ACTA ARITHMETICA
XCIII.4 (2000)

Universal normal bases for the abelian closure of the field of rational numbers

by

Dirk Hachenberger (Augsburg)

1. Introduction. If E/F is a finite-dimensional Galois extension with Galois group G, then, by the Normal Basis Theorem, there exist elements $w \in E$ such that $\{g(w) \mid g \in G\}$ is an F-basis of E, a so-called *normal basis*, whence w is called *normal* in E/F.

In the present paper, we study normal bases for *cyclotomic fields*. Let $\mathbb{Q}$ be the field of rational numbers; for a positive integer n, we let $\mathbb{Q}_n$ denote the nth cyclotomic field, i.e., $\mathbb{Q}_n = \mathbb{Q}(\zeta_n)$, where ζ_n is a primitive nth root of unity. For the basics on cyclotomic fields, we refer to [Ri] or [Wa]; we just remark that $\mathbb{Q}_n = \mathbb{Q}_m$ with $n > m$ holds if and only if $n = 2m$ and m is odd. As index set for the cyclotomic fields we therefore use the set $\mathcal{N}$ of positive integers which are either odd or divisible by 4. Thus, if $n, e \in \mathcal{N}$, then $\mathbb{Q}_n \subseteq \mathbb{Q}_e$ if and only if n divides e. We call $\mathbb{Q}_e/\mathbb{Q}_n$ a *cyclotomic extension*.

Definition 1.1. Let $e, n \in \mathcal{N}$ be such that n divides e. Then $w \in \mathbb{Q}_e$ is called *universally normal in* $\mathbb{Q}_e/\mathbb{Q}_n$ if w is normal in $\mathbb{Q}_e/\mathbb{Q}_d$ for every cyclotomic intermediate field $\mathbb{Q}_d$ of $\mathbb{Q}_e/\mathbb{Q}_n$ (i.e., for every divisor $d \in \mathcal{N}$ of e which is divisible by n). If $w \in \mathbb{Q}_e$ is simultaneously normal in $\mathbb{Q}_e/K$ for every intermediate field K of $\mathbb{Q}_e$ over $\mathbb{Q}_n$, then w is called *completely normal in* $\mathbb{Q}_e/\mathbb{Q}_n$.

The study of simultaneously normal elements is a nontrivial task which was first considered by Faith [Fa], but it was first proved by Blessenohl and Johnsen [BlJo1] that completely normal elements exist for arbitrary finite Galois extensions E/F. For more details we refer to the recent monograph [Ha], which is an extensive treatment of (completely) normal elements for finite fields, the central topics being their characterization, enumeration as

2000 *Mathematics Subject Classification*: 11R18, 12F05, 11B99.
Key words and phrases: cyclotomic field, abelian closure, normal basis/element, universally normal basis/element, completely normal basis/element, trace-compatible sequence.

well as explicit and algorithmic constructions of these objects. Many ideas of [Ha] are also essential for the present work.

In Section 3 we characterize and provide explicit constructions of completely normal elements for $\mathbb{Q}_{r^m}/\mathbb{Q}$, where r is any odd prime number and where $m \geq 1$ is any integer. In Section 5 we characterize and provide explicit constructions of universally normal elements for $\mathbb{Q}_{2^m}/\mathbb{Q}$, where $m \geq 2$ is any integer. Both constructions draw from Sections 4 and 2. In Section 4 we study regular cyclotomic extensions, which are defined to be extensions of the form $\mathbb{Q}_e/\mathbb{Q}_n$, where e and n have the same prime divisors. In Section 2 we provide important results on simultaneous generators for submodules of cyclic Galois extensions which apply to most of the situations considered in Sections 3–5. In Section 6, based on a product construction, we provide universally normal elements for $\mathbb{Q}_n/\mathbb{Q}$ where $n \in \mathcal{N}$ is arbitrary.

When working in a fixed algebraic closure of $\mathbb{Q}$, a famous theorem of Kronecker and Weber (see e.g. [Wa]) states that

$$\widehat{\mathbb{Q}} := \bigcup_{n \in \mathcal{N}} \mathbb{Q}_n$$

is the *abelian closure over* $\mathbb{Q}$, i.e., $\widehat{\mathbb{Q}}$ is the smallest algebraic extension A over $\mathbb{Q}$ such that any finite abelian extension of $\mathbb{Q}$ is contained in A. In Section 6 we provide a constructive version of the Normal Basis Theorem for $\widehat{\mathbb{Q}}/\mathbb{Q}$ by explicitly determining *trace-compatible sequences* entirely consisting of universally normal elements.

DEFINITION 1.2. For $n \in \mathcal{N}$ let $w_n \in \widehat{\mathbb{Q}}$ be such that $\mathbb{Q}_n = \mathbb{Q}(w_n)$. The sequence $(w_n)_{n \in \mathcal{N}}$ is called *trace-compatible* if the $(\mathbb{Q}_e, \mathbb{Q}_d)$-trace of w_e is equal to w_d whenever d divides e ([1]).

By results of Lenstra [Le], trace-compatible sequences of normal elements can be seen as analogues of normal basis generators of infinite-dimensional Galois extensions. The notion of trace-compatibility seems to be introduced by Scheerhorn [Sche], where additive representations of the algebraic closure of a finite field are studied.

Explicit descriptions of cyclotomic fields are important for various applications where computations with roots of unity are involved, e.g., for representation theory or the discrete Fourier transform (see [Bo], [Br] and the literature cited there). In [Bo] and [Br] there are determined special integral bases for cyclotomic fields, which in general are not normal bases. We also mention that Johnsen [Jo] has explicitly determined normal elements for all cyclotomic fields $\mathbb{Q}_n$ over $\mathbb{Q}$, but these are not universally normal in general.

([1]) Recall that for a Galois extension E/F with Galois group G the (E, F)-*trace* of $w \in E$ is $\sum_{g \in G} g(w)$.

2. Simultaneous generators for cyclic Galois extensions. In the present section we assume that E/F is a finite Galois extension with cyclic Galois group, but F is an arbitrary field, with characteristic p, say. We shall prove two theorems which are very useful for the cyclotomic extensions to be considered in Sections 3–5.

We start with some general remarks on cyclic Galois extensions; for details we refer to [Ha, Section 8]. For an intermediate field K of E/F let G_K be the Galois group of E/K. After fixing a generator α_F of G_F (as module over the ring of integers), we take $\alpha_K := \alpha_F^{[K:F]}$ as a generator for G_K (where $[K : F]$ is the degree of K/F). The entire KG_K-module structure of $(E, +)$ is described in terms of the polynomial ring $K[x]$ and α_K as follows: for $f \in K[x]$ and $v \in E$, we let $f \circ_K v := f(\alpha_K)(v)$. The (K, α_K)-*order* of $v \in E$ is the monic polynomial $g \in K[x]$ of least degree such that $g \circ_K v = 0$; it is denoted by $\mathrm{Ord}_{K,\alpha_K}(v)$. The monic K-divisors of $x^{[E:K]} - 1$ correspond bijectively to the KG_K-submodules of E: the divisor g corresponds to the kernel of $g(\alpha_K)$, which is denoted by $U_{K,g}$ throughout; we say that g is the *annihilator of* $U_{K,g}$ *with respect to* K *and* α_K, and call $U_{K,g}$ a (K, α_K)-*module*. Moreover, $U_{K,g}$ is cyclic, i.e., free on one generator as a (K, α_K)-module. Any $v \in E$ such that $KG_K v = U_{K,g}$ is called a (K, α_K)-*generator* of $U_{K,g}$; the latter is the case if and only if $\mathrm{Ord}_{K,\alpha_K}(v) = g$.

We have to consider the situation where a subgroup U of $(E, +)$ is equipped with more than one module structure. We summarize some basic facts and refer to [Ha, Section 11] for details. Let $\mathcal{C}$ be a nonempty set of intermediate fields of E/F. A subgroup U of $(E, +)$ is called a $\mathcal{C}$-*module* if U is a (K, α_K)-module for all $K \in \mathcal{C}$. If $v \in U$ is such that $KG_K v = U$ for all $K \in \mathcal{C}$, then v is called a $\mathcal{C}$-*generator* for U. It is proved in [Ha, Section 12] that such elements do always exist. Here, we are concerned with a construction of $\mathcal{C}$-generators in a situation which is applicable to certain cyclotomic field extensions. Now, if U is an $\{M, L\}$-module, then there are monic L- and M-divisors f_L of $x^{[E:L]} - 1$ and f_M of $x^{[E:M]} - 1$, respectively, such that $U = U_{L,f_L} = U_{M,f_M}$. If additionally M is a subfield of L, then f_M and f_L are related as follows: $f_L(x^{[L:M]}) = f_M$, and therefore, in particular, $f_L \in M[x]$.

Throughout, for an integer $n \geq 1$ which is not divisible by p, and for an algebraic extension K of F, let K_n denote the nth *cyclotomic field* over K, i.e., K_n is obtained by adjoining a primitive nth root of unity to K (we assume that everything takes place in a fixed algebraic closure of F). Also, let Φ_n denote the nth cyclotomic polynomial (over F).

THEOREM 2.1. *As above let* M, L *be intermediate fields of the cyclic Galois extension* E/F *with* $M \subseteq L$. *Let* f_L *be a monic* M*-divisor of* $x^{[E:L]} - 1$ *and let* $f_M = f_L(x^{[L:M]})$. *Consider the* $\{M, L\}$*-module* $U = U_{L,f_L} = U_{M,f_M}$.

Assume that $L \cap M_n = M$ for every divisor n of $[E:L]$ which is not divisible by p and for which Φ_n and f_L are not relatively prime. Then every (M, α_M)-generator of U is likewise an (L, α_L)-generator of U.

Proof. We consider the decomposition $f_L = \prod_n f_n^{\varrho(n)}$, where n runs over all divisors of $[E:L]$ which are not divisible by p and where $f_n := \gcd(\Phi_n, f_L) \neq 1$ ($\varrho(n) \geq 1$ for all n). Since $f_L \in M[x]$, each f_n is also a polynomial with coefficients in M, and, with $g_n := f_n(x^{[L:M]})$ we have $U_n := U_{M,g_n^{\varrho(n)}} = U_{L,f_n^{\varrho(n)}}$ and $\bigoplus_n U_n$ is a decomposition of U as an $\{M, L\}$-module (see [Ha, Section 12]). Every (M, α_M)-generator v of U can be uniquely written as $v = \sum_n v_n$, where for each n, v_n is an (M, α_M)-generator of U_n (see [Ha, Theorem 8.6]). Moreover, the (L, α_L)-order of each v_n divides $f_n^{\varrho(n)}$. Now, let $u = v_n$ be some component of v and let $\gamma = \mathrm{Ord}_{L,\alpha_L}(u)$. Since $L \cap M_n = M$ by assumption, we have $[L_n : L] = [M_n : M]$, which means that Φ_n splits over L as over M. Thus, $\gamma \in M[x]$, and hence $\gamma = f_n^{\varrho(n)}$ for otherwise $\gamma(x^{[L:M]})$ would be a proper divisor of $g_n^{\varrho(n)}$ annihilating u. Since this holds for all n, we conclude that v has (L, α_L)-order equal to f_L (see again [Ha, Theorem 8.6]), and everything is proved. ∎

Theorem 2.2. *Let $\mathcal{C}$ be a set of intermediate fields of the cyclic Galois extension E/F containing (with respect to set-theoretic inclusion) a unique maximal element L and a unique minimal element M. Let n be a divisor of $[E:L]$ which is not divisible by p and assume that g_L is an irreducible monic L-divisor of Φ_n. For each $K \in \mathcal{C}$ let g_K be the unique irreducible monic K-divisor of Φ_n such that g_L divides g_K (in $L[x]$) and let $f_K := g_K(x^{[L:K]})$. Then $U_{N,f_N} \subseteq U_{K,f_K}$ whenever $K \subseteq N$ and U_{M,f_M} is a $\mathcal{C}$-module.*

Now, assume moreover that L is contained in M_n. Then, for any nonzero v of U_{L,f_L}, the following two assertions hold:

(1) *For all $K \in \mathcal{C}$, $\mathrm{Ord}_{K,\alpha_K}(v) = f_K$.*

(2) *$w := \sum_{j=0}^{[L:M]-1} \alpha_M^j(v)$ is a $\mathcal{C}$-generator of U_{M,f_M}.*

Proof. It is clear that $U_{N,f_N} \subseteq U_{K,f_K}$ whenever $K \subseteq N$, as g_N divides g_K in this case. It is also clear that U_{M,f_M} is a $\mathcal{C}$-module, as $f_M = g_M(x^{[L:M]})$ by definition and as $[K:M]$ divides $[L:M]$ for every $K \in \mathcal{C}$. Now, let $K \in \mathcal{C}$. As $M \subseteq K$ and $L \subseteq M_n$ by assumption, we have $L \subseteq K_n$, and therefore $[L \cap K_n : K] = [L:K]$. Hence, g_K splits over L into $[L:K]$ irreducible monic polynomials, namely

$$g_K = \prod_{j=0}^{[L:K]-1} \alpha_K^j(g_L)$$

(the Galois automorphisms are naturally extended to polynomial rings). Next, let v be as in the assertion. Then $\mathrm{Ord}_{L,\alpha_L}(v) = g_L$ as g_L is irreducible

over L. An application of (1) of Theorem 14.5 in [Ha] to the fields L and K shows that $\mathrm{Ord}_{K,\alpha_K}(v) = g_K(x^{[L:K]})$, and this proves assertion (1). Finally, let w be as in (2). For $K \in \mathcal{C}$ we have $w = \sum_{i=0}^{[K:M]-1} \alpha_M^i(u)$, where $u = \sum_{j=0}^{[L:K]-1} \alpha_K^j(v)$. Now, an application of (2) of Theorem 14.5 in [Ha] to the fields L and K shows that $\mathrm{Ord}_{K,\alpha_K}(u) = f_K = g_K(x^{[L:K]})$, and therefore, the (K,α_K)-order of $\alpha_M^i(u)$ is equal to $\alpha_M^i(f_K)$. By assumption we further have $K \subseteq L \subseteq M_n$, whence $[K \cap M_n : M] = [K : M]$, and therefore, g_M splits over K as

$$g_M = \prod_{i=0}^{[K:M]-1} \alpha_M^i(g_K).$$

An application of Theorem 8.6 in [Ha] thus yields $\mathrm{Ord}_{K,\alpha_K}(w) = g_M(x^{[L:K]})$, which means that w is a (K,α_K)-generator of U_{M,f_M}, since as a (K,α_K)-module the latter is equal to $U_{K,g_M(x^{[L:K]})}$. This completes the proof of the theorem. ∎

3. Complete normal bases for cyclotomic r-extensions, r odd. If r is a prime and $m \geq 1$, then we call $\mathbb{Q}_{r^m}/\mathbb{Q}$ a *cyclotomic r-extension*. In the present section, we consider the case where r is odd. We give an efficient characterization of completely normal elements for such extensions and also provide explicit constructions of those elements.

For simplicity, let throughout $E := \mathbb{Q}_{r^m}$, where $m \geq 1$. Since $E/\mathbb{Q}$ is a cyclic extension of degree $r^{m-1}(r-1)$, we may use the approach of Section 2.

Assume first that $m = 1$. If L is an intermediate field of $E/\mathbb{Q}$, then $L \cap \mathbb{Q}_{r-1} \subseteq E \cap \mathbb{Q}_{r-1} = \mathbb{Q}$. We therefore may apply Theorem 2.1 with $M = \mathbb{Q}$ and $f_L = x^{[E:L]} - 1$ to deduce that each normal element of $E/\mathbb{Q}$ is normal in E/L. As L was chosen arbitrarily, any normal element of $E/\mathbb{Q}$ is already completely normal. We remark that the latter also follows from a more general result on abelian extensions from Blessenohl and Johnsen [BlJo2]. As it is well known (see the historical remark in [Jo]) that any primitive rth root of unity is normal in $E/\mathbb{Q}$, we note the following.

THEOREM 3.1. *Let μ be a primitive rth root of unity, where r is an odd prime. Then μ is completely normal in $\mathbb{Q}_r/\mathbb{Q}$.*

We now consider the case $m \geq 2$. Let $\mathcal{C}$ be the set of proper cyclotomic subfields of E, i.e., $\mathcal{C} = \{\mathbb{Q}, \mathbb{Q}_r, \ldots, \mathbb{Q}_{r^{m-1}}\}$. Furthermore, let $\widehat{\mathcal{C}}$ be the set of all subfields of $\mathbb{Q}_{r^{m-1}}$, and let T_{r^m} be the kernel of the $(E, \mathbb{Q}_{r^{m-1}})$-trace mapping. Then $\mathbb{Q}_{r^{m-1}} \oplus T_{r^m}$ is a decomposition of E as a $\widehat{\mathcal{C}}$-module. Moreover, with respect to a fixed generator α of the Galois group of $E/\mathbb{Q}$, $\mathbb{Q}_{r^{m-1}}$ is annihilated by $x^{r^{m-2}(r-1)} - 1$ and T_{r^m} is annihilated by $\Phi_r(x^{r^{m-2}(r-1)}) = \Phi_{r^{m-1}}(x^{r-1})$. (Observe that the product of the latter two polynomials is

equal to

$$x^{r^{m-1}(r-1)} - 1 = x^{[E:\mathbb{Q}]} - 1,$$

the annihilator polynomial of α over $\mathbb{Q}$.)

THEOREM 3.2. *Let $w = u + v$ be the decomposition of $w \in E$ corresponding to $\mathbb{Q}_{r^{m-1}} \oplus T_{r^m}$. Then w is completely normal in $E/\mathbb{Q}$ if and only if u and v are $\widehat{\mathcal{C}}$-generators for $\mathbb{Q}_{r^{m-1}}$ and T_{r^m}, respectively, where $\widehat{\mathcal{C}}$ as above is the set of subfields of $\mathbb{Q}_{r^{m-1}}$.*

Proof. It suffices to show that any sum $u+v$ of $\widehat{\mathcal{C}}$-generators u of $\mathbb{Q}_{r^{m-1}}$ and v of T_{r^m} is a completely normal element of $E/\mathbb{Q}$. Let therefore L be a subfield of E which is not contained in $\widehat{\mathcal{C}}$. Then $[L : \mathbb{Q}] = r^{m-1}t$, where $t \neq 1$ is a divisor of $r - 1$. We consider further the unique subfield M of L with $[M : \mathbb{Q}] = r^{m-2}t$. Then $M \in \widehat{\mathcal{C}}$, and therefore $w = u + v$ is normal in E/M (we have used [Ha, Theorem 8.6] for the latter argument). Now, $[E : L] = t$ divides $r - 1$, whence $L \cap M_t \subseteq E \cap M_t = M$. Hence, Theorem 2.1 is applicable to $f_L = x^{[E:L]} - 1$ and yields the normality of w in E/L. As the latter holds for all L, we conclude that w is completely normal in $E/\mathbb{Q}$. ∎

Observing that, by the definition of $\widehat{\mathcal{C}}$, $u \in \mathbb{Q}_{r^{m-1}}$ is completely normal over $\mathbb{Q}$ if and only if u is a $\widehat{\mathcal{C}}$-generator of $\mathbb{Q}_{r^{m-1}}$, using Theorem 3.1 and induction, it remains to determine a $\widehat{\mathcal{C}}$-generator for T_{r^m}, where $m \geq 2$. With α as above we provide the following construction.

THEOREM 3.3. *Let $m \geq 2$ and $\lambda := \lfloor m/2 \rfloor$ be the integer part of $m/2$. Then $\lambda \geq 1$ and $L := \mathbb{Q}_{r^\lambda}$ is an intermediate field of $E = \mathbb{Q}_{r^m}$ over $\mathbb{Q}_r$. Let g be an irreducible L-divisor of $\Phi_{r^{m-\lambda}}$, and assume that $y \in U_{L,g}$ is any nonzero element. Then, with $\widehat{\mathcal{C}}$ as in Theorem 3.2, $v := \sum_{j=0}^{r^{\lambda-1}(r-1)-1} \alpha^j(y)$ is a $\widehat{\mathcal{C}}$-generator of T_{r^m}.*

Proof. Let $\mathcal{K}$ be the set of all intermediate fields of $L/\mathbb{Q}$. We have $[E : L] = r^{m-\lambda}$, and $L \subseteq \mathbb{Q}_{r^{m-\lambda}}$ by definition of λ. We are therefore able to apply Theorem 2.2 (with M replaced by $\mathbb{Q}$). Since g is irreducible, any nonzero $y \in U_{L,g}$ is an $(L, \alpha^{[L:\mathbb{Q}]})$-generator of $U_{L,g}$. Furthermore, as $\Phi_{r^{m-\lambda}}$ is irreducible over $\mathbb{Q}$, Theorem 2.2 yields that v is a $\mathcal{K}$-generator of $U_{\mathbb{Q},f}$, where

$$f = \Phi_{r^{m-\lambda}}(x^{r^{\lambda-1}(r-1)}) = \Phi_{r^{m-1}}(x^{r-1}).$$

Thus, $U_{\mathbb{Q},f} = T_{r^m}$, and it remains to show that v generates T_{r^m} with respect to all fields $N \in \widehat{\mathcal{C}} \setminus \mathcal{K}$. Let N be such a field. Then $[N : \mathbb{Q}]$ is of the form $r^l t$, where $m - 2 \geq l \geq \lambda - 1$ and where $t \geq 1$, but $r^l t \neq r^{\lambda-1}$. Thus, $K := N \cap \mathbb{Q}_{r^\lambda}$ has degree $r^{\lambda-1}t$ over $\mathbb{Q}$. We seek to apply Theorem 2.1 with L replaced by N and M replaced by K: $[E : N] = r^{m-1-l}(r-1)/t$ and T_{r^m}

as an $(N, \alpha^{[N:\mathbb{Q}]})$-module is annihilated by $\Phi_{r^{m-1-l}}(x^{(r-1)/t})$, which is equal to $\prod_{d|(r-1)/t} \Phi_{dr^{m-1-l}}$; for all d we have $N \cap K_{dr^{m-1-l}} = N \cap K_{r^{m-1-l}} = K$, because $K_{r^{m-1-l}} = K\mathbb{Q}_{r^{m-1-l}} = \mathbb{Q}_{r^\lambda}$ as $m - 1 - l \geq 1$. Thus, Theorem 2.1 yields that each $(K, \alpha^{[K:\mathbb{Q}]})$-generator of T_{r^m} is an $(N, \alpha^{[N:\mathbb{Q}]})$-generator of T_{r^m}. Since N was chosen arbitrarily, we conclude that every $\mathcal{K}$-generator of T_{r^m} is a $\widehat{\mathcal{C}}$-generator of T_{r^m}, and everything is proved. ∎

In Section 4 (see the proof of Theorem 4.1), we will see that any irreducible L-divisor of $\Phi_{r^{m-\lambda}}$ is a binomial, i.e., of the form $x^b - \zeta$ (with explicit values for b and ζ), whence a nonzero y as in the assertion of Theorem 3.3 is just an eigenvector of α^b over L. We shall also see that any r^mth root of unity can be chosen as y. Using Theorems 3.1 and 3.2 and induction, we therefore altogether have the following result whose proof is covered by Section 4.

THEOREM 3.4. *Assume that $m \geq 2$ and that r is an odd prime. Let η be any primitive r^mth root of unity and assume that α is any generator of the Galois group of $\mathbb{Q}_{r^m}/\mathbb{Q}$. Then, with $\widehat{\mathcal{C}}$ and T_{r^m} as before,*

$$\sum_{j=0}^{r^{\lfloor m/2 \rfloor - 1}(r-1)-1} \alpha^j(\eta)$$

is a $\widehat{\mathcal{C}}$-generator of T_{r^m}. Moreover,

$$\eta^{r^{m-1}} + \sum_{k=2}^{m} \sum_{j=0}^{r^{\lfloor k/2 \rfloor - 1}(r-1)-1} \alpha^{jr^{m-k}}(\eta^{r^{m-k}})$$

is completely normal in $\mathbb{Q}_{r^m}/\mathbb{Q}$.

4. Normal bases for regular cyclotomic extensions. For an integer n let $\nu(n)$ denote the square-free part of n. If $e, n \in \mathcal{N}$ with e being a multiple of n, we call $\mathbb{Q}_e/\mathbb{Q}_n$ a *regular cyclotomic extension* if $\nu(e) = \nu(n)$. In the present section, among other things, we shall explicitly provide normal bases for these kind of extensions. The results apply to the extension $\mathbb{Q}_{r^m}/\mathbb{Q}_{r^\lambda}$ which occurred in Theorem 3.3 ($m \geq 2$), as $\lambda \geq 1$.

First, it is not difficult to show that a regular cyclotomic extension is cyclic of degree e/n, whence, again, the approach of Section 2 is applicable. Throughout, let σ be any generator of the Galois group of $\mathbb{Q}_e/\mathbb{Q}_n$.

THEOREM 4.1. *Consider a regular cyclotomic extension $\mathbb{Q}_e/\mathbb{Q}_n$. For any divisor k of e/n let ζ_k be a primitive (nk)th root of unity, and let I_k be the set of $j \in \{1, \ldots, \gcd(k, n)\}$ which are relatively prime to $\gcd(k, n)$. Then the following two assertions hold*:

(1) *The $(\mathbb{Q}_n, \sigma)$-order of $\sum_{j \in I_k} \zeta_k^j$ is equal to Φ_k.*

(2) *$w := \sum_{k|e/n} \sum_{j \in I_k} \zeta_k^j$ is normal in $\mathbb{Q}_e/\mathbb{Q}_n$.*

P r o o f. We fix a divisor k of e/n and let $a := \gcd(k,n)$. The kth cyclotomic polynomial Φ_k splits over $\mathbb{Q}_n$ as

$$\Phi_k = \prod_{j \in I_k} (x^{k/a} - \lambda^j),$$

where $\lambda \in \mathbb{Q}_n$ is a primitive ath root of unity. For $j \in I_k$ let $g_j := x^{k/a} - \lambda^j$. Let η be any primitive (nk)th root of unity. The restriction of σ to $\mathbb{Q}_{nk}$ (likewise denoted by σ) satisfies $\sigma(\eta) = \eta^{1+sn}$, where $s \in \{1, \dots, k\}$ is some integer which is relatively prime to k. Now,

$$(1+sn)^{k/a} - 1 = \frac{nk}{a} \cdot S,$$

where S and k are relatively prime, whence

$$g_j(\sigma)(\eta) = \eta(\eta^{\frac{nk}{a} \cdot S} - \lambda^j).$$

As $\eta^{\frac{nk}{a} \cdot S}$ is a primitive ath root of unity and as g_j is irreducible over $\mathbb{Q}_n$, a suitable choice of $j \in I_k$ shows that the $(\mathbb{Q}_n, \sigma)$-order of η is equal to g_j. (Observe that, as remarked in Section 3, the latter justifies the choice of η (in Theorem 3.4) as y (from Theorem 3.3) with k replaced by $r^{m-\lambda}$ yields that η is a $\widehat{\mathcal{C}}$-generator of T_{r^m}.)

Furthermore, for $i \in I_k$ the $(\mathbb{Q}_n, \sigma)$-orders of the elements η^i run through all irreducible $\mathbb{Q}_n$-divisors g_j of Φ_k, whence v_k as in the statement has $(\mathbb{Q}_n, \sigma)$-order Φ_k (by [Ha, Theorem 8.6]). This proves (1), and (2) holds as (again by [Ha, Theorem 8.6]) the $(\mathbb{Q}_n, \sigma)$-order of w is equal to the product of the $(\mathbb{Q}_n, \sigma)$-orders of the v_k which is equal to $\prod_{k|e/n} \Phi_k = x^{e/n} - 1$, whence w is normal in $\mathbb{Q}_e/\mathbb{Q}_n$. ∎

Observe that the conclusion of Theorem 4.1 also holds when, for every k, η_k is any eigenvector of $\sigma^{k/\gcd(k,n)}$ (over $\mathbb{Q}_n$).

Remark 4.2. Since we have determined generators of modules which are annihilated by cyclotomic polynomials, our approach naturally leads to sequences of normal elements for *towers of regular cyclotomic extensions* over a field $\mathbb{Q}_n$: let $k, l \geq 1$, $n \in \mathcal{N}$ and assume that $\nu(kl)$ divides $\nu(n)$. If u is normal in $\mathbb{Q}_{nk}/\mathbb{Q}_n$, and if σ is a generator of the Galois group of $\mathbb{Q}_{nkl}$ over $\mathbb{Q}_n$, then for every divisor d of kl which is not a divisor of k, we let v_d be an element (in $\mathbb{Q}_{nkl}$) having $(\mathbb{Q}_n, \sigma)$-order Φ_d. Then $u + \sum_d v_d$ is normal in $\mathbb{Q}_{nkl}/\mathbb{Q}_n$.

Observe also that the $(\mathbb{Q}_{nkl}, \mathbb{Q}_{nk})$-trace-mapping τ is equal to $(\sigma^{kl} - 1)/(\sigma^k - 1)$, whence $\tau(v_d) = 0$ for every d dividing kl but not k. Consequently, $w := l^{-1}(u + \sum_d v_d)$ is normal in $\mathbb{Q}_{nkl}/\mathbb{Q}_n$ and $\tau(w) = u$, and this indicates how to obtain trace-compatible sequences of normal elements for towers of regular cyclotomic extensions.

Even more generally, we may consider the set $\mathcal{R}_n$ of all e such that $\mathbb{Q}_e$ is regular cyclotomic over $\mathbb{Q}_n$. Since $\mathcal{R}_n$ is closed under taking greatest common divisors, $\mathbb{Q}_{n^\infty} := \bigcup_{e\in\mathcal{R}_n} \mathbb{Q}_e$ is an algebraic extension over $\mathbb{Q}_n$, which we call the *regular cyclotomic closure* of $\mathbb{Q}_n$, and which for $n > 1$ is infinite by the definition of $\mathcal{N}$. Now, define $u_n := 1$ and let u_{n^2} be normal in $\mathbb{Q}_{n^2}$ over $\mathbb{Q}_n$ with $\mathrm{Tr}_{n^2,n}(u_{n^2}) = u_n$, where $\mathrm{Tr}_{n^2,n}$ denotes the $(\mathbb{Q}_{n^2}, \mathbb{Q}_n)$-trace mapping. Inductively, for every $t \geq 2$, let $u_{n^{t+1}}$ be normal in $\mathbb{Q}_{n^{t+1}}$ over $\mathbb{Q}_n$ such that $\mathrm{Tr}_{n^{t+1},n^t}(u_{n^{t+1}}) = u_{n^t}$. Finally, for any $e \in \mathcal{R}_n$, take a t such that e divides n^t, and define $u_e := \mathrm{Tr}_{n^t,e}(u_{n^t})$. The transitivity of the trace mappings and the well known fact that the trace of a normal element again is normal imply that the sequence $(u_m)_{m\in\mathcal{R}_n}$ is trace-compatible for $\mathcal{R}_n$ and entirely consists of normal elements over $\mathbb{Q}_n$, and thus provides a normal basis for $\mathbb{Q}_{n^\infty}$ over $\mathbb{Q}_n$.

5. Universal normal bases for cyclotomic 2-extensions. In the present section we explicitly determine universal normal bases for cyclotomic 2-extensions. For simplicity, let $E := \mathbb{Q}_{2^m}$, where $m \geq 2$. We denote by $\widetilde{E} := \bigcup_{m\geq 2} \mathbb{Q}_{2^m}$ the 2-*primary closure* of $\mathbb{Q}$ in $\widehat{\mathbb{Q}}$, i.e., $\widetilde{E}$ is obtained by adjoining the set $R := \{\eta \in \widehat{\mathbb{Q}} \mid \eta^{2^i} = 1 \text{ for some } i\}$ to $\mathbb{Q}$. Let s be any odd integer. For $\eta \in R$ define

$$\sigma(\eta) := \eta^{1+4s} \quad \text{and} \quad \iota(\eta) = \eta^{-1}.$$

The restrictions of σ and ι to E (likewise denoted by σ and ι) generate the Galois group of $E/\mathbb{Q}$, throughout denoted by G (in that context the group orders of σ and ι are 2^{m-2} and 2, respectively). Using this description, it is easy to show that for $m \in \{2, 3\}$, each normal element of $E/\mathbb{Q}$ is completely normal in $E/\mathbb{Q}$. Moreover, with Linear Algebra, normal elements are easily obtained in these cases, and one can show that the following holds.

THEOREM 5.1. *Let λ be a primitive 8th root of unity. Then $-1 + \lambda^2$ is completely normal in $\mathbb{Q}_4/\mathbb{Q}$, and $-1+\lambda+\lambda^2$ is completely normal in $\mathbb{Q}_8/\mathbb{Q}$.*

From now on, we may restrict our attention to the case $m \geq 4$. Let $\mathcal{C}^- = \{\mathbb{Q}_4, \ldots, \mathbb{Q}_{2^{m-1}}\}$. Similarly to Section 3, if T_{2^m} denotes the kernel of the $(E, \mathbb{Q}_{2^{m-1}})$-trace mapping, then $\mathbb{Q}_{2^{m-1}} \oplus T_{2^m}$ is a decomposition of E into $\mathcal{C}^-$-modules, respecting additionally the action of $\mathbb{Q}G$. Moreover, just by definition, $w = u + v$ is universally normal in $E/\mathbb{Q}$ if and only if its components u and v with respect to the decomposition $\mathbb{Q}_{2^{m-1}} \oplus T_{2^m}$ of E are $\mathcal{C}^-$-generators as well as $\mathbb{Q}G$-generators of $\mathbb{Q}_{2^{m-1}}$ and T_{2^m}, respectively. Observing that the $\mathcal{C}^-$-generators of $\mathbb{Q}_{2^{m-1}}$ which are additionally $\mathbb{Q}G$-generators are exactly the universally normal elements of $\mathbb{Q}_{2^{m-1}}/\mathbb{Q}$, by Theorem 5.1 and induction it remains to determine $\mathcal{C}^-$-generators for T_{2^m} which are additionally $\mathbb{Q}G$-generators of T_{2^m}.

Since we want to make use of the results from Section 4, we first consider the extension $E/\mathbb{Q}_4$, which is regular cyclotomic (and cyclic of degree 2^{m-2} with Galois group generated by σ, restricted to E). If $\kappa := \lfloor (m-4)/2 \rfloor$, then $K = \mathbb{Q}_{2^{2+\kappa}}$ is a member of $\mathcal{C}^-$. We have $[E : K] = 2^{m-2-\kappa}$ and $\Phi_{2^{m-2-\kappa}}$ splits over $\mathbb{Q}_4$ as follows (where i denotes a primitive 4th root of unity):

$$(x^{2^{n-4-\kappa}} - i) \cdot (x^{2^{n-4-\kappa}} + i). \tag{5.1}$$

Let f be the first of these factors and $V_f = U_{K,f}$ the (K, σ_K)-submodule of T_{2^m} corresponding to f, where $\sigma_K = \sigma^{2^\kappa}$. As shown in the first part of the proof of Theorem 4.1, the (K, σ_K)-order of a primitive 2^mth root of unity η is an irreducible K-divisor of $\Phi_{2^{m-2-\kappa}}$, without loss of generality a divisor of f. Now, by the choice of κ, we may apply Theorem 2.2 with L replaced by K and M replaced by $\mathbb{Q}_4$ to deduce that

$$v := \sum_{j=0}^{2^\kappa - 1} \sigma^j(\eta)$$

is a $\mathcal{K}$-generator of V_f, where $\mathcal{K}$ is the set of intermediate fields of $K/\mathbb{Q}_4$.

What has been said for v and f likewise holds for $\iota(v)$ and the codivisor $g = x^{2^{m-\kappa-4}} + i$ of f in $\Phi_{2^{m-\kappa-2}}$ over $\mathbb{Q}_4$, i.e., $\iota(v)$ is a $\mathcal{K}$-generator of $V_g = U_{K,g}$. Summarizing, by (5.1) and the fact that T_{2^m} as a (K, σ_K)-module is annihilated by $\Phi_{2^{m-2-\kappa}}$, this yields that

$$u := v + \iota(v) \text{ is a } \mathcal{K}\text{-generator of } T_{2^m}.$$

Next, for each intermediate field L of E/K, we may apply Theorem 2.1 with $f_L = \Phi_{[E:L]}$ and M replaced by K to conclude that

$$u \text{ is even a } \mathcal{C}^-\text{-generator of } T_{2^m}.$$

Unfortunately, u is not a generator of T_{2^m} as a module over $\mathbb{Q}G$, because u is fixed under ι, whence $\mathbb{Q}(u)$ only is the largest real subfield of E (which has degree 2^{m-2} over $\mathbb{Q}$ and is different from $\mathbb{Q}_{2^{m-1}}$). We therefore seek to modify u to obtain a $\mathbb{Q}G$-generator of T_{2^m}. Let $y := (1 + i)u$. Since $1 + i \in \mathbb{Q}_4$ is nonzero, y is a $\mathcal{C}^-$-generator of T_{2^m}. In particular, the $(\mathbb{Q}_4, \sigma)$-order of y is equal to $\Phi_{2^{m-2}}$. Now, the $(\mathbb{Q}, \sigma)$-order of y, which we define to be the minimal polynomial of y with respect to σ over $\mathbb{Q}$, likewise is equal to $\Phi_{2^{m-2}}$, whence the $(\mathbb{Q}, \sigma)$-submodule A of T_{2^m} (i.e., the σ-invariant $\mathbb{Q}$-subspace of T_{2^m}) generated by y has $\mathbb{Q}$-dimension $2^{m-3} = \deg(\Phi_{2^{m-2}})$. Let B be the $(\mathbb{Q}, \sigma)$-module generated by $\iota(y) = (1-i)\iota(u) = (1-i)u$. Again, this space has $\mathbb{Q}$-dimension 2^{m-3} and with respect to σ is annihilated by $\Phi_{2^{m-2}}$. Now, it is not difficult to show that $A \cap B = \{0\}$, and therefore $A \oplus B = T_{2^m}$. Moreover, since $B = \iota(A)$, we see that T_{2^m} in fact is the $\mathbb{Q}G$-module generated by y. Summarizing, this yields that

$$y \text{ is a } \mathcal{C}^-\text{-generator and a } \mathbb{Q}G\text{-generator of } T_{2^m}.$$

Using Theorem 5.1 and induction, we have proved the following theorem.

THEOREM 5.2. *Let $m \geq 4$ be an integer and let σ be a generator of the Galois group of $\mathbb{Q}_{2^m}$ over $\mathbb{Q}_4$. Let i be a primitive 4th root of unity and η a primitive 2^mth root of unity. Then, with $\mathcal{C}^-$, G and T_{2^m} as above,*

$$(1+i)\sum_{j=0}^{2^{\lfloor (m-4)/2 \rfloor}-1} \sigma^j(\eta+\eta^{-1})$$

is a $\mathcal{C}^-$-generator and a $\mathbb{Q}G$-generator of T_{2^m}. Moreover,

$$-1+\eta^{2^{m-2}}+\eta^{2^{m-3}}+(1+i)\Big(\sum_{k=4}^{m}\sum_{j=0}^{2^{\lfloor (k-4)/2 \rfloor}-1}\sigma^j(\eta^{2^{m-k}}+\eta^{-2^{m-k}})\Big)$$

is universally normal in $\mathbb{Q}_{2^m}/\mathbb{Q}$.

6. The product construction and trace-compatibility. In this final section, we show how to obtain universally normal elements for arbitrary cyclotomic fields as well as trace-compatible sequences of universally normal elements for the abelian closure $\widehat{\mathbb{Q}}$ over $\mathbb{Q}$. The first task is solved by the following theorem in combination with Theorems 3.4 and 5.2.

THEOREM 6.1. *Let $n \in \mathcal{N}$ and $\prod_j r_j^{a_j}$ be the prime factorization of n. Assume that for each j, w_j is universally normal in $\mathbb{Q}_{r_j^{a_j}}/\mathbb{Q}$. Then $w := \prod_j w_j$ is universally normal in $\mathbb{Q}_n/\mathbb{Q}$.*

Proof. The argument is similar to the proof of the Reduction Theorem in [Ha, Section 4] (see also [BlJo1, Hilfssatz 4.4]). Let $m, n \in \mathcal{N}$ be relatively prime and let $l \in \mathcal{N}$ be a divisor of mn. If u is universally normal in $\mathbb{Q}_m/\mathbb{Q}$, then u is normal in $\mathbb{Q}_m$ over $\mathbb{Q}_m \cap \mathbb{Q}_l = \mathbb{Q}_{\gcd(m,l)}$. Since $\mathbb{Q}_m$ and $\mathbb{Q}_l$ are linearly disjoint over $\mathbb{Q}_{\gcd(m,l)}$, u also provides a normal element for $\mathbb{Q}_m\mathbb{Q}_l = \mathbb{Q}_{\mathrm{lcm}(l,m)}$ over $\mathbb{Q}_l$. Analogously, if v is universally normal in $\mathbb{Q}_n/\mathbb{Q}$, then v provides a normal element for $\mathbb{Q}_n\mathbb{Q}_l = \mathbb{Q}_{\mathrm{lcm}(l,n)}$ over $\mathbb{Q}_l$. Finally, since $\mathbb{Q}_m\mathbb{Q}_l$ and $\mathbb{Q}_n\mathbb{Q}_l$ are linearly disjoint over $\mathbb{Q}_l$, uv is normal in $\mathbb{Q}_{mn}/\mathbb{Q}_l$. As the latter holds for all L, everything is proved. ∎

The determination of trace-compatible sequences of universally normal elements for $\widehat{\mathbb{Q}}$ over $\mathbb{Q}$ is similar to the corresponding task for completely normal elements in an algebraic closure of a finite field (see [Ha, Section 25]). It relies on the idea of Scheerhorn [Sche] that a product construction as in Theorem 6.1 can be used to achieve trace-compatibility.

CONSTRUCTION 6.2. *Start with a nonzero $w_1 \in \mathbb{Q}$. If $m = r$ is an odd prime, let η be a primitive rth root of unity (see Theorem 3.1) and $w_r := -w_1\eta$. If $m = 4$, let $w_4 := (-w_1/2)(-1+i)$, where i is a primitive 4th root of unity. If $m = 8$, let $w_8 := (-w_1/2)(-1+i+\lambda)$, where λ is a primitive 8th root of unity (see Theorem 5.1).*

Assume that $n \in \mathcal{N}$ and that for $k < n$, the element w_k already constructed is universally normal in $\mathbb{Q}_k/\mathbb{Q}$ and that the constructed sequence $(w_k)_{k\in\mathcal{N},\, k\le n-1}$ is trace-compatible. If $n = r^m$, where r is a prime, $m \ge 2$ if r is odd and $m \ge 4$ if $r = 2$, use Theorems 3.4 *and* 5.2 *to obtain a $v \in T_{r^m}$ which generates that space with respect to all cyclotomic subfields of $\mathbb{Q}_{r^{m-1}}$. Define $w_{r^m} := (1/r)w_{r^{m-1}} + v$. If n is not a prime power, consider the prime factorization $\prod_{j=1}^{k} r_j^{a_j}$ of n and define $w_n := \prod_{j=1}^{k} w_{r_j^{a_j}}$ (see Theorem* 6.1*). In any case, w_n is universally normal in $\mathbb{Q}_n/\mathbb{Q}$. Moreover, $(w_k)_{k\in\mathcal{N},\, k\le n}$ is trace-compatible.*

P r o o f. To justify the assertions in Construction 6.2, it remains to prove the trace-compatibility of the sequences. This is easily checked for the initialization. For the other case one has to show that $\mathrm{Tr}_{n,n/r}(w_n) = w_{n/r}$ for all prime divisors r of n (the latter denotes the $(\mathbb{Q}_n, \mathbb{Q}_{n/r})$-trace mapping). Let therefore r be some prime divisor of n, say $r = r_1$. Since $v := \prod_{j=2}^{k} w_{r_j^{a_j}}$ is an element of $\mathbb{Q}_{n/r}$, one has

$$\mathrm{Tr}_{n,n/r}(w_n) = v \cdot \mathrm{Tr}_{n,n/r}(w_{r_1^{a_1}}). \tag{6.1}$$

As the restriction of the Galois group of $\mathbb{Q}_n/\mathbb{Q}_{n/r}$ to $\mathbb{Q}_{r_1^{a_1}}$ is equal to the Galois group of $\mathbb{Q}_{r_1^{a_1}}/\mathbb{Q}_{r_1^{a_1-1}}$, one has further

$$\mathrm{Tr}_{n,n/r}(w_{r_1^{a_1}}) = \mathrm{Tr}_{r_1^{a_1}, r_1^{a_1-1}}(w_{r_1^{a_1}}) = w_{r_1^{a_1-1}}.$$

Since we have used Theorem 6.1 throughout Construction 6.2, the term in (6.1) in fact is equal to $w_{m/r}$, and we are done. ∎

References

[BlJo1] D. Blessenohl und K. Johnsen, *Eine Verschärfung des Satzes von der Normalbasis*, J. Algebra 103 (1986), 141–159.

[BlJo2] —, —, *Stabile Teilkörper galoisscher Erweiterungen und ein Problem von C. Faith*, Arch. Math. (Basel) 56 (1991), 245–253.

[Bo] W. Bosma, *Canonical bases for cyclotomic fields*, Appl. Algebra Engrg. Comm. Comput. 1 (1990), 125–134.

[Br] T. Breuer, *Integral bases for subfields of cyclotomic fields*, ibid. 8 (1997), 279–289.

[Fa] C. C. Faith, *Extensions of normal bases and completely basic fields*, Trans. Amer. Math. Soc. 85 (1957), 406–427.

[Ha] D. Hachenberger, *Finite Fields: Normal Bases and Completely Free Elements*, Kluwer, Boston, 1997.

[Jo] K. Johnsen, *Lineare Abhängigkeiten von Einheitswurzeln*, Elem. Math. 40 (1985), 57–59.

[Le] H. W. Lenstra, Jr., *A normal basis theorem for infinite Galois extensions*, Indag. Math. 47 (1985), 221–228.

[Ri] P. Ribenboim, *Algebraic Numbers*, Pure Appl. Math. 27, Wiley, New York, 1972.

[Sche] A. Scheerhorn, *Trace- and norm-compatible extensions of finite fields*, Appl. Algebra Engrg. Comm. Comput. 3 (1992), 435–447.

[Wa] L. C. Washington, *Introduction to Cyclotomic Fields*, Grad. Texts in Math. 83, Springer, Berlin, 1982.

Institut für Mathematik
Universität Augsburg
86159 Augsburg, Germany
E-mail: hachenberger@math.uni-augsburg.de

Received on 29.4.1999 (3591)