Journal of Number Theory **81**, 1–15 (2000)
Article ID jnth.1999.2443, available online at http://www.idealibrary.com on IDEAL®

Construction of Bases for the Group of Cyclotomic Units

Marc Conrad

Fachbereich Mathematik, Universität des Saarlandes, Postfach 15 11 50, D-66041 Saarbrücken, Germany
E-mail: marc@math.uni-sb.de

Communicated by M. Pohst

Received October 16, 1998

Subject of investigation is the construction of a basis B_n for the group of cyclotomic units of the nth cyclotomic field. These bases have the property that $B_d \subseteq B_n$ for $d \mid n$. For this purpose the notion of weak σ-bases of a module with an involution operating on it is introduced. The weak σ-basis of a special module then leads via explicit given isomorphisms to the desired bases for the group of cyclotomic units.

Key Words: basis; cyclotomic field; cyclotomic units; involution; Stickelberger ideal; unit group.

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 $1-\varepsilon_n^k$ with $k \not\equiv 0 \bmod n$ modulo roots of unity in order to avoid torsion. The group of *cyclotomic units* $C^{(n)}$ is defined as the subgroup of $D^{(n)}$ containing the elements which are units in $\mathbf{Z}[\varepsilon_n]$. This group has been often subject of investigation ([2], [3], [6], [7], [8], ...) and is well known in the case that n is the power of a prime.

In the past, Ramachandra [5] found a system of independent units in $C^{(n)}$ for general n generating a subgroup of finite index. Later, Kučera [4] constructed a basis for $C^{(n)}$ using the notion of distributions. Here, a different approach is used which leads to a basis for $C^{(n)}$ and $C^{(\infty)} = \bigcup_{n \in \mathbf{N}} C^{(n)}$.

We consider free $\mathbf{Z}$-modules M with an involution σ operating on it and show different methods to construct bases for $M_+ = M/\ker_M(1+\sigma)$. We further introduce special systems of modules which are defined as a set of triples $(M_d, \mathscr{E}_d, \mathtt{n}_d)_{d \in \Delta}$ where Δ is an ordered indexing set, the M_d are modules, $\mathscr{E}_d \subseteq M_d$ and $\mathtt{n}_d: \mathscr{E}_d \to \bigoplus_{t<d} M_t$ is a mapping for each $d \in \Delta$. Explicit conditions are given how to handle the *combination*

$$\mathscr{L} = \left(\bigoplus_{d \in \Delta} M_d \right) \Big/ \sum_{d \in \Delta} \langle r + \mathtt{n}_d(r); r \in \mathscr{E}_d \rangle \tag{1}$$

0022-314X/00 $35.00

of the system, and we work out how to construct a basis for $\mathscr{L}_+$ using special bases, the so called *weak σ-bases* of the modules $M_d/\langle \mathscr{E}_d \rangle$.

For well chosen input parameters Δ, M_d, $\mathscr{E}_d$ and $\mathfrak{n}_d$ we obtain as combination a module $\mathscr{L}(n)$ for which an isomorphism $\mathscr{L}(n)_+ \cong D^{(n)}$ holds. This leads via weak σ-bases of the modules $M_d/\langle \mathscr{E}_d \rangle$ to a basis for $D^{(n)}$ which can be easily modified to a basis for the group of cyclotomic units $C^{(n)}$. By this construction, we obtain a basis B_n for $C^{(n)}$ such that $B_d \subseteq B_n$ whenever $d \mid n$. This leads obviously to a basis for $C^{(\infty)}$.

In the last section there is a short discussion about further applications of these methods. These are the explicit construction of the relations in $C^{(n)}$ and similar results for the Stickelberger ideal as for cyclotomic units.

2. WEAK σ-BASES

For a set B, a finitely generated 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. We assume further that an involution σ operates on each module. The involution then defines the two modules $M_- = M/\ker_M(1-\sigma)$ and $M_+ = M/\ker_M(1+\sigma)$.

A *weak 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) $\sigma e \equiv e \bmod \langle E^0 \cup \sigma E^0 \rangle$ for $e \in E^+$

(ii) $\sigma e \equiv -e \bmod \langle E^0 \cup \sigma E^0 \rangle$ for $e \in E^-$

hold. We write $B = [E^0, E^+, E^-]$ for short.

We state some results about weak σ-bases which can be straightforwardly proved. For details see [1].

(I) $E^0 \cup E^+$ induces a basis of M_+ and $E^0 \cup E^-$ induces a basis of M_-.

(II) 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 $H^1(\sigma, M)$.

(III) Let $C = [F^0, F^+, F^-]$ a weak σ-basis of a second 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 weak σ-basis of $M \otimes L$.

(IV) Let x be one of the symbols $+$ or $-$. Given an exact sequence of free modules

$$0 \to M \to L \to K \to 0 \tag{2}$$

the following three statements are equivalent:

(i) The sequence (2) splits over σ.

(ii) The sequences $0 \to M_+ \to L_+ \to K_+ \to 0$ and $0 \to M_- \to L_- \to K_- \to 0$ are exact.

(iii) The equation $m^x(L) = m^x(M) + m^x(K)$ holds.

Moreover, if (i)–(iii) hold and $C = [F^0, F^+, F^-] \subseteq L$ induces a weak σ-basis of K we obtain from (I) and by the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \longrightarrow & L & \longrightarrow & K & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & M_x & \longrightarrow & L_x & \longrightarrow & K_x & \longrightarrow & 0, \end{array} \tag{3}$$

that $E^0 \cup E^x \cup F^0 \cup F^x$ induces a basis of L_x.

Repeated application of (IV) leads to the following lemma.

LEMMA 2.1. *Let* $x \in \{+, -\}$ *and* $0 = L^{(0)} \leqslant L^{(1)} \leqslant \cdots \leqslant L^{(i)} \leqslant \cdots \leqslant L$ *an ascending chain of modules with* $L = \bigcup_{i=0}^{\infty} L^{(i)}$. *Suppose that for every* $i \in \mathbf{N}$ *there exists a module* $M^{(i)}$ *such that the sequence*

$$0 \to L^{(i-1)} \to L^{(i)} \to M^{(i)} \to 0 \tag{4}$$

is exact and splits over σ. *If* $B_x^{(i)} \subseteq L^{(i)}$ *induces a basis of* $M_x^{(i)}$ *for all* $i \in \mathbf{N}$ *then* $\bigcup_{i=1}^{\infty} B_x^{(i)}$ *induces a basis of* L_x.

For the rest of this section let Δ be a finite or countable, partially ordered indexing set whose ordering can be completed. We assume further that $\{d \in \Delta; d \leqslant t\}$ is finite for every $t \in \Delta$. Examples are the set of all divisors of a number $n \in \mathbf{N}$ or $\mathbf{N}$ itself ordered by divisibility.

DEFINITION 2.2. For every $d \in \Delta$ let M_d be a module, $\mathscr{E}_d$ a subset of M_d with $\sigma\mathscr{E}_d = \mathscr{E}_d$ and $\mathrm{n}_d: \mathscr{E}_d \to \bigoplus_{t<d} M_t$ a mapping. We call a system of triples $(M_d, \mathscr{E}_d, \mathrm{n}_d)_{d \in \Delta}$ a *M*$\mathscr{E}$n*-system.*

Let $N'_d = \bigoplus_{t<d} M_t$ and $Q'_d = \sum_{t<d} \langle r + \mathrm{n}_t(r); r \in \mathscr{E}_t \rangle \subseteq N'_d$. We call the *M*$\mathscr{E}$n-system Γ *combinable*, if the mappings n_d can be extended to σ-homomorphisms

$$\bar{\mathrm{n}}_d: \langle \mathscr{E}_d \rangle \to N'_d/Q'_d. \tag{5}$$

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

DEFINITION 2.3. In the case that Δ is finite we say that Γ splits over σ if $m^+(\mathscr{L}) = \sum_{d \in \Delta} m^+(M_d/\langle \mathscr{E}_d \rangle)$. If Δ is infinite we say that Γ splits over σ if $(M_d, \mathscr{E}_d, \mathtt{n}_d)_{d \leqslant t}$ splits for every $t \in \Delta$.

THEOREM 2.4. *If $M_d/\langle \mathscr{E}_d \rangle$ is free for all $d \in \Delta$ then the combination $\mathscr{L}$ is also free. Under the additional assumption that Γ splits over σ we have for $x \in \{+, -\}$ that if $B_x^{(d)} \subseteq M_d$ induces a basis of $(M_d/\langle \mathscr{E}_d \rangle)_x$ for each $d \in \Delta$ then $\bigcup_{d \in \Delta} B_x^{(d)} \subseteq \bigoplus_{d \in \Delta} M_d$ induces a basis of $\mathscr{L}_x$.*

Proof. We complete the ordering of Δ and therefore assume that $\Delta = \mathbf{N}$ or $\Delta = \{1, ..., n\}$ with the canonical ordering. For $i \in \Delta \cup \{0\}$ let $N_i = M_1 \oplus \cdots \oplus M_i$ and

$$Q_i = \sum_{j=1}^{i} \langle r + \mathtt{n}_j(r); r \in \mathscr{E}_j \rangle \leqslant N_i . \tag{6}$$

We show first $Q_i \cap N_{i-1} = Q_{i-1}$. We have $q \equiv \sum_{e \in \mathscr{E}_i} \alpha_e (e + \mathtt{n}_i(e)) \bmod Q_{i-1}$ with $\alpha_e \in \mathbf{Z}$ for $q \in Q_i$. Because $\bar{\mathtt{n}}_i$ is a homomorphism modulo Q_{i-1} it follows

$$q \equiv r + \bar{\mathtt{n}}_i(r) \bmod Q_{i-1} \tag{7}$$

with $r = \sum_{e \in \mathscr{E}_i} \alpha_e e$. Reducing (7) modulo N_{i-1} and assuming $q \in N_{i-1}$ we get $r = 0$. This implies $\bar{\mathtt{n}}_i(r) = 0$ in (7) which leads to $q \in Q_{i-1}$.

From $Q_i \cap N_{i-1} = Q_{i-1}$ we deduce inductively $Q \cap N_{i-1} = Q_{i-1}$ where $Q = \bigcup_{i \in \Delta} Q_i$. So we have an ascending chain of modules

$$0 = N_0/Q_0 \leqslant N_1/Q_1 \leqslant N_2/Q_2 \leqslant \cdots \leqslant N/Q \tag{8}$$

with exact sequences

$$0 \to N_{i-1}/Q_{i-1} \to N_i/Q_i \to M_i/\langle \mathscr{E}_i \rangle \to 0. \tag{9}$$

The claim of the theorem follows by Lemma 2.1 if we prove that (9) splits over σ. Let $x_i = m^+(N_i/Q_i)$ and $y_i = m^+(M_i/\langle \mathscr{E}_i \rangle)$. For all exact sequences we have $x_i \leqslant x_{i-1} + y_i$ and the assumption that Γ splits gives (in the case that n is finite) $\sum_{i=1}^{n} x_i = y_n$. Putting this together we obtain $x_i = x_{i-1} + y_i$ which implies by (IV) that (9) splits over σ. The infinite case can be reduced directly to the finite case. ∎

In the case that Γ does not split over σ it is possible to save the construction by introducing the notion of a derived $M\mathscr{E}\mathrm{n}$-system.

DEFINITION 2.5. Assume that 0 is an element which is not in Δ. Let the ordering on $\Delta \cup \{0\}$ be defined by saying that 0 is smaller than any $d \in \Delta$. Then we set $\Delta^D = \{0\} \cup \{t \in \Delta; t \nleqslant D\}$ for $D \in \Delta$ and define the derived $M\mathscr{E}\mathrm{n}$-system $\Gamma^{(D)} = (M_d, \mathscr{E}_d, \mathrm{n}_d)_{d \in \Delta^D}$ by the settings $M_0 = \bigoplus_{t \leqslant D} M_t$, $\mathscr{E}_0 = \bigcup_{t \leqslant D} \{r + \mathrm{n}_t(r); r \in \mathscr{E}_t\}$ and $\mathrm{n}_0 \equiv 0$.

With this definition we see directly:

LEMMA 2.6. *If Γ is combinable then $\Gamma^{(D)}$ is combinable and the combinations of Γ and $\Gamma^{(D)}$ are identical.*

3. THE CYCLOTOMIC MODULE

For a finite subset S of a module M we write $\Sigma(S)$ for $\sum_{s \in S} s$. Further, let $G_d = \{1 \leqslant a < d; (a, d) = 1\}$.

DEFINITION 3.1. For $n > 1$ 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 $A_p = \{0, ..., p-1\}$.

If $n = q_1 \cdots q_r$ where q_i are powers of distinct primes 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.

With (III) from the previous section it is possible to construct weak σ-bases of $Z(n)$ by weak σ-bases of $Z(q)$. Table 1 gives a weak σ-basis for $Z(q)$.

The rank of $Z(q)$ is (by Table 1) $\varphi(q) - \varphi(q/p)$ where φ is Euler's function. Therefore the rank of $Z(n)$ is $\prod_{p \mid n} (\varphi(p^{\alpha_p}) - \varphi(p^{\alpha_p - 1}))$ where p runs over all prime divisors of n and α_p is the exponent of p in n.

LEMMA 3.2. *There is an isomorphism $Z(n) \cong \langle G_n \rangle / R_n$. The submodule R_n of $\langle G_n \rangle$ is generated by $\mathscr{E}_n = \{s(n, p, a); p \mid n$ with p prime, $a \in G_{n/p}\}$ with*

$$s(n, p, a) = \Sigma(\{x \in G_n; x \equiv a \bmod (n/p)\}). \tag{10}$$

TABLE I

Weak σ-bases of $Z(q)$

module	weak σ-basis
$Z(2)$	$[\varnothing, \varnothing, \varnothing]$
$Z(p)$, $p \neq 2$, p prime	$[\{2, ..., (p-1)/2\}, \varnothing, \{1\}]$
$Z(4)$	$[\varnothing, \varnothing, \{(1, 0)\}]$
$Z(q)$, $q = p^\alpha$, $\alpha > 1$, p prime, $q \neq 4$	$[\{(b, a);\ 1 \leqslant b < \frac{1}{2}q/p,\ p \nmid b,\ 1 \leqslant a < p\}, \varnothing, \varnothing]$

Proof. We arrange the prime factors p_i of n such that

$$n = p_1^{\alpha_1} \cdots p_t^{\alpha_t} p_{t+1} \cdots p_r \tag{11}$$

with $\alpha_i > 1$ for $i = 1, ..., t$. Further we set $q_i = p_i^{\alpha_i}$ if $i = 1, ..., t$ and $q_i = p_i$ else. Let

$$S = G_{q_1/p_1} \times A_{p_1} \times \cdots \times G_{q_t/p_t} \times A_{p_t} \times G_{p_{t+1}} \times \cdots \times G_{p_r}. \tag{12}$$

It is obvious by the definition of the tensor product that $Z(n)$ is isomorphic to $\langle S \rangle$ modulo suitable relations. We show that S is as set isomorphic to G_n. Using the bijection between S and G_n it can be shown directly that the sums of (10) correspond one to one to the sums used in Definition 3.1.

We obtain $S \cong G_n$ by combining isomorphisms ξ_i and η in the following way:

$$\begin{array}{ccccccccc} \underbrace{G_{q_1/p_1} \times A_{p_1}} & \times \cdots \times & \underbrace{G_{q_t/p_t} \times A_{p_t}} & \times & G_{p_{t+1}} & \times \cdots \times & G_{p_r} \\ \downarrow \xi_1 & & \downarrow \xi_t & & \downarrow \mathrm{id} & & \downarrow \mathrm{id} \\ G_{q_1} & \times \cdots \times & G_{q_t} & \times & G_{q_{t+1}} & \times \cdots \times & G_{q_r} \\ & & & & \downarrow \eta & & \\ & & & & G_n & & \end{array} \tag{13}$$

The maps ξ_i for $i = 1, ..., t$ 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}, $i = 1, ..., r$. ∎

We observe that a weak σ-basis of $Z(n)$ can be constructed with the bases of Table 1 and (III) as a subset of S. We give an example how such a basis looks like. A complete list can be found in [1]. In the case that n is odd and square free $[F^0, F^+, F^-]$ is a weak σ-basis where

$$F^0 = \bigcup_{i=1}^{r} \{(1, ..., 1, a_i, ..., a_r) \in G_{p_1} \times \cdots \times G_{p_r};\ 1 < a_i < p_i/2$$
$$\text{and } 1 \leqslant a_j < p_j - 1 \text{ for } j = i+1, ..., r\},$$
$$F^+ = \{(1, ..., 1)\} \text{ for } r \text{ even and } F^+ = \varnothing \text{ for } r \text{ odd},$$
$$F^- = \{(1, ..., 1)\} \setminus F^+.$$

In the sequel we write $\mathbf{N}_\infty = \mathbf{N} \cup \{\infty\}$ and agree that the set of all d with $d \mid \infty$ means $\mathbf{N}$ (and not $\mathbf{N}_\infty$).

DEFINITION 3.3. For $d \in \mathbf{N}$ let $M_d = \langle G_d \rangle$. If d is not a prime we denote by $\mathscr{E}_d \subseteq M_d$ the set of the sums $s(d, p, a)$ as in Lemma 3.2. For d prime we define $\mathscr{E}_d = \varnothing$. On $\mathscr{E}_d$ we define the mapping

$$\mathrm{n}_d: \mathscr{E}_d \to \bigoplus_{t \mid d,\ t \neq d} M_t,\ s(d, p, a) \mapsto \begin{cases} -[d/p; a] & \text{if } p^2 \mid d, \\ [d/p; p^{-1}a] - [d/p; a] & \text{if } p^2 \nmid d \end{cases} \tag{14}$$

where $[m; x]$ denotes $y \in G_m$ with $x \equiv y \bmod m$.

For $n \in \mathbf{N}_\infty$ we call the $M\mathscr{E}\mathrm{n}$-system $\Gamma(n) = (M_d, \mathscr{E}_d, \mathrm{n}_d)_{d \mid n}$ the nth *cyclotomic system.*

LEMMA 3.4. *Let $n \in \mathbf{N}_\infty$. Then $\Gamma(n)$ is combinable.*

Proof. We have to show that it is possible to extend each n_d to a homomorphism modulo $Q'_d = \sum_{t \mid d,\ t \neq d} \langle r + \mathrm{n}_t(r);\ r \in \mathscr{E}_t \rangle$. In order to do so we have to investigate the relations between the elements of $\mathscr{E}_d$.

The module $Z(n)$ is the tensor product of modules $\langle A \rangle / R$ with suitable sets A where either R is equal zero or is generated by $\Sigma(A)$. In the special case $Z(n) \cong (M_1/R_1) \otimes (M_2/R_2)$ where R_1 and R_2 are generated by the sum of the free generators of M_1 and M_2 respectively, the isomorphism $(M_1/R_1) \otimes (M_2/R_2) \cong (M_1 \otimes M_2)/(R_1 \otimes M_2 + M_1 \otimes R_2)$ and $(R_1 \otimes M_2) \cap (M_1 \otimes R_2) = R_1 \otimes R_2$ show that the only relation between the sums is given by the double sum over the generators of M_1 and M_2. By induction and applying the isomorphism of Lemma 3.2 we obtain in the general case that all relations are given by

$$\sum_{\substack{x \in G_d \\ x \equiv a \bmod d/p'}} s(d, p, x) = \sum_{\substack{x \in G_d \\ x \equiv a \bmod d/p}} s(d, p', x) \tag{15}$$

where p and p' are two different primes dividing d. So we have to check

$$\sum_{\substack{x \in G_d \\ x \equiv a \bmod d/p'}} \mathtt{n}_d(s(d, p, x)) \equiv \sum_{\substack{x \in G_d \\ x \equiv a \bmod d/p}} \mathtt{n}_d(s(d, p', x)) \qquad \bmod Q'_d \tag{16}$$

which is done by a straightforward calculation. ∎

In the sequel we denote by $\mathscr{L}(n)$ the combination of $\Gamma(n)$. For finite n the module $\mathscr{L}(n)$ is isomorphic to a module introduced in [6]. We shall use this isomorphism to determine the σ-cohomology of $\mathscr{L}(n)$.

LEMMA 3.5. *Let $n > 2$ and r be the number of prime factors of n. Then we have*:

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

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

Proof. A similar claim is given in [6], Theorem 2 for a module $A = V/U$ where V is the free module over $\{e(1), ..., e(n-1)\}$ and U is generated by elements

$$a(d, x) = e(dx) - \sum_{\nu=0}^{d-1} e\left(x + \nu \frac{n}{d}\right) \tag{17}$$

with $d \mid n$ and $x = 1, ..., n/d - 1$. We show $A \cong \mathscr{L}(n)$.

We have $\mathscr{L}(n) = N/Q$ where $N = \bigoplus_{d \mid n} M_d$ and $Q = \sum_{d \mid n} \langle r + \mathtt{n}_d(r); r \in \mathscr{E}_d \rangle$. The bijection $G_d \ni a \mapsto e(an/d)$ shows $N \cong V$.

With $s(d, p, b)$ as in (10) the isomorphism $Q \cong U$ is verified by showing that $s(d, p, b) + \mathtt{n}_d(s(d, p, b))$ maps to $-a(p, bn/d)$ and noting that the elements $a(p, x)$ where p is prime generate already U. This follows from the relation

$$a(dt, x) = a(d, tx) + \sum_{j=0}^{d-1} a\left(t, x + j \frac{n}{dt}\right), \tag{18}$$

for $dt \mid n$, $d > 1$, $t > 1$ and $1 \leqslant x < n/dt$. ∎

LEMMA 3.6. *Let $n \in \mathbf{N}_\infty$.*

(a) *$\Gamma(n)$ splits over σ if and only if $n \not\equiv 0 \bmod 4$.*

(b) *For $n \equiv 0 \bmod 4$ the system $\Gamma(n)^{(4)}$ splits over σ.*

Proof. For $n=1$ and $n=2$ Lemma 3.6 is obviously valid, and we assume $n>2$ for the rest of the proof.

For $d\in\mathbf{N}$ we define $g(d)=\prod_{p\mid d}(\varphi(p^{\alpha_p})-\varphi(p^{\alpha_p-1}))$ where α_p is maximal with $p^{\alpha_p}\mid d$ and φ is Euler's function. Induction gives $\varphi(n)=\sum_{d\mid n} g(d)$.

$\Gamma(n)$ is defined as a $M\mathscr{E}\mathrm{n}$-system $(M_d, \mathscr{E}_d, \mathrm{n}_d)_{d\mid n}$ and we set $Y_d = M_d/\langle \mathscr{E}_d\rangle$. So we have

$$Y_d=\begin{cases}0 & \text{if } d=1,\\ \langle G_d\rangle & \text{if } d \text{ is prime},\\ Z(d) & \text{otherwise.}\end{cases} \tag{19}$$

By elementary computations in the first two cases and from Definition 3.1 in the third case we calculate the rank and the invariants m^x of the Y_d which are summarized in Table 2 where $r(d)$ denotes the number of distinct primes dividing d.

Therefore we have

$$\sum_{d\mid n} m^+(Y_d)=\begin{cases}2^{r-1}-1 & \text{if } n\equiv 1, 3 \bmod 4,\\ 2^{r-1} & \text{if } n\equiv 0 \bmod 4,\\ 2^{r-2} & \text{if } n\equiv 2 \bmod 4.\end{cases} \tag{20}$$

with $r=r(n)$ the number of distinct primes dividing n.

The number $m^+(\mathscr{L}(n))$ is the $\mathbf{F}_2$-dimension of $H^0(\sigma, \mathscr{L}(n))$. So by Lemma 3.5 we find $m^+(\mathscr{L}(n))=\sum_{d\mid n} m^+(Y_d)$ if and only if $n\not\equiv 0 \bmod 4$ and part (a) of Lemma 3.6 follows.

In the case $n\equiv 0 \bmod 4$ and $n\neq\infty$ we have $m^+(\mathscr{L}(n))+1=\sum_{d\mid n} m^+(Y_d)$. By definition, $\Gamma(n)^{(4)}$ is formed by replacing the modules Y_2

TABLE II

Invariants of Y_d

	m^+	m^-	rank
$d=1$	0	0	$g(d)-1$
$d=2$	1	0	$g(d)+1$
$d=p$ an odd prime	0	0	$g(d)+1$
$d=u$ or $d=4u$ where u is odd, square free and $2\mid r(d)$	1	0	$g(d)$
d not prime, $d=u$ or $d=4u$ where u is odd, square free and $2\nmid r(d)$	0	1	$g(d)$
all other d	0	0	$g(d)$

and Y_4 with $\mathscr{L}(4)$. Part (b) follows with $m^+(\mathscr{L}(4)) = m^+(Y_4) = 0$ and $m^+(Y_2) = 1$.

The case $n = \infty$ follows directly from the finite case. ∎

4. CYCLOTOMIC NUMBERS

We denote as in the introduction by $D^{(n)}$ the group of *cyclotomic numbers*. Especially we write $D^{(\infty)} = \bigcup_{d \in \mathbf{N}} D^{(n)}$.

LEMMA 4.1. *Let $n \in \mathbf{N}_\infty$. Then the sequence*

$$0 \to T \to \mathscr{L}(n)/(1-\sigma)\,\mathscr{L}(n) \xrightarrow{\bar{\mu}} D^{(n)} \to 1, \tag{21}$$

where T is the torsion group of $\mathscr{L}(n)/(1-\sigma)\,\mathscr{L}(n)$, is exact. The homomorphism $\bar{\mu}$ is defined by the maps $\mu_d\colon G_d \to D^{(n)}$, $a \mapsto 1-\varepsilon_d^a$ for $d \mid n$ where ε_d is a primitive dth root of unity such that $\varepsilon_d = \varepsilon_t^{t/d}$ whenever $d \mid t$.

Proof. We write $\mathscr{L}(n) = N/Q$ such that we have $N = \bigoplus_{d \mid n} M_d$ and $Q = \sum_{d \mid n} \langle r + \mathrm{n}_d(r);\, r \in \mathscr{E}_d \rangle$.

We will first show that $\bar{\mu}$ is well defined. Because of the isomorphism $\mathscr{L}(n)/(1-\sigma)\,\mathscr{L}(n) \cong N/((1-\sigma)\,N + Q)$ we have to show that $(1-\sigma)\,N$ and Q are mapped by μ to unit roots.

- For $(1-\sigma)\,N$ this follows from $(1-\varepsilon_d^a)/(1-\varepsilon_d^{-a}) = -\varepsilon_d^a$.
- The generators of Q correspond to relations which arise by taking norms in cyclotomic fields. If $N_{d,p}$ for $p \mid d$ denotes the relative norm from $\mathbf{Q}(\varepsilon_d)$ to $\mathbf{Q}(\varepsilon_{d/p})$ we have for $d \neq p$ that

$$N_{d,p}(1-\varepsilon_d^a) = \prod_{\substack{c \in G_d \\ c \equiv a \bmod d/p}} (1-\varepsilon_d^c) = \begin{cases} 1-\varepsilon_{d/p}^a & \text{if } p^2 \mid d, \\ (1-\varepsilon_{d/p}^a)/(1-\varepsilon_{d/p}^{a'}) & \text{if } p^2 \nmid d \end{cases} \tag{22}$$

with $pa' \equiv a \bmod d/p$ in the case $p^2 \nmid d$. Note that these relations can be derived directly from the polynomial identity $\prod_{\nu=0}^{p-1}(1-x\varepsilon_p^\nu) = 1-x^p$.

The module Q is generated by elements $s(d,p,a) + \mathrm{n}_d(s(d,p,a))$. Noting that $s(d,p,a)$ is mapped under μ on the product in the middle of (22) and $-\mathrm{n}_d(s(d,p,a))$ is mapped to the right side of (22) the claim follows.

Up to now we have shown that $\bar{\mu}$ is well defined and obviously $\bar{\mu}$ is surjective. It remains to show that the kernel of $\bar{\mu}$ is indeed the torsion group of $\mathscr{L}(n)/(1-\sigma)\,\mathscr{L}(n)$.

We look only at the case $n < \infty$. The case $n = \infty$ follows directly by reducing to the finite case. Because $D^{(n)}$ is free it is sufficient to show that

the rank of the free part of $\mathscr{L}(n)/(1-\sigma)\,\mathscr{L}(n)$ is equal to the rank of $D^{(n)}$. In Lemma 5.2 we will show that $\operatorname{rank}(D^{(n)}) = \frac{1}{2}\varphi(n) + r - 1$ where r denotes the number of primes dividing n. The module M_+ is the free part of $M/(1-\sigma)\,M$ for any free module M, especially for $M = \mathscr{L}(n)$. We complete the proof by computing the rank of $\mathscr{L}(n)_+$.

First we observe that for any module M we have the formula $\operatorname{rank}(M_+) = \frac{1}{2}(\operatorname{rank}(M) + m^+(M) - m^-(M))$ and we apply it for $M = \mathscr{L}(n)$. Lemma 3.5 gives us the values $m^+(\mathscr{L}(n))$ and $m^-(\mathscr{L}(n))$. The rank of $\mathscr{L}(n)$ is equal the sum of all ranks of the Y_d with $d \mid n$. These are listed in Table 2. All this together gives $\operatorname{rank}(\mathscr{L}(n)_+) = \frac{1}{2}\varphi(n) + r - 1$. ∎

LEMMA 4.2. $\mathscr{L}(n)_+ \cong D^{(n)}$.

Proof. The claim is a direct consequence of Lemma 4.1. ∎

Using Lemma 4.2 we are now able to determine a basis of $D^{(n)}$. By means of weak σ-bases of the Y_d for $d \mid n$ and (I) of Section 2 bases of $(Y_d)_+$ can be constructed. With the help of Theorem 2.4 we construct a basis of $\mathscr{L}(n)_+$ which leads via the isomorphism of Lemma 4.2 to a basis of $D^{(n)}$.

In the sequel we will give another approach using *relative* cyclotomic numbers that opens the way for the construction of bases for cyclotomic units. For $n \in \mathbf{N}$ let $K^{(n)} = \prod_{d \mid n,\, d \neq n} D^{(d)}$. We call $\widehat{D^{(n)}} = D^{(n)}/K^{(n)}$ the group of nth *relative cyclotomic numbers*.

LEMMA 4.3. $\widehat{D^{(n)}} \cong (Y_n)_+$ *for* $n \neq 4$.

Proof. Setting $N' = \bigoplus_{d \mid n,\, d \neq n} M_d$ and $Q' = \sum_{d \mid n,\, d \neq n} \langle r + \mathrm{n}_d(r);\, r \in \mathscr{E}_d \rangle$ we obtain the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & (N'/Q')_+ & \longrightarrow & \mathscr{L}(n)_+ & \longrightarrow & (Y_n)_+ & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & K^{(n)} & \longrightarrow & D^{(n)} & \longrightarrow & \widehat{D^{(n)}} & \longrightarrow & 0. \end{array} \tag{23}$$

The lower sequence is exact by definition. The upper sequence is exact because the same sequence without "+" splits over σ (which is not the case for $n = 4$, so we have to exclude this case in the theorem). All vertical arrows are surjective and the arrow in the middle is according to Lemma 4.2 an isomorphism. The left vertical arrow in the diagram is a restriction of this isomorphism and therefore also an isomorphism. With that also the right vertical arrow is an isomorphism. ∎

LEMMA 4.4. *$\widehat{D^{(n)}}$ is free for $n \neq 4$.*

Proof. Because $(Y_n)_+$ is free this follows directly from Lemma 4.3. ∎

Remark 4.5. Elementary calculations show that $\widehat{D^{(4)}}$ is a group with two elements and therefore not free.

THEOREM 4.6. *Let $n \in \mathbf{N}_\infty$. If for each $d \mid n$, $d \neq 4$ the set $\widehat{B_d} \subseteq D^{(n)}$ induces a basis of $\widehat{D^{(d)}}$ we have*:

(a) $\bigcup_{d \mid n} \widehat{B_d}$ *is a basis of $D^{(n)}$ for $n \not\equiv 0 \bmod 4$.*

(b) $\{1-\varepsilon_4\} \cup \bigcup_{\substack{d \mid n \\ d \neq 2,4}} \widehat{B_d}$ *is a basis of $D^{(n)}$ for $n \equiv 0 \bmod 4$.*

Proof. With Lemma 3.6 and Theorem 2.4 a basis of $\mathscr{L}(n)_+$ is given by the union of bases of the $(Y_d)_+$ where $d \mid n$ with some slight modifications for $n \equiv 0 \bmod 4$. This leads to the theorem via the isomorphisms from Lemma 4.2 and Lemma 4.3. ∎

5. CYCLOTOMIC UNITS

We write uniquely

$$n = q_1 \cdots q_r = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \tag{24}$$

with $q_i = p_i^{\alpha_i}$ for $i = 1, ..., r$ and p_i prime. Then the group of cyclotomic units $C^{(n)}$ is modulo unit roots generated by

$$\frac{1-\varepsilon_{q_i}^a}{1-\varepsilon_{q_i}} \quad \text{where} \quad a \in G_{q_i} \quad \text{for} \quad i = 1, ..., r$$

and

$$1-\varepsilon_d^a \quad \text{where} \quad 1 < d \mid n \quad \text{and} \quad d \text{ is not a prime power}, \quad a \in G_d.$$

The key for the construction of bases of cyclotomic units from bases of cyclotomic numbers is given in the next lemma.

LEMMA 5.1. *Let $B \subseteq C^{(n)}$. Then $B \cup \bigcup_{i=1}^r \{1-\varepsilon_{q_i}\}$ is a basis of $D^{(n)}$ if and only if B is a basis of $C^{(n)}$.*

Proof. We show first the "only if"-case. Of course B is multiplicatively independent in $C^{(n)}$. So it remains to show that B is a set of generators of $C^{(n)}$.

We write $u \in C^{(n)}$ as $u = v \prod_{i=1}^{r} (1-\varepsilon_{q_i})^{b_i}$ with $v \in \langle B \rangle$ and $b_i \in \mathbf{Z}$. Taking the absolute norm of $\mathbf{Q}(\varepsilon_n)$ on both sides gives $1 = \prod_{i=1}^{r} p_i^{b_i k_i}$ with $k_i = \varphi(n)/\varphi(q_i) \neq 0$ and it follows that $b_i = 0$ for all $i \in \{1, ..., r\}$.

For the "if"-case we use the relation

$$\prod_{\substack{b \in G_q \\ b \equiv 1 \bmod q/p}} (1-\varepsilon_q^b) = 1 - \varepsilon_{q/p} \tag{25}$$

which holds for $q = p^\alpha$ with $\alpha > 1$. Because of $(1-\varepsilon_q^a)/(1-\varepsilon_q) \in C^{(n)}$ the set $B \cup \bigcup_{i=1}^{r} \{1-\varepsilon_{q_i}\}$ is a set of generators of $D^{(n)}$. The multiplicatively independence of the $1-\varepsilon_{q_i}$ and B follows by taking norms as in the "only if"-case. ∎

LEMMA 5.2. *Let $n > 2$. The rank of $D^{(n)}$ is $\frac{1}{2}\varphi(n) + r - 1$.*

Proof. The group of cyclotomic units has finite index in the full unit group of $\mathbf{Q}(\varepsilon_n)$ (see [7]). Therefore we have $\operatorname{rank}(C^{(n)}) = \frac{1}{2}\varphi(n) - 1$ for $n > 2$ ([9], Proposition 7-6-1). The claim follows from Lemma 5.1. ∎

We define the *relative cyclotomic units* by $\widehat{C^{(n)}} = C^{(n)}/L^{(n)}$ with $L^{(n)} = \prod_{d \mid n,\, d \neq n} C^{(d)}$. The connection between relative cyclotomic units and relative cyclotomic numbers is given by the isomorphisms

$$\widehat{C^{(n)}} \cong \widehat{D^{(n)}} \text{ if } n \text{ is not a prime power,}$$

$$\widehat{C^{(q)}} \cong \left\langle \frac{1-\varepsilon_q^a}{1-\varepsilon_q} K^{(q)}; a \in G_q \right\rangle \leqslant \widehat{D^{(q)}} \text{ if } n = q \text{ is a prime power.}$$

Analogously to Theorem 4.6 we obtain:

THEOREM 5.3. *Let $n \in \mathbf{N}_\infty$. If $\widehat{B_d} \subseteq C^{(n)}$ induces a basis of $\widehat{C^{(d)}}$ for $d \mid n$ then $B_n = \bigcup_{d \mid n} \widehat{B_d}$ is a basis of $C^{(n)}$.*

Proof. It is enough to consider the case when n is finite. The case $n = \infty$ follows directly from the finite case. Let p be a prime and $\alpha > 0$. Because of $C^{(p^{\alpha-1})} = L^{(p^\alpha)}$ the sequence

$$1 \to C^{(p^{\alpha-1})} \to C^{(p^\alpha)} \to \widehat{C^{(p^\alpha)}} \to 1 \tag{26}$$

is exact. The group $\widehat{C^{(p^\alpha)}}$ is free, because it is isomorphic to a subgroup of $\widehat{D^{(p^\alpha)}}$ which is free for $p^\alpha \neq 4$ and directly from the definition follows $\widehat{C^{(4)}} = 1$. By induction we deduce the claim of the theorem for $n = p^\alpha$. From Lemma 5.1 it follows that $E_q = \{1-\varepsilon_q\} \cup B_q$ is a basis of $D^{(q)}$.

Let Θ_n be the set of all divisors of n which are not prime powers. By Theorem 4.6 there exist $\widehat{F_d} \subseteq D^{(n)}$ with the following properties:

(a) $F_n = \bigcup_{d \mid n} \widehat{F_d}$ is a basis of $D^{(n)}$,

(b) $F_{q_i} = \bigcup_{d \mid q_i} \widehat{F_d}$ is is a basis of $D^{(q_i)}$ for $i = 1, ..., r$,

(c) $\widehat{F_d} = \widehat{B_d}$ for $d \in \Theta_n$.

By (c) we get $F_n = \bigcup_{i=1}^{r} F_{q_i} \cup \bigcup_{d \in \Theta_n} \widehat{B_d}$ which is by (a) a basis of $D^{(n)}$. Using (b) we can exchange F_{q_i} by E_{q_i} and obtain

$$\bigcup_{i=1}^{r} E_{q_i} \cup \bigcup_{d \in \Theta_n} \widehat{B_d} = \bigcup_{i=1}^{r} \{1 - \varepsilon_{q_i}\} \cup \bigcup_{d \mid n} \widehat{B_d} = \bigcup_{i=1}^{r} \{1 - \varepsilon_{q_i}\} \cup B_n \tag{27}$$

as basis of $D^{(n)}$. With Lemma 5.1 the claim follows. ∎

For $n \in \Theta_n$ we have

$$Z(n)_+ = (Y_n)_+ \cong \widehat{D^{(n)}} \cong \widehat{C^{(n)}}. \tag{28}$$

A basis of $Z(n)_+$ follows from a weak σ-basis of $Z(n)$. A weak σ-basis of $Z(n)$ can be constructed with the help of Table 1 and method (III) of Section 2. In order to complete the construction of a basis of $C^{(n)}$ it remains to give a basis for $\widehat{C^{(q)}}$ when $q = p^\alpha$. For $\alpha = 1$ it is well known [8] that

$$\left\{ \frac{1 - \varepsilon_p^a}{1 - \varepsilon_p};\ 1 < a < p/2 \right\} \tag{29}$$

induces a basis of $\widehat{C^{(p)}}$. For $\alpha > 1$ let $\Gamma = \{ b \in G_{q/p};\ 1 \leqslant b \leqslant \frac{1}{2} q/p \}$. Then

$$\left\{ \frac{1 - \varepsilon_q^{ap^{a-1}+b}}{1 - \varepsilon_q};\ (b, a) \in \Gamma \times \{1, ..., p-1\} \right\} \tag{30}$$

induces a basis of $\widehat{C^{(q)}}$.

6. REMARKS

The aim of this paper is the construction of bases for cyclotomic units. However there are further applications concerning the cyclotomic module and weak σ-bases. We give here two examples. For details see [1].

- A similar construction as for the group of cyclotomic units can be done for the Stickelberger ideal. Let I_n the ideal generated by the Stickelberger elements $\theta(a) = \sum_{\tau \in G_n} \langle -a\tau/n \rangle \tau^{-1}$ and $\omega_n = \Sigma(G_n)$ for n odd and $\omega_n = \frac{1}{2}\Sigma(G_n)$ for n even. Then we have in analogy to Lemma 4.2 the isomorphism $\mathscr{L}(n)_- \cong I / \langle \omega_n \rangle$ via $G_d \ni a \mapsto \theta(an/d)$.

• A stronger definition of weak σ-bases can be used to construct explicitly relations in the group of cyclotomic units, especially the relations not arising from norm relations or complex conjugation which has been discovered first by Ennola [2]. These relations are in our context implicitly given by the set T in the exact sequence (21).

REFERENCES

1. M. Conrad, "Basen von Moduln mit Anwendung auf Kreiseinheiten und Stickelberger-elemente," Dissertation an der Universität des Saarlandes, Saarbrücken, 1997.
2. V. Ennola, On relations between cyclotomic units, *J. Number Theory* **4** (1972), 236–247.
3. R. Gold and J. Kim, Bases for cyclotomic units, *Compositio Math.* **71** (1989), 13–28.
4. 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.
5. K. Ramachandra, On the units of cyclotomic fields, *Acta Arith.* **12** (1966), 165–173.
6. C.-G. Schmidt, Die Relationsfaktorgruppen von Stickelberger-Elementen und Kreiszahlen, *J. Reine Angew. Math.* **315** (1980), 60–72.
7. W. Sinnott, On the Stickelberger ideal and the circular units of a cyclotomic field, *Ann. Math.* **108** (1978), 107–134.
8. L. C. Washington, "Introduction to Cyclotomic Fields," Springer, New York, 1982.
9. E. Weiss, "Algebraic Number Theory," McGraw–Hill, New York, 1963.