ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 47, Number 4, 2017

THE INTEGRAL TRACE FORM OF CYCLIC EXTENSIONS OF ODD PRIME DEGREE

EVERTON LUIZ DE OLIVEIRA, J. CARMELO INTERLANDO,
TRAJANO PIRES DA NÓBREGA NETO
AND JOSÉ OTHON DANTAS LOPES

ABSTRACT. Let $L/\mathbb{Q}$ be a cyclic extension of degree p, where p is an odd unramified prime in $L/\mathbb{Q}$. An explicit description of the integral trace form $\mathrm{Tr}_{L/\mathbb{Q}}(x^2)|_{\mathfrak{O}_L}$, where $\mathfrak{O}_L$ is the ring of algebraic integers of L, is given, and an application to finding the minima of certain algebraic lattices is presented.

1. Introduction. The integral trace form associated to a number field F is the integral quadratic form given by $\mathrm{Tr}_{F/\mathbb{Q}}(x\overline{x}) \mid \mathfrak{O}_F$, where $\mathfrak{O}_F$ is the ring of algebraic integers of F. The book by Conner and Perlis [**4**] provides a thorough account on the subject. The papers by Scharlau [**14**] and Epkenhans [**6**] contain relevant extensions of two results by Conner and Perlis concerning, respectively, Witt equivalence of nondegenerate forms of number fields and existence of a field having a prescribed quadratic form. Both papers also give an account of several relevant developments on the subject. Particularly noteworthy is the extensive work of Bayer on the trace form in cyclotomic fields in connection with knot theory, see [**1, 2, 3**], for example. More recently, a description of the trace form in cyclotomic fields, amenable to computations, was given in [**8**].

One of the important applications of the trace form is to the study of lattices associated to number fields [**5,** pages 224–225]: Let $F/\mathbb{Q}$ be a Galois extension, $\sigma_1, \ldots, \sigma_n$ the automorphisms of F, and $\sigma_F : \mathfrak{O}_F$

2010 AMS *Mathematics subject classification.* Primary 11E12, 11H31, 11H50, 11R18, 11R33.

Keywords and phrases. Cyclotomic fields, cyclic extensions, Galois module theory, integral trace forms, lattice packings.

The first author was supported by the CAPES Foundation, Ministry of Education of Brazil, grant No. 3001-13-0.

Received by the editors on May 6, 2015, and in revised form on October 20, 2015.

DOI:10.1216/RMJ-2017-47-4-1075

$\to \mathbb{R}^n$ the canonical embedding of $\mathfrak{O}_F$ in $\mathbb{R}^n$. If $\mathcal{M}$ is a free $\mathbb{Z}$-submodule of $\mathfrak{O}_F$ of rank n, then $\sigma_F(\mathcal{M})$ is an n-dimensional lattice [**13,** page 56] whose minimum is given by $d^2 = \min\{|\sigma_F(x)|^2 \mid x \in \mathcal{M}, x \neq 0\}$, where

$$|\sigma_F(x)|^2 = \begin{cases} \mathrm{Tr}_{F/\mathbb{Q}}(x^2) & \text{if } F \text{ is totally real;} \\ (1/2)\ \mathrm{Tr}_{F/\mathbb{Q}}(x\overline{x}) & \text{if } F \text{ is totally complex,} \end{cases}$$

see [**5,** page 225]. The center density of $\sigma_F(\mathcal{M})$ is equal to

$$\delta = \frac{(d/2)^n}{\sqrt{|\mathrm{Disc}\,(F)|}[\mathfrak{O}_F : \mathcal{M}]}\,, \tag{1.1}$$

where Disc (F) denotes the discriminant of F regarded as an extension of $\mathbb{Q}$ [**13,** page 57].

Motivated by the above application, in particular, the determination of lattice minima, the objective of the present work is to find an explicit description of the integral trace form of certain number fields L. For simplicity, the focus will be on tamely ramified cyclic extensions $L/\mathbb{Q}$ of odd prime degree which possess a normal integral basis. In Section 2, after relevant properties of Abelian extensions are briefly reviewed, the main result, namely, the trace form, is derived. In Section 3, the calculation of the minimum of the form restricted to a submodule of $\mathfrak{O}_L$ is presented along with applications. These include the construction of three-, five- and seven-dimensional lattices whose packing densities can be made arbitrarily close to optimum in those dimensions. Lastly, Section 4 contains the conclusions.

2. Cyclic extensions of $\mathbb{Q}$ of degree p. Let $L/\mathbb{Q}$ be a cyclic extension of odd prime degree p and conductor n where p is unramified in $L/\mathbb{Q}$, that is, $L/\mathbb{Q}$ is tamely ramified. The conductor of L is of the form $n = p_1 \cdots p_s$, where $p_1, \ldots, p_s$ are distinct odd primes with $p_j \equiv 1 \pmod{p}$, $j = 1, \ldots, s$ and Disc $(L) = n^{p-1}$, see [**4,** page 186]. Let $\zeta_n \in \mathbb{C}$ be a primitive nth root of unity and $K = \mathbb{Q}(\zeta_n)$. If θ is a generator of Gal $(L/\mathbb{Q})$ and $t = \mathrm{Tr}_{K/L}(\zeta_n)$, then L can be expressed as $L = \mathbb{Q}(t)$, and $\{t, \theta(t), \ldots, \theta^{p-1}(t)\}$ is an integral basis for L, see [**11,** page 166]. This statement is the Hilbert-Speiser theorem, namely, if L is an absolute Abelian field, then $L/\mathbb{Q}$ has a normal integral basis if and only if $L/\mathbb{Q}$ is tamely ramified [**11,** page 187]. This, in turn, is a special case of Leopoldt's theorem [**9, 10**]: If $\mathscr{G} = \mathrm{Gal}(L/\mathbb{Q})$ and

$A_{L/\mathbb{Q}} = \{\alpha \in \mathbb{Q}[\mathscr{G}] \mid \alpha\mathfrak{O}_L \subset \mathfrak{O}_L\}$ (associated order of $L/\mathbb{Q}$), then $\mathfrak{O}_L = A_{L/\mathbb{Q}} \cdot w$ for a suitable $w \in \mathfrak{O}_L$.

Throughout this paper, G denotes $\mathrm{Gal}(K/\mathbb{Q})$ and H the subgroup of G that fixes L. Henceforth, the elements of G and H will be represented as s-tuples in $\mathbb{Z}_{p_1}^{\times} \times \cdots \times \mathbb{Z}_{p_s}^{\times}$, where $\mathbb{Z}_{p_j}^{\times}$ is the multiplicative group of integers modulo p_j, $j = 1, \dots, s$.

Lemma 2.1. *Let $x = (x_1, \dots, x_s) \in H$, $1 \leq q < s$, and let $\Pi : H \to \mathbb{Z}_{p_{j_1}}^{\times} \times \cdots \times \mathbb{Z}_{p_{j_q}}^{\times}$ be the projection defined by $\Pi(x) = (x_{j_1}, \dots, x_{j_q})$, with $1 \leq j_1 < \cdots < j_q \leq s$. Then,*

$$|\mathrm{Ker}\ \Pi| = \frac{\prod_{\ell=1}^{r}(p_{i_\ell} - 1)}{p},$$

where $1 \leq i_1 < \cdots < i_r \leq s$ are the coordinates of x distinct from $j_1, \dots, j_q$.

Proof. Let $Z = \mathbb{Z}_{p_{j_1}}^{\times} \times \cdots \times \mathbb{Z}_{p_{j_q}}^{\times}$ and $Z^c = \mathbb{Z}_{p_{i_1}}^{\times} \times \cdots \times \mathbb{Z}_{p_{i_r}}^{\times}$. Then,

$$H \leq \Pi(H) \times Z^c \leq G.$$

The index of H in G equals p, that is, either $\Pi(H) \times Z^c = H$ or $\Pi(H) \times Z^c = G$. The first equality cannot occur since, otherwise, H would have Z^c as a factor, which contradicts the hypothesis that the conductor of L equals n. Hence, Π is a surjecive homomorphism, that is, $H/\mathrm{Ker}\,\Pi \cong Z$. Therefore,

$$|\mathrm{Ker}\,\Pi| = \frac{\phi(n)/p}{(p_{j_1} - 1) \cdots (p_{j_q} - 1)} = \frac{\prod_{\ell=1}^{r}(p_{i_\ell} - 1)}{p}. \qquad \square$$

Given $z \in \Pi(H)$, we have

$$\Pi^{-1}(z) = x_0(\mathrm{Ker}\,\Pi)$$

where $z = \Pi(x_0)$. Hence, $|\Pi^{-1}(z)| = |\mathrm{Ker}\,\Pi|$. Henceforth, let $q_j = p_j - 1$ for $j = 1, \dots, s$, and

$$A_{i_1,\dots,i_r} = \frac{(p_{i_1} - 1) \cdots (p_{i_r} - 1)}{p} = \frac{q_{i_1} \cdots q_{i_r}}{p}$$

with $1 \leq i_1 < \cdots < i_r \leq s$.

Theorem 2.2. *Let θ be a generator of* $\operatorname{Gal}(L/\mathbb{Q})$ *and* $t = \operatorname{Tr}_{K/L}(\zeta_n)$. *Then,*

$$\operatorname{Tr}_{L/\mathbb{Q}}(t \cdot \theta^k(t)) \begin{cases} n - ((n-1)/p) & \textit{if } k = 0; \\ -(n-1)/p & \textit{if } k = 1, \ldots, p-1. \end{cases}$$

Proof. Let $h = \phi(n)/p$, so that $\operatorname{Tr}_{L/\mathbb{Q}}(t \cdot \theta^k(t)) = (1/h) \operatorname{Tr}_{K/\mathbb{Q}}(t \cdot \theta^k(t))$. We now seek to evaluate the latter expression. We have $\theta = \sigma_r \mid L$ for some $\sigma_r \in G$ defined by $\sigma_r(\zeta_n) = \zeta_n^r$. Hence,

$$t \cdot \theta^k(t) = \sum_{x,y \in H} \zeta_n^{x+yr^k}.$$

Let $x = (x_1, \ldots, x_s)$, $y = (y_1, \ldots, y_s) \in H$ and $r = (r_1, \ldots, r_s) \in \mathbb{Z}_{p_1}^\times \times \cdots \times \mathbb{Z}_{p_s}^\times$. Then,

$$\begin{aligned} \operatorname{Tr}_{K/\mathbb{Q}}(t \cdot \theta^k(t)) &= \sum_{x,y \in H} \operatorname{Tr}_{K/\mathbb{Q}}(\zeta_{p_1}^{x+yr^k} \cdots \zeta_{p_s}^{x+yr^k}) \\ &= \sum_{x,y \in H} \operatorname{Tr}_{\mathbb{Q}(\zeta_{p_1})/\mathbb{Q}}(\zeta_{p_1}^{x_1+y_1r_1^k}) \cdots \operatorname{Tr}_{\mathbb{Q}(\zeta_{p_s})/\mathbb{Q}}(\zeta_{p_s}^{x_s+y_sr_s^k}), \end{aligned}$$

where

$$\operatorname{Tr}_{\mathbb{Q}(\zeta_{p_j})/\mathbb{Q}}(\zeta_{p_j}^{x_j+y_jr_j^k}) = \begin{cases} p_j - 1 & \text{if } x_j + y_jr_j^k = 0; \\ -1 & \text{if } x_j + y_jr_j^k \neq 0, \end{cases}$$

for $j = 1, \ldots, s$. The proof will be split into two cases, namely, $k = 0$ and $1 \leq k \leq p-1$.

Case (i). $k = 0$. Let $x = (x_1, \ldots, x_s) \in H$. The extension $L/\mathbb{Q}$ is totally real. Then, the complex conjugation automorphism of K belongs to H; hence, $y = (-x_1, \ldots, -x_s) \in H$. In addition, y is the only element of H such that $x_j + y_j = 0$ for $j = 1, \ldots, s$. Hence,

$$\operatorname{Tr}_{\mathbb{Q}(\zeta_{p_1})/\mathbb{Q}}(\zeta_{p_1}^{x_1+y_1}) \cdots \operatorname{Tr}_{\mathbb{Q}(\zeta_{p_s})/\mathbb{Q}}(\zeta_{p_s}^{x_s+y_s}) = (p_1 - 1) \cdots (p_s - 1) = \phi(n),$$

and $h = |H|$ summation terms in (2.1) are equal to $\phi(n)$. Thus, the sum of these terms is equal to $T_0 = h\phi(n)$.

By Lemma 2.1, for each $1 \leq u \leq s$, there exist

$$\begin{aligned} S_{i_1,\ldots,i_u} = A_{i_1,\ldots,i_u} - \sum_{1\leq \ell_1 < \cdots < \ell_{u-1} \leq u} A_{i_{\ell_1},\ldots,i_{\ell_{u-1}}} + \cdots \\ + (-1)^{u-1} \sum_{\ell=1}^{u} A_{i_\ell} + (-1)^u \end{aligned}$$

elements $y = (y_1, \ldots, y_s) \in H$ such that $y_j + x_j = 0$ for each $j \neq i_1, \ldots, i_u$ and $x_{i_\ell} + y_{i_\ell} \neq 0$ for each $\ell = 1, \ldots, u$. In this case,

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_{p_1})/\mathbb{Q}}(\zeta_{p_1}^{x_1+y_1}) \cdots \mathrm{Tr}_{\mathbb{Q}(\zeta_{p_s})/\mathbb{Q}}(\zeta_{p_s}^{x_s+y_s}) = \frac{(-1)^u \phi(n)}{q_{i_1} q_{i_2} \cdots q_{i_u}}.$$

Hence, the sum of these terms equals

$$T_u = (-1)^u h \sum_{i_1 < \cdots < i_u} \frac{\phi(n)}{q_{i_1} \cdots q_{i_u}} \, S_{i_1,\ldots,i_u},$$

which is equal to

$$\begin{aligned} (-1)^u h \Bigg[\frac{1}{p} \Bigg(\binom{s}{s-u} \phi(n) - \cdots \\ + (-1)^{u-1} \binom{s-(u-1)}{s-u} \sum_{i_1 < \cdots < i_{u-1}} \frac{\phi(n)}{q_{i_1} \cdots q_{i_{u-1}}} \Bigg) \\ + (-1)^u \sum_{i_1 < \cdots < i_u} \frac{\phi(n)}{q_{i_1} \cdots q_{i_u}} \Bigg]. \end{aligned}$$

Therefore,

$$\begin{aligned} \mathrm{Tr}_{K/\mathbb{Q}}(t^2) &= T_0 + T_1 + \cdots + T_s \\ &= h \Bigg[\Bigg(1 + \frac{\sum_{j=1}^{s} (-1)^j \binom{s}{s-j}}{p} \Bigg) \phi(n) + \cdots \\ &\qquad + \Bigg(1 - \frac{\binom{1}{0}}{p} \Bigg) \sum_{i_1 < \cdots < i_{s-1}} \frac{\phi(n)}{q_{i_1} \cdots q_{i_{s-1}}} + 1 \Bigg] \end{aligned}$$

$$= h\bigg[\bigg(1-\frac{1}{p}\bigg)\bigg(\phi(n)+\sum_{i_1=1}^{s}\frac{\phi(n)}{q_{i_1}}+\cdots+\sum_{i_1<\cdots<i_{s-1}}\frac{\phi(n)}{q_{i_1}\cdots q_{i_{s-1}}}\bigg)+1\bigg]$$
$$= h\bigg[\frac{(p-1)(n-1)}{p}+1\bigg].$$

Case (ii). $k \neq 0$. As before, let $x = (x_1, \ldots, x_s) \in H$. We claim that $x + yr^k \neq 0$ for all $y \in H$. Indeed, if $y \in H$ is such that $x + yr^k = 0$, then $x = -yr^k \in r^k H$ since $-1 \in H$. On the other hand, $G/H \cong \mathrm{Gal}\,(L/\mathbb{Q})$. Hence, $G = H \cup \sigma_r H \cup \cdots \cup \sigma_{r^{p-1}} H$, that is, $\mathbb{Z}_n^\times = H \cup rH \cup \cdots \cup r^{p-1}H$ is a union of disjoint cosets, whence $x \notin H$, a contradiction. Therefore, the sum T_0 of the summation terms $\mathrm{Tr}_{\mathbb{Q}(\zeta_{p_1})/\mathbb{Q}}(\zeta_{p_1}^{x_1+y_1r_1^k}) \cdots \mathrm{Tr}_{\mathbb{Q}(\zeta_{p_s})/\mathbb{Q}}(\zeta_{p_s}^{x_s+y_sr_s^k})$ in (2.1) corresponding to the pairs $x, y \in H$ such that $x_j + y_j r_j^k = 0$ for all $1 \leq j \leq s$ is zero, that is, $T_0 = 0$.

Since $-xr^{-k} = (-x_1r_1^{-k}, \ldots, -x_sr_s^{-k}) \in \mathbb{Z}_{p_1}^\times \times \cdots \times \mathbb{Z}_{p_s}^\times$, it follows from Lemma 2.1 that, for $1 \leq u \leq s$, there exist

$$S_{i_1,\ldots,i_u} = A_{i_1,\ldots,i_u} - \sum_{1\leq \ell_1<\cdots<\ell_{u-1}\leq u} A_{i_{\ell_1},\ldots,i_{\ell_{u-1}}} + \cdots + (-1)^{u-1}\sum_{\ell=1}^{u} A_{i_\ell}$$

elements $y = (y_1, \ldots, y_s) \in H$ such that $y_j = -x_j r_j^{-k}$ for all $j \neq i_1, \ldots, i_u$ and $x_{i_\ell} + y_{i_\ell} r_{i_\ell}^{-k} \neq 0$ for all $\ell = 1, \ldots, u$. In this case, each summation term in (2.1) equals

$$\frac{(-1)^u \phi(n)}{q_{i_1} q_{i_2} \cdots q_{i_u}},$$

and their sum is given by

$$T_u = (-1)^u \frac{h}{p}\bigg(\binom{s}{s-u}\phi(n) - \binom{s-1}{s-u}\sum_{i_1=1}^{s}\frac{\phi(n)}{q_{i_1}} + \cdots$$
$$+ (-1)^{u-1}\binom{s-(u-1)}{s-u}\sum_{i_1<\cdots<i_{u-1}}\frac{\phi(n)}{q_{i_1}\cdots q_{i_{u-1}}}\bigg).$$

Therefore,

$$\mathrm{Tr}_{K/\mathbb{Q}}(t \cdot \theta^k(t)) = T_0 + T_1 + \cdots + T_s$$

$$= \frac{h}{p}\left[\left(\sum_{j=1}^{s}(-1)^j\binom{s}{s-j}\right)\phi(n) + \cdots - \binom{1}{0}\sum_{i_1<\cdots<i_{s-1}}\frac{\phi(n)}{q_{i_1}\cdots q_{i_{s-1}}}\right]$$
$$= -h\left(\frac{n-1}{p}\right). \qquad \square$$

With notation as in Theorem 2.2, we can now state the main result of the paper:

Corollary 2.3. *Let* $x = \sum_{i=0}^{p-1} a_i\theta^i(t)$ *be any element of the ring of integers* $\mathfrak{O}_L$*. Then,*

$$\mathrm{Tr}_{L/\mathbb{Q}}(x^2) = n\cdot\left(\sum_{i=0}^{p-1} a_i^2\right) - \frac{n-1}{p}\left(\sum_{i=0}^{p-1} a_i\right)^2. \tag{2.1}$$

Proof. From the hypothesis,

$$x^2 = \sum_{i,j=0}^{p-1} a_i a_j \theta^i(t)\theta^j(t).$$

Since

$$\mathrm{Tr}_{L/\mathbb{Q}}(\theta^i(t)\theta^j(t)) = \mathrm{Tr}_{L/\mathbb{Q}}(t\theta^{i-j}(t)),$$

we have

$$\begin{aligned}\mathrm{Tr}_{L/\mathbb{Q}}(x^2) &= \sum_{i,j=0}^{p-1} a_i a_j\,\mathrm{Tr}_{L/\mathbb{Q}}(t\theta^{i-j}(t))\\ &= \sum_{i=0}^{p-1} a_i^2\,\mathrm{Tr}_{L/\mathbb{Q}}(t^2) + \sum_{\substack{i,j=0\\ i\neq j}}^{p-1} a_i a_j\,\mathrm{Tr}_{L/\mathbb{Q}}(t\theta^{i-j}(t))\\ &= \left(n - \frac{n-1}{p}\right)\left(\sum_{i=0}^{p-1} a_i^2\right) - 2\left(\frac{n-1}{p}\right)\left(\sum_{\substack{i,j=0\\ i<j}}^{p-1} a_i a_j\right)\\ &= n\left(\sum_{i=0}^{p-1} a_i^2\right) - \frac{n-1}{p}\left(\sum_{i=0}^{p-1} a_i\right)^2. \qquad \square\end{aligned}$$

3. Minimum of the integral trace form in cyclic extensions of prime degree. In this section, we derive a procedure for finding the minimum of the form in (2.1) under the restriction that x is a nonzero element of the $\mathbb{Z}$-module $\mathcal{M}_m$, defined as:

$$\begin{multline} \{a_0 t + a_1\theta(t) + \cdots + a_{p-1}\theta^{p-1}(t) \in \mathfrak{O}_L \mid \\ a_0 + a_1 + \cdots + a_{p-1} \equiv 0 \pmod{m}\}, \end{multline} \tag{3.1}$$

where m is a fixed, positive integer. This problem arises in the determination of minima of point-lattices that are images of $\mathbb{Z}$-modules in $\mathfrak{O}_L$ via the canonical embedding [**13,** pages 56, 57].

The case $m = 1$ is easily handled: for $x \in \mathfrak{O}_L, x \neq 0$,

$$\mathrm{Tr}_{L/\mathbb{Q}}(x^2) \geq pN_{L/\mathbb{Q}}(x^2)^{1/p} \geq p,$$

where $N_{L/\mathbb{Q}}(\cdot)$ represents the norm. Since $\mathrm{Tr}_{L/\mathbb{Q}}(1) = p$, the minimum of $\mathrm{Tr}_{L/\mathbb{Q}}(x^2)$ for nonzero $x \in \mathfrak{O}_L$ equals p. Thus, the minimum of $\mathrm{Tr}_{L/\mathbb{Q}}(x^2)$ for $x \in \mathcal{M}_1$ and $x \neq 0$, equals p.

The case $m > 1$ is handled next. For each pair (i, j) with $i, j \in \{0, \ldots, p-1\}$ and $i \neq j$, define

$$\begin{array}{cccc} \tau_{ij}: & \mathbb{Z}^p & \longrightarrow & \mathbb{Z}^p \\ & (a_0, \ldots, a_{p-1}) & \longmapsto & (b_0, \ldots, b_{p-1}), \end{array}$$

where

$$b_k = \begin{cases} a_i - 1 & \text{if } k = i; \\ a_j + 1 & \text{if } k = j; \\ a_k & \text{otherwise.} \end{cases}$$

If $a = (a_0, \ldots, a_{p-1})$ and $b = (b_0, \ldots, b_{p-1})$ are such that $\tau_{ij}(a) = b$, then

$$\sum_{i=0}^{p-1} a_i = \sum_{i=0}^{p-1} b_i.$$

On the other hand, if the latter equality holds, then a composition of suitable τ_{ij} exists which maps a to b.

For brevity's sake, for any $a = (a_0, \ldots, a_{p-1}) \in \mathbb{Z}^p$, the sum $\sum_{i=0}^{p-1} a_i^2$ will be denoted by $||a||^2$.

Lemma 3.1. *With notation as above, let $a = (a_0, \ldots, a_{p-1})$ and $b = (b_0, \ldots, b_{p-1})$ be two elements of $\mathbb{Z}^p$ such that $\tau_{ij}(a) = b$. Then, $||a||^2 > ||b||^2$ if and only if $a_i - a_j > 1$.*

Proof. We have

$$||a||^2 > ||b||^2 \Leftrightarrow a_i^2 + a_j^2 > (a_i - 1)^2 + (a_j + 1)^2 \Leftrightarrow a_i - a_j > 1. \quad \square$$

In preparation for the next results, for any $a = (a_0, \dots, a_{p-1}) \in \mathbb{Z}^p$, we define the orbit of a as the set

$$\mathcal{O}(a) = \left\{ (b_0, \dots, b_{p-1}) \in \mathbb{Z}^p \;\middle|\; \sum_{i=0}^{p-1} b_i = \sum_{i=0}^{p-1} a_i \right\}.$$

Similarly, for any $x = a_0 t + a_1\theta(t) + \cdots + a_{p-1}\theta^{p-1}(t) \in \mathfrak{O}_L$, we define the orbit of x as the set

$$\mathcal{O}(x) = \left\{ b_0 t + b_1\theta(t) + \cdots + b_{p-1}\theta^{p-1}(t) \in \mathfrak{O}_L \;\middle|\; \sum_{i=0}^{p-1} b_i = \sum_{i=0}^{p-1} a_i \right\}.$$

Lemma 3.2. *Let S be a nonnegative integer, $a = (a_0, \dots, a_{p-1}) \in \mathbb{Z}^p$ with $a_0 + \cdots + a_{p-1} = S$, and q and r the quotient and remainder, respectively, of the division of S by p. Then,*

$$\min_{b \in \mathcal{O}(a)} ||b||^2 = pq^2 + 2rq + r,$$

and it is attained exactly at all $b \in \mathbb{Z}^p$ having r entries equal to $q + 1$ and $p - r$ entries equal to q.

Proof. By Lemma 3.1, any two entries of a p-tuple $b \in \mathcal{O}(a)$ with $||b||^2$ minimum may not differ by more than 1. Therefore, one such tuple must be a permutation of $(q + 1, \dots, q + 1, q, \dots, q)$, where the number of entries $= q + 1$ must be $\leq p - 1$. Hence, $S = pq + r$, which determines q and r uniquely. □

Theorem 3.3. *For $x = a_0 t + a_1\theta(t) + \cdots + a_{p-1}\theta^{p-1}(t) \in \mathfrak{O}_L$, let $S = S(x) = a_0 + \cdots + a_{p-1}$, and let q and r be the quotient and remainder, respectively, of the division of S by p. If $S \geq 0$, then*

$$M(S) := \min_{y \in \mathcal{O}(x)} \operatorname{Tr}_{L/\mathbb{Q}}(y^2) = pq^2 + 2rq + nr + \frac{1-n}{p} r^2. \tag{3.2}$$

Proof. The statement is an immediate consequence of Corollary 2.3 and Lemma 3.2. □

Corollary 3.4. *With notation as above,*

(i) *if* $S = 0$, *then* $\min_{y\in\mathcal{O}(x), y\neq 0} \mathrm{Tr}_{L/\mathbb{Q}}(y^2) = 2n$;
(ii) *if* $S > 0$ *and* $p \mid S$, *then* $\min_{j\in\mathbb{N}^* M(jS)} = S^2/p$.

In conclusion, if $p \mid S$, *then* $M(S) = \min\{2n, S^2/p\}$.

Proof. For (i), by Corollary 2.3, note that, for x in the orbit of zero but $x \neq 0$, the minimum of $\mathrm{Tr}_{L/\mathbb{Q}}(x^2)$ equals $2n$, and it is attained at $x = a_0t + a_1\theta(t) + \cdots + a_{p-1}\theta^{p-1}(t)$ with $(a_0, a_1, \ldots, a_{p-2}) = (1, -1, 0, \ldots, 0)$, or a permutation of it. For (ii), we have $S = pq$, so $q = S/p$ and $r = 0$, and the result follows from Theorem 3.3. □

Corollary 3.5. *With notation as above, if* $p \nmid S$, *then*

$$\min\{M(jS) \mid j \in \mathbb{N}^*\} = \min\{M(S), M(2S), \ldots, M(pS)\}.$$

Proof. The assertion follows from the fact that $\{jS \mid 1 \leq j \leq p\}$ is a complete set of residues modulo p and the observation that the expression on the right-hand side of (3.2) is a strictly increasing function of q. □

Corollaries 3.4 and 3.5 yield the following theorem, which is the main result of this section.

Theorem 3.6. *Let* m *be a positive integer and*

$$M^* = \min_{\substack{x\in\mathcal{M}_m \\ x\neq 0}} \mathrm{Tr}_{L/\mathbb{Q}}(x^2). \tag{3.3}$$

Then,

$$M^* = \begin{cases} \min\{2n, m^2/p\} & \text{if } p \mid m; \\ \min\{2n, M(m), \ldots, M(pm)\} & \text{otherwise.} \end{cases}$$

Remark 3.7. The proofs of Lemma 3.2 and Corollary 3.4 provide a procedure for determining the elements that achieve M^* in (3.3). More specifically, if $M^* = 2n$, then the minimum is attained at $x = a_0t+a_1\theta(t)+\cdots+a_{p-1}\theta^{p-1}(t)$ with $(a_0, a_1, \ldots, a_{p-2}) = (1, -1, 0, \ldots, 0)$, or a permutation of it; if $p \mid m$ and $M^* = m^2/p$, then the minimum is attained at $x = a_0t+a_1\theta(t)+\cdots+a_{p-1}\theta^{p-1}(t)$ with $(a_0, a_1, \ldots, a_{p-1}) =$

$(m/p, \ldots, m/p)$; otherwise, the minimum is attained at $x = a_0 t + a_1\theta(t) + \cdots + a_{p-1}\theta^{p-1}(t)$ with

$$(a_0, a_1, \ldots, a_{p-1}) = (\underbrace{q^* + 1, \ldots, q^* + 1}_{r^* \text{ copies}}, q^*, \ldots, q^*)$$

or a permutation of it, and $M(pq^* + r^*) = \min\{M(m), \ldots, M(pm)\}$. The procedure will be illustrated next.

Example 3.8. This example illustrates the use of Theorem 3.6 in finding M^* in (3.3) when $p = 3$, $n = 1123$ and $m = 67$. Since $p \nmid m$,

$$\begin{aligned} M^* &= \min\{2n, M(m), M(2m), M(3m)\} \\ &= \min\{2246, 2245, 6734, 13467\} \\ &= 2245. \end{aligned}$$

We have $q^* = 22$ and $r^* = 1$ $(67 = 3 \cdot 22 + 1)$, and the minimum is attained at all $x \in \mathfrak{O}_L$ of the form $a_0 t + a_1\theta(t) + a_2\theta^2(t)$, where $t = \mathrm{Tr}_{K/L}(\zeta_n)$, $\theta = \langle \mathrm{Gal}\,(L/\mathbb{Q})\rangle$ and $(a_0, a_1, a_2) = (23, 22, 22)$, or a permutation of it.

Now, consider the lattice $\Lambda := \sigma_L(\mathcal{M}_m)$. Its rank equals 3, and its center density is given by

$$\delta = \frac{\rho^3}{\sqrt{|\mathrm{Disc}\,(L)|} \cdot [\mathfrak{O}_L : \mathcal{M}_m]} = \frac{(\sqrt{M^*}/2)^3}{n \cdot m} = 0.17672.$$

Among all lattices of rank 3, that with the highest center density is the face-centered cubic lattice. Its center density equals $1/(4\sqrt{2}) = 0.17678$.

Example 3.9. This example illustrates the use of Theorem 3.6 in finding M^* in (3.3) when $p = 5$, $n = 92111$ and $m = 607$. Since $p \nmid m$,

$$\begin{aligned} M^* &= \min\{2n, M(m), M(2m), M(3m), M(4m), M(5m)\} \\ &= \min\{184222, 736897, 184223, 1289570, 295245, 1842245\} \\ &= 184222. \end{aligned}$$

The minimum is attained at all $x \in \mathfrak{O}_L$ of the form $a_0 t + a_1\theta(t) + a_2\theta^2(t) + a_3\theta^3(t) + a_4\theta^4(t)$, where $t = \mathrm{Tr}_{K/L}(\zeta_n)$, $\theta = \langle \mathrm{Gal}\,(L/\mathbb{Q})\rangle$, and $(a_0, a_1, a_2, a_3, a_4) = (1, -1, 0, 0, 0)$, or a permutation of it.

Now, consider the lattice $\Lambda := \sigma_L(\mathcal{M}_m)$. Its rank equals 5, and its center density is given by

$$\delta = \frac{\rho^5}{\sqrt{|\mathrm{Disc}\,(L)|} \cdot [\mathfrak{O}_L : \mathcal{M}_m]} = \frac{(\sqrt{M^*}/2)^5}{n^2 \cdot m} = 0.08838.$$

Among all lattices of rank 5, that with the highest center density is D_5. Its center density equals $1/(8\sqrt{2}) = 0.08839$.

Example 3.10. This example illustrates the use of Theorem 3.6 in finding M^* in (3.3) when $p = 7$, $n = 600601$ and $m = 1096$. Since $p \nmid m$,

$$\begin{aligned} M^* &= \min\{2n, M(m), M(2m), M(3m), \\ &\qquad M(4m), M(5m), M(6m), M(7m)\} \\ &= \min\{1201202, 1201210, 3603638, 7207284, \\ &\qquad 1201204, 2402422, 4804858, 8408512\} \\ &= 1201202. \end{aligned}$$

The minimum is attained at all $x \in \mathfrak{O}_L$ of the form $a_0 t + a_1\theta(t) + a_2\theta^2(t) + a_3\theta^3(t) + a_4\theta^4(t)$, where $t = \mathrm{Tr}_{K/L}(\zeta_n)$, $\theta = \langle \mathrm{Gal}\,(L/\mathbb{Q})\rangle$ and $(a_0, a_1, a_2, a_3, a_4, a_5, a_6) = (1, -1, 0, 0, 0, 0, 0)$, or a permutation of it.

Now, consider the lattice $\Lambda := \sigma_L(\mathcal{M}_m)$. Its rank equals 7, and its center density is given by

$$\delta = \frac{\rho^7}{\sqrt{|\mathrm{Disc}\,(L)|} \cdot [\mathfrak{O}_L : \mathcal{M}_m]} = \frac{(\sqrt{M^*}/2)^7}{n^3 \cdot m} = 0.0624996.$$

Among all lattices of rank 7, that with the highest center density is Λ_7. Its center density equals $1/16 = 0.0625$.

4. Conclusion.

The integral trace form $\mathrm{Tr}_{L/\mathbb{Q}}(x^2)$, $x \in \mathfrak{O}_L$, where $L/\mathbb{Q}$ is a cyclic extension of odd prime degree p with p unramified in $L/\mathbb{Q}$, was presented in an explicit manner, amenable to computations. In particular, the presentation allowed us to find the minimum of the form under the restriction that x was a non-zero element of a certain sub-module of $\mathfrak{O}_L$. An application of this result was the construction of p-dimensional lattices via the Minkowski homomophism from $\mathfrak{O}_L$ to $\mathbb{R}^p$.

Future directions for the present work include:

(i) determining other p-dimensional lattices for values of p larger than those considered here, and

(ii) extending it to address wildly ramified extensions $L/\mathbb{Q}$, where a normal integral basis does not exist.

Finally, lattices obtained from suitable fractional ideals in absolute Abelian extensions might be interesting: related to this are the works of Erez **[7]**, Pickett **[12]** and Vinatier **[15, 16]** concerning the ambiguous ideal which is the square root of the different inverse.

Acknowledgments. The authors sincerely thank the editor for handling the manuscript and the referee for his/her careful reading and for pointing out further relevant references on the subject.

REFERENCES

1. E. Bayer, *Factorisation is not unique for higher dimensional knots*, Comm. Math. Helv. **55** (1980), 583–592.

2. ______, *Unimodular Hermitian and skew-Hermitian forms*, J. Algebra **74** (1982), 341–373.

3. ______, *Definite Hermitian forms and the cancellation of simple knots*, Arch. Math. **40** (1983), 182–185.

4. P.E. Conner and R. Perlis, *A survey of trace forms of algebraic number fields*, World Scientific Publishing Co., Singapore, 1984.

5. J.H. Conway and N.J.A. Sloane, *Sphere packings, lattices, and groups*, Springer Verlag, New York, 1999.

6. M. Epkenhans, *On trace forms of algebraic number fields*, Arch. Math. **60** (1993), 527–529.

7. B. Erez, *The Galois structure of the trace form in extensions of odd prime degree*, J. Algebra **118** (1988), 438–446.

8. J.C. Interlando, T.P. da Nóbrega Neto, T.M. Rodrigues and J.O.D. Lopes, *A note on the integral trace form in cyclotomic fields*, J. Alg. Appl. **14** (2015) article id 1550045.

9. H.W. Leopoldt, *Uber die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers*, J. reine angew. Math. **201** (1959), 119–149.

10. G. Lettl, *The ring of integers of an Abelian number field*, J. reine angew. Math. **404** (1990), 162–170.

11. W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, Springer Mono. Math., Springer-Verlag, Berlin, 2004.

12. E.J. Pickett and S. Vinatier, *Self-dual integral normal bases and Galois module structure*, Compositio Math. **149** (2013), 1175–1202.

13. P. Samuel, *Algebraic theory of numbers*, Hermann, Paris, 1970.

14. W. Scharlau, *On trace forms of algebraic number fields*, Math. Z. **196** (1987), 125–127.

15. S. Vinatier, *Structure galoisienne dans les extensions faiblement ramifiées de* $\mathbb{Q}$, J. Num. Theory **91** (2001), 126–152.

16. ———, *p-extensions faiblement ramifiées*, Publ. Math. Besan., University of Franche-Comté, Besançon.

Universidade Federal de Mato Grosso do Sul, Instituto de Matemática, Campo Grande, MS, 79074-460 Brazil
Email address: **everton.luiz@ufms.br**

San Diego State University, Department of Mathematics and Statistics, San Diego, CA 92182
Email address: **carmelo.interlando@sdsu.edu**

Universidade Estadual Paulista, Departamento de Matemática, São José do Rio Preto, SP, 15054-000 Brazil
Email address: **trajano@sjrp.unesp.br**

Universidade Federal do Ceará, Departamento de Matemática, Fortaleza, CE, 60455-900 Brazil
Email address: **othon@mat.ufc.br**