Archivum Mathematicum

Vladimír Sedláček

Circular units of real abelian fields with four ramified primes

Archivum Mathematicum, Vol. 53 (2017), No. 4, 221–252

Persistent URL: http://dml.cz/dmlcz/146984

ARCHIVUM MATHEMATICUM (BRNO)
Tomus 53 (2017), 221–252

CIRCULAR UNITS OF REAL ABELIAN FIELDS WITH FOUR RAMIFIED PRIMES

Vladimír Sedláček

Abstract. In this paper we study the groups of circular numbers and circular units in Sinnott's sense in real abelian fields with exactly four ramified primes under certain conditions. More specifically, we construct $\mathbb{Z}$-bases for them in five special infinite families of cases. We also derive some results about the corresponding module of relations (in one family of cases, we show that the module of Ennola relations is cyclic). The paper is based upon the thesis [6], which builds upon the results of the paper [2].

1. Introduction

Circular units appear in many situations in algebraic number theory because in some sense, for a given abelian field, they form a good approximation of the full group of units, which is usually very hard to describe explicitly. The index of the group of circular units in the full group of units is closely related to the class number of the maximal real subfield of the respective field, which was already known to E. Kummer in the case of a prime-power cyclotomic field and which was generalized by W. Sinnott to any abelian field. Circular units can be also used for a construction of annihilators of ideal class group of a given real abelian field, which was discovered by F. Thaine and generalized by K. Rubin (see [8] and [4]).

In contrast to the full group of units, the Sinnott group of circular units is given by explicit generators, nevertheless a $\mathbb{Z}$-basis of this group was described only in a few very special cases, for example when the abelian field is cyclotomic, has at most two ramified primes, or has three ramified primes and satisfies some other conditions. More details can be found in [1] and [2].

The aim of this paper is to present new results in the case of a real abelian field having four ramified primes under some other assumptions. Additionally, we will also explore the structure of the module of all relations (among the generators of the group of circular numbers) modulo the norm relations.

Except for some parts of Section 7, all results in this self-contained paper come from the author's thesis [6], where they are usually explained in greater detail (and

2010 *Mathematics Subject Classification*: primary 11R20.
Key words and phrases: circular units, abelian fields, four ramified primes, Ennola relations.
The author was supported under project 15-15785S of the Czech Science Foundation.
Received August 2, 2017, revised November 2017. Editor R. Kučera.
DOI: 10.5817/AM2017-4-221

the notation used there is exactly the same as here). In particular, the complete proofs of the theorems in Section 6 can be found there.

2. Basic definitions and results about circular numbers and units

For the remainder of this section, let $k \neq \mathbb{Q}$ be a real abelian field, K be its genus field in the narrow sense, P be the set of ramified primes of $k/\mathbb{Q}$ and K_p be the maximal subfield of K ramified over $\mathbb{Q}$ only at $p \in P$. Since $\mathrm{Gal}(K/\mathbb{Q})$ has a natural action on K (given by evaluating an automorphism on an element), this makes K and $K^\times$ into $\mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})]$-modules.

Definition 2.1. The group $D(k)$ of circular numbers of k is given as

$$D(k) := \big\langle \{-1\} \cup \{\eta_I \big| \emptyset \subsetneq I \subseteq P\}\big\rangle_{\mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})]},$$

where $\langle \dots \rangle_{\mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})]}$ means "generated as a $\mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})]$-submodule of $K^\times$" and

$$\eta_I := \mathrm{N}_{\mathbb{Q}(\zeta_{\mathrm{cond}\left(\prod_{i\in I} K_i\right)})/\left(\prod_{i\in I} K_i\right)\cap k}\Big(1 - \zeta_{\mathrm{cond}\left(\prod_{i\in I} K_i\right)}\Big),$$

where N denotes the norm operator, $\mathrm{cond}(L)$ is the conductor of an abelian field L, and the product of fields denotes their compositum. The subgroup of totally positive elements of $D(k)$ will be denoted by $D^+(k)$.

Definition 2.2. The group $C(k)$ of circular numbers of k is $E(k) \cap D(k)$, where $E(k)$ is the group of units of the ring of algebraic integers of k. The subgroup of totally positive elements of $C(k)$ will be denoted by $C^+(k)$.

In [3], it is proven that the above definition of $C(k)$ gives the same group as Sinnott's original definition in [7].

Here are a few well known facts about circular units:

Lemma 2.3. *Let $\emptyset \subsetneq I \subseteq P$.*

(1) *For $|I| > 1$, we have $\eta_I \in E(k)$.*

(2) *For $|I| = 1$, we have $\eta_I \notin E(k)$, but $\eta_I^{1-\sigma} \in E(k)$ for any $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$.*

Corollary 2.4. *We have*

$$C(k) = \big\langle \{-1\} \cup \{\eta_I \big| I \subseteq P, |I| \geq 2\} \cup \{\eta_{\{p\}}^{1-\sigma} \mid p \in P, \sigma \in \mathrm{Gal}(K/\mathbb{Q}))\}\big\rangle_{\mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})]}$$

and

$$C^+(k) = \big\langle \{\eta_I \big| I \subseteq P, |I| \geq 2\} \cup \{\eta_{\{p\}}^{1-\sigma} \mid p \in P, \sigma \in \mathrm{Gal}(K/\mathbb{Q}))\}\big\rangle_{\mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})]}.$$

Proposition 2.5. *The $\mathbb{Z}$-rank of $D^+(k)$ is $[k : \mathbb{Q}] + |P| - 1$ and the $\mathbb{Z}$-rank of $C^+(k)$ is $[k : \mathbb{Q}] - 1$.*

Lemma 2.6. *If $L' \subseteq L$ are abelian fields, then for any $\epsilon \in C(L)$ (or $C^+(L)$) we have $\mathrm{N}_{L/L'}(\epsilon) \in C(L')$ (or $C^+(L')$), respectively.*

3. The special case of four ramified primes

In the remainder of the paper, we will fix k to be a real abelian field with exactly four ramified primes p_1, p_2, p_3, p_4 and we will abbreviate $D(k)$, $D^+(k)$, $C(k)$, $C^+(k)$ simply as D, D^+, C, C^+. We will also use the convention that whenever any of the indices i, j, l, h appear on the same line, they denote pairwise distinct integers satisfying $1 \leq i, j, l, h \leq 4$, unless stated otherwise. Finally, for any positive integer n, ζ_n will denote a primitive n-th root of unity (without loss of generality we can take $\zeta_n = \mathrm{e}^{2\pi i/n}$).

Let K be the genus field in the narrow sense of k and let $G := \mathrm{Gal}(K/\mathbb{Q})$. Then we can identify G with the direct product $T_1 \times T_2 \times T_3 \times T_4$, where T_i is the inertia group corresponding the ramified prime p_i. Next, we will define:

- $H := \mathrm{Gal}(K/k)$,
- $m := |H|$,
- the canonical projections $\pi_i \colon G \to T_i$,
- $a_i := [T_i : \pi_i(H)]$,
- $r_i := |H \cap \ker \pi_i|$,
- $s_{ij} := |H \cap \ker(\pi_i \pi_j)|$,
- $n_i := \frac{m}{r_i}$,
- $\eta := \eta_{\{p_1,p_2,p_3,p_4\}}$,
- K_i as the maximal subfield of K ramified only at p_i.

Note that we have $T_i = \mathrm{Gal}(K/K_j K_l K_h) \cong \mathrm{Gal}(K_i/\mathbb{Q})$ and

$$K = kK_iK_jK_l = K_1K_2K_3K_4$$

by ramification theory.

Assumption 3.1. In the remainder of the paper, we will assume the following:

- H is cyclic, generated by τ,
- each T_i is cyclic, generated by σ_i.

Note that the second assumption isn't very restrictive, as it is automatically true for example if all the ramified primes of k are odd (because $T_i \cong \mathrm{Gal}(K_i/\mathbb{Q})$ is a quotient of the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_{\mathrm{cond}(K_i)})/\mathbb{Q}) \cong (\mathbb{Z}/p_i^f)^\times$ for some positive integer f).

Lemma 3.2. *Without loss of generality, we can assume* $\tau = \sigma_1^{a_1}\sigma_2^{a_2}\sigma_3^{a_3}\sigma_4^{a_4}$.

Proof. We know that $a_i = [T_i : \pi_i(H)]$, hence $\pi_i(\tau)$ generates a subgroup of T_i of index a_i. The cyclicity of T_i then implies that $\pi_i(\tau)$ must be the a_i-th power of some generator of T_i, without loss of generality σ_i. The statement now follows, because τ is determined by its four projections. □

Proposition 3.3. *We have*

$$\begin{aligned}[k \cap K_i : \mathbb{Q}] &= a_i\,, \\ [K : kK_i] &= r_i \\ |T_i| &= a_i n_i\,, \\ [K : kK_iK_j] &= s_{ij}\,, \\ [K_i : k \cap K_i] &= |\pi_i(H)| = n_i\,, \\ [K_iK_j : k \cap K_iK_j] &= |\pi_i\pi_j(H)| = \frac{m}{s_{ij}}\end{aligned}$$

and

$$[K_iK_jK_l : k \cap K_iK_jK_l] = |\pi_i\pi_j\pi_l(H)| = m\,.$$

Proof. Since

$$\begin{aligned}\mathrm{Gal}(K/K_i) &= \mathrm{Gal}(K/K_iK_jK_l \cap K_iK_jK_h \cap K_iK_lK_h) \\ &= \mathrm{Gal}(K/K_iK_jK_l) \cdot \mathrm{Gal}(K/K_iK_jK_h) \cdot \mathrm{Gal}(K/K_iK_lK_h) = T_jT_lT_h\end{aligned}$$

and $\mathrm{Gal}(K/k) = H$, it follows that $\mathrm{Gal}(K/k \cap K_i) = T_jT_lT_h \cdot H$. Now consider the short exact sequence

$$0 \to H \cap \ker \pi_i \to H \xrightarrow{\pi_i|_H} \pi_i(H) \to 0\,.$$

It follows that $|\pi_i(H)| = \frac{m}{r_i} = n_i$ and

$$\begin{aligned}\pi_i(H) &\cong \frac{H}{H \cap \ker \pi_i} = \frac{H}{H \cap T_jT_lT_h} \cong \frac{T_jT_lT_h \cdot H}{T_jT_lT_h} \\ &= \frac{\mathrm{Gal}(K/k \cap K_i)}{\mathrm{Gal}(K/K_i)} \cong \mathrm{Gal}(K_i/k \cap K_i)\,.\end{aligned}$$

Therefore

$$[k \cap K_i : \mathbb{Q}] = \frac{|\mathrm{Gal}(K_i/\mathbb{Q})|}{|\mathrm{Gal}(K_i/k \cap K_i)|} = \frac{|T_i|}{|\pi_i(H)|} = a_i$$

and

$$[K : kK_i] = \frac{|\mathrm{Gal}(K/k)|}{|\mathrm{Gal}(kK_i/k)|} = \frac{|H|}{|\mathrm{Gal}(K_i/k \cap K_i)|} = \frac{m}{|\pi_i(H)|} = r_i\,.$$

Putting everything together, we obtain

$$|T_i| = [K_i : k \cap K_i] \cdot [k \cap K_i : \mathbb{Q}] = a_i|\pi_i(H)| = a_in_i\,.$$

Next, we also have

$$\begin{aligned}\mathrm{Gal}(K/K_iK_j) &= \mathrm{Gal}(K/K_iK_jK_l \cap K_iK_jK_h) \\ &= \mathrm{Gal}(K/K_iK_jK_l) \cdot \mathrm{Gal}(K/K_iK_jK_h) = T_lT_h\end{aligned}$$

so that $\mathrm{Gal}(K/k \cap K_iK_j) = T_lT_h \cdot H$. Thus we can consider the short exact sequence

$$0 \to H \cap \ker \pi_i\pi_j \to H \xrightarrow{\pi_i\pi_j|_H} \pi_i\pi_j(H) \to 0$$

to conclude that $|\pi_i\pi_j(H)| = \frac{m}{s_{ij}}$ and

$$\pi_i\pi_j(H) \cong \frac{H}{H \cap \ker \pi_i\pi_j} = \frac{H}{H \cap T_lT_h} \cong \frac{T_lT_h \cdot H}{T_lT_h}$$
$$\cong \frac{\mathrm{Gal}(K/k \cap K_iK_j)}{\mathrm{Gal}(K/K_iK_j)} \cong \mathrm{Gal}(K_iK_j/k \cap K_iK_j)\,.$$

Then it follows that

$$[K : kK_iK_j] = \frac{|\mathrm{Gal}(K/k)|}{|\mathrm{Gal}(kK_iK_j/k)|} = \frac{|H|}{|\mathrm{Gal}(K_iK_j/k \cap K_iK_j)|} = \frac{m}{|\pi_i\pi_j(H)|} = s_{ij}\,.$$

Finally, we have

$$\mathrm{Gal}(K_iK_jK_l/k \cap K_iK_jK_l) \cong \mathrm{Gal}(kK_iK_jK_l/k) = \mathrm{Gal}(K/k) = H\,,$$

and we can consider the short exact sequence

$$0 \to H \cap \ker \pi_i\pi_j\pi_l \to H \xrightarrow{\pi_i\pi_j\pi_l|_H} \pi_i\pi_j\pi_l(H) \to 0$$

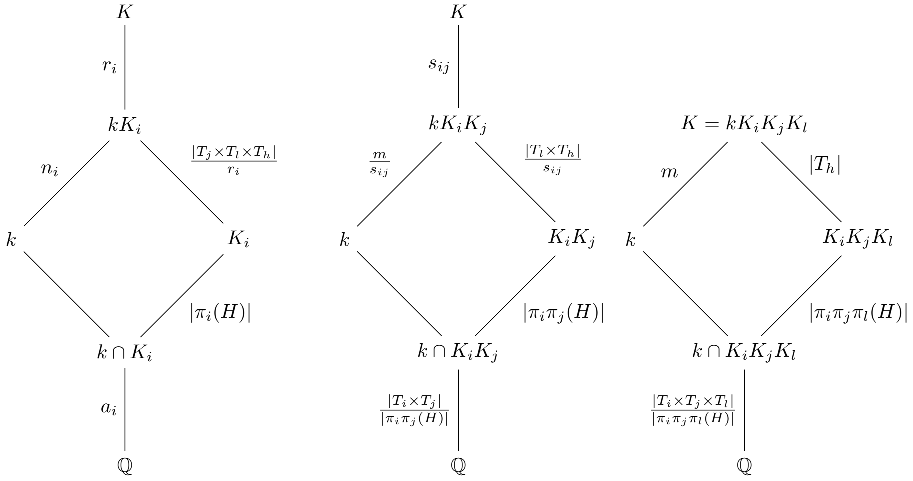
where

$$H \cap \ker \pi_i\pi_j\pi_l = H \cap T_h = \mathrm{Gal}(K/kK_iK_jK_l) = 0\,.$$

Thus $|\pi_i\pi_j\pi_l(H)| = m$ and

$$\pi_i\pi_j\pi_l(H) \cong H \cong \frac{T_h \cdot H}{T_h}$$
$$\cong \frac{\mathrm{Gal}(K/k \cap K_iK_jK_l)}{\mathrm{Gal}(K/K_iK_jK_l)} \cong \mathrm{Gal}(K_iK_jK_l/k \cap K_iK_jK_l)\,.$$

□



Remark 3.4. Note that Proposition 3.3 implies that $a_in_i \neq 1$, otherwise T_i would be trivial and p_i wouldn't ramify in k.

Corollary 3.5. *We have*

$$[k \cap K_iK_j : \mathbb{Q}] = a_ia_j\frac{m}{r_ir_j}s_{ij}\,,$$

$$[k \cap K_iK_jK_l : \mathbb{Q}] = a_ia_ja_l\frac{m^2}{r_ir_jr_l}$$

and

$$[k : \mathbb{Q}] = a_1a_2a_3a_4\frac{m^3}{r_1r_2r_3r_4}\,.$$

Proof. This follows from the computations

$$[k \cap K_iK_j : \mathbb{Q}] = \frac{[K_iK_j : \mathbb{Q}]}{[K_iK_j : k \cap K_iK_j]} = \frac{|T_i|\cdot|T_j|}{m/s_{ij}} = a_ia_j\frac{m}{r_ir_j}s_{ij}\,,$$
$$[k \cap K_iK_jK_l : \mathbb{Q}] = \frac{[K_iK_jK_l : \mathbb{Q}]}{[K_iK_jK_l : k \cap K_iK_jK_l]} = \frac{|T_i|\cdot|T_j|\cdot|T_l|}{m} = a_ia_ja_l\frac{m^2}{r_ir_jr_l}$$

and

$$[k : \mathbb{Q}] = \frac{[K : \mathbb{Q}]}{[K : k]} = \frac{|T_1|\cdot|T_2|\cdot|T_3|\cdot|T_4|}{m} = a_1a_2a_3a_4\frac{m^3}{r_1r_2r_3r_4}\,.$$

□

Lemma 3.6. *We have*

$$\gcd(r_i, r_j) = s_{ij}\,,$$

$$\gcd(r_i, r_j, r_l) = 1\,,$$
$$\operatorname{lcm}(n_i, n_j, n_l) = m$$

and

$$\gcd(n_i, n_j) = s_{ij}\frac{m}{r_ir_j}\,.$$

Proof. It follows from Proposition 3.3 that $s_{ij} \mid r_i$, $s_{ij} \mid r_j$ and

$$|\pi_i(H)| = n_i\,, \quad |\pi_i\pi_j(H)| = \frac{m}{s_{ij}} \quad \text{and} \quad |\pi_i\pi_j\pi_l(H)| = m\,.$$

The cyclicity of H then implies

$$\frac{m}{s_{ij}} = |\pi_i\pi_j(H)| = |\langle\pi_i\pi_j(\tau)\rangle| = |\langle\pi_i(\tau)\pi_j(\tau)\rangle| = \operatorname{lcm}(n_i, n_j)\,,$$

because $\langle\pi_i(\tau)\rangle = \pi_i(H)$ and any power of the product $\pi_i(\tau)\pi_j(\tau)$ is trivial if and only if the same power of both its factors is (since G is the direct product of the T_i's). Now for any common divisor t of r_i, r_j, we have

$$\frac{m}{s_{ij}} = \operatorname{lcm}(n_i, n_j) = \operatorname{lcm}\Big(\frac{m}{r_i}, \frac{m}{r_j}\Big) \Bigm| \frac{m}{t}\,,$$

which implies $t \mid s_{ij}$. Hence $s_{ij} = \gcd(r_i, r_j)$.

Similarly, we can compute

$$m = |\pi_i\pi_j\pi_l(H)| = |\langle\pi_i\pi_j\pi_l(\tau)\rangle| = |\langle\pi_i(\tau)\pi_j(\tau)\pi_l(\tau)\rangle| = \operatorname{lcm}(n_i, n_j, n_l)\,.$$

In addition, if t is any positive common divisor of r_i, r_j, r_l, we have

$$m = \operatorname{lcm}(n_i, n_j, n_l) = \operatorname{lcm}\Big(\frac{m}{r_i}, \frac{m}{r_j}, \frac{m}{r_l}\Big) \Bigm| \frac{m}{t}\,,$$

which implies $t = 1$, hence $\gcd(r_i, r_j, r_l) = 1$.

Finally, using the first result, we have

$$s_{ij}\frac{m}{r_ir_j} = \frac{m}{r_ir_j/s_{ij}} = \frac{m}{\operatorname{lcm}(r_i, r_j)}\,,$$

which clearly divides both $\frac{m}{r_i} = n_i$ and $\frac{m}{r_j} = n_j$. Moreover, if t is any common divisor of $n_i = \frac{m}{r_i}$ and $n_j = \frac{m}{r_j}$, then both r_it and r_jt divide m, hence

$$t \cdot \operatorname{lcm}(r_i, r_j) = \operatorname{lcm}(r_it, r_jt) \mid m\,.$$

Thus $t \mid \frac{m}{\operatorname{lcm}(r_i,r_j)}$ and we are done. □

Remark 3.7. If k is fixed, we have shown in Lemmas 3.3 and 3.6 and Remark 3.4 that

$$r_i \mid m, \gcd(r_i, r_j, r_l) = 1\,,\ a_in_i \neq 1\,.$$

Conversely, using the theory of Dirichlet characters, it can be shown that for any choice of positive integers m, a_1, a_2, a_3, a_4, r_1, r_2, r_3, r_4 satisfying

$$r_i \mid m, \gcd(r_i, r_j, r_l) = 1\,,\ a_in_i \neq 1\,,$$

there exist infinitely many real abelian fields k ramified at exactly four primes satisfying the assumptions on page 223 (in particular, the family of fields we are studying is nonempty). The proof of this is analogous to the proof of a similar statement in Chapter 6 of [5] and we omit it.

Proposition 3.8. *We have*

$$\begin{aligned}\operatorname{Gal}(k/\mathbb{Q}) \cong \{\sigma_1^{x_1}\sigma_2^{x_2}\sigma_3^{x_3}\sigma_4^{x_4}|_k; 0 \le x_1 < a_1\frac{m}{r_1}, 0 \le x_2 < a_2\frac{m}{r_2s_{34}},\\ 0 \le x_3 < a_3\frac{m}{r_3r_4}s_{34}, 0 \le x_4 < a_4\}\,,\end{aligned}$$

where each automorphism of k determines the quadruple (x_1, x_2, x_3, x_4) uniquely.

Proof. First note that by Lemma 3.6, we have

$$a_3\frac{m}{r_3r_4}s_{34} = a_3\gcd(n_3, n_4) \in \mathbb{Z}$$

and

$$a_2\frac{m}{r_2s_{34}} \in \mathbb{Z}$$

(this follows from $r_2 \mid m$, $s_{34} \mid m$ and $\gcd(r_2, s_{34}) = \gcd(r_2, r_3, r_4) = 1$). By Corollary 3.5, the set on the right hand side has at most $|\mathrm{Gal}(k/\mathbb{Q})|$ elements. Now let ρ be any automorphism of k. If we can show that ρ can be written as

$$\rho = \sigma_1^{x_1}\sigma_2^{x_2}\sigma_3^{x_3}\sigma_4^{x_4}\,|_k$$

for a quadruple (x_1, x_2, x_3, x_4) satisfying

$$0 \le x_1 < a_1\frac{m}{r_1}\,,\ 0 \le x_2 < a_2\frac{m}{r_2 s_{34}}\,,\ 0 \le x_3 < a_3\frac{m}{r_3 r_4}s_{34}\,,\ 0 \le x_4 < a_4\,,$$

it will follow that the cardinalities agree and we will be done.

Since $\mathrm{Gal}(k \cap K_4/\mathbb{Q})$ is a cyclic group of order a_4 (by Lemma 3.3) generated by $\sigma_4|_{k\cap K_4}$ (as a quotient of $\mathrm{Gal}(K_4/\mathbb{Q}) = \langle\sigma_4|_{K_4}\rangle$), there must exist a unique $x_4 \in \mathbb{Z}$, $0 \le x_4 < a_4$ such that ρ and $\sigma_4^{x_4}$ have the same restrictions to $k \cap K_4$. Therefore $\rho\sigma_4^{-x_4}\big|_k \in \mathrm{Gal}(k/k \cap K_4)$.

Next, $\mathrm{Gal}(k \cap K_3K_4/k \cap K_4)$ is a cyclic group of order $\frac{[k\cap K_3K_4:\mathbb{Q}]}{[k\cap K_4:\mathbb{Q}]} = a_3\frac{m}{r_3r_4}s_{34}$ (by Corollary 3.5) generated by $\sigma_3|_{k\cap K_3K_4}$ (as it is isomorphic by restriction to

$$\mathrm{Gal}\big((k \cap K_3K_4)K_4/K_4\big)\,,$$

which is a quotient of $\mathrm{Gal}(K_3K_4/K_4) = \langle\sigma_3|_{K_3K_4}\rangle$), so there must exist a unique $x_3 \in \mathbb{Z}$ with $0 \le x_3 < a_3\frac{m}{r_3r_4}s_{34}$ such that $\rho\sigma_4^{-x_4}\big|_k$ and $\sigma_3^{x_3}$ have the same restriction to $k \cap K_3K_4$. Therefore $\rho\sigma_3^{-x_3}\sigma_4^{-x_4}\big|_k \in \mathrm{Gal}(k/k \cap K_3K_4)$.

Following the pattern, $\mathrm{Gal}(k \cap K_2K_3K_4/k \cap K_3K_4)$ is a cyclic group of order

$$\frac{[k \cap K_2K_3K_4 : \mathbb{Q}]}{[k \cap K_3K_4 : \mathbb{Q}]} = a_2\frac{m}{r_2s_{34}}$$

(by Corollary 3.5) generated by $\sigma_2|_{k\cap K_2K_3K_4}$ (as it is isomorphic by restriction to

$$\mathrm{Gal}\big((k \cap K_2K_3K_4)K_3K_4/K_3K_4\big)\,,$$

which is a quotient of

$$\mathrm{Gal}(K_2K_3K_4/K_3K_4) = \langle\sigma_2|_{K_2K_3K_4}\rangle)\,,$$

so there must exist a unique $x_2 \in \mathbb{Z}$, $0 \le x_2 < a_2\frac{m}{r_2s_{34}}$ such that $\rho\sigma_3^{-x_3}\sigma_4^{-x_4}\big|_k$ and $\sigma_2^{x_2}$ have the same restriction to $k \cap K_2K_3K_4$. Therefore

$$\rho\sigma_2^{-x_2}\sigma_3^{-x_3}\sigma_4^{-x_4}\big|_k \in \mathrm{Gal}(k/k \cap K_2K_3K_4)\,.$$

Finally, we have

$$\mathrm{Gal}(k/k \cap K_2K_3K_4) \cong \mathrm{Gal}(kK_2K_3K_4/K_2K_3K_4) = \mathrm{Gal}(K/K_2K_3K_4) = \langle\sigma_1\rangle\,,$$

where the isomorphism is given by restriction. Since the order of σ_1 is $a_1\frac{m}{r_1}$, it follows that there must exist a unique $x_1 \in \mathbb{Z}$, $0 \le x_1 < a_1\frac{m}{r_1}$ such that $\rho\sigma_2^{-x_2}\sigma_3^{-x_3}\sigma_4^{-x_4}\big|_k$ and $\sigma_1^{x_1}$ have the same restriction to k. Thus $\rho = \sigma_1^{x_1}\sigma_2^{x_2}\sigma_3^{x_3}\sigma_4^{x_4}|_k$ and the proof is finished.

$$\begin{tikzcd}
K_1K_2K_3K_4 = K \arrow[d, dash, "\langle\sigma_1\rangle"'] \arrow[dr, dash] & \\
K_2K_3K_4 \arrow[d, dash, "\langle\sigma_2|_{K_2K_3K_4}\rangle"'] \arrow[dr, dash] & k \arrow[d, dash, "a_1\frac{m}{r_1}"] \\
K_3K_4 \arrow[d, dash, "\langle\sigma_3|_{K_3K_4}\rangle"'] \arrow[dr, dash] & k\cap K_2K_3K_4 \arrow[d, dash, "a_2\frac{m}{r_2s_{34}}"] \\
K_4 \arrow[d, dash, "\langle\sigma_4|_{K_4}\rangle"'] \arrow[dr, dash] & k\cap K_3K_4 \arrow[d, dash, "a_3\frac{m}{r_3r_4}s_{34}"] \\
\mathbb{Q} \arrow[dr, dash] & k\cap K_4 \arrow[d, dash, "a_4"] \\
 & \mathbb{Q}
\end{tikzcd}$$

□

4. General strategy for the construction of bases of circular numbers and circular units

Our goal will be to find explicit $\mathbb{Z}$-bases of D^+ and C^+. To achieve this, we will build upon the results in [2]. The generators of D^+ are subject to norm relations that correspond to the sum of all elements of the respective inertia groups T_i. Namely, let

$$R_i = \sum_{u=0}^{a_i-1} \sigma_i^u,\ N_i = \sum_{u=0}^{n_i-1} \sigma_i^{ua_i}\,.$$

Then the norm operator from K to $K_jK_lK_h$ can be given as R_iN_i, because both are equal to the sum of all elements from T_i. Moreover, we have

$$\mathrm{Gal}(k/k\cap K_jK_lK_h) \cong \mathrm{Gal}(K/K_jK_lK_h) = T_i\,,$$

where the first isomorphism is given by restriction, hence R_iN_i also acts as the norm operator from k to $k\cap K_jK_lK_h$. If we denote the congruence corresponding to the canonical projection $\mathbb{Z}[G] \to \mathbb{Z}[G/H]$ by $\equiv$, then we have (using Lemma 3.2)

$$N_4 \equiv \sum_{u=0}^{n_4-1} \sigma_1^{ua_1}\sigma_2^{ua_2}\sigma_3^{ua_3}\,.$$

Note that any subgroup of $k^\times$ is naturally a $\mathbb{Z}[G/H]$-module, since the action of H on k is trivial.

Moreover, we will denote the congruence corresponding to the composition of canonical projections

$$\mathbb{Z}[G] \to \mathbb{Z}[G/H] \to \mathbb{Z}[G/H]/(R_1N_1, R_2N_2, R_3N_3, R_4N_4)$$

by $\sim$, where $(R_1N_1, R_2N_2, R_3N_3, R_4N_4)$ is the ideal generated in $\mathbb{Z}[G/H]$ by the images of the elements R_iN_i. Lemma 2.3 shows that $\eta \in C^+$, therefore by Lemma 2.6, we have $\eta^{\rho R_i N_i} \in C^+(k \cap K_jK_lK_h)$ for any $\rho \in G$. We will make use of this extensively, because explicit $\mathbb{Z}$-bases of $D^+(k \cap K_iK_jK_l)$ and $C^+(k \cap K_iK_jK_l)$ have already been constructed in [1] if exactly two of the primes p_i, p_j, p_l ramify in $k \cap K_iK_jK_l$, or in [2] if all three primes ramify in this field, as the following lemma shows. (If at most one prime ramifies in $k \cap K_iK_jK_l$, it is quite trivial to describe explicit $\mathbb{Z}$-bases of $D^+(k \cap K_iK_jK_l)$ and $C^+(k \cap K_iK_jK_l)$ as well.)

Lemma 4.1. *If the field $k \cap K_iK_jK_l$ is ramified at all three primes p_i, p_j, p_l then this field satisfies the assumptions of* [2]. *In other words, if K' is the genus field in the narrow sense of $k \cap K_iK_jK_l$, then* $\mathrm{Gal}(K'/k \cap K_iK_jK_l)$ *is cyclic and the inertia subgroups of* $\mathrm{Gal}(K'/\mathbb{Q})$ *are all cyclic.*

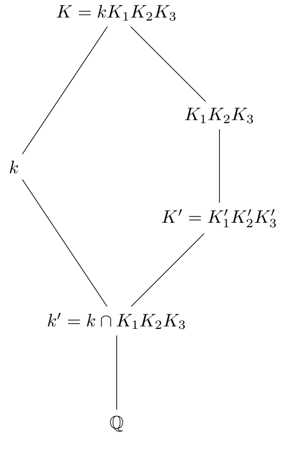
Proof. It's clear that $k \cap K_iK_jK_l$ is real, abelian (its absolute Galois group is a quotient of G) and at most three primes ramify in it. By the symmetry between the ramified primes, we can take $\{i, j, l\} = \{1, 2, 3\}$ in the rest of the proof and we will denote $k' := k \cap K_1K_2K_3$ to improve readability.

Now let K' be the genus field in the narrow sense of k', and for any $u \in \{1, 2, 3\}$, let K'_u be the maximal subfield of K' ramified only at p_u and T'_u be the inertia subgroup of $\mathrm{Gal}(K'/\mathbb{Q})$ corresponding to p_u. Then by ramification theory, we have $K'_u \subseteq K_u$, hence $T'_u \cong \mathrm{Gal}(K'_u/\mathbb{Q})$ is isomorphic to a quotient of the cyclic group $\mathrm{Gal}(K_u/\mathbb{Q}) \cong T_u$, so it must also be cyclic.

Finally note that we have $K' = K'_1K'_2K'_3 \subseteq K_1K_2K_3$ and $kK_1K_2K_3 = K$, hence $\mathrm{Gal}(K'/k') = \mathrm{Gal}(K'_1K'_2K'_3/k \cap K_1K_2K_3)$ is a quotient of

$$\mathrm{Gal}(K_1K_2K_3/k \cap K_1K_2K_3) \cong \mathrm{Gal}(K/k),$$

which is cyclic. This concludes the proof.



□

Using the results in [1] and [2], we can thus take the $\mathbb{Z}$-bases of

$$D^+(k\cap K_1K_2K_3), D^+(k\cap K_1K_2K_4), D^+(k\cap K_1K_3K_4), D^+(k\cap K_2K_3K_4)$$

and we will denote their union by B_D. Analogously, we can take the $\mathbb{Z}$-bases of

$$C^+(k\cap K_1K_2K_3), C^+(k\cap K_1K_2K_4), C^+(k\cap K_1K_3K_4), C^+(k\cap K_2K_3K_4)$$

and denote their union by B_C. Note that B_D and B_C contain the same conjugates of η_I for each $I\subsetneq\{p_1,p_2,p_3,p_4\}$, $|I|\ge 2$.

To construct a $\mathbb{Z}$-basis of D^+ (or C^+), we will take the union of B_D (or B_C, respectively) with a set B of suitably chosen conjugates of the highest generator η. In order to have a chance to obtain a $\mathbb{Z}$-basis of D^+, this set should have cardinality

$$\begin{aligned} N :&= [k:\mathbb{Q}]+4-1-|B_D| \\ &= [k:\mathbb{Q}]+3-\sum_{i,j,l}([k\cap K_iK_jK_l:\mathbb{Q}]+2) \\ &\quad+\sum_{i,j}([k\cap K_iK_j:\mathbb{Q}]+1)-\sum_i[k\cap K_i:\mathbb{Q}] \\ &= a_1a_2a_3a_4\frac{m^3}{r_1r_2r_3r_4}-\sum_{i,j,l}a_ia_ja_l\frac{m^2}{r_ir_jr_l}+\sum_{i,j}a_ia_js_{ij}\frac{m}{r_ir_j}-\sum_i a_i+1 \qquad (4.1)\end{aligned}$$

by Proposition 2.5 and Corollary 3.5, using the principle of inclusion and exclusion (due to the fact that these bases were constructed "inductively"). Note that all conjugates of η are units by Lemma 2.3, so this number N will remain the same in the case of constructing a $\mathbb{Z}$-basis of C^+. Thus we do not have to distinguish between the cases of D^+ and C^+ anymore and we can take the set B to be the same for both of them.

We cannot guarantee at the moment that the set $B_D\cup B$ (or $B_C\cup B$, respectively) is not linearly dependent, but if we will show how to obtain all the missing conjugates of η using the relations

$$R_1N_1\sim 0,\ R_2N_2\sim 0,\ R_3N_3\sim 0,\ R_4\sum_{u=0}^{n_4-1}\sigma_1^{ua_1}\sigma_2^{ua_2}\sigma_3^{ua_3}\sim 0$$

and their $\mathbb{Z}[G]$-linear combinations, it will follow that we really have a $\mathbb{Z}$-basis thanks to the discussion just above Lemma 4.1. A typical way to do that will be the following: if $R\sim 0$ for some $R\in\mathbb{Z}[G]$ and η^R is a product of conjugates of η such that we can already generate all of them except for precisely one, then we can generate the last one as well, because η^R can also be expressed as a $\mathbb{Z}$-linear combination of elements in B_C.

We will always refer to the conjugates of η by their coordinates x_1, x_2, x_3, x_4 according to Proposition 3.8. This allows us to visualise $\mathrm{Gal}(k/\mathbb{Q})$ geometrically as a discrete (at most) four-dimensional cuboid.

5. The special case $a_1 = a_2 = a_3 = r_4 = 1,\ r_1 \neq 1,\ r_2 \neq 1,\ r_3 \neq 1,$ $s_{12} = s_{13} = s_{23} = 1,\ \gcd(n_1, n_2, n_3) = 1$

In this case, we have

$$\mathrm{Gal}(k/\mathbb{Q}) \cong \{\sigma_1^{x_1}\sigma_2^{x_2}\sigma_3^{x_3}\sigma_4^{x_4}|_k; 0 \leq x_1 < n_1, 0 \leq x_2 < n_2, 0 \leq x_3 < n_3, 0 \leq x_4 < a_4\},$$
$$s_{12} = s_{13} = s_{14} = s_{23} = s_{24} = s_{34} = 1$$

and

$$N_1 \sim 0, N_2 \sim 0, N_3 \sim 0, R_4 \sum_{u=0}^{m-1} \sigma_1^u\sigma_2^u\sigma_3^u \sim 0\,.$$

The condition $r_1 \neq 1$, $r_2 \neq 1$, $r_3 \neq 1$ is actually not restrictive, since we will discuss the cases where it is not satisfied in Section 6.

Lemma 5.1. *If* $s_{12} = s_{13} = s_{23} = 1$, *the following are equivalent:*

(1) $\gcd(n_1, n_2, n_3) = 1$,

(2) $\mathrm{lcm}(r_1, r_2, r_3) = m$,

(3) $r_1r_2r_3 = m$,

(4) $n_1 = r_2r_3, n_2 = r_1r_3, n_3 = r_1r_2$,

(5) $\frac{n_1n_2n_3}{m} = m$,

(6) $\gcd(n_1, n_2) = r_3, \gcd(n_1, n_3) = r_2, \gcd(n_2, n_3) = r_1$.

Proof. This is just elementary number theory (recall that by Lemma 3.6, we have $s_{ij} = \gcd(r_i, r_j)$). □

Thus $\frac{n_1n_2n_3}{m} = m = r_2n_2 = \gcd(n_1, n_3)n_2$ by Lemma 5.1 and using Lemma 3.6, we get

$$\begin{aligned} N &= a_4n_1n_2n_3 - \frac{n_1n_2n_3}{m} - a_4(n_1n_2 + n_1n_3 + n_2n_3) - a_4 - 2 + a_4(n_1 + n_2 + n_3) \\ &\quad + \gcd(n_1, n_2) + \gcd(n_1, n_3) + \gcd(n_2, n_3) \\ &= (a_4 - 1)(n_1 - 1)(n_2 - 1)(n_3 - 1) + (n_1 - 1)(n_2 - 1)(n_3 - 2) \\ &\quad + n_1n_2 - (\gcd(n_1, n_3) + 1)n_2 - (n_1 - \gcd(n_1, n_3) - 1) \\ &\quad + \gcd(n_2, n_3) + \gcd(n_1, n_2) - 2 \\ &= (a_4 - 1)(n_1 - 1)(n_2 - 1)(n_3 - 1) + (n_1 - 1)(n_2 - 1)(n_3 - 2) \\ &\quad + (n_2 - 1)(n_1 - r_2 - 1) + r_1 + r_3 - 2. \end{aligned}$$

We will define B_5 as the set of the following N conjugates $\eta^{\sigma_1^{x_1}\sigma_2^{x_2}\sigma_3^{x_3}\sigma_4^{x_4}}$:

- $0 \leq x_1 < n_1 - 1$, $0 \leq x_2 < n_2 - 1$, $0 \leq x_3 < n_3 - 1$, $0 < x_4 \leq a_4 - 1$,
- $0 \leq x_1 < n_1 - 1$, $0 \leq x_2 < n_2 - 1$, $1 < x_3 \leq n_3 - 1$, $x_4 = 0$,
- $0 \leq x_1 < n_1 - r_2 - 1$, $0 \leq x_2 < n_2 - 1$, $x_3 = 0$, $x_4 = 0$,
- $x_1 = n_1 - r_2 - 1$, $0 \leq x_2 < r_1 + r_3 - 2$, $x_3 = 0$, $x_4 = 0$.

(Note that $n_3 = r_1r_2 \geq 4$, $n_1 - r_2 - 1 = r_2(r_3 - 1) - 1 > 0$ and $n_2 - 1 > r_1 + r_3 - 2 > 0$, since $r_1, r_2, r_3 > 1$ and $n_2 = r_1r_3$.)

First we will recover the cases $0 < x_4 < a_4$, $x_1 = n_1 - 1$ or $x_2 = n_2 - 1$ or $x_3 = n_3 - 1$ using the relations $N_1 \sim 0$, $N_2 \sim 0$, $N_3 \sim 0$. From now on, we only need to deal with the cases where $x_4 = 0$. Next, we will recover the cases $1 < x_3 \leq n_3 - 1$, $x_1 = n_1 - 1$ or $x_2 = n_2 - 1$ (and always $x_4 = 0$) using the relations $N_1 \sim 0, N_2 \sim 0$ and the cases $x_3 = x_4 = 0$, $0 \leq x_1 < n_1 - r_2 - 1$, $x_2 = n_2 - 1$ using the relation $N_2 \sim 0$.

At this moment, we are only missing all the cases with $x_3 = 1$, $x_4 = 0$ and some of those with $x_3 = x_4 = 0$. From now on, we will only focus on recovering those with $x_3 = x_4 = 0$, because once we have those, we can recover those with $x_3 = 1, x_4 = 0$ just by using the relation $N_3 \sim 0$.

From now on, we will write $\overline{z} := z \pmod{r_3}$ for any $z \in \mathbb{Z}$, hence we will always have $\overline{z} \in \{0, 1, \ldots, r_3 - 1\}$. We will also define h to be the unique integer satisfying

$$r_1 \cdot h \equiv r_2 \pmod{r_3} \quad \text{and} \quad h \in \{0, 1, \ldots, r_3 - 1\}$$

and similarly h' to be the unique integer satisfying

$$r_2 \cdot h' \equiv r_1 \pmod{r_3} \quad \text{and} \quad h' \in \{0, 1, \ldots, r_3 - 1\}$$

(both are well defined, since $\gcd(r_1, r_3) = \gcd(r_2, r_3) = 1$). Clearly $h \cdot h' \equiv 1 \pmod{r_3}$.

Let Q' be the quotient $\mathbb{Z}[G]$-module

$$D^+ / \big\langle \{\eta_I \big| \emptyset \subsetneq I \subsetneq P\} \big\rangle_{\mathbb{Z}[G]}$$

and let Q be the quotient $\mathbb{Z}$-module of Q' by the classes of conjugates we have already recovered, i.e.,

$$\begin{aligned} Q := Q' / \big\langle \{\eta^{\sigma_1^{x_1}\sigma_2^{x_2}\sigma_3^{x_3}\sigma_4^{x_4}}; \quad & 0 \leq x_1 < n_1, 0 \leq x_2 < n_2, 0 \leq x_3 < n_3, 0 < x_4 < a_4, \\ \text{or} \quad & 0 \leq x_1 < n_1, 0 \leq x_2 < n_2, 1 < x_3 < n_3, x_4 = 0, \\ \text{or} \quad & 0 \leq x_1 < n_1 - r_2 - 1, 0 \leq x_2 < n_2, x_3 = x_4 = 0, \\ \text{or} \quad & x_1 = n_1 - r_2 - 1, 0 \leq x_2 < r_1 + r_3 - 2, x_3 = x_4 = 0\} \big\rangle_{\mathbb{Z}} \end{aligned}$$

(where we denote $\eta^\rho \in D^+$ and its class in Q' in the same way for any $\rho \in G$). We will write Q additively, denoting the class of η in Q by μ, hence denoting the class of η^ρ in Q by $\rho \cdot \mu$ for any $\rho \in \mathrm{Gal}(k/\mathbb{Q})$ or $\rho \in G$. Showing that we have indeed chosen a basis now amounts to showing that Q is trivial. Since

$$0 = \sigma_1^{x_1}\sigma_2^{x_2} N_3 \cdot \mu = \sigma_1^{x_1}\sigma_2^{x_2} \cdot \mu + \sigma_1^{x_1}\sigma_2^{x_2}\sigma_3 \cdot \mu$$

for any $x_1, x_2 \in \mathbb{Z}$, this is equivalent with showing that $\sigma_1^{x_1}\sigma_2^{x_2} \cdot \mu = 0$ for each $0 \leq x_1 < n_1$, $0 \leq x_2 < n_2$.

The conjugates with $x_3 = 0$ and $x_4 = 0$ (i.e., those of the form $\eta^{\sigma_1^{x_1}\sigma_2^{x_2}}$) can be visualized as a discrete rectangle with n_1 rows and n_2 columns. Since for each x_4, there are n_3 layers of such rectangles in total, the sum $\eta^{R_4 \sum_{u=0}^{m-1} \sigma_1^u \sigma_2^u \sigma_3^u}$ must contain $\frac{m}{n_3} = r_3$ conjugates in each of these rectangles. We will now describe the sum of these.

Let

$$T := \sum_{u=0}^{r_3 - 1} \sigma_1^{un_3} \sigma_2^{un_3} .$$

Lemma 5.2. *In Q, we have*

$$\sigma_1^{x_1}\sigma_2^{x_2}(1-\sigma_1\sigma_2)T\cdot\mu=0$$

for any $x_1, x_2 \in \mathbb{Z}$.

Proof. Using the fact that every $0 \le w < m$ can be uniquely written as $un_3 + v$, where $0 \le u < r_3$, $0 \le v < n_3$, together with the fact that the order of σ_3 is n_3, we get

$$R_4T\sum_{v=0}^{n_3-1}\sigma_1^v\sigma_2^v\sigma_3^v = R_4\sum_{u=0}^{r_3-1}\sigma_1^{un_3}\sigma_2^{un_3}\sigma_3^{un_3}\cdot\sum_{v=0}^{n_3-1}\sigma_1^v\sigma_2^v\sigma_3^v = R_4\sum_{w=0}^{m-1}\sigma_1^w\sigma_2^w\sigma_3^w \sim 0\,.$$

Together with $N_3 \sim 0$, this means that

$$\begin{aligned}0 &\sim \sigma_1^{x_1}\sigma_2^{x_2}\left(R_4T\sum_{v=0}^{n_3-1}\sigma_1^v\sigma_2^v\sigma_3^v - \sigma_1\sigma_2N_3R_4T\right)\\ &= \sigma_1^{x_1}\sigma_2^{x_2}R_4T\sum_{v=0}^{n_3-1}\left(\sigma_1^v\sigma_2^v-\sigma_1\sigma_2\right)\sigma_3^v\\ &= \sigma_1^{x_1}\sigma_2^{x_2}(1-\sigma_1\sigma_2)R_4T + \sigma_1^{x_1}\sigma_2^{x_2}R_4T\sum_{v=2}^{n_3-1}\left(\sigma_1^v\sigma_2^v-\sigma_1\sigma_2\right)\sigma_3^v\\ &= \sigma_1^{x_1}\sigma_2^{x_2}(1-\sigma_1\sigma_2)T + \sigma_1^{x_1}\sigma_2^{x_2}(1-\sigma_1\sigma_2)T\sum_{u=1}^{a_4-1}\sigma_4^u\\ &\qquad + \sigma_1^{x_1}\sigma_2^{x_2}R_4T\sum_{v=2}^{n_3-1}\left(\sigma_1^v\sigma_2^v-\sigma_1\sigma_2\right)\sigma_3^v\,.\end{aligned}$$

Since all the summands in the expression

$$\sigma_1^{x_1}\sigma_2^{x_2}(1-\sigma_1\sigma_2)T\sum_{u=1}^{a_4-1}\sigma_4^u + \sigma_1^{x_1}\sigma_2^{x_2}R_4T\sum_{v=2}^{n_3-1}\left(\sigma_1^v\sigma_2^v-\sigma_1\sigma_2\right)\sigma_3^v$$

have either $x_4 > 0$ or $x_3 > 1$ (where x_3 and x_4 denote the respective exponents of σ_3 and σ_4 in each term), the result of their action on μ becomes trivial in Q, which yields the result. □

The rest of this section will again be stated purely algebraically, but perhaps it is helpful (although not strictly required) to see some of its parts geometrically.

We will decompose our rectangle (of conjugates of η having $x_3 = x_4 = 0$) into $r_3 \times r_3$ rectangular blocks of height r_2 and width r_1 in the natural way. In the following, by a big row (resp. a big column) we will understand a row of blocks (resp. columns), that is r_3 consecutive blocks next to (resp. above) each other. Since $r_2 \mid n_3$, $r_1 \mid n_3$ and the conjugates contained in η^T are given by $\eta^{\sigma_1^{qn_3}\sigma_2^{qn_3}}$ for $0 \le q \le r_3 - 1$, the Chinese remainder theorem implies that $\eta^{\sigma_1^{x_1}\sigma_2^{x_2}T}$ contains exactly one conjugate in every big row (resp. every big column) for any $0 \le x_1 < n_1$, $0 \le x_2 < n_2$, and these have the same relative position in each of the respective blocks (determined only by $\overline{r_1}, \overline{r_2}, x_1, x_2$). We can be even more precise: the horizontal distance between $\eta^{\sigma_1^{qn_3+x_1}\sigma_2^{qn_3+x_2}}$ and $\eta^{\sigma_1^{(q+1)n_3+x_1}\sigma_2^{(q+1)n_3+x_2}}$ for $0 \le q \le r_3 - 1$ and $0 \le x_1 < n_1$, $0 \le x_2 < n_2$ is exactly $\overline{r_2} \cdot r_1$, i.e., $\overline{r_2}$ blocks, and the vertical distance between them is exactly $\overline{r_1} \cdot r_2$, i.e., $\overline{r_1}$ blocks (again this follows easily from the Chinese remainder theorem). It follows that the horizontal distance between any two conjugates in η^T with a vertical distance of one block is h blocks.

For all $0 \le u \le n_2$, we will denote $X_u := \sigma_1^{n_1-2}\sigma_2^u \cdot \mu$ and $Y_u := \sigma_1^{r_2(r_3-1)-1}\sigma_2^u \cdot \mu$. By definition, X_u and Y_u are elements of Q. It will be convenient to allow any integers in the indices of the X's and Y's and regard them only modulo n_2 (to be more precise, as in the set $\{0, 1, \dots, n_2 - 1\}$). Moreover note that by definition, $Y_u = 0$ for $0 \le u < r_1 + r_3 - 2$.

Lemma 5.3. *We have $X_q = X_{q'}$ for any $q \equiv q' \pmod{r_3}$. Moreover, for any $0 \le x_1 < n_1$, $0 \le x_2 < n_2$, we have*

$$\sigma_1^{x_1}\sigma_2^{x_2} \cdot \mu = \begin{cases} 0 & \textit{if} \quad 0 \le x_1 < r_2(r_3-1) - 1\,, \\ Y_{x_2} & \textit{if} \quad x_1 = r_2(r_3-1) - 1\,, \\ X_{x_2-x_1-2} & \textit{if} \quad r_2(r_3-1) \le x_1 < n_1 - 1\,, \\ X_{x_2-x_1-2} - Y_{x_2-h\cdot r_1} & \textit{if} \quad x_1 = n_1 - 1\,. \end{cases}$$

Proof. The first part will be proven in a moment, we will now focus on the second.

The first case ($x_1 < r_2(r_3-1) - 1$) follows directly from the definition of Q and the second case ($x_1 = r_2(r_3-1) - 1$) directly from the definition of Y_{x_2}.

Now for every $0 \le u < n_2$, we will prove that

$$\sigma_1^{n_1-2-v}\sigma_2^{u-v} \cdot \mu = X_u \tag{5.1}$$

by induction with respect to $v = 0, 1, \dots, r_2 - 2$. The base step $v = 0$ is just the definition of X_u. Now suppose that $0 < v \le r_2 - 2$ and the statement holds for $v - 1$. Then in the equality

$$\left(\sigma_1^{n_1-2-v}\sigma_2^{u-v}(1 - \sigma_1\sigma_2)\sum_{w=0}^{r_3-1}\sigma_1^{wn_3}\sigma_2^{wn_3}\right) \cdot \mu = 0\,, \tag{5.2}$$

which follows from Lemma 5.2, we claim that all the terms with $w > 0$ do not contribute anything to the sum. Indeed, all the exponents of σ_1 are pairwise congruent modulo r_2 (since $r_2 \mid n_3$), and since $n_1 - r_2 \le n_1 - 2 - v < n_1 - 2$ and $n_1 - r_2 + 1 \le n_1 - 1 - v < n_1 - 1$, we have

$$\left(\sigma_1^{n_1-2-v}\sigma_2^{u-v}(1 - \sigma_1\sigma_2)\sigma_1^{wn_3}\sigma_2^{wn_3}\right) \cdot \mu = 0$$

for any $w > 0$, because r_3 does not divide wn_3 in this case. Hence (5.2) implies that

$$0 = \left(\sigma_1^{n_1-2-v}\sigma_2^{u-v}(1 - \sigma_1\sigma_2)\right) \cdot \mu = \sigma_1^{n_1-2-v}\sigma_2^{u-v} \cdot \mu - \underbrace{\sigma_1^{n_1-2-(v-1)}\sigma_2^{u-(v-1)} \cdot \mu}_{=X_u}\,,$$

therefore $\sigma_1^{n_1-2-v}\sigma_2^{u-v} \cdot \mu = X_u$ by the induction hypothesis. This completes the induction, so (5.1) holds.

Now for any $0 \leq u < n_2$, we will take $v = r_2 - 1$ in (5.2). Again, since all the exponents of σ_1 are pairwise congruent modulo r_2 (since $r_2 \mid n_3$) in this sum, the only terms which could be nonzero are those arising from $w = 0$ and from w satisfying

$$wn_3 + n_1 - 2 - (r_2 - 1) \equiv n_1 - 1 \pmod{n_1},$$

which is equivalent to $wn_3 \equiv r_2 \pmod{n_1}$, which implies $wn_3 \equiv r_2 \pmod{r_3}$. Together with $wn_3 \equiv 0 \pmod{r_1}$ and the fact that $\gcd(r_1, r_3) = 1$, this means that the only solution to the above congruence is $wn_3 \equiv h \cdot r_1 \pmod{n_2}$.

Thus we have

$$\begin{aligned} 0 &= \Big(\sigma_1^{n_1-r_2-1}\sigma_2^{u-r_2+1}(1-\sigma_1\sigma_2) + \sigma_1^{n_1-1}\sigma_2^{u-r_2+1+h\cdot r_1}(1-\sigma_1\sigma_2)\Big)\cdot\mu \\ &= \underbrace{\sigma_1^{n_1-r_2-1}\sigma_2^{u-r_2+1}\cdot\mu}_{=Y_{u-r_2+1}} - \underbrace{\sigma_1^{n_1-r_2}\sigma_2^{u-r_2+2}\cdot\mu}_{=X_u \text{ due to (5.1)}} + \sigma_1^{n_1-1}\sigma_2^{u-r_2+1+h\cdot r_1}\cdot\mu \\ &\quad - \underbrace{\sigma_1^{n_1}\sigma_2^{u-r_2+1+h\cdot r_1+1}\cdot\mu}_{=0}\,. \end{aligned}$$

Therefore

$$\sigma_1^{n_1-1}\sigma_2^{u-r_2+1+h\cdot r_1}\cdot\mu = X_u - Y_{u-r_2+1}\,. \tag{5.3}$$

Finally, for any $0 \leq u < n_2$, we will take $v = r_2$ in (5.2). Again, since all the exponents of σ_1 are pairwise congruent modulo r_2 in this sum, we only get nonzero terms for $w = 0$ and for w satisfying

$$wn_3 + n_1 - 2 - r_2 \equiv n_1 - 2 \pmod{n_1}\,,$$

which implies (because we have got the same congruence as above) $wn_3 \equiv h \cdot r_1 \pmod{n_2}$.

Thus we have

$$\begin{aligned} 0 = &\underbrace{\sigma_1^{n_1-r_2-2}\sigma_2^{u-r_2}\cdot\mu}_{=0} - \underbrace{\sigma_1^{n_1-r_2-1}\sigma_2^{u-r_2+1}\cdot\mu}_{=Y_{u-r_2+1}} \\ &+ \underbrace{\sigma_1^{n_1-2}\sigma_2^{u-r_2+h\cdot r_1}\cdot\mu}_{=X_{u-r_2+h\cdot r_1}} - \underbrace{\sigma_1^{n_1-1}\sigma_2^{u-r_2+1+h\cdot r_1}\cdot\mu}_{=X_u - Y_{u-r_2+1} \text{ due to (5.3)}}\,. \end{aligned}$$

Therefore $X_{u-r_2+h\cdot r_1} = X_u$. Note that

$$h \cdot r_1 - r_2 \equiv 0 \pmod{r_3}$$

and

$$h \cdot r_1 - r_2 \equiv -r_2 \pmod{r_1}\,.$$

Since $\gcd(-r_2, r_1) = 1$ and $n_2 = r_1 r_3$, this means that for all q, $q' \in \mathbb{Z}$ satisfying

$$q \equiv q' \pmod{r_3}\,,$$

there is some $w \in \mathbb{Z}$ such that

$$q' \equiv w(h \cdot r_1 - r_2) + q \pmod{n_2}\,.$$

Without loss of generality, we can assume that $w \geq 0$ (otherwise we can just swap q and q'). But then

$$X_q = X_{q+(h\cdot r_1 - r_2)} = X_{q+2(h\cdot r_1 - r_2)} = \cdots = X_{q+w(h\cdot r_1 - r_2)} = X_{q'}\,.$$

Now for any x_1, x_2 satisfying $r_2(r_3-1) \leq x_1 < n_1 - 1$ and $0 \leq x_2 < n_2$, denoting

$$v = n_1 - 2 - x_1\,, \quad u = v + x_2\,,$$

we get $0 \leq v \leq r_2 - 2$ and the equality (5.1) implies

$$\sigma_1^{x_1}\sigma_2^{x_2}\mu = X_{n_1-2-x_1+x_2} = X_{x_2-x_1-2}\,,$$

because $r_3 \mid n_1$.

Similarly, for $x_1 = n_1 - 1$ and any $0 \leq x_2 < n_2$, denoting $u = x_2 + r_2 - 1 - h\cdot r_1$, the equality (5.3) implies that

$$\sigma_1^{x_1}\sigma_2^{x_2}\cdot\mu = X_u - Y_{u-r_2+1} = X_{x_2-x_1-2} - Y_{x_2-h\cdot r_1}\,,$$

since

$$u = x_2 - 1 + r_2 - h\cdot r_1 \equiv x_2 - 1 \equiv x_2 - 2 + 1 - n_1 = x_2 - x_1 - 2 \pmod{r_3}$$

by definition of h and the fact that $r_3 \mid n_1$.

This concludes the proof. □

Thanks to Lemma 5.3, from now on we will regard the indices of the X's only modulo r_3. The lemma also implies the equality

$$\sigma_1^{n_1-1}\sigma_2^{x_2}\cdot\mu + \sigma_1^{n_1-r_2-1}\sigma_2^{x_2-h\cdot r_1}\cdot\mu = X_{x_2-1} - Y_{x_2-h\cdot r_1} + Y_{x_2-h\cdot r_1} = X_{x_2-1} \tag{5.4}$$

for any $x_2 \in \mathbb{Z}$, which we will use several times. Another simple observation that will come in handy in the proofs of the following lemmas is that the unary operation of adding a fixed integer induces an automorphism of $\mathbb{Z}/r_3$, which we will not mention explicitly anymore.

To show that Q is trivial, it now suffices to show that $X_u = 0$ for all $0 \leq u < r_3$ and $Y_v = 0$ for all $r_1 + r_3 - 2 \leq v < n_2$ (knowing already that $Y_v = 0$ for all $0 \leq v < r_1 + r_3 - 2$). To achieve this, we will use linear algebra.

Let

$$\alpha := Y_{r_1+r_3-2} + Y_{r_1+r_3-1} + \cdots + Y_{n_2-1} \in Q$$

and

$$\beta := X_0 + X_1 + \cdots + X_{r_3-1} \in Q\,. \tag{5.5}$$

Lemma 5.4. *We have $\alpha = \beta = 0$.*

Proof. Using the relation $N_2 \sim 0$, we have

$$0 = \sigma_1^{r_2(r_3-1)-1}N_2\cdot\mu = \sum_{x_2=0}^{n_2-1}\sigma_1^{r_2(r_3-1)-1}\sigma_2^{x_2}\cdot\mu = \sum_{x_2=0}^{n_2-1} Y_{x_2} = \alpha$$

and

$$
\begin{aligned}
0 = \sigma_1^{r_2(r_3-1)} N_2 \cdot \mu &= \sum_{x_2=0}^{n_2-1} \sigma_1^{r_2(r_3-1)} \sigma_2^{x_2} \cdot \mu = \sum_{x_2=0}^{n_2-1} X_{x_2 - r_2(r_3-1)-2} \\
&= \sum_{x_2=0}^{r_1 r_3 - 1} X_{x_2+r_2-2} = \sum_{u=0}^{r_1-1} \sum_{v=0}^{r_3-1} X_{ur_3+v+r_2-2} = r_1 \cdot \sum_{v=0}^{r_3-1} X_{v+r_2-2} = r_1 \cdot \beta \,,
\end{aligned}
$$

since each $x_2 \in \{0, 1, \dots, r_1 r_3 - 1\}$ can be uniquely written as $ur_3 + v$, where $0 \le u < r_1$, $0 \le v < r_3$.

Similarly, using Lemma 5.3 together with the relation $N_1 \sim 0$ and the equality (5.4), we get

$$
\begin{aligned}
0 &= \sum_{q=0}^{r_3-1} \sigma_2^{qr_1} N_1 \cdot \mu = \sum_{q=0}^{r_3-1} \left(\sigma_1^{n_1-1} + \sigma_1^{r_2(r_3-1)-1} \right) \sigma_2^{qr_1} \cdot \mu + \sum_{x_1=r_2(r_3-1)}^{n_1-2} \sum_{q=0}^{r_3-1} \sigma_1^{x_1} \sigma_2^{qr_1} \cdot \mu \\
&= \sum_{q=0}^{r_3-1} (\sigma_1^{n_1-1} \sigma_2^{qr_1} + \sigma_1^{r_2(r_3-1)-1} \sigma_2^{(q-h)\cdot r_1}) \cdot \mu + \sum_{x_1=r_2(r_3-1)}^{n_1-2} \sum_{q=0}^{r_3-1} \sigma_1^{x_1} \sigma_2^{qr_1} \cdot \mu \\
&= \sum_{q=0}^{r_3-1} X_{qr_1-1} + \sum_{x_1=r_2(r_3-1)}^{n_1-2} \sum_{q=0}^{r_3-1} X_{qr_1-x_1-2} = \sum_{x_1=r_2(r_3-1)}^{n_1-1} \sum_{q=0}^{r_3-1} X_{qr_1-x_1-2} = r_2 \cdot \beta \,,
\end{aligned}
$$

since for any x_1, all possible remainders modulo r_3 occur exactly once as the indices in the sum $\sum_{q=0}^{r_3-1} X_{qr_1-x_1-2}$ (due to the fact that the order of the class of r_1 is r_3 in $\mathbb{Z}/r_3$, due to their coprimality). Since $\gcd(r_1, r_2) = 1$, this implies $\beta = 0$ by Bézout's identity. □

Next, for $0 \le q \le r_3 - 3$, we will define

$$
\Gamma_q := \sum_{u=0}^{r_3-h'-1} \sum_{v=0}^{\overline{r_2}-1} X_{q+v-ur_2-1} \in Q \,. \tag{5.6}
$$

Lemma 5.5. *For any $0 \le q \le r_3 - 3$, we have $\Gamma_q = 0$.*

Proof. Using Lemma 5.3, the relation $N_1 \sim 0$ and the equality (5.4), we get

$$
\begin{aligned}
0 &= \sum_{u=0}^{r_3-h'-1} \sigma_2^{q-uhr_1} N_1 \cdot \mu \\
&= \sum_{u=0}^{r_3-h'-2} \underbrace{\left(\sigma_1^{n_1-1} \sigma_2^{q-uhr_1} + \sigma_1^{r_2(r_3-1)-1} \sigma_2^{q-(u+1)hr_1} \right) \cdot \mu}_{= X_{q-uhr_1-1} \text{ due to (5.4)}}
\end{aligned}
$$

$$+\underbrace{\sigma_1^{r_2(r_3-1)-1}\sigma_2^{q}\cdot\mu}_{=Y_q}+\underbrace{\sigma_1^{n_1-1}\sigma_2^{q-(r_3-h'-1)hr_1}\cdot\mu}_{=X_{q-(r_3-h'-1)hr_1-1}-Y_{q+r_1}}$$
$$+\sum_{x_1=r_2(r_3-1)}^{n_1-2}\ \sum_{u=0}^{r_3-h'-1}\sigma_1^{x_1}\sigma_2^{q-uhr_1}\cdot\mu\,.$$

Now we will use the fact that $q\le r_3-3\le r_1+r_3-3$ (implying $Y_q=0$) and

$$q-(r_3-h'-1)hr_1-hr_1=q-r_1r_3h+r_1hh'\equiv q+r_1\pmod{n_2}\,,$$

since the congruence holds modulo both r_1 and r_3 (and $\gcd(r_1,r_3)=1$). Also note that $Y_{q+r_1}=0$, since

$$r_1\le q+r_1\le r_1+r_3-3\,,$$

which precisely justifies the bounds on q that we used in the definition of Γ_q and also explains why the upper bound in the first sum was chosen to be $r_3-h'-1$.

Continuing with the previous equality and using Lemma 5.3 together with the congruence $hr_1\equiv r_2\pmod{r_3}$, we thus have

$$\begin{aligned}0&=\Big(\sum_{u=0}^{r_3-h'-2}X_{q-uhr_1-1}\Big)+X_{q-(r_3-h'-1)hr_1-1}+\sum_{x_1=r_2(r_3-1)}^{n_1-2}\ \sum_{u=0}^{r_3-h'-1}X_{q-uhr_1-x_1-2}\\&=\sum_{u=0}^{r_3-h'-1}X_{q-ur_2-1}+\sum_{x_1=r_2(r_3-1)}^{n_1-2}\ \sum_{u=0}^{r_3-h'-1}X_{q-ur_2-x_1-2}\\&=\sum_{x_1=r_2(r_3-1)}^{n_1-1}\ \sum_{u=0}^{r_3-h'-1}X_{q-ur_2-x_1-2}\,.\end{aligned}$$

After using the substitution $v=n_1-1-x_1$, this becomes

$$\begin{aligned}0&=\sum_{u=0}^{r_3-h'-1}\sum_{v=0}^{r_2-1}X_{q+v-ur_2-1}\\&=\sum_{u=0}^{r_3-h'-1}\Big(\sum_{v=0}^{\overline{r_2}-1}X_{q+v-ur_2-1}+\sum_{v=\overline{r_2}}^{r_2-1}X_{q+v-ur_2-1}\Big)\\&=\sum_{u=0}^{r_3-h'-1}\sum_{v=0}^{\overline{r_2}-1}X_{q+v-ur_2-1}+\sum_{u=0}^{r_3-h'-1}\frac{r_2-\overline{r_2}}{r_3}\sum_{v=\overline{r_2}}^{\overline{r_2}+r_3-1}X_{q+v-ur_2-1}\\&=\Gamma_q+\sum_{u=0}^{r_3-h'-1}\frac{r_2-\overline{r_2}}{r_3}\cdot\beta\,,\end{aligned}$$

which equals Γ_q since $\beta=0$ by Lemma 5.4. □

Finally, let

$$\Delta := \sum_{u=0}^{r_3-1} u \cdot \sum_{v=0}^{\overline{r_2}-1} \sum_{w=0}^{\overline{r_1}-1} X_{v+w-ur_2-1} \in Q\,. \tag{5.7}$$

Lemma 5.6. *We have* $\Delta = 0$.

Proof. Using Lemma 5.3, the relation $N_1 \sim 0$ and the equality (5.4), we get

$$\begin{aligned}
0 &= \sum_{u=0}^{r_3-1} u \cdot \sum_{x_2=0}^{r_1-1} \sigma_2^{x_2-uhr_1} N_1 \cdot \mu \\
&= \sum_{u=0}^{r_3-1} u \cdot \sum_{x_2=0}^{r_1-1} \left(\sigma_1^{n_1-1}\sigma_2^{x_2-uhr_1} + \sigma_1^{r_2(r_3-1)-1}\sigma_2^{x_2-uhr_1}\right) \cdot \mu \\
&\quad + \sum_{u=0}^{r_3-1} u \cdot \sum_{x_1=r_2(r_3-1)}^{n_1-2} \sum_{x_2=0}^{r_1-1} \sigma_1^{x_1}\sigma_2^{x_2-uhr_1} \cdot \mu \\
&= \sum_{u=0}^{r_3-2} \sum_{x_2=0}^{r_1-1} \left(u \cdot \underbrace{\sigma_1^{n_1-1}\sigma_2^{x_2-uhr_1} \cdot \mu}_{=X_{x_2-uhr_1-1}-Y_{x_2-(u+1)hr_1}} + (u+1) \cdot \underbrace{\sigma_1^{r_2(r_3-1)-1}\sigma_2^{x_2-(u+1)hr_1} \cdot \mu}_{=Y_{x_2-(u+1)hr_1}} \right) \\
&\quad + \sum_{x_2=0}^{r_1-1} (r_3-1) \cdot \underbrace{\sigma_1^{n_1-1}\sigma_2^{x_2-(r_3-1)hr_1} \cdot \mu}_{=X_{x_2-(r_3-1)hr_1-1}-Y_{x_2-hr_1r_3}} \\
&\quad + \sum_{u=0}^{r_3-1} u \cdot \sum_{x_1=r_2(r_3-1)}^{n_1-2} \sum_{x_2=0}^{r_1-1} \sigma_1^{x_1}\sigma_2^{x_2-uhr_1} \cdot \mu\,.
\end{aligned}$$

Since

$$x_2 - hr_1r_3 \equiv x_2 \pmod{n_2}$$

and $0 \le x_2 < r_1$, we have $Y_{x_2-hr_1r_3} = 0$. Also note that for any $r_1 \le q < n_2$, there exist unique

$$u \in \{0, 1, \ldots, r_3-2\}, x_2 \in \{0, 1, \ldots, r_1-1\}$$

such that

$$q \equiv x_2 - (u+1)hr_1 \pmod{n_2}$$

by the Chinese remainder theorem, since $\gcd(h, r_3) = 1$ and for $u = r_3 - 1$, we would get $q \equiv x_2 \pmod{n_2}$ and $0 \le x_2 < r_1$. Thus we get a bijection

$$\{0, 1, \ldots, r_3-2\} \times \{0, 1, \ldots, r_1-1\} \to \{r_1, r_1+1, \ldots, n_2-1\}\,,$$

which we will use in a moment to transform a double sum into a simple one.

Continuing with the above equality and using the congruence $hr_1 \equiv r_2 \pmod{r_3}$, we thus have

$$\begin{aligned}
0 &= \sum_{u=0}^{r_3-2}\sum_{x_2=0}^{r_1-1} u\cdot X_{x_2-ur_2-1} + \sum_{u=0}^{r_3-2}\sum_{x_2=0}^{r_1-1} Y_{x_2-(u+1)hr_1} + \underbrace{\sum_{q=0}^{r_1-1} Y_q}_{=0} \\
&\quad + \sum_{x_2=0}^{r_1-1}(r_3-1)\cdot X_{x_2-(r_3-1)r_2-1} + \sum_{u=0}^{r_3-1} u\cdot \sum_{x_1=r_2(r_3-1)}^{n_1-2}\sum_{x_2=0}^{r_1-1} X_{x_2-ur_2-x_1-2} \\
&= \sum_{u=0}^{r_3-1}\sum_{x_2=0}^{r_1-1} u\cdot X_{x_2-ur_2-1} + \underbrace{\sum_{q=r_1}^{n_2-1} Y_q + \sum_{q=0}^{r_1-1} Y_q}_{=\alpha} \\
&\quad + \sum_{u=0}^{r_3-1} u\cdot \sum_{x_1=r_2(r_3-1)}^{n_1-2}\sum_{x_2=0}^{r_1-1} X_{x_2-ur_2-x_1-2} \\
&= \alpha + \sum_{u=0}^{r_3-1} u\cdot \sum_{x_1=r_2(r_3-1)}^{n_1-1}\sum_{x_2=0}^{r_1-1} X_{x_2-ur_2-x_1-2}.
\end{aligned}$$

After using the equality $\alpha = 0$ by Lemma 5.4 and the substitutions $v = n_1-1-x_1$, $w = x_2$, this becomes

$$\begin{aligned}
0 &= \sum_{u=0}^{r_3-1} u\cdot \sum_{v=0}^{r_2-1}\sum_{w=0}^{r_1-1} X_{v+w-ur_2-1} \\
&= \sum_{u=0}^{r_3-1} u\cdot \sum_{v=0}^{r_2-1}\Big(\sum_{w=0}^{\overline{r_1}-1} X_{v+w-ur_2-1} + \sum_{w=\overline{r_1}}^{r_1-1} X_{v+w-ur_2-1}\Big) \\
&= \sum_{u=0}^{r_3-1} u\cdot \sum_{w=0}^{\overline{r_1}-1}\sum_{v=0}^{r_2-1} X_{v+w-ur_2-1} + \sum_{u=0}^{r_3-1} u\cdot \sum_{v=0}^{r_2-1} \frac{r_1-\overline{r_1}}{r_3}\cdot\beta.
\end{aligned}$$

Using the fact that $\beta = 0$ by Lemma 5.4, this equals

$$\begin{aligned}
&\sum_{u=0}^{r_3-1} u\cdot \sum_{w=0}^{\overline{r_1}-1}\sum_{v=0}^{r_2-1} X_{v+w-ur_2-1} \\
&= \sum_{u=0}^{r_3-1} u\cdot \sum_{w=0}^{\overline{r_1}-1}\Big(\sum_{v=0}^{\overline{r_2}-1} X_{v+w-ur_2-1} + \sum_{v=\overline{r_2}}^{r_2-1} X_{v+w-ur_2-1}\Big) \\
&= \Delta + \sum_{u=0}^{r_3-1} u\cdot \sum_{w=0}^{\overline{r_1}-1} \frac{r_2-\overline{r_2}}{r_3}\cdot\beta\,,
\end{aligned}$$

which equals Δ again by $\beta = 0$. □

Now let $\mathcal{X}$ be the free $\mathbb{Z}$-module with generators $\widehat{X}_0, \widehat{X}_1, \ldots, \widehat{X}_{r_3-1}$. Analogously to the definitions (5.5), (5.6), (5.7), we will define

$$\begin{aligned}\widehat{\beta} &:= \widehat{X}_0 + \widehat{X}_1 + \cdots + \widehat{X}_{r_3-1} \in \mathcal{X}\,, \\ \widehat{\Gamma}_q &:= \sum_{u=0}^{r_3-h'-1} \sum_{v=0}^{\overline{r_2}-1} \widehat{X}_{\overline{q+v-ur_2-1}} \in \mathcal{X}\,, \\ \widehat{\Delta} &:= \sum_{u=0}^{r_3-1} u \cdot \sum_{v=0}^{\overline{r_2}-1} \sum_{w=0}^{\overline{r_1}-1} \widehat{X}_{\overline{v+w-ur_2-1}} \in \mathcal{X}\end{aligned}$$

for all $0 \leq q \leq r_3 - 3$. Also let $\psi\colon \mathcal{X} \to Q$ be the $\mathbb{Z}$-module homomorphism satisfying $\psi(\widehat{X}_u) = X_u$ for all $0 \leq u < r_3$ (since $\mathcal{X}$ is free, this is well defined and determines ψ uniquely). Then for all $0 \leq q \leq r_3 - 3$, it's clear by Lemmas 5.4, 5.5 and 5.6 that

$$\psi(\widehat{\beta}) = \beta = 0, \quad \psi(\widehat{\Gamma}_q) = \Gamma_q = 0, \quad \psi(\widehat{\Delta}) = \Delta = 0\,,$$

hence

$$\widehat{\beta},\ \widehat{\Gamma}_q,\ \widehat{\Delta} \in \ker\psi\,. \tag{5.8}$$

Since $\mathcal{X}$ is free, each of its elements can be expressed as $\sum_{c=0}^{r_3-1} c_u \widehat{X_u}$ for a unique r_3-tuple of integer coefficients $(c_0, c_1, \ldots, c_{r_3-1})$. Using this correspondence, we will now construct a matrix M with integer entries of size $r_3 \times r_3$ (indexing its dimensions from 0 to $r_3 - 1$) as follows:

- The 0-th row will correspond to the coefficients of $\widehat{\beta}$ (i.e., it will consist of all 1's).
- The q-th row for $1 \leq q \leq r_3 - 2$ will correspond to the coefficients of $\widehat{\Gamma}_{q-1}$.
- The $(r_3 - 1)$-th row will correspond to the coefficients of $\widehat{\Delta}$.

By the definition of M, we have

$$M \cdot \begin{pmatrix} \widehat{X}_0 \\ \widehat{X}_1 \\ \widehat{X}_2 \\ \widehat{X}_3 \\ \vdots \\ \widehat{X}_{r_3-2} \\ \widehat{X}_{r_3-1} \end{pmatrix} = \begin{pmatrix} \widehat{\beta} \\ \widehat{\Gamma}_0 \\ \widehat{\Gamma}_1 \\ \widehat{\Gamma}_2 \\ \vdots \\ \widehat{\Gamma}_{r_3-3} \\ \widehat{\Delta} \end{pmatrix} \tag{5.9}$$

We need to show that M is unimodular, i.e., invertible over $\mathbb{Z}$, from which it will follow that $\ker\psi = \mathcal{X}$, and consequently $X_u = 0$ for all $0 \leq u < r_3$. To achieve that, we will study the effect of multiplying M by a character matrix (i.e., basically performing the discrete Fourier transform). But first we will need two technical lemmas, which will prove useful in a while.

Let

$$R(x) := \sum_{q=0}^{r_3-1} x^q \in \mathbb{Z}[x]\,,$$

$$D(x) := \sum_{q=0}^{r_3-1} q \cdot x^q \in \mathbb{Z}[x]\,,$$

$$P(x) := -x^{r_2-1} \cdot \sum_{q=0}^{r_1-1} x^q \in \mathbb{Z}[x]\,.$$

Lemma 5.7. *Let $\zeta \neq 1$ be any r_3-th root of unity. Then we have $R(\zeta) = 0$ and*

$$D(\zeta) \cdot (\zeta - 1) = r_3\,.$$

Proof. The first assertion is immediate since $R(\zeta) \cdot (\zeta - 1) = \zeta^{r_3} - 1 = 0$, but $\zeta \neq 1$. The second follows from the computation

$$\begin{aligned} D(\zeta) \cdot (\zeta - 1) &= \sum_{q=1}^{r_3-1} q \cdot \zeta^{q+1} - \sum_{q=1}^{r_3-1} q \cdot \zeta^q = \sum_{q=2}^{r_3} (q-1) \cdot \zeta^q - \sum_{q=1}^{r_3-1} q \cdot \zeta^q \\ &= (r_3 - 1)\zeta^{r_3} + \sum_{q=1}^{r_3-1} (q-1) \cdot \zeta^q - \sum_{q=1}^{r_3-1} q \cdot \zeta^q \\ &= r_3 - 1 - \sum_{q=1}^{r_3-1} \zeta^q \\ &= r_3 - R(\zeta) = r_3\,. \end{aligned}$$

□

Lemma 5.8. *For any positive integer b and $y \in \mathbb{C}$, we have the equality*

$$(y-1) \cdot \sum_{u=1}^{b} u \cdot y^u = (b+1)y^{b+1} - \sum_{u=0}^{b} y^{u+1}\,.$$

Proof. We have

$$\begin{aligned} (y-1) \cdot \sum_{u=1}^{b} u \cdot y^u &= \sum_{u=1}^{b} u \cdot y^{u+1} - \sum_{u=1}^{b} u \cdot y^u \\ &= \sum_{u=0}^{b} u \cdot y^{u+1} - \sum_{u=0}^{b-1} (u+1) \cdot y^{u+1} \\ &= b \cdot y^{b+1} + \sum_{u=0}^{b-1} \big(u - (u+1)\big) \cdot y^{u+1} \\ &= (b+1)y^{b+1} - \sum_{u=0}^{b} y^{u+1}\,. \end{aligned}$$

□

Now let ζ be any r_3-th root of unity and consider the $\mathbb{Z}$-module homomorphism from $\mathcal{X}$ to the cyclotomic field $\mathbb{Q}(\zeta)$ given by

$$\sum_{u=0}^{r_3-1} c_u \widehat{X}_u \mapsto \sum_{u=0}^{r_3-1} c_u \zeta^u$$

(since $\mathcal{X}$ is free, this is well defined and determines the homomorphism uniquely). We can apply this homomorphism to $\widehat{\beta}$, $\widehat{\Gamma_q}$, $\widehat{\Delta}$ for any $0 \leq q \leq r_3 - 3$, and we will denote its respective values on these elements by $\beta(\zeta)$, $\Gamma_q(\zeta)$, $\Delta(\zeta) \in \mathbb{Q}(\zeta)$. Note that since $\zeta^{r_3} = 1$, we have $\zeta^u = \zeta^{\overline{u}}$ for any $u \in \mathbb{Z}$.

Lemma 5.9. *Let $\zeta \neq 1$ be any r_3-th root of unity. Then for all $0 \leq q < r_3 - 3$, we have*

$$\beta(\zeta) = 0\,,$$
$$\Gamma_q(\zeta) = \zeta^q \cdot P(\zeta)$$

and

$$\Delta(\zeta) = D(\zeta) \cdot P(\zeta)\,.$$

Proof. Note that $\zeta^{-r_2} \neq 1$, since $\gcd(r_3, -r_2) = 1$ and $\zeta \neq 1$.

From the definitions and Lemma 5.7, we directly get $\beta(\zeta) = R(\zeta) = 0$. For the second assertion, we have

$$\begin{aligned}
\Gamma_q(\zeta) &= \sum_{u=0}^{r_3-h'-1} \sum_{v=0}^{\overline{r_2}-1} \zeta^{\overline{q+v-ur_2-1}} \\
&= \zeta^{q-1} \cdot \sum_{v=0}^{\overline{r_2}-1} \zeta^v \sum_{u=0}^{r_3-h'-1} \zeta^{-ur_2} \\
&= \zeta^{q-1} \cdot \frac{\zeta^{\overline{r_2}} - 1}{\zeta - 1} \cdot \frac{\zeta^{-(r_3-h')r_2} - 1}{\zeta^{-r_2} - 1} \\
&= \zeta^{q-1} \cdot \frac{\zeta^{r_2} - 1}{\zeta^{-r_2} - 1} \cdot \frac{\zeta^{r_1} - 1}{\zeta - 1} \\
&= \zeta^q \cdot P(\zeta)\,.
\end{aligned}$$

Similarly, using Lemma 5.8 with $y = \zeta^{-r_2}$ and $b = r_3 - 1$, we can see that

$$\begin{aligned}
\Delta(\zeta) &= \sum_{u=0}^{r_3-1} u \cdot \sum_{v=0}^{\overline{r_2}-1} \sum_{w=0}^{\overline{r_1}-1} \zeta^{\overline{v+w-ur_2-1}} \\
&= \zeta^{-1} \cdot \sum_{v=0}^{\overline{r_2}-1} \zeta^v \sum_{w=0}^{\overline{r_1}-1} \zeta^w \sum_{u=0}^{r_3-1} u \cdot \zeta^{-ur_2} \\
&= \zeta^{-1} \cdot \frac{\zeta^{\overline{r_2}} - 1}{\zeta - 1} \cdot \frac{\zeta^{\overline{r_1}} - 1}{\zeta - 1} \cdot \frac{r_3 \zeta^{-r_2 r_3} - \sum_{u=0}^{r_3-1} \zeta^{-r_2(u+1)}}{\zeta^{-r_2} - 1}
\end{aligned}$$

$$\begin{aligned}
&= \zeta^{-1} \cdot \frac{\zeta^{\overline{r_2}} - 1}{\zeta - 1} \cdot \frac{\zeta^{\overline{r_1}} - 1}{\zeta - 1} \cdot \frac{r_3 - \zeta^{-r_2} \cdot R(\zeta^{-r_2})}{\zeta^{-r_2} - 1} \\
&= \zeta^{-1} \cdot \frac{\zeta^{r_2} - 1}{\zeta - 1} \cdot \frac{\zeta^{r_1} - 1}{\zeta - 1} \cdot \frac{r_3}{\zeta^{-r_2} - 1} \\
&= \zeta^{-1} \cdot \frac{r_3}{\zeta - 1} \cdot \frac{\zeta^{r_2} - 1}{\zeta^{-r_2} - 1} \cdot \frac{\zeta^{r_1} - 1}{\zeta - 1} \\
&= D(\zeta) \cdot P(\zeta)
\end{aligned}$$

by Lemma 5.7. □

Proposition 5.10. *M is unimodular.*

Proof. Let ζ_{r_3} be a primitive r_3-th root of unity and let C be the corresponding $r_3 \times r_3$ character matrix, i.e., $C = (\zeta_{r_3}^{r \cdot c})_{0 \le r, c < r_3}$. We will use the two previous lemmas together with the fact that multiplying a column of successive powers of ζ_{r_3} by a row of M from the left corresponds to evaluating the polynomial obtained from this row at ζ_{r_3}. Hence we have $M \cdot C = C'$, where $C'_{0,0} = R(1) = r_3$ and the c-th column of C' is

$$\begin{pmatrix} R(\zeta_{r_3}^c) \\ P(\zeta_{r_3}^c) \\ \zeta_{r_3}^c \cdot P(\zeta_{r_3}^c) \\ (\zeta_{r_3}^c)^2 \cdot P(\zeta_{r_3}^c) \\ \vdots \\ (\zeta_{r_3}^c)^{r_3-3} \cdot P(\zeta_{r_3}^c) \\ D(\zeta_{r_3}^c) \cdot P(\zeta_{r_3}^c) \end{pmatrix} = \begin{pmatrix} 0 \\ P(\zeta_{r_3}^c) \\ \zeta_{r_3}^c \cdot P(\zeta_{r_3}^c) \\ \zeta_{r_3}^{2c} \cdot P(\zeta_{r_3}^c) \\ \vdots \\ \zeta_{r_3}^{(r_3-3)c} \cdot P(\zeta_{r_3}^c) \\ D(\zeta_{r_3}^c) \cdot P(\zeta_{r_3}^c) \end{pmatrix}$$

for any $0 < c < r_3$ (we don't need to specify the rest of the 0-th column, since it doesn't influence the determinant of C'). Thus by taking out $P(\zeta_{r_3}^c)$ from each of these columns, we get (using that multiplication by r_1 is an automorphism of $\mathbb{Z}/r_3$, since $\gcd(r_1, r_3) = 1$)

$$\begin{aligned}
|\det C'| &= |\det C''| \cdot \Big| \prod_{0<c<r_3} P(\zeta_{r_3}^c) \Big| \\
&= |\det C''| \cdot \Big| \prod_{0<c<r_3} -\zeta_{r_3}^{c(r_2-1)} \Big| \cdot \Big| \prod_{0<c<r_3} \frac{\zeta_{r_3}^{cr_1} - 1}{\zeta_{r_3}^c - 1} \Big| \\
&= |\det C''|,
\end{aligned}$$

where

$$C'' = \begin{pmatrix} r_3 & 0 & \dots & 0 & \dots & 0 \\ * & 1 & \dots & 1 & \dots & 1 \\ * & \zeta_{r_3} & \dots & \zeta_{r_3}^{c} & \dots & \zeta_{r_3}^{r_3-1} \\ * & \zeta_{r_3}^{2} & \dots & \zeta_{r_3}^{2c} & \dots & \zeta_{r_3}^{2(r_3-1)} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ * & \zeta_{r_3}^{r_3-3} & \dots & \zeta_{r_3}^{(r_3-3)c} & \dots & \zeta_{r_3}^{(r_3-3)(r_3-1)} \\ * & D(\zeta_{r_3}) & \dots & D(\zeta_{r_3}^{c}) & \dots & D(\zeta_{r_3}^{r_3-1}) \end{pmatrix}.$$

On the other hand, we can take the matrix C, add all of its rows to the (r_3-1)-th one (thus creating $\begin{pmatrix} r_3 & 0 & 0 & \dots & 0 \end{pmatrix}$ there) and then, using the equality

$$-\zeta_{r_3}^{(r_3-2)c} + \sum_{u=0}^{r_3-3} (u - r_3 + 1) \cdot \zeta_{r_3}^{uc} = \sum_{u=0}^{r_3-1} u \cdot \zeta_{r_3}^{uc} - (r_3-1) \cdot \underbrace{\sum_{u=0}^{r_3-1} \zeta_{r_3}^{uc}}_{=0},$$

multiply the (r_3-2)-th row by -1 and add the u-th row multiplied by $(u - r_3 + 1)$ for each $0 \leq u \leq r_3 - 3$, so that the (r_3-2)-th row will become

$$\begin{pmatrix} * & D(\zeta_{r_3}) & \dots & D(\zeta_{r_3}^{c}) & \dots & D(\zeta_{r_3}^{r_3-1}) \end{pmatrix}.$$

Thus we will obtain a matrix with the same determinant as C'' (up to a sign). Since the elementary row operations preserve the determinant up to a sign, it follows that

$$|\det C| = |\det C''| = |\det C'| = |\det M| \cdot |\det C|.$$

Now, C can be seen as a special type of a Vandermonde matrix, so we have

$$\det C = \prod_{0 \leq r < c < r_3} (\zeta_{r_3}^{r} - \zeta_{r_3}^{c}) \neq 0$$

(in fact it is well known that $|\det C| = \sqrt{r_3^{r_3}}$), which implies that $|\det M| = 1$, as needed. □

Corollary 5.11. *We have $X_u = 0$ for all $0 \leq q < r_3$.*

Proof. Let M^{-1} be the inverse matrix to M. By Proposition 5.10, it exists and it has integer entries. From the equation (5.9), it then follows that

$$\begin{pmatrix} \widehat{X}_0 \\ \widehat{X}_1 \\ \widehat{X}_2 \\ \widehat{X}_3 \\ \vdots \\ \widehat{X}_{r_3-2} \\ \widehat{X}_{r_3-1} \end{pmatrix} = M^{-1} \cdot \begin{pmatrix} \widehat{\beta} \\ \widehat{\Gamma}_0 \\ \widehat{\Gamma}_1 \\ \widehat{\Gamma}_2 \\ \vdots \\ \widehat{\Gamma}_{r_3-3} \\ \widehat{\Delta} \end{pmatrix},$$

which implies that $\widehat{\beta}$, $\widehat{\Gamma}_0$, $\widehat{\Gamma}_1, \dots, \widehat{\Gamma}_{r_3-3}, \widehat{\Delta}$ generate $\mathcal{X}$. But all of these elements lie in $\ker \psi$ by (5.8), hence $\ker \psi = \mathcal{X}$ and ψ is the zero homomorphism. On the other hand, we know that the image of ψ is generated by $X_0, X_1, \ldots, X_{r_3-1}$ by the definition of ψ, so all of these must be zero as well. □

Corollary 5.12. *We have $Y_u = 0$ for all $r_1 + r_3 - 2 \leq u < n_2$.*

Proof. By the Chinese remainder theorem, it suffices to show by induction with respect to $u = 0, 1, \ldots, r_3 - 1$ that for any $0 \leq v < r_1$, we have $Y_{v-uhr_1} = 0$. The base case $u = 0$ follows directly from the definition of Y_u. Now suppose the statement is true for a given $0 \leq u < r_3 - 1$. Then using $N_1 \sim 0$ and Lemma 5.3, we get

$$\begin{aligned} 0 = \sigma_2^{v-uhr_1} N_1 \cdot \mu &= \sum_{x_1=r_2(r_3-1)-1}^{n_1-1} \sigma_1^{x_1} \sigma_2^{v-uhr_1} \cdot \mu \\ &= \underbrace{Y_{v-uhr_1}}_{=0} - Y_{v-uhr_1-hr_1} + \sum_{x_1=r_2(r_3-1)}^{n_1-1} \underbrace{X_{v-uhr_1-x_1-2}}_{=0} = -Y_{v-(u+1)hr_1} \end{aligned}$$

by the induction hypothesis and by Corollary 5.11. This completes the induction. □

By Lemma 5.3, it now follows that Q is trivial, so we have proven the following theorem for the set B_5 defined on page 232:

Theorem 5.13. *Under Assumption 3.1, if*

$a_1 = a_2 = a_3 = r_4 = 1, r_1 \neq 1, r_2 \neq 1, r_3 \neq 1, s_{12} = s_{13} = s_{23} = 1, \gcd(n_1, n_2, n_3) = 1,$

then the set $B_5 \cup B_D$ forms a basis of D^+ and the set $B_5 \cup B_C$ forms a basis of C^+.

6. Four more special cases

In a similar, although less technical way, a $\mathbb{Z}$-basis of D^+ and C^+ can be constructed in another four cases, as given below. The details can be found in [6].

Theorem 6.1. *Under Assumption 3.1, if $r_1 = r_2 = r_3 = r_4 = 1$, then the set $B_1 \cup B_D$ forms a basis of D^+ and the set $B_1 \cup B_C$ forms a basis of C^+, where B_1 is the set of the following conjugates $\eta^{\sigma_1^{x_1}\sigma_2^{x_2}\sigma_3^{x_3}\sigma_4^{x_4}}$:*

- $0 \leq x_1 < a_1 m - 1$, $0 \leq x_2 < a_2 m - 1$, $0 \leq x_3 < a_3 m - 1$, $1 \leq x_4 < a_4$,
- $0 \leq x_1 < a_1 m - 1$, $0 \leq x_2 < a_2(m-1) - 1$, $0 \leq x_3 < a_3 m - 1$, $x_4 = 0$,
- $0 \leq x_1 < a_1 - 1$, $x_2 = a_2(m-1) - 1$, $0 \leq x_3 < a_3 m - 1$, $x_4 = 0$,
- $x_1 = a_1 - 1$, $x_2 = a_2(m-1) - 1$, $0 \leq x_3 < a_3(m-1)$, $x_4 = 0$.

Theorem 6.2. *Under Assumption 3.1, if $r_1 = r_2 = a_3 = r_4 = 1$, then the set $B_2 \cup B_D$ forms a basis of D^+ and the set $B_2 \cup B_C$ forms a basis of C^+, where B_2 is the set of the following conjugates $\eta^{\sigma_1^{x_1}\sigma_2^{x_2}\sigma_3^{x_3}\sigma_4^{x_4}}$:*

- $0 \leq x_1 < a_1 m - 1$, $0 \leq x_2 < a_2 m - 1$, $0 \leq x_3 < n_3 - 1$, $1 \leq x_4 < a_4$,
- $0 \leq x_1 < a_1 m - 1$, $0 \leq x_2 < a_2(m-1) - 1$, $1 \leq x_3 < n_3$, $x_4 = 0$,
- $0 \leq x_1 < a_1$, $x_2 = a_2(m-1) - 1$, $1 \leq x_3 < n_3$, $x_4 = 0$.

Theorem 6.3. *Under Assumption 3.1, if $a_1 = a_2 = r_3 = r_4 = 1$, then the set $B_3 \cup B_D$ forms a basis of D^+ and the set $B_3 \cup B_C$ forms a basis of C^+, where B_3 is the set of the following conjugates $\eta^{\sigma_1^{x_1}\sigma_2^{x_2}\sigma_3^{x_3}\sigma_4^{x_4}}$:*

- $0 \leq x_1 < n_1 - 1$, $0 \leq x_2 < n_2 - 1$, $0 \leq x_3 < a_3 m - 1$, $0 < x_4 \leq a_4 - 1$,
- $0 \leq x_1 < n_1 - 1$, $0 \leq x_2 < n_2 - 1$, $a_3 < x_3 < a_3 m$, $x_4 = 0$,
- $1 \leq x_1 < \gcd(n_1, n_2)$, $x_2 = 0$, $x_3 = 0$, $x_4 = 0$.

Theorem 6.4. *Under Assumption 3.1, if*

$$a_1 = a_2 = a_3 = r_4 = 1, \gcd(n_1, n_2, n_3) = \gcd(n_1, n_2)\,,$$

then the set $B_4 \cup B_D$ forms a basis of D^+ and the set $B_4 \cup B_C$ forms a basis of C^+, where B_4 is the set of the following N conjugates $\eta^{\sigma_1^{x_1}\sigma_2^{x_2}\sigma_3^{x_3}\sigma_4^{x_4}}$:

- $0 \leq x_1 < n_1 - 1$, $0 \leq x_2 < n_2 - 1$, $0 \leq x_3 < n_3 - 1$, $0 < x_4 \leq a_4 - 1$,
- $0 \leq x_1 < n_1 - 1$, $0 \leq x_2 < n_2 - 1$, $1 < x_3 \leq n_3 - 1$, $x_4 = 0$,
- $1 \leq x_1 < n_1$, $\gcd(n_2, n_3) \leq x_2 < n_2$, $x_3 = 0$, $x_4 = 0$,
- $\gcd(n_1, n_3) \leq x_1 < n_1$, $1 \leq x_2 < \gcd(n_2, n_3)$, $x_3 = 0$, $x_4 = 0$,
- $1 \leq x_1 < \gcd(n_1, n_2)$, $x_2 = 0$, $x_3 = 0$, $x_4 = 0$.

7. The module of relations

In this section, we will study the relations between the generators of the group of circular numbers more abstractly, following the approach in [2]. Sometimes we will only state the results and just outline the proofs or even omit them altogether.

Consider the (additively written) $\mathbb{Z}[G]$-module

$$\begin{aligned}\mathcal{X} := &\bigoplus_{\emptyset \subsetneq I \subseteq \{1,2,3,4\}} \mathbb{Z}[\mathrm{Gal}(k \cap \prod_{i \in I} K_i)/\mathbb{Q})] \\ = &\,\mathbb{Z}[\mathrm{Gal}(k/\mathbb{Q})] \oplus \bigoplus_{i,j,l} \mathbb{Z}[\mathrm{Gal}(k \cap K_i K_j K_l)/\mathbb{Q})] \\ &\oplus \bigoplus_{i,j} \mathbb{Z}[\mathrm{Gal}(k \cap K_i K_j)/\mathbb{Q})] \oplus \bigoplus_{i} \mathbb{Z}[\mathrm{Gal}(k \cap K_i)/\mathbb{Q})]\,,\end{aligned}$$

where G acts on each summand via restriction. For any $\emptyset \subsetneq I \subseteq \{1, 2, 3, 4\}$, we will denote x_I the element of $\mathcal{X}$ having all coordinates zero except for 1 at the position corresponding to I. To simplify the notation, we will sometimes write simply

$$x := x_{\{1,2,3,4\}}, x_{ijl} := x_{\{i,j,l\}}, x_{ij} := x_{\{i,j\}}, x_i := x_{\{i\}}$$

and similarly

$$\eta_{ijl} := \eta_{\{p_i,p_j,p_l\}}, \eta_{ij} := \eta_{\{p_i,p_j\}}, \eta_i := \eta_{\{p_i\}}\,.$$

Therefore we have

$$\mathcal{X} = \langle x, x_{123}, x_{124}, x_{134}, x_{234}, x_{12}, x_{13}, x_{14}, x_{23}, x_{24}, x_{34}, x_1, x_2, x_3, x_4 \rangle_{\mathbb{Z}[G]}$$

and

$$D^+ = \langle \eta, \eta_{123}, \eta_{124}, \eta_{134}, \eta_{234}, \eta_{12}, \eta_{13}, \eta_{14}, \eta_{23}, \eta_{24}, \eta_{34}, \eta_1, \eta_2, \eta_3, \eta_4 \rangle_{\mathbb{Z}[G]}\,.$$

Since

$$\eta \in k, \quad \eta_{ijl} \in k \cap K_i K_j K_l\,, \quad \eta_{ij} \in k \cap K_i K_j \quad \text{and} \quad \eta_i \in k \cap K_i\,,$$

this gives us a surjective homomorphism of $\mathbb{Z}[G]$-modules $\varphi\colon \mathcal{X} \to D^+$ defined by

$$\varphi(x) = \eta\,, \quad \varphi(x_{ijl}) = \eta_{ijl}\,, \quad \varphi(x_{ij}) = \eta_{ij}\,, \quad \varphi(x_i) = \eta_i\,.$$

Then $\ker\varphi$ is a $\mathbb{Z}[G]$-submodule of $\mathcal{X}$, and we will call it *the module of relations* of k, because we can regard its elements as the relations between the generators of the group of circular numbers of k.

Lemmas 2.3 and 2.6 imply that for any $I \subseteq \{1,2,3,4\}$, $|I| \geq 2$ and $i \in I$, we have

$$\mathrm{N}_{k\cap\prod\limits_{u\in I} K_u/k\cap\prod\limits_{u\in I\setminus\{i\}} K_u}\ \varphi(x_I) \in C^+\left(k \cap \prod_{u\in I\setminus\{i\}} K_u\right),$$

hence there exists some

$$\rho_{i,I} \in \langle\{x_J | \emptyset \subsetneq J \subseteq I \setminus \{i\}\}\rangle_{\mathbb{Z}[G]}$$

such that

$$N_{i,I} := \mathrm{N}_{k\cap\prod\limits_{u\in I} K_u/k\cap\prod\limits_{u\in I\setminus\{i\}} K_u} x_I - \rho_{i,I} \in \ker\varphi\,.$$

We will call $N_{i,I}$ a *norm relation.* Note that for $I = \{1,2,3,4\}$, we have

$$\mathrm{N}_{k\cap\prod\limits_{u\in I} K_u/k\cap\prod\limits_{u\in I\setminus\{i\}} K_u} x = R_i N_i x\,.$$

Remark 7.1. In fact, the relation $N_{i,I}$ can be described much more explicitly using the Frobenius automorphisms, but we won't go into the details here.

Now let M be the $\mathbb{Z}[G]$-submodule of $\ker\varphi$ generated by the norm relations $N_{i,I}$ for all possible $I \subseteq \{1,2,3,4\}$, $|I| \geq 2$ and $i \in I$. Our goal will be to describe the quotient $\mathbb{Z}[G]$-module $\ker\varphi/M$, which we will call *the module of Ennola relations* of k. (However, to follow the terminology in [2], by an *Ennola relation* we will mean an element of $\ker\varphi \setminus M$ rather than $\ker\varphi/M$.)

Let E_{ijl} be the Ennola relation described by Theorem 10 in [2] applied to the field $k \cap K_iK_jK_l$. By Theorem 19 there, E_{ijl} generates all the Ennola relations (modulo the norm relations) for this field.

Proposition 7.2. *In all the cases described in sections 5 and 6, the $\mathbb{Z}[G]$-module $\ker\varphi/M$ is generated by the classes of E_{123}, E_{124}, E_{134}, E_{234}. In addition, the action of G on $\ker\varphi/M$ is trivial.*

Proof. For any case described in Sections 5 and 6, let B be a $\mathbb{Z}$-basis of D^+. For any element of B, we will fix its preimage with respect to φ; let Y be the set of these fixed preimages. Then the elements of Y are $\mathbb{Z}$-linearly independent and we have $\mathcal{X} = \ker\varphi \oplus Y$. Recall that in order to construct B, we always used only ($\mathbb{Z}[G]$-linear combinations of) norm relations together with the four implicit Ennola relations E_{123}, E_{124}, E_{134}, E_{234} from [2]. This shows that $\ker\varphi$ is generated by $M \cup \{E_{123}, E_{124}, E_{134}, E_{234}\}$, which proves the first part of the proposition. The second part follows from the observation that the action of G on E_{ijl} is the same as the action of $\mathrm{Gal}(k\cap K_iK_jK_l/\mathbb{Q})$ on E_{ijl}, which is trivial by Theorem 19 in [2]. □

In certain cases, we can say something stronger. For the rest of this paragraph and for the next lemma, we will only use Assumption 3.1 (so we're not focusing on the five cases in Sections 5 and 6 yet). As in the proof of Lemma 4.1, let K' be the genus field in the narrow sense of $k' = k \cap K_1K_2K_3$, and for any $u \in \{1,2,3\}$, let K'_u be the maximal subfield of K' ramified only at p_u, T'_u be the inertia subgroup of $\mathrm{Gal}(K'/\mathbb{Q})$ corresponding to p_u and $r'_u := [K' : k'K'_u]$. The order of E_{123} in the module $\ker\varphi/M$ of Ennola relations of k is a divisor of the order of E_{123} in the module of Ennola relations of k', which is equal to $\frac{[K':k']}{r'_1r'_2r'_3}$ by Theorem 19 of [2].

Lemma 7.3. *Let $s_{ij} = 1$ for all i, $j \in \{1,2,3\}$. Then we have $T'_u = T_u$, $K_u = K'_u$ and $r'_u = r_u$ for all $u \in \{1,2,3\}$ and moreover $[K' : k'] = m$.*

Proof. Using Proposition 3.3, the ramification index of p_1 in $k'/\mathbb{Q}$ is

$$|T'_1| = [k' : k' \cap K_2K_3] = \frac{[K_1K_2K_3 : k \cap K_2K_3]}{[K_1K_2K_3 : k \cap K_1K_2K_3]} = \frac{|T_1| \cdot \frac{m}{s_{23}}}{m} = \frac{|T_1|}{s_{23}}\,.$$

Since $s_{23} = 1$, we have $|T'_1| = |T_1|$ and $K'_1 = K_1$. Similarly, $|T'_2| = |T_2|$, $|T'_3| = |T_3|$ and $K'_2 = K_2$, $K'_3 = K_3$. Hence

$$[K' : k'] = [K_1K_2K_3 : k \cap K_1K_2K_3] = m$$

and

$$r'_1 = [K' : K'_1k'] = \frac{[K' : k']}{[K_1k' : k']} = \frac{m}{[K_1 : K_1 \cap k']} = \frac{m}{[K_1 : k \cap K_1]} = \frac{m}{\frac{m}{r_1}} = r_1$$

by Proposition 3.3 again (and similarly $r'_2 = r_2$, $r'_3 = r_3$).

□

Obvious analogies of Lemma 7.3 could be also stated for the fields $k \cap K_1K_2K_4$, $k \cap K_1K_3K_4$ and $k \cap K_2K_3K_4$, but we would get a collision in notation, because of our assymetric definition of k'. The proofs would be exactly the same though, because the only assymetry present is purely notational.

Corollary 7.4. *In the following three cases, more can be said about* $\ker\varphi/M$*:*

(i) *If $r_1 = r_2 = r_3 = r_4 = 1$, then* $\ker\varphi/M$ *is a quotient of* $(\mathbb{Z}/m)^4$.

(ii) *If $r_1 = r_2 = a_3 = r_4 = 1$, then* $\ker\varphi/M$ *is a quotient of* $(\mathbb{Z}/n_3)^3 \times \mathbb{Z}/m$.

(iii) *If*

$$a_1 = a_2 = a_3 = r_4 = 1\,,\ r_1 \neq 1\,,\ r_2 \neq 1\,,\ r_3 \neq 1\,,$$
$$s_{12} = s_{13} = s_{23} = 1\,,\ \gcd(n_1, n_2, n_3) = 1\,,$$

then $\ker\varphi/M$ *is a quotient of* $\mathbb{Z}/r_1 \times \mathbb{Z}/r_2 \times \mathbb{Z}/r_3$*, so it is in particular cyclic.*

Proof. This follows immediately from Proposition 7.2 and the mentioned analogies of Lemma 7.3 (in the third part we also use the pairwise coprimality of r_1, r_2, r_3 by Lemma 3.6). □

Remark 7.5. In the case

$$a_1 = a_2 = a_3 = a_4 = r_1 = r_2 = r_3 = r_4 = 1$$

(which is a special case of the first case in Section 6), it can be shown that $\ker\varphi/M \cong (\mathbb{Z}/m)^4$, which is a stronger result than in Corollary 7.4. The proof is too technical to be included here, but essentialy it consists of constructing a $\mathbb{Z}$-module (not $\mathbb{Z}[G]$-module!) homomorphism from $\mathcal{X}$ to $\mathbb{Z}/m$ and showing that all the norm relations together with three of the four Ennola relations lie in its kernel, while the fourth Ennola relation maps to the class of 1 modulo m. It is possible that a similar approach could be used in other cases to improve the bounds in Corollary 7.4.

Remark 7.6. A crucial part of the proof of Proposition 7.2 was the fact that in all of the cases studied in Sections 5 and 6, we never encountered any new Ennola relation, i.e., an element of $\ker\varphi \setminus M$ having a nonzero coefficient at x. This will not always be the case though, because we have already found a new Ennola relation E in the special case

$$m = a_3 = r_3 = 2, a_1 = a_2 = a_4 = r_1 = r_2 = r_4 = 1\,.$$

It's not very hard to show that $E \notin M$ (and $2E \in M$), but the proof that $E \notin \ker\varphi$ is again too technical to be described here. Note that in this case, we have $N = 0$ (recall that N was defined by the equation (4.1)), but it is still possible to recover all the conjugates of η using this new Ennola relation E.

In fact, it appears quite plausible that a new Ennola relation could arise whenever we have $a_i > 1$ and $r_i > 1$ at the same time. It is not a coincidence that this didn't happen in any of the cases studied in Sections 5 and 6, because it seems that this assumption will drastically increase the difficulty of the construction of $\mathbb{Z}$-bases of D^+ and C^+.

References

[1] Dohmae, K., *A note on Sinnott's index formula*, Acta Arith. **82** (1997), 57–67.

[2] Kučera, R., Salami, A., *Circular units of an abelian field ramified at three primes*, J. Number Theory **163** (2016), 296–315. DOI: https://doi.org/10.1016/j.jnt.2015.11.023

[3] Lettl, G., *A note on Thaine's circular units*, J. Number Theory **35** (1990), 224– 226. DOI: http://dx.doi.org/10.1016/0022-314X(90)90115-8

[4] Rubin, K., *Global units and ideal class groups*, Invent. Math. **89** (1987), 511–526.

[5] Salami, A., *Bases of the group of cyclotomic units of some real abelian extension*, Ph.D. thesis, Université Laval Québec, 2014.

[6] Sedláček, V., *Circular units of abelian fields*, Master's thesis, Masaryk University, Faculty of Science, Brno, 2017, [online], [cit. 2017-07-17].

[7] Sinnott, W., *On the Stickelberger ideal and the circular units of an abelian field*, Invent. Math. **62** (1980/81), 181–234.

[8] Thaine, F., *On the ideal class groups of real abelian number fields*, Ann. of Math. (2) **128** (1988), 1–18.

Department of Mathematics, Faculty of Science,
Masaryk University,
611 37 Brno, Czech Republic
E-mail: vlada.sedlacek@mail.muni.cz