On Explicit Relations between Cyclotomic Numbers

by
Marc Conrad (Universität des Saarlandes)

1 Introduction

For $n \in \mathbf{N}$ let ϵ_n be a primitive nth root of unity and $D^{(n)}$ the multiplicative group generated by the elements $1 - \epsilon_n^k$ with $k \not\equiv 0 \bmod n$ modulo roots of unity in order to avoid torsion. We call $D^{(n)}$ the group of *cyclotomic numbers*. This group and its subgroups, especially the group of *cyclotomic units*, have been often subject of investigation (see [1], [4], [5], [6], [7], [10], ...). Here, we focus on the relations between the generators $1 - \epsilon_n^k$.
In $D^{(n)}$ there are two types of relations which we call the *obvious relations*.

- Relations arising by relative norms in cyclotomic fields. They can be deduced from the polynomial identity

$$\prod_{\nu=0}^{p-1} (1 - x\epsilon_p^{\nu}) = 1 - x^p \tag{1}$$

  where p is a prime, by inserting an appropriate root of unity for x.

- Relations arising by complex conjugation:

$$1 - \epsilon_n = -\epsilon_n \overline{(1 - \epsilon_n)} = -\epsilon_n (1 - \epsilon_n^{-1}). \tag{2}$$

Surprisingly, Ennola gave in [4] for $n = 105$ a relation that is not generated by the obvious relations. In the following we will call such a relation an *Ennola* relation. Schmidt investigated in [7] the gap between the obvious relations and all relations. He connected this gap to cohomology groups which have been computed in [9].
Here, we will give explicit algorithms on how to construct all Ennola relations in $D^{(n)}$ for an arbitrary n. This will be done in a general context. We consider a free $\mathbf{Z}$-module M with an involution σ operating on it and introduce algorithms focusing on the construction of special bases of M, the so called *σ-bases*, that lead to generators of the torsion group of $M/(1-\sigma)M$

and $M/(1+\sigma)M$. Then we introduce a module $\mathcal{L}(n)$ for which we have by [2] an exact sequence

$$0 \to T(n) \to \mathcal{L}(n)/(1-\sigma)\mathcal{L}(n) \to D^{(n)} \to 1 \tag{3}$$

where $T(n)$ is the torsion group of $\mathcal{L}(n)/(1-\sigma)\mathcal{L}(n)$. The relations in (1) correspond to relations in $\mathcal{L}(n)$ and the relations in (2) correspond to the factorisation by $(1-\sigma)\mathcal{L}(n)$. Thus, the Ennola relations are implicitly given in the torsion group $T(n)$, and the construction of a σ-basis of $\mathcal{L}(n)$ allows the construction of the elements of $T(n)$ explicitly.

In the last two sections we present similar results for the group of *relative* cyclotomic numbers and the Stickelberger ideal.

2 σ-bases

In the following all modules are finitely generated **Z**-modules. When we speak of a basis we mean a **Z**-basis. We assume further that an involution σ operates on each module. The homomorphisms between two modules will be always compatible with the action of σ. So, we will have in fact $\mathbf{Z}[\sigma]$-modules and $\mathbf{Z}[\sigma]$-homomorphisms.

For a set B, a module M and a mapping $\xi : B \to M$ we say that B induces a basis of M if the set $\{\xi(b);\ b \in B\}$ is a basis of M. Saying that some set is a basis of M includes that M is free. Further, we assume that an involution σ operates on each module.

A *σ-basis* of a module M is defined as a triple $[E^0, E^+, E^-]$ of subsets of M such that the union $B = E^0 \cup \sigma E^0 \cup E^+ \cup E^-$ is disjoint, B is a basis of M and the two conditions

(i) $\sigma e = e$ for $e \in E^+$

(ii) $\sigma e = -e$ for $e \in E^-$

hold. We write $B = [E^0, E^+, E^-]$ for short, regarding the triple as a subset of M. Note that a σ-basis is always a weak σ-basis as it is defined in [2]. Note also that every free module has a σ-basis (see Remark 2.8).

In the following we state some results about σ-bases and give algorithms how to construct them. The proofs of the lemmata and the verification of the algorithms can be done straightforward. For details see [3].

Lemma 2.1 *The set* $(1-\sigma)E^0 \cup E^+$ *is a basis of* $\ker_M(1+\sigma)$ *and the set* $(1+\sigma)E^0 \cup E^-$ *is a basis of* $\ker_M(1-\sigma)$.

Lemma 2.2 *The set* E^- *generates the torsion group of* $M/(1-\sigma)M$, *that means the torsion elements are of the form* $\sum_{e\in E^-}\delta_e e + (1-\sigma)M$ *with* $\delta_e \in \{0,1\}$. *Similarly,* E^+ *generates the torsion group of* $M/(1+\sigma)M$.

Remark 2.3 *The values* $m^+ = m^+(M) = |E^+|$ *and* $m^- = m^-(M) = |E^-|$ *are invariants of* M. *They are independent of a special choice of* E^+ *or* E^-. *More concretely,* m^+ *is the dimension of the* $\mathbf{F}_2$*-vector space* $H^0(\sigma, M)$, *and* m^- *is the dimension of* $H^1(\sigma, M)$.

Algorithm 2.4 *Let* $C = [F^0, F^+, F^-]$ *be a* σ*-basis of another module* L. *Then* $[G^0, G^+, G^-] \subseteq M \times L$ *with*

$$G^0 = (E^0 \times C) \cup (E^+ \times F^0) \cup (E^- \times F^0),$$

$$G^+ = (E^+ \times F^+) \cup (E^- \times F^-),$$

$$G^- = (E^+ \times F^-) \cup (E^- \times F^+)$$

induces a σ*-basis of* $M \otimes L$.

A direct consequence of Algorithm 2.4 is the following lemma.

Lemma 2.5 *For* $i = 1, \dots, r$ *let* M_i *be a module with a* σ*-basis* $[E_i^0, \emptyset, E_i^-]$. *The repeated application of Algorithm 2.4 leads to a* σ*-basis* $[F^0, F^-, F^+]$ *of* $\bigotimes_{i=1}^r M_i$ *with*

$$F^+ = E_1^- \times \cdots \times E_r^- \text{ and } F^- = \emptyset \text{ if } r \text{ is even},$$

$$F^+ = \emptyset \text{ and } F^- = E_1^- \times \cdots \times E_r^- \text{ if } r \text{ is odd}.$$

Algorithm 2.6 *Given sets* B, C *and an exact sequence of modules*

$$0 \to M \to L \to K \to 0 \tag{4}$$

such that B *is a* σ*-basis of* M *and* $\emptyset \neq C \subseteq L$ *induces a* σ*-basis of* K. *We show how to construct sets* B' *and* C' *such that* *(i)* B' *is a* σ*-basis of* $M' = \langle B' \rangle$,

(ii) C' *is a* σ*-basis of* $K' = \langle C' \rangle$,

(iii) *The sequence* $0 \to M' \to L \to K' \to 0$ *is exact,*

(iv) $|C'| < |C|$.

We write $B = [F^0, F^+, F^-]$ *and* $C = [E^0, E^+, E^-]$. *Without loss of generality we assume that* M *is a submodule of* L. *If* $E^0 \neq \emptyset$ *we define* $B' = [F^0 \cup E^0, F^+, F^-]$ *and* $C' = [\emptyset, E^+, E^-]$. *Otherwise we choose an* $e \in C$ *and set* $C' = C \setminus \{e\}$. *The basis* $B' = [G^0, G^+, G^-]$ *is now defined through the following cases.*

$c \in E^+$: *We have* $c - \sigma c \in \ker_M(1+\sigma) \subseteq M$. *Therefore, by Lemma 2.1, we find* $a \in M$ *and* $F' \subseteq F^-$ *such that* $c - \sigma c = (1-\sigma)a + \sum_{b \in F'} b$. *Let* $f = c - a$.

If $F' = \emptyset$ *we define* $G^0 = F^0$, $G^+ = F^+ \cup \{f\}$ *and* $G^- = F^-$.

If $F' \neq \emptyset$ *we choose* $f' \in F'$ *and define* $G^0 = F^0 \cup \{f\}$, $G^+ = F^+$ *and* $G^- = F^- \setminus \{f'\}$.

$c \in E^-$: *Analogously to the first case we have* $a \in M$ *and* $F' \subseteq F^+$ *such that* $c + \sigma c = (1+\sigma)a + \sum_{b \in F'} b$. *Let* $f = c - a$.

If $F' = \emptyset$ *we define* $G^0 = F^0$, $G^+ = F^+$ *and* $G^- = F^- \cup \{f\}$.

If $F' \neq \emptyset$ *we choose* $f' \in F'$ *and define* $G^0 = F^0 \cup \{f\}$, $G^+ = F^+ \setminus \{f'\}$ *and* $G^- = F^-$.

Algorithm 2.7 *Given sets* B, C *and an exact sequence* $0 \to M \to L \to K \to 0$ *such that* B *is a* σ*-basis of* M *and* C *is a* σ*-basis of* K *we construct a* σ*-basis of* L *by successive applying Algorithm 2.6 until we have an exact sequence* $0 \to M' \to L \to 0 \to 0$ *with a* σ*-basis of* $M' \cong L$.

Remark 2.8 *Algorithm 2.7 gives an easy proof that every free module* L *has a* σ*-basis:*
Let $M = \{a \in L;\ \sigma a = a\}$ *and* B *be a basis of* M. *Obviously,* $[\emptyset, B, \emptyset]$ *is a* σ*-basis of* M *and any set* $C \subseteq L$ *which induces a basis of* L/M *induces*

a σ-basis $[\emptyset, \emptyset, C]$ of L/M (note that L/M is free). Algorithm 2.7 for the exact sequence

$$0 \to M \to L \to L/M \to 0 \tag{5}$$

leads then to a σ-basis of L.

We recall the definition of a $M\mathcal{E}\mathtt{n}$-system as introduced in [2]. In the following let Δ be a finite, partially ordered indexing set.

Definition 2.9 *For every $d \in \Delta$ let M_d be a module, $\mathcal{E}_d$ a σ-invariant subset of M_d and $\mathtt{n}_d : \mathcal{E}_d \to \bigoplus_{t<d} M_t$ a mapping. We call such a system of triples $(M_d, \mathcal{E}_d, \mathtt{n}_d)_{d\in\Delta}$ a $M\mathcal{E}\mathtt{n}$-*system.
Let $N'_d = \bigoplus_{t<d} M_t$ and $Q'_d = \sum_{t<d}\langle r+\mathtt{n}_t(r);\ r \in \mathcal{E}_t\rangle \subseteq N'_d$. The $M\mathcal{E}\mathtt{n}$-system Γ is combinable*, if the mappings $\mathtt{n}_d$ can be extended to σ-homomorphisms*

$$\bar{\mathtt{n}}_d : \langle \mathcal{E}_d \rangle \to N'_d/Q'_d. \tag{6}$$

In this case Γ defines the module $\mathcal{L} = N/Q$ with $N = \bigoplus_{t\in\Delta} M_t$ and $Q = \sum_{t\in\Delta}\langle r + \mathtt{n}_t(r);\ r \in \mathcal{E}_t\rangle$. We call $\mathcal{L}$ the combination *of Γ.*

Algorithm 2.10 *We show how to construct explicitly a σ-basis of $\mathcal{L}$ from σ-bases of the modules $M_d/\langle\mathcal{E}_d\rangle$.*
We complete the ordering of Δ and may assume $\Delta = \{1, \ldots, n\}$. For $i \in \Delta$ let $N_i = M_1 \oplus \cdots \oplus M_i$ and

$$Q_i = \sum_{j=1}^{i} \langle r + \mathtt{n}_j(r);\ r \in \mathcal{E}_j\rangle \leq N_i. \tag{7}$$

From [2] we know that the sequences

$$0 \to N_{i-1}/Q_{i-1} \to N_i/Q_i \to M_i/\langle\mathcal{E}_i\rangle \to 0 \tag{8}$$

(with $N_0 = Q_0 = \{0\}$) are exact. Starting with $i = 1$ and using Algorithm 2.7 we successively construct a σ-basis of N_i/Q_i from σ-bases of $M_i/\langle\mathcal{E}_i\rangle$ and N_{i-1}/Q_{i-1}. The algorithm ends for $i = n$ and we obtain a σ-basis of $\mathcal{L} = N_n/Q_n$.

3 The Cyclotomic System

In this section we recall the definitions and the properties of the cyclotomic module and the cyclotomic system. More details and proofs of the lemmata can be found in [2]. For a subset S of a module M we write ΣS for $\sum_{s\in S} s$. Further, let $G_d = \{1 \le a < d;\ (a,d)=1\}$ and for each $d > 2$ we fix a subset $H_d \subseteq G_d$ such that for all $a \in G_d$ either $a \in H_d$ or $d - a \in H_d$. For instance we can choose $H_d = \{1, \ldots, \lfloor d/2 \rfloor\} \cap G_d$.

Definition 3.1 *For $n \in \mathbf{N}$ we define the cyclotomic module $Z(n)$ as follows:*

If $n = p$ prime then $Z(p) = \langle G_p \rangle / \langle \Sigma G_p \rangle$.

If $n = q = p^\alpha$ with $\alpha > 1$ then $Z(q) = \langle G_{q/p} \rangle \otimes \langle A_p \rangle / \langle \Sigma A_p \rangle$ with $A_p = \{0, \ldots, p-1\}$.

If $n = q_1 \cdots q_r$ where q_i are pairwise relatively prime prime powers then $Z(n) = Z(q_1) \otimes \cdots \otimes Z(q_r)$.

We define the operation of σ on $b \in G_d$ by $\sigma b = d - b$ and on $a \in A_p$ by $\sigma a = p - 1 - a$. By this $Z(n)$ becomes a module with an involution σ.

Lemma 3.2 *We have $Z(n) \cong \langle G_n \rangle / R_n$ where the submodule R_n of $\langle G_n \rangle$ is generated by $\mathcal{E}_n = \{s(n,p,a);\ p|n \text{ with } p \text{ prime},\ a \in G_{n/p}\}$ with*

$$s(n,p,a) = \Sigma\{x \in G_n;\ x \equiv a \bmod (n/p)\}. \tag{9}$$

Remark 3.3 *The isomorphism in Lemma 3.2 can be described explicitly: We arrange the prime factors p_i of n such that $n = p_1^{\alpha_1} \cdots p_t^{\alpha_t} p_{t+1} \cdots p_r$ with $\alpha_i > 1$ for $i = 1, \ldots, t$. Further, we set $q_i = p_i^{\alpha_i}$ if $i = 1, \ldots, t$ and $q_i = p_i$ else. Let*

$$S = G_{q_1/p_1} \times A_{p_1} \times \cdots \times G_{q_t/p_t} \times A_{p_t} \times G_{p_{t+1}} \times \cdots \times G_{p_r}. \tag{10}$$

It is obvious, by the definition of the tensor product, that $Z(n)$ is isomorphic to $\langle S \rangle$ modulo suitable relations. We obtain $S \cong G_n$ by a combination of *isomorphisms ξ_i and η in the following way:*

$$
\begin{array}{ccccccc}
\underbrace{G_{q_1/p_1} \times A_{p_1}} & \times \cdots \times & \underbrace{G_{q_t/p_t} \times A_{p_t}} & \times & G_{p_{t+1}} & \times \cdots \times & G_{p_r} \\
\downarrow \xi_1 & & \downarrow \xi_t & & \downarrow id & & \downarrow id \\
G_{q_1} & \times \cdots \times & G_{q_t} & \times & G_{q_{t+1}} & \times \cdots \times & G_{q_r} \\
 & & & \downarrow \eta & & & \\
 & & & G_n & & &
\end{array}
\tag{11}
$$

The maps ξ_i for $i = 1, \dots, t$ are explicitly given by $\xi_i(b, a) = ap_i^{\alpha_i - 1} + b$. The map η is defined by the Chinese remainder theorem, that means η^{-1} is the map $a \mapsto a \bmod q_i$ in each component G_{q_i}, $i = 1, \dots, r$. □

Definition 3.4 *For $d \in \mathbf{N}$ let $M_d = \langle G_d \rangle$. If d is not a prime we denote by $\mathcal{E}_d \subseteq M_d$ the set of the sums $s(d, p, a)$ as in Lemma 3.2. For d prime we define $\mathcal{E}_d = \emptyset$. On $\mathcal{E}_d$ we define the mapping*

$$
\mathtt{n}_d : \mathcal{E}_d \to \bigoplus_{t|d, t \neq d} M_t, \; s(d, p, a) \mapsto \begin{cases} -[d/p; a] & \text{if } p^2 | d, \\ [d/p; p^{-1}a] - [d/p; a] & \text{if } p^2 \nmid d \end{cases}
\tag{12}
$$

where $[m; x]$ denotes $y \in G_m$ with $x \equiv y \bmod m$.
*For $n \in \mathbf{N}$ we call the $M\mathcal{E}\mathtt{n}$-system $\Gamma(n) = (M_d, \mathcal{E}_d, \mathtt{n}_d)_{d|n}$ the n*th cyclotomic system.

Lemma 3.5

(a) $\Gamma(n)$ is combinable. We denote by $\mathcal{L}(n)$ the combination of $\Gamma(n)$.

(b) Let $n > 2$ and r be the number of prime factors of n. Then we have:

(i) $$H^0(\sigma, \mathcal{L}(n)) \cong \begin{cases} \mathbf{F}_2^{2^{r-1}-1} & \text{if } n \not\equiv 2 \bmod 4, \\ \mathbf{F}_2^{2^{r-2}} & \text{if } n \equiv 2 \bmod 4. \end{cases}$$

(ii) $$H^1(\sigma, \mathcal{L}(n)) \cong \begin{cases} \mathbf{F}_2^{2^{r-1}-r} & \text{if } n \not\equiv 2 \bmod 4, \\ \mathbf{F}_2^{2^{r-2}-r+1} & \text{if } n \equiv 2 \bmod 4. \end{cases}$$

(c) The sequences in (8) for the cyclotomic system split over σ (with one exception for $n = 4$). This has especially the consequence that in Algorithm 2.6 only the case $F' = \emptyset$ occurs.

(d) The sequence

$$0 \to T(n) \to \mathcal{L}(n)/(1-\sigma)\mathcal{L}(n) \xrightarrow{\overline{\mu}} D^{(n)} \to 1 \tag{13}$$

where $T(n)$ is the torsion group of $\mathcal{L}(n)/(1-\sigma)\mathcal{L}(n)$, is exact. The homomorphism $\overline{\mu}$ is defined by the maps $\mu_d : G_d \to D^{(n)}$, $a \mapsto 1-\epsilon_d^a$ for $d|n$ where ϵ_d is a primitive dth *root of unity such that $\epsilon_d = \epsilon_t^{t/d}$ whenever $d|t$.*

(e) Let $K^{(n)} = \prod_{d|n, d\neq n} D^{(d)}$. We call $\widehat{D^{(n)}} = D^{(n)}/K^{(n)}$ the group of nth relative cyclotomic numbers. *Then for $n \neq 4$ we have an exact sequence*

$$0 \to \widehat{T}(n) \to Y(n)/(1-\sigma)Y(n) \xrightarrow{\overline{\mu}} \widehat{D^{(n)}} \to 1 \tag{14}$$

where $Y(n) = M_n/\langle \mathcal{E}_n \rangle$ with M_n and $\mathcal{E}_n$ as in Definition 3.4.

Table 1: Some examples of σ-bases

module	σ-basis
$\langle G_2 \rangle$	$[\emptyset, \{1\}, \emptyset]$
$\langle G_p \rangle$, $p \neq 2$, p prime	$[H_p, \emptyset, \emptyset]$
$Z(2)$	$[\emptyset, \emptyset, \emptyset]$
$Z(p)$, $p \neq 2$, p prime	$[\{2, \ldots, (p-1)/2\}, \emptyset, \Sigma H_p]$
$Z(4)$	$[\emptyset, \emptyset, \{(1,0)\}]$
$Z(q)$, $q = p^\alpha$, $\alpha > 1$, p prime, $q \neq 4$	$[\{(b,a);\ b \in H_{q/p},\ 1 \leq a < p\}, \emptyset, \emptyset]$

Note that we can construct with Algorithm 2.10 a σ-basis of $\mathcal{L}(n)$ by σ-bases of the modules $Y(d)$ for $d|n$. Using the isomorphism of Lemma 3.2 and Algorithm 2.4 we are able to construct σ-bases of the $Y(d)$ with the σ-bases from Table 1.

4 Ennola Relations

In this section we have a closer look to the exact sequence (13). Note that the norm relations as in (1) are implicitly in (13) given as the relations of the form $s(d,p,a) + \mathtt{n}_d(s(d,p,a))$ in the definition of $\mathcal{L}(n)$. The relations of (2) correspond to factoring $(1-\sigma)\mathcal{L}(n)$.

Algorithm 4.1 *We construct Ennola relations for $D^{(n)}$ performing the following steps.*

1. *With the algorithms of Section 2 compute a σ-basis $[E^0, E^+, E^-]$ of $\mathcal{L}(n)$.*
2. *Each element of E^- gives by Lemma 2.2 a nontrivial element of $T(n)$ which is via the mapping $\overline{\mu}$ in (13) a relation in $D^{(n)}$.*

Note that Algorithm 4.1 has been implemented in a C++ extension of the computer algebra system SIMATH [8]. A description of the implementation and examples can be found in [3].
The smallest number where $T(n)$ is nontrivial is $n = 60$. An Ennola relation in $D^{(60)}$ is

$$(1-\epsilon_{60})\left(1-\epsilon_{60}^{37}\right)\left(1-\epsilon_{20}^{17}\right)^{-1}(1-\epsilon_{15})^{-1}(1-\epsilon_{12})^{-1} = \epsilon_{15} \tag{15}$$

where $\epsilon_d = \epsilon_n^{n/d}$ for $d|n$.

Theorem 4.2 *For $n > 2$ let r be the number of prime factors of n and*

$$c = \begin{cases} 2^{r-1} - r & \text{for } n \not\equiv 2 \bmod 4, \\ 2^{r-2} - r + 1 & \text{for } n \equiv 2 \bmod 4. \end{cases} \tag{16}$$

Then there exist in $D^{(n)}$ exactly $2^c - 1$ different Ennola relations which are generated by c relations. More exactly, we have elements $d_1, \ldots, d_c$ in the free group generated by the set $\{1-\epsilon_d^a;\ d|n,\ a \in G_d\}$ such that the Ennola relations are of the form $\prod_{i=1}^c d_i^{\delta_i}$ with $\delta_i \in \{0,1\}$.
The d_i for $i = 1, \ldots, c$ can be constructed explicitly with Algorithm 4.1.

Proof: Let $[E^0, E^+, E^-]$ be a σ-basis of $\mathcal{L}(n)$. Then we have by Lemma 2.2 $c = |E^-|$. Because $|E^-|$ is the dimension of $H^1(\sigma, \mathcal{L}(n))$ the claim follows from Lemma 3.5. □
As noted in Lemma 3.5, we see that in the process of constructing a σ-basis of $\mathcal{L}(n)$ in Algorithm 2.6 for $n > 4$ always the subcase $F' = \emptyset$ happens. So we can force $T(d) \subseteq T(n)$ for $d|n$ and get immediately the following corollary.

Corollary 4.3 *Let* $D^{(\infty)} = \bigcup_{d\in\mathbf{N}} D^{(d)}$. *Then there exist elements* $d_1, d_2, \ldots$ *in the free group generated by the set* $\{1-\epsilon_d^a;\ d\in\mathbf{N},\ a\in G_d\}$ *such that the Ennola relations are of the form* $\prod_{i\in I} d_i^{\delta_i}$ *with* $\delta_i \in \{0,1\}$ *where* I *is a finite subset of* $\mathbf{N}$.
The d_i *for* $i\in\mathbf{N}$ *can be constructed explicitly with Algorithm 4.1.*

A closer look to the explicit structure of the Ennola relations is given in the next section.

5 Ennola Relations in $\widehat{D^{(n)}}$

Let $n \neq 4$. We write $n = q_1\cdots q_r$ where the q_i are relatively prime prime powers.

Lemma 5.1 *The torsion group* $\widehat{T}(n)$ *in (14) is isomorphic to* $\mathbf{Z}/2\mathbf{Z}$ *in the following two cases:*

$$r \text{ odd},\ r\neq 1 \text{ and } n = u, \qquad r \text{ odd},\ r\neq 1 \text{ and } n = 4u \tag{17}$$

where u *is odd and square free. In all other cases* $\widehat{T}(n)$ *is trivial.*

Proof: By Lemma 2.2, $\widehat{T}(n)$ is generated by the set E^- where $[E^0, E^+, E^-]$ is a σ-basis of $Y(n)$. If $n = p$ is a prime then $Y(p) = \langle G_p\rangle$ and Table 1 shows $E^- = \emptyset$. In the other cases we have by Lemma 3.2 $Y(n) \cong Z(q_1)\otimes\cdots\otimes Z(q_r)$. Here, Lemma 2.5 shows how we obtain a σ-basis of $Z(n)$ by σ-bases of the $Z(q_i)$ which are given in Table 1. Note that $E^- = \emptyset$ if for at least one of the σ-bases $[E_i^{\emptyset}, \emptyset, E_i^-]$ of the modules $Z(q_i)$ we have $E_i^- = \emptyset$. ☐

Theorem 5.2 *The relations in the group of relative cyclotomic numbers* $\widehat{D^{(n)}} = D^{(n)}/K^{(n)}$ *are the obvious relations (as in (1) and (2)) and in the cases of (17)* Ennola relations.
Ennola relations are given implicitly by the set $\widehat{T}(n)$ *in (14) and can be explicitly written as*

$$\prod_{a\in V_n} (1-\epsilon_n^a) \in K^{(n)} \tag{18}$$

where $V_n \cong H_{q_1}\times\cdots\times H_{q_r}$ *such that* $a \equiv b_i \bmod q_i$ *for all* $a\in V_n$ *and* $i = 1,\ldots,r$.

Proof: Lemma 5.1 describes $\widehat{T}(n)$ and how it can be constructed explicitly from a σ-basis of the modules $Z(q_i)$. The isomorphism in Remark 3.3 shows (18). □

6 Stickelberger Elements

Let I_n be the ideal generated by the Stickelberger elements

$$\theta(a) = \sum_{\tau \in G_n} \langle -a\tau/n \rangle \tau^{-1} \tag{19}$$

and $\omega_n = \Sigma G_n$ for n odd and $\omega_n = \frac{1}{2}\Sigma G_n$ for n even. There is a strong connection between the relations of cyclotomic numbers and the relations between Stickelberger elements (see [5], [7], ...). In the context here, in analogy to the exact sequence (13), the sequence

$$0 \to T'(n) \to \mathcal{L}(n)/(1+\sigma)\mathcal{L}(n) \to I/\langle \omega_n \rangle \xrightarrow{\overline{\nu}} 0 \tag{20}$$

is exact where the homomorphism $\overline{\nu}$ is defined by the maps $\nu_d : G_d \to I_n$, $a \mapsto \theta(an/d)$.

This situation can be handled as in the case of cyclotomic numbers. We denote the elements of $T'(n)$ as Ennola relations.

Algorithm 6.1 *We construct Ennola relations for $I/\langle \omega_n \rangle$ performing the following steps.*

1. *As in Algorithm 4.1, compute a σ-basis $[E^0, E^+, E^-]$ of $\mathcal{L}(n)$.*
2. *Each element of E^+ leads to a nontrivial element of $T'(n)$ which is via the mapping $\overline{\nu}$ in (20) a relation in $I_n/\langle \omega_n \rangle$.*

Theorem 6.2 *For $n > 2$ let r be the number of prime factors of n and*

$$c' = \begin{cases} 2^{r-1} - 1 & \text{for } n \not\equiv 2 \bmod 4, \\ 2^{r-2} & \text{for } n \equiv 2 \bmod 4. \end{cases} \tag{21}$$

Then there exist in $I_n/\langle \omega_n \rangle$ exactly $2^{c'}$ different Ennola relations which are generated by c' different relations. These relations can be constructed explicitly with Algorithm 6.1.

As an example, we show here an Ennola relation for $n = 15$. We have

$$\theta(1) + \theta(7) - \theta(3) - \theta(5) = 0. \tag{22}$$

Remark 6.3 *There is no canonical definition of a "relative Stickelberger ideal" as there is one for relative cyclotomic numbers. However, we can investigate the torsion group* $\widehat{T'}(n)$ *of* $Y(n)/(1+\sigma)Y(n)$ *and get in analogy to Lemma 5.1 the following result:*
The torsion group $\widehat{T'}(n)$ *is isomorphic to* $\mathbf{Z}/2\mathbf{Z}$ *in the following two cases:*

$$\begin{aligned} &r \text{ even and } n = u, \\ &r \text{ even and } n = 4u \end{aligned} \tag{23}$$

where u *is odd and square free. In all other cases* $\widehat{T'}(n)$ *is trivial.*

References

[1] H. Bass, *Generators and relations for cyclotomic units*, Nagoya Mathematical Journal 27 (1966), 401-407.

[2] M. Conrad, *Construction of Bases for the Group of Cyclotomic Units*, J. Number Theory, to appear.

[3] M. Conrad, *Basen von Moduln mit Anwendung auf Kreiseinheiten und Stickelbergerelemente*, Dissertation an der Universität des Saarlandes, Saarbrücken, 1997.

[4] V. Ennola, *On Relations between Cyclotomic Units*, J. Number Theory **4** (1972), 236-247.

[5] R. Kučera, *On bases of the Stickelberger ideal and of the group of circular units of a cyclotomic field*, J. Number Theory **40** (1992), 284-316.

[6] K. Ramachandra, *On the units of cyclotomic fields*, Acta Arith. **12** (1966), 165–173.

[7] C.-G. Schmidt, *Die Relationsfaktorgruppen von Stickelberger-Elementen und Kreiszahlen*, J. Reine Angew. Math. **315** (1980), 60–72.

[8] SIMATH, *Ein Computeralgebrasystem für algorithmische Zahlentheorie*, http://emmy.math.uni-sb.de/∼simath.

[9] W. Sinnot, *On the Stickelberger ideal and the circular units of a cyclotomic field*, Ann. Math. **108** (1978), 107-134.

[10] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer, New York 1982.