The shape of cyclic number fields

Wilmar Bolaños and Guillermo Mantilla-Soler

Abstract. Let $m > 1$ and $\mathfrak{d} \ne 0$ be integers such that $v_p(\mathfrak{d}) \ne m$ for any prime p. We construct a matrix $A(\mathfrak{d})$ of size $(m-1) \times (m-1)$ depending on only of $\mathfrak{d}$ with the following property: For any tame $\mathbb{Z}/m\mathbb{Z}$-number field K of discriminant $\mathfrak{d}$, the matrix $A(\mathfrak{d})$ represents the Gram matrix of the integral trace-zero form of K. In particular, we have that the integral trace-zero form of tame cyclic number fields is determined by the degree and discriminant of the field. Furthermore, if in addition to the above hypotheses, we consider real number fields, then the shape is also determined by the degree and the discriminant.

1 Introduction

Let K be a number field of degree $n := [K : \mathbb{Q}]$, and let $\mathfrak{o}_K$ be its maximal order. The *trace-zero module* of $\mathfrak{o}_K$ is the $\mathbb{Z}$-submodule of $\mathfrak{o}_K$ given by the Kernel of the trace map, i.e., $\mathfrak{o}_K^0 = K^0 \cap \mathfrak{o}_K$, where $K^0 := \{x \in K : \mathrm{Tr}_{K/\mathbb{Q}}(x) = 0\}$. The *integral trace-zero form* of K is the isometry class of the rank $(n-1)$ quadratic $\mathbb{Z}$-module $\langle \mathfrak{o}_K^0, \mathrm{Tr}_{K/\mathbb{Q}}()_{\mathfrak{o}_K} \rangle$ given by restricting the trace pairing from $\mathfrak{o}_K \times \mathfrak{o}_K$ to $\mathfrak{o}_K^0 \times \mathfrak{o}_K^0$. For K of degree $n = 1, 2$, it is clear, by checking the discriminant, that the isometry class of the quadratic module $\langle \mathfrak{o}_K^0, \mathrm{Tr}_{K/\mathbb{Q}}()|_{\mathfrak{o}_K} \rangle$ determines the field K. For general degrees, this is not the case (see, for instance, [7, Section 3]). However, recently, the second-named author and one of his coauthors have shown that for square-free discriminants, with some extra conditions on the signature and the degree, the integral trace-zero form determines the conjugacy class of the field.

Theorem 1.1 [11, Theorem 2.13]   *Suppose that K is a degree n totally real number field, of fundamental discriminant d, such that $\gcd(n, d) = 1$. If $(\mathbb{Z}/n\mathbb{Z})^*$ is cyclic, then $\langle \mathfrak{o}_K^0, \mathrm{Tr}_{K/\mathbb{Q}}()|_{\mathfrak{o}_K} \rangle$ is a complete invariant for K. In other words, for any number field L, we have that*

$$\langle \mathfrak{o}_K^0, \mathrm{Tr}_{K/\mathbb{Q}}()|_{\mathfrak{o}_K} \rangle \simeq \langle \mathfrak{o}_L^0, \mathrm{Tr}_{L/\mathbb{Q}}()|_{\mathfrak{o}_L} \rangle \text{ if and only if } K \simeq L.$$

In contrast to the above result in the case of Galois number fields of prime degree $\ell = n$, the integral trace-zero form does not discriminate beyond the discriminant. Moreover, in such a case, the integral trace-zero form is isometric to the root lattice $\mathbb{A}_{\ell-1}$ times a constant defined solely in terms of the discriminant. Recall that for a given positive integer m, the root lattice $\mathbb{A}_m$ is the m-dimensional lattice associated

---

with the quadratic form

$$\sum_{1 \le i \le m} 2x_i^2 - \sum_{\substack{1 \le i,j \le m \\ |i-j|=1}} x_i x_j$$

or equivalently with a Gram matrix in some basis given by

$$\mathcal{A}_m := \begin{pmatrix} 2 & -1 & 0 & 0 & \dots & 0 \\ -1 & 2 & -1 & 0 & \cdots & 0 \\ 0 & -1 & 2 & -1 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & -1 & 2 & -1 \\ 0 & 0 & 0 & 0 & -1 & 2 \end{pmatrix}.$$

Given an integer d, let $\mathrm{rad}(d)$ be the square-free integer that has the same signature and the same prime factors as d.

Theorem 1.2 [6, Theorem 2.9]   *Let ℓ be a prime, and let K be a $\mathbb{Z}/\ell\mathbb{Z}$-number field of discriminant $\mathfrak{d}(K)$. Suppose that $\gcd(\ell, \mathfrak{d}(K)) = 1$. Then, the Gram matrix of $\left\langle \mathfrak{o}_K^0, \mathrm{Tr}_{K/\mathbb{Q}}()|_{\mathfrak{o}_K} \right\rangle$ with respect to some basis is equal to*

$$\mathrm{rad}(\mathfrak{d}(K)).\mathcal{A}_{\ell-1}.$$

In particular, if L is a $\mathbb{Z}/\ell\mathbb{Z}$-number field with $\gcd(\ell, \mathfrak{d}(L)) = 1$, then

$$\left\langle \mathfrak{o}_K^0, \mathrm{Tr}_{K/\mathbb{Q}}()|_{\mathfrak{o}_K} \right\rangle \simeq \left\langle \mathfrak{o}_L^0, \mathrm{Tr}_{L/\mathbb{Q}}()|_{\mathfrak{o}_L} \right\rangle \ \textit{if and only if } \mathfrak{d}(K) = \mathfrak{d}(L).$$

Remark 1.3   Note that the condition $\gcd(\ell, \mathfrak{d}(K)) = 1$ is equivalent to say that the field K is tame, i.e., that there is no rational prime that is wildly ramified in K.

The purpose of this paper is to generalize the result above to general cyclic number fields of arbitrary degree. Our main theorem is the following.

Theorem (cf. Theorem 2.10)   *Let $m \ne 1$ be a positive integer, and let K be a $\mathbb{Z}/m\mathbb{Z}$-number field of discriminant $\mathfrak{d}(K)$. Suppose that K is tame. There exists a matrix $A(\mathfrak{d}(K)) \in \mathrm{M}_{(m-1)\times(m-1)}(\mathbb{Z})$ depending only on $\mathfrak{d}(K)$ such that the Gram matrix of*

$$\left\langle \mathfrak{o}_K^0, \mathrm{Tr}_{K/\mathbb{Q}}()|_{\mathfrak{o}_K} \right\rangle$$

with respect to some basis is equal to

$$A(\mathfrak{d}(K)).$$

In particular, if L is a tame $\mathbb{Z}/m\mathbb{Z}$-number field, then

$$\left\langle \mathfrak{o}_K^0, \mathrm{Tr}_{K/\mathbb{Q}}()|_{\mathfrak{o}_K} \right\rangle \simeq \left\langle \mathfrak{o}_L^0, \mathrm{Tr}_{L/\mathbb{Q}}()|_{\mathfrak{o}_L} \right\rangle \ \textit{if and only if } \mathfrak{d}(K) = \mathfrak{d}(L).$$

Remark 1.4   In the case that $m = \ell$ is a prime number, $A(\mathfrak{d}(K)) = \mathrm{rad}(\mathfrak{d}(K))\mathcal{A}_{\ell-1}$. Hence, the construction here directly generalizes the results in [6].

1.1 The shape

Another quadratic invariant, with a more geometric interpretation and closely related to the trace zero form, that has been studied by several authors is the shape of K. Endow K with the real-valued $\mathbb{Q}$-bilinear form b_K whose associated quadratic form is given by

$$b_K(x,x) := \sum_{\sigma:K \hookrightarrow \mathbb{C}} |\sigma(x)|^2.$$

The *shape* of K, denoted by $\mathrm{Sh}(K)$, is the isometry equivalence class of $(\mathfrak{o}_K^\perp, b_K)$ up to scalar multiplication, where $\mathfrak{o}_K^\perp$ is the image of $\mathfrak{o}_K$ under the projection map, $\alpha \mapsto \alpha_\perp := n\alpha - \mathrm{Tr}_{K/\mathbb{Q}}(\alpha)$, i.e.,

$$\mathfrak{o}_K^\perp := \{\alpha_\perp : \alpha \in \mathfrak{o}_K\} = (\mathbb{Z} + n\mathfrak{o}_K) \cap \mathfrak{o}_K^0.$$

Thus, $\mathrm{Sh}(K) = \mathrm{Sh}(L)$ if and only if $(\mathfrak{o}_K^\perp, b_K) \simeq (\mathfrak{o}_L^\perp, \lambda b_L)$ for some $\lambda \in \mathbb{R}^*$. Equivalently, $\mathrm{Sh}(K)$ can be thought as the $(n-1)$-dimensional lattice inside $\mathbb{R}^n$, via the Minkowski embedding, that is the orthogonal complement of 1 and that is defined up to reflection, rotations, and scaling by $\mathbb{R}^*$. Hence, $\mathrm{Sh}(K)$ corresponds to an element to the *space of shapes*

$$\mathcal{S}_{n-1} := \mathrm{GL}_{n-1}(\mathbb{Z}) \smallsetminus \mathrm{GL}_{n-1}(\mathbb{R}) / \mathrm{GO}_{n-1}(\mathbb{R}).$$

The distribution of shapes of number fields in $\mathcal{S}_n$ has been the subject of interesting current research (see [1, 3, 4, 6]). It turns out that, for cyclic real number fields, the Shape is determined by the discriminant, moreover:

Theorem (cf. Theorem 2.14)   *Let m be a positive integer, and let K and L be two totally real tame $\mathbb{Z}/m\mathbb{Z}$-number fields. Then, the following are equivalent:*

(a) $\langle \mathfrak{o}_K, \mathrm{Tr}_{K/\mathbb{Q}}() \rangle \simeq \langle \mathfrak{o}_L, \mathrm{Tr}_{L/\mathbb{Q}}() \rangle$.
(b) $(\mathfrak{o}_K^\perp, b_K) \simeq (\mathfrak{o}_L^\perp, b_L)$.
(c) $\langle \mathfrak{o}_K^0, \mathrm{Tr}_{K/\mathbb{Q}}()|_{\mathfrak{o}_K} \rangle \simeq \langle \mathfrak{o}_L^0, \mathrm{Tr}_{L/\mathbb{Q}}()|_{\mathfrak{o}_L} \rangle$.
(d) $\mathfrak{d}(K) = \mathfrak{d}(L)$.

2 The trace-zero module

In this section, we study the behavior of the trace-zero module of tamely ramified cyclic number fields and the connection with their discriminant. The main goal is to extend some results about trace-zero modules developed in [6, 7].

Definition 2.1   Let K be a number field, and let $\mathfrak{o}_K$ be its maximal order. The trace-zero module $\mathfrak{o}_K^0$ is defined as

$$\mathfrak{o}_K^0 := \{x \in \mathfrak{o}_K : \mathrm{Tr}_{K/\mathbb{Q}}(x) = 0\}.$$

Lemma 2.1   *Let K be a tamely ramified cyclic number field of degree m. Let $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ be a generator of the Galois group. Suppose $B := \{e_1, \ldots, e_m\}$ is a normal*

integral basis for $\mathfrak{o}_K$, i.e., an integral basis such that $\sigma(e_m) = e_1$ and $\sigma(e_j) = e_{j+1}$ for $1 \le j \le m - 1$. Then, $B_0 := \{e_1 - e_2, e_2 - e_3, \ldots, e_{m-1} - e_m\}$ is an integral basis for $\mathfrak{o}_K^0$.

Proof　　Since B is a normal basis, each element $e_j - e_{j+1}$ of B_0 belongs to $\mathfrak{o}_K^0$. On the other hand, thanks to Hilbert's 90, if $u \in K$ is such that $\mathrm{Tr}_{K/\mathbb{Q}}(u) = 0$, then there exist $b \in K$ such that $u = b - \sigma(b)$. Therefore, if $u \in \mathfrak{o}_K^0$, then

$$
\begin{aligned}
u &= b - \sigma(b) \\
&= (c_1 e_1 + c_2 e_2 + \cdots + c_m e_m) - \sigma(c_1 e_1 + c_2 e_2 + \cdots + c_m e_m) \\
&= (c_1 - c_m) e_1 + (c_2 - c_1) e_2 + \cdots + (c_m - c_{m-1}) e_m,
\end{aligned}
$$

for some $c_i \in \mathbb{Q}$. Since $u \in \mathfrak{o}_K$, we must have $c_{j+1} - c_j \in \mathbb{Z}$ for $j = 0, 1, \ldots, (m-1)$, where we define $c_0 := c_m$. Moreover, since

$$
c_i - c_m = \sum_{j=1}^{i} (c_j - c_{j-1}) \in \mathbb{Z},
$$

by rearranging, we obtain

$$
\begin{aligned}
u &= (c_1 - c_m) e_1 + (c_2 - c_1) e_2 + \cdots + (c_m - c_{m-1}) e_m \\
&= (c_1 - c_m)(e_1 - e_2) + (c_2 - c_m)(e_2 - e_3) + \cdots + (c_{m-1} - c_m)(e_{m-1} - e_m).
\end{aligned}
$$

By ranks, we conclude that $\{e_1 - e_2, e_2 - e_3, \ldots, e_{m-1} - e_m\}$ is an integral basis for $\mathfrak{o}_K^0$. ∎

2.1　A Gram matrix representation of the trace-zero form

In this section, we use a trace-zero basis, coming from a normal integral basis as in the previous section, to find a canonical Gram matrix for the integral trace zero form.

Lemma 2.2　　*Let K be a number field of degree m, and let $G_K := \mathbb{Z} + \mathfrak{o}_K^0$. We have*

$$
|\mathfrak{o}_K/G_K| = \left| \mathrm{Tr}_{K/\mathbb{Q}}(\mathfrak{o}_K)/m\mathbb{Z} \right|.
$$

Proof　　By the isomorphism theorem on groups, the result follows from:
- The group G_K is a subgroup of $\mathfrak{o}_K$ that contains the Kernel of the trace map.
- The image of G_K under the trace is equal to $m\mathbb{Z}$. ∎

Corollary　　*If K is a tamely ramified number field of degree m, then*

$$
|\mathfrak{o}_K/G_K| = m.
$$

Proof　　Since K is tamely ramified, by [12, Corollary 5 to Theorem 4.24],

$$
\mathrm{Tr}_{K/\mathbb{Q}}(\mathfrak{o}_K) = \mathbb{Z}.
$$

Using this, the result follows from Lemma 2.2. ∎

Theorem 2.4 *Let K and L be tamely ramified cyclic number fields of degree m. Then,*

$$\left\langle \mathfrak{o}_K^0, \mathrm{Tr}_{K/\mathbb{Q}}()|_{\mathfrak{o}_K} \right\rangle \simeq \left\langle \mathfrak{o}_L^0, \mathrm{Tr}_{L/\mathbb{Q}}()|_{\mathfrak{o}_L} \right\rangle \ \text{if and only if } \mathfrak{d}(L) = \mathfrak{d}(K).$$

Proof Suppose that $\left\langle \mathfrak{o}_K^0, \mathrm{Tr}_{K/\mathbb{Q}}()|_{\mathfrak{o}_K} \right\rangle \simeq \left\langle \mathfrak{o}_L^0, \mathrm{Tr}_{L/\mathbb{Q}}()|_{\mathfrak{o}_L} \right\rangle$. Since the decomposition of $G_K = \mathbb{Z} + \mathfrak{o}_K^0$ (resp. $G_L = \mathbb{Z} + \mathfrak{o}_L^0$) is an orthogonal decomposition with respect to the trace pairing, we have the following equalities between determinants of the trace in the respective modules:

$$\mathfrak{d}(G_K) = \mathfrak{d}(\mathfrak{o}_K^0)m = \mathfrak{d}(\mathfrak{o}_L^0)m = \mathfrak{d}(G_L).$$

Since

$$\mathfrak{d}(G_K) = |\mathfrak{o}_K/G_K|^2 \mathfrak{d}(\mathfrak{o}_K) \text{ and } \mathfrak{d}(G_L) = |\mathfrak{o}_L/G_L|^2 \mathfrak{d}(\mathfrak{o}_L),$$

the result follows thanks to Corollary 2.3.

On the other hand, if $\mathfrak{d}(K) = \mathfrak{d}(L)$, then, by [9, Theorems 4.2 and 4.5], there exist normal integral bases $B := \{e_1, \ldots, e_m\}$ and $B' := \{e_1', \ldots, e_m'\}$ of $\mathfrak{o}_K$ and $\mathfrak{o}_L$, respectively, such that $\left\langle \mathfrak{o}_K, \mathrm{Tr}_{K/\mathbb{Q}}() \right\rangle$ and $\left\langle \mathfrak{o}_L, \mathrm{Tr}_{L/\mathbb{Q}}() \right\rangle$ are isometric via an isometry

$$\gamma : \mathfrak{o}_K \to \mathfrak{o}_L$$

such that $\gamma(e_i) = e_i'$ for all $1 \le i \le m$. It follows from Lemma 2.1 that such an isometry γ restricts to an isometry between the quadratic modules $\left\langle \mathfrak{o}_K^0, \mathrm{Tr}_{K/\mathbb{Q}}()|_{\mathfrak{o}_K} \right\rangle$ and $\left\langle \mathfrak{o}_L^0, \mathrm{Tr}_{L/\mathbb{Q}}()|_{\mathfrak{o}_L} \right\rangle$. ∎

Definition 2.2 Let m be a positive integer. For every d a positive divisor of m, we let A_d be an $m \times m$ matrix defined as

$$(A_d)_{i,j} := \begin{cases} 1, & \text{if } \frac{m}{d} \big| (i - j), \\ \\ 0, & \text{otherwise.} \end{cases}$$

Suppose that K is a tame cyclic number field of degree m. Theorems 4.2 and 4.5 of [9] state that there exists a normal integral basis B of $\mathfrak{o}_K$ such that the Gram matrix of $\left\langle \mathfrak{o}_K, \mathrm{Tr}_{K/\mathbb{Q}}() \right\rangle$ in such basis is equal to

$$\sum_{d|m} a_d A_d,$$

where a_d are integers given in Lemma 4.3 of [9] that only depend on the discriminant of K. For the reader's convenience, see also Definition 2.5.

We devote the rest of this section to describe a similar canonical decomposition, i.e., a Gram matrix depending only on the discriminant of the field, for the trace-zero module $\left\langle \mathfrak{o}_K^0, \mathrm{Tr}_{K/\mathbb{Q}}() \right\rangle$.

Let $n \geq 2$ be an integer. Then, we define $\mathbb{B}_n$ as the $n \times n$ matrix

$$\begin{pmatrix} 1 & 0 & 0 & \ldots & -1 \\ -1 & 1 & 0 & \ldots & 0 \\ 0 & -1 & 1 & \ldots & 0 \\ \vdots & 0 & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & -1 & 1 \end{pmatrix}.$$

In other words,

$$(\mathbb{B}_n)_{i,j} := \begin{cases} 1, & \text{if } i = j, \\ -1, & \text{if } i = j+1 \text{ or } (i,j) = (1,n), \\ 0, & \text{otherwise.} \end{cases}$$

Proposition   *Let m be an integer bigger than 1, and let K be a degree m number field. Let M be the Gram Matrix of $\langle \mathfrak{o}_K, \mathrm{Tr}_{K/\mathbb{Q}}() \rangle$ with respect to $\{e_1, \ldots, e_m\}$, an integral basis of $\mathfrak{o}_K$. Let M_0 be the Gram matrix of $\langle \mathfrak{o}_K^0, \mathrm{Tr}_{K/\mathbb{Q}}()|_{\mathfrak{o}_K^0} \rangle$ with respect to $\{e_1 - e_2, e_2 - e_3, \ldots, e_{m-1} - e_m\}$. Then, M_0 is equal to $(\mathbb{B}_m^T M \mathbb{B}_m)_{(m,m)}$, the (m,m) minor of $\mathbb{B}_m^T M \mathbb{B}_m$ (the matrix obtained by deleting the last row and column).*

Proof   Let i, j be integers such that $1 \leq i, j < m$. Then,

$$\begin{aligned} (\mathbb{B}_m^T M \mathbb{B}_m)_{i,j} &= \sum_{k=1}^{m} \sum_{l=1}^{m} \mathbb{B}_{k,i} M_{k,l} \mathbb{B}_{l,j} \\ &= M_{i,j} - M_{i,j+1} - M_{i+1,j} + M_{i+1,j+1} \\ &= \mathrm{Tr}_{K/\mathbb{Q}}(e_i e_j) - \mathrm{Tr}_{K/\mathbb{Q}}(e_i e_{j+1}) - \mathrm{Tr}_{K/\mathbb{Q}}(e_{i+1} e_j) + \mathrm{Tr}_{K/\mathbb{Q}}(e_{i+1} e_{j+1}) \\ &= \mathrm{Tr}_{K/\mathbb{Q}}\big((e_i - e_{i+1})(e_j - e_{j+1})\big) \\ &= (M_0)_{i,j}. \qquad\blacksquare \end{aligned}$$

Corollary   *Let K be a tame cyclic number field of degree $m \neq 1$. There exists a basis of $\mathfrak{o}_K^0$ such that the Gram matrix of $\langle \mathfrak{o}_K^0, \mathrm{Tr}_{K/\mathbb{Q}}()|_{\mathfrak{o}_K^0} \rangle$ with respect to such basis is equal to the (m,m) minor of*

$$\sum_{d|m} a_d \mathbb{B}_m^T A_d \mathbb{B}_m,$$

where the coefficients a_d are given in Lemmas 3.7, 3.10, and 4.3 of [9] and depend solely on the discriminant of K. See also Definition 2.5.

Proof   Since

$$M = \sum_{d|m} a_d A_d,$$

the corollary is an immediate consequence of Proposition 2.5 and [9, Theorems 4.2 and 4.5]. $\blacksquare$

2.1.1 The matrix $A(\mathfrak{d})$.

Given a prime p, we denote by v_p the usual p-adic valuation on the rationals.

Definition 2.3 Suppose that $m > 0$ and $\mathfrak{d}$ are integers, and let p be a prime. Suppose that $m \neq v_p(\mathfrak{d})$. The p-ramification index of $\mathfrak{d}$ is the rational number defined as

$$e_p(\mathfrak{d}) := \frac{m}{m - v_p(\mathfrak{d})}.$$

Remark 2.7 The above definition is motivated by the following fact: If K is a Galois number field of degree m and discriminant $\mathfrak{d}$, then $e_p(\mathfrak{d})$ is the ramification index of p in K for any prime p that is not wildly ramified in K.

Definition 2.4 Let $m > 1$ and $\mathfrak{d} \neq 0$ be integers. Let $\mathrm{div}(\mathfrak{d})$ be the set of prime divisors of $\mathfrak{d}$. Let $1 = d_1 < d_2 < \cdots < d_{\tau(m)} = m$ be the set of positive divisors of m. Let

$$P(m) := \left\{ \left(d_2^{\varepsilon_2}, d_3^{\varepsilon_3}, \ldots, d_{\tau(m)}^{\varepsilon_{\tau(m)}} \right) \in \mathbb{Z}^{\tau(m)-1} : \varepsilon_i \in \{0,1\} \text{ for all } i \right\},$$

and for every $\vec{v} \in P(m)$, let

$$\mathrm{lcm}(\vec{v}) := \mathrm{lcm}\left[d_2^{\varepsilon_2}, d_3^{\varepsilon_3}, \ldots, d_{\tau(m)}^{\varepsilon_{\tau(m)}} \right],$$

$$\gcd(\vec{v}) := \gcd\left(d_2^{\varepsilon_2}, d_3^{\varepsilon_3}, \ldots, d_{\tau(m)}^{\varepsilon_{\tau(m)}} \right),$$

and for every divisor d of m, let

$$P_d := \{ \vec{v} \in P(m) : \mathrm{lcm}(\vec{v}) = d \}.$$

If $d > 1$ is a divisor of m, let

$$\mathbb{P}_d := \{ p \in \mathrm{div}(\mathfrak{d}) : e_p(\mathfrak{d}) = d \}$$

and

$$w_d := \prod_{p \in \mathbb{P}_d} p \text{ and } f_d := \frac{w_d - 1}{d}.$$

Definition 2.5 Let $m > 0$ and $\mathfrak{d}$ be integers. For d, a divisor of m not equal to 1, we let

$$a_d := \sum_{\vec{v} \in P_d} \left(\gcd(\vec{v}) \prod_{\varepsilon_i = 0} w_{d_i} \prod_{\varepsilon_j = 1} (-f_{d_j}) \right)$$

and let $a_1 := \prod_{p \in \mathrm{div}(\mathfrak{d})} p$. Let $A(\mathfrak{d})$ be the $(m-1) \times (m-1)$ matrix defined as

$$A(\mathfrak{d}) := \sum_{\substack{d \mid m \\ d \neq m}} a_d \widehat{A}_d,$$

where $\widehat{A}_d := \left(\mathbb{B}_m^T A_d \mathbb{B}_m \right)_{(m,m)}.$

Example 2.8   Let $m = 9$ and $\mathfrak{d} = 9,644,443,241,083,841,416,681 = 7^6 \cdot 13^6 \cdot 19^8$. Here, the set of positive divisors of m is $1 < 3 < 9$ and $\mathrm{div}(\mathfrak{d}) = \{7, 13, 19\}$. Hence, $P(9)$ is the subset of $\mathbb{Z}^2$ given by

$$P(9) = \{(1,1), (1,9), (3,1), (3,9)\},$$

and thus

$$P_3 = \{(3,1)\} \text{ and } P_9 = \{(1,9), (3,9)\}.$$

On the other hand, $e_7(\mathfrak{d}) = 3$, $e_{13}(\mathfrak{d}) = 3$, and $e_{19}(\mathfrak{d}) = 9$. Thus, $\mathbb{P}_3 = \{7, 13\}$ and $\mathbb{P}_9 = \{19\}$. Therefore, $w_3 = 91$, $f_3 = 30$, and $w_9 = 19$, $f_9 = 2$. From this, we calculate that

$$a_3 = 1 \cdot 19 \cdot (-30) = -570 \text{ and } a_9 = 1 \cdot 91 \cdot (-2) + 3 \cdot 1 \cdot (60) = -2;$$

moreover, $a_1 = 7 \cdot 13 \cdot 19 = 1,729$. Since A_1 is the identity matrix of dimension 9, we have that

$$A(\mathfrak{d}) = 1,729(\mathbb{B}_9^t \mathbb{B}_9)_{(9,9)} - 570(\mathbb{B}_9^t A_3 \mathbb{B}_9)_{(9,9)}.$$

In other words,

$$A(\mathfrak{d}) = \begin{pmatrix} 2,318 & -1,159 & 570 & -1,140 & 570 & 570 & -1,140 & 570 \\ -1,159 & 2,318 & -1,159 & 570 & -1,140 & 570 & 570 & -1,140 \\ 570 & -1,159 & 2,318 & -1,159 & 570 & -1,140 & 570 & 570 \\ -1,140 & 570 & -1,159 & 2,318 & -1,159 & 570 & -1,140 & 570 \\ 570 & -1,140 & 570 & -1,159 & 2,318 & -1,159 & 570 & -1,140 \\ 570 & 570 & -1,140 & 570 & -1,159 & 2,318 & -1,159 & 570 \\ -1,140 & 570 & 570 & -1,140 & 570 & -1,159 & 2,318 & -1,159 \\ 570 & -1,140 & 570 & 570 & -1,140 & 570 & -1,159 & 2,318 \end{pmatrix}.$$

Example 2.9   Suppose that $m = \ell$ is a prime number. In such case,

$$A(\mathfrak{d}) = a_1 \widehat{A}_1 = \mathrm{rad}(\mathfrak{d}) \left(\mathbb{B}_\ell^T A_1 \mathbb{B}_\ell \right)_{(\ell,\ell)} = \mathrm{rad}(\mathfrak{d}) \left(\mathbb{B}_\ell^T \mathbb{B}_\ell \right)_{(\ell,\ell)} = \mathrm{rad}(\mathfrak{d}) \mathcal{A}_{\ell-1}.$$

Now, we are in position to state and prove one of the main theorems in the paper.

Theorem 2.10   *Let m be an integer not equal to 1, and let K be a tame $\mathbb{Z}/m\mathbb{Z}$-number field of discriminant $\mathfrak{d}(K)$. There exists a $\mathbb{Z}$-basis of $\mathfrak{o}_K^0$ such that the Gram matrix of*

$$\left\langle \mathfrak{o}_K^0, \mathrm{Tr}_{K/\mathbb{Q}}()|_{\mathfrak{o}_K} \right\rangle$$

with respect to such basis is equal to

$$A(\mathfrak{d}(K)).$$

In particular, if L is a tame $\mathbb{Z}/m\mathbb{Z}$-number field, then

$$\left\langle \mathfrak{o}_K^0, \mathrm{Tr}_{K/\mathbb{Q}}()|_{\mathfrak{o}_K} \right\rangle \simeq \left\langle \mathfrak{o}_L^0, \mathrm{Tr}_{L/\mathbb{Q}}()|_{\mathfrak{o}_L} \right\rangle \text{ if and only if } \mathfrak{d}(K) = \mathfrak{d}(L).$$

Proof   For each d divisor of m, let

$$\widehat{A}_d := \left(\mathbb{B}_m^T A_d \mathbb{B}_m \right)_{(m,m)}$$

be the $(m-1) \times (m-1)$ matrix obtained by erasing the last row and column of $\mathbb{B}_m^T A_d \mathbb{B}_m$. By definition, all the entries in A_m are equal to 1, and hence the columns of $\mathbb{B}_m$ belong to $\mathrm{Ker}(A_m)$. In particular, $\mathbb{B}_m^T A_m \mathbb{B}_m = 0$, and thus the result follows from Corollary 2.6 and [9, Theorems 4.2 and 4.5]. ∎

Example 2.11 There are four $\mathbb{Z}/9\mathbb{Z}$-number fields with discriminant $\mathfrak{d} = 7^6 \cdot 13^6 \cdot 19^8$ (see John Jones' database [5]). Since 3 is unramified in any of those fields, neither of the fields have wild ramification. Such fields are defined, respectively, by the following polynomials:

- $x^9 - x^8 - 578x^7 - 1,855x^6 + 87,155x^5 + 310,749x^4 - 4,599,958x^3 - 6,198,626x^2 + 102,071,235x - 169,800,379.$

- $x^9 - x^8 - 578x^7 - 1,855x^6 + 87,155x^5 + 518,229x^4 - 2,594,318x^3 - 22,409,730x^2 - 36,985,319x - 7,889,903.$

- $x^9 - x^8 - 578x^7 + 1,603x^6 + 88,884x^5 - 430,992x^4 - 3,668,027x^3 + 27,283,459x^2 - 40,339,579x - 7,447,279.$

- $x^9 - x^8 - 578x^7 + 1,603x^6 + 88,884x^5 - 119,772x^4 - 5,379,737x^3 - 3,169,418x^2 + 113,584,646x + 256,187,183.$

Let $A(\mathfrak{d})$ be the matrix calculated in Example 2.8. It follows from Theorem 2.10 that for each of those fields, there is a basis of the trace-zero integral module such that all the Gram matrices of the trace form in that basis are equal to the matrix $A(\mathfrak{d})$. This can be verified computationally, for instance, in MAGMA [2], using the code found in [8, Section 3.1].

2.2 Another explicit description

In this subsection, we show that if we apply the results obtained here to the case $m = \ell$, a prime, we recover the formulas obtained in [6]. We also see how some of the polynomial descriptions of the trace-zero form of [6] are extended to the general case of this paper.

Let n be a positive integer bigger than 1. The extended n-dimensional $\mathcal{A'}_n$ lattice is the lattice associated with the matrix

$$\mathcal{A'}_n := \mathbb{B}_n^T \mathbb{B}_n = \begin{pmatrix} 2 & -1 & 0 & 0 & \ldots & -1 \\ -1 & 2 & -1 & 0 & \cdots & 0 \\ 0 & -1 & 2 & -1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & -1 & 2 & -1 \\ -1 & 0 & 0 & 0 & -1 & 2 \end{pmatrix}.$$

For any positive integer n, we denote by 1_n the $n \times n$ matrix with all its entries equal to 1 and by I_n the identity matrix of dimension n

Lemma 2.12 Let m be an integer bigger than 1, and let $d \neq m$ be a positive divisor of m. Then,

$$\mathbb{B}_m^T A_d \mathbb{B}_m = 1_d \otimes \mathcal{A'}_{\frac{m}{d}}.$$

Proof   First notice that, for every $d|m$, we have $A_d = 1_d \otimes I_{\frac{m}{d}}$. After doing block multiplication, the result follows from the definition of $\mathcal{A}'_n$.   ∎

Applying Lemma 2.12 to the situation of Theorem 2.10, we deduce that the Gram matrix M_0 of $\langle \mathfrak{o}_K^0, \mathrm{Tr}_{K/\mathbb{Q}}()|_{\mathfrak{o}_K} \rangle$ in the given basis has the form

(2.1)
$$M_0 = \left(\sum_{\substack{d|m \\ d<m}} a_d 1_d \otimes \mathcal{A}'_{\frac{m}{d}} . \right)_{(m,m)} .$$

If m is equal to a prime ℓ, then the above equation is simply

$$M_0 = (a_1 \mathcal{A}'_\ell)_{(\ell,\ell)}.$$

Since $a_1 = \mathrm{rad}(\mathfrak{d}(K))$ and $(\mathcal{A}'_\ell)_{(\ell,\ell)}$ is the usual $(\ell-1)$-dimensional root lattice $\mathcal{A}_{\ell-1}$, the equation $M_0 = (a_1 \mathcal{A}'_\ell)_{(\ell,\ell)}$ is precisely [6, Theorem 2.9].

An explicit polynomial description of the integral trace-zero form is the following.

Corollary   *Let K be a tame totally real cyclic number field of degree $m > 1$. Then,*

$$\left\langle \mathfrak{o}_K^0, \mathrm{Tr}_{K/\mathbb{Q}}()\Big|_{\mathfrak{o}_K} \right\rangle$$

is the lattice associated with the form

$$\sum_{1 \le i \le j \le m-1} c_{i,j} x_i x_j,$$

where

$$c_{i,j} := \sum_{\substack{d|m, d \ne m \\ m|(i-j)d}} 2a_d - \sum_{\substack{d|m, d \ne m \\ m|(|i-j|-1)d}} a_d.$$

Proof   Note that, for every $d|m$ and $d \ne m$, we have

$$1_d \otimes \mathcal{A}'_{\frac{m}{d}} := \begin{cases} 2, & \text{if } (i-j) \equiv 0 \mod \left(\frac{m}{d}\right), \\ -1, & \text{if } |i-j| \equiv 1 \mod \left(\frac{m}{d}\right), \\ 0, & \text{otherwise.} \end{cases}$$

Then, the result follows from formula 2.1.   ∎

2.3   Equivalences on the shape of cyclic number fields

Finally, we show that for real cyclic fields, that have no wild ramification, the shape of the field is characterized by the discriminant. More specifically, we show the following theorem.

Theorem 2.14   *Let m be a positive integer, and let K and L be two totally real tame $\mathbb{Z}/m\mathbb{Z}$-number fields. Then, the following are equivalent:*

(a) $\langle \mathfrak{o}_K, \mathrm{Tr}_{K/\mathbb{Q}}() \rangle \simeq \langle \mathfrak{o}_L, \mathrm{Tr}_{L/\mathbb{Q}}() \rangle.$

(b) $(\mathfrak{o}_K^\perp, b_K) \simeq (\mathfrak{o}_L^\perp, b_L)$.

(c) $\left\langle \mathfrak{o}_K^0, \mathrm{Tr}_{K/\mathbb{Q}}()|_{\mathfrak{o}_K} \right\rangle \simeq \left\langle \mathfrak{o}_L^0, \mathrm{Tr}_{L/\mathbb{Q}}()|_{\mathfrak{o}_L} \right\rangle$.

(d) $\mathfrak{d}(K) = \mathfrak{d}(L)$.

Proof   The equivalence between (c) and (d) is Theorem 2.4; however, this equivalence also follows from Theorem 2.10. The equivalence between (a) and (d) follows from [9, Theorems 4.2 and 4.5]. Since K and L are totally real, the bilinear forms b_K and b_L are just the corresponding trace forms. Hence, $(b) \Rightarrow (d)$ follows from [11, Lemma 2.1]. To check the missing implication, we see that $(a) \Rightarrow (b)$ follows from [10, Lemma 5.1]   ∎

References

[1]   M. Bhargava and P. Harron, *The equidistribution of lattice shapes of rings of integers in cubic, quartic, and quintic number fields.* Compos. Math. **152**(2016), no. 6, 1111–1120.

[2]   W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language.* J. Symbolic Comput. **24**(1997), 235–265; **34**, V2.16-5 and V2.16-12.

[3]   R. Harron, *The shapes of pure cubic fields.* Proc. Amer. Math. Soc. **145**(2017), no. 2, 509–524.

[4]   R. Harron, *Equidistribution of shapes of complex cubic fields of fixed quadratic resolvent.* Algebra Number Theory **15**(2021), no. 5, 1095–1125.

[5]   J. Jones and D. Roberts, *A data base of number fields.* LMS J. Comput. Math. **17**(2014), no. 1, 595–618.

[6]   G. Mantilla and M. Monsurrò, *The shape of $\mathbb{Z}/\ell\mathbb{Z}$ -number fields.* Ramanujan J. **39**(2016), no. 3 451–463.

[7]   G. Mantilla-Soler, *Integral trace forms associated to cubic extensions.* Algebra Number theory **4**(2010), no. 6, 681–699.

[8]   G. Mantilla-Soler, *On number fields with equivalent integral trace forms.* Int. J. Number Theory **8**(2012), no. 7, 1569–1580.

[9]   G. Mantilla-Soler and W. Bolaños, *The trace form over cyclic number fields.* Canad. J. Math. **73**(2021), no. 4, 947–969.

[10]   G. Mantilla-Soler and C. Rivera, *Real S_n number fields and trace forms.* Preprint, 2019. arXiv:1812.03133v3

[11]   G. Mantilla-Soler and C. Rivera, *A proof of a conjecture on trace-zero forms and shapes of number fields.* Res. Number Theory **6**(2020), 35.

[12]   W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, Springer Monographs in Mathematics, 67, Springer, Berlin–Heidelberg, 2004.

Department of Mathematics, Fundación Universitaria Konrad Lorenz, Bogotá, Colombia
e-mail: wilmarr.bolanosc@konradlorenz.edu.co

Department of Mathematics, Universidad Nacional de Colombia sede Medellín, Medellín, Colombia
e-mail: gmantelia@gmail.com