Noname manuscript No.
(will be inserted by the editor)

Gaussian periods in cyclotomic fields and relative traces as generators of intermediate subfields

M. A. Gómez-Molleda

Received: date / Accepted: date

Abstract We study relative traces to provide primitive elements for all the subfields of any cyclotomic field. We also build a primitive element for a cyclotomic extension such that every intermediate field is generated by its relative trace.

Keywords cyclotomics · trace · subfields

Mathematics Subject Classification (2000) 12F05 · 11R18

1 Introduction

In section VII of his Disquisitiones [6] Gauss defined the concept of cyclotomic periods to prove the constructibility by straightedge and compass of regular p-sided polygons for certain odd primes p. Given the p-th root of unity $\xi_p = e^{2\pi i/p}$, an integer λ relatively prime to p and a divisor f of $p-1$, an f-period is

$$(f,\lambda) = \sum_{a\in H} \xi_p^{a\lambda}$$

where H is the unique subgroup of $\mathbb{Z}_p^*$ of order f. In the terminology of modern Galois theory, every f-period is a primitive element of the subfield of $\mathbb{Q}(\xi_p)$ fixed by H and it can be expressed as a relative trace:

$$(f,\lambda) = T^{\mathbb{Q}(\xi_p)}_{\mathbb{Q}(\xi_p)^H}(\xi_p^\lambda)$$

M. A. Gómez-Molleda
Dpto. de Álgebra, Geometría y Topología
Universidad de Málaga, 29071 Spain
Tel.: +34-952-132134
Fax: +34-952-132008
E-mail: gomezma@uma.es

where $\mathbb{Q}(\xi_p)^H$ denotes the subfield of $\mathbb{Q}(\xi_p)$ fixed by H. While these facts are well-known (see for example [2] for more details), their generalization to any cyclotomic field $\mathbb{Q}(\xi_n)$, providing a primitive element for each subfield, is not common knowledge and references for the subject have been difficult to find.

The related question most generally tackled has been that of deciding for what subgroups H of $\mathbb{Z}_n^*$ the corresponding trace $T_{\mathbb{Q}(\xi_n)^H}^{\mathbb{Q}(\xi_n)}(\xi_n)$ does not vanish. Weber [12] gave a complete solution when n is a prime power. Fuchs [5] solved that question for general n and cyclic subgroups. In [3] Diamond, Gerth and Vaaler proved the general result:

> Let H be a subgroup of $\mathbb{Z}_n^*$. Then $T_{\mathbb{Q}(\xi_n)^H}^{\mathbb{Q}(\xi_n)}(\xi_n) \neq 0$ if and only if no non trivial element of H is congruent to 1 modulo r, where r denotes the product of the distinct prime factors of n or twice, according as $8 \nmid n$ or $8 \mid n$.

It can also be proved that the nonvanishing trace has degree $|\mathbb{Z}_n^*/H|$ over $\mathbb{Q}$ (see [4], Theorem 6), which implies that it is a primitive element of the subfield of $\mathbb{Q}(\xi_n)$ fixed by H. In the present paper we also consider the subgroups H of $\mathbb{Z}_n^*$ for which the trace vanishes and prove that a primitive element for $\mathbb{Q}(\xi_n)^H$ is $T_{\mathbb{Q}(\xi_n)^H}^{\mathbb{Q}(\xi_n)}(\xi_n^{m_H})$, where m_H is determined from H. Indeed, $\mathbb{Q}(\xi_n^{m_H})$ is the smallest cyclotomic field containing $\mathbb{Q}(\xi_n)^H$. From the analysis made in the development of the previous questions, we construct, in a natural way, a primitive element θ_n of $\mathbb{Q}(\xi_n)$ whose relative traces generate every subfield. This element turns out to be similar to Leopoldt's Basiszahl [9, 10] for $\mathbb{Q}(\xi_n)$, which gives a normal basis for $\mathbb{Q}(\xi_n)$ over $\mathbb{Q}$. Whereas our result could be obtained as a consequence of Leopoldt's work, the proof given here is direct, using basically the elementary properties of cyclotomic fields, the Fundamental Theorem of Galois theory and the transitivity of the field trace.

2 Subfields of a cyclotomic field

Let n be a positive integer. We consider the n-th primitive root of unity $\xi_n = e^{\frac{2\pi i}{n}}$ and the n-th cyclotomic extension $\mathbb{Q}(\xi_n)$ over $\mathbb{Q}$. It is well-known that the Galois group of $\mathbb{Q}(\xi_n)$ over $\mathbb{Q}$ is isomorphic to

$$\mathbb{Z}_n^* = \{m : 1 \leq m \leq n, (n, m) = 1\}.$$

Indeed, if $m \in \mathbb{Z}_n^*$, the corresponding automorphism of $\mathbb{Q}(\xi_n)$ sends ξ_n to ξ_n^m. From now on we will identify the Galois group with $\mathbb{Z}_n^*$.

Our first aim is to explicitly associate, to every subgroup H of $\mathbb{Z}_n^*$, a primitive element of $\mathbb{Q}(\xi_n)^H$ over $\mathbb{Q}$. For it, we will consider the structure of the subgroups of $\mathbb{Z}_n^*$, particularly those which are associated to the cyclotomic subfields by the Galois correspondence. We shall see that $\mathbb{Q}(\xi_n)^H$ is generated over $\mathbb{Q}$ by the relative trace of a power of ξ_n, and the exponent depends on the smallest cyclotomic field containing $\mathbb{Q}(\xi_n)^H$, which is determined from H.

When $n = p^a$, with p an odd prime, $\mathbb{Z}_n^*$ is cyclic and it has exactly one subgroup of order d for every divisor d of $\varphi(n) = (p-1)p^{a-1}$. If $n = 2^a$, $\mathbb{Z}_{2^a}^*$ is cyclic only when $a = 1, 2$; in the remaining cases, $\mathbb{Z}_{2^a}^*$ is isomorphic to the direct product $C_2 \times C_{2^{a-2}}$ (see [11] for the details), where C_2 and $C_{2^{a-2}}$ are the cyclic groups of orders 2 and 2^{a-2}, respectively.

For a general $n = p_1^{a_1} \dots p_\ell^{a_\ell}$, with $p_1, \dots, p_l$ distinct primes, we can use the Chinese Remainder Theorem to identify $\mathbb{Z}_n^*$ with

$$\mathbb{Z}_{p_1^{a_1}}^* \times \mathbb{Z}_{p_2^{a_2}}^* \times \cdots \times \mathbb{Z}_{p_\ell^{a_\ell}}^*$$

by the canonical isomorphism given by

$$\phi(\sigma) = (\sigma_1, \dots, \sigma_l),$$

where $\sigma_i \equiv \sigma \bmod p_i^{a_i}$ for every $i = 1, \dots, \ell$.

2.1 Odd prime powers

Throughout this section we assume that p is an odd prime and $n = p^a$.

Given $0 \le t \le a-1$, we denote

$$H_t = \{1 + ip^{a-t} : 1 \le i \le p^t\},$$

the unique subgroup of $\mathbb{Z}_n^*$ of order p^t. It is clear that

$$\mathbb{Q}(\xi_n)^{H_t} = \mathbb{Q}(\xi_n^{p^t}), 0 \le t \le a-1,$$

are the cyclotomic subfields of $\mathbb{Q}(\xi_n)$.

Since $T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^{H_t}}(\xi_n) = 0$, because of the transitivity of the trace we have that $T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^H}(\xi_n) = 0$ for every subgroup H of $\mathbb{Z}_n^*$ such that p divides $|H|$. Indeed, given a proper subgroup H of $\mathbb{Z}_n^*$, p divides $|H|$ if and only if $T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^H}(\xi_n) = 0$. Moreover:

Proposition 1 *Let H be a proper subgroup of $\mathbb{Z}_n^*$. Then $T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^H}(\xi_n)$ generates $\mathbb{Q}(\xi_n)^H$ over $\mathbb{Q}$ if and only if p does not divide $|H|$.*

A first proof of this result can be found in [5]. Another elementary proof, in a more general case, is given in [4]. Since we are interested in these traces as primitive elements of the intermediate fields, we will complete the preceding result by giving generators of $\mathbb{Q}(\xi_n)^H$ over $\mathbb{Q}$ when p divides $|H|$:

Proposition 2 *Let H be a subgroup of $\mathbb{Z}_n^*$ and let m, s be non-negative integers such that $|H| = mp^s$ with $(m, p) = 1$. Then $\mathbb{Q}(\xi_n^{p^s})$ is the smallest cyclotomic field containing $\mathbb{Q}(\xi_n)^H$ and $T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^H}(\xi_n^{p^s})$ is a primitive element of $\mathbb{Q}(\xi_n)^H$ over $\mathbb{Q}$.*

Proof: Since H_s is a subgroup of H, the Fundamental Theorem of Galois Theory asserts that $\mathbb{Q}(\xi_n)^H$ is the subfield of $\mathbb{Q}(\xi_n)^{H_s}$ fixed by H/H_s. Since $\mathbb{Q}(\xi_n)^{H_s} = \mathbb{Q}(\xi_n^{p^s})$, we can write $\mathbb{Q}(\xi_n)^H = \mathbb{Q}(\xi_n^{p^s})^{H/H_s}$ and denoting by $H\backslash\backslash H_s$ a set of representatives of the cosets of H_s in H we have

$$T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^H}(\xi_n^{p^s}) = \sum_{\sigma\in H}\sigma(\xi_n^{p^s}) = \sum_{\sigma\in H\backslash\backslash H_s}\sigma\left(\sum_{\tau\in H_s}\xi_n^{\tau p^s}\right) =$$

$$\sum_{\sigma\in H\backslash\backslash H_s}\sigma\left(\sum_{i=1}^{p^s}\xi_n^{(1+ip^{a-s})p^s}\right) = p^s\sum_{\sigma\in H\backslash\backslash H_s}\sigma(\xi_n^{p^s}) = p^s T^{\mathbb{Q}(\xi_n^{p^s})}_{\mathbb{Q}(\xi_n^{p^s})^{H/H_s}}(\xi_n^{p^s}).$$

By Proposition 1, $T^{\mathbb{Q}(\xi_n^{p^s})}_{\mathbb{Q}(\xi_n^{p^s})^{H/H_s}}(\xi_n^{p^s})$ generates $\mathbb{Q}(\xi_n^{p^s})^{H/H_s}$ over $\mathbb{Q}$, since p does not divide $|H/H_s| = m$. ∎

2.2 Powers of 2

The following result describes the subgroups of $\mathbb{Z}^*_{2^a}$ and give explicit primitive elements for the corresponding intermediate fields of $\mathbb{Q}(\xi_n)$ over $\mathbb{Q}$, with $n = 2^a$. Since the cases $a = 1, 2$ are trivial, we will consider $a \geq 3$.

Proposition 3 *Assume $a \geq 3$ and let $s < a-1$ be a positive integer. Then $\mathbb{Z}^*_{2^a}$ has exactly 3 subgroups of order 2^s, which are:*

$$H_{s,1} = \{\pm(1+i2^{a-s+1}) : 1 \leq i \leq 2^{s-1}\}$$
$$H_{s,2} = \{1+i2^{a-s} : 1 \leq i \leq 2^s\}$$
$$H_{s,3} = \{(-1)^i(1+i2^{a-s}) : 1 \leq i \leq 2^s\}$$

Proof: It is easy to check that $H_{s,1}, H_{s,2}$ and $H_{s,3}$ are groups with 2^s elements. The result follows from the structure of $\mathbb{Z}^*_{2^a}$ as a direct product isomorphic to $C_2 \times C_{2^{a-2}}$. ∎

When $a = 2$, it will be convenient to denote $H_{1,2} = \mathbb{Z}^*_4$.

Proposition 4 *Let $a \geq 3$ and let $s < a-1$ be a positive integer. Then*

(i) $T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^{H_{s,2}}}(\xi_n^{2^k}) = \begin{cases} 0 & \text{if } k < s \\ 2^s\xi_n^{2^k} & \text{if } k \geq s. \end{cases}$

(ii) $T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^{H_{s,1}}}(\xi_n^{2^k}) = \begin{cases} 0 & \text{if } k < s-1 \\ 2^s\cos(2\pi/2^{a-k}) & \text{if } k \geq s-1. \end{cases}$

(iii) $T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^{H_{s,3}}}(\xi_n^{2^k}) = \begin{cases} 0 & \text{if } k < s-1 \\ i2^s\sin(2\pi/2^{a-k}) & \text{if } k = s-1 \\ 2^s\cos(2\pi/2^{a-k}) & \text{if } k > s-1. \end{cases}$

Proof: Part (i) is a simple exercise. Parts (ii) and (iii) follow from (i) using that $H_{s-1,2}$ is contained in $H_{s,1}$ and $H_{s,3}$ and the transitivity of the trace. ∎

We can give now generators for $\mathbb{Q}(\xi_n)^{H_{s,1}}, \mathbb{Q}(\xi_n)^{H_{s,2}}$ y $\mathbb{Q}(\xi_n)^{H_{s,3}}$:

Theorem 1 *Let $a \geq 3$ and let $s < a-1$ be a positive integer. Then $\mathbb{Q}(\xi_n)^{H_{s,j}}$ is generated over $\mathbb{Q}$ by*

$T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^{H_{s,1}}}(\xi_n^{2^{s-1}}) = 2^s \cos(2\pi/2^{a-s+1})$ *if* $j = 1$.
$T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^{H_{s,2}}}(\xi_n^{2^s}) = 2^s \xi_n^{2^s}$ *if* $j = 2$.
$T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^{H_{s,3}}}(\xi_n^{2^{s-1}}) = i2^s \sin(2\pi/2^{a-s+1})$ *if* $j = 3$.

Moreover, in every case, the trace of smaller powers of ξ_n is not a primitive element of the corresponding subfield.

Proof: The theorem follows from Proposition 4, considering the degrees over $\mathbb{Q}$ of $\cos(2\pi/2^{a-s+1})$ and $i\sin(2\pi/2^{a-s+1})$:

The degrees of $\cos(2\pi/2^{a-s+1})$ and $\sin(2\pi/2^{a-s+1})$ are both 2^{a-s-1} (see [1] or [8]). Observe that $i\sin(2\pi/2^{a-s+1})$ is fixed by $H_{s,3}$. However, since 4 does not divide $1 + 5^{2^{a-s-2}}$, $i \notin \mathbb{Q}(\xi_n)^{H_{s,3}}$. Therefore,

$$\mathbb{Q}(i\sin(2\pi/2^{a-s+1}) \subsetneq \mathbb{Q}(i, \sin(2\pi/2^{a-s+1})) = \mathbb{Q}(i, i\sin(2\pi/2^{a-s+1}))$$

and $i\sin(2\pi/2^{a-s+1})$ has degree 2^{a-s-1} over $\mathbb{Q}$. ∎

Notice that $\mathbb{Q}(\xi_n^{2^s}) = \mathbb{Q}(\xi_n)^{H_{s,2}}$ is a cyclotomic subfield, whereas $\mathbb{Q}(\xi_n^{2^{s-1}})$ is the smallest cyclotomic field containing $\mathbb{Q}(\xi_n)^{H_{s,1}}$ and $\mathbb{Q}(\xi_n)^{H_{s,3}}$.

2.3 General case

Let $n = p_1^{a_1} \dots p_\ell^{a_\ell}$ with $p_1 < p_2 < \cdots < p_l$ prime numbers, $a_i \geq 1$ for every $i = 1, \dots, \ell$.

If n is odd, then $\mathbb{Q}(\xi_n) = \mathbb{Q}(\xi_{2n})$. Then, in order to study the subfields of the n-th cyclotomic field, we will always consider n even (and thus $p_1 = 2$). When n is even, the roots of unity in $\mathbb{Q}(\xi_n)$ are precisely the n-th roots of unity, i.e., the set $\{\xi_n^t : 1 \leq t \leq n\}$ and the cyclotomic subfields of $\mathbb{Q}(\xi_n)$ are those of the form $\mathbb{Q}(\xi_n^m)$ with m a divisor of n.

Remark 1 *Let m, m' be divisors of n, with $m < m'$. Since the k-th cyclotomic fields, for k even, are all distinct, we have that $\mathbb{Q}(\xi_n^m) = \mathbb{Q}(\xi_n^{m'})$ if and only if $\frac{n}{m'}$ is odd and $m' = 2m$. Thus m divides $n/2$. Indeed*

$$\{\mathbb{Q}(\xi_n^m) : m \text{ divides } n/2\}$$

is the set of cyclotomic subfields of $\mathbb{Q}(\xi_n)$.

Next, we describe explicitly the subgroups of $\mathbb{Z}_n^*$ associated with the cyclotomic subfields of $\mathbb{Q}(\xi_n)$:

Proposition 5 *Let m divide $n/2$, with $m = p_1^{b_1} p_2^{b_2} \dots p_\ell^{b_\ell}$, $b_i \geq 0$ for every $i = 1, \dots, \ell$. Then the cyclotomic field $\mathbb{Q}(\xi_n^m)$ is the subfield of $\mathbb{Q}(\xi_n)$ fixed by $S_m = S_{m,1} \times S_{m,2} \times \cdots \times S_{m,\ell}$ where*

$$S_{m,1} = \begin{cases} H_{b_1,2} & \text{if } 0 < b_1 \\ <1> & \text{if } b_1 = 0 \end{cases}$$

and, for $i > 1$,

$$S_{m,i} = \begin{cases} \text{the unique subgroup of } \mathbb{Z}^*_{p_i^{a_i}} \text{ of order } p_i^{b_i} & \text{if } b_i < a_i \\ \mathbb{Z}^*_{p_i^{a_i}} & \text{if } b_i = a_i. \end{cases}$$

Moreover,

$$S_m = \left\{ \sigma \in \mathbb{Z}_n^* : \sigma \equiv 1 \bmod \frac{n}{m} \right\}.$$

Proof: It is easy to check that $\mathbb{Q}(\xi_n^m)$ and $\mathbb{Q}(\xi_n)^{S_m}$ have the same degree over $\mathbb{Q}$. Therefore, to prove that they are equal, it is enough to show that ξ_n^m is fixed by S_m. If $\sigma \in S_m$, then

$$\sigma(\xi_n^m) = \xi_n^m \Leftrightarrow \xi_n^{\sigma m} = \xi_n^m \Leftrightarrow n \text{ divides } (\sigma - 1)m \Leftrightarrow$$

$$\Leftrightarrow \sigma \equiv 1 \bmod p_i^{a_i - b_i} \text{ for every } i = 1, \dots, \ell \Leftrightarrow$$

$$\Leftrightarrow \sigma_i \equiv 1 \bmod p_i^{a_i - b_i} \text{ for every } i = 1, \dots, \ell.$$

When $a_i = b_i$ or $b_i = 0$, this is trivial. When $i \neq 1$ and $b_i < a_i$, $S_{m,i}$ is the set of elements in $\mathbb{Z}^*_{p_i^{a_i}}$ which are 1 mod $p_i^{a_i - b_i}$. As for $i = 1$, when $a_1 \leq 2$ it is trivial; otherwise $S_{m,1} = H_{b_1,2}$ and the result holds by Proposition 3. ∎

Let us define

$$r = \begin{cases} 2p_1 \dots p_\ell \text{ if } a_1 > 2 \\ p_1 \dots p_\ell \text{ if } a_1 \leq 2 \end{cases}$$

and denote $S = S_{\frac{n}{r}}$. By Proposition 5,

$$S = \{\sigma \in \mathbb{Z}_n^* : \sigma \equiv 1 \bmod r\}.$$

If H is a subgroup of $\mathbb{Z}_n^*$, we denote by m_H the order of $H \cap S$, i.e. the number of elements of H which are congruent to 1 mod r.

The number m_H plays an important role in the determination of a primitive element of $\mathbb{Q}(\xi_n)^H$ over $\mathbb{Q}$, since $\mathbb{Q}(\xi_n^{m_H})$ is the smallest cyclotomic field containing $\mathbb{Q}(\xi_n)^H$:

Lemma 1 *Let H be a subgroup of $\mathbb{Z}_n^*$. Then*

$$H \cap S = S_{m_H} \text{ and } \mathbb{Q}(\xi_n^{m_H}) = \mathbb{Q}(\xi_n)^{H \cap S}.$$

Moreover, $\mathbb{Q}(\xi_n^{m_H})$ is the smallest cyclotomic field containing $\mathbb{Q}(\xi_n)^H$.

Proof: By Proposition 5,

$$S = S_{n/r,1} \times S_{n/r,2} \times \cdots \times S_{n/r,\ell}$$

where

$$S_{n/r,1} = \begin{cases} H_{a_1-2,2} \text{ if } a_1 > 2 \\ \mathbb{Z}^*_{p_1^{a_1}} \quad \text{if } a_1 \leq 2 \end{cases}$$

and, for $i \geq 2$, $S_{n/r,i}$ is the unique subgroup of $\mathbb{Z}^*_{p_i^{a_i}}$ of order $p_i^{a_i-1}$.

Therefore $|S| = n/r$ and m_H divides n/r. Now

$$S_{m_H} = S_{m_H,1} \times S_{m_H,2} \times \cdots \times S_{m_H,\ell}$$

where $S_{m_H,1}$ is a subgroup of $S_{n/r,1}$ and, for $i \geq 2$, $S_{m_H,i}$ is the unique subgroup of $\mathbb{Z}^*_{p_i^{a_i}}$ of order $p_i^{b_i}$ with $b_i \leq a_i - 1$. This implies that $m_H = |S_{m_H}|$ and therefore, to prove that $H \cap S = S_{m_H}$, it is enough to show that $H \cap S \subseteq S_{m_H}$:

Let $\sigma = (\sigma_1, \ldots, \sigma_\ell) \in H \cap S$. Since the order of σ divides m_H and $\sigma_i \in S_{n/r,i}$, the order of $\sigma_i \in \mathbb{Z}^*_{p_i^{a_1}}$ divides $(m_H, |S_{n/r,i}|) = |S_{m_H,i}|$ for every $i = 1, \ldots, \ell$. Then, $\sigma_i \in S_{m_H,i}$ for every i and $\sigma \in S_{m_H}$.

The rest of the statement follows by Proposition 5. ∎

Again, the relative trace of ξ_n is different from zero precisely when $\mathbb{Q}(\xi_n)$ is the smallest cyclotomic field containing $\mathbb{Q}(\xi_n)^H$:

Proposition 6 *Let H be a subgroup of $\mathbb{Z}^*_n$.*

$$T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^H}(\xi_n) \neq 0 \text{ if and only if } m_H = 1.$$

Moreover, if $m_H = 1$ then $T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^H}(\xi_n)$ is a primitive element of $\mathbb{Q}(\xi_n)^H$ over $\mathbb{Q}$.

A proof of the first part can be found in [3], whereas the second part of the proposition is proven in [7]. Both proofs use characters. An elementary proof of the whole statement is given in [4].

When $m_H > 1$, we can use the structure of $H \cap S$ to determine a primitive element of $\mathbb{Q}(\xi_n)^H$ over $\mathbb{Q}$:

Theorem 2 *If H is a subgroup of $\mathbb{Z}^*_n$, then $T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^H}(\xi_n^{m_H})$ is a primitive element of $\mathbb{Q}(\xi_n)^H$ over $\mathbb{Q}$.*

Proof: By the Fundamental Theorem of Galois Theory, $H/H\cap S$ is a subgroup of $\mathbb{Z}_n^*/H\cap S$, the Galois group of $\mathbb{Q}(\xi_n)^{H\cap S}$ over $\mathbb{Q}$. By Lemma 1, $\mathbb{Q}(\xi_n)^{H\cap S} = \mathbb{Q}(\xi_n^{m_H})$. Since $m_{H/H\cap S} = 1$, by Proposition 6 we have that

$$T^{\mathbb{Q}(\xi_n^{m_H})}_{\mathbb{Q}(\xi_n^{m_H})^{H/H\cap S}}(\xi_n^{m_H}) = T^{\mathbb{Q}(\xi_n)^{H\cap S}}_{\mathbb{Q}(\xi_n)^H}(\xi_n^{m_H})$$

is a primitive element of $\mathbb{Q}(\xi_n^{m_H})^{H/H\cap S} = \mathbb{Q}(\xi_n)^H$ over $\mathbb{Q}$.

Notice that

$$T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^H}(\xi_n^{m_H}) = T^{\mathbb{Q}(\xi_n)^{H\cap S}}_{\mathbb{Q}(\xi_n)^H}\left(T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^{H\cap S}}(\xi_n^{m_H})\right)$$

and, since $\xi_n^{m_H} \in \mathbb{Q}(\xi_n)^{H\cap S}$, we have that

$$T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^H}(\xi_n^{m_H}) = |H\cap S| T^{\mathbb{Q}(\xi_n)^{H\cap S}}_{\mathbb{Q}(\xi_n)^H}(\xi_n^{m_H}),$$

which is a primitive element of $\mathbb{Q}(\xi_n)^H$ over $\mathbb{Q}$. ∎

3 A primitive element whose relative trace generates every intermediate field

Throughout this section we will consider that $n > 1$ is any natural number which is either odd or divisible by 4.

We want to construct a primitive element in $\mathbb{Q}(\xi_n)$ whose relative trace generates every intermediate subfield. For it, regarding the previous section, we make the following consideration: for every subgroup $H \leq \mathbb{Z}_n^*$, m_H is a divisor of n such that $T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^H}(\xi_n^{m_H})$ generates $\mathbb{Q}(\xi_n)^H$ over $\mathbb{Q}$. Moreover, for every t dividing m_H, the relative trace of ξ_n^t vanishes. Therefore it seems natural to think at the following element

$$\theta_n = \sum_{k|n'} \xi_n^k, \text{ where } n' = \begin{cases} n & \text{if } n \text{ odd} \\ n/2 & \text{if } 4 \mid n. \end{cases}$$

as a candidate to fulfill our requirement.

Lemma 2 *Let $p, d \in \mathbb{N}$ such that $d \mid n$ and p is a prime dividing d. Let*

$$\theta = \sum_{k|d} \xi_n^k \text{ and } \theta' = \sum_{\substack{k|d \\ p|k}} \xi_n^k.$$

Let H be a subgroup of $\mathbb{Z}_n^*$ and $\tau \in \mathbb{Z}_n^*$. If $\tau\left(T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^H}(\theta)\right) = T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^H}(\theta)$, then $\tau\left(T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^H}(\theta')\right) = T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^H}(\theta')$.

Proof: Let $n = p^a q$ with $(p, q) = 1$, let A, B be integers such that $Aq + Bp = 1$ and $\alpha = \xi_n^{Aq}$. Then

$$\theta = \theta' + \sum_{\substack{k|d \\ p\nmid k}} \xi_n^{(Aq+Bp)k} = \theta' + \sum_{\substack{k|d \\ p\nmid k}} \xi_n^{Bpk} \alpha^k.$$

Let $\sigma, \tau \in \mathbb{Z}_n^*$ and let $k \in \mathbb{N}$ such that $p \nmid k$. We shall write $\sigma k = C_{\sigma k} p + D_{\sigma k}$ and $\tau\sigma k = C'_{\sigma k} p + D'_{\sigma k}$ with $0 < D_{\sigma k}, D'_{\sigma k} < p$.

If $\tau\left(T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^H}(\theta)\right) = T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^H}(\theta)$ then

$$M + \sum_{\sigma\in H} \sum_{\substack{k|d \\ p\nmid k}} (\xi_n^{Bp\sigma k} \alpha^{C_{\sigma k} p} \alpha^{D_{\sigma k}} - \xi_n^{Bp\tau\sigma k} \alpha^{C'_{\sigma k} p} \alpha^{D'_{\sigma k}}) = 0,$$

where $M = T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^H}(\theta') - \tau\left(T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^H}(\theta')\right)$. Therefore α is a root of

$$F(x) = M + \sum_{\sigma\in H} \sum_{\substack{k|d \\ p\nmid k}} (\xi_n^{Bp\sigma k} \alpha^{C_{\sigma k} p} x^{D_{\sigma k}} - \xi_n^{Bp\tau\sigma k} \alpha^{C'_{\sigma k} p} x^{D'_{\sigma k}}), \tag{1}$$

a polynomial in $\mathbb{Q}(\xi_n^p)[x]$ whose degree is smaller than p.

The degree of α over $\mathbb{Q}(\xi_n^p)$ is equal to $[\mathbb{Q}(\xi_n) : \mathbb{Q}(\xi_n^p)]$. When p^2 divides n, this degree is p and then $F(x)$ is the zero polynomial, so that, in particular, its independent coefficient M is zero and then

$$\tau\left(T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^H}(\theta')\right) = T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^H}(\theta').$$

When p^2 does not divide n, then α is a primitive p-th root of unity and its degree over $\mathbb{Q}(\xi_n^p)$ is $p - 1$, so that

$$F(x) = M(1 + x + x^2 + \cdots + x^{p-1}). \tag{2}$$

Evaluating $x = 1$ in (2), we get $F(1) = pM$. Doing it in (1) we obtain

$$F(1) = M + B\left(T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^H}(\theta') - \tau\left(T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^H}(\theta')\right)\right) = M + B(M),$$

considering B as an element in the Galois group of $\mathbb{Q}(\xi_n^p)$ over $\mathbb{Q}$. Thus

$$(p-1)M = B(M).$$

Since M and $B(M)$ are conjugate roots over $\mathbb{Q}$, they have the same norm and

$$(p-1)^{[\mathbb{Q}(\xi_n^p):\mathbb{Q}]} N_{\mathbb{Q}}^{\mathbb{Q}(\xi_n^p)}(M) = N_{\mathbb{Q}}^{\mathbb{Q}(\xi_n^p)}(M).$$

This is only possible when $M = 0$, since $p = 2$ implies $p^2 | n$. Thus

$$\tau\left(T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^H}(\theta')\right) = T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^H}(\theta').$$

■

Now we can prove that the relative trace of θ_n generates every intermediate field of $\mathbb{Q}(\xi_n)$ over $\mathbb{Q}$:

Theorem 3 *If H is a subgroup of $\mathbb{Z}_n^*$, then $T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^H}(\theta_n)$ is a primitive element of $\mathbb{Q}(\xi_n)^H$ over $\mathbb{Q}$.*

Proof: Let $\eta = T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^H}(\theta_n)$. We will prove that if $\tau \in \mathbb{Z}_n^*$ and $\eta = \tau(\eta)$ then $\tau \in H$, which implies that η generates $\mathbb{Q}(\xi_n)^H$ over $\mathbb{Q}$.

Let p be any prime divisor of n'. Taking $d = n'$ in Lemma 2, $\theta = \theta_n$ and $\theta' = \theta_{n/p}$. If $\eta = \tau(\eta)$, by Lemma 2,

$$\tau\left(T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^H}(\theta_{\frac{n}{p}})\right) = T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^H}(\theta_{\frac{n}{p}}).$$

Since $\theta_{\frac{n}{p}} \in \mathbb{Q}(\xi_n^p) = \mathbb{Q}(\xi_n)^{S_p}$ for a certain subgroup S_p of $\mathbb{Z}_n^*$, we have that, on one hand,

$$T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^{<H,S_p>}}(\theta_{\frac{n}{p}}) = \frac{|<H,S_p>|}{|H|}\, T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^H}(\theta_{\frac{n}{p}})$$

and, on the other hand,

$$T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^{<H,S_p>}}(\theta_{\frac{n}{p}}) = [\mathbb{Q}(\xi_n) : \mathbb{Q}(\xi_n^p)]\, T^{\mathbb{Q}(\xi_n^p)}_{\mathbb{Q}(\xi_n^p)^{<H,S_p>/S_p}}(\theta_{\frac{n}{p}}).$$

Therefore

$$T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^H}(\theta_{\frac{n}{p}}) = |H \cap S_p|\, T^{\mathbb{Q}(\xi_n^p)}_{\mathbb{Q}(\xi_n^p)^{<H,S_p>/S_p}}(\theta_{\frac{n}{p}})$$

and

$$\tau\left(T^{\mathbb{Q}(\xi_n^p)}_{\mathbb{Q}(\xi_n^p)^{<H,S_p>/S_p}}(\theta_{\frac{n}{p}})\right) = T^{\mathbb{Q}(\xi_n^p)}_{\mathbb{Q}(\xi_n^p)^{<H,S_p>/S_p}}(\theta_{\frac{n}{p}}).$$

We have shown that, for every prime p dividing n' and $\tau \in \mathbb{Z}_n^*$,

$$\tau(\eta) = \eta \Rightarrow \tau\left(T^{\mathbb{Q}(\xi_n^p)}_{\mathbb{Q}(\xi_n^p)^{<H,S_p>/S_p}}(\theta_{\frac{n}{p}})\right) = T^{\mathbb{Q}(\xi_n^p)}_{\mathbb{Q}(\xi_n^p)^{<H,S_p>/S_p}}(\theta_{\frac{n}{p}}). \qquad (3)$$

Now we can use induction on n to prove that

$$\tau \in \mathbb{Z}_n^*, \tau(\eta) = \eta \Rightarrow \tau \in H :$$

We know that the result is true when $n = 4$ or n is an odd prime. Let n be neither prime nor 4 and assume the result is true for every natural number smaller than n which is either odd or a multiple of 4. If p is a prime factor of n' such that n/p is either odd or a multiple of 4, then by (3) and by induction hypothesis, $\tau \in < H, S_p >$, since $\mathbb{Q}(\xi_n^p)^{<H,S_p>/S_p} = \mathbb{Q}(\xi_n)^{<H,S_p>}$.

Then, if k divides n' and there exists a prime p such that p divides k and n/p is either odd or divisible by 4, we have that

$$T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^H}(\xi_n^k) \in \mathbb{Q}(\xi_n^p) \cap \mathbb{Q}(\xi_n)^H = \mathbb{Q}(\xi_n)^{<H,S_p>}$$

and therefore τ fixes $T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^H}(\xi_n^k)$.

Thus if n is odd or 8 divides n, then τ fixes

$$\eta - T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^H}\left(\sum_{\substack{k|n'\\k\neq 1}} \xi_n^k\right) = T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^H}(\xi_n).$$

If $n = 4q$ with q odd, then τ fixes

$$\eta - T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^H}\left(\sum_{\substack{k|n'\\k\neq 1,2}} \xi_n^k\right) = T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^H}(\xi_n) + T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^H}(\xi_n^2).$$

Applying Lemma 2 to $d = 2$, we conclude that τ fixes $T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^H}(\xi_n^2)$.

Therefore τ fixes $T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^H}(\xi_n^k)$ for every k dividing n'. In particular, if n is even τ fixes $T^{\mathbb{Q}(\xi_n)}_{\mathbb{Q}(\xi_n)^H}(\xi_n^k)$ for $k = m_H$ and, by Theorem 2, $\tau \in H$. If n is odd, then $\mathbb{Q}(\xi_n) = \mathbb{Q}(\xi_{2n})$ and $\xi_{2n} = -\xi_n^{\frac{1-n}{2}}$ is a conjugate of $-\xi_n$ over $\mathbb{Q}$. We can consider then m_H, which divides $n = n'$ and we have that τ fixes $T^{\mathbb{Q}(\xi_{2n})}_{\mathbb{Q}(\xi_{2n})^H}(\xi_{2n}^{m_H})$. By Theorem 2, $\tau \in H$. ∎

Let r_n be the product of the distinct prime divisors of n and let now $n' = n/r_n$. If we redefine

$$\theta_n = \sum_{k|n'} \xi_n^k,$$

the previous theorem is still right. Indeed, the proof can be simplified taking into account that $p \mid n'$ implies $p^2 \mid n$. In this case, $\theta_n = \xi_n$ when n is squarefree.

This last element turns out to be similar to Leopoldt's Basiszahl (see [9,10]) when, in Lettl's notation, $K = \mathbb{Q}^{(n)}$. In this case, $\theta_n = T$ as defined in [9].

In general, Lettl defines a generator T for any absolute abelian number field K of conductor n :

$$T = \sum_{d\in D} T^{\mathbb{Q}(\xi_d)}_{K\cap\mathbb{Q}(\xi_d)}(\xi_d)$$

where D is the set of positive integers d such that $d \mid n$, d is multiple of every odd prime divisor of n and $d \not\equiv 2 \bmod 4$.

Since T gives a normal basis for K over $\mathbb{Q}$, it is easy to check that its relative traces must generate the corresponding intermediate subfields in our case $K = \mathbb{Q}(\theta_n)$. Our result, however, intends to generalize the idea of cyclotomic periods using elementary concepts of Galois theory.

Example 1 *Consider the* 48*-th cyclotomic field and* H *the subgroup of* $\mathbb{Z}_{48}^*$ *generated by* 7.

The relative trace over $\mathbb{Q}(\xi_{48})^H$ *of the element* θ_{48} *in Theorem 3 is*

$$\xi_{48}^{14} + \xi_{48}^{13} - \xi_{48}^{10} + 2\xi_{48}^{8} + \xi_{48}^{7} + \xi_{48}^{6} - \xi_{48}^{5} + \xi_{48}^{3} + 2\xi_{48}^{2} + \xi_{48} - 2$$

with minimal polynomial

$$x^8 + 8x^7 + 32x^6 + 200x^5 + 1362x^4 + 4848x^3 + 9096x^2 + 9824x + 6748.$$

If we use instead the expression θ_n *given after the proof of Theorem 3, we have*

$$\xi_{48}^{14} + 2\xi_{48}^{8} + \xi_{48}^{7} + \xi_{48}^{2} + \xi_{48}$$

with minimal polynomial

$$x^8 - 8x^7 + 40x^6 - 72x^5 + 154x^4 - 112x^3 + 24x^2 + 96x + 28.$$

Finally, the Lettl's element is

$$T = 2\xi_{24}^{4} + \xi_{24}^{2} + \xi_{24} - 2$$

and its minimal polynomial is

$$x^8 + 8x^7 + 38x^6 + 124x^5 + 346x^4 + 792x^3 + 1386x^2 + 1620x + 873.$$

Acknowledgements This work was partially supported by the spanish MICINN project MTM2015-66180-R.

References

1. Beslin, S.; de Angelis, V., *The minimal Polynomials of* $\sin(2\pi/p)$ *and* $\cos(2\pi/p)$, Mathematics Magazine 77, no.2, 146-149, (2004).
2. Cox, D.A., *Galois Theory*, John Wiley & Sons, (2004).
3. Diamond, H.G.; Gerth, F.; Vaaler, J.D., *Gauss sums and Fourier analysis on multiplicative subgroups of* $\mathbb{Z}_q$, Trans. Am. Math. Soc. 227, no. 2, 711-726 (1983).
4. Evans, R.J., *Period polynomials for generalized cyclotomic periods.* Manuscripta Mathematica 40, 217-243, (1982).
5. Fuchs, L., *Ueber die Perioden, welche aus den Wurzeln der Gleichung* $\omega^n = 1$ *gebildet sind, wenn n eine zusammengesetzte Zahl ist.* J. Reine Angew. Math. 61, 374-386, (1863).
6. Gauss, C. F., *Disquisitiones arithmeticae*, Fleischer, 1801 (traduction française par A. C. M. Poullet-Delisle, Recherches arithmétiques, Courcier, Paris, 1807).
7. Gurak, S., *Minimal Polynomials for Circular Numbers*, Pacific J. of Math, 112, n.2, 313-331, 1984.
8. Lehmer, D. H., *Questions, Discussions, and Notes: A Note on Trigonometric Algebraic Numbers.*, Amer. Math. Monthly 40, no. 3, 165-166, (1933).
9. Lettl, G.,*The ring of integers of an abelian number field*, J. Reine Angew. Math. 404, 162-170, (1990).
10. Leopoldt, H. W., *Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkrpers*, J. reine angew. Math.201, 119-149, 1959.
11. Marcus, D.A., *Number Fields*, Springer-Verlag, (1977).
12. Weber, H., *Lehrbuch der Algebra*, Chelsea Pub. Co, (1979).