Jordan constants of quaternion algebras over number fields and simple abelian surfaces over fields of positive characteristic

WonTae Hwang

Department of Mathematics, and Institute of Pure and Applied Mathematics at Jeonbuk National University, Jeonju, South Korea

Correspondence
WonTae Hwang, Department of Mathematics, and Institute of Pure and Applied Mathematics, Jeonbuk National University, 567 Baekje-daero, Deokjin-gu, Jeonju-si, Jeollabuk-do, 54896, South Korea. Email: hwangwon@jbnu.ac.kr

Funding information
Korea Institute for Advanced Study, Grant/Award Number: Individual Grant (MG069901)

Abstract
We compute and provide a detailed description on the Jordan constants of the multiplicative subgroup of quaternion algebras over number fields of small degree. As an application, we determine the Jordan constants of the multiplicative subgroup of the endomorphism algebras of simple abelian surfaces over fields of positive characteristic.

KEYWORDS
abelian surfaces over fields of positive characteristic, Jordan groups and Jordan constants, quaternion algebras over number fields

MSC (2020)
11G10, 11R52, 14G17, 14K02, 20E07

1 INTRODUCTION

The notion of Jordan group, which is named after the French mathematician Camille Jordan, was introduced by Vladimir Popov in [22]. A group \( G \) is called a Jordan group if there exists an integer \( d > 0 \) such that every finite subgroup \( H \) of \( G \) contains a normal abelian subgroup whose index in \( H \) is at most \( d \). The minimal such \( d \) is called the Jordan constant of \( G \) and is denoted by \( J_G \). In view of the classical result of Jordan, saying that the general linear group \( GL_n(k) \) for an integer \( n \geq 1 \) and an algebraically closed field \( k \) of characteristic zero is a Jordan group, we can deduce that every affine algebraic group is also a Jordan group. Other interesting examples arise in connection with algebraic geometry. Let \( X \) be an irreducible algebraic variety over an algebraically closed field \( k \) of characteristic zero, and let \( G = \text{Bir}(X) \), the group of birational automorphisms of \( X \). We might ask whether \( G \) is a Jordan group or not. If \( X \) is a smooth projective rational variety of dimension \( n \), then \( G = \text{Cr}_n(k) \), the Cremona group of degree \( n \) over \( k \), and it was known that \( \text{Cr}_n(k) \) is a Jordan group for \( n = 1, n = 2 \) (see [27, Theorem 5.3]), and \( n = 3 \) (see [24, Corollary 1.9]). Yuri Prokhorov and Constantin Shramov [24, 25] showed (modulo the Borisov–Alexeev–Borisov conjecture, see [24, Conjecture 1.7], recently proved by Caucher Birkar [5]) that \( \text{Cr}_n \) is indeed a Jordan group for arbitrary \( n > 3 \), and computed an upper bound for the Jordan constants of the Cremona groups of rank 2 and 3. The exact value of the Jordan constant of \( \text{Cr}_3(k) \) was found by Egor Yasinsky [29]. Furthermore, Sheng Meng and De-Qi Zhang [18] proved that the full automorphism group of any projective variety over \( k \) is a Jordan group, using algebraic group theoretic arguments. On the other hand, if \( \dim X \leq 2 \), then it is known [22, Theorem 2.32] that the group \( \text{Bir}(X) \) is a Jordan group if and only if \( X \) is not birationally isomorphic to \( \mathbb{P}_k^1 \times E \) where \( E \) is an elliptic curve over \( k \). In addition, we have a similar but slightly more complicated result for the case of \( X \) being a threefold [26, Theorem 1.8].

On the other hand, to the author’s best knowledge, not much is known in the case when the base field \( k \) is not algebraically closed or the characteristic of the base field \( k \) is positive. The primary goal of this paper is to consider those two
cases in the context of $X$ being a simple abelian surface over a field of positive characteristic. To this aim, we first recall that the author [12] gave a classification of finite groups that can be realized as the full automorphism group of arbitrary polarized abelian surfaces over finite fields, and he [13] also classified completely all the possible automorphism groups of simple polarized abelian varieties of odd prime dimension over finite fields. These results can be used to answer some special cases of the following problem.

**Problem 1.1.** Let $X$ be a (unpolarized) simple abelian variety over a field $k$ with $\text{char}(k) = p > 0$.

1. Is the automorphism group $\text{Aut}_k(X)$ of $X$ over $k$ a Jordan group?
2. If the answer for (1) is yes, then what is $J_{\text{Aut}_k(X)}$?

More precisely, in this paper, we aim to answer Problem 1.1 mainly for the case when $X$ is a simple abelian surface over a field $k$, which is either a finite field or an algebraically closed field of positive characteristic. To achieve the goal, in view of Lemma 2.3 below, we first consider the case of $G$ being the multiplicative subgroup of a quaternion division algebra over a number field of degree $\leq 2$ to prove that $G$ is a Jordan group, and we also explicitly compute the Jordan constant $J_G$ of $G$. This gives another context that connects the theory of Jordan groups, algebraic geometry, and algebraic number theory. In this aspect, one of our main results is the following theorem.

**Theorem 1.2.** Let $D$ be a quaternion division algebra over $\mathbb{Q}$ (resp. over a quadratic number field). Then $D^\times$ is a Jordan group and $J_{D^\times} \in \{1, 2, 12\}$ (resp. $J_{D^\times} \in \{1, 2, 12, 24, 60\}$). Furthermore, we have an explicit description on the relation between $D$ and $J_{D^\times}$ in terms of the center of $D$ and the ramification set of $D$.

The proof of Theorem 1.2 combines the theory of quaternion algebras over number fields with the ramification theory of number fields. For more details, see Theorems 3.9 and 3.15 below.

As an application of the above result, we compute the Jordan constants of the multiplicative subgroup of the endomorphism algebras of simple abelian surfaces over fields of positive characteristic. To this aim, we recall: let $X$ be an abelian surface over a field $k$. We denote the endomorphism ring of $X$ over $k$ by $\text{End}_k(X)$. It is a free $\mathbb{Z}$-module of rank $\leq 16$. Because it is usually harder to deal with the ring $\text{End}_k(X)$, we also consider $\text{End}^0_k(X) = \text{End}_k(X) \otimes_{\mathbb{Z}} \mathbb{Q}$. This $\mathbb{Q}$-algebra $\text{End}^0_k(X)$ is called the endomorphism algebra of $X$ over $k$. Then $\text{End}^0_k(X)$ is a finite dimensional semisimple algebra over $\mathbb{Q}$ with $\dim_{\mathbb{Q}} \text{End}^0_k(X) \leq 16$. Moreover, if $X$ is $k$-simple, then $\text{End}^0_k(X)$ is a division algebra over $\mathbb{Q}$. Another main result of this paper is summarized as follows.

**Theorem 1.3.** Let $n$ be an integer. Then we have:

(a) There exists a simple abelian surface $X$ over a finite field $k = \mathbb{F}_q$ with $q = p^a$ for some prime $p > 0$ and an integer $a \geq 1$ such that $J_{D^\times} = n$, where $D = \text{End}^0_k(X)$ if and only if $n \in \{1, 2, 12, 24, 60\}$.
(b) There exists a simple abelian surface $X$ over some algebraically closed field $k$ of characteristic $p > 0$ such that $J_{D^\times} = n$, where $D = \text{End}^0_k(X)$ if and only if $n = 1$.

The proof of Theorem 1.3 requires concrete knowledge of the theory of abelian varieties over fields of positive characteristic, together with Theorem 1.2. More precisely, the proof of one direction of part (a) is obtained by constructing desired simple abelian surfaces concretely, while the proof of the same direction of part (b) is achieved by adopting a slightly more abstract argument.

For more details, see Theorems 3.18, 3.19, and 4.2 below.

Finally, the following observation is related to Theorem 1.3-(a) above.

**Theorem 1.4.** Let $S$ be the set of pairs $(n, p)$ of an integer $n \geq 1$ and a prime $p$ with the property that there is a simple abelian surface $X$ over $k = \mathbb{F}_q$ with $q = p^a$ ($a \geq 1$) and $J_{D^\times} = n$, where $D = \text{End}^0_k(X)$. If we choose an element $(n, p)$ randomly from $S$, then it is most probable that $n = 12$ in the sense of the prime number theorem for arithmetic progression.

This can be derived from Corollary 3.17. For a slightly more detailed statement, see Remark 3.20 below.
This paper is organized as follows: In Section 2, we recall some of the facts in the theory of Jordan groups and the general theory of abelian varieties over a field. In Section 3, we obtain the desired results (Theorems 1.2 and 1.3-(a) above) using the facts that were introduced in the previous sections. Finally, in Section 4, we prove Theorem 1.3-(b) above.

In the sequel, let $k$ denote an algebraic closure of a field $k$. Also, for a prime $p \geq 3$ and an integer $n \geq 1$, we denote the cyclic group of order $n$ by $C_n$, and $\left( \frac{n}{p} \right)$ will denote the Legendre symbol. Finally, for a number field $K$ and a place $v$ of $K$, we let $K_v$ be the completion of $K$ with respect to $v$.

2 | PRELIMINARIES

In this section, we briefly review the theory of Jordan groups (§2.1), and then, we recall some facts about endomorphism algebras of simple abelian varieties (§2.2), the theorem of Tate (§2.3), and Honda–Tate theory (§2.4). Our main references are [10, 19], and [23].

2.1 | Jordan groups

In this section, we review some basic facts about Jordan groups, which is our main interest in this paper.

First of all, we note that if every finite subgroup of a group $G$ is abelian, then $G$ is a Jordan group and $J_G = 1$. The following example illustrates this observation.

Example 2.1. Let $k$ be an algebraically closed field of characteristic zero, and let $X \subseteq \mathbb{A}^4_k$ be the nonsingular hypersurface defined by the equation $x_1^2 x_2 + x_3^2 + x_4^4 + x_1 = 0$. Then in view of [23, §2.2.5], every finite subgroup of $\text{Aut}(X)$ is cyclic, and hence, we have $J_{\text{Aut}(X)} = 1$.

For our later use in Section 3 to compute the Jordan constants of certain infinite groups, we also record the following elementary, but useful result.

Lemma 2.2. Let $G$ be a Jordan group. Then every subgroup $H \leq G$ is a Jordan group and we have

$$J_G = \sup_{H \leq G} J_H$$

where the supremum is taken over all finite subgroups $H$ of $G$.

2.2 | Endomorphism algebras of simple abelian varieties over a finite field

In this section, we review some general facts about the endomorphism algebras of simple abelian varieties over a finite field.

Let $X$ be a simple abelian variety of dimension $g$ over a finite field $k$. Then $\text{End}_0^0(X)$ is a division algebra over $\mathbb{Q}$ with $2g \leq \dim_{\mathbb{Q}} \text{End}_0^0(X) < (2g)^2$ (see [10, Corollary 12.7] and Corollary 2.5-(c),(d) below). Before giving our first result, we also recall Albert’s classification. We choose a polarization $\lambda : X \to \hat{X}$ where $\hat{X}$ denotes the dual abelian variety of $X$. Using the polarization $\lambda$, we can define an involution, called the Rosati involution, $^\vee$ on $\text{End}_0^0(X)$. (For a more detailed discussion about the Rosati involution, see [19, §20].) In this way, to the pair $(X, \lambda)$ we associate the pair $(D, ^\vee)$ with $D = \text{End}_0^0(X)$ and $^\vee$, the Rosati involution on $D$. Let $K$ be the center of $D$ so that $D$ is a central simple $K$-algebra, and let $K_0 = \{ x \in K \mid x^\vee = x \}$ be the subfield of symmetric elements in $K$. By a theorem of Albert (see [1] and [2], or [19, Application I in §21]), $D$ (together with $^\vee$) is of one of the following four types:

(i) Type I: $K_0 = K = D$ is a totally real field.
(ii) Type II: $K_0 = K$ is a totally real field, and $D$ is a quaternion algebra over $K$ with $D \otimes_{K, \sigma} \mathbb{R} \cong M_2(\mathbb{R})$ for every embedding $\sigma : K \hookrightarrow \mathbb{R}$ (where $M_2(\mathbb{R})$ is the ring of $2 \times 2$ matrices over $\mathbb{R}$).
TABLE 1 Numerical restrictions on endomorphism algebras

| Type   | char(k) = 0 | char(k) = p > 0 |
|--------|-------------|----------------|
| Type I | e|g | e|g |
| Type II| 2e|g | 2e|g |
| Type III| 2e|g | e|g |
| Type IV| e|0d|2|g | e|0d|g |

(iii) Type III: $K_0 = K$ is a totally real field, and $D$ is a quaternion algebra over $K$ with $D \otimes_K \mathbb{R} \cong \mathbb{H}$ for every embedding $\sigma : K \to \mathbb{R}$ (where $\mathbb{H}$ is the Hamiltonian quaternion algebra over $\mathbb{R}$).

(iv) Type IV: $K_0$ is a totally real field, $K$ is a totally imaginary quadratic field extension of $K_0$, and $D$ is a central simple algebra over $K$.

Keeping the notations as above, we let

$$e_0 = \left[ K_0 : \mathbb{Q} \right], \quad e = \left[ K : \mathbb{Q} \right], \quad \text{and} \quad d = \left[ D : K \right]^\frac{1}{2}.$$

As our last preliminary fact of this section, we note some numerical restrictions on those values $e_0, e,$ and $d$ in the next table, following [19, §21].

If $g = 2$ i.e. if $X$ is a simple abelian surface over $k$, then we readily have the following.

**Lemma 2.3.** Let $X$ be a simple abelian surface over a finite field $k = \mathbb{F}_{q}$, and let $\lambda : X \to \hat{X}$ be a polarization. Then $D = \text{End}_k^0(X)$ (together with the Rosati involution $\vee$ corresponding to $\lambda$) is of one of the following three types:

1. $D$ is a totally definite quaternion algebra over either $\mathbb{Q}$ or a real quadratic field;
2. $D$ is a CM-field of degree 4;
3. $D$ is a quaternion division algebra over an imaginary quadratic field.

**Proof.** First, we recall that $X$ is of CM-type (see Corollary 2.5-(c) below), and hence, either $D$ is of Type III or of Type IV in Albert’s classification. We consider each type one by one.

(i) Suppose that $D$ is of Type III. By Table 1, either $e = 1$ or $e = 2$, and hence, we get (1).

(ii) Suppose that $D$ is of Type IV. Then by the fact that $4 \leq \dim_{\mathbb{Q}} D < 16$ and Table 1, we have that the pair $(e_0, d)$ is contained in the set $\{(2,1), (2,1), (1,2)\}$. If $(e_0, d) = (2,1)$, then we get (2). Finally, if $(e_0, d) = (1,2)$, then we get (3).

This completes the proof. \(\square\)

### 2.3 The theorem of Tate

In this section, we recall an important theorem of Tate, and give some interesting consequences of it.

Let $k$ be a field and let $l$ be a prime number with $l \neq \text{char}(k)$. If $X$ is an abelian variety of dimension $g$ over $k$, then we can introduce the Tate $l$-module $T_lX$ and the corresponding $\mathbb{Q}_l$-vector space $V_lX = T_lX \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$. In light of [10, (10.3)], $T_lX$ is a free $\mathbb{Z}_l$-module of rank $2g$ and $V_lX$ is a $2g$-dimensional $\mathbb{Q}_l$-vector space. In [28], Tate showed the following important result for the case when $k$ is a finite field.

**Theorem 2.4.** Let $k$ be a finite field and let $\Gamma = \text{Gal}(\overline{k}/k)$. If $l$ is a prime number with $l \neq \text{char}(k)$, then we have:

(a) For any abelian variety $X$ over $k$, the representation

$$\rho_l = \rho_l^X : \Gamma \to \text{GL}(V_lX)$$

is semisimple.
(b) For any two abelian varieties $X$ and $Y$ over $k$, the map

$$\mathbb{Z}_l \otimes \mathbb{Z} \text{Hom}_k(X, Y) \to \text{Hom}_\Gamma(T_lX, T_lY)$$

is an isomorphism.

Now, we recall that an abelian variety $X$ over a (finite) field $k$ is called elementary if $X$ is $k$-isogenous to a power of a simple abelian variety over $k$. Then, as an interesting consequence of Theorem 2.4, we have the following fundamental result.

**Corollary 2.5** ([28, Theorem 2]). Let $X$ be an abelian variety of dimension $g$ over a finite field $k = \mathbb{F}_q$ ($q = p^a$). Then we have:

(a) The center of $\text{End}_k^0(X)$ is the subalgebra $\mathbb{Q}[\pi_X]$ where $\pi_X$ denotes the Frobenius endomorphism of $X$. In particular, $X$ is elementary if and only if $\mathbb{Q}(\pi_X) = \mathbb{Q}(\pi_X)$ is a field.

(b) Suppose that $X$ is elementary. Let $h = f_{\pi_X}^X$ be the minimal polynomial of $\pi_X$ over $\mathbb{Q}$, and let $f_X$ be the characteristic polynomial of $\pi_X$. Also, let $d = [\text{End}_k^0(X) : \mathbb{Q}(\pi_X)]^{\frac{1}{2}}$ and $e = [\mathbb{Q}(\pi_X) : \mathbb{Q}]$. Then $de = 2g$ and $f_X = h^d$.

(c) We have $2g \leq \dim_k \text{End}_k^0(X) \leq (2g)^2$ and $X$ is of CM-type.

(d) The following conditions are equivalent:

(d-1) $\dim_k \text{End}_k^0(X) = (2g)^2$;

(d-2) $\text{End}_k^0(X) \cong M_g(D_{p,\infty})$ where $D_{p,\infty}$ is the unique quaternion algebra over $\mathbb{Q}$ that is ramified at $p$ and $\infty$, and split at all other primes;

(d-3) $X$ is isogenous to $E^g$ for a supersingular elliptic curve $E$ over $k$ all of whose endomorphisms are defined over $k$.

For a precise description of the structure of the endomorphism algebra of a simple abelian variety $X$, viewed as a simple algebra over its center $\mathbb{Q}[\pi_X]$, we record the following useful result.

**Proposition 2.6** ([10, Corollary 16.30 and Corollary 16.32]). Let $X$ be a simple abelian variety over a finite field $k = \mathbb{F}_q$ ($q = p^a$). Let $K = \mathbb{Q}[\pi_X]$. Then we have:

(a) If $\nu$ is a place of $K$, then the local invariant of $\text{End}_k^0(X)$ in the Brauer group $\text{Br}(K)$ is given by

$$\text{inv}_\nu \left( \text{End}_k^0(X) \right) = \begin{cases} 0 & \text{if } \nu \text{ is a finite place not above } p; \\
\frac{\text{ord}_\nu(\pi_X)}{\text{ord}_\nu(q)} \cdot [K_\nu : \mathbb{Q}_p] & \text{if } \nu \text{ is a place above } p; \\
\frac{1}{2} & \text{if } \nu \text{ is a real place of } K; \\
0 & \text{if } \nu \text{ is a complex place of } K. \end{cases}$$

(b) If $d$ is the degree of the division algebra $D = \text{End}_k^0(X)$ over its center $K$ (so that $d = [D : K]^{\frac{1}{2}}$ and $f_X = (f_{\pi_X}^X)^d$), then $d$ is the least common denominator of the local invariants $\text{inv}_\nu(D)$.

### 2.4 Abelian varieties up to isogeny and Weil numbers: Honda–Tate theory

In this section, we recall an important theorem of Honda and Tate. Throughout this section, let $q = p^a$ for some prime $p$ and an integer $a \geq 1$. To achieve our goal, we first give the following definition.
Definition 2.7.

(a) A $q$-Weil number is an algebraic integer $\pi$ such that $|t(\pi)| = \sqrt{q}$ for all embeddings $t : \mathbb{Q}[\pi] \hookrightarrow \mathbb{C}$.
(b) Two $q$-Weil numbers $\pi$ and $\pi'$ are said to be conjugate if they have the same minimal polynomial over $\mathbb{Q}$, or equivalently, there is an isomorphism $\mathbb{Q}[\pi] \rightarrow \mathbb{Q}[\pi']$ sending $\pi$ to $\pi'$.

Regarding $q$-Weil numbers, we record the following facts.

Remark 2.8. Let $X$ and $Y$ be simple abelian varieties over a finite field $k = \mathbb{F}_q$. Then we have:

(i) The Frobenius endomorphism $\pi_X$ is a $q$-Weil number (see [10, (16.39)]).
(ii) $X$ and $Y$ are $k$-isogenous if and only if $\pi_X$ and $\pi_Y$ are conjugate (see [10, Lemma 16.40]).

Now, we introduce the main result of this section.

Theorem 2.9 ([11, Main Theorem] or [10, §16.5]). For every $q$-Weil number $\pi$, there exists a simple abelian variety $X$ over $\mathbb{F}_q$ such that $\pi_X$ is conjugate to $\pi$. Moreover, we have a bijection between the set of isogeny classes of simple abelian varieties over $\mathbb{F}_q$ and the set of conjugacy classes of $q$-Weil numbers given by $X \mapsto \pi_X$.

The inverse of the map $X \mapsto \pi_X$ associates to a $q$-Weil number $\pi$ a simple abelian variety $X$ over $\mathbb{F}_q$ such that $f_X$ is a power of the minimal polynomial $f_\mathbb{Q}^\pi$ of $\pi$ over $\mathbb{Q}$.

3 | MAIN RESULT

In this section, we give the main results of this paper.

3.1 | Quaternion algebras over number fields

In this section, we prove Theorem 1.2 above. Throughout this section, let $D$ be a quaternion division algebra over an algebraic number field $K$ with $[K : \mathbb{Q}] \leq 2$, unless otherwise specified. Then the multiplicative subgroup $D^\times$ of $D$ is infinite, containing $K^\times$. Let $\text{Ram}(D)$ be the set of all primes of $K$ at which $D$ is ramified. Then the following is fundamental.

Remark 3.1. Let $D$ and $D'$ be quaternion division algebras over an algebraic number field $K$ with $[K : \mathbb{Q}] \leq 2$. Then we have:

(i) The set $\text{Ram}(D)$ is finite and the cardinality of $\text{Ram}(D)$ is even and positive (see [16, Theorem 2.7.3]).
(ii) $D \cong D'$ if and only if $\text{Ram}(D) = \text{Ram}(D')$ (see [16, Theorem 2.7.5]).
(iii) $D \cong D'$ if and only if $D \otimes_K K_v \cong D' \otimes_K K_v$ for all places $v$ of $K$ (see the proof of [16, Theorem 2.7.5]).

Example 3.2. Let $p \geq 2$ be a prime. In the sequel, we let $D_{p,\infty}$ denote the unique quaternion division algebra over $\mathbb{Q}$ which is ramified precisely at the primes $p$ and $\infty$. In other words, we have $\text{Ram}(D_{p,\infty}) = \{p, \infty\}$. (The existence of such a quaternion division algebra $D_{p,\infty}$ is guaranteed by [16, Theorem 7.3.6-(3)].) In particular, if $p$ and $p'$ are two distinct rational primes, then $D_{p,\infty}$ is not isomorphic to $D_{p',\infty}$ by Remark 3.1-(ii).

We also record one useful fact which will be used later.

Proposition 3.3 ([3, Proposition 1.14]). Let $D$ be a quaternion algebra over a number field $K$, and let $L$ be a quadratic extension field of $K$. Then the following conditions are equivalent:

(a) $L$ splits $D$ i.e. $D \otimes_K L \cong M_2(L)$. (In particular, $D \otimes_K L$ is not a division algebra.)
(b) There exists a $K$-embedding of $L$ into $D$.
Every place $\nu$ of $K$ at which $D$ is ramified does not split completely in $L$.

Now, we consider the case when $K = \mathbb{Q}$, in more details.

**Lemma 3.4.** Let $D$ be a quaternion division algebra over $\mathbb{Q}$. Then the group $D^\times$ is Jordan, and we have $J_{D^\times} \leq 60$.

**Proof.** Since $D \otimes_{\mathbb{Q}} \mathbb{C} \cong M_2(\mathbb{C})$, it follows from [23, Theorems 1 and 3-(1)] that $D^\times$ is Jordan and $J_{D^\times} \leq J_{GL_2(\mathbb{C})} = 60$. □

Next, we look into the case when $[K : \mathbb{Q}] = 2$, distinguishing between real and imaginary quadratic fields.

**Lemma 3.5.** Let $D$ be a quaternion division algebra over a real quadratic field $K$. Then the group $D^\times$ is Jordan, and we have $J_{D^\times} \leq 3600$.

**Proof.** Note that if $D$ is totally definite (resp. indefinite), then we have $D \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{H} \oplus \mathbb{H}$ (resp. $D \otimes_{\mathbb{Q}} \mathbb{R} \cong M_2(\mathbb{R}) \oplus M_2(\mathbb{R})$) so that $D \otimes_{\mathbb{Q}} \mathbb{C} \cong M_2(\mathbb{C}) \oplus M_2(\mathbb{C})$ in both cases. Then since $D^\times \leq GL_2(\mathbb{C}) \times GL_2(\mathbb{C})$, it follows from [23, Theorems 1 and 3-(1),(2)] that $D^\times$ is Jordan and $J_{D^\times} \leq J_{GL_2(\mathbb{C})}^2 = 3600$. □

**Lemma 3.6.** Let $D$ be a quaternion division algebra over an imaginary quadratic field $K$. Then the group $D^\times$ is Jordan, and we have $J_{D^\times} \leq 60$.

**Proof.** Note that we have $D \otimes_{\mathbb{Q}} \mathbb{R} \cong M_2(\mathbb{C})$, and then, since $D^\times \leq GL_2(\mathbb{C})$, it follows from [23, Theorems 1 and 3-(1)] that $D^\times$ is Jordan and $J_{D^\times} \leq J_{GL_2(\mathbb{C})} = 60$. □

Now, we would like to describe the exact value of $J_{D^\times}$, and see that all the upper bounds in Lemmas 3.4, 3.5, and 3.6 are not sharp. To this aim, we first introduce two lemmas.

**Lemma 3.7.** For any integer $n \geq 2$, we have

$$J_{\text{Dic}_{4n}} = 2$$

where $\text{Dic}_{4n}$ denotes the dicyclic group of order $4n$.

**Proof.** Let $G = \text{Dic}_{4n}$ ($n \geq 2$) and $H$ a subgroup of $G$. Note that $G$ admits a 2-dimensional faithful irreducible symplectic representation (see [6]), and hence, $H$ admits a faithful symplectic representation (which is induced from that of $G$). If this representation is irreducible, then $H$ must be a dicyclic group, too. If it is reducible, then $H$ must be cyclic (so that it does not contribute to the Jordan constant of $G$).

Now, since $G$ contains a $C_{2n}$ as an abelian normal subgroup, we have $J_G \geq [G : C_{2n}] = 2$. If $J_G > 2$, then by the minimality of $J_G$, it follows that there is a subgroup $H$ of $G$ such that $H$ contains no abelian normal subgroups of index $\leq 2$. But then, since $H$ is either a dicyclic group or a cyclic group by the above observation, this is a contradiction. Hence we can see that $J_G = 2$, as desired.

This completes the proof. □

**Lemma 3.8.** Let $\mathfrak{T}^*$ (resp. $\mathfrak{O}^*$, resp. $\mathfrak{I}^*$) denote the binary tetrahedral (resp. octahedral, resp. icosahedral) group. Then, we have

$$J_G = \begin{cases} 12 & \text{if } G = \mathfrak{T}^*; \\ 24 & \text{if } G = \mathfrak{O}^*; \\ 60 & \text{if } G = \mathfrak{I}^*. \end{cases}$$

**Proof.** Let $G = \mathfrak{T}^*$. Then all the abelian subgroups of $G$ are $C_n$ for $n \in \{1, 2, 3, 4, 6\}$, among which the normal ones are $C_2$ and the trivial group (see [7]). Hence it follows that $J_G \geq [G : C_2] = 12$. On the other hand, if $H$ is an arbitrary proper
subgroup of $G$, then $|H| \leq 8$, (where the equality holds if we take $H = Q_8$), and hence, we can see that $H$ contains an abelian normal subgroup of index $\leq 8 < 12$. Then it follows from the minimality of the Jordan constant that $J_G \leq 12$. Thus we get $J_G = 12$, as desired.

Similarly, for $G = \mathfrak{D}^*$, among the normal subgroups $\mathfrak{D}^*$, $\text{SL}_2(F_3), Q_8, C_2$, and the trivial group of $\mathfrak{D}^*$, the only abelian groups are $C_2$ and the trivial group (see [8]), and hence, it follows that $J_G \geq [G : C_2] = 24$. On the other hand, if $H$ is an arbitrary proper subgroup of $G$, then $|H| \leq 24$, (where the equality holds if we take $H = \text{SL}_2(F_3)$), and hence, we can see that $H$ contains an abelian normal subgroup of index $\leq 24$. Then it follows from the minimality of the Jordan constant that $J_G \leq 24$, and hence, we get $J_G = 24$, as desired.

Finally, if $G = \mathfrak{K}^*$, then among the normal subgroups $\mathfrak{K}^*, C_2$, and the trivial group of $\mathfrak{K}^*$, the only abelian groups are $C_2$ and the trivial group (see [9]), and hence, it follows that $J_G \geq [G : C_2] = 60$. Let $d = J_G$ and assume that $d > 60$. Then by definition, there is a subgroup $H$ of $G$ such that $H$ contains no abelian normal subgroups of index $\leq 60$. But then since $|H| \leq 24$ (by looking at the list of all subgroups of $G$), this is a contradiction. Hence we can see that $J_G = d = 60$.

This completes the proof. □

Using Lemmas 2.2, 3.7, and 3.8 above, we obtain the following result.

**Theorem 3.9.** Let $D$ be a quaternion division algebra over $\mathbb{Q}$ and let $R_D = \text{Ram}(D)$. Then the group $D^\times$ is Jordan, and we have

$$J_{D^\times} = \begin{cases} 12 & \text{if } R_D = \{2, \infty\}; \\ 2 & \text{if } R_D = \{3, \infty\}; \\ 1 & \text{otherwise.} \end{cases}$$

**Proof.** We first recall that $D^\times$ is a Jordan group by Lemma 3.4. Let $G$ be a finite subgroup of $D^\times$. Then in light of [12, Theorem 5.10], together with dimension counting over $\mathbb{Q}$, we can see that $G$ is either $\mathfrak{K}^*, \text{Dic}_{12}, Q_8$ or a cyclic group. Note that $J_{\mathfrak{K}^*} = 12, J_{\text{Dic}_{12}} = J_{Q_8} = 2$ by Lemmas 3.7, 3.8, and the Jordan constant of cyclic groups is equal to 1.

Now, we observe that $R_D = \{2, \infty\}$ if and only if $D \cong D_{2,\infty}$. In light of [4, Theorem 9] and [20, Theorem 6.1], we also have that $\mathfrak{K}^*$ is an absolutely irreducible maximal finite subgroup of $D^\times$ if and only if $D \cong D_{2,\infty}$. Now, suppose that $R_D = \{2, \infty\}$. Then since every finite subgroup of $D^\times \cong D_{2,\infty}^\times$ is a subgroup of $\mathfrak{K}^*$, it follows from Lemma 2.2 that $J_{D^\times} = J_{\mathfrak{K}^*} = 12$.

Conversely, if $J_{D^\times} = 12$, then by Lemmas 2.2 and 3.8, we know that $\mathfrak{K}^* \leq D^\times$, and hence, $D \cong D_{2,\infty}$. In a similar fashion, we can see that $J_{D^\times} = 2$ if and only if $\text{Dic}_{12} \leq D^\times$, which is also equivalent to the fact that $D \cong D_{3,\infty}$. (Here, we implicitly use the fact that if $Q_8 \leq D^\times$, then $D \cong D_{2,\infty}$ by [4, Theorem 9], in which case, we have seen that $J_{D^\times} = 12$.) The last item follows from the observation that, in this case, every finite subgroup of $D^\times$ is cyclic.

This completes the proof. □

The following is a restatement of the above theorem in a special case, that is related to our application.

**Corollary 3.10.** Assume that $D = D_{p,\infty}$ for some prime $p \geq 2$. Then we have

$$J_{D^\times} = \begin{cases} 12 & \text{if } p = 2; \\ 2 & \text{if } p = 3; \\ 1 & \text{if } p \geq 5. \end{cases}$$

**Proof.** We recall that $D_{p,\infty}$ is ramified exactly at the primes $p$ and $\infty$, and hence, the desired result follows immediately from Theorem 3.9. □

The main difference between Theorem 3.9 and Corollary 3.10 is that the $R_D$ in the last item of Theorem 3.9 can be any set of places of $\mathbb{Q}$, whose cardinality is even and positive (see Remark 3.1 above).

**Remark 3.11.** In fact, if $p \equiv 11 \pmod{12}$, then both of $C_4$ and $C_6$ are subgroups of $D^\times = D_{p,\infty}^\times$. To see this, we note that if $p \equiv 11 \pmod{12}$, then we have $(-1/p) = (3/p) = -1$ so that $p$ is inert in both $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$ (see [17, Theorem
Then since the infinite place of \( \mathbb{Q} \) is ramified in both \( \mathbb{Q}(\sqrt{-1}) \) and \( \mathbb{Q}(\sqrt{-3}) \) (because they are imaginary quadratic fields), it follows from Proposition 3.3 that both of \( \mathbb{Q}(\sqrt{-1}) \) and \( \mathbb{Q}(\sqrt{-3}) \) embed into \( D \), which, in turn, proves the claim. Similarly, if \( p \equiv 5 \pmod{12} \) (so that \( \left( \frac{-1}{p} \right) = 1 \) and \( \left( \frac{-3}{p} \right) = -1 \)), then \( C_6 \) is a subgroup of \( D^\times \) while \( C_4 \) is not. Also, if \( p \equiv 7 \pmod{12} \) (so that \( \left( \frac{-1}{p} \right) = -1 \) and \( \left( \frac{-3}{p} \right) = 1 \)), then \( C_4 \) is a subgroup of \( D^\times \) while \( C_6 \) is not, and if \( p \equiv 1 \pmod{12} \) (so that \( \left( \frac{-1}{p} \right) = \left( \frac{-3}{p} \right) = 1 \)), then neither \( C_4 \) nor \( C_6 \) is a subgroup of \( D^\times \).

To describe the case when the center \( K \) of \( D \) is a quadratic number field, we first need the following three lemmas.

**Lemma 3.12.** Let \( D \) be a quaternion division algebra over a quadratic number field \( K \), and let \( d > 0 \) be a square-free integer. Then the following conditions are equivalent:

(a) \( \mathfrak{X}^* \leq D^\times \) while \( \mathfrak{Σ}^* \) and \( \mathfrak{Z}^* \) are not subgroups of \( D^\times \).

(b) \( D = D_{2,∞} \otimes_\mathbb{Q} K \) where either \( K = \mathbb{Q}(\sqrt{d}) \) with \( d \neq 2, 5 \), or \( K = \mathbb{Q}(\sqrt{-d}) \) with \( d \equiv 7 \pmod{8} \).

**Proof.** Suppose first that \( \mathfrak{X}^* \leq D^\times \) while \( \mathfrak{Σ}^* \) and \( \mathfrak{Z}^* \) are not subgroups of \( D^\times \). Then it follows from [4, Theorem 9] that we have \( D \cong D_{2,∞} \otimes_\mathbb{Q} K \) that is a division algebra. Moreover, note that if \( \sqrt{2} \in K \) (resp. \( \sqrt{5} \in K \)), then \( \mathfrak{X}^* \leq D^\times \) (resp. \( \mathfrak{Z}^* \leq D^\times \)) by [20, Theorem 6.1], and hence, we get that \( \sqrt{2}, \sqrt{5} \notin K \), by assumption. Now, if \( K = \mathbb{Q}(\sqrt{d}) \) is a real quadratic field, then \( D \equiv D_{2,∞} \otimes_\mathbb{Q} K \) is always a division algebra by Proposition 3.3 (because the infinite place of \( \mathbb{Q} \) splits completely in \( K \)) so that it suffices to exclude the cases of \( d = 2 \) and \( d = 5 \). If \( K = \mathbb{Q}(\sqrt{-d}) \) is an imaginary quadratic field, then it suffices to find the condition of \( D \equiv D_{2,∞} \otimes_\mathbb{Q} K \) being a division algebra, which is equivalent to the fact that it splits completely in \( \mathbb{Q}(\sqrt{-d}) \) by Proposition 3.3, and the latter condition is equivalent to \( d \equiv 7 \pmod{8} \). For the converse, we can argue in a similar fashion, by observing that \( \mathfrak{X}^* \leq D_{2,∞}^\times \leq D^\times \).

This completes the proof. \( \square \)

**Lemma 3.13.** Let \( D \) be a quaternion division algebra over a quadratic number field \( K \), and let \( d > 0 \) be a square-free integer. Then the following conditions are equivalent:

(a) \( \text{Dic}_{12} \leq D^\times \) while \( \mathfrak{X}^* \) is not a subgroup of \( D^\times \).

(b) \( D = D_{3,∞} \otimes_\mathbb{Q} K \) where either \( K = \mathbb{Q}(\sqrt{d}) \) with \( d \equiv 9, 17 \pmod{24} \) or \( d \equiv 1 \pmod{3} \), or \( K = \mathbb{Q}(\sqrt{-d}) \) with \( d \equiv 2 \pmod{3} \).

**Proof.** Suppose first that \( \text{Dic}_{12} \leq D^\times \) while \( \mathfrak{X}^* \) is not a subgroup of \( D^\times \). Then it follows from [20, Theorem 6.1] that we have \( D_{3,∞} \subset D \), and then, since \( K \) is the center of \( D \), we can see that \( D \cong D_{3,∞} \otimes_\mathbb{Q} K \) that is a division algebra. Moreover, note that if \( D \cong D_{2,∞} \otimes_\mathbb{Q} K \), then \( \mathfrak{X}^* \leq D^\times \) by [20, Theorem 6.1], and hence, we get that \( D \not\cong D_{2,∞} \otimes_\mathbb{Q} K \), by assumption. Now, if \( K = \mathbb{Q}(\sqrt{d}) \) is a real quadratic field, then it suffices to consider the last condition, and we can see from Remark 3.1-(ii)’ and [17, Theorem 25] that \( D \not\cong D_{2,∞} \otimes_\mathbb{Q} K \) if and only if \( d \equiv 17 \pmod{24} \) (in which case, 3 is inert and 2 splits completely in \( \mathbb{Q}(\sqrt{d}) \)) or \( d \equiv 1 \pmod{3} \) (in which case, 3 splits completely in \( \mathbb{Q}(\sqrt{d}) \) so that the ramification behavior of 2 does not matter), or \( d \equiv 9 \pmod{24} \) (in which case, 3 is ramified and 2 splits completely in \( \mathbb{Q}(\sqrt{d}) \)). If \( K = \mathbb{Q}(\sqrt{-d}) \) is an imaginary quadratic field, then it suffices to find the condition of \( D \cong D_{3,∞} \otimes_\mathbb{Q} K \) being a division algebra, which is equivalent to the fact that 3 splits completely in \( \mathbb{Q}(\sqrt{-d}) \) by Proposition 3.3, and the latter condition is equivalent to \( d \equiv 2 \pmod{3} \). For the converse, we can argue in a similar fashion, by observing that \( \text{Dic}_{12} \leq D_{2,∞}^\times \leq D^\times \).

This completes the proof. \( \square \)

**Lemma 3.14.** Let \( D \) be a quaternion division algebra over a quadratic number field \( K \), and let \( G \in \{ \mathbb{Q}_8, \text{Dic}_{16}, \text{Dic}_{20}, \text{Dic}_{24} \} \). If \( G \leq D^\times \), then \( \mathfrak{X}^* \leq D^\times \).

**Proof.** If \( G = \mathbb{Q}_8 \) or \( \text{Dic}_{24} \) (resp. \( G = \text{Dic}_{16} \)), then since the 2-Sylow subgroup of \( G \) is a quaternion group of order 8 (resp. a generalized quaternion group of order 16), we can see that \( D \cong D_{2,∞} \otimes_\mathbb{Q} K \) by [4, Theorem 9], and hence, it follows that
\( \mathfrak{T}^* \leq D^\times \), as well. Now, if \( G = \text{Dic}_{20} \), then in view of the proof of [15, Theorem 11], we have \( D = D_{2,\infty} \otimes \mathbb{Q} \sqrt[\frac{5}{2}]{} \), and hence, it follows again that \( \mathfrak{T}^* \leq D^\times \).

This completes the proof. \( \square \)

Using the previous lemmas, we can obtain the following result.

**Theorem 3.15.** Let \( D \) be a quaternion division algebra over a quadratic number field \( K \), \( R_D = \text{Ram}(D) \), and let \( R_{\infty} \) be the set of all infinite places of \( K \). Also, let \( d > 0 \) be a square-free integer. Then the group \( D^\times \) is Jordan, and we have

\[
J_{D^\times} = \begin{cases} 
60 & \text{if } K = \mathbb{Q} \sqrt[\frac{5}{2}]{} \text{ and } R_D = R_{\infty}; \\
24 & \text{if } K = \mathbb{Q} \sqrt[\frac{2}{2}]{} \text{ and } R_D = R_{\infty}; \\
12 & \text{if } D = D_{2,\infty} \otimes \mathbb{Q} K \text{ where } K = \mathbb{Q} \sqrt[\frac{d}{2}]{} \text{ with } d \neq 2, 5, \text{ or } 12 \\
& \text{ } D = D_{2,\infty} \otimes \mathbb{Q} K \text{ where } K = \mathbb{Q} \sqrt[\frac{-d}{2}]{} \text{ with } d \equiv 7 \pmod{8}; \\
2 & \text{if } D = D_{3,\infty} \otimes \mathbb{Q} K \text{ where } K = \mathbb{Q} \sqrt[\frac{d}{2}]{} \text{ with } d \equiv 9, 17 \pmod{24} \text{ or } d \equiv 1 \pmod{3}, \text{ or} \\
& \text{ } D = D_{3,\infty} \otimes \mathbb{Q} K \text{ where } K = \mathbb{Q} \sqrt[\frac{-d}{2}]{} \text{ with } d \equiv 2 \pmod{3}; \\
1 & \text{otherwise.} 
\end{cases}
\]

**Proof.** We first recall that \( D^\times \) is a Jordan group by Lemmas 3.5 and 3.6. Let \( G \) be a finite subgroup of \( D^\times \). Then in light of [12, Theorem 5.10], we can see that \( G \) is either one of the following three groups \( \mathfrak{T}^*, \mathfrak{O}^*, \mathfrak{S}^* \) or is a dicyclic group or is a cyclic group. Note that \( J_{\mathfrak{T}^*} = 12, J_{\mathfrak{O}^*} = 24, J_{\mathfrak{S}^*} = 60 \) by Lemma 3.8, the Jordan constant of dicyclic groups equals 2 by Lemma 3.7, and the Jordan constant of cyclic groups is equal to 1.

Now, we observe that \( K = \mathbb{Q} \sqrt[\frac{5}{2}]{} \) and \( R_D = R_{\infty} \) if and only if \( D \cong D_{2,\infty} \otimes \mathbb{Q} \sqrt[\frac{5}{2}]{} \). In light of [4, Theorem 9] and [20, Theorem 6.1], we also have that \( \mathfrak{S}^* \) is an absolutely irreducible maximal finite subgroup of \( D^\times \) if and only if \( D \cong D_{2,\infty} \otimes \mathbb{Q} \sqrt[\frac{5}{2}]{} \). Now, suppose that \( K = \mathbb{Q} \sqrt[\frac{5}{2}]{} \) and \( R_D = R_{\infty} \). Then since every finite subgroup of \( D^\times \cong \left(D_{2,\infty} \otimes \mathbb{Q} \sqrt[\frac{5}{2}]{} \right)^\times \) is a subgroup of \( \mathfrak{S}^* \), it follows from Lemma 2.2 that \( J_{D^\times} = J_{\mathfrak{S}^*} = 60 \). Conversely, if \( J_{D^\times} = 60 \), then by Lemmas 2.2 and 3.8, we know that \( \mathfrak{S}^* \leq D^\times \), and hence, \( D \cong D_{2,\infty} \otimes \mathbb{Q} \sqrt[\frac{5}{2}]{} \). In a similar fashion, we can see that \( J_{D^\times} = 24 \) if and only if \( \mathfrak{O}^* \leq D^\times \), which is also equivalent to the fact that \( K = \mathbb{Q} \sqrt[\frac{2}{2}]{} \) and \( R_D = R_{\infty} \). For \( J_{D^\times} = 12 \), we note that \( J_{D^\times} = 12 \) if and only if \( \mathfrak{T}^* \leq D^\times \) and \( \mathfrak{O}^*, \mathfrak{S}^* \) are not subgroups of \( D^\times \), which is also equivalent to the given condition by Lemma 3.12.

Similarly, we can see that \( J_{D^\times} = 2 \) if and only if \( \text{Dic}_{20} \leq D^\times \), while \( \mathfrak{T}^* \) is not a subgroup of \( D^\times \) (by virtue of Lemma 3.14), which is also equivalent to the given condition by Lemma 3.13. Finally, the last item follows from the observation that, in this case, every finite subgroup of \( D^\times \) is cyclic (in view of [12, Theorem 5.10]).

This completes the proof. \( \square \)

**Remark 3.16.** Let \( \text{Pl}(K) \) be the set of all places of a number field \( K \). To give a slightly more detailed description on the case when \( J_{D^\times} = 1 \), we consider the following three cases:

**Case I** \( K = \mathbb{Q}(\sqrt{1}) \) and \( R_D \subseteq \{ p \in \text{Pl}(K) \mid p \text{ lies over 2 or 3 or } p \equiv 5 \pmod{12} \} \) or \( K = \mathbb{Q}(\sqrt{-3}) \) and \( R_D \subseteq \{ p \in \text{Pl}(K) \mid p \text{ lies over 2 or 3 or } p \equiv 7 \pmod{12} \} \) or \( K = \mathbb{Q}(\sqrt{3}) \) and \( R_D \subseteq \{ p \in \text{Pl}(K) \mid p \text{ lies over 2 or 3 or } p \equiv 11 \pmod{12} \text{ or } \infty \} \), \( R_D \neq R_{\infty} \).

**Case II** \( K = \mathbb{Q}(\sqrt{5}) \) and \( R_D \subseteq \{ p \in \text{Pl}(K) \mid p \text{ lies over 2 or 5 or } p \equiv 3, 7, 9 \pmod{10} \text{ or } \infty \} \), \( R_D \neq R_{\infty} \).

**Case III** \( K = \mathbb{Q}(\sqrt{-1}) \) and \( R_D \subseteq \{ p \in \text{Pl}(K) \mid p \text{ lies over 2 or } p \equiv 5 \pmod{8} \} \), \( R_D \subseteq \{ p \in \text{Pl}(K) \mid p \text{ lies over 2 or 3 or } p \equiv 5 \pmod{12} \} \) or \( K = \mathbb{Q}(\sqrt{-2}) \) and \( R_D \subseteq \{ p \in \text{Pl}(K) \mid p \text{ lies over 2 or } p \equiv 3 \pmod{8} \} \), \( R_D \neq \{ p \in \text{Pl}(K) \mid p \text{ lies over 3} \} \) or

This completes the proof. \( \square \)
\( K = \mathbb{Q}(\sqrt{2}) \) and \( R_D \subseteq \{ p \in \text{Pl}(K) \mid p \text{ lies over } 2 \text{ or } p \equiv 7 \pmod{8} \} , R_D \neq R_{\infty} \).

If (Case I) holds for \( D \), then we have \( C_{12} \leq D^\times \). Similarly, if (Case II) (resp. (Case III)) holds for \( D \), then we have \( C_{10} \leq D^\times \) (resp. \( C_8 \leq D^\times \)).

Now, we further specify the quaternion algebra to work with, and obtain a somewhat interesting result.

**Corollary 3.17.** Assume that \( D = D_{p,\infty} \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{p}) \) for some prime \( p \). Then we have

\[
J_{D^\times} = \begin{cases} 
60 & \text{if } p = 5; \\
24 & \text{if } p = 2; \\
12 & \text{if } p \equiv 3 \pmod{4} \text{ or } p > 5 \text{ and } p \equiv 5 \pmod{8}; \\
2 & \text{if } p \equiv 17 \pmod{24}; \\
1 & \text{otherwise}.
\end{cases}
\]

**Proof.** The cases of \( J_{D^\times} = 60 \) or 24 follow immediately from Theorem 3.15. For \( J_{D^\times} = 12 \), we note that \( J_{D^\times} = 12 \) if and only if \( D = D_{p,\infty} \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{p}) \cong D_{2,\infty} \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{p}) \) with \( p \neq 2, 5 \) by Theorem 3.15, which, in turn, is equivalent to the fact that \( p \equiv 3 \pmod{4} \) or \( p > 5 \) and \( p \equiv 5 \pmod{8} \). Similarly, for \( J_{D^\times} = 2 \), we note that \( J_{D^\times} = 2 \) if and only if \( D = D_{p,\infty} \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{p}) \cong D_{3,\infty} \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{p}) \) with \( p \equiv 9, 17 \pmod{24} \) or \( p \equiv 1 \pmod{3} \) by Theorem 3.15, which, in turn, is equivalent to the fact that \( p \equiv 17 \pmod{24} \).

This completes the proof. \( \square \)

### 3.2 Simple abelian surfaces over finite fields

In this section, we prove Theorem 1.3-(a) as an application of what we have done in Section 3.1. To be precise, we can first obtain the following theorem by combining some of the previous results.

**Theorem 3.18.** Let \( X \) be a simple abelian surface over a finite field \( k = \mathbb{F}_q \) with \( q = p^a \) for some prime \( p \) and an integer \( a \geq 1 \). Let \( D = \text{End}_k^0(X) \). Then the Jordan constant \( J_{D^\times} \) of \( D^\times \) is contained in the set \( \{1, 2, 12, 24, 60\} \).

**Proof.** By Lemma 2.3, we need to consider the following three cases:

1. If \( D \) is a totally definite quaternion algebra over \( \mathbb{Q} \) or over a real quadratic field, then the desired assertion follows from Theorems 3.9 and 3.15.
2. If \( D \) is a CM-field of degree 4, then every finite subgroup of \( D^\times \) is cyclic, and hence, it follows that \( J_{D^\times} = 1 \).
3. If \( D \) is a quaternion division algebra over an imaginary quadratic field, then it follows from Theorem 3.15 that \( J_{D^\times} \in \{1, 2, 12\} \).

This completes the proof. \( \square \)

The following theorem is the converse of Theorem 3.18.

**Theorem 3.19.** Let \( n \) be an integer contained in the set \( \{1, 2, 12, 24, 60\} \). Then there is a simple abelian surface \( X \) over some finite field \( k = \mathbb{F}_q \) with \( q = p^a \) for a prime \( p \) and an integer \( a \geq 1 \) such that \( J_{D^\times} = n \), where \( D = \text{End}_k^0(X) \).

**Proof.** We consider each case one by one. More precisely, we will give an irreducible polynomial \( h \in \mathbb{Z}[t] \) such that \( h^2 = f_X \) for some simple abelian surface \( X \) over a finite field \( k = \mathbb{F}_q \) (\( q = p^a \)) with the multiplicative subgroup of the endomorphism algebra \( \text{End}_k^0(X) \) having the desired Jordan constant. We provide a detailed proof for the case of \( n = 1 \), and then we can proceed in a similar fashion with the specified polynomial \( h \) for the other cases.
(1) For \( n = 1 \), take \( h = t^2 - 73 \). Let \( \pi \) be a zero of \( h \) so that \( \pi \) is a 73-Weil number. By Theorem 2.9, there exists a simple abelian variety \( X \) over \( k = \mathbb{F}_{73} \) of dimension \( r \) such that \( \pi_X \) is conjugate to \( \pi \) so that \( K = \mathbb{Q}(\pi_X) = \mathbb{Q}(\sqrt{73}) \). Then since 73 is totally ramified in \( K \), it follows from both parts of Proposition 2.6 that \( D = \text{End}_k^0(X) \) is a quaternion division algebra over \( K \), that is ramified exactly at the real places of \( K \), and hence, we get \( r = 2 \) by Corollary 2.5-(b). In particular, \( X \) is a simple abelian surface over \( k \), and \( D \cong D_{73,\infty} \otimes_{\mathbb{Q}} K \), which, in turn, implies that \( J_{D^\times} = 1 \) by Corollary 3.17.

(2) For \( n = 2 \), take \( h = t^2 - 17 \).

(3) For \( n = 12 \), take \( h = t^2 - 3 \).

(4) For \( n = 24 \), take \( h = t^2 - 2 \).

(5) For \( n = 60 \), take \( h = t^2 - 5 \).

This completes the proof.

Another way to view the aforementioned results is the following.

Remark 3.20. Consider a set \( S \) of pairs \((n, p)\) of an integer \( n \geq 1 \) and a prime \( p \) with the property that there is a simple abelian surface \( X \) over \( k = \mathbb{F}_q \) with \( q = p^a \) \((a \geq 1)\) and \( J_{D^\times} = n \), where \( D = \text{End}_k^0(X) \). Then we can see that:

(i) \( n \in \{1, 2, 12, 24, 60\} \) (see Theorem 3.18);
(ii) \((1, 73), (2, 17), (12, 3), (24, 2), (60, 5) \in S \) (see the proof of Theorem 3.19);
(iii) If we choose an element \((n, p)\) randomly from \( S \), then it is most probable that \( n = 12 \) in the sense of the prime number theorem for arithmetic progression (see [14, page 4]). More precisely, we note from Corollary 3.17 and the construction in the proof of Theorem 3.19 that \((1, p) \in S \) if and only if \( p \equiv 1 \) (mod 24), \((2, p) \in S \) if and only if \( p \equiv 17 \) (mod 24), and \((12, p) \in S \) if and only if \( p = 3 \) or \( p \equiv 7, 11, 13, 19, 23 \) (mod 24) or \( p \equiv 5 \) (mod 24) with \( p > 5 \). Furthermore, \((24, p) \in S \) (resp. \((60, p) \in S \)) if and only if \( p = 2 \) (resp. \( p = 5 \)). Hence we obtain the claim by virtue of the prime number theorem for arithmetic progression.

4 | ALGEBRAICALLY CLOSED FIELDS

In this section, we briefly consider the case when the base field of an abelian surface is algebraically closed of positive characteristic. To this aim, we first recall the following fact from Oort [21].

Proposition 4.1 ([21, Proposition 6.1]). Let \( X \) be a simple abelian surface over an algebraically closed field \( k \) of characteristic \( p > 0 \). Then the endomorphism algebra \( \text{End}_k^0(X) \) is of one of the following types:

(1) \( \mathbb{Q} \);
(2) a real quadratic field;
(3) an indefinite quaternion algebra over \( \mathbb{Q} \);
(4) a CM-field of degree 4.

In view of Proposition 4.1 and Theorems 3.9, 3.15, we obtain the following result.

Theorem 4.2. Let \( n \) be an integer and let \( p > 0 \) be a prime. Then there exists a simple abelian surface \( X \) over some algebraically closed field \( k \) of characteristic \( p \) such that \( J_{D^\times} = n \), where \( D = \text{End}_k^0(X) \) if and only if \( n = 1 \).

Proof. Suppose first that there is a simple abelian surface \( X \) over an algebraically closed field \( k \) of characteristic \( p \) with \( D = \text{End}_k^0(X) \). Then \( D \) is of one of the four types in Proposition 4.1. If \( D \) is either \( \mathbb{Q} \) or a real quadratic field or a quartic CM-field, then every finite subgroup of \( D^\times \) is cyclic, and hence, we get \( J_{D^\times} = 1 \). If \( D \) is an indefinite quaternion algebra over \( \mathbb{Q} \), then since \( D \) is not ramified at the infinite place of \( \mathbb{Q} \) (by the definition of indefiniteness), it follows from Theorem 3.9 that \( J_{D^\times} = 1 \). Conversely, take \( n = 1 \). Let \( D \) be an indefinite quaternion division algebra over \( \mathbb{Q} \) such that \( D \) is not ramified at \( p \). Then by [21, Proposition 3.11], there exists a field \( k \) of characteristic \( p \) and an absolutely simple abelian surface \( X \) over \( k \) with \( \text{End}_k^0(X) = D \), where \( X_k = X \times_k \mathbb{Q} \). Now, we note that \( J_{D^\times} = 1(= n) \) by Theorem 3.9.
This completes the proof.

In particular, both of Theorems 3.19 and 4.2 assert that every candidate for the Jordan constant is indeed realizable. An immediate consequence of Theorem 4.2 is the following corollary.

**Corollary 4.3.** Let \( p > 0 \) be a prime and let \( X \) be a simple abelian surface over an algebraically closed field \( k \) of characteristic \( p \). Then we have \( J_{\text{Aut}_k(X)} = 1 \).

**Proof.** By Theorem 4.2, we have \( J_{D^\times} = 1 \), where \( D = \text{End}_k^0(X) \). Then the desired assertion follows from the fact that \( \text{Aut}_k(X) \) is a subgroup of \( D^\times \). \( \square \)

**Remark 4.4.** In fact, we can obtain a similar result for special higher dimensional cases in the following sense: let \( g \geq 3 \) be a prime. Let \( X \) be a simple abelian variety of dimension \( g \) over an algebraically closed field \( k \) with \( \text{char}(k) = p > 0 \). Let \( D = \text{End}_k^0(X) \). Then in view of [21, §7] or [13, Remark 2.2], \( D \) is of one of the following types:

(i) \( D = \mathbb{Q} \);
(ii) \( D \) is a totally real field of degree \( g \);
(iii) \( D = D_{p,\infty} \) if (and only if) \( g \geq 5 \);
(iv) \( D \) is an imaginary quadratic field;
(v) \( D \) is a CM-field of degree 2g;
(vi) \( D \) is a central simple division algebra of degree \( g \) over an imaginary quadratic field and the \( p \)-rank of \( X \) is equal to 0.

Now, for items (i), (ii), (iv), and (v), we easily see that \( J_{D^\times} = 1 \). For the case when \( D = D_{p,\infty} \) and \( g \geq 5 \), then \( J_{D^\times} = 1 \) by Theorem 3.9. A possibly different phenomenon can occur only for the item (vi). But then, in light of [13, Theorem 3.5], we know that every finite subgroup of \( D^\times \) is cyclic, and hence, we also get \( J_{D^\times} = 1 \). Consequently, we can conclude that \( J_{D^\times} = 1 \) if \( g = 3 \), and \( J_{D^\times} \in \{1, 2, 12\} \) if \( g \geq 5 \).

**ACKNOWLEDGMENTS**

The author was supported by a KIAS Individual Grant (MG069901) at Korea Institute for Advanced Study. Also, the author sincerely thanks Professor Prokhorov for making valuable comments on the Introduction of this paper. Finally, he is sincerely grateful to the referee for reading the manuscript carefully, and for many invaluable comments to improve the quality and the readability of the article.

**ORCID**

Won Tae Hwang [https://orcid.org/0000-0001-8657-3253](https://orcid.org/0000-0001-8657-3253)

**REFERENCES**

[1] A. A. Albert, *A solution of the principal problem in the theory of Riemann matrices*, Ann. of Math. 35 (1934), no. 3, 500–515.
[2] A. A. Albert, *On the construction of Riemann matrices II*, Ann. of Math. 36 (1935), no. 2, 376–394.
[3] M. Alsina and P. Bayer, *Quaternion orders, quadratic forms, and shimura curves*, Amer. Math. Soc., Providence, RI, 2004.
[4] S. A. Amitsur, *Finite subgroups of division rings*, Trans. Amer. Math. Soc. 80 (1955), 361–386.
[5] C. Birkar, *Singularities of linear systems and boundedness of Fano varieties*, arXiv:1609.05543, 2016.
[6] T. Dokchitser, *GroupNames*, available at: [https://people.maths.bris.ac.uk/~matyd/GroupNames/R.html](https://people.maths.bris.ac.uk/~matyd/GroupNames/R.html) [last accessed July 2020].
[7] T. Dokchitser, *GroupNames*, available at: [https://people.maths.bris.ac.uk/~matyd/GroupNames/1/SL(2,3).html](https://people.maths.bris.ac.uk/~matyd/GroupNames/1/SL(2,3).html) [last accessed July 2020].
[8] T. Dokchitser, *GroupNames*, available at: [https://people.maths.bris.ac.uk/~matyd/GroupNames/1/CSU(2,3).html](https://people.maths.bris.ac.uk/~matyd/GroupNames/1/CSU(2,3).html) [last accessed July 2020].
[9] T. Dokchitser, *GroupNames*, available at: [https://people.maths.bris.ac.uk/~matyd/GroupNames/97/SL(2,5).html](https://people.maths.bris.ac.uk/~matyd/GroupNames/97/SL(2,5).html) [last accessed July 2020].
[10] B. Edixhoven, G. van der Geer, and B. Moonen, *Abelian varieties*, https://gerard.vdgeer.net/AV.pdf.
[11] T. Honda, *Isogeny classes of abelian varieties over finite fields*, J. Math. Soc. Japan 20 (1968), 83–95.
[12] W. Hwang, *On a classification of the automorphism groups of polarized abelian surfaces over finite fields*, J. Number Theory 204 (2019), 561–578.
[13] W. Hwang, *Automorphism groups of simple polarized abelian varieties of odd prime dimension over finite fields*, J. Number Theory 204 (2019), 561–578.
[14] D. Koukoulopoulos, *The distribution of prime numbers*, Amer. Math. Soc., Providence, RI, 2019.
[15] M. Lewis and M. Schacher, *Subgroups of division rings*, Rocky Mountain J. Math. 49 (2019), no. 7, 2227–2251.
[16] C. Maclachlan and A. Reid, *The arithmetic of hyperbolic 3-manifolds*, Springer-Verlag, New York, 2003.
[17] D. Marcus, *Number fields*, Springer-Verlag, New York–Heidelberg, 1977.
[18] S. Meng and D. Zhang, *Jordan properties for non-linear algebraic groups and projective varieties*, Amer. J. Math. 140 (2018), 1133–1145.
[19] D. Mumford, *Abelian varieties*, Corrected reprint of the 2nd ed., Hindustan Book Agency, New Delhi, 2008.
[20] G. Nebe, *Finite quaternionic matrix groups*, Represent. Theory 2 (1998), 106–223.
[21] F. Oort, *Endomorphism algebras of abelian varieties*, Algebraic Geometry and Commutative Algebra. Vol. II. In Honor of Masayoshi Nagata, (H. Hijikata et al., eds.), Kinokuniya Company Ltd., Tokyo, 1988, pp. 469–502.
[22] V. L. Popov, *On the Makar–Limanov, Derksen invariants, and finite automorphism groups of algebraic varieties*, Affine Algebraic Geometry: The Russell Festschrift, (D. Daigle, R. Ganong, and M. Koras, eds.), Amer. Math. Soc., Providence, RI, 2011, pp. 289–311.
[23] V. L. Popov, *Jordan groups and automorphism groups of algebraic varieties*, Automorphisms in birational and affine geometry, (I. Cheltsov et al., eds.), Springer, Cham, 2014, pp. 185–213.
[24] Y. Prokhorov and C. Shramov, *Jordan property for Cremona groups*, Amer. J. Math. 138 (2016), no. 2, 403–418.
[25] Y. Prokhorov and C. Shramov, *Jordan constant for Cremona group of rank 3*, Mosc. Math. J. 17 (2017), no. 3, 457–509.
[26] Y. Prokhorov and C. Shramov, *Finite groups of birational selfmaps of threefolds*, Math. Res. Lett. 25 (2018), no. 3, 957–972.
[27] J. P. Serre, *A Minkowski-style bound for the orders of the finite subgroups of the Cremona group of rank 2 over an arbitrary field*, Mosc. Math. J. 9 (2009), no. 1, 193–208.
[28] J. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. 2 (1966), 131–144.
[29] E. Yasinsky, *The Jordan constant for Cremona group of rank 2*, Bull. Korean Math. Soc. 54 (2017), no. 5, 1859–1871.

**How to cite this article:** Hwang W. *Jordan constants of quaternion algebras over number fields and simple abelian surfaces over fields of positive characteristic*. Mathematische Nachrichten. 2022;295:560–573. https://doi.org/10.1002/mana.202000183