Circular numbers of certain abelian fields

Vladimír Sedláček

March 27, 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 $1 \leq i, j, l, h \leq 4$.

1 Basic definitions and assumptions

Let k be a real abelian field with exactly four ramified primes p_1, p_2, p_3, p_4. Let K be the genus field (in the narrow sense) of k and assume $K \neq k$. Let $G := \mathrm{Gal}(K/\mathbb{Q})$, then (by the properties of the genus field) we can identy 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 $\pi_i : G \to T_i$,
- $a_i := [T_i : \pi_i(H)]$,
- $r_i := |H \cap \ker \pi_i|$,
- $s_{ij} := |H \cap \ker(\pi_i \pi_j)|$,
- $n_i := \frac{m}{r_i}$,
- K_i as the maximal subfield of K ramified only at p_i (so that

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

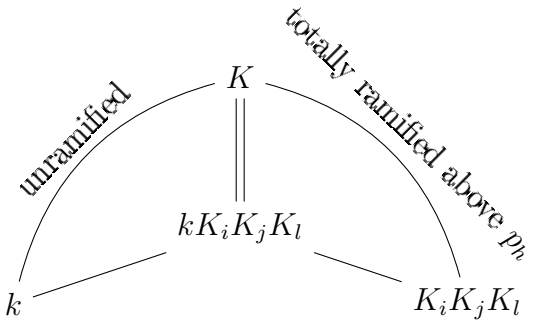
We will assume the following:

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

2 Auxiliary results

Lemma 1. *We have $kK_iK_jK_l = K$ and $K_1K_2K_3K_4 = K$.*

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 $\mathrm{Gal}(K_i/\mathbb{Q}) = T_i$ and $G = T_1 \times T_2 \times T_3 \times T_4$. □



Proposition 2. *We have $a_i = [k \cap K_i : \mathbb{Q}]$, $r_i = [K : kK_i]$, $|T_i| = a_i\frac{m}{r_i}$, $s_{ij} = [K : kK_iK_j]$. Also $[K_i : k \cap K_i] = \frac{m}{r_i}$, $[K_iK_j : k \cap K_iK_j] = \frac{m}{s_{ij}}$ and $[K_iK_jK_l : k \cap K_iK_jK_l] = m$.*

Proof. Since

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

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 $|\pi_i(H)| = \frac{m}{r_i}$ and

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

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

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

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

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

Then it follows that

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

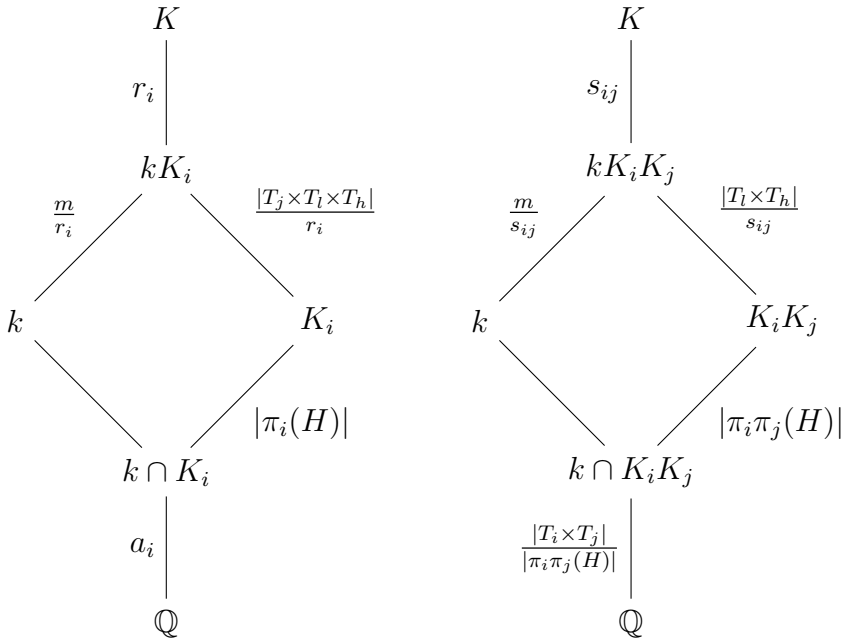
The last part of the statement is a consequence of Lemma 1, since we have

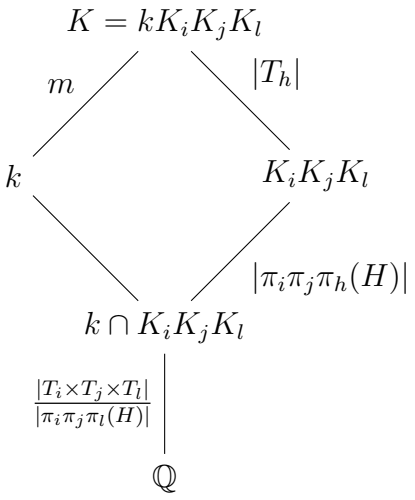
$$\mathrm{Gal}(K_iK_jK_l/k\cap K_iK_jK_l) \cong \mathrm{Gal}(kK_iK_jK_l/k) = \mathrm{Gal}(K/k) = H.$$

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 1 implies that $|H\cap T_h| = 1$). □





Corollary 3. *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

$$\begin{aligned}[k : \mathbb{Q}] &= [k \cap K_i : \mathbb{Q}] \cdot [k : k \cap K_i] = a_i \cdot [kK_i : K_i] = a_i\frac{[K : K_i]}{[K : kK_i]} \\ &= a_i\frac{|T_j| \cdot |T_l| \cdot |T_h|}{r_i} = a_1a_2a_3a_4\frac{m^3}{r_1r_2r_3r_4}.\end{aligned}$$

□

Lemma 4. *We have* $s_{ij} = \gcd(r_i, r_j)$, $\gcd(r_i, r_j, r_l) = 1$ *(this is also equivalent to* $\operatorname{lcm}\left(\frac{m}{r_i}, \frac{m}{r_j}, \frac{m}{r_l}\right) = m$ *and to* $\gcd(s_{ij}, r_l) = 1$*) and* $s_{ij}\frac{m}{r_ir_j} = \gcd(\frac{m}{r_i}, \frac{m}{r_j})$.

Proof. It follows from Proposition 2 that $s_{ij} \mid r_i, s_{ij} \mid r_j$ and from its proof that $|\pi_i(H)| = \frac{m}{r_i}$, $|\pi_i\pi_j(H)| = \frac{m}{s_{ij}}$ and $|\pi_i\pi_j\pi_l(H)| = m$. The cyclicity of H then implies

$$\frac{m}{s_{ij}} = |\pi_i\pi_j(H)| = |\langle\pi_i\pi_j(\tau)\rangle| = |\langle\pi_i(\tau)\pi_j(\tau)\rangle| = \operatorname{lcm}\left(\frac{m}{r_i}, \frac{m}{r_j}\right),$$

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 $\frac{m}{s_{ij}} = \operatorname{lcm}\left(\frac{m}{r_i}, \frac{m}{r_j}\right) \mid \frac{m}{t}$, which implies $t \mid s_{ij}$ and we are done.

Similarly, we have

$$m = |\pi_i\pi_j\pi_l(H)| = |\langle \pi_i\pi_j\pi_l(\tau)\rangle| = |\langle \pi_i(\tau)\pi_j(\tau)\pi_l(\tau)\rangle| = \operatorname{lcm}\left(\frac{m}{r_i}, \frac{m}{r_j}, \frac{m}{r_l}\right),$$

so if t is any common divisor of r_i, r_j, r_l, we have $m = \operatorname{lcm}\left(\frac{m}{r_i}, \frac{m}{r_j}, \frac{m}{r_l}\right) \mid \frac{m}{t}$, which implies $t = 1$.

Finally, using the first result, we have $s_{ij}\frac{m}{r_i r_j} = \frac{m}{\operatorname{lcm}(r_i, r_j)}$, which clearly divides both $\frac{m}{r_i}$ and $\frac{m}{r_j}$. Moreover, if t is any common divisor of $\frac{m}{r_i}$ and $\frac{m}{r_j}$, then both $r_i t$ and $r_j t$ divide m, hence $t \cdot \operatorname{lcm}(r_i, r_j) = \operatorname{lcm}(r_i t, r_j t) \mid m$. Thus $t \mid \frac{m}{\operatorname{lcm}(r_i, r_j)}$ and we are done. □

Proposition 5. *We have*

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

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

Proof. By Corollary 3, the set on the right hand side has at most $|\operatorname{Gal}(k/\mathbb{Q})|$ 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 $\operatorname{Gal}(k \cap K_4/\mathbb{Q})$ is a cyclic group of order a_4 (by lemma 2) generated by $\sigma_4|_{k\cap K_4}$ (as a quotient of $\operatorname{Gal}(K_4/\mathbb{Q}) = \langle \sigma_4|_{K_4}\rangle$), 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 $\rho\sigma_4^{-x_4}\big|_k \in \operatorname{Gal}(k/k \cap K_4)$.

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

Following the pattern, $\operatorname{Gal}(k \cap K_2K_3K_4/k \cap K_3K_4)$ 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 3) generated by $\sigma_2|_{k\cap K_2K_3K_4}$ (as a quotient of

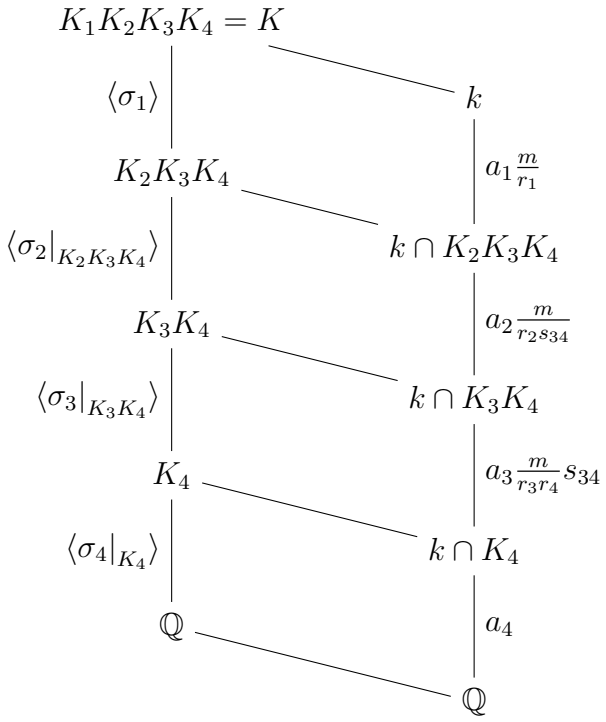
$$\operatorname{Gal}(K_2K_3K_4/K_3K_4) = \langle \sigma_2|_{K_2K_3K_4}\rangle),$$

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

Finally, we have

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

(using Lemma 1), 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 $\rho\sigma_2^{-x_2}\sigma_3^{-x_3}\sigma_4^{-x_4}$ and $\sigma_1^{x_1}$ have the same restriction to k. Thus $\rho=\sigma_1^{x_1}\sigma_2^{x_2}\sigma_3^{x_3}\sigma_4^{x_4}$ and the proof is finished.



□

Lemma 6. *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 generater of T_i, WLOG σ_i. The statement now follows, because τ is determined by its four projections. □

3 The group of circular numbers

Recall that D^+, the subgroup of totally positive elements of the group D of circular numbers of a real abelian field k' (using Lettl's modification of Sinnott's definition), has one generator η_I for each nonempty subset $I\subseteq P$, where P is the set of ramified primes of k'. (Since k' is real, D^+ is also canonically isomorphic to the non-torsion part of D.)

More explicitly, if we let K_i' be the largest subfield of K' (the genus field of k' in the narrow sense) in which p_i is the only ramified prime for any $i \in I$, we have

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

It is well known that D^+ is a $\mathbb{Z}[G]$-module of $\mathbb{Z}$-rank $[k:\mathbb{Q}] + |P| - 1$.

(In our case, we have $k' = k, K' = K, K_i' = K_i, |P| = 4$, $\eta := \eta_{\{1,2,3,4\}}$.)

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

$$R_i = \sum_{u=0}^{a_i-1} \sigma_i^u,\ N_i = \sum_{u=0}^{\frac{m}{r_i}-1} \sigma_i^{au_i}.$$

Then the norm operators from k to a maximal subfield ramified at three primes can be given as R_iN_i (i.e. the sum of all elements of T_i). If we denote the congruence corresponding to the canonical projection $\mathbb{Z}[G] \to \mathbb{Z}[G/H]$ by $\equiv$, then we have $N_4 \equiv \sum_{u=0}^{m-1} \sigma_1^{ua_1}\sigma_2^{ua_2}\sigma_3^{ua_3}$.

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

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

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

(which have three ramified primes, so we can use the results in [1]) and add in

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

(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

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

We will always refer to the conjugates of η by their coordinates x_1, x_2, x_3, x_4 according to Proposition 5. This allows for geometric interpretation.

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

(Note that in this case we have $s_{34} = 1$.)

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

- $x_1 = a_1 m - 1$ or $x_2 = a_2 m - 1$ or $x_3 = \frac{m}{r_3} - 1$,
- $a_1 \leq x_1 < a_1 m - 1, a_2(m-1) - 1 \leq x_2 < a_2 m - 1, 0 \leq x_3 < \frac{m}{r_3} - 1, x_4 = 0$,
- $0 \leq x_1 < a_1, a_2(m-1) \leq x_2 < a_2 m - 1, 0 \leq x_3 < \frac{m}{r_3} - 1, x_4 = 0$.

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

$$((a_1 m - 1)a_2(m-2) + (a_1 m - 1)(a_2 - 1) + a_1 + (a_4 - 1)(a_1 m - 1)(a_2 m - 1)) \left(\frac{m}{r_3} - 1\right) = c.$$

First we will recover the cases $0 < x_4 < a_4$, $x_1 = a_1 m - 1$ or $x_2 = a_2 m - 1$ or $x_3 = \frac{m}{r_3} - 1$ using the relations $R_1 N_1 \sim 0, R_2 N_2 \sim 0, R_3 N_3 \sim 0$. From now on, we only need to deal with the cases where $x_4 = 0$.

Next, we will recover the cases

$$x_1 = a_1 m - 1, 0 \leq x_2 < a_2(m-1) - 1, 0 \leq x_3 < \frac{m}{r_3} - 1$$

using the relation $R_1 N_1 \sim 0$ and subsequently the cases

$$0 \leq x_1 < a_1 m - 1, 0 \leq x_2 < a_2(m-1) - 1, 0 \leq x_3 < \frac{m}{r_3} - 1$$

and

$$0 \leq x_1 < a_1 - 1, x_2 = a_2(m-1) - 1, 0 \leq x_3 < \frac{m}{r_3} - 1$$

using the relation $R_3 N_3 \sim 0$.

Next, we will sequentially recover all the cases

$$0 \leq x_1 < a_1 m - 1, a_2(m-1) \leq x_2 < a_2 m - 1, 0 \leq x_3 < \frac{m}{r_3} - 1$$

using the relation $R_4 \sum_{u=0}^{m-1} \sigma_1^{a_1 u} \sigma_2^{a_2 u} \sigma_3^u$. 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

$$0 \leq x_1 < a_1, x_2 = a_2 m - 1, 0 \leq x_3 < \frac{m}{r_3} - 1$$

using the relation $R_2 N_2 \sim 0$.

Finally, we can use the relation $R_4 \sum_{u=0}^{m-1} \sigma_1^{a_1 u} \sigma_2^{a_2 u} \sigma_3^u$ to recover the cases

$$a_1 \leq x_1 < 2a_1, x_2 = a_2 m - 1, 0 \leq x_3 < \frac{m}{r_3} - 1$$

and subsequently $R_4 \sum_{u=0}^{m-1} \sigma_1^{a_1 u} \sigma_2^{a_2 u} \sigma_3^u$ to recover the cases

$$a_1 \leq x_1 < 2a_1, x_2 = a_2(m-1) - 1, 0 \leq x_3 < \frac{m}{r_3} - 1.$$

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

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

(Recall that $n_i = \frac{m}{r_i}$.)

In this case, using Lemma 4, we have

$$\begin{aligned} c = {} & a_3 (n_1 - 1)(n_2 - 1)(m - 1) - (n_1 - 1)(n_2 - 1) + \gcd(n_1, n_2) - 1 \\ & + (a_4 - 1)(a_3 (n_1 - 1)(n_2 - 1) m - (n_1 - 1)(n_2 - 1)). \end{aligned}$$

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

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

First we will recover the cases $0 < x_4 < a_4$, $x_1 = n_1 - 1$ or $x_2 = n_2 - 1$ or $x_3 = a_3 m - 1$ using the relations $N_1 \sim 0, N_2 \sim 0, R_3 N_3 \sim 0$. From now on, we only need to deal with the cases where $x_4 = 0$.

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

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

At this moment, we are only missing all the cases with $x_3 = a_3(m-1) - 1$ and some of those with $x_3 = a_3 m - 1$. Let's focus on the second kind. The conjugates with $x_3 = a_3 m - 1$ (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

$\operatorname{lcm}(n_1, n_2)$ elements (two conjugates lie in the same diagonal iff one can be obtained from the other as a multiple of $\sigma_1^v \sigma_2^v$ for some $v \in \mathbb{Z}$). Now consider the relations

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

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, S_v contains no conjugate with $x_3 = a_3(m-1) - 1$ and contains exactly one conjugate with $x_3 = a_3 m - 1$ that we cannot recover yet minus $\sigma_3^{a_3 m - 1}$, 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

$$n_1 - (\gcd(n_1, n_2) - 1) \leq x_1 \leq n_1 - 1, \leq x_2 = n_2 - 1, x_3 = a_3 m - 1$$

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 $x_3 = a_3 m - 1$ except $\operatorname{lcm}(n_1, n_2)$ of them, which share a diagonal. By using the relation $\sigma_1^{\gcd(n_1,n_2)-1}(S_v - S_w) \sim 0$ 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

$$n_1' := \frac{n_1}{\gcd(n_1, n_2)}, \quad n_2' := \frac{n_2}{\gcd(n_1, n_2)}$$

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

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

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

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

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 $x_3 = a_3 m - 1$. 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.

6 The case $a_1 = a_2 = a_3 = r_4 = 1, s_{12} = s_{13} = s_{23} = 1, \gcd(n_1, n_2, n_3) = 1$

In this case, using Lemma 4, we have

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

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

- $0 \le x_1 < n_1 - 1, 0 \le x_2 < n_2 - 1, 0 \le x_3 < a_3 m - 1, 0 < x_4 \le a_4 - 1,$
- $0 \le x_1 < n_1 - 1, 0 \le x_2 < n_2 - 1, 1 \le x_3 < n_3 - 1, x_4 = 0,$
- $0 \le x_1 < n_1 - \gcd(n_1, n_3) - 1, 0 \le x_2 < n_2 - 1, x_3 = 0, x_4 = 0,$
- $x_1 = n_1 - \gcd(n_1, n_3) - 1, 0 \le x_2 < \gcd(n_2, n_3) + \gcd(n_1, n_2) - 2, x_3 = 0, x_4 = 0.$

First we will recover the cases $0 < x_4 < a_4$, $x_1 = n_1 - 1$ or $x_2 = n_2 - 1$ or $x_3 = a_3 m - 1$ 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 $1 < x_3 \le n_3 - 1$, $x_1 = n_1 - 1$ or $x_2 = n_2 - 1$ using the relations $N_1 \sim 0, N_2 \sim 0$ and the cases $x_3 = 0$, $0 \le x_1 < n_1 - \gcd(n_1, n_3) - 1$, $x_2 = n_2 - 1$ 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 $N_3 \sim 0$.

Now let $t, u, v \in \mathbb{Z}$ be such that $n_1 = tu, n_2 = tv$ and $\gcd(u, v) = 1$, i.e. $t = \gcd(n_1, n_2)$. Since $s_{12} = 1$, this implies that $m = \operatorname{lcm}(n_1, n_2) = tuv$. But we also have the conditions $s_{13} = s_{23} = 1$ which imply that $tuv = m = \operatorname{lcm}(tu, n_3) = \operatorname{lcm}(tv, n_3)$. Next, since $\gcd(n_1, n_2, n_3) = 1$, t must be coprime with n_3, therefore $n_3 \mid uv$. Finally, the equalities

$$\operatorname{lcm}(tu, n_3) = \frac{tun_3}{(tu, n_3)} = tuv = \frac{tvn_3}{(tv, n_3)} = \operatorname{lcm}(tv, n_3)$$

show that $u, v \mid n_3$, hence $uv = \gcd(u, v) \mid n_3$ and $n_3 = uv$. It follows that $t = r_3, u = r_2, v = r_1$ (and thus $u = \gcd(n_1, n_3)$ and $v = \gcd(n_2, n_3)$. Thanks to the symmetry, we will assume $1 < t < u < v$ (if any of t, u, v would equal 1, this case could be reduced to one of the previous two). We will also write $\overline{u} := u \pmod t$, $\overline{v} := v \pmod t$ (so that $\overline{u}, \overline{v} \in \{1, 2, \ldots, t-1\}$) and similarly for other expressions. In particular, the expressions $\overline{u}/\overline{v}$ and $\overline{v}/\overline{u}$ will be regarded modulo t as well.

The conjugates with $x_3 = 0$ (and $x_4 = 0$) can be visualized as a discrete rectangle with sides n_1 and n_2. Since for each x_4, there are n_3 rectangles in total, the relation $R_4 \sum_{u=0}^{m-1} \sigma_1^u \sigma_2^u \sigma_3^u$ must contain $\frac{m}{n_3} = r_3$ conjugates in each of these rectangles. Thus the relation

$$T' := R_4 \sum_{q=0}^{m-1} \sigma_1^q \sigma_2^q \sigma_3^q - \sum_{q=0}^{r_3-1} \sigma_1^{1+qn_3} \sigma_2^{1+qn_3} N_3$$

contains only elements we have already recovered and those with $x_3 = 0$ (and clearly $T' \sim 0$). More specifically, if we let T be the sum of the conjugates contained in $R_4 \sum_{u=0}^{m-1} \sigma_1^u \sigma_2^u \sigma_3^u$ with $x_3 = 0$, then the relations $(1 - \sigma_1\sigma_2)T$ and T' differ only by conjugates which we have already recovered.

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

From now on, we will regard the elements of our rectangle as their images in the quotient module of $\mathbb{Z}[G/H]/(N_1, N_2, N_3, N_4)$ by the $\mathbb{Z}$-module of the conjugates we can already recover (including those living in the maximal subfields ramified at three primes). We will call this quotient module Q. Showing that we have indeed chosen a basis then amounts to showing that the class of each conjugate in our rectangle is trivial in Q. For all $1 \leq q \leq t$, we will denote the class of $\eta^{\sigma_1^{tu-q}}$ by X_q and we will also put $X_{q'} := X_q$ for all $q' \in \mathbb{Z}$, $q' \equiv q \pmod t$. Also for all $v + t - 2 \leq q \leq tv - 1$ we will denote the class of $\eta^{\sigma_1^{(t-1)u-1}\sigma_2^q}$ by Y_q.

Now it suffices to show that $X_q = 0$ for all $1 \leq q \leq t$ and $Y_q = 0$ for all $v + t - 2 \leq q \leq tv - 1$.

Using the relation $N_1 \sim 0$, we obtain the equation $u \cdot (X_1 + \cdots + X_t) = 0$, and similarly the relation $N_2 \sim 0$ implies $v \cdot (X_1 + \cdots + X_t) = 0$. Since $\gcd(u, v) = 1$, this implies $X_1 + \cdots + X_t = 0$ be Bezout's identity. We will put $\beta = X_1 + \cdots + X_t$. Next, we will put

$$\Gamma := \sum_{q=0}^{-\overline{u}/\overline{v}-1} \sum_{p=1}^{\overline{u}} X_{\overline{p-qv}}$$

and

$$\Delta := \sum_{q=0}^{t-1} q \cdot \sum_{p=1}^{\overline{u}} X_{\overline{p-qv}}.$$

It's easy to check that all the Y_q's cancel out in both of them, and that any shift in the indices in Γ by $1, 2, \ldots, t-3$ will also result in a valid relation.

Letting t, u, v vary (but with the same meaning as before), we will construct a matrix $M(t, u, v)$ of type $t \times t$ as follows:

- The first row will consist of all 1's (corresponding to the relation β).
- The second row will correspond to the relation Γ.
- The q-th row for $3 \leq q \leq t-1$ will correspond to the relation Γ shifted by q to the right.
- The last row will correspond to the relation Δ.

Since the rows of $M(t, u, v)$ are the coefficients of valid relations, we have $M(t, u, v) \cdot X^T = 0$, where $X = (X_1, \ldots, X_t)$. We will show that $M(t, u, v)$ is unimodular, i.e. invertible over $\mathbb{Z}$, from which it will follow that $X = 0$. To do that, we will first need several technical results to describe $M(t, u, v)$ more precisely.

Lemma 7. *For any u, u', v, v' with $u \equiv u' \pmod{t}$, $v \equiv v' \pmod{t}$, we have $|\det M(t, u, v)| = |\det M(t, u', v')|$.*

Proof. This follows from the facts that $\overline{u} = \overline{u'}, \overline{v} = \overline{v'}$, the shifts in both Δ and Γ (and the number of summands in case of Γ) depend only on $\overline{u}, \overline{v}$ and each summand in both Γ and Δ changes only by a multiple of β whenever we alter $\overline{u}$ or $\overline{v}$ by a multiple of m. □

Lemma 8. *For any u, u', the matrices $M(t, u', v)$ is obtained from the matrix $M(t, u, v)$ be cyclic column shift by $u' - u$ places to the right. In particular, $|\det M(t, u, v)| = |\det M(t, u', v)|$.*

Proof. It suffices to show this for the second and the last row. We will start with the second. Let $P(t, \overline{u}, \overline{v})$ be the polynomial in the localization L of the quotient ring $\mathbb{Z}[x]/(1 + x + x^2 + \cdots + x^{t-1})$ at the multiplicative subset generated by $\{(1-x), (1-x^2), (1-x^3), \ldots\}$ such that its coefficient at x^q is exactly the coefficent at X_{q+1} in Γ for all $0 \leq q \leq t-1$. Since a cyclic shift of the indices of X_q corresponds to multiplication by x in L, we have

$$\begin{aligned} P(t, \overline{u}, \overline{v}) &= (1 + x + \cdots + x^{\overline{u}-1})(1 + x^{m-\overline{u}} + x^{2(m-\overline{u})} + \cdots + x^{(t-\overline{v}/\overline{u}-1)(t-\overline{u})}) \\ &= \frac{x^{\overline{u}} - 1}{x - 1} \cdot \frac{x^{(t-\overline{v}/\overline{u})(t-\overline{u})} - 1}{x^{t-\overline{u}} - 1} \\ &= \frac{x^{\overline{u}} - 1}{x^{t-\overline{u}} - 1} \cdot \frac{x^{\overline{v}} - 1}{x - 1} \qquad (1) \\ &= -x^{\overline{u}} \cdot (1 + x + x^2 + \cdots + x^{\overline{v}-1}) \\ &= x^{\overline{u}} \cdot (x^{\overline{v}} + x^{\overline{v}+1} + \cdots + x^{t-1}). \end{aligned}$$

Coming back to the coefficients in Γ, this means that incrementing $\overline{u}$ by 1 results in a cyclic shift of Γ by 1 to the right.

Similarly, let $P'(t, \overline{u}, \overline{v})$ be the polynomial in L corresponding to the last row. Then we have (using the substitution $y = x^{t-\overline{u}}$, so that $y^m = 1$ in L)

$$\begin{aligned} P(t,\overline{u},\overline{v}) &= (1 + x + \cdots + x^{\overline{u}-1})(1 + x + \cdots + x^{\overline{v}-1})(x^{t-\overline{u}} + 2x^{2(t-\overline{u})} + \cdots + (t-1)x^{(t-1)(t-\overline{u})}) \\ &= \frac{x^{\overline{u}}-1}{x-1} \cdot \frac{x^{\overline{v}}-1}{x-1} \cdot y \cdot \frac{\partial}{\partial y}\left(\frac{y^m-1}{y-1}\right) \\ &= \frac{x^{\overline{u}}-1}{x-1} \cdot \frac{x^{\overline{v}}-1}{x-1} \cdot y \cdot \frac{my^{m-1}(y-1) - (y^m-1)}{(y-1)^2} \\ &= \frac{x^{\overline{u}}-1}{x-1} \cdot \frac{x^{\overline{v}}-1}{x-1} \cdot \frac{m}{y-1} \\ &= \frac{x^{\overline{u}}-1}{x^{t-\overline{u}}-1} \cdot m \cdot \frac{x^{\overline{v}}-1}{(x-1)^2} \\ &= -m \cdot x^{\overline{u}} \cdot \frac{x^{\overline{v}}-1}{(x-1)^2} \end{aligned} \tag{2}$$

Again, this means that incrementing $\overline{u}$ by 1 results in a cyclic shift of Δ by 1 to the right. □

Thanks to this result, we will fix $\overline{u} = 1$ in the following and write simply $M(t, v)$.

Lemma 9. *The second row of $M(t, v)$ is exactly*

$$(1, \underbrace{0, \ldots, 0}_{\overline{v}}, \underbrace{1, \ldots, 1}_{t-\overline{v}}).$$

Proof. This follows from the equation (1). □

Lemma 10. *The last row of $M(t, v)$ is*

$$(0, t-\overline{v}, 2(t-\overline{v}), \ldots, (\overline{v}-2)(t-\overline{v}), (\overline{v}-1)(t-\overline{v}), \overline{v}(t-\overline{v}), \overline{v}(t-\overline{v}-1), \overline{v}(t-\overline{v}-2), \ldots, \overline{v}).$$

Proof. This follows from the equation (2) after some computations (it can also be done in elementary way for $\overline{u} = 1$). □

Lemma 11. *For $v \neq 1$, we have $|\det M(t, v)| = |\det M(v, (v-t) \mod v)|$.*

Proof. By substracting the second row from the third, the third from the fourth, ..., the

$t-2$-th from the $t-1$-th, the matrix $M(t,v)$ becomes

$$\begin{pmatrix} 1 & 1 & 1 & \dots & 1 & 1 & 1 & \dots & 1 & 1 \\ 1 & 0 & 0 & \dots & 0 & 1 & 1 & \dots & 1 & 1 \\ 0 & 1 & 0 & \dots & 0 & -1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 & -1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \ddots & \vdots & -1 \\ -1 & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \vdots & -1 & \vdots & \dots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & t-\overline{v} & 2(t-\overline{v}) & \dots & \overline{v}(t-\overline{v}) & \overline{v}(t-\overline{v}-1) & \overline{v}(t-\overline{v}-2) & \dots & 2\overline{v} & \overline{v} \end{pmatrix}.$$

In other words, we have the equality $X_q = X_{q+\overline{v}}$ for all $2 \le q \le t-\overline{v}$ (and even for some others, but we won't need those now). Therefore by adding the corresponding rows to the last one, we can get zeroes everywhere in the last row except for the second, third,... and $\overline{v}$-th column. After this operation, the last row will become □

Lemma 12. *$M(t,v)$ is unimodular, hence $X = 0$.*

Proof. Since $1 = \gcd(t,v) = \gcd(v, (v-t) \mod v)$ and $(v-t) \mod v < v$, after finitely many applications of Lemma 11 we can make a reduction to the case $\overline{v} = 1$. Then by substracting the first row from all the others except the last one, we have

$$\begin{aligned} \det M(t,v) &= \pm \det \begin{pmatrix} 1 & 1 & 1 & 1 & \dots & 1 & 1 \\ 1 & 0 & 1 & 1 & \dots & 1 & 1 \\ 1 & 1 & 0 & 1 & \dots & 1 & 1 \\ 1 & 1 & 1 & 0 & \dots & 1 & 1 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 1 & 1 & 1 & \dots & 0 & 1 \\ 0 & t-1 & t-2 & t-3 & \dots & 2 & 1 \end{pmatrix} \\ &= \pm \det \begin{pmatrix} 1 & 1 & 1 & 1 & \dots & 1 & 1 \\ 0 & -1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & -1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & -1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & -1 & 0 \\ 0 & t-1 & t-2 & t-3 & \dots & 2 & 1 \end{pmatrix} \\ &= \pm 1. \end{aligned}$$

□

Lemma 13. $Y = 0$.

Proof. Almost done (starting at the first big column and using $N_1 \sim 0$ while doing shifts, since $\gcd(\overline{u}/\overline{v}, t) = 1$). □

7 The module of relations

8 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.

First, we will fix distinct primes p_1, p_2, p_3, p_4 such that $p_i \equiv 1 \pmod{2a_i\frac{m}{r_i}}$ (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 $a_i\frac{m}{r_i}$ (namely, these can be given as $\chi_i := \chi^{\frac{p_i-1}{a_i m_i/r_i}}$, 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 $\mathrm{Gal}(K_i/\mathbb{Q})$ is cyclic of order $a_i\frac{m}{r_i}$, say $\mathrm{Gal}(K_i/\mathbb{Q}) = \langle\sigma_i\rangle$. 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 $K = K_1K_2K_3K_4$. By the theory of Dirichlet characters, K is ramified exactly at primes p_i (with inertia subgroups isomorphic to $\mathrm{Gal}(K_i/\mathbb{Q})$) and

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

so that $[K : \mathbb{Q}] = a_1a_2a_3a_4\frac{m^4}{r_1r_2r_3r_4}$. 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 1 and Proposition 2 as definitions instead).

Theorem 14. *In the above notation, we have* $[K : k] = m$, $[K : kK_i] = r_i$, $[k \cap K_i : \mathbb{Q}] = a_i$ *and* $kK_iK_jK_l = K$ *(i.e. K is the genus field of k).*

Proof. Using Lemma 4 several times, we can compute

$$[K : k] = |\langle\tau\rangle| = \mathrm{lcm}\left(\frac{m}{r_i}, \frac{m}{r_j}, \frac{m}{r_l}\right) = m,$$

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

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

and

$$[K : kK_iK_jK_l] = |\langle \tau \rangle \cap \langle \sigma_h \rangle| = |\langle \tau^{\operatorname{lcm}\left(\frac{m}{r_i}, \frac{m}{r_j}, \frac{m}{r_l}\right)} \rangle| = |\langle \tau^m \rangle| = 1.$$

□