UNIT GROUPS OF MAXIMAL ORDERS IN TOTALLY DEFINITE QUATERNION ALGEBRAS OVER REAL QUADRATIC FIELDS

QUN LI, JIANGWEI XUE, AND CHIA-FU YU

Abstract. We study a form of refined class number formula (resp. type number formula) for maximal orders in totally definite quaternion algebras over real quadratic fields, by taking into consideration the automorphism groups of right ideal classes (resp. unit groups of maximal orders). For each finite noncyclic group $G$, we give an explicit formula for the number of conjugacy classes of maximal orders whose unit groups modulo center are isomorphic to $G$, and write down a representative for each conjugacy class. This leads to a complete recipe (even explicit formulas in special cases) for the refined class number formula for all finite groups. As an application, we prove the existence of superspecial abelian surfaces whose endomorphism algebras coincide with $\mathbb{Q}(\sqrt{p})$ in all positive characteristic $p \not\equiv 1 \pmod{24}$.

Contents

1. Introduction ...................................................... 2
2. Preliminaries on orders in quaternion algebras .................. 6
3. General strategy .................................................. 11
4. Minimal $G$-orders ............................................... 13
5. Maximal orders with non-cyclic reduced unit groups: part I .... 21
6. Maximal orders with non-cyclic reduced unit groups: part II ..... 25
7. Quadratic $O_F$-orders in CM-fields ............................ 33
   7.1. Orders in $F(\sqrt{-1})$ and $F(\sqrt{-3})$ ..................... 33
   7.2. Orders in $F(\sqrt{-\epsilon})$ .................................. 35
8. Calculations for $F = \mathbb{Q}(\sqrt{p})$ and $D = D_{\infty_1, \infty_2}$ ....... 38
   8.1. Case $p \in \{2, 3, 5\}$ ....................................... 38
   8.2. Case $p \equiv 3 \pmod{4}$ and $p > 3$ .......................... 39
9. Superspecial abelian surfaces ..................................... 40
   9.1. The first application ......................................... 41
   9.2. Pop’s result on embedding problems ......................... 41
   9.3. The second application ..................................... 42
Acknowledgements .................................................. 43
References ......................................................... 43

Date: July 13, 2018.
2010 Mathematics Subject Classification. 11R52, 11R29, 11G10.
Key words and phrases. quaternion orders, unit groups, superspecial abelian surfaces, class number formula.
1. Introduction

Let $F$ be a totally real number field with ring of integers $O_F$, and $D$ a totally definite quaternion $F$-algebra, that is, $D \otimes_{F, \sigma} \mathbb{R}$ is isomorphic to the Hamilton quaternion algebra $\mathbb{H}$ for every embedding $\sigma : F \hookrightarrow \mathbb{R}$. Fix a maximal order $\mathcal{O}$ in $D$. The class number $h(\mathcal{O})$, by definition, is the cardinality of the finite set $\text{Cl}(\mathcal{O})$ of right ideal classes of $\mathcal{O}$. It depends only on $D$ and is also denoted by $h(D)$ and called the class number of $D$. Similarly, the type number $t(D)$ is the cardinality of the finite set $\text{Tp}(D)$ of all $D^\times$-conjugacy classes of maximal $O_F$-orders of $D$.

For any $O_F$-order $\mathcal{O}$ in $D$, the quotient group $\mathcal{O}^* := \mathcal{O}^\times / O_F^\times$ of the unit group $\mathcal{O}^\times$ by $O_F^\times$ is finite by [40, Theorem V.1.2] and called the reduced unit group of $\mathcal{O}$. For a right ideal $I$ of $\mathcal{O}$, the reduced automorphism group of $I$ is defined to be $\mathcal{O}_I(I)^*$, where $\mathcal{O}_I(I) := \{ x \in D \mid xI \subseteq I \}$ is the left ideal of $I$. The reduced unit group $\mathcal{O}^*$ can easily be regarded as a finite subgroup of $SO_3(\mathbb{R})$ (see Subsection 3.1). By the well-known classification of finite subgroups of $SO_3(\mathbb{R})$, $\mathcal{O}^*$ is isomorphic to either a cyclic group $C_n$, of order $n$, a dihedral group $D_n$, of order $2n$, or one of the groups $A_4, S_4$ and $A_5$ (see [40, Theorem I.3.6]). For any group $G$ in this list, we define

\begin{align}
\text{Cl}(D, G) &:= \{ \mathcal{O}' \in \text{Cl}(\mathcal{O}) \mid \mathcal{O}_I(I)^* \simeq G \}, \quad h(D, G) := |\text{Cl}(D, G)|, \\
\text{Tp}(D, G) &:= \{ [\mathcal{O}'] \in \text{Tp}(\mathcal{O}) \mid \mathcal{O}'^* \simeq G \}, \quad t(D, G) := |\text{Tp}(D, G)|,
\end{align}

where $[\mathcal{O}]$ denotes the ideal class of $\mathcal{O}$, and $[\mathcal{O}']$ denotes the $D^\times$-conjugacy class of the maximal order $\mathcal{O}'$. The quantity $h(D, G)$ (resp. $t(D, G)$) can be regarded as a refined class number (resp. refined type number) of $D$. Similar as before, $h(D, G)$ does not depend on the choice of the maximal order $\mathcal{O}$. If $D$ is clear from the context, then we drop it from the notation and write $h(G)$ and $t(G)$ instead.

The main tool for studying class numbers and type numbers is Eichler’s trace formula ([15, 29], cf. [40]). This has been used to study various arithmetic problems concerning totally definite quaternion algebras including the analogous Gauss problem and the cancellation property by several people [8, 17, 21, 22, 35, 39]. Brzeziński [8] obtains a complete list of all orders (including non-Gorenstein orders) in definite quaternion $\mathbb{Q}$-algebras with class number one. Kirschmer and Voight [22] determine all Eichler $O_F$-orders with class number $\leq 2$. Kirschmer and Lorch [21] determine all Eichler $O_F$-orders with type number $\leq 2$.

Vignéras [38, Theorem 3.1] gives an explicit formula for $h(\mathcal{O})$ (including Eichler orders $\mathcal{O}$) when $F$ is a real quadratic field. Explicit formulas for type numbers, however, are comparably unknown. In [30] Pizer proves a general formula for type numbers, and uses this to deduce an explicit type number formula for Eichler orders in an arbitrary definite quaternion $\mathbb{Q}$-algebra [30]. So far there is no known explicit formula for $t(D)$ in the literature when $F$ is an arbitrary quadratic field. The only case we know are due to Kitaoa [23, 1.12 and 3.1] and Ponomarev [31, Theorem part (c), p. 102] when $F = \mathbb{Q}(\sqrt{p})$ with a prime number $p$, and $D = D_{\infty_1, \infty_2}$ is the totally definite quaternion $F$-algebra unramified at every finite place of $F$. Under the same hypothesis of $D$, we prove the following result for more general totally real fields in [46].

**Proposition 1.1.** Let $D$ be a totally definite quaternion algebra over a totally real number field $F$. Assume $D$ that is unramified at all finite places of $F$ and that $h(F)$
is odd. Then for any finite group $G$ in the list, one has $h(D, G) = h(F)t(D, G)$. In particular, the equality $h(D) = h(F)t(D)$ holds.

Thanks to Vigéras’s explicit formula [38, Theorem 3.1], we obtain an explicit formula for $t(D_{\infty_1, \infty_2})$ when $F$ has odd class number. For a complete list of quadratic fields with odd class numbers, see [11, Corollary 18.4].

The task of this paper is to determine explicitly the refined class number $h(D, G)$ for an arbitrary totally definite $D$ over any real quadratic field $F$. A key step turns out to be determining explicitly $t(D, G)$ for all finite noncyclic $G$. Let $d \in \mathbb{N}$ be the square-free positive integer such that $F = \mathbb{Q}(\sqrt{d})$, and $\varepsilon \in O_F^*$ be the fundamental unit of $F$. The cases $d = 2, 3, 5$ will be treated separately. For $d \geq 6$, the reduced unit group $\mathcal{O}^*$ of any $O_F$-order $\mathcal{O} \subset D$ falls into the following list as shown in Section 4.

\begin{equation}
\mathcal{G} = \{C_1, C_2, C_3, C_4, C_6, D_2, D_2^5, D_3, D_3^5, D_4, D_4, A_4, S_4\}.
\end{equation}

Here the reduced unit groups isomorphic to $D_s$ for $s = 2, 3$ are further distinguished into two different kinds (labeled by $D_2^4$ and $D_2^5$ respectively) according to the reduced norms of certain units (See Definition 4.5). For a noncyclic group $G$ in $\mathcal{G}$, we also introduce in Definition 4.5 the notion of minimal $G$-orders. Essentially, a minimal $G$-order is an $O_F$-order $\mathcal{O}$ in $D$ such that $\mathcal{O}^* \cong G$ and minimal with respect to inclusion. By Lemma 4.7, a minimal $G$-order, if exists, is unique up to $D^\times$-conjugate. Since any maximal order $\mathcal{O}$ with $\mathcal{O}^* \supseteq G$ contains a minimal $G$-order, the calculation of $t(D, G)$ reduces to counting and classifying the maximal orders containing a fixed minimal $G$-order $\mathcal{O}$. We write $\mathcal{R}(\mathcal{O})$ for the number of maximal orders containing $\mathcal{O}$, and $\mathfrak{N}(\mathcal{O})$ for the number of conjugacy classes of maximal orders containing $\mathcal{O}$.

We summarize our main results as the following two theorems. See Sections 5 and 6.

**Theorem 1.2.** Suppose that $d \geq 6$. We have

\begin{align}
t(D_6) &= \begin{cases} 1 & \text{if } D = \left(\frac{-1-\sqrt{-3}}{2}\right) \text{ and } 3\varepsilon \in F^{\times 2}; \\
0 & \text{otherwise}; \end{cases} \\
t(S_4) = t(D_4) &= \begin{cases} 1 & \text{if } D = \left(\frac{-1-\sqrt{-1}}{2}\right) \text{ and } 2\varepsilon \in F^{\times 2}; \\
0 & \text{otherwise}; \end{cases} \\
t(A_4) &= \begin{cases} 1 & \text{if } D = \left(\frac{-1-\sqrt{-3}}{2}\right) \text{ and } 2\varepsilon \in F^{\times 2}; \\
0 & \text{otherwise}; \end{cases} \\
t(D_2^4) &= \begin{cases} 1 & \text{if } D = \left(\frac{-1-\sqrt{-1}}{2}\right) \text{ and } 2\varepsilon \in F^{\times 2}; \\
0 & \text{otherwise}; \end{cases} \\
t(D_3^4) &= \begin{cases} 1 & \text{if } D = \left(\frac{-1-\sqrt{-3}}{2}\right) \text{ and } 3\varepsilon \notin F^{\times 2}; \\
0 & \text{otherwise}. \end{cases}
\end{align}

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

Moreover, for each finite group $G$, if a maximal $G$-order (maximal order with reduced unit group $G$) exists, then we write down explicitly a representative $\mathcal{O}'$ and calculate its normalizer $\mathcal{N}(\mathcal{O}')$. 


Theorem 1.3. Suppose that \( d \geq 6 \). For \( s \in \{2, 3\} \), let \( O'_s^1 \) be a minimal \( D^1_s \)-order, which is unique up to \( D^x \)-conjugation if exists.

If \( N_{F/Q}(\varepsilon) = 1 \) and \( D = \left( \frac{-1 - \sqrt{-s}}{F} \right) \), then
\[
(1.9) \quad t(D_2^1) + t(D_4) + t(S_4) + t(D_6) = \mathbb{Z}(\Theta_2^1).
\]
If \( N_{F/Q}(\varepsilon) = 1 \) and \( D = \left( \frac{-3 - \sqrt{-s}}{F} \right) \), then
\[
(1.10) \quad t(D_2^3) + t(S_4) + t(D_6) = \mathbb{Z}(\Theta_3^1).
\]
The numbers \( \mathbb{Z}(\Theta_s^1) \) for \( s = 2, 3 \) are determined explicitly in Propositions 6.2 and 6.3. In all the remaining cases, minimal \( D^1_s \)-orders do not exist and \( t(D_s^1) = 0 \).

Moreover, if maximal \( D^1_s \)-orders exist, we write down a representative \( \mathbb{O}' \) in each \( D^x \)-conjugacy class and calculate its normalizer \( N(\mathbb{O}') \).

By Theorems 1.2 and 1.3, we can determine an explicit formula for \( h(G) \) for each noncyclic \( G \in \mathcal{G} \) by formula (3.11).

We now describe the strategy for computing \( h(C_n) \). Let \( \mathcal{B}_n \) be the finite set of \( O_F \)-orders \( B \) in some CM-extension of \( F \) such that \( B^x/O_F^x \simeq C_n \). We divide the type set \( Tp(D) \) into two parts:
\[
Tp^s(D) := \{ [\mathbb{O}'] \in Tp(D) \mid \mathbb{O}'^* \text{ is cyclic} \}, \quad \text{and} \quad Tp^\circ(D) := Tp(D) - Tp^s(D).
\]
For each \( B \in \mathcal{B}_n \), let
\[
h(C_n, B) = h(D, C_n, B) := \# \{ [I] \in Cl(\mathbb{O}) \mid \mathbb{O}_I^* \simeq C_n, \ \text{and} \ \text{Emb}(B, \mathbb{O}_I) \neq \emptyset \},
\]
where \( \text{Emb}(B, \mathbb{O}_I) \) is the set of optimal embeddings of \( B \) into \( \mathbb{O}_I \). Then we have
\[
h(C_n) = \sum_{B \in \mathcal{B}_n} h(C_n, B).
\]
Let \( m(B, \mathbb{O}', \mathbb{O}'^x) = |\text{Emb}(B, \mathbb{O}')/\mathbb{O}'^x| \). We then establish the following identity in (3.11):
\[
(1.12) \quad 2^{\omega(D)} h(F) \sum_{[\mathbb{O}'] \in Tp^s(D)} \frac{m(B, \mathbb{O}', \mathbb{O}'^x)}{|N(\mathbb{O}')/(F \times \mathbb{O}'^x)|} + 2h(D, C_n, B) = h(B) \prod_p m_p(B),
\]
where \( \omega(D) \) is the number of finite primes of \( F \) that are ramified in \( D \). Since we have listed all representatives \( \mathbb{O}' \) in \( Tp^\circ(D) \) and calculated their normalizer \( N(\mathbb{O}') \), it then reduces to compute the numbers of global optimal embeddings \( m(B, \mathbb{O}', \mathbb{O}'^x) \) for all \( B \in \mathcal{B}_n \) and \( [\mathbb{O}'] \in Tp^\circ(D) \), which is comparably much more manageable. Thus, we achieve the following goal:

Let \( F = \mathbb{Q}(\sqrt{d}) \) be a real quadratic field and \( D \) be an arbitrary totally definite quaternion \( F \)-algebra. We have a complete recipe for writing down \( h(G) \) for each finite group \( G \).

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 \( D = D_{\infty_1, \infty_2} \) and \( d = p \) is a prime; see Theorems 1.5 and 1.6.

This extends a result of Hashimoto [18] by a different method.
Remark 1.4. We emphasize that same as Vigéras’s explicit formula, our refined formula not just depends on the square-free integer $d$ defining $F$ but also on a good understanding of the fundamental unit $\varepsilon \in O_F^\times$. Note that our recipe for $h(G)$ refines the explicit formula for $h(D)$ given by Vignéras. However, we do not deduce her formula in any different way. Indeed, we use (1.12) to solve for $h(G)$ for each cyclic group $C_n$ with $n \in \{2, 3, 4, 6\}$. This step produces formulas for $h(G)$ except for $G = C_1$. Then we use Vignéras’s formula to deduce the formula for $h(C_1)$.

For the following two theorems, let $p \in \mathbb{N}$ be a prime, $F = \mathbb{Q}(\sqrt{p})$, and $D = D_{\infty_1, \infty_2}$ be the totally definite quaternion $F$-algebra unramified at all the finite places of $F$. For simplicity, denote the class number $h(\mathbb{Q}(\sqrt{m}))$ by $h(m)$ for any square-free $m \in \mathbb{Z}$. We first recall a result of Hashimoto [18].

**Theorem 1.5** (Hashimoto). If $p \equiv 1 \pmod{4}$ and $p > 5$, then

\[
\begin{align*}
\frac{t(C_1)}{2} &= \frac{\zeta_F(-1)}{2} - \frac{h(-p)}{8} - \frac{h(-3p)}{12} - \frac{1}{4} \left(\frac{p}{3}\right) - \frac{1}{4} \left(\frac{2}{p}\right) + \frac{1}{2}, \\
\frac{t(C_2)}{4} &= \frac{h(-p)}{4} + \frac{1}{2} \left(\frac{p}{3}\right) + \frac{1}{4} \left(\frac{2}{p}\right) - \frac{3}{4}, \\
\frac{t(C_3)}{4} &= \frac{h(-3p)}{4} + \frac{1}{2} \left(\frac{p}{3}\right) + \frac{1}{2} \left(\frac{2}{p}\right) - \frac{3}{4}, \\
\frac{t(D_3)}{2} &= \frac{1}{2} \left(1 - \left(\frac{p}{3}\right)\right), \\
\frac{t(A_4)}{2} &= \frac{1}{2} \left(1 - \left(\frac{2}{p}\right)\right).
\end{align*}
\]

We get the results for the remaining primes $p$ as a direct application of our recipe.

**Theorem 1.6.** If $p \equiv 3 \pmod{4}$ and $p > 5$, then

\[
\begin{align*}
\frac{t(C_1)}{2} &= \frac{\zeta_F(-1)}{2} + \left(-7 + 3 \left(\frac{2}{p}\right)\right) \frac{h(-p)}{8} - \frac{h(-2p)}{4} - \frac{h(-3p)}{12} + \frac{3}{2}, \\
\frac{t(C_2)}{2} &= \left(2 - \left(\frac{2}{p}\right)\right) \frac{h(-p)}{2} + \frac{h(-2p)}{2} - \frac{5}{2}, \\
\frac{t(C_3)}{2} &= \frac{h(-3p)}{2} - 1, \\
\frac{t(C_4)}{2} &= \left(3 - \left(\frac{2}{p}\right)\right) \frac{h(-p)}{2} - 1, \\
\frac{t(D_3)}{2} &= 1, \\
\frac{t(D_4)}{4} &= 1, \\
\frac{t(S_4)}{4} &= 1.
\end{align*}
\]

For $p = 2, 3$ and 5, we have

| $p$ | 2 | 3 | 5 |
|-----|---|---|---|
| $t(D)$ | 1 | 2 | 1 |
| $t(G)$ | $t(S_4)$ = 1 | $t(S_4) = t(D_{12}) = 1$ | $t(A_5) = 1$ |

Lastly, we apply the above results to the study of superspecial abelian surfaces [24, Definition 1.7, Ch.1]. Indeed, one of our motivations is to count the number of certain superspecial abelian surfaces with a fixed reduced automorphism.
group $G$. This extends results of our earlier works \cite{12,14,11,15} where we compute explicitly the number of these abelian surfaces over finite fields. We also construct superspecial abelian surfaces $X$ over some field $K$ of characteristic $p$ with endomorphism algebra $\text{End}^0(X) = \mathbb{Q}(\sqrt{p})$, provided that $p \not\equiv 1 \pmod{24}$. The construction makes use of results of Florian Pop \cite{32} on embedding problems for large fields.

This paper is organized as follows. In Section 2 we recall some preliminary results on orders in quaternion algebras. The general strategy for computing $h(G)$ for totally definite quaternion algebras over arbitrary totally real fields is explained in Section 3. We restrict ourselves to the case of quadratic real fields $F = \mathbb{Q}(\sqrt{d})$ starting from Section 4, where we introduce the concept of minimal $G$-orders for finite non-cyclic groups $G$. Section 5 and Section 6 contain the case-by-case study of the maximal orders containing the minimal $G$-orders for each $G$, and the results are summarized in Theorems 1.2 and 1.4 respectively. In Section 7, we classify the quadratic orders with nontrivial reduced unit groups in CM-extensions of $F$. The formulas in Theorem 1.6 are calculated in Section 8. We conclude with two applications to superspecial abelian surfaces in Section 9.

2. Preliminaries on orders in quaternion algebras

Throughout this section, $F$ is either a global field or non-archimedean local field, and $D$ is a quaternion $F$-algebra. The algebra $D$ admits a canonical involution $x \mapsto \overline{x}$ such that $\text{Tr}(x) = x + \overline{x}$ and $\text{Nr}(x) = x\overline{x}$ are respectively the reduced trace and reduced norm of $x \in D$. We always assume that $\text{char}(F) \neq 2$. If $D = \left( \frac{a,b}{F} \right)$ for $a, b \in F^\times$, then $\{1, i, j, k\}$ denotes the standard $F$-basis of $D$ subjecting to the following multiplication rules

\begin{equation}
(2.1) \quad k = ij, \quad i^2 = a, \quad j^2 = b, \quad \text{and} \quad ij = -ji.
\end{equation}

When $F$ is local, $D$ splits over $F$ if and only if the Hilbert symbol $(a,b) = 1$. Often, $D$ is also presented as $K + Kx$, where $K$ is a separable algebra of dimension 2 over $F$, and $x \in D$ is an element such that

\begin{equation}
(2.2) \quad x^2 = c \in F^\times, \quad \text{and} \quad \forall y \in K, \quad xy = y\overline{x}.
\end{equation}

Here $y \mapsto \overline{y}$ is the unique nontrivial $F$-automorphism of $K$. Following \cite[Section I.1]{40}, we denote $D = \{K, c\}$ for the above presentation.

\begin{lemma}
Let $K$ and $x \in D$ be as above. Two elements $z_1, z_2 \in K^\times x \subset D^\times$ with $\text{Nr}(z_1) = \text{Nr}(z_2)$ are conjugate by an element $y \in K^\times$.
\end{lemma}

\begin{proof}
Suppose that $z_1 = tz_2$ with $t \in K$ and $\text{Nr}(t) = N_{K/F}(t) = 1$. By Hilbert Theorem 90, there exists $y \in K^\times$ such that $t = y\overline{y}^{-1}$. We then have

\[ z_1 = tz_2 = y\overline{y}^{-1} \overline{z_2} = yz_2 y^{-1}. \]

If $F$ is local, then we fix a uniformizer $\pi \in F^\times$, and write $\nu: F^\times \to \mathbb{Z}$ for the discrete valuation of $F$. Denote by $O_F, p, t$ respectively the valuation ring, the maximal ideal and the residue field of $\nu$. If $F$ is global, we fix a finite set of places $S$ of $F$ containing all the archimedean ones, and write $O_F$ for the ring of $S$-integers of $F$. Given a nonzero prime ideal $p \subset O_F$, its corresponding discrete valuation is denoted by $\nu_p$, and the $p$-adic completion of $F$ is denoted by $F_p$.

Let $\Lambda$ be an $O_F$-lattice in $D$, i.e. a finitely generated $O_F$-submodule that spans $D$ over $F$. Its dual lattice is defined to be $\Lambda^\vee := \{x \in D \mid \text{Tr}(x\Lambda) \subseteq O_F\}$. An
order in $D$ always refers to an $O_F$-lattice that is at the same time a subring of $D$
containing $O_F$. For an order $O \subset D$, any maximal order $\mathcal{O}$ containing $O$ is a lattice
intermediate to $O \subsetneq O'$. There are only finitely many such lattices. A lattice $\Lambda$ is a
semi-order if $\Lambda \supseteq O_F$ and $\text{Nr}(\Lambda) = O_F$. See [6] Proposition 1.3 for a criterion
for a semi-order to be an order.

The discriminant of an order $O \subset D$ is denoted by $\mathfrak{d}(O)$. If $O$ is a free $O_F$-
module with basis $\{x_1, \ldots, x_4\}$ (e.g. when $F$ is local), then $\mathfrak{d}(O)$ is the square
root of the $O_F$-ideal $\text{det}(\text{Tr}(x_1x_2)_{1 \leq i, j \leq 4})O_F$. If $O' \subsetneq O$ is a suborder of $O$, then
$\mathfrak{d}(O') = \chi(O, O')\mathfrak{d}(O)$, where $\chi(O, O')$ is the ideal index of $O' \subseteq O$ as in [34]
Section III.1. For any finite extension $K/F$, we have $\mathfrak{d}(O \otimes O_K) = \mathfrak{d}(O)O_K$.
An order $O$ is maximal if and only if $\mathfrak{d}(O)$ coincides with the discriminant $\mathfrak{d}(D)$ of
$D$, the product of finite primes of $F$ that are ramified in $D$. As before, $O_p$ denotes
the $p$-adic completion of $O$ at a nonzero prime $p$ when $F$ is global.

2.2. Let $\mathcal{N}(O) = \{x \in D^\times \mid xOx^{-1} = O\}$ be the normalizer of $O$. First suppose
that $F$ is local. Following [7] Section 2, we say that an element $x \in D^\times$ is even (resp. odd) if $\nu(\text{Nr}(x))$ is even (resp. odd). The notion of parity applies to elements
of $D^\times/F^\times$ as well. Clearly, any unit $u \in O^\times$ of an order $O$ is even. Let $O$
be a maximal order in a split quaternion algebra $D \simeq M_2(F)$. Then $O$ is $D^\times$-
conjugate to $M_2(O_F)$, and $\mathcal{N}(O) = F^\times O^\times$ by [10] Section II.2, p.40 (See also [7]
Proposition 2.1). In particular, if $x$ is odd, then $x \notin \mathcal{N}(O)$. If $F$ is global and $p$
is a nonzero prime of $F$, an element $x \in D^\times$ is said to be even (resp. odd) at $p$ if $\nu_p(x)$ is even (resp. odd).

**Lemma 2.3.** Let $\mathcal{O}$ be a maximal order in $D$, and $u \in \mathcal{N}(O)$ an element of the
normalizer of $O$. If $\text{Nr}(u) \in O_F$, then $u \in \mathcal{O}$; if further $\text{Nr}(u) \in O_F^\times$, then $u \in O^\times$.

**Proof.** Suppose that $\text{Nr}(u) \in O_F$. It is enough to show that the two-sided ideal $\mathcal{O}u$
of $O$ is integral. Recall that the nonzero two-sided ideals of $O$ form a free abelian
group generated by the nonzero prime two-sided ideals (See [33] Theorem 22.10). A nonzero prime two-sided ideal $\mathfrak{P}$
is uniquely determined by the intersection $p = \mathfrak{P} \cap O_F$; and $\text{Nr}(\mathfrak{P})$ coincides with either $p$ or $p^2$ by [33] Section I.4. If $\text{Nr}(u) \in O_F$,
then $\mathcal{O}u$ is a product of non-negative powers of two-sided primes ideals, hence
integral. The second part of the lemma follows immediately. \qed

2.4. Given an order $O$ in $D$, we write $\mathfrak{S}(O)$ for the set of maximal orders containing $O$,
and $\mathfrak{N}(O)$ for the cardinality of $\mathfrak{S}(O)$. The quotient group $\mathcal{N}(O)/O^\times$ acts
naturally on $\mathfrak{S}(O)$ by conjugation. If $F$ is global and $p$ is a nonzero prime ideal of
$O_F$, we set $\mathfrak{N}_p(O) := \mathfrak{N}(O_p)$. Note that $O_p$ is maximal (forcing $\mathfrak{N}_p(O) = 1$) for
almost all $p$, and

$$\mathfrak{N}(O) = \prod_p \mathfrak{N}_p(O),$$

(2.3)

where the product runs over all nonzero prime ideals of $O_F$. If further $F$ is a
number field and $p \in \mathbb{N}$ is an integral prime, then we set $\mathfrak{N}_p(O) = \prod_p [pO_F] \mathfrak{N}_p(O)$.

Suppose that $F$ is local. If $D$ is division, then it has a unique maximal order,
so $\mathfrak{N}(O) = 1$ for all $O$. Now suppose that $D = M_2(F)$. The Bruhat-Tits tree $\mathcal{T}$
(of $\text{PGL}_2(F)$) is a homogeneous tree of degree $|\mathfrak{t}| + 1$ whose vertices are the maximal
orders of $M_2(F)$ and such that two vertices are connected by an edge if and only
if the two maximal orders have distance one (See [40] Section II.2). Let $\mathcal{T}(O)$ be
the subtree whose set of vertices is $\mathfrak{S}(O)$. For example, if $O = O \cap O'$ is an Eichler
order of level $\pi^n$, i.e. the intersection of two maximal orders $\mathcal{O}$ and $\mathcal{O}'$ of distance $n$, then by [3 Corollary 2.5], $\mathcal{T}(\mathcal{O})$ is the unique path connecting $\mathcal{O}$ and $\mathcal{O}'$ on $\mathcal{T}$, and $\mathcal{N}(\mathcal{O}) = n + 1$. In general, Arenas-Carmona [3] has shown that $\mathcal{T}(\mathcal{O})$ is a thick line, i.e. the maximal subtree whose vertices lie no further than a fixed distance (called the depth) from a line segment, which is called the stem of the thick line. The stem may have length 0, in which case it degenerates into a single vertex. A thick line with stem length 0 and depth 1 is called a star, and its stem is called the center of the star. Arenas-Carmona and Saavedra [4] provide concrete formulas for the depth and stem length (and hence $\mathcal{N}(\mathcal{O})$) of $\mathcal{T}(\mathcal{O})$ when $\mathcal{O}$ is generated by a pair of orthogonal pure quaternions. However, the present paper does not depend on their formulas. It is also worthwhile to mention Fang-Ting Tu’s result [37] that the intersection of any finite number of maximal orders coincides with the intersection of three maximal orders.

2.5. Let $\mathcal{J}(\mathcal{O})$ be the Jacobson radical of $\mathcal{O}$, and $\mathcal{F}'/\mathfrak{t}$ be the unique quadratic extension of the finite field $\mathfrak{t}$. First, suppose that $F$ is local. Using lifting of idempotents, one shows that $\mathcal{O} \simeq M_2(\mathcal{O}_F)$ if and only if $\mathcal{O}/\mathcal{J}(\mathcal{O}) \simeq M_2(\mathfrak{t})$ (cf. [6 Proposition 2.1]). When $\mathcal{O} \neq M_2(\mathcal{O}_F)$, we have

$$\mathcal{O}/\mathcal{J}(\mathcal{O}) \simeq \mathfrak{t}, \quad \mathfrak{t} \times \mathfrak{t}, \text{ or } \mathfrak{t'},$$

and the Eichler invariant $e(\mathcal{O})$ is defined to be 0, 1 or $-1$ accordingly (see [6 Definition 1.8]). By [14, Chapter 6, Exercise 14], $e(\mathcal{O})$ behaves under a finite field extension $K/F$ in the following way: if $e(\mathcal{O}) = -1$ and $\mathcal{F}'$ is contained in the residue field of $K$, then $e(\mathcal{O} \otimes_{\mathcal{O}_F} \mathcal{O}_K) = 1$, otherwise $e(\mathcal{O} \otimes_{\mathcal{O}_F} \mathcal{O}_K) = e(\mathcal{O})$. We refer to [6 Section 1] for the concept of Gorenstein, Bass, and hereditary orders. If $e(\mathcal{O}) = 1$, then $\mathcal{O}$ is an Eichler order and hence a Bass order. If $e(\mathcal{O}) = -1$, then $\mathcal{O}$ is Bass as well. The Bass orders are explicitly described in [7 Section 1]. The orders with Eichler invariant 0 are more complicated, and the Gorenstein ones are discussed in [3 Section 4].

If $F$ is global and $p$ is a nonzero prime ideal of $\mathcal{O}_F$, we denote by $e_p(\mathcal{O})$ the Eichler invariant of $\mathcal{O}_p$. An order $\mathcal{O}$ is Gorenstein (resp. Bass, resp. hereditary) if and only if $\mathcal{O}_p$ is Gorenstein (resp. Bass, resp. hereditary) for every $p$.

**Lemma 2.6.** Let $D \simeq M_2(\mathcal{F})$ be a split quaternion algebra over a local field $\mathcal{F}$, and $\mathcal{O} \subseteq D$ a Bass order with Eichler invariant $e(\mathcal{O}) = 0$. Then $\mathcal{N}(\mathcal{O}) = 2$.

**Proof.** By [6 Corollary 4.3] and [7 Section 1], every maximal order containing $\mathcal{O}$ necessarily contains its hereditary closure $H(\mathcal{O})$, which has discriminant $\pi\mathcal{O}_F$. Since $D$ splits over $\mathcal{F}$, $H(\mathcal{O})$ is an Eichler order of level $\pi\mathcal{O}_F$. There are precisely two maximal orders containing it.

**Lemma 2.7.** Let $\mathcal{F}$ be a local field, and $D = M_2(\mathcal{F})$. Up to $D^\times$-conjugation, $\mathcal{O} = \mathcal{O}_F + \pi M_2(\mathcal{O}_F)$ is the unique non-Gorenstein order with $\mathcal{d}(\mathcal{O}) = \pi^3 \mathcal{O}_F$. The subtree $\mathcal{T}(\mathcal{O})$ is a star centered at the Gorenstein saturation\(^1\) $M_2(\mathcal{O}_F)$ of $\mathcal{O}$. In particular, $\mathcal{N}(\mathcal{O}) = |\mathfrak{t}| + 2$.

**Proof.** Clearly, $\mathcal{d}(\mathcal{O}) = \chi(M_2(\mathcal{O}_F), \mathcal{O}) \mathcal{d}(M_2(\mathcal{O}_F)) = \pi^3 \mathcal{O}_F$ for $\mathcal{O} = \mathcal{O}_F + \pi M_2(\mathcal{O}_F)$. The dual lattice of $\mathcal{O}$ is

$$\mathcal{O}' = \left\{ \left[ \begin{array}{cc} a & b \\ c & d \end{array} \right] \in M_2(\mathcal{O}_F) \mid a \equiv d \pmod{\pi\mathcal{O}_F} \right\},$$

\(^1\)It is also called the Gorenstein closure in some literature.
which has reduced norm $\text{Nr}(\mathcal{O}^\vee) = \frac{1}{\pi} \mathcal{O}_F$. So the Brandt invariant $b(\mathcal{O})$ is $\mathfrak{d}(\mathcal{O}) \text{Nr}(\mathcal{O}^\vee) = \pi \mathcal{O}_F$. By the criterion in [3, Proposition 1.3], $\mathcal{O}$ is non-Gorenstein. In the notation of [4, Section 1.1], $\mathcal{O} = \mathcal{M}_2(\mathcal{O}_F)_1[1]$, so $\mathfrak{S}(\mathcal{O})$ is a star centered at $\mathcal{M}_2(\mathcal{O}_F)$. More concretely, a maximal order contains $\mathcal{O} = \mathcal{O}_F + \pi \mathcal{M}_2(\mathcal{O}_F)$ if and only if it has at most distance 1 from $\mathcal{M}_2(\mathcal{O}_F)$. The star has a unique center and 1 + $|\mathfrak{t}|$ external vertices, showing that $\mathfrak{N}(\mathcal{O}) = |\mathfrak{t}| + 2$.

Conversely, let $\mathcal{O}$ be an arbitrary non-Gorenstein order in $\mathcal{D} = \mathcal{M}_2(\mathcal{F})$ with $\mathfrak{d}(\mathcal{O}) = \pi^3 \mathcal{O}_F$, and $\text{Gor}(\mathcal{O})$ be its Gorenstein saturation. By [6, Proposition 1.4],

$$\mathcal{O} = \mathcal{O}_F + b(\mathcal{O}) \text{Gor}(\mathcal{O}), \quad \text{where } b(\mathcal{O}) = \pi^r \mathcal{O}_F \quad \text{with } r > 1.$$  

Hence $\mathfrak{d}(\text{Gor}(\mathcal{O})) = \chi(\text{Gor}(\mathcal{O}), \mathcal{O})^{-1} d(\mathcal{O}) = b(\mathcal{O})^{-3} d(\mathcal{O}) = \pi^{3-3r} \mathcal{O}_F$. Since $\mathfrak{d}(\text{Gor}(\mathcal{O}))$ is integral, $r = 1$ and $\text{Gor}(\mathcal{O})$ is a maximal order in $\mathcal{M}_2(\mathcal{F})$. Thus $\mathcal{O}$ is conjugate to $\mathcal{O}_F + \pi \mathcal{M}_2(\mathcal{O}_F)$.

\begin{lemma}
Let $\mathcal{D} = \left(\begin{array}{cc} a & b \\ \pi b & -a \end{array}\right)$ with $a, b \in \mathcal{O}_F \setminus \{0\}$. Then the order $\mathcal{O} = \mathcal{O}_F[i, j]$ is a Gorenstein order with discriminant $\mathfrak{d}(\mathcal{O}) = 4ab \mathcal{O}_F$. Suppose further that $\mathcal{F}$ is a number field, and both $a, b \in \mathcal{O}_F$. Then $\mathcal{O}$ is maximal at every non-dyadic prime of $\mathcal{F}$, and $e_p(\mathcal{O}) = 0$ for every dyadic prime $p$. Moreover, if $a = -1$, then $(1 + i) \in \mathfrak{N}(\mathcal{O})$.
\end{lemma}

\begin{proof}
One calculates that $\mathfrak{d}(\mathcal{O}) = 4ab \mathcal{O}_F$, and the dual basis of $\{1, i, j, k\}$ is

$$\left\{ \frac{1}{2}, \frac{i}{2a}, \frac{j}{2b}, \frac{-k}{2ab} \right\}.$$  

The fact that $\mathcal{O}$ is a Gorenstein order can be checked using the criterion [6, Proposition 1.3]. Suppose that $\mathcal{F}$ is a number field and $a, b \in \mathcal{O}_F$. We have $\mathfrak{d}(\mathcal{O}) = 4 \mathcal{O}_F$, and the maximality of $\mathcal{O}$ at the non-dyadic primes of $\mathcal{F}$ follows directly. Let $p$ be a non-dyadic prime of $\mathcal{F}$ with finite residue field $\mathfrak{t}$. Then $\mathcal{O}_p$ is not maximal since $\mathfrak{d}(\mathcal{O}_p)$ is not square-free. By [2, 4], an equation of the form $x^2 = c \in \mathfrak{t}$ with $x \in \mathcal{O}_p/\mathfrak{d}(\mathcal{O}_p)$ has a unique solution that lies in $\mathfrak{t}$. It follows that the reductions of both $i$ and $j$ modulo $\mathfrak{d}(\mathcal{O}_p)$ are in $\mathfrak{t}$, and hence $\mathcal{O}_p/\mathfrak{d}(\mathcal{O}_p) = \mathfrak{t}$, i.e. $\mathfrak{e}_p(\mathcal{O}) = 0$. When $a = -1$, we have

$$\chi(\mathcal{O}, \mathcal{O'}) = \chi(\mathcal{O}, \mathcal{O'})^{-1} = i \quad \text{and} \quad (1 + i)^{-1} = k.$$  

Thus $(1 + i) \in \mathfrak{N}(\mathcal{O})$.
\end{proof}

\begin{lemma}
Let $\mathcal{D} = \left(\begin{array}{cc} a & b \\ \pi b & -a \end{array}\right)$ with $a, b \in \mathcal{O}_F \setminus \{0\}$, and $\mathcal{O} = \mathcal{O}_F[i, j]$. Suppose that $\mathcal{F}$ is a local field, and $\mathfrak{d}(\mathcal{O}) = 4ab \mathcal{O}_F$ is divisible by $\pi^3 \mathcal{O}_F$. Then $\mathcal{O}$ is a Bass order if and only if one of the orders $\mathcal{O}_F[i]$ or $\mathcal{O}_F[j]$ is maximal in its total quotient ring.
\end{lemma}

\begin{proof}
The sufficiency follows directly from [7, Proposition 1.11]. We prove the converse. So assume that neither $\mathcal{O}_F[i]$ nor $\mathcal{O}_F[j]$ are maximal orders. Then there exists a unique overorder $B \subset \mathcal{F}(i)$ of $\mathcal{O}_F[i]$ such that $\chi(B, \mathcal{O}_F[i]) = \pi \mathcal{O}_F$. Similarly, we find an overorder $B' \subset \mathcal{F}(j)$ of $\mathcal{O}_F[j]$ with $\chi(B', \mathcal{O}_F[j]) = \pi \mathcal{O}_F$. Now let $\mathcal{O} = B + Bj$, and $\mathcal{O}' = B' + iB'$. These are distinct overorders of $\mathcal{O}$ since $\mathcal{O} \cap \mathcal{F}(i) = B$ while $\mathcal{O}' \cap \mathcal{F}(i) = \mathcal{O}_F[i] \neq B$. The choices of $B$ and $B'$ imply that

$$\chi(\mathcal{O}, \mathcal{O}) = \chi(\mathcal{O}', \mathcal{O}) = \pi^2 \mathcal{O}_F.$$  

Hence $\mathfrak{d}(\mathcal{O}) = \mathfrak{d}(\mathcal{O'}) = \pi^2 \mathfrak{d}(\mathcal{O}) \neq \mathcal{O}_F$ by the assumption on $\mathfrak{d}(\mathcal{O})$. It follows from [6, Corollary 4.3] that $\mathcal{O}$ cannot be Bass, otherwise the overorder of $\mathcal{O}$ satisfying (2.6) is unique.
\end{proof}
Lemma 2.10. Let $D = \left( \frac{ab}{F} \right)$ with $a, b \in O_F \setminus \{0\}$ and $b \equiv 1 \pmod{4O_F}$. Then $O := O_F[i, (1 + j)/2]$ is a Gorenstein order with $\mathfrak{d}(O) = abO_F$ and $j \in \mathcal{N}(O)$. Suppose further that $F$ is a number field, $a \in O_F$ and $b = -3$. Then $O$ is maximal at any nonzero prime of $O_F$ coprime to 3. Let $p$ be a prime of $O_F$ above 3 with residue field $\mathfrak{t}$. If $D_p$ is division and $p$ is unramified above 3, then $O$ is maximal at $p$; otherwise we have

$$e_p(O) = \begin{cases} 1 & \text{if } (a \mod p) \in \mathfrak{t}^{x_2}, \\ -1 & \text{if } (a \mod p) \notin \mathfrak{t}^{x_2}. \end{cases}$$

Proof. Note that $(1 + j)/2$ is integral over $O_F$ since $b \equiv 1 \pmod{4O_F}$, and one easily verifies that $j \in \mathcal{N}(O)$. The order $O$ is a free $O_F$-module with basis $\{1, i, (1 + j)/2, (i + k)/2\}$. Direct calculation shows that the dual basis is

$$(2.7) \quad \frac{b - j}{2b}, \quad \frac{bi + k}{2ab}, \quad \frac{j}{b}, \quad \frac{k}{ab},$$

and $\mathfrak{d}(O) = abO_F$. By [6, Proposition 1.3(b)], $O$ is Gorenstein since $b(O) = O_F$.

Now suppose that $F$ is a number field, $a \in O_F$ and $b = -3$. Then $\mathfrak{d}(O) = 3O_F$, and hence $O$ is maximal at any nonzero prime of $O_F$ coprime to 3. If $p$ is a prime unramified above 3 and $D_p$ is division, then $\mathfrak{d}(O_p) = pO_{F_p} = \mathfrak{d}(D_p)$, so $O_p$ is the unique maximal order in $D_p$. In the remaining cases, $O_p$ is non-maximal. Since $(1 + j)/2$ is a primitive third root of unity and $\text{char}(\mathfrak{t}) = 3$, we have $(1 + j)/2 \equiv 1 \pmod{3(\mathfrak{d}(O_p))}$ by (2.4). Let $\overline{i}$ denote the image of $i$ in $O_p/3(\mathfrak{d}(O_p))$. We then have

$$\mathfrak{t}[\overline{i}] = \begin{cases} \mathfrak{t} & \text{if } (a \mod p) \in \mathfrak{t}^{x_2}, \\ \mathfrak{t}' & \text{if } (a \mod p) \notin \mathfrak{t}^{x_2}. \end{cases}$$

The formula for $e_p(O)$ follows. \hfill \Box

For the convenience of the reader, we state the following well-known lemma.

Lemma 2.11. Let $Q$ be a non-archimedean local field with ring of integers $R$ and uniformizer $\pi_0$, and $D_0$ a quaternion division algebra over $Q$ with the unique maximal $R$-order $O_0$. Suppose that $F/Q$ is an unramified quadratic extension. Then $O := O_0 \otimes R O_F$ is an Eichler order of level $\pi_0 O_F$ in $D := D_0 \otimes_Q F \simeq M_2(F)$. $\mathfrak{d}$

Proof. As remarked in Subsection [2.5], $O$ is an order with Eichler invariant 1 and discriminant $\pi_0 O_F$. The lemma follows from [6, Proposition 2.1]. \hfill \Box

We also treat the case where $F/Q$ is ramified.

Lemma 2.12. Let $Q, R, D_0, O_0$ and $\pi_0$ be the same as in Lemma 2.11. Suppose that $F/Q$ is a ramified quadratic extension. Then there is a unique $O_F$-order $\mathcal{O}$ in $D := D_0 \otimes_Q F \simeq M_2(F)$ properly containing $\mathcal{O} := O_0 \otimes_R O_F$. The order $\mathcal{O}$ is necessarily maximal, and $\mathcal{O} \simeq O_L + \pi \mathcal{O}$, where $L/F$ is the unique unramified quadratic extension of $F$, identified with a subfield of $D$ such that $O_L \subset \mathcal{O}$.

By [10, Theorem 3.2], any two embeddings of $O_L$ into $\mathcal{O}$ are conjugate by an element of $\mathcal{O}^\times$. Thus the structure of $O_L + \pi \mathcal{O}$ does not depend on the embedding.

Proof. By Subsection [2.5], $e(O) = e(O_0) = -1$. So according to [6, Proposition 3.1], there is a unique minimal overorder $\mathcal{O}$ containing $O$ with $\chi(\mathcal{O}, O) = \pi^2 O_F$ and $\mathfrak{d}(O) = \pi O_F$. We have

$$\mathfrak{d}(\mathcal{O}) = \mathfrak{d}(O_0) \chi(\mathcal{O}, O)^{-1} = \pi_0 \pi^{-2} O_F = O_F.$$
Therefore, \( \mathcal{O} \) is a maximal order in \( D \), and hence the unique order properly containing \( \mathcal{O} \).

Let \( L_0/Q \) be the unique unramified quadratic extension of \( Q \), identified with a subfield of \( D_0 \) such that \( D_0 = L_0 + L_0x \) with \( x^2 = \pi_0 \) and \( xy = \bar{y}x \) for all \( y \in L_0 \). Then by [40] Corollary II.1.7, \( \mathcal{O}_0 = O_{L_0} + O_{L_0}x \). Since \( F/Q \) is ramified, we have \( L = L_0 \otimes Q F \) and \( O_L = O_{L_0} \otimes_R O_F \). Hence

\[
(2.8) \quad \mathcal{O} = \mathcal{O}_0 \otimes_R O_F = O_L + O_Lx.
\]

In particular, \( \mathcal{O} \supseteq O_L + \mathcal{O} \). On the other hand, \( \chi(\mathcal{O}, O_L + \mathcal{O}) = \pi^2 O_F = \chi(\mathcal{O}, \mathcal{O}) \).

Let \( \tilde{u} \in \mathcal{O}^* \) be a nontrivial element, and \( u \in \mathcal{O}^X \) a representative of \( \tilde{u} \). The subfield \( K_{\tilde{u}} := F(u) \subset F \) does not depend on the choice of \( u \) and is denoted by \( K_{\tilde{u}} \). Let \( O_{K_{\tilde{u}}} \) be the ring of integers of \( K_{\tilde{u}} \), and \( B_{\tilde{u}} \subseteq O_{K_{\tilde{u}}} \) the \( O_F \)-suborder \( K_{\tilde{u}} \cap \mathcal{O} \). Since \( D \) is totally definite over \( F \), \( K_{\tilde{u}} \) is a CM-extension (i.e. a totally imaginary quadratic extension) of \( F \). We have \( u \in B_{\tilde{u}}^X \), and hence

\[
(3.1) \quad [O_{K_{\tilde{u}}}^X : O_F^X] \geq [B_{\tilde{u}}^X : O_F^X] > 1.
\]

For any fixed totally real field \( F \), there are only finitely many CM-extensions \( K/F \) such that \( [O_K^X : O_F^X] > 1 \). Let \( \mu(K) \) be the group of roots of unity in an arbitrary CM-extension \( K/F \). The Hasse index

\[
(3.2) \quad Q_{K/F} := [O_K^X : O_F^X \mu(K)]
\]

is either 1 or 2. Following [40] Section 13, we call \( K/F \) a CM-extension of type I if \( [O_K^X : O_F^X \mu(K)] = 1 \), and of type II if \( [O_K^X : O_F^X \mu(K)] = 2 \). If \( K/F \) is of type I, then \( O_K^X/O_F^X \cong \mu(K)/\{\pm 1\} \), otherwise \( O_K^X/O_F^X \) is a cyclic group of order \( |\mu(K)| \) by [40] Section 2]. Either way, \( O_K^X/O_F^X \) is a cyclic group, so is \( B^X/O_F^X \) for any \( O_F \)-suborder \( B \subseteq O_K \).

Suppose \( \text{ord}(\tilde{u}) = r > 1 \). The cyclic group \( O_{K_{\tilde{u}}}^X/O_F^X \) contains a unique cyclic subgroup of order \( r \), namely \( \langle \tilde{u} \rangle \). Given \( v \in O_{K_{\tilde{u}}}^X \), denote by \( \tilde{v} \) the image of \( v \) under the canonical projection \( O_{K_{\tilde{u}}}^X \to O_{K_{\tilde{u}}}^X/O_F^X \). Then the preimage of \( \langle \tilde{u} \rangle \) coincides with
\(\{v \in O_{K_0}^\times \mid \text{ord}(v) \text{ divides } r\}\), which is necessarily a subgroup of \(B_{K_0}^\times\). For example, if \(r\) is odd, then \(2r\) divides \(|\mu(K_0)|\), and \(\tilde{u}\) is represented by a primitive \(r\)-th root of unity in \(\mu(K_0)\).

**3.3.** Given an \(O_F\)-order \(B\) inside a CM-extension \(K/F\), we write \(\text{Emb}(B, O)\) for the finite set of optimal \(O_F\)-embeddings of \(B\) into \(O\). In other words,

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

The group \(O^\times\) acts on \(\text{Emb}(B, O)\) from the right by \(\varphi \mapsto u^{-1}\varphi u\) for all \(\varphi \in \text{Emb}(B, O)\) and \(u \in O^\times\). We denote \(m(B, O, O^\times) := |\text{Emb}(B, O)/O^\times|\). For each nonzero prime ideal \(p\) of \(O_F\), we set \(m_p(B) := m(B_p, O_p, O_p^\times)\). Let \(h = h(O)\), and \(I_1, \ldots, I_h\) be a complete set of representatives of the right ideal class set \(\text{Cl}(O)\).

Define \(O_s := O(I_s)\) for each \(1 \leq s \leq h\), where \(O(I)\) stands for the associated left order \(\{x \in D \mid xI \subseteq I\}\). By [40, Theorem 5.11, p. 92],

\[
(3.3) \quad \sum_{s=1}^{h} m(B, O_s, O_s^\times) = h(B) \prod_p m_p(B),
\]

where the product on the right runs over all nonzero prime ideals of \(O_F\). A priori, Theorem 5.11 of [40] is stated for Eichler orders, but it applies in much more general settings. See [41, Lemma 3.2] and [13, Lemma 3.2.1]. When \(O\) is maximal, we have

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

where \(\left(\frac{B}{p}\right)\) is the Eichler symbol [40, p.94].

For the rest of this section, we fix a maximal \(O_F\)-order \(\mathfrak{O} \subset D\).

**3.4.** Let \(I\) be a fractional right ideal \(I\) of \(\mathfrak{O}\), whose ideal class in \(\text{Cl}(\mathfrak{O})\) is denoted by \([I]\). Denote the \(D^\times\)-conjugacy class of a maximal order \(\mathfrak{O}' \subset D\) by \([\mathfrak{O}']\). There is a surjective map of finite sets

\[
(3.4) \quad \Upsilon : \text{Cl}(\mathfrak{O}) \to \text{Tp}(D), \quad [I] \mapsto [\mathcal{O}_I(I)].
\]

The fibers of \(\Upsilon\) is studied in [35, Section 1.7], whose result we briefly recall below.

By [33, Theorem 22.10], the set of nonzero two-sided fractional ideals of \(\mathfrak{O}\) forms a commutative multiplicative group \(\mathcal{I}(\mathfrak{O})\), which is a free abelian group generated by the nonzero prime two-sided ideals of \(\mathfrak{O}\). Let \(\mathcal{P}(\mathfrak{O}) \subseteq \mathcal{I}(\mathfrak{O})\) be the subgroup of nonzero principal two-sided fractional ideals of \(\mathfrak{O}\), and \(\mathcal{P}(O_F)\) the group of nonzero principal fractional \(O_F\)-ideals, identified with a subgroup of \(\mathcal{P}(\mathfrak{O})\) via \(xO_F \mapsto x\mathfrak{O}, \forall x \in F^\times\). For any maximal order \(\mathfrak{O}'\), there is a bijection ( [35, Section 1.7], [40, Lemma III.5.6])

\[
(3.5) \quad \Upsilon^{-1}(\mathcal{O}') \leftrightarrow \mathcal{I}(\mathfrak{O}')/\mathcal{P}(\mathfrak{O})\mathfrak{O}'.
\]

The quotient group \(\mathcal{I}(\mathfrak{O}')/\mathcal{P}(\mathfrak{O}')\) sits in a short exact sequence [13, Theorem 55.22]

\[
(3.6) \quad 1 \rightarrow K(\mathfrak{O}')/(F^\times \mathfrak{O}')^\times \rightarrow \text{Pic}(\mathfrak{O}') \rightarrow \mathcal{I}(\mathfrak{O}')/\mathcal{P}(\mathfrak{O}') \rightarrow 1.
\]

Here \(\text{Pic}(\mathfrak{O}')\) denotes the Picard group \(\mathcal{I}(\mathfrak{O}')/\mathcal{P}(O_F)\), whose cardinality can be calculated using the short exact sequence [13, Theorem 55.27]

\[
(3.7) \quad 1 \rightarrow \text{Cl}(O_F) \rightarrow \text{Pic}(\mathfrak{O}') \rightarrow \prod_{p \mid \mathfrak{b}(D)} (\mathbb{Z}/2\mathbb{Z}) \rightarrow 0.
\]
Combining (3.3) and (3.8), we obtain for each fixed $B$

\[ |\mathcal{O}| = \frac{2^{\omega(D)} h(F)}{|\mathcal{N}(\mathcal{O})/(\mathcal{O}^\times)|}, \]

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

### 3.5. Strategy for Calculating $h(D, G)$

When $G = C_n$ is a cyclic group of order $n$, we divide the type set $\mathcal{T}(D)$ into two parts:

- $\mathcal{T}_1 := \left\{ [\mathcal{O}] \in \mathcal{T}(D) \mid \mathcal{O}^\times \text{ is cyclic} \right\}$, and
- $\mathcal{T}_2 := \mathcal{T}(D) - \mathcal{T}_1$.

Let $\mathcal{B}_n$ be the finite set of $O_F$-orders $B$ in some CM-extension of $F$ such that $B^\times /O_F^\times \cong C_n$. Let $h = h(0)$, and $I_1, \ldots, I_h$ be a complete set of representatives of $\mathcal{C}(\mathcal{O})$. For each $1 \leq s \leq h$, let $\mathcal{O}_s := \mathcal{O}_s(I_s)$. If $\mathcal{O}_s \in \mathcal{T}_1$, then $\mathcal{O}_s^\times \cong C_n$ if and only if $\text{Emb}(B, \mathcal{O}_s) \neq \emptyset$ for some $B \in \mathcal{B}_n$. When the latter condition holds, such an order $B$ is then uniquely determined, and $m(B, \mathcal{O}_s, \mathcal{O}_s^\times) = 2$. For each fixed $B \in \mathcal{B}_n$, let

\[ h(D, C_n, B) := \# \{ [I] \in \mathcal{C}(\mathcal{O}) \mid \mathcal{O}_s(I)^\times \cong C_n, \text{ and } \text{Emb}(B, \mathcal{O}_s(I)) \neq \emptyset \}. \]

Then we have

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

Combining (3.3) and (3.8), we obtain for each fixed $B$ the following equation:

\[ 2^{\omega(D)} h(F) \sum_{[\mathcal{O}] \in \mathcal{T}_1} \frac{m(B, \mathcal{O}, \mathcal{O}^\times)}{|\mathcal{N}(\mathcal{O})/(\mathcal{O}^\times)|} + 2h(D, C_n, B) = h(B) \prod_p m_p(B). \]

Therefore, to compute $h(D, C_n, B)$ (and hence $h(D, C_n)$), it is crucial to classify all isomorphism classes of maximal orders with non-cyclic reduced unit groups, and ideally, to write them down as explicitly as possible. Sections 4.4.5 are devoted to this task. Once this is done, then for any non-cyclic group $G$,

\[ h(D, G) = \sum_{B \in \mathcal{B}_n} \frac{2^{\omega(D)} h(F)}{|\mathcal{N}(\mathcal{O})/(\mathcal{O}^\times)|}, \]

where the summation runs over all $[\mathcal{O}] \in \mathcal{T}_2(D)$ with $\mathcal{O}^\times \cong G$.

### 4. Minimal $G$-orders

In this section, we assume that $F = \mathbb{Q}(\sqrt{d})$ is a real quadratic field, whose fundamental unit is denoted by $\varepsilon$. Starting from Subsection 4.4, we assume further that $d \geq 6$. The cases $d \in \{2, 3, 5\}$ are treated separately in Subsection 3.5.

For an $O_F$-order $\mathcal{O}$ in $D$, we set $\mathcal{O}^1 := \{ u \in \mathcal{O}^\times \mid \text{Nr}(u) = 1 \}$, the group of units with reduced norm 1. It is known [10] Section V.1 that $\mathcal{O}^1$ is a finite normal subgroup of $\mathcal{O}^\times$, and $|\mathcal{O}^\times : O_F^\times \mathcal{O}^1| = 1, 2, 4$ for an arbitrary totally real $F$.

**Lemma 4.1.** If $F = \mathbb{Q}(\sqrt{d})$ is a real quadratic field, then $|\mathcal{O}^\times : O_F^\times \mathcal{O}^1| \in \{1, 2\}$. Moreover, if $\text{N}_{F/\mathbb{Q}}(\varepsilon) = -1$, then $\mathcal{O}^\times = O_F^\times \mathcal{O}^1$.

**Proof.** Since $D$ is totally definite, we have $O_F^{+2} \subset \text{N}(\mathcal{O}^\times) \subset O_F^{+}$, the group of totally positive units in $O_F^\times$. This gives rise to an embedding

\[ \mathcal{O}^\times / (O_F^\times \mathcal{O}^1) \hookrightarrow O_F^{+} / O_F^{+2}. \]
When $F$ is a real quadratic field, the fundamental unit $\varepsilon \in O_F^\times$ is totally positive if and only if $N_{F/Q}(\varepsilon) = 1$. We have

$$O_{F,+}^\times = \begin{cases} \langle \varepsilon \rangle & \text{if } N_{F/Q}(\varepsilon) = 1, \\ \langle \varepsilon^2 \rangle & \text{if } N_{F/Q}(\varepsilon) = -1, \end{cases} \quad \text{while } O_F^{x^2} = \langle \varepsilon^2 \rangle .$$

The lemma follows directly from (4.1).

\[\square\]

**Remark 4.2.** It is well known [11 Section 11.5] that for $F = \mathbb{Q}(\sqrt{d})$,

- $N_{F/Q}(\varepsilon) = 1$ if $d$ is divisible by a prime $p \equiv 3 \pmod{4}$;
- $N_{F/Q}(\varepsilon) = -1$ if $d = p$ with a prime $p \equiv 1 \pmod{4}$, or $d = 2p$ with $p \equiv 5 \pmod{8}$, or $d = p_1p_2$ with primes $p_1, p_2 \equiv 1 \pmod{4}$ and $(\frac{p_1}{p_2}) = (\frac{p_2}{p_1}) = -1$.

Before the discussion leads us too far astray, we also refer to the classes of $d$ with known signs of $N_{F/Q}(\varepsilon)$ in Corollaries 21.10 and 24.5 of [11].

4.3. Let $K/F$ be a CM-extension. Since $[K : \mathbb{Q}] = 4$, the possible orders of $\mu(K)$ are $2, 4, 6, 8, 10, 12$ by [11 Subsection 2.3]. Moreover,

- $|\mu(K)| = 8$ if and only if $F = \mathbb{Q}(\sqrt{2})$ and $K = \mathbb{Q}(\sqrt{2}, \sqrt{-3})$;
- $|\mu(K)| = 10$ if and only if $F = \mathbb{Q}(\sqrt{5})$ and $K = \mathbb{Q}(\sqrt{5})(\varepsilon)$;
- $|\mu(K)| = 12$ if and only if $F = \mathbb{Q}(\sqrt{3})$ and $K = \mathbb{Q}(\sqrt{3}, \sqrt{-1})$.

Here $\varepsilon_n$ denotes the primitive $n$-th root of unity $\varepsilon^{2n/3}$ for all positive $n \in \mathbb{N}$.

For simplicity, we assume that $d \geq 6$. Then $|\mu(K_{\varepsilon})| \in \{2, 4, 6\}$ for any nontrivial element $\tilde{u} \in O^*$. By Subsection 3.2 we have $\text{ord}(\tilde{u}) \in \{2, 3, 4, 6\}$, and $\text{ord}(\tilde{u}) = 4$ (resp. 6) only if $K_{\varepsilon} = F(\sqrt{-d})$ (resp. $F(\sqrt{-3})$) and $K_{\varepsilon}/F$ is a CM-extension of type II. According to [9 Lemma 2], $F(\sqrt{-d})/F$ (resp. $F(\sqrt{-3})/F$) is of type II if and only if $2\varepsilon \in F^{x^2}$ (resp. $3\varepsilon \in F^{x^2}$). For example, we have $2\varepsilon \in F^{x^2}$ if $d = p$ or $2p$ with $p \equiv 3 \pmod{4}$ by [20 Lemma 3] or [17 Lemma 3.2(1)]. Similarly, $3\varepsilon \in F^{x^2}$ if $d = 3p$ with $p \equiv 3 \pmod{4}$ by [9 Lemma 3]. Note that $2\varepsilon$ and $3\varepsilon$ are simultaneously perfect squares in $F^\times$ if and only if $d = 6$. Lastly, if $\{2\varepsilon, 3\varepsilon\} \cap F^{x^2} = \emptyset$, then $\text{ord}(\tilde{u}) \in \{2, 3\}$. For instance, if $N_{F/Q}(\varepsilon) = -1$, then $\{2\varepsilon, 3\varepsilon\} \cap F^{x^2} = \emptyset$. In fact, when $N_{F/Q}(\varepsilon) = -1$, any CM-extension $K/F$ is of type I by [11 Lemma 13.6]. The possible structures of non-cyclic $O^*$ for $d \geq 6$ are listed in the following table.

| $F = \mathbb{Q}(\sqrt{d})$, $d \geq 6$ | $\text{ord}(\tilde{u}) > 1$ | possible non-cyclic $O^*$ |
|------------------------------------------|----------------------------|-----------------------------|
| $2\varepsilon \in F^{x^2}$              | 2, 3, 4                    | $D_2, D_3, D_4, A_4, S_4$  |
| $3\varepsilon \in F^{x^2}$              | 2, 3, 6                    | $D_2, D_3, D_6, A_4$       |
| $\{2\varepsilon, 3\varepsilon\} \cap F^{x^2} = \emptyset$ | 2, 3                       | $D_2, D_3, A_4$            |

Suppose that $N_{F/Q}(\varepsilon) = 1$, and factorize $\text{Tr}_{F/Q}(\varepsilon) - 2 \in \mathbb{N}$ into $mn$ such that $m, n \in \mathbb{N}$ and $n$ is square-free. By [25 Proposition 3.1], $n$ divides $d$ or $4d$, and $n\varepsilon \in F^{x^2}$. In particular, $F(\sqrt{-\varepsilon}) = F(\sqrt{-n})$ is a bicyclic biquadratic field. See [15 Lemma 7.8] for the example when $F = \mathbb{Q}(\sqrt{p_1p_2})$ where $p_1$ and $p_2$ are distinct primes with $p_1 \equiv p_2 \equiv 3 \pmod{4}$.

For the rest of this section, we assume that $d \geq 6$.

4.4. We set $\mathcal{S} = \{1, \varepsilon\}$ if $N_{F/Q}(\varepsilon) = 1$, and $\mathcal{S} = \{1\}$ otherwise. Then $\mathcal{S}$ is a complete set of representatives of $O_{F,+}^\times/O_F^{x^2}$. After multiplying a representative $u \in O^\times$ of $\tilde{u} \in O^*$ by a suitable element of $O_F^\times$, we may and will assume that
Let $O_u := \text{Nr}(u)$ belong to $\mathcal{S}$. This determines $u$ uniquely up to sign. Subsequently, all representatives of $\tilde{u}$ refer exclusively to these ones. The representative of the identity element of $O^\times$ is always chosen to be 1. By an abuse of notation, we set $\text{Nr}(\tilde{u}) = \text{Nr}(u) \in \mathcal{S}$. Let $P_u(x) = x^2 - t_u x + n_u \in F[x]$ be the minimal polynomial over $F$ of $u$. Changing $u$ to $-u$ switches the sign of $t_u$ and leaves $n_u$ invariant, so we put $P_u(x) = x^2 \pm t_u x + n_u$.

If $2 \varepsilon \in F^{\times 2}$, then we fix $\vartheta \in F^{\times}$ such that $\varepsilon = 2 \vartheta^2$; similarly if $3 \varepsilon \in F^{\times 2}$, then we fix $\varsigma \in F^{\times}$ such that $\varepsilon = 3 \varsigma^2$. In Table 1 we list all the possible $P_u(x)$ for each nontrivial $\tilde{u}$, whose order lies in $\{2, 3, 4, 6\}$. The method is the same as that of [44 Lemma 2.2], hence omitted.

We make the following observations based on Table 1:

1. For each $r \in \{3, 4, 6\}$, the representatives of reduced units of order $r$ for all $O_F$-orders are $D^\times$-conjugate up to sign. The same holds for each of the two classes of reduced units of order 2, provided that we make the additional requirement that $\text{Nr}(\tilde{u}) = 1$ (alternatively, $\text{Nr}(\tilde{u}) = \varepsilon$).

2. If $K/F$ is a CM-extension with $[O^\times_K : O^\times_F] > 1$, then

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

3. Suppose that $\text{Nr}_{F/Q}(\varepsilon) = 1$. If $3 \varepsilon \notin F^{\times 2}$, then $\mu(F(\sqrt{-\varepsilon})) = \{\pm 1\}$ since $F(\sqrt{-\varepsilon})$ contains neither $\sqrt{-1}$ nor $\sqrt{-3}$; otherwise $F(\sqrt{-\varepsilon}) = F(\sqrt{-3})$, and $\mu(F(\sqrt{-\varepsilon})) = \{\varsigma_6\}$. Conversely, if $K/F$ is a CM-extension of type II with $\mu(K) = \{\pm 1\}$, then $K = F(\sqrt{-\varepsilon})$ and $3 \varepsilon \notin F^{\times 2}$ by [44 Lemma 2.2].

4. If $3 \varepsilon \in F^{\times 2}$, then the unique element of order 2 in the cyclic group $O^\times_K(\sqrt{-3})/O^\times_F$ of order 6 is represented by $\pm \sqrt{-\varepsilon} = \pm \varsigma_6 \sqrt{-3}$.

Let $O$ be an order such that $O^\times$ contains a non-cyclic group $G$. The $O_F$-submodule spanned by the representatives of all elements of $G$ is a suborder of $O$.

**Definition 4.5.** Let $G$ be one of the non-cyclic groups in the table of Subsection 4.3. An $O_F$-order $O$ in $D$ is called a minimal $G$-order if

- $O^\times$ contains a subgroup isomorphic to $G$; and
- $O$ is spanned over $O_F$ by the representatives of elements of $G$. 

| $\text{ord}(\tilde{u})$ | Conditions | $P_{\tilde{u}}(x) \in F[x]$ | roots of $P_{\tilde{u}}(x)$ |
|-----------------------|------------|----------------------------|-----------------------------|
| 2                     | $\text{Nr}(\tilde{u}) = 1$ | $x^2 + 1$ | $\pm \sqrt{-1}$ |
|                       | $\text{Nr}_{F/Q}(\varepsilon) = 1$, $\text{Nr}(\tilde{u}) = \varepsilon$ | $x^2 + \varepsilon$ | $\pm \sqrt{-\varepsilon}$ |
| 3                     | $x^2 \pm x + 1$ | $\pm \varsigma_3^\pm 1$ |
| 4                     | $\text{Nr}_{F/Q}(\varepsilon) = 1$, $2 \varepsilon \in F^{\times 2}$ | $x^2 \pm 2 \vartheta x + \varepsilon$ | $\pm \sqrt{\pm \varsigma_3 \sqrt{-1}} = \pm \vartheta(1 \pm \sqrt{-1})$ |
| 6                     | $\text{Nr}_{F/Q}(\varepsilon) = 1$, $3 \varepsilon \in F^{\times 2}$ | $x^3 \pm 3 \varsigma x + \varepsilon$ | $\pm \sqrt{\pm \varsigma_6^\pm 1} = \pm \varsigma_6 \sqrt{-3}$ |
Let $\mathcal{O}$ be a minimal $G$-order with $G = D_2$ 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 $II$.

By the definition, any order $\mathcal{O}'$ with $\mathcal{O}' \supseteq G$ contains a minimal $G$-order $\mathcal{O}$. For simplicity, we put either a $\dagger$ or $\ddagger$ as a superscript of $\mathcal{O}$ for $m = 2, 3$ to indicate its type. For example, a minimal $D_2$-order means a minimal $D_2$-order of type I. The concept of type is vacuous if $G \not\supseteq D_2$ nor $D_3$. This is explained for $G \simeq D_4$ or $D_6$ in Subsection 4.6 and it will also be clear as we workout the minimal $A_4$ or $S_4$-orders. A priori, the minimality of $\mathcal{O}$ depends on the embedding $G \hookrightarrow \mathcal{O}$*. But we show later in Corollary 4.14 that such an embedding is in fact an isomorphism, so any two of them differ by an automorphism of $G$.

4.6. Let $D_m$ be a dihedral group of order $2m$ with $m \in \{2, 3, 4, 6\}$, and $\mathcal{O}_m$ be a minimal $D_m$-order. Write

$$D_m = \langle \tilde{u}, \tilde{\eta} \in \mathcal{O}_m^* \mid \text{ord}(\tilde{u}) = 2, \text{ord}(\tilde{\eta}) = m, \tilde{u} \tilde{\eta} = \tilde{\eta}^{-1} \tilde{u} \rangle.$$ 

Let $u, \eta \in \mathcal{O}_m^*$ be the respective representative of $\tilde{u}, \tilde{\eta}$, and $K = F(\eta)$. Then

$$\mathcal{O}_m = O_F + O_F u + O_F \eta + O_F u \eta.$$ 

By (4.3), $uKu^{-1} \subseteq K$, and conjugation by $u$ induces the unique nontrivial $F$-automorphism $y \mapsto \tilde{y}$ on $K$. In particular,

$$u \eta u^{-1} = \tilde{\eta}.$$ 

We have $u^2 \in \{-1, -\epsilon\} \subseteq O_F^\times$ as shown in Subsection 4.4 and hence $D = \{K, -1\}$ or $\{K, -\epsilon\}$ accordingly.

If $m \in \{4, 6\}$, then $\text{Nr}(\eta) = \epsilon$. Replacing $u$ by $u\eta$ if necessary, we may and will assume that $\text{Nr}(u) = 1$ when $m \in \{4, 6\}$. When $m = 2$, there always exists a nontrivial element of $D_2 \subseteq \mathcal{O}_2^*$ with reduced norm 1, which we denote by $\tilde{u}$. The two elements of $D_2$ outside $\langle \tilde{u} \rangle$ have the same reduced norm, and we pick one of them to be $\tilde{\eta}$. When $m = 3$, $\text{Nr}(\eta) = 1$ and all elements of order 2 in $D_3$ have the same reduced norm (either 1 or $\epsilon$). As before, we put either a $\dagger$ or $\ddagger$ as a superscript of $\mathcal{O}_m$ for $m = 2, 3$ to indicate its type.

Lemma 4.7. For each $m \in \{2, 3, 4, 6\}$, all minimal $D_m$-orders of $D$ of the same type are $D^\times$-conjugate.

Proof. Let $\mathcal{O}_m$ and $\mathcal{O}_m'$ be two minimal $O_F$-orders of same type. By Subsection 4.6 we can pick pairs of elements $\eta, u \in \mathcal{O}_m^\times$ and $\eta', u' \in \mathcal{O}_m'^\times$ respectively such that their reduction modulo $O_F^\times$ satisfy the relations in (4.3), and

$$\text{Nr}(\eta) = \text{Nr}(\eta'), \quad \text{Nr}(u) = \text{Nr}(u').$$ 

By Subsection 4.4 $\eta$ and $\eta'$ are $D^\times$-conjugate up to sign. So conjugating $\mathcal{O}_m'$ by a suitable element of $D^\times$, and replacing $\eta'$ by $-\eta'$ if necessary, we assume that $\eta' = \eta$. By (1.5), $u^{-1}u'$ commutes with $\eta$, and thus with every element of $K = F(\eta)$. It follows that $u^{-1}u' \in K$, i.e., $u' \in uK = K u$. Now Lemma 2.1 implies that there exists $y \in K^\times$ such that $u = yu'y^{-1}$. Conjugation by $y \in K^\times$ leaves $\eta$ invariant. We conclude that $\mathcal{O}_m = y\mathcal{O}_m'y^{-1}$.

It turns out that Lemma 4.7 holds for $G = A_4$ or $S_4$ as well (to be shown in Lemma 4.9 and Proposition 4.11, respectively). In Table 2, we list for each $G$ a representative in the conjugacy class of minimal $G$-orders and calculate its
discriminant (See Lemma 2.8 and 2.10). In each case, the existence of a minimal $G$-order determines $D$ uniquely up to isomorphism. Since all the the dihedral cases are similar, we only work out the details for $G = D_6$ in Proposition 4.8. Suppose that $\varepsilon = 2\vartheta^2$ with $\vartheta \in F^\times$ and $\alpha \in D$ satisfies $\alpha^2 = -1$. For ease of notation, we put $\sqrt{\varepsilon \alpha} := \vartheta(1 + \alpha)$ since $(\pm \vartheta(1 + \alpha))^2 = \varepsilon \alpha$. Throughout this paper,

$$(4.7) \quad \xi := (1 + i + j)/2 \in \left(\frac{-1, -1}{Q}\right) \subset \left(\frac{-1, -1}{F}\right).$$

| $G$ | condition on $\varepsilon$ | $D$ | minimal $G$-order | $\mathfrak{o}(O)$ |
|-----|-----------------|-----|----------------|----------------|
| $D_2^1$ | $N_F/Q(\varepsilon) = 1$ | $\left(\frac{-1}{p}\right)$ | $\mathcal{O}_2^1 := O_F[i, j]$ | $4O_F$ |
| $D_2^1$ | $N_F/Q(\varepsilon) = 1$ | $\left(\frac{-1}{p}\right)$ | $\mathcal{O}_2^1 := O_F[i, j]$ | $4O_F$ |
| $D_3^1$ | $N_F/Q(\varepsilon) = 1$ | $\left(\frac{-1}{p}\right)$ | $\mathcal{O}_3^1 := O_F[i, j]$ | $3O_F$ |
| $D_3^1$ | $N_F/Q(\varepsilon) = 1$ | $\left(\frac{-1}{p}\right)$ | $\mathcal{O}_3^1 := O_F[i, j]$ | $3O_F$ |
| $D_4$ | $2\varepsilon \in F^\times$ | $\left(\frac{-1}{p}\right)$ | $\mathcal{O}_4 := O_F + O_Fi + O_F\sqrt{\varepsilon}j + O_F\sqrt{\varepsilon}i$ | $2O_F$ |
| $D_6$ | $3\varepsilon \in F^\times$ | $\left(\frac{-1}{p}\right)$ | $\mathcal{O}_6 := O_F(j) + iO_F(j)$ | $O_F$ |
| $A_4$ | $O_{12} := O_F + O_Fi + O_Fj + O_F\xi$ | $\left(\frac{-1}{p}\right)$ | $O_{24} := O_F + O_F\sqrt{\varepsilon}i + O_F\sqrt{\varepsilon}j + O_F\xi$ | $O_F$ |

**Proposition 4.8.** There exists a minimal $D_6$-order in $D$ if and only if $3\varepsilon \in F^\times$ and $D = \left(\frac{-1, -1}{F}\right)$. Any minimal $D_6$-order is $D^\times$-conjugate to $\mathcal{O}_6 = O_F(j) + iO_F(j)$ and is a maximal order.

**Proof.** Suppose that $D$ contains a minimal $D_6$-order $\mathcal{O}_6 = O_F + O_Fu + O_F\eta + O_Fu\eta$ as in (4.2). Necessarily, $3\varepsilon \in F^\times$ by Subsection 4.3. According to Subsection 4.4, we may assume that $u^2 = -1$. Let $i := u$, and $j' := \eta^3/\varepsilon$. Then $j'^2 = -\varepsilon$ by Table 1 and $ij = j'i$ by (4.3). It follows that $D = \left(\frac{-1}{p}\right)$ and $\eta = \pm \xi(3 + j)/2$ with $j = j'/\xi$. Hence

$$(4.8) \quad \mathcal{O}_6 = O_F + O_Fi + O_F(3 + j)/2 + O_F\xi(3 + j)/2.$$ 

Since $O_F(j) = O_F + O_F(3 + j)/2$, we may write $\mathcal{O}_6 = O_F(j) + iO_F(j)$.

Conversely, one checks directly that $\mathcal{O}_6$ as stated is a minimal $D_6$-order. It is a maximal order because $\mathfrak{o}(\mathcal{O}_6) = O_F$. \hfill \Box

As a consequence, we have

$$(4.9) \quad t(D, D_6) = \begin{cases} 1 & \text{if } D = \left(\frac{-1, -1}{F}\right) \text{ and } 3\varepsilon \in F^\times; \\ 0 & \text{otherwise.} \end{cases}$$

Let $D_{2,\infty} = \left(\frac{1, -1}{q}\right)$, $D_{3,\infty} = \left(\frac{-1, -3}{q}\right)$, and $\xi$ be the element in (4.7). Define

$$(4.10) \quad \mathcal{O}_2 := \{Z[i, j] = Z + Zi + Zj + Zk \subset D_{2,\infty},$$

$$(4.11) \quad \mathcal{O}_2 := Z + Zi + Zj + Z\xi \subset D_{2,\infty},$$
Then $O_{4m}^1 = \varnothing_m \otimes \mathbb{Z} O_F$ for $m = 2, 3$. It is well known that both $\varnothing_2$ and $\varnothing_3$ are maximal orders in their respective quaternion algebras, and $[\varnothing_2 : \varnothing_2] = 2$.

**Lemma 4.9.** There exists a minimal $A_4$-order in $D$ if and only if $D = (\frac{-1 - \sqrt{3}}{2}) = D_{2, \infty} \otimes \mathbb{Q} F$. Every minimal $A_4$-order is $D^\times$-conjugate to $O_{12} := \varnothing_2 \otimes \mathbb{Z} O_F$.

**Proof.** Clearly, if $D = (\frac{-1 - \sqrt{3}}{2})$, then $O_{12}$ is a minimal $A_4$-order. Conversely, suppose that $D$ contains a minimal $A_4$-order $\mathcal{O}$. Let $G$ be a subgroup of $O^\times$ isomorphic to $A_1$. We claim that $G \supseteq D_{2, \infty}$, and hence $\mathcal{O}$ contains a minimal $D_{2, \infty}$-order. It then follows from Table 22 that $D = (\frac{-1 - \sqrt{3}}{2})$.

Recall that $O_{F, \mathcal{O}}/O_{F, \mathcal{O}}^2$ is either trivial or a cyclic group of order 2. Since $G \simeq A_4$ has no subgroup of index 2, it falls into

$$\ker \left( O^\times / O_{F, \mathcal{O}}^\times \xrightarrow{N_{G/F}} O_{F, \mathcal{O}}^\times / O_{F, \mathcal{O}}^\times \right) = (O_{F, \mathcal{O}}^\times / O_{F, \mathcal{O}}^\times) / O_{F, \mathcal{O}}^\times \cong \mathbb{O} / \{\pm 1\}.$$ 

In particular, the unique Sylow 2-subgroup $V$ of $G$ is isomorphic to $D_{2, \infty}$, and our claim is verified. It follows that there exists an isomorphism $D \simeq (\frac{-1 - \sqrt{3}}{2})$ such that $\mathcal{O} \supset O_{2, \infty}^2 = O_F[i, j]$ and $V = \{1, i, j, k\}$. Let $\Aut(V)$ be the group of automorphisms of $V$. The inner automorphisms of $G$ induces an embedding

$$G / V \hookrightarrow \Aut(V) \simeq S_3,$$

which identifies $G / V$ with the subgroup $A_3 \simeq \mathbb{Z} / 3\mathbb{Z}$ of $S_3$. In particular, there exists an element $\xi' \in G$ of order 3 such that conjugation by $\xi'$ induces the cyclic permutation $(i, j, k)$. Thus $\xi'i = \pm j \xi'$ for a representative $\xi' \in \mathcal{O}$ of $\xi'$. Changing the signs of $j$ and $\xi'$ if necessary, we may assume that

$$\xi'i = j \xi', \quad \text{and} \quad \xi'^2 - \xi' + 1 = 0.$$ 

Solving for $\xi' \in \mathcal{O}$, we find that $\xi' \in \{1 + k)(1 \pm i)/2\}$. Because $\mathcal{O} \supseteq O_F[i, j]$, both $(1 + k)(1 \pm i)/2$ lie in $\mathcal{O}$ if one of them does. Hence $\xi'$ can take either values, e.g. $\xi' = \xi = (1 + k)(1 + i)/2$. Therefore, $\mathcal{O} \supseteq O_{12}$, and the equality holds by the minimality of $\mathcal{O}$.

**Lemma 4.10.** Let $O_{12} = \varnothing_2 \otimes \mathbb{Z} O_F \subset (\frac{-1 - \sqrt{3}}{2})$. Then $O_{12}^* \simeq A_4$.

**Proof.** By the classification of finite subgroups of $SO_3(\mathbb{R})$, if $O_{12}^* \not\simeq A_4$, then $O_{12}^* \simeq S_4$ with $\varnothing_2^* / \{\pm 1\} \simeq A_4$ as its unique subgroup of index 2. If $\eta \in O_{12}^*$ represents an element of order 4 in $O_{12}^*$, then $F(\eta)$ coincides with one of the CM-subfields $F(i), F(j)$ or $F(k)$ in $D = (\frac{-1 - \sqrt{3}}{2})$ by Table 1. Without lose of generality, assume that $F(\eta) = F(i)$. Note that $O_{12} \cap F(i) = O_F[i]$. On the other hand, we have $2\varepsilon \in F^\times \setminus 1$, and $[O_F[\varepsilon] : O_F[i]] = 2$ by the classification in Subsection 7.1. The contradiction implies that $O_{12}^* \simeq A_4$.

**Proposition 4.11.** There exists a minimal $S_4$-order in $D$ if and only if $2\varepsilon \in F^\times \setminus 1$ and $D = (\frac{-1 - \sqrt{3}}{2})$. Every minimal $S_4$-order is $D^\times$-conjugate to $O_{24} = O_F + O_F\sqrt{\varepsilon_1} + O_F\sqrt{\varepsilon_2} + O_F \xi$ and is a maximal order. In particular,

$$t(D, S_4) = \begin{cases} 1 & \text{if } D = (\frac{-1 - \sqrt{3}}{2}) \text{ and } 2\varepsilon \in F^\times \setminus 1, \\ 0 & \text{otherwise}. \end{cases}$$
Lemma 2.12, order properly containing $O$ of order 4 in $\mathcal{O}^\ast_{24}$, we have $\mathcal{O}^\ast_{24} \simeq S_4$ by the classification in Subsection 4.3. Note that $\sqrt{\xi} = (2\theta - \sqrt{\xi})\xi \in \mathcal{O}_{24}$. The order $\mathcal{O}_{24}$ is maximal because $\mathfrak{d}(\mathcal{O}_{24}) = \mathcal{O}_F$.

Conversely, suppose that $\mathcal{O}$ is a minimal $S_4$-order in $D$. Thanks to Lemma 4.9 and Lemma 4.10, we may identify $D$ with $(\frac{-1 - \sqrt{-1}}{2})$ in such a way that $\mathcal{O}$ properly contains $\mathcal{O}_{12} = \mathfrak{o}_2 \otimes \mathbb{Z} \mathcal{O}_F$. Recall that $\mathfrak{o}_2$ is a maximal order in $D_0 = \left(\frac{-1 - \sqrt{-1}}{2}\right)$, which is ramified at 2 and splits at all other finite places of $\mathbb{Q}$. Hence for every prime $\ell \neq 2$, $\mathcal{O} \otimes \mathbb{Z}_\ell = \mathcal{O}_{12} \otimes \mathbb{Z}_\ell$, since the latter is maximal in $D \otimes \mathbb{Q}_\ell$.

Necessarily $2 \mathfrak{e} \in F^{\times 2}$ by Subsection 4.3 so $F$ is ramified over $\mathbb{Q}$ above 2. By Lemma 2.12, $\mathcal{O} \otimes \mathbb{Z}_2$ coincides with the unique maximal order of $D \otimes \mathbb{Q}_2$ containing $\mathcal{O}_{12} \otimes \mathbb{Z}_2$. It follows that $\mathcal{O}$ is not only a maximal order, but also the unique $\mathcal{O}$-order properly containing $\mathcal{O}_{12}$. But $\mathcal{O}_{24} \supsetneq \mathcal{O}_{12}$ is already such an order. Therefore, $\mathcal{O} = \mathcal{O}_{24}$, and the lemma is proved.

Proof. Suppose that $2\mathfrak{e} \in F^{\times 2}$ and $D = (\frac{-1 - \sqrt{-1}}{2})$. Clearly, $\mathcal{O}_{24} \supsetneq \mathcal{O}_{12}$. One checks by direct computation that $\mathcal{O}_{24}$ is an $\mathcal{O}_F$-order. Since $\sqrt{\xi}$ represents an element of order 4 in $\mathcal{O}^\ast_{24}$, we have $\mathcal{O}^\ast_{24} \simeq S_4$ by the classification in Subsection 4.3. Note that $\sqrt{\xi} = (2\theta - \sqrt{\xi})\xi \in \mathcal{O}_{24}$. The order $\mathcal{O}_{24}$ is maximal because $\mathfrak{d}(\mathcal{O}_{24}) = \mathcal{O}_F$.

Conversely, suppose that $\mathcal{O}$ is a minimal $S_4$-order in $D$. Thanks to Lemma 4.9 and Lemma 4.10, we may identify $D$ with $(\frac{-1 - \sqrt{-1}}{2})$ in such a way that $\mathcal{O}$ properly contains $\mathcal{O}_{12} = \mathfrak{o}_2 \otimes \mathbb{Z} \mathcal{O}_F$. Recall that $\mathfrak{o}_2$ is a maximal order in $D_0 = \left(\frac{-1 - \sqrt{-1}}{2}\right)$, which is ramified at 2 and splits at all other finite places of $\mathbb{Q}$. Hence for every prime $\ell \neq 2$, $\mathcal{O} \otimes \mathbb{Z}_\ell = \mathcal{O}_{12} \otimes \mathbb{Z}_\ell$, since the latter is maximal in $D \otimes \mathbb{Q}_\ell$.

Necessarily $2 \mathfrak{e} \in F^{\times 2}$ by Subsection 4.3 so $F$ is ramified over $\mathbb{Q}$ above 2. By Lemma 2.12, $\mathcal{O} \otimes \mathbb{Z}_2$ coincides with the unique maximal order of $D \otimes \mathbb{Q}_2$ containing $\mathcal{O}_{12} \otimes \mathbb{Z}_2$. It follows that $\mathcal{O}$ is not only a maximal order, but also the unique $\mathcal{O}$-order properly containing $\mathcal{O}_{12}$. But $\mathcal{O}_{24} \supsetneq \mathcal{O}_{12}$ is already such an order. Therefore, $\mathcal{O} = \mathcal{O}_{24}$, and the lemma is proved.

Let $K = F(i) \subset \left(\frac{-1 - \sqrt{-1}}{2}\right)$, and

$$B := \begin{cases} O_K & \text{if } d \equiv 2 \pmod{4}; \\ O_F + \mathfrak{p}O_K & \text{if } d \equiv 3 \pmod{4}; \end{cases}$$

(4.14)

where $\mathfrak{p}$ denotes the unique dyadic prime of $F$. In both cases, we have $\chi(B, O_F[i]) = \mathfrak{p}$. Suppose that $2\mathfrak{e} \in F^{\times 2}$. Then

$$B = O_F[\sqrt{\mathfrak{e}}], \quad \text{and} \quad \mathcal{O}_{24} = B + B\xi.$$  

(4.15)

**Remark 4.12.** Since all automorphisms of $S_4$ are inner, any two isomorphisms $S_4 \simeq \mathcal{O}^\ast_{24}$ differ by a conjugation. There are two conjugacy classes of elements of order 2 in $S_4$. The conjugacy class of transpositions corresponds to the set $\{\bar{u} \in \mathcal{O}^\ast_{24} \mid \text{ord}(\bar{u}) = 2, \text{Nr}(\bar{u}) = \mathfrak{e}\}$. The remaining conjugacy class corresponds to $\{\bar{i}, \bar{j}, \bar{k}\} \subseteq \mathcal{O}^\ast_{24}$. It follows that $O_F[i, j]$ is the unique minimal $D_2$-suborder of $\mathcal{O}_{24}$. On the other hand, $O_F[i, \vartheta(j + k)]$ is a minimal $D_2$-suborder of $\mathcal{O}_{24}$. Any other minimal $D_2$-suborder of $\mathcal{O}_{24}$ is $\mathcal{O}^\ast_{24}$-conjugate to it. We have $O_F[i, \vartheta(j + k)] \not\subseteq O_F + (2\vartheta)\mathcal{O}_{24}$ since the latter order does not contain $\vartheta(j + k)$. Note that $\mathcal{O}_{24}$ contains no minimal $D_2$-suborders since $\mathcal{O}^\ast_{24} = \mathcal{O}^\ast_{12}$ and $A_4$ contains no subgroup of index 2.

We make a few observations based on Table 2

**Corollary 4.13.** If $D$ is not isomorphic to any of the quaternion algebras in Table 2 (e.g. $\mathfrak{d}(D) \nmid 6O_F$), then $\mathcal{O}^\ast$ is cyclic for every $O_F$-order $\mathcal{O} \subset D$.

**Proof.** If $G := \mathcal{O}^\ast$ is non-cyclic, then $\mathcal{O}$ contains a minimal $G$-order. Thus $D$ is necessarily isomorphic to one of the quaternion algebras listed in Table 2.

**Corollary 4.14.** Let $G$ be one of the non-cyclic groups listed in the table of Subsection 4.3. If $\mathcal{O}$ is a minimal $G$-order, then $\mathcal{O}^\ast \simeq G$.

**Proof.** The case that $G = A_4$ is already proved in Lemma 4.10. In general, if $G' := \mathcal{O}^\ast$ contains $G$ as a proper subgroup, then $\mathcal{O}$ contains a minimal $G'$-order $\mathcal{O}'$. However, Table 2 shows that $\mathfrak{d}(\mathcal{O}')$ is a proper divisor of $\mathfrak{d}(\mathcal{O})$ for all pairs of groups $G \subseteq G'$. This leads to a contradiction and forces $\mathcal{O}^\ast = G$. 

□
Lemma 4.15. Let \( \mathcal{O} \) be one of the minimal \( G \)-orders in Table 2. Then the kernel of the natural homomorphism \( \varphi : \mathcal{N}(\mathcal{O}) \to \text{Aut}(\mathcal{O}^*) \) is given as follows

\[
\ker(\varphi) = \begin{cases} 
F^\times \mathcal{O}^x & \text{if } \mathcal{O}^* \simeq D_2; \\
F^\times (j) & \text{if } \mathcal{O}^* \simeq D_m \text{ with } m \in \{3, 4, 6\}; \\
F^\times & \text{if } \mathcal{O}^* \simeq A_4 \text{ or } S_4.
\end{cases}
\]

Proof. Let \( \tilde{v} \in \mathcal{O}^* \) be a nontrivial element represented by \( v \in \mathcal{O}^x \), and \( x \in \ker(\varphi) \subseteq \mathcal{N}(\mathcal{O}) \). Since \( xv^{-1} = \tilde{v} \), we have \( xF(v)x^{-1} = F(\tilde{v}) \), so either \( xvx^{-1} = v \) or \( xvx^{-1} = \tilde{v} \). The latter case is possible only if \( \tilde{v}/v \in \mathcal{O}_F^x \). On the other hand, \( \tilde{v}/v \) is a root of unity in the CM-field \( F(v) \). So necessarily \( \tilde{v} = -v \), i.e. \( \mathcal{O}(v) \) is a minimal \( D_m \)-order with \( i^2 \in \{-1, -\varepsilon\} \) and \( m = \mathcal{O}(v) \geq 3 \). Note that \( F(\eta) = F(j) \) for all \( \mathcal{O} \) in this case. Given any \( x \in \ker(\varphi) \), if \( xix^{-1} = i \), then \( x \in F(i)^x \cap F(j)^x = F^\times \), otherwise \( xix^{-1} = -i \), and hence \( x \in F^\times j \). It follows that \( \ker(\varphi) = F^\times \cup F^\times j = F^\times (j) \) in this case.

Next, suppose that \( \mathcal{O} = F^\times (i, j) \) in either \( \{-\frac{1+\varepsilon}{2}, \frac{1+\varepsilon}{2}\} \). For any \( x \in \ker(\varphi) \), we have \( xix^{-1} = \pm i \) and \( xjx^{-1} = \pm j \). There exists a suitable element in \( \{i, j, k\} \) whose product with \( x \) commutes with both \( i \) and \( j \), and hence lie in \( F^\times \). Therefore, \( \ker(\varphi) = F^\times \mathcal{O}^x \). □

Since we can write down \( \text{Aut}(G) \) for every \( G \) in Table 2 it is a simple exercise to work out the normalizer \( \mathcal{N}(\mathcal{O}) \) for each minimal \( G \)-order \( \mathcal{O} \). Note that for \( \mathcal{O}^* \simeq D_m \) with \( m = 4, 6 \), the non-central elements of order 2 fall into two conjugacy classes with distinct reduced norms. Hence the image of \( \varphi \) coincides with the inner automorphism group \( \text{Inn}(\mathcal{O}^*) \) in this case. For a set of elements \( S \subset D^\times \), let \( F^\times \mathcal{O}^x \langle S \rangle \) be the subgroup of \( D^\times \) generated by \( F^\times \mathcal{O}^x \) and \( S \). Then

\[
\begin{align*}
\mathcal{N}(\mathcal{O}_2^1) &= F^\times (\mathcal{O}_2^1)^x \langle 1 + i, 1 + j \rangle, \\
\mathcal{N}(\mathcal{O}_2^1) &= F^\times (\mathcal{O}_2^1)^x \langle 1 + i \rangle, \\
\mathcal{N}(\mathcal{O}_3^1) &= F^\times (\mathcal{O}_3^1)^x \langle j \rangle, \\
\mathcal{N}(\mathcal{O}_3^1) &= F^\times (\mathcal{O}_3^1)^x \langle 1 + i \rangle, \\
\mathcal{N}(\mathcal{O}_2^1) &= F^\times \mathcal{O}_2^1 \langle 1 + i \rangle, \\
\mathcal{N}(\mathcal{O}_2^1) &= F^\times \mathcal{O}_2^1 \langle 1 + i \rangle, \\
\mathcal{N}(\mathcal{O}_2^1) &= F^\times \mathcal{O}_2^1 \langle 1 + i \rangle.
\end{align*}
\]

Let us denote \( \overline{\mathcal{N}}(\mathcal{O}) := \mathcal{N}(\mathcal{O})/F^\times \mathcal{O}^x \) for any order \( \mathcal{O} \subset D \). Then \( \overline{\mathcal{N}}(\mathcal{O}_2^1) \simeq S_4 \), and \( \overline{\mathcal{N}}(\mathcal{O}_2^1) \simeq \mathbb{Z}/2\mathbb{Z} \) if \( \mathcal{O} \) is isomorphic to one of the orders \( \mathcal{O}_2^1, \mathcal{O}_2^1, \mathcal{O}_2^1, \mathcal{O}_2^1, \mathcal{O}_2^1 \). The natural action of \( \mathcal{N}(\mathcal{O}) \) on the set \( \mathcal{S}(\mathcal{O}) \) of maximal orders containing \( \mathcal{O} \) descends to \( \overline{\mathcal{N}}(\mathcal{O}) \). The number of orbits is denoted by

\[
\overline{\mathcal{S}}(\mathcal{O}) := |\overline{\mathcal{N}}(\mathcal{O})/\overline{\mathcal{S}}(\mathcal{O})| = |\mathcal{N}(\mathcal{O})/\mathcal{S}(\mathcal{O})|.
\]

Lemma 4.16. Let \( \mathcal{O} \) be a minimal \( D_s \)-orders with \( s = 2, 3 \) in Table 2. If \( \mathcal{O}, \mathcal{O}' \in \mathcal{S}(\mathcal{O}) \) are two distinct \( D^\times \)-conjugate maximal orders containing \( \mathcal{O} \), then there exists \( x \in \mathcal{N}(\mathcal{O}) \) representing a nontrivial element of \( \overline{\mathcal{N}}(\mathcal{O}) \) such that \( \mathcal{O}' = x\mathcal{O}x^{-1} \).

Proof. For simplicity, we only prove the lemma for \( \mathcal{O} = \mathcal{O}_2^1 \). The remaining cases are proved similarly and hence omitted. Suppose that \( \mathcal{O}_2^1 \subseteq \mathcal{O} \cap \mathcal{O}' \) and...
there exists \( y \in D^\times \) such that \( \mathcal{O}' = y\mathcal{O}y^{-1} \). The proof of Lemma 4.19 shows that \( \mathcal{O}^* \not\simeq A_4 \). So \( \mathcal{O}^* \simeq \mathcal{O}'^* \) are isomorphic to one of the following groups: \( D_2^1, D_4, D_6 \) or \( S_4 \). Note that \( D_4 = \mathcal{O}_4^* \) contains a unique subgroup isomorphic to \( D_2^1 \) (the only other subgroup isomorphic to \( D_2 \) is of type I). The three Sylow 2-subgroups of \( D_6 = \mathcal{O}_6^* \) are isomorphic to \( D_2^1 \) and they are all conjugate. Lastly, there is a unique normal subgroup of \( S_4 \simeq \mathcal{O}_4^* \) isomorphic to \( D_2^1 \), namely \((1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\). All the three non-normal subgroups isomorphic to \( D_2 \) are of type II, and they lie in the same conjugacy class. Therefore, in all cases, \((y\mathcal{O}_2^1y^{-1})^* \) is conjugate to \((\mathcal{O}_2^1)^* \) as subgroups of \( \mathcal{O}'^* \). Let \( x \) be the product of a suitable element of \( \mathcal{O}'^* \) with \( y \), we then have

\[ \mathcal{O}' = x\mathcal{O}x^{-1} \text{ and } \mathcal{O}_2^1 = x\mathcal{O}_2^1x^{-1}. \]

Necessarily \( x \not\in F^x(\mathcal{O}_2^1)^* \subseteq F^x\mathcal{O}^* \) since \( \mathcal{O}' \neq \mathcal{O} \) by the assumption. \( \square \)

Therefore, if \( \mathcal{O} \) is a minimal \( D_s \)-order of either type with \( s \in \{2, 3\} \), then \( 2(\mathcal{O}) \) is the number of conjugacy classes of maximal orders containing \( \mathcal{O} \).

5. Maximal orders with non-cyclic reduced unit groups: part I

Let \( D \) be a totally definite quaternion algebra over a real quadratic field \( F = \mathbb{Q}(\sqrt{d}) \) with \( d \geq 6 \). We study all the maximal \( O_F \)-orders with non-cyclic reduced unit group \( G \) in \( D \). After a suitable conjugation, such a maximal order contains one of the minimal \( G \)-orders in Table 2. It has already been shown in Proposition 4.8 and Proposition 4.11 respectively that the maximal order with reduced unit group \( D_6 \) or \( S_4 \) is unique up to conjugation if it exists. For ease of exposition, we restrict to the cases \( G \in \{A_4, D_4, D_2^1, D_3^1\} \) in this section. The cases where \( G \in \{D_2^1, D_3^1\} \) are postponed to the next section.

**Proposition 5.1.** We have

\[
\begin{align*}
t(D, A_4) &= \begin{cases} 
1 & \text{if } D = (\frac{-1}{d}) \text{ and } 2\mathcal{E} \not\in F^x; \\
0 & \text{otherwise}.
\end{cases}
\end{align*}
\]

Let \( \mathcal{O}_{12} \subset (\frac{-1}{d}) \) be a maximal order with \( \mathcal{O}_{12}^* \simeq A_4 \). Then

\[
N(\mathcal{O}_{12}) = \begin{cases} 
F^x\mathcal{O}_{12}^* & \text{if } d \equiv 5 \pmod{8}; \\
F^x\mathcal{O}_{12}(1+i) & \text{otherwise}.
\end{cases}
\]

**Proof.** Let \( \mathcal{O} \) be a maximal order in \( D \) with \( \mathcal{O}^* \simeq A_4 \). Then by Lemma 4.9 \( D = (\frac{-1}{d}) \), and we may assume that \( \mathcal{O} \supseteq \mathcal{O}_{12} \). Necessarily, \( 2\mathcal{E} \not\in F^x \), otherwise \( \mathcal{O} = \mathcal{O}_{24} \), which has reduced unit group \( S_4 \).

Conversely, suppose that \( D = (\frac{-1}{d}) \) and \( 2\mathcal{E} \not\in F^x \). Any maximal order \( \mathcal{O} \) containing \( \mathcal{O}_{12} = q_2 \mathcal{O}_2\mathcal{O}_F \) necessarily has \( \mathcal{O}^* \simeq A_4 \) by Subsection 4.1. This implies that \( \mathcal{O}^* = \mathcal{O}_{12}^* \), and according to (4.18),

\[
N(\mathcal{O}) \subseteq N(\mathcal{O}_{12}) = F^x\mathcal{O}_{12}^*(1+i) = F^x\mathcal{O}^*(1+i).
\]

We show all maximal orders in \( \mathcal{C}(\mathcal{O}_{12}) \) are \( D^x \)-conjugate. If \( F \) splits at 2, then \( \mathcal{O}_{12} \) is already a maximal order. In the remaining cases, there is a unique dyadic prime \( p \) of \( F \), and \( D \) splits at all finite places of \( F \). If \( F \) is ramified at 2, then \( e_F(\mathcal{O}_{12}) = -1 \) and there is a unique maximal order \( \mathcal{O} \) properly containing \( \mathcal{O}_{12} \) by Lemma 2.12. If \( F \) is inert at 2, i.e.
\( d \equiv 5 \pmod{8} \), then \( e_p(O_{12}) = 1 \) and \( O_{12} \) is an Eichler order of level \( p = 2O_F \) by Lemma \[2.11\]. Let \( \mathcal{O} \) and \( \mathcal{O}' \) be the two maximal orders containing \( O_{12} \). Note that \((1 + i) \in \mathcal{N}(O_{12})\), but \((1 + i) \notin \mathcal{N}(\mathcal{O})\) since it is odd at \( p \) (See Subsection \[2.2\]). Therefore, \((1 + i)\mathcal{O}(1 + i)^{-1} = \mathcal{O}'\), and \( \mathcal{N}(\mathcal{O}) = F^\times \mathcal{O}^\times \) by \[(5.2)\]. Lastly, if \( d \neq 5 \pmod{8} \), then \( \text{det}(\mathcal{O}_{12}) = 1 \), i.e. there is a unique maximal order \( \mathcal{O}_{12} \) containing \( O_{12} \). So \( \mathcal{N}(\mathcal{O}_{12}) = \mathcal{N}(\mathcal{O}_{12}) \). \( \square \)

Recall that \( \xi = (1+i+j+k)/2 \in \{ \frac{1-\sqrt{-d}}{p} \} \) as defined in \[(4.7)\]. A direct calculation shows that the dual basis of \( \{1, i, j, \xi\} \subset \{ \frac{1-\sqrt{-d}}{p} \} \) is

\[
\begin{align*}
&\left\{ \frac{1+k}{2}, \frac{-i+k}{2}, \frac{-j+k}{2}, \frac{-k}{2} \right\}.
\end{align*}
\]

If \( 2 \) is inert in \( F \), i.e. \( d \equiv 5 \pmod{8} \), then

\[
O_{12} = O_F + O_F \frac{(1 + \sqrt{d}) - 2i + (1 - \sqrt{d})j}{4} + O_F j + O_F \xi \subset O_{12}^\prime
\]

is one of the two conjugating maximal orders in \( \mathfrak{S}(O_{12}) \). Let \( O_{12} \) be the unique maximal order in \( \mathfrak{S}(O_{12}) \) in the remaining cases. If \( d \equiv 1 \pmod{8} \), then \( O_{12} = O_{12} \); and if \( d \equiv 2, 3 \pmod{4} \), then \( O_{12} = B + B\xi \), where \( B \) is defined in \[(4.14)\].

**Definition 5.2.** Suppose that \( 2 \) is ramified in \( F \), and \( D = (\frac{-1}{p}) \). Let \( L \) be the following subfield of \( D \):

\[
L = \begin{cases} 
F((1+i+j+k)/2) \simeq F(\sqrt{-(d+1)}) & \text{if } d \equiv 2 \pmod{4}; \\
F(j) \simeq F(\sqrt{-1}) & \text{if } d \equiv 3 \pmod{4}.
\end{cases}
\]

If \( 2\varepsilon \in F^\times \), then we denote the order \( O_L + iO_L \) by \( \mathfrak{O}_8 \), otherwise we denote it by \( \mathfrak{O}_4 \). More explicitly,

\[
O_L + iO_L = \begin{cases} 
O_F + O_F i + O_F \frac{1+\sqrt{d}+j}{2} + O_F \frac{-\sqrt{d}+i+k}{2} & \text{if } d \equiv 2 \pmod{4}; \\
O_F + O_F i + O_F \frac{\sqrt{d}+j}{2} + O_F \frac{-\sqrt{d}+i+k}{2} & \text{if } d \equiv 3 \pmod{4}.
\end{cases}
\]

We leave it as an exercise to show that \( \mathfrak{d}(O_L + iO_L) = O_F = \mathfrak{d}(D) \) in both cases, so the order is maximal. Since \( (O_L + iO_L) \cap F(i) = O_F[i] \neq B \), we have \( O_L + iO_L \neq B + B\xi \).

**Proposition 5.3.** We have

\[
t(D, D_4) = \begin{cases} 
1 & \text{if } D = \left( \frac{-1}{p} \right) \text{ and } 2\varepsilon \in F^\times; \\
0 & \text{otherwise}.
\end{cases}
\]

In particular,

\[
t(D, D_4) = t(D, S_4) \quad \text{for all } D.
\]

When \( t(D, D_4) = 1 \), any maximal order \( \mathcal{O} \) with \( \mathcal{O}^\times \simeq D_4 \) is \( D^\times \)-conjugate to \( \mathfrak{O}_8 \) in Definition \[5.3\]. Moreover,

\[
\mathcal{N}(\mathfrak{O}_8) = F^\times \mathfrak{O}_8^\times.
\]

**Proof.** By Table \[2\] there exists a minimal \( D_4 \)-order only if \( D = \left( \frac{-1}{p} \right) \) and \( 2\varepsilon \in F^\times \). We show that \( t(D, D_4) = 1 \) in this case. Let \( p = (2\varepsilon)O_F \) be the unique dyadic prime of \( F \), where \( 2\varepsilon^2 = \varepsilon \). By \[8\] Corollary 1.6, \( \mathcal{O}_4 = O_F[i, \sqrt{\varepsilon}] \) is a Bass order since \( \mathfrak{d}(\mathcal{O}_4) = 2O_F = p^2 \) is cube-free. Note that \( i^2 \equiv (\sqrt{\varepsilon})^4 \equiv 1 \pmod{p} \). The same proof as that of Lemma \[2.8\] shows that \( \mathcal{O}_4 \) is maximal at every nonzero prime
ideal of $O_F$ coprime to 2, and the Eichler invariant $e_p(\mathcal{O}_4) = 0$. It then follows from Lemma 2.4 that $O_{24}$ and $O_8$ are the only two maximal orders containing $\mathcal{O}_4$. The order $O_8$ cannot be $D^\times$-conjugate to $O_{24}$, because $O_8 \cap F(i) = O_F[i]$, which is a proper suborder of $B = O_F[\sqrt{\varepsilon i}]$ by Subsection 7.1. Since $O_{24}$ is the unique minimal $S_4$-order up to conjugation, we have $O_8^* = \mathcal{O}_4^* \simeq D_4$, and hence $\mathcal{N}(O_8) \subseteq \mathcal{N}(\mathcal{O}_4) = F^\times \mathcal{O}_4^\times$. Therefore, \begin{equation}
abla(O_8) = F^\times \mathcal{O}_4^\times = F^\times O_8^*.
\end{equation}

5.4. It might be worthwhile to explain where the orders in (5.5) come from. Consider the following overorder of $\mathcal{O}_4$:
\begin{equation}
\mathcal{O} = O_F[i, \sqrt{\varepsilon j}, \xi - \sqrt{\varepsilon i}] = O_F + O_F i + O_F \sqrt{\varepsilon j} + O_F (\xi - \sqrt{\varepsilon i}).
\end{equation}

Since $\chi(\mathcal{O}, \mathcal{O}_4) = p$, the order $\mathcal{O}$ is the unique minimal overorder of $\mathcal{O}_4$. On the other hand, $\mathfrak{d}(\mathcal{O}) = p$ and $D$ splits at $p$, so $\mathcal{O}$ is an Eichler order of level $p$. A lengthy but straightforward calculation shows that the dual basis of $\{1, i, \sqrt{\varepsilon j}, \xi - \sqrt{\varepsilon i}\}$ is
\[
\begin{pmatrix}
1 + j - 2dk, & -i + (1 - 2\theta)k, & -j + k, & -k
\end{pmatrix}
\]
When $d \equiv 2$ (mod 4), we have $2\theta \equiv \sqrt{d}$ (mod 2$O_F$), and hence
\[
\mathcal{O}^\vee = O_F \frac{1 + j - \sqrt{d}k}{2} + O_F \frac{i + (\sqrt{d} - 1)k}{2} + O_F \theta(j + k) + O_F k;
\]
\[
O_8 = \mathcal{O} / \mathcal{O}^\vee = O_F + O_F i + O_F \frac{1 + \sqrt{d}i + j}{2} + O_F \frac{-\sqrt{d} + i + k}{2}.
\]
When $d \equiv 3$ (mod 4), we have $2\theta \equiv 1 + \sqrt{d}$ (mod 2$O_F$), and hence
\[
\mathcal{O}^\vee = O_F \frac{1 + j - (1 + \sqrt{d})k}{2} + O_F \frac{i + \sqrt{d}k}{2} + O_F \theta(j + k) + O_F k;
\]
\[
O_8 = \mathcal{O} / \mathcal{O}^\vee = O_F + O_F i + O_F \frac{\sqrt{d} + j}{2} + O_F \frac{\sqrt{d}i + k}{2}.
\]

Proposition 5.5. We have
\[
t(D, D_2) = \begin{cases}
1 & \text{if } D = \left(\frac{-1}{p}\right), \left(\frac{\ell}{\mathbb{Q}}\right) = 0 \text{ and } 2\varepsilon \notin F^\times \mathbb{Z};
0 & \text{otherwise;}
\end{cases}
\]
where the Artin symbol $\left(\frac{\ell}{\mathbb{Q}}\right) = 0$ if and only if 2 is ramified in $F$. Any maximal order $\mathfrak{O}$ with $\mathfrak{O}^\times \simeq D_2^\times$ is conjugate to $\mathfrak{O}_1 = \mathcal{O}_L + i\mathcal{O}_L$ in (5.3). Moreover, \[
\mathcal{N}(\mathfrak{O}_1) = F^\times (\mathfrak{O}_1^\times \mathfrak{O}_1^\times)(1 + i).
\]

Proof. We focus on the case that $D = \left(\frac{-1}{p}\right)$ since $t(D, D_2^\dagger) = 0$ otherwise. Thanks to Lemma 2.3, $\mathcal{O}_2 = O_F[i, j]$ is a Gorenstein order maximal at every prime $\ell \neq 2$. We study the maximal orders in $D$ containing $\mathcal{O}_2^\dagger$.

If $\left(\frac{\ell}{\mathbb{Q}}\right) = 1$, i.e. $F$ splits above 2, then $t(D, D_2^\dagger) = 0$. Indeed, $D$ is ramified at the two places of $F$ above 2 in this case, and $\mathfrak{O}_{12}$ is the unique maximal order containing $\mathcal{O}_2^\dagger$ with $\mathfrak{O}_{12}^\times \simeq A_4$. Suppose that $\left(\frac{\ell}{\mathbb{Q}}\right) \neq 1$ and let $p$ be the unique dyadic prime of $F$. Then $e_p(\mathcal{O}_2^\dagger) = 0$ by Lemma 2.3. It follows from [6 Proposition 4.1] that there is a unique minimal overorder $\mathfrak{O}$ of $\mathcal{O}_2^\dagger$, and $\chi(\mathfrak{O}, \mathcal{O}_2^\dagger) = p$. In particular, $\mathfrak{O}_{12} \supseteq \mathfrak{O}$,
and the equality holds if \( (-\frac{2}{3}) \) = \(-1\), forcing every maximal order containing \( \theta_1^\perp \) to contain \( \Omega_{12} \) as well. Therefore, \( t(D, D_1^\perp) \neq 0 \) only if \( (-\frac{2}{3}) \) = \( 0 \), which we assume for the rest of the proof.

Recall that \( \Omega_0 := B + B\xi \) is the unique maximal order containing \( \Omega_{12} = \sigma_2 \otimes O_F \). By [3, Proposition 3.1], the Jacobson radical \( \mathfrak{J}(\Omega_{12} \otimes \mathbb{Z}_2) = p\Omega_0 \otimes \mathbb{Z}_2 \). Let \( \mathcal{O}' \) be the unique suborder of \( \Omega_{12} \) such that

\[
\mathcal{O}' \otimes \mathbb{Z}_2 = O_F \otimes \mathbb{Z}_2 + p\Omega_0 \otimes \mathbb{Z}_2 \quad \text{and} \quad \mathcal{O}' \otimes \mathbb{Z}_2 = \Omega_{12} \otimes \mathbb{Z}_2, \forall \ell \neq 2.
\]

Recall that \( e_\mathcal{O}(\Omega_{12}) = -1 \), i.e., \( (\Omega_{12} \otimes \mathbb{Z}_2)/\mathfrak{J}(\Omega_{12} \otimes \mathbb{Z}_2) \simeq F_4 \). The image of \( \theta_1^\perp \otimes \mathbb{Z}_2 \) in this quotient is \( F_2 \) because \( i^2 = j^2 = -1 \). Therefore, \( \theta_1^\perp \subseteq \mathcal{O}' \). Since \( \chi(\mathcal{O}', \theta_1^\perp) = \chi(\Omega_{12}, \theta_1^\perp)/\chi(\Omega_{12}, \mathcal{O}') = p^2/p = p \), the order \( \mathcal{O}' \) coincides with the minimal overorder \( \mathcal{O} \) of \( \theta_1^\perp \). It follows from (5.10) that \( \mathcal{N}(\theta_1^\perp) = \mathcal{N}(\theta_2^\perp) = 4 \). More precisely, the subtree \( \Sigma(\theta_2^\perp \otimes \mathbb{Z}_2) \) of the Bruhat-Tits tree of \( D \otimes \mathbb{Q}_2 \) is a star centered at \( \Omega_0 \otimes \mathbb{Z}_2 \) with 3 external vertices.

Clearly, \( \Omega_0 \) is fixed under the action of \( \mathcal{N}(\theta_1^\perp) \) on \( \mathcal{G}(\theta_1^\perp) \). By Lemma 3.1, \( \Omega_0 \) is not \( D^\perp \)-conjugate to any other maximal order in \( \mathcal{G}(\theta_1^\perp) \). Let \( \mathcal{G}'(\theta_1^\perp) := \mathcal{G}(\theta_1^\perp) \setminus \{ \Omega_0 \} \), which contains the order \( O_L + iO_L \) defined in (5.5). We claim that the action of \( \xi = (1 + i + j + k)/2 \in \mathcal{N}(\theta_1^\perp) \) on \( \mathcal{G}'(\theta_1^\perp) \) is transitive. Otherwise, \( \xi \) lies in the normalizer of one of its members, say \( \mathcal{O}' \). Then \( \xi \in \mathcal{O}' \) by Lemma 2.3 and hence \( \mathcal{O}' \) contains \( \Omega_{12} = \theta_1^\perp + O_F\xi \) as well. But this contradicts the uniqueness of \( \Omega_0 \) as an overorder of \( \Omega_{12} \). Since \( \xi \) generates the only nontrivial normal proper subgroup of \( \mathcal{N}(\theta_1^\perp) \simeq S_3 \), the action of \( \mathcal{N}(\theta_1^\perp) \) on \( \mathcal{G}'(\theta_1^\perp) \) identifies \( \mathcal{N}(\theta_1^\perp) \) with the full symmetric group on \( \mathcal{G}'(\theta_1^\perp) \).

Lastly, if \( 2\varepsilon \in F^{\times 2} \), then the orbits of \( \mathcal{N}(\theta_1^\perp) \setminus \mathcal{G}(\theta_1^\perp) \) are represented by \( \Omega_0 = \Omega_{24} \) and \( \Omega_8 = O_L + iO_L \), with \( \Omega_{24} \simeq S_4 \) and \( \Omega_8 \simeq D_4 \) respectively. Thus there are no maximal orders \( \mathcal{O} \) with \( \mathcal{O} \simeq \theta_1^\perp \) in this case. If \( 2\varepsilon \not\in F^{\times 2} \), then \( \mathcal{G}'(\theta_2^\perp) \geq D_2^\perp \) for every \( \mathcal{O}' \in \mathcal{G}'(\theta_2^\perp) \), but \( \mathcal{G}'(\theta_2^\perp) \not\geq A_4 \) since \( \mathcal{O}' \) is not conjugate to \( \Omega_0 = \Omega_{12} \). We conclude that \( \mathcal{O} \simeq D_2^\perp \) by the classification in Subsection 4.3. The three maximal orders in \( \mathcal{G}'(\theta_2^\perp) \) are \( D^\perp \)-conjugate as already observed. Any maximal order with reduced unit group \( D_1^\perp \) is conjugate to \( \mathcal{O}_1^\perp = O_L + iO_L \). Since \( (\mathcal{O}_1^\perp)^\times = (\theta_2^\perp)^\times \) and \( \theta_2^\perp \) is generated over \( O_F \) by its units, we have \( \mathcal{N}(\mathcal{O}_1^\perp) \subseteq \mathcal{N}(\theta_2^\perp) \). One verifies directly that \( (1 + i) \in \mathcal{N}(\mathcal{O}_1^\perp) \), but \( \xi \not\in \mathcal{N}(\mathcal{O}_1^\perp) \) as demonstrated. It follows that

\[
\mathcal{N}(\mathcal{O}_1^\perp) = F^\times (\theta_2^\perp)^\times (1 + i) = F^\times (\mathcal{O}_1^\perp)^\times (1 + i).
\]

Lastly, we study the maximal orders with reduced unit group \( D_3^\perp \).

**Proposition 5.6.** We have

\[
t(D, D_3^\perp) = \begin{cases} 1 & \text{if } D \simeq (-\frac{1}{2}, -\frac{3}{2}) \text{ and } 3\varepsilon \not\in F^{\times 2}; \\ 0 & \text{otherwise.} \end{cases}
\]

Let \( \mathcal{O}_3^\perp \subseteq (-\frac{1}{2}, -\frac{3}{2}) \) be a maximal order with \( \mathcal{O}_3^\perp \simeq D_3^\perp \). Then

\[
\mathcal{N}(\mathcal{O}_3^\perp) = \begin{cases} F^\times (\mathcal{O}_3^\perp)^\times & \text{if } d \equiv 2 \pmod{3}; \\ F^\times (\mathcal{O}_3^\perp)^\times (j) & \text{otherwise.} \end{cases}
\]

Recall that \( \theta_3^\perp = \sigma_3 \otimes O_F \), where \( \sigma_3 \subseteq (-\frac{1}{2}, -\frac{3}{2}) \) is the maximal \( \mathbb{Z} \)-order defined in (4.12). It is pointed out in Remark 5.12 that the minimal \( S_4 \)-order \( \Omega_{24} \) does not
contain any minimal $D_1^f$-orders. The proof of Proposition 5.6 is similar to that of Proposition 5.1 and hence omitted.

If $d \equiv 1 \pmod{3},$ then 3 splits in $F,$ and $D = \left( \frac{-1 - \sqrt{-3}}{F} \right)$ is ramified at the two primes of $F$ above 3. In this case, we set $O_3^f = \mathcal{O}_3^f$ since it is already maximal. If $3 \mid d$ and $3 \varepsilon \notin F^{x^2},$ then we set $O_3^f = O_{F(j)} + iO_{F(j)},$ which is the unique maximal order containing $\mathcal{O}_3^f.$ Lastly, suppose that $d \equiv 2 \pmod{3}.$ By (2.7), the dual lattice of $\mathcal{O}_3^f$ is

\[(5.12) \quad (\mathcal{O}_3^f)^\vee = O_F \frac{3 + j}{6} + O_F \frac{-3i + k}{6} + O_F \frac{j}{3} + O_F \frac{k}{3}.\]

We define

\[(5.13) \quad \mathcal{O}_3^f = \mathcal{O}_3^f + O_F \frac{\sqrt{d}j + k}{3} = O_F + O_F \frac{i + k}{2} + O_F \frac{1 + j}{2} + O_F \frac{\sqrt{d}j + k}{3}.\]

Any maximal order $\mathcal{O}$ with $\mathcal{O}^\star \simeq D_3^f$ is $D^\times$-conjugate to $\mathcal{O}_3^f.$

6. MAXIMAL ORDERS WITH NON-CYCLIC REDUCED UNIT GROUPS: PART II

We keep the notation and assumptions of Section 5 and study the maximal orders with reduced unit groups $D_2^f$ or $D_3^f.$ In particular, $F = \mathbb{Q}(\sqrt{d})$ with $d \geq 6.$ Assume further that the fundamental unit $\varepsilon \in O_F^\times$ has $N_{F/\mathbb{Q}}(\varepsilon) = 1$ throughout this section.

We first write down the ramified places of $\left( \frac{-1 - \sqrt{-3}}{F} \right).$ By Lemma (7.1) if $d \equiv 1 \pmod{8},$ then $\varepsilon$ is of the form $a + bv_d \in \mathbb{Z}[\sqrt{d}]$ with $a$ odd and $b$ divisible by 4.

**Lemma 6.1.** The quaternion algebra $D = \left( \frac{-1 - \sqrt{-3}}{F} \right)$ splits at all finite places of $F$ except when $d \equiv 1 \pmod{8}$ and $\varepsilon = a + bv_d$ with $a \equiv 1 \pmod{4}.$ In the exceptional case, $D$ is ramified at the two finite places of $F$ above 2.

**Proof.** By Lemma (2.8), $D$ splits at all nonzero primes of $F$ coprime to 2. First suppose that $\left( \frac{d}{p} \right) \neq 1$ so that there is a unique dyadic prime $p \subset O_F.$ Since the number of ramified places of $D$ is even, $D$ necessarily splits at $p$ as well. Hence $D$ splits at all the finite places of $F$ in this case.

Now suppose that $d \equiv 1 \pmod{8}.$ We have $F_p = \mathbb{Q}_2$ for every dyadic prime $p,$ and by [24, Corollary V.3.3],

\[N_{Q_2(\sqrt{-1})/Q_2}(\mathbb{Z}_2[\sqrt{-1}]) = \{ u \in \mathbb{Z}_2^\times \mid u \equiv 1 \pmod{4}) \}.
\]

It follows that the Hilbert symbol $(-1, -\varepsilon)_p = 1$ if and only if $v_p(\varepsilon + 1) \geq 2,$ or equivalently, $a \equiv 3 \pmod{4}.$

Let $D = \left( \frac{-1 - \sqrt{-3}}{F} \right)$ and $\mathcal{O}_3^f = O_F[i, j]$ be the minimal $D_2^f$-order in Table 2. Recall that $\mathcal{N}(\mathcal{O}_3^f) = F^\times(\mathcal{O}_3^f)^\times(1 + i)$ by (4.11), so $\overline{\mathcal{N}}(\mathcal{O}_3^f) = \mathcal{N}(\mathcal{O}_3^f)/F^\times(\mathcal{O}_3^f)^\times$ is a cyclic group of order 2 generated by $1 + i.$ By Lemma (4.16), two distinct maximal orders containing $\mathcal{O}_3^f$ are $D^\times$-conjugate if and only if they are conjugate by $1 + i.$ As defined in (12.20), $[D(\mathcal{O}_3^f)] = [\mathcal{N}(\mathcal{O}_3^f) \setminus \mathfrak{O}(\mathcal{O}_3^f)].$ According to [27, 63:3], $F(j)/F$ is unramified at every dyadic prime of $F$ and only if $-\varepsilon$ is congruent to a square modulo $4O_F.$ If this is the case, then $O_F[j] = O_F + 2O_{F(j)}$ by (7.6), and hence the order

\[(6.1) \quad \mathfrak{O}_j := O_{F(j)} + iO_{F(j)}
\]

is maximal because $\mathfrak{d}(\mathfrak{O}_j) = \chi(\mathfrak{O}_j : \mathcal{O}_3^f)^{-1}\mathfrak{d}(\mathcal{O}_3^f) = (2O_F)^{-2} \cdot 4O_F = O_F.$
Proposition 6.2. Let $D = (\frac{-1 - \epsilon}{p})$. Write $\epsilon = a + b\sqrt{d}$ with $a, b \in \mathbb{N}$ if $\epsilon \in \mathbb{Z}[\sqrt{d}]$. Moreover, $\mathfrak{d} = 4O_F$, and $\mathcal{O}^1_2$ is maximal at all non-dyadic primes of $F$. It follows that $\mathfrak{N}(\mathcal{O}^1_2) = \prod_{p|\mathfrak{d}O_F} \mathfrak{N}(\mathcal{O}^1_2)$.

| $d \equiv 1$ (mod 8) | $a \equiv 1$ (mod 4) | $\mathfrak{N}(\mathcal{O}^1_2)$ | $\mathfrak{d}(\mathcal{O}^1_2)$ |
|----------------------|----------------------|-----------------|-----------------|
| $d \equiv 1$ (mod 8) | $a \equiv 3$ (mod 4) | 4               | 2               |
| $d \equiv 5$ (mod 8) | 2                    | 1               |                |
| $d \equiv 3$ (mod 4) | $a$ is even          | 2               | 2               |
| otherwise            | 4                    | 3               |                |

Proof. By Lemma 2.8, the Eichler invariant $e_p(\mathcal{O}^1_2) = 0$ for every dyadic prime $p$ of $F$. Moreover, $\mathfrak{d}(\mathcal{O}^1_2) = 4O_F$, and $\mathcal{O}^1_2$ is maximal at all non-dyadic primes of $F$. It follows that $\mathfrak{N}(\mathcal{O}^1_2) = \prod_{p|\mathfrak{d}O_F} \mathfrak{N}(\mathcal{O}^1_2)$.

If $d \equiv 1$ (mod 8) and $a \equiv 1$ (mod 4), then $D$ is ramified at the two dyadic primes of $F$. Hence there is a unique maximal order containing $\mathcal{O}^1_2$, and it is necessarily normalized by $1 + i$.

If $d \equiv 1$ (mod 8) and $a \equiv 3$ (mod 4), then $D$ splits at the two dyadic primes of $F$. By Corollary 1.6, $\mathcal{O}^1_2$ is a Bass order. Then Lemma 2.4 shows that $\mathfrak{N}(\mathcal{O}^1_2) = 2$ for each dyadic prime $p$ of $F$, and hence $\mathfrak{N}(\mathcal{O}^1_2) = 2 \cdot 2 = 4$. Since $(1 + i)$ is odd at every dyadic $p$, it does not belong to $\mathcal{N}(\mathfrak{O})$ for any $\mathfrak{O} \in \mathfrak{S}(\mathcal{O}^1_2)$. Thus conjugation by $(1 + i)$ separates $\mathfrak{S}^1_2$ into two pairs of maximal orders.

When $d \equiv 5$ (mod 8), $p = 2O_F$ is the unique dyadic prime in $F$. The same line of argument as the previous case applies here and yields the desired result.

Now suppose that 2 is ramified in $F$, i.e. $d \equiv 2, 3$ (mod 4). By Subsection 7.1, $O_F[i]$ is a proper suborder of $O_{F(i)}$. It then follows from Lemma 2.4 that $\mathcal{O}^1_2$ is a Bass order if and only if $O_{F(\sqrt{-\epsilon})}$ coincides with the ring of integers of $F(\sqrt{-\epsilon})$. The latter condition holds if and only if $d \equiv 3$ (mod 4) and $a$ is even by Lemmas 7.4 and 7.5. Assume that this is the case so that $\mathcal{O}^1_2$ is Bass, and we apply Lemma 2.4 again to obtain $\mathfrak{N}(\mathcal{O}^1_2) = 2$. By Subsection 7.1 we have $\chi(O_{F(i)}) = 2O_F$, so

$$O_i := O_{F(i)} + jO_{F(i)}$$

is one of the two maximal orders containing $\mathcal{O}^1_2$. Furthermore,

$$(1 + i)O_i(1 + i)^{-1} = O_{F(i)} + kO_{F(i)} = i(O_{F(i)} + jO_{F(i)}) = O_i.$$

Hence $\mathcal{N}(\mathcal{O}^1_2)$ acts trivially on $\mathfrak{S}(\mathcal{O}^1_2)$.

In the remaining cases, $\mathcal{O}^1_2$ is not a Bass order. Let $p$ be the unique dyadic prime of $F$. We write $\mathcal{O} = \mathcal{O}^1_2 \otimes \mathbb{Z}_2 = (\mathcal{O}^1_2)_p$, and denote the minimal overorder of $\mathfrak{O}$ by $\mathfrak{O}^*$.

Then $\mathfrak{d}(\mathfrak{O}^*) = p^3O_{F_p}$ by [6, Proposition 4.1]. Moreover, [5, Proposition 1.12] implies that $\mathfrak{O}^*$ is non-Gorenstein since $\mathfrak{O}$ is not Bass. Now we apply Lemma 2.7 to obtain that $\mathfrak{N}(\mathfrak{O}) = \mathfrak{N}(\mathfrak{O}^*) = 4$. In fact, $\mathfrak{O}^*$ is a star centered at the Gorenstein saturation $\text{Gor}(\mathfrak{O}^*)$ with 3 exterior vertices. The symmetry forces $(1 + i) \in \mathcal{N}(\text{Gor}(\mathfrak{O}^*))$. To obtain $\mathfrak{N}(\mathcal{O}^1_2) = 3$, it is enough to show that conjugation by $(1 + i)$ acts non-trivially on $\mathfrak{S}(\mathfrak{O}^*)$. Suppose that $d \equiv 2$ (mod 4), so $(1 + i)/\sqrt{d}$ is integral over $O_{F_p}$. If $(1 + i)/\sqrt{d}$ acts trivially on $\mathfrak{S}(\mathfrak{O}^*)$, then $(1 + i)/\sqrt{d} \in \mathfrak{O}$ for
every $\mathcal{O} \in \mathcal{G}(\mathcal{O}')$ by Lemma 2.3. Thus
\[
\frac{1 + i}{\sqrt{d}} \in \bigcap_{\mathcal{O} \in \mathcal{G}(\mathcal{O}')} \mathcal{O} = \mathcal{O}'.
\]
However, $(1 + i)/\sqrt{d}$ generates the ring of integers of $F_p(i)$ over $O_{F_p}$. In light of Proposition 1.11, this contradicts the fact that $\mathcal{O}'$ is non-Gorenstein. Lastly, suppose that $d \equiv 3 \pmod{4}$ and $a$ is odd. By Lemma 7.3, $F(j)/F$ is unramified at the dyadic prime of $F$, so the order $\mathcal{O}_j$ in (6.1) is a maximal order containing $\mathcal{O}_2^j$. We claim that
\[
\mathcal{O}_k := (1 + i)\mathcal{O}_j(1 + i)^{-1} = O_{F(k)} + iO_{F(k)}
\]
is distinct from $\mathcal{O}_j$. Indeed,
\[
\mathcal{O}_j \cap F(k) = O_F + k((j^{-1}O_{F(j)}) \cap F) = O_F + k(O_{F(j)} \cap F) = O_F + kO_F \neq O_{F(k)}.
\]
The proposition is proved. □

Corollary 6.3. Let $D = \left(\frac{-1 - i}{4}\right)$. Then
\[
t(D_2^j) + t(D_4) + t(S_4) + t(D_6) = \sharp(\mathcal{O}_2^j).
\]
(6.4)

For $d \geq 7$, either $t(D_6) = 0$ or $t(S_4) = t(D_4) = 0$.

Particularly, if $\{2\varepsilon, 3\varepsilon\} \cap F^{\times 2} = \emptyset$, then
\[
t(D_2^j) = \sharp(\mathcal{O}_2^j).
\]
(6.5)

Proof. For every $\mathcal{O} \in \mathcal{G}(\mathcal{O}_2^j)$, we have $\mathcal{O}^\ast \in \{D_2^j, D_4, S_4, D_6\}$. Hence (6.4) follows from Lemma 6.4. Formula (6.5) holds because $2\varepsilon$ and $3\varepsilon$ cannot be simultaneously square in $F$ when $d \geq 7$. When $\{2\varepsilon, 3\varepsilon\} \cap F^{\times 2} = \emptyset$, every term other than $t(D, D_2^j)$ on the left side of (6.5) is zero, which yields (6.6). □

Lemma 6.4. Assume that $F(j)/F$ is unramified at every dyadic prime of $F$ so that $\mathcal{O}_j$ in (6.1) is a maximal order containing $\mathcal{O}_2^j$. Then $\mathcal{O}_j^\ast$ is isomorphic to neither $D_4$ nor $S_4$.

Proof. Clearly, the lemma holds if $2\varepsilon \notin F^{\times 2}$. So assume that $2\varepsilon \in F^{\times 2}$. Suppose that $\mathcal{O}_j^\ast$ is isomorphic to $D_4$ or $S_4$. Then there exists an element $\tilde{v} \in \mathcal{O}_j^\ast$ of order 4 such that $\tilde{v}^2 \in (\mathcal{O}_2^j)^\ast$. However, $i \in (\mathcal{O}_2^j)^\ast$ is the unique element of order 2 with $\text{Nr}(i) = 1$. So we must have $\tilde{v}^2 = i$. This leads to a contradiction since $\mathcal{O}_j \cap F(i) = O_F[i] \neq O_F[\sqrt{\varepsilon i}]$ by Subsection 7.1. □

6.5. We keep the assumptions of Proposition 6.2. If $d \equiv 1 \pmod{8}$ and $a \equiv 1 \pmod{4}$, then
\[
\mathcal{O} = O_F + O_{F,i} + O_{F,j} + O_F \frac{1 + i + j + k}{2} \subset D = \left(\frac{-1 - \varepsilon}{F}\right)
\]
is the unique maximal order containing $\mathcal{O}_2^j$. Clearly, $\mathcal{O}^\ast$ cannot be isomorphic to $S_4$, $D_4$, or $D_6$, otherwise $D$ splits at all finite places of $F$, which is not the case here. Therefore, we have
\[
\mathcal{O}^\ast \simeq D_2^j \quad \text{and} \quad N(\mathcal{O}) = F^{\times} \mathcal{O}^\ast \langle 1 + i \rangle.
\]
Note that $-\varepsilon$ coincides with $3$ in $O_F/4O_F \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ in this case. So $F(j)/F$ is ramified at both of the dyadic primes of $F$. 

UNIT GROUPS 27
Suppose that \( d \equiv 1 \pmod{8} \) and \( a \equiv 3 \pmod{4} \). Then \( -\varepsilon \equiv 1 \pmod{4D_F} \), and \( F(j)/F \) is unramified at every dyadic prime of \( F \). We leave it to the reader to check that the following are two distinct maximal orders containing \( \mathcal{O}_2^2 \):\[
(6.9) \quad \mathcal{O}_j = O_{F(j)} + iO_{F(j)} = O_F + O_F i + O_F \frac{1 + j}{2} + O_F \frac{i + k}{2}, \\
\quad \mathcal{O} = O_F + O_F i + O_F \frac{(-1 + \sqrt{d}) + (1 + \sqrt{d})i + 2j}{4} \\
\quad + O_F \frac{(1 + \sqrt{d}) + (-1 + \sqrt{d})i + 2k}{4}.
\]
We have \((1 + i)\mathcal{O}_j(1 + i)^{-1} = \mathcal{O}_k\), which coincides with neither \(\mathcal{O}_j\) nor \(\mathcal{O}\). Since \(\varepsilon \in F^\times\) if this is the case. Then \((-\frac{1 - \varepsilon}{p}) = (\frac{-1 - 3}{p})\), and \(\mathcal{O}_j\) coincides with \(\mathcal{O}_6 \subseteq (\frac{-1 - 3}{F})\) in \((4.8)\) since \(3k \equiv 1 \pmod{2O_F}\). On the other hand, \(\mathcal{O}^* \not\cong \mathcal{O}_6\) since it is not \(D^\times\)-conjugate to \(\mathcal{O}_j\). Therefore,\[
(6.11) \quad \mathcal{O}_j^* = \begin{cases} D_2^1 & \text{if } 3\varepsilon \not\in F^{x^2} \\
\quad D_6 & \text{if } 3\varepsilon \in F^{x^2}, \end{cases} \quad \mathcal{N}(\mathcal{O}_j) = F^\times \mathcal{O}_j^\times; \\
(6.12) \quad \mathcal{O}^* = D_2^1, \quad \mathcal{N}(\mathcal{O}) = F^\times \mathcal{O}^\times.
\]
Now suppose that \(d \equiv 5 \pmod{8}\) so that \(p = 2O_F\) is the unique dyadic prime of \(F\). If \(F(j)\) is unramified at \(p\), then \(\mathcal{S}(\mathcal{O}_2^2) = \{\mathcal{O}_j, \mathcal{O}_k\}\). Once again, it can happen that \(3\varepsilon \in F^{x^2}\) (e.g. when \(d = 3p > 9\) with \(p \equiv 3 \pmod{8}\)). Write \(\varepsilon = 3\zeta^2\) with \(\zeta \in F^\times\) if this is the case. Then \((-\frac{1 - \varepsilon}{p}) = (\frac{-1 - 3}{p})\), and \(\mathcal{O}_j\) coincides with \(\mathcal{O}_6 \subseteq (\frac{-1 - 3}{F})\) as before. Moreover, the formulas in \((6.11)\) still hold for \(\mathcal{O}_j\). So suppose further that \(F(j)/F\) is ramified at \(p\). Then \(O_F[j] = O_{F(j)}\) by Lemma \(7.3\). There are three subcases to consider.

(i) If \(\varepsilon = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]\), then \(a \equiv 1 \pmod{4} \) and \(4 \mid b\). Hence \(\mathcal{O}\) in \((6.11)\) is a maximal order containing \(\mathcal{O}_2^2\).

(ii) If \(\varepsilon = (a + b\sqrt{d})/2\) with \(a\) odd and \(b \equiv 1 \pmod{4}\), then it follows from Lemma \(7.3\) that\[
(6.13) \quad \mathcal{O} = O_F + O_F i + O_F \frac{(-1 + \sqrt{d}) + 2i + 2j}{4} + O_F \frac{2 + (-1 + \sqrt{d})i + 2k}{4}
\]
is a maximal order containing \(\mathcal{O}_1^1\).

(iii) If \(\varepsilon = (a + b\sqrt{d})/2\) with \(a\) odd and \(b \equiv 3 \pmod{4}\), the same lemma implies that\[
(6.14) \quad \mathcal{O} = O_F + O_F i + O_F \frac{(1 + \sqrt{d}) + 2i + 2j}{4} + O_F \frac{2 + (1 + \sqrt{d})i + 2k}{4}
\]
is a maximal order containing \(\mathcal{O}_2^1\).

In all three cases, we have\[
(6.15) \quad \mathcal{O}^* \simeq D_2^1, \quad \mathcal{N}(\mathcal{O}) = F^\times \mathcal{O}^\times.
\]
Next, suppose that \(d \equiv 3 \pmod{4}\) and \(\varepsilon = a + b\sqrt{d}\) with \(a\) even. Then \(F(j)/F\) is ramified at the unique dyadic prime \(p\) of \(F\), and \(O_{F(j)} = O_F[j]\) by
We treat the remaining cases where one of the following is true:

6.6.

We have $\mathcal{S}(\mathcal{O}_2) = \{\mathcal{O}_i, \mathcal{O}\}$, where $\mathcal{O}_i$ is defined in (6.2), and $\mathcal{O} = O_{F(j)} + O_{F(j)} \frac{1 + i + (1 + \sqrt{d})j}{2}$. More explicitly,

$$\mathcal{O} = O_F + O_F \frac{1 + i + (1 + \sqrt{d})j}{2} + O_F(j) \frac{1 + \sqrt{d} + j + k}{2}.$$

Clearly, $F(j) \neq F(3)$ since the latter is unramified at $p$. Hence $3 \varepsilon \notin F^{x^2}$. On the other hand, it is possible that $2 \varepsilon \in F^{x^2}$ (e.g. when $d = p$ with $p \equiv 3 \pmod{4}$). The reduced unit groups and normalizers are given by the following table:

| $2 \varepsilon \notin F^{x^2}$ | $\mathcal{O}_i$ | $\mathcal{N}(\mathcal{O}_i)$ | $\mathcal{O}^*$ | $\mathcal{N}(\mathcal{O})$ |
|------------------------------|-----------------|-----------------|-----------------|-----------------|
| $2 \varepsilon \in F^{x^2}$  | $D_2^1$         | $F^* \mathcal{O}_i^\times (1 + i)$ | $D_2^1$         | $F^* \mathcal{O}_i^\times$ |

6.6. We treat the remaining cases where one of the following is true:

- $d \equiv 2 \pmod{4}$;
- $d \equiv 3 \pmod{4}$ and $\varepsilon = a + b\sqrt{d}$ with $a$ odd.

Let $p$ be the unique dyadic prime of $F$. Then $\mathcal{S}(\mathcal{O}_2 \otimes \mathbb{Z}_2)$ is a star on which conjugation by $(1 + i)$ acts as a reflection, and $\mathcal{N}(\mathcal{O}_2) = 4$. For simplicity, let $\varrho = (1 + i+j+k)/2 \in (\frac{1-i}{2})$, and $B$ be the order of $F(i) \subset (\frac{1-i}{2})$ defined in (4.14). We claim that

$$\mathcal{O}_0 = B + B \varrho$$

is the maximal order in $\mathcal{S}(\mathcal{O}_2)$ corresponding to the center of the star $\mathcal{S}(\mathcal{O}_2 \otimes \mathbb{Z}_2)$. Clearly, $\varrho = -\varrho + (1 + i)$. For any $x + yi \in B$ with $x, y \in F$, we have $(1 + iy) \in B$, and hence $\varrho (x+yi) = (x-yi)\varrho + y(1+i) \in \mathcal{O}_0$. Therefore, $\mathcal{O}_0$ is an order containing $\mathcal{O}_2$, and it is maximal because $\chi(\mathcal{O}_0, \mathcal{O}_2) = 4O_F$. Let $\pi = \sqrt{d}$ if $d \equiv 2 \pmod{4}$, and $\pi = 1 + \sqrt{d}$ if $d \equiv 3 \pmod{4}$. Then $p = (2, \pi)$, and the norm of $(1+i)\pi/2 \in B$ over $F$ is a $p$-adic unit. It follows that $\mathcal{O}_2 \subseteq O_F + p\mathcal{O}_0$. Thus $\mathcal{S}(\mathcal{O}_2 \otimes \mathbb{Z}_2)$ is centered at $(\mathcal{O}_0)_p$. Although the expression looks similar, $\mathcal{O}_0$ is not isomorphic to $\mathcal{O}_{2a}$ in (4.15) by Remark 4.12.

First suppose that $d \equiv 3 \pmod{4}$ and $\varepsilon = a + b\sqrt{d}$ with $a$ odd. Then $\mathcal{S}(\mathcal{O}_2) = \{\mathcal{O}_i, \mathcal{O}_j, \mathcal{O}_k, \mathcal{O}_0\}$, and $(1 + i)\mathcal{O}_j(1 + i)^{-1} = \mathcal{O}_k$. Note that $2 \varepsilon \notin F^{x^2}$ in this case by Lemma 7.3. On the other hand, it is possible that $3 \varepsilon \in F^{x^2}$ (e.g. $d = 3p$ with $p \equiv 1 \pmod{4}$). The reduced unit groups and normalizers are given by the following table:

| $3 \varepsilon \notin F^{x^2}$ | $\mathcal{O}_j^*$ | $\mathcal{N}(\mathcal{O}_j)$ | $\mathcal{O}_j^*$ | $\mathcal{N}(\mathcal{O}_j)$ |
|------------------------------|-----------------|-----------------|-----------------|-----------------|
| $3 \varepsilon \in F^{x^2}$  | $D_2^1$         | $F^* \mathcal{O}_j^\times (1 + i)$ | $D_2^1$         | $F^* \mathcal{O}_j^\times$ |

Next, suppose that $d \equiv 2 \pmod{4}$ and $\varepsilon = a + b\sqrt{d}$. Then $a$ is odd and $b$ is even. Hence

$$\mathcal{O}_i' = O_F + O_F \frac{1 + i + \sqrt{d}j}{2} + O_F(j) \frac{1 + \sqrt{d} + j + k}{2}$$

is an order containing $\mathcal{O}_2^\times$. Moreover, $(1 + i)\mathcal{O}_i'(1 + i)^{-1} = \mathcal{O}_i'$. Note that $\mathcal{O}_i' \neq \mathcal{O}_0$ since $(1 + i + j+k)/2 \notin \mathcal{O}_i'$. Suppose further that $F(j)/F$ is unramified at $p$. Then $\mathcal{S}(\mathcal{O}_2^\times) = \{\mathcal{O}_i', \mathcal{O}_0, \mathcal{O}_j, \mathcal{O}_k\}$. Either $2 \varepsilon \in F^{x^2}$ (e.g. when $d = 2p$ with $p \equiv 3 \pmod{4}$) or $3 \varepsilon \in F^{x^2}$ (e.g. when $d = 78$ or $222$) can happen in this case. By Lemma 6.3 $\mathcal{O}_i^\times$ is isomorphic to neither $D_4$ nor $S_4$. When $2 \varepsilon \in F^{x^2}$, we must
have \( \{ \mathcal{O}_i^*, \mathcal{O}_i^\dagger \} = \{ D_4, S_4 \} \). It has already been remarked that \( \mathcal{O}_0 \not\simeq \mathcal{O}_{24} \). Thus \( \mathcal{O}_i^\dagger \simeq D_4 \) and \( \mathcal{O}_i^* \simeq S_4 \) when \( 2\varepsilon \in F^{\times 2} \). The reduced unit groups and normalizers are given by the following table

| \( \{2\varepsilon, 3\varepsilon\} \cap F^{\times 2} = \emptyset \) | \( \mathcal{O}_i^\dagger \) | \( N(\mathcal{O}_i) \) | \( \mathcal{O}_0^\dagger \) | \( N(\mathcal{O}_0) \) | \( \mathcal{O}_i^* \) | \( N(\mathcal{O}_i^*) \) |
|---|---|---|---|---|---|---|
| \( F^{\times \mathcal{O}_j^\dagger} \) | \( D_2^\dagger \) | \( F^{\times \mathcal{O}_j^\dagger} \) | \( D_2^\dagger \) | \( F^{\times \mathcal{O}_0^\dagger} (1 + i) \) | \( D_2^\dagger \) | \( F^{\times \mathcal{O}_i^\dagger} (1 + i) \) |
| \( 3\varepsilon \in F^{\times 2} \) | \( D_6 \) | \( D_2^\dagger \) | \( D_2^\dagger \) | \( F^{\times \mathcal{O}_0^\dagger} \) | \( S_4 \) | \( F^{\times \mathcal{O}_i^\dagger} \) |
| \( 2\varepsilon \in F^{\times 2} \) | \( D_2^\dagger \) | \( D_4 \) | \( D_2^\dagger \) | \( F^{\times \mathcal{O}_0^\dagger} \) | \( S_4 \) | \( F^{\times \mathcal{O}_i^\dagger} \) |

Lastly, suppose that \( d \equiv 2 \pmod{4} \) and \( F(j)/F \) is ramified at \( p \). By Lemma 7.6 if \( 4 \mid b \), then \( a \equiv 1 \pmod{4} \), and hence

\[
(6.19) \quad \mathcal{O}_j' = O_F + O_Fi + O_F \frac{\sqrt{d} + i + j}{2} + O_F \frac{1 + \sqrt{d}i + k}{2}
\]

is a maximal order containing \( \mathcal{O}_j^\dagger \); if \( b \equiv 2 \pmod{4} \), then \( a \equiv 3 \pmod{4} \), and hence

\[
(6.20) \quad \mathcal{O}_j' = O_F + O_Fi + O_F \frac{1 + \sqrt{d} + \sqrt{d}i + j}{2} + O_F \frac{\sqrt{d} + (1 + \sqrt{d})i + k}{2}
\]

is a maximal order containing \( \mathcal{O}_j^\dagger \). Let \( \mathcal{O}_k' = (1 + i)\mathcal{O}_j'(1 + i)^{-1} \). It is straightforward to check that \( \mathcal{O}_k' \neq \mathcal{O}_j' \) in both cases. So \( \mathfrak{S}(\mathcal{O}_j^\dagger) = \{ \mathcal{O}_0, \mathcal{O}_j', \mathcal{O}_j', \mathcal{O}_k' \} \). Since \( F(\sqrt{-3})/F \) is unramified at \( p \), we have \( 3\varepsilon \not\in F^{\times 2} \) in this case. On the other hand, it is possible that \( 2\varepsilon \in F^{\times 2} \) (e.g. when \( d = 2p \) for some prime \( p \equiv 1 \pmod{8} \) and \( p \) not of the form \( x^2 + 32y^2 \) for any \( x, y \in \mathbb{Z} \). See [11, Corollary 24.5]). The reduced unit groups and normalizers are given by the following table

| \( 2\varepsilon \not\in F^{\times 2} \) | \( \mathcal{O}_j^\dagger \) | \( N(\mathcal{O}_j') \) | \( \mathcal{O}_0^\dagger \) | \( N(\mathcal{O}_0) \) | \( \mathcal{O}_i^* \) | \( N(\mathcal{O}_i^*) \) |
|---|---|---|---|---|---|---|
| \( \mathcal{O}_j^\dagger \) | \( F^{\times \mathcal{O}_j^\dagger} \) | \( D_2^\dagger \) | \( D_2^\dagger \) | \( F^{\times \mathcal{O}_0^\dagger} (1 + i) \) | \( D_2^\dagger \) | \( F^{\times \mathcal{O}_i^\dagger} (1 + i) \) |
| \( 2\varepsilon \in F^{\times 2} \) | \( D_2^\dagger \) | \( D_4 \) | \( D_2^\dagger \) | \( F^{\times \mathcal{O}_0^\dagger} \) | \( S_4 \) | \( F^{\times \mathcal{O}_i^\dagger} \) |

Next, we study the maximal orders containing \( \mathcal{O}_j^\dagger \subseteq \left( \frac{\varepsilon - 3}{p} \right) \). By [6 Corollary 1.6], \( \mathcal{O}_j^\dagger \) is always a Bass order since \( \mathfrak{d}(\mathcal{O}_j^\dagger) = 3O_F \) is square-free. We first determine the ramified primes of \( D = \left( \frac{\varepsilon - 3}{p} \right) \). Write \( \varepsilon = \frac{a + \sqrt{N_F}}{b} \), where \( a, b \) are positive integers such that \( a \equiv b \pmod{2} \). If \( d \equiv 1 \pmod{3} \) and \( N_F/q(\varepsilon) = 1 \), then \( 3 \mid b \), which is immediately seen by taking both sides of \( a^2 - b^2d = 4 \) modulo 3. Therefore, \( \varepsilon \equiv \pm 1 \pmod{30F} \) in this case.

**Lemma 6.7.** Let \( D = \left( \frac{\varepsilon - 3}{p} \right) \). Then \( D \) splits at all finite places of \( F \) coprime to 3. If \( d \not\equiv 1 \pmod{3} \), then \( D \) splits at the unique prime of \( F \) above 3 as well. When \( d \equiv 1 \pmod{3} \), \( D \) splits at the two places of \( F \) above 3 if and only if \( \varepsilon \equiv -1 \pmod{30F} \).

**Proof.** Since \( \mathfrak{d}(D) \) divides \( \mathfrak{d}(\mathcal{O}_j^\dagger) \), \( D \) splits at all finite places of \( F \) coprime to 3. If \( F \) has a unique prime \( q \) above 3, i.e. \( d \not\equiv 1 \pmod{3} \), then \( D \) splits at \( q \) as well because it has to split at an even number of places.

Lastly, suppose that \( d \equiv 1 \pmod{3} \). Let \( q \) be a prime of \( F \) above 3. Then \( F_q = \mathbb{Q}_3 \). By Hensel’s lemma, the quadratic form \( -\varepsilon x^2 - 3y^2 \) represents 1 with \( x, y \in \mathbb{Q}_3 \) if and only if \( \varepsilon \equiv -1 \pmod{3} \). Therefore, the Hilbert symbol \( (\varepsilon, -3)_q = 1 \) (i.e. \( D \) splits at \( q \)) if and only if \( \varepsilon \equiv -1 \pmod{3} \). \( \square \)
Proposition 6.8. Let $D = \left( \frac{-3}{F} \right)$, and $q$ be a prime of $F$ above 3. The values of $\mathcal{N}(\mathcal{O}_3^1)$ and $\mathfrak{d}(\mathcal{O}_3^1)$ are listed in the following table.

| $d \geq 6$ | $\mathcal{N}(\mathcal{O}_3^1)$ | $\mathfrak{d}(\mathcal{O}_3^1)$ |
|------------|-----------------|-----------------|
| $d \equiv 0 \pmod{3}$ | $\varepsilon \equiv 1 \pmod{q}$ | 1 |
| | $\varepsilon \equiv -1 \pmod{q}$ | 3 |
| $d \equiv 1 \pmod{3}$ | $\varepsilon \equiv 1 \pmod{3O_F}$ | 1 |
| | $\varepsilon \equiv -1 \pmod{3O_F}$ | 4 |
| $d \equiv 2 \pmod{3}$ | | 2 |

Proof. First suppose that $3 \mid d$ so that $q = (3, \sqrt{D})$. For simplicity, let $L = F(j) \simeq F(\sqrt{-3})$. Then $O_F[(1+j)/2] = O_F + qO_L$, and hence $O_j = O_L + iO_L$ is a maximal order containing $\mathcal{O}_3^1$ with $j \in \mathcal{N}(O_j)$. By Lemma 2.10, $\mathcal{O}_3^1$ is maximal at all finite places of $F$ coprime to $q$, and

$$e_q(\mathcal{O}_3^1) = \begin{cases} 1 & \text{if } \varepsilon \equiv 2 \pmod{q}; \\ -1 & \text{if } \varepsilon \equiv 1 \pmod{q}. \end{cases}$$

If $e_q(\mathcal{O}_3^1) = -1$, then $\mathcal{N}(\mathcal{O}_3^1) = 1$ by [II, Corollary 3.2]. Thus $O_j$ is the unique maximal order containing $\mathcal{O}_3^1$. Suppose that $e_q(\mathcal{O}_3^1) = 1$ next. Then $\mathcal{O}_3^1$ is an Eichler order of level $3O_F = q^2$ by [II, Corollary 2.2]. Hence $\mathcal{N}(\mathcal{O}_3^1) = 3$. Let $\mathcal{O}$ and $\mathcal{O}'$ be the remaining two maximal orders distinct from $O_j$ that contain $\mathcal{O}_3^1$. Then $\mathcal{O} \cap L = O_F[(1+j)/2]$. Otherwise, we have $O_L \subseteq \mathcal{O}$, and hence $\mathcal{O} \subseteq O_j$, which contradicts our assumption. For simplicity, write $R = O_{F_3}$. By [40, Theorem II.3.2], there exists an isomorphism $\mathcal{O} \otimes_{O_{F_3}} R \simeq M_2(R)$ such that $(1+j)/2$ is identified with

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$ 

Then $j$ is identified with

$$\begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix},$$

which does not normalize $M_2(R)$. It follows that $j \notin \mathcal{N}(\mathcal{O})$. Therefore, $j \mathcal{O} j^{-1} = \mathcal{O}'$, and hence $\mathfrak{d}(\mathcal{O}_3^1) = 2$.

Next, suppose that $d \equiv 1 \pmod{3}$. By Lemma 6.7, if $\varepsilon \equiv 1 \pmod{3O_F}$, then $D$ is ramified at the two places of $F$ above 3 and splits at all other finite places. So $\mathcal{O}(D) = 3O_F = \mathcal{O}(\mathcal{O}_3^1)$, which implies that $\mathcal{O}_3^1$ is maximal. Suppose further that $\varepsilon \equiv -1 \pmod{3O_F}$. Then $D$ splits at all finite places of $F$. For any prime $q$ of $F$ above 3, we have $\mathcal{O}(\mathcal{O}_3^1) = 3O_{F_3} = qO_{F_3}$. It follows that $(\mathcal{O}_3^1)_q$ is an Eichler order of level $qO_{F_3}$, and hence $\mathcal{N}(\mathcal{O}_3^1)_q = 2$. Therefore, $\mathcal{N}(\mathcal{O}_3^1) = \prod q \mathcal{N}(\mathcal{O}_3^1)_q = 2 \cdot 2 = 4$. By Subsection 2.2, $j \notin \mathcal{N}((\mathcal{O}_3^1)_q)$ for any maximal order $\mathcal{O}$ containing $\mathcal{O}_3^1$ since it is odd at $q$. Hence conjugation by $j$ acts as the product of two disjoint transpositions on $\mathcal{O}(\mathcal{O}_3^1)$, and $\mathfrak{d}(\mathcal{O}_3^1) = 2$.

Lastly, the calculation of $\mathcal{N}(\mathcal{O}_3^1)$ and $\mathfrak{d}(\mathcal{O}_3^1)$ for $d \equiv 2 \pmod{3}$ is similar to the case $d \equiv 1 \pmod{3}$ and $\varepsilon \equiv -1 \pmod{3O_F}$ above, hence omitted.\[\square\]

Corollary 6.9. Let $D = \left( \frac{-3}{F} \right)$. Then

$$t(D_3^1) + t(S_4) + t(D_6) = \mathfrak{d}(\mathcal{O}_3^1).$$

(6.21)

For $d \geq 7$, either $t(S_4) = 0$ or $t(D_6) = 0$.

Particularly, if $(2\varepsilon, 3\varepsilon) \cap F^\times = \emptyset$, then

$$t(D_3^1) = \mathfrak{d}(\mathcal{O}_3^1).$$

(6.23)

The proof is similar to that of Corollary 6.3 and hence omitted.
6.10. Suppose that $3 \mid d$. Write
\[
\varepsilon = a + b\sqrt{d} \quad \text{with} \quad a, b \in \frac{1}{2} \mathbb{Z} \quad \text{and} \quad a \equiv b \pmod{\mathbb{Z}}.
\]
Assume that $a \equiv 2 \pmod{\frac{3}{2} \mathbb{Z}}$. We define
\[
\delta = \begin{cases}
\frac{-3i + 2j + k}{6} & \text{if } b \equiv 0 \pmod{\frac{3}{2} \mathbb{Z}}; \\
\frac{-3i + 2(1 + \sqrt{d})j + k}{6} & \text{if } b \equiv 1 \pmod{\frac{3}{2} \mathbb{Z}}; \\
\frac{-3i + 2(-1 + \sqrt{d})j + k}{6} & \text{if } b \equiv 2 \pmod{\frac{3}{2} \mathbb{Z}}.
\end{cases}
\]
Then $\mathcal{O}$ is a maximal order containing $\mathcal{O}_j$ and distinct from $\mathcal{O}_j$. It follows from the proof of Proposition 6.8 that $\mathcal{S}(\mathcal{O}_j^3) = \{\mathcal{O}, \mathcal{O}_j, j\mathcal{O}_j^{-1}\}$.

If $2\varepsilon \in F^{\times 2}$, then $\varepsilon \equiv -1 \pmod{q}$. This case is possible, as demonstrated by the example $d = 66$ and $\varepsilon = 65 + 8\sqrt{6}$. When $d = 3p$ with $p > 3$ and $p \equiv 3 \pmod{4}$, we have $3\varepsilon \in F^{\times 2}$ by [9] Lemma 3(a)]. Examples with $d = 21$ and $d = 33$ show that both cases of $\varepsilon \equiv \pm 1 \pmod{q}$ may occur when $3\varepsilon \in F^{\times 2}$. The reduced unit groups and normalizers are given by the following table:

| $\{2\varepsilon, 3\varepsilon\} \cap F^{\times 2} = \emptyset$ | $\mathcal{O}_j^*$ | $\mathcal{N}(\mathcal{O}_j)$ | $\mathcal{O}^*$ | $\mathcal{N}(\mathcal{O})$ |
|---------------------------------------------------------------|-----------------|----------------|-----------------|----------------|
| $2\varepsilon \in F^{\times 2}$                              | $\mathcal{O}_j^*$ | $\mathcal{N}(\mathcal{O}_j)$ | $\mathcal{O}^*$ | $\mathcal{N}(\mathcal{O})$ |
| $3\varepsilon \in F^{\times 2}$                              | $\mathcal{O}_j^*$ | $\mathcal{N}(\mathcal{O}_j)$ | $\mathcal{O}^*$ | $\mathcal{N}(\mathcal{O})$ |

Note that the result for $\mathcal{O}_j$ holds regardless of $\varepsilon \equiv \pm 1 \pmod{q}$.

6.11. Let $d \equiv 1 \pmod{3}$ and $\varepsilon \equiv -1 \pmod{3\mathcal{O}_F}$. We define
\[
\mathcal{O} = \mathcal{O}_F + O_F i + O_F \frac{1 + j}{2} + O_F \frac{-3i + 2j + k}{6};
\]
\[
\mathcal{O}' = \mathcal{O}_F + O_F i + O_F \frac{1 + j}{2} + O_F \frac{-3i + 2\sqrt{d}j + k}{6}.
\]
Then $\mathcal{O} \neq \mathcal{O}'$ and $j\mathcal{O}_j^{-1} \neq \mathcal{O}'$. Therefore, $\mathcal{S}(\mathcal{O}_j^3) = \{\mathcal{O}, \mathcal{O}', j\mathcal{O}_j^{-1}, j\mathcal{O}_j'^{-1}\}$. Note that $3\varepsilon \not\in F^{\times 2}$ since $F/\mathbb{Q}$ is unramified at 3. On the other hand, it is possible that $2\varepsilon \in F^{\times 2}$ (e.g. $d = p$ with $p \equiv 7 \pmod{12}$ or $d = 2p$ with $p \equiv 11 \pmod{12}$).

Suppose that this is the case. Then $\{\mathcal{O}^*, \mathcal{O}'^*\} = \{S_4, D_3^3\}$. Indeed, we cannot have $\mathcal{O}^* \simeq \mathcal{O}'^* \simeq S_4$ since $\mathcal{O}$ and $\mathcal{O}'$ are not $D^{\times}$-conjugate. Write $\varepsilon = 2\theta^2$ and $2\theta = x + y\sqrt{d} \in \mathcal{O}_F$ with $x, y \in \frac{1}{2}\mathbb{Z}$ and $x \equiv y \pmod{\mathbb{Z}}$. Note that either $x$ or $y$ lies in $\frac{3}{2}\mathbb{Z}$, and
\[
\left(\frac{j}{3} \pm \frac{2\theta k}{3\varepsilon}\right)^2 = -1, \quad i \left(\frac{j}{3} \pm \frac{2\theta k}{3\varepsilon}\right) = - \left(\frac{j}{3} \pm \frac{2\theta k}{3\varepsilon}\right)^2.
\]
If $y \in \frac{3}{2}\mathbb{Z}$, then $\frac{j}{3} \pm \frac{2\theta k}{3\varepsilon} \in \mathcal{O}$ for a suitable choice of sign depending on $(x \pmod{\frac{3}{2}\mathbb{Z})}$. Hence $\mathcal{O}^* \simeq S_4$ in this case. Similarly, if $x \in \frac{3}{2}\mathbb{Z}$, then $\frac{j}{3} \pm \frac{2\theta k}{3\varepsilon} \in \mathcal{O}'$ for a suitable choice of sign depending on $(y \pmod{\frac{3}{2}\mathbb{Z})}$. Hence $\mathcal{O}'^* \simeq S_4$ in this case. The reduced unit groups and normalizers are summarized in the following table.
Let \( d \equiv 2 \pmod{3} \), and \( \varepsilon = a + b\sqrt{d} \) be the same as in (6.24). Then either \( a \) or \( b \) lies in \( \frac{1}{2}\mathbb{Z} \). We define

\[
\mathfrak{O} = \mathfrak{O}_\varepsilon^3 + O_F \delta = O_F + O_F i + O_F \frac{1 + j}{2} + O_F \delta,
\]

where

\[
\delta = \begin{cases} 
\frac{-3i + 2\sqrt{d}j + k}{6} & \text{if } a \equiv 1 \pmod{\frac{3}{2}\mathbb{Z}} \text{ and } b \equiv 0 \pmod{\frac{3}{2}\mathbb{Z}}; \\
\frac{-3i + 2j + k}{6} & \text{if } a \equiv 2 \pmod{\frac{3}{2}\mathbb{Z}} \text{ and } b \equiv 0 \pmod{\frac{3}{2}\mathbb{Z}}; \\
\frac{-3i + 2(1 + \sqrt{d})j + k}{6} & \text{if } a \equiv 0 \pmod{\frac{3}{2}\mathbb{Z}} \text{ and } b \equiv 1 \pmod{\frac{3}{2}\mathbb{Z}}; \\
\frac{-3i + 2(-1 + \sqrt{d})j + k}{6} & \text{if } a \equiv 0 \pmod{\frac{3}{2}\mathbb{Z}} \text{ and } b \equiv 2 \pmod{\frac{3}{2}\mathbb{Z}}.
\end{cases}
\]

Then \( \mathfrak{O} \) is the unique maximal order containing \( \mathfrak{O}_\varepsilon^3 \) up to conjugation by \( j \). It is possible that \( 2\varepsilon \in F^{\times 2} \) (e.g., when \( d = 2p \) with \( p \equiv 7 \pmod{12} \)). On the other hand, \( 3\varepsilon \notin F^{\times 2} \) since \( F/\mathbb{Q} \) is unramified at 3. We have

\[
\mathfrak{O}^* \simeq \begin{cases} 
D_3^\dagger & \text{if } 2\varepsilon \notin F^{\times 2}; \\
S_4 & \text{if } 2\varepsilon \in F^{\times 2},
\end{cases}
\]

and \( \mathcal{N}(\mathfrak{O}) = F^{\times} \mathfrak{O}^{\times} \).

7. Quadratic \( O_F \)-orders in CM-fields

Let \( F = \mathbb{Q} (\sqrt{d}) \) be a real quadratic field with square-free \( d \geq 6 \), and \( K/F \) a CM-extension of \( F \). Given an \( O_F \)-order \( B \) in \( K \), we put \( w(B) = [B^\times : O_F^\times] \), and denote the conductor of \( B \) by \( f_B \). The CM-extensions \( K/F \) with \( w(O_K) > 1 \) have been listed in (4.2). For our purpose, it is necessary to classify all \( B \) in \( K \) with \( w(B) > 1 \). When \( K = F(\sqrt{-1}) \) or \( F(\sqrt{-3}) \), this is carried out in [38, Chapter 3], whose results are recalled in Subsection [7.1]. Subsection [7.2] studies the orders \( B \) in \( F(\sqrt{-\varepsilon}) \) with \( w(B) > 1 \) when \( N_{F/\mathbb{Q}}(\varepsilon) = 1 \). For simplicity, we set \( h(m) = h(\mathbb{Q}((\sqrt{m})) \) for any square-free \( m \in \mathbb{Z} \).

7.1. Orders in \( F(\sqrt{-1}) \) and \( F(\sqrt{-3}) \). First, assume that \( K = F(\sqrt{-1}) \). Then

\[
h(K) = \frac{1}{2} Q_{K/F} h(d) h(-d),
\]

where the Hasse index \( Q_{K/F} = 2 \) if \( 2\varepsilon \in F^{\times 2} \), and \( Q_{K/F} = 1 \) otherwise.

Write \( p \) for the unique dyadic prime of \( O_F \) if \( 2 \) is ramified in \( F \) (i.e. \( d \equiv 1 \pmod{4} \)). If further \( d \equiv 3 \pmod{4} \), then we define

\[
B_{1,2} := O_F + p O_K = \mathbb{Z} [\sqrt{-1}, \alpha_d], \quad \text{where } \alpha_d = (1 + \sqrt{-1})(1 + \sqrt{d})/2.
\]

Suppose that \( 2\varepsilon \in F^{\times 2} \). Necessarily \( d \equiv 1 \pmod{4} \). Fix \( \vartheta \in F \) such that \( \varepsilon = 2\vartheta^2 \), and set \( \eta := \sqrt{\varepsilon / -1} \). If \( d \equiv 3 \pmod{4} \), then the same proof as that of [44, Proposition 3.3] shows that \( O_F[\eta] = B_{1,2} \). We claim that \( O_F[\eta] = O_K \) when \( d \equiv 2 \pmod{4} \). Note that \( 2\vartheta \equiv \sqrt{d} \pmod{2 O_F} \) since both sides represent the unique nontrivial nilpotent element in \( O_F/2O_F \). Thus \( \vartheta(1 + \sqrt{-1}) \equiv (\sqrt{d} + \sqrt{-d})/2 \pmod{O_F[\sqrt{-1}]} \), which implies that \( O_F[\eta] = O_K \).
The $O_F$-orders $B \subseteq O_K$ with $w(B) > 1$ are summarized in Table 3, where $\left( \frac{Q}{2} \right)$ is the Artin symbol (See [40, p. 94]). The class number $h(B)$ can be calculated using formula (2) in [38, p. 75].

**Table 3.** $O_F$-orders $B$ with $w(B) > 1$ in $K = F(\sqrt{-1})$.

| $d$ | $B$ | $\varepsilon$ | $\mathfrak{f}_B$ | $w(B)$ | $h(B)$ |
|-----|-----|---------------|-------------|--------|--------|
| $d \equiv 1 \pmod{4}$ | $O_K$ | $2\varepsilon \not\in F^{\times 2}$ | $O_F^2$ | 2 | $h(K)$ |
| $d \equiv 2 \pmod{4}$ | $O_K$ | $2\varepsilon \not\in F^{\times 2}$ | $O_F^2$ | 2 | $h(K)$ |
|  | $O_F[\sqrt{-1}]$ | $2\varepsilon \not\in F^{\times 2}$ | $p$ | 2 | $2h(K)$ |
|  | $O_F[\sqrt{-1}]$ | $2\varepsilon \in F^{\times 2}$ | $h(K)$ |  |  |
| $d \equiv 3 \pmod{4}$ | $B_{1,2}$ | $2\varepsilon \not\in F^{\times 2}$ | $O_F^2$ | 2 | $h(K)$ |
|  | $O_F[\sqrt{-1}]$ | $2\varepsilon \not\in F^{\times 2}$ | $2O_F$ | 2 | $2h(B_{1,2})$ |

Next, assume that $K = F(\sqrt{-3})$. Then

$$(7.3) \quad h(K) = \frac{1}{2}Q_{K/F}h(d)h(-3d),$$

where the Hasse index $Q_{K/F} = 2$ if $3\varepsilon \in F^{\times 2}$, and $Q_{K/F} = 1$ otherwise. Moreover, if $3\varepsilon \in F^{\times 2}$, then $K = F(\sqrt{-\varepsilon})$.

If $3 \mid d$, we write $q$ for the unique prime ideal of $O_F$ above 3. Let $p$ denote any dyadic prime of $O_F$ if $\left( \frac{d}{2} \right) \neq -1$. When 2 splits in $F$ (i.e. $\left( \frac{2}{d} \right) = 1$) and $p$ runs over the two dyadic primes of $F$, we get two distinct orders of the form $O_F + pO_K$. The $O_F$-orders $B$ in $K$ with $w(B) > 1$ are summarized in Table 4.

**Table 4.** $O_F$-orders $B$ with $w(B) > 1$ in $K = F(\sqrt{-3})$.

| $d$ | $B$ | $\varepsilon$ | $\mathfrak{f}_B$ | $w(B)$ | $h(B)$ |
|-----|-----|---------------|-------------|--------|--------|
| $3 \mid d$ | $O_K$ | $3\varepsilon \not\in F^{\times 2}$ | $O_F^3$ | 3 | $h(K)$ |
|  | $O_K$ | $3\varepsilon \in F^{\times 2}$ | $O_F^3$ | 3 | $h(K)$ |
|  | $O_F[\zeta_6]$ | $3\varepsilon \not\in F^{\times 2}$ | $q$ | 3 | $\left( 3 - \left( \frac{d}{6} \right) \right) h(K)$ |
|  | $O_F[\sqrt{-\varepsilon}]$ | $3\varepsilon \not\in F^{\times 2}$ | $h(K)$ |  |  |
|  | $O_F[\sqrt{-\varepsilon}]$ | $3\varepsilon \in F^{\times 2}$ | $2O_F$ | 2 | $\left( 2 + \left( \frac{d}{3} \right) \right) h(K)$ |
| $3 \mid d, \left( \frac{d}{3} \right) \neq -1$ | $O_F + pO_K$ | $3\varepsilon \in F^{\times 2}$ | $p$ | 2 | $h(K)$ |
7.2. Orders in $F(\sqrt{-\varepsilon})$. Throughout this subsection, we assume that $N_{F/Q}(\varepsilon) = 1$ and write $p$ for a dyadic prime of $F = \mathbb{Q}(\sqrt{d})$. In particular, if $\left(\frac{d}{p}\right) \neq 1$, then $p$ is the unique dyadic prime of $F$. We study the orders $B$ in $L = F(\sqrt{-\varepsilon})$ with $w(B) > 1$. The case that $3\varepsilon \in F^{\times 2}$ is already covered in the previous subsection, so we further assume that $3\varepsilon \notin F^{\times 2}$. In this case, $O_L^\times/O_F^\times$ is a cyclic group of order 2 generated by the image of $\sqrt{-\varepsilon}$, hence any $O_F$-order $B \subset L$ with $w(B) > 1$ contains $O_L[\sqrt{-\varepsilon}]$.

Let $f$ be the conductor of $O_L[\sqrt{-\varepsilon}] \subseteq O_L$. Then by [34, Proposition III.5],

\begin{equation}
\tag{7.4}
f^2d_{O_L/O_F} = d_{O_L[\sqrt{-\varepsilon}]/O_F} = 4O_F;
\end{equation}

\begin{equation}
\tag{7.5}
d_{O_L[\sqrt{-\varepsilon}]\cap\mathbb{Z}} = (d_{O_F}\mathbb{Z})^2N_{F/Q}(4O_F) = \begin{cases} 2^4d^2 & \text{if } d \equiv 1 \pmod{4}, \\ 2^s d^2 & \text{otherwise}. \end{cases}
\end{equation}

In particular, $L/F$ is unramified at all finite non-dyadic primes of $F$. If furthermore $L/F$ is unramified at every dyadic prime $p$ as well, then $d_{O_L/O_F} = O_F$. In this case we have

\begin{equation}
\tag{7.6}
f = 2O_F, \quad O_L[\sqrt{-\varepsilon}] = O_F + 2O_L, \quad \text{and}
\end{equation}

\begin{equation}
\tag{7.7}
h(O_L[\sqrt{-\varepsilon}]) = 4h(L) \prod_{p \mid (2O_F)} \left(1 - \frac{1}{N(p)} \left(\frac{L}{p}\right)\right) \quad \text{if } 3\varepsilon \notin F^{\times 2}.
\end{equation}

By [27, 63:3], $L/F$ is unramified above $p$ if and only if $-\varepsilon$ is a square in $(O_F/4O_F)_p$.

If $O_L[\sqrt{-\varepsilon}]$ is non-maximal, then $O_L[\sqrt{-\varepsilon}] \subseteq O_F + pO_L$ for any dyadic prime of $F$. When $\left(\frac{d}{p}\right) \neq -1$, we have $O_F/p \simeq \mathbb{F}_2$, and hence

\begin{equation}
\tag{7.8}
h(O_F + pO_L) = \left(2 - \left(\frac{L}{p}\right)\right) h(L) \quad \text{if } 3\varepsilon \notin F^{\times 2}.
\end{equation}

**Lemma 7.1.** Suppose that $d \equiv 1 \pmod{8}$. Then $\varepsilon$ is of the form $a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ with $a$ odd and $b$ divisible by 4. Moreover, if $a \equiv 3 \pmod{4}$, then $L/F$ is unramified at every dyadic prime of $F$; otherwise, $L/F$ is ramified at both the dyadic primes of $F$.

**Proof.** When $d \equiv 1 \pmod{8}$, $O_F^{\times} = \mathbb{Z}[\sqrt{d}]^{\times}$ by [44, Lemma 4.1]. In particular, $\varepsilon \in \mathbb{Z}[\sqrt{d}]$, so we may write $\varepsilon = a + b\sqrt{d}$ with $a, b \in \mathbb{N}$ and $a^2 - b^2d = 1$. The first part of the lemma is obtained by taking modulo 8 on both sides of $a^2 - b^2d = 1$. The second part follows directly from [27, 63:3] by noting that $O_F/4O_F \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. \qed

**Lemma 7.2.** Suppose that $d \equiv 1 \pmod{4}$, and $L/F$ is ramified at the dyadic primes of $F$. Then $O_L = O_F[\sqrt{-\varepsilon}]$.

**Proof.** By [9, Lemma 3], there exists a pair of positive integers $r, s \in \mathbb{N}$ such that $rs = d$ and $L = F(\sqrt{-r})$. Hence $L/F$ is ramified at the dyadic primes of $F$ if and only if $r \equiv 1 \pmod{4}$, in which case

\[d(O_L/\mathbb{Z}) = d \cdot (-4r) \cdot (-4s) = 2^4d^2 = d_{O_F[\sqrt{-\varepsilon}]/\mathbb{Z}}\]

by [24, Exercise II.42(f), p.52] and (7.5). Therefore, $O_L = O_F[\sqrt{-\varepsilon}]$ if $L/F$ is ramified at the dyadic primes of $F$. \qed

Next, suppose that $d \equiv 5 \pmod{8}$. It is a classical problem of Eisenstein to characterize those $d$ such that $\varepsilon \in \mathbb{Z}[\sqrt{d}]$. If $\varepsilon \in \mathbb{Z}[\sqrt{d}]$, then we write $\varepsilon = a + b\sqrt{d}$
as before, otherwise write \( \varepsilon = (a + b\sqrt{d})/2 \) with both \( a \) and \( b \) odd. It has been shown \([2,36]\) that the number of \( d \) is infinite in each case.

**Lemma 7.3.** Suppose that \( d \equiv 5 \pmod{8} \). Then \( L = F(\sqrt{-\varepsilon}) \) is ramified at \( \mathfrak{p} = 2O_F \) if and only if one of the following conditions holds:

(i) \( a \equiv 1 \pmod{4} \) and \( 4 \mid b \) if \( \varepsilon = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}] \);

(ii) \( a \equiv 3 \pmod{4} \) if \( \varepsilon = (a + b\sqrt{d})/2 \) with both \( a \) and \( b \) odd. In this case, \( d, a, b \)

fall into one of the subcases listed in the table below:

| \( d \pmod{16} \) | \( a \pmod{8} \) | \( b \pmod{8} \) |
|-----------------|-----------------|-----------------|
| 5               | 3               | \pm 1           |
|                 | 7               | \pm 3           |
| 13              | 7               | \pm 1           |
|                 | 3               | \pm 3           |

**Proof.** First suppose that \( \varepsilon = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}] \). Modulo 8 on both sides of \( a^2 - b^2d = 1 \), we find that \( 4 \mid b \) and \( a \) is odd. If \( a \equiv 3 \pmod{4} \), then \(-\varepsilon \equiv 1 \pmod{4} \), and hence \( L/F \) is unramified at \( \mathfrak{p} = 2O_F \). On the other hand, \((O_F/4O_F)\times \simeq \mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2 \). So the nontrivial element \(-1 \in (O_F/4O_F)\times \) of order 2 cannot be a perfect square. Thus if \( a \equiv 1 \pmod{4} \), then \( L/F \) is ramified at \( \mathfrak{p} \).

Next, suppose that \( \varepsilon = (a + b\sqrt{d})/2 \) with both \( a \) and \( b \) odd. Let \( r \) be the same as in the proof of Lemma \( 7.2 \). Write \( r\varepsilon = (x + y\sqrt{d})^2 \) with both \( x, y \) odd. Then \( ra = x^2 + y^2d \equiv 3 \pmod{4} \). Therefore \( r \equiv 1 \pmod{4} \) if and only if \( a \equiv 3 \pmod{4} \). Now suppose further that \( d \equiv 5 \pmod{16} \) and \( b \equiv \pm 1 \pmod{8} \). Taking modulo 16 on both sides of \( a^2 - b^2d = 4 \), we get \( a \equiv \pm 3 \pmod{8} \). It follows that \( L/F \) is ramified at \( \mathfrak{p} \) if and only if \( a \equiv 3 \pmod{8} \) in this case. The remaining cases are treated similarly and hence omitted.

We now study the cases where \( (\frac{d}{F}) = 0 \), that is, \( d \not\equiv 1 \pmod{4} \). Let \( \mathfrak{p} \) be the unique dyadic prime of \( F \).

**Lemma 7.4.** Suppose that \( d \equiv 3 \pmod{4} \). Write \( \varepsilon = a + b\sqrt{d} \) with \( a, b \in \mathbb{N} \). If \( b \) is odd, then \( L = F(\sqrt{-\varepsilon}) \) is ramified at \( \mathfrak{p} \), and \( O_L = O_F[\sqrt{-\varepsilon}] \); otherwise, \( L/F \) is unramified at all finite places of \( F \), and \( O_F[\sqrt{-\varepsilon}] = O_F + 2O_L \).

**Proof.** By \([9, \text{Lemma 3}] \), there exists a pair of positive integers \( r, s \in \mathbb{N} \) such that \( rs = d \) and

(7.9) \[ L = \begin{cases} \mathbb{Q}(\sqrt{d}, \sqrt{-2r}, \sqrt{-2s}), & \text{if } 2 \nmid b; \\ \mathbb{Q}(\sqrt{d}, \sqrt{-r}, \sqrt{-s}), & \text{if } 2 \mid b. \end{cases} \]

First, suppose that \( b \) is odd. Then \( L/F \) is ramified above \( \mathfrak{p} \) (In fact, \( L/Q \) is totally ramified above 2). It follows from \([23, \text{Exercise II.42(f)} \), p. 52\] that \( \mathfrak{d}_{O_L/Z} = (4d) \cdot 4(-2r) \cdot 4(-2s) = 2^6d^2 \). Comparing with (7.3), we get \( O_L = O_F[\sqrt{-\varepsilon}] \).

Next, suppose that \( b \) is even. Without lose of generality, we may assume that \( r \equiv 3 \pmod{4} \) so that \( \mathbb{Q}(\sqrt{-r}) \) is unramified at 2. Therefore, \( L = F(\sqrt{-r}) \) is unramified at \( \mathfrak{p} \), and thus unramified at all finite primes. We conclude that \( \mathfrak{d}_{O_L/O_F} = O_F \) and hence \( f = 2O_F \) by (7.4).

**Remark 7.5.** By \([17, \text{Theorem 1.1}] \), we have \( 2 \nmid b \) when \( d = p \) is a prime congruent to 3 modulo 4. Thus \( O_F[\sqrt{-\varepsilon}] = O_L \) in this case (See \([44, \text{Proposition 2.6}] \)).
Suppose that \( d = pp' \) is a product of primes with \( p \equiv 3 \pmod{4} \) and \( p' \equiv 1 \pmod{4} \). By [11 Corollary 18.6], the 2-primary subgroup of \( \text{Cl}(O_F) \) is a nontrivial cyclic group in this case, and it is a cyclic group of order 2 if either \( \left( \frac{2}{p} \right) = -1 \) or \( \left( \frac{2}{p'} \right) = -1 \) (see [20 Table 1]). If \( \left( \frac{2}{p'} \right) = -1 \), then \( 2 \nmid b \). If \( \left( \frac{2}{p} \right) = 1 \) and \( \left( \frac{2}{p'} \right) = -1 \), then \( 2 \mid b \). For the remaining case where \( d = pp' \) with \( \left( \frac{2}{p} \right) = \left( \frac{2}{p'} \right) = 1 \), we merely provide a few examples to show its complexity.

| \( d \) | \( p \) | \( p' \) | \( \varepsilon \) | \( h(F) \) | \( d \) | \( p \) | \( p' \) | \( \varepsilon \) | \( h(F) \) |
|-------|-----|-----|-----|------|-------|-----|-----|-----|------|
| 323   | 19  | 17  | 18 + \( \sqrt{323} \) | 4    | 799   | 47  | 17  | 424 + 15\( \sqrt{799} \) | 8    |
| 2419  | 59  | 41  | 2951 + 60\( \sqrt{2419} \) | 12   | 943   | 23  | 41  | 737 + 24\( \sqrt{943} \) | 4    |

**Lemma 7.6.** Suppose that \( d \equiv 2 \pmod{4} \). Then \( \varepsilon = a + b\sqrt{d} \) with \( a \) odd and \( b \) even, and \( L/F \) is ramified at \( p \) if and only if the following is true:

\[
(a \mod 4) \equiv \begin{cases} 
1 & \text{if } b \equiv 0 \pmod{4}; \\
3 & \text{if } b \equiv 2 \pmod{4}.
\end{cases}
\]

If \( L/F \) is ramified at \( p \), then \( O_F[\sqrt{-\varepsilon}] = O_F + pO_L \), otherwise \( O_F[\sqrt{-\varepsilon}] = O_F + 2O_L \).

**Proof.** The parity of \( a \) and \( b \) follows directly from \( N_{F/Q}(\varepsilon) = a^2 - b^2d = 1 \). By [9 Lemma 3(a)], there exists a factorization \( d = rs \in \mathbb{N} \) such that both \( r, s \in F \times \). Since \( d \equiv 2 \pmod{4} \), we assume that \( r \) is odd and \( s \) is even. Then \( L = F(\sqrt{-\varepsilon}) = F(\sqrt{-r}) \), and \( L/F \) is ramified at \( p \) if and only if \( r \equiv 1 \pmod{4} \).

Write \( rs = (x + y\sqrt{d})^2 \) with \( x, y \in \mathbb{N} \). Then

\[
ra = x^2 + dy^2 \quad \text{and} \quad rb = 2xy.
\]

Necessarily, \( x \) is odd. If \( b \equiv 2 \pmod{4} \), then \( y \) is odd, and hence \( ra \equiv 3 \pmod{4} \). If \( b \equiv 0 \pmod{4} \), then \( y \) is even, and hence \( ra \equiv 1 \pmod{4} \). Thus \( r \equiv 1 \pmod{4} \) if and only if \( a \equiv 1 \pmod{4} \).

If \( L/F \) is unramified at \( p \), then \( O_F[\sqrt{-\varepsilon}] = O_F + 2O_L \) by (7.6). Suppose that \( r \equiv 1 \pmod{4} \) so that \( L/F \) is ramified at \( p \). Then

\[
\sqrt{-\varepsilon} = \frac{1}{r} \sqrt{-r} \sqrt{-s} \in (\mathbb{Q}\sqrt{-r} + \mathbb{Q}\sqrt{-s}) \cap O_L = \mathbb{Z}\sqrt{-r} + \mathbb{Z}\sqrt{-s}.
\]

Hence \( O_F[\sqrt{-\varepsilon}] \subset \mathbb{Z}[\sqrt{-r}, \sqrt{-s}] \). One calculates that \( \text{disc}_{\mathbb{Z}[\sqrt{-r}, \sqrt{-s}]/\mathbb{Z}} = 2^8 d^2 = \text{disc}_{O_F[\sqrt{-\varepsilon}]/\mathbb{Z}} \) by (7.3). Therefore, \( O_F[\sqrt{-\varepsilon}] = \mathbb{Z}[\sqrt{-r}, \sqrt{-s}] \), which has index 2 in \( O_L \) by [25 Exercise II.42(b), p. 51]. We conclude that \( O_F[\sqrt{-\varepsilon}] = O_F + pO_L \). \( \square \)

**Remark 7.7.** Suppose that \( d = 2p \) with \( p \) prime. If \( p \equiv 3 \pmod{4} \), then \( N_{F/Q}(\varepsilon) = 1 \) by [10 (V.1.7)]. Necessarily, \( r = p \) in this case, so \( L/F \) is unramified above \( p \) by Lemma 7.6. If \( p \equiv 5 \pmod{8} \), then \( N_{F/Q}(\varepsilon) = -1 \) by [11 Proposition 19.9]. The sign of \( N_{F/Q}(\varepsilon) \) for \( p \equiv 1 \pmod{8} \) is more complicated and is discussed in [11 Section 24]. The following table lists the first few examples of square-free \( d \in 2\mathbb{N} \) with more than 2 distinct odd prime factors.

| \( d \) | \( \varepsilon \) | \( r \equiv 1 \pmod{4} \) | \( d \) | \( \varepsilon \) | \( r \equiv 3 \pmod{4} \) |
|-------|-----|----------------|-------|-----|----------------|
| 30    | 11 + 2\( \sqrt{30} \) | 5     | 42   | 13 + 2\( \sqrt{42} \) | 7     |
| 66    | 65 + 8\( \sqrt{66} \) | 33    | 78   | 53 + 6\( \sqrt{78} \) | 3     |
| 70    | 251 + 30\( \sqrt{70} \) | 5     | 102  | 101 + 10\( \sqrt{102} \) | 51    |
8. Calculations for \( F = \mathbb{Q}(\sqrt{p}) \) and \( D = D_{\infty_1, \infty_2} \)

Let \( p \) be a prime number, \( F = \mathbb{Q}(\sqrt{p}) \), and \( D = D_{\infty_1, \infty_2} \) be the totally definite quaternion \( F \)-algebra that splits at all finite places of \( F \). We calculate \( h(G) = h(D, G) \) for all finite groups \( G \). By [11] Corollary 18.4, \( h(\mathbb{Q}(\sqrt{p})) \) is odd for every prime \( p \). Base on this observation, we show in [10] that

\[
(8.1) \quad h(G) = h(F)t(G) \quad \text{for all } G.
\]

Hence it is simpler to list all \( t(G) \) instead. The case that \( p \equiv 1 \pmod{4} \) with \( p > 5 \) has already been treated by Hashimoto [18]. We focus on the cases that \( p \in \{2, 3, 5\} \) or \( p \equiv 3 \pmod{4} \).

8.1. Case \( p \in \{2, 3, 5\} \). Note that \( N_{F/\mathbb{Q}}(\varepsilon) = -1 \) if \( d = 2 \) or 5. If \( d = 3 \), then \( N_{F/\mathbb{Q}}(\varepsilon) = 1, 2 \varepsilon \in F^{\times^2}, \) and \( F(\sqrt{-1}) = F(\sqrt{-3}) \). The CM-extensions \( K/F \) with \( \left[ O_K^{\times} : O_F^{\times} \right] > 1 \) are classified in [14] Subsection 2.8. For a nontrivial element \( \tilde{u} \in O_K^{\times}/O_F^{\times} \), we have

- \( \text{ord}(\tilde{u}) \in \{2, 3, 4\} \) if \( d = 2 \);
- \( \text{ord}(\tilde{u}) \in \{2, 3, 4, 6, 12\} \) if \( d = 3 \);
- \( \text{ord}(\tilde{u}) \in \{2, 3, 5\} \) if \( d = 5 \).

The results in Table 1 hold for \( p = 2, 3, 5 \) as well. Thus our knowledge on minimal \( D_2 \) or \( D_3 \)-orders applies here. If \( \text{ord}(\tilde{u}) = 5 \), then \( p = 5 \) and \( F(\tilde{u}) = \mathbb{Q}(\zeta_5) \).

Let \( D' \) be an arbitrary totally definite quaternion \( F \)-algebra. We claim that \( D' = D_{\infty_1, \infty_2} \) if it contains an \( O_F \)-order \( O \) with non-cyclic reduced unit group \( O^{\ast} \). Indeed, we have

\[
O^{\ast} \in \begin{cases} 
\{D_2, D_3, D_4, A_4, S_4\} & \text{if } p = 2; \\
\{D_2, D_3, D_4, A_4, S_4, D_6, D_{12}\} & \text{if } p = 3; \\
\{D_2, D_3, A_4, D_5, A_5\} & \text{if } p = 5. 
\end{cases}
\]

First, suppose that \( O^{\ast} \supseteq D_2 \). Recall that a minimal \( D_2 \)-order has discriminant \( 4O_F \). Thus \( D' \) splits at all non-dyadic primes of \( F \). Since 2 is either inert or ramified in \( F \) and the number of ramified places of \( D' \) is even, \( D' \) necessarily splits at the dyadic prime of \( F \) as well. Similarly, \( D = D_{\infty_1, \infty_2} \) if \( O^{\ast} \supseteq D_3 \). This verifies our claim in the cases \( p = 2, 3 \). Lastly, if \( O^{\ast} \simeq D_5 \) or \( A_5 \), then \( O \) contains a minimal \( D_5 \)-order, which implies (by the argument in Subsection 4.6) that \( D' = \{\mathbb{Q}(\zeta_5), -1\} = D_{\infty_1, \infty_2} \).

Thanks to [38] (See also [43] Theorem 1.3), we have

\[
(8.2) \quad t(D) = h(D) = \begin{cases} 
1 & \text{if } p = 2, 5; \\
2 & \text{if } p = 3.
\end{cases}
\]

Using the Magma Computational Algebra System [5], one easily checks that

| \( p \) | 2 | 3 | 5 |
|---|---|---|---|
| \( t(G) \) | \( t(S_4) = 1 \) | \( t(S_4) = t(D_{12}) = 1 \) | \( t(A_5) = 1 \) |

This can also be obtained by hand using the mass formula [40] Corollaire V.2.3], which we leave to the interested readers.
8.2. **Case** \( p \equiv 3 \pmod{4} \) **and** \( p > 3 \). First, we write down \( t(G) \) for \( G \) non-cyclic. Since 3 is unramified in \( F \), we have \( 3 \notin F^{\times 2} \). In particular, \( t(D_6) = 0 \). On the other hand, \( 2 \varepsilon \in F^{\times 2} \) by [25] Lemma 3, p. 91 or [47] Lemma 3.2(1)). It follows from the results of Section 5 that

\[
(8.3) \quad t(S_4) = t(D_4) = 1, \quad t(A_4) = t(D_2^2) = 0.
\]

The unique conjugacy class of maximal orders with reduced unit group \( D \) is represented by \( O_{24} \) in (4.15) (resp. \( O_8 \) in Definition 5.2). Write \( \varepsilon = a + b\sqrt{p} \) with \( a, b \in \mathbb{N} \). Then \( a \) is even and \( b \) is odd by [17] Theorem 1.1(1)), and hence \( \varepsilon \) is even by Proposition 6.2. Therefore, \( t(D_1^2) = 0 \) by Corollary 6.3. For \( p > 3 \), \( D_{\infty_1, \infty_2} \cong \left( \frac{-1-3}{p} \right) \) if and only if \( p \equiv 2 \pmod{3} \). Thus

\[
(8.4) \quad t(D_3) = \frac{1}{2} \left( 1 - \left( \frac{p}{3} \right) \right).
\]

If \( p \equiv 1 \pmod{3} \), then the fact that \( 2 \varepsilon \in F^{\times 2} \) implies that \( \varepsilon \equiv -1 \pmod{3O_F} \). Therefore, \( \left( \frac{-3}{p} \right) \cong D_{\infty_1, \infty_2} \) for all \( p > 3 \) by Lemma 6.7. It follows from Corollary 6.9 that

\[
(8.5) \quad t(D_3) = \varepsilon(O_2^3) - t(S_4) - t(D_6) = \frac{1}{2} \left( 1 + \left( \frac{p}{3} \right) \right).
\]

Combining (8.4) and (8.5), we obtain

\[
(8.6) \quad t(D_3) = t(D_3^1) + t(D_3^2) = 1.
\]

Next, we calculate \( t(C_n) \) for \( n \in \{2, 3, 4\} \). Recall that \( \mathcal{B}_n \) denotes the finite set of \( O_F \)-orders \( B \) in some CM-extension of \( F \) such that \( B^\times/O_F^\times \cong C_n \). We set

\[
t(C_n, B) := \# \{ [O'] \in \text{Tp}(D) \mid O'^\times \cong C_n, \text{ and } \text{Emb}(B, O') \neq \emptyset \}.
\]

It will be shown in [45] that

\[
(8.7) \quad h(C_n, B) = h(F)t(C_n, B) \quad \forall B \in \mathcal{B}_n.
\]

When \( n = 4 \), we have \( \mathcal{B}_n = \{ O_{F(\sqrt{-1})}, B_{1,2} \} \), where \( B_{1,2} \) is defined in [47]. One calculates that

\[
(8.8) \quad m(O_{F(\sqrt{-1})}, O_{24}, O_{24}^\times) = 0, \quad m(O_{F(\sqrt{-1})}, O_8, O_8^\times) = 1;
\]

\[
(8.9) \quad m(B_{1,2}, O_{24}, O_{24}^\times) = 1, \quad m(B_{1,2}, O_8, O_8^\times) = 0.
\]

For simplicity, let \( h(m) := h(O(\sqrt{m})) \) for any square-free \( m \in \mathbb{Z} \). Combining the above formulas with (8.10) and (8.11), we obtain

\[
(8.10) \quad t(C_4, O_{F(\sqrt{-1})}) = \frac{h(F(\sqrt{-1}))}{2h(F)} - \frac{1}{2} = \frac{h(-p) - 1}{2};
\]

\[
(8.11) \quad t(C_4, B_{1,2}) = \frac{h(B_{1,2})}{2h(F)} - \frac{1}{2} = \frac{1}{2} \left( \left( 2 - \left( \frac{2}{p} \right) \right) h(-p) - 1 \right).
\]

Here, we used the formula of Herglotz [19] to rewrite \( h(F(\sqrt{-1}))/h(F) \) (see also [44] (2.16)). Then

\[
(8.12) \quad t(C_4) = t(C_4, O_{F(\sqrt{-1})}) + t(C_4, B_{1,2}) = \left( 3 - \left( \frac{2}{p} \right) \right) \frac{h(-p)}{2} - 1.
\]

When \( n = 3 \), we have \( \mathcal{B}_3 = \{ O_{F(\sqrt{-1})} \} \). Let \( O_6 = O \) in (8.27) if \( p \equiv 1 \pmod{3} \), and \( O_6 = O_3^1 \) in (5.13) if \( p \equiv 2 \pmod{3} \). Then \( O_6 \) is a representative
of the unique conjugacy class of maximal orders with reduced unit group $D_3$, and $\mathcal{N}(\mathcal{O}_0) = F^\times \mathcal{O}_0^\times$ by either Subsection 6.11 or Proposition 5.6. We have
\[(8.13)\quad m(O_{F(\sqrt{-7}), \mathcal{O}_{24}}) = 1 \quad \text{and} \quad m(O_{F(\sqrt{-7}), \mathcal{O}_{6}}) = 1.\]
Applying (3.10) again, we obtain
\[(8.14)\quad t(C_3) = \frac{h(-3p)}{4} - 1.\]
When $n = 2$, we have $\mathcal{R}_2 = \{O_F[\sqrt{-1}], \mathcal{O}_F[\sqrt{-2}]\}$, where $\mathcal{O}_F[\sqrt{-2}]$ coincides with the ring of integers of $F(\sqrt{-2}) = F(\sqrt{-2})$ by Lemma 7.4. We calculate that
\[
m(O_F[\sqrt{-1}], \mathcal{O}_{24}, \mathcal{O}_{24}^\times) = 0, \quad m(O_F[\sqrt{-2}], \mathcal{O}_{24}, \mathcal{O}_{24}^\times) = 1,
\]
\[
m(O_F[\sqrt{-1}], \mathcal{O}_8, \mathcal{O}_8^\times) = 1, \quad m(O_F[\sqrt{-2}], \mathcal{O}_8, \mathcal{O}_8^\times) = 1,
\]
\[
m(O_F[\sqrt{-1}], \mathcal{O}_6, \mathcal{O}_6^\times) = 1 - \left(\frac{p}{3}\right), \quad m(O_F[\sqrt{-2}], \mathcal{O}_6, \mathcal{O}_6^\times) = 1 + \left(\frac{p}{3}\right).\]
For simplicity, we set $t(C_2^1) = t(C_2, O_F[\sqrt{-1}])$, and $t(C_2^1) = t(C_2, O_F[\sqrt{-2}])$. Then
\[
(8.15)\quad t(C_2^1) = \left(2 - \left(\frac{2}{p}\right)\right) \frac{h(-p)}{2} + \frac{1}{2} \left(\frac{p}{3}\right) - 1;
\]
\[
(8.16)\quad t(C_2^1) = \frac{h(-2p)}{2} - \frac{1}{2} \left(\frac{p}{3}\right) - \frac{3}{2};
\]
\[
(8.17)\quad t(C_2) = t(C_2^1) + t(C_2^1) = \left(2 - \left(\frac{2}{p}\right)\right) \frac{h(-p)}{2} + \frac{h(-2p)}{2} - \frac{5}{2}.
\]
Lastly, using the class number formula for $D$ (see [28,31,38] or [43, Theorem 1.3]), we obtain
\[
(8.18)\quad t(C_1) = \frac{h(D)}{h(F)} - t(S_5) - t(D_4) - t(D_3) - t(C_4) - t(C_3) - t(C_2)
\]
\[
= \frac{\zeta / (1)}{2} + \left(-7 + 3 \left(\frac{2}{p}\right)\right) \frac{h(-p)}{8} - \frac{h(-2p)}{4} - \frac{h(-3p)}{12} + \frac{3}{2}.
\]
Here $h(D)/h(F) = t(D)$ by (8.1).
As $t(G) = 0$ for all $G \not\in \{S_4, D_4, D_3, C_4, C_3, C_2, C_1\}$, this concludes the computation of $t(G)$ for all $G$.

9. Superspecial abelian surfaces

We keep the notation of the previous section. In particular, $F = \mathbb{Q}(\sqrt{p})$, where $p$ is a prime number, $D = D_{\infty_1, \infty_2}$. In this section, we give two applications of Theorems 1.5 and 1.6 to superspecial abelian surfaces. The first one gives for each finite group $G$ an explicit formula for the number of certain superspecial abelian surfaces with reduced automorphism group $G$; this one is straightforward. For the second application we construct superspecial abelian surfaces $X$ over some field $k$ of characteristic $p$ with endomorphism algebra $\text{End}^0(X) := \text{End}_k(X) \otimes \mathbb{Q} \simeq \text{End}_k(X)$. We caution the reader that the notation $\text{End}(X)$ is also used for the endomorphism ring of $X \otimes_k k$ over $k$ in the literature, where $k$ is an algebraic closure of $k$.

\footnote{For an abelian variety $X$ over a field $k$, we write $\text{End}_k(X)$, or simply $\text{End}(X)$ if the ground field $k$ is clear, for the endomorphism ring of $X$ over $k$. For any field extension $K/k$, we write $\text{End}_k(X \otimes_k K)$ or simply $\text{End}(X \otimes_k K)$ for the endomorphism ring of $X \otimes_k K$ (over $K$). Some authors denote the latter by $\text{End}_k(X)$. We caution the reader that the notation $\text{End}(X)$ is also used for the endomorphism ring of $X \otimes_k k$ over $k$ in the literature, where $k$ is an algebraic closure of $k$.}
F, provided that \( p \not\equiv 1 \pmod{24} \). Recall that an abelian variety over a field \( k \) of characteristic \( p \) is said to be \textit{superspecial} if it is isomorphic to a product of supersingular elliptic curves over an algebraic closure \( \overline{k} \) of \( k \).

9.1. **The first application.** Fix a Weil \( p \)-number \( \pi = \sqrt{p} \) and a maximal order \( \mathcal{O} \) in \( D \). Let \( \text{Isog}^{O_P}(\pi) \) denote the set of \( \mathbb{F}_p \)-isomorphism classes of simple abelian varieties \( X \) over \( \mathbb{F}_p \) with Frobenius endomorphism \( \pi_X \) satisfying \( \pi_X^2 = p \) and with endomorphism ring \( \text{End}(X) \supset O_P \). Any member \( X \) in \( \text{Isog}^{O_P}(\pi) \) is necessarily a superspecial abelian surface. Let

\[
(9.1) \quad \text{Tp}(\pi) := \{ \text{End}(X) \mid X \in \text{Isog}^{O_P}(\pi) \}/ \cong .
\]

By [43, Theorem 6.1.2], we have a natural bijection \( \text{Cl}(\mathcal{O}) \cong \text{Isog}^{O_P}(\pi) \). If the superspecial class \( [X] \) corresponds to the ideal class \( [I] \), then \( \text{End}(X) \cong O_I \). Thus, one obtains a natural bijection \( \text{Tp}(\pi) \cong \text{Tp}(D) \). In particular,

\[
(9.2) \quad h(\pi) := \# \text{Isog}^{O_P}(\pi) = h(D), \quad t(\pi) := \# \text{Tp}^{O_P}(\pi) = t(D).
\]

For any finite group \( G \), define

\[
(9.3) \quad h(\pi, G) := \#\{ X \in \text{Isog}^{O_P}(\pi) \mid \text{RAut}(X) \cong G \},
\]

where \( \text{RAut}(X) := \text{Aut}(X)/O_P^X \) is the reduced automorphism group of \( X \). As the above correspondence preserves the automorphism groups, one has \( h(\pi, G) = h(G) \), which is also equal to \( h(F)t(D) \) by Proposition 1.1. By Theorems 1.5 and 1.6, we obtain explicit formulas for \( h(\pi, G) \).

**Proposition 9.1.** For any finite group \( G \), we have \( h(\pi, G) = h(F)t(G) \), where an explicit formula for each \( t(G) \) is given by Theorems 1.5 and 1.6.

9.2. **Pop’s result on embedding problems.** We state a main result of F. Pop on embedding problems for large fields in [32]. Let \( k \) be any field. Let \( \Gamma_k := \text{Gal}(k_s/k) \) denote the absolute Galois group of \( k \), where \( k_s \) is a separable closure of \( k \). An embedding problem (EP) for \( k \) is a diagram of surjective morphisms of profinite groups \( (\gamma : \Gamma_k \to A, \alpha : B \to A) \). An EP is said to be \textit{finite} if the profinite group \( B \) is finite (hence \( A \) is also finite); it is called \textit{split} if the homomorphism \( \alpha \) has a section. We write \( k_{\text{EP}} \) for the fixed subfield of \( \ker \gamma \). A solution of an EP is a homomorphism of profinite groups \( \beta : \Gamma_k \to B \) such that \( \alpha \beta = \gamma \); it is called a \textit{proper} solution if \( \beta \) is surjective.

Let \( K = k(t) \), where \( t \) is a variable. We fix a separable closure \( K_s \) of \( K \) which contains \( k_s \), and let \( \pi : \Gamma_K \to \Gamma_k \) be the canonical projection. To each EP \( \gamma(\alpha) \) for \( k \) one associates an EP \( K \) := \( (\gamma \pi, \alpha) \) for \( K \). If \( \beta \) is a solution of \( \text{EP}_K \), define

\[
K_{\beta} := K_{\text{ker} \beta}, \quad \overline{k}_\beta := K_{\beta} \cap k_s.
\]

A (proper) \textit{regular} solution of an EP is a (proper) solution \( \beta \) of \( \text{EP}_K \) such that \( k_{\beta} = k_{\text{EP}} \).

The regular inverse Galois problem for \( k \) asks whether for a given finite group \( G \), there exists a regular finite Galois extension \( L/k(t) \) (regularity means that \( L \cap k_s = k \) in a separable closure \( k(t)_s \) of \( k(t) \)) with Galois group \( \text{Gal}(L/k(t)) \cong G \). If \( A = \{1\} \) and \( B = G \) is finite, then a proper solution for an EP is precisely a solution for an inverse Galois problem, and a proper regular solution for an EP is precisely a solution for a regular inverse Galois problem.
Definition 9.2. A field $k$ is said to be large if for any smooth curve $C$ over $k$, we have implication

$$C(k) \neq \emptyset \implies |C(k)| = \infty.$$ 

Theorem 9.3 ([32 Main Theorem A]). Assume that $k$ is large. Then every finite split EP for $k$ has proper regular solutions. In particular, every finite group $G$ is regularly realizable as a Galois group over $k(t)$.

The proof in [32] also shows that that there are infinitely many solutions in Theorem 9.3.

9.3. The second application. Let $X_0$ be an abelian variety over any field $K$. It is well known that the Galois cohomology $H^1(\Gamma_K, \text{Aut}(X_0 \otimes_K K))$ classifies all $K$-forms of $X_0/K$ up to $K$-isomorphism. Any class in $H^1(\Gamma_K, \text{Aut}(X_0 \otimes_K K))$ is represented by a 1-cocycle $\xi = (\xi_\sigma) \in Z^1(\text{Gal}(L/K), \text{Aut}(X_0 \otimes_K L))$ for some finite Galois extension $L/K$.

Lemma 9.4. Suppose $X_\xi/K$ is the abelian variety corresponding to a 1-cocycle $\xi = (\xi_\sigma) \in Z^1(\text{Gal}(L/K), \text{Aut}(X_0 \otimes_K L))$. Then

$$\text{End}(X_\xi) \cong \{y \in \text{End}(X_0 \otimes_K L) \mid \xi_\sigma(y)\xi_\sigma^{-1}, \forall \sigma \in \text{Gal}(L/K)\}.$$ 

Lemma 9.5. For any fixed power $q$ of $p$ and any positive integer $\ell$, the field

$$k := \mathbb{F}_{q^{\ell m}} := \bigcup_{m \geq 1} \mathbb{F}_{q^{\ell m}}$$

is large.

Proof. This follows immediately from the Hasse-Weil bound for the size $|C(\mathbb{F}_{q^{\ell m}})|$ of $\mathbb{F}_{q^{\ell m}}$-rational points of a curve $C$. □ □

Proposition 9.6. There exists a maximal $O_F$-order $O$ in $D = D_{\infty_1, \infty_2}$ for which the unit group $O^\times$ contains a finite non-abelian group if and only if $p \neq 1 \pmod{24}$.

Proof. The reduced norm map $N_r : O^\times \to O_F^\times$ induces a map $N_r : O^\times \to O_F^\times/(O_F^\times)^2$. The kernel of this map is $O^1/\{\pm 1\}$, where $O^1 \subset O^\times$ is the reduced norm one subgroup. Thus the index $[O^\times : O^1/\{\pm 1\}] = 1, 2$, and $[O^\times : O^1/\{\pm 1\}] = 1$ if $N(\varepsilon) = -1$. If $p \leq 5$ or $p \equiv 3 \pmod{4}$, then there is a maximal order $O$ such that $O^\times \cong S_4$ or $A_5$ by Theorem 1.6. Then the finite group $O^1/\{\pm 1\}$ must be non-abelian and hence $O^1$ is a non-abelian finite subgroup of $O^\times$. Note that $p \leq 5$ or $p \equiv 3 \pmod{4}$ implies that $p \neq 1 \pmod{24}$. Now assume that $p \equiv 1 \pmod{4}$ and $p \geq 7$. In this case $N(\varepsilon) = -1$ and $O^\times = O^1/\{\pm 1\}$. One has $O^1/\{\pm 1\} \cong C_n$ for $n = 1, 2, 3$ if and only if $O^1/\mu_{2n} \cong C_{2n}$. It then follows from Theorem 1.6 that there exists a maximal order $O$ with $O^1$ non-abelian if and only if $\left(\frac{2}{p}\right) = -1$ or $\left(\frac{2}{p}\right) = -1$. The latter is equivalent to $p \neq 1 \pmod{24}$ under the condition $p \equiv 1 \pmod{4}$. This proves the proposition. □

Proposition 9.7. Suppose $X_0/\mathbb{F}_p \in \text{Isog}^{O_F}(\pi)$ is a member such that $\text{Aut}(X_0)$ contains a finite non-abelian group $G$. There exist a positive integer $\ell$ and infinitely many abelian varieties $X$ over $K := \mathbb{F}_{p^{\infty}}(t)$, which are $K$-forms of $X_0 \otimes_{\mathbb{F}_p} K$, such that the endomorphism algebra $\text{End}(X)$ of $X$ is isomorphic to $F = \mathbb{Q}(\sqrt{p})$. □
Proof. Let $\mathbb{F}_{p^n}/\mathbb{F}_p$ be a finite extension such that $\text{End}(X_0 \otimes \mathbb{F}_p^n) = \text{End}(X_0 \otimes \mathbb{F}_p)$. Let $\ell$ be any positive integer with $(\ell, n) = 1$ and put $k = \mathbb{F}_p\ell$ and $K = k(t)$. Then $k \cap \mathbb{F}_p = \mathbb{F}_p$ and one has $\text{End}(X_0 \otimes k) = \text{End}(X_0)$, which is a maximal order in $D$. Since $K/k$ is primary, $\text{End}(X_0 \otimes K) = \text{End}(X_0 \otimes k) = \text{End}(X_0)$ by Chow’s Theorem [10]; see also [12, Theorem 3.19]. Since $k$ is large (Lemma 9.5), there exist infinitely many regular finite Galois extensions $L/K$ with Galois group $\text{Gal}(L/K) \simeq G$ by Theorem 9.3. Consider the homomorphism $\xi : \text{Gal}(L/K) \rightarrow \text{Aut}(X_0 \otimes L)$ defined by the composition $\text{Gal}(L/K) \xrightarrow{\sim} G \subset \text{Aut}(X_0 \otimes L) \subset \text{Aut}(X_0 \otimes K)$. Since $L/K$ is regular, we have $\text{End}(X_0 \otimes L) = \text{End}(X_0 \otimes K) = \text{End}(X_0)$ by Chow’s Theorem again. Thus, $\text{Gal}(L/K)$ acts trivially on $\text{Aut}(X_0 \otimes L)$ and hence $\xi$ is a 1-cocycle. Let $X/K$ be the abelian variety corresponding to $\xi$. Then by Lemma 9.4, $\text{End}^0(X)$ is isomorphic to the centralizer of $G$ in $\text{End}^0(X_0) = D$ which is the center $F = \mathbb{Q}(\sqrt{p})$. □

Corollary 9.8. Assume that $p \not\equiv 1 \pmod{24}$. Then there is a superspecial abelian surface $X$ over some field $K$ of characteristic $p$ such that $\text{End}^0_K(X) \simeq \mathbb{Q}(\sqrt{p})$.

Proof. This follows from Propositions 9.6 and 9.7 □

Acknowledgements

J. Xue is partially supported by the 1000-plan program for young talents and Natural Science Foundation grant #11601395 of PRC. He thanks the Morningside Center of Mathematics (CAS), Academia Sinica and NCTS for their hospitality and great working conditions during his visits in 2017, hosted by Xu Shen and Chia-Fu Yu, respectively. C.-F. Yu is partially supported by the grant MoST 104-2115-M-001-001-MY3.

References

[1] Saban Alaca and Kenneth S. Williams. Introductory algebraic number theory. Cambridge University Press, Cambridge, 2004.
[2] Roger C. Alperin. Remarks on a problem of Eisenstein. JP J. Algebra Number Theory Appl., 7(1):97–102, 2007.
[3] Luis Arenas-Carmona. Eichler orders, trees and representation fields. Int. J. Number Theory, 9(7):1725–1741, 2013.
[4] Luis Arenas-Carmona and Ignacio Saavedra. On some branches of the Bruhat-Tits tree. Int. J. Number Theory, 12(3):813–831, 2016.
[5] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. J. Symbolic Comput., 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).
[6] J. Brzeziński. On orders in quaternion algebras. Comm. Algebra, 11(5):501–522, 1983.
[7] J. Brzeziński. On automorphisms of quaternion orders. J. Reine Angew. Math., 403:166–186, 1990.
[8] Juliusz Brzeziński. Definite quaternion orders of class number one. J. Théor. Nombres Bordeaux, 7(1):93–96, 1995. Les Dix-huitièmes Journées Arithmétiques (Bordeaux, 1993).
[9] D. A. Buell, H. C. Williams, and K. S. Williams. On the imaginary bicyclic biquadratic fields with class-number 2. Math. Comp., 31(140):1034–1042, 1977.
[10] Wei-Liang Chow. Abelian varieties over function fields. Trans. Amer. Math. Soc., 78:253–275, 1955.
[11] P. E. Conner and J. Hurrelbrink. Class number parity, volume 8 of Series in Pure Mathematics. World Scientific Publishing Co., Singapore, 1988.
[12] Brian Conrad. Chow’s $K/k$-image and $K/k$-trace, and the Lang-Néron theorem. *Enseign. Math.* (2), 52(1-2):37–108, 2006.

[13] Charles W. Curtis and Irving Reiner. *Methods of representation theory. Vol. II.* Pure and Applied Mathematics (New York). John Wiley & Sons, Inc., New York, 1987. With applications to finite groups and orders, A Wiley-Interscience Publication.

[14] Yuriy A. Drozd and Vladimir V. Kirichenko. *Finite-dimensional algebras.* Springer-Verlag, Berlin, 1994. Translated from the 1980 Russian original and with an appendix by Vlastimil Dlab.

[15] Martin Eichler. Zur Zahlentheorie der Quaternionen-Algebren. *J. Reine Angew. Math.* 195:127–151 (1956), 1955.

[16] A. Fröhlich and M. J. Taylor. *Algebraic number theory*, volume 27 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1993.

[17] Emmanuel Hallouin and Christian Maire. Cancellation in totally definite quaternion algebras. *J. Reine Angew. Math.*, 595:189–213, 2006.

[18] Ki-ichiro Hashimoto. Twisted trace formula of the Brandt matrix. *Proc. Japan Acad. Ser. A Math. Sci.*, 53(3):98–102, 1977.

[19] G. Herglotz. Über einen Dirichletschen Satz. *Math. Z.*, 12(1):255–261, 1922.

[20] Jae Moon Kim and Jado Ryu. On the class number and the fundamental unit of the real quadratic field $k = \mathbb{Q}(\sqrt{pq})$. *Bull. Aust. Math. Soc.*, 85(3):359–370, 2012.

[21] Markus Kirschmer and David Lorch. Ternary quadratic forms over number fields with small class number. *J. Number Theory*, 161:343–361, 2016.

[22] Markus Kirschmer and John Voight. Algorithmic enumeration of ideal classes for quaternion orders. *SIAM J. Comput.*, 39(5):1714–1747, 2010.

[23] Yoshiyuki Kitaoka. Quaternary even positive definite quadratic forms of prime discriminant. *Nagoya Math. J.*, 52:147–161, 1973.

[24] Ke-Zheng Li and Frans Oort. *Moduli of supersingular abelian varieties*, volume 1680 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1998.

[25] O. Timothy O’Meara. *Introduction to quadratic forms*. Classics in Mathematics. Springer-Verlag, Berlin, 2000. Reprint of the 1973 edition.

[26] Daniel A. Marcus. *Number fields*. Springer-Verlag, New York, 1977. Universitext.

[27] Arnold Pizer. On the arithmetic of quaternion algebras. *Acta Arith.*, 31(1):61–89, 1976.

[28] Arnold K. Pizer. Type numbers of Eichler orders. *J. Reine Angew. Math.*, 264:76–102, 1973.

[29] I. Reiner. *Maximal orders*, volume 28 of *London Mathematical Society Monographs. New Series*. The Clarendon Press Oxford University Press, Oxford, 2003. Corrected reprint of the 1975 original, With a foreword by M. J. Taylor.

[30] Marie-France Vignéras. Arithmétique des algèbres de quaternions, volume 800 of *Lecture Notes in Mathematics*. Springer, Berlin, 1980.

[31] Fu-Tsun Wei and Chia-Fu Yu. Class numbers of central simple algebras over global function fields. *Int. Math. Res. Not. IMRN*, (11):3525–3575, 2015.
J. Xue, T.-C. Yang, and C.-F. Yu. On superspecial abelian surfaces over finite fields II. ArXiv e-prints, January 2018, arXiv:1801.09374.

Jiangwei Xue, Tse-Chung Yang, and Chia-Fu Yu. Supersingular abelian surfaces and Eichler’s class number formula. ArXiv e-prints, April 2014, arXiv:1404.2978 to appear in The Asian Journal of Mathematics.

Jiangwei Xue, Tse-Chung Yang, and Chia-Fu Yu. Numerical invariants of totally imaginary quadratic $\mathbb{Z}[\sqrt{p}]$-orders. Taiwanese J. Math., 20(4):723–741, 2016.

Jiangwei Xue, Tse-Chung Yang, and Chia-Fu Yu. On superspecial abelian surfaces over finite fields. Doc. Math., 21:1607–1643, 2016.

Jiangwei Xue and Chia-Fu Yu. On superspecial abelian surfaces and type numbers of definite quaternion algebras. In preparation.

Zhe Zhang and Qin Yue. Fundamental units of real quadratic fields of odd class number. J. Number Theory, 137:122–129, 2014.