J. Korean Math. Soc. **34** (1997), No. 4, pp. 791–807

ON THE CERTAIN PRIMITIVE ORDERS

SUNGTAE JUN

ABSTRACT. There are several kinds of orders in a quaternion algebra. In this article, the relation between the orders is studied.

1. Introduction

It is well known that there is a close connection between primitive orders in a quaternion algebra and modular forms of weight 2 on $\Gamma_0(N)$. A primitive order in a quaternion algebra over a number field K is an order which contains the ring of integers in a quadratic extension field of K.

There are two types of quaternion algebra over a local field k, a division algebra and a 2×2 matrix algebra. In quaternion algebras over a local field, primitive orders can be classified into three kinds of types. That is, a primitive order in a quternion division algebra which contains the ring of integers of a quadratic extension field of k. In a 2×2 matrix algebra, there are two types of primitive orders. One is an order which contains $\mathcal{O} \times \mathcal{O}$ where $\mathcal{O}$ is the ring of integers in k and the other is an order in a 2×2 matrix algebra which contains the ring of integers of a quadratic extension field of k.

Primitive orders in 2×2 matrix algebra which contains $\mathcal{O} \times \mathcal{O}$ where $\mathcal{O}$ is the ring of integers were studied by Hijikata [4]. Primitive orders in a division algebra, so called, "special orders" were studied by Hijikata, Pizer and Shemanske [5]. They constructed Brandt matrices associated with the arithmetic theories of these orders. Using optimal embedding theory of special orders, they finally solved basis problem with Brandt matrices [6].

Received October 20, 1996. Revised July 8, 1997.
1991 Mathematics Subject Classification: 11R52.
Key words and phrases: quaternion algebra, Brandt matrix, primitive order.
This work is partially supported by BSRI-96-1438.

The remaining type of primitive orders was studied by Brezinski and he found the formula of the number of equivalence classes of optimal embeddings in primitive orders [1]. However, with the results of [1], there are some technical problems to construct Brandt matrices associated with the remaining type of orders. These Brandt matrices will play a central role in the study of certain theta series [8].

In this paper we investigate the arithmetic theory of primitive orders in a 2×2 matrix algebra containing the ring of integers of a quadratic extension field of k and tabulate the number of equivalence classes of optimal embeddings concretely. This arithmetic theory and table will enable us to study Brandt matrices associated with these orders and a certain space of modular forms of weight 2 on $\Gamma_0(N)$ (See [8]).

2. Orders in quaternion algebra

2.1 Let B be a quaternion algebra which is split over a nondyadic local field k and let L be a quadratic extension field of k contained in B. Then there exists an element ξ in $B^\times$ such that $B = L + \xi L$ and $x\xi = \xi\bar{x}$ for all $x \in L$ (See [9] p54). To see this clearly, we can identify B with $\left\{ \begin{pmatrix} \alpha & \bar{\beta} \\ \beta & \bar{\alpha} \end{pmatrix} | \alpha, \beta \in L \right\}$ and L with $\left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \bar{\alpha} \end{pmatrix} | \alpha \in L \right\}$, where $-$ is the conjugation of L over k. Then ξ is identified with $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Hence the norm and the trace of an element in B are defined as the determinant and the trace of corresponding element in $\left\{ \begin{pmatrix} \alpha & \bar{\beta} \\ \beta & \bar{\alpha} \end{pmatrix} | \alpha, \beta \in L \right\}$. Also, $N(\xi) = -1$ implies that $\bar{\xi} = -\xi$. Further, for an arbitrary $x \in L$, $\overline{\xi x} = \bar{x}\bar{\xi} = -\xi x$.

Let $\mathcal{O}_L(\mathcal{O})$ be the ring of integers in $L(k)$, $P_L(P)$ the prime ideal of $\mathcal{O}_L(\mathcal{O})$. Let $\pi_L(\pi)$ be the prime element of $P_L(P)$.

2.2 If α is integral of degree 2 over $\mathcal{O}$ satisfying $\alpha^2 - s\alpha + n = 0$. We denote the discriminant of α by $\Delta(\alpha) = s^2 - 4n$. If Γ is an $\mathcal{O}$ algebra of rank 2, $\Gamma = \mathcal{O} + \mathcal{O}\alpha$ for some α and $\Delta(\Gamma) = \Delta(\alpha)U^2$ where $U = \mathcal{O}^\times$.

DEFINITION 2.1. $t = t(L) = \mathrm{ord}_k(\Delta(L)) - 1$.

2.3 Thus it is easy to see if $x \in \mathcal{O}_L$, then $\mathrm{ord}_I(x) \geq \mathrm{ord}_k(\Delta(L)) = t + 1$.

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 nondyadic field, k, then $t = 0$ (See 1.3 in [5]).

PROPOSITION 2.2. *Let the notation be as above. Let R be an order of B and L a quadratic extension field in B. Then R contains $\mathcal{O}_L$ if and only if*

$$R = \begin{cases} \mathcal{O}_L + \xi P_L^n & \text{if } L \text{ is an unramified extension field, or} \\ \mathcal{O}_L + (1+\xi)P_L^{n-1} & \text{if } L \text{ is a ramified extension field, or} \\ \mathcal{O}_L + (1-\xi)P_L^{n-1} & \text{if } L \text{ is a ramified extension field} \end{cases}$$

for some nonnegative integers n.

Proof. Suppose that R is an order which contains $\mathcal{O}_L$. Then $R = u\mathcal{O}_L + y\mathcal{O}_L$ for some $u, y \in R$. Since $1 \in R$, let $u = 1$ without loss of generality. Now, $y \in R \subset B = L + \xi L$, let $y = \alpha + \xi\beta$ for some $\alpha, \beta \in L$ and $\beta \neq 0$. If $x \in \mathcal{O}_L$, then $xy = x(\alpha + \xi\beta) = (x - \bar{x})\alpha + y\bar{x}$. So $(x - \bar{x})\alpha = xy - y\bar{x} \in R$ for any $x \in \mathcal{O}_L$. Since $\mathrm{ord}_L(x - \bar{x}) \geq t + 1$ by 1.3, $\alpha \in P_L^{-t-1}$.

If $\alpha \in \mathcal{O}_L$, then $\beta \in \mathcal{O}_L$ since $N(y) = N(\alpha) - N(\beta) \in \mathcal{O}$. Let $n = \mathrm{ord}_L\beta$. Then $R = \mathcal{O}_L + \xi\beta\mathcal{O}_L = \mathcal{O}_L + \xi P_L^n$.

If $\alpha \notin \mathcal{O}_L$, then this is the case that L is ramified and $\alpha \in P_L^{-1} - \mathcal{O}_L$. Let $\alpha = \pi_L^{-1}u$ and $\beta = \pi_L^{-1}w$ where π_L is the prime element of P_L. From $N(y) = N(\alpha) - N(\beta) \in \mathcal{O}$, it is easy to see $N(u/w) \equiv 1 \mod P$. That is, $u/w \equiv \pm 1 \mod P_L$. Thus R is either $\mathcal{O}_L + (1+\xi)P_L^{-1}$ or $\mathcal{O}_L + (1-\xi)P_L^{-1}$.

The other direction of the proof is trivial. □

2.4 Let $\pi(\pi_L)$ be a prime element in the ring of integers in k (L respectively). Then if L is ramified, $\pi \equiv \pi_L^2 \mod \mathcal{O}_L^\times$ and if L is unramified, $\pi \equiv \pi_L \mod \mathcal{O}_L^\times$. We now need new notations of orders for the next step.

DEFINITION 2.3. Let L be a quadratic extension field of k and $\mathcal{O}_L$ its ring of integers. Then

(1) if L is unramified,

$$R_{2n}(L) = \mathcal{O}_L + \xi\pi_L^n\mathcal{O}_L \quad \text{for } n \geq 0,$$

(2) if L is ramified,

$$\begin{aligned} R_n(L) =& \mathcal{O}_L + \xi\pi_L^{n-1}\mathcal{O}_L \quad \text{for } n \geq 1, \text{ or} \\ R_0(L) =& \mathcal{O}_L + (1+\xi)\pi_L^{-1}\mathcal{O}_L, \quad \text{or} \\ \overline{R_0(L)} =& \mathcal{O}_L + (1-\xi)\pi_L^{-1}\mathcal{O}_L. \end{aligned}$$

LEMMA 2.4. *Let the notations be as above. Then*

(1) *if L is unramified,*

$$\cdots \subset R_{2n}(L) \subset R_{2n-2}(L) \cdots \subset R_0(L).$$

(2) *if L is ramified,*

$$\cdots \subset R_n(L) \subset R_{n-1}(L) \cdots \subset R_1(L) \subset \left\{ \begin{array}{c} R_0(L) \\ \overline{R_1(L)} \end{array} \right. .$$

Proof. This is immediate from definition 2.3. □

LEMMA 2.5. *Let L be a quadratic ramified extension field of k. Then* $R_1(L) \simeq \begin{pmatrix} \mathcal{O} & \mathcal{O} \\ P & \mathcal{O} \end{pmatrix} \simeq \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} | \alpha, \beta, \delta \in \mathcal{O} \text{ and } \gamma \in P \right\}$.

Proof. If an order R is either maximal or there exists a uniquely determined pair of orders $\{R', R''\}$ such that $R = R' \cap R''$, then R is $B^\times$ conjugate to $\begin{pmatrix} \mathcal{O} & \mathcal{O} \\ P^\nu & \mathcal{O} \end{pmatrix}$ for some nonnegative integer ν (See 2.2 [4]). Since $R_1(L) = R_0(L) \cap \overline{R_0(L)}$ and $R_1(L)$ is the second largest order containing $\mathcal{O}_L$, $R_1(L) \simeq \begin{pmatrix} \mathcal{O} & \mathcal{O} \\ P & \mathcal{O} \end{pmatrix}$. □

REMARK. All maximal orders are $B^\times$ conjugate each other. i.e. all maximal orders are isomorphic to

$$\begin{pmatrix} \mathcal{O} & \mathcal{O} \\ \mathcal{O} & \mathcal{O} \end{pmatrix} \simeq \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} | \alpha, \beta, \delta \in \mathcal{O} \text{ and } \gamma \in \mathcal{O} \right\}$$

(See 17.3 [12]).

2.5 By lemma 2.5 and the remark, all maximal orders and $R_1(L)$ are hereditary orders (See p27 [12]).

THEOREM 2.6. *Let the notations be as above. Then*

(1) *if L is unramified,*

$$|R_2^\times(L)\backslash R_0^\times(L)| = q^2 - q,$$
$$|R_{2n+2}^\times(L)\backslash R_{2n}^\times(L)| = q^2 \quad \text{for } n \geq 1,$$

(2) *if L is ramified,*

$$|R_1^\times(L)\backslash R_0^\times(L)| = q+1, \quad |R_2^\times(L)\backslash R_1^\times(L)| = q-1 \text{ and}$$
$$|R_{n+1}^\times(L)\backslash R_n^\times(L)| = q \quad \text{for } n \geq 2.$$

Proof. First, assume that L is unramified. If $n \geq 1$, define a map $\psi : R_{2n}^\times(L) \to P_L^n/P_L^{n+1}$ by $\psi(\alpha+\xi\beta) \equiv \beta/\bar{\alpha} \mod P_L^{n+1}$. Then for $\alpha+\xi\beta \in R_{2n}^\times(L) = (\mathcal{O}_L + \xi P_L^n)^\times$, $\alpha'+\xi\beta' \in R_{2n+2}^\times(L) = (\mathcal{O}_L + \xi P_L^{n+1})^\times$, i.e. $\alpha, \alpha' \in \mathcal{O}_L^\times$ and $\beta \in P_L^n, \beta \in P_L^{n+1}$,

$$\psi((\alpha'+\xi\beta')(\alpha+\xi\beta)) \equiv \frac{\beta'\alpha + \bar{\alpha}'\beta}{\alpha'\alpha + \bar{\beta}'\beta} \equiv \frac{\beta'\alpha' + \bar{\alpha}'\beta}{\overline{\alpha'\alpha}} \mod P_L^{n+1}$$
$$\equiv \frac{\beta}{\bar{\alpha}} \mod P_L^{n+1}.$$

Hence ψ induces a map $\tilde{\psi}$ of $R_{2n+2}^\times(L)\backslash R_{2n}^\times(L)$ onto P_L^n/P_L^{n+1}. It is not difficult to show $\tilde{\psi}$ is one to one. Thus $R_{2n+2}\times(L)\backslash R_{2n}^\times(L)| = |P_L^n/P_L^{n+1}| = q^2$. Next, the direct computations show that $R_2^\times(L)\backslash R_0^\times(L) = \{R_2^\times(L), R_2^\times(L)\xi\} \cup \{R_2^\times(L)(1+\xi v) | v \in (\mathcal{O}_L/P_L)^\times\}$, which is of $2+(q^2-q-2) = q^2-q$ elements.

Second, assume that L is ramified. $|R_1^\times/R_0^\times| = q-1$ is calculated by Hijikata [4] and $R_2^\times\backslash R_1^\times = \{R_2^\times, R_2^\times\xi\} \cup \{R_2^\times(1+\xi v) | v \in S\}$ where $S = \{x \in (\mathcal{O}/P)_L^\times | N(x) \neq 1 \mod P\}$ by similar calculations as in the unramified case. Since the number of elements in S is $q-3$, $|R_1^\times/R_2^\times| = 2+(q-3) = q-1$. Finally, if $n \geq 2$, let ψ be a map from $R_n^\times$ onto P_L^{n-1}/P_L^n defined by $\psi(\alpha+\xi\beta) \equiv \frac{\beta}{\bar{\alpha}} \mod P_L^n$, where $\alpha+\xi\beta \in R_n^\times$. Then

$$\psi((\alpha+\xi\beta)(\alpha'+\xi\beta')) \equiv \frac{\beta}{\bar{\alpha}} + \frac{\beta'}{\bar{\alpha}'} \mod P_L^n,$$

which means that ψ is a homomorphism of $R_n^\times$ onto P_L^{n-1}/P_L^n. It is easy to see that ψ induces an isomorphism of $R_n^\times/R_{n+1}^\times$ onto P_L^{n-1}/P_L^n. Thus $|R_{n+1}^\times \backslash R_n^\times| = |P_L^{n-1}/P_L^n| = |\mathcal{O}_L/P_L| = q$. □

3. Embeddings

3.1 Throughout this section, we assume that k is a nondyadic local field and B is a quaternion algebra which is split over k. Let K be a semi simple algebra of dimension 2 over k (i.e. K is either a field or K is isomorphic to $k \times k$). Suppose that K is a field. Then the definition of $R_m(K)$ is given in the definition 2.3. If K is not a field, then we will denote by $R_m(K) = \begin{pmatrix} \mathcal{O} & \mathcal{O} \\ P^m & \mathcal{O} \end{pmatrix}$. In this section, we will determine all possible embeddings of $R_n(L)$ into $R_m(K)$ for nonnegative integers n and m. By an embedding we mean a k (or $\mathcal{O}_k$, the ring of integers) injective homomorphism.

3.2 Assume that $K \subset B$. Let $\mathcal{O}_K$ be the maximal order of K. We say $\mathcal{O}_K$ is embeddable in $R_n(L)$ if there exists an embedding ϕ of K into B such that $\phi(\mathcal{O}_K) \subset R_n(L)$. According to theorem 17.3 [12], all maximal orders of B are $B^\times$ conjugate to each other. Hence $\mathcal{O}_K$ is embeddable into $R_0(L)$ and $\mathcal{O}_L$ is embeddable into $R_0(K)$.

DEFINITION 3.1. Let K and L be quadratic extensions of k contained in B. Then $\mu(K, L)$ is the nonnegative integer or ∞ such that $\mu(K, L) \geq n$ if and only if $\mathcal{O}_K$ is embeddable into $R_n(L)$.

3.3 We introduce the following notation;

$$\Delta R_n(L) = \{\Delta(\alpha) | \alpha \in R_n(L)\} \mod U^2,$$

where $U = \mathcal{O}_L^\times$ and $\Delta(\alpha) = \mathrm{Tr}(\alpha)^2 - 4\mathrm{N}(\alpha)$.

LEMMA 3.2. *Let K and L be quadratic extensions of k contained in B. The followings are equivalent.*

(1) *$\mathcal{O}_K$ is embeddable in $R_n(L)$.*
(2) *$\Delta(K) \in \Delta R_n(K)$.*
(3) *$n \leq \mu(K, L)$.*
(4) *$R_n(K) \simeq R_n(L)$*
(5) *$\mathcal{O}_L$ is embeddable in $R_n(K)$.*

Proof. By the definition of 3.1. (1) is equivalent to (3). (1) implies (2).

Suppose that $\Delta(K) \in \Delta R_n(L)$. Then there exists $x \in R_n(L)$ such that $\Delta(K) = \Delta(x) \mod U^2$. Let $K'' = k + kx$. Then $\mathcal{O}_{K''} \subset R_n(L)$. $\Delta(K) = \Delta(K'') \mod U^2$ implies that $K \simeq K''$. Hence $\mathcal{O}_K \simeq \mathcal{O}_{K''} \subset R_n(L)$. This proves (2) imples (1).

(4) $\Rightarrow$ (1) is clear. Conversely, suppose $\mathcal{O}_K$ is embeddable in $R_n(L)$. Then $R_n(L)$ is isomorphic to an n-th ($\frac{n}{2}$-th for K unramified) largest order containing $\mathcal{O}_K$, which is $R_n(K)$ by lemma 2.4.

(4) $\Rightarrow$ (5) is clear and (5) $\Rightarrow$ (4) is immediate from (1) and (4). □

COROLLARY 3.3. *Let K and L be quadratic extensions of k contained in B. Then $\mu(K, L) = \mu(L, K)$.*

Proof. It is immediate from lemma 3.2. □

LEMMA 3.4. *If K is an unramified extension field and L is a ramified field, or if K is an unramified extension field and $L \simeq k \times k$, then $\mu(K, L) = \mu(L, K) = 0$. On the other hand, if K is a ramified extension field and $L \simeq k \times k$, then $\mu(K, L) = \mu(L, K) = 1$.*

Proof. Since all maximal orders of B are $B^\times$ conjugate to each other, $\mu(K, L) \geq 0$ for all cases. If $K \simeq k \times k$, then an order of B which contains $\mathcal{O}_K$ is isomorphic to $\begin{pmatrix} \mathcal{O} & \mathcal{O} \\ P^n & \mathcal{O} \end{pmatrix}$ for some nonnegative integer n (See [4]). If K is an unramified extension field of k, then R_n is not isomorphic to an order of $\begin{pmatrix} \mathcal{O} & \mathcal{O} \\ P^n & \mathcal{O} \end{pmatrix}$ unless $n = 0$. However, if K a ramified extension field of k, then $R_1(L) \simeq \begin{pmatrix} \mathcal{O} & \mathcal{O} \\ P & \mathcal{O} \end{pmatrix}$ by lemma 2.5. If $n \geq 2$, $R_n(L)$ is not a maximal order and there are no distinct orders R', R'' such that $R_n(L) = R' \cap R''$ by lemma 2.4. Thus, by 2.2 in [4], $R_n(L) \not\simeq \begin{pmatrix} \mathcal{O} & \mathcal{O} \\ P^n & \mathcal{O} \end{pmatrix}$. Hence lemma is proved. □

LEMMA 3.5. *Assume that L and K are nonisomorphic quadratic ramified extension fields of k contained in B. Then $\mu(K, L) = \mu(L, K) = 2$.*

Proof. By lemma 2.4, $\mu(K,L) \geq 1$. So let $\pi_K = \alpha + \xi\beta \in R_1(L) = \mathcal{O}_L + \xi\mathcal{O}_L$. $\Delta(\pi_K) = \Delta(\alpha) + 4N(\beta)$ and $\mathrm{ord}_k(\Delta(\alpha)) \geq \mathrm{ord}_k(\Delta(\mathcal{O}_L)) = 1$. So $\beta \in P_L$, which implies $\pi_K \in R_2(L)$. On the other hand, if $\pi_K = \alpha + \xi\beta \in R_3(L) = \mathcal{O}_L + \xi P_L^2$, $\Delta(\alpha) = \Delta(L) \mod U^2$ since $\beta \in P_L^2$. However, as we assumed that L and K are not isomorphic each other, this is a contradiction. Hence $\mathcal{O}_K$ is not embeddable into $R_3(L)$. □

Finally, we are now able to answer the questions about the embeddability. as follows.

THEOREM 3.6. *Let K and L be quadratic extensions of k in B. The number $\mu(K,L)$ is determined as follows.*

(1) *If K is an unramified field extension of k, then*

$$\mu(K,L) = \begin{cases} 0 & \text{if } K \text{ is a ramified extension field of } k \\ & \text{or if } \ K \simeq k \times k \\ \infty & \text{if } K \text{ is an unramified extension field of } k\ . \end{cases}$$

(2) *If K is a ramified field extension of k, then*

$$\mu(K,L) = \begin{cases} 0 & \text{if } K \text{ is an unramified extension field of } k \\ 1 & \text{if } \ K \simeq k \times k \\ 2 & \text{if } K \text{ is a ramified extension field of } k \text{ and} \\ & K \text{ is not isomorphic to } L \\ \infty & \text{if } K \text{ is isomorphic to } L\ . \end{cases}$$

(3) *If $K \simeq k \times k$, then*

$$\mu(K,L) = \begin{cases} 0 & \text{if } K \text{ is an unramified extension field of } k \\ 1 & \text{if } K \text{ is a ramified extension field of } k \\ \infty & \text{if } \ K \simeq k \times k. \end{cases}$$

4. Optimal embeddings

Throughout this section, we assume that B is a quaternion algebra over k and K is a semi simple algebra of dimension 2 over a nondyadic local field k. (i.e. K is either a field or K is isomorphic to $k \times k$). Also let α generate the maximal order $\mathcal{O} + \mathcal{O}\pi^m\alpha$ of K where $\mathcal{O}$ is the ring of integers of k.

DEFINITION 4.1. Let α be the same as above. For a nonnegative integer m,

$$\begin{aligned}&\mathrm{Emb}(\pi^m\alpha, R_n)\\ &\quad = \{\phi | \phi \text{ is an embedding of } k(\alpha) \text{ into } B \text{ with } \phi(\pi^m\alpha) \in R_n\}\\ &\mathrm{Emb}_{op}(\pi^m\alpha, R_n)\\ &\quad = \{\phi \in \mathrm{Emb}(\pi^m\alpha, R_n) | \phi(k + k\alpha) \cap R_n = \varphi(\mathcal{O} + \mathcal{O}\pi^m\alpha)\}\end{aligned}$$

where $n \geq 0$.

4.1 Two different embeddings $\phi_1, \phi_2 \in \mathrm{Emb}(\pi^m\alpha, R_n)$ are said to R_n equivalent if there exists $\gamma \in R_n^\times$ such that $\phi_2(x) = \gamma\phi_1(x)\gamma^{-1}$ for all $x \in \mathcal{O} + \mathcal{O}\pi^m\alpha$.

We will calculate the number of equivalence classes of optimal embeddings from an order of K, $\mathcal{O} + \mathcal{O}\pi^m\alpha$ into the various orders, $R_n(L)$ containing the ring of integers of a quadratic extension field L. The number of equivalence classes of optimal embeddings will play the central role in computing the traces of Brandt matrices associated with these orders, $R_n(L)$ [8].

4.2 From the definition 4.1, the relation between embeddings and optimal embeddings is $\mathrm{Emb}_{op}(\pi^m\alpha, R_n) = \mathrm{Emb}(\pi^m\alpha, R_n) - \mathrm{Emb}(\pi^{m-1}\alpha, R_n)$ for $m \geq 1$. Also, when $n \geq 3$ for L ramified and $n \geq 2$ for L unramified, $\mathrm{Emb}(\pi^m\alpha, R_n) = \mathrm{Emb}(\pi^{m-1}\alpha, R_{n-1})$. Thus $\mathrm{Emb}_{op}(\pi^m\alpha, R_n)$ can be reduced to one of the followings;

$\mathrm{Emb}_{op}(\pi^\nu\alpha, R_0)$, $\mathrm{Emb}_{op}(\pi^{\nu'}\alpha, R_1)$ or $\mathrm{Emb}_{op}(\alpha, R_k)$ for some nonegative integers ν, ν', k.

In [5],[10], it is easy to see the number of R_m equivalence classes of $\mathrm{Emb}_{op}(\pi^\nu\alpha, R_m)$ is 1 for $m = 0, 1$ and the number of R_k equivalence classes of $\mathrm{Emb}_{op}(\alpha, R_k)$ is 2.

Then by Noether Skolem theorem, each of these can be expressed with the cosets of a certain conjuagte of an order, $\mathcal{O}+\mathcal{O}\alpha$. That is, we have the following theorem.

THEOREM 4.2. *Let the notations be same as 4.1. If L is unramified, then there exists $g \in B^\times$*

$$Emb_{op}(\pi^m\alpha, R_0) \approx R_0^\times/(\mathcal{O}+\mathcal{O}\pi^m g\alpha g^{-1})^\times$$

where $\pi^m g\alpha g^{-1} \in R_0 - R_2$, and $Emb_{op}(\alpha, R_0) \approx R_0^\times/\mathcal{O}_\alpha^\times$.

On the other hand if L is ramified,

$$Emb_{op}(\pi^m\alpha, R_1) \approx R_1^\times/(\mathcal{O}+\mathcal{O}\pi^m g_1\alpha g_1^{-1})^\times \cup R_1^\times/(\mathcal{O}+\mathcal{O}\pi^m g_2\alpha g_2^{-1})^\times$$

where the union is disjoint and $\pi^m g_i\alpha g_i^{-1} \in R_1 - R_3$ for each $i = 1, 2$, and

$$Emb_{op}(\alpha, R_1) \approx \begin{cases} \phi \text{ if } k(\alpha) \text{ is an unramified field extension of } k \\ R_1^\times/\mathcal{O}_\alpha^\times \text{ if } k(\alpha) \text{ is an ramified field extension of } k \\ R_1^\times/(g_1\mathcal{O}_\alpha^\times g_1^{-1}) \cup (g_2\mathcal{O}_\alpha^\times g_2^{-1}) \text{ if } k(\alpha) \simeq k \oplus k. \end{cases}$$

Proof. See lemma 5.17 in[7] □

Thus R_n equivalence classes of optimal embeddings are written as double cosets of R_n and a certain conjuagte of $\mathcal{O}+\mathcal{O}\alpha$. As same manner as in [5], we are able to identify these double cosets with the product of $R_{i+1}^\times \backslash R_i^\times$. By theorem 1.6, the number of R_n equivalence classes of optimal embeddings can be computed.

4.3 In [1], Brezinski has found the general formula of the equivalence classes of optimal embeddings with the global approaches of arithemetic theories of primitive orders. Before we copy Brezinski's theorem, let us explain the notations first. Let R be a complete discrete valuation ring with maximal ideal m and perfect residue field R/m. Let A be a quaternion algebra over the quotient field k of R. If an R order Λ is generated by $\{x_1, x_2, x_3, x_4\}$, then the discriminant $d(\Lambda)$ of Λ is the square root of the R-ideal $(\det[\mathrm{Tr}(x_i\bar{x}_j])$. If $d(\Lambda) = m^n$, let $n_\Lambda = n$.

An order Λ is a Bass order if and only if Λ is a primitive order (See proposition 1.11 in [2]). Hence $R_n(L)$ is a Bass order for a nonnegative integer n.

4.4 Let $J(\Lambda)$ be the Jacobson radical of Λ. The definition of $e(\Lambda)$ is as follows.

$$e(\Lambda) = \begin{cases} 1 & \text{if} \quad \Lambda/J(\Lambda) \simeq R/m \times R/m \\ 0 & \text{if} \quad \Lambda/J(\Lambda) \simeq R/m \\ -1 & \text{if} \quad \Lambda/J(\Lambda) \text{ is a quadratic extension of } R/m. \end{cases}$$

If $k \geq 1$, the Jacobson radical of $\mathcal{O}_L + \xi P_L^k$ is $P_L - \xi P_L^k$ and

$$(\mathcal{O}_L + \xi P_L^k)/J(\mathcal{O}_L + \xi P_L^k) \simeq \mathcal{O}_L/P_L,$$

hence

$$e(\mathcal{O}_L + \xi P_L^k) = \begin{cases} -1 & \text{if } L \text{ is unramified} \\ 0 & \text{if } L \text{ is ramified.} \end{cases}$$

Thus for $n \geq 2$, if L is ramified, then $e(R_n(L)) = 0$ and if L is unramified, $e(R_n(L)) = -1$.

4.5 Let L be a quadratic k algebra. Then L is one of the following types; $k \times k$, a unramified extension field of k, or a ramified extension field of k. If S_0 is the maximal order in L, then let $S_i = R + \pi^i S_0$. Thus $S_i = \mathcal{O} + \mathcal{O}\pi^i\alpha$ where $S_0 = \mathcal{O} + \mathcal{O}\alpha$. Then

$$[S_{i-1}^* : S_i^*] = \begin{cases} q & \text{if} \quad i \geq 2 \\ q-1 & \text{if} \quad i = 1 \text{ and } L \supset k \text{ is split} \\ q & \text{if} \quad i = 1 \text{ and } L \supset k \text{ is ramified} \\ q+1 & \text{if} \quad i = 1 \text{ and } L \supset k \text{ is unramified.} \end{cases}$$

where $q = |R/m|$. Finally, $M(\Lambda)$ is the overorder of Λ and $M^2(\Lambda) = M(M(\Lambda))$.

THEOREM 4.3. (Brezinski) *Let Λ be a Bass order with $e(\Lambda) = -1$ and let S_i be a quadratic R-order in L. If $n_\Lambda \geq 2$ and $i \geq 1$, then with the exceptions of $i = 1$ and $M(\Lambda)$ maximal in a split k- algebra or $i = 1$ and $L \supset k$ unramified:*

$$e(S_i, \Lambda) = \frac{[M(\Lambda)^* : \Lambda^*]}{[S_{i-1}^* : S_i^*]} e(S_{i-1}, M(\Lambda)), \tag{4-1}$$

where $[M(\Lambda)^* : \Lambda^*] = \begin{cases} q^2 - q & \text{if } M(\Lambda) \text{ is maximal in a split } A \\ q^2 & \text{otherwise.} \end{cases}$

In the exceptional cases:

$$(4\text{-}2) \qquad e(S_1, \Lambda) = \frac{1}{[S_0^* : S_1^*]}\{(M(\Lambda)^* : \Lambda^*)e(S_0, M(\Lambda)) - e(S_0, \Lambda)\}.$$

The initial values of $e(S_i, \Lambda)$ *are following.* $e(S_0, \Lambda) = 2$ *if* $L \supset K$ *is unramified, and* $e(S_0, \Lambda) = 0$ *in all other cases, while* $e(S_i, \Lambda)$ *for maximal orders* Λ *are given in (4-2) if* A *is split and* Λ *is maximal.*

4.6 With the above theorem, we tabulate the equivalence classes of optimal embeddings. $\mathrm{Emb}_{op}^*(\pi^m\alpha, R_\nu)$ means the number of $R_\nu^\times$ equivalence classes of optimal emebddings, $\mathrm{Emb}_{op}(\pi^m\alpha, R_{2n})$ for the notational convenience.

Suppose L is an unramified quadratic extension field of k. The n_Λ of $R_{2n}(L) = \mathcal{O}_L + \xi P_L^n$ is $2n$ and $e(R_{2n}(L)) = -1$. It now suffices to calculate the initial values of $\mathrm{Emb}_{op}^*(\pi^m\alpha, R_n)$ by (4-1).

$\mathrm{Emb}_{op}^*(\pi^m\alpha, R_{2n}) = e(S_m, R_{2n})$ depends on what $k + k\alpha$ is. Thus let $K = k + k\alpha$.

If K is the unramified quadratic extension field of k, i.e. $\mu(K, L) = \infty$ by theorem 3.6, then by 4.2 $\mathrm{Emb}_{op}^*(\alpha, R_{2n}) = 2$ for $n \geq 1$ and $\mathrm{Emb}_{op}^*(\alpha, R_0) = 1$. Also, by (4-2),

$$\begin{aligned} \mathrm{Emb}_{op}^*(\pi\alpha, R_{2n}) &= \frac{1}{q+1}\{[R_{2n-2}(L)^* : R_{2n}(L)^*]e(S_0, R_{2n-2}(L)) \\ &\quad - e(S_0, R_{2n}(L))\} \\ &= \begin{cases} \frac{1}{q+1}\{(q^2 - q)\cdot 1 - 2\}, & n = 1 \\ \frac{1}{q+1}\{2q^2 - 2\}, & n \geq 1 \end{cases} \end{aligned}$$

for $n \geq 2$.

If K is a ramified extension field of k, i.e. $\mu(K, L) = 0$ by theorem 3.6, then $\mathrm{Emb}_{op}^*(\alpha, R_{2n}) = 0$ for $n \geq 1$ and $\mathrm{Emb}_{op}^*(\alpha, R_0) = 1$ by 4.2. Also, for $m \geq 1$,

$$\begin{aligned} \mathrm{Emb}_{op}^*(\pi^m\alpha, R_2) &= \frac{1}{q}\{[R_0(L)^* : R_2(L)^*]e(S_0, R_0(L)) - e(S_0, R_2(L))\} \\ &= \frac{1}{q}\{(q^2 - q)\cdot 1 - 0\}. \end{aligned}$$

Suppose $K \simeq k \times k$. By theorem 3.6 $\mathrm{Emb}^*_{op}(\alpha, R_{2n}) = 0$ for $n \geq 1$ and $\mathrm{Emb}^*_{op}(\alpha, R_0) = 1$ by 4.2. Also, for $n \geq 1$

$$\begin{aligned} &\mathrm{Emb}^*_{op}(\pi\alpha, R_{2n}) \\ &= \frac{1}{q-1}\{[R_0(L)^* : R_2(L)^*]e(S_0, R_0(L)) - e(S_0, R_2(L))\} \\ &= \frac{1}{q-1}\{(q^2-q)\cdot 1 - 0\}. \end{aligned}$$

Hence, by (4-1), $\mathrm{Emb}^*_{op}(\pi^m\alpha, R_{2n})$ is recursively calculated and R^*_{2n} equivalence classes of $\mathrm{Emb}^*_{op}(\pi^m\alpha, R_{2n})$ are given as follows.

	K : unramified	K : ramified	$K \simeq k \times k$
$m > n$	$q^n - q^{n-1}$	$q^n - q^{n-1}$	$q^n - q^{n-1}$
$m = n > 0$	$q^n - 2q^{n-1}$	$q^n - q^{n-1}$	q^n
$m = n = 0$	1	1	1
$m < n$	$2q^n - 2q^{n-1}$	0	0

where $q = |\mathcal{O}/P|$ and $q^{-1} = 0$.

THEOREM 4.4. (Brezinski) *Let Λ be a Bass order with $e(\Lambda) = 0$ and let S_i be a quadratic R-order in L. If $n_\Lambda \geq 3$ and $i \geq 1$, then with the exceptions of $i = 1$ and $L \supset k$ ramified:*

$$e(S_i, \Lambda) = \frac{[M^2(\Lambda)^* : \Lambda^*]}{[S^*_{i-1} : S^*_i]} e(S_{i-1}, M^2(\Lambda)), \tag{4-3}$$

where

$$[M^2(\Lambda)^* : \Lambda^*] = \begin{cases} q^2 - q & \text{if } A \text{ is split and } M^2(\Lambda) \text{ is hereditary,} \\ q^2 + q & \text{if } A \text{ is ramified and } M^2(\Lambda) \text{ is hereditary,} \\ q^2 & \text{otherwise.} \end{cases}$$

In the exceptional cases:

$$e(S_1, \Lambda) = \frac{1}{q}\{(M^2(\Lambda)^* : \Lambda^*)e(S_0, M^2(\Lambda)) - e(S_0, \Lambda)\}. \tag{4-4}$$

The initial values of $e(S_i, \Lambda)$ *are given in the following way. If* $L \supset k$ *is ramified, then for* $n_\Lambda = 2$, $e(S_0, \Lambda) = q - 1$ *or* $e(S_0, \Lambda) = q + 1$ *depending whether* A *is split or ramified, and if* $n_\Lambda \geq 3$, $e(S_0, \Lambda) \neq 0$, *then*

$$e(S_0, \Lambda) = \begin{cases} q^{[n_\Lambda/2]} \text{ if } \omega_\Lambda = [n_\Lambda/2] \text{ or } \Omega_\Lambda \geq [(n_\Lambda + 1)/2], \\ 2q^{\Omega_\Lambda} \text{ otherwise} \end{cases}$$

If $L \supset k$ *is unramified or split, then* $e(S_0, \Lambda) = 0$ *for* $n_\Lambda \geq 2$. *If* $n_\Lambda = 2$, *then* $e(S_i, \Lambda) = 0$ *when* A *is ramified and* $e(S_i, \Lambda) = 2q - 2$ *when* A *is split with two exceptions:* $e(S_1, \Lambda) = 2$ *when* $L \supset k$ *is unramified and* A *is ramified, and* $e(S_i, \Lambda) = 2q$ *when* $L \supset k$ *and* A *are split.*

4.7 Here, we are restricted ourselves only when A is split over k and primitive orders, $R_n(L)$, of A containing the ring of integers of L which is a quadratic extension field of k. Then by lemma 2.4 and remark below, all maximal orders are hereditary. If L is a ramified extension field of k, $R_1(L)$ is also a hereditary order by lemma 1.5 [12].

Suppose L is a ramified quadratic extension field of k and K is a quadratic extension field of k. Then the n_Λ of $R_n(L) = \mathcal{O}_L + \xi P_L^{n-1}$ is n by 4.3.

Here $\mathrm{Emb}^*_{op}(\pi^m\alpha, R_\nu)$ means the number of $R_\nu^\times$ equivalence classes of optimal emebddings, $\mathrm{Emb}_{op}(\pi^m\alpha, R_{2n})$ for the notational convenience. Further, let $q = |\mathcal{O}/P|$ and $q^{-1} = 0$.

Case i) $K = k + k\alpha$ is the unramified quadratic extension field.

That is, $\mu(K, L) = 0$. $\mathrm{Emb}^*_{op}(\alpha, R_\nu) = 0$ for $\nu \geq 1$ and $\mathrm{Emb}^*_{op}(\alpha, R_0) = 1$ by 4.2. On the other hand, $\mathrm{Emb}^*_{op}(\pi^m\alpha, R_1) = 2$ and $\mathrm{Emb}^*_{op}(\pi^m\alpha, R_2) = 2q - 2$ for $m \geq 1$.

		$\mathrm{Emb}^*_{op}(\pi^m\alpha, R_{2n})$	$\mathrm{Emb}^*_{op}(\pi^m\alpha, R_{2n+1})$
$m \geq n+1$	$n > 0$	$2q^n - 2q^{n-1}$	$2q^n - 2q^{n-1}$
$m = n$	$n > 0$	$2q^n - 2q^{n-1}$	0
$m \geq 1$	$n = 0$	1	2
$m = 0$	$n = 0$	1	0
$m = 0$	$n = 1$	0	0
$m \geq 0$	$n \geq m+1$	0	0

Case ii) $K = k + k\alpha$ is a ramified quadratic extension field and K is not isomorphic to L. i.e. $\mu(K, L) = 2$. $\mathrm{Emb}^*_{op}(\alpha, R_\nu) = 0$ for $\nu \geq 3$ and $\mathrm{Emb}^*_{op}(\alpha, R_0) = 1$ by 4.2. $\mathrm{Emb}^*_{op}(\alpha, R_2) = q - 1$, $\mathrm{Emb}^*_{op}(\alpha, R_1) = 1$ by 4.2, $\mathrm{Emb}^*_{op}(\pi^m\alpha, R_1) = 2$ and from the theorem 4.4, $\mathrm{Emb}^*_{op}(\pi^m\alpha, R_1) = 2q - 2$ for $m \geq 1$.

		$\mathrm{Emb}^*_{op}(\pi^m\alpha, R_{2n})$	$\mathrm{Emb}^*_{op}(\pi^m\alpha, R_{2n+1})$
$m \geq n-1$	$n > 0$	$2q^n - 2q^{n-1}$	$2q^n - 2q^{n-1}$
$m = n$	$n > 0$	$2q^n - 2q^{n-1}$	$q^n - q^{n-1}$
$m \geq 1$	$n = 0$	1	2
$m = 0$	$n = 0$	1	1
$m = 0$	$n = 1$	$q - 1$	0
$m = 0$	$n > 1$	0	0
$m > 1$	$n = m + 1$	$q^n - q^{n-1}$	0
$m > 0$	$n > m + 1$	0	0

Case iii) $K = k + k\alpha$ is a ramified quadratic extension field and K is isomorphic to L. i.e., $\mu(K, L) = \infty$.

By 4.2, $\mathrm{Emb}^*_{op}(\alpha, R_0) = 1$ and $\mathrm{Emb}^*_{op}(\alpha, R_1) = 1$. From the theorem 4.4, $\mathrm{Emb}^*_{op}(\alpha, R_2) = q - 1$. For $\nu \geq 3$, by theorem 3.6, $\mathrm{Emb}^*_{op}(\alpha, R_\nu) \neq 0$. Since $\omega_{R_\nu} = 0$ and $\Omega_{R_\nu} = 1$, $\mathrm{Emb}^*_{op}(\alpha, R_\nu) = 2q$.

$\mathrm{Emb}^*_{op}(\pi^m\alpha, R_1) = 2$ and $\mathrm{Emb}^*_{op}(\pi^m\alpha, R_1) = 2q - 2$ for $m \geq 1$.

$$\begin{aligned}\mathrm{Emb}^*_{op}(\pi\alpha, R_3) =& \frac{1}{q}\{[R_1^* : R_3^*]e(S_0, R_1) - e(S_0, R_3)\\ =& \frac{1}{q}(q^2 - q) \cdot 1 - 2q)\\ =& q - 3\end{aligned}$$

and

$$\begin{aligned}\mathrm{Emb}^*_{op}(\pi\alpha, R_4) =& \frac{1}{q}\{[R_2^* : R_4^*]e(S_0, R_2) - e(S_0, R_4)\\ =& \frac{1}{q}\{q^2(q - 1) - 2q\}\\ =& q^2 - q - 2.\end{aligned}$$

Hence by (4-3), we obtain

		$\mathrm{Emb}^*_{op}(\pi^m\alpha, R_{2n})$	$\mathrm{Emb}^*_{op}(\pi^m\alpha, R_{2n+1})$
$m \geq n+1$	$n > 0$	$2q^n - 2q^{n-1}$	$2q^n - 2q^{n-1}$
$m = n$	$n > 0$	$2q^n - 2q^{n-1}$	$q^n - 3q^{n-1}$
$m \geq 1$	$n = 0$	1	2
$m = 0$	$n = 0$	1	1
$m = 0$	$n = 1$	$q - 1$	$2q$
$m = 0$	$n > 1$	$2q$	$2q$
$m > 1$	$n = m+1$	$q^n - q^{n-1} - 2q^{n-2}$	$2q^n - 2q^{n-1}$
$m > 0$	$n > m+1$	$2q^{m+1} - 2q^{m-1}$	$2q^{m+1} - 2q^{m-1}$

Case iv) Suppose $K \simeq k \times k$. i.e.$\mu(K, L) = 1$

$\mathrm{Emb}^*_{op}(\alpha, R_\nu) = 0$ for $\nu \geq 2$ and $\mathrm{Emb}^*_{op}(\alpha, R_0) = 1$ by 4.2. On the other hand, $\mathrm{Emb}^*_{op}(\pi\alpha, R_2) = 2q$, $\mathrm{Emb}^*_{op}(\pi^m\alpha, R_4) = 2q - 2$ and $\mathrm{Emb}^*_{op}(\pi^m\alpha, R_3) = 2q - 2$ for $m \geq 1$ by the theorem 4.4.

By (4-3), we have

	$\mathrm{Emb}^*_{op}(\pi^m\alpha, R_{2n})$	$\mathrm{Emb}^*_{op}(\pi^m\alpha, R_{2n+1})$
$m \geq n = 0$	1	2
$m > n > 0$	$2q^n - 2q^{n-1}$	$2q^n - 2q^{n-1}$
$m = n > 0$	$2q^n$	$2q^n - 2q^{n-1}$
$m < n$	0	0

References

[1] J. Brezinski, *On automorphisms of Quaternion orders*, J. Reine Angew Math. **43** (1992), 102-109.

[2] M. Eichler, *Über die Darstellbarkeit von Modulformen durch Thetareihen*, J. Reine Angew. Math. **195** (1955), 156-171.

[3] M. Eichler, *The basis problem for modular forms and the traces of Hecke operators*, Lecture Notes in Math **320**, Springer-Verlag, 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] H. Hijikata, A. Pizer and T. Shemanske, *The basis problem for modular forms on* $\Gamma_0(N)$, Memoirs of AMS **82** (1982).

[7] S. Jun, *Thesis*, University of Rochester, 1991.

[8] S. Jun, *On the representatives of modular forms by theta series*, preprint.

[9] T. Lam, *The algebraic theory of quadratic forms*, W. A. Benjamin, 1980.
[10] A. Pizer, *On the arithmetic of Quaternion algebras II*, J. Math. Soc. Japan **28** (1976), 676-698.
[11] A. Pizer, *An Algorithm for computing modular forms on* $\Gamma_0(N)$, J. Algebra (1980), 340-390.
[12] I. Reiner, *Maximal Orders*, Academic Press, 1975.
[13] A. Weil, *Basic Number Theory*, Springer Verlag, 1984.
[14] E. Weiss, *Algebraic Number Theory*, McGraw Hill New York.

Department of Applied Mathematics
Kunkuk University
Choongju 380-701, Korea