JOURNAL de Théorie des Nombres de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Unit Reducible Fields and Perfect Unary Forms II. Cyclotomic Fields

par Christian PORTER, Cong LING, Piero SARTI et Alar LEIBAK

RÉSUMÉ. Dans cet article, nous poursuivons l'étude des corps réductibles à l'unité, telle qu'introduite dans [10] pour le cas particulier des corps cyclotomiques. Plus précisément, nous en déduisons que les corps cyclotomiques des conducteurs $3, 4, 5, 7, 8, 9, 12, 15$ sont tous réductibles à l'unité, et montrons que tout corps cyclotomique de conducteur N n'est pas réductible à l'unité si 2^4, 3^3, $5^2, 7^2, 11^2$ ou tout nombre premier $p \geq 13$ divise N, ce qui signifie que les corps cyclotomiques réductibles à l'unité sont en nombre fini. Enfin, si a est un élément totalement positif d'un corps cyclotomique, nous montrons que pour tout a' équivalent, l'écart entre $\mathrm{Tr}_{K/\mathbb{Q}}(a')$ et le plus court élément non nul de la forme quadratique $\mathrm{Tr}_{K/\mathbb{Q}}(axx^*)$ où x est tiré de l'anneau des entiers tend vers l'infini lorsque le conducteur N tend vers l'infini.

ABSTRACT. In this paper, we continue the study of unit reducible fields as introduced in [10] for the special case of cyclotomic fields. Specifically, we deduce that the cyclotomic fields of conductors $3, 4, 5, 7, 8, 9, 12, 15$ are all unit reducible, and show that any cyclotomic field of conductor N is not unit reducible if $2^4, 3^3, 5^2, 7^2, 11^2$ or any prime $p \geq 13$ divide N, meaning the unit reducible cyclotomic fields are finite in number. Finally, if a is a totally positive element of a cyclotomic field, we show that for all equivalent a', the discrepancy between $\mathrm{Tr}_{K/\mathbb{Q}}(a')$ and the shortest nonzero element of the quadratic form $\mathrm{Tr}_{K/\mathbb{Q}}(axx^*)$ where x is taken from the ring of integers tends to infinity as the conductor N goes to infinity.

1. Introduction

Let K be a Galois extension of $\mathbb{Q}$ of degree n, where n is either r if K is totally real or $2s$ if K is totally complex, for some integers r or $2s$. Associate to K the canonical embeddings $\sigma_1, \ldots, \sigma_n$ into $\mathbb{R}$ if K is totally real, or into $\mathbb{C}$, if K is totally complex. We define a quadratic form $f : K^m \to K$ by

$$f(x_1, \ldots, x_m) = \sum_{k,l=1}^{m} f_{k,l} x_k x_l^*,$$

where $f_{k,l} \in K$ and $*$ denotes complex conjugation if K is totally complex, or fixes x_l if K is totally real. Usually, we take $f_{k,l} = f_{l,k}^*$ for all k, l. f is said to be positive definite if

$$\sigma_i(f)(x_1, \ldots, x_m) = \sum_{k,l} \sigma_i(f_{k,l})\sigma_i(x_k)\sigma_i(x_l)^*$$

is a real positive definite quadratic form or positive definite hermitian form, for all $1 \leq i \leq n$. From now on, we will assume all quadratic forms are positive-definite and simply refer to them as quadratic forms.

A quadratic form f is called a unary form if it is defined in a single variable in K, i.e. the quadratic form takes the form axx^*. We say that the element a is totally positive if $\sigma_i(a) \in \mathbb{R}_{>0}$ for all $1 \leq i \leq n$. We denote the set of totally positive elements of K by $K_{\gg 0}$. Let $\mathcal{O}_K$ and $\mathcal{O}_K^*$ respectively denote the ring of integers and unit group of K. Then for any $a \in K_{\gg 0}$, we will use the notation

$$\mu(a) = \min_{x \in \mathcal{O}_K \setminus \{0\}} \mathrm{Tr}_{K/\mathbb{Q}}(axx^*),$$
$$\mu^*(a) = \min_{u \in \mathcal{O}_K^*} \mathrm{Tr}_{K/\mathbb{Q}}(auu^*),$$
$$\mathcal{M}(a) = \{x \in \mathcal{O}_K : \mathrm{Tr}_{K/\mathbb{Q}}(axx^*) = \mu(a)\}.$$

We say that a is reduced if $\mathrm{Tr}_{K/\mathbb{Q}}(auu^*) \geq \mathrm{Tr}_{K/\mathbb{Q}}(a)(= \mu^*(a))$ for all $u \in \mathcal{O}_K^*$. Note that the set $\{auu^* : u \in \mathcal{O}_K^*\}$ induces an equivalence class for each totally positive a. The set $\mathcal{F}_K$ denotes the set of all reduced totally positive elements of K, which we refer to as the reduction domain of K. This leads us to the following definition:

Definition 1.1. A number field K is said to be unit reducible if $\mu(a) = \mu^*(a)$ for all $a \in K_{\gg 0}$ - that is, every totally positive a attains its trace-minimum at a unit.

In [10], it was shown that a real quadratic field $\mathbb{Q}(\sqrt{d})$ is unit reducible if and only if d took one of the following forms:

$$d = m^2 + 1, \ m \in \mathbb{N}, \ m \text{ odd},$$
$$d = m^2 - 1, \ m \in \mathbb{N}, \ m \text{ even},$$
$$d = m^2 + 4, \ m \in \mathbb{N}, \ m \text{ even},$$
$$d = m^2 - 4, \ m \in \mathbb{N}, \ m > 3 \text{ odd}.$$

Moreover, it was shown that the cubic field with defining polynomial

$$x^3 - tx^2 - (t+3)x - 1, \ t \in \mathbb{Z}_{\geq 0},$$

is unit reducible if the field is monogenic. Specifically, we will call a unit reducible field K strongly unit reducible if $\mathcal{M}(a) \subset \mathcal{O}_K^*$ for all totally positive a and weakly unit reducible field otherwise.

We define by $\zeta_N = \exp(2\pi i/N)$ a primitive Nth root of unity. We consider the field $K = \mathbb{Q}(\zeta_N)$, which has degree $\phi(N)$ over $\mathbb{Q}$. We will use the notation $K_N = \mathbb{Q}(\zeta_N)$ from now on.

We define the reduction discrepancy of a field by the quantity

$$\delta_K = \sup_{a \in K_{\gg 0}} \frac{\mu^*(a)}{\mu(a)}.$$

Clearly $\delta_K \geq 1$ for every field K, and if $\delta_K = 1$ then K is unit reducible.

Finally, we define the Hermite constant of the number field K by

$$\gamma_K = \sup_{a \in K_{\gg 0}} \frac{\mu(a)}{\mathrm{Nm}_{K/\mathbb{Q}}(a)^{1/n}}.$$

For any positive definite real quadratic form $q(x_1, \ldots, x_n)$ of rank n, we define by

$$\gamma(q) = \frac{\min_{(x_1, \ldots, x_n) \in \mathbb{Z}^n \setminus (0, \ldots, 0)} q(x_1, \ldots, x_n)}{\det(q)^{1/n}},$$

where $\det(q)$ is the determinant of the matrix $Q = \{q_{i,j}\}_{1 \leq i,j \leq n}$, where $q(x_1, \ldots, x_n) = \sum_{i,j=1}^n q_{i,j} x_i x_j$. Then the Hermite constant $\gamma_n = \max_q \gamma(q)$, where the maximum is taken over all positive definite real quadratic forms q.

1.1. Motivation. In this paper, we are concerned with unit reducible cyclotomic fields. Cyclotomic fields are of significant importance in the field of post-quantum cryptography, underpinning the security and enjoying efficient implementation of mainstream lattice-based cryptosystems (see e.g. [12, 17]). In July 2022, the US National Institute of Standards and Technology (NIST) announced the selection of four post-quantum cryptographic algorithms to be standardized, three of which are based on cyclotomic fields [14]. Lattice-based cryptography relies on the hardness of the "shortest vector problem" (SVP), where an adversary tries to find a shortest nonzero vector in a given lattice. A common strategy of attack is to run lattice reduction over these number fields to find short vectors. Some cyclotomic lattice cryptosystems make use of principal ideals (see e.g. [2, 4, 7, 16]). The study of principal ideals as lattices has a natural correspondence with the theory of unary forms. Finding the smallest nonzero value of a unary quadratic form gives the shortest vector of such a lattice.

Specifically, the recovery of short generators of principal ideals in cyclotomic fields was studied in [3], where the length of ideal elements was measured by their length under the canonical embedding. Let $\mathcal{I}$ be a principal ideal in some number field K with ring of integers $\mathcal{O}_K$. If we denote by g a generator of $\mathcal{I}$, then solving the shortest generator problem (as in the setting of [3]) corresponds to finding a unit $u \in \mathcal{O}_K^*$ such that

$$\mathrm{Tr}_{K/\mathbb{Q}}(auu^*) = \mu^*(a),$$

where $a = gg^*$, and solving the shortest vector problem in $\mathcal{I}$ corresponds to finding $x \in \mathcal{O}_K$ such that

$$\text{Tr}_{K/\mathbb{Q}}(axx^*) = \mu(a).$$

Though the reduction discrepancy was not formally defined, it was shown that for any prime power M,

$$\exp\left(\Omega\left(\frac{\sqrt{M}}{h' \log(M)}\right)\right) \leq \delta_{K_M} \leq \phi(M) \exp(O(\sqrt{M \log(M)}),$$

where $h' = h^{+ \frac{1}{\varphi(M)-1}}$, and h^+ is the class number of the maximal totally real subfield of K_M. These seem to be the best asymptotic bounds for large values of M.

When the field has a special "unit reducible" property, the smallest quadratic form value also gives the shortest generator of the ideal. Although this connection breaks down in high dimensions as shown above, it can well hold in low dimensions. Our ultimate goal is to find a full list of cyclotomic fields which are unit reducible. Meanwhile, studying unit reducible fields in low dimensions could lead to lattice reduction algorithms in high dimensions (since the former can be used as a subroutine of the latter), an active research area [5, 8, 10]. In summary, the unit reducible property connects the SVP to ideal generators in certain cyclotomic fields, with implications for cryptanalysis.

1.2. Contributions. The main results of the paper are as follows.

Theorem 1.2. *For any number field K such that $K/\mathbb{Q}$ is Galois, let*

$$\mathcal{S} = \{x \in \mathcal{O}_K : |\text{Nm}_{K/\mathbb{Q}}(x)| \geq 2\} = \mathcal{O}_K \setminus \{\mathcal{O}_K^* \cup \{0\}\},$$

and

$$\eta_K = \min_{x \in \mathcal{S}} |\text{Nm}_{K/\mathbb{Q}}(x)|.$$

If $\gamma_K < \eta_K^{2/[K:\mathbb{Q}]}[K : \mathbb{Q}]$, then K is strongly unit reducible.

Theorem 1.3. *For any integers M, N such that $N \mid M$, if K_N is not unit reducible, the cyclotomic fields K_M is also not unit reducible. Moreover, $\delta_{K_M} \geq \delta_{K_N}$.*

We also find a more concrete lower bound for δ_{K_M} when M is a prime power which, whilst asymptotically worse than that in [3], provides us a framework by which we can deduce whether or not such fields are unit reducible.

Theorem 1.4. *The field K_N is unit reducible for $N = 3, 4, 5, 7, 8, 9, 12, 15$. Of these, the fields of conductors $N = 3, 4, 5, 7, 12, 15$ are strongly unit*

reducible, whilst the fields of conductors $N = 8, 9$ are weakly unit reducible. Moreover, for all integers $n \geq 1$ and odd primes $p \geq 3$,

$$\delta_{K_{2^n}} \geq 2^{n-3},$$

$$\delta_{K_{p^n}} \geq p^{n-1}\frac{p+1}{12}.$$

An immediate consequence of Theorems 1.3 and 1.4 are the following corollaries, the second of which we will prove, whilst the first is trivial.

Corollary 1.5. *The field K_N is not unit reducible if $2^4, 3^3, 5^2, 7^2, 11^2$ or any prime $p \geq 13$ divides N.*

Corollary 1.6. $\lim_{N \to \infty} \delta_{K_N} = \infty$.

2. Unit Reducible Cyclotomic Fields

Throughout the paper, we will use Δ_K to denote the discriminant of a number field K.

Proof of Theorem 1.2. By the definition of γ_K, every totally positive element $a \in K_{\gg 0}$,

$$\mu(a) \leq \gamma_K \operatorname{Nm}_{K/\mathbb{Q}}(a)^{\frac{1}{n}},$$

where $n = [K : \mathbb{Q}]$. Suppose that $\operatorname{Tr}_{K/\mathbb{Q}}(axx^*) = \mu(a)$ for some nonzero $x \in \mathcal{O}_K$. By the arithmetic-geometric inequality,

$$n \operatorname{Nm}_{K/\mathbb{Q}}(a)^{\frac{1}{n}} \operatorname{Nm}_{K/\mathbb{Q}}(x)^{\frac{2}{n}} = n \operatorname{Nm}_{K/\mathbb{Q}}(axx^*)^{\frac{1}{n}}$$

$$\leq \operatorname{Tr}_{K/\mathbb{Q}}(axx^*) = \mu(a) \leq \gamma_K \operatorname{Nm}_{K/\mathbb{Q}}(a)^{\frac{1}{n}}.$$

Rearranging gives

$$\operatorname{Nm}_{K/\mathbb{Q}}(xx^*)^{\frac{2}{n}} \leq \frac{\gamma_K}{n}.$$

If $n\eta_K^{\frac{2}{n}} > \gamma_K$, clearly the only nonzero elements of $\mathcal{O}_K$ that any totally positive $a \in K_{\gg 0}$ can attain their trace-minimum at must be units, which completes the proof. $\square$

Proof of Theorem 1.3. We first consider the special case where M/N is a prime power. Consider the field K_N for some integer $N \geq 3$, and assume that it is not unit reducible. Then there exists an $a \in K_{N \gg 0}$ such that $\mathcal{M}(a) \subset \mathcal{S}$, i.e. $\mu(a) < \mu^*(a)$. Let $N = sp^n$ for some $n \geq 0$ where p is a prime number, and $\gcd(p, s) = 1$. Now consider the field K_M, where $M = sp^m$ and $m \geq n \geq 0$. For any $y \in \mathcal{O}_{K_M}$, we can express y as

$$(2.1) \qquad\qquad y = \sum_{i=0}^{p^{m-n}-1} x_i' \zeta_M^i,$$

where $x_i \in \mathcal{O}_{K_N}$ and x_i' is the inclusion of x_i into K_M. Let a' denote the element $a \in K_{N \gg 0}$ after being lifted into the field K_M. Clearly a' is still a totally positive element. Then

$$a'yy^* = \sum_{i,j=0}^{p^{m-n}-1} a' x_i' x_j'^* \zeta_M^{i-j}.$$

Using the fact that

$$\mathrm{Tr}_{K_M/\mathbb{Q}}\left(\sum_{i,j=0}^{p^{m-n}-1} a' x_i' x_j'^* \zeta_M^{i-j} \right) = \sum_{i,j=0}^{p^{m-n}-1} \mathrm{Tr}_{K_M/\mathbb{Q}}\left(a' x_i' x_j'^* \zeta_M^{i-j} \right)$$

$$= \sum_{i,j=0}^{p^{m-n}-1} \mathrm{Tr}_{K_N/\mathbb{Q}}\left(a' x_i' x_j'^* \, \mathrm{Tr}_{K_M/K_N}(\zeta_M^{i-j}) \right),$$

$$\mathrm{Tr}_{K_M/K_N}(\zeta_M^{i-j}) = \begin{cases} p^{m-n} & \text{if } i = j, \\ 0 & \text{otherwise,} \end{cases}$$

it follows that

$$(2.2) \qquad \mathrm{Tr}_{K_M/\mathbb{Q}}(a'yy^*) = p^{m-n} \sum_{i=0}^{p^{m-n}-1} \mathrm{Tr}_{K_N/\mathbb{Q}}(axx_i^*).$$

We may assume without loss of generality that $a' \in \mathcal{F}_{K_M}$, so

$$\mathrm{Tr}_{K_M/\mathbb{Q}}(a') \le \mathrm{Tr}_{K_M/\mathbb{Q}}(a'uu^*),$$

for any $u \in \mathcal{O}_{K_M}^*$. However, by the assumptions made on a, there exists an element $x \in \mathcal{O}_{K_N}$ such that x is not a unit or zero, and

$$\mathrm{Tr}_{K_N/\mathbb{Q}}(avv^*) > \mathrm{Tr}_{K_N/\mathbb{Q}}(axx^*),$$

for all $v \in \mathcal{O}_{K_N}^*$. Therefore,

$$\mathrm{Tr}_{K_M/\mathbb{Q}}(a') = p^{m-n} \mathrm{Tr}_{K_N/\mathbb{Q}}(a) > p^{m-n} \mathrm{Tr}_{K_N/\mathbb{Q}}(axx^*) = \mathrm{Tr}_{K_M/\mathbb{Q}}(a'x'x'^*),$$

where x' is the element x after being lifted into K_M, which is not a unit. Thus $\mu^*(a') > \mu(a')$, and so

$$\delta_{K_M} \ge \frac{\mu^*(a')}{\mu(a')} \ge \frac{\mathrm{Tr}_{K_M/\mathbb{Q}}(a')}{\mathrm{Tr}_{K_M/\mathbb{Q}}(a'x'x'^*)} > 1.$$

So far we have shown that if $N = sp^n, M = sp^m$ with $m \ge n \ge 0$ and $\gcd(s,p) = 1$, K_N not being unit reducible implies that K_M is not unit reducible. We now want to focus on the more general case where $N \mid M$. Let $M = \prod_{i=1}^t p_i^{e_i}$, where p_i are prime and $e_i \ge 0$. Then if $N \mid M$, $N = \prod_{i=1}^t p_i^{f_i}$ where $e_i \ge f_i \ge 0$. However, it can be deduced that K_M will not be unit reducible if K_N is not unit reducible, since any cyclotomic field of conductor $N' = p_j^{f_j+k} \prod_{i=1:i \ne j}^t p_i^{f_i}$ for any $1 \le j \le t$, $k \ge 0$ will also not be

TABLE 2.1. A table of values for constants associated to K_N. The values of η_{K_N} were computed using SAGEMath, whilst the values of γ_n for $2 \le n \le 5$ were calculated in [6] and the values for $6 \le n \le 8$ were calculated in [1].

Value of N	η_{K_N}	γ_n **where** $n = [K : \mathbb{Q}]$	$|\Delta_{K_N}|^{1/n}$
5	5	$\sqrt{2}$	$5^{3/4}$
7	7	$\left(\frac{64}{3}\right)^{1/6}$	$7^{5/6}$
8	2	$\sqrt{2}$	4
9	3	$\left(\frac{64}{3}\right)^{1/6}$	$3^{3/2}$
12	4	$\sqrt{2}$	$2\sqrt{3}$
15	16	2	$5^{3/4}\sqrt{3}$

unit reducible, and so applying this argument inductively, the cyclotomic field of conductor M is not unit reducible. The inequality $\delta_{K_M} \ge \delta_{K_N}$ in this case follows similarly. $\qquad\square$

Before diving into the proof of Theorem 1.4, we will prove a useful Lemma, which is directly based off Theorem 2.2 from [9].

Lemma 2.1. *For every totally real number field K of degree n over $\mathbb{Q}$, we have $\gamma_K \le \gamma_n |\Delta_K|^{1/n}$.*

Proof. Let ax^2 define the unary form such that $\frac{\mu(a)}{\mathrm{Nm}_{K/\mathbb{Q}}(a)^{1/n}} = \gamma_K$. The proof of the Lemma follows from the fact that the rational quadratic form $\mathrm{Tr}_{K/\mathbb{Q}}(ax^2)$ is an n-dimensional totally positive rational quadratic form $q(x_1, \ldots, x_n)$ with $\det(q) = \mathrm{Nm}_{K/\mathbb{Q}}(a)|\Delta_K|$. $\qquad\square$

Proof of Theorem 1.4. Throughout the first part of the proof, we will make use of the values obtained in Table 2.1. The cyclotomic fields of conductors $3, 4$ are trivially unit reducible. Note that by Lemma 2.1, any field satisfying $\gamma_n |\Delta_K|^{1/n} < n\eta_K^{1/n}$ is strongly unit reducible by Theorem 1.2. Referring to Table 2.1, we can immediately see that the strict inequality holds for the fields K_N where $N = 5, 7, 12, 15$ which implies these fields are strongly unit reducible.

When $N = 8$, since $\eta_{K_8} = 2$ we have $\gamma_4 |\Delta_{K_8}|^{1/4} = 4\eta_{K_8}^{1/2}$. However, note that Theorem 1.2 fails to prove that K_8 is unit reducible in this case only if we have $[K_8 : \mathbb{Q}] \mathrm{Nm}_{K_8/\mathbb{Q}}(axx^*)^{1/4} = \mathrm{Tr}_{K_8/\mathbb{Q}}(axx^*)$, for which we would need axx^* to be fixed by all the Galois conjugates, i.e. $axx^* \in \mathbb{Q}$. Since $|\mathrm{Nm}_{K_8/\mathbb{Q}}(x)| = 2$ is achieved when $x = 1 + \zeta_8$ (or an associate of this element, or a conjugate-associate of this element, though all conjugates of $1 + \zeta_8$ are associates of $1 + \zeta_8$), we let $a = q(1 + \zeta_8)^{-1}(1 + \zeta_8^*)^{-1}$,

where q is some positive rational number. Performing HKZ reduction on the real quadratic form $\mathrm{Tr}_{K_8/\mathbb{Q}}(axx^*)$ yields $\mu(a) = \mathrm{Tr}_{K_8/\mathbb{Q}}(a) = 4q$, and so this form is unit reducible, so K_8 is unit reducible. However, $\mathrm{Tr}_{K_8/\mathbb{Q}}(a) = \mathrm{Tr}_{K_8/\mathbb{Q}}(a(1+\zeta_8)(1+\zeta_8)^*) = \mu(a)$, and since $1+\zeta_8$ is not a unit, this means K_8 is weakly unit reducible.

Similarly when $N = 9$ we have $\gamma_6|\Delta_{K_9}|^{1/6} = 6\eta_{K_9}^{1/3}$, where $\eta_{K_9} = 3$. Again, Theorem 1.2 fails to prove that K_9 is unit reducible in this case only if we have $[K_9 : \mathbb{Q}]\mathrm{Nm}_{K_9/\mathbb{Q}}(axx^*)^{1/4} = \mathrm{Tr}_{K_9/\mathbb{Q}}(axx^*)$, which occurs when $a = q/xx^*$ and $x = 1+\zeta_9+\zeta_9^3$. Performing HKZ reduction on the quadratic form yields $\mu(a) = \mathrm{Tr}_{K_9/\mathbb{Q}}(a) = 6q$, and so this form is unit reducible, so K_9 is unit reducible. Again, though, $\mathrm{Tr}_{K_9/\mathbb{Q}}(a) = \mathrm{Tr}_{K_9/\mathbb{Q}}(a(1+\zeta_9+\zeta_9^3)(1+\zeta_9+\zeta_9^3)^*) = \mu(a)$, and since $1+\zeta_9+\zeta_9^3$ is not a unit, this means that K_9 is weakly unit reducible.

From now on, we will use the notation

$$\rho_N(x) \triangleq \mathrm{Tr}_{K_N/\mathbb{Q}}(xx^*),$$

for any $x \in K_N$ for any conductor N.

Consider now the field K_{2^n} for $n \geq 4$. Let $a = ((1+\zeta_{2^n})(1+\zeta_{2^n}^{-1}))^{-1}$. We want to show that $\mu^*(a) > \mu(a)$ for this particular a, and therefore conclude that K_{2^n} is not unit reducible. Clearly $a \in K_{2^n \gg 0}$.

Set $x = \sum_{i=0}^{2^{n-1}-1} x_i \zeta_{2^n}^i \in \mathcal{O}_{K_{2^n}}^*$ with $x_i \in \mathbb{Z}$ to be some unit. Note that we can rewrite

$$x = e + y,$$

where $e \in \{0, 1\}$ and y is some $\mathbb{Z}$-linear combination of $2, 1+\zeta_{2^n}^i$ for each $1 \leq i \leq 2^{n-1} - 1$. Since $\frac{2}{1+\zeta_{2^n}}, \frac{1+\zeta_{2^n}^i}{1+\zeta_{2^n}}$ are both in $\mathcal{O}_{K_{2^n}}$, and $x \in \mathcal{O}_{K_{2^n}}^*$ by assumption, we have

$$x = \frac{1}{1+\zeta_{2^n}} + y',$$

where $y' \in \mathcal{O}_{K_{2^n}}$. Since

$$\rho_{2^n}\left(\sum_{i=0}^{2^{n-1}-1} z_i \zeta_{2^n}^i\right) = 2^{n-1}\sum_{i=0}^{2^{n-1}} z_i^2$$

for any $z_i \in \mathbb{Q}$, and

$$\frac{\zeta_{2^n}^k}{1+\zeta_{2^n}} = \zeta_{2^n}^k \sum_{i=0}^{2^{n-1}-1} \frac{(-1)^i}{2}\zeta_{2^n}^i,$$

it immediately holds that

$$\rho_{2^n}(x) = \rho_{2^n}\left(\frac{1}{1+\zeta_{2^n}} + y'\right) \geq \rho_{2^n}\left(\frac{1}{1+\zeta_{2^n}}\right),$$

(since $\pm 1/2$ cannot be rounded by an integer to be any smaller), and so for any unit u,

$$\mathrm{Tr}_{K_{2^n}/\mathbb{Q}}(auu^*) \geq \mathrm{Tr}_{K_{2^n}/\mathbb{Q}}(a),$$

i.e. a is reduced. But since $\rho(1) = 2^{n-1}$ and $\rho\left(\frac{1}{1+\zeta_{2^n}}\right) = 2^{2n-4}$,

$$\rho_{2^n}(1) < \rho_{2^n}\left(\frac{1}{1+\zeta_{2^n}}\right)$$

for all $n \geq 4$, which implies

$$\mathrm{Tr}_{K_{2^n}/\mathbb{Q}}(a(1+\zeta_{2^n})(1+\zeta_{2^n}^{-1})) < \mathrm{Tr}_{K_{2^n}/\mathbb{Q}}(a) = \mu^*(a).$$

Hence the field cannot be unit reducible. More specifically, we have

$$\frac{\mu^*(a)}{\mu(a)} = 2^{n-3},$$

and so

$$\delta_{K_{2^n}} \geq 2^{n-3} > 1,$$

for all $n \geq 4$.

Now consider the field K_{p^n}, for some odd prime p, and again take $a = ((1-\zeta_{p^n})(1-\zeta_{p^n}^{-1}))^{-1}$. Again, we want to show that K_{p^n} is not unit reducible by showing that $\mu^*(a) > \mu(a)$ in this instance. Let $x = \sum_{i=0}^{(p-1)p^{n-1}} x_i \zeta_{p^n}^i \in \mathbb{O}_{K_{p^n}}^*$ for some $x_i \in \mathbb{Z}$ be some unit. Note that we can rewrite x as

$$x = e + y,$$

where $e \in \{0, \ldots, p-1\}$ and y is a $\mathbb{Z}$-linear sum of p and $1 - \zeta_{p^n}^i$, $1 \leq i \leq (p-1)p^{n-1} - 1$. Since $\frac{p}{1-\zeta_{p^n}}, \frac{1-\zeta_{p^n}^i}{1-\zeta_{p^n}}$ are both in $\mathcal{O}_{K_{p^n}}$, and x is a unit by assumption, we must have

$$\frac{x}{1 - \zeta_{p^n}} = y' + \frac{e}{1 - \zeta_{p^n}},$$

for some $y' \in \mathcal{O}_{K_{p^n}}$ and $e \in \{1, \ldots, p-1\}$. We compute

$$\frac{1}{1 - \zeta_{p^n}} = \frac{1}{p} \sum_{i=0}^{p^{n-1}-1} \sum_{j=0}^{p-2} (p-1-j)\zeta_{p^n}^{i+jp^{n-1}}.$$

Since $\alpha \neq 0 \mod p$, $\alpha(p-1-i)$ permutes each $(p-1-i)$ to a unique element mod p for each distinct $0 \leq i \leq p-2$, so

$$\frac{x}{1 - \zeta_{p^n}} = y^\dagger + \frac{1}{p} \sum_{i=0}^{p^{n-1}-1} \sum_{j=0}^{p-2} (p-1-j)\zeta_{p^n}^{i+r(j)p^{n-1}},$$

where r denotes some permutation of the set $\{0, \ldots, p-2\}$, and $y^\dagger \in \mathcal{O}_{K_{p^n}}$.

Now, for any $z = \sum_{i=0}^{p^{n-1}(p-1)-1} z_i \zeta_{p^n}^i$ with $z_i \in \mathbb{Q}$, a simple computation yields

$$\rho_{p^n}(z) = p^{n-1} \sum_{i=0}^{p^{n-1}-1} Q(z_i, z_{i+p^{n-1}}, z_{i+2p^{n-1}}, \ldots, z_{i+(p-2)p^{n-1}}),$$

where Q defines the $p-1$-dimensional positive-definite quadratic form

$$Q(m_1, \ldots, m_{p-1}) = (p-1) \sum_{i=1}^{p-1} m_i^2 - 2 \sum_{i<j} m_i m_j.$$

It was shown in [11, Proposition 3.1, p. 461] that

$$Q\left(\frac{r(p-1)}{p} - m_1, \frac{r(p-2)}{p} - m_2, \ldots, \frac{r(1)}{p} - m_{p-1}\right)$$
$$\geq Q\left(\frac{r(p-1)}{p}, \frac{r(p-2)}{p}, \ldots, \frac{r(1)}{p}\right),$$

for all integers $m_1, \ldots, m_{p-1}$ and permutations r of the set $\{1, \ldots, p-1\}$. Collectively, this means that

$$\rho_{p^n}\left(\frac{x}{1-\zeta_{p^n}}\right) = \rho_{p^n}\left(\frac{1}{1-\zeta_{p^n}} + y^\dagger\right) \geq \rho_{p^n}\left(\frac{1}{1-\zeta_{p^n}}\right),$$

and so

$$\mathrm{Tr}_{K_{p^n}/\mathbb{Q}}(auu^*) \geq \mathrm{Tr}_{K_{p^n}/\mathbb{Q}}(a)$$

for all units u, i.e. a is reduced. Also note that

$$\mathrm{Tr}_{K_{p^n}/\mathbb{Q}}(a) = p^{2(n-1)}\frac{p^2-1}{12}.$$

However, we also have

$$\mathrm{Tr}_{K_{p^n}/\mathbb{Q}}(a(1-\zeta_{p^n})(1-\zeta_{p^n}^{-1})) = \mathrm{Tr}_{K_{p^n}/\mathbb{Q}}(1) = p^{n-1}(p-1) = \mu(a),$$

and so

$$\delta_{K_{p^n}} \geq \frac{\mathrm{Tr}_{K_{p^n}/\mathbb{Q}}(a)}{\mu(a)} = \frac{\mu^*(a)}{\mu(a)} = p^{n-1}\frac{p+1}{12} > 1,$$

if $p = 3$ and $n \geq 3$, $p = 5$ and $n \geq 2$, $p = 7$ and $n \geq 2$, $p = 11$ and $n \geq 2$ or $p \geq 13$. $\square$

Proof of Corollary 1.6. It suffices to show that for each positive $1 \leq \delta < \infty$, there can only be finitely many integers M satisfying $\delta_{K_M} \leq \delta$. Suppose that $M = 2^e \prod_{i=1}^t p_i^{e_i}$, for some odd primes $p_1, \ldots, p_t$ ordered so $p_i < p_{i+1}$ for all $1 \leq i \leq t-1$, and positive integers $e, e_1, \ldots, e_t$. Recall that Theorem 1.3 states that for any N dividing M, $\delta_{K_N} \leq \delta_{K_M}$. Since $\delta_{K_{p^n}} \geq p^{n-1}\frac{p+1}{12} \geq \frac{p+1}{12}$ for any odd prime p and integer $n \geq 1$, if $\delta_{K_M} \leq \delta$ we must have $p_t \leq 12\delta - 1$.

Moreover, since $\delta \geq \delta_{K_M} \geq \delta_{K_{p_i^{e_i}}} \geq p^{e_i-1}\frac{p_i+1}{12} > \frac{p^{e_i}}{12}$ for each $1 \leq i \leq t$, this implies $e_i < \frac{\log(\delta)}{\log(p_i)} + \log(12)$ for each e_i. Similarly, $e \leq \frac{\log(\delta)}{\log(2)} + 4$. Therefore if M satisfies $\delta_{K_M} \leq \delta$ we must have

$$M < 2^{\frac{\log(\delta)}{\log(2)}+4} \prod_{i=1}^{t} p_i^{\frac{\log(\delta)}{\log(p_i)}+\log(12)},$$

satisfying $p_t \leq 12\delta - 1$. Clearly there are only finitely many integers that satisfy this inequality if δ is finite. $\qquad\square$

3. Totally Real Subfields of Cyclotomic Fields

For any cyclotomic field K_N for some conductor N, we will use the notation K_N^+ to refer to the maximal totally real subfield of K_N, i.e. $K_N^+ = \mathbb{Q}(\zeta_N + \zeta_N^{-1})$. A natural question to ask is whether K_N being (not) unit reducible implies that K_N^+ is unit reducible and vice versa.

Recall that for every unit u in K_N, there exists a unit v in K_N^+ such that $u = \zeta_N^i v$ (see e.g. [13, Proposition 6.7]). For any field K and any subset S, denote by $S^2 = \{xx^* : x \in S\}$. It then follows that $\mathcal{O}_{K_N}^*{}^2 = \mathcal{O}_{K_N^+}^*{}^2$. We also have $\mathcal{O}_{K_N^+}^2 \subseteq \mathcal{O}_{K_N}^2$.

The set of totally positive elements in K_N and K_N^+ are identical (since necessarily the set of totally positive elements must be a subset of the totally real subfield). Then for any $a \in K_{N\gg0}^+$ and its associated element a' after being lifted into K_N (notice every element of $K_{N\gg0}$ can be constructed in this manner), $\mu^*(a) = \frac{1}{2}\mu^*(a')$ (where the $\frac{1}{2}$ factor comes from the fact that $[K_N : K_N^+] = 2$). Since $\mathcal{O}_{K_N^+}^2 \subseteq \mathcal{O}_{K_N}^2$, $\frac{1}{2}\mu(a') \leq \mu(a)$. From this we can deduce that if K_N is unit reducible, then K_N^+ is unit reducible, and if K_N^+ is not unit reducible then K_N is not unit reducible.

From this, combined with Theorem 1.4, we deduce that K_N^+ is unit reducible for $N = 3, 4, 5, 7, 8, 9, 12, 15$. However, of these the result that K_N^+ for $N = 15$ is unit reducible is the only new result. The maximal totally real subfields of K_3, K_4 are trivially unit reducible (as they are both $\mathbb{Q}$), whilst the maximal totally real subfields of K_N are real quadratic for $N = 5, 8, 12$ and simplest cubic fields for $N = 7, 9$, the cases of which were both covered in [10].

We now deduce a lower bound on $\delta_{K_N^+}$ using similar techniques in the last section.

Proposition 3.1. *For all $n \geq 1$,*

$$\delta_{K_{2^n}^+} \geq 2^{n-4},$$

and for all odd primes p,

$$\delta_{K_{p^n}^+} \geq \frac{p^{n-1}(p^2-1)}{24(p-2)}.$$

Proof. From now on, we will use the notation $\theta_N \triangleq \zeta_N + \zeta_N^{-1}$. Consider the field $K_{2^n}^+$ for some $n \geq 1$. We set $a = (2 + \theta_{2^n})^{-1}$, which is totally positive for any n. Lifting a to K_{2^n} as $a' = (1 + \zeta_{2^n})^{-1}(1 + \zeta_{2^n}^{-1})^{-1}$, we have already shown that $\mu^*(a') = \text{Tr}_{K_{2^n}/\mathbb{Q}}(a') = 2^{2n-4}$, and so $\mu^*(a) = 2^{2n-5}$. However, $a(2 + \theta_{2^n})^2 = 2 + \theta_{2^n} = a^{-1}$, and since $\text{Tr}_{K_{2^n}/\mathbb{Q}}(a'^{-1}) = 2^n$ we have $\text{Tr}_{K_{2^n}^+/\mathbb{Q}}(a(2 + \theta_{2^n})^2) = \text{Tr}_{K_{2^n}^+/\mathbb{Q}}(a^{-1}) = 2^{n-1} \geq \mu(a)$. Hence

$$\delta_{K_{2^n}^+} \geq \frac{\mu^*(a)}{\mu(a)} \geq \frac{\mu^*(a)}{\text{Tr}_{K_{2^n}^+/\mathbb{Q}}(a^{-1})} = 2^{n-4}.$$

Similarly, when we consider the field $K_{p^n}^+$ for some odd prime p and $n \geq 1$, we take $a = 2 - \theta_{p^n}$, which is totally positive for any n. Following similar logic to before, and using the fact that $\text{Tr}_{K_{p^n}/\mathbb{Q}}((1 - \zeta_{p^n})(1 - \zeta_{p^n}^{-1})) = 2p^{n-1}(p-2)$,

$$\delta_{K_{p^n}^+} \geq \frac{\mu^*(a)}{\mu(a)} \geq \frac{\mu^*(a)}{\text{Tr}_{K_{p^n}^+/\mathbb{Q}}(a^{-1})} = \frac{p^{n-1}(p^2-1)}{24(p-2)}. \qquad \square$$

Proposition 3.2. *If $N \mid M$, if K_N^+ is not unit reducible then K_M^+ is not unit reducible. Moreover, $\delta_{K_M^+} \geq \delta_{K_N^+}$.*

Proof. The proof follows almost identically to the proof of Theorem 1.3, using the fact that $\mathcal{O}_{K_M^+} = \mathbb{Z}[\theta_M]$. $\qquad \square$

We immediately obtain the following corollaries as a result, and omit the proofs as they are identical to that of the cyclotomic case.

Corollary 3.3. *The field K_N^+ is not unit reducible if N is divisible by 2^5, 3^3, 5^2, 7^2, 11^2, 13^2, 17^2, 19^2, or any odd prime $p \geq 23$.*

Corollary 3.4. $\delta_{K_N^+} \to \infty$ *as $N \to \infty$.*

4. Concluding Remarks

In this work, we have deduced a number of results regarding unit reducibility in cyclotomic fields and their totally real subfields. Specifically, we determined that the number of unit reducible cyclotomic fields must be finite in number, and that the discrepancy between the trace of the shortest generator of a positive unary form and the shortest nonzero vector length of the corresponding positive-definite quadratic form can become arbitrarily large, as the conductor for the cyclotomic field grows. We also showed a similar result for their maximal totally real subfields. We deduced a simple

method by which we can determine whether an arbitrary field is unit reducible, and used this to prove that a number of cyclotomic fields are unit reducible, though this list is not complete.

Of course, the principal open problem is to determine the entire list of unit reducible cyclotomic fields. The authors make the following conjecture:

Conjecture 4.1. *The cyclotomic fields K_N where $N = 3$, 4, 5, 7, 8, 9, 11, 12, 15, 20, 21, 24 are the only unit reducible cyclotomic fields.*

The authors's reasoning for this conjecture hinges on a discovery made in [15], where the number of homothety classes of perfect unary forms in cyclotomic fields were studied. Of these, the fields of conductors $N = 3$, 4, 5, 7, 8, 9, 11, 20, 21, 24 were found to have all the perfect unary forms (up to homothety class) correspond to perfect rational quadratic forms of dimension $\phi(N)$. Moreover, none of the other cyclotomic fields considered satisfied this property.

In [10], it was shown that there was an intimate connection between unit reducible fields and the number of classes of perfect unary forms for the case of real quadratic and simplest cubic fields. It therefore would be interesting to pursue the idea that this connection is apparent in cyclotomic, and perhaps even more general number fields.

References

[1] H. F. Blichfeldt, "The minimum values of positive quadratic forms in six, seven and eight variables", *Math. Z.* **39** (1935), p. 1-15.

[2] P. Campbell, M. Groves & D. Shepherd, "Soliloquy: A cautionary tale", 2014, ETSI 2nd Quantum-Safe Crypto Workshop.

[3] R. Cramer, L. Ducas, C. Peikert & O. Regev, "Recovering short generators of principal ideals in cyclotomic rings", in *Advances in cryptology – EUROCRYPT 2016*, Lecture Notes in Computer Science, vol. 9666, Springer, 2016, p. 559-585.

[4] S. Garg, C. Gentry & S. Halevi, "Candidate multilinear maps from ideal lattices", in *Advances in cryptology – EUROCRYPT 2013*, Lecture Notes in Computer Science, vol. 7881, Springer, 2013, p. 1-17.

[5] T. Kim & C. Lee, "Lattice reduction over Euclidean rings with applications to cryptanalysis", in *Cryptography and Coding – IMACC 2017*, Lecture Notes in Computer Science, vol. 10655, Springer, 2017, p. 371-391.

[6] A. Korkine & G. Zolotarev, "Sur les formes quadratiques", *Math. Ann.* **6** (1873), p. 366-389.

[7] A. Langlois, D. Stehlé & R. Steinfeld, "GGHLite: More efficient multilinear maps from ideal lattices", in *Advances in cryptology – EUROCRYPT 2014*, Lecture Notes in Computer Science, vol. 8441, Springer, 2014, p. 239-256.

[8] C. Lee, A. Pellet-Mary, D. Stehlé & A. Wallet, "An LLL algorithm for module lattices", in *Advances in cryptology – ASIACRYPT 2019*, Lecture Notes in Computer Science, vol. 11922, Springer, 2019, p. 59-90.

[9] A. Leibak, "On additive generalization of Voronoï's theory for algebraic number fields", *Proc. Est. Acad. Sci., Phys. Math.* **54** (2005), no. 4, p. 195-211.

[10] A. Leibak, C. Porter & C. Ling, "Unit reducible fields and perfect unary forms", *J. Théor. Nombres Bordeaux* **35** (2023), no. 3, p. 867-895.

[11] j. Lenstra, Hendrik W., "Euclid's algorithm in cyclotomic fields", *J. Lond. Math. Soc. (2)* **10** (1975), no. 4, p. 457-465.

[12] V. Lyubashevsky, C. Peikert & O. Regev, "On ideal lattices and learning with errors over rings", in *Advances in cryptology – EUROCRYPT 2010*, Lecture Notes in Computer Science, vol. 6110, Springer, 2010, p. 1-23.

[13] J. S. Milne, "Algebraic Number Theory", 2020, e-book, `https://www.jmilne.org/math/CourseNotes/ANT.pdf`.

[14] D. Moody, G. Alagic, D. C. Apon, D. A. Cooper, Q. H. Dang, J. M. Kelsey, Y.-K. Liu, C. A. Miller, R. C. Peralta, R. A. Perlner, A. Y. Robinson, D. C. Smith-Tone & J. Alperin-Sheriff, *Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process*, NIST Interagency/Internal Report (NISTIR), NIST Pubs, 2020.

[15] F. Sigrist, "Cyclotomic quadratic forms", *J. Théor. Nombres Bordeaux* **12** (2000), no. 2, p. 519-530.

[16] N. P. Smart & F. Vercauteren, "Fully homomorphic encryption with relatively small key and ciphertext sizes", in *Public key cryptography – PKC 2010*, Lecture Notes in Computer Science, vol. 6056, Springer, 2010, p. 420-443.

[17] D. Stehlé & R. Steinfeld, "Making NTRU as secure as worst-case problems over ideal lattices", in *Advances in cryptology – EUROCRYPT 2011*, Lecture Notes in Computer Science, vol. 6632, Springer, 2011, p. 27-47.

Christian Porter (corresponding author)
Imperial College London
United Kingdom
E-mail: `c.porter17@imperial.ac.uk`
URL: `https://www.researchgate.net/profile/Christian-Porter`

Cong Ling
Imperial College London
United Kingdom
E-mail: `c.ling@imperial.ac.uk`
URL: `https://www.imperial.ac.uk/people/c.ling`

Piero Sarti
Imperial College London
United Kingdom
E-mail: `piero.sarti21@imperial.ac.uk`

Alar Leibak
Tallinn University of Technology
Estonia
E-mail: `alar.leibak@taltech.ee`
URL: `https://taltech.ee/en/contacts/division-mathematics/alar-leibak`