<table>
<thead>
<tr>
<th>Title</th>
<th>REDUCED UNIT GROUPS IN TOTALLY DEFINITE QUATERNION ALGEBRAS OVER REAL QUADRATIC FIELDS (Analytic and Arithmetic Theory of Automorphic Forms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Li, Qun; Xue, Jiangwei; Yu, Chia-Fu</td>
</tr>
<tr>
<td>Citation</td>
<td>数理解析研究所講究録 2019, 2100: 80-93</td>
</tr>
<tr>
<td>Issue Date</td>
<td>2019-01</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/2433/251795">http://hdl.handle.net/2433/251795</a></td>
</tr>
<tr>
<td>Type</td>
<td>Departmental Bulletin Paper</td>
</tr>
<tr>
<td>Textversion</td>
<td>publisher</td>
</tr>
</tbody>
</table>

Kyoto University
REDUCED UNIT GROUPS IN TOTALLY DEFINITE QUATERNION ALGEBRAS OVER REAL QUADRATIC FIELDS

QUN LI, JIANGWEI XUE, AND CHIA-FU YU

Abstract. This is the survey paper of the joint work [8] in progress. The purpose is to report the results on the classification and enumeration of reduced unit groups of maximal orders in totally definite quaternion algebras over real quadratic fields.

1. Introduction

Let $F$ be a totally real number field with ring of integers $O_F$, and $B$ a totally definite quaternion $F$-algebra. Fix a maximal $O_F$-order $\mathbb{O}$ in $B$. Denote by $\text{Cl}(\mathbb{O})$ the set of right ideal classes of $\mathbb{O}$ and by $h(\mathbb{O}) := |\text{Cl}(\mathbb{O})|$ the class number of $\mathbb{O}$, which depends only on $B$ and is independent of the choice of $\mathbb{O}$, hence also denoted by $h(B)$. Two $O_F$-orders in $B$ have the same type if they are $B^\times$-conjugate. Denote by $T_p(B)$ the finite set of conjugacy classes of all maximal $O_F$-orders in $B$ and write $t(B) = t(\mathbb{O}) := |T_p(\mathbb{O})|$ for the type number of $B$.

Using Eichler's trace formula ([5], [9], cf. [12]) one can compute, for each given $B$, both the class number $h(B)$ and the type number $t(B)$. However, the formula for $t(B)$ is more involved; it requires the knowledge of the ideal class group $\text{Cl}(F)$ of $F$. In some cases where the totally real field $F$ has "simpler structure" there is an alternative way of computing $t(B)$. Instead of working through Eichler's trace formula for $t(B)$, one can compute $t(B)$ directly from $h(B)$. More precisely, one has the following result (see [16]).

Proposition 1. Let $B$ be a totally definite quaternion algebra over a totally real number field $F$. If $B$ is unramified at all finite places of $F$ and $h(F)$ is odd, then $h(B) = h(F)t(B)$.

For example if $F = \mathbb{Q}(\sqrt{p})$, where $p$ is a prime number, then $h(F)$ is odd. In [3, Corollary 18.4] one can find a complete list of quadratic fields with odd class numbers.

Vignéras [11, Theorem 3.1] gave an explicit formula for $h(\mathbb{O})$ (also including Eichler orders $\mathbb{O}$) where $F$ is a real quadratic field. Explicit formulas tend to be very complicated for more general fields $F$. However, one can use Eichler's trace formula to evaluate $h(\mathbb{O})$ for each given case. Kirschmer and Voight [7] have worked out the analogous Gauss class number in this setting. They determined all Eichler $O_F$-orders with class number $\leq 2$. Previously Brzezinski [1] obtained a complete list of all orders (including non-Gorenstein orders) in definite quaternion $\mathbb{Q}$-algebras with class number one.

Date: May 16, 2018.
Let \( I_1, \ldots, I_h \) be a complete set of representatives of the right ideal class set \( \text{Cl}(\mathcal{O}) \). The mass of \( \text{Cl}(\mathcal{O}) \) is defined to be

\[
\text{Mass}(\mathcal{O}) := \sum_{i=1}^{h} \frac{1}{|\mathcal{O}_i^\times/O_F^\times|},
\]

where \( \mathcal{O}_i := \mathcal{O}_l(I_i) \) is the left order of \( I_i \).

The group \( \mathcal{O}_i^\times/O_F^\times \) is finite and called the reduced unit group of \( \mathcal{O}_i \). The mass is much easier to compute. For example, if \([F: \mathbb{Q}] = 2\), the mass formula states

\[
\text{Mass}(\mathcal{O}) = \frac{1}{2} \zeta_F(-1) \prod_{p \mid d(\mathcal{O})} (N(p) - 1),
\]

where \( \zeta_F(s) \) is the Dedekind zeta function of \( F \), \( N(p) = |O_F/p| \), and \( d(\mathcal{O}) \) is the discriminant of \( \mathcal{O} \). In general, Eichler’s trace formula gives

\[
h(\mathcal{O}) = \text{Mass}(\mathcal{O}) + \text{Ell}(\mathcal{O}),
\]

where the calculation of the elliptic part \( \text{Ell}(\mathcal{O}) \) involves listing all imaginary quadratic \( O_F \)-orders \( R \) with non-trivial reduced unit group \( R^\times/O_F^\times \), and computing their class numbers and the number of local optimal embeddings into \( \mathcal{O} \).

It is expected that \( \text{Mass}(\mathcal{O}) \) is the “main term” for \( h(\mathcal{O}) \). In other words, the ideal classes \([I_i] \in \text{Cl}(\mathcal{O})\) with \( \mathcal{O}_i^\times/O_F^\times = 1 \) should constitute the majority of \( \text{Cl}(\mathcal{O}) \). More precisely, one has the following conjecture.

**Conjecture 2.** We have

\[
\frac{\text{Mass}(\mathcal{O})}{h(\mathcal{O})} \rightarrow 1, \quad \text{as long as } h(\mathcal{O}) \rightarrow \infty.
\]

This expectation is verified \cite[Section 6.3]{15} for the family of totally definite quaternion \( \mathbb{Q}(\sqrt{p}) \)-algebras \( B_{\infty_1, \infty_2} \) which are unramified at all finite places of \( \mathbb{Q}(\sqrt{p}) \) with \( p \) running through all prime numbers. In general, it follows from Eichler’s trace formula that the term \( \text{Ell}(\mathcal{O}) \) is a linear combination of class numbers of two kinds of CM extensions \( K/F \):

- \( K = F(\zeta_{2n}) \) for a suitable class of \( n \in \mathbb{N} \);
- \( K = F(\sqrt{-\varepsilon_i}) \) for a finite system of totally positive units \( \varepsilon_i \in O_F^\times \).

(See \( (5.1) \) for the possible CM fields \( K \) in the case \([F: \mathbb{Q}] = 2\). Therefore, one needs to compare the term \( \zeta_F(-1)h(F) \) with the class numbers \( h(F(\zeta_{2n})) \) and \( h(F(\sqrt{-\varepsilon_i})) \). When the degree \([F: \mathbb{Q}] \) is bounded, the numbers of terms \( h(F(\zeta_{2n})) \) and \( h(F(\sqrt{-\varepsilon_i})) \) are bounded. However, as \([F: \mathbb{Q}] \) increases, one needs to show that the number of terms increases moderately compared with the growth of \( \zeta_F(-1)h(F) \). One can ask whether or not \( h(\mathcal{O}) \rightarrow \infty \) if and only if the absolute discriminant \( \text{disc}(F) \rightarrow \infty \). If this is the case, then the problem would be reduced to the analysis of the growth behavior of \( \zeta_F(-1) \) and the relative class numbers \( h(K)/h(F) \) in terms of the growth of the discriminant of \( F \).

2. **THE EXAMPLE OF QUATERNION \( \mathbb{Q} \)-ALGEBRAS**

Let \( B \) be a definite quaternion \( \mathbb{Q} \)-algebra and \( \mathcal{O} \) a maximal order in \( B \). For each \( n \geq 1 \), denote by \( C_n \) the cyclic group of order \( n \). Then (see \cite[Chapter V, Proposition 3.1]{12})

\[
\mathcal{O}^\times \in \{C_2, C_4, C_6\}
\]
UNIT GROUPS

except that

\[ B = B_{2,\infty}, \quad h(\mathcal{O}) = 1, \quad \mathcal{O}^\times \simeq \text{SL}_2(\mathbb{F}_3), \quad \text{or} \]

\[ B = B_{3,\infty}, \quad h(\mathcal{O}) = 1, \quad \mathcal{O}^\times \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, \]

where \( B_{p,\infty} \) denotes the quaternion \( \mathbb{Q} \)-algebra ramified exactly at \( \{p, \infty\} \). Thus, \( \mathcal{O}^\times \)

is cyclic except for finitely many definite quaternion \( \mathbb{Q} \)-algebras \( B \) and for finitely many (not necessarily maximal) orders \( \mathcal{O} \) up to conjugate. Put

\begin{equation}
(2.2) \quad h(B, G) := \# \{ [I] \in \text{Cl}(\mathcal{O}) | \mathcal{O}_l(I)^\times /\{\pm 1\} \simeq G \},
\end{equation}

and set \( h(G) = h(B, G) \) if \( B \) is clear from the context. By the Deuring-Eichler-Igusa class number formula [4], for \( B = B_{p,\infty} \) and \( p \geq 5 \), one can deduce

\begin{equation}
(2.3) \quad h(C_1) = h(B, C_1) = \frac{p - 1}{12} - \frac{1}{4} \left( 1 - \left( -\frac{4}{p} \right) \right) - \frac{1}{6} \left( 1 - \left( \frac{-3}{p} \right) \right),
\end{equation}

\begin{equation}
(2.4) \quad h(C_2) = \frac{1}{2} \left( 1 - \left( -\frac{4}{p} \right) \right), \quad h(C_3) = \frac{1}{2} \left( 1 - \left( \frac{-3}{p} \right) \right).
\end{equation}

In particular, we have

\begin{equation}
(2.5) \quad \mathcal{O}_l(I)^\times = \{\pm 1\}, \quad \forall [I] \in \text{Cl}(\mathcal{O}) \iff p \equiv 1 \pmod{12}.
\end{equation}

Note that for any fixed maximal order \( \mathcal{O} \subset B_{p,\infty} \), we have a natural bijection

\begin{equation}
\text{Cl}(\mathcal{O}) \simeq \left\{ \text{isomorphism classes of supersingular elliptic curves over } \overline{\mathbb{F}}_p \right\}
\end{equation}

\begin{equation}
[I] \quad \longleftrightarrow \quad [E]
\end{equation}

which identifies \( \mathcal{O}_l(I) \) with End\((E)\). Using (2.4) and the geometric interpretation above, we compute in [17] forms of supersingular elliptic curves over a suitable non-

perfect field, and compute their endomorphism algebras. As a result, we obtain the following result.

**Proposition 3** ([17, Theorem 1.3]). There exists a supersingular elliptic curve \( E \)

over some field \( k \supset \mathbb{F}_p \) with \( \text{End}_k^0(E) = \mathbb{Q} \) if and only if \( p \not\equiv 1 \pmod{12} \).

For the remainder of this note, we shall focus on the case where \( F = \mathbb{Q}(\sqrt{d}) \) is a real quadratic field with a square free \( d \in \mathbb{N} \).

3. RESULTS FOR \( F = \mathbb{Q}(\sqrt{p}), \ p \) A PRIME

Let \( p \) be a prime number and \( B \) the totally definite quaternion \( F = \mathbb{Q}(\sqrt{p}) \)-

algebra ramified only at the two infinite places of \( F \), which is also denoted by \( B_{\infty_1,\infty_2} \). Fix again a maximal \( O_F \)-order \( \mathcal{O} \) in \( B \). In this case, there is a natural bijection (see [13, Theorem 6.2] and [15, Theorem 6.1.2])

\begin{equation}
\text{Cl}(\mathcal{O}) \simeq \left\{ \begin{array}{l}
\text{\( F_p \)-isomorphism classes of supersingular abelian surfaces } X \text{ over } \overline{\mathbb{F}}_p \text{ with Frobenius endomorphism }
\pi_X^2 = p \text{ and endomorphism ring } \text{End}_{\overline{\mathbb{F}}_p}(X) \supset O_F
\end{array} \right\}.
\end{equation}

For any finite group \( G \), put

\begin{equation}
t(G) := \# \left\{ \text{\( B^\times \)-conjugacy classes of maximal } \mathcal{O}_l(\mathcal{O}) \subset B \text{ with } O_l^\times /O_F^\times \simeq G \right\}.
\end{equation}
Proposition 1 also gives the class-type number relation

\[(3.1) \quad h(G) = h(F) \cdot t(G).\]

Thus, knowing \(t(G)\) amounts to knowing \(h(G)\). For any \(n \geq 1\), denote by \(D_n\) the dihedral group of order \(2n\).

**Lemma 4.** We have
- \(p = 2\), \(h(\mathbb{O}) = 1\) and \(h(S_4) = 1\).
- \(p = 3\), \(h(\mathbb{O}) = 2\) and \(h(S_4) = h(D_{12}) = 1\).
- \(p = 5\), \(h(\mathbb{O}) = 1\) and \(h(A_5) = 1\).

**Theorem 5.** Assume \(p \geq 7\).

1. (Hashimoto [6]) For \(p \equiv 1\) mod 4, we have
   \[
   \begin{align*}
   t(C_1) &= \frac{\zeta_F(-1)}{2} - \frac{h(-p)}{8} - \frac{h(-3p)}{12} - \frac{1}{4} \left(\frac{p}{3}\right) - \frac{1}{4} \left(\frac{2}{p}\right) + \frac{1}{2}, \\
   t(C_2) &= \frac{h(-p)}{4} + \frac{1}{2} \left(\frac{p}{3}\right) + \frac{1}{4} \left(\frac{2}{p}\right) - \frac{3}{4}, \\
   t(C_3) &= \frac{h(-3p)}{4} + \frac{1}{2} \left(\frac{p}{3}\right) + \frac{1}{2} \left(\frac{2}{p}\right) - \frac{3}{4}, \\
   t(D_3) &= \frac{1}{2} \left(1 - \left(\frac{p}{3}\right)\right), \quad t(A_4) = \frac{1}{2} \left(1 - \left(\frac{2}{p}\right)\right),
   \end{align*}
   \]
   and \(t(G) = 0\) for any group \(G\) not in the above list. Here \(h(m)\) is short for \(h(\mathbb{Q}(\sqrt{m}))\) for a square-free integer \(m \in \mathbb{Z}\).

2. (Li-Xue-Yu) For \(p \equiv 3\) mod 4, we have
   \[
   \begin{align*}
   t(C_1) &= \frac{\zeta_F(-1)}{2} + \left(-7 + 3 \left(\frac{2}{p}\right)\right) \frac{h(-p)}{8} - \frac{h(-2p)}{4} - \frac{h(-3p)}{12} + \frac{3}{2}, \\
   t(C_2) &= \left(2 - \left(\frac{2}{p}\right)\right) \frac{h(-p)}{2} + \frac{h(-2p)}{2} - \frac{5}{2}, \\
   t(C_3) &= \frac{h(-3p)}{4} - 1, \\
   t(C_4) &= \left(3 - \left(\frac{2}{p}\right)\right) \frac{h(-p)}{2} - 1, \\
   t(D_3) &= 1, \quad t(D_4) = 1, \quad t(S_4) = 1,
   \end{align*}
   \]
   and \(t(G) = 0\) for any group \(G\) not listed above.

By Theorem 5, there exists a superingular abelian surface \(X\) over \(\mathbb{F}_p\) with non-abelian reduced automorphism group \(\text{RAut}(X) = \text{Aut}(X)/O_F^\times\) if and only if \(p \equiv 3\) (mod 4) or \(p \not\equiv 1\) (mod 24). Note that \(p \equiv 3\) (mod 4) implies \(p \not\equiv 1\) (mod 24).

Using a similar idea of the proof of Proposition 3, one can prove

**Proposition 6.** If \(p \not\equiv 1\) (mod 24), then there exists a superingular abelian surface \(X\) over some field \(k \supset \mathbb{F}_p\) such that \(\text{End}^0_k(X) \simeq \mathbb{Q}(\sqrt{p})\).

**Question 7.** (1) Is \(p \not\equiv 1\) (mod 24) a necessary condition for the assertion of Proposition 6?

(2) For a given prime \(p\), what are all possible endomorphism algebras of super-singular abelian surfaces over some field of characteristic \(p > 0\)?
One can use results of [17] to deduce all possible endomorphism algebras of non-simple supersingular abelian surfaces. The most interesting part of Question 7 (2) then is for simple supersingular abelian surfaces.

4. RESULTS FOR $F = \mathbb{Q}(\sqrt{d})$

Let $F = \mathbb{Q}(\sqrt{d})$ be an arbitrary quadratic real field, with a square free $d \in \mathbb{N}$, and $B$ be any totally definite quaternion $F$-algebra. Our main result may be rephrased roughly as follows:

We have explicit formulas $t(G)$ for each finite non-cyclic group $G$ (See Proposition 14) and a complete recipe for calculating $h(G)$ for each finite group $G$ (See Section 8). When $B = B_{\infty_1,\infty_2}$ and $h(F)$ is odd, we have an explicit formula for $t(G)$ for each finite group $G$.

Remark 8. (1) In fact, the only obstacle between us and a complete formula for $h(G)$ is the overwhelming number of cases that the problem naturally divides into, rendering any unified formula too cumbersome and unwieldy. However, for any class of quadratic real fields that one has a good grasp on the fundamental units, deduction of explicit formulas for $h(G)$ based on our recipe becomes entirely routine. One such example is when $B = B_{\infty_1,\infty_2}$ and $d = p$ is a prime as in part (2) of Theorem 5.

(2) If one drops one of the conditions $B = B_{\infty_1,\infty_2}$ and $h(F)$ being odd in Theorem 4, there is no known explicit formula for $t(B)$ even for $[F: \mathbb{Q}] = 2$. Thus, our assumption for the result of $t(G)$ is not too restricted. The main reason for making this assumption is based on Proposition 1. However, the present method goes beyond these restrictions. Indeed, our result of determination of $t(G)$ for non-cyclic groups $G$ does not require this assumption and it is even simpler if $B \not\cong B_{\infty_1,\infty_2}$. It is possible to explore relations of $h(G)$ and $t(G)$ more explicitly by cases under a weaker condition than that $h(F)$ is odd.

(3) Our result refines the explicit formula for $h(B)$ given by Vignéras [11]. However, we do not have a new approach for Vignéras’s explicit class number formula. Indeed, the way we compute all $h(G)$ is to treat those $G \neq C_1$ first, and then use Vignéras’s explicit formula to obtain $h(C_1)$.

Let $\mathcal{O}$ be an $O_F$-order in $B$. Then

$$\mathcal{O}^* := \mathcal{O}^\times/O_F^\times \in \{C_n, D_n (1 \leq n \leq 6) \cup \{12\}, A_4, S_4, A_5\}.$$  

The idea is to regard $\mathcal{O}^*$ as a finite subgroup of $SO_3(\mathbb{R})$ via the embedding

$$\mathcal{O}^* \rightarrow (B \otimes F \mathbb{R})^\times/\mathbb{R}^\times = \mathbb{H}^\times/\mathbb{R}^\times \cong SO_3(\mathbb{R}),$$

and use the well-known classification of finite subgroups of $SO_3(\mathbb{R})$ (See [12, Theorem I.3.6]). Note that if $\tilde{u} \in \mathcal{O}^*$ is an element of finite order, then ord($\tilde{u}$) $\in \{1 \leq n \leq 6\} \cup \{12\}$.

There are strong restrictions on $F$ and $B$ if one of the groups $C_5, C_{12}, A_5$ may occur. More explicitly,

$$C_5 \subset \mathcal{O}^* \iff F = \mathbb{Q}(\sqrt{5}) \text{ and } \mathbb{Q}(\zeta_{10}) \subset B,$$

$$C_{12} \subset \mathcal{O}^* \implies F = \mathbb{Q}(\sqrt{3}) \text{ and } \mathbb{Q}(\zeta_{12}) \subset B,$$

$$A_5 \text{ occurs } \iff F = \mathbb{Q}(\sqrt{5}) \text{ and } B = B_{\infty_1,\infty_2}.$$
In fact, when \( d \in \{2, 3, 5\} \), there exists an \( O_F \)-order with non-cyclic reduced unit group if and only if \( B \cong B_{\infty, \infty_2} \), which has already been treated in Section 3. Thus, we may consider only the following list for square-free \( d \geq 6 \):

\[
G := \{C_1, C_2, C_3, C_4, C_6, D_2, D_3, D_4, D_6, A_4, S_4\}.
\]

For non-cyclic groups in \( G \), one has the following inclusions:

\[
D_2 \subset D_4 \subset S_4, \quad D_2 \subset A_4 \subset S_4, \quad D_3 \subset \{S_4, D_6\}, \quad \{D_2, D_3\} \subset D_6.
\]

The proof of Theorem 4 is divided into the following steps:

1. Make finer classification of the possibly non-cyclic groups \( G \) that may occur (See Definition 10).
2. Determine explicitly \( t(G) \) for non-cyclic groups \( G \).
3. Determine \( h(G) \) from \( t(G) \) for non-cyclic groups \( G \).
4. Use the relation of global and local optimal embeddings. This step produces linear relations roughly of the form

\[
\sum_{C_n \subset G} a_n(G) h(G) = \sum_R h(R) \prod_p m_p(R), \quad \forall n \geq 2,
\]

where \( R \) runs through certain \( O_F \)-orders in CM extensions of \( F \) and \( m_p(R) \) denotes the number of conjugacy classes of local optimal embeddings from \( R \) to \( \mathcal{O} \) at \( p \). Then we solve recursively for \( h(G) \) starting from the maximal groups to smaller groups. This step produces formulas for \( h(G) \) except for \( G = C_1 \).
5. For \( G = C_1 \), the relation (4.3) reduces to

\[
\sum_G h(G) = h(\mathcal{O}).
\]

We then use Vignéras's explicit formula for \( h(\mathcal{O}) \) to obtain \( h(C_1) \).

The remaining part of this note will illustrate the steps of the proof.

5. OCCURRENCE OF NON-CYCLIC GROUPS

In this section, we let \( F = \mathbb{Q}(\sqrt{d}) \) with \( d \geq 6 \), and let \( B, \mathcal{O} \) be the same as in the previous section. Denote by \( \varepsilon \) the fundamental unit of \( O_F \). Put

\[
S := \begin{cases} 
\{1\} & \text{if } N_{F/\mathbb{Q}}(\varepsilon) = -1; \\
\{1, \varepsilon\} & \text{otherwise.} 
\end{cases}
\]

For any non-trivial element \( \tilde{u} \in \mathcal{O}^\times = \mathcal{O}^\times / \mathfrak{O}_F^\times \), denote by \( K_{\tilde{u}} := F[u] \) and \( O_F[\tilde{u}] := O_F[u] \), respectively, the field and order generated by any lifting \( u \in \mathcal{O} \) of \( \tilde{u} \). Clearly, \( K_{\tilde{u}} \) and \( O_F[\tilde{u}] \) are independent of the choice of \( u \). One can always choose a representative \( u \in \mathcal{O}^\times \) so that \( N_F(\varepsilon) \in S \). Such a choice of representative is unique up to sign. For any CM extension \( K \) with maximal totally real subfield \( F \), the Hasse index is defined to be \( Q_{K/F} := [O_K^\times : \mu_K \mathfrak{O}_F^\times] \in \{1, 2\} \), where \( \mu_K \) is the group of roots of unity in \( K \).

Definition 9. We say a CM extension \( K/F \) is of type I (resp. of type II) if \( Q_{K/F} = 1 \) (resp. \( Q_{K/F} = 2 \)).
UNIT GROUPS

If $K/F$ is of type I, then $O_K^\times/O_F^\times \simeq \mu_K/\{\pm 1\}$, otherwise, $O_K^\times/O_F^\times$ is a cyclic group of order $|\mu_K|$. Thus, if $\mu_K = \{\pm 1\}$, then $[O_K^\times : O_F^\times] \in \{1, 2\}$ and

$$K/F \text{ is of type I } \iff [O_K^\times : O_F^\times] = 1.$$  

We list some properties:

(i) If $N_{F/\mathbb{Q}}(\varepsilon) = -1$, then ord($\bar{u}$) $\in \{2, 3\}$, otherwise, ord($\bar{u}$) $\in \{2, 3, 4, 6\}$.

(ii) If ord($\bar{u}$) = 4 then $N_{F/\mathbb{Q}}(\varepsilon) = 1$, $K_\varepsilon = F(\sqrt{-1})$ and $F(\sqrt{-1})/F$ is of type II. The CM extension $F(\sqrt{-1})/F$ is of type II if and only if $2\varepsilon \in (F^\times)^2$ (See [2, Lemma 2]). In particular,

$$2\varepsilon \in (F^\times)^2 \implies O_{F(\sqrt{-1})}^\times/O_F^\times \simeq \mathbb{Z}/4\mathbb{Z} \text{ and } N_{F/\mathbb{Q}}(\varepsilon) = 1.$$  

(iii) If ord($\bar{u}$) = 6 then $N_{F/\mathbb{Q}}(\varepsilon) = 1$, $K_\varepsilon = F(\sqrt{-3})$ and $F(\sqrt{-3})/F$ is of type II. The CM extension $F(\sqrt{-3})/F$ is of type II if and only if $3\varepsilon \in (F^\times)^2$ (ibid.). In particular,

$$3\varepsilon \in (F^\times)^2 \implies O_{F(\sqrt{-3})}^\times/O_F^\times \simeq \mathbb{Z}/6\mathbb{Z} \text{ and } N_{F/\mathbb{Q}}(\varepsilon) = 1.$$  

(iv) If $N_{F/\mathbb{Q}}(\varepsilon) = -1$, then by (ii) and (iii) both $F(\sqrt{-1})/F$ and $F(\sqrt{-3})/F$ are of type I. In this case ord($\bar{u}$) = 2, 3, then there is no element in $O^\times$ of order 4 nor 6, and hence $O^\times$ cannot be isomorphic to $S_4$ nor $D_6$.

(v) If $N_{F/\mathbb{Q}}(\varepsilon) = 1$, and $K/F$ is a CM-extension of type II with $\mu_K = \{\pm 1\}$ (so $[O_K^\times : O_F^\times] = 2$), then $K = F(\sqrt{-\varepsilon})$ and $3\varepsilon \notin F^\times^2$. Thus, if $K/F$ is a CM-extension with $[O_K^\times : O_F^\times] > 1$, then

$$(5.1) \quad K = \begin{cases} F(\sqrt{-1}) \text{ or } F(\sqrt{-3}) & \text{ if } N_{F/\mathbb{Q}}(\varepsilon) = -1; \\ F(\sqrt{-1}), F(\sqrt{-3}) & \text{ if } N_{F/\mathbb{Q}}(\varepsilon) = 1. \end{cases}$$  

(vi) Note that $2\varepsilon$ and $3\varepsilon$ cannot be perfect squares in $\mathbb{Q}(\sqrt{d})$ simultaneously unless $d = 6$, in which case it does happen.

(vii) Let $O^1$ be the subgroup of $O^\times$ consisting of elements of reduced norm 1. Then $[O^\times : O^1/\{\pm 1\}] \leq 2$, and the equality holds if and only if $N_{F/\mathbb{Q}}(\varepsilon) = 1$ and there exists $u \in O^\times$ such that $\text{Nr}(u) = \varepsilon$. Since $A_4$ has no subgroup of index 2, if $O^\times \simeq A_4$ for a maximal order $O$, then $O^\times = O_F^\times O^1$.

According to the above discussion, we list possible values of ord($\bar{u}$) and possible reduced unit groups that may occur.

<table>
<thead>
<tr>
<th>$F = \mathbb{Q}(\sqrt{d})$, $d \neq 2, 3, 5$</th>
<th>ord($\bar{u}$)</th>
<th>$O^\times$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2\varepsilon \in F^\times^2$</td>
<td>2, 3, 4</td>
<td>$C_2, C_3, C_4, D_2, D_3, D_4, A_4, S_4$</td>
</tr>
<tr>
<td>$3\varepsilon \in F^\times^2$</td>
<td>2, 3, 6</td>
<td>$C_2, C_3, C_6, D_2, D_3, D_6, A_4$</td>
</tr>
<tr>
<td>${2\varepsilon, 3\varepsilon} \cap F^\times^2 = \emptyset$</td>
<td>2, 3</td>
<td>$C_2, C_3, D_2, D_3, A_4$</td>
</tr>
</tbody>
</table>

If $d = p$ is an odd prime, then

- $N_{F/\mathbb{Q}}(\varepsilon) = -1$ if $p \equiv 1 \mod 4$, so $\{2\varepsilon, 3\varepsilon\} \cap F^\times^2 = \emptyset$;
- $2\varepsilon \in (F^\times)^2$ if $p \equiv 3 \mod 4$.

Let $d = 6$ and $B = B_{\infty_1, \infty_2}$. We know that $h(\mathbb{Q}(\sqrt{6})) = 1$ and $h(O) = 3$ for any maximal $O_F$-order $O$ in $B$. By (ii) and (iii), we have $h(D_6) = 1$ and at least one of $D_4$ and $S_4$ occurs. On the other hand, $\zeta_F(-1) = 1/2$, so $\text{Mass}(O) = 1/4$. The only possibility is $1/|S_4| + 1/|D_4| + 1/|D_6| = 1/4$. Therefore, $h(D_4) = h(D_6) = h(S_4) = 1$. On the other hand, if $B \neq B_{\infty_1, \infty_2}$, then $O^\times$ is cyclic for every maximal order $O$. 


in $B/\mathbb{Q}(\sqrt{6})$ (See Proposition 12).

Below we list the conditions on $F$ for which order $\text{ord}(\bar{u})$ may occur, and their characteristic polynomials $P_{\bar{u}}(x)$. If $2\varepsilon \in F^{\times 2}$, then we write $\varepsilon = 2\vartheta^2$ with $\vartheta \in F$, and if $3\varepsilon \in F^{\times 2}$, we write $\varepsilon = 3\varsigma^2$ with $\varsigma \in F$.

<table>
<thead>
<tr>
<th>$\text{ord}(\bar{u})$</th>
<th>Conditions</th>
<th>$P_{\bar{u}}(x) \in F[x]$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>$\text{Nr}(u) = 1$</td>
<td>$x^2 + 1$</td>
</tr>
<tr>
<td></td>
<td>$N_{F/\mathbb{Q}}(\varepsilon) = 1$, $\text{Nr}(u) = \varepsilon$</td>
<td>$x^2 + \varepsilon$</td>
</tr>
<tr>
<td>3</td>
<td>$N_{F/\mathbb{Q}}(\varepsilon) = 1$</td>
<td>$x^2 \pm x + 1$</td>
</tr>
<tr>
<td>4</td>
<td>$N_{F/\mathbb{Q}}(\varepsilon) = 1$, $2\varepsilon \in F^{\times 2}$</td>
<td>$x^2 \pm 2\vartheta x + \varepsilon$</td>
</tr>
<tr>
<td>6</td>
<td>$N_{F/\mathbb{Q}}(\varepsilon) = 1$, $3\varepsilon \in F^{\times 2}$</td>
<td>$x^2 \pm 3\varsigma x + \varepsilon$</td>
</tr>
</tbody>
</table>

Remark that

- for each $r \in \{3, 4, 6\}$, the representatives of elements of order $r$ are $B^\times$-conjugate up to sign;
- there are two different kinds of units of order 2 if $N_{F/\mathbb{Q}}(\varepsilon) = 1$.

6. MINIMAL $G$-ORDERS

In this section, let $F = \mathbb{Q}(\sqrt{d})$ be a real quadratic field with a square free $d \geq 6$ and $B$ be a totally definite quaternion $F$-algebra.

**Definition 10.** Let $G$ be a non-cyclic group in $\mathcal{G}$ in (4.1). An $O_F$-order $\mathcal{O}$ in $B$ is called a minimal $G$-order if

- $\mathcal{O}^* = \mathcal{O}^\times / O_F^\times$ contains a subgroup isomorphic to $G$;
- $\mathcal{O}$ is generated over $O_F$ by the representatives of elements of $G$.

If $G = D_2$ or $D_3$, we say $\mathcal{O}$ is of type $I$ if every element of order 2 in $G$ has minimal polynomial $x^2 + 1$. Otherwise, we say $\mathcal{O}$ is of type $II$.

If $\mathcal{O}$ is a maximal order with $\mathcal{O}^* \supseteq G$, then $\mathcal{O}$ contains a minimal $G$-order. For $G = D_4, D_6$ or $S_4$, there always exist elements of order 2 in $G$ with minimal polynomial $x^2 + \varepsilon$. On the other hand, if $G = A_4$ then every element of order 2 in $G$ has minimal polynomial $x^2 + 1$ (See property (vii) in Section 5).

**Theorem 11** (Uniqueness of minimal $G$-orders). Fix a non-cyclic group $G$ and a type ($I$ or $II$ if necessary). If a minimal $G$-order of that type exists, then it is unique up to $B^\times$-conjugation.

Below we list the conditions on $F$ and $B$ in order for a minimal $G$-order to occur and explicit representatives of minimal $G$-orders.
Here $\xi = (1 + i + j + k)/2 \in (\frac{-1,-1}{F})$ and $\mathfrak{d}(\mathcal{O})$ is the (reduced) discriminant of $\mathcal{O}$.

From this table, we can draw a few conclusions:

(i) We have $t(S_4) \in \{0,1\}$, and $t(S_4) = 1$ if and only if $2\varepsilon \in F^{\times 2}$ and $B \simeq (\frac{-1,-1}{F}) \simeq B_{\infty_1,\infty_2}$.

(ii) We have $t(D_6) \in \{0,1\}$, and $t(D_6) = 1$ if and only if $3\varepsilon \in F^{\times 2}$ and $B \simeq (\frac{-1,-3}{F}) \simeq B_{\infty_1,\infty_2}$.

(iii) If $t(D_4) \geq 1$, then $2\varepsilon \in F^{\times 2}$ and $B \simeq (\frac{-1,-1}{F}) \simeq B_{\infty_1,\infty_2}$.

(iv) If $t(A_4) \geq 1$, then $B \simeq (\frac{-1,-1}{F})$. Conversely, if $B \simeq (\frac{-1,-1}{F})$ and 2 splits in $F$, then any minimal $A_4$-order is maximal and $t(A_4) = 1$.

(v) If $B \simeq (\frac{-1,-3}{F})$ and 3 splits in $F$, then any minimal $D_3^{II}$-order is maximal and $t(D_3^{II}) = 1$.

(vi) If $N_{F/\mathbb{Q}}(\varepsilon) = 1$ and $B \simeq (\frac{-\varepsilon,-3}{F})$ has reduced discriminant $3\mathcal{O}_F$, then any minimal $D_3^{II}$-order is maximal and $t(D_3^{II}) = 1$.

(vii) If $B \not\simeq B_{\infty_1,\infty_2}$ and neither 2 nor 3 splits in $F$, then $t(G) = 0$ for any non-cyclic group $G$. This applies to the case, for example, $F = \mathbb{Q}(\sqrt{6})$.

(viii) If $N_{F/\mathbb{Q}}(\varepsilon) = 1$, then the quaternion $F$-algebra $(\frac{-\varepsilon,-1}{F})$ (resp. $(\frac{-\varepsilon,-3}{F})$) is unramified at all finite places $v$ of $F$ with $v \nmid 2$ (resp. with $v \nmid 3$). This follows from results of $\mathfrak{d}(\mathcal{O})$.

**Proposition 12.** Let $F$ be a real quadratic field and $B$ a totally definite quaternion $F$-algebra. Then any reduced unit group of an order in $B$ is cyclic except when

$$B \in \left\{ \left( \frac{-1,-1}{F} \right), \left( \frac{-1,-3}{F} \right) \right\} \text{ if } N_{F/\mathbb{Q}}(\varepsilon) = -1, \text{ or}$$

$$B \in \left\{ \left( \frac{-1,-1}{F} \right), \left( \frac{-1,-3}{F} \right), \left( \frac{-\varepsilon,-1}{F} \right), \left( \frac{-\varepsilon,-3}{F} \right) \right\} \text{ if } N_{F/\mathbb{Q}}(\varepsilon) = 1.$$
7. COMPUTATION OF \( t(G) \) FOR NON-CYCLIC GROUPS \( G \)

In this section, \( F = \mathbb{Q}(\sqrt{d}) \) with \( d \geq 7 \) and \( B \) is a totally definite quaternion \( F \)-algebra. For a minimal \( G \)-order \( \mathcal{O} \) with a noncyclic \( G \in \mathcal{G} \), we write \( \aleph(\mathcal{O}) \) for the number of maximal orders containing \( \mathcal{O} \), and \( \supset(\mathcal{O}) \) for the number of conjugacy classes of maximal orders containing \( \mathcal{O} \). Clearly, \( \supset(\mathcal{O}) \leq \aleph(\mathcal{O}) \).

**Proposition 14.** We have

\[
(7.1) \quad t(D_6) = \begin{cases} 
1 & \text{if } B = (\frac{-1,-3}{F}) \text{ and } 3\varepsilon \in F^{\times^2}; \\
0 & \text{otherwise}; 
\end{cases}
\]

\[
(7.2) \quad t(S_4) = t(D_4) = \begin{cases} 
1 & \text{if } B = (\frac{-1,-1}{F}) \text{ and } 2\varepsilon \in F^{\times^2}; \\
0 & \text{otherwise}; 
\end{cases}
\]

\[
(7.3) \quad t(A_4) = \begin{cases} 
1 & \text{if } B = (\frac{-1}{F}) \text{ and } 2\varepsilon \not\in F^{\times^2}; \\
0 & \text{otherwise}. 
\end{cases}
\]

Note that \( 2\varepsilon \in (F^{\times})^2 \) implies that 2 is ramified in \( F \). Thus, \( t(D_4) = t(S_4) = 0 \) if 2 is unramified in \( F \). Similarly, if \( 3 \nmid d \), then \( 3\varepsilon \not\in (F^{\times})^2 \), and hence \( t(D_6) = 0 \).

**Proposition 15.** We have

\[
(7.4) \quad t(D_2^I) = \begin{cases} 
1 & \text{if } B = (\frac{-1,-1}{F}) \text{, } (\frac{F}{2}) = 0 \text{ and } 2\varepsilon \not\in F^{\times^2}; \\
0 & \text{otherwise.} 
\end{cases}
\]

Here the Artin symbol \( (\frac{F}{2}) = 0 \) if and only if 2 is ramified in \( F \).

The computation of \( t(D_2^{II}) \) requires much detailed case studies. By the table in Section 6, \( t(D_2^{II}) = 0 \) if \( B \) is not isomorphic to \( (\frac{-1,-\varepsilon}{F}) \). Now let \( B = (\frac{-1,-\varepsilon}{F}) \) and \( \mathcal{O}_2^{II} \) be the minimal \( D_2^{II} \)-order in the table of Section 6, whence we assume that \( N_{F/\mathbb{Q}}(\varepsilon) = 1 \). One can show that if \( d \equiv 1 \pmod{8} \) then \( \varepsilon = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}] \) with \( a \) odd.

**Lemma 16.** Suppose that \( N_{F/\mathbb{Q}}(\varepsilon) = 1 \). Then \( B = (\frac{-1,-\varepsilon}{F}) \) splits at all finite places of \( F \) except when \( d \equiv 1 \pmod{8} \) and \( \varepsilon = a + b\sqrt{d} \) with \( a \equiv 1 \pmod{4} \). In the exceptional case, \( B \) is ramified at the two dyadic places of \( F \).

We have the following table for \( \aleph(\mathcal{O}_2^{II}) \) and \( \supset(\mathcal{O}_2^{II}) \).

<table>
<thead>
<tr>
<th>( d \geq 7 )</th>
<th>( \varepsilon = a + b\sqrt{d} )</th>
<th>( \aleph(\mathcal{O}_2^{II}) )</th>
<th>( \supset(\mathcal{O}_2^{II}) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( d \equiv 1 \pmod{8} )</td>
<td>( a \equiv 1 \pmod{4} )</td>
<td>1 ( \beta )</td>
<td>1 ( \beta )</td>
</tr>
<tr>
<td>( d \equiv 1 \pmod{8} )</td>
<td>( a \equiv 3 \pmod{4} )</td>
<td>4 ( \beta )</td>
<td>2 ( \beta )</td>
</tr>
<tr>
<td>( d \equiv 5 \pmod{8} )</td>
<td>( a \equiv 1 \pmod{4} )</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>( d \equiv 3 \pmod{4} )</td>
<td>( a ) is even</td>
<td>2 ( \beta )</td>
<td>2 ( \beta )</td>
</tr>
<tr>
<td>otherwise</td>
<td></td>
<td>4 ( \beta )</td>
<td>3 ( \beta )</td>
</tr>
</tbody>
</table>

**Proposition 17.** Suppose that \( d \geq 7 \) and \( B = (\frac{-1,-\varepsilon}{F}) \). Then

\[
(7.5) \quad t(D_2^{II}) + t(D_4) + t(S_4) + t(D_6) = \supset(\mathcal{O}_2^{II}).
\]

In most cases, formula (7.5) can be simplified further. The fact that \( 2\varepsilon \) and \( 3\varepsilon \) cannot simultaneously be perfect squares in \( F \) for \( d \geq 7 \) implies that \( t(D_6)(t(S_4) + t(D_4)) = 0 \). For example, if \( d \equiv 1 \pmod{4} \), then \( 2\varepsilon \not\in F^{\times^2} \) and hence \( t(S_4) = 0 \).
\( t(D_4) = 0 \). So in this case \( t(D_2^{II}) + t(D_6) = \mathbb{Z}(O_2^{II}) \). If further \( d \equiv 1 \pmod{8} \) and \( a \equiv 1 \pmod{4} \), then \( t(D_2) = t(D_2^{II}) = 1 \).

Finally we turn to the computation of \( t(D_3^{I}) \) and \( t(D_3^{II}) \).

We first consider the case \( B = \left( \frac{-1,-3}{F} \right) \), which is necessary for \( t(D_3^{I}) \neq 0 \). One can show that the minimal \( S_4 \)-order \( O_{24} \) in the table of Section 6 does not contain any minimal \( D_3 \)-order and the minimal \( D_6 \)-order there contains the minimal \( D_3^{-} \)-order \( O_3^{I} \).

Note that \( O_3^{I} \cong O_{3,\infty} \otimes O_F \), where \( O_{3,\infty} \) is the unique maximal order up to conjugation of the quaternion \( \mathbb{Q} \)-algebra \( B_{3,\infty} = \left( \frac{-1,-3}{\mathbb{Q}} \right) \). If 3 splits in \( F \), then \( B \) is ramified at two places of \( F \) over 3 and \( O_3^{I} \) is maximal. If 3 is ramified in \( F \), then one can show that there is a unique maximal order containing \( O_3^{I} \). If 3 is inert in \( F \), then \( O_3^{I} \) is an Eichler order of prime level \( 3O_F \) and the two maximal over-orders are mutually conjugate. Therefore, we always have \( \mathbb{Z}(O_3^{I}) = 1 \).

**Proposition 18.** There is only one maximal order up to conjugation containing \( O_3^{I} \) and \( t(D_3^{I}) + t(D_6) = 1 \). Thus,

\[
(7.6) \quad t(D_3^{II}) = \begin{cases} 
1 & \text{if } B = \left( \frac{-1,-3}{F} \right) \text{ and } 3 \notin F^{x2}; \\
0 & \text{otherwise.}
\end{cases}
\]

Lastly, suppose that \( N_{F/\mathbb{Q}}(\varepsilon) = 1 \). Let \( B = \left( \frac{-\varepsilon,-3}{F} \right) \) be the minimal \( D_3^{II} \)-order in the table of Section 6. Write \( \varepsilon = \frac{a+b\sqrt{d}}{2} \) with \( a \equiv b \pmod{2} \). If \( d \equiv 1 \pmod{3} \) and \( N_{F/\mathbb{Q}}(\varepsilon) = 1 \), then \( 3 | b \). This is immediately seen by taking both sides of \( a^2 - b^2d = 4 \) modulo 3. We have \( \varepsilon \equiv \pm 1 \pmod{3O_F} \) in this case. Note that \( \left( \frac{\varepsilon}{3} \right) = 0, 1, -1 \) according to \( d \equiv 0, 1, 2 \pmod{3} \).

**Lemma 19.** The quaternion algebra \( B = \left( \frac{-\varepsilon,-3}{F} \right) \) splits at all finite places of \( F \) coprime to 3. If \( d \not\equiv 1 \pmod{3} \), then \( B \) splits at the unique prime of \( F \) above 3 as well. When \( d \equiv 1 \pmod{3} \), \( B \) splits at the two places of \( F \) above 3 if and only if \( \varepsilon \equiv -1 \pmod{3O_F} \).

We list \( \mathbb{N}(O_3^{II}) \) and \( \mathbb{Z}(O_3^{II}) \) in the following table.

<table>
<thead>
<tr>
<th>( d \geq 7 )</th>
<th>( \varepsilon )</th>
<th>( \mathbb{N}(O_3^{II}) )</th>
<th>( \mathbb{Z}(O_3^{II}) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( d \equiv 0 \pmod{3} )</td>
<td>( \varepsilon \equiv 1 \pmod{p} )</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>( \varepsilon \equiv -1 \pmod{p} )</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>( d \equiv 1 \pmod{3} )</td>
<td>( \varepsilon \equiv 1 \pmod{3O_F} )</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>( \varepsilon \equiv -1 \pmod{3O_F} )</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>( d \equiv 2 \pmod{3} )</td>
<td></td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

Here \( p = (3,\sqrt{d}) \) denotes the unique prime ideal of \( F \) above 3 when \( 3 | d \).

**Proposition 20.** Suppose that \( d > 6 \) and \( B = \left( \frac{-\varepsilon,-3}{F} \right) \). Then

\[
(7.7) \quad t(D_3^{II}) + t(S_4) + t(D_6) = \mathbb{Z}(O_3^{II}).
\]

As mentioned before, \( t(D_6) = 0 \) in (7.7) when \( d \not\equiv 0 \pmod{3} \). If further \( d \equiv 1 \pmod{3} \) and \( \varepsilon \equiv 1 \pmod{3O_F} \), then \( O_3^{II} \) is maximal in \( B \) and \( t(D_3^{II}) = 1 \).
8. OPTIMAL EMBEDDINGS AND CLASS-TYPE NUMBER RELATIONS

In previous sections we determine the refined type numbers \( t(G) \) for non-cyclic groups \( G \). As described in the previous section, for \( G = D_2 \) or \( D_3 \) one actually needs finer invariants and conditions on \( B \) and \( F \) in order to determine the numbers \( t(G) \) explicitly. The next step is to compute \( h(G) \) for each non-cyclic group \( G \). In this section we discuss a class-and-type number relation in sufficient generality.

Let \( F \) be a number field with the ring of integers \( \mathcal{O}_F \). Let \( B \) be a division quaternion \( F \)-algebra, and \( \mathcal{O}_F \) the group of principal fractional \( \mathcal{O}_F \)-ideals, identified with a subgroup of \( \mathcal{P}(\mathcal{O}) \) via \( x\mathcal{O}_F \mapsto x\mathcal{O}, \forall x \in F^\times \).

Fix a maximal order \( \mathcal{O}_0 \) in \( B \). There is a surjective map of finite sets

\begin{equation}
\Upsilon : \text{Cl}(\mathcal{O}_0) \to \text{Tp}(B), \quad [I] \mapsto \{\mathcal{O}_I(I) := D^\times \text{-conjugacy class of } \mathcal{O}_I(I)\}.
\end{equation}

The cardinality of each fiber of \( \Upsilon \) may be calculated as follows. For each maximal order \( \mathcal{O} \), then there is bijection [12, Lemma III.5.6]

\begin{equation}
\Upsilon^{-1}([\mathcal{O}]) \leftrightarrow \mathcal{I}(\mathcal{O})/\mathcal{P}(\mathcal{O}).
\end{equation}

The quotient group \( \mathcal{I}(\mathcal{O})/\mathcal{P}(\mathcal{O}) \) sits in a short exact sequence

\begin{equation}
1 \to \mathcal{N}(\mathcal{O})/(F^\times \mathcal{O}^\times) \to \text{Pic}(\mathcal{O}) \to \mathcal{I}(\mathcal{O})/\mathcal{P}(\mathcal{O}) \to 1.
\end{equation}

Here \( \text{Pic}(\mathcal{O}) \) denotes the Picard group \( \mathcal{I}(\mathcal{O})/\mathcal{P}(\mathcal{O}) \), whose cardinality can be calculated using the short exact sequence

\begin{equation}
1 \to \text{Cl}(\mathcal{O}_F) \to \text{Pic}(\mathcal{O}) \to \prod_{p|\mathfrak{d}(B)} (\mathbb{Z}/2\mathbb{Z}) \to 0.
\end{equation}

It follows that

\begin{equation}
|\Upsilon^{-1}([\mathcal{O}])| = \frac{2^{\omega(B)}h(F)}{\mathcal{N}(\mathcal{O})/(F^\times \mathcal{O}^\times)},
\end{equation}

where \( \omega(B) \) denotes the number of finite primes of \( F \) that are ramified in \( B \).

Let \( \mathcal{O}_1, \ldots, \mathcal{O}_{t(G)} \) be representatives for maximal orders with non-cyclic reduced unit group \( G \). Then by (8.5), one gets

\begin{equation}
h(G) = \sum_{i=1}^{t(G)} \frac{2^{\omega(B)}h(F)}{\mathcal{N}(\mathcal{O}_i)/(F^\times \mathcal{O}_i^\times)}.
\end{equation}

Lastly, we describe the strategy for computing \( h(C_n) \). Suppose further that \( B \) is a totally definite quaternion \( F \)-algebra, and \( \mathcal{O} \) is an \( O_F \)-order in \( B \). For an \( O_F \)-order \( R \) inside a CM-extension \( K/F \), we write \( \text{Emb}(R, \mathcal{O}) \) for the finite set of optimal \( O_F \)-embeddings of \( R \) into \( \mathcal{O} \). In other words,

\[ \text{Emb}(R, \mathcal{O}) := \{ \varphi \in \text{Hom}_F(K, B) \mid \varphi(K) \cap \mathcal{O} = \varphi(R) \}. \]

The group \( \mathcal{O}^\times \) acts on \( \text{Emb}(R, \mathcal{O}) \) from the right by \( \varphi \mapsto u^{-1}\varphi u \) for all \( \varphi \in \text{Emb}(R, \mathcal{O}) \) and \( u \in \mathcal{O}^\times \). We denote \( m(R, \mathcal{O}, \mathcal{O}^\times) := |\text{Emb}(R, \mathcal{O})/\mathcal{O}^\times| \). For each
nonzero prime ideal \( p \) of \( O_F \), we set \( m_p(R) := m(R_p, O_p, O_p^\times) \). Let \( h = h(O) \), and \( I_1, \ldots, I_h \) be a complete set of representatives of the right ideal class \( \text{Cl}(O) \). Define \( O_i := O_l(I_i) \) for each \( 1 \leq i \leq h \). By [12, Theorem 5.11, p. 92],

\[
\sum_{i=1}^{h} m(R, O_i, O_i^\times) = h(R) \prod_p m_p(R),
\]

where the product on the right hand side runs over all nonzero prime ideals of \( O_F \).

A priori, Theorem 5.11 of [12] is stated for Eichler orders, but it applies in much more generality. See [14, Lemma 3.2] and [15, Lemma 3.2.1]. When \( O = \mathbb{O} \) is maximal, we have

\[
m_p(R) := \begin{cases} 1 - \left( \frac{R}{p} \right) & \text{if } p \mid \mathfrak{d}(B), \\ 1 & \text{otherwise,} \end{cases}
\]

where \( \left( \frac{R}{p} \right) \) is the Eichler symbol [12, p. 94].

Let \( \mathcal{A}_n \) be the finite set of \( O_F \)-orders \( R \) in CM-extension of \( F \) such that \( R^\times / O_F^\times \simeq C_n \). We also define two subsets of \( \text{Tp}(B) \):

\[
\text{Tp}^o(B) := \{ [O] \in \text{Tp}(B) \mid O^\star \text{ is cyclic} \}, \quad \text{and} \quad \text{Tp}^b(B) := \text{Tp}(B) - \text{Tp}^o(B).
\]

If \( [O_i] \in \text{Tp}^o(B) \), then \( O_i^\star \simeq C_n \) if and only if \( \text{Emb}(R, O_i) \neq \emptyset \) for some \( R \in \mathcal{A}_n \). When the latter condition holds, such an order \( R \) is uniquely determined, and \( m(R, O_i, O_i^\times) = 2 \). For each fixed \( R \in \mathcal{A}_n \), let

\[
h(C_n, R) = h(B, C_n, R) := \# \{ [I] \in \text{Cl}(O_0) \mid O_l(I)^\star \simeq C_n, \text{ and } \text{Emb}(R, O_l(I)) \neq \emptyset \}.
\]

Then we have

\[
h(C_n) = \sum_{R \in \mathcal{A}_n} h(C_n, R).
\]

Combining (8.6) and (8.7), we obtain

\[
2^{\omega(B)} h(F) \sum_{[O] \in \text{Tp}^b(B)} \frac{m(R, O, O^\times)}{|N(O)/(F \times O^\times)|} + 2h(C_n, R) = h(R) \prod_p m_p(R).
\]

It is a calculation intensive process to list \( N(O) \) for each \( [O] \in \text{Tp}^b(B) \). Once this is completed, it then reduces to compute the numbers of global optimal embeddings \( m(R, O, O^\times) \) for all \( R \in \mathcal{A}_n \) and \( [O] \in \text{Tp}^b(B) \), which is comparably much more manageable.

**Acknowledgements:** The present notes grow from the materials of the talks given by J. Xue in the NCTS-POSTECH PMI Joint workshop in Number Theory, held in December 27-29, 2017 at Taipei, and by C.-F. Yu in the RIMS Workshop “Analytic and Arithmetic Theory of Automorphic Forms” held in January 15-19, 2018. We would like to thank the organizers of the workshops for the opportunities to speak. C.-F. Yu would like to thank Professors Tomoyoshi Ibukiyama and Akio Tamagawa for their invitation to RIMS. J. Xue and Q. Li would like to thank the Institute of Mathematics, Academia Sinica and the NCTS for their hospitality during our visit in the Fall of 2017.
REFERENCES


(Li) School of Mathematics and Statistics, Wuhan University, Luojiashan, Wuhan, Hubei, 430072, P.R. China.
E-mail address: qun-li@whu.edu.cn

(Xue) Collaborative Innovation Centre of Mathematics, School of Mathematics and Statistics, Wuhan University, Luojiashan, Wuhan, Hubei, 430072, P.R. China.

(Yu) Institute of Mathematics, Academia Sinica, Astronomy-Mathematics Building, No. 1, Sec. 4, Roosevelt Road. Taipei 10617, TAIWAN.
E-mail address: chiafu@math.sinica.edu.tw

(Yu) National Center for Theoretical Sciences, Astronomy-Mathematics Building, No. 1, Sec. 4, Roosevelt Road. Taipei 10617, TAIWAN.
E-mail address: chiafu@math.sinica.edu.tw