Let ϵ_n be a primitve n-th root of unity, e.g. $\epsilon_n := e^{2\pi i/n}$.

Define the group of Cyclotomic Units $C^{(n)}$ *as*

$$C^{(n)} := \mathbf{Z}[\epsilon_n]^* \cap \langle 1 - \epsilon_n^a; a = 1, \ldots, n-1 \rangle_{mult}$$

$$C^{(\infty)} := \bigcup_{n \in \mathbf{N}} C^{(n)}$$

Examples:

- *Generators:*

$$1 - \epsilon_{12},\ 1 - \epsilon_{30},\ 1 - \epsilon_{105}^{91},\ \frac{1 - \epsilon_5^2}{1 - \epsilon_5},\ \frac{1 - \epsilon_{81}^{13}}{1 - \epsilon_{81}},\ \ldots$$

- *Products and Quotients of generators:*

$$(1 - \epsilon_{12}) \frac{1 - \epsilon_5^2}{1 - \epsilon_5^3} (1 - \epsilon_{60}^7)^3,\ \frac{(1 - \epsilon_{17}^3)(1 - \epsilon_{15})^2 (1 - \epsilon_5)}{(1 - \epsilon_{17}^2)(1 - \epsilon_5^2)},\ \ldots$$

— Applications of Cyclotomic Units —

Cyclotomic Fields (Algebraic Number Theory):

$$[\mathbf{Z}[\epsilon_n]^* : C^{(n)}] < \infty$$

$(h_n = 1 \Rightarrow [\mathbf{Z}[\epsilon_n]^* : C^{(n)}] = 1)$

Used in Kummer's approach to FLT:

$$z^p - y^p = \prod_{a=0}^{p-1}(z - \epsilon_p^a y) = x^p$$

Units in cyclic grouprings (K. Hoechsmann, 1986ff):

$$\mathbf{Z}C_n \cong \mathbf{Z}[x]/x^n - 1 \quad \stackrel{x \mapsto \epsilon_n}{\longrightarrow} \quad \mathbf{Z}[\epsilon_n]$$

— Obvious Relations —

Symmetry (involution, complex conjugation):

$$1 - \epsilon_n = -\epsilon_n(1 - \epsilon_n^{-1}) \qquad \text{(S)}$$

Normrelations:

$$\prod_{i=0}^{p-1}(1 - \epsilon_p^i \eta) = 1 - \eta^p \qquad \text{(N)}$$

Example for $n = 15$:

$$(1 - \epsilon_5)(1 - \epsilon_3\epsilon_5)(1 - \epsilon_3^2\epsilon_5) = 1 - \epsilon_5^3$$

can be rearranged as:

$$(1 - \epsilon_{15}^8)(1 - \epsilon_{15}^{13}) = \frac{1 - \epsilon_5^3}{1 - \epsilon_5} \quad \text{with } \epsilon_d := \epsilon_n^{n/d} \text{ for } d|n.$$

Some remarks on the history of $C^{(n)}$

Franz (1935) proves an "independence" theorem for $C^{(n)}$.

Ramachandra (1966) gives a system of independent units generating a subgroup of finite index in $C^{(n)}$.

Milnor (1966) (according to Bass) conjectured that all relations in $C^{(n)}$ are of type (N) or (S).

Ennola (1972) showed a relation in $C^{(n)}$ that is not a combination of (N) and (S) relations.

Sinnot (1978) computes the index of $C^{(n)}$ in the full unit group (and the Stickelberger ideal ...).

Schmidt (1980) links Sinnot's results to relations between cyclotomic units (and the Stickelberger ideal ...).

Kučera (1992) gives a basis for $C^{(n)}$ $(n < \infty)$ (and ...).

- Forget about *units*.
  Consider $D^{(n)}$ generated by $1 - \epsilon_n^a$.
- Forget about torsion: (S) becomes $1 - \epsilon_n \equiv 1 - \epsilon_n^{-1}$.
- Forget about $C^{(d)}$ with $d < n$.
  Consider $\widehat{D^{(n)}} := D^{(n)} / \prod_{d|n, d \neq n} D^{(d)}$.
  Use $G_n \cong G_{p_1} \times \ldots \times G_{p_r}$ $(G_n = (\mathbf{Z}/n\mathbf{Z})^*,\ n = p_1 \cdots p_r \text{ sqf.})$
  (N) becomes $\displaystyle\prod_{i \in G_p} (1 - \epsilon_n^{(i,a_2,\ldots,a_r)}) \equiv 1$
- Forget about 1, $-$, ϵ, n, use $\sum$ instead of $\prod$, and get:

$$(a_1, \ldots, a_r) = (-a_1, \ldots, -a_r) \qquad \text{(S)}$$

$$\sum_{i=0}^{p} (i, a_2, \ldots, a_r) = 0 \qquad \text{(N)}$$

Stickelberger ideal: $(a_1, \ldots, a_r) = -(-a_1, \ldots, -a_r)$

Let $n = p_1 \cdots p_r$ be square free, odd and composite.

Consider the free $\mathbf{Z}$-module M_n over $G_{p_1} \times \ldots \times G_{p_r}$ and

$$\overline{\xi_n} : \quad M_n / \ker \xi_n \quad \cong \quad \widehat{D^{(n)}}$$

with

- $\xi_n(a_1, \ldots, a_r) = 1 - \epsilon_n^a$ where $a_i \equiv a \bmod p_i$,
- $\xi_n(\sum \ldots) = \prod \ldots$.

$$\boxed{\text{Relations in } \widehat{D^{(n)}} \longleftrightarrow \ker \xi_n}$$

Dirichlet's unit theorem [...] $\Rightarrow$

$\operatorname{rank} D^{(n)} = \frac{1}{2}\varphi(n) + r - 1$, therefore

$$\operatorname{rank} M_n / \ker \xi_n = \operatorname{rank} \widehat{D^{(n)}} = \frac{1}{2} \prod_{i=1}^{r} (\varphi(p_i) - 1) - \frac{1}{2} + (-1)^r$$

Task: Find a basis of $M_n / \ker \xi_n$