Bull. Korean Math. Soc. **42** (2005), No. 3, pp. 639–652

THE CLASS NUMBER OF ORDERS IN A QUATERNION ALGEBRA OVER A DYADIC LOCAL FIELD

SUNGTAE JUN AND INSUK KIM*

ABSTRACT. We find the class number of orders in a quaternion algebra over a dyadic local field.

1. Introduction

A quaternion algebra over a field F means a semi simple algebra of dimension 4 over k. It is known that there are three kinds of primitive orders in quaternion algebras over a local field. An order R of a quaternion algebra A over a local field k is called primitive if it satisfies one of following conditions. If A is a division algebra, R contains the full ring of integers of a quadratic extension field of k. If A is isomorphic to $\mathrm{Mat}_{2\times 2}(k)$, then R contains a subset which is isomorphic either to $\mathfrak{o}_k \oplus \mathfrak{o}_k$ where $\mathfrak{o}_k$ is the ring of integers in k, or to the full ring of integers in a quadratic extension field of k. The arithmetic properties of first two types of primitive orders were studied in [4], [5]. For the remaining type was studied in [6] only for the nondyadic local field case. In this paper we study the remaining type over a dyadic local field and we compute the class number of primitive orders over a dyadic local field.

2. Orders

In this section, we summarize the arithmetic theory of a quaternion algebra and its order.

A lattice on A is a finitely generated $\mathbb{Z}$ module containing a base of A over $\mathbb{Q}$. An order of A is a lattice on A which is also a subring with 1.

Received July 14, 2004.
2000 Mathematics Subject Classification: 11R11.
Key words and phrases: quaternion algebra, order, class number, normalizer.
* This author was supported by Wonkwang University in 2004.

The analogous definitions hold for lattices and orders in $A_p = A \otimes \mathbb{Q}_p$ for a prime p.

Throughout this paper we assume that k is a dyadic local field. Let $\mathfrak{o}$ denote the ring of integers in k, $\mathfrak{p}$ the maximal ideal of $\mathfrak{o}$. By $\Delta(\alpha)$, we denote the discriminant of α.

$$\Delta(\alpha) = \mathrm{Tr}(\alpha)^2 - 4N(\alpha),$$

where Tr and N are the trace and norm of L over k respectively, where L is a quadratic extension field of k. If Γ is an $\mathfrak{o}$ algebra of rank 2 contained in L, then $\Gamma = \mathfrak{o} + \mathfrak{o}x$ and the discriminant of Γ is

$$\Delta(\Gamma) = \Delta(x) \mod U^2,$$

where U is the set of all units in $\mathfrak{o}$.

Let $\mathfrak{o}^2 - 4\mathfrak{o} = \{s^2 - 4n \mid s, n \in \mathfrak{o}\}$. Then we consider the set of all possible discriminants $(\mathfrak{o}^2 - 4\mathfrak{o})/U^2$. Note that $\Delta^*_\sigma \neq \phi$ only if $\sigma = 2\rho, 0 \leq \rho \leq e$ or $\sigma = 2e+1$ where $e = \mathrm{ord}_k(2)$. Let

$$\Delta^* = \bigcup_{\sigma=0}^{\infty} \Delta^*_\sigma = \left(\bigcup_{\rho=0}^{e} \Delta^*_{2\rho} \right) \cup \Delta^*_{2e+1}.$$

Then we know Γ is a maximal order of a quadratic extension field of k if and only if $\Delta(\Gamma) \in \Delta^*$. If $e > 0$ and $1 \leq \rho \leq e$

$$\Delta^*_{2\rho} = \pi^{2\rho}(U^2 + \pi^{2e-2\rho+1}U)/U^2.$$

There is a bijective correspondence between elements of Δ^* and quadratic extension fields of k given by $\Delta(\Gamma) \to \Gamma \otimes \mathfrak{o}_k$ for $\Delta(\Gamma)$, an element of Δ^*.

Thus we can classify all quadratic extension fields of a dyadic local field k as follows: Δ^*_0 contains one point which corresponds to a unique unramified quadratic extension of k and

$$\Delta^*_{2e+1} = \pi^{2e+1}U/U^2$$

contains $2q^2$ points representatives where $q = |\mathfrak{o}/\mathfrak{p}|$.

DEFINITION 1. Let L be a quadratic extension of k. We define

$$t = t(L) = \mathrm{ord}_k(\Delta(L)) - 1.$$

REMARK. Note that if L is an unramified extension field of k, then $t = -1$. On the other hand, if L is a ramified extension field of a dyadic field k, then $t > 0$ (see 1.3 in [5]).

Let A be a rational quaternion algebra ramified precisely at the odd prime q and ∞. That is, $A_q = A \otimes \mathbb{Q}_q$ and $A_\infty = A \otimes \mathbb{R}$ are division algebras. Otherwise, $A_p = A \otimes \mathbb{Q}_p$ is isomorphic to a 2×2 matrix algebra, $M_2(\mathbb{Q}_p)$ for a finite prime $p \neq q$ (see [6]).

Fix a prime $p \neq q$ and let L be a quadratic extension field of $\mathbb{Q}_p$. Then $\left\{ \begin{pmatrix} \alpha & \bar{\beta} \\ \beta & \bar{\alpha} \end{pmatrix} \middle| \alpha, \beta \in L \right\}$ is a quaternion algebra over $\mathbb{Q}_p$ (see [7], [11]).

Let $\left\{ \begin{pmatrix} \alpha & \bar{\beta} \\ \beta & \bar{\alpha} \end{pmatrix} \middle| \alpha, \beta \in L \right\} = L + \xi L$, where $\xi = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Then $\xi\alpha = \overline{\alpha}\xi, \xi^2 = 1$ and $\bar{\xi} = -\xi$.

Hence, we can define the norm of an element in A as its determinant.

Let $\mathfrak{o}$ and p be the ring of integers and the prime of k. Let L be a quadratic extension field of k and let P_L be the prime ideal of $\mathcal{O}_L$ which is the ring of integers in L. Finally let Δ be the discriminant of L over k. In [7], we have computed that the possibilities of an order, R of A_2 containing $\mathcal{O}_L$. We state the results in the following theorem.

THEOREM 2.1. *Let the notations be as above. If an order R of A_2 contains $\mathcal{O}_L$, then R is one of the followings.*

(i) *If 2 is a unramified prime in L, $R = \mathcal{O}_L + \xi P_L^{\nu}$.*

(ii) *If 2 is a ramified prime in L, $R = \mathcal{O}_L + (1+\xi)P_L^{\nu-t-1}$ or $\overline{R_\nu} = \mathcal{O}_L + (1-\xi)P_L^{\nu-t-1}$, where $t = \operatorname{ord}_L(\Delta)$.*

Here, ν is a nonnegative integer.

Proof. See [7]. □

DEFINITION 2. Let A be a rational quaternion algebra ramified precisely at one finite prime q and ∞. An order M of A has level $\tilde{N} = (q; L(2), \nu)$ if

(i) $M \otimes \mathbb{Z}_p$ is the maximal order of $A \otimes \mathbb{Q}_p$ for an odd prime p,

(ii) there exists a quadratic extension field $L(2)$ of $\mathbb{Q}_2$ and a nonnegative integer ν (which is even if $L(2)$ is unramified) such that an order of A_2 containing the ring of integers of $L(2)$ is either R_ν or $\overline{R_\nu}$.

If L is ramified, then an order of A_2 is either R_ν or $\overline{R_\nu}$. The relation between R_ν and $\overline{R_\nu}$ is as follows. Let $e = \operatorname{ord}_k 2$. Then $\operatorname{ord}_L 2 = 2e$. Thus if $t < 2e$, then $R_0 = \overline{R_0}$. If $t = 2e$, $R_0 \neq \overline{R_0}$ and $R_1 = \overline{R_1}$ (see remark 1.8 in [4]).

Thus we have the following lemma.

LEMMA 2.2. *If R_ν is an order of A_2 containing the ring of integers of L, then*

1. *if L is unramified,*
$$R_{2\nu}(L) \subset R_{2\nu-2} \subset \cdots \subset R_0,$$
2. *if L is ramified and $t < 2e$,*
$$R_\nu(L) \subset R_{\nu-1} \subset \cdots \subset R_0,$$
3. *if L is ramified and $t = 2e$,*
$$R_\nu(L) \subset R_{\nu-1} \subset \cdots R_1 \subset R_0 \subset \overline{R_0}.$$

REMARK. The level $\tilde{N}$ can be generalized to arbitrary primes without any difficulties. In this paper, we consider only $p = 2$ case for the computational convenience.

DEFINITION 3. Let M be an order of level $\tilde{N}$ in A. A left M ideal I is a lattice on A such that $I_p = M_p a_p$ (for some $a_p \in A_p^\times$) for all $p < \infty$. Two left M ideals I and J are said to belong to the same class if $I = Ja$ for some $a \in A^\times$. One has the analogous definition for right M ideals.

DEFINITION 4. The class number of the left ideals for any order M of level $\tilde{N}$ is the number of distinct classes of such ideals. We denote this by $H(\tilde{N})$.

REMARK. Let A be a quaternion algebra and let M be any order of A. The ideal group of J_A of A is
$$J_A = \left\{ \tilde{a} = (a_p) \in \prod_p A_p^\times \mid a_p \in U(M_p) \text{ for almost all } p \right\},$$
where $U(M_p)$ is the set of all units in M_p.

Here the product is over all primes, finite and infinite. Note that since two orders M and N of A, $M_p = N_p$ for almost all p, J_A is independent of the particular used in this definition. J_A is a locally compact group with the topology induced by the product topology on the open set $\prod_{p \in S} A_p^\times \prod_{p \notin S} U(M_p)$, where S ranges over all finite subset of primes containing ∞. If $\tilde{a} \in J_A$, we define the volume of $\tilde{a}$ as $\mathrm{vol}(\tilde{a}) = \prod_p |N(a_p)|_p$ where $|\cdot|_p$ is normalized such that $|p|_p = \frac{1}{p}$ for $p < \infty$ and $|\cdot|_\infty$ is the ordinary absolute value in $\mathbb{R}$. Let $J_A^1 = \{\tilde{a} \in J_A \mid \mathrm{vol}(\tilde{a}) = 1\}$ and embed $A^\times \subset J_A^1$ along the diagonal. Finally, if M is an any order of A, let $\mathfrak{U}(M) = \{\tilde{a} \in J_A^1 \mid a_p \in U(M_p) \text{ for all } p < \infty\}$.

PROPOSITION 2.3. *Let M be any order of level $\tilde{N}$ in A. Then*

1. *$A^\times$ is a discrete subgroup of J_A^1.*
2. *$J_A^1/A^\times$ is compact.*
3. *$\mathfrak{U}(M)$ is an open compact subgroup of J_A^1.*

Proof. See Weil[13]. □

PROPOSITION 2.4. *The double coset $\mathfrak{U}(M)\backslash J_A^1/A^\times$ are in 1-1 correspondence with the ideal classes of left M ideals.*

Proof. If $J_A^1 = \bigcup_{i=1}^H \mathfrak{U}(M)\tilde{a}_i A^\times$, then $M\tilde{a}_i$, $i = 1, \cdots, H$, represent the distinct left M ideal classes. □

PROPOSITION 2.5. *J_A^1 acts transitively*(by conjugation) *on orders of level $\tilde{N}$ in A.*

Proof. The action is for $\tilde{a} \in J_A^1$ and M an order of level $\tilde{N}$: $M \leftrightarrow \{M_p\} \mapsto \{a_p^{-1}M_p a_p\} \leftrightarrow M'$ and we write $M' = \tilde{a}^{-1}M\tilde{a}$. The action is obviously transitive. □

3. The Selberg trace formula

Let G be a locally compact group with an open compact subgroup U and a discrete subgroup Γ with G/Γ compact. Then G is unimodular (i.e., every left Haar measure is right Haar measure) and we normalize Haar measure dx on G such that $\int_U dx = 1$. Let $L(G, U)$ be the set of complex valued continuous functions F on G with compact support such that $F(ugu') = F(g)$ for all $g \in G, u, u' \in U$. Let $L(U\backslash G/\Gamma)$ be the set of all complex valued continuous functions f on G such that $f(ug\gamma) = f(g)$ for all $u \in U, g \in G, \gamma \in \Gamma$, For any $\gamma \in \Gamma$, let $\{\gamma\}$ denote the conjugacy class of γ in Γ and let $\Gamma(\gamma)$ denote the centralizer of γ in Γ. For a discrete subgroup S of G, we also denote by dx the invariant quotient measure on G/S, i.e., if f is continuous with compact support on G, then

$$\int_G f(x)dx = \int_{G/S}\left(\sum_{s\in S} f(xs)\right)dx.$$

Any $F \in L(U, G)$ induces a linear transformation on the finite dimensional complex vector space $L(U\backslash G/\Gamma)$ by convolution,

$$(F(f))(x) = (F * f)(x) = \int_G F(xy^{-1})f(y)dy$$

and its trace is given by

PROPOSITION 3.1. (Selberg Trace Formula).

$$\operatorname{Trace} F = \sum_{\{\gamma\}} \int_{G/\Gamma(\gamma)} \psi_\gamma(x)dx,$$

where $\psi_\gamma(x) = F(x\gamma x^{-1})$ and the sum is over representatives of all conjugacy classes in Γ.

Proof. See [12]. □

For the next lemmas, we let $G = J_A$, $U = \mathfrak{U}(M)$ and $\Gamma = A^\times$.

LEMMA 3.2. *Let F be the characteristic function on U. Let dx be the measure on G normalized so that $\int_U dx = 1$. Then*

$$H(\tilde{N}) = \sum_{\{\gamma\}} \int_{G/\Gamma(\gamma)} \psi_\gamma(x)dx,$$

where $\psi_\gamma(x) = F(x\gamma x^{-1})$.

Proof. It is easy to see that F induces the identity map on $L(U\backslash G/\Gamma)$. Thus $\operatorname{Trace} F = \dim L(U\backslash G/\Gamma) = |U\backslash G/\Gamma|$. By Proposition 2.4, Trace F is the class number of order M of level $\tilde{N}$. □

LEMMA 3.3. *If*

$$\int_{G/\Gamma(\gamma)} \psi_\gamma(x)dx \neq 0,$$

then $\gamma = \pm 1$, or has a minimal polynomial, $x^2 \pm 1$ or $x^2 \pm x + 1$.

Proof. Let $x \in G$. If $\psi_\gamma(x) \neq 0$, then $F(x\gamma x^{-1}) \neq 0$. That is,

$$x\gamma x^{-1} \in \mathfrak{U}(M) \Leftrightarrow \gamma \in \mathfrak{U}(x^{-1}Mx) \cap A^\times = \mathfrak{U}(x^{-1}Mx).$$

Thus γ is a unit of some order of A. If γ belongs to $\mathbb{Q}$, then $\gamma = \pm 1$. If $\gamma \notin \mathbb{Q}$, $N(\gamma)$ is a unit in $\mathbb{Z}$. The minimal polynomial of γ is $f(x) = x^2 - sx + n$ where $s \in \mathbb{Z}$, $n = \pm 1$. If $f(x)$ had a real root, it would mean that $\mathbb{R}$ is a splitting field for A. Thus $s^2 - 4n < 0$, i.e., $n = 1$ and $s = 0$ or $s = \pm 1$. □

4. The class number

Let A be a rational quaternion algebra ramified precisely at the odd prime q and ∞ and let M be the order in a quaternion algebra of $\tilde{N} = (q; L(2), \nu)$ with $\nu > 1$, where $L(2)$ is the quadratic extension field of $\mathbb{Q}_2$.

REMARK. We define the normalizer of an order M as

$$\mathfrak{N}(M) = \{\tilde{a} \in J_A^1 | \ \tilde{a}^{-1} M \tilde{a} = M\}$$

locally, $\mathcal{N}(M_p) = \{a_p \in A_p^\times | \ a_p^{-1} M_p a_p = M_p\}$.

In order to compute the normalizer of orders, we first compute the normalizer of orders locally. For the nondyadic case, the normalizer of orders were computed in [6], [8]. Here, we will compute the only dyadic local field case, i.e. $p = 2$ case.

Recall the definition of orders, R_ν. For the computational convenience, we introduce a new notation :

$$M(R_\nu) = \{x \in R_0(L)^\times \mid x^{-1} R_\nu x = R_\nu\}.$$

THEOREM 4.1. *Let L be a unramified quadratic extension field of k and $k = \mathbb{Q}_2$. Then for an order of $A_2 = A \otimes k$, $R_\nu(L)$, we have*

$$M(R_\nu) = \begin{cases} R_0^\times, & \\ R_\nu^\times \cup \xi R_\nu^\times & \text{for } \nu > 0. \end{cases}$$

Proof. $\nu = 0$ case is trivial. Hence assume that $\nu > 0$. Let $\alpha + \xi\beta \in R_\nu(L) = \mathcal{O}_L + \xi P_L^\nu$ and $g \in R_0^\times = (\mathcal{O}_L + \xi\mathcal{O}_L)^\times$.

$$\begin{aligned} g(\alpha + \xi\beta)\overline{g} &= (\gamma + \xi\delta) \cdot (\alpha + \xi\beta) \cdot (\overline{\gamma + \xi\delta}) \\ &= (\alpha\gamma + \beta\overline{\delta} + \xi(\alpha\delta + \beta\overline{\gamma}))) \cdot (\overline{\gamma} - \xi\delta) \\ &= \alpha\gamma\overline{\gamma} + \beta\overline{\gamma\delta} - \overline{\alpha\delta}\delta - \overline{\beta}\gamma\delta + \xi(\alpha\overline{\gamma}\delta + \beta\overline{\gamma}^2 - \overline{\alpha\gamma}\delta - \beta\delta^2) \\ &\in \mathcal{O}_L + \xi P_L^\nu. \end{aligned}$$

$\alpha\overline{\gamma}\delta + \beta\overline{\gamma}^2 - \overline{\alpha\gamma}\delta - \beta\delta^2 \in P_L^\nu$ implies that $\mathrm{ord}_k((\alpha - \overline{\alpha})\overline{\gamma}\delta) \geq \nu$. Hence either $\mathrm{ord}_L(\delta) \geq \nu$ and $\gamma \in \mathcal{O}_L^\times$, or $\mathrm{ord}_L(\gamma) \geq \nu$ and $\delta \in \mathcal{O}_L^\times$. This implies that $M(R_\nu(L)) = R_\nu(L)^\times \cup \xi R_\nu(L)^\times$. □

COROLLARY 4.2. *Let L be a unramified quadratic extension field of k and $k = \mathbb{Q}_2$. Then $M(R_\nu)/R_\nu^\times \approx \{1, \xi\}$ as a set theoretical equivalence for $\nu > 0$.*

Proof. This is immediate from the above theorem. □

THEOREM 4.3. *Let L be a ramified quadratic extension field of k and $k = \mathbb{Q}_2$. Then for an order of $A_2 = A \otimes k$, $R_\nu(L)$, we have*

$$M(R_\nu) = \begin{cases} R_\nu^\times & \text{if } \nu = 0, \\ R^\times_{[\frac{1}{2}(\nu+1)]} & \text{if } 0 < \nu \leq 2t + 2, \\ R^\times_{\nu-t-1} \cup \xi R^\times_{\nu-t-1} & \text{if } 2t + 2 < \nu, \end{cases}$$

where $[x]$ is the largest integer not greater than x.

Proof. If $\nu = 0$, R_0 is a maximal order. $M(R_0) = R_0^\times$ clear from the definition.

Now assume that L is ramified. Let $g \in M(R_\nu)$. Then gR_1g^{-1} contains R_ν and gR_1g^{-1} is the second largest order containing R_ν, which implies $gR_\nu g^{-1} = R_\nu$. Without loss of generality, we assume that $M(R_\nu) \subset M(R_1) = R_1^\times$. Let $g = c + d + \xi d \in R_1^\times$ and $a + b + \xi b \in R_\nu = \mathcal{O}_L + (1+\xi)P_L^{\nu-t-1}$.

$$\begin{aligned}
&g(\alpha + \xi\beta)\overline{g}\\
&= (c+d+\xi d)\cdot(a+b+\xi b)\cdot(\overline{c+d+\xi d})\\
&= (c+d+\xi d)\cdot(a+b+\xi b)\cdot(\overline{c+d} - \xi d)\\
&= ((c+d)(a+b) + b\overline{d} + \xi((a+b)d + b(\overline{c+d}))\cdot(\overline{c+d} - \xi d)\\
&= N(c+d)(a+b) + b\overline{d}(\overline{c+d}) - (\overline{a+b})\overline{d}d - \overline{b}(c+d)d\\
&\qquad + \xi((a+b)(\overline{c+d})d + b(\overline{c+d})^2 - \overline{(c+d)(a+b)}d - \overline{b}d^2)\\
&\in \mathcal{O}_L + (1+\xi)P_L^{\nu-t-1}.
\end{aligned}$$

Thus we need two conditions,

$$(a+b)(\overline{c+d})d + b(\overline{c+d})^2 - \overline{(c+d)(a+b)}d - \overline{b}d^2 \in P_L^{\nu-t-1}$$

and

$$\begin{aligned}
&N(c+d)(a+b) + b\overline{d}(\overline{c+d}) - (\overline{a+b})\overline{d}d - \overline{b}(c+d)d\\
&\qquad - \{(a+b)(\overline{c+d})d + b(\overline{c+d})^2 - \overline{(c+d)(a+b)}d - \overline{b}d^2\} \in \mathcal{O}_L.
\end{aligned}$$

For the first one, we have the followings.

$$\begin{aligned}
&(a+b)(\overline{c+d})d + b(\overline{c+d})^2 - \overline{(c+d)(a+b)}d - \overline{b}d^2\\
&= ((a+b) - (\overline{a+b}))(\overline{c+d})d + b(\overline{c+d})^2 - \overline{b}d^2\\
&= ((a-\overline{a})(\overline{c+d})d + (b-\overline{b})(\overline{c+d})d + b\overline{c}^2 + 2b\overline{c}\overline{d} + b\overline{d}^2 - \overline{b}d^2\\
&= ((a-\overline{a})(\overline{c+d})d + (b-\overline{b})\overline{c}d + b\overline{c}^2 + 2b\overline{c}\overline{d} + b\overline{d}^2 - \overline{b}d^2 + (b-\overline{b})d\overline{d}\\
&= ((a-\overline{a})(\overline{c+d})d + (b-\overline{b})\overline{c}d + b\overline{c}^2 + 2b\overline{c}\overline{d} + (b\overline{d} - \overline{b}d)(d+\overline{d}).
\end{aligned}$$

Since $d \in P_L^{-t}$, $\mathrm{Tr}(d) = d + \overline{d} \in \mathcal{O}_L$. Hence, $b \in P_L^{\nu-t-1}$ implies that $\mathrm{ord}_L((a-\overline{a})(\overline{c+d})d) = t + 1 + 2\,\mathrm{ord}_L(d) \geq \nu - t - 1$ is necessary. That is, $\mathrm{ord}_L(d) \geq \frac{1}{2}\nu - t - 1$ and the second condition is easily satisfied if $\mathrm{ord}_L(d) \geq \frac{1}{2}\nu - t - 1$. Thus $M(R_\nu(L)) = R_{[\frac{1}{2}(\nu+1)]}(L)$, where $[x]$ is the largest integer not greater than x.

$$M(R_\nu) = R^\times_{[\frac{1}{2}(\nu+1)]}.$$

On the other hand, if $d \in \mathcal{O}_L$ i.e. $\mathrm{ord_L(d)} \geq 2\mathrm{t}+2$, then $\mathrm{ord}_L((a-\bar{a})(\overline{c+d})d) = t+1+\mathrm{ord}_L(d) \geq \nu - t - 1$. That is $d \in P_L^{\nu-2t-2}$. Since $\xi \in M(R_\nu)$ for every $\nu > t+1$,

$$M(R_\nu) = R_{\nu-t-1}^\times \cup \xi R_{\nu-t-1}^\times. \qquad \square$$

COROLLARY 4.4. *Let L be a ramified quadratic extension field of k and $k = \mathbb{Q}_2$. Then for an order of $A_2 = A \otimes k$, $R_\nu(L)$,*

$$M(R_\nu)/R_\nu^\times \approx \begin{cases} \{1\} & \text{if } \nu = 0, \\ R^\times_{[\frac{(\nu+1)}{2}]}/R^\times_{[\frac{(\nu+1)}{2}]+1} \times \cdots \times R^\times_{\nu-1}/R^\times_\nu & \text{if } 0 < \nu \leq 2t+2, \\ R^\times_{\nu-t-1}/R^\times_{\nu-t} \times \cdots \times R^\times_{\nu-1}/R^\times_\nu & \text{if } 2t+2 < \nu, \end{cases}$$

where $\approx$ is the set theoretical bijective relation.

Proof. $\nu = 0$ case is trivial. Assume that $\nu > 0$. By Theorem 4.3, $M(R_\nu)/R_\nu^\times = R^\times_{[\frac{1}{2}(\nu+1)]}/R_\nu^\times$.

$$R^\times_{[\frac{1}{2}(\nu+1)]}/R_\nu^\times \approx R^\times_{[\frac{1}{2}(\nu+1)]}/R^\times_{[\frac{1}{2}(\nu+1)]+1} \times R^\times_{[\frac{1}{2}(\nu+1)]+1}/R_\nu^\times$$

and inductively, we can prove

$$M(R_\nu)/R_\nu^\times \approx R^\times_{[\frac{1}{2}(\nu+1)]}/R^\times_{[\frac{1}{2}(\nu+1)]+1} \times \cdots \times R^\times_{\nu-1}/R^\times_\nu$$

for $0 < \nu \leq 2t+2$. Similarly,

$$M(R_\nu)/R_\nu^\times = R^\times_{\nu-t-1}/R^\times_\nu \approx R^\times_{\nu-t-1}/R^\times_{\nu-t} \times \cdots \times R^\times_{\nu-1}/R^\times_\nu$$

for $\nu > 2t+2$. $\square$

REMARK. If $k = \mathbb{Q}_2$, $|R_\nu^\times/R_{\nu+1}^\times| = 2$ was proved for each $\nu > 0$ (see [7]). This will be used in Theorem 4.7 later.

DEFINITION 5. Let K be a quadratic field extension of $\mathbb{Q}$ contained in A. If $\mathcal{O}$ is an order of K and M is an order of A. $\mathcal{O}$ is optimally embedded in M if $K \cap M = \mathcal{O}$.

REMARK. It is well known that

$$K \cap M = \mathcal{O} \Leftrightarrow K_p \cap M_p = \mathcal{O}_p \quad \text{for all } p < \infty.$$

Any order M' of level $\tilde{N}$ can be written as $M' = \tilde{b}^{-1}M\tilde{b}$ with some $\tilde{b} \in J_A^1$, where M is the canonical order of level $\tilde{N}$. Suppose $K \cap \tilde{b}^{-1}M\tilde{b} = \mathcal{O}$. If $\tilde{c} \in \mathfrak{N}(M)$, then $K \cap \tilde{b}^{-1}\tilde{c}^{-1}M\tilde{c}\tilde{b} = \mathcal{O}$. Hence it suffices to consider $\tilde{b} \mod \mathfrak{N}(M)$. Further, if $\tilde{a} \in J_K^1$, then we have $K \cap \tilde{a}^{-1}\tilde{b}^{-1}M\tilde{b}\tilde{a} = \mathcal{O}$. Thus $D(\mathcal{O})$ will denote that the number of double cosets $\mathfrak{N}(M)\tilde{b}J_K^1$ in J_A^1 such that $K \cap \tilde{b}^{-1}M\tilde{b} = \mathcal{O}$.

Locally, we define $D(\mathcal{O})$ as followings.

DEFINITION 6. $D(\mathcal{O}_p)$ is the number of double cosets $\mathcal{N}(M_p)b_pK_p^\times$ in $A_p^\times$ such that $K_p \cap b_p^{-1}M_pb_p = \mathcal{O}_p$.

$D(\mathcal{O}_p)$ is the number of essentially different orders (of level $\tilde{N}$) of A_p in which $\mathcal{O}_p$ is optimally embedded.

The number $D(\mathcal{O}_p)$ can be determined as follows.

THEOREM 4.5. *Let K and A be as above and let M be an order of A with level $\tilde{N} = (q; L(2), \nu(2))$. Then we have the followings.*

1. $p = q$. $D(\mathcal{O}_q) = \begin{cases} 1 & \text{if } \mathcal{O}_p \text{ is maximal in } K_p, \\ 0 & \text{otherwise.} \end{cases}$
2. $p \nmid 2q$. $D(\mathcal{O}_p) = 1$.
3. $p = 2$. $D(\mathcal{O}_2) = \begin{cases} 1 & \text{if both } K \text{ and } L(2) \text{ are ramified or both unramified,} \\ 0 & \text{if one of } K_2 \text{ and } L(2) \text{ is ramified and the other is unramified extension field.} \end{cases}$

Proof. We prove three cases separately.

1. $p = q$. $K_p \cap M_p$ is the maximal order of K_p and $\mathcal{N}(M_p) = A_p^\times$. Thus $D(\mathcal{O}_p) = 1$ or 0 according as $\mathcal{O}_p$ is maximal in K_p or not.
2. $p \nmid 2q$. Chevalley-Hasse-Noether implies $D(\mathcal{O}_p) = 1$ always. See [3, p.97].
3. $p = 2$. We divide into three cases. First, one of K_2 and $L(2)$ is ramified and the other is unramified extension field. In this case, there does not exists optimal embedding from K_2 into an order R_ν. Second, both K_2 and $L(2)$ are unramified. By Lemma 2.2, there is a unique chain of orders, $R_{2i} \subset R_{2i-2} \subset \cdots R_0$. Hence, there is a unique order of level 2ν, i.e. $D(\mathcal{O}_2) = 1$. Finally, both K_2 and $L(2)$ are ramified. By Lemma 2.2, if $\nu > 0$, then the exists a unique order containing $\mathcal{O}_L$. Hence $D(\mathcal{O}_2) = 1$. □

LEMMA 4.6. *Assume that $\gamma \neq \pm 1$ and suppose that $\psi_\gamma(x)$ is not identically zero. Let $K = \mathbb{Q}(\gamma)$. Then the support of $\psi_\gamma(x)$ in G consists of the disjoint union of the double cosets $\mathfrak{N}(M)\tilde{b}J_K^1$ satisfying $K \cap \tilde{b}^{-1}M\tilde{b} = \mathcal{O}_K$ for some order $\mathcal{O}_K$ of K containing γ.*

Proof. Suppose $\tilde{y} \in \text{Support}\,\psi_\gamma$. Then $\psi_\gamma(\tilde{y}) \neq 0 \Rightarrow \tilde{y}\gamma\tilde{y}^{-1} \in \mathfrak{U}(M) \Leftrightarrow \gamma \in K \cap \tilde{y}^{-1}M\tilde{y} = \mathcal{O}_K$ for some order $\mathcal{O}_K$ in K. Conversely, if $\gamma \in \mathcal{O}_K = K \cap \tilde{y}M\tilde{y}^{-1}$ for some $\tilde{y} \in J_A^1$, then $\tilde{y}^{-1}\gamma\tilde{y} \in \mathfrak{U}(M)$. which implies that $\psi_\gamma(\tilde{y}) = 1$. That is $\tilde{y} \in \text{Support}\,\psi_\gamma$. □

THEOREM 4.7. *Assume $\gamma \in A^\times$, $\gamma \notin \mathbb{Q}$ and the minimal polynomial of γ is x^2+sx+n with $s,n \in \mathcal{O}$. Finally, assume $\gamma \in \mathfrak{N}(\tilde{b}M\tilde{b}^{-1})$. Then $\mathfrak{N}(M)\tilde{b}J_K^1$ consists of the disjoint union of $E(\mathcal{O})$ translates of $\mathfrak{U}(M)\tilde{b}J_K^1$, where $E(\mathcal{O}) = \prod_{p<\infty} E(\mathcal{O}_p)$ and*

$$E(\mathcal{O}_q) = \begin{cases} 1 & \text{if } q \text{ ramifies in } K, \\ 2 & \text{if } q \text{ remains prime in } K, \end{cases}$$

$$E(\mathcal{O}_2) = \begin{cases} 1 & \text{if } \nu = 0, \\ 2 & \text{if } L(2) \text{ is unramified and } \nu > 0, \\ 2^{\nu - [\frac{1}{2}(\nu+1)]} & \text{if } L(2) \text{ is ramified and } \quad 0 < \nu \le 2t+2, \\ 2^{t+2} & \text{if } L(2) \text{ is ramified and } \quad \nu > 2t+2, \end{cases}$$

$E(\mathcal{O}_p) = 1$ *if* $p \nmid 2q$.

Proof. We will compute this locally. For a prime q, $E(\mathcal{O}_q)$ is given at Proposition 22 in [8]. If $\pi_q \in K^\times$, i.e., q is ramified in K, then $\mathcal{N}(R_0(L(q))) = R_0^\times(L(q))K^\times$. If q is unramified in K, then $\pi_q \notin K^\times$. There is no split case for q in K contained in A.

Next, for $p = 2$, $\mathcal{N}(R_0(L(2))) = R_0^\times(L(2))K^\times$. Now assume that $\nu > 0$. By Corollary 4.4, if $L(2)$ is ramified and $1 \le \nu < 2t+2$, then $|M(R_\nu)/R_\nu^\times| = 2^{\nu-[\frac{1}{2}(\nu+1)]}$. Otherwise, $\mathcal{N}(R_\nu(L(2))) = R_\nu^\times(L(2))K^\times \cup \xi R_\nu^\times(L(2))K^\times$. Thus $|M(R_\nu)/R_\nu^\times| = 2\cdot 2^{t+1}$. Finally, if $p \nmid 2q$, then M_p is a maximal order in A_p. Thus $E(M_p) = 1$ was computed in [9], [7]. □

THEOREM 4.8. *Let M be an order of level $\tilde{N}$. Then*

$$\mathrm{Mass}(M) = \frac{1}{12}(q-1)\delta,$$

where $\delta = \begin{cases} (p^2-p)p^{\nu-2} & \text{if } L(2) \text{ is unramified}, \\ (p+1)p^{\nu-1} & \text{if } L(2) \text{ is ramified}. \end{cases}$

Proof. See [7]. □

REMARK. As we mentioned at the remark of Lemma 2.2, $p = 2$.

LEMMA 4.9. *Let M be an order of level $\tilde{N}$ and let K be a quadratic extension field of k. Then*

$$\mathrm{vol}(\mathfrak{U}(M)\tilde{b}J_K^1/K^\times) = \frac{h(\mathcal{O})}{w(\mathcal{O})},$$

where $h(\mathcal{O})$ is the class number of locally principal $\mathcal{O}$ ideals in K. i.e., $h(\mathcal{O}) = |J_K^1/\mathfrak{U}(\mathcal{O})K^\times|$ and $w(\mathcal{O}) = |U(\mathcal{O})|$. Here, $\mathfrak{U}(\mathcal{O}) = \mathfrak{U}(M) \cap J_K^1 =$

$(\prod_{p<\infty} U(\mathcal{O}_p) \times K_\infty^\times) \cap J_K^1$. *The volume is taken with respect to the quotient measure on* $J_A^1/K^\times$.

Proof. Let $J_K^1 = \bigcup_{i=1}^{h(\mathcal{O})} \tilde{x}_i \mathfrak{U}(\mathcal{O}) K^\times$. Then

$$\begin{aligned} &\mathrm{vol}(\mathfrak{U}(M)\tilde{b}J_K^1/K^\times) \\ =\ &\mathrm{vol}(\tilde{b}^{-1}\mathfrak{U}(M)\tilde{b}J_K^1/K^\times) \\ =\ &\mathrm{vol}(\bigcup_{i=1}^{h(\mathcal{O})} \tilde{x}_i \mathfrak{U}(\tilde{b}^{-1}M\tilde{b})K^\times) \\ =\ &h(\mathcal{O})\,\mathrm{vol}(\mathfrak{U}(\tilde{b}^{-1}M\tilde{b})/\mathfrak{U}(\tilde{b}^{-1}M\tilde{b}) \cap K^\times) \\ =\ &\frac{h(\mathcal{O})}{w(\mathcal{O})}. \end{aligned}$$

□

LEMMA 4.10. *Let* γ, K *be as in Lemma 4.6 and let* $\mathcal{O}$ *be a fixed order of* K *containing* γ. *Then* $\Gamma(\gamma) = K^\times$ *and the volume in* $G/\Gamma(\gamma)$ *of the support of* $\psi_\gamma(x)$ *attached to* $\mathcal{O}$, *that is, the sum of volumes of* $\mathfrak{N}(M)\tilde{b}J_K^1/K^\times$ *over all double cosets satisfying* $K \cap \tilde{b}^{-1}M\tilde{b} = \mathcal{O}$ *is* $D(\mathcal{O})E(\mathcal{O})\frac{h(\mathcal{O})}{w(\mathcal{O})}$.

Proof. See [8]. □

THEOREM 4.11. *The class number* $H(\tilde{N})$ *of orders of level* $\tilde{N}$ *is given by*

$$H(\tilde{N}) = \begin{cases} \frac{1}{12}(q-1)(2^2-2)2^{\nu-2} + \frac{1}{3}\left(1 - \left(\frac{-3}{q}\right)\right) & \text{if } L(2) \text{ is unramififed,} \\ \frac{1}{12}(q-1)(2+1)2^{\nu-1} + \frac{1}{4}\left(1 + \left(\frac{-1}{q}\right)\right)\delta(L(2)) & \text{if } L(2) \text{ is ramififed,} \end{cases}$$

where

$$\delta(L(2)) = \begin{cases} 2^{\nu-[\frac{1}{2}(\nu+1)]} & \text{for } \nu \le 2t+2, \\ 2^{t+1} & \text{for } \nu > 2t+2. \end{cases}$$

Here $(\cdot)$ *is the Kronecker symbol.*

Proof. By Selberg trace formula, we need to compute $\int_{G/\Gamma(\gamma)} \psi_x(x)dx$ for each value of γ. The possible value of γ is by Lemma 3.3, ± 1, a root of x^2+1 or $x^2 \pm x + 1$.

Case 1: $\gamma = 1$. $\Gamma(\gamma) = \Gamma$ implies that $\int_{G/\Gamma(\gamma)} \psi_x(x)dx = \mathrm{vol}(G/\Gamma) = \mathrm{Mass}(M)$. By Theorem 4.5, $\mathrm{Mass}(M)$ was computed.

Case 2: γ is a root of x^2+1. Let $K = \mathbb{Q}_2(\gamma)$ and assume that K is embedded in A. By Lemma 4.6, it suffices to compute the number of elements $\tilde{b}$ satisfying $\tilde{b}^{-1}M\tilde{b} \cap K = \mathcal{O}_K$. That is, the number of optimal embeddings from γ into R_ν. Since $K = \mathbb{Q}_2(\gamma)$ is a ramified extension field of $\mathbb{Q}_2$, if $L(2)$ is unramified, no optimal embedding exists unless R_ν is a maximal order. On the other hand, if $L(2)$ is ramified, then $D(\mathcal{O}_2)$ is given at Theorem 4.5. Hence by Lemma 4.7,

$$\begin{aligned} \frac{h(\mathcal{O})}{w(\mathcal{O})} &= \frac{1}{4} \\ D(\mathcal{O}_2)E(\mathcal{O}_2) &= D(\mathcal{O}_2)E(\mathcal{O}_2) \cdot \begin{cases} 2^{\nu-[\frac{1}{2}(\nu+1)]} & \text{for } \nu \le 2t+2, \\ 2^{t+1} & \text{for } \nu > 2t+2, \end{cases} \\ D(\mathcal{O}_q)E(\mathcal{O}_q) &= 1 \cdot \left(1 + \left(\frac{-1}{q}\right)\right). \end{aligned}$$

Here $(\cdot)$ is the Kronecker symbol.

Case 3: γ is a root of $x^2 \pm x + 1$. Let $K = \mathbb{Q}_2(\gamma)$. Then K is a unramified quadratic extension field of $\mathbb{Q}_2$. As in the case 2, we should compute the number of optimal embeddings from K into R_ν where $L(2)$ is the unramified extension field of $\mathbb{Q}_2$. The number of optimal embeddings is 1. Hence, $D(\mathcal{O}_q) = 1$ and

$$\begin{aligned} \frac{h(\mathcal{O})}{w(\mathcal{O})} &= \frac{1}{6}, \\ D(\mathcal{O}_2)E(\mathcal{O}_2) &= \delta(L(2)), \\ D(\mathcal{O}_q)E(\mathcal{O}_q) &= 1 \cdot \left(1 - \left(\frac{-3}{q}\right)\right), \end{aligned}$$

where $\delta(L(2)) = 1$ if $L(2)$ is unramified and -1 if $L(2)$ is ramified. Here $(\cdot)$ is the Kronecker symbol. □

References

[1] A. Atkin and J. Lehner, *Hecke operators on* $\Gamma_0(N)$, Math. Ann. **185** (1970), 134–160.

[2] M. Deuring, *Die An zahl der Typen von Maximalordnungen einer definitn Quaternionalgebra mit primer Grundzahl*, Jber. Deutsch. Math. Verein. **54** (1950), 24–41.

[3] M. Eichler, *The basis problem for modular forms and the traces of Hecke operators*, Springer-Verlag, Lecture Notes in Math. **320** (1972), 75–151.
[4] H. Hijikata, *Explicit formula of the traces of the Hecke operators for* $\Gamma_0(N)$, J. Math. Soc. Japan **26** (1974), 56–82.
[5] H. Hijikata, A. Pizer, and T. Shemanske, *Orders in Quaternion Algebras*, J. Reine Angew Math. **394** (1989), 59–106.
[6] S. Jun, *On the certain primitive orders* J. Korean Math. Soc. **4** (1995), 473–481.
[7] ———, *Mass formula of an order over a dyadic local field*, preprint.
[8] A. Pizer, *On the arithmetic of Quaternion algebras II* , J. Math. Soc. Japan **28** (1976), 676–698.
[9] ———, *The action of the Canonical involution on Modular forms of weigh 2 on* $\Gamma_0(N)$, Math. Ann. **226** (1977), 99–116.
[10] ———, *An Algorithm for computing modular forms on* $\Gamma_0(N)$, J. Algebra **64** (1980), 340–390.
[11] I. Reiner, *Maximal orders*, Academic Press, 1975.
[12] T. tamagawa, *On the trace formula*, J. Fac. Sci. Univ. Tokyo Sec. **I** (1960), 363–380.
[13] A. Weil, *Basic number theory*, Berlin, Hedelberg, New York, Springer, 1967.

Sungtae Jun, Division of Mathematics and Computer Science, Konkuk University, Choongju 380-151, Korea
E-mail: sjun@kku.ac.kr

Insuk Kim, Department of Mathematics Education, Wonkwang University, Iksan 570-749, Korea
E-mail: iki@wonkwang.ac.kr