An Algorithm to Calculate a Basis Representation for Cyclotomic Units and Cyclotomic Numbers

Marc Conrad

March 21, 2016

Abstract

This paper presents an explicit algorithm to calculate a basis for the group of cyclotomic units and the basis representation for a given group of cyclotomic units. In addition, for a given product of cyclotomic units it calculates the unique basis representation of this product. For more information on relations between cyclotomic units see http://perisic.com/cyclotomic.

1 Introduction and Definition

For $n \in \mathbb{N}$, let ϵ_n be a primitive nth unit root (e.g. $\epsilon_n := e^{2\pi i/n}$). We denote with $G_n \cong (\mathbb{Z}/n\mathbb{Z})^* \cong \{a = 1, \ldots, n-1; (n,a) = 1\}$ the Galois group of the cyclotomic field extension $\mathbb{Q}(\epsilon_n)/\mathbb{Q}$. Further we define a cyclotomic number as the expression $1 - \epsilon_n^a$ with $n \in \mathbb{N}$ and $a \in G_n$. We focus on multiplicative relations between cyclotomic numbers modulo unit roots. There are two obvious relations between cyclotomic numbers. Symmetry relations because of the obvious relationship $1 - \epsilon_n^a = 1 - \epsilon_n^{-a}$ modulo unit roots (because of $1 - \epsilon_n^a = -\epsilon_n^a(1 - \epsilon_n^{-a})$) and relations implied by relative norms in the algebraic extensions $\mathbb{Q}(\epsilon_n)/\mathbb{Q}(\epsilon_d)$ for $d|n$. A third relation has been discovered by Ennola (see below) and it can be shown that the square of an Ennola relation is indeed a combination of norm and symmetry relations. For details see http://perisic.com/cyclotomic where an introduction is given into the theoretical underpinnings of the algorithms plus relevant publications and references.

The following collection of algorithms calculates a basis representation of products of cyclotomic numbers (Algorithms 1.1 to 1.4) and cyclotomic units (Algorithms 2.1 to 2.3). Starting with cyclotomic numbers we work with the following two definitions:

- Cyclotomic numbers $u_{n,a} := 1 - \epsilon_n^a$.
- Finite products of cyclotomic numbers: $P = \prod u_{n,a}^{e_{n,a}}$ with $n \in \mathbb{N}$, $a \in G_n$ and $\nu \in \mathbb{Z}$. We will also write somewhat shorter $P = \prod u_\nu^{e_\nu}$ where ν denotes the pair (n, a).

Following the usual definition of a basis (as e.g. in the context of vector spaces) we say that a collection of cyclotomic numbers $\mathcal{B}$ is a basis of the group

of cyclotomic numbers if every cyclotomic number can be expressed as a product of elements of $\mathcal{B}$ and that the elements of $\mathcal{B}$ are independent from each other, i.e. $\prod_{\mathcal{B}} u_\nu^{e_\nu} = 1$(modulo unit roots) $\Rightarrow e_\nu = 0 \ \forall \nu$.

For the remainder of this paper we assume that all equations of cyclotomic numbers and units are modulo unit roots without explicitly stating this.

Algorithm 1.1

This algorithm calculates a basis representation of a product of cyclotomic numbers $\prod u_\nu^{e_\nu}$.

1. (Initialization) Set $P := \prod u_\nu^{e_\nu}$
2. If all the u_ν are already within the basis (i.e. Algorithm 1.2 returns 'B' for this u_ν) then P is the basis representation. Return P and stop the algorithm.
3. Choose μ with $e_\mu \neq 0$ such that u_μ is not a basis element.
4. Use Algorithms 1.3 and 1.4 via Algorithm 1.2 to write $u_\mu = \prod u_\nu^{f_\nu}$.
5. Set $P := u_\mu^{-e_\mu} \prod u_\nu^{e_\nu + e_\mu f_\nu}$
6. Go to Step 2.

Note that the representation of u_μ in Step 4 may or may not be a basis representation. It is straightforward to see that if this algorithm terminates in Step 2 then the result will be a basis representation.

The correctness of the Algorithm 1.1 (i.e. that the algorithm terminates) can be proven as follows: define a complete order '<' on the u_ν and establish that any development in Algorithms A.1.3 and A.1.4 writes the cyclotomic unit as a product of cyclotomic units that are 'smaller' in this order. An explicit construction of such an order is given in Satz A.1.5 in the PhD thesis available at http://perisic.com/cyclotomic.

Algorithm 1.2

Let $u_\nu = u_{n,a}$ for $n \in \mathbb{N}$ and $a \in G_n$ be a cyclotomic number. This algorithm returns one of the methods B, S, Z-p, E or H that will then be used in Algorithms 1.3 (for methods S, Z-p and H) and 1.4 (for method E) to develop u_ν into a product.

1. (Initialization) Let $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ the unique factorization of n into prime powers and $q_i := p_i^{\alpha_i}$.
2. (Decision) Check the cases I-VI in the order below:

   I Is $n = 2$? Return H (see discussion below).

   II Is $n = 4$? If $a = 1$ return B; otherwise there is $a = 3$ and return S.

   III Is $n = p_1$ a prime number? If $a < p_1/2$ return B; otherwise return S.

   IV Is $n \equiv 2 \bmod 4$? Return Z-2.

V Is n squarefree or $n = 4u$ with u odd and squarefree? For $i = 1, \ldots, r$ let $a_i := a \bmod q_i$. (Note that with that definition either $q_i = p_i$ is a prime or $q_i = 4$).

V,i If $a_i = 1$ for all $i = 1, \ldots, r$ return E if r is odd and return B if r is even.

V,ii Let l be minimal with $a_l \neq 1$. If $a_l < q_l/2$ return S.

V,iii If $a_i \neq q_i - 1$ for all $i = 1, \ldots, r$ return B

V,iv Let k be minimal such that $a_k = q_k - 1$. Return Z-p_k.

VI All other n. For $i = 1, \ldots, r$ let $a_i := a \bmod p_i$ if $\alpha_i = 1$. For $\alpha_i > 1$ let $\lambda_i := a \bmod p_i^{\alpha_i - 1}$ and $a_i := ((a \bmod q_i) - \lambda_i)/p_i^{\alpha_i - 1}$.

VI,i Let l minimal with $q_l \neq 4$ and $\alpha_l > 1$. If $\lambda_l > p_l^{\alpha_l - 1}/2$ return S.

VI,ii If $a_i \neq p_i - 1$ for all $i = 1, \ldots, r$, return B.

VI,iii Let k minimal such that $a_k = p_k - 1$. Return Z-p_k.

The next two algorithms show how a cyclotomic number is developed into a product following the methods returned from Algorithm 1.2.

Algorithm 1.3

For a a cyclotomic number $u_\nu = u_{n,a}$ the developments according to methods S, Z-p and H are as follows:

S Return $u_{n,n-a}$

Z-p Let $d := n/p$ and $b := a \bmod d$. Further let:

$$s_p := \prod_{\substack{i=0,\ldots,p-1 \\ (c_i,n)=1}} u_{n,c_i} \text{ where } c_i := b + id.$$

$\mathtt{n}(s_p) := u_{d,b}^{-1}$ for $p|d$ and $\mathtt{n}(s_p) := u_{d,b}^{-1} u_{d,bc}$ if p does not divide d and with $c := p^{-1} \bmod d$.

Return $u_\nu s_p^{-1} \mathtt{n}(s_p)^{-1}$.

H Return $u_{4,1}u_{4,3}$. Note that this is the only case where a cyclotomic $u_{d,a}$ is developed into a product of cyclotomic numbers $u_{n,\cdot}$ with $n > d$. This inconsistency disappears for cyclotomic *units* as $u_{2,1} = 2$ is not a unit.

The next Algorithm calculates the so called Ennola relation (method E). Note that for Algorithm 1.1 we only need this development for $u_{n,1}$. However we can do this development more generically for $u_{n,a}$. Note that r is odd and that the construction will not work for r even.

Algorithm 1.4

1. (Initialization) Let $n = p_i^{\alpha_i} \cdots p_r^{\alpha_r}$ the unique factorization of n into prime powers and $q_i := p_i^{\alpha_i}$.

2. (The S^q operator) Define the operator S^q with $q = q_i$ via $S^q(u_{n,b}) = u_{n,c}$ such that $c \equiv -b \bmod q$ and $c \equiv b \bmod n/q$.

3. (Calculate $v^{(i)}$) Define $u^{(1)} := u_k$ and for $i = 1, \ldots, r$ let $u^{(i+1)} := S^{q_i} u^{(i)}$.

4. (Calculate Q_i) For each cyclotomic number $u^{(i)}$ with $i = 1, \ldots, r$ calculate $Q_i := s_{p_i}\mathfrak{n}(s_{p_i})$ where s_{p_i} and $\mathfrak{n}(s_{p_i})$ are as in part Z-p of Algorithm A.1.3.

5. (Calculate P) Let $P := u^{(1)}u^{(r+1)}\prod_{i=1}^{r} Q_i^{(-1)^i}$.

6. (Calculate base representation) With Algorithm 1.1 calculate the basis representation $\prod u_\nu^{e_\nu}$ of P. Return $\prod u_\nu^{e_\nu/2}$ Note that all e_ν are even; however the proof of this is non-trivial, see http://perisic.com/cyclotomic for details. In a more pragmatic approach the algorithm may check here if all e_ν are even and flag up an error if not. If any of the e_ν is odd it indicates that either there is an error in the software or that there is an error in the underpinning Mathematics. Usually it is the software that is wrong. Please contact me if you find out otherwise.

We use the same strategy as in Algorithm 1.1 to calculate a representation of a cyclotomic unit as a product of basis elements (Algorithm 2.4). To support Algorithm 2.4 we need the following three algorithms.

We write a cyclotomic unit as $v_{n,a}$ with $n \in \mathbb{N}$ and $a \in G_n$. We also write v_ν for short where ν is the pair (n, a). In particular we have $v_{n,a} := u_{n,a} = 1 - \epsilon_n^a$ if n is not the power of a prime and $v_{q,a} := u_{q,a}/u_{q,1} = (1 - \epsilon_q^a)/(1 - \epsilon_q)$ if $n = q = p^\alpha$ is the power of a prime. Similarly, as before for cyclotomic numbers, we write $\prod_\nu v_\nu^{e_\nu}$ for a finite product of cyclotomic units.

Algorithm 2.1

This algorithm transfers a product $P := \prod_\nu u_\nu^{e_\nu}$ of generating cyclotomic numbers into a product $Q = \prod_\mu v_\mu^{f_\mu}$ of generating cyclotomic units. If P is not a unit it will flag up an error.

1. (Initialization) Let m be the smallest common multiple of all n with $e_\nu = e_{n,a} \neq 0$ and $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ the unique factorization of m in powers of prime. Let $q_i := p_i^{\alpha_i}$.

2. (Reduce problem to prime powers) Let $Q := \prod_{v_\nu = u_\nu} u_\nu^{e_\nu}$ where the product is taken over all cyclotomic numbers u_ν that are already units v_ν; i.e. those $v_\nu = v_{n,a}$ where n is not a power of a prime. Set $P := P/Q$; and P consists only of factors where n is the power of a prime.

3. (Deal with prime powers) For all $j = 1, \ldots, r$ do the following:

   I) Set $p := p_j$, $\alpha := \alpha_j$.

   II) For $\beta = 1, \ldots, \alpha - 1$ and all $v_{p^\beta,a}$ with $a \in G_{p^\beta}$ do

   $Q := Qv_\nu^{e_\nu}$

   $P := P/(u_{p^\beta,a}/s_p)^{e_\nu}$ with $s_p = \prod_{i=0}^{p-1} u_{p^{\beta+1},1+ip^\beta}$. Note that we use the norm relation $u_{p^\beta,1} = s_p$.

   III) Let $q := p^\alpha$. For all $a \in G_q$ and $\nu = (q, a)$ do the following operations:

   $Q := Qv_\nu^{e_\nu}$

$P := P/(u_\nu/u_{q,1})^{e_\nu}$.

4. (Decision and Output) If $P = 1$ return Q. Otherwise the product of cyclotomic numbers is not a unit and no representation as product of units v_ν exists.

Note that the product PQ is an invariant in Algorithm 2.1 This and the observation that $P = 1$ in the last step proves the correctness of the algorithm.

Algorithm 2.2

Similar as Algorithm 1.2 this algorithms returns one of the methods B, S, Z, T, E, Y-p or Z-p that is then used in the following algorithm to develop the cyclotomic unit. For the cyclotomic unit $v_{n,a}$ consider the following cases:

I Is n not the power of a prime (i.e. $v_{n,a} = u_{n,a}$)? Return the output of Algorithm 1.2 (one of B, S, Z-p or E) for $u_{n,a}$.

II Is $n = 2$ or $n = 4$? Return T.

III Is $n = p$ a prime? If $a = 1$ return T; if otherwise $a < p/2$ return B; otherwise return S.

IV All other n. In this case we have $n = p^\alpha$ the power of a prime p with $\alpha > 1$. Let $\lambda := a \bmod p^{\alpha-1}$ and $b := (a - \lambda)/p^{\alpha-1}$

IV,i Is $\lambda > p^{\alpha-1}/2$? Return S.

IV,ii Is $b \neq 0$? Return B.

IV,iii Is $\lambda = 1$? Return T.

IV,iv Otherwise return Y-p.

Algorithm 2.3

For a a cyclotomic unit $v_\nu = v_{n,a}$ the developments according to methods E, Z-p, S, T and Z are as follows:

E, Z-p Develop $v_{n,a} = u_{n,a}$ with Algorithms 1.1 to 1.4 as $u_{n,a} = \prod_\nu u_\nu^{e_\nu}$. Then use Algorithm 2.1 to calculate $u_{n,a} = \prod_\nu u_\nu^{e_\nu}$ as $\prod_\nu v_\nu^{f_\nu}$ and return $\prod_\nu v_\nu^{f_\nu}$.

S Return $v_{n,n-a} = u_{n,n-a}/u_{n,1}$

T Return 1.

Y-p Let $n = p^\alpha$, $d = q/p = p^{\alpha-1}$ and $b := a \bmod d$. Return $v_{n,a} s_a^{-1} s_1 \mathfrak{n}(s_a/s_1)^{-1}$ where $s_a := \prod_{i=0}^{p-1} v_{n,b+id}$ and accordingly $s_1 := \prod_{i=0}^{p-1} v_{n,1+id}$ and $\mathfrak{n}(s_a/s_1) := v_{d,b}^{-1}$

The algorithm to calculate a basis representation for cyclotomic units is then analogous to Algorithm 1.1 as follows:

Algorithm 2.4

This algorithm calculates a basis representation of a product of cyclotomic units $\prod v_\nu^{e_\nu}$.

1. (Initialization) Set $Q := \prod v_\nu^{e_\nu}$
2. If all the v_ν are already within the basis (i.e. Algorithm 2.2 returns 'B' for this v_ν) then Q is the basis representation. Return Q and stop the algorithm.
3. Choose μ with $e_\mu \neq 0$ such that v_μ is not a basis element.
4. Use Algorithms 2.3 to write $v_\mu = \prod v_\nu^{f_\nu}$.
5. Set $Q := v_\mu^{-e_\mu} \prod v_\nu^{e_\nu + e_\mu f_\nu}$
6. Go to Step 2.