Journal de Théorie des Nombres de Bordeaux
anciennement Séminaire de Théorie des Nombres de Bordeaux

Ha Thanh Nguyen TRAN, Peng TIAN et Amy FEAVER

The size function for imaginary cyclic sextic fields

Tome 35, nº 3 (2023), p. 841-866.
https://doi.org/10.5802/jtnb.1266

CENTRE MERSENNE

Le Journal de Théorie des Nombres de Bordeaux *est membre du Centre Mersenne pour l'édition scientifique ouverte*
http://www.centre-mersenne.org/
e-ISSN : 2118-8572

Journal de Théorie des Nombres de Bordeaux **35** (2023), 841–866

The size function for imaginary cyclic sextic fields

par Ha Thanh Nguyen TRAN, Peng TIAN et Amy FEAVER

Résumé. Dans cet article, nous étudions la fonction de taille h^0 pour les corps de nombres. Cette fonction est analogue à la fonction donnant la dimension de l'espace de Riemann–Roch d'un diviseur sur une courbe algébrique. Van der Geer et Schoof ont conjecturé que h^0 atteint son maximum sur la classe triviale des diviseurs d'Arakelov. Cette conjecture a été prouvée pour tous les corps de nombres dont le groupe des unités est de rang 0 et 1, ainsi que pour les corps cubiques cycliques dont le groupe des unités est de rang 2. Nous prouvons que cette conjecture est également valable pour les corps sextiques cycliques totalement imaginaires, une autre classe de corps de nombres dont le groupe des unités est de rang 2.

Abstract. In this paper, we investigate the size function h^0 for number fields. This size function is analogous to the dimension of the Riemann–Roch spaces of divisors on an algebraic curve. Van der Geer and Schoof conjectured that h^0 attains its maximum at the trivial class of Arakelov divisors. This conjecture was proved for all number fields with the unit group of rank 0 and 1, and also for cyclic cubic fields which have unit group of rank two. We prove the conjecture also holds for totally imaginary cyclic sextic fields, another class of number fields with unit group of rank two.

1. Introduction

The size function h^0 for a number field F is well-defined on the Arakelov class group Pic_F^0 of F (see [13]). This function was first introduced by van der Geer and Schoof [5] and also by Groenwegen [6, 7]. Van der Geer and Schoof conjectured that h^0 assumes its maximum on the trivial class O_F, the ring of integers of F, whenever $F/\mathbb{Q}$ is Galois or F is Galois over an imaginary quadratic field [5]. Experiments supported this conjecture [14].

By 2004 Francini proved the conjecture for all imaginary and real quadratic fields [3] and showed that the conclusion of the conjecture holds for certain pure cubic fields which are not Galois [4]. This establishes the

Manuscrit reçu le 18 juillet 2022, révisé le 18 décembre 2022, accepté le 3 mars 2023.

2020 *Mathematics Subject Classification.* 11Y40, 11H06, 11R20.

Mots-clefs. Arakelov divisor; size function; imaginary cyclic sextic fields; hexagonal lattice; unit lattice; cyclic cubic field.

Ha T. N. Tran acknowledges the support of the Natural Sciences and Engineering Research Council of Canada (NSERC) (funding RGPIN-2019-04209 and DGECR-2019-00428). Peng Tian is supported by the National Natural Science Foundation of China (grant #11601153) and Fundamental Research Funds for the Central Universities (grant #222201514319).

conjecture for fields with unit group of rank zero and some with the unit group of rank one. Tran proved the conjecture for any quadratic extension of a complex quadratic field [15] and, along with Tian, for all cyclic cubic fields [16]. In these cases, the fields have unit group of rank one and two respectively.

In this paper, we consider another class of number fields with unit group of rank two: totally imaginary cyclic sextic fields. This class of number fields poses its own set of challenges. To prove our main result we develop new techniques which are presented in Sections 3 and 4. Using these methods we are able to prove:

Theorem 1.1. *Let F be an imaginary cyclic sextic field. Then the function h^0 on Pic_F^0 obtains its unique global maximum at the trivial class $[D_0] = [(O_F, 1)]$.*

To prove Theorem 1.1, we prove the equivalent statement

$$h^0(O_F, 1) > h^0(I, u) \text{ whenever } [(I, u)] \neq [(O_F, 1)].$$

The proof strategy is outlined in Section 5. We consider two cases:

(1) Section 6 proves the case where I is not principal and is the shorter of the proofs.
(2) Sections 7 and 8 provide the proof for principal I. The reason this is split over two sections is that the proof differs depending on the value of $\|\log u\|$.

The size function h^0 is given by the logarithm of the sum

$$k^0(I, u) := \sum_{f \in I} e^{-\pi\|uf\|^2}.$$

To more fully understand this definition and its context, see Sections 2.4, 2.5, and 2.6. In order to prove Theorem 1.1 it is sufficient to show

$$k^0(O_F, 1) > k^0(I, u) \text{ whenever } [(I, u)] \neq [(O_F, 1)].$$

To procure an upper bound on $k^0(I, u)$ in Sections 6 and 7, we split it into four summands:

$$k^0(I, u) = 1 + \Sigma_1(I, u) + \Sigma_2(I, u) + \Sigma_3(I, u)$$

where each sum Σ_i, $i \in \{1, 2, 3\}$ is taken over a set S_i with $I\backslash\{0\} = S_1 \cup S_2 \cup S_3$. Specifically,

$$\Sigma_i(I, u) := \sum_{f \in S_i} e^{-\pi\|uf\|^2},$$

with the sets S_i being chosen strategically in a way that groups the elements of $I\backslash\{0\}$ based on the size of $\|uf\|^2$ as defined in Section 4. The set S_1 is chosen with the smallest values, $\|uf\|^2 < 6 \cdot 2^{1/3}$, and the set S_3 has the largest values, with $\|uf\| \geq 6\cdot 3^{1/3}$. Theorem 1.1 is then proved in Sections 6 and 7 by finding a sufficiently small upper bound for each summand by applying the results in Section 4 and Corollary 2.17.

Seeing this outline at this stage, while it is not fully explained, serves to help the reader understand why we prove results that depend on the value $\|uf\|^2$.

To this end, we also highlight the use of the bound $\|f\|^2 < 22$ which appears in Corollary 2.17 and at the beginning in Section 3 as an assumed condition on the size of f in several propositions and lemmas. These results are applied to the proof of Theorem 1.1 in Section 8. This is the case where I is a principal ideal and $\|\log u\| < 0.24163$. As a very high-level explanation, one may suspect that this case is more difficult because the class $[(I, u)]$ bears a lot of similarities to the trivial class $[(O_F, 1)]$ in that I and O_F are both principal and u and 1 are, geometrically speaking, sufficiently close to one another.

To prove that $k^0(O_F, 1) > k^0(I, u)$ in Section 8 we show that $k^0(I, u) - k^0(O_F, 1) < 0$. As this difference may be very small, we instead prove

$$\frac{k^0(I, u) - k^0(O_F, 1)}{\|\log u\|^2} < 0,$$

since this fraction is larger in absolute value and easier to work with. If all nonzero elements $f \in O_F$ which are not roots of unity have the property that $\|f\|^2 \geq 22$, we can prove that this quotient is negative by Corollary 2.17. Otherwise, we compute this quotient case by case using the results in Section 3 (see the proof of Proposition 8.6 and Table 8.1).

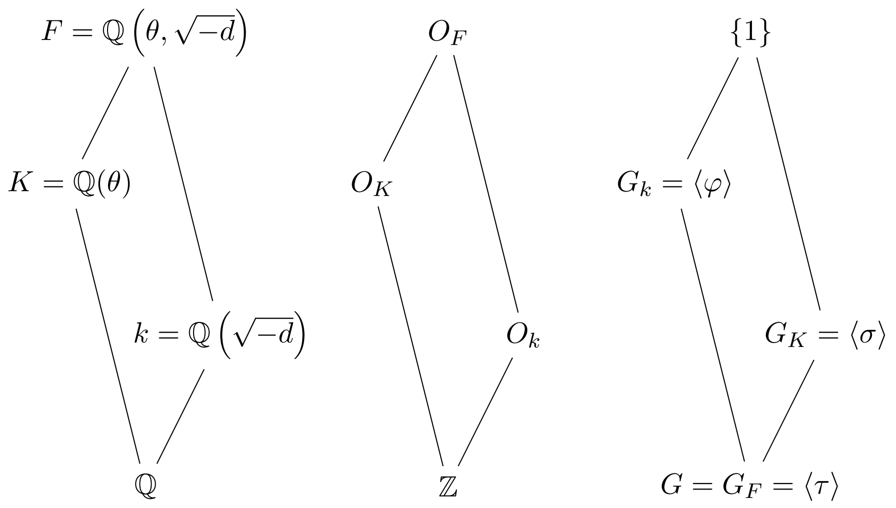
Through trying different bounds on $\|f\|^2$ we were able to determine that $\|f\|^2 < 22$ was the smallest bound necessary in order to make the mathematics work out. We also remark that the assumption that F is cyclic is vital. The Galois property allows us to make use of several invariance properties (see Lemmas 2.1 and 2.14) which are crucial in our proofs of Lemma 8.2 and Propositions 8.1 and 8.3. Moreover, as F is cyclic we can obtain an explicit description of the discriminant of F (Lemma 3.1) and the unit group $O_F^\times$ (Lemma 2.6). The cyclic property also implies that the log unit lattice of F is hexagonal and allows for the efficient calculation of lower bounds on the lengths of elements of O_F, when viewed as a lattice in $\mathbb{R}^6$ (see Propositions 2.4, 3.2, 3.3, 3.6 and 3.7).

All of the computer-aided computations in this paper are straightforward; we only need to call a function either in Mathematica or in Pari/gp to obtain the results. We use Mathematica [17] for the approximations in Section 2.7 and for calculating the upper and lower bounds in Sections 7.1, 7.2, and Proposition 8.4. We apply the LLL algorithm [11] and the function **qfminim()** in Pari/gp [12], which utilizes the Fincke–Pohst algorithm [2] and enumerates all vectors of length bounded in a given lattice. These enumerations are used in the proofs of Propositions 4.3, 4.4, and 8.6.

Acknowledgments. The authors would like to thank René Schoof for a useful discussion and the reviewers for their insightful comments that helped improve the manuscript.

2. Preliminaries

2.1. Notation. Let F be an imaginary cyclic sextic field with maximal real subfield K and imaginary quadratic subfield k. Then K is a cyclic cubic field with the form $K = \mathbb{Q}(\theta)$ for some integral element θ. Further, $k = \mathbb{Q}(\sqrt{-d})$ for some squarefree positive integer d, and $F = K(\sqrt{-d})$. Thus we have the following setup:



Here, O_F, O_K and O_k are the rings of integers and $G = \langle \tau \rangle, G_K = \langle \sigma \rangle$ and $G_k = \langle \varphi \rangle$ the Galois groups of F, K and k respectively. Then $O_k = \mathbb{Z}[\delta]$ where

$$\delta = \begin{cases} \sqrt{-d} & \text{if } d \equiv 1, 2 \bmod 4 \\ \frac{1+\sqrt{-d}}{2} & \text{otherwise.} \end{cases}$$

Observe that $\tau(\theta) = \sigma(\theta)$ and $\tau(\delta) = \varphi(\delta)$. We have the six embeddings $F \hookrightarrow \mathbb{C}$:

$$\tau_1 = \mathbf{1} = \tau^0, \qquad \tau_2 = \tau^1, \qquad \tau_3 = \tau^2,$$
$$\overline{\tau_1} = \overline{\mathbf{1}} = \tau^3, \qquad \overline{\tau_2} = \tau^4, \qquad \overline{\tau_3} = \tau^5.$$

In this paper, we use the map $\Phi : F \longrightarrow \mathbb{C}^3$ defined by

$$\Phi(f) = (\tau_i(f))_{1 \le i \le 3} = (\tau_1(f), \tau_2(f), \tau_3(f)) \text{ for all } f \in F.$$

The length function on each $f \in F$ is given by

$$\|f\|^2 := \|\Phi(f)\|^2 = 2 \sum_{i=1}^{3} |\tau_i(f)|^2.$$

For each $g \in K$, we also define

$$\|g\|_K^2 := \|(\sigma^i(g)_i)\|^2 = \sum_{i=1}^{3} |\sigma^i(g)|^2,$$

thus $\|g\|^2 = 2\|g\|_K^2$.

Lemma 2.1. *Let $f \in F$. Then $\|\tau_1(f)\| = \|\tau_2(f)\| = \|\tau_3(f)\|$.*

The image $\Phi(I)$ of a fractional ideal I of F is a lattice in $\mathbb{C}^3$ and thus maps to a lattice in $\mathbb{R}^6$ via $z \mapsto (\Re(z), \Im(z))$ where $\Re(z)$ and $\Im(z)$ are the real and imaginary parts of z.

Let p be the conductor of K and $t = \gcd(p, d)$. The discriminant of K is $\Delta_K = p^2$ and the discriminant of k is

$$\Delta_k = \begin{cases} -4d & \text{if } d \equiv 1, 2 \bmod 4 \\ -d & \text{otherwise.} \end{cases}$$

Remark 2.2. By [8], the conductor p of K has the form $p = p_1 p_2 \cdots p_r$, where $r \in \mathbb{Z}_{>0}$ and $p_1, \dots, p_r$ are distinct integers from the set

$$\{9\} \cup \{q \mid q \text{ is prime}, q \equiv 1 \bmod 3\} = \{7, 9, 13, 19, 31, 37, \dots\}.$$

2.2. The ring of integers O_K. We recall the following result from [16].

Proposition 2.3. *There exists an element $g \in O_K$ such that $\mathrm{Tr}(g) = g + \sigma(g) + \sigma^2(g) = 0$ and one of the following holds:*

(i) *$O_K = \mathbb{Z} \oplus \mathbb{Z}[\sigma] \cdot g$ or*

(ii) *$O_K \supset \mathbb{Z} \oplus \mathbb{Z}[\sigma] \cdot g$ and $[O_K : (\mathbb{Z} \oplus \mathbb{Z}[\sigma] \cdot g)] = 3$.*

Using the proof from [16, Proposition 2.3] in combination with the equation $\|g\|^2 = 2\|g\|_K^2$ for $g \in K$ we obtain the following result.

Proposition 2.4. *We have $\|g\|_K^2 \geq \frac{2p}{3}$ and $\|g\|^2 \geq \frac{4p}{3}$ for all $g \in O_K \backslash \mathbb{Z}$.*

Another structural observation of O_K is described in the next lemma.

Lemma 2.5. *For any $f \in O_K \backslash \mathbb{Z}$, the set $\{1, f, \sigma(f)\}$ is $\mathbb{R}$-linearly independent.*

2.3. The unit lattice. We define the map $\log : F^\times \longrightarrow \mathbb{R}^3$, the plane $\mathcal{H}$ and the log unit lattice Λ as follows:

$$\log(f) := (\log |\tau_i(f)|)_{1 \leq i \leq 3} \in \mathbb{R}^3 \text{ for all } f \in F^\times,$$

$$\mathcal{H} = \{(v_1, v_2, v_3) \in \mathbb{R}^3 : v_1 + v_2 + v_3 = 0\},$$

$$\Lambda = \log(O_F^\times) = \{(\log |\tau_i(\varepsilon)|)_{i=1}^3 : \varepsilon \in O_F^\times\}.$$

Here Λ is a full-rank lattice contained in $\mathcal{H}$ by Dirichlet's unit theorem. Let μ_F be the set of roots of unity of F, and let $O_K^\times$ and $O_k^\times$ be the unit groups of K and k respectively.

Lemma 2.6. *The unit group of O_F is $O_F^\times = \mu_F O_K^\times$.*

Proof. The Hasse unit index of F is $Q_F = [O_F^\times : \mu_F O_K^\times]$ by [9]. Since k is an imaginary quadratic field, its unit index $Q_k = 1$. Both k and F are totally complex and abelian with $[F : k] = 3$. Thus by [10, Lemma 2], $Q_F = Q_k = 1$. Therefore $O_F^\times = \mu_F O_K^\times$. □

A lattice is called *hexagonal* if it is isometric to the lattice $M \cdot \mathbb{Z}[\zeta_3]$ for some $M \in \mathbb{R}_+$ and a primitive cube root of unity ζ_3.

Corollary 2.7. *The lattice Λ is hexagonal.*

Proof. By Lemma 2.6, we have that $\Lambda = \log(O_F^\times) = \log(\mu_F \times O_K^\times) = \log(O_K^\times)$. The result follows since $\log(O_K^\times)$ is hexagonal by [16, Proposition 2.1]. □

Corollary 2.7 implies that Λ has a $\mathbb{Z}$-basis given by two shortest vectors $b_1 = \log \varepsilon_1$ and $b_2 = \log \varepsilon_2$ for some $\varepsilon_1, \varepsilon_2 \in O_F^\times$ and with $\|b_1\| = \|b_2\| = \|b_2 - b_1\|$ (Figure 2.1). Let $\mathcal{F}$ be the fundamental domain of Λ given by

$$\mathcal{F} = \left\{ \alpha_1 \cdot b_1 + \alpha_2 \cdot b_2 : \alpha_1, \alpha_2 \in \left(-\frac{1}{2}, \frac{1}{2} \right] \right\}.$$

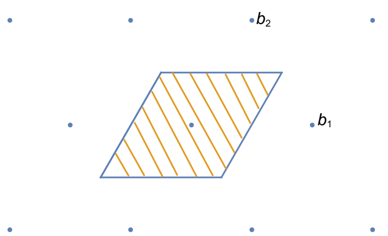


FIGURE 2.1. The lattice Λ and $\mathcal{F}$ (the shaded area).

Remark 2.8. We could also choose a different fundamental domain, such as the Voronoi domain. This would make the proof in Section 7.1 slightly different but the proofs in Sections 7.2 and 8 would remain the same.

We further define λ to be the length of the shortest vectors of Λ, and

$$B(w) = \{\mathbf{x} \in O_F^\times : \|\log \mathbf{x} - w\| < \lambda\} \text{ for each } w \in \mathcal{F}.$$

Lemma 2.9. *Let $w \in \mathcal{F}$. Then $\#B(w) \leq 4 \cdot (\#\mu_F)$. Moreover,*

$$B(w) \subset \{1, \mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3\} \cdot \mu_F \subset O_F^\times \text{ where}$$

$$\|\log \mathbf{x}_1 - w\| \geq \sqrt{3}\lambda/4, \|\log \mathbf{x}_2 - w\| \geq \lambda/2 \text{ and } \|\log \mathbf{x}_3 - w\| \geq \sqrt{3}\lambda/2.$$

Proof. See the proof of [16, Lemma 2.2], replacing ± 1 with μ_F. □

Lemma 2.10. *If $p = 7$ then $\lambda \approx 1.44975$. Moreover, $\lambda > 1.83336$ when $p \geq 9$.*

Proof. This lemma follows from the argument in the proof of [16, Lemma 2.3], combined with Lemma 2.6 and the fact that $\|g\|^2 = 2\|g\|_K^2$ for $g \in K$. □

2.4. Arakelov divisors.

Definition 2.11. An *Arakelov divisor* of F is a pair $D = (I, u)$ where I is a fractional ideal of F and u is any element in $\mathbb{R}_+^3$.

The Arakelov divisors of F form the additive group Div_F. The *degree* of a divisor $D = (I, u)$ is $\deg(D) := -\log(N(u)N(I))$, where the *norm* of $u = (u_1, u_2, u_3) \in \mathbb{R}^3$ is $N(u) := u_1 u_2 u_3$. Define

$$uf := u \cdot \Phi(f) = (u_i \cdot \tau_i(f)) \in \mathbb{C}^3 \text{ for all } f \in I.$$

Then

$$\|uf\|^2 = \|u \cdot \Phi(f)\|^2 = 2\sum_{i=1}^{3} u_i^2 \cdot |\tau_i(f)|^2.$$

Further, $uI := \{uf : f \in I\}$ is a lattice in $\mathbb{C}^3$. We call uI the *lattice associated* to D. Each element $f \in F^\times$ is attached to a *principal Arakelov divisor* $(f) := (f^{-1}O_F, |f|)$. Here, $f^{-1}O_F$ is the principal ideal generated by f^{-1}, and

$$|f| := |\Phi(f)| = (|\tau^i(f)|)_{0 \leq i \leq 2} \in \mathbb{R}_+^3.$$

This divisor has degree 0 by the product formula [5, 13].

2.5. The Arakelov class group. The Arakelov divisors of degree 0 form a group Div_F^0.

Definition 2.12. The *Arakelov class group* Pic_F^0 is the quotient of Div_F^0 by its subgroup of principal divisors.

This class group is similar to the Picard group of an algebraic curve. Define $\mathrm{T}^0 = \mathcal{H}/\Lambda$, a real torus of dimension 2. Each class $v = (v_1, v_2, v_3) \in \mathrm{T}^0$ can be embedded into Pic_F^0 by $v \mapsto D_v = (O_F, u)$ with $u = (e^{-v_i})_i$. Therefore, T^0 can be viewed as a subgroup of Pic_F^0, and, by [13, Proposition 2.2] we know:

Proposition 2.13. *The map that sends the Arakelov class represented by a divisor $D = (I, u)$ to the ideal class of I is a homomorphism from Pic_F^0 to the class group Cl_F of F. It induces the exact sequence*

$$0 \longrightarrow \mathrm{T}^0 \longrightarrow \mathrm{Pic}_F^0 \longrightarrow \mathrm{Cl}_F \longrightarrow 0.$$

The group T^0 is the connected component of the identity of the topological group Pic_F^0. Each class of Arakelov divisors in T^0 is represented by a divisor $D = (O_F, u)$ for some $u \in \mathbb{R}_+^3$, $N(u) = 1$. Here u is unique up to multiplication by a unit in $O_F^\times$; see [13, Section 6] for more details.

2.6. The function h^0. Let $D = (I, u)$ be an Arakelov divisor of F. Define

$$h^0(D) := \log(k^0(D)),$$
$$k^0(D) := \sum_{f\in I} e^{-\pi\|uf\|^2} = \sum_{\mathsf{x}\in uI} e^{-\pi\|\mathsf{x}\|^2}.$$

The function h^0 is well-defined on Pic_F^0 and analogous to the dimension of the Riemann–Roch space $H^0(D)$ of a divisor D on an algebraic curve[5, 13]. From [16] we have:

Lemma 2.14. *The function h^0 on T^0 is invariant under the action of τ. That is,*

$$h^0(D) = h^0(\tau(D)) \textit{ for all } D \in \mathrm{T}^0.$$

Remark 2.15. Let I be the principal ideal $I = fO_F$ for some $f \in F^\times$. Then

$$D = (I, u) = (fO_F, u) = (fO_F, |f|^{-1}) + (O_F, u|f|) = (f^{-1}) + (O_F, u').$$

Here (f^{-1}) is the principal Arakelov divisor generated by f^{-1} and

$$u' = u|f| = (u_i|\sigma_i(f)|)_i \in \mathbb{R}_+^3.$$

Thus D and $D' = (O_F, u')$ are in the same class of divisors in Pic_F^0, and hence $k^0(D) = k^0(D')$. Therefore, without loss of generality, we can assume that D has the form (O_F, u) for some $u \in \mathbb{R}_+^3$ and $N(u) = 1$. In other words, $[D] \in \mathrm{T}^0$.

2.7. Some estimates. Let L be a lattice in $\mathbb{R}^6$ and λ the length of its shortest vectors. Using an argument similar to the proof of [15, Lemma 3.2], replacing π with ξ, we have:

Lemma 2.16. *For $M \geq \lambda^2 \geq a^2 > 0$ and $\xi > 0$,*

$$\sum_{\substack{\mathsf{x}\in L\\ \|\mathsf{x}\|^2\geq M}} e^{-\xi\|\mathsf{x}\|^2} \leq \xi \int_M^\infty \left(\left(\frac{2\sqrt{t}}{a}+1\right)^6 - \left(\frac{2\sqrt{M}}{a}-1\right)^6\right) e^{-\xi t}\,\mathrm{d}t.$$

The next result can be obtained by applying Lemma 2.16 with $a = \sqrt{6}$ and $\xi = \pi$.

Corollary 2.17. *If* $\lambda^2 \geq 6$, *then*

$$\sum_{\substack{\mathsf{x}\in L \\ \|\mathsf{x}\|^2 \geq 6\cdot 3^{1/3}}} e^{-\pi\|\mathsf{x}\|^2} < 2.6049 \cdot 10^{-9}, \qquad \sum_{\substack{\mathsf{x}\in L \\ \|\mathsf{x}\|^2 \geq 22}} e^{-(\pi-2/7)\|\mathsf{x}\|^2} < 10^{-23},$$

$$\sum_{\substack{\mathsf{x}\in L \\ \|\mathsf{x}\|^2 \geq 22}} e^{-(\pi-2\sqrt{2}\cdot 0.170856\,\pi-2/7)\|\mathsf{x}\|^2} < 2.19277 \cdot 10^{-9}.$$

3. Upper bounds for p and d

In this section, we find upper bounds for p and d if there exists a nonzero element $f \in O_F \backslash \mu_F$ such that $\|f\|_F^2 < 22$. We restrict to this case, as these are the results needed for the proof of Theorem 1.1 in Section 8.

Lemma 3.1. *The discriminant of* F *is* $\Delta_F = \frac{p^4\Delta_k^3}{\gcd(p,d)^2}$. *Consequently, the index*

$$[O_F : O_K[\delta]] = \gcd(p, d) = t.$$

Proof. Observe that $O_K[\delta] = O_k \times O_K$ since $O_k = \mathbb{Z}[\delta]$. The discriminant of the tensor product $O_k \times O_K$ is $(p^2)^{[k:\mathbb{Q}]}(\Delta_k)^{[K:\mathbb{Q}]} = p^4\Delta_k^3$.

By the conductor-discriminant formula [1], the discriminant of F is equal to the product of the conductors of the characters of F. The trivial character, the quadratic character, and the two cubic characters have conductors 1, Δ_k, p, and p respectively. The two characters of order 6 have conductor $\operatorname{lcm}(p, \Delta_k)$. Hence $\Delta_F = \Delta_k p^2(\operatorname{lcm}(p, \Delta_k))^2 = \frac{p^4\Delta_k^3}{\gcd(p,\Delta_k)^2} = \frac{p^4\Delta_k^3}{\gcd(p,d)^2}$. The last equality is because $\Delta_k \in \{d, 4d\}$ and p is odd by Remark 2.2. Thus the index of $O_k \times O_K$ inside O_F is $\sqrt{\frac{p^4\Delta_k^3}{\Delta_F}} = \gcd(p, d)$. □

Further, since $t = [O_F : O_K[\delta]]$, for every $f \in O_F$, we have $tf \in O_K[\delta]$. Hence,

$$f = \frac{1}{t}(\gamma + \beta\delta) \text{ for some } \gamma, \beta \in O_K.$$

Proposition 3.2. *Let* $d \equiv 1, 2 \mod 4$. *Assume that* $f = \frac{1}{t}(\gamma + \beta\delta) \in O_F \backslash (O_K \cup O_k \cup \mu_F)$ *where* $\gamma, \beta \in O_K$ *such that* $\|f\|^2 < 22$. *Then we have the following.*

(i) *If* $\beta \in O_K \backslash \mathbb{Z}$, *then* $p \leq 19$ *and* $d \leq 22$.
(ii) *If* $\beta \in \mathbb{Z} \backslash \{0\}$, *then* $p \leq 61$ *and* $d \leq 14$.

Proof. Assume that f satisfies the criterion in the statement of the proposition. Then

$$22 > \|f\|^2 = 2\frac{\|\gamma\|_K^2}{t^2} + 2\frac{\|\beta\|_K^2 d}{t^2}. \tag{3.1}$$

Let $\alpha \in O_K \backslash \mathbb{Z}$ be a shortest element. By the proof of [16, Proposition 2.3],

$$\|\alpha\|_K^2 \leq \frac{2p+1}{3}. \tag{3.2}$$

Recall that $\delta = \sqrt{-d}$. We consider two cases:

Case i: $\beta \in O_K \backslash \mathbb{Z}$. Note that $\tau^i|_K = \Re(\tau^i) = \sigma^i, i = 1,2,3$ and $\tau^3 = \overline{\mathbf{1}}$. The discriminant of the set $\mathcal{S} = \{1, \alpha, \tau(\alpha), \delta, f, \tau(f)\} \subset O_F$ is $\det(\mathcal{S})$, which is computed as follows:

$$\begin{aligned}\det(\mathcal{S}) &= \left(\det(\tau^i(g))_{g\in\mathcal{S}, 0\leq i\leq 5}\right)^2 \\ &= \frac{2^6\left(\sqrt{d}\right)^6}{t^4}\begin{vmatrix}1 & \alpha & \sigma(\alpha)\\ 1 & \sigma(\alpha) & \sigma^2(\alpha)\\ 1 & \sigma^2(\alpha) & \alpha\end{vmatrix}^2 \cdot \begin{vmatrix}1 & \beta & \sigma(\beta)\\ 1 & \sigma(\beta) & \sigma^2(\beta)\\ 1 & \sigma^2(\beta) & \beta\end{vmatrix}^2.\end{aligned}$$

Since $\alpha, \beta \in O_K \backslash \mathbb{Z}$, the two sets $\{1, \alpha, \sigma(\alpha)\}$ and $\{1, \beta, \sigma(\beta)\}$ are $\mathbb{R}$-linearly independent (Lemma 2.5), so $\det(\mathcal{S}) \neq 0$. Thus $\mathcal{S}$ is a set of independent elements in O_F, and, by Lemma 3.1,

$$\det(\mathcal{S}) \geq |\Delta_F| = \frac{p^4 \cdot (4d)^3}{t^2}. \tag{3.3}$$

Combining this with Hadamard's inequality leads to

$$\begin{aligned}\det(\mathcal{S}) &\leq \frac{2^6 \cdot d^3}{t^4} \cdot \|1\|_K^2 \cdot \|\alpha\|_K^2 \cdot \|\sigma(\alpha)\|_K^2 \cdot \|1\|_K^2 \cdot \|\beta\|_K^2 \cdot \|\sigma(\beta)\|_K^2 \\ &= 2^6 \cdot d \cdot 3^2 \cdot \|\alpha\|_K^4 \cdot \left(\frac{\|\beta\|_K^2 \cdot d}{t^2}\right)^2.\end{aligned}$$

From (3.1) and (3.2) we have

$$\det(\mathcal{S}) < 2^6 \cdot d \cdot 3^2 \cdot \left(\frac{2p+1}{3}\right)^2 \cdot 11^2 = 2^6 \cdot d \cdot 11^2 \cdot (2p+1)^2. \tag{3.4}$$

Applying (3.3) and (3.4) gives:

$$\frac{p^2 \cdot d}{t} < 11 \cdot (2p+1). \tag{3.5}$$

Since $t \leq d$, this bound implies $p^2 < 11 \cdot (2p+1)$, which gives $p \leq 19$. We also have $t \leq p$, then by (3.5), $p \cdot d < 11 \cdot (2p+1)$. As $p \leq 19$, it follows that $d \leq 22$.

Case ii: $\beta \in \mathbb{Z}$. Since $f \notin O_k$, it follows that $\gamma \notin \mathbb{Z}$. Consequently, $\gamma \in O_K \backslash \mathbb{Z}$ and

$$\frac{2\gamma}{t} = f + \overline{\mathbf{1}}(f) \in O_F \cap K,$$

which implies $\frac{2\gamma}{t} \in O_K \backslash \mathbb{Z}$. By Proposition 2.4, $\|\frac{2\gamma}{t}\|^2 \geq 4p/3$, and therefore

$$\frac{4p}{3} \leq \left\|\frac{2\gamma}{t}\right\|^2 \leq \|f\|^2 + \|\overline{\mathbf{1}}(f)\|^2 < 22 + 22 = 44.$$

Thust $p \leq 61$.

Now since $\frac{2\beta\sqrt{-d}}{t} = f - \overline{\mathbf{1}}(f) \in O_F \cap k$, we have $\frac{2\beta\sqrt{-d}}{t} \in O_k = \mathbb{Z}[\sqrt{-d}]$. Hence $\frac{2\beta}{t} = a \in \mathbb{Z}$. Note that $\beta \neq 0$ since $f \notin O_K$. By (3.1),

$$22 > 2\frac{\|\beta\|_K^2 d}{t^2} \geq \frac{6a^2 d}{4} \geq \frac{3d}{2}.$$

As a result, $d \leq 14$. □

Proposition 3.3. *Let* $d \equiv 3 \mod 4$. *Assume that there exists*

$$f = \frac{1}{t}(\alpha + \beta\delta) \in O_F \backslash (O_K \cup O_k \cup \mu_F)$$

where $\alpha, \beta \in O_K$ *and* $\|f\|^2 < 22$. *Then:*

(i) *If* $\beta \in O_K \backslash \mathbb{Z}$, *then* $p \leq 61$ *and* $d \leq 59$.
(ii) *If* $\beta \in \mathbb{Z} \backslash \{0\}$, *then* $p \leq 61$ *and* $d \leq 11$.

Proof. This is similar to the proof of Proposition 3.2, with $\delta = \frac{1+\sqrt{-d}}{2}$, $\Delta_F = \frac{p^4 d^3}{t^2}$, and

$$22 > \|f\|^2 = \frac{\|2\gamma + \beta\|_K^2}{2t^2} + \frac{\|\beta\|_K^2 d}{2t^2}. \tag{3.6}$$

When $\beta \in O_K \backslash \mathbb{Z}$, we obtain the inequality

$$\frac{p^2 \cdot d}{t} < 22\sqrt{2} \cdot (2p + 1). \tag{3.7}$$

It leads to $p \leq 61$ and $d \leq 59$.

When $\beta \in \mathbb{Z}$, we have that $(2\gamma + \beta)/t = f + \overline{\mathbf{1}}(f) \in O_F \cap K = O_K$, and this element is not in $\mathbb{Z}$. Thus Proposition 2.4 gives

$$4p/3 \leq \|(2\gamma + \beta)/t\|^2 \leq \|f\|^2 + \|\overline{\mathbf{1}}(f)\|^2 < 44.$$

Therefore $p \leq 61$. Now since

$$\beta\sqrt{-d}/t = f - \overline{\mathbf{1}}(f) \in O_F \cap k = O_k = \mathbb{Z}\left[\frac{1 + \sqrt{-d}}{2}\right],$$

we have $\beta/t = a \in \mathbb{Z}$. Hence (3.6) provides that $22 > \frac{d}{2}\|\frac{\beta}{t}\|_K^2 = \frac{3a^2 d}{2} \geq \frac{3d}{2}$, and thus $d \leq 11$. □

Proposition 3.4. *Assume there exists* $f \in O_k \backslash \mathbb{Z}$ *with* $\|f\|^2 < 22$. *Then* $d \in \{1, 2, 3, 7, 11\}$.

Proof. Since $f \in O_k \backslash \mathbb{Z}$, $f = m + n\delta$ for some $m, n \in \mathbb{Z}$, $n \neq 0$. If $d \equiv 1, 2 \mod 4$, $\|f\|^2 = 6(m^2 + n^2 d) < 22$, then $d \in \{1, 2\}$. When $d \equiv 3 \mod 4$, we have $\|f\|^2 = 6\left((m + n/2)^2 + n^2 d/4\right) < 22$, which implies $d \in \{3, 7, 11\}$. □

Proposition 3.5. *Assume there exists $f \in O_K \backslash \mathbb{Z}$ with $\|f\|^2 < 22$. Then $p \in \{7, 9, 13\}$.*

Proof. If $f \in O_K \backslash \mathbb{Z}$, $\|f\|^2 \geq 4p/3$ by Proposition 2.4. The result follows. □

Proposition 3.6. *Let $p \leq 61$ and $d \equiv 1, 2 \mod 4$ with $d \leq 22$. Assume that there exists $f \in O_F \backslash (O_K \cup O_k \cup \mu_F)$ such that $\|f\|^2 < 22$. Then $(p, d) \in \{(7, 1), (9, 1), (13, 1), (19, 1), (7, 2), (9, 2), (9, 6), (13, 13), (7, 14), (7, 21), (9, 21)\}$.*

Proof. We consider two cases and use a similar idea to the proof of Proposition 3.2. In the first case, when $\beta \in O_K \backslash \mathbb{Z}$, we have that $p^2 d/t \leq 11(2p+1)$. In the second case, $\beta \in \mathbb{Z}$. Since $2\|\gamma\|_K^2/t^2 + 2\|\beta\|_K^2 d/t^2 = \|f\|^2 < 22$, we have the bound $1/t^2(4p/3 + 6d) < 22$. Using these inequalities, we obtain the values for (p, d). □

Proposition 3.7. *Let $p \leq 61$ and $d \equiv 3 \mod 4, d \leq 59$. Assume there exists $f \in O_F \setminus (O_K \cup O_k \cup \mu_F)$ such that $\|f\|^2 < 22$. Then the possible values for (p, d) are:*

- *$(p, 3)$ with $p \in \{7, 9, 13, 19, 31, 37, 43\}$,*
- *$(p, 7)$ with $p \in \{7, 9, 13, 19, 31\}$, and*
- *$(7, 11)$, $(9, 11)$, $(13, 11)$, $(9, 15)$, $(19, 19)$, $(31, 31)$, $(7, 35)$, $(9, 39)$, $(13, 39)$, $(43, 43)$, $(9, 51)$.*

Proof. Either $p^2 d/t \leq 22\sqrt{2}(2p + 1)$ or $1/t^2(2p/3 + 3d) < 22$, yielding the result. □

4. Counting short elements

Given u, I and an Arakelov divisor $D = (I, u)$ of degree 0, we split the set $I \setminus \{0\}$ into three disjoint subsets, since each subset will be counted using different techniques:

$$S_1(I, u) = \{f \in I \setminus \{0\} : \|uf\|^2 < 6 \cdot 2^{1/3}\},$$
$$S_2(I, u) = \{f \in I \setminus \{0\} : 6 \cdot 2^{1/3} \leq \|uf\|^2 < 6 \cdot 3^{1/3}\}, \text{ and}$$
$$S_3(I, u) = \{f \in I \setminus \{0\} : \|uf\|^2 \geq 6 \cdot 3^{1/3}\}.$$

In this section, we determine an upper bound for the cardinality of the set of "short" elements in $S_2(I, u)$.

For any $f \in S_2(I, u)$, we have $|N(uf)| < 3$ since $\|uf\|^2 \geq 6 \cdot |N(uf)|^{1/3}$. As the degree of D is 0, $N(u) \cdot N(I) = 1$. Therefore $|N(f)|/N(I) =$

$|N(uf)| < 3$ and $|N(f)|/N(I) \in \{1,2\}$. We split $S_2(I,u)$ into two disjoint subsets according to whether $|N(f)|/N(I)$ is 1 or 2:

$$\text{(4.1)} \quad S_{2,i}(I,u) = \Big\{ f \in I : 6\cdot 2^{1/3} \leq \|uf\|^2 < 6\cdot 3^{1/3} \text{ and } |N(f)|/N(I) = i \Big\}.$$

Then,

$$S_2(I,u) = S_{2,1}(I,u) \cup S_{2,2}(I,u).$$

Lemma 4.1. *If O_K has a prime ideal of norm 2 and there exists $\epsilon \in O_F^\times$ with $\|\epsilon\|^2 < 81$, then $\epsilon \in \mu_F$.*

Proof. For the sake of contradiction, assume $\epsilon \notin \mu_F$. By Lemma 2.6, $\epsilon = \zeta\cdot\epsilon'$ for some $\zeta \in \mu_F$ and some $\epsilon' \in O_K^\times$. Now $81 > \|\epsilon\|^2 = \|\epsilon'\|^2 \geq 4p/3$ by Proposition 2.4. Thus $p \in \{7, 9, 13, 19, 31, 37, 43\}$. If O_K has an ideal of norm 2 then $p \in \{31, 43\}$. If $p = 31$, the regulator of K is $R_K \approx 12.196$. Since Λ is hexagonal (Remark 2.7), $\|\log(\epsilon)\|^2 \geq 2R_K \approx 24.392$. This leads to $\|\epsilon\|^2 \geq 225.615$, contradicting the condition $\|\epsilon\|^2 < 81$. Similarly, if $p = 43$, $R_K \approx 18.9218$. This leads to a contradiction, as $\|\epsilon\|^2 \geq 607.392$. □

Proposition 4.2. *Assume that $N(u) = 1/N(I)$.*

(i) *If $p < 31$, then $\#S_{2,2}(I,u) = 0$.*
(ii) *If $p \geq 31$, then $\#S_{2,2}(I,u) \leq 6 \cdot (\#\mu_F)$.*

Proof. Let $m_2 = \#S_{2,2}(I,u)$. Since $|N(f)|/N(I) = |N(uf)| = 2$ for all $f \in S_{2,2}$, $fO_F = PI$ for some ideal P in O_F with $N(P) = 2$. That is, each $f \in S_{2,2}$ corresponds to a prime ideal of norm 2 of O_F. If $m_2 > 0$, then O_F has a prime ideal of norm 2 and so does O_K.

(i). If $p \in \{7, 9, 13, 19\}$, O_K has no ideals of norm 2. Thus $m_2 = 0$.

(ii). If $p \geq 31$ then we have at most 6 distinct ideals of norm 2. Hence there are $m_2/6$ elements of $S_{2,2}$ which correspond to the same ideal of norm 2. Each of these elements must differ (pairwise) by a multiple of a unit. Thus there are $m_2/6$ distinct units; denote one of them by ϵ. Then $\epsilon = fg^{-1}$ for some $f, g \in S_{2,2}$, and

$$\begin{aligned}\|\epsilon\|^2 = \|fg^{-1}\|^2 &= 2\left(\frac{|u_1 f|^2}{|u_1 g|^2} + \frac{|u_2\tau_2(f)|^2}{|u_2\tau_2(g)|^2} + \frac{|u_3\tau_3(f)|^2}{|u_3\tau_3(g)|^2}\right)\\ &\leq 2\left(|u_1 f|^2 + |u_2\tau_2(f)|^2 + |u_3\tau_3(f)|^2\right)\left(\frac{1}{|u_1 g|^2} + \frac{1}{|u_2\tau_2(g)|^2} + \frac{1}{|u_3\tau_3(g)|^2}\right)\\ &\leq \|uf\|^2 \cdot \frac{\|ug\|^4}{4\cdot|N(ug)|} < 6\cdot 3^{1/3}\cdot\frac{(6\cdot 3^{1/3})^2}{8} = 81.\end{aligned}$$

If $m_2 > 0$, the above bound implies that those units are roots of unity by Lemma 4.1. Hence $m_2/6 \leq \#\mu_F$ and the result follows. □

Proposition 4.3. *Assume that $N(u) = 1$ and $m_1 = \#S_{2,1}(O_F, u)$. Then:*

(i) *if* $p < 31$*, then* $m_1 \leq 19 \cdot (\#\mu_F)$ *and*
(ii) *if* $p \geq 31$*, then* $m_1 \leq \#\mu_F$*.*

Proof. For all $f \in S_{2,1}(O_F, u)$, $f \in O_F$ and $|N(f)| = N(O_F) = 1$. Thus all elements in $S_{2,1}(O_F, u)$ are units. Let $\epsilon = fg^{-1}$ for two distinct elements $f, g \in S_{2,1}$. Then

$$\begin{aligned}\|\epsilon\|^2 = \|fg^{-1}\|^2 &= 2\left(\frac{|u_1 f|^2}{|u_1 g|^2} + \frac{|u_2\tau_2(f)|^2}{|u_2\tau_2(g)|^2} + \frac{|u_3\tau_3(f)|^2}{|u_3\tau_3(g)|^2}\right)\\ &= \|uf\|^2 \cdot \left(\frac{1}{|u_1 g|^2} + \frac{1}{|u_2\tau_3(g)|^2} + \frac{1}{|u_3\tau_3(g)|^2}\right)\\ &\leq 6 \cdot 3^{1/3} \cdot 5.15519 \approx 44.61.\end{aligned}$$

The last inequality is obtained because, if $x_1 \cdot x_2 \cdot x_3 = 1$ and $6 \cdot 2^{1/3} \leq 2 \cdot (x_1^2 + x_2^2 + x_3^2) < 6 \cdot 3^{1/3}$, then

$$\frac{1}{x_1^2} + \frac{1}{x_2^2} + \frac{1}{x_3^2} < 5.15519.$$

Hence there are m_1 distinct units ϵ with $\|\epsilon\|^2 \leq 44.61$. Assume that there exists such an ϵ where $\epsilon \notin \mu_F$. By Lemma 2.6, $\epsilon = \zeta \cdot \epsilon'$ for some $\zeta \in \mu_F$ and some $\epsilon' \in O_K^\times \backslash \{\pm 1\}$. Using Proposition 2.4, $44.61 > \|\epsilon\|^2 = \|\epsilon'\|^2 \geq 4p/3$. Thus $p \in \{7, 9, 13, 19, 31\}$, and:

- If $p \geq 37$, then all m_1 units ϵ belong to μ_F. It follows that $m_1 \leq \#\mu_F$.
- If $p \in \{7, 9, 13, 19, 31\}$, denote by m_1' the number of ϵ' up to sign, then $m_1 =$ (the number of such $\epsilon \in \mu_F$) + (the number of such $\epsilon \notin \mu_F$). Therefore an upper bound for m_1 is

$$m_1 \leq \#\mu_F + (\#\mu_F) \cdot m_1' = (\#\mu_F) \cdot (m_1' + 1). \tag{4.2}$$

We can find all $\epsilon' \in O_K \backslash \{\pm 1\}$ up to sign for which $\|\epsilon'\|_K^2 < 44.61/2$ (equivalently $\|\epsilon'\|^2 < 44.61$), and $|N_K(\epsilon')| = 1$ using an LLL-reduced basis [11, Section 12] of the lattice O_K or by applying the Fincke–Pohst algorithm [2, Algorithm 2.12]:

p	7	9	13	19	31
$m_1' \leq$	18	12	6	6	0

The result then follows by the bound for m_1 in (4.2). ☐

Proposition 4.4. *Assume that* $N(u) = 1$*,* $m_1 = \#S_{2,1}(O_F, u)$ *and* $\|u\|^2 \leq 6.4653$*.*

(i) *If* $p < 31$ *then* $m_1 \leq 12 \cdot (\#\mu_F)$*.*
(ii) *If* $p \geq 31$ *then* $m_1 = 0$*.*

Proof. First, we see that $S_{2,1}(O_F, u) \cap \mu_F = \emptyset$. This is because if there exists $f \in S_{2,1}(O_F, u) \cap \mu_F$, then $\|uf\|^2 = \|u\|^2 \leq 6.4653 < 6 \cdot 2^{1/3}$ which is a contradiction.

As every $f \in S_{2,1}(O_F, u)$ is a unit, we bound $\|f^{-1}\|$ as in the proof of Proposition 4.3:

$$\begin{aligned}\|f^{-1}\|^2 = \|u/uf\|^2 &= 2\left(\frac{|u_1|^2}{|u_1 f|^2} + \frac{|u_2|^2}{|u_2\tau_2(f)|^2} + \frac{|u_3|^2}{|u_3\tau_3(f)|^2}\right)\\ &= \|u\|^2 \cdot \left(\frac{1}{|u_1 f|^2} + \frac{1}{|u_2\tau_2(f)|^2} + \frac{1}{|u_3\tau_3(f)|^2}\right)\\ &\leq 6.4653 \cdot 5.15519 \approx 33.33.\end{aligned}$$

Thus there are m_1 units with squared length at most 33.33. Similar to the proof of Proposition 4.3, and using the fact that $S_{2,1}(O_F, u) \cap \mu_F = \emptyset$, we have $m_1 = (\#\mu_F) \cdot m_1'$ where

$$m_1' = \#\{\epsilon' \in O_K^\times \backslash \{\pm 1\} : \|\epsilon'\|_K^2 \leq 33.33/2\}.$$

When $p \geq 31$, then $m_1' = 0$ by Proposition 2.4. When $p < 31$, we compute the numbers m_1' and find

p	7	9	13	19
$m_1' \leq$	12	6	6	3

In these cases, $m_1' \leq 12$. Hence $m_1 \leq 12 \cdot (\#\mu_F)$. □

5. Road map for the proof of Theorem 1.1

In this section, we give a road map for the proof of Theorem 1.1. This proof requires us to consider several cases which we outline below. We seek to prove:

$$h^0(O_F, 1) > h^0(I, u) \text{ whenever } [(I, u)] \neq [(O_F, 1)].$$

The case where I is not principal is proved in Section 6 and is the shorter of the proofs. Sections 7 and 8 prove the theorem in the case where I is principal.

For an (Arakelov) divisor $D = (I, u)$, recall that $k^0(D) = \sum_{f \in I} e^{-\pi\|uf\|^2}$. Also recall $D_0 := (O_F, 1)$. Since $h^0(D) = \log(k^0(D))$, it is sufficient to prove:

$$k^0(D) < k^0(D_0) \text{ whenever } [D] \neq [D_0].$$

We split $k^0(D)$ into four summands:

$$\begin{aligned}&k^0(D) = 1 + \Sigma_1(I, u) + \Sigma_2(I, u) + \Sigma_3(I, u), \text{ where}\\ &\Sigma_i(I, u) = \sum_{f \in S_i(I, u)} e^{-\pi\|uf\|^2}, \; i \in \{1, 2, 3\}.\end{aligned} \tag{5.1}$$

In previous papers on the size function for number fields [3, 4, 15, 16], $k^0(D)$ was split into three summands which were then bounded to conclude $k^0(D) < k^0(D_0)$. The proof in this paper is more technical and requires four summands to find a sufficiently tight upper bound on $k^0(D)$. We bound them as follows:

- $\Sigma_1(I,u)$: We bound this sum twice, in Sections 6 and 7, obtaining different results depending whether I is principal.
- $\Sigma_2(I,u)$: This is bounded using results from Section 4. Establishing this bound is very different than techniques used in previous papers.
- $\Sigma_3(I,u)$: Bounding $\Sigma_3(I,u)$ is accomplished by applying Corollary 2.17.

5.1. Strategy for Section 6: *I* is not principal. We prove that $\Sigma_1(I,u) = 0$, thus getting a small upper bound on $k^0(D)$. The result follows quickly.

5.2. Strategy for Sections 7 and 8: *I* is principal. By Remark 2.15, when I is principal, we can assume that the class of divisors $[D]$ has the form $[(O_F, u)]$ for some $u \in \mathbb{R}^3_+$ and $N(u) = 1$. With the notation from Section 2, the vector u can be chosen such that $w = -\log u \in \mathcal{F}$. Therefore $w = \alpha_1 \cdot b_1 + \alpha_2 \cdot b_2$ for some $\alpha_1, \alpha_2 \in \left(-\frac{1}{2}, \frac{1}{2}\right]$.

To establish Theorem 1.1 we divide this case into subcases depending on $\|w\|$. When $\|w\|$ is sufficiently large we can bound $\Sigma_1(O_F, u)$ to obtain the result $k^0(D) < k^0(D_0)$ via Proposition 7.1. We use this method in Section 7, which considers the case where $\|w\| \geq 0.24163$. This is divided into two separate subcases in Sections 7.1 and 7.2 depending on the value of $\|w\|$, but the strategy remains similar for both cases.

Finally, in Section 8 we consider values of w with $0 < \|w\| < 0.24163$. Geometrically speaking, this is the case where u is close to 1, so that $k^0(D)$ and $k^0(D_0)$ are very close in value, which makes this case more difficult than the others. We cannot obtain a useful bound on $\Sigma_1(O_F, u)$ and we must approach this case differently than the others. Here we use a technique called "amplification"[1]. Instead of proving that $k^0(D) - k^0(D_0) < 0$, we consider the quantity

$$[k^0(D) - k^0(D_0)]/\|w\|^2$$

and prove it is negative. We divide by $\|w\|^2$ because $k^0(D) - k^0(D_0)$ may be extremely small, and this division scales it up to a value that is more tractable to bound. We split this quantity into three separate sums,

$$[k^0(D) - k^0(D_0)]/\|w\|^2 = T_1(u) + T_2(u) + T_3(u)$$

[1]We thank René Schoof for introducing this technique to us.

where $T_i(u)$, $i \in \{1,2,3\}$ are defined at the beginning of Section 8, and we prove that $T_1(u)+T_2(u)+T_3(u)<0$. The definition of these $T_i(u)$ values takes several lines to develop, hence we will not define them here. We will only note that these are defined differently than the $\Sigma_i(I,u)$ values used in the previous two sections. Thus the proofs in Section 8 rely on different techniques to establish, including the Galois properties of the fields. The bound for $T_3(u)$ uses the most innovative techniques and relies on Section 3. We prove Theorem 1.1 directly by applying Propositions 8.1 and 8.4–8.6.

6. Proof of Theorem 1.1 when I is not principal

When I is not principal, $|N(f)|/N(I) \geq 2$ for all $f \in I \backslash \{0\}$. Recall that $N(I)N(u)=1$ since $\deg(D)=0$. As a consequence,

$$\|uf\|^2 \geq 6|N(uf)|^{2/6} = 6|N(u)N(f)|^{1/3} = 6\left(\frac{|N(f)|}{N(I)}\right)^{1/3} \geq 6 \cdot 2^{1/3}.$$

This inequality holds for any nonzero $f \in I$. Therefore, the squared length of the shortest vectors of the lattice uI is $\lambda^2 \geq 6 \cdot 2^{1/3}$. This implies that $\Sigma_1(I,u)=0$ since $S_1(I,u)=\emptyset$, and that $\Sigma_3(I,u) < 2.6049 \cdot 10^{-9}$ by Corollary 2.17.

We now show that $\Sigma_2(I,u) \leq 6 \cdot (\#\mu_F) \cdot e^{-6 \cdot 2^{1/3}\pi}$. It is sufficient to find an upper bound for $\#S_2(I,u)$. First, we show that $S_{2,1}(I,u)=\emptyset$. This is because if $S_{2,1}(I,u)$ were to contain some $f \in I$, then $fO_F = I$, which contradicts the fact that I is not principal. Hence $\#S_2(I,u) = \#S_{2,2}(I,u)$ by (4.1). By Proposition 4.2, one has $\#S_{2,2}(I,u) \leq 6 \cdot (\#\mu_F)$. The upper bound for $\Sigma_2(I,u)$ is implied. It follows that

$$\begin{aligned} k^0(D) &= 1 + \Sigma_1(I,u) + \Sigma_2(I,u) + \Sigma_3(I,u) \\ &< 1 + 6 \cdot (\#\mu_F) \cdot e^{-6 \cdot 2^{1/3}\pi} + 2.6049 \cdot 10^{-9}. \end{aligned}$$

It is obvious that $k^0(D_0) > 1 + (\#\mu_F) \cdot e^{-6\pi}$. Therefore $k^0(D) < k^0(D_0)$ and Theorem 1.1 is proved when I is not principal.

7. Proof of Theorem 1.1 when I is principal and $\|w\| \geq 0.24163$

Proposition 7.1. *Let $D=(O_F,u)$ be a divisor of degree 0. Then $k^0(D_0) > k^0(D)$ if one of the following conditions holds:*

(i) $\Sigma_1(O_F,u) < (\#\mu_F) \cdot 4.28 \cdot 10^{-9}$, *or*
(ii) $\|u\|^2 \leq 6.4653$ *and* $\Sigma_1(O_F,u) < (\#\mu_F) \cdot 4.62 \cdot 10^{-9}$.

Proof. As $\deg(D)=0$, one has $N(u)=1$. For $f \in O_F \setminus \{0\}$, one has $|N(f)| \geq N(O_F)=1$, hence

$$\|uf\|^2 \geq 6|N(uf)|^{1/3} \geq 6|N(u)N(f)|^{1/3} = 6N(u)^{1/3}|N(f)|^{1/3} \geq 6.$$

Therefore, the length of the shortest vectors of the lattice uO_F is $\lambda \geq \sqrt{6}$. By Corollary 2.17, $\Sigma_3(O_F, u) < 2.6049 \cdot 10^{-9}$.

We have $\#S_2(O_F, u) = \#S_{2,1}(O_F, u) + \#S_{2,2}(O_F, u)$. By Propositions 4.2 and 4.3, $\#S_2(O_F, u) \leq 19 \cdot (\#\mu_F)$. As a consequence,

$$\Sigma_2(O_F, u) \leq (\#S_2(O_F, u)) \cdot e^{-6 \cdot 2^{1/3}\pi} \leq 19 \cdot (\#\mu_F) \cdot e^{-6 \cdot 2^{1/3}\pi}.$$

Substituting this into $k^0(D) = 1 + \Sigma_1(O_F, u) + \Sigma_2(O_F, u) + \Sigma_3(O_F, u)$, we have

$$k^0(D) < 1 + \Sigma_1(O_F, u) + 19 \cdot (\#\mu_F) \cdot e^{-6 \cdot 2^{1/3}\pi} + 2.6049 \cdot 10^{-9}.$$

Since $k^0(D_0) > 1 + (\#\mu_F) \cdot e^{-6\pi}$, to show $k^0(D_0) > k^0(D)$, it is sufficient to prove

$$\Sigma_1(O_F, u) < (\#\mu_F) \cdot \left(e^{-6\pi} - 19 \cdot e^{-6 \cdot 2^{1/3}\pi}\right) - 2.6049 \cdot 10^{-9}.$$

The right hand side is greater than $(\#\mu_F) \cdot 4.28 \cdot 10^{-9}$ because $\#\mu_F \geq 2$. Thus, the first statement (i) is proved. If $\|u\|^2 \leq 6.4653$, then Propositions 4.2 and 4.4 imply that $\#S_2(O_F, u) \leq 12 \cdot (\#\mu_F)$. Statement (ii) is then proved by using a similar argument. □

Proposition 7.1 is essential in proving the main theorem as shown below.

Remark 7.2. To prove Theorem 1.1, it is sufficient to show that $\Sigma_1(O_F, u) < (\#\mu_F) \cdot 4.28 \cdot 10^{-9}$ for all $w = (x, y, z) \neq (0, 0, 0)$.

Lemma 7.3. *Recall* $S_1(O_F, u) = \{f \in O_F^\times : \|uf\|^2 < 6 \cdot 2^{1/3}\}$. *For each* $f \in O_F \setminus \{0\}$, *define* $v_f = \log f$. *Then* $v_f \in \Lambda$ *for each* $f \in S_1(O_F, u)$.

Proof. Assume $f \in O_F \setminus \{0\}$ and $\|uf\|^2 < 6 \cdot 2^{1/3}$. Since $N(u) = 1$, $N(uf) = N(f)$. Thus

$$6 \cdot 2^{1/3} > \|uf\|^2 \geq 6|N(uf)|^{1/3} = 6|N(f)|^{1/3}.$$

This implies that $|N(f)| = 1$. That is, $f \in O_F^\times$. □

Let $w \in \mathcal{F}$. We consider two subcases in the next two subsections. As $w \in \mathcal{F}$ $\|w\| \leq \sqrt{3}\lambda/2$, where, from Lemma 2.10, one has $\lambda \geq 1.44975$.

7.1. Case $\mathbf{0.324096 \cdot \sqrt{2} < \|w\| \leq \sqrt{3}\lambda_1/2}$. As $0.324096\sqrt{2} < \|w\| = \|-\log u\|$, one obtains that $\|u\|^2 \geq 6.38985$. Let $f \in S_1(O_F, u)$. Then by Lemma 7.3, $v_f \in \Lambda$. It follows that

$$\|\log(uf)\| = \|\log f + \log u\| = \|v_f - w\|,$$

and $\|v_f - w\| < \lambda_1$ since otherwise $\|uf\|^2 > 6 \cdot 2^{1/3}$. Hence $f \in B(w)$. Therefore $S_1(O_F, u) \subset B(w)$. By Lemma 2.9,

$$S_1(O_F, u) \subset \{1, \mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3\} \cdot \mu_F \subset O_F^\times,$$

where

$\|\log \mathbf{x}_1 - w\| \geq 0.62776$, $\|\log \mathbf{x}_2 - w\| \geq 0.72487$ and $\|\log \mathbf{x}_3 - w\| \geq 1.25552$.

Since $\log \mathbf{x}_i - w = \log(u\mathbf{x}_i)$ for $1 \leq i \leq 3$, we have that

$$\|u\mathbf{x}_1\|^2 \geq 6.71608,\ \|u\mathbf{x}_2\|^2 \geq 6.94478 \text{ and } \|u\mathbf{x}_3\|^2 \geq 8.72718.$$

Thus $\|u\mathbf{x}_3\|^2 > 6 \cdot 2^{1/3}$, which implies $\mathbf{x}_3 \notin S_1(O_F, u)$ and $S_1(O_F, u) \subset \{1, \mathbf{x}_1, \mathbf{x}_2\} \cdot \mu_F$.

Then Theorem 1.1 is proved by Proposition 7.1 (i) and the inequality:

$$\begin{aligned}\Sigma_1(O_F, u) &\leq \sum_{f \in \{1, \mathbf{x}_1, \mathbf{x}_2\} \cdot \mu_F} e^{-\pi\|uf\|^2} \\ &= (\#\mu_F) \cdot \left(e^{-\pi\|u\|^2} + e^{-\pi\|u\mathbf{x}_1\|^2} + e^{-\pi\|u\mathbf{x}_2\|^2}\right) \\ &\leq (\#\mu_F) \cdot \left(e^{-6.38985\pi} + e^{-6.71608\pi} + e^{-6.94478\pi}\right) \\ &\approx (\#\mu_F) \cdot 2.5 \cdot 10^{-9}.\end{aligned}$$

7.2. Case $0.24163 \leq \|w\| \leq 0.324096 \cdot \sqrt{2}$. The bounds on $\|w\|$ give $6.11188 \leq \|u\|^2 \leq 6.4653$. For $f \in S_1(O_F, u) \backslash \mu_F$, one has $0 \neq v_f \in \Lambda$ by Lemma 7.3 and

$$\begin{aligned}\|\log(uf)\| = \|\log f + \log u\| = \|v_f - w\| &\geq |\|v_f\| - \|w\|| \\ &\geq \lambda_1 - 0.324096 \cdot \sqrt{2} \geq 0.9914.\end{aligned}$$

It follows that $\|uf\|^2 \geq 7.7265 > 6 \cdot 2^{1/3}$. Thus, $S_1(O_F, u) \subset \mu_F$ and

$$\begin{aligned}\Sigma_1(O_F, u) \leq \sum_{f \in \mu_F} e^{-\pi\|uf\|^2} = (\#\mu_F) \cdot e^{-\pi\|u\|^2} &\leq (\#\mu_F) \cdot e^{-6.11188\pi} \\ &\approx (\#\mu_F) \cdot 4.582 \cdot 10^{-9}.\end{aligned}$$

Theorem 1.1 is then established in this case using Proposition 7.1 (ii).

8. Proof of Theorem 1.1 when I is principal and $0 < \|w\| < 0.24163$

We first fix the following notation, which will be used but not re-stated in lemmas and propositions throughout this section: Given any $u \in \mathbb{R}_+^3$, let $x, y, z \in \mathbb{R}$ be such that $u = (e^x, e^y, e^z)$. Then $w = -\log u = (-x, -y, -z) \in \mathbb{R}^3$ and $x + y + z = 0$.

For any $f \in O_F$, we define $f_i = |\tau_i(f)|$, $i \in \{1, 2, 3\}$. Then

$$\begin{aligned}\|uf\|^2 &= 2\left(e^{2x}|\tau_1(f)|^2 + e^{2y}|\tau_2(f)|^2 + e^{2z}|\tau_3(f)|^2\right) \\ &= 2\left(f_1^2 e^{2x} + f_2^2 e^{2y} + f_3^2 e^{2z}\right).\end{aligned}$$

For $f \in O_F$ we now define

$$G(u,f) = e^{-\pi\|f\|^2} G_2(f,u)/\|w\|^2,$$

where

$$G_1(u,f) = e^{-\pi[\|uf\|^2-\|f\|^2]} - 1 = e^{-2\pi[(e^{2x}-1)f_1^2+(e^{2y}-1)f_2^2+(e^{2z}-1)f_3^2]} - 1,$$
$$G_2(u,f) = G_1(u,\tau_1(f)) + G_1(u,\tau_2(f)) + G_1(u,\tau_3(f)).$$

We then use $G(u,f)$ to define

$$T_1(u) = \sum_{f\in\mu_F} G(u,f) = (\#\mu_F)\cdot G(u,1),$$
$$T_2(u) = \sum_{f\in O_F,\, \|f\|^2\geq 22} G(u,f),$$
$$T_3(u) = \sum_{f\in O_F\setminus\mu_F,\, \|f\|^2<22} G(u,f).$$

Proposition 8.1. *Theorem 1.1 holds if and only if* $T_1(u)+T_2(u)+T_3(u) < 0$ *for all* $u = (e^x, e^y, e^z) \neq (1,1,1)$.

Proof. Since $3[k^0(D) - k^0(D_0)]/\|w\|^2 = \sum_{f\in O_F} G(u,f) = T_1(u) + T_2(u) + T_3(u)$ by [16, Proposition 4.1], the result follows. □

We now establish Theorem 1.1 in this case by proving several results which are achieved using the Galois property of F, the Taylor expansion of e^t, and the symmetry of $G_2(u,f)$.

Lemma 8.2. *For all* $u \in \mathbb{R}_+^3$ *and* $f \in O_F$,

$$G(u,\tau_1(f)) = G(u,\tau_2(f)) = G(u,\tau_3(f)).$$

Proof. This can be seen from the formulas of $G(u,\tau_i(f))$, $i \in \{1,2,3\}$ and the fact that $\|\tau_1(f)\| = \|\tau_2(f)\| = \|\tau_3(f)\|$ for all $f \in O_F$. □

Proposition 8.3. *Let* $\|w\|^2 = 2(x^2+y^2+z^2) > 0$. *Then for all* $f \in O_F$,

$$G(u,f) \leq 4\pi^2\|f^2\|^2 e^{-\pi\|f\|^2}\left(1 + \frac{1}{2}e^{2\pi\|w\|\|f^2\|}\right).$$

In particular, if $f \in O_F$ *with* $\|f\|^2 \geq 22$ *then*

$$G(u,f) \leq 2\pi^2\left(e^{-(\pi-2/7)\|f\|^2} + \frac{1}{2}e^{-(\pi-2\pi\|w\|-2/7)\|f\|^2}\right).$$

Proof. The first inequality is from [16, Proposition 4.2]. The second is obtained from the first combined with

$$\|f^2\|^2 \leq \frac{1}{2}\|f\|^4 \leq \frac{1}{2}e^{2\|f\|^2/7} \text{ and } \|f^2\| \leq \|f\|^2 \text{ for all } \|f\|^2 \geq 22. \quad \square$$

Proposition 8.4. *If* $\|w\|^2 \in (0, 0.24163^2)$, *then*

$$T_1(u) < -98.4664\cdot 10^{-9}\cdot(\#\mu_F).$$

Proof. As $T_1(u) = (\#\mu_F) \cdot G(u,1)$, it is sufficient to prove $G(u,1) < -98.4664 \cdot 10^{-9}$. Since $0 < \|w\| < 0.24163$,

$$2(e^{2x} + e^{2y} + e^{2z} - 3) \geq 1.9 \cdot 2(x^2 + y^2 + z^2) = 1.9\|w\|^2.$$

Consequently,

$$G_1(u,1) = e^{-2\pi[e^{2x}+e^{2y}+e^{2z}-3]} - 1 \leq e^{-1.9\pi\|w\|^2} - 1.$$

The bounds on $\|w\|$ also imply

$$G_2(u,1)/\|w\|^2 = 3G_1(u,1)/\|w\|^2 \leq 3[e^{-1.9\pi\|w\|^2} - 1]/\|w\|^2 < -15.1198.$$

Therefore $G(u,1) = e^{-6\pi} G_2(u,1)/\|w\|^2 < -98.4664 \cdot 10^{-9}$. □

Proposition 8.5. *If* $\|w\|^2 \in (0, 0.24163^2)$ *then* $T_2(u) < 2.19278 \cdot 10^{-9}$.

Proof. By Proposition 8.3, one has

$$T_2(u) \leq 2\pi^2 \sum_{f \in O_F,\, \|f\|^2 \geq 22} e^{-(\pi - 2/7)\|f\|^2} + \pi^2 \sum_{f \in O_F,\, \|f\|^2 \geq 22} e^{-(\pi - 2\pi\|w\| - 2/7)\|f\|^2}.$$

The first sum is at most 10^{-23} by Corollary 2.17. Further, since $\|w\| < 0.24163$, one has

$$\pi - 2\pi\|w\| - 2/7 \geq \pi - 2 \cdot 0.24163\,\pi - 2/7.$$

The second sum is then bounded by $2.19277 \cdot 10^{-9}$ by Corollary 2.17. Thus $T_2(u) \leq 2.19278 \cdot 10^{-9}$. □

Bounding $T_3(u)$ is more technical than bounding $T_1(u)$ and $T_2(u)$. We bound $T_3(u)$ in the following proposition.

Proposition 8.6. *If* $\|w\|^2 \in (0, 0.24163^2)$ *then*

$$T_3(u) < 98.4664 \cdot 10^{-9} \cdot (\#\mu_F) - 2.19278 \cdot 10^{-9}.$$

Proof. Since $\#\mu_F \geq 2$, we have

$$98.4664 \cdot 10^{-9} \cdot (\#\mu_F) - 2.19278 \cdot 10^{-9} > 1.9474 \cdot 10^{-7}.$$

Therefore it is sufficient prove $T_3(u) < 1.9474 \cdot 10^{-7}$. For $f \in O_F$ define the lengths l_1 and l_2 by $l_1 = \|f\|^2$ and $l_2 = \|f^2\|^2$. For $\|w\| \in (0, 0.24163)$ apply Proposition 8.3 to bound $G(u,f)$ as a function of l_1 and l_2:

$$G(u,f) \leq \mathcal{G}(l_1, l_2) := 4\pi^2 l_2 e^{-\pi l_1}\left(1 + \frac{1}{2} e^{2\pi \cdot 0.24163\sqrt{l_2}}\right). \tag{8.1}$$

Based on the results of Section 3, we divide our proof into four cases.

Case (1). $p > 61$ and either

- $d \equiv 1, 2 \mod 4$ and $d > 22$, or
- $d \equiv 3 \mod 4$ and $d > 59$.

Using the result in Section 3, one can show that $T_3(u) = 0$ for these values.

Case (2). $p > 61$ and either

- $d \equiv 1, 2 \mod 4$ and $d \leq 22$, or
- $d \equiv 3 \mod 4$ and $d \leq 59$.

If $d > 11$, then $T_3(u) = 0$. If $d \leq 11$, $d \in \{1, 2, 3, 7, 11\}$. If $d \in \{1, 2\}$, then any $f \in O_k$ has the form $m + n\sqrt{-d}$, and $\|f\|^2 = 6(m^2 + n^2 d)$. When $d = 1$, $f \in \{\pm 1 \pm i\}, f^2 \in \{\pm 2i\}$, and $\|f\|^2 = 12$, $\|f^2\|^2 = 24$. As a result, one has $T_3(u) \leq 4 \cdot \mathcal{G}(12, 24) \approx 1.4 \cdot 10^{-10}$. Similarly, if $d = 2$, then either $f = \pm 1 \pm \sqrt{-2}$ or $f = \pm\sqrt{-2}$. When $f = \pm 1 \pm \sqrt{-2}$ we have $f^2 = -1 \pm 2\sqrt{-2}$, $\|f\|^2 = 18$ and $\|f^2\|^2 = 54$. When $f = \pm\sqrt{-2}$, then $f^2 = 2$. Thus $\|f\|^2 = 12$ and $\|f^2\|^2 = 24$. As a consequence, $T_3(u) \leq 4 \cdot \mathcal{G}(18, 54) + 2 \cdot \mathcal{G}(12, 24) < 10^{-10}$. For $d \in \{3, 7, 11\}$, we do the same computation. If $d = 3$: $f \in \{\pm 3/2 \pm \sqrt{-3}/2, \pm\sqrt{-3}\}$ and $T_3(u) \leq 6 \cdot \mathcal{G}(18, 54) < 10^{-10}$. If $d = 7$: $f \in \{\pm 1/2 \pm \sqrt{-7}/2\}$ and $T_3(u) \leq 4 \cdot \mathcal{G}(12, 24) < 1.4 \cdot 10^{-10}$. If $d = 11$: $f \in \{\pm 1/2 \pm \sqrt{-11}/2\}$ and $T_3(u) \leq 4 \cdot \mathcal{G}(18, 54) < 10^{-10}$.

Case (3). $p \leq 61$ and either

- $d > 22$ with $d \equiv 1, 2 \mod 4$ or
- $d > 59$ with $d \equiv 3 \mod 4$.

Section 3 implies $T_3(u) = 0$ for $p > 13$. Therefore, we only consider $p \in \{7, 9, 13\}$. For each of these values for p there is exactly one cyclic cubic field K with conductor p. We can find all vectors $f \in O_K \backslash \{0\}$ for which $\|f\|_K^2 < 11$, equivalently, $\|f\|^2 < 22$ using an LLL-reduced basis of the lattice O_K [11, Section 12] or by applying the Fincke–Pohst algorithm [2, Algorithm 2.12]). We first consider $p = 7$. There are 18 elements $f \in O_K \backslash \{0\}$ such that $\|f\|^2 < 22$:

$\|f\|^2$	$\|f^2\|$	Number of elements f
10	26	6
12	52	6
20	132	6

Therefore,

$$T_3(u) \leq 6 \cdot \mathcal{G}(10, 26) + 6 \cdot \mathcal{G}(12, 52) + 6 \cdot \mathcal{G}(20, 132) < 1.76 \cdot 10^{-7}.$$

For $p = 9$, we do a similar computation and obtain,

$$T_3(u) \leq 6 \cdot \mathcal{G}(12, 36) + 6 \cdot \mathcal{G}(18, 98) + 6 \cdot \mathcal{G}(18, 138) < 1.64 \cdot 10^{-9}.$$

When $p = 13$, one has $T_3(u) \leq 6 \cdot \mathcal{G}(18, 106) + 6 \cdot \mathcal{G}(84, 120) < 3 \cdot 10^{-14}$.

Case (4). $p \leq 61$ and either

- $d \equiv 1, 2 \mod 4$ and $d \leq 22$, or
- $d \equiv 3 \mod 4$ and $d \leq 59$.

Let $\mathcal{L}_1 = \{(7,1),\ (9,1),\ (13,1),\ (19,1),\ (7,2),\ (9,2),\ (9,6),\ (13,13),\ (7,14),\ (7,21),\ (9,21)\}$, and $\mathcal{L}_2 = \{(7,3),\ (9,3),\ (13,3),\ (19,3),\ (31,3),\ (37,3),\ (43,3),\ (7,7),\ (9,7),\ (13,7),\ (19,7),\ (31,7),\ (7,11),\ (9,11),\ (13,11),\ (9,15),\ (19,19),\ (31,31),\ (7,35),\ (9,39),\ (13,39),\ (43,43),\ (9,51)\}$.

By Proposition 3.6, if (p,d) is not in $\mathcal{L}_1 \cup \mathcal{L}_2$, then

$$T_3(u) \le \sum_{f \in O_k \setminus \mu_F,\, \|f\|^2 < 22} G(u,f) + \sum_{f \in O_K \setminus \mu_F,\, \|f\|^2 < 22} G(u,f).$$

The first sum is nonzero when $d \in \{1,2,3,7,11\}$ by Proposition 3.4 and the second is nonzero when $p \in \{7,9,13\}$ by Proposition 3.5. These sums are at most $1.4 \cdot 10^{-10}$ (see Case (2)) and $1.76 \cdot 10^{-7}$ (see Case (3)), respectively. Thus $T_3(u) < 1.9474 \cdot 10^{-7}$. We now consider the cases in which $(p,d) \in \mathcal{L}_1 \cup \mathcal{L}_2$. Using an LLL-reduced basis of the lattice O_F viewed as a lattice in $\mathbb{R}^6$ [11, Section 12] or by applying the Fincke–Pohst algorithm [2, Algorithm 2.12]), we first list all elements $f \in O_F$ such that $\|f\|^2 < 22$. After that, we compute the function $\mathcal{G}(l_1, l_2)$ to find an upper bound for $T_3(u)$ using Proposition 8.3 as done in Case (2). The results are shown in Table 8.1. When $(p,d) \in \{(7,7),(7,3),(7,1)\}$, the number of roots of unity of F is $\#\mu_F \in \{14,6,4\}$ respectively. Therefore, in these cases we still have that $T_3(u) < 98.4664 \cdot 10^{-9} \cdot (\#\mu_F) - 2.19278 \cdot 10^{-9}$ as desired. For other values of (p,d) in Table 8.1, $T_3(u) < 1.9474 \cdot 10^{-7}$. ☐

9. A comparison to previous work

Compared to previous papers [3, 4, 15, 16], many of the details of our proofs are more technical and required us to develop new techniques, though the overall structure of our proof is similar to previous work. In terms of structural similarity, we considered the case where I is principal separately from the case where it is not. When I is principal, we subdivide further based on the length of $w = -\log(u)$.

The techniques that are unique to this paper are:

- We split $h^0(D)$ into three summations instead of two as in previous papers. The reason is that the upper bound for

  $$\sum_{f \in I, \|uf\|^2 > 6 \cdot 2^{1/3}} e^{-\pi \|uf\|^2}$$

  obtained by Lemma 2.16 is too large to be useful for imaginary cyclic sextic fields. To solve this problem, we split this sum into $\Sigma_2 + \Sigma_3$ (see 5.1) and find an efficient bound for Σ_2. We compute this bound in Section 6 and the proof of Lemma 7.1. The bound is a multiple of $\#\mu_F$. To bound Σ_2, we find an upper bound for $\#S_2$, which is the primary goal of Section 4 (see Propositions 4.2, 4.3, 4.4). These bounds are not given in previous work. Further, when I is principal, Σ_1 can be bounded by a multiple of $\#\mu_F$, minus a constant (see Lemma 7.1).

Table 8.1. Computing an upper bound for $T_3(u)$ for $(p,d) \in \mathcal{L}_1 \cup \mathcal{L}_2$

(p,d)	$\|f\|^2$	$\|f^2\|$	# elements f	$T_3(u) \leq$	(p,d)	$\|f\|^2$	$\|f^2\|$	# elements f	$T_3(u) \leq$
$(7,1)$	10	26	12	$3.5200 \cdot 10^{-7}$	$(7,3)$	10	26	18	$5.2784 \cdot 10^{-7}$
	12	24	4			12	52	18	
	12	52	12			14	42	36	
	16	52	24			16	52	36	
	18	82	24			18	54	6	
	20	76	24			18	82	36	
	20	104	12			20	132	18	
	20	132	12						
$(9,1)$	12	24	4	$3.4064 \cdot 10^{-9}$	$(9,3)$	12	36	108	$2.9425 \cdot 10^{-8}$
	12	36	12			18	54	18	
	18	66	24			18	66	108	
	18	90	12			18	90	54	
	18	138	12			18	138	54	
$(13,1)$	12	24	4	$1.3672 \cdot 10^{-9}$	$(13,3)$	18	54	6	$6.4034 \cdot 10^{-14}$
	18	106	12			18	106	18	
	20	84	12			20	84	18	
$(19,1)$	12	24	4	$1.3668 \cdot 10^{-10}$	$(19,3)$, $(31,3)$,	18	54	6	$1.2367 \cdot 10^{-16}$
					$(37,3)$ or $(43,3)$				
$(7,2)$	10	26	6	$1.7600 \cdot 10^{-7}$	$(7,7)$	10	26	42	$1.2326 \cdot 10^{-6}$
	12	24	2			12	24	28	
	12	52	6			12	52	42	
	18	54	4			14	42	42	
	20	104	6			20	76	84	
	20	132	6			20	104	84	
						20	132	42	
$(9,2)$	12	24	2	$1.7032 \cdot 10^{-9}$	$(9,7)$	12	24	4	$1.7716 \cdot 10^{-9}$
	12	36	6			12	36	6	
	18	54	4			18	90	6	
	18	90	6			18	138	6	
	18	138	6						
$(9,6)$	12	36	6	$1.6349 \cdot 10^{-9}$	$(13,7)$	12	24	4	$1.3670 \cdot 10^{-10}$
and	18	90	6			18	106	6	
$(9,21)$	18	138	6			20	84	6	
$(13,13)$	18	106	6	$2.1304 \cdot 10^{-14}$	$(7,14)$	10	26	6	$1.7593 \cdot 10^{-7}$
	20	84	6		and	12	52	6	
					$(7,21)$	20	132	6	

- In this paper $T_1(u)$ (Proposition 8.4) and $T_3(u)$ (Proposition 8.6), depend on a multiple of $\#\mu_F$, in contrast to the cyclic cubic case [16]. Using $\#\mu_F$ is necessary to show that $T_1(u) + T_2(u) + T_3(u) < 0$.
- To compute an efficient upper bound for $T_3(u)$, we bound the discriminant Δ_F of F. Previous papers have used two different approaches to achieve this goal:

  (1) The complex quartic case: This case uses a short fundamental unit ε to bound Δ_F, where $\|\varepsilon\|^2 < 1 + \sqrt{2}$ [15, Lemma 6.3]. In the imaginary cyclic sextic case, we cannot take this approach because the unit group of F depends on p but not d (see Lemma 2.6) and hence does not depend on Δ_F. Therefore we cannot bound for Δ_F based on the size of the units of F. When p is fixed, the fundamental units are fixed, yet we can make Δ_F as large as we want by choosing a large value for d (Lemma 3.1).

  (2) The cyclic cubic case: This case uses the existence of short elements $f \in O_F \backslash \mu_F$ with $\|f\|^2 < 10$ [16, Proposition 2.3]. For imaginary cyclic sextic fields there was no existing result to bound the length of an element in O_F in terms of Δ_F, so we develop this in Section 3. We show that if F has short elements $f \in O_F \backslash \mu_F$, where short means that $\|f\|^2 < 22$, then one of three things holds: (i) $p \leq 61$ and $d \leq 59$, (ii) f is in the quadratic subfield $k = \mathbf{Q}(\sqrt{-d})$ with $d \leq 11$, or (iii) f is in the cubic subfield K with conductor $p \leq 13$. Using upper bounds for p and d, we can list all imaginary cyclic sextic fields in which there exist elements $f \in O_F \backslash \mu_F$ with $\|f\|^2 < 22$. For each such field, we compute these short elements and make use of the function $\mathcal{G}$ in (8.1) to find an upper bound for $T_3(u)$ (see Table 8.1).

References

[1] E. Artin, "Die gruppentheoretische Struktur des Diskriminanten algebraischer Zahlkörper.", *J. Reine Angew. Math.* **164** (1931), p. 1-11.

[2] U. Fincke & M. Pohst, "Improved methods for calculating vectors of short length in a lattice, including a complexity analysis", *Math. Comput.* **44** (1985), no. 170, p. 463-471.

[3] P. Francini, "The size function h^0 for quadratic number fields", *J. Théor. Nombres Bordeaux* **13** (2001), no. 1, p. 125-135, 21st Journées Arithmétiques (Rome, 2001).

[4] ———, "The size function h° for a pure cubic field", *Acta Arith.* **111** (2004), no. 3, p. 225-237.

[5] G. van der Geer & R. Schoof, "Effectivity of Arakelov divisors and the theta divisor of a number field", *Sel. Math., New Ser.* **6** (2000), no. 4, p. 377-398.

[6] R. P. Groenewegen, "The size function for number fields", PhD Thesis, Universiteit van Amsterdam, 1999.

[7] ———, "An arithmetic analogue of Clifford's theorem", *J. Théor. Nombres Bordeaux* **13** (2001), no. 1, p. 143-156, 21st Journées Arithmétiques (Rome, 2001).

[8] H. Hasse, "Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage", *Math. Z.* **31** (1930), no. 1, p. 565-582.

[9] H. Hasse & J. Martinet, *Über die Klassenzahl abelscher Zahlkorper*, vol. 195, Citeseer, 1952.

[10] M. Hirabayashi & K.-i. Yoshino, "Remarks on unit indices of imaginary abelian number fields", *Manuscr. Math.* **60** (1988), no. 4, p. 423-436.

[11] H. W. Lenstra, Jr, "Lattices", in *Algorithmic number theory: lattices, number fields, curves and cryptography*, Mathematical Sciences Research Institute Publications, vol. 44, Cambridge University Press, 2008, p. 127-181.

[12] The PARI Group, "PARI/GP version `2.13.4`", 2022, available from `http://pari.math.u-bordeaux.fr/`.

[13] R. Schoof, "Computing Arakelov class groups", in *Algorithmic number theory: lattices, number fields, curves and cryptography*, Mathematical Sciences Research Institute Publications, vol. 44, Cambridge University Press, 2008, p. 447-495.

[14] H. T. N. Tran, "Computing dimensions of spaces of Arakelov divisors of number fields", *Int. J. Number Theory* **13** (2017), no. 2, p. 487-512.

[15] ———, "The size function for quadratic extensions of complex quadratic fields", *J. Théor. Nombres Bordeaux* **29** (2017), no. 1, p. 243-259.

[16] H. T. N. Tran & P. Tian, "The size function for cyclic cubic fields", *Int. J. Number Theory* **14** (2018), p. 399-415.

[17] Wolfram Research, Inc., "Mathematica, Version 13.1", Champaign, IL, 2022.

Ha Thanh Nguyen Tran
Department of Mathematical and Physical Sciences
Concordia University of Edmonton
7128 Ada Blvd NW
Edmonton, AB T5B 4E4, Canada
E-mail: `hatran1104@gmail.com`

Peng Tian
Department of Mathematics
East China University of Science and Technology
Meilong Road 130
200237, Shanghai, P. R. China
E-mail: `tianpeng@ecust.edu.cn`

Amy Feaver
Department of Mathematics and Computer Science
Gordon College
255 Grapevine Rd
Wenham, MA 01984, United States
E-mail: `mathfeaver@gmail.com`