J. Math. Soc. Japan
Vol. 28, No. 4, 1976

# On the arithmetic of quaternion algebras II

By Arnold PIZER*

(Received Sept. 30, 1975)

## § 1. Introduction.

The purpose of this paper is to develop an aspect of the arithmetic of quaternion algebras that will allow us to generalize (see [9]) results of Eichler ([2], [3] and [4]) and Hijikata-Saito ([6]) on the representability of modular forms by theta series. Specifically we define a certain type of order in rational quaternion algebras, construct corresponding "Brandt" Matrices, obtain some properties of these matrices, and finally obtain a trace formula for them (Theorem 26). In [9], we give a relation which holds between the trace of the Brandt Matrix and the traces of Hecke Operators from which we obtain results on the representability of modular forms by theta series in the case of $\Gamma_0(N)$, $N$ not a perfect square. This paper is independent of [8].

## § 2. Orders.

Let $\mathfrak{A}_p$ denote the unique (up to isomorphism) quaternion division algebra over $Q_p$. Let $L$ denote the unique unramified quadratic extension field of $Q_p$. Then $\mathfrak{A}_p$ can be represented as the subalgebra of the $2\times 2$ matrix algebra over $L$ given by

$$\mathfrak{A}_p=\left\{\begin{pmatrix}\alpha & \beta\\ p\bar{\beta} & \bar{\alpha}\end{pmatrix}\middle|\ \alpha,\ \beta\in L\right\}$$

where $-$ denotes conjugation of $L/Q_p$. The canonical trace (tr) and norm ($N$) of $\mathfrak{A}_p$ are respectively the trace and determinant in the matrix representation. In order to make the typography simpler, we will often denote the matrix $\begin{pmatrix}\alpha & \beta\\ p\bar{\beta} & \bar{\alpha}\end{pmatrix}\in\mathfrak{A}_p$ by $[\alpha, \beta]$. For any ring $S$ we denote by $U(S)$ the unit group of $S$. For a non-negative integer $r$ let $\mathfrak{O}_{2r+1}^{(p)}=\{[\alpha, p^r\beta]\in\mathfrak{A}_p \mid \alpha,\ \beta\in R_p\}$ where $R_p$ denotes the integers of $L$. Then $\mathfrak{O}_{2r+1}^{(p)}$ is an order of $\mathfrak{A}_p$. It is easy to see (either directly or by calculating the discriminants) that $\mathfrak{O}_1^{(p)}$ is the maximal order of $\mathfrak{A}_p$.

* Partially supported by NSF Grant MPS 74-08108 A01.

DEFINITION 1. An order $\mathfrak{O}$ of $\mathfrak{A}_p$ is said to have *level* $p^{2r+1}$ for $r=0, 1, 2, 3, \cdots$ if $\mathfrak{O}$ is isomorphic (over $Z_p$) to $\mathfrak{O}_{2r+1}^{(p)}$.

$\mathfrak{A}_p \otimes_{Q_p} L$ is isomorphic to $M(2, L)$ and we can extend the conjugation of $L/Q_p$ to $\mathfrak{A}_p \otimes L$ by letting $^{-}$ operate on $L$. Explicitly $\overline{\begin{pmatrix} x & y \\ z & w \end{pmatrix}} = \begin{pmatrix} \bar{w} & \bar{z}p^{-1} \\ p\bar{y} & \bar{x} \end{pmatrix}$. An element $G \in \mathfrak{A}_p \otimes L$ is actually in $\mathfrak{A}_p$ $(=\mathfrak{A}_p \otimes 1)$ if and only if $\bar{G}=G$. $\mathfrak{O}_{2r+1}^{(p)} \otimes_{Z_p} R = \begin{pmatrix} R & p^r R \\ p^{r+1}R & R \end{pmatrix}$ is the type of order studied by Hijikata in [5]. There is a close analogy between orders of level $p^{2r+1}$ in $\mathfrak{A}_p$ and those isomorphic to $\mathfrak{O}_{2r+1}^{(p)} \otimes R$ in $\mathfrak{A}_p \otimes L$. This is illustrated by the following two results.

PROPOSITION 2. *An order $\mathfrak{O}$ in $\mathfrak{A}_p$ has level $p^{2r+1}$ for some $r$ if and only if $\mathfrak{O}$ contains a subring isomorphic to $R_p$.*

PROOF. One direction is immediate. For the other, we can assume (by conjugating if necessary) that $\mathfrak{O}$ contains $R_p = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \bar{\alpha} \end{pmatrix} \middle| \alpha \in R_p \right\}$. Let $A=[\alpha, \beta] \in \mathfrak{O}$. By adding an element of $R_p$ to $A$, if necessary, we can assume $\mathrm{Tr}(A)=0$. Since $N(A) \in Z_p$, we see that $\alpha$ and $\beta$ are both in $R_p$. Letting $r=\min\{v_p(y) \mid [x, y] \in \mathfrak{O}\}$, we have $\mathfrak{O}=\mathfrak{O}_{2r+1}^{(p)}$.

PROPOSITION 3. *$[N(\mathfrak{O}_{2r+1}^{(p)}) : U(\mathfrak{O}_{2r+1}^{(p)})Q_p^x]=2$ and $[1, 0]$ and $[0, p^r]$ are the coset representatives of $U(\mathfrak{O}_{2r+1}^{(p)})Q_p^x$ in $N(\mathfrak{O}_{2r+1}^{(p)})$ where $N(\mathfrak{O}_{2r+1}^{(p)})=\{A \in \mathfrak{A}_p^x \mid A\mathfrak{O}_{2r+1}^{(p)}A^{-1}=\mathfrak{O}_{2r+1}^{(p)}\}$.*

PROOF. It is easy to see that $[0, p^r]\mathfrak{O}_{2r+1}[0, p^r]^{-1}=\mathfrak{O}_{2r+1}$ and thus $U(\mathfrak{O}_{2r+1})Q_p^x[0, p^r] \subseteq N(\mathfrak{O}_{2r+1})$. Conversely, let $A \in N(\mathfrak{O}_{2r+1})$. Then $A$ normalizes $\mathfrak{O}_{2r+1} \otimes R$ and hence by 2.2 of [5] we have either $A \in U\begin{pmatrix} R & p^r R \\ p^{r+1}R & R \end{pmatrix} L^x$ or $A \in U\begin{pmatrix} R & p^r R \\ p^{r+1}R & R \end{pmatrix} L^x \begin{pmatrix} 0 & p^r \\ p^{r+1} & 0 \end{pmatrix}$. In the former case let $B=A$ and in the latter let $B=A[0, p^r]^{-1}$. Thus $B \in U\begin{pmatrix} R & p^r R \\ p^{r+1}R & R \end{pmatrix} p^s$ for some $s \in Z$. But $\bar{B}=B$ implies $B \in U(\mathfrak{O}_{2r+1})p^s$ and hence $A \in U(\mathfrak{O}_{2r+1})Q_p^x$ or $A \in U(\mathfrak{O}_{2r+1})Q_p^x[0, p^r]$.

## § 3. Optimal embeddings.

The major tool we will need in obtaining a trace formula for Brandt Matrices is the optimal embedding theory for $\mathfrak{O}_{2r+1}=\mathfrak{O}_{2r+1}^{(p)}$. For $r=0$, this is well known (and trivial) (see [4], p. 97). The analogous theory (which we will implicitly use) in the case of a split quaternion algebra over $Q_p$ was developed by Eichler ([1], [4]) and in the general case by Hijikata ([5] § 2, see also [8] § 3). Let $K$ be a semi-simple algebra of dimension 2 over $Q_p$ [i. e. $K$ is a quadratic field extension of $Q_p$ or $K \cong Q_p \oplus Q_p$] and let $\mathfrak{o}$ be an order of $K$ (with $\mathfrak{o} \otimes_{Z_p} Q_p = K$).

DEFINITION 4. An embedding (injective $Q_p$ homomorphism) $\varphi : K \to \mathfrak{A}_p$ is called an *optimal embedding* of $\mathfrak{o}$ into $\mathfrak{O}_{2r+1}$ if $\varphi(K) \cap \mathfrak{O}_{2r+1} = \varphi(\mathfrak{o})$. Two such optimal embeddings $\varphi_1$ and $\varphi_2$ are *equivalent* mod $U(\mathfrak{O}_{2r+1})$ if there exists $A\in U(\mathfrak{O}_{2r+1})$ so that $\varphi_1(\alpha)=A^{-1}\varphi_2(\alpha)A$ for all $\alpha\in K$.

Let us fix some notation. If $p=2$, let $v=\dfrac{1+\sqrt{5}}{2}$ and $u=5$. If $p\neq 2$, let $v=\sqrt{u}$ where $u$ is an integer which is a quadratic non-residue mod $p$. Then $L=Q_p(v)$ and $R_p=R=Z_p+Z_pv$ is the set of integers of $L$. We will keep this notation for the remainder of this paper.

PROPOSITION 5. *Let $K=Q_p(g)$ with $Z_p+Z_pg$ an order of $K$. Then $\varphi$ is an optimal embedding of $Z_p+Z_pg$ into $\mathfrak{O}_{2r+1}$ if and only if $\varphi(g)=[\alpha, p^r\beta]$ with $\alpha, \beta\in R$ and where either $\beta\in U(R)$ or $\alpha=a+bv$ with $b\in U(Z_p)$.*

PROOF. $Z_p+Z_pg$ is optimally embedded in $\mathfrak{O}_{2r+1}$ if and only if $Z_p+Z_p\varphi(g)=\mathfrak{O}_{2r+1}\cap(Q_p+Q_p\varphi(g))$ and from this the proposition follows easily.

Let $K$, $\mathfrak{o}$ be as in Definition 4. We denote by $\Delta(\mathfrak{o})$ the discriminant of $\mathfrak{o}$. $\Delta(\mathfrak{o})$ is defined mod $U(Z_p)^2$ and we will write $\Delta(\mathfrak{o})=d$ to mean $\Delta(\mathfrak{o})=dU(Z_p)^2$. If $K=Q_p(g)$ and $\mathfrak{o}=Z_p+Z_pg$, then $\Delta(\mathfrak{o})=\mathrm{tr}\,(g)^2-4N(g)$.

PROPOSITION 6. *Let $G=[\alpha, p^r\beta]\in\mathfrak{O}_{2r+1}$ with $\alpha=a+bv$. Assume $\varphi$=identity gives an optimal embedding of $\mathfrak{o}=Z_p+Z_pG$ into $\mathfrak{O}_{2r+1}$. Then*

i) *If $b$ is a unit, then $\Delta(\mathfrak{o})=u$*

ii) *If $b$ is not a unit, then*

a) *If $0<r_p(b)=s\leqq r$, then $\Delta(\mathfrak{o})=p^{2s}u$*

b) *If $p\neq 2$ and $v_p(b)>r$, then $\Delta(\mathfrak{o})=p^{2r+1}$ or $p^{2r+1}u$*

*If $p=2$ and $v_p(b)=r+1$, then $\Delta(\mathfrak{o})=2^{2r+2}3$ or $2^{2r+2}7$*

*If $p=2$ and $v_p(b)>r+1$, then $\Delta(\mathfrak{o})=2^{2r+3}u'$ where $u'=1, 3, 5$, or $7$.*

PROOF. This follows by a direct verification using Proposition 5.

Our main task in the next two sections will be to count the number of inequivalent mod $U(\mathfrak{O}_{2r+1})$ optimal embeddings of an order $\mathfrak{o}$ into $\mathfrak{O}_{2r+1}$. For this we will need the following two lemmas.

LEMMA 7. *$[U(\mathfrak{O}_1):U(\mathfrak{O}_{2r+1})]=p^{2r}$ and further a set of representatives of $U(\mathfrak{O}_1)$ mod $U(\mathfrak{O}_{2r+1})$ is given by $[1, \gamma]$ where $\gamma$ ranges over $R$ (mod $p^r$). In fact if $[\alpha, \beta]\in U(\mathfrak{O}_1)$, then $[\alpha, \beta]=[w, p^r\delta][1, \gamma]$ where $\gamma\equiv\beta/\alpha$ (mod $p^r$) for some $w$, $\delta\in R$.*

PROOF. It suffices to prove the last statement and this is easy.

LEMMA 8. *Let $G, H\in\mathfrak{O}_{2r+1}$. Then $G$ and $H$ are conjugate by an element of $U(\mathfrak{O}_{2r+1})$ if and only if $G(=G\otimes 1)$ and $H$ are conjugate in $\mathfrak{O}_{2r+1}\otimes R$ by an element of $U(\mathfrak{O}_{2r+1}\otimes R)$.*

PROOF. Let us fix $r$ and write $\mathfrak{O}=\mathfrak{O}_{2r+1}$. Assume $AGA^{-1}=H$ for some $A\in U(\mathfrak{O}\otimes R)$. If we can find a $Y\in U(\mathfrak{O}\otimes R)$ commuting with $G$ such that $AY\in U(\mathfrak{O})$ we will be done. But $AY\in U(\mathfrak{O})$ if and only if $AY\in U(\mathfrak{O}\otimes R)$ and $AY=\overline{AY}=\bar{A}\bar{Y}$, i.e. $\bar{A}^{-1}A=\bar{Y}Y^{-1}$. Letting $B=\bar{A}^{-1}A$, we have

i) $B\in U(\mathfrak{O}\otimes R)$

ii) $B\bar{B}=1$

and

iii) $B$ commutes with $G$.

We claim there exists $z\in L$ such that $z+\bar{z}B=X\in U(\mathfrak{O}\otimes R)$ and $X$ commutes with $G$. Note first that $z\in L$ implies that $X$ commutes with $G$. Let $B=\begin{pmatrix} a & bp^r \\ cp^{r+1} & d\end{pmatrix}$, $a, b, c, d\in R$. Then $B\in U(\mathfrak{O}\otimes R)$ implies $a, d\in U(R)$ and $B\bar{B}=1$ implies $a\bar{d}\equiv\bar{a}d\equiv 1 \pmod p$. Thus $a\equiv -1 \pmod p \Leftrightarrow d\equiv -1 \pmod p$. If $a\not\equiv -1 \pmod p$, then $z=1$ works and if $a\equiv -1 \pmod p$, then $z=v$ works. Now $\bar{X}B=X\Rightarrow B=\bar{X}^{-1}X$. Letting $Y=X^{-1}$, we have $\bar{A}^{-1}A=\bar{Y}Y^{-1}$ where $Y$ commutes with $G$ and $AY\in U(\mathfrak{O}\otimes R)$. This completes the proof.

## § 4. The case $p\neq 2$.

Assume in this section that $p\neq 2$. Further we assume $K/Q_p$ and $\mathfrak{o}$ are as in Definition 4 and we write $\mathfrak{O}_{2r+1}$ for $\mathfrak{O}_{2r+1}^{(p)}$.

LEMMA 9. *$[v, 0]$ and $[\bar{v}, 0]$ are not conjugate by any element of $U(\mathfrak{O}_1)$.*

PROOF. This is immediate.

PROPOSITION 10. *If $\Delta(\mathfrak{o})=u$, then $\mathfrak{o}$ has exactly 2 inequivalent* mod $U(\mathfrak{O}_{2r+1})$ *optimal embeddings into $\mathfrak{O}_{2r+1}$.*

PROOF. We can assume $\mathfrak{o}=Z_p+Z_pv$. By Proposition 5 and Lemma 9 $\varphi_1(v)=[v, 0]$ and $\varphi_2(v)=[\bar{v}, 0]$ give non-equivalent optimal embeddings. Suppose $\varphi$ is an optimal embedding. Then $\varphi(v)=[bv, p^ry]=G$ (say) with $b\in U(Z_p)$ and $y\in R$. Then $-u=N(v)=N(G)=-b^2u-p^{2r+1}y\bar{y}$ implies $b\equiv\pm 1$ $(p)$. Suppose $b\equiv 1(p)$ $(\Rightarrow b\equiv 1(p^{2r+1}))$. $G$ and $[v, 0]$ are conjugate by an element of $\mathfrak{A}^x$. Since $\mathfrak{A}^x=U(\mathfrak{O}_1)Q_p^x\cup U(\mathfrak{O}_1)\begin{pmatrix} 0 & 1 \\ p & 0\end{pmatrix}Q_p^x$, we must have $[w, x][v, 0][w, x]^{-1}=[bv, p^ry]$ for some $[w, x]\in U(\mathfrak{O}_1)$. This gives $b=\dfrac{w\bar{w}+px\bar{x}}{w\bar{w}-px\bar{x}}$, hence $b-1\equiv O(p^{2r+1})\Rightarrow x\equiv O(p^r)$ $\Rightarrow [w, x]\in U(\mathfrak{O}_{2r+1})$. Thus $\varphi$ is equivalent to $\varphi_1$. The case $b\equiv -1(p)$ gives $\varphi$ equivalent to $\varphi_2$.

PROPOSITION 11. *If $\Delta(\mathfrak{o})=p^{2s}u$ with $1\leqq s\leqq r$, then $\mathfrak{o}$ has exactly $2p^s-2p^{s-1}$ inequivalent* mod $U(\mathfrak{O}_{2r+1})$ *optimal embeddings into $\mathfrak{O}_{2r+1}$.*

PROOF. We can assume $\mathfrak{o}=Z_p+Z_pp^sv$. Let $\varphi$ be an optimal embedding. Then $\varphi(p^sv)=G$ (say) is conjugate to either $[p^sv, 0]$ or $[p^s\bar{v}, 0]$ by an element of $U(\mathfrak{O}_1)$ (see proof of Proposition 10). Suppose $G$ is conjugate by $U(\mathfrak{O}_1)$ to $[p^sv, 0]$ (the other case is similar). Then by Lemma 7 $G$ is conjugate by $U(\mathfrak{O}_{2r+1})$ to some

$$[1, \gamma][p^sv, 0][1, \gamma]^{-1}=\left[\frac{p^sv+p^{s+1}\gamma\bar{\gamma}v}{1-p\gamma\bar{\gamma}}, \frac{2\gamma p^s\bar{v}}{1-p\gamma\bar{\gamma}}\right]=A \text{ (say)}$$

where $\gamma\in R \pmod{p^s}$. But $G$ conjugate to $A$ by $U(\mathfrak{O}_{2r+1})$ implies $Z_p+Z_pA$ is optimally embedded in $\mathfrak{O}_{2r+1}$ which is true if and only if (by Proposition 5)

$\dfrac{2\gamma p^s \bar{v}}{1-p\gamma\bar{\gamma}}=p^r\beta'$ for some $\beta'\in U(R)$ if and only if $\gamma=p^{r-s}\beta$ for some $\beta\in U(R)$. As $\gamma\in R \pmod{p^r}$, we have $\gamma=p^{r-s}\beta$ where $\beta\in R \pmod{p^s}$, $\beta\in U(R)$. Thus $G$ is conjugate by $U(\mathfrak{O}_{2r+1})$ to some

$$\left[\frac{p^s v+p^{2r-s+1}\beta\bar{\beta}v}{1-p^{2r-2s+1}\beta\bar{\beta}},\ \frac{2p^r\beta\bar{v}}{1-p^{2r-2s+1}\beta\bar{\beta}}\right]=\tilde{\beta}\quad\text{(say)}\tag{1}$$

with $\beta\in R \pmod{p^s}$, $\beta\in U(R)$. Let $\tilde{\beta}_1$ be defined as in (1) by replacing $\beta$ by $\beta_1$ with $\beta_1\in R \pmod{p^s}$, $\beta_1\in U(R)$. We claim

(2) $\tilde{\beta}$ is conjugate to $\tilde{\beta}_1$ by $U(\mathfrak{O}_{2r+1})$ if and only if $\beta\bar{\beta}=\beta_1\bar{\beta}_1(p^s)$.

By Lemma 8, $\tilde{\beta}$ is conjugate to $\tilde{\beta}_1$ by $U(\mathfrak{O}_{2r+1})$ if and only if $\tilde{\beta}$ is conjugate to $\tilde{\beta}_1$ by $U(\mathfrak{O}_{2r+1}\otimes R)$ which is true if and only if $\begin{pmatrix}1&0\\0&p^r\end{pmatrix}\tilde{\beta}\begin{pmatrix}1&0\\0&p^{-r}\end{pmatrix}$ is conjugate to $\begin{pmatrix}1&0\\0&p^r\end{pmatrix}\tilde{\beta}_1\begin{pmatrix}1&0\\0&p^{-r}\end{pmatrix}$ by $\begin{pmatrix}1&0\\0&p^r\end{pmatrix}U(\mathfrak{O}_{2r+1}\otimes R)\begin{pmatrix}1&0\\0&p^{-r}\end{pmatrix}=U\begin{pmatrix}Z_p&Z_p\\p^{2r+1}Z_p&Z_p\end{pmatrix}$. Our claim is now reduced to showing

$$\frac{1}{1-p^{2r-2s+1}\ \beta\bar{\beta}}\begin{pmatrix}p^s v+p^{2r-s+1}\beta\bar{\beta} & 2\beta\bar{v}\\ 2p^{2r+1}\bar{\beta}v & p^s\bar{v}+p^{2r-s+1}\beta\bar{\beta}\end{pmatrix}=B\quad\text{(say)}$$

is conjugate by $U\begin{pmatrix}Z_p&Z_p\\p^{2r+1}Z_p&Z_p\end{pmatrix}$ to

$$\frac{1}{1-p^{2r-2s+1}\beta_1\bar{\beta}_1}\begin{pmatrix}p^s v+p^{2r-s+1}\beta_1\bar{\beta}_1 & 2\beta_1\bar{v}\\ 2p^{2r+1}\bar{\beta}_1 v & p^s\bar{v}+p^{2r-s+1}\beta_1\bar{\beta}_1\end{pmatrix}=B_1\quad\text{(say)}$$

if and only if $\beta\bar{\beta}=\beta_1\bar{\beta}_1 \pmod{p^s}$. As elements of $\begin{pmatrix}Z_p&Z_p\\p^{2r+1}Z_p&Z_p\end{pmatrix}$ are upper triangular mod $p^{2r+1}$, $B$ conjugate to $B_1$ by $U\begin{pmatrix}Z_p&Z_p\\p^{2r+1}Z_p&Z_p\end{pmatrix}$ implies

$$\frac{p^s v+p^{2r-s+1}\beta\bar{\beta}}{1-p^{2r-2s+1}\beta\bar{\beta}}\equiv\frac{p^s v+p^{2r-s+1}\beta_1\bar{\beta}_1}{1-p^{2r-2s+1}\beta_1\bar{\beta}_1}\qquad\pmod{p^{2r+1}}.\tag{3}$$

But one easily sees that (3) is equivalent to $\beta\bar{\beta}\equiv\beta_1\bar{\beta}_1 \pmod{p^s}$. For the converse, we have that $\beta\bar{\beta}\equiv\beta_1\bar{\beta}_1 \pmod{p^s}$ implies (3) holds. Let

$$\delta=\frac{2\beta\bar{v}}{1-p^{2r-2s+1}\beta\bar{\beta}},\qquad \delta_1=\frac{2\beta_1\bar{v}}{1-p^{2r-2s+1}\beta_1\bar{\beta}_1},$$

and

$$t=\frac{p^s v+p^{2r-s+1}\beta\bar{\beta}}{1-p^{2r-2s+1}\beta\bar{\beta}}-\frac{p^s v+p^{2r-s+1}\beta_1\bar{\beta}_1}{1-p^{2r-2s+1}\beta_1\bar{\beta}_1}\in p^{2r+1}R.$$

Then $C=\begin{pmatrix}1&0\\t\delta_1^{-1}&\delta\delta_1^{-1}\end{pmatrix}\in U\begin{pmatrix}Z_p&Z_p\\p^{2r+1}Z_p&Z_p\end{pmatrix}$ and direct verification (using the fact that $CBC^{-1}$ and $B_1$ have the same norm and trace) shows $CBC^{-1}=B_1$. This proves our claim (2). The last part of the proof of our claim is essentially Hijikata's proof of Lemma 2.5 part (ii) in [5]. As $\beta$ ranges over all units in $R \pmod{p^s}$, $\beta\bar{\beta}$ ranges over all units in $Z_p \pmod{p^s}$ and the number of such units is $p^s - p^{s-1}$. Thus (2) shows that there are exactly $p^s - p^{s-1}$ inequivalent $\operatorname{mod} U(\mathfrak{O}_{2r+1})$ optimal embeddings $\varphi$ of $\mathfrak{o}$ into $\mathfrak{O}_{2r+1}$ with $\varphi(p^s v)$ conjugate by $U(\mathfrak{O}_1)$ to $[p^s v, 0]$. Similarly, there are exactly $p^s - p^{s-1}$ inequivalent optimal embeddings with $\varphi(p^s v)$ conjugate by $U(\mathfrak{O}_1)$ to $[p^s \bar{v}, 0]$. This completes the proof of Proposition 11.

PROPOSITION 12. *If* $\Delta(\mathfrak{o}) = p^{2r+1}u'$ *where* $u'=1$ *or* $u$, *then* $\mathfrak{o}$ *has exactly* $p^r$ *inequivalent* $\operatorname{mod} U(\mathfrak{O}_{2r+1})$ *optimal embeddings into* $\mathfrak{O}_{2r+1}$.

PROOF. Define and fix an element $w \in L$ by letting $w=1$ if $u'=1$ and $N(w) = u$ if $u'=u$. We can assume $\mathfrak{o} = Z_p + Z_p p^r \sqrt{pu'}$. Let $\varphi$ be an optimal embedding. Then $\varphi(p^r\sqrt{pu'}) = G$ (say) is conjugate to $[0, p^r w]$ by an element of $U(\mathfrak{O}_1)$ (since $[0, w]$ centralizes $[0, p^r w]$). Thus by Lemma 7, $G$ is conjugate by $U(\mathfrak{O}_{2r+1})$ to some

$$(4) \qquad [1, \gamma][0, p^r w][1, \gamma]^{-1} = \left[\frac{p^{r+1}(\gamma\bar{w} - \bar{\gamma}w)}{1 - p\gamma\bar{\gamma}}, \frac{p^r(w - p\gamma^2\bar{w})}{1 - p\gamma\bar{\gamma}}\right] = \hat{\gamma} \quad \text{(say)}$$

where $\gamma \in R \pmod{p^r}$. To complete the proof of Proposition 12, we need only

LEMMA 13. *Let* $S = \{awv \mid a \in Z_p \pmod{p^r}\}$.

i) *Let* $\alpha, \beta \in S$ *and define* $\hat{\alpha}, \hat{\beta}$ *as in* (4). *Then* $\hat{\alpha}$ *is conjugate to* $\hat{\beta}$ *by* $U(\mathfrak{O}_{2r+1}) \Leftrightarrow \alpha = \beta$.

ii) *Let* $G$ *be as in Proposition* 12. *Then* $G$ *is conjugate to some* $\hat{\alpha}$, $\alpha \in S$.

PROOF. i) $\hat{\alpha}$ is conjugate to $\hat{\beta}$ by $U(\mathfrak{O}_{2r+1}) \Leftrightarrow \hat{\alpha}$ is conjugate to $\hat{\beta}$ by $U(\mathfrak{O}_{2r+1} \otimes R)$. This is equivalent (see proof of (2) in the proof of Proposition 11) to $\dfrac{p^{r+1}(\alpha\bar{w} - \bar{\alpha}w)}{1 - p\alpha\bar{\alpha}} \equiv \dfrac{p^{r+1}(\beta\bar{w} - \bar{\beta}w)}{1 - p\beta\bar{\beta}} \pmod{p^{2r+1}}$. Letting $\alpha = awv$, $\beta = bwv$, this gives $a \equiv b \pmod{p^r}$ which implies $a = b$, hence $\alpha = \beta$.

ii) We need only show that each $\hat{\gamma}$, $\gamma \in R \operatorname{mod} p^r$ is conjugated by $U(\mathfrak{O}_{2r+1})$ to some $\hat{\alpha}$, $\alpha \in S$. As mentioned above, this is equivalent to finding $\alpha \in S$ such that

$$(5) \qquad \frac{p^{r+1}(\alpha\bar{w} - \bar{\alpha}w)}{1 - p\alpha\bar{\alpha}} \equiv \frac{p^{r+1}(\gamma\bar{w} - \bar{\gamma}w)}{1 - p\gamma\bar{\gamma}} \qquad \pmod{p^{2r+1}}.$$

Letting $\gamma = (c + dv)w$ with $c, d \in Z_p$ and $\alpha = awv$, $a \in Z_p$, (5) is equivalent to finding $a \in Z_p \pmod{p^r}$ such that $a^2(dpuu') - a(1 - c^2pu' + uu'd^2p) + d \equiv 0\ (p^r)$ and it is not hard to see that this equation is always solvable $\operatorname{mod} p^r$. This completes the proof of the lemma and Proposition 12.

We collect the results of this section in

THEOREM 14. *Let* $p$ *be a prime* $\neq 2$. *Let* $K$ *be a semi-simple algebra of dimension* 2 *over* $Q_p$ *and* $\mathfrak{o}$ *an order of* $K$ *with discriminant* $\Delta$. *Then the number of inequivalent* $\operatorname{mod} U(\mathfrak{O}_{2r+1}^{(p)})$ *optimal embeddings of* $\mathfrak{o}$ *into* $\mathfrak{O}_{2r+1}^{(p)}$ *is given by* *the table*

| $\Delta$ | $s<r$ | $s=r$ | $s>r$ |
|---|---|---|---|
| $p^{2s}$ | 0 | 0 | 0 |
| $p^{2s}u$ | $2p^s-2p^{s-1}$ | $2p^r-2p^{r-1}$ | 0 |
| $p^{2s+1}$ | 0 | $p^r$ | 0 |
| $p^{2s+1}u$ | 0 | $p^r$ | 0 |

*Here for* $s=0$, *read* $p^{-1}=0$.

PROOF. The only thing not covered above is the case $\Delta=p^{2s}$. But then $K$ is not a field $\Rightarrow K$ has zero divisors $\Rightarrow K$ can not be embedded in $\mathfrak{A}_p$.

## § 5. The case $p=2$.

We recall that $u=5$ and $v=\frac{1+\sqrt{5}}{2}$ when $p=2$. The analogue of Theorem 14 is

THEOREM 15. *Let $K$ be a semi-simple algebra of dimension 2 over $Q_2$ and $\mathfrak{o}$ an order of $K$ with discriminant $\Delta$. Then the number of inequivalent* mod $U(\mathfrak{O}_{2r+1}^{(2)})$ *optimal embeddings of $\mathfrak{o}$ into $\mathfrak{O}_{2r+1}^{(2)}$ is given by the table*

| $\Delta$ | $s<r$ | $s=r$ | $s>r$ |
|---|---|---|---|
| 1 | 0 | 0 | 0 |
| $2^{2s+2}$ | 0 | 0 | 0 |
| 5 | 2 | 2 | 2 |
| $2^{2s+2}5$ | $2^{s+1}$ | 0 | 0 |
| $2^{2s+2}3$ *or* $2^{2s+2}7$ | 0 | $2^r$ | 0 |
| $2^{2s+3}a$ *where* $a=1, 3, 5$ *or* 7 | 0 | $2^r$ | 0 |

PROOF. The proof will be given in a series of propositions, the proofs of which are similar to those in section 4. First note that the case $\Delta$ a square can not occur and that by Proposition 6 we need only consider the cases where the entries of the table are non zero. In this section $K$ and $\mathfrak{o}$ will have the same meaning as in Theorem 15.

PROPOSITION 16. *If $\Delta(\mathfrak{o})=5$, then $\mathfrak{o}$ has exactly* 2 *inequivalent* mod $U(\mathfrak{O}_{2r+1})$ *optimal embeddings into $\mathfrak{O}_{2r+1}$.*

PROOF. We can assume $\mathfrak{o}=Z_2+Z_2v$. Then $\varphi_1(v)=[v, 0]$ and $\varphi_2(v)=[\bar{v}, 0]$ give inequivalent optimal embeddings. Suppose $\varphi$ is an optimal embedding. Then $\varphi(v)=\left[\frac{1+b\sqrt{5}}{2}, 2^ry\right]=G$ (say) with $b\in U(Z_2)$ and $y\in R$. Hence $b\equiv\pm1(4)$.

Just as in the proof of Proposition 10, $b\equiv 1(4)$ implies $G$ is conjugate by $U(\mathfrak{O}_{2r+1})$ to $[v, 0]$ and $b\equiv -1(4)$ implies $G$ is conjugate by $U(\mathfrak{O}_{2r+1})$ to $[\bar{v}, 0]$.

PROPOSITION 17. *If* $\Delta(\mathfrak{o})=2^{2s+2}5$ *with* $0\leqq s<r$, *then* $\mathfrak{o}$ *has exactly* $2^{s+1}$ *inequivalent* $\bmod U(\mathfrak{O}_{2r+1})$ *optimal embeddings into* $\mathfrak{O}_{2r+1}$.

PROOF. We can assume $\mathfrak{o}=Z_2+Z_2 2^s\sqrt{5}$. Let $\varphi$ be an optimal embedding. Then $\varphi(2^s\sqrt{5})=G$ (say) is conjugate to $[2^s\sqrt{5}, 0]$ or $[-2^s\sqrt{5}, 0]$ by an element of $U(\mathfrak{O}_1)$. Suppose $G$ is conjugate to $[2^s\sqrt{5}, 0]$. Then as in Lemma 11, $G$ is conjugate by $U(\mathfrak{O}_{2r+1})$ to some

$$(6)\qquad \left[\frac{2^s\sqrt{5}+2^{2r-s-1}\beta\bar{\beta}\sqrt{5}}{1-2^{2r-2s-1}\beta\bar{\beta}}, \frac{-2^r\beta\sqrt{5}}{1-2^{2r-2s-1}\beta\bar{\beta}}\right]=\tilde{\beta}\qquad \text{(say)}$$

where $\beta\in R \pmod{2^{s+1}}$ and $\beta\in U(R)$. Let $\tilde{\beta}_1$ be defined as in (6) by replacing $\beta$ by $\beta_1$ with $\beta_1\in R \pmod{2^{s+1}}$, $\beta_1\in U(R)$. We claim

$$(7)\qquad \tilde{\beta} \text{ is conjugate to } \tilde{\beta}_1 \text{ by } U(\mathfrak{O}_{2r+1}) \Longleftrightarrow \beta\bar{\beta}\equiv\beta_1\bar{\beta}_1 \pmod{2^{s+1}}.$$

The proof of (7) is exactly the same as the proof of (2) in Proposition 11. Now as $\beta$ ranges over units in $R \pmod{2^{s+1}}$, $\beta\bar{\beta}$ ranges over all units in $Z_2 \pmod{2^{s+1}}$. This gives $2^s$ optimal embeddings $\varphi$ and the case where $G$ is conjugate to $[-2^s\sqrt{5}, 0]$ by $U(\mathfrak{O}_1)$ gives the other $2^s$.

PROPOSITION 18. *If* $\Delta(\mathfrak{o})=2^{2r+3}u'$ *with* $u'=1, 3, 5$, *or* 7, *then* $\mathfrak{o}$ *has exactly* $2^r$ *inequivalent optimal embeddings into* $\mathfrak{O}_{2r+1}$.

PROOF. Define and fix an element $w\in L$ such that $N(w)=u'$. We can assume $\mathfrak{o}=Z_2+Z_2 2^r\sqrt{2u'}$. Let $\varphi$ be an optimal embedding. Then $\varphi(2^r\sqrt{2u'})=G$ (say) is conjugate to $[0, 2^r w]$ by $U(\mathfrak{O}_1)$ (since $[0, w]$ commutes with $[0, 2^r w]$). Then as in Proposition 12, $G$ is conjugate by $U(\mathfrak{O}_{2r+1})$ to some

$$(8)\qquad \left[\frac{2^{r+1}(\gamma\bar{w}-\bar{\gamma}w)}{1-2\gamma\bar{\gamma}}, \frac{2^r(w-2\gamma^2\bar{w})}{1-2\gamma\bar{\gamma}}\right]=\hat{\gamma}\qquad \text{(say)}$$

where $\gamma\in R \pmod{2^r}$. To complete the proof we need only

LEMMA 19. *Let* $S=\{awv \mid a\in Z_2 \pmod{2^r}\}$.

i) *Let* $\alpha, \beta\in S$ *and define* $\hat{\alpha}, \hat{\beta}$ *as in* (8). *Then* $\hat{\alpha}$ *is conjugate to* $\hat{\beta}$ *by* $U(\mathfrak{O}_{2r+1})\Leftrightarrow\alpha=\beta$.

ii) *Let* $G$ *be as in Proposition* 18. *Then* $G$ *is conjugate by* $U(\mathfrak{O}_{2r+1})$ *to some* $\hat{\alpha}$, $\alpha\in S$.

PROOF. i) As in Lemma 13, $\hat{\alpha}$ is conjugate to $\hat{\beta}$ by $U(\mathfrak{O}_{2r+1})$ is equivalent to $\dfrac{2^{r+1}(\alpha\bar{w}-\bar{\alpha}w)}{1-2\alpha\bar{\alpha}}\equiv\dfrac{2^{r+1}(\beta\bar{w}-\bar{\beta}w)}{1-2\beta\bar{\beta}} \pmod{2^{2r+1}}$. Letting $\alpha=awv$ and $\beta=bwv$, this gives $a\equiv b(2^r)\Rightarrow\hat{\alpha}=\hat{\beta}$.

ii) We need only show each $\hat{\gamma}$, $\gamma\in R \bmod 2^r$ is conjugate by $U(\mathfrak{O}_{2r+1})$ to some $\hat{\alpha}$, $\alpha\in S$. Letting $\alpha=awv$ and $\gamma=(c+dv)w$ with $c, d\in Z_2$, this is equivalent to finding $a\in Z_2 \pmod{2^r}$ such that

$$a^2(2du')-a(1-2(c^2+cd-d^2)u')+d\equiv 0 \pmod{2^r}$$

and it is not hard to see that this equation is always solvable $\pmod{2^r}$.

PROPOSITION 20. *If* $\Delta(\mathfrak{o})=2^{2r+2}u'$ *where* $u'=3$ *or* 7, *then* $\mathfrak{o}$ *has exactly* $2^r$ *inequivalent* mod $U(\mathfrak{O}_{2r+1})$ *optimal embeddings into* $\mathfrak{O}_{2r+1}$.

PROOF. Define and fix an element $w\in R$ by letting $N(w)=1$ if $u'=7$ and $N(w)=-1$ if $u'=3$. We can assume $\mathfrak{o}=Z_2+Z_2g$ where $\mathrm{tr}(g)=2^{r+1}$ and $N(g)=-2^{2r+1}(2+w\bar{w})$. Let $\varphi$ be an optimal embedding. Then $\varphi(g)=G$ (say) is conjugate to $[2^{r+1}v, 2^rw]$ by an element of $U(\mathfrak{O}_1)$ (since $[w, v][0, 1]=[2v, w]$ commutes with $[2^{r+1}v, 2^rw]$). Thus $G$ is conjugate by $U(\mathfrak{O}_{2r+1})$ to some

$$\left[\frac{2^{r+1}(\gamma\bar{w}-\bar{\gamma}w)+2^{r+1}(v-2\gamma\bar{\gamma}\bar{v})}{1-2\gamma\bar{\gamma}}, \frac{2^r(w-2\gamma\bar{w})+2^{r+1}(\gamma\bar{v}-\gamma v)}{1-2\gamma\bar{\gamma}}\right]=\hat{\gamma} \quad \text{(say)} \tag{9}$$

where $\gamma\in R \pmod{2^r}$. To complete the proof we need only

LEMMA 21. *Let* $S=\{awv\,|\,a\in Z_2 \pmod{2^r}\}$.

i) *Let* $\alpha, \beta\in S$ *and define* $\hat{\alpha}, \hat{\beta}$ *as in* 9. *Then* $\hat{\alpha}$ *is conjugate to* $\hat{\beta}$ *by* $U(\mathfrak{O}_{2r+1})\Leftrightarrow\alpha=\beta$.

ii) *Let* $G$ *be as in Proposition* 20. *Then* $G$ *is conjugate by* $U(\mathfrak{O}_{2r+1})$ *to some* $\hat{\alpha}$, $\alpha\in S$.

PROOF. The proof is similar to and only slightly more complicated than the proof of Lemma 19.

## § 6. Orders of level $q_1q_2$ and the Mass formula.

Let $q_1=p_1^{s_1}\cdots p_f^{s_f}$ where the $p_i$ are distinct primes and $f, s_1, \cdots, s_f$ are all *odd* positive integers. Let $q_2$ be any positive integer such that $(q_1, q_2)=1$. Let $\mathfrak{A}$ be the (unique) quaternion algebra over $Q$ such that the set of primes at which $\mathfrak{A}$ is ramified (i.e. such that $\mathfrak{A}\otimes Q_p$ is a division algebra) is precisely $\{p_1, \cdots, p_f, \infty\}$.

DEFINITION 22. Let $q_1$, $q_2$, and $\mathfrak{A}$ be as above. An order $\mathfrak{O}$ of $\mathfrak{A}$ is said to have *level* $q_1q_2$ if

a) $\mathfrak{O}_{p_i}=\mathfrak{O}\otimes_Z Z_{p_i}$ is an order of level $p_i^{s_i}$ in $\mathfrak{A}\otimes Q_{p_i}$ for $p_i\,|\,q_1$

b) $\mathfrak{O}_p$ is isomorphic (over $Z_p$) to $\begin{pmatrix} Z_p & Z_p \\ q_2Z_p & Z_p\end{pmatrix}$ for $p\nmid q_1$.

REMARK. If $q_1$ is square free and $q_2=1$, these are just the maximal orders of $\mathfrak{A}$. If $q_1q_2$ is square free, they are the Eichler orders studied in [1], [4], and [7]. If $q_1$ is square free they are the "split" orders studied in [5] and [8].

Let us fix $q_1$, $q_2$ and $\mathfrak{A}$ as above for the remainder of this section. Let $\mathfrak{O}$ be an order of level $q_1q_2$ on $\mathfrak{A}$. Then just as in [4] and [8], $\mathfrak{O}$ has an ideal theory. Let $J_{\mathfrak{A}}$ denote the idele group of $\mathfrak{A}$ and $J_{\mathfrak{A}}^1$ the ideles of volume 1 (if

$\alpha=(\alpha_p)\in J_{\mathfrak{A}}$, we let $\mathrm{vol}(\alpha)=\prod_p |N(\alpha_p)|_p$, the product over all $p$ including $\infty$). Also let $\mathfrak{U}(\mathfrak{O})=\{\alpha=(\alpha_p)\in J^1_{\mathfrak{A}} \mid \alpha_p\in U(\mathfrak{O}_p) \text{ for all } p<\infty\}$. Then left $\mathfrak{O}$ ideals can be identified with the cosets $\mathfrak{U}(\mathfrak{O})\backslash J^1_{\mathfrak{A}}$. We say two left $\mathfrak{O}$-ideals $I$ and $J$ are *equivalent* if and only if $I=J\alpha$ for some $\alpha\in\mathfrak{A}^x$. Thus the set of left $\mathfrak{O}$-ideal classes is identified with the double cosets $\mathfrak{U}(\mathfrak{O})\backslash J^1_{\mathfrak{A}}/\mathfrak{A}^x$. In fact if $J^1_{\mathfrak{A}}=\bigcup_{i=1}^{h}\mathfrak{U}(\mathfrak{O})g_i\mathfrak{A}^x$, then $\mathfrak{O}g_i$, $i=1,\cdots,h$ represent all the left $\mathfrak{O}$-ideal classes. Here if $g=(g_p)\in J^1_{\mathfrak{A}}$, $\mathfrak{O}g$ denotes the unique lattice $I$ on $\mathfrak{A}$ with $I_p=I\otimes Z_p=\mathfrak{O}_pg_p$ for all $p<\infty$.

Let $\mathfrak{O}$ be an order of level $q_1q_2$ on $\mathfrak{A}$. Let $M_1,\cdots,M_n$ be representatives of the (left) $\mathfrak{O}$-ideal classes. Let $\mathfrak{O}_i$, $i=1,\cdots,h$ be the right orders of the $M_i$, i.e. $\mathfrak{O}_i=\{a\in\mathfrak{A} \mid M_ia\subseteq M_i\}$. If $M_i=\mathfrak{O}g_i$, then $\mathfrak{O}_i=g_i^{-1}\mathfrak{O}g_i$. The $\mathfrak{O}_i$ are also orders of level $q_1q_2$. We define a weighted class number called the Mass by

DEFINITION 23. The Mass $M_{q_1q_2}$ (for $\mathfrak{O}$-ideals, $\mathfrak{O}$ an order of level $q_1q_2$) is given by

$$M_{q_1q_2}=2\sum_{i=1}^{h}\frac{1}{|U(\mathfrak{O}_i)|}.$$

REMARK. The Mass $M_{q_1q_2}$ depends only on the level, not on the particular order or on the left or right ideals (see Proposition 24). Also the 2 in the definition comes from the fact that we really should consider $U(\mathfrak{O}_i) \bmod U(Z)$, at least if we want our definition to extend to quaternion algebras over totally real number fields.

We need an explicit formula for the Mass. If $q_1$ is square free this is given by Lemma 19 of [8]. The formula in the present case is similar. For completeness we sketch a proof. For simplicity let $G=J^1_{\mathfrak{A}}$ and $\Gamma=\mathfrak{A}^x$. Then $G$ is a locally compact unimodular group and $\Gamma$ is a discrete subgroup with $G/\Gamma$ compact. Finally $\mathfrak{U}(\mathfrak{O})$ is an open compact subgroup (see [**10**]). If $dx$ is a Haar measure on $G$, we also denote (by abuse of notation) the invariant quotient measure on $G/\Gamma$ by $dx$, i.e. if $f$ is a continuous function with compact support on $G$, then $\int_G f(x)dx=\int_{G/\Gamma}(\sum_{\gamma\in\Gamma}f(x\gamma))dx$.

PROPOSITION 24. *Let $\mathfrak{O}$ be an order of level $q_1q_2$. Denote by dx the Haar measure on G normalized so that* $\mathrm{vol}(\mathfrak{U}(\mathfrak{O}))=1$. *Then* $M_{q_1q_2}=2\,\mathrm{Vol}(G/\Gamma)$.

PROOF. $G=\bigcup_{i=1}^{h}\mathfrak{U}(\mathfrak{O})g_i\Gamma$ where $\mathfrak{O}g_i$, $i=1,\cdots,h$ represent all the (left) $\mathfrak{O}$-ideal classes. Thus $\mathrm{Vol}(G/\Gamma)=\sum_i \mathrm{vol}(\mathfrak{U}(\mathfrak{O})g_i\Gamma/\Gamma)=\sum_i \mathrm{vol}(g_i^{-1}\mathfrak{U}(\mathfrak{O})g_i\Gamma/\Gamma)=\sum_i \mathrm{vol}(\mathfrak{U}(g_i^{-1}\mathfrak{O}g_i)\Gamma/\Gamma)=\sum_i \mathrm{vol}(\mathfrak{U}(g_i^{-1}\mathfrak{O}g_i)/\mathfrak{U}(g_i^{-1}\mathfrak{O}g_i)\cap\Gamma)=\sum_i\frac{1}{|U(g_i^{-1}\mathfrak{O}g_i)|}=\frac{1}{2}M_{q_1q_2}$ by the definition of $M_{q_1q_2}$.

PROPOSITION 25. $M_{q_1q_2}=\frac{q_1q_2}{12}\prod_{p\mid q_1}\left(1-\frac{1}{p}\right)\prod_{p\mid q_2}\left(1+\frac{1}{p}\right)$.

PROOF. If $\mathfrak{O}$ is a maximal order, i.e. if $q_1$ is square free and $q_2=1$, then the Mass is well known to be

$$\frac{1}{12}\prod_{p\mid q_1}(p-1) \qquad \text{(see [1] p. 137 or [4] p. 95)}. \tag{10}$$

Now let $\mathfrak{O}$ be an order of level $q_1q_2$. Then $\mathfrak{O}$ is contained in an order $\mathfrak{O}'$ of level $q1$ where $q=\prod_{p\mid q_1} p$. Now $[\mathfrak{U}(\mathfrak{O}'):\mathfrak{U}(\mathfrak{O})]=\prod_p [U(\mathfrak{O}'_p):U(\mathfrak{O}_p)]$. If $p\mid q_1$, $[U(\mathfrak{O}'_p):U(\mathfrak{O}_p)]=[U(\mathfrak{O}_1^{(p)}):U(\mathfrak{O}_{2r+1}^{(p)})]=p^{2r}$ where $v_p(q_1)=2r+1$ by Lemma 7. As

$$\left[U\begin{pmatrix} Z_p & Z_p \\ p^r Z_p & Z_p\end{pmatrix}:U\begin{pmatrix} Z_p & Z_p \\ p^{r+1} Z_p & Z_p\end{pmatrix}\right]=\begin{cases} p+1 & \text{if } r=0 \\ p & \text{if } r>0\end{cases}$$

we see that for $p\mid q_2$, $[U(\mathfrak{O}'_p):U(\mathfrak{O}_p)]=p^r\left(1+\frac{1}{p}\right)$ where $r=v_p(q_2)$. Thus

$$[\mathfrak{U}(\mathfrak{O}'):\mathfrak{U}(\mathfrak{O})]=q_1q_2\prod_{p\mid q_1}\left(1-\frac{1}{p}\right)\prod_{p\mid q_2}\left(1+\frac{1}{p}\right)\Big(\prod_{p\mid q_1}(p-1)\Big)^{-1}. \tag{11}$$

Now by (10) and Proposition 24, the volume of $G/\Gamma$ under the assumption $\mathrm{vol}\,(\mathfrak{U}(\mathfrak{O}'))=1$ is $\frac{1}{24}\prod_{p\mid q_1}(p-1)$. Hence the volumn in the present case $(\mathrm{vol}\,(\mathfrak{U}(\mathfrak{O}))=1)$ is $[\mathfrak{U}(\mathfrak{O}'):\mathfrak{U}(\mathfrak{O})]$ times as large. This by (11) and Proposition 24 completes the proof.

## § 7. The Brandt Matrices.

Let $q_1$, $q_2$, and $\mathfrak{A}$ be as in section 6 and let $\mathfrak{O}$ be an order of level $q_1q_2$ on $\mathfrak{A}$. Fixing a set of representatives of the (left) $\mathfrak{O}$-ideal classes, we define (generalized) Brandt matrices $B(n)=B_l(n\,;q_1,q_2)$ in exactly the same manner as Eichler (see [4], equations 15 and 15a on page 105). Then as in Theorem 2, Chapter 2 of [4], the $B(n)$ (for fixed $l$, $q_1$, $q_2$) with $(n, q_1q_2)=1$ generate a semi-simple commutative ring and satisfy the same identities as the Hecke operators $T(n)$, $(n, q_1q_2)=1$.

We are interested in the trace of the Brandt Matrix. This is given by the following theorem where we follow the notation of Hijikata [5].

THEOREM 26. *The trace of the Brandt Matrix $B_{k-2}(n\,;q_1,q_2)$ is given by*

$$\begin{aligned}\mathrm{Tr}\,B_{k-2}(n\,;q_1,q_2)&=\sum_s a_k(s)\sum_f b(s,f)\prod_{p\mid q_1q_2}c(s,f,p)\\ &\quad+\delta(\sqrt{n})\left(\frac{k-1}{12}\right)q_1q_2\prod_{p\mid q_1}\left(1-\frac{1}{p}\right)\prod_{p\mid q_2}\left(1+\frac{1}{p}\right)\end{aligned} \tag{12}$$

*where* $\delta(\sqrt{n})=\begin{cases} n^{\frac{k-2}{2}} & \textit{if } n \textit{ is a square} \\ 0 & \textit{otherwise.}\end{cases}$

The meaning of $s$, $a_k(s)$, $f$, $b(s,f)$, and $c(s,f,p)$ are given as follows.

Let $s$ run over all integers such that $s^2-4n$ is not a positive non-square, hence by some positive integer $t$ and square free negative integer $m$ we can classify $s^2-4n$ into cases by

$$s^2-4n=\begin{cases} 0 & & (p) \\ t^2 & & (h) \\ t^2m & m=1(4) & (e1) \\ t^2 4m & m=2,3(4) & (e23) \end{cases} \Big\} (e).$$

Let $\Phi_s(X)=X^2-sX+n$ and let $x$, $y$ be the roots of $\Phi_s(X)=0$. Corresponding to the type of $s$, put

$$a_k(s)=\begin{cases} \dfrac{|x|}{4}(\mathrm{sgn}(x))^k & (p) \\ \mathrm{Min}\{|x|, |y|\}^{k-1}|x-y|^1(\mathrm{sgn}(x))^k & (h) \\ 1/2(x^{k-1}-y^{k-1})(x-y)^{-1} & (e). \end{cases}$$

For each $s$ (fixed), let $f$ run over $\begin{cases} 1 & (p) \\ \text{all positive divisors of } t & (h)+(e). \end{cases}$

Put $\Delta=(s^2-4n)/f^2$. Let $K$ denote the quotient ring $Q[X]/\Phi_s(X)$ and $\xi$ the canonical image of $X$ in $K$. $K$ is a commutative semi-simple algebra of dimension 2 over $Q$ and $\xi$ generates the order $Z+Z\xi$ on $K$. For each $f$ there exists a uniquely determined order $\Lambda=\Lambda_\Delta$ containing $Z+Z\xi$ as a submodule of index $f$ (with disc $(\Lambda)=\Delta$). Let $h(\Delta)$ (resp. $w(\Delta)$) denote the class number of locally principal $\Lambda$-ideals (resp. $1/2|U(\Lambda)|$. Then

$$b(s,f)=\begin{cases} 1 & (p) \\ \dfrac{1}{2}\varphi(\sqrt{\Delta}) & (h) \\ \dfrac{h(\Delta)}{w(\Delta)} & (e). \end{cases}$$

Let $\mathfrak{O}$ be an order of level $q_1q_2$ on $\mathfrak{A}$. Then $c(s,f,p)$ is the number of inequivalent mod $U(\mathfrak{O}\otimes Z_p)$ optimal embeddings of $\Lambda\otimes Z_p$ into $\mathfrak{O}\otimes Z_p$.

REMARKS. As $\mathfrak{A}$ is a division algebra, $c(s,f,p)=0$ in cases $(p)$ and $(h)$. We included those cases to show the similarity of $\mathrm{Tr}(B(n))$ and $\mathrm{Tr}(T(n))$ (see Theorem 1 of [**9**]) and to make the statement of Theorem 2 in [**9**] simpler. For $p|q_1$, $c(s,f,p)$ is given by Theorems 14 and 15 of this paper. For $p|q_2$, $c(s,f,p)$ is given by Theorem 2.3 of [**5**] and explicitly in the proof of Theorem 4 of [**9**]. For $p\nmid q_1q_2$, $c(s,f,p)=1$ (by Corollary 2.6 of [**5**]).

PROOF. Eichler gives a proof of this (see [**4**], Chapter 2, §8) in the case $q_1q_2$ is square free. Using the results of [**5**] for $p|q_2$ and the results of sections 1-6 of this paper for $p|q_1$ one can easily generalize Eichler's proof to obtain (12).

## References

[1] M. Eichler, Zur Zahlentheorie der Quaternionen Algebren, J. Reine Angew. Math., **195** (1955), 127-151.
[2] M. Eichler, Über die Darstellbarkeit von Nodulformen durch Thetareihen, J. Reine Angew. Math., **195** (1955), 156-171.
[3] M. Eichler, Quadratische Formen und Modulfunktionen, Acta Arith., **4** (1958), 217-239.
[4] M. Eichler, The basis problem for modular forms and the traces of the Hecke operators, Lecture Notes in Math. #320, Springer-Verlag, 75-151.
[5] H. Hijikata, Explicit formula of the traces of Hecke operators for $\Gamma_0(N)$, J. Math. Soc. Japan, **26** (1974), 56-82.
[6] H. Hijikata and H. Saito, On the representability of modular forms by theta series, Number Theory, Algebraic Geometry, and Commutative Algebra in honor of Y. Akizuki, Kinokuniya, Tokyo, 1973, 13-21.
[7] A. Pizer, Type numbers of Eichler orders, J. Reine Angew. Math., **264** (1973), 76-102.
[8] A. Pizer, On the arithmetic of quaternion algebras, to appear in Acta Arith., Vol. **31** n. 1.
[9] A. Pizer, The Representability of modular forms by theta series, J. Math. Soc. Japan, **28** (1976), 689-698.
[10] A. Weil, Basic Number Theory, Springer-Verlag, 1967.

Arnold PIZER
Department of Mathematics
University of Rochester
Rochester, N.Y. 14627
U.S.A.