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

QUN LI, JIANGWEI XUE, AND CHIA-FU YU

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

1. INTRODUCTION

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

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

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

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

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

Date: May 16, 2018.

Let $I_1, \dots, I_h$ be a complete set of representatives of the right ideal class set $\mathrm{Cl}(\mathbb{O})$. The mass of $\mathrm{Cl}(\mathbb{O})$ is defined to be

$$\mathrm{Mass}(\mathbb{O}) := \sum_{i=1}^{h} \frac{1}{|\mathbb{O}_i^\times / O_F^\times|}, \qquad \text{where } \mathbb{O}_i := \mathcal{O}_l(I_i) \text{ is the left order of } I_i.$$

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

$$\mathrm{Mass}(\mathbb{O}) = \frac{1}{2}\zeta_F(-1) \prod_{\mathfrak{p} \mid \mathfrak{d}(\mathbb{O})} (N(\mathfrak{p}) - 1),$$

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

$$h(\mathbb{O}) = \mathrm{Mass}(\mathbb{O}) + \mathrm{Ell}(\mathbb{O}),$$

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

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

Conjecture 2. We have

$$\frac{\mathrm{Mass}(\mathbb{O})}{h(\mathbb{O})} \to 1, \quad \text{as long as } h(\mathbb{O}) \to \infty.$$

This expectation is verified [15, Section 6.3] for the family of totally definite quaternion $\mathbb{Q}(\sqrt{p})$-algebras B_{∞_1,∞_2} which are unramified at all finite places of $\mathbb{Q}(\sqrt{p})$ with p running through all prime numbers. In general, it follows from Eichler's trace formula that the term $\mathrm{Ell}(\mathbb{O})$ is a linear combination of class numbers of two kinds of CM extensions K/F:

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

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

2. The Example of quaternion $\mathbb{Q}$-algebras

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

$$\mathbb{O}^\times \in \{C_2, C_4, C_6\} \tag{2.1}$$

except that

$$\begin{aligned} B &= B_{2,\infty}, \quad h(\mathbb{O}) = 1, \quad \mathbb{O}^\times \simeq \mathrm{SL}_2(\mathbb{F}_3), \quad \text{or} \\ B &= B_{3,\infty}, \quad h(\mathbb{O}) = 1, \quad \mathbb{O}^\times \simeq \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}, \end{aligned}$$

where $B_{p,\infty}$ denotes the quaternion $\mathbb{Q}$-algebra ramified exactly at $\{p,\infty\}$. Thus, $\mathbb{O}^\times$ is cyclic except for finitely many definite quaternion $\mathbb{Q}$-algebras B and for finitely many (not necessarily maximal) orders $\mathbb{O}$ up to conjugate. Put

$$h(B,G) := \#\{[I] \in \mathrm{Cl}(\mathbb{O}) \mid \mathcal{O}_l(I)^\times/\{\pm 1\} \simeq G\}, \tag{2.2}$$

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

$$h(C_1) = h(B,C_1) = \frac{p-1}{12} - \frac{1}{4}\left(1 - \left(\frac{-4}{p}\right)\right) - \frac{1}{6}\left(1 - \left(\frac{-3}{p}\right)\right), \tag{2.3}$$

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

In particular, we have

$$\mathcal{O}_l(I)^\times = \{\pm 1\}, \ \forall\, [I] \in \mathrm{Cl}(\mathbb{O}) \iff p \equiv 1 \pmod{12}. \tag{2.5}$$

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

$$\begin{array}{ccc} \mathrm{Cl}(\mathbb{O}) & \simeq & \left\{ \begin{array}{l} \text{isomorphism classes of supersin-} \\ \text{gular elliptic curves over } \overline{\mathbb{F}}_p \end{array} \right\} \\ {[I]} & \longleftrightarrow & [E] \end{array}$$

which identifies $\mathcal{O}_l(I)$ with $\mathrm{End}(E)$. Using (2.4) and the geometric interpretation above, we compute in [17] forms of supersingular elliptic curves over a suitable *non-perfect* field, and compute their endomorphism algebras. As a result, we obtain the following result.

Proposition 3 ([17, Theorem 1.3]). *There exists a supersingular elliptic curve E over some field $k \supset \mathbb{F}_p$ with $\mathrm{End}_k^0(E) = \mathbb{Q}$ if and only if $p \not\equiv 1 \pmod{12}$.*

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

3. Results for $F = \mathbb{Q}(\sqrt{p}\,)$, p a prime

Let p be a prime number and B the totally definite quaternion $F = \mathbb{Q}(\sqrt{p}\,)$-algebra ramified only at the two infinite places of F, which is also denoted by B_{∞_1,∞_2}. Fix again a maximal O_F-order $\mathbb{O}$ in B. In this case, there is a natural bijection (see [13, Theorem 6.2] and [15, Theorem 6.1.2])

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

For any finite group G, put

$$t(G) := \#\left\{ \begin{array}{l} B^\times\text{-conjugacy classes of maximal} \\ O_F\text{-orders } \mathcal{O} \subset B \text{ with } \mathcal{O}^\times/O_F^\times \simeq G \end{array} \right\}.$$

Proposition 1 also gives the class-type number relation

$$h(G) = h(F) \cdot t(G). \tag{3.1}$$

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

Lemma 4. *We have*

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

Theorem 5. *Assume* $p \geq 7$.
(1) (Hashimoto [6]) *For* $p \equiv 1 \mod 4$, *we have*

$$\begin{aligned}
t(C_1) &= \frac{\zeta_F(-1)}{2} - \frac{h(-p)}{8} - \frac{h(-3p)}{12} - \frac{1}{4}\left(\frac{p}{3}\right) - \frac{1}{4}\left(\frac{2}{p}\right) + \frac{1}{2}, \\
t(C_2) &= \frac{h(-p)}{4} + \frac{1}{2}\left(\frac{p}{3}\right) + \frac{1}{4}\left(\frac{2}{p}\right) - \frac{3}{4}, \\
t(C_3) &= \frac{h(-3p)}{4} + \frac{1}{4}\left(\frac{p}{3}\right) + \frac{1}{2}\left(\frac{2}{p}\right) - \frac{3}{4}, \\
t(D_3) &= \frac{1}{2}\left(1 - \left(\frac{p}{3}\right)\right), \quad t(A_4) = \frac{1}{2}\left(1 - \left(\frac{2}{p}\right)\right),
\end{aligned}$$

and $t(G) = 0$ *for any group* G *not in the above list. Here* $h(m)$ *is short for* $h(\mathbb{Q}(\sqrt{m}))$ *for a square-free integer* $m \in \mathbb{Z}$.
(2) (Li-Xue-Yu) *For* $p \equiv 3 \mod 4$, *we have*

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

and $t(G) = 0$ *for any group* G *not listed above.*

By Theorem 5, there exists a superingular abelian surface X over $\mathbb{F}_p$ with *non-abelian* reduced automorphism group $\mathrm{RAut}(X) = \mathrm{Aut}(X)/O_F^\times$ if and only if $p \equiv 3 \pmod 4$ or $p \not\equiv 1 \pmod{24}$. Note that $p \equiv 3 \pmod 4$ implies $p \not\equiv 1 \pmod{24}$. Using a similar idea of the proof of Proposition 3, one can prove

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

Question 7. (1) Is $p \not\equiv 1 \pmod{24}$ a necessary condition for the assertion of Proposition 6?

(2) For a given prime p, what are all possible endomorphism algebras of supersingular abelian surfaces over some field of characteristic $p > 0$?

One can use results of [17] to deduce all possible endomorphism algebras of *non-simple* supersingular abelian surfaces. The most interesting part of Question 7 (2) then is for *simple* supersingular abelian surfaces.

4. Results for $F = \mathbb{Q}(\sqrt{d}\,)$

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

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

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

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

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

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

$$\mathcal{O}^\star := \mathcal{O}^\times / O_F^\times \in \{C_n, D_n \ (1 \le n \le 6 \text{ or } n = 12),\ A_4,\ S_4,\ A_5\}.$$

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

$$\mathcal{O}^\star \hookrightarrow (B \otimes_F \mathbb{R})^\times / \mathbb{R}^\times = \mathbb{H}^\times / \mathbb{R}^\times \simeq \mathrm{SO}_3(\mathbb{R}),$$

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

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

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

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

$$A_5 \text{ occurs } \iff F = \mathbb{Q}(\sqrt{5}\,) \text{ and } B = B_{\infty_1,\infty_2}.$$

In fact, when $d \in \{2,3,5\}$, there exists an O_F-order with non-cyclic reduced unit group if and only if $B \simeq B_{\infty_1,\infty_2}$, which has already been treated in Section 3. Thus, we may consider only the following list for square-free $d \geq 6$:

$$\mathcal{G} := \{C_1, C_2, C_3, C_4, C_6, D_2, D_3, D_4, D_6, A_4, S_4\}. \tag{4.1}$$

For non-cyclic groups in $\mathcal{G}$, one has the following inclusions:

$$D_2 \subset D_4 \subset S_4, \quad D_2 \subset A_4 \subset S_4, \quad D_3 \subset \{S_4, D_6\}, \quad \{D_2, D_3\} \subset D_6. \tag{4.2}$$

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

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

$$\sum_{C_n \subset G} a_n(G) h(G) = \sum_R h(R) \prod_{\mathfrak{p}} m_{\mathfrak{p}}(R), \qquad \forall n \geq 2, \tag{4.3}$$

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

$$\sum_G h(G) = h(\mathbb{O}).$$

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

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

5. Occurence of non-cyclic groups

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

$$S := \begin{cases} \{1\} & \text{if } \mathrm{N}_{F/\mathbb{Q}}(\varepsilon) = -1; \\ \{1, \varepsilon\} & \text{otherwise.} \end{cases}$$

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

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

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

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

We list some properties:

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

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

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

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

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

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

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

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

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

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

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

$F = \mathbb{Q}(\sqrt{d}\,)$, $d \neq 2,3,5$	$\mathrm{ord}(\tilde{u})$	$\mathcal{O}^\star$
$2\varepsilon \in F^{\times 2}$	$2,3,4$	$C_2, C_3, C_4, D_2, D_3, D_4, A_4, S_4$
$3\varepsilon \in F^{\times 2}$	$2,3,6$	$C_2, C_3, C_6, D_2, D_3, D_6, A_4$
$\{2\varepsilon, 3\varepsilon\} \cap F^{\times 2} = \emptyset$	$2,3$	C_2, C_3, D_2, D_3, A_4

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

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

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

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

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

$\mathrm{ord}(\tilde{u})$	Conditions	$P_{\tilde{u}}(x) \in F[x]$
2	$\mathrm{Nr}(u) = 1$	$x^2 + 1$
	$\mathrm{N}_{F/\mathbb{Q}}(\varepsilon) = 1, \quad \mathrm{Nr}(u) = \varepsilon$	$x^2 + \varepsilon$
3		$x^2 \pm x + 1$
4	$\mathrm{N}_{F/\mathbb{Q}}(\varepsilon) = 1, \quad 2\varepsilon \in F^{\times 2}$	$x^2 \pm 2\vartheta x + \varepsilon$
6	$\mathrm{N}_{F/\mathbb{Q}}(\varepsilon) = 1, \quad 3\varepsilon \in F^{\times 2}$	$x^2 \pm 3\varsigma x + \varepsilon$

Remark that

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

6. Minimal G-orders

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

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

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

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

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

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

Below we list the conditions on F and B in order for a minimal G-order to occur and explicit representatives of minimal G-orders.

G	ε	B	minimal G-order $\mathcal{O}$	$\mathfrak{d}(\mathcal{O})$
D_2^{I}		$\left(\frac{-1,-1}{F}\right)$	$\mathcal{O}_F[i,j]$	$4\mathcal{O}_F$
D_2^{II}	$\mathrm{N}_{F/\mathbb{Q}}(\varepsilon)=1$	$\left(\frac{-1,-\varepsilon}{F}\right)$	$\mathcal{O}_F[i,j]$	$4\mathcal{O}_F$
D_3^{I}		$\left(\frac{-1,-3}{F}\right)$	$\mathcal{O}_F[i,(1+j)/2]$	$3\mathcal{O}_F$
D_3^{II}	$\mathrm{N}_{F/\mathbb{Q}}(\varepsilon)=1$	$\left(\frac{-\varepsilon,-3}{F}\right)$	$\mathcal{O}_F[i,(1+j)/2]$	$3\mathcal{O}_F$
D_4	$2\varepsilon\in F^{\times 2}$	$\left(\frac{-1,-1}{F}\right)$	$\mathcal{O}_F+\mathcal{O}_Fi+\mathcal{O}_F\sqrt{\varepsilon j}+\mathcal{O}_Fi\sqrt{\varepsilon j}$	$2\mathcal{O}_F$
D_6	$3\varepsilon\in F^{\times 2}$	$\left(\frac{-1,-3}{F}\right)$	$\mathcal{O}_{F(j)}+i\mathcal{O}_{F(j)}$	$\mathcal{O}_F$
A_4		$\left(\frac{-1,-1}{F}\right)$	$\mathcal{O}_F+\mathcal{O}_Fi+\mathcal{O}_Fj+\mathcal{O}_F\xi$	$2\mathcal{O}_F$
S_4	$2\varepsilon\in F^{\times 2}$	$\left(\frac{-1,-1}{F}\right)$	$\mathcal{O}_F+\mathcal{O}_F\sqrt{\varepsilon i}+\mathcal{O}_F\sqrt{\varepsilon j}+\mathcal{O}_F\xi$	$\mathcal{O}_F$

Here $\xi=(1+i+j+k)/2\in\left(\frac{-1,-1}{F}\right)$ and $\mathfrak{d}(\mathcal{O})$ is the (reduced) discriminant of $\mathcal{O}$.

From this table, we can draw a few conclusions:

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

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

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

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

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

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

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

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

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

$$B\in\left\{\left(\frac{-1,-1}{F}\right),\left(\frac{-1,-3}{F}\right)\right\}\quad \textit{if}\ \mathrm{N}_{F/\mathbb{Q}}(\varepsilon)=-1,\ \textit{or}$$

$$B\in\left\{\left(\frac{-1,-1}{F}\right),\left(\frac{-1,-3}{F}\right),\left(\frac{-\varepsilon,-1}{F}\right),\left(\frac{-\varepsilon,-3}{F}\right)\right\}\quad \textit{if}\ \mathrm{N}_{F/\mathbb{Q}}(\varepsilon)=1.$$

Proposition 12 and (2.1) may be generalized to arbitrary totally real fields.

Proposition 13. *Let F be a totally real field. Then there exists a finite set $\mathscr{B}_F$ of totally definite quaternion F-algebras depending only on F such that for any totally definite F-algebra $B\notin\mathscr{B}_F$, the reduced unit group of any $\mathcal{O}_F$-order in B is cyclic.*

7. Computation of $t(G)$ for non-cyclic groups G

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

Proposition 14. *We have*

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

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

$$t(A_4)=\begin{cases}1 & \text{if } B=\left(\frac{-1,-1}{F}\right) \text{ and } 2\varepsilon\notin F^{\times 2};\\ 0 & \text{otherwise;}\end{cases} \tag{7.3}$$

Note that $2\varepsilon\in(F^\times)^2$ implies that 2 is ramified in F. Thus, $t(D_4)=t(S_4)=0$ if 2 is unramified in F. Similarly, if $3\nmid d$, then $3\varepsilon\notin(F^\times)^2$, and hence $t(D_6)=0$.

Proposition 15. *We have*

$$t(D_2^{\mathrm{I}})=\begin{cases}1 & \text{if } B=\left(\frac{-1,-1}{F}\right),\ \left(\frac{F}{2}\right)=0 \text{ and } 2\varepsilon\notin F^{\times 2};\\ 0 & \text{otherwise.}\end{cases} \tag{7.4}$$

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

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

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

We have the following table for $\aleph(\mathscr{O}_2^{\mathrm{II}})$ and $\beth(\mathscr{O}_2^{\mathrm{II}})$.

$d\geq 7$	$\varepsilon=a+b\sqrt{d}$	$\aleph(\mathscr{O}_2^{\mathrm{II}})$	$\beth(\mathscr{O}_2^{\mathrm{II}})$
$d\equiv 1\pmod 8$	$a\equiv 1\pmod 4$	1	1
$d\equiv 1\pmod 8$	$a\equiv 3\pmod 4$	4	2
$d\equiv 5\pmod 8$		2	1
$d\equiv 3\pmod 4$	a is even	2	2
otherwise		4	3

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

$$t(D_2^{\mathrm{II}})+t(D_4)+t(S_4)+t(D_6)=\beth(\mathscr{O}_2^{\mathrm{II}}). \tag{7.5}$$

In most cases, formula (7.5) can be simplified further. The fact that 2ε and 3ε cannot simutaneously be perfect squares in F for $d\geq 7$ implies that $t(D_6)(t(S_4)+t(D_4))=0$. For example, if $d\equiv 1\pmod 4$, then $2\varepsilon\notin F^{\times 2}$ and hence $t(S_4)=$

$t(D_4) = 0$. So in this case $t(D_2^{\mathrm{II}}) + t(D_6) = \beth(\mathscr{O}_2^{\mathrm{II}})$. If further $d \equiv 1 \pmod 8$ and $a \equiv 1 \pmod 4$, then $t(D_2) = t(D_2^{\mathrm{II}}) = 1$.

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

We first consider the case $B = \left(\frac{-1,-3}{F}\right)$, which is necessary for $t(D_3^{\mathrm{I}}) \neq 0$. One can show that the minimal S_4-order $\mathbb{O}_{24}$ in the table of Section 6 does not contain any minimal D_3^{I}-order and the minimal D_6-order there contains the minimal D_3^{I}-order $\mathscr{O}_3^{\mathrm{I}}$.

Note that $\mathscr{O}_3^{\mathrm{I}} \simeq O_{3,\infty} \otimes O_F$, where $O_{3,\infty}$ is the unique maximal order up to conjugation of the quaternion $\mathbb{Q}$-algebra $B_{3,\infty} = \left(\frac{-1,-3}{\mathbb{Q}}\right)$. If 3 splits in F, then B is ramified at two places of F over 3 and $\mathscr{O}_3^{\mathrm{I}}$ is maximal. If 3 is ramified in F, then one can show that there is a unique maximal order containing $\mathscr{O}_3^{\mathrm{I}}$. If 3 is inert in F, then $\mathscr{O}_3^{\mathrm{I}}$ is an Eichler order of prime level $3O_F$ and the two maximal over-orders are mutually conjugate. Therefore, we always have $\beth(\mathscr{O}_3^{\mathrm{I}}) = 1$.

Proposition 18. *There is only one maximal order up to conjugation containing $\mathscr{O}_3^{\mathrm{I}}$ and $t(D_3^{\mathrm{I}}) + t(D_6) = 1$. Thus,*

$$t(D_3^{\mathrm{I}}) = \begin{cases} 1 & \text{if } B = \left(\frac{-1,-3}{F}\right) \text{ and } 3\varepsilon \notin F^{\times 2}; \\ 0 & \text{otherwise.} \end{cases} \tag{7.6}$$

Lastly, suppose that $\mathrm{N}_{F/\mathbb{Q}}(\varepsilon) = 1$. Let $B := \left(\frac{-\varepsilon,-3}{F}\right)$ and $\mathscr{O}_3^{\mathrm{II}}$ be the minimal D_3^{II}-order in the table of Section 6. Write $\varepsilon = \frac{a+b\sqrt{d}}{2}$ with $a \equiv b \pmod 2$. If $d \equiv 1 \pmod 3$ and $\mathrm{N}_{F/\mathbb{Q}}(\varepsilon) = 1$, then $3 \mid b$. This is immediately seen by taking both sides of $a^2 - b^2 d = 4$ modulo 3. We have $\varepsilon \equiv \pm 1 \pmod{3O_F}$ in this case. Note that $\left(\frac{F}{3}\right) = 0, 1, -1$ according to $d \equiv 0, 1, 2 \pmod 3$.

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

We list $\aleph(\mathscr{O}_3^{\mathrm{II}})$ and $\beth(\mathscr{O}_3^{\mathrm{II}})$ in the following table.

$d \geq 7$	ε	$\aleph(\mathscr{O}_3^{\mathrm{II}})$	$\beth(\mathscr{O}_3^{\mathrm{II}})$
$d \equiv 0 \pmod 3$	$\varepsilon \equiv 1 \pmod{\mathfrak{p}}$	1	1
	$\varepsilon \equiv -1 \pmod{\mathfrak{p}}$	3	2
$d \equiv 1 \pmod 3$	$\varepsilon \equiv 1 \pmod{3O_F}$	1	1
	$\varepsilon \equiv -1 \pmod{3O_F}$	4	2
$d \equiv 2 \pmod 3$		2	1

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

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

$$t(D_3^{\mathrm{II}}) + t(S_4) + t(D_6) = \beth(\mathscr{O}_3^{\mathrm{II}}). \tag{7.7}$$

As mentioned before, $t(D_6) = 0$ in (7.7) when $d \not\equiv 0 \pmod 3$. If further $d \equiv 1 \pmod 3$ and $\varepsilon \equiv 1 \pmod{3O_F}$, then $\mathscr{O}_3^{\mathrm{II}}$ is maximal in B and $t(D_3^{\mathrm{II}}) = 1$.

8. Optimal embeddings and class-type number relations

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

Let F be a number field with the ring of integers O_F. Let B be a division quaternion F-algebra, and $\mathrm{Tp}(B)$ the set of types of maximal orders in B. For any maximal O_F-order $\mathbb{O}$ in B, we write $\mathrm{Cl}(\mathbb{O})$ for the set of right ideal classes of $\mathbb{O}$, and $\mathcal{N}(\mathbb{O})$ for the normalizer of $\mathbb{O}$. By [10, Theorem 22.10], the set of nonzero two-sided fractional ideals of $\mathbb{O}$ forms a commutative multiplicative group $\mathscr{I}(\mathbb{O})$, which is a free abelian group generated by the prime ideals of $\mathbb{O}$. Let $\mathscr{P}(\mathbb{O}) \subseteq \mathscr{I}(\mathbb{O})$ be the subgroup of principal two-sided fractional ideals of $\mathbb{O}$, and $\mathscr{P}(O_F)$ the group of principal fractional O_F-ideals, identified with a subgroup of $\mathscr{P}(\mathbb{O})$ via $xO_F \mapsto x\mathbb{O}, \forall x \in F^\times$.

Fix a maximal order $\mathbb{O}_0$ in B. There is a surjective map of finite sets

$$(8.1) \qquad \Upsilon : \mathrm{Cl}(\mathbb{O}_0) \to \mathrm{Tp}(B), \qquad [I] \mapsto [\![\mathcal{O}_l(I)]\!] := D^\times\text{-conjugacy class of } \mathcal{O}_l(I).$$

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

$$(8.2) \qquad \Upsilon^{-1}([\![\mathbb{O}]\!]) \longleftrightarrow \mathscr{I}(\mathbb{O})/\mathscr{P}(\mathbb{O}).$$

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

$$(8.3) \qquad 1 \to \mathcal{N}(\mathbb{O})/(F^\times\mathbb{O}^\times) \to \mathrm{Pic}(\mathbb{O}) \to \mathscr{I}(\mathbb{O})/\mathscr{P}(\mathbb{O}) \to 1.$$

Here $\mathrm{Pic}(\mathbb{O})$ denotes the Picard group $\mathscr{I}(\mathbb{O})/\mathscr{P}(O_F)$, whose cardinality can be calculated using the short exact sequence

$$(8.4) \qquad 1 \to \mathrm{Cl}(O_F) \to \mathrm{Pic}(\mathbb{O}) \to \prod_{\mathfrak{p} \mid \mathfrak{d}(B)} (\mathbb{Z}/2\mathbb{Z}) \to 0.$$

It follows that

$$(8.5) \qquad |\Upsilon^{-1}([\![\mathbb{O}]\!])| = \frac{2^{\omega(B)}h(F)}{|\mathcal{N}(\mathbb{O})/(F^\times\mathbb{O}^\times)|},$$

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

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

$$(8.6) \qquad h(G) = \sum_{i=1}^{t(G)} \frac{2^{\omega(B)}h(F)}{|\mathcal{N}(\mathbb{O}_i)/(F^\times\mathbb{O}_i^\times)|}.$$

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

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

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

$$\sum_{i=1}^{h} m(R, \mathcal{O}_i, \mathcal{O}_i^{\times}) = h(R) \prod_{\mathfrak{p}} m_{\mathfrak{p}}(R), \tag{8.7}$$

where the product on the right hand side runs over all nonzero prime ideals of O_F. A priori, Theorem 5.11 of [12] is stated for Eichler orders, but it applies in much more generality. See [14, Lemma 3.2] and [15, Lemma 3.2.1]. When $\mathcal{O} = \mathbb{O}$ is maximal, we have

$$m_{\mathfrak{p}}(R) := \begin{cases} 1 - \left(\frac{R}{\mathfrak{p}}\right) & \text{if } \mathfrak{p} | \mathfrak{d}(B), \\ 1 & \text{otherwise}, \end{cases} \tag{8.8}$$

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

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

$$\mathrm{Tp}^{\circ}(B) := \{\llbracket \mathbb{O} \rrbracket \in \mathrm{Tp}(B) \mid \mathbb{O}^{\star} \text{ is cyclic}\}, \quad \text{and} \quad \mathrm{Tp}^{\natural}(B) := \mathrm{Tp}(B) - \mathrm{Tp}^{\circ}(B).$$

If $\llbracket \mathbb{O}_i \rrbracket \in \mathrm{Tp}^{\circ}(B)$, then $\mathbb{O}_i^{\star} \simeq C_n$ if and only if $\mathrm{Emb}(R, \mathbb{O}_i) \neq \emptyset$ for some $R \in \mathscr{R}_n$. When the latter condition holds, such an order R is uniquely determined, and $m(R, \mathbb{O}_i, \mathbb{O}_i^{\times}) = 2$. For each fixed $R \in \mathscr{R}_n$, let

$$h(C_n, R) = h(B, C_n, R) := \#\{[I] \in \mathrm{Cl}(\mathbb{O}_0) \mid \mathcal{O}_l(I)^{\star} \simeq C_n, \text{ and } \mathrm{Emb}(R, \mathcal{O}_l(I)) \neq \emptyset\}.$$

Then we have

$$h(C_n) = \sum_{R \in \mathscr{R}_n} h(C_n, R). \tag{8.9}$$

Combining (8.6) and (8.7), we obtain

$$2^{\omega(B)} h(F) \sum_{\llbracket \mathbb{O} \rrbracket \in \mathrm{Tp}^{\natural}(B)} \frac{m(R, \mathbb{O}, \mathbb{O}^{\times})}{|\mathcal{N}(\mathbb{O})/(F^{\times}\mathbb{O}^{\times})|} + 2h(C_n, R) = h(R) \prod_{\mathfrak{p}} m_{\mathfrak{p}}(R). \tag{8.10}$$

It is a calculation intensive process to list $\mathcal{N}(\mathbb{O})$ for each $\llbracket \mathbb{O} \rrbracket \in \mathrm{Tp}^{\natural}(B)$. Once this is completed, it then reduces to compute the numbers of global optimal embeddings $m(R, \mathbb{O}, \mathbb{O}^{\times})$ for all $R \in \mathscr{R}_n$ and $\llbracket \mathbb{O} \rrbracket \in \mathrm{Tp}^{\natural}(B)$, which is comparably much more managable.

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

REFERENCES

[1] Juliusz Brzezinski. Definite quaternion orders of class number one. *J. Théor. Nombres Bordeaux*, 7(1):93–96, 1995. Les Dix-huitièmes Journées Arithmétiques (Bordeaux, 1993).

[2] 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.

[3] P. E. Conner and J. Hurrelbrink. *Class number parity*, volume 8 of *Series in Pure Mathematics*. World Scientific Publishing Co., Singapore, 1988.

[4] M. Eichler. Über die Idealklassenzahl total definiter Quaternionenalgebren. *Math. Z.*, 43(1):102–109, 1938.

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

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

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

[8] Qun Li, Jiangwei Xue, and Chia-Fu Yu. Reduced unit groups of maximal orders in certain totally definite quaternion algebras. In preparation.

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

[10] 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.

[11] Marie-France Vignéras. Nombre de classes d'un ordre d'Eichler et valeur au point −1 de la fonction zêta d'un corps quadratique réel. *Enseignement Math. (2)*, 21(1):69–105, 1975.

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

[13] William C. Waterhouse. Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup. (4)*, 2:521–560, 1969.

[14] 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.

[15] Jiangwei Xue, Tse-Chung Yang, and Chia-Fu Yu. Supersingular abelian surfaces and Eichler class number formula. *ArXiv e-prints*, April 2014, `arXiv:1404.2978`.

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

[17] C.-F. Yu. A note on supersingular abelian varieties. *ArXiv e-prints*, December 2014, `arXiv:1412.7107`.

(LI) SCHOOL OF MATHEMATICS AND STATISTICS, WUHAN UNIVERSITY, LUOJIASHAN, WUHAN, HUBEI, 430072, P.R. CHINA.
E-mail address: qun_l@whu.edu.cn

(XUE) COLLABORATIVE INNOVATION CENTRE OF MATHEMATICS, SCHOOL OF MATHEMATICS AND STATISTICS, WUHAN UNIVERSITY, LUOJIASHAN, WUHAN, HUBEI, 430072, P.R. CHINA.

(XUE) HUBEI KEY LABORATORY OF COMPUTATIONAL SCIENCE (WUHAN UNIVERSITY), WUHAN, HUBEI, 430072, P.R. CHINA.
E-mail address: xue_j@whu.edu.cn

(YU) INSTITUTE OF MATHEMATICS, ACADEMIA SINICA, ASTRONOMY-MATHEMATICS BUILDING, NO. 1, SEC. 4, ROOSEVELT ROAD, TAIPEI 10617, TAIWAN.
E-mail address: chiafu@math.sinica.edu.tw

(YU) NATIONAL CENTER FOR THEORETICAL SCIENCES, ASTRONOMY-MATHEMATICS BUILDING, NO. 1, SEC. 4, ROOSEVELT ROAD, TAIPEI 10617, TAIWAN.
E-mail address: chiafu@math.sinica.edu.tw