— *Weak σ-bases* —

Let M be a module with an involution σ.
A **weak σ-basis** of M is 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

$$\sigma e \equiv e \bmod \langle E^0 \cup \sigma E^0 \rangle \text{ for } e \in E^+,$$

$$\sigma e \equiv -e \bmod \langle E^0 \cup \sigma E^0 \rangle \text{ for } e \in E^-.$$

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

Note that

$$m^+ = m^+(M) = |E^+| \text{ and } m^- = m^-(M) = |E^-|$$

are invariants of M. We have

$$H^0(\sigma, M) \cong \mathbf{F}_2^{m^+} \text{ and } H^1(\sigma, M) \cong \mathbf{F}_2^{m^-}.$$

— *Examples* —

$A = \{a, \sigma a, b, \sigma b\}$, $\mathcal{E} = \{\sum_{x \in A} x\}$:

$[\{a, b\}, \emptyset, \emptyset]$ defines a weak σ-basis of $\langle A \rangle$,

$[\{a\}, \emptyset, \{b\}]$ defines a weak σ-basis of $\langle A \rangle / \langle \mathcal{E} \rangle$.

Let

$B = [E^0, E^+, E^-]$ be a weak σ-basis of M.

$C = [F^0, F^+, F^-]$ be a weak σ-basis of L.

Then $[G^0, G^+, G^-] \subseteq M \times L$ with

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

defines a weak σ-basis of $M \otimes L$.

Let $[E^0, E^+, E^-]$ be a weak σ-basis of M. Then
$E^0 \cup E^+$ defines a basis of $M_+ = M/\ker_M(\sigma + 1)$.

Lemma 1 *Given an exact sequence*

$$0 \to M \to L \to K \to 0. \tag{$*$}$$

Let $[F^0, F^+, F^-] \subseteq L$ *define a weak* σ*-basis of* K*. If* $(*)$ *splits over* σ *then* $E^0 \cup E^+ \cup F^0 \cup F^+$ *defines a basis of* L_+*.*

Lemma 2 *Let*

$$0 = L^{(0)} \leq L^{(1)} \leq \cdots \leq L^{(i)} \leq \cdots \leq L = \bigcup_{i=0}^{\infty} L^{(i)}.$$

be a chain with the property that for every $i \in \mathbf{N}$ *there exists a module* $M^{(i)}$ *such that the sequence*

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

is exact and splits over σ*. If* $B_+^{(i)} \subseteq L^{(i)}$ *defines a basis of* $M_+^{(i)}$ *for all* $i \in \mathbf{N}$ *then* $\bigcup_{i=1}^{\infty} B_+^{(i)}$ *defines a basis of* L_+*.*

Let Δ be an appropriate indexing set and for $d \in \Delta$:

M_d a module,

$\mathcal{E}_d \subseteq M_d$,

$\mathtt{n}_d : \mathcal{E}_d \to \bigoplus_{t<d} M_t$ a mapping.

Then we call the module $\mathcal{L} = N/Q$ with

$$N = \bigoplus_{t\in\Delta} M_t,$$

$$Q = \sum_{t\in\Delta} \langle r + \mathtt{n}_t(r);\ r \in \mathcal{E}_t \rangle$$

the **combination** of the system $\Gamma = (M_d, \mathcal{E}_d, \mathtt{n}_d)_{d\in\Delta}$.

Theorem 1 *If* Γ *is* combinable *and* splits over σ *(two technical conditions) we have:*
If $B_+^{(d)} \subseteq M_d$ *defines a basis of* $(M_d/\langle\mathcal{E}_d\rangle)_+$ *for each* $d \in \Delta$ *then* $\bigcup_{d\in\Delta} B_+^{(d)} \subseteq \bigoplus_{d\in\Delta} M_d$ *defines a basis of* $\mathcal{L}_+$*.*

Let

$G_d=\{1 \le b < d;\ (b,d)=1\}$, $\sigma b = d-b$ for $b \in G_d$,

$A_p = \{0,\ldots,p-1\}$, $\sigma a = p-1-a$ for $a \in A_p$.

Write $\Sigma(S)$ for $\displaystyle\sum_{s\in S} s$.

Define the **cyclotomic module** $Z(n)$ as follows:

For $n=p$ prime let $Z(p) = \langle G_p\rangle / \langle \Sigma(G_p)\rangle$.

For $n = q = p^\alpha$, $\alpha > 1$ let

$$Z(q) = \langle G_{q/p}\rangle \otimes \langle A_p\rangle / \langle \Sigma(A_p)\rangle.$$

For $n = q_1 \cdots q_r$ let $Z(n) = Z(q_1) \otimes \cdots \otimes Z(q_r)$.

Lemma 3

$$Z(n) \cong M_n / \langle \mathcal{E}_n \rangle$$

where $M_n = \langle G_n \rangle$ *and*

$$\mathcal{E}_n = \{s(n,p,a);\ p|n \text{ with } p \text{ prime},\ a \in G_{n/p}\}$$

with

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

The n**th cyclotomic system** $\Gamma(n)$ is defined as a system $(M_d, \mathcal{E}_d, \mathtt{n}_d)_{d|n}$ with

$M_d = \langle G_d \rangle$,

$\mathcal{E}_d$ as before if d is not prime, else $\mathcal{E}_d = \emptyset$,

$$\begin{aligned} \mathtt{n}_d : \quad \mathcal{E}_d \quad & \to \bigoplus_{t|d, t\neq d} M_t \\ s(d,p,a) \quad & \mapsto \begin{cases} -[d/p; a] & \text{if } p^2 | d, \\ [d/p; p^{-1}a] - [d/p; a] & \text{if } p^2 \not| d, \end{cases} \end{aligned}$$

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

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

Lemma 4

> *If* $4 \not| n$ *then* $\Gamma(n)$ *is combinable and splits over* σ.
>
> *If* $4|n$ *we can make some modifications to get a similar result.*

$\longrightarrow$ *we can construct a basis of* $\mathcal{L}(n)_+$ *by weak* σ*-bases of the modules* $M_d/\langle \mathcal{E}_d \rangle$.

Let ϵ_d be a primitive dth root of unity. We call

$$D^{(n)} = \langle 1-\epsilon_d^a;\ a \in G_d,\ d|n\rangle / \langle \pm\epsilon_n\rangle$$

the group of the n**th cyclotomic numbers**.

Lemma 5 *The sequence*

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

where T is the torsion group of $\mathcal{L}(n)/(1-\sigma)\mathcal{L}(n)$ is exact. The homomorphism μ is defined by the maps $\mu_d : G_d \to D^{(n)}$, $a \mapsto 1-\epsilon_d^a$ for $d|n$.
$\longrightarrow$ From $(*)$ follows $\mathcal{L}(n)_+ \cong D^{(n)}$.

Let $\widehat{D^{(n)}} = D^{(n)} / \prod_{d|n, d\neq n} D^{(d)}$.

Theorem 2 *Let $\widehat{B_d} \subseteq D^{(n)}$ define a basis of $\widehat{D^{(d)}}$.*

(a) $\bigcup_{d|n} \widehat{B_d}$ *is a basis of* $D^{(n)}$ *if* $4 \nmid n$.

(b) $\{1-\epsilon_4\} \cup \bigcup_{\substack{d|n \\ d\neq 2,4}} \widehat{B_d}$ *is a basis of* $D^{(n)}$ *if* $4|n$.

Define the group of n**th cyclotomic units** by

$$C^{(n)} = D^{(n)} \cap (\mathbf{Z}[\epsilon_n]/\langle \pm \epsilon_n \rangle).$$

Let $\widehat{C^{(n)}} = C^{(n)} / \prod_{d|n,\, d \neq n} C^{(d)}$.

The connection between cyclotomic units and cyclotomic numbers is given by the two isomorphisms

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

$\widehat{C^{(q)}} \cong \langle \frac{1-\epsilon_q^a}{1-\epsilon_q};\ a \in G_q \rangle \leq \widehat{D^{(q)}}$ if $n = q$ is a prime power.

Theorem 3 *If $\widehat{B_d} \subseteq C^{(n)}$ defines a basis of $\widehat{C^{(d)}}$ for $d|n$ then $B_n = \bigcup_{d|n} \widehat{B_d}$ is a basis of $C^{(n)}$.*

$\longrightarrow \quad \bigcup_{d \in \mathbf{N}} \widehat{B_d}$ *defines a basis of* $C^{(\infty)} := \bigcup_{d \in \mathbf{N}} C^{(d)}$.

Consider again the exact sequence

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

There are three kinds of relations in $D^{(n)}$.

Norms: $N_{\mathbf{Q}(\epsilon_n)\to\mathbf{Q}(\epsilon_d)}(1-\epsilon_n) \in D^{(d)}$

for instance: $(1-\epsilon_{18})(1-\epsilon_{18}^7)(1-\epsilon_{18}^{13}) = 1-\epsilon_6$

$\longrightarrow$ relations in $\mathcal{L}(n)$.

Complex conjugation:

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

$\longrightarrow$ factoring out $(1-\sigma)\mathcal{L}(n)$.

Ennola-relations: ...

$\longrightarrow T$.

Ennola-relations can be constructed explicitely by means of σ-bases. We have

$$T \cong H^0(\sigma, \mathcal{L}(n)) \cong \mathbf{F}_2^{m^+(\mathcal{L}(n))}.$$

— *The Stickelberger Elements* —

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 an exact sequence

$$0 \to T \to \mathcal{L}(n)/(1+\sigma)\mathcal{L}(n) \xrightarrow{\nu} I_n/\langle \omega_n \rangle \to 0.$$

where T is the torsion group of $\mathcal{L}(n)/(1+\sigma)\mathcal{L}(n)$. The homomorphism ν is given by the maps

$$\nu_d : G_d \to I_n,\ a \mapsto \theta(an/d).$$

So with the same mechanism used for cyclotomic units we can construct bases and relations, especially Ennola-relations for I_n.