

Circular numbers of certain abelian fields

Vladimír Sedláček

April 23, 2017

Throughout this thesis, we will use the convention that whenever any of the indices i, j, l, h appear on the same line, they are pairwise distinct and moreover $1 \leq i, j, l, h \leq 4$, unless stated otherwise. Also for any $n \in \mathbb{N}$, ζ_n will denote a primitive n -th root of unity (WLOG we can take $\zeta_n = e^{2\pi i/n}$).

1 Preliminaries

Definition 1.1. An *abelian field* is a finite Galois extension of \mathbb{Q} with an abelian Galois group.

Definition 1.2. The *genus field* (in the narrow sense) of an abelian field is its maximal extension which is abelian over \mathbb{Q} and unramified at all (finite) primes.

Lemma 1. If K is the genus field (in the narrow sense) of an abelian field k and P is the set of ramified primes of k , we have $\text{Gal}(K/\mathbb{Q}) \cong \prod_{p \in P} T_p$, where T_p is the inertia subgroup of $\text{Gal}(K/\mathbb{Q})$ corresponding to p .

Proof.

□

Theorem 2 (Kronecker-Weber). *Every abelian field is a subfield of some cyclotomic field.*

Proof.

□

Definition 1.3. Let k be an abelian field. The least number $n \in \mathbb{N}$ such that $k \subseteq \mathbb{Q}(\zeta_n)$ is called the conductor of k and denoted by $\text{cond } k$.

Definition 1.4. Let G be any group. The (integral) *group ring* $\mathbb{Z}[G]$ is the free \mathbb{Z} -module with basis G , which is made into a ring, extending linearly the group law on G .

Definition 1.5. An element α of a totally real number field K is called totally positive if for any embedding $\sigma : K \rightarrow \mathbb{R}$, we have $\sigma(\alpha) > 0$.

2 The group of circular numbers

Let k be a real abelian field, K its the genus field in the narrow sense, P is the set of ramified primes of k , K_p is the maximal subfield of K ramified only at $p \in P$. Since $\text{Gal}(K/\mathbb{Q})$ has a natural action on K (given by evaluating an automorphism on an element), this makes K into a $\mathbb{Z}[\text{Gal}(K/\mathbb{Q})]$ -module.

Definition 2.1. The group $D(k)$ of circular numbers of k (using Lettl's modification of Sinnott's definition) is given as

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

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

$$\eta_I = N_{\mathbb{Q}(\zeta_{\text{cond}(\prod_{i \in I} K_i)) / (\prod_{i \in I} K_i)} \cap k \left(1 - \zeta_{\text{cond}(\prod_{i \in I} K_i)} \right),$$

where N denotes the norm operator and the product of fields denotes their compositum. The subset 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 $E(k) \cap D$, where $E(k)$ is the group of units of the ring of algebraic integers of k . The subset of totally positive elements of $C(k)$ will be denoted by $C^+(k)$.

One of the reasons that $C(k)$ is important is the following famous result, due to Sinnott:

Theorem 3. *The index $[E(k) : C(k)]$ is finite.*

Proof. □

Lemma 4.

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

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

Proof. □

Corollary 5. *We have*

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

The next result shows that $D^+(k)$ and $C^+(k)$ are free \mathbb{Z} -modules.

Lemma 6. *$D^+(k)$ is a subgroup of $D(k)$ given as*

$$D^+(k) = \langle \eta_I \mid \emptyset \subsetneq I \subseteq P \rangle_{\mathbb{Z}[\text{Gal}(K/\mathbb{Q})]},$$

hence canonically isomorphic to the non-torsion part of $D(k)$. Similarly, $C^+(k)$ is a subgroup of $C(k)$ given as

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

Proof. □

Lemma 7. *The \mathbb{Z} -rank of $D^+(k)$ is $[k : \mathbb{Q}] + |P| - 1$.*

Proof. □

3 Notation and assumptions

In the remainder of the thesis, 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^+ .

Let K be the genus field in the narrow sense of k and let $G := \text{Gal}(K/\mathbb{Q})$. Then by Lemma 1, 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:

- $H := \text{Gal}(K/k)$,
- $m := |H|$,
- the canonical projections $\pi_i : G \rightarrow T_i$,
- $a_i := [T_i : \pi_i(H)]$,
- $r_i := |H \cap \ker \pi_i|$,
- $s_{ij} := |H \cap \ker(\pi_i \pi_j)|$,
- $n_i := \frac{m}{r_i}$,
- $\eta := \eta_{\{1234\}}$,
- K_i as the maximal subfield of K ramified only at p_i (so that

$$T_i = \text{Gal}(K/K_j K_l K_h) \cong \text{Gal}(K_i/\mathbb{Q}).)$$

We will assume the following:

- $K \neq k$,
- H is cyclic, generated by τ ,
- each T_i is cyclic, generated by σ_i .

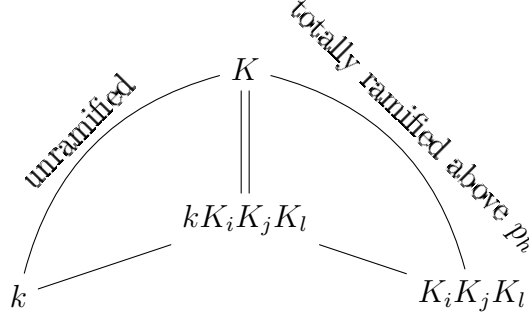
4 Auxiliary results

Lemma 8. *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 , WLOG σ_i . The statement now follows, because τ is determined by its four projections. \square

Lemma 9. *We have $kK_i K_j K_l = K$ and $K_1 K_2 K_3 K_4 = K$.*

Proof. The extension $K/K_iK_jK_l$ is totally ramified at the prime ideals above p_h , so the same must be true for the extension $K/kK_iK_jK_l$. But since the extension K/k is unramified (by the definition of K), so is $K/kK_iK_jK_l$. Therefore $[K : kK_iK_jK_l] = 1$. The second claim follows from the facts $T_i = \text{Gal}(K/K_jK_lK_h)$ and $G = T_1 \times T_2 \times T_3 \times T_4$. \square



Proposition 10. We have $a_i = [k \cap K_i : \mathbb{Q}]$, $r_i = [K : kK_i]$, $|T_i| = a_i n_i$, $s_{ij} = [K : kK_iK_j]$. Also $[K_i : k \cap K_i] = n_i$, $[K_iK_j : k \cap K_iK_j] = \frac{m}{s_{ij}}$ and $[K_iK_jK_l : k \cap K_iK_jK_l] = m$.

Proof. Since

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

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

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

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

$$\pi_i(H) \cong \frac{H}{H \cap \ker \pi_i} = \frac{H}{H \cap T_jT_lT_h} \cong \frac{T_jT_lT_h \cdot H}{T_jT_lT_h} = \frac{\text{Gal}(K/k \cap K_i)}{\text{Gal}(K/K_i)} \cong \text{Gal}(K_i/k \cap K_i).$$

Therefore

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

and

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

Putting everything together, we obtain

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

Next, we also have

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

so that $\text{Gal}(K/k \cap K_i K_j) = T_l T_h \cdot H$. Thus we can consider the short exact sequence

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

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

$$\begin{aligned} \pi_i \pi_j(H) &\cong \frac{H}{H \cap \ker \pi_i \pi_j} = \frac{H}{H \cap T_l T_h} \cong \frac{T_l T_h \cdot H}{T_l T_h} \\ &\cong \frac{\text{Gal}(K/k \cap K_i K_j)}{\text{Gal}(K/K_i K_j)} \cong \text{Gal}(K_i K_j/k \cap K_i K_j). \end{aligned}$$

Then it follows that

$$[K : k K_i K_j] = \frac{|\text{Gal}(K/k)|}{|\text{Gal}(k K_i K_j/k)|} = \frac{|H|}{|\text{Gal}(K_i K_j/k \cap K_i K_j)|} = \frac{m}{|\pi_i \pi_j(H)|} = s_{ij}.$$

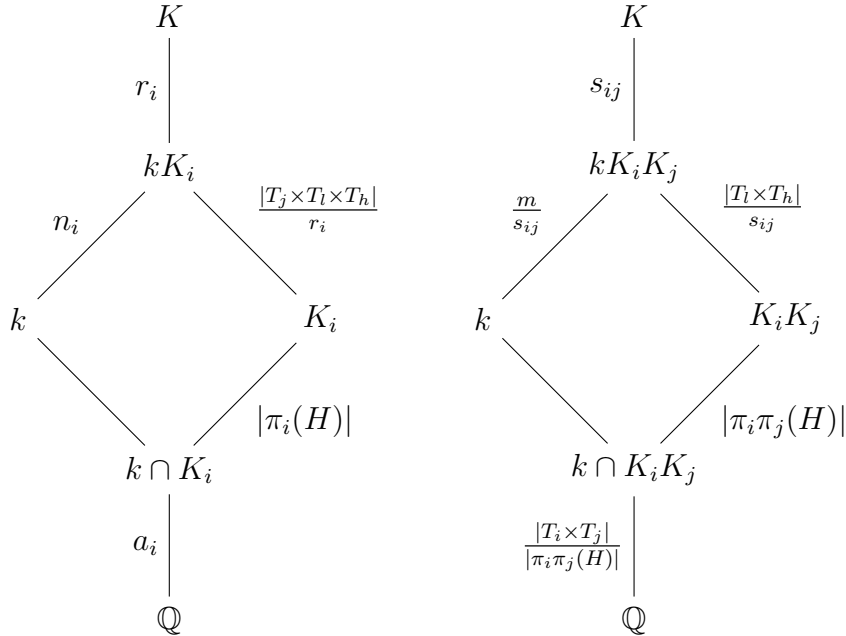
The last part of the statement is a consequence of Lemma 9, since we have

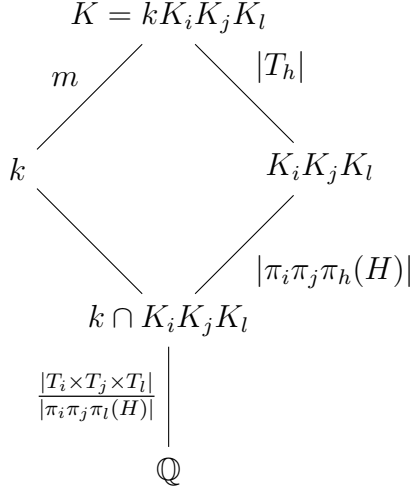
$$\text{Gal}(K_i K_j K_l/k \cap K_i K_j K_l) \cong \text{Gal}(k K_i K_j K_l/k) = \text{Gal}(K/k) = H.$$

Finally note that in the same way as above, we could show that

$$\pi_i \pi_j \pi_l(H) \cong \frac{H}{H \cap T_h} \cong H$$

(since Lemma 9 implies that $|H \cap T_h| = 1$). □





Corollary 11. We have $[k \cap K_iK_j : \mathbb{Q}] = a_i a_j \frac{m}{r_i r_j} s_{ij}$, $[k \cap K_iK_jK_l : \mathbb{Q}] = a_i a_j a_l \frac{m^2}{r_i r_j r_l}$ and $[k : \mathbb{Q}] = a_1 a_2 a_3 a_4 \frac{m^3}{r_1 r_2 r_3 r_4}$.

Proof. This follows from the computations

$$[k \cap K_iK_j : \mathbb{Q}] = \frac{[K_iK_j : \mathbb{Q}]}{[K_iK_j : k \cap K_iK_j]} = \frac{|T_i| \cdot |T_j|}{m/s_{ij}} = a_i a_j \frac{m}{r_i r_j} s_{ij},$$

$$[k \cap K_iK_jK_l : \mathbb{Q}] = \frac{[K_iK_jK_l : \mathbb{Q}]}{[K_iK_jK_l : k \cap K_iK_jK_l]} = \frac{|T_i| \cdot |T_j| \cdot |T_l|}{m} = a_i a_j a_l \frac{m^2}{r_i r_j r_l}$$

and

$$[k : \mathbb{Q}] = \frac{[K : \mathbb{Q}]}{[K : k]} = \frac{|T_1| \cdot |T_2| \cdot |T_3| \cdot |T_4|}{m} = a_1 a_2 a_3 a_4 \frac{m^3}{r_1 r_2 r_3 r_4}.$$

□

Lemma 12. We have

$$s_{ij} = \gcd(r_i, r_j), \gcd(r_i, r_j, r_l) = 1, \text{lcm}(n_i, n_j, n_l) = m \text{ and } s_{ij} \frac{m}{r_i r_j} = \gcd(n_i, n_j).$$

Proof. It follows from Proposition 10 that $s_{ij} \mid r_i, s_{ij} \mid r_j$ and from its proof that

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

The cyclicity of H then implies

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

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

$$\frac{m}{s_{ij}} = \text{lcm}(n_i, n_j) = \text{lcm}\left(\frac{m}{r_i}, \frac{m}{r_j}\right) \mid \frac{m}{t},$$

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

Similarly, we have

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

so if t is any common divisor of r_i, r_j, r_l , we have

$$m = \text{lcm}(n_i, n_j, n_l) = \text{lcm}\left(\frac{m}{r_i}, \frac{m}{r_j}, \frac{m}{r_l}\right) \mid \frac{m}{t},$$

which implies $t = 1$. This implies both $m = \text{lcm}(n_i, n_j, n_l)$ and $\text{gcd}(r_i, r_j, r_l) = 1$ (in fact, these are equivalent).

Finally, using the first result, we have

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

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 $r_i t$ and $r_j t$ divide m , hence $t \cdot \text{lcm}(r_i, r_j) = \text{lcm}(r_i t, r_j t) \mid m$. Thus $t \mid \frac{m}{\text{lcm}(r_i, r_j)}$ and we are done. \square

Proposition 13. *We have*

$$\begin{aligned} \text{Gal}(k/\mathbb{Q}) \cong \{ \sigma_1^{x_1} \sigma_2^{x_2} \sigma_3^{x_3} \sigma_4^{x_4} |_k; & 0 \leq x_1 < a_1 \frac{m}{r_1}, 0 \leq x_2 < a_2 \frac{m}{r_2 s_{34}}, \\ & 0 \leq x_3 < a_3 \frac{m}{r_3 r_4} s_{34}, 0 \leq x_4 < a_4 \}, \end{aligned}$$

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

Proof. First note that by Lemma 12, we have

$$a_3 \frac{m}{r_3 r_4} s_{34} = a_3 \text{gcd}(n_3, n_4) \in \mathbb{N}$$

and

$$a_2 \frac{m}{r_2 s_{34}} = a_2 \text{lcm}(r_3, r_4) \frac{m}{r_2 r_3 r_4} \in \mathbb{N}$$

(this follows from $r_i \mid m$ and $\text{gcd}(r_2, r_3, r_4) = 1$), so the expressions make sense. By Corollary 11, the set on the right hand side has at most $|\text{Gal}(k/\mathbb{Q})|$ elements. Now let ρ be any automorphism of k . If we can show that ρ determines the quadruple (x_1, x_2, x_3, x_4)

belonging to the set on the right hand side uniquely, it will follow that the cardinalities agree and we will be done. Since $\text{Gal}(k \cap K_4/\mathbb{Q})$ is a cyclic group of order a_4 (by Lemma 10) generated by $\sigma_4|_{k \cap K_4}$ (as a quotient of $\text{Gal}(K_4/\mathbb{Q}) = \langle \sigma_4|_{K_4} \rangle$), there must exist a unique $x_4 \in \mathbb{Z}$, $0 \leq x_4 < a_4$ such that ρ and $\sigma_4^{x_4}$ have the same restrictions to $k \cap K_4$. Therefore $\rho\sigma_4^{-x_4}|_k \in \text{Gal}(k/k \cap K_4)$.

Next, $\text{Gal}(k \cap K_3K_4/k \cap K_4)$ is a cyclic group of order $\frac{[k \cap K_3K_4:\mathbb{Q}]}{[k \cap K_4:\mathbb{Q}]} = a_3 \frac{m}{r_3 r_4} s_{34}$ (by Corollary 11) generated by $\sigma_3|_{k \cap K_3K_4}$ (as it is isomorphic by restriction to $\text{Gal}((k \cap K_3K_4)K_4/K_4)$, which is a quotient of $\text{Gal}(K_3K_4/K_4) = \langle \sigma_3|_{K_3K_4} \rangle$), so there must exist a unique $x_3 \in \mathbb{Z}$, $0 \leq x_3 < a_3 \frac{m}{r_3 r_4} s_{34}$ such that $\rho\sigma_4^{-x_4}|_k$ and $\sigma_3^{x_3}$ have the same restriction to $k \cap K_3K_4$. Therefore $\rho\sigma_3^{-x_3}\sigma_4^{-x_4}|_k \in \text{Gal}(k/k \cap K_3K_4)$.

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

$$\frac{[k \cap K_2K_3K_4:\mathbb{Q}]}{[k \cap K_3K_4:\mathbb{Q}]} = a_2 \frac{m}{r_2 s_{34}}$$

(by Corollary 11) generated by $\sigma_2|_{k \cap K_2K_3K_4}$ (as it is isomorphic by restriction to $\text{Gal}((k \cap K_2K_3K_4)K_3K_4/K_3K_4)$, which is a quotient of

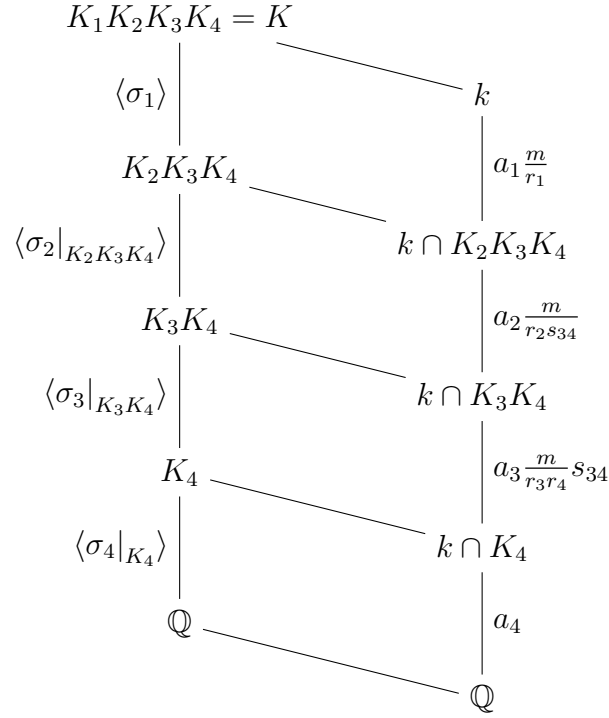
$$\text{Gal}(K_2K_3K_4/K_3K_4) = \langle \sigma_2|_{K_2K_3K_4} \rangle,$$

so there must exist a unique $x_2 \in \mathbb{Z}$, $0 \leq x_2 < a_2 \frac{m}{r_2 s_{34}}$ such that $\rho\sigma_3^{-x_3}\sigma_4^{-x_4}|_k$ and $\sigma_2^{x_2}$ have the same restriction to $k \cap K_2K_3K_4$. Therefore $\rho\sigma_2^{-x_2}\sigma_3^{-x_3}\sigma_4^{-x_4}|_k \in \text{Gal}(k/k \cap K_2K_3K_4)$.

Finally, we have

$$\text{Gal}(k/k \cap K_2K_3K_4) \cong \text{Gal}(kK_2K_3K_4/K_2K_3K_4) = \text{Gal}(K_1K_2K_3K_4/K_2K_3K_4) = \langle \sigma_1 \rangle$$

(using Lemma 9), 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 $x_1 \in \mathbb{Z}$, $0 \leq x_1 < a_1 \frac{m}{r_1}$ such that $\rho\sigma_2^{-x_2}\sigma_3^{-x_3}\sigma_4^{-x_4}|_k$ 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.



□

5 General strategy

Our goal will be to find a basis of D^+ (it can then be easily modified in order to obtain a basis of the group of circular units). 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

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

Then the norm operators from k to a maximal subfield ramified at three primes can be given as $R_i N_i$ (i.e. the sum of all elements of T_i). If we denote the congruence corresponding to the canonical projection $\mathbb{Z}[G] \rightarrow \mathbb{Z}[G/H]$ by \equiv , then we have (using Lemma 8)

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

Note that any subgroup of k^* 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

$$\mathbb{Z}[G] \rightarrow \mathbb{Z}[G/H] \rightarrow \mathbb{Z}[G/H]/(R_1 N_1, R_2 N_2, R_3 N_3, R_4 N_4)$$

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 . When we apply any element of this ideal to the highest generator η , we will obtain a multiplicative \mathbb{Z} -linear combination of circular units belonging to subfields with less ramified primes. We will make use of this extensively.

Lemma 14. *The fields*

$$k \cap K_1K_2K_3, k \cap K_1K_2K_4, k \cap K_1K_3K_4, k \cap K_2K_3K_4$$

satisfy the assumptions of [1].

Proof.

□

To construct a basis of D^+ , we can take the union of all bases for the fields

$$k \cap K_1K_2K_3, k \cap K_1K_2K_4, k \cap K_1K_3K_4, k \cap K_2K_3K_4$$

(we can use the results in [1] to find these) and add in

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

(by the principle of inclusion and exclusion due to the fact that these bases were constructed “inductively”) conjugates of η . Then we will need to show how to obtain the missing conjugates of η using the relations

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

We will always refer to the conjugates of η by their coordinates x_1, x_2, x_3, x_4 according to Proposition 13. This allows us to visualise $\text{Gal}(k/\mathbb{Q})$ geometrically as a discrete (at most) four-dimensional cuboid.

6 The case $r_1 = r_2 = r_3 = r_4 = 1$

7 The case $r_1 = r_2 = a_3 = r_4 = 1$

(Note that in this case we have $s_{34} = 1$ and $n_1 = n_2 = n_4 = m$.)

We will add all the conjugates of η to our basis except the following cases:

- $x_1 = a_1m - 1$ or $x_2 = a_2m - 1$ or $x_3 = n_3 - 1$,
- $a_1 \leq x_1 < a_1m - 1, a_2(m - 1) - 1 \leq x_2 < a_2m - 1, 0 \leq x_3 < n_3 - 1, x_4 = 0$,
- $0 \leq x_1 < a_1, a_2(m - 1) \leq x_2 < a_2m - 1, 0 \leq x_3 < n_3 - 1, x_4 = 0$.

These cases are all disjoint, so it's easy to see that the number of conjugates of η that we chose is exactly

$$((a_1m - 1)a_2(m - 2) + (a_1m - 1)(a_2 - 1) + a_1 + (a_4 - 1)(a_1m - 1)(a_2m - 1))(n_3 - 1) = c.$$

First we will recover the cases $0 < x_4 < a_4, x_1 = a_1m - 1$ or $x_2 = a_2m - 1$ or $x_3 = n_3 - 1$ using the relations $R_1N_1 \sim 0, R_2N_2 \sim 0, R_3N_3 \sim 0$. From now on, we only need to deal with the cases where $x_4 = 0$.

Next, we will recover the cases

$$x_1 = a_1m - 1, 0 \leq x_2 < a_2(m - 1) - 1, 0 \leq x_3 < n_3 - 1$$

using the relation $R_1N_1 \sim 0$ and subsequently the cases

$$0 \leq x_1 < a_1m - 1, 0 \leq x_2 < a_2(m - 1) - 1, 0 \leq x_3 < n_3 - 1$$

and

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

using the relation $R_3N_3 \sim 0$.

Next, we will sequentially recover all the cases

$$0 \leq x_1 < a_1m - 1, a_2(m - 1) \leq x_2 < a_2m - 1, 0 \leq x_3 < n_3 - 1$$

using the relation $R_4 \sum_{u=0}^{m-1} \sigma_1^{a_1u} \sigma_2^{a_2u} \sigma_3^u$. We can do this since any two conjugates of η used in this relation differ by at least a_2 in their second coordinate. After this, we can recover the cases

$$0 \leq x_1 < a_1, x_2 = a_2m - 1, 0 \leq x_3 < n_3 - 1$$

using the relation $R_2N_2 \sim 0$.

Finally, we can use the relation $R_4 \sum_{u=0}^{m-1} \sigma_1^{a_1u} \sigma_2^{a_2u} \sigma_3^u$ to recover the cases

$$a_1 \leq x_1 < 2a_1, x_2 = a_2m - 1, 0 \leq x_3 < n_3 - 1$$

and subsequently $R_4 \sum_{u=0}^{m-1} \sigma_1^{a_1u} \sigma_2^{a_2u} \sigma_3^u$ to recover the cases

$$a_1 \leq x_1 < 2a_1, x_2 = a_2(m - 1) - 1, 0 \leq x_3 < n_3 - 1.$$

By repeating these two steps $(m - 2)$ more times, increasing the first coordinate by a_1 each time, we will recover all the conjugates.

8 The case $a_1 = a_2 = r_3 = r_4 = 1$

In this case, using Lemma 12, we have

$$N = a_3(n_1 - 1)(n_2 - 1)(m - 1) - (n_1 - 1)(n_2 - 1) + \gcd(n_1, n_2) - 1 \\ + (a_4 - 1)(a_3(n_1 - 1)(n_2 - 1)m - (n_1 - 1)(n_2 - 1)).$$

We will add the following N conjugates of η to our basis:

- $0 \leq x_1 < n_1 - 1, 0 \leq x_2 < n_2 - 1, 0 \leq x_3 < a_3m - 1, 0 < x_4 \leq a_4 - 1,$
- $0 \leq x_1 < n_1 - 1, 0 \leq x_2 < n_2 - 1, 0 \leq x_3 < a_3(m - 1) - 1, x_4 = 0,$
- $n_1 - (\gcd(n_1, n_2) - 1) \leq x_1 \leq n_1 - 1, x_2 = n_2 - 1, x_3 = a_3m - 1, x_4 = 0.$

First we will recover the cases $0 < x_4 < a_4, x_1 = n_1 - 1$ or $x_2 = n_2 - 1$ or $x_3 = a_3m - 1$ using the relations $N_1 \sim 0, N_2 \sim 0, R_3N_3 \sim 0$. From now on, we only need to deal with the cases where $x_4 = 0$.

Next, we will recover the cases $0 \leq x_3 < a_3(m - 1) - 1, x_1 = n_1 - 1$ or $x_2 = n_2 - 1$ using the relations $N_1 \sim 0, N_2 \sim 0$. Now we can also use the relation $R_4 \sum_{u=0}^{m-1} \sigma_1^u \sigma_2^u \sigma_3^{a_3u} \sim 0$ multiple times to recover the cases

$$0 \leq x_1 \leq n_1 - 1, 0 \leq x_2 \leq n_2 - 1, a_3(m - 1) \leq x_3 < a_3m - 1.$$

At this moment, we are only missing all the cases with $x_3 = a_3(m - 1) - 1$ and some of those with $x_3 = a_3m - 1$. Let's focus on the second kind. The conjugates with $x_3 = a_3m - 1$ (and $x_4 = 0$) can be visualized as a discrete rectangle with sides n_1 and n_2 . It is easy to see that such a rectangle can be partitioned into $\gcd(n_1, n_2)$ diagonals, each containing $\text{lcm}(n_1, n_2)$ elements (two conjugates lie in the same diagonal iff their quotient is of the form $\eta^{\sigma_1^v \sigma_2^v}$ for some $v \in \mathbb{Z}$). Now consider the relations

$$T := - \left(\sigma_3^{a_3-1} R_4 \sum_{u=0}^{m-1} \sigma_1^u \sigma_2^u \sigma_3^{a_3u} \right) - \sigma_1^{\frac{m}{r_1}-2} \sigma_2^{\frac{m}{r_2}-2} R_3 N_3$$

and

$$S_v := \sum_{u=0}^v \sigma_1^{-u} \sigma_2^{-u} T \text{ for } v \in \mathbb{Z}.$$

Clearly $T \sim 0, S_v \sim 0$ for all $v \in \mathbb{Z}$. Also note that for any v , η^{S_v} contains no conjugate with $x_3 = a_3(m - 1) - 1$ and contains exactly one conjugate with $x_3 = a_3m - 1$ that we cannot recover yet minus $\sigma_3^{a_3m-1}$, and these two always lie on the same diagonal. Moreover, any conjugate sharing this diagonal can occur as the one with positive sign for suitable $v \in \mathbb{Z}$. Therefore, since we already have the conjugates

$$n_1 - (\gcd(n_1, n_2) - 1) \leq x_1 \leq n_1 - 1, x_2 = n_2 - 1, x_3 = a_3m - 1$$

in our basis, we can recover all the conjugates that share the same diagonal with any (and therefore all) of these.

Now we can recover all the conjugates with $x_3 = a_3m - 1$ except $\text{lcm}(n_1, n_2)$ of them, which share a diagonal. By using the relation $\sigma_1^{\text{gcd}(n_1, n_2)-1} (S_v - S_w) \sim 0$ for suitable $v, w \in \mathbb{Z}$, it is clear that we can generate the difference of any two conjugates lying on this diagonal. Now let

$$n'_1 := \frac{n_1}{\text{gcd}(n_1, n_2)}, \quad n'_2 := \frac{n_2}{\text{gcd}(n_1, n_2)}$$

and note that in each column, there are exactly n'_1 conjugates lying on this diagonal, and in each row, there are exactly n'_2 conjugates lying on this diagonal. Moreover, we have

$$\text{gcd}(n'_1, n'_2) = 1$$

by construction, so there exists an integer $z > 0$ such that

$$n'_2 z \equiv 1 \pmod{n'_1}.$$

Using the observation above, we can generate $n'_2 z$ differences of conjugates lying on the last diagonal in such a way that we will obtain each of the conjugates in the row $x_1 = 0$ exactly z times with a negative sign, each of the conjugates in the column $x_2 = 0$ exactly $\frac{n'_2 z - 1}{n'_1}$ times with a positive sign and finally one conjugate with a positive sign with

$$x_1 = n_1 - (\text{gcd}(n_1, n_2) - 1) - 1, x_2 = n_2 - 1.$$

We can keep this last one and get rid of the rest using the relations $N_1 \sim 0, N_2 \sim 0$. Using this last one, we can generate the rest of its diagonal in the same way as above. Hence we have recovered all the conjugates with $x_3 = a_3m - 1$. Finally, using the relation $R_3 N_3 \sim 0$, we can now recover all the conjugates with $x_3 = a_3(m - 1) - 1$ and we are done.

9 The case $a_1 = a_2 = a_3 = r_4 = 1, r_1 \neq 1, r_2 \neq 1, r_3 \neq 1, \text{gcd}(n_1, n_2, n_3) = \text{gcd}(n_1, n_2)$

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

In this case, we have

$$\text{Gal}(k/\mathbb{Q}) \cong \{\sigma_1^{x_1} \sigma_2^{x_2} \sigma_3^{x_3} \sigma_4^{x_4} |_k; 0 \leq x_1 < n_1, 0 \leq x_2 < n_2, 0 \leq x_3 < n_3, 0 \leq x_4 < a_4\}$$

and

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

Note that the condition $r_1 \neq 1, r_2 \neq 1, r_3 \neq 1$ is actually not restrictive, since we have already solved the cases where it is not true. Also r_1, r_2, r_3 must be pairwise distinct, otherwise their coprimality would imply that two of them equal 1. This means that we can without loss of generality assume that $r_1 > r_2 > r_3$ (MAYBE NOT NEEDED?).

Lemma 15. *Under the assumptions $s_{12} = s_{13} = s_{23} = 1$, the following are equivalent:*

- (i) $\gcd(n_1, n_2, n_3) = 1$,
- (ii) $\text{lcm}(r_1, r_2, r_3) = m$,
- (iii) $r_1 r_2 r_3 = m$,
- (iv) $n_1 = r_2 r_3, n_2 = r_1 r_3, n_3 = r_1 r_2$,
- (v) $\frac{n_1 n_2 n_3}{m} = m$,
- (vi) $\gcd(n_1, n_2) = r_3, \gcd(n_1, n_3) = r_2, \gcd(n_2, n_3) = r_1$.

Proof.

“(i) \Leftrightarrow (ii)” : For any $t \in \mathbb{Z}$, we have

$$\begin{aligned} t \mid \gcd(n_1, n_2, n_3) &\Leftrightarrow t \mid n_1, t \mid n_2, t \mid n_3 \Leftrightarrow r_1 \mid \frac{m}{t}, r_2 \mid \frac{m}{t}, r_3 \mid \frac{m}{t} \\ &\Leftrightarrow \text{lcm}(r_1, r_2, r_3) \mid \frac{m}{t} \Leftrightarrow t \mid \frac{m}{\text{lcm}(r_1, r_2, r_3)}, \end{aligned}$$

from which it follows that $\gcd(n_1, n_2, n_3) = \frac{m}{\text{lcm}(r_1, r_2, r_3)}$.

“(ii) \Leftrightarrow (iii)” : Since $s_{12} = s_{13} = s_{23} = 1$, any common multiple of r_1, r_2, r_3 is in fact a multiple of $r_1 r_2 r_3$, hence $\text{lcm}(r_1, r_2, r_3) = r_1 r_2 r_3$.

“(iii) \Leftrightarrow (iv)” : This follows straight from the definition $n_i = \frac{m}{r_i}$.

“(iii) \Leftrightarrow (v)” : We have $\frac{n_1 n_2 n_3}{m} = \frac{m^2}{r_1 r_2 r_3}$, which equals m iff $\frac{m}{r_1 r_2 r_3} = 1$.

“(iv) \Rightarrow (vi)” : For $\{i, j, l\} = \{1, 2, 3\}$, we have $\gcd(n_i, n_j) = \gcd(r_j r_l, r_i r_l) = r_l s_{ij} = r_l$.

“(vi) \Rightarrow (i)” : Since $\gcd(n_1, n_2, n_3)$ must divide $\gcd(n_1, n_2)$, $\gcd(n_1, n_3)$, $\gcd(n_2, n_3)$ and these are pairwise coprime, it must be equal to 1.

□

Thus $\frac{n_1 n_2 n_3}{m} = m = r_2 n_2 = \gcd(n_1, n_3) n_2$ and we have

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

We will add the following N conjugates of η to our basis:

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

(Note that $n_1 - r_2 - 1 = r_2(r_3 - 1) - 1 > 0$ and $r_1 + r_3 - 2 > 0$ since $r_1, r_2, r_3 > 1$.)

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 $x_2 = n_2 - 1$ using the relations $N_1 \sim 0, N_2 \sim 0$ and the cases $x_3 = 0, 0 \leq x_1 < n_1 - r_2 - 1$, $x_2 = n_2 - 1$ using the relation $N_2 \sim 0$.

At this moment, we are only missing all the cases with $x_3 = 1$ and some of those with $x_3 = 0$. From now on, we will only focus on recovering those with $x_3 = 0$ (without explicitly mentioning it anymore), because once we have those, we can recover those with $x_3 = 1$ using just the relation $N_3 \sim 0$.

From now on, we will write $\bar{r}_2 := r_2 \pmod{r_3}$, $\bar{r}_1 := r_1 \pmod{r_3}$ (so that $\bar{r}_2, \bar{r}_1 \in \{1, 2, \dots, r_3 - 1\}$) and similarly for other expressions. In particular, the expressions \bar{r}_2/\bar{r}_1 and \bar{r}_1/\bar{r}_2 will be regarded as being in the previous set.

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

$$D^+ / \langle \{\eta_I \mid \emptyset \subsetneq I \subsetneq P\} \rangle_{\mathbb{Z}[\text{Gal}(K/\mathbb{Q})]}$$

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

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

We will write Q additively, denoting the class of η by μ , hence for any $\rho \in \text{Gal}(k/\mathbb{Q})$, denoting the class of η^ρ in Q by $\rho \cdot \mu$. Showing that we have indeed chosen a basis now amounts to showing that Q is trivial. For all $2 \leq q \leq r_3$, we will denote $X_q := \sigma_1^{n_1-2} \sigma_2^{q-2} \cdot \mu$ and $X_1 := \sigma_1^{n_1-2} \sigma_2^{r_3-1} \cdot \mu$. Also for all $r_1 + r_3 - 2 \leq q \leq r_2 - 1$ we will denote $Y_q := \sigma_1^{r_2(r_3-1)-1} \sigma_2^q \cdot \mu$. It is natural to regard the indices of the Y 's only modulo n_2 . We will refer to the set of these Y_q as to the *critical strip*.

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.

Now let T be the sum of the automorphisms contained in $R_4 \sum_{u=0}^{m-1} \sigma_1^u \sigma_2^u \sigma_3^u$ with $x_3 = x_4 = 0$, i.e.

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

and let

$$T' := R_4 \left(\sum_{u=0}^{m-1} \sigma_1^u \sigma_2^u \sigma_3^u - \sigma_1 \sigma_2 T N_3 \right).$$

Lemma 16. *The expression $\eta^{T'}$ contains no conjugates having $x_3 = 1$ and $\eta^{(1-\sigma_1\sigma_2)T-T'}$ contains only conjugates having $x_4 > 0$ or $x_3 > 1$.*

Proof. Since the order of σ_3 is n_3 , we have $\sigma_3^u = \sigma_3^1$ iff $u = vn_3 + 1$ for some $v \in \mathbb{Z}$. But since

$$R_4 \left(\sum_{v=0}^{r_3-1} \sigma_1^{vn_3+1} \sigma_2^{vn_3+1} \sigma_3^{vn_3+1} - \sigma_1 \sigma_2 \sigma_3 T \right) = 0,$$

it follows that there are no automorphisms in T' whose power of σ_3 is 1.

Proof of the second part...

□

Corollary 17. *In Q , we have $((1 - \sigma_1\sigma_2)T - T') \cdot \mu = 0$ and $(1 - \sigma_1\sigma_2)T \cdot \mu = 0$.*

Proof. The first part is immediate, because the conjugates of η having $x_4 > 0$ or $x_3 > 1$ become trivial in Q . The second equality follows from the fact that $T' \sim 0$, hence $T' \cdot \mu = 0$ (in fact, the image of $\eta^{T'}$ is already trivial in Q'). □

Now 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. 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 $0 \leq q \leq r_3 - 1$, 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. big column) for any $0 \leq x_1 < n_1, 0 \leq x_2 < n_2$, and these have the same relative position in each of the respective blocks (determined only by $n_3 \pmod{r_3}$ and 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 $0 \leq q \leq r_3 - 1$ and $0 \leq x_1 < n_1, 0 \leq x_2 < n_2$ is exactly $\bar{r}_2 \cdot r_1$, i.e. \bar{r}_2 blocks, and the vertical distance between them is exactly $\bar{r}_1 \cdot r_2$, i.e. \bar{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 \bar{r}_2/\bar{r}_1 blocks.

Lemma 18. For any $0 \leq x_1 < n_1, 0 \leq x_2 < n_2$, we have

$$\sigma_1^{x_1} \sigma_2^{x_2} \cdot \mu = \begin{cases} 0 & \begin{aligned} &\text{if } x_1 < r_2(r_3 - 1) - 1 \\ &\text{or } x_1 = r_2(r_3 - 1) - 1, x_2 < r_1 + r_3 - 2 \end{aligned} \\ Y_{x_2} & \text{if } x_1 = r_2(r_3 - 1) - 1, r_1 + r_3 - 2 \leq x_2 < n_2 \\ \overline{X_{-x_1+x_2}} & \\ \\ X_{\overline{-x_1+x_2}} - Y_{x_2 - \overline{r_2}/\overline{r_1} \cdot r_1} & \begin{aligned} &\text{if } r_2(r_3 - 1) - 1 < x_1 < n_3 - 1 \\ &\text{or } x_1 = n_3 - 1, x_2 \equiv q + \overline{r_2}/\overline{r_1} \cdot r_1 \pmod{n_2} \\ &\text{for some } 0 \leq q < r_1 + r_3 - 2 \end{aligned} \\ \\ \overline{X_{-x_1+x_2}} - Y_{x_2 - \overline{r_2}/\overline{r_1} \cdot r_1} & \begin{aligned} &\text{if } x_1 = n_1 - 1, x_2 \not\equiv q + \overline{r_2}/\overline{r_1} \cdot r_1 \pmod{n_2} \\ &\text{for any } 0 \leq q < r_1 + r_3 - 2, \end{aligned} \end{cases}$$

where the expression $\overline{-x_1+x_2}$ is taken in the set $\{1, 2, \dots, r_3\}$. In particular, this implies that the action of $\sigma_1^{-x_1} \sigma_2^{x_2}$ on X_q results in $X_{\overline{q+x_1+x_2}}$ (unless the result is 0 and ignoring all the Y 's).

Proof. We will partition our $n_1 \times n_2$ rectangle (of conjugates of η having $x_3 = x_4 = 0$) into $r_3 = \gcd(n_1, n_2)$ two-dimensional diagonals in the following way: for any $x_1, x_2 \in \mathbb{Z}$, the conjugate $\eta^{\sigma_1^{x_1} \sigma_2^{x_2}}$ lies in the q -th diagonal for $1 \leq q \leq r_3$ iff $x_1 - x_2 \equiv q \pmod{r_3}$ (this is well defined, since $r_3 = \gcd(n_1, n_2)$). It's easy to see that each of these r_3 diagonals goes through exactly one of $\eta^{\sigma_1^{n_1-2} \sigma_2^{q-2}}$ for $2 \leq q \leq r_3 + 1$. Thus after projecting the diagonals to Q , each of them goes through exactly one X_q for $1 \leq q \leq r_3$. We will use this together with the fact that $(1 - \sigma_1 \sigma_2)T \cdot \mu = 0$ in Q to find the classes of all conjugates in our rectangle in terms of X_q, Y_q . There are several possibilities.

The first case ($x_1 < r_2(r_3 - 1) - 1$ or $x_1 = r_2(r_3 - 1) - 1, x_2 < r_1 + r_3 - 2$) follows directly from the definition of Q and the second case ($x_1 = r_2(r_3 - 1) - 1, r_1 + r_3 - 2 \leq x_2$) directly from the definition of Y_{x_2} .

Now for a moment suppose that all the Y_q 's are zero (we do not know that yet, but this will make the description easier). Then based on the observations above, we could say that for any $0 \leq x_1 < n_1, 0 \leq x_2 < n_2$,

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

is always a difference of two possibly nonzero elements that lie on the same diagonal. Thus we could say that these two elements are the same in Q . After increasing both x_1 and x_2 by 1, we could use the same argument. Thus using the fact that all the automorphisms in T lie on the same diagonal and repeating this process $\text{lcm}(n_1, n_2) = m$ times, we would obtain that in Q , all the elements in the big row $r_2(r_3 - 1) \leq x_1 < n_1$ sharing a diagonal are the same. This would imply $\sigma_1^{x_1} \sigma_2^{x_2} \cdot \mu = \overline{X_{-x_1+x_2}}$ for all such x_1 , as can be easily checked (it agrees with the definition of X_q 's and respects the diagonals).

This assertion is almost correct, but we need to account for the Y_q ' as well. Whenever

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

contains an element from the critical strip having coefficient 1, say Y_q (where $r_1 + r_3 - 2 \leq q < r_2$), we must have (based on the earlier geometric observations) $x_1 = r_2(r_3 - 1) - 1$, $x_2 = q$, so that

$$0 = \sigma_1^{x_1} \sigma_2^{x_2} (1 - \sigma_1 \sigma_2) T \cdot \mu = Y_q - \sigma_1^{r_2(r_3-1)} \sigma_2^{q+1} \cdot \mu + \sigma_1^{n_3-1} \sigma_2^{q+(\overline{r_2}/\overline{r_1}) \cdot r_1} \cdot \mu,$$

hence

$$\sigma_1^{n_3-1} \sigma_2^{q+(\overline{r_2}/\overline{r_1}) \cdot r_1} \cdot \mu = \sigma_1^{r_2(r_3-1)} \sigma_2^{q+1} \cdot \mu - Y_q.$$

Similarly, whenever

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

contains an element from the critical strip having coefficient -1 , say $-Y_q$ (where $r_1 + r_3 - 2 \leq q < r_2$), we must have $x_1 = r_2(r_3 - 1) - 2$, $x_2 = q - 1$, so that

$$0 = \sigma_1^{x_1} \sigma_2^{x_2} (1 - \sigma_1 \sigma_2) T \cdot \mu = -Y_q + \sigma_1^{n_3-2} \sigma_2^{q+(\overline{r_2}/\overline{r_1}) \cdot r_1 - 1} \cdot \mu - \sigma_1^{n_3-1} \sigma_2^{q+(\overline{r_2}/\overline{r_1}) \cdot r_1} \cdot \mu,$$

hence

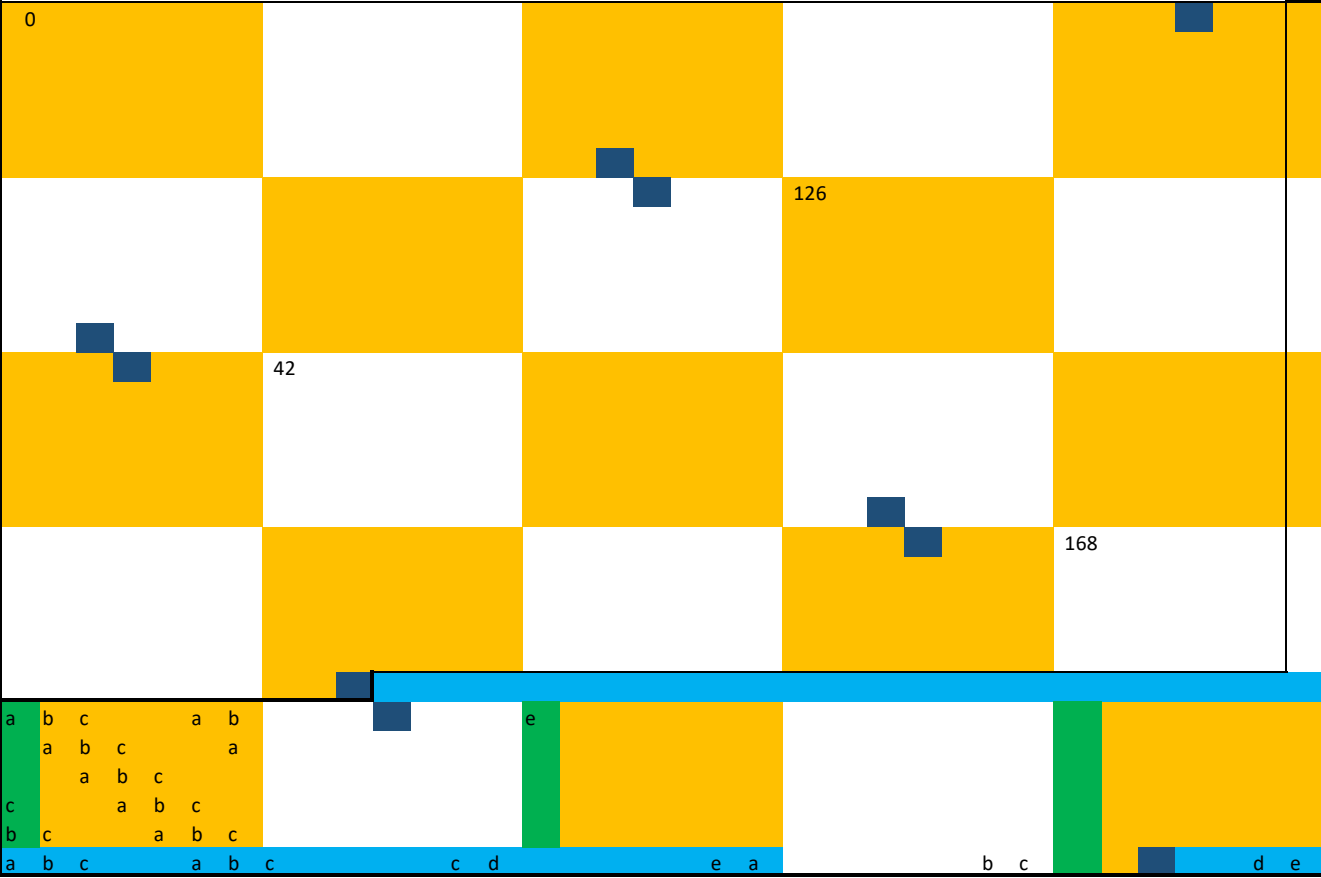
$$\sigma_1^{n_3-1} \sigma_2^{q+(\overline{r_2}/\overline{r_1}) \cdot r_1} \cdot \mu = \sigma_1^{n_3-2} \sigma_2^{q+(\overline{r_2}/\overline{r_1}) \cdot r_1 - 1} \cdot \mu - Y_q.$$

A slight alteration of the above naive proof and putting everything together now yields the result. \square

Thanks to this result, from now on we will regard the indices of the X 's only modulo r_3 (to be more precise, in the set $\{1, 2, \dots, r_3\}$) and drop the bar notation for them. We will also put $Y_q := 0$ for all $0 \leq q < r_1 + r_3 - 2$ (again regarded modulo n_2), so that the equality

$$\sigma_1^{n_1-1} \sigma_2^{x_2} \cdot \mu = X_{1+x_2} - Y_{x_2 - \overline{r_2}/\overline{r_1} \cdot r_1}$$

will hold for all $x_2 \in \mathbb{Z}$.



Now it suffices to show that $X_q = 0$ for all $1 \leq q \leq r_3$ and $Y_q = 0$ for all $r_1 + r_3 - 2 \leq q \leq r_2 - 1$. To achieve this, we will use linear algebra.

Let $\alpha := Y_{r_1+r_3-2} + \cdots + Y_{r_2-1} \in Q$ and $\beta := X_1 + X_2 + \cdots + X_{r_3} \in Q$.

Lemma 19. *We have $\alpha = \beta = 0$.*

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

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

and

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

since each $x_2 \in \{0, 1, \dots, r_1 r_3 - 1\}$ can be uniquely written as $ur_3 + v$, where $0 \leq u < r_1$, $0 \leq v < r_3$ and the unary operation of adding r_2 induces an isomorphism of \mathbb{Z}/r_3 .

Similarly, using the relation $N_1 \sim 0$ and the fact that

$$(\sigma_1^{n_1-1} \sigma_2^{x_2} + \sigma_1^{r_2(r_3-1)-1} \sigma_2^{x_2 - \overline{r_2}/\overline{r_1} \cdot r_1}) \cdot \mu = X_{1+x_2}$$

for all $x_2 \in \mathbb{Z}$, we have

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

since for any x_1 , all possible remainders modulo r_3 occur exactly once as the indices in the sum $\sum_{q=0}^{r_3-1} X_{-x_1+qr_1}$ (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 Bezout's identity. \square

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

$$\Gamma_q := \sum_{u=0}^{r_3 - \overline{r_2}/\overline{r_1} - 1} \sum_{v=1}^{\overline{r_2}} X_{q+v-ur_2} \in Q.$$

Lemma 20. For any $0 \leq q \leq r_3 - 3$, we have $\Gamma_q = 0$.

Proof. Using the relation $N_1 \sim 0$ and the fact that

$$(\sigma_1^{n_1-1} \sigma_2^{x_2} + \sigma_1^{r_2(r_3-1)-1} \sigma_2^{x_2 - \bar{r}_2/\bar{r}_1 \cdot r_1}) \cdot \mu = X_{1+x_2}$$

for all $x_2 \in \mathbb{Z}$, we have

$$\begin{aligned} 0 &= \sum_{u=0}^{r_3 - \bar{r}_2/\bar{r}_1 - 1} \sigma_2^{q - u \cdot \bar{r}_2/\bar{r}_1 \cdot r_1} N_1 \cdot \mu \\ &= \sum_{u=0}^{r_3 - \bar{r}_2/\bar{r}_1 - 2} \left(\sigma_1^{n_1-1} \sigma_2^{q - u \cdot \bar{r}_2/\bar{r}_1 \cdot r_1} + \sigma_1^{r_2(r_3-1)-1} \sigma_2^{q - (u+1) \cdot \bar{r}_2/\bar{r}_1 \cdot r_1} \right) \cdot \mu \\ &\quad + \sigma_1^{n_1-1} \sigma_2^{q - (r_3 - \bar{r}_2/\bar{r}_1 - 1) \cdot (\bar{r}_2/\bar{r}_1 \cdot r_1)} + \sum_{x_1=r_2(r_3-1)}^{n_1-2} \sum_{u=0}^{r_3 - \bar{r}_2/\bar{r}_1 - 1} \sigma_1^{x_1} \sigma_2^{q - u \cdot \bar{r}_2/\bar{r}_1 \cdot r_1} \cdot \mu \\ &= \left(\sum_{u=0}^{r_3 - \bar{r}_2/\bar{r}_1 - 2} X_{q+1-u \cdot \bar{r}_2/\bar{r}_1 \cdot r_1} \right) + X_{q+1-(r_3 - \bar{r}_2/\bar{r}_1 - 1) \cdot (-\bar{r}_2/\bar{r}_1 \cdot r_1)} \\ &\quad + \sum_{x_1=r_2(r_3-1)}^{n_1-2} \sum_{u=0}^{r_3 - \bar{r}_2/\bar{r}_1 - 1} X_{q-x_1-u \cdot \bar{r}_2/\bar{r}_1 \cdot r_1} \\ &= \sum_{u=0}^{r_3 - \bar{r}_2/\bar{r}_1 - 1} X_{q+1-ur_2} + \sum_{x_1=r_2(r_3-1)}^{n_1-2} \sum_{u=0}^{r_3 - \bar{r}_2/\bar{r}_1 - 1} X_{q-x_1-ur_2} \\ &= \sum_{x_1=r_2(r_3-1)}^{n_1-1} \sum_{u=0}^{r_3 - \bar{r}_2/\bar{r}_1 - 1} X_{q+x_1-ur_2} = \sum_{u=0}^{r_3 - \bar{r}_2/\bar{r}_1 - 1} \sum_{v=1}^{r_2} X_{q+v-ur_2} \\ &= \sum_{u=0}^{r_3 - \bar{r}_2/\bar{r}_1 - 1} \left(\sum_{v=1}^{\bar{r}_2} X_{q+v-ur_2} + \sum_{v=\bar{r}_2+1}^{r_2} X_{q+v-ur_2} \right) \\ &= \sum_{u=0}^{r_3 - \bar{r}_2/\bar{r}_1 - 1} \sum_{v=1}^{\bar{r}_2} X_{q+v-ur_2} + \sum_{u=0}^{r_3 - \bar{r}_2/\bar{r}_1 - 1} \frac{r_2 - \bar{r}_2}{r_3} \sum_{v=\bar{r}_2+1}^{\bar{r}_2+r_3} X_{q+v-ur_2} \\ &= \Gamma_q + \sum_{u=0}^{r_3 - \bar{r}_2/\bar{r}_1 - 1} \frac{r_2 - \bar{r}_2}{r_3} \beta = \Gamma_q. \end{aligned}$$

Note that we also used the fact that

$$\sigma_1^{n_1-1} \sigma_2^{q - (r_3 - \bar{r}_2/\bar{r}_1 - 1) \cdot (\bar{r}_2/\bar{r}_1 \cdot r_1)} \cdot \mu = \sigma_1^{n_1-1} \sigma_2^{q+r_1+\bar{r}_2/\bar{r}_1 \cdot r_1} \cdot \mu = X_{1+q+r_1+\bar{r}_2/\bar{r}_1 \cdot r_1}$$

by Lemma 18, since $0 \leq q + r_1 < r_1 + r_3 - 2$ (which also explains why this wouldn't work for higher q).

□

Finally, let

$$\Delta := \sum_{u=0}^{r_3-1} u \cdot \sum_{v=1}^{\bar{r}_2} \sum_{w=1}^{\bar{r}_1} X_{v+w-ur_2} \in Q.$$

Lemma 21. *We have $\Delta = 0$.*

Proof. Using the relation $N_1 \sim 0$ and the fact that

$$(\sigma_1^{n_1-1} \sigma_2^{x_2} + \sigma_1^{r_2(r_3-1)-1} \sigma_2^{x_2-\bar{r}_2/\bar{r}_1 \cdot r_1}) \cdot \mu = X_{1+x_2}$$

for all $x_2 \in \mathbb{Z}$, we have

$$\begin{aligned} 0 &= \sum_{u=0}^{r_3-1} u \cdot \sum_{x_2=0}^{r_1-1} \sigma_2^{x_2-u \cdot \bar{r}_2/\bar{r}_1 \cdot r_1} N_1 \cdot \mu \\ &= \sum_{u=0}^{r_3-1} u \cdot \sum_{x_2=0}^{r_1-1} \left(\sigma_1^{n_1-1} \sigma_2^{x_2-u \cdot \bar{r}_2/\bar{r}_1 \cdot r_1} + \sigma_1^{r_2(r_3-1)-1} \sigma_2^{x_2-u \cdot \bar{r}_2/\bar{r}_1 \cdot r_1} \right) \cdot \mu + \\ &\quad + \sum_{u=0}^{r_3-1} u \cdot \sum_{x_1=r_2(r_3-1)}^{n_1-2} \sum_{x_2=0}^{r_1-1} \sigma_1^{x_1} \sigma_2^{x_2-u \cdot \bar{r}_2/\bar{r}_1 \cdot r_1} \cdot \mu \\ &= \dots (\text{not finished}) \\ &= \alpha + \sum_{u=0}^{r_3-1} u \cdot \sum_{x_1=r_2(r_3-1)}^{n_1-1} \sum_{x_2=0}^{r_1-1} \sigma_1^{x_1} \sigma_2^{x_2-u \cdot \bar{r}_2/\bar{r}_1 \cdot r_1} \cdot \mu \\ &= \sum_{u=0}^{r_3-1} u \cdot \sum_{x_1=r_2(r_3-1)}^{n_1-1} \sum_{x_2=0}^{r_1-1} X_{-x_1+x_2-ur_2} \\ &= \sum_{u=0}^{r_3-1} u \cdot \sum_{v=1}^{\bar{r}_2} \sum_{w=0}^{\bar{r}_1} X_{v+w-ur_2} \\ &= \dots (\text{not finished}) \\ &= \sum_{u=0}^{r_3-1} u \cdot \sum_{v=1}^{\bar{r}_2} \sum_{w=0}^{\bar{r}_1} X_{v+w-ur_2} = \Delta. \end{aligned}$$

□

Since β, Γ_q and Δ are linear combinations of the X_u , they can be written as $\sum_{c=1}^{r_3} c_u X_u$, and thus correspond to the r_3 -tuples of coefficients $(c_1, c_2, \dots, c_{r_3})$. Using this correspondence, we will now construct a matrix M of size $r_3 \times r_3$ as follows:

- The first row will correspond to β (i.e., it will consist only of 1's).

- The q -th row for $2 \leq q \leq r_3 - 1$ will correspond to Γ_{q-2} .
- The last row will correspond to Δ .

Since the rows of M are coefficients of valid equalities in Q , we have $M \cdot X' = 0$, where $X = (X_1, \dots, X_{r_3})$ and $'$ denotes transposition. We will show that M is unimodular, i.e. invertible over \mathbb{Z} , from which it will follow that $X = 0$. To do that, we will first need to describe M in a better way.

Let

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

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

and

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

Lemma 22. *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 part is immediate since $R(\zeta) \cdot (\zeta - 1) = \zeta^{r_3} - 1 = 0$, but $\zeta \neq 1$. The second follows from the computation

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

□

Formally, we can regard β, Γ_q and Δ as elements of $\mathbb{Z}[X_1, X_2, \dots, X_{r_3}]$. By abuse of notation, we can then denote $\beta(x), \Gamma_q(x)$ and $\Delta(x)$ their respective images under the homomorphism $\mathbb{Z}[X_1, X_2, \dots, X_{r_3}] \rightarrow \mathbb{Z}[x]$ determined by $X_u \mapsto x^{u-1}$ for all $1 \leq u \leq r_3$. Since we regard the indices of X_u modulo r_3 , this map is well defined only modulo

$x^3 - 1$ (so we should in fact take the codomain to be $\mathbb{Z}[x]/(x^{r_3} - 1)$), but we will only be interested in the values of these polynomials at r_3 -th roots of unity, so this isn't an issue. With this in mind, we have

$$\beta(x) \approx R(x),$$

$$\Gamma_q(x) \approx x^q \cdot (1 + x + \dots + x^{\overline{r_2}-1})(1 + x^{r_3-\overline{r_2}} + x^{2(r_3-\overline{r_2})} + \dots + x^{(r_3-\overline{r_1}/\overline{r_2}-1)(r_3-\overline{r_2})})$$

and

$$\Delta(x) \approx (1 + x + \dots + x^{\overline{r_2}-1})(1 + x + \dots + x^{\overline{r_1}-1})(x^{r_3-\overline{r_2}} + 2x^{2(r_3-\overline{r_2})} + \dots + (r_3 - 1)x^{(r_3-1)(r_3-\overline{r_2})}),$$

where \approx denotes the congruence modulo $x^{r_3} - 1$. In cases where there could be confusion, we will denote the evaluation homomorphism $\mathbb{Z}[x] \rightarrow \mathbb{Z}[\zeta]$ given by $x \mapsto \zeta$ by ev_ζ .

Lemma 23. *Let $\zeta \neq 1$ be any r_3 -th root of unity. Then for all $2 \leq q < r_3$, we have*

$$\Gamma_q(\zeta) = \zeta^q \cdot P(\zeta)$$

and

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

Proof. Since $R(\zeta) = 0$, we can regard the polynomial $\Gamma_q(x)$ only modulo $R(x)$ during the proof (PROBABLY NOT NEEDED?). Then we have

$$\begin{aligned} \Gamma_q(\zeta) &= \zeta^q \cdot (1 + \zeta + \dots + \zeta^{\overline{r_2}-1})(1 + \zeta^{r_3-\overline{r_2}} + \zeta^{2(r_3-\overline{r_2})} + \dots + \zeta^{(r_3-\overline{r_1}/\overline{r_2}-1)(r_3-\overline{r_2})}) \\ &= \zeta^q \cdot \frac{\zeta^{\overline{r_2}} - 1}{\zeta - 1} \cdot \frac{\zeta^{(r_3-\overline{r_1}/\overline{r_2})(r_3-\overline{r_2})} - 1}{\zeta^{r_3-\overline{r_2}} - 1} \\ &= \zeta^q \cdot \frac{\zeta^{\overline{r_2}} - 1}{\zeta^{r_3-\overline{r_2}} - 1} \cdot \frac{\zeta^{\overline{r_1}} - 1}{\zeta - 1} \\ &= -\zeta^q \cdot \zeta^{\overline{r_2}} \cdot (1 + \zeta + \zeta^2 + \dots + \zeta^{\overline{r_1}-1}) \\ &= \zeta^q \cdot P(\zeta). \end{aligned}$$

Similarly, using the substitution $y = x^{r_3-\overline{r_2}}$, we can see that

$$\begin{aligned} \Delta(\zeta) &= \text{ev}_\zeta((1 + x + \dots + x^{\overline{r_2}-1})(1 + x + \dots + x^{\overline{r_1}-1})(x^{r_3-\overline{r_2}} + 2x^{2(r_3-\overline{r_2})} + \dots + (r_3 - 1)x^{(r_3-1)(r_3-\overline{r_2})})) \\ &= \frac{\zeta^{\overline{r_2}} - 1}{\zeta - 1} \cdot \frac{\zeta^{\overline{r_1}} - 1}{\zeta - 1} \cdot \zeta^{-\overline{r_2}} \cdot \frac{\partial}{\partial y} \left(\frac{y^t - 1}{y - 1} \right) \Big|_{y=\zeta^{-\overline{r_2}}} \\ &= \frac{\zeta^{\overline{r_2}} - 1}{\zeta - 1} \cdot \frac{\zeta^{\overline{r_1}} - 1}{\zeta - 1} \cdot \zeta^{-\overline{r_2}} \cdot \text{ev}_\zeta \left(\frac{r_3 y^{r_3-1}(y - 1) - (y^{r_3} - 1)}{(y - 1)^2} \right) \\ &= \frac{\zeta^{\overline{r_2}} - 1}{\zeta - 1} \cdot \frac{\zeta^{\overline{r_1}} - 1}{\zeta - 1} \cdot \frac{r_3}{\zeta^{-\overline{r_2}} - 1} \\ &= \frac{r_3}{\zeta - 1} \cdot \frac{\zeta^{\overline{r_2}} - 1}{\zeta^{-\overline{r_2}} - 1} \cdot \frac{\zeta^{\overline{r_1}} - 1}{\zeta - 1} \\ &= -D(\zeta) \cdot \zeta^{\overline{r_2}} \cdot \frac{\zeta^{\overline{r_1}} - 1}{\zeta - 1} \\ &= D(\zeta) \cdot P(\zeta). \end{aligned}$$

□

Theorem 24. M is unimodular, hence $X = 0$.

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. $C = (\zeta_{r_3}^{r \cdot c})_{0 \leq r, c < r_3}$. 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} . After reindexing the dimensions of M from 0 to $r_3 - 1$, 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 $0 < c < t$ (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 (since multiplication by \bar{r}_1 is an automorphism of \mathbb{Z}/r_3)

$$|\det C'| = |\det C''| \cdot \left| \prod_{0 < c < r_3} P(\zeta_{r_3}^c) \right| = |\det C''| \cdot \left| \prod_{0 < c < r_3} -\zeta_{r_3}^{c\bar{r}_2} \right| \cdot \left| \prod_{0 < c < r_3} \frac{\zeta_{r_3}^{c\bar{r}_1} - 1}{\zeta_{r_3}^c - 1} \right| = |\det C''|,$$

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, if we take the matrix C , add all of its rows to the last one (thus creating $(r_3 \ 0 \ 0 \ \dots \ 0)$ there) and then add a suitable linear combination of rows $0, 1, \dots, r_3 - 3$ to the $r_3 - 2$ -th row times -1 using the equality

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

so that the $r_3 - 2$ -th row will become $(* \ D(\zeta_{r_3}) \ \dots \ D(\zeta_{r_3}^c) \ \dots \ D(\zeta_{r_3}^{r_3-1}))$, 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 this equals $\pm \sqrt{r_3^{r_3}}$), which implies that $|\det M| = 1$, as needed. \square

Corollary 25. *We have $Y_q = 0$ for all $r_1 + r_3 - 2 \leq q \leq n_2 - 1$.*

Proof. For any $r_1 - 2 \leq x_2 < r_1 + r_3 - 2$, we have $\sigma_2^{x_2} N_1 \sim 0$, hence (using the fact that $X = 0$)

$$0 = \sigma_2^{x_2} N_1 \cdot \mu = -Y_{x_2 + (r_3 - \overline{r_2}/\overline{r_1}) \cdot r_1} \pmod{n_2}$$

and consequently

$$\begin{aligned} 0 &= \sigma_2^{x_2 + (r_3 - \overline{r_2}/\overline{r_1}) \cdot r_1} N_1 \cdot \mu = Y_{x_2 + (r_3 - \overline{r_2}/\overline{r_1}) \cdot r_1} \pmod{n_2} && -Y_{x_2 + 2 \cdot (r_3 - \overline{r_2}/\overline{r_1}) \cdot r_1} \pmod{n_2} \\ &= && -Y_{x_2 + 2 \cdot (r_3 - \overline{r_2}/\overline{r_1}) \cdot r_1} \pmod{n_2}, \\ 0 &= \sigma_2^{x_2 + 2 \cdot (r_3 - \overline{r_2}/\overline{r_1}) \cdot r_1} N_1 \cdot \mu = Y_{x_2 + 2 \cdot (r_3 - \overline{r_2}/\overline{r_1}) \cdot r_1} \pmod{n_2} && -Y_{x_2 + 3 \cdot (r_3 - \overline{r_2}/\overline{r_1}) \cdot r_1} \pmod{n_2} \\ &= && -Y_{x_2 + 3 \cdot (r_3 - \overline{r_2}/\overline{r_1}) \cdot r_1} \pmod{n_2}, \end{aligned}$$

and so on. Continuing in this way, we will obtain the result. \square

11 The module of relations

12 Construction of suitable abelian fields

Let $m, a_1, a_2, a_3, a_4, r_1, r_2, r_3, r_4$ be positive integers such that

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

We will construct an infinite family of fields k that satisfy all of our assumptions such that these integers correspond to the parameters in our problem of the same name (again we will denote $n_i = \frac{m}{r_i}$).

First, we will fix distinct primes p_1, p_2, p_3, p_4 such that $p_i \equiv 1 \pmod{2a_i n_i}$ (by Dirichlet's theorem on primes in arithmetic progressions, there are infinitely many ways of doing this). Then there exist even Dirichlet characters χ_i of conductors p_i and orders $a_i n_i$ (namely, these can be given as $\chi_i := \chi^{\frac{p_i - 1}{a_i n_i}}$, where χ is any generator of the cyclic group $(\widehat{\mathbb{Z}/p_i\mathbb{Z}})^\times$ (note that $p_i > 2$)).

Now let K_i be the field associated to $\langle \chi_i \rangle$. Then K_i is real (because χ_i is even) and $\text{Gal}(K_i/\mathbb{Q})$ is cyclic of order $a_i n_i$, say $\text{Gal}(K_i/\mathbb{Q}) = \langle \sigma_i \rangle$. Moreover, since the conductors p_i are coprime, the group $\langle \chi_1, \chi_2, \chi_3, \chi_4 \rangle$ corresponds to the compositum field

$K = K_1 K_2 K_3 K_4$. By the theory of Dirichlet characters, K is ramified exactly at primes p_i (with inertia subgroups isomorphic to $\text{Gal}(K_i/\mathbb{Q})$) and

$$\text{Gal}(K/\mathbb{Q}) = \text{Gal}(K_1/\mathbb{Q})\text{Gal}(K_2/\mathbb{Q})\text{Gal}(K_3/\mathbb{Q})\text{Gal}(K_4/\mathbb{Q}) = \langle \sigma_1, \sigma_2, \sigma_3, \sigma_4 \rangle,$$

so that $[K : \mathbb{Q}] = a_1 a_2 a_3 a_4 \frac{m^4}{r_1 r_2 r_3 r_4}$. Now let $\tau := \sigma_1^{a_1} \sigma_2^{a_2} \sigma_3^{a_3} \sigma_4^{a_4}$ and let k be the subfield of K fixed by τ . Since k is a subfield of a compositum of real fields, it must also be real. In order to reach our goal, we now only need to prove the following theorem (it is not hard to see that we could have used the results from Lemma 9 and Proposition 10 as definitions instead).

Theorem 26. *In the above notation, we have $[K : k] = m$, $[K : kK_i] = r_i$, $[k \cap K_i : \mathbb{Q}] = a_i$ and $kK_i K_j K_l = K$ (i.e. K is the genus field of k).*

Proof. Using Lemma 12 several times, we can compute

$$[K : k] = |\langle \tau \rangle| = \text{lcm}(n_i, n_j, n_l) = m,$$

$$[K : kK_i] = |\langle \tau \rangle \cap \langle \sigma_j \sigma_l \sigma_h \rangle| = |\langle \tau^{a_i n_i} \rangle| = r_i,$$

$$[k \cap K_i : \mathbb{Q}] = [\langle \sigma_1, \sigma_2, \sigma_3, \sigma_4 \rangle : \langle \tau, \sigma_j, \sigma_l, \sigma_h \rangle] = [\langle \sigma_1, \sigma_2, \sigma_3, \sigma_4 \rangle : \langle \sigma_i^{a_i}, \sigma_j, \sigma_l, \sigma_h \rangle] = a_i$$

and

$$[K : kK_i K_j K_l] = |\langle \tau \rangle \cap \langle \sigma_h \rangle| = |\langle \tau^{\text{lcm}(n_i, n_j, n_l)} \rangle| = |\langle \tau^m \rangle| = 1.$$

□