Canad. J. Math. Vol. 73 (4), 2021 pp. 947–969
http://dx.doi.org/10.4153/S0008414X20000255

The Trace Form Over Cyclic Number Fields

Wilmar Bolaños and Guillermo Mantilla-Soler

Abstract. In the mid 80's Conner and Perlis showed that for cyclic number fields of prime degree p the isometry class of integral trace is completely determined by the discriminant. Here we generalize their result to tame cyclic number fields of arbitrary degree. Furthermore, for such fields, we give an explicit description of a Gram matrix of the integral trace in terms of the discriminant of the field.

1 Introduction

An interesting arithmetic invariant of a number field K is its integral trace form, i.e., the integral quadratic form obtained by restricting the bilinear trace pairing

$$(x, y) \mapsto \mathrm{Tr}_K(x \cdot y)$$

to the maximal order $\mathfrak{o}_K$. One of several reasons why the integral trace is of importance in number theory (see [1, 2, 3, 6, 9]) is that it is a refinement of the discriminant $\mathfrak{d}_K$. Moreover, by a result of Tausky (see [16]) the integral trace is also a refinement of the signature. It follows that two necessary conditions for two number fields K and L to have isometric integral traces is that they have equal degrees and equal discriminants. A result of Conner and Perlis form the early 80's states that if the fields in question are Galois and of prime degree then such conditions are also sufficient:

Theorem 1.1 [5, §IV] *Let p be an odd prime and let K, L be two $\mathbb{Z}/p\mathbb{Z}$-number*[1] *fields. Then*

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

The objective of this paper is to generalize the above result to cyclic extensions of arbitrary degree. At the moment we can do so under the additional hypothesis that the fields are *tame number fields* i.e., that there is no rational prime that ramifies wildly in either field. Our main result is the following:

Theorem (cf. Theorem 4.2 and Theorem 4.5). *Let n be a positive integer and let K, L be two tame $\mathbb{Z}/n\mathbb{Z}$-number fields. Then*

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

Received by the editors July 28, 2019; revised March 21, 2020.
Published online on Cambridge Core April 14, 2020.
AMS subject classification: **11R04, 11R18, 11R29, 11R32.**
Keywords: Cyclic number fields, trace form.

[1]Recall that for a finite group G a number field K is called a *G-number field* if the Galois closure of $K/\mathbb{Q}$ has Galois group isomorphic to G.

Remark 1.2 Given two number fields K, L, we say they have isometry integral trace, $\langle \mathfrak{o}_K, \mathrm{Tr}_{K/\mathbb{Q}} \rangle \cong \langle \mathfrak{o}_L, \mathrm{Tr}_{L/\mathbb{Q}} \rangle$, if and only if there exist a $\mathbb{Z}$-linear isomorphism $\varphi : \mathfrak{o}_K \to \mathfrak{o}_L$ such that

$$\mathrm{Tr}_{K/\mathbb{Q}}(x \cdot y) = \mathrm{Tr}_{L/\mathbb{Q}}(\varphi(x) \cdot \varphi(y)) \text{ for every } x, y \in \mathfrak{o}_K.$$

Remark 1.3 We should note that in the above situation our result implies that the signature of K is determined by its discriminant and its degree; this is not surprising if the degree n is odd since in such a case K is totally real. However, for even n this is saying something not at all obvious not even from the point of view of the genus of the integral trace.

1.1 A Duality Between $\mathbb{Z}/n\mathbb{Z}$ and S_n Number Fields

Let K be a totally real degree n number field, and let $G(K)$ be the Galois group of the Galois closure of K over $\mathbb{Q}$. If we wanted to try to define a sort of notion of complexity for the field K in terms of the group $G(K)$ we could say that such complexity is very high if $G(K)$ is as big as it can be; i.e., if $G(K) \cong S_n$. At the other side of the spectrum, we could argue that the such complexity is very low if $G(K)$ is as uncomplicated as it can be. For instance, it should have the smallest possible order, n, and among those it should have not many automorphisms; for example degree 4 extensions with cyclic Galois group should be "easier" than those with Galois group the Klein group. The group $G(K) \cong \mathbb{Z}/n\mathbb{Z}$ meets such requirements. The results presented in this paper are about the behavior of the trace in the low complexity case; in this case, under some ramification assumptions, the trace as an invariant is just the same as the discriminant. In contrast, for the high complexity case (see [10]) the trace, under some ramification hypotheses as well, is a complete invariant. In other words the strength of the invariant $\langle \mathfrak{o}_K, \mathrm{Tr}_{K/\mathbb{Q}} \rangle$ with respect to $\mathfrak{d}(K)$ presents a duality that seems to be determined, at least in the extreme cases, from the complexity of the group $G(K)$. In the recent preprint [8] the authors show that the shape is a complete invariant for V_4-quartic fields. As we explained above the complexity of V_4-quartic extensions should be greater than that of $\mathbb{Z}/4\mathbb{Z}$-quartics, however intuition says that perhaps it should not be at the same level of S_4-quartics. It would be interesting to see if the informal notion of complexity described above really exists or if it is only a fact about S_n and $\mathbb{Z}/n\mathbb{Z}$-extensions.

1.2 Structure of the Paper

In §2 we set up the notation, and facts, that we will use later in our proofs regarding Hermitian forms over group rings. Then we start with the proofs of our results. The overall strategy is the following: We know by the Hilbert-Speiser theorem that the fields we study have a normal integral basis (NIB). Using Hermitian forms on abelian groups, and the Kronecker-Weber theorem, we construct a specific NIB and we show that the Gram matrix of the trace, with respect such a basis, depends solely on the discriminant and the degree of the field. This strategy is executed in several stages; in §3 we deal with number fields of prime power degree, there also dealing with different levels:

(a) First we deal with number fields of prime power discriminant, and odd degree.

https://doi.org/10.4153/S0008414X20000255 Published online by Cambridge University Press

(b) Then we deal with general discriminants, but still odd degree.
(c) Then we deal with the case of degree a power of 2.

Finally in §4, using that the number field has a cyclic Galois group, we do a gluing construction to pass from prime power degree to general degree. Here too we must make the distinction between odd and even degrees.

2 Hermitian Forms Over Group Rings

Let G be a finite abelian group, and let $\mathbb{Z}[G]$ be the group ring of G over $\mathbb{Z}$. Let $X \to \overline{X}$ be the usual involutary ring automorphism of $\mathbb{Z}[G]$ such that for every $g \in G$, $g \to \overline{g} = g^{-1}$. The projection map, which is a morphism of $\mathbb{Z}[G]$-modules, and the augmentation map, which is a ring homomorphism, are given by

$$\Pr : \mathbb{Z}[G] \longrightarrow \mathbb{Z} \qquad\qquad \varepsilon : \mathbb{Z}[G] \longrightarrow \mathbb{Z}$$

$$\Pr\left(\sum_{g\in G} d_g g\right) = d_e, \qquad\qquad \varepsilon\left(\sum_{g\in G} d_g g\right) = \sum_{g\in G} d_g,$$

where $e \in G$ denotes the identity of G. A *Hermitian form* on a left $\mathbb{Z}[G]$-module M is a $\mathbb{Z}$-bilinear map

$$H : M \times M \to \mathbb{Z}[G]$$

such that for all $X \in \mathbb{Z}[G]$ and $m_1, m_2 \in M$:

$$H(Xm_1, m_2) = XH(m_1, m_2),$$

$$H(m_1, m_2) = \overline{H(m_2, m_1)}.$$

Notice that, since G is abelian, the two conditions above imply that $H(m_1, \overline{X}m_2) = H(Xm_1, m_2)$. For example, if

$$\beta : M \times M \to \mathbb{Z}$$

is a $\mathbb{Z}$-bilinear and symmetric form such that

$$\beta(Xm_1, m_2) = \beta(m_1, \overline{X}m_2)$$

then β induces an Hermitian form H given by

$$H(m_1, m_2) = \sum_{g\in G} \beta(g^{-1}m_1, m_2)g.$$

Definition 2.1 A *symmetric circulant* β on $\mathbb{Z}[G]$ is a $\mathbb{Z}$-bilinear and symmetric form on $\mathbb{Z}[G]$ with values in $\mathbb{Z}$ such that

$$\beta(gX, gY) = \beta(X, Y)$$

for every $g \in G$ and $X, Y \in \mathbb{Z}[G]$.

If β is a symmetric circulant and H the Hermitian form induced by β, then

$$H(X, Y) = H(e, e)X\overline{Y},$$

https://doi.org/10.4153/S0008414X20000255 Published online by Cambridge University Press

for every $X, Y \in \mathbb{Z}[G]$. If we denote by

$$s := H(e,e) = \sum_{g\in G} \beta(g^{-1},e)g = \sum_{g\in G} \beta(e,g)g$$

then $s = \bar{s}$ and $\Pr(sX\overline{Y}) = \beta(X,Y)$. Thus, we have a 1-to- 1 correspondence between symmetric circulants and the elements s of the group ring such that $s = \overline{s} \in \mathbb{Z}[G]$. We call s the circulant associated to H or β in $\mathbb{Z}[G]$. If β and β_1 are symmetric circulants on $\mathbb{Z}[G]$ we may ask if there is a $\mathbb{Z}[G]$-module automorphism

$$L : \mathbb{Z}[G] \simeq \mathbb{Z}[G]$$

such that

$$\beta_1(L(X), L(Y)) = \beta(X,Y).$$

Surely $L(X) = XL(e) = XV$ for some unit $V \in \mathbb{Z}[G]^*$. Thus, for all $X, Y \in \mathbb{Z}[G]$

$$\begin{aligned}\Pr(s_1 V\overline{V}X\overline{Y}) &= \beta_1(L(X), L(Y)) \\ &= \beta(X,Y) \\ &= \Pr(sX\overline{Y}).\end{aligned}$$

Hence,

$$s = s_1 V\overline{V} = Vs_1\overline{V}.$$

In this case we say s_1 *is congruent to* s. This is an equivalence relation on the set of elements s of the group ring such that $s = \overline{s} \in \mathbb{Z}[G]$. Thus, the classification of circulants, up to isometry, is equivalent to the classification of such elements s up to congruence.

2.1 Induced Circulants

In this subsection we collect some of the basic results about circulants that we will need later in the paper. We do not give proofs of most of the results. For the interested reader proofs can be found in [5, §IV.2-3].

Let $H \subset G$ be a subgroup, $|H| = h$ and χ the canonical quotient homomorphism

$$\chi : G \to G/H.$$

Then χ induces a ring homomorphism between group rings

$$\chi : \mathbb{Z}[G] \twoheadrightarrow \mathbb{Z}[G/H].$$

We set $\Sigma_H = \sum_{h\in H} h \in \mathbb{Z}[G]$, and note that for $X \in \mathbb{Z}[H]$, $X\Sigma_H = \varepsilon(X)\Sigma_H$.

Lemma 2.2 *The principal ideal $\langle\Sigma_H\rangle \subset \mathbb{Z}[G]$ is the ideal of elements fixed under H; that is, $X \in \langle\Sigma_H\rangle$ if and only if $hX = X$ for all $h \in H$.*

Lemma 2.3 *The kernel of*

$$\chi : \mathbb{Z}[G] \to \mathbb{Z}[G/H]$$

is the annihilator ideal in $\mathbb{Z}[G]$ of Σ_H.

https://doi.org/10.4153/S0008414X20000255 Published online by Cambridge University Press

Lemma 2.3 means the $\mathbb{Z}[G]$-module structure of $\langle \Sigma_H \rangle \subset \mathbb{Z}[G]$ naturally induces a $\mathbb{Z}[G/H]$-module structure on this principal ideal. Furthermore,

$$X\Sigma_H \to \chi(X)$$

is a $\mathbb{Z}[G/H]$-module isomorphism of $\langle \Sigma_H \rangle$ with $\mathbb{Z}[G/H]$.

Now, suppose that $\beta(X, Y)$ is a symmetric circulant on $\mathbb{Z}[G]$ and $s = \bar{s} \in \mathbb{Z}[G]$ is the associated circulant for which

$$\beta(X, Y) = \Pr(sX\overline{Y}).$$

Additionally, note that $\chi(s) = \overline{\chi(s)}$. Thus, the image $\chi(s) \in \mathbb{Z}[G/H]$ induces a symmetric circulant on $\mathbb{Z}[G/H]$. We seek an interpretation of this induced circulant.

Lemma 2.4 *For $X, Y \in \mathbb{Z}[G]$ we have*

$$\beta\left(X\Sigma_H, Y\right) = \Pr(\chi(s)\chi(X)\chi(\overline{Y})).$$

Furthermore, note that

$$\begin{aligned}\beta(X\Sigma_H, Y\Sigma_H) &= \beta(X\Sigma_H^2, Y)\\ &= \beta(hX\Sigma_H, Y)\\ &= h\beta(X\Sigma_H, Y).\end{aligned}$$

Also $\chi : \mathbb{Z}[G] \to \mathbb{Z}[G/H]$ sends the congruence class of $s = \bar{s} \in \mathbb{Z}[G]$ to the congruence class of $\chi(s) \in \mathbb{Z}[G/H]$.

2.2 Product of Circulants

Let G_1 and G_2 be finite abelian groups. Using the inclusions $G_1 \subset G_1 \times G_2$; $G_1 \to G_1 \times \{e\}$ and $G_2 \subset G_1 \times G_2$; $G_2 \to \{e\} \times G_2$ we obtain maps $\mathbb{Z}[G_i] \subset \mathbb{Z}[G_1 \times G_2]$. This yields a bilinear form

$$\mathbb{Z}[G_1] \times \mathbb{Z}[G_2] \to \mathbb{Z}[G_1 \times G_2]$$

given by

$$(X_1, X_2) \to X_1X_2 \in \mathbb{Z}[G_1 \times G_2]$$

and further, an isomorphism

$$\mathbb{Z}[G_1] \otimes_{\mathbb{Z}} \mathbb{Z}[G_2] \simeq \mathbb{Z}[G_1 \times G_2]$$

which sends $X_1 \otimes X_2$ to X_1X_2. Therefore, if $X_1 \in \mathbb{Z}[G_1] \subset \mathbb{Z}[G]$ and $X_2 \in \mathbb{Z}[G_2] \subset \mathbb{Z}[G]$ then,

$$\Pr_G(X_1X_2) = \Pr_{G_1}(X_1)\Pr_{G_2}(X_2) \in \mathbb{Z}.$$

Hence, the following:

https://doi.org/10.4153/S0008414X20000255 Published online by Cambridge University Press

Lemma 2.5 *If $s_1 = \overline{s_1} \in \mathbb{Z}[G_1]$ is a circulant associated to β_1 and $s_2 = \overline{s_2} \in \mathbb{Z}[G_2]$ is associated to β_2 then $s = s_1 s_2 \in \mathbb{Z}[G]$ is canonically associated to the product circulant $\beta_1 \otimes \beta_2$.*

3 Prime Power Degree

Let q be a prime and r be a positive integer. In this section we consider tame cyclic number fields of degree q^r. The main goal of this section is to present a canonical Gram Matrix of the quadratic module $\langle \mathfrak{o}_K, \mathrm{Tr}_{K/\mathbb{Q}} \rangle$ that depends only on the degree and the discriminant of K.

We state the following well known result since we will use it often.

Lemma 3.1 *Let $K/\mathbb{Q}$ be an abelian extension. Suppose that K is tame. Then, the conductor of K is $f = \mathrm{rad}(\mathfrak{d}(K))$.*

Proof This follows from the fact that the conductor is the product over ramified primes of the local conductors. See also [11, Proposition 8.1]. ∎

3.1 One Prime Ramifying

Throughout K denotes a tame cyclic number field of degree q^r, and $p \neq q$ the only prime ramifying in K.

Thanks to Lemma 3.1 we know that $K \subset \mathbb{Q}(\eta_p)$, where η_p is a primitive p-th root of unity. Furthermore, since $\mathrm{Gal}(\mathbb{Q}(\eta_p)/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^*$ is cyclic, K is the only subfield of $\mathbb{Q}(\eta_p)$ of degree q^r. Also $q^r | (p-1)$. The ring of integers of $\mathbb{Q}(\eta_p)$ is $\mathbb{Z}[\eta_p]$ and $\{\eta_p, \eta_p^2, \ldots, \eta_p^{p-1}\}$ is a normal integral basis of $\mathbb{Z}[\eta_p]$. We endow $\mathbb{Z}[\eta_p]$ with a structure of a $\mathbb{Z}[(\mathbb{Z}/p\mathbb{Z})^*]$-module in the following way:

$$g \cdot \eta_p = \eta_p^g$$

for every $g \in (\mathbb{Z}/p\mathbb{Z})^*$ and extend by linearity. Thus, we have an isomorphism of $\mathbb{Z}[(\mathbb{Z}/p\mathbb{Z})^*]$-modules of rank 1.

$$\begin{aligned} \varphi : \mathbb{Z}[(\mathbb{Z}/p\mathbb{Z})^*] &\to \mathbb{Z}[\eta_p] \\ X = \sum a_i g_i &\to \sum a_i g_i \cdot \eta_p. \end{aligned} \tag{1}$$

Additionally, we define a symmetric circulant β on $\mathbb{Z}[(\mathbb{Z}/p\mathbb{Z})^*]$ by

$$\beta(X, Y) := \mathrm{Tr}_{\mathbb{Q}(\eta_p)/\mathbb{Q}}(\varphi(X)\varphi(Y))$$

Lemma 3.2 *Suppose that t is a generator of $(\mathbb{Z}/p\mathbb{Z})^*$. Then, the associated circulant of β is*

$$s = pt^{(p-1)/2} - \Sigma_{(\mathbb{Z}/p\mathbb{Z})^*}$$

and $t^{(p-1)/2} \in (\mathbb{Z}/p\mathbb{Z})^*$ is independent of the choice of t.

https://doi.org/10.4153/S0008414X20000255 Published online by Cambridge University Press

Proof The relationship between s and β is given by

$$s = \bar{s} = \sum_{g \in (\mathbb{Z}/p\mathbb{Z})^*} \beta(I, g) g.$$

Our goal is to calculate the coefficients $\beta(I, g)$ for every g. For this purpose, let t be a generator of $(\mathbb{Z}/p\mathbb{Z})^*$, then each $g \in (\mathbb{Z}/p\mathbb{Z})^*$ is equal to t^j for some $1 \leq j \leq p-1$. Now, suppose that $\varphi(t) = t(\eta_p) = \eta_p^r$ for some $1 < r \leq p-1$, then $\varphi(t^j) = \eta_p^{r^j}$ and

$$\begin{aligned}
\beta(I, t^j) &= \mathrm{Tr}_{\mathbb{Q}(\eta_p)/\mathbb{Q}}(\eta_p \cdot \eta_p^{r^j}) \\
&= \mathrm{Tr}_{\mathbb{Q}(\eta_p)/\mathbb{Q}}(\eta_p^{r^j+1}) \\
&= \begin{cases} p-1 & \text{if } r^j + 1 \equiv 0 \mod p \\ -1 & \text{otherwise.} \end{cases}
\end{aligned}$$

But, $r^j + 1 \equiv 0 \mod p$ only when $j = \frac{p-1}{2}$ no matter the choice of the generator t. Hence, we have

$$\begin{aligned}
s &= \sum_{g \in (\mathbb{Z}/p\mathbb{Z})^*} \beta(I, g) g \\
&= \sum_{j=0}^{p-1} \beta(I, t^j) t^j \\
&= p t^{(p-1)/2} - \Sigma_{(\mathbb{Z}/p\mathbb{Z})^*}.
\end{aligned}$$

■

Lemma 3.3 *Let K be a cyclic number field of degree q^r with discriminant dvivisible by only one prime $p \neq q$, and let $h = \frac{p-1}{q^r}$. Then, there is a normal integral basis of $\mathfrak{o}_K$ such that the Gram matrix of the trace in such basis is equal to*

$$\begin{pmatrix} p-h & -h & \dots & -h \\ -h & p-h & \dots & -h \\ \vdots & \vdots & \ddots & \vdots \\ -h & -h & \dots & p-h \end{pmatrix}$$

if K is totally real, or equal to

$$\left(\begin{array}{ccc|ccc} -h & \dots & -h & p-h & \dots & -h \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ -h & \dots & -h & -h & \dots & p-h \\ \hline p-h & \dots & -h & -h & \dots & -h \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ -h & \dots & p-h & -h & \dots & -h \end{array}\right)$$

if K is totally complex.

https://doi.org/10.4153/S0008414X20000255 Published online by Cambridge University Press

Proof Since p is the only prime ramifying in K, Lemma 3.1 says that $K \subset \mathbb{Q}(\eta_p)$. Thus, for every $x, y \in \mathfrak{o}_K$, by transitivity of the trace

$$\begin{aligned}\mathrm{Tr}_{\mathbb{Q}(\eta_p)/\mathbb{Q}}(xy) &= \mathrm{Tr}_{K/\mathbb{Q}}\left(\mathrm{Tr}_{\mathbb{Q}(\eta_p)/K}(xy)\right)\\ &= \mathrm{Tr}_{K/\mathbb{Q}}(hxy)\\ &= h\cdot \mathrm{Tr}_{K/\mathbb{Q}}(xy).\end{aligned}$$

If t is a generator of $G = \mathrm{Gal}(\mathbb{Q}(\eta_p)/\mathbb{Q})$ then $H = \left\langle t^{q^r}\right\rangle$ is the only subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$ of order $h := \frac{p-1}{q^r}$, K is the fixed field of H and K is totally real if and only if $|H| = \frac{p-1}{q^r}$ is even. The last part part follows since otherwise K would be totally complex. In addition, if h is even, then $t^{(p-1)/2} = \left(t^{q^r}\right)^{h/2} \in H$, otherwise $t^{(p-1)/2} \notin H$.

On the other hand, under the isomorphism φ defined in (1) we have $\varphi(\langle \Sigma_H\rangle) = \mathfrak{o}_K$ and if we set $\mathfrak{e}_1 = \mathrm{Tr}_{\mathbb{Q}(\eta_p)/K}(\eta_p)$ then the action of $\mathrm{Gal}(K/\mathbb{Q})$ over $\mathfrak{e}_1$ generates a normal integral basis $\mathfrak{e} := \{\mathfrak{e}_1, \mathfrak{e}_2, \ldots, \mathfrak{e}_{q^r}\}$ of $\mathfrak{o}_K$.
Denote by χ the epimorphism from $\mathrm{Gal}(\mathbb{Q}(\eta_p)/\mathbb{Q})$ to $\mathrm{Gal}(K/\mathbb{Q})$

$$\chi : G \to G/H$$

$$\sigma \to \sigma\restriction_K$$

and extend this to a ring homomorphism

$$\chi : \mathbb{Z}[G] \to \mathbb{Z}[G/H] \simeq \mathbb{Z}[\mathbb{Z}/q^r\mathbb{Z}].$$

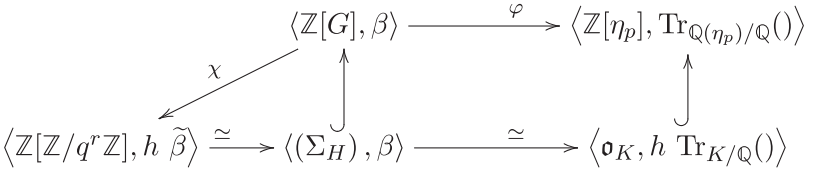
Under this homomorphism we obtain

$$\begin{aligned}\chi(\Sigma_G) &= h\Sigma_{G/H},\\ \chi(t^{(p-1)/2}) &= I_{G/H}, \quad \text{if } h \text{ is even},\\ \chi(t^{(p-1)/2}) &= \overline{C}, \qquad \text{if } h \text{ is odd},\end{aligned}$$

where I is the identity map and $\overline{C}$ is the conjugation map $\overline{C} : K \to K$. Hence,

$$\begin{aligned}\chi(s) &= pI_{G/H} - h\Sigma_{G/H} \qquad \text{if } h \text{ is even},\\ \chi(s) &= p\overline{C} - h\Sigma_{G/H} \qquad \text{if } h \text{ is odd}.\end{aligned}$$

From Lemmas 2.2, 2.3 and 2.4 the following diagram is commutative,



https://doi.org/10.4153/S0008414X20000255 Published online by Cambridge University Press

we conclude that $\chi(s)$ is the circulant associated to $\mathrm{Tr}_{K/\mathbb{Q}}$ in the basis $\mathfrak{e}$. Therefore the Gram matrix of the trace in the basis $\mathfrak{e}$ is

$$\begin{pmatrix} p-h & -h & \dots & -h \\ -h & p-h & \dots & -h \\ \vdots & \vdots & \ddots & \vdots \\ -h & -h & \dots & p-h \end{pmatrix} \quad \text{if } K \text{ is totally real,}$$

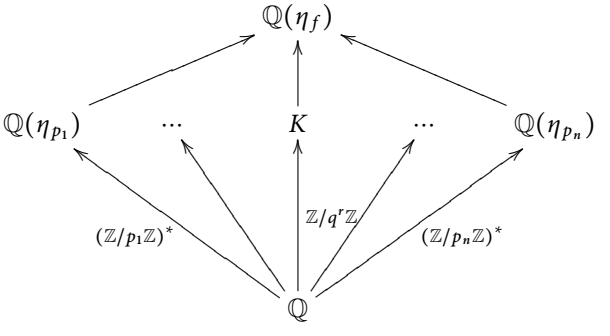
and

$$\left(\begin{array}{ccc|ccc} -h & \dots & -h & p-h & \dots & -h \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ -h & \dots & -h & -h & \dots & p-h \\ \hline p-h & \dots & -h & -h & \dots & -h \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ -h & \dots & p-h & -h & \dots & -h \end{array}\right) \quad \text{if } K \text{ is totally complex.}$$

■

3.2 Several Primes Ramifying

Throughout this section K will denote a tame cyclic number field of degree q^r. Let $p_1, p_2, \dots, p_n$ be the primes ramifying in K. We will denote by e_{p_i} the ramification index of p_i in K. By Lemma 3.1, $f = \mathrm{rad}(\mathfrak{d}(K))$ is the conductor of K. The following diagram illustrates this situation:



We denote by $\chi : \mathrm{Gal}(\mathbb{Q}(\eta_f)/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q})$ the canonical group homomorphism

$$\begin{aligned} \chi : (\mathbb{Z}/f\mathbb{Z})^* &\to \mathbb{Z}/q^r\mathbb{Z} \\ \sigma &\to \sigma \restriction_K \end{aligned}$$

Lemma 3.4 *For every p_i the image of the restriction $\chi \restriction_{(\mathbb{Z}/p_i\mathbb{Z})^*} : (\mathbb{Z}/p_i\mathbb{Z})^* \to \mathbb{Z}/q^r\mathbb{Z}$ is $\mathcal{V}_{p_i}(K/\mathbb{Q})$, the ramification group of p_i in $K/\mathbb{Q}$.*

Proof Let P be a prime in $\mathbb{Z}[\eta_f]$ above of p_i and $P_i := \mathbb{Z}[\eta_{p_i}] \cap P$. Since since p_i is unramified in $\mathbb{Q}(\eta_{p_j})$ with $j \neq i$, it is unramified in their compositum. Under the Galois correspondence, this latter field corresponds to the subgroup $\mathrm{Gal}(\mathbb{Q}(\eta_{p_i})/\mathbb{Q}) \leq \mathrm{Gal}(\mathbb{Q}(\eta_f)/\mathbb{Q})$. Since the inertia subfield of any prime above p_i in $\mathbb{Q}(\eta_f)$ is the maximal

https://doi.org/10.4153/S0008414X20000255 Published online by Cambridge University Press

subfield in which p_i is unramified, see [11, Proposition 6.8],

$$\mathcal{V}_P(\mathbb{Q}(\eta_f)/\mathbb{Q}) \leq \mathrm{Gal}(\mathbb{Q}(\eta_{p_i})/\mathbb{Q}).$$

In fact, this is an equality since the ramification index of p_i in $\mathbb{Q}(\eta_{p_i})$ is $\phi(p_i)$. Thus we have isomorphisms

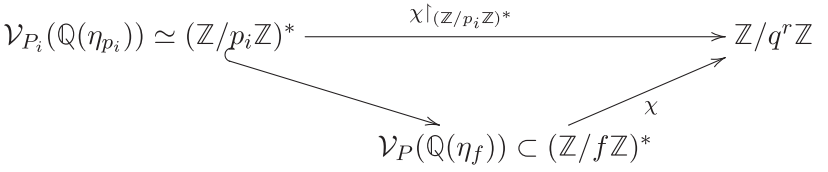
$$\mathcal{V}_P(\mathbb{Q}(\eta_f)/\mathbb{Q}) \simeq (\mathbb{Z}/p_i\mathbb{Z})^* \simeq \mathcal{V}_{P_i}(\mathbb{Q}(\eta_{p_i})).$$

On the other hand, the image of the restriction of the canonical map

$$\chi : (\mathbb{Z}/f\mathbb{Z})^* \to \mathbb{Z}/q^r\mathbb{Z}$$

$$\chi(\sigma) = \sigma \restriction_F$$

to $\mathcal{V}_P(\mathbb{Q}(\eta_f)/\mathbb{Q})$ is $\mathcal{V}_{P_i}(K/\mathbb{Q})$. Finally, the composition



sends $(\mathbb{Z}/p_i\mathbb{Z})^*$ onto $\mathcal{V}_{P_i}(K/\mathbb{Q})$. ∎

Corollary 3.5 *Following the notation above, for every p_i with $i = 1, \ldots, n$*

$$p_i \equiv 1 \pmod{e_{p_i}}.$$

Proof If p_i ramifies in K, then $\mathcal{V}_{p_i}(K/\mathbb{Q}) \subset \mathbb{Z}/q^r\mathbb{Z}$ is not trivial. Additionally, since

$$\chi : (\mathbb{Z}/p_i\mathbb{Z})^* \to \mathcal{V}_{p_i}(K/\mathbb{Q})$$

is onto, then taking cardinalities we conclude that $e_{p_i} \big| (p_i - 1)$. ∎

We proceed now to analyze the general case. Remember that K will denote a cyclic number field of degree q^r, q a prime number, and $p_1, p_2, \ldots, p_n$ the primes ramifying in K. Also we suppose that K is tame.

By Lemma 3.4 we know that for every i, $p_i \equiv 1 \mod e_{p_i}$, and the restriction

$$\chi \restriction (\mathbb{Z}/p_i\mathbb{Z})^* : (\mathbb{Z}/p_i\mathbb{Z})^* \twoheadrightarrow \mathbb{Z}/e_{p_i}\mathbb{Z} \hookrightarrow \mathbb{Z}/q^r\mathbb{Z}$$

is onto. Additionally, since for every i, $(\mathbb{Z}/p_i\mathbb{Z})^*$ is a cyclic group of order $p_i - 1$ and $e_{p_i} \big| (p_i - 1)$, then there exist an unique subgroup $H_i \subset (\mathbb{Z}/p_i\mathbb{Z})^*$ for which the quotient is cyclic group of order e_{p_i}. This subgroup must be the kernel of the restriction of the canonical homomorphism

$$\chi \restriction (\mathbb{Z}/p_i\mathbb{Z})^* : (\mathbb{Z}/p_i\mathbb{Z})^* \to \mathbb{Z}/q^r\mathbb{Z}.$$

Thus the kernel of

$$\chi : (\mathbb{Z}/f\mathbb{Z})^* \twoheadrightarrow \mathbb{Z}/q^r\mathbb{Z}$$

https://doi.org/10.4153/S0008414X20000255 Published online by Cambridge University Press

contains the product

$$\tilde{H} := H_1 \times H_2 \times \cdots \times H_n,$$

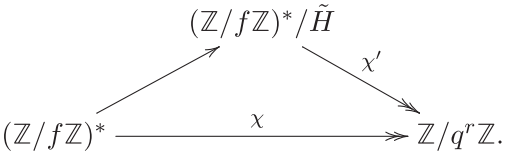
since $\tilde{H} \subset \mathrm{Ker}(\chi)$, then χ factors through the quotient epimorphism

$$(\mathbb{Z}/f\mathbb{Z})^* \twoheadrightarrow (\mathbb{Z}/f\mathbb{Z})^*/\tilde{H}$$

to produce

$$\chi' : (\mathbb{Z}/f\mathbb{Z})^*/\tilde{H} \twoheadrightarrow \mathbb{Z}/q^r\mathbb{Z}.$$

That is, the following diagram is commutative



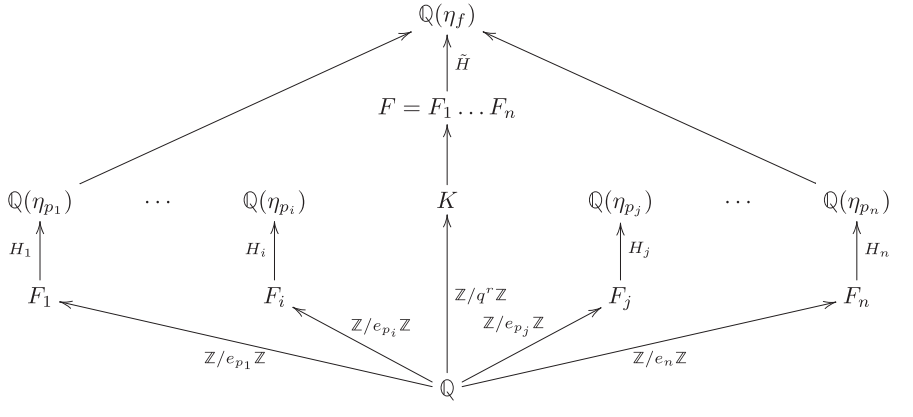
Furthermore, the kernel of χ' is $\mathrm{Ker}(\chi)/\tilde{H}$, and for each i the restriction of χ' to $G_i := (\mathbb{Z}/p_i\mathbb{Z})^*/H_i$ is an isomorphism

$$\chi' \restriction_{G_i} : G_i \simeq \mathbb{Z}/e_{p_i}\mathbb{Z}.$$

Letting F be the fixed field of $\tilde{H}$ we have that $K \subset F \subset \mathbb{Q}(\eta_f)$, moreover if for each i we define $F_i := \mathrm{Fix}(H_i)$ then the Galois correspondence yields

$$F_i \subset \mathbb{Q}(\eta_{p_i}) \subset \mathbb{Q}(\eta_f);\ F = F_1 \ldots F_n$$

and $G_i \cong \mathrm{Gal}(F_i/\mathbb{Q})$.



In particular, each extension $F_i/\mathbb{Q}$ has degree e_{p_i}, Galois group $\mathbb{Z}/e_{p_i}\mathbb{Z} \simeq G_i$, and p_i is the only prime ramifying.

Thus, by Lemma 3.3 we can find a normal integral basis $\{w_i^j\}_j$ of F_i such that

$$\varphi_i : \mathbb{Z}[G_i] \simeq \mathfrak{o}_{F_i}$$

https://doi.org/10.4153/S0008414X20000255 Published online by Cambridge University Press

is given by $\varphi_i(I) = w_i^1$ and

$$s_i = p_i Y_i - h_i \Sigma_{G_i}$$

where

$$Y_i := \begin{cases} I & \text{if } F_i \text{ is totally real} \\ \overline{C} & \text{if } F_i \text{ is totally complex} \end{cases}$$

and $h_i := \frac{p_i - 1}{e_{p_i}}$.

Since the discriminants of $\mathbb{Q}(\eta_{p_i})$ are pairwise coprime, the discriminant of $F_i \subset \mathbb{Q}(\eta_{p_i})$ are pairwise coprime. Hence, since F is the compositum $F_1 \dots F_n$ it follows from [11, Theorem 4.26] that

$$F = F_1 \dots F_n = F_1 \otimes_{\mathbb{Q}} \cdots \otimes_{\mathbb{Q}} F_n,$$

and that

$$\mathfrak{o}_F = \mathfrak{o}_{F_1} \dots \mathfrak{o}_{F_n} = \mathfrak{o}_{F_1} \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} \mathfrak{o}_{F_n}.$$

Thus, we can define $\varphi : \mathbb{Z}[\tilde{G}] \to \mathfrak{o}_F$ where $\tilde{G} := G_1 \times \cdots \times G_n$, such that the following diagram is commutative

$$\begin{array}{ccc} \mathbb{Z}[G_1] \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} \mathbb{Z}[G_n] & \xrightarrow{\simeq} & \mathbb{Z}[\tilde{G}] \\ \bigotimes_i \varphi_i \downarrow & & \downarrow \varphi \\ \mathfrak{o}_{F_1} \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} \mathfrak{o}_{F_n} & \xrightarrow{\simeq} & \mathfrak{o}_F \end{array}$$

It follows that $\varphi : \mathbb{Z}[\tilde{G}] \to \mathfrak{o}_F$ satisfies

$$\varphi(I) = w_1 \cdot \ldots \cdot w_n := w.$$

Remark 3.6 Notice that $\tilde{G} = \mathrm{Gal}(F/\mathbb{Q})$ and that the action of $\tilde{G}$ on w generates a normal integral basis for $\mathfrak{o}_F$.

Now, since the trace form on $\mathfrak{o}_F$ down to $\mathbb{Z}$ is the tensor product of the trace forms on $\mathfrak{o}_{F_i}$, we can extend φ to the following quadratic spaces in the following way

$$\begin{array}{ccc} \left\langle \mathbb{Z}[\tilde{G}], \otimes\beta_i \right\rangle & \xrightarrow{\varphi} & \left\langle \mathfrak{o}_F, \mathrm{Tr}_{F/\mathbb{Q}} \right\rangle \\ \simeq \uparrow & & \uparrow \simeq \\ \bigotimes \langle \mathbb{Z}[G_i], \beta_i \rangle & \xrightarrow[\otimes\varphi_i]{} & \bigotimes \left\langle \mathfrak{o}_{F_i}, \mathrm{Tr}_{F_i/\mathbb{Q}} \right\rangle \end{array}$$

The resulting circulant, $s = \overline{s} \in \mathbb{Z}[\tilde{G}]$, for the symmetric bilinear form $\beta := \otimes\beta_i$ on $\mathbb{Z}[\tilde{G}]$ is $s_1 \cdot \ldots \cdot s_n$.

Finally, remember that $\chi' : \tilde{G} \twoheadrightarrow \mathbb{Z}/q^r\mathbb{Z}$ has a kernel H, whose fixed field is K. Additionally, χ' induces a ring homomorphism

$$\chi' : \mathbb{Z}[\tilde{G}] \twoheadrightarrow \mathbb{Z}[\mathbb{Z}/q^r\mathbb{Z}],$$

https://doi.org/10.4153/S0008414X20000255 Published online by Cambridge University Press

with kernel equal to the annihilator ideal in $\mathbb{Z}[\tilde{G}]$ of Σ_H. Furthermore,

$$X\Sigma_{\tilde{G}} \to \chi'(X)$$

is a $\mathbb{Z}[\mathbb{Z}/q^r\mathbb{Z}]$-module isomorphism of $(\Sigma_{\tilde{G}})$ with $\mathbb{Z}[\mathbb{Z}/q^r\mathbb{Z}]$ and the following diagram is commutative:

$$\begin{array}{ccccc} & & \left\langle \mathbb{Z}[\tilde{G}], \beta \right\rangle & \xrightarrow{\varphi} & \left\langle \mathfrak{o}_F, \mathrm{Tr}_{F/\mathbb{Q}}() \right\rangle \\ & \overset{\chi'}{\swarrow} & \uparrow & & \uparrow \\ \left\langle \mathbb{Z}[\mathbb{Z}/q^r\mathbb{Z}], k\widetilde{\beta} \right\rangle & \xrightarrow{\simeq} & \left\langle (\Sigma_{G'}), \beta \right\rangle & \xrightarrow{\simeq} & \left\langle \mathfrak{o}_K, k\mathrm{Tr}_{K/\mathbb{Q}} \right\rangle \end{array}$$

The circulant associated to $\tilde{\beta}$ is $\chi'(s) = \chi'(s_1) \cdot \chi'(s_2) \cdot \ldots \cdot \chi'(s_n)$. Since $\chi' \restriction_{G_i}$: $G_i \simeq \mathbb{Z}/e_{p_i}\mathbb{Z}$, by Lemma 3.3, we have

$$\chi'(s_i) = \chi'\left(p_i Y_i - h_i \Sigma_{G_i}\right) = p_i I - h_i \Sigma_{\langle e_{p_i} \rangle} \in \mathbb{Z}[\mathbb{Z}/q^r\mathbb{Z}], \quad \text{if } q \text{ is odd}$$

$$\chi'(s_i) = \chi'\left(p_i Y_i - h_i \Sigma_{G_i}\right) = p_i Y_i' - h_i \Sigma_{\langle e_{p_i} \rangle} \in \mathbb{Z}[\mathbb{Z}/q^r\mathbb{Z}], \quad \text{if } q \text{ is even}$$

where $\langle e_{p_i} \rangle$ represents the only subgroup of $\mathbb{Z}/q^r\mathbb{Z}$ of order e_{p_i}, and

$$Y_i' := \begin{cases} I & \text{if } F_i \text{ is totally real} \\ \sigma & \text{if } F_i \text{ is totally complex} \end{cases}$$

where σ is the only element of order 2 in $\mathbb{Z}/q^r\mathbb{Z}$. Thus, if K is totally complex then σ is complex conjugation.

Lemma 3.7 *Let K be a cyclic number field of degree q^r, q odd prime. In keeping up with the notation above, let $\{p_1, \ldots p_n\}$ be the set of primes that ramify in K, all tame, let e_i be the usual ramification index and let $h_i := \frac{p_i - 1}{e_{p_i}}$. Let s and χ' be as above. Suppose $a_0, \ldots, a_r$ are integers such that*

$$\chi'(s) = \prod_{i=1}^{n} \left(p_i I - h_i \Sigma_{\langle e_{p_i} \rangle} \right) = a_0 I + a_1 \Sigma_{\langle q \rangle} + a_2 \Sigma_{\langle q^2 \rangle} + \cdots + a_r \Sigma_{\langle q^r \rangle}.$$

For each $1 \le j \le r$, let $\mathbb{P}_j(K) := \{p_i : e_{p_i}(K/\mathbb{Q}) = q^j\}$. If[2]

$$m_i := \prod_{p \in \mathbb{P}_i(K)} p \text{ and } f_i := \frac{m_i - 1}{q^i}$$

then,

$$a_0 = p_1 \cdot p_2 \cdot \ldots \cdot p_n$$

and for $1 \le i \le r$

$$a_i = -f_i \prod_{j > i} m_j.$$

[2] as it is standard the product over the empty set is defined to be 1.

https://doi.org/10.4153/S0008414X20000255 Published online by Cambridge University Press

Proof By reindexing, if necessary, we have

$$\begin{aligned}
&\prod_{i=1}^{n}\left(p_iI - h_i\Sigma_{\langle e_{p_i}\rangle}\right)\\
&= \underbrace{(p_1I - h_1\Sigma_{\langle q\rangle})\dots(p_jI - h_j\Sigma_{\langle q\rangle})}_{e_{p_i}=q}\dots\underbrace{(p_lI - h_l\Sigma_{\langle q^r\rangle})\dots(p_nI - h_n\Sigma_{\langle q^r\rangle})}_{e_{p_i}=q^r}\\
&= \left(m_1I - f_1\Sigma_{\langle q\rangle}\right)\left(m_2I - f_2\Sigma_{\langle q^2\rangle}\right)\dots\left(m_rI - f_r\Sigma_{\langle q^r\rangle}\right).
\end{aligned}$$

Using that

$$\Sigma_{\langle q^j\rangle}\Sigma_{\langle q^{j+1}\rangle} = q^j\Sigma_{\langle q^{j+1}\rangle}$$

and that

$$m_j - q^jf_j = 1$$

we finish the proof by induction on the number of $f_j \neq 0$. ∎

Corollary 3.8 *Let K be as in Lemma 3.7. For all $0 \leq i \leq r$ let A_i be the $q^r \times q^r$ matrix defined by*

$$(A_i)_{l,m} := \begin{cases} 1 & \text{if } q^{r-i}|(m-l),\\ 0 & \text{otherwise.}\end{cases}$$

Then, there is an normal integral basis $\mathbb{e}$ of $\mathfrak{o}_K$ such that the Gram matrix of the trace form in such a basis is equal to

$$M = a_0A_0 + a_1A_1 + \dots + a_rA_r.$$

Proof Let t be a generator of $\mathrm{Gal}(K/\mathbb{Q})$, and let w be as in Remark 3.6. If we let $\mathbb{e}_1 := \mathrm{Tr}_{F/K}(w)$, and $\mathbb{e}_{j+1} := t^j(\mathbb{e}_1)$ for $j = 0, 1, 2, \dots, q^r - 1$ then $\mathbb{e} := \{\mathbb{e}_1, \dots, \mathbb{e}_{q^r}\}$ is a normal integral basis. Furthermore, for this basis we have

$$\begin{aligned}
\mathrm{Tr}_{K/\mathbb{Q}}(\mathbb{e}_{j+1}) &= (-1)^n && \forall_j\\
\mathrm{Tr}_{K/\mathbb{Q}}(\mathbb{e}_{j+1}\mathbb{e}_{i+1}) &= \sum_{k=r-l}^{r} a_k && \text{if } (i-j, q^r) = q^l\\
\mathrm{Tr}_{K/\mathbb{Q}}(\mathbb{e}_{j+1}\mathbb{e}_{i+1}) &= a_r && \text{if } (i-j, q^r) = 1.
\end{aligned}$$

from which the result follows. ∎

Theorem 3.9 *Let K, K' be two tame cyclic number fields of degree q^r, where q is an odd prime. Then,*

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

Proof We show the non trivial implication. Thanks to Corollary 3.8 we know that K and K' have integral basis such that the Gram matrices of their traces, in their respective basis, are $M = a_0A_0 + a_1A_1 + \dots + a_rA_r$ and $M' = a_0'A_0 + a_1'A_1 + \dots + a_r'A_r$.

https://doi.org/10.4153/S0008414X20000255 Published online by Cambridge University Press

It suffices to show that for all i, $a_i = a_i'$. By Lemma 3.7 we see that the values a_i and a_i' are completely determined by the ramification indices of each ramified prime. Hence, it is enough to show that $e_p(K/\mathbb{Q}) = e_p(K'/\mathbb{Q})$ for all prime p. This is indeed the case since for a Galois number field E of degree n and discriminant $\mathfrak{d}(E)$; the exponent of p in $\mathfrak{d}(E)$ is equal to $n(1-\frac{1}{e_p(E/\mathbb{Q})})$ for every prime tame in E. Indeed, for all $\mathfrak{P}|p$ in K, $\mathfrak{P}^{(e_p-1)}$ exactly divides the different of $K/\mathbb{Q}$, so that $p^{f_p g_p(e_p-1)}$ exactly divides its discriminant ∎

Lemma 3.10 *Let K be a tame cyclic number field of degree 2^r. Let $\{p_1, p_2, \ldots, p_n\}$ be the set of primes ramifying in K, let $h_i := \frac{p_i-1}{e_{p_i}}$, where e_{p_i} is the usual ramification index of p_i in K and let ε be the number of i's such that $e_i||(p_i-1)$. Let s and χ' be as before. Then, there exist $a_0, \ldots, a_r$ integers such that*

$$\chi'(s) = \prod_{i=1}^{n} \chi'(s_i) = a_0\sigma^{\varepsilon} + a_1\Sigma_{\langle 2\rangle} + a_2\Sigma_{\langle 2^2\rangle} + \cdots + a_r\Sigma_{\langle 2^r\rangle}.$$

For each $1 \le j \le r$, let $\mathbb{P}_j := \{p_i : e_{p_i}(K/\mathbb{Q}) = 2^j\}$. If

$$m_i := \prod_{p\in\mathbb{P}_i(K)} p \text{ and } f_i := \frac{m_i - 1}{2^i}$$

then,

$$a_0 = p_1 \cdot p_2 \cdot \ldots \cdot p_n$$

and for $1 \le i \le r$

$$a_i = -f_i \prod_{j>i} m_j.$$

Proof By reindexing, if necessary, we have

$$\begin{aligned}
&\prod_{i=1}^{n}\left(p_i Y_i' - h_i\Sigma_{\langle e_{p_i}\rangle}\right)\\
&= \underbrace{\left(p_1Y_1' - h_1\Sigma_{\langle 2\rangle}\right)\ldots\left(p_jY_j' - h_j\Sigma_{\langle 2\rangle}\right)}_{e_{p_i}=2}\ldots\underbrace{\left(p_lY_l' - h_l\Sigma_{\langle 2^r\rangle}\right)\ldots\left(p_nY_n' - h_n\Sigma_{<2^r>}\right)}_{e_{p_i}=2^r}\\
&= \left(m_1\sigma^{\varepsilon_1} - f_1\Sigma_{\langle 2\rangle}\right)\left(m_2\sigma^{\varepsilon_2} - f_2\Sigma_{\langle 2^2\rangle}\right)\ldots\left(m_r\sigma^{\varepsilon_r} - f_r\Sigma_{\langle 2^r\rangle}\right).
\end{aligned}$$

Where for every i, ε_i means the number of i's such that $e_{p_i}||(p_i-1)$ and $e_{p_i} = 2^i$. Using that

$$\varepsilon = \sum_{i=1}^{r}\varepsilon_i$$

and that

$$\Sigma_{\langle 2^j\rangle}\Sigma_{\langle 2^{j+1}\rangle} = 2^j\Sigma_{2^{j+1}}$$

the result follows by induction on the number of $f_j \neq 0$. ∎

https://doi.org/10.4153/S0008414X20000255 Published online by Cambridge University Press

Corollary 3.11 *Let K as in Lemma 3.10. For every $0 \leq i \leq r$ let A_i be the $2^r \times 2^r$ matrix defined by*

$$(A_i)_{l,m} := \begin{cases} 1 & \text{if } 2^{r-i} | (m-l), \\ 0 & \text{otherwise.} \end{cases}$$

Then, there is a normal integral basis $\mathbb{e}$ of $\mathfrak{o}_K$ such that the Gram matrix of $\langle \mathfrak{o}_K, \mathrm{Tr}_{K/\mathbb{Q}} \rangle$ in such basis is equal to

$$M = a_0 A_1^{\varepsilon} + a_1 A_1 + \cdots + a_r A_r.$$

Proof Let t be a generator of $\mathrm{Gal}(K/\mathbb{Q})$, and let w be as in Remark 3.6. If we let $\mathbb{e}_1 := \mathrm{Tr}_{F/K}(w)$, and $\mathbb{e}_{j+1} := t^j(\mathbb{e}_1)$ for $j = 0, 1, 2, \ldots, 2^r - 1$ then $\mathbb{e} := \{\mathbb{e}_1, \ldots, \mathbb{e}_{2^r}\}$ is a normal integral basis. Furthermore, for this basis we have

$$\begin{aligned} \mathrm{Tr}_{K/\mathbb{Q}}(\mathbb{e}_{j+1}) &= (-1)^n && \forall_j \\ \mathrm{Tr}_{K/\mathbb{Q}}(\mathbb{e}_{j+1}\mathbb{e}_{i+1}) &= \sum_{k=r-l}^{r} a_k && \text{if } (i-j, 2^r) = 2^l \\ \mathrm{Tr}_{K/\mathbb{Q}}(\mathbb{e}_{j+1}\mathbb{e}_{i+1}) &= a_r && \text{if } (i-j, 2^r) = 1. \end{aligned}$$

from which the result follows. ∎

Theorem 3.12 *Let K, K' be two tame cyclic number fields of degree 2^n. Then,*

$$\langle \mathfrak{o}_K, \mathrm{Tr}_{K/\mathbb{Q}} \rangle \simeq \langle \mathfrak{o}_{K'}, \mathrm{Tr}_{K'/\mathbb{Q}} \rangle \text{ if and only if } \mathfrak{d}(K) = \mathfrak{d}(K').$$

Proof We show the non trivial implication. By the same argument at the end of the proof of Theorem 3.9 we see that $e_p(K'/\mathbb{Q}) = e_p(K/\mathbb{Q})$ for every prime p. Hence, the respective associated circulants

$$s(K/\mathbb{Q}) = \prod_{i=1}^{n} \left(p_i Y_i' - h_i \Sigma_{<e_{p_i}>} \right)$$

and

$$s(K'/\mathbb{Q}) = \prod_{i=1}^{n} \left(p_i Y_i' - h_i \Sigma_{\langle e_{p_i} \rangle} \right)$$

must be equal, so $\langle \mathfrak{o}_K, \mathrm{Tr}_{K/\mathbb{Q}}() \rangle$ and $\langle \mathfrak{o}_{K'}, \mathrm{Tr}_{K'/\mathbb{Q}}() \rangle$ are equivalent. ∎

4 General Degree

In this section, we study the behaviour of $\langle \mathfrak{o}_K, \mathrm{Tr}_{K/\mathbb{Q}} \rangle$ when $\mathrm{Gal}(K/\mathbb{Q})$ is cyclic of order m, arbitrary, and K tame. Let $m = q_1^{r_1} \cdot \ldots \cdot q_l^{r_l}$ be the prime decomposition of m. Since $\mathrm{Gal}(K/\mathbb{Q})$ is cyclic there exist $G_1, G_2, \ldots, G_l \subset \mathrm{Gal}(K/\mathbb{Q})$ subgroups, such that $G_i \simeq \mathbb{Z}/q_i^{r_i}\mathbb{Z}$ and that

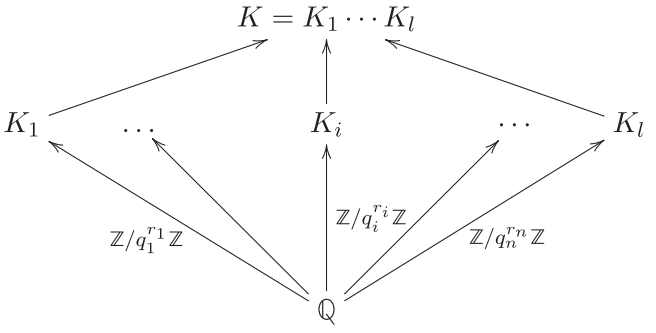
$$\mathrm{Gal}(K/\mathbb{Q}) = G_1 \cdot G_2 \cdot \ldots \cdot G_l.$$

https://doi.org/10.4153/S0008414X20000255 Published online by Cambridge University Press

By the Galois correspondence, there are fields $K_1, K_2, \ldots, K_l \subset K$ such that

$$K = K_1 K_2 \ldots K_l,$$

and $\mathrm{Gal}(K_i/\mathbb{Q}) \simeq \mathbb{Z}/q_i^{r_i}\mathbb{Z}$.



Furthermore, this decomposition is unique and only depends on K. Additionally, every K_i is tame since K is tame by hypothesis.

We denote $P_i \subset \{p_1, p_2, \ldots, p_n\}$ the set of primes ramifying in K_i. Since every K_i is a tame cyclic number field of degree $q_i^{r_i}$, then we can proceed as in §3 in order to find number fields $F_1^i, \ldots, F_{|P_i|}^i$ such that every F_k^i is cyclic, tame, and only one prime is ramifying in F_k^i; additionally, we have

$$K_i \subset F_1^i \ldots F_{|P_i|}^i.$$

We can continue this process with every K_i in order to obtain numbers fields F_k^i, with $1 \le i \le l$ and $1 \le k \le |P_i|$, each one cyclic, tame, only one prime is ramifying, degree $[F_k^i : \mathbb{Q}] = e_p(K_i/\mathbb{Q})$ and $F_k^i \subset \mathbb{Q}(\eta_p)$ where p is the only prime ramifying in F_k^i.

Lemma 4.1 *Let $p_1, p_2, \ldots, p_n$ be the primes ramifying in K, then there exist subfields $F_1, F_2, \ldots F_n \subset \mathbb{Q}(\eta_f)$ such that for every i, $F_i \subset \mathbb{Q}(\eta_{p_i})$, $K \subset F_1 F_2 \ldots F_n$, and $[F_i : \mathbb{Q}] = e_{p_i}(K/\mathbb{Q})$.*

Proof Based on the construction above, we have number fields F_k^i, with $1 \le i \le l$ and $1 \le k \le |P_i|$. For every prime p_j, we associate the $F_k^i, 1 \le i \le l, 1 \le k \le |P_i|$, according the prime which is ramifying in each one and denote by F_j its composition. Let us check that this construction has the properties that we claimed. Clearly, every $F_j \subset \mathbb{Q}(\eta_{p_j})$ since by construction the only prime ramifying in F_j is p_j, additionally,

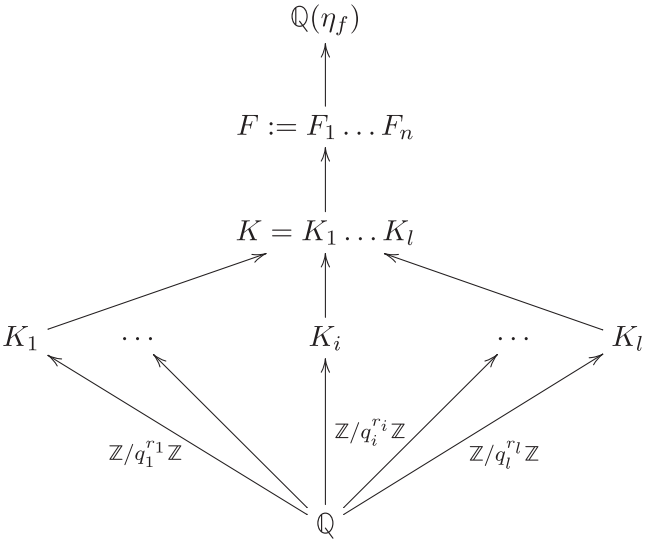
$$F_1 F_2 \ldots F_n = \prod_{i,k} F_k^i \supset K_1 \ldots K_l = K.$$

Now, suppose that p_j ramifies only in K_i, then $e_{p_j}(K/\mathbb{Q}) = e_{p_j}(K_i/\mathbb{Q}) = [F_i : \mathbb{Q}]$. On the other hand, if p_j ramifies in $\{K_{j_1}, K_{j_2}, \ldots, K_{j_s}\}$ then the respective number field $F_k^{j_l}$ in which p_j ramifies has degree $e_{p_j}(K_{j_l}/\mathbb{Q})$, since every K_i has degree $q_i^{r_i}$ then the numbers $e_{p_j}(K_{j_l}/\mathbb{Q})$ are mutually coprimes, then the degree of F_j, being the composite of

https://doi.org/10.4153/S0008414X20000255 Published online by Cambridge University Press

the number field $F_k^{j_l}$ in which p_j is ramifying, is the product of these degrees, but this product is the ramification index $e_{p_j}(K/\mathbb{Q})$. ∎

From Lemmas 3.1 and 4.1, we have the following diagram



As before, we denote by χ the canonical projection from $\mathrm{Gal}(\mathbb{Q}(\eta_f)/\mathbb{Q})$ to $\mathrm{Gal}(K/\mathbb{Q})$,

$$\chi : (\mathbb{Z}/f\mathbb{Z})^* \to \mathbb{Z}/m\mathbb{Z}$$
$$\chi(\sigma) = \sigma \restriction_K .$$

For every i the ramification group of p_i in $\mathbb{Q}(\eta_f)$ is

$$\mathcal{V}_{p_i}(\mathbb{Q}(\eta_f)/\mathbb{Q}) = \{id\} \times \cdots \times (\mathbb{Z}/p_i\mathbb{Z})^* \times \cdots \times \{id\},$$

and the restriction of χ to $\mathcal{V}_{p_i}(\mathbb{Q}(\eta_f)/\mathbb{Q})$ is onto to the ramification group of $K/\mathbb{Q}$

$$\chi \restriction V_{p_i}(\mathbb{Q}(\eta)/\mathbb{Q}) : V_{p_i}(\mathbb{Q}(\eta)/\mathbb{Q}) \twoheadrightarrow \mathcal{V}_{p_i}(K/\mathbb{Q}).$$

Now, by Lemma 4.1 there exist a subfield $F := F_1 \dots F_n$ such that $\mathbb{Q} \subset K \subset F \subset \mathbb{Q}(\eta_f)$, therefore χ factors trough $\mathrm{Gal}(F/\mathbb{Q})$ into

$$\chi' : \mathrm{Gal}(F/\mathbb{Q}) \to \mathbb{Z}/m\mathbb{Z}.$$

Our main interest at this point is to understand the behaviour of $\langle \mathfrak{o}_F, \mathrm{Tr}_{F/\mathbb{Q}} \rangle$. Since $F = F_1F_2 \dots F_n$ and for every i, $\mathfrak{d}(F_i)$ is a power of p_i, then $\mathfrak{d}(F_i)$ is mutually coprime to $\mathfrak{d}(F_j)$ for $j \neq i$, therefore

$$\langle o_F, \mathrm{Tr}_{F/\mathbb{Q}} \rangle = \bigotimes_{i=1}^{n} \langle o_{F_i}, \mathrm{Tr}_{F_i/\mathbb{Q}} \rangle .$$

Thus, it's enough to understand the behaviour of each $\langle o_{F_i}, \mathrm{Tr}_{F_i/\mathbb{Q}} \rangle$ in order to complete our task.

https://doi.org/10.4153/S0008414X20000255 Published online by Cambridge University Press

4.1 Odd Degree

Let us assume that the degree of K, $m = q_1^{r_1} \dots q_l^{r_l}$ is an odd number. For $1 \le i \le l$ let s_i be the circulant associated to F_i. Since F_i has odd degree, we get

$$s_i = p_i I - h_i \Sigma_{G^i}$$

where, $h_i := \dfrac{p_i - 1}{[F_i : \mathbb{Q}]} = \dfrac{p_i - 1}{e_{q_i}(K/\mathbb{Q})}$ and $G^i := \mathrm{Gal}(F_i/\mathbb{Q}) \simeq \mathbb{Z}/e_{q_i}(K/\mathbb{Q})\mathbb{Z}$.

Therefore, the circulant s associated to F is

$$\begin{aligned} s &= s_1 \cdot s_2 \cdot \ldots \cdot s_n \\ &= \prod_{i=1}^{n} (p_i I - h_i \Sigma_{G^i}.) \end{aligned}$$

Now, since $\chi' : \mathrm{Gal}(F/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q})$ is onto, then the circulant associated to K is

$$\begin{aligned} \chi'(s) &= \prod_{i=1}^{n} \chi'(s_i) \\ &= \prod_{i=1}^{n} \chi' \left(p_i I - h_i \Sigma_{G^i}\right) \\ &= \prod_{i=1}^{n} \left(p_i I - h_i \Sigma_{\langle e_{p_i} \rangle}\right). \end{aligned}$$

Where $\langle e_{p_i} \rangle$ denotes the unique subgroup of $\mathbb{Z}/m\mathbb{Z}$ of order $e_{p_i}(K/\mathbb{Q})$.

Theorem 4.2 *Let K, K' be two tame cyclic number fields of odd degree m. Then,*

$$\langle \mathfrak{o}_K, \mathrm{Tr}_{K/\mathbb{Q}} \rangle \simeq \langle \mathfrak{o}_{K'}, \mathrm{Tr}_{K'/\mathbb{Q}} \rangle \text{ if and only if } \mathfrak{d}(K) = \mathfrak{d}(K').$$

Proof We show the non trivial implication. As usual the hypotheses imply that $e_p(K/\mathbb{Q}) = e_p(K'/\mathbb{Q})$ for every prime p. Therefore, the respective associated circulants

$$s(K) = \prod_{i=1}^{n} \left(p_i I - h_i \Sigma_{\langle e_{p_i} \rangle}\right) = s(K')$$

are equal and therefore the quadratics modules $\langle \mathfrak{o}_K, \mathrm{Tr}_{K/\mathbb{Q}} \rangle$ and $\langle \mathfrak{o}_{K'}, \mathrm{Tr}_{K'/\mathbb{Q}} \rangle$ are isometric. ∎

We now describe the circulant s associated to a cyclic tame number field K of odd degree m. Let $1 = d_1 < d_2 < \cdots < d_{\tau(m)} = m$ be the set of positive divisors of m, and let

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

Additionally, for every $\vec{v} \in P$ we define

$$\begin{aligned} \mathrm{lcm}(\vec{v}) &:= \mathrm{lcm}\left[d_2^{\varepsilon_2}, d_3^{\varepsilon_3}, \dots, d_{\tau(m)}^{\varepsilon_{\tau(m)}} \right], \\ \gcd(\vec{v}) &:= \gcd\left(d_2^{\varepsilon_2}, d_3^{\varepsilon_3}, \dots, d_{\tau(m)}^{\varepsilon_{\tau(m)}} \right), \end{aligned}$$

https://doi.org/10.4153/S0008414X20000255 Published online by Cambridge University Press

and for every $d|m$

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

With this notation in mind we state the following Lemma:

Lemma 4.3 *Let K be a tame cyclic number field K of odd degree m and let $p_1, p_2, \ldots, p_n$ be the primes ramifying in K. Then, the circulant s associated to K is given by*

$$\begin{aligned} s(K) &= \prod_{i=1}^{n} \left(p_i I - h_i \Sigma_{\langle e_{p_i} \rangle} \right) \\ &= \sum_{d|m} a_d \Sigma_{\langle d \rangle} \end{aligned}$$

where $\langle d \rangle$ denotes the only subgroup of $\mathbb{Z}/m\mathbb{Z}$ of order d, and a_i is given by the formula

$$\begin{cases} a_1 &= p_1 \cdot p_2 \cdot \ldots \cdot p_n \\ &\vdots \\ a_d &= \sum_{\vec{v} \in P_d} \gcd(\vec{v}) \prod_{\varepsilon_i = 0} w_{d_i} \prod_{\varepsilon_j = 1} (-f_{d_j}) \end{cases}$$

in which $d > 1$ is a divisor of m, and for $\mathbb{P}_d := \{p_i : e_{p_i}(K/\mathbb{Q}) = d\}$,

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

Proof Let $1 = d_1 < d_2 < \cdots < d_{\tau(m)} = m$ be the divisors of m. Then by reindexing, if necessary, we have

$$\begin{aligned} &\prod_{i=1}^{n} \left(p_i I - h_i \Sigma_{\langle e_{p_i} \rangle} \right) \\ &= \underbrace{(p_1 I - h_1 \Sigma_{\langle d_2 \rangle}) \ldots (p_j I - h_j \Sigma_{\langle d_2 \rangle})}_{e_{p_i} = d_2} \ldots \underbrace{(p_l I - h_l \Sigma_{\langle m \rangle}) \ldots (p_n I - h_n \Sigma_{\langle m \rangle})}_{e_{p_i} = m} \\ &= \left(w_{d_2} I - f_{d_2} \Sigma_{\langle d_2 \rangle} \right) \ldots \left(w_m I - f_m \Sigma_{\langle m \rangle} \right). \end{aligned}$$

Using the fact that

$$\Sigma_{\langle d_1 \rangle} \Sigma_{\langle d_2 \rangle} = \gcd(d_1, d_2) \Sigma_{\langle \mathrm{lcm}[d_1, d_2] \rangle}$$

we finish by induction on the number of $f_j \neq 0$. ∎

Corollary 4.4 *Let K as in Lemma 4.3. For every $d|m$, $d \geq 1$ let A_d be the $m \times m$ matrix defined by*

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

https://doi.org/10.4153/S0008414X20000255 Published online by Cambridge University Press

Then, there is a normal integral basis $\mathfrak{e} := \{\mathfrak{e}_1, \ldots, \mathfrak{e}_m\}$ *of* $\mathfrak{o}_K$ *such that the Gram matrix of* $\langle \mathfrak{o}_K, \mathrm{Tr}_{K\mathbb{Q}}() \rangle$ *in such basis is*

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

Proof As in Remark 3.6, for every $1 \leq i \leq n$, F_i has a normal integral basis $\mathfrak{e}^i$ of $\mathfrak{o}_{F_i}$. Since F is the composite of the F_i's and $\mathfrak{d}(F_i)$ are pairwise co-primes, then the product of such a basis form a normal integral basis $\{b_1, b_2, \ldots, b_{[F:\mathbb{Q}]}\}$ of $\mathfrak{o}_F$.

Finally, let t be a generator of $\mathrm{Gal}(K/\mathbb{Q})$, $\mathfrak{e}_1 := \mathrm{Tr}_{F/K}(b_1)$, and $\mathfrak{e}_{j+1} := t^j(\mathfrak{e}_1)$. Then $\mathfrak{e} := \{\mathfrak{e}_1, \ldots, \mathfrak{e}_m\}$ is a normal integral basis of $\mathfrak{o}_K$ and

$$\mathrm{Tr}_{K/\mathbb{Q}}(\mathfrak{e}_j \mathfrak{e}_j) = \sum_{d|m} a_d \qquad \forall j$$

$$\mathrm{Tr}_{K/\mathbb{Q}}(\mathfrak{e}_i \mathfrak{e}_j) = \sum_{k \Big| (j-i,m)} a_{\frac{mk}{(j-i,m)}} \qquad \text{if } i \neq j.$$

from which the result follows. ∎

4.2 Even Degree

Let K be a tame cyclic number field of degree $m = 2^{r_0} q_1^{r_1} \ldots q_l^{r_l}$, where $r_i \geq 1$ and q_i are odd primes for every $1 \leq i \leq l$. If $p_1, p_2, \ldots, p_n$ are the primes ramifying in K then by Lemma 4.1 there exist number fields $F_1, F_2, \ldots, F_l$ such that $K \subset F_1 F_2 \ldots F_l$, $[F_i : \mathbb{Q}] = e_{p_i}(K/\mathbb{Q})$, and the only prime ramifying in F_i is p_i.

We define

$$h_i := [\mathbb{Q}(\eta_{p_i}) : F_i] = \frac{p_i - 1}{e_{p_i}(K/\mathbb{Q})},$$

thus, by Lemma 3.3 for every i such that h_i is even, the associated circulant to F_i will be equivalent to

$$s(F_i) = p_i I - h_i \Sigma_{G^i},$$

meanwhile for every j such that h_j is odd the associated circulant to F_j should be equivalent to

$$s(F_j) = p_j \overline{C} - h_j \Sigma_{G^i},$$

where $G^i := \mathrm{Gal}(F_i/\mathbb{Q}) \simeq \mathbb{Z}/e_{q_i}(K/\mathbb{Q})\mathbb{Z}$.

Therefore, if $F := F_1 F_2 \ldots F_l$ then the respective associated circulant s to F is equivalent to

$$\begin{aligned} s(F) &= s(F_1) \cdot s(F_2) \cdot \ldots \cdot s(F_l) \\ &= \prod_{i=1}^{l} (p_i Y_i - h_i \Sigma_{G^i}.) \end{aligned}$$

https://doi.org/10.4153/S0008414X20000255 Published online by Cambridge University Press

where,

$$Y_i := \begin{cases} I & \text{if } h_i \text{ is even} \\ \\ \overline{C} & \text{if } h_i \text{ is odd.} \end{cases}$$

Finally, since $\chi' : \mathrm{Gal}(F/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q})$ is surjective the associated circulant to K is

$$\begin{aligned} \chi'(s) &= \prod_{i=1}^{l} \chi'(s(F_i)) \\ &= \prod_{i=1}^{l} \chi'(p_i Y_i - h_i \Sigma_{G^i}) \\ &= \prod_{i=1}^{l} \left(p_i Y_i' - h_i \Sigma_{\langle e_{p_i} \rangle} \right). \end{aligned}$$

Where $\langle e_{p_i} \rangle$ denotes the unique subgroup of $\mathbb{Z}/m\mathbb{Z}$ of order $e_{p_i}(K/\mathbb{Q})$,

$$Y_i' := \begin{cases} I & \text{if } h_i \text{ is even} \\ \\ \sigma & \text{if } h_i \text{ is odd} \end{cases}$$

and σ represent the only element in $\mathrm{Gal}(K/\mathbb{Q})$ of order 2; For example, if K is totally complex then σ will be the complex conjugation.

Theorem 4.5 *Let K, K' be two tame cyclic number fields with the same even degree. Then,*

$$\langle \mathfrak{o}_K, \mathrm{Tr}_{K/\mathbb{Q}} \rangle \simeq \langle \mathfrak{o}_{K'}, \mathrm{Tr}_{K'/\mathbb{Q}} \rangle \text{ if and only if } \mathfrak{d}(K) = \mathfrak{d}(K').$$

Proof As usual we only show the non trivial implication. As we have seen before the hypotheses imply that $e_p(K/\mathbb{Q}) = e_p(K'/\mathbb{Q})$ for all prime p. Then,

$$h_i(K) = \frac{q_i - 1}{e_{p_i}(K/\mathbb{Q})} = \frac{q_i - 1}{e_{p_i}(K'/\mathbb{Q})} = h_i(K')$$

for all i. Therefore, the respective associated circulants

$$s(K) = \prod_{i=1}^{l} \left(p_i Y_i' - h_i \Sigma_{\langle e_{p_i} \rangle} \right) = s(K')$$

are equal. Thus, the integral quadratic modules $\langle \mathfrak{o}_K, \mathrm{Tr}_{K/\mathbb{Q}} \rangle$, $\langle \mathfrak{o}_{K'}, \mathrm{Tr}_{K'/\mathbb{Q}} \rangle$ are isometric. ∎

Acknowledgment We would like to thank the referee for the careful reading of the paper, and for their helpful comments.

References

[1] E. Bayer-Fluckiger, *Galois Cohomology and the Trace form.* Jahresber. Deutsch. Math.-Verein **96**–2(1994), 35–55.
[2] M. Bhargava, A. Shankar and X Wang, Squarefree values of polynomial discriminants I. Preprint, 2016. arXiv:1611.09806.
[3] M. Bhargava and A. Shnidman, *On the number of cubic orders of bounded discriminant having automorphism group C3 and related problems.* Algebra. Number Theory, **8**–1(2014), 53–88.
[4] J. Cassels, *Rational quadratic forms*. Dover Publications, Inc., Mineola, NY 2008.
[5] P. Conner and R. Perlis, *A survey of trace forms of algebraic number fields.* World Scientific, Singapore, 1984.
[6] J. S. Ellenberg and A. Venkatesh, *The number of extensions of a number field with fixed degree and bounded discriminant.* Ann. of Math. **163**(2), 723–741 (2006).
[7] A. Frohlich and M. Taylor, *Algebraic number theory.* Cambridge Studies in Advanced Mathematics, Cambridge University Press, Cambridge, 1991.
[8] P. Harron and R. Harron, The shapes of Galois quartic fields. Preprint, 2019. arXiv:1908.03969.
[9] G Mantilla-Soler, *On the arithmetic determination of the trace.* J. Algebra 444(2015), 272–283.
[10] G. Mantilla-Soler and C. Rivera-Guaca, An introduction to Casimir pairings and some arithmetic applications. Preprint, 2019. arXiv:1812.03133v3.
[11] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*. 3rd edition, Springer-Verlag, Berlin Heidelberg, New York, 2004.
[12] J. Neukirch, *Algebraische Zahlentheorie.* Springer-Verlag, Berlin Heidelberg, 2007.
[13] W. M Schmidt, *Number fields of given degree and bounded discriminant.* Astérisque **228** (1995), 189–195. Columbia University Number Theory Seminar (New York, 1992).
[14] J. Serre, *Local fields*. Graduate Texts in Mathematics, 67, Springer-Verlag, New York-Berlin, 1979.
[15] J. Serre, *L'invariant de Witt de la forme Tr* $\left(x^2\right)$. Comm. Math. Helv. **27** (1984), 651.
[16] O. Taussky, *The discriminant matrix of a number field*. J. London. Math. Soc. **43** (1968), 152–154.
[17] D. J. Wright, *Distribution of discriminants of abelian extensions*. Proceedings of the London Mathematical Society, **3**(1989), 17–50.

Department of Mathematics, Universidad de los Andes, Bogotá, Colombia
e-mail: wr.bolanos915@uniandes.edu.co

Guillermo Mantilla-Soler, Department of Mathematics, Universidad Konrad Lorenz, Bogotá, Colombia, and
Department of Mathematics and Systems Analysis, Aalto University, Espoo, Finland
e-mail: gmantelia@gmail.com

https://doi.org/10.4153/S0008414X20000255 Published online by Cambridge University Press