2)^2$ .

**Lemma 3.13.** *Let  $F, m$ , and  $\mathfrak{p}$  be as in Proposition 3.12. Let  $\delta \in F_{\mathfrak{p}}$ . Then  $\delta \in (\mathfrak{o}_{\mathfrak{p}}^\times)^2$  if and only if*

- (i)  $N_{F_{\mathfrak{p}}/\mathbf{Q}_2}(\delta) \in (\mathbf{Z}_2^\times)^2$ ; and
- (ii)  $\text{Tr}_{F_{\mathfrak{p}}/\mathbf{Q}_2}(\delta) + 2N_{F_{\mathfrak{p}}/\mathbf{Q}_2}(\delta)^{1/2}, \\ \text{Tr}_{F_{\mathfrak{p}}/\mathbf{Q}_2}(\delta) - 2N_{F_{\mathfrak{p}}/\mathbf{Q}_2}(\delta)^{1/2} \in (\mathbf{Z}_2)^2 \cup m(\mathbf{Z}_2)^2.$

*Proof:* In this proof, we abbreviate  $\text{Tr}_{F_{\mathfrak{p}}/\mathbf{Q}_2}$  and  $N_{F_{\mathfrak{p}}/\mathbf{Q}_2}$  by  $\text{Tr}$  and  $N$ . Since  $\mathfrak{o}_{\mathfrak{p}}$  is the topological closure of  $\mathfrak{o}_F$  in  $F_{\mathfrak{p}}$ , we have

$$\mathfrak{o}_{\mathfrak{p}} = \{2^{-1}(x + y\sqrt{m}) \mid x, y \in \mathbf{Z}_2, x - y \in 2\mathbf{Z}_2\}.$$

We first prove the ‘‘only if’’ part. Since  $\delta \in (\mathfrak{o}_{\mathfrak{p}}^\times)^2$ , there exist  $x, y \in \mathbf{Z}_2$  such that  $\delta = (2^{-1}(x + y\sqrt{m}))^2$ , and hence  $\text{Tr}(\delta) = 2^{-1}(x^2 + y^2m)$  and  $N(\delta) = (4^{-1}(x^2 - y^2m))^2$ . Since  $\text{ord}_{\mathfrak{p}}(\delta) = 0$ , we have  $N(\delta) \in (\mathbf{Z}_2^\times)^2$ . Now we have  $N(\delta)^{1/2} = (-1)^l 4^{-1}(x^2 - y^2m)$  with  $l = 0$  or  $1$ . Therefore,

$$\text{Tr}(\delta) + (-1)^l 2N(\delta)^{1/2} = x^2 \in (\mathbf{Z}_2)^2, \\ \text{Tr}(\delta) - (-1)^l 2N(\delta)^{1/2} = y^2m \in m(\mathbf{Z}_2)^2.$$

Now we prove the ‘‘if’’ part. Since  $N(\delta) \in (\mathbf{Z}_2^\times)^2$ , we have  $\delta \in \mathfrak{o}_{\mathfrak{p}}^\times$ . Set  $\delta = 2^{-1}(a + b\sqrt{m})$  with  $a, b \in \mathbf{Z}_2$ . Since  $\text{Tr}(\delta)^2 - 4N(\delta) = b^2m$ , we have

$$a = \text{Tr}(\delta), \quad b = (-1)^j (m^{-1}(\text{Tr}(\delta)^2 - 4N(\delta)))^{1/2}$$

with  $j = 0$  or  $1$ . On the other hand, since  $(\text{Tr}(\delta)^2 - 4N(\delta)) \in m(\mathbf{Z}_2)^2$ , we have  $\text{Tr}(\delta) + (-1)^l 2N(\delta)^{1/2} \in (\mathbf{Z}_2)^2$  and  $\text{Tr}(\delta) - (-1)^l 2N(\delta)^{1/2} \in m(\mathbf{Z}_2)^2$  with  $l = 0$  or  $1$ . Thus we set

$$\begin{aligned} x &= (-1)^j (\text{Tr}(\delta) + (-1)^l 2N(\delta)^{1/2})^{1/2} \quad (\in \mathbf{Z}_2), \\ y &= (m^{-1}(\text{Tr}(\delta) - (-1)^l 2N(\delta)^{1/2}))^{1/2} \quad (\in \mathbf{Z}_2). \end{aligned}$$

Then

$$\begin{aligned} &(2^{-1}(x + y\sqrt{m}))^2 \\ &= 2^{-1}(\text{Tr}(\delta) + (-1)^j (m^{-1}(\text{Tr}(\delta)^2 - 4N(\delta)))^{1/2} \sqrt{m}) \\ &= 2^{-1}(a + b\sqrt{m}) = \delta. \end{aligned}$$

Since  $\delta \in \mathfrak{o}_{\mathfrak{p}}^{\times}$ , we have  $\delta \in (\mathfrak{o}_{\mathfrak{p}}^{\times})^2$ . This completes the proof.  $\square$

From the above lemma, we obtain the following result:

**Proposition 3.14.** *Let  $F$ ,  $m$ , and  $\mathfrak{p}$  be as in Proposition 3.12. Let  $\delta \in \mathfrak{o}_F$ , and set  $\delta = 2^{-1}(a + b\sqrt{m})$  with  $a, b \in \mathbf{Z}$ . Then  $\delta \in (\mathfrak{o}_{\mathfrak{p}}^{\times})^2$  if and only if*

- (i)  $8 \mid 4^{-1}(a^2 - b^2m) - 1$ ; and
- (ii)  $b = 0$  and  $4 \mid 2^{-1}a - 1$ ; or  
 $b \neq 0$  and  $4 \mid a + 1$ ; or  
 $b \neq 0$ ,  $\text{ord}_2(a) = 1$ ,  $2 \mid r$ , and  $4 \mid 2^{-r}(a + 2u) - 1$ ,

where  $u$  is a rational integer such that  $u^2 \equiv 4^{-1}(a^2 - b^2m) \pmod{2^{2\text{ord}_2(b)}\mathbf{Z}}$  and  $u \equiv 1 \pmod{4\mathbf{Z}}$ , and  $r = \text{ord}_2(a + 2u)$ .

*Proof:* In this proof, again abbreviate  $\text{Tr}_{F_{\mathfrak{p}}/\mathbf{Q}_2}$  and  $N_{F_{\mathfrak{p}}/\mathbf{Q}_2}$  by  $\text{Tr}$  and  $N$ . Then  $\text{Tr}(\delta) = a$  and  $N(\delta) = 4^{-1}(a^2 - b^2m) \in \mathbf{Z}$ . By Lemma 3.13, we have

$$\begin{aligned} \delta \in (\mathfrak{o}_{\mathfrak{p}}^{\times})^2 &\iff N(\delta) \in (\mathbf{Z}_2^{\times})^2, \\ &\text{Tr}(\delta) + 2N(\delta)^{1/2}, \\ &\text{Tr}(\delta) - 2N(\delta)^{1/2} \in (\mathbf{Z}_2)^2 \cup m(\mathbf{Z}_2)^2. \end{aligned} \tag{3-10}$$

Here, by (3-9), we have  $(\mathbf{Z}_2^{\times})^2 = 1 + 8\mathbf{Z}_2$ , and hence

$$(\mathbf{Z}_2)^2 \cup m(\mathbf{Z}_2)^2 = \left( \bigcup_{j=0}^{\infty} 4^j(1 + 4\mathbf{Z}_2) \right) \cup \{0\}.$$

Since  $N(\delta) \in \mathbf{Z}$ , we have

$$N(\delta) \in (\mathbf{Z}_2^{\times})^2 \iff 8 \mid 4^{-1}(a^2 - b^2m) - 1. \tag{3-11}$$

Henceforth, until the end of this proof, we may assume  $N(\delta) \in (\mathbf{Z}_2^{\times})^2$ . When  $b = 0$ , we have  $N(\delta)^{1/2} = (-1)^l 2^{-1}a \in \mathbf{Z}_2^{\times}$  with  $l = 0$  or  $1$ , and hence

$$\begin{aligned} \text{Tr}(\delta) + (-1)^l 2N(\delta)^{1/2} &= 4 \cdot 2^{-1}a, \\ \text{Tr}(\delta) - (-1)^l 2N(\delta)^{1/2} &= 0. \end{aligned}$$

Note that  $2^{-1}a \in \mathbf{Z}_2^{\times} \cap \mathbf{Z} = 1 + 2\mathbf{Z}$ . If  $4 \mid 2^{-1}a - 1$ , then  $4 \cdot 2^{-1}a \in 4(1 + 4\mathbf{Z}) \subset (\mathbf{Z}_2)^2 \cup m(\mathbf{Z}_2)^2$ ; if  $4 \mid 2^{-1}a - 3$ , then  $4 \cdot 2^{-1}a \notin (\bigcup_{j=0}^{\infty} 4^j(1 + 4\mathbf{Z}_2)) \cup \{0\} = (\mathbf{Z}_2)^2 \cup m(\mathbf{Z}_2)^2$ . Therefore, by (3-10), we have

$$\delta \in (\mathfrak{o}_{\mathfrak{p}}^{\times})^2 \iff 4 \mid 2^{-1}a - 1.$$

Now we also assume  $b \neq 0$ . Since  $(\text{Tr}(\delta) + 2N(\delta)^{1/2})(\text{Tr}(\delta) - 2N(\delta)^{1/2}) = b^2m \neq 0$ , we have  $\text{Tr}(\delta) + 2N(\delta)^{1/2} \neq 0$ . Hence, if  $\text{Tr}(\delta) + 2N(\delta)^{1/2} \in (\mathbf{Z}_2)^2 \cup m(\mathbf{Z}_2)^2$ , then

$$\begin{aligned} \text{Tr}(\delta) - 2N(\delta)^{1/2} &= b^2m(\text{Tr}(\delta) + 2N(\delta)^{1/2})^{-1} \\ &\in ((\mathbf{Q}_2^{\times})^2 \cup m(\mathbf{Q}_2^{\times})^2) \cap \mathbf{Z}_2 \\ &\subset (\mathbf{Z}_2)^2 \cup m(\mathbf{Z}_2)^2. \end{aligned}$$

Thus

$$\begin{aligned} \text{Tr}(\delta) + 2N(\delta)^{1/2}, \text{Tr}(\delta) - 2N(\delta)^{1/2} &\in (\mathbf{Z}_2)^2 \cup m(\mathbf{Z}_2)^2 \\ \iff \text{Tr}(\delta) + 2N(\delta)^{1/2} &\in (\mathbf{Z}_2)^2 \cup m(\mathbf{Z}_2)^2. \end{aligned} \tag{3-12}$$

When  $\text{ord}_2(a) \geq 2$ , we have  $\text{Tr}(\delta) = a \in 4\mathbf{Z}_2$ . Since  $N(\delta)^{1/2} \in 1 + 2\mathbf{Z}_2$ , we have  $\text{Tr}(\delta) + 2N(\delta)^{1/2} \in 2(1 + 2\mathbf{Z}_2) = 2\mathbf{Z}_2^{\times}$ . Thus  $\text{Tr}(\delta) + 2N(\delta)^{1/2} \notin (\mathbf{Z}_2)^2 \cup m(\mathbf{Z}_2)^2$ , and hence  $\delta \notin (\mathfrak{o}_{\mathfrak{p}}^{\times})^2$  by (3-10). When  $\text{ord}_2(a) = 0$ , we have  $\text{Tr}(\delta) + 2N(\delta)^{1/2} \in a + 2 + 4\mathbf{Z}_2 \subset \mathbf{Z}_2^{\times}$ . Thus, by (3-10) and (3-12), we have

$$\delta \in (\mathfrak{o}_{\mathfrak{p}}^{\times})^2 \iff 4 \mid a + 1.$$

When  $\text{ord}_2(a) = 1$ , we have  $\text{ord}_2(b) \geq 2$  by Equation (3-11). Thus, by Lemma 3.8, we have  $u \equiv N(\delta)^{1/2} \pmod{2^{2\text{ord}_2(b)-1}\mathbf{Z}_2}$ , and hence  $a + 2u \equiv \text{Tr}(\delta) + 2N(\delta)^{1/2} \pmod{2^{2\text{ord}_2(b)}\mathbf{Z}_2}$ . Since  $\text{Tr}(\delta), 2N(\delta)^{1/2} \in 2(1 + 2\mathbf{Z}_2)$ , we have  $\text{Tr}(\delta) - 2N(\delta)^{1/2} \in 4\mathbf{Z}_2$ . Thus, since  $(\text{Tr}(\delta) + 2N(\delta)^{1/2})(\text{Tr}(\delta) - 2N(\delta)^{1/2}) = mb^2$ , we have  $\text{ord}_2(\text{Tr}(\delta) + 2N(\delta)^{1/2}) \leq 2\text{ord}_2(b) - 2$ , and hence

$$r = \text{ord}_2(a + 2u) = \text{ord}_2(\text{Tr}(\delta) + 2N(\delta)^{1/2}).$$

It follows that  $a + 2u \equiv \text{Tr}(\delta) + 2N(\delta)^{1/2} \pmod{2^{r+2}\mathbf{Z}_2}$ , that is,

$$2^{-r}(a + 2u) \equiv 2^{-r}(\text{Tr}(\delta) + 2N(\delta)^{1/2}) \pmod{4\mathbf{Z}_2}.$$

p	$C_f(p)$	$N((C_f(p))_{K_f})$	p	$C_f(p)$	$N((C_f(p))_{K_f})$
[2, $\omega$ ]	$(1 \pm \sqrt{13})/2$	3	[349, $206 + \omega$ ]	$-18 \pm \sqrt{13}$	311
[11, $4 + \omega$ ]	1	1	[373, $233 + \omega$ ]	27	$3^6$
[13, $9 + \omega$ ]	$\pm\sqrt{13}$	13	[379, $153 + \omega$ ]	$15 \pm 2\sqrt{13}$	173
[17, $11 + \omega$ ]	$4 \pm \sqrt{13}$	3	[397, $164 + \omega$ ]	$-20 \pm 3\sqrt{13}$	283
[23, $10 + \omega$ ]	$4 \pm \sqrt{13}$	3	[401, $80 + \omega$ ]	$14 \pm \sqrt{13}$	$3 \cdot 61$
[29, $2 + \omega$ ]	$2 \pm \sqrt{13}$	$3^2$	[419, $222 + \omega$ ]*	$-19 \pm \sqrt{13}$	$2^2 \cdot 3 \cdot 29$
[31, $29 + \omega$ ]	$1 \pm 2\sqrt{13}$	$3 \cdot 17$	[433, $30 + \omega$ ]	$-24 \pm \sqrt{13}$	563
[59, $45 + \omega$ ]	$\pm\sqrt{13}$	13	[457, $43 + \omega$ ]	-15	$3^2 \cdot 5^2$
[61, $23 + \omega$ ]*	$-1 \pm \sqrt{13}$	$2^2 \cdot 3$	[479, $434 + \omega$ ]	$5 \pm 6\sqrt{13}$	443
[67, $24 + \omega$ ]*	$-3 \pm 3\sqrt{13}$	$2^2 \cdot 3^3$	[491, $340 + \omega$ ]	$14 \pm 5\sqrt{13}$	$3 \cdot 43$
[73, $14 + \omega$ ]	$4 \pm 3\sqrt{13}$	101	[499, $130 + \omega$ ]*	$9 \pm 7\sqrt{13}$	$2^2 \cdot 139$
[79, $19 + \omega$ ]	$12 \pm \sqrt{13}$	131	[503, $105 + \omega$ ]	$9 \pm 6\sqrt{13}$	$3^2 \cdot 43$
[89, $68 + \omega$ ]	$-1 \pm 2\sqrt{13}$	$3 \cdot 17$	[523, $303 + \omega$ ]	21	$3^2 \cdot 7^2$
[113, $62 + \omega$ ]*	$5 \pm 3\sqrt{13}$	$2^2 \cdot 23$	[563, $34 + \omega$ ]	$17 \pm 4\sqrt{13}$	$3^4$
[137, $89 + \omega$ ]	$14 \pm \sqrt{13}$	$3 \cdot 61$	[571, $172 + \omega$ ]	$21 \pm 2\sqrt{13}$	389
[139, $18 + \omega$ ]	$-12 \pm \sqrt{13}$	131	[587, $445 + \omega$ ]*	$-2 \pm 4\sqrt{13}$	$2^2 \cdot 3 \cdot 17$
[157, $73 + \omega$ ]*	$\pm 2\sqrt{13}$	$2^2 \cdot 13$	[593, $478 + \omega$ ]	$-16 \pm \sqrt{13}$	$3^5$
[173, $27 + \omega$ ]	$3 \pm 6\sqrt{13}$	$3^3 \cdot 17$	[613, $486 + \omega$ ]	-19	$19^2$
[193, $100 + \omega$ ]*	$-3 \pm \sqrt{13}$	$2^2$	[631, $559 + \omega$ ]*	$-18 \pm 8\sqrt{13}$	$2^2 \cdot 127$
[197, $40 + \omega$ ]*	$-1 \pm 3\sqrt{13}$	$2^2 \cdot 29$	[643, $336 + \omega$ ]*	$12 \pm 4\sqrt{13}$	$2^6$
[199, $177 + \omega$ ]	$-18 \pm \sqrt{13}$	311	[647, $51 + \omega$ ]	39	$3^2 \cdot 13^2$
[211, $136 + \omega$ ]	$-4 \pm 3\sqrt{13}$	101	[653, $173 + \omega$ ]*	$10 \pm 8\sqrt{13}$	$2^2 \cdot 3 \cdot 61$
[223, $152 + \omega$ ]	$-8 \pm 3\sqrt{13}$	53	[673, $620 + \omega$ ]	$-21 \pm 6\sqrt{13}$	$3^3$
[227, $102 + \omega$ ]*	$2 \pm 2\sqrt{13}$	$2^4 \cdot 3$	[683, $133 + \omega$ ]	$-16 \pm \sqrt{13}$	$3^5$
[239, $148 + \omega$ ]	$-5 \pm 6\sqrt{13}$	443	[701, $452 + \omega$ ]	$6 \pm 3\sqrt{13}$	$3^4$
[241, $122 + \omega$ ]*	$-19 \pm 3\sqrt{13}$	$2^2 \cdot 61$	[709, $38 + \omega$ ]	$27 \pm 4\sqrt{13}$	521
[283, $95 + \omega$ ]	$-16 \pm 3\sqrt{13}$	139	[719, $310 + \omega$ ]	$-14 \pm 7\sqrt{13}$	$3^2 \cdot 7^2$
[293, $267 + \omega$ ]	1	1	[727, $205 + \omega$ ]	$-6 \pm 13\sqrt{13}$	2161
[307, $116 + \omega$ ]	$-3 \pm 4\sqrt{13}$	199	[739, $558 + \omega$ ]*	14	$2^2 \cdot 7^2$
[317, $280 + \omega$ ]	$\pm 3\sqrt{13}$	$3^2 \cdot 13$	[769, $550 + \omega$ ]	$-17 \pm 2\sqrt{13}$	$3 \cdot 79$

\* : principal prime ideal

TABLE 1. The eigenvalues  $C_f(p)$  of  $T(p)|_{S_{(2,2)}^0(\mathfrak{o}_{\mathbf{Q}(\sqrt{257})}, 1)}$  and their norm for a split prime  $p$ .

Therefore, by (3–10) and (3–12), we have

$$\begin{aligned} \delta \in (\mathfrak{o}_p^\times)^2 &\iff \text{Tr}(\delta) + 2N(\delta)^{1/2} \in \prod_{j=0}^{\infty} 4^j(1 + 4\mathbf{Z}_2) \\ &\iff 2 \mid \text{ord}_2(\text{Tr}(\delta) + 2N(\delta)^{1/2}), \\ &\quad 2^{-\text{ord}_2(\text{Tr}(\delta) + 2N(\delta)^{1/2})}(\text{Tr}(\delta) + 2N(\delta)^{1/2}) \\ &\quad \in 1 + 4\mathbf{Z}_2 \\ &\iff 2 \mid r, 4 \mid 2^{-r}(a + 2u) - 1. \end{aligned}$$

This completes the proof. □

Note that we can easily find  $u$  of Proposition 3.14 by Remark 3.11, since  $4^{-1}(a^2 - b^2m) = N_{F_p/\mathbf{Q}_2}(\delta) \in 1 + 8\mathbf{Z}$ .

#### 4. NUMERICAL EXAMPLES FOR $\mathbf{Q}(\sqrt{257})$ AND $\mathbf{Q}(\sqrt{401})$

In this section, we shall give numerical examples of eigenvalues and characteristic polynomials of Hecke operators

for real quadratic fields  $\mathbf{Q}(\sqrt{257})$  and  $\mathbf{Q}(\sqrt{401})$ , whose class numbers are three and five, respectively.

Let  $F$  and  $m$  be as in Section 3. We treat only the case  $k = (2, 2)$  and  $\psi$  is the identity (i.e.,  $\psi(F_{\mathbf{A}}^\times) = \{1\}$ ). We denote this character by 1. Let  $S_2(\Gamma_0(m), (\frac{m}{\cdot}))$  be the space of elliptic cusp forms of ‘‘Neben’’-type of level  $m$ , and  $\mathcal{S}_{(2,2)}^N(\mathfrak{o}_F, 1)$  the subspace of  $\mathcal{S}_{(2,2)}(\mathfrak{o}_F, 1)$  that consists of Hilbert cusp forms coming from  $S_2(\Gamma_0(m), (\frac{m}{\cdot}))$  through the Doi–Naganuma lifting (cf. [Doi and Naganuma 69] and [Naganuma 73]). We denote by  $\mathcal{S}_{(2,2)}^0(\mathfrak{o}_F, 1)$  the ‘‘ $F$ -proper’’ subspace of  $\mathcal{S}_{(2,2)}(\mathfrak{o}_F, 1)$ , that is, the orthogonal complement of  $\mathcal{S}_{(2,2)}^N(\mathfrak{o}_F, 1)$  with respect to the standard inner product. It is known that  $\mathcal{S}_{(2,2)}^0(\mathfrak{o}_F, 1)$  and  $\mathcal{S}_{(2,2)}^N(\mathfrak{o}_F, 1)$  are stable under the action of  $T(p)$  for all prime ideals  $p$  of  $F$ . In the following, we shall determine eigenvalues and characteristic polynomials of  $T(p)|_{S_{(2,2)}^0(\mathfrak{o}_F, 1)}$  for several prime ideals  $p$ .

We denote by  $\Psi_p(X)$  the characteristic polynomial of  $T(p)|_{S_{(2,2)}^0(\mathfrak{o}_F, 1)}$ . For a primitive form  $f$  in  $\mathcal{S}_{(2,2)}^0(\mathfrak{o}_F, 1)$ , we denote by  $C_f(p)$  the eigenvalue of  $T(p)$  satisfying

$\mathfrak{f}|T(\mathfrak{p}) = C_{\mathfrak{f}}(\mathfrak{p})\mathfrak{f}$ , and then denote by  $K_{\mathfrak{f}}$  the Hecke field of  $\mathfrak{f}$ , that is, the field generated over  $\mathbf{Q}$  by  $C_{\mathfrak{f}}(\mathfrak{p})$  for all prime ideals  $\mathfrak{p}$ . Let  $K_{\mathfrak{f}}^+$  be the subfield of  $K_{\mathfrak{f}}$  generated by  $C_{\mathfrak{f}}((p)_F)$  for all rational primes  $p$ . We note that  $[K_{\mathfrak{f}} : K_{\mathfrak{f}}^+] = 2$ .

Now we set  $\Lambda_{\mathfrak{f}}(\mathfrak{p}) = \mathfrak{o}_{K_{\mathfrak{f}}^+} + C_{\mathfrak{f}}(\mathfrak{p})\mathfrak{o}_{K_{\mathfrak{f}}^+}$  for a split prime  $\mathfrak{p}$ . Then  $\Lambda_{\mathfrak{f}}(\mathfrak{p})$  is an order in  $\mathcal{O}_{K_{\mathfrak{f}}/K_{\mathfrak{f}}^+}$  in the sense of Section 2.2, and the conductor  $c(\Lambda_{\mathfrak{f}}(\mathfrak{p}))$  is given by Lemma 2.3 as follows:

$$c(\Lambda_{\mathfrak{f}}(\mathfrak{p})) = (D_{K_{\mathfrak{f}}/K_{\mathfrak{f}}^+}(C_{\mathfrak{f}}(\mathfrak{p}))) \cdot (D_{K_{\mathfrak{f}}/K_{\mathfrak{f}}^+})^{-1})^{1/2}.$$

### 4.1 Example for $\mathbf{Q}(\sqrt{257})$

Let  $F = \mathbf{Q}(\sqrt{257})$ . Then  $h_F = h_F^+ = 3$ . We have

$$\begin{aligned} \dim_{\mathbf{C}} \mathcal{S}_{(2,2)}^0(\mathfrak{o}_F, 1) &= \dim_{\mathbf{C}} \mathcal{S}_{(2,2)}(\mathfrak{o}_F, 1) \\ &\quad - \frac{1}{2} \dim_{\mathbf{C}} S_2(\Gamma_0(257), \left(\frac{257}{\cdot}\right)) \\ &= \text{tr } T(\mathfrak{o}_F) - \frac{1}{2} \cdot 20 = 2. \end{aligned}$$

- Table 1 gives numerical data for the eigenvalues of  $T(\mathfrak{p})|_{\mathcal{S}_{(2,2)}^0(\mathfrak{o}_F, 1)}$  and their norms for split primes  $\mathfrak{p}$  satisfying  $N(\mathfrak{p}) \leq 769$ .
- Table 2 gives numerical data for the eigenvalues of  $T((p)_F)|_{\mathcal{S}_{(2,2)}^0(\mathfrak{o}_F, 1)}$  for rational primes  $p$  such that  $p$  remains prime in  $F$  and  $p \leq 97$ . (Note that the characteristic polynomial of  $T((p)_F)|_{\mathcal{S}_{(2,2)}^0(\mathfrak{o}_F, 1)}$  has a double root.)

$\mathfrak{p}$	$C_{\mathfrak{f}}(\mathfrak{p})$	$\mathfrak{p}$	$C_{\mathfrak{f}}(\mathfrak{p})$	$\mathfrak{p}$	$C_{\mathfrak{f}}(\mathfrak{p})$
$(3)_F$	-4	$(37)_F$	52	$(53)_F$	-8
$(5)_F$	-2	$(41)_F$	-18	$(71)_F$	-30
$(7)_F$	0	$(43)_F$	30	$(83)_F$	50
$(19)_F$	-18	$(47)_F$	46	$(97)_F$	90

**TABLE 2.** The eigenvalue  $C_{\mathfrak{f}}(\mathfrak{p})$  of  $T(\mathfrak{p})|_{\mathcal{S}_{(2,2)}^0(\mathfrak{o}_{\mathbf{Q}(\sqrt{257})}, 1)}$  for  $\mathfrak{p} = (p)_F$ .

For a primitive form  $\mathfrak{f}$  in  $\mathcal{S}_{(2,2)}^0(\mathfrak{o}_F, 1)$ , we have

$$K_{\mathfrak{f}} = \mathbf{Q}(\sqrt{13}), \quad K_{\mathfrak{f}}^+ = \mathbf{Q}.$$

Within the limit of Table 1, we observe that

$$\mathfrak{p} \text{ is principal} \iff (2)_{K_{\mathfrak{f}}} \mid C_{\mathfrak{f}}(\mathfrak{p})$$

for split primes  $\mathfrak{p}$ ; in particular, we remark that

$$2 \mid c(\Lambda_{\mathfrak{f}}(\mathfrak{p}))$$

for all principal split primes  $\mathfrak{p}$  in the table.

### 4.2 Example for $\mathbf{Q}(\sqrt{401})$

Let  $F = \mathbf{Q}(\sqrt{401})$ . Then  $h_F = h_F^+ = 5$ . We have

$$\dim_{\mathbf{C}} \mathcal{S}_{(2,2)}^0(\mathfrak{o}_F, 1) = 24 - \frac{1}{2} \cdot 32 = 8.$$

- Table 3 gives numerical data for the characteristic polynomials  $\Psi_{(p)_F}(X)$  of  $T((p)_F)|_{\mathcal{S}_{(2,2)}^0(\mathfrak{o}_F, 1)}$  for rational primes  $p$  such that  $p$  remains prime in  $F$  and  $p \leq 23$ .

$\mathfrak{p}$	$\Psi_{\mathfrak{p}}(X)$
$(3)_F$	$(X^4 + 7X^3 + 4X^2 - 32X + 1)^2$
$(13)_F$	$(X^4 + 24X^3 + 120X^2 - 113X - 571)^2$
$(17)_F$	$(X^4 + 2X^3 - 110X^2 - 111X + 3019)^2$
$(19)_F$	$(X^4 + 10X^3 - 339X^2 - 1360X + 22759)^2$
$(23)_F$	$(X^4 - 16X^3 - 495X^2 + 8532X - 11671)^2$

**TABLE 3.** The characteristic polynomial  $\Psi_{\mathfrak{p}}(X)$  of  $T(\mathfrak{p})|_{\mathcal{S}_{(2,2)}^0(\mathfrak{o}_{\mathbf{Q}(\sqrt{401})}, 1)}$  for  $\mathfrak{p} = (p)_F$ .

- Table 4 gives numerical data for the coefficients of the characteristic polynomials  $\Psi_{\mathfrak{p}}(X) = X^8 + a_1X^7 + \dots + a_7X + a_8$  of  $T(\mathfrak{p})|_{\mathcal{S}_{(2,2)}^0(\mathfrak{o}_F, 1)}$  for principal split primes  $\mathfrak{p}$  satisfying  $N(\mathfrak{p}) \leq 643$  and nonprincipal split primes  $\mathfrak{p}$  satisfying  $N(\mathfrak{p}) \leq 263$ .

The characteristic polynomial  $\Psi_{[2, \omega]}(X)$  of  $T([2, \omega])|_{\mathcal{S}_{(2,2)}^0(\mathfrak{o}_F, 1)}$  is irreducible over  $\mathbf{Q}$ , and the roots of  $\Psi_{[2, \omega]}(X)$  are

$$\begin{aligned} c_{ijl} &= \frac{1}{40} \left( 15 - (-1)^i 5\sqrt{5} + (-1)^{i+j} \sqrt{5} \sqrt{110 + 10\sqrt{5}} \right. \\ &\quad \left. + (-1)^l \sqrt{4900 - (-1)^i 100\sqrt{5} + (-1)^j (150 - (-1)^i 10\sqrt{5}) \sqrt{110 + 10\sqrt{5}}} \right), \end{aligned}$$

where  $0 \leq i, j, l \leq 1$ . Now we take the primitive form  $\mathfrak{f}$  such that  $\mathfrak{f}|T([2, \omega]) = c_{000}\mathfrak{f}$ . Then we have

$$\begin{aligned} K_{\mathfrak{f}} &= \mathbf{Q} \left( \sqrt{4900 - 100\sqrt{5} + (150 - 10\sqrt{5}) \sqrt{110 + 10\sqrt{5}}} \right), \\ K_{\mathfrak{f}}^+ &= \mathbf{Q} \left( \sqrt{110 + 10\sqrt{5}} \right). \end{aligned}$$

(The degree of the Galois closure of  $K_{\mathfrak{f}}$  over  $\mathbf{Q}$  is  $128 = 2^7$ .) Then we have

$$D_{K_{\mathfrak{f}}/\mathbf{Q}} = 5^4 \cdot 29^2 \cdot 131 \cdot 139,$$

$$D_{K_{\mathfrak{f}}^+/\mathbf{Q}} = 5^2 \cdot 29,$$

$$N(D_{K_{\mathfrak{f}}/K_{\mathfrak{f}}^+}) = 131 \cdot 139.$$

- Table 5 gives numerical data for the norm of  $c(\Lambda_{\mathfrak{f}}(\mathfrak{p}))$ .

p	a <sub>1</sub> ,	a <sub>2</sub> ,	a <sub>3</sub> ,	a <sub>4</sub> ,	a <sub>5</sub> ,	a <sub>6</sub> ,	a <sub>7</sub> ,	a <sub>8</sub>
[2, ω]	-3,	-10,	28,	37,	-78,	-58,	53,	19
[5, ω]	-3,	-18,	41,	111,	-163,	-234,	155,	1
[7, 5 + ω]	-6,	-12,	120,	-175,	-42,	175,	-83,	11
[11, 7 + ω]	9,	10,	-101,	-253,	149,	918,	809,	179
[29, 22 + ω]	13,	-5,	-523,	-408,	8053,	1917,	-48078,	38359
[41, 27 + ω]	-16,	-90,	2332,	-2437,	-86432,	249407,	263905,	43909
[43, 26 + ω]	-32,	309,	-148,	-11780,	43156,	18606,	-138350,	-42131
[47, 44 + ω]	15,	-46,	-1114,	861,	24682,	-30282,	-133239,	211541
[73, 39 + ω]	4,	-362,	-1343,	36721,	107356,	-1265768,	-1867352,	14282224
[83, 30 + ω] *	-32,	92,	5761,	-41264,	-341588,	3084758,	6681459,	-69332531
[89, 60 + ω]	-10,	-278,	3166,	13505,	-241434,	703443,	-114403,	-611281
[103, 85 + ω]	27,	-118,	-6456,	-10369,	372198,	1371298,	-3479619,	-15228421
[109, 74 + ω]	29,	-186,	-10994,	-61417,	448682,	4111874,	7230513,	-1231091
[113, 23 + ω]	-34,	88,	7570,	-77675,	-156608,	5544655,	-26618987,	40066931
[149, 55 + ω]	-68,	1775,	-22208,	131704,	-237922,	-810800,	2670928,	1079011
[151, 92 + ω]	-22,	-151,	5415,	-7430,	-329865,	1334049,	-291087,	-2791879
[173, 110 + ω]	-11,	-381,	7795,	-37942,	-157229,	2060155,	-6349795,	5629151
[179, 107 + ω]	-88,	2950,	-45092,	245937,	1261812,	-21112768,	83231088,	-104306576
[181, 21 + ω]	-7,	-310,	2548,	18965,	-210804,	594832,	-493872,	-100624
[197, 45 + ω]	40,	168,	-9515,	-110360,	121710,	6701416,	29340685,	31232399
[223, 31 + ω]	-68,	1453,	-2076,	-317709,	3811290,	-9269721,	-49448362,	130826831
[229, 57 + ω]	33,	-67,	-8851,	-51342,	253023,	1988777,	-1662381,	-18676169
[239, 206 + ω]	-53,	1066,	-10574,	54335,	-132516,	96784,	72897,	-69191
[241, 167 + ω]	-35,	218,	2705,	-15695,	-84085,	59836,	48125,	-30371
[257, 122 + ω] *	10,	-1119,	-14842,	336025,	6080144,	-7871441,	-548680256,	-2339785241
[263, 201 + ω]	-36,	-295,	12183,	91010,	-605219,	-5055489,	-2431643,	17176609
[337, 172 + ω] *	-47,	105,	24343,	-327430,	-1820659,	57625757,	-337202462,	582948571
[379, 103 + ω] *	-25,	-1214,	26233,	458881,	-6336001,	-81101528,	302094243,	3696976091
[383, 205 + ω] *	-63,	286,	61218,	-1739923,	17945914,	-49335124,	-306466744,	1582083824
[397, 197 + ω] *	-77,	690,	64185,	-1089907,	-15159265,	255263350,	1030269191,	-910014589
[421, 304 + ω] *	48,	-494,	-47086,	-216435,	13127696,	123014259,	-842081917,	-9542329681
[487, 70 + ω] *	-25,	-1553,	38867,	743048,	-20170693,	-84273537,	3477790992,	-11951208719
[499, 264 + ω] *	-22,	-1402,	39386,	246139,	-13711178,	90023337,	71238749,	-717378001
[643, 474 + ω] *	-72,	-896,	147914,	-1370115,	-68019308,	937509055,	3125818491,	-4860460921

\* : principal prime ideal

**TABLE 4.** The coefficients of the characteristic polynomial  $X^8 + a_1X^7 + \dots + a_7X + a_8$  of  $T(\mathfrak{p})|_{S_{(2,2)}^0(\mathfrak{o}_{\mathbf{Q}(\sqrt{401})}, t)}$  for a split prime  $\mathfrak{p}$ .

From Table 5, we immediately observe that

$$19 \mid N(c(\Lambda_{\mathfrak{f}}(\mathfrak{p})))$$

for all principal split primes  $\mathfrak{p}$  in the table. Moreover, if we set

$$\mathfrak{P}_{19} = c(\Lambda_{\mathfrak{f}}([83, 30 + \omega])),$$

then  $\mathfrak{P}_{19}$  is a prime ideal of  $K_{\mathfrak{f}}^+$ , and there exist prime ideals  $\mathfrak{P}'_{19}, \mathfrak{P}''_{19}$  of  $K_{\mathfrak{f}}^+$  such that

$$(19)_{K_{\mathfrak{f}}^+} = \mathfrak{P}_{19}\mathfrak{P}'_{19}\mathfrak{P}''_{19},$$

$$\mathfrak{P}_{19}\mathfrak{P}'_{19} = [19, 4 + (1 + \sqrt{5})/2] \cdot \mathfrak{o}_{K_{\mathfrak{f}}^+},$$

$$\mathfrak{P}''_{19} = [19, 14 + (1 + \sqrt{5})/2] \cdot \mathfrak{o}_{K_{\mathfrak{f}}^+}.$$

Then we can observe that

$$\mathfrak{P}_{19} \mid c(\Lambda_{\mathfrak{f}}(\mathfrak{p}))$$

for all principal split primes  $\mathfrak{p}$  in the table.

### 4.3 Calculation Based on Hida's Suggestion

We check (1), (2), and (3) of the Introduction.

When  $F = \mathbf{Q}(\sqrt{257})$ , the common factor of  $N_{K_{\mathfrak{f}}/\mathbf{Q}}(1 + N(\mathfrak{p}) - C_{\mathfrak{f}}(\mathfrak{p})) = \Psi_{\mathfrak{p}}(1 + N(\mathfrak{p}))$  is  $2^2$  from Table 6. Moreover, it follows immediately from Table 1 that the common factor of  $1 + N(\mathfrak{p}) - C_{\mathfrak{f}}(\mathfrak{p})$  is  $(2)_{K_{\mathfrak{f}}} = \mathfrak{f}_{\mathfrak{f}}\mathfrak{o}_{K_{\mathfrak{f}}}$ . When  $F = \mathbf{Q}(\sqrt{401})$ , the common factor of  $N_{K_{\mathfrak{f}}/\mathbf{Q}}(1 + N(\mathfrak{p}) - C_{\mathfrak{f}}(\mathfrak{p})) = \Psi_{\mathfrak{p}}(1 + N(\mathfrak{p}))$  is  $19^2$  from Table 7.

$\mathfrak{p}$	$N(c(\Lambda_{\mathfrak{f}}(\mathfrak{p})))$
[2, $\omega$ ]	1
[5, $\omega$ ]	1
[7, $5 + \omega$ ]	1
[11, $7 + \omega$ ]	1
[29, $22 + \omega$ ]	1
[41, $27 + \omega$ ]	31
[43, $26 + \omega$ ]	31
[47, $44 + \omega$ ]	31
[73, $39 + \omega$ ]	$3^4$
[83, $30 + \omega$ ]	* 19
[89, $60 + \omega$ ]	41
[103, $85 + \omega$ ]	$23^2$
[109, $74 + \omega$ ]	$19 \cdot 29$
[113, $23 + \omega$ ]	1
[149, $55 + \omega$ ]	$5^2$
[151, $92 + \omega$ ]	29
[173, $110 + \omega$ ]	41
[179, $107 + \omega$ ]	19
[181, $21 + \omega$ ]	11
[197, $45 + \omega$ ]	379
[223, $31 + \omega$ ]	61
[229, $57 + \omega$ ]	19
[239, $206 + \omega$ ]	1
[241, $167 + \omega$ ]	$7^2$
[257, $122 + \omega$ ]	* $19 \cdot 139$
[263, $201 + \omega$ ]	409
[337, $172 + \omega$ ]	* $19 \cdot 41$
[379, $103 + \omega$ ]	* $19 \cdot 31$
[383, $205 + \omega$ ]	* $7^2 \cdot 19$
[397, $197 + \omega$ ]	* $19 \cdot 41$
[421, $304 + \omega$ ]	* $11 \cdot 19^2$
[487, $70 + \omega$ ]	* $19^2 \cdot 31$
[499, $264 + \omega$ ]	* $11^2 \cdot 19$
[643, $474 + \omega$ ]	* $19 \cdot 79$

\* : principal prime ideal

**TABLE 5.** The norm of  $c(\Lambda_{\mathfrak{f}}(\mathfrak{p}))$  for the primitive form  $\mathfrak{f}$  in  $\mathcal{S}_{(2,2)}^0(\mathfrak{o}_{\mathbf{Q}(\sqrt{401})}, 1)$  and a split prime  $\mathfrak{p}$ .

Moreover, we can observe that the common factor of  $1 + N(\mathfrak{p}) - C_{\mathfrak{f}}(\mathfrak{p})$  is  $\mathfrak{P}_{19\mathfrak{o}_{K_{\mathfrak{f}}}} = \mathfrak{F}_{\mathfrak{f}\mathfrak{o}_{K_{\mathfrak{f}}}}$ . Thus (1) and (2) are affirmative, and (3) is correct in this case.

By using [Siegel 69, (22)], we have calculated the value at 2 of the Hecke  $L$ -function associated with a nontrivial class character  $\chi$ . In the case  $F = \mathbf{Q}(\sqrt{257})$ , we have

$$\prod_{\chi:\text{nontrivial}} \frac{D_F^{3/2}}{(2\pi)^4} L_F(2, \chi) = 2^2.$$

In the case  $F = \mathbf{Q}(\sqrt{401})$ , we have

$$\prod_{\chi:\text{nontrivial}} \frac{D_F^{3/2}}{(2\pi)^4} L_F(2, \chi) = 19^2.$$

$\mathfrak{p}$	$N_{K_{\mathfrak{f}}/\mathbf{Q}}(1 + N(\mathfrak{p}) - C_{\mathfrak{f}}(\mathfrak{p}))$
$(3)_F$	$2^2 \cdot 7^2$
$(5)_F$	$2^4 \cdot 7^2$
$(7)_F$	$2^2 \cdot 5^4$
$(19)_F$	$2^4 \cdot 5^2 \cdot 19^2$
$(37)_F$	$2^2 \cdot 659^2$
$(41)_F$	$2^4 \cdot 5^4 \cdot 17^2$
$(43)_F$	$2^4 \cdot 5^2 \cdot 7^2 \cdot 13^2$
$(47)_F$	$2^4 \cdot 541^2$
$(53)_F$	$2^2 \cdot 1409^2$
$(71)_F$	$2^8 \cdot 317^2$
$(83)_F$	$2^6 \cdot 3^4 \cdot 5^2 \cdot 19^2$
$(97)_F$	$2^6 \cdot 5^2 \cdot 233^2$
[61, $23 + \omega$ ]	$2^2 \cdot 23 \cdot 43$
[67, $24 + \omega$ ]	$2^2 \cdot 1231$
[113, $62 + \omega$ ]	$2^2 \cdot 17 \cdot 173$
[157, $73 + \omega$ ]	$2^4 \cdot 3^2 \cdot 173$
[193, $100 + \omega$ ]	$2^2 \cdot 3 \cdot 53 \cdot 61$
[197, $40 + \omega$ ]	$2^2 \cdot 9871$
[227, $102 + \omega$ ]	$2^4 \cdot 3 \cdot 1063$
[241, $122 + \omega$ ]	$2^2 \cdot 3^2 \cdot 1889$
[419, $222 + \omega$ ]	$2^2 \cdot 3^2 \cdot 53 \cdot 101$
[499, $130 + \omega$ ]	$2^2 \cdot 3^2 \cdot 6679$
[587, $445 + \omega$ ]	$2^2 \cdot 3 \cdot 53 \cdot 547$
[631, $559 + \omega$ ]	$2^2 \cdot 3^2 \cdot 13 \cdot 17 \cdot 53$
[643, $336 + \omega$ ]	$2^4 \cdot 3 \cdot 8317$
[653, $173 + \omega$ ]	$2^4 \cdot 3 \cdot 8623$
[739, $558 + \omega$ ]	$2^2 \cdot 3^2 \cdot 11^4$

**TABLE 6.**  $N_{K_{\mathfrak{f}}/\mathbf{Q}}(1 + N(\mathfrak{p}) - C_{\mathfrak{f}}(\mathfrak{p}))$  for a principal prime  $\mathfrak{p}$ , where  $C_{\mathfrak{f}}(\mathfrak{p})$  is an eigenvalue of  $T(\mathfrak{p})|_{\mathcal{S}_{(2,2)}^0(\mathfrak{o}_{\mathbf{Q}(\sqrt{257})}, 1)}$ .

$\mathfrak{p}$	$N_{K_{\mathfrak{f}}/\mathbf{Q}}(1 + N(\mathfrak{p}) - C_{\mathfrak{f}}(\mathfrak{p}))$
$(3)_F$	$19^2 \cdot 29^2 \cdot 31^2$
$(13)_F$	$11^4 \cdot 19^4 \cdot 61^2 \cdot 359^2$
$(17)_F$	$11^2 \cdot 19^2 \cdot 34030181^2$
$(19)_F$	$7^4 \cdot 11^2 \cdot 19^2 \cdot 521^2 \cdot 3299^2$
$(23)_F$	$19^2 \cdot 4020433831^2$
[83, $30 + \omega$ ]	$19^2 \cdot 31 \cdot 11059 \cdot 12836389$
[257, $122 + \omega$ ]	$11 \cdot 19^2 \cdot 1279 \cdot 3191 \cdot 1236962761$
[337, $172 + \omega$ ]	$19^2 \cdot 641 \cdot 1109 \cdot 2011 \cdot 8111 \cdot 35099$
[379, $103 + \omega$ ]	$11^3 \cdot 19^2 \cdot 1638061 \cdot 511689281$
[383, $205 + \omega$ ]	$2^4 \cdot 11 \cdot 19^2 \cdot 1621 \cdot 1790869 \cdot 2150221$
[397, $197 + \omega$ ]	$11^2 \cdot 19^2 \cdot 131 \cdot 94781 \cdot 942456979$
[421, $304 + \omega$ ]	$19^2 \cdot 60830069 \cdot 50854477409$
[487, $70 + \omega$ ]	$11 \cdot 19^2 \cdot 2699 \cdot 17191 \cdot 16454332679$
[499, $264 + \omega$ ]	$11^2 \cdot 19^2 \cdot 61 \cdot 829 \cdot 1681246642091$
[643, $474 + \omega$ ]	$19^2 \cdot 421 \cdot 334889 \cdot 515366804791$

**TABLE 7.**  $N_{K_{\mathfrak{f}}/\mathbf{Q}}(1 + N(\mathfrak{p}) - C_{\mathfrak{f}}(\mathfrak{p}))$  for a principal prime  $\mathfrak{p}$ , where  $C_{\mathfrak{f}}(\mathfrak{p})$  is an eigenvalue of  $T(\mathfrak{p})|_{\mathcal{S}_{(2,2)}^0(\mathfrak{o}_{\mathbf{Q}(\sqrt{401})}, 1)}$ .

## ACKNOWLEDGMENTS

I would like to express my deep gratitude to Professor Haruzo Hida for giving an introductory lecture on Hilbert modular forms in the summer of 1994 at Ritsumeikan University and for suggesting the explicit goal as described above. Also, I wish to thank Dr. Keiji Goto, who read the original draft with deep interest and offered both mathematical and linguistic comments. Finally, I would like to thank one of the referees for encouraging further study of the observed phenomenon, which gave me the chance to investigate Professor Hida's suggestion.

## REFERENCES

- [Dirichlet 1894] P. G. L. Dirichlet. *Vorlesungen über Zahlen-theorie*, Herausgegeben und mit Zusätzen versehen von R. Dedekind, Vierte, Braunschweig, 1894.
- [Doi and Naganuma 69] K. Doi and H. Naganuma. "On the functional equation of certain Dirichlet series." *Invent. Math.* **9** (1969), 1–14.
- [Doi et al. 98] K. Doi, H. Hida, and H. Ishii. "Discriminant of Hecke fields and twisted adjoint  $L$ -values for  $GL(2)$  ." *Invent. Math.* **134** (1998), 547–577.
- [Iwasawa 72] K. Iwasawa. *Lectures on  $p$ -Adic  $L$ -Functions*, Ann. of Math. Studies 74, Princeton Univ. Press, 1972.
- [Miyake 89] T. Miyake. *Modular Forms*, Springer-Verlag, Berlin, Heidelberg, and New York, 1989.
- [Naganuma 73] H. Naganuma. "On the coincidence of two Dirichlet series associated with cusp forms of Hecke's "Neben"-type and Hilbert modular forms over a real quadratic field." *J. Math. Soc. Japan* **25** (1973), 547–555.
- [Neukirch 86] J. Neukirch. *Class Field Theory*, Springer-Verlag, Berlin, Heidelberg, and New York, 1986.
- [Okazaki 91] R. Okazaki. "On evaluation of  $L$ -functions over real quadratic fields." *J. Math. Kyoto Univ.* **31** (1991), 1125–1153.
- [Saito 84] H. Saito. "On an operator  $U_\chi$  acting on the space of Hilbert cusp forms." *J. Math. Kyoto Univ.* **24** (1984), 285–303.
- [Shimura 71] G. Shimura. *Introduction to the Arithmetic Theory of Automorphic Functions*, Iwanami Shoten and Princeton Univ. Press, 1971.
- [Shimura 78] G. Shimura. "The special values of the zeta functions associated with Hilbert modular forms." *Duke Math. J.* **45** (1978), 637–679.
- [Shimura 91] G. Shimura. "The critical values of certain Dirichlet series attached to Hilbert modular forms." *Duke Math. J.* **63** (1991), 557–613.
- [Shintani 76] T. Shintani. "On evaluation of zeta functions of totally real algebraic number fields at non-positive integers." *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **23** (1976), 393–417.
- [Siegel 69] C. L. Siegel. "Berechnung von Zetafunktionen an ganzzahligen Stellen." *Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl.* (1969), 87–102.
- [Weil 67] A. Weil. *Basic Number Theory*, Springer-Verlag, Berlin, Heidelberg, and New York, 1967.

Kaoru Okada, Department of Mathematical Sciences, Ritsumeikan University, Kusatsu, Shiga 525-8577, Japan  
(okada-k@se.ritsumei.ac.jp)

Received May 3, 2000; accepted in revised form October 12, 2001.