Circular numbers of certain abelian fields

Vladimír Sedláček

April 15, 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 abelian extension (i.e., finite Galois extension with an abelian Galois group) 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* $\mathrm{Gal}(K/\mathbb{Q}) \cong \prod_{p \in P} T_p$*, where T_p is the inertia subgroup of* $\mathrm{Gal}(K/\mathbb{Q})$ *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 $\mathrm{cond}\, k$.

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 by using the group law on G and extending linearly.

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

2 The group of circular numbers

Let k 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 $\mathrm{Gal}(K/k)$ has a natural action on K (given by evaluating an automorphism on an element), this makes K into a $\mathbb{Z}[\mathrm{Gal}(K/k)]$-module.

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

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

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

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

where N denotes the norm operator. 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:

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 σ in the inertia subgroup of $\mathrm{Gal}(K/k)$ corresponding to p.*

Proof. □

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

Lemma 5. *$D^+(k)$ is a subgroup of $D(k)$ given as*

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

hence canonically isomorphic to the non-torsion part of $D(k)$. The similar statement is true for $C^+(k)$ and $C(k)$.

Proof. □

Lemma 6. *The $\mathbb{Z}$-rank of D^+ 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. Let K be the genus field in the narrow sense of k. Let $G := \mathrm{Gal}(K/\mathbb{Q})$, 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:

- $H := \mathrm{Gal}(K/k)$,
- $m := |H|$,
- the canonical projections $\pi_i : G \to T_i$,
- $a_i := [T_i : \pi_i(H)]$,
- $r_i := |H \cap \ker \pi_i|$,
- $s_{ij} := |H \cap \ker(\pi_i \pi_j)|$,
- $n_i := \frac{m}{r_i}$,
- $\eta := \eta_{1234}$,
- 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.

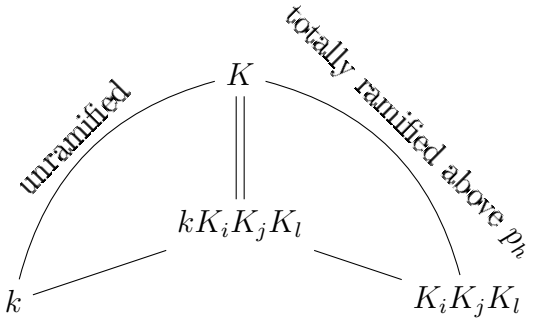
4 Auxiliary results

Lemma 7. *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. □

Lemma 8. *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 $\mathrm{Gal}(K_i/\mathbb{Q}) \cong T_i$ and $G = T_1 \times T_2 \times T_3 \times T_4$. □



Proposition 9. *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

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

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

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

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

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

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

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

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

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

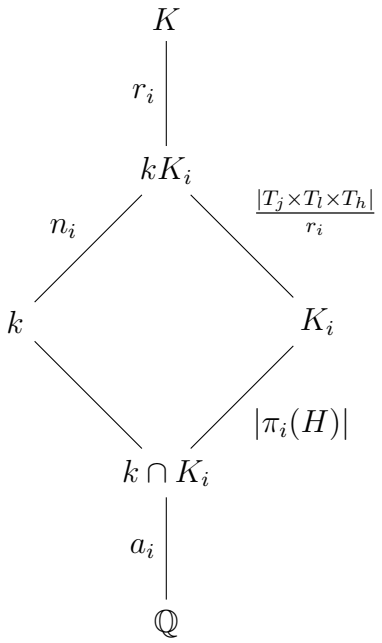
The last part of the statement is a consequence of Lemma 8, since we have

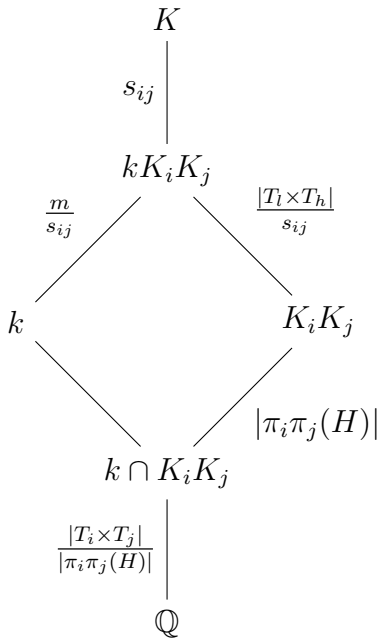
$$\mathrm{Gal}(K_iK_jK_l/k \cap K_iK_jK_l) \cong \mathrm{Gal}(kK_iK_jK_l/k) = \mathrm{Gal}(K/k) = H.$$

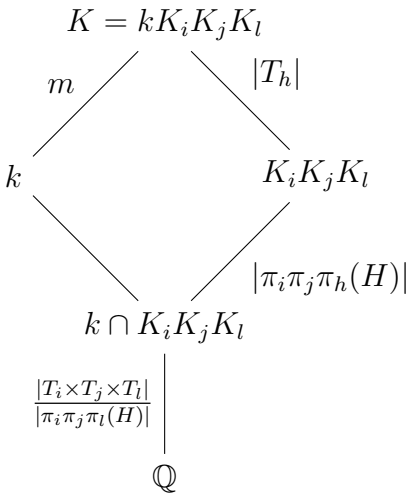
Finally note that in the same way as above, we could show that

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

(since Lemma 8 implies that $|H \cap T_h| = 1$). □







Corollary 10. *We have* $[k \cap K_iK_j : \mathbb{Q}] = a_ia_j\frac{m}{r_ir_j}s_{ij}$, $[k \cap K_iK_jK_l : \mathbb{Q}] = a_ia_ja_l\frac{m^2}{r_ir_jr_l}$ *and* $[k : \mathbb{Q}] = a_1a_2a_3a_4\frac{m^3}{r_1r_2r_3r_4}$.

Proof. This follows from the computations

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

$$[k \cap K_iK_jK_l : \mathbb{Q}] = \frac{[K_iK_jK_l : \mathbb{Q}]}{[K_iK_jK_l : k \cap K_iK_jK_l]} = \frac{|T_i| \cdot |T_j| \cdot |T_l|}{m} = a_ia_ja_l\frac{m^2}{r_ir_jr_l}$$

and

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

□

Lemma 11. *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 9 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 12. *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 10, 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 9) 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 10) 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 $\rho\sigma_4^{-x_4}\big|_k$ and $\sigma_3^{x_3}$ have the same restriction to $k \cap K_3K_4$. Therefore $\rho\sigma_3^{-x_3}\sigma_4^{-x_4}\big|_k \in \operatorname{Gal}(k/k \cap K_3K_4)$.

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 10) generated by $\sigma_2|_{k\cap K_2K_3K_4}$ (as a quotient of

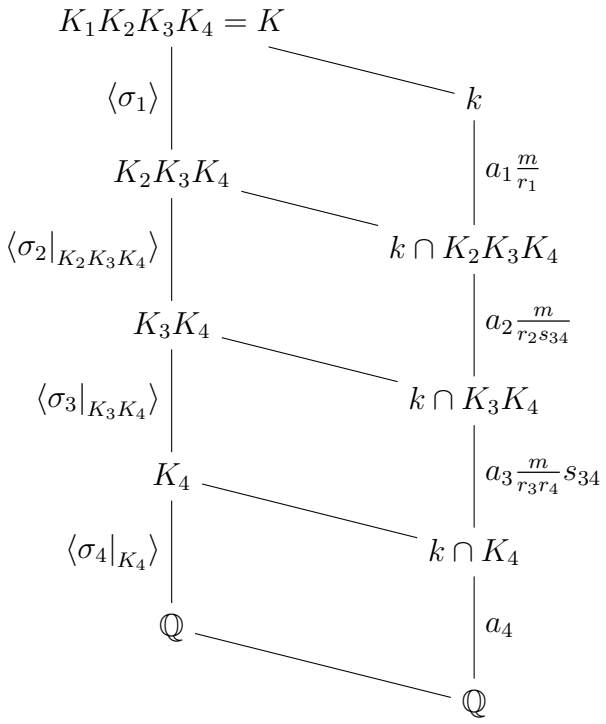
$$\operatorname{Gal}(K_2K_3K_4/K_3K_4) = \langle \sigma_2|_{K_2K_3K_4} \rangle),$$

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

Finally, we have

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

(using Lemma 8), 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 $\rho\sigma_2^{-x_2}\sigma_3^{-x_3}\sigma_4^{-x_4}\big|_k$ and $\sigma_1^{x_1}$ have the same restriction to k. Thus $\rho = \sigma_1^{x_1}\sigma_2^{x_2}\sigma_3^{x_3}\sigma_4^{x_4}|_k$ and the proof is finished.



□

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

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

Then the norm operators from k to a maximal subfield ramified at three primes can be given as R_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

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

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

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

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 $\mathbb{Z}$-linear combination of circular units belonging to subfields with less ramified primes. We will make use of this extensively.

Lemma 13. *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

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

(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

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

We will always refer to the conjugates of η by their coordinates x_1, x_2, x_3, x_4 according to Proposition 12. This allows us to visualise $\mathrm{Gal}(k/\mathbb{Q})$ 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:

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

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

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

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 $x_3 = n_3 - 1$ 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

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

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

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

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 $R_3 N_3 \sim 0$.

Next, we will sequentially recover all the cases

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

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

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

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

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

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

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

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 11, 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 their quotient is a power of $\eta^{\sigma_1^v \sigma_2^v}$ for some $v \in \mathbb{Z}$). Now consider the relations

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

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, 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

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

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 $\operatorname{lcm}(n_1, n_2)$ 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 $x_3 = a_3m - 1$. Finally, using the relation $R_3N_3 \sim 0$, we can now recover all the conjugates with $x_3 = a_3(m-1) - 1$ and we are done.

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

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

In this case, we have

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

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

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

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

(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

$$t \mid \gcd(n_1, n_2, n_3) \Leftrightarrow t \mid n_1, t \mid n_2, t \mid n_3 \Leftrightarrow r_1 \mid \frac{m}{t}, r_2 \mid \frac{m}{t}, r_3 \mid \frac{m}{t}$$
$$\Leftrightarrow \mathrm{lcm}(r_1, r_2, r_3) \mid \frac{m}{t} \Leftrightarrow t \mid \frac{m}{\mathrm{lcm}(r_1, r_2, r_3)},$$

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

"(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 $\mathrm{lcm}(r_1, r_2, r_3) = r_1 r_2 r_3$.

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

"(iii) $\Leftrightarrow$ (v)": We have $\frac{n_1n_2n_3}{m} = \frac{m^2}{r_1r_2r_3}$, which equals m iff $\frac{m}{r_1r_2r_3} = 1$.

"(iv) $\Rightarrow$ (vi)": For $\{i,j,l\} = \{1,2,3\}$, we have $\gcd(n_i,n_j) = \gcd(r_jr_l, r_ir_l) = r_ls_{ij} = r_l$.

"(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 $\frac{n_1n_2n_3}{m} = m = r_2n_2 = \gcd(n_1,n_3)n_2$ and we have

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

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

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

(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 $1 < x_3 \le n_3 - 1$, $x_1 = n_1 - 1$ or $x_2 = n_2 - 1$ using the relations $N_1 \sim 0, N_2 \sim 0$ and the cases $x_3 = 0$, $0 \le x_1 < n_1 - r_2 - 1$, $x_2 = n_2 - 1$ 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 use the notation $t := r_3, u := r_2, v := r_1$ (PROBABLY NOT?). 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 as being in the previous set.

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

$$D^+/\left\langle \{-1, \eta_I \middle| \emptyset \subsetneq I \subsetneq P\} \right\rangle_{\mathbb{Z}[\mathrm{Gal}(K/k)]}$$

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

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

We will write Q additively and for any $\rho \in \mathrm{Gal}(k/\mathbb{Q})$, we will denote the image 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 $2 \le q \le t+1$, we will denote the class of $\eta^{\sigma_1^{tu-2}\sigma_2^{q-2}}$ 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 $v + t - 2 \le q \le tv - 1$ we will denote the class of $\eta^{\sigma_1^{(t-1)u-1}\sigma_2^q}$ by Y_q. We will refer to the set of these $\eta^{\sigma_1^{(t-1)u-1}\sigma_2^q}$ with $v + t - 2 \le q \le tv - 1$ as the critical line.

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 $\frac{m}{n_3} = r_3 = t$ 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 15. *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 16. *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 alredy trivial in Q'). □

Now we will decompose our rectangle (of conjugates having $x_3 = x_4 = 0$) 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 $u \mid n_3, v \mid n_3$ and the conjugates contained in η^T are given by $\sigma_1^{qn_3}\sigma_2^{qn_3}$ for $0 \le q \le r_3 - 1$, the Chinese remainder theorem implies that η^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 $n_3 \pmod t$). We can be even more precise: the horizontal distance between $\eta^{\sigma_1^{qn_3}\sigma_2^{qn_3}}$ and $\eta^{\sigma_1^{(q+1)n_3}\sigma_2^{(q+1)n_3}}$ for $0 \le q \le r_3 - 1$ 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). It follows that the horizontal distance between any two conjugates in η^T with a vertical distance of one block is $\overline{u}/\overline{v}$ blocks.

Lemma 17. *For any $0 \le x_1 \le tu-1, 0 \le x_2 \le tv-1$, we have*

$$\sigma_1^{x_1}\sigma_2^{x_2}\cdot\mu = \begin{cases} 0 & \text{if } x_1 < u(t-1)-1 \\ & \quad \text{or } x_1 = u(t-1)-1, x_2 < v+t-2 \\ Y_{x_2} & \text{if } x_1 = u(t-1)-1, v+t-2 \le x_2 \\ X_{-x_1+x_2+1} & \text{if } t(u-1)-1 < x_1 < tu-1 \\ & \quad \text{or } x_1 = tu-1, x_2 \equiv q + \overline{u}/\overline{v}\cdot v \pmod{tv} \\ & \quad \text{for some } 0 \le q < v+t-2 \\ X_{-x_1+x_2+1} - Y_{x_2+(t-\overline{u}/\overline{v})\cdot v} & \text{if } x_1 = tu-1, x_2 \not\equiv q + \overline{u}/\overline{v}\cdot v \pmod{tv} \\ & \quad \text{for any } 0 \le q < v+t-2. \end{cases}$$

Proof. It is easy to see that our rectangle can be partitioned into $t = \gcd(n_1, n_2)$ (2D) diagonals, each going through exactly one of $\eta^{\sigma_1^{tu-2}\sigma_2^{q-2}}$ for $2 \le q \le t+1$ (two conjugates lie in the same diagonal iff their difference is a power of $\eta^{\sigma_1^q\sigma_2^q}$ for some $q \in \mathbb{Z}$). We will use this together with the fact that $\eta^{(1-\sigma_1\sigma_2)T}$ is trivial in Q to find the classes of all conjugates in our rectangle in terms of X_q, Y_q. More specifically, if $\eta^{\sigma_1^{x_1}\sigma_2^{x_2}(1-\sigma_1\sigma_2)T}$ contains no elements from the critical line, it is just a difference of two conjugates, hence their classes are the same. On the other hand, if it contains Y_q for some q and a difference of two conjugates, the classes of these two conjugates differ only by $\pm Y_q$ (depending on the sign of Y_q in $\eta^{\sigma_1^q\sigma_2^r(1-\sigma_1\sigma_2)T}$). Using the earlier observations, we can see that these are the only options, hence it follows that by going along each of the t 2D diagonals starting at $\eta^{\sigma_1^{tu-2}\sigma_2^{q-2}}$ for $2 \le q \le t+1$, will will obtain that ...Note that this implies that the action of $\sigma_1^{-x_1}\sigma_2^{x_2}$ on X_q results in $X_{q+x_1+x_2}$ (unless the result is 0 and ignoring all the Y's). □

Now it suffices to show that $X_q = 0$ for all $1 \le q \le t$ and $Y_q = 0$ for all $v+t-2 \le q \le tv-1$. To achieve this, we will use linear algebra.

Let $\alpha := Y_{v+t-2} + \cdots + Y_{tv-1}$ and $\beta := X_1 + X_2 + \cdots + X_t$.

Lemma 18. *We have $\alpha = \beta = 0$.*

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

$$0 = \sigma_1^{n_1 - r_1 - 1} N_2 \cdot \mu = \sum_{x_2=0}^{tv-1} \sigma_1^{t(u-1)} \sigma_2^{x_2} \cdot \mu = \alpha$$

and

$$0 = \sigma_1^{u(t-1)} N_2 \cdot \mu = \sum_{x_2=0}^{tv-1} \sigma_1^{u(t-1)} \sigma_2^{x_2} \cdot \mu = \sum_{x_2=0}^{tv-1} X_{-u(t-1)+x_2+1} = \sum_{x_2=0}^{tv-1} X_{x_2+u+1} = v \cdot \beta.$$

Similarly, using the relation $N_1 \sim 0$, we have

$$0 = N_1 \cdot \mu = \cdots = u \cdot \beta.$$

Since $\gcd(u, v) = 1$, this implies $\beta = 0$ by Bezout's identity. □

Next, for $0 \le q \le t-3$, we can see that taking the sum of all conjugates with $x_2 = q + r \cdot \overline{u}/\overline{v} \cdot v$ for $0 \le r \le t - \overline{u}/\overline{v} - 1$ (using the relation $N_1 \sim 0$) will result in 0 in Q. By construction, all the Y's involved will cancel out, and since $(t - \overline{u}/\overline{v}) \cdot v \equiv -\overline{u} \pmod{t}$, this implies (using $\beta = 0$) that $\Gamma_q = 0$ in Q, where

$$\Gamma_q := \sum_{r=0}^{t-\overline{u}/\overline{v}-1} \sum_{p=1}^{\overline{u}} X_{\overline{q+p-rv}}.$$

Similarly, taking the sum of all conjugates with $r \cdot \overline{u}/\overline{v} \cdot v \le x_2 \le v - 1 + r \cdot \overline{u}/\overline{v} \cdot v$ times r for $0 \le r \le t - \overline{u}/\overline{v} - 1$ gives us 0 (again using $N_1 \sim 0$), hence so does summing over all such r (where by construction all the Y's involved cancel out except for one of each, and their sum is zero anyway). Therefore we have (by using $(t - \overline{u}/\overline{v}) \cdot v \equiv -\overline{v} \pmod{t}$ and $\beta = 0$ again) $\Delta = 0$ in Q, where

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

Now we will construct a matrix M of type $t \times t$ as follows:

- The first row will consist of all 1's (corresponding to the relation β).
- The q-th row for $2 \leq q \leq t-1$ will correspond to the relation Γ_{q-2}.
- The last row will correspond to the relation Δ.

Since the rows of M are the coefficients of valid equlities in Q, we have $M \cdot X' = 0$, where $X = (X_1, \ldots, X_t)$ 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 L be the localization of the quotient ring $\mathbb{Z}[x]/(1 + x + x^2 + \cdots + x^{t-1})$ at the multiplicative subset generated by $x - 1$ and $x^{t-\overline{u}} - 1$. (By abuse of notation, we will denote the class of x in L also by x). Note that since

$$\gcd(x^t - 1, x^q - 1) = x^{\gcd(t,q)} - 1$$

for any $q \in \mathbb{Z}$ and $\gcd(t, 1) = \gcd(t, t - \overline{u}) = 1$, we have

$$\gcd(1 + x + x^2 + \cdots + x^{t-1}, x - 1) = \gcd(1 + x + x^2 + \cdots + x^{t-1}, x^{t-\overline{u}} - 1) = 1,$$

so that $x - 1$ nor $x^{t-\overline{u}} - 1$ are zero-divisors, hence L is nontrivial. Moreover let

$$D(x) := \sum_{q=1}^{t-1} q \cdot x^q \in L.$$

Lemma 19. *We have $D(x) \cdot (x - 1) = t$.*

Proof. This follows from the computation

$$\begin{aligned}
D(x) \cdot (x-1) &= \sum_{q=1}^{t-1} q \cdot x^{q+1} - \sum_{q=1}^{t-1} q \cdot x^q = \sum_{q=2}^{t} (q-1) \cdot x^q - \sum_{q=1}^{t-1} q \cdot x^q \\
&= (t-1)x^t + \sum_{q=1}^{t-1} (q-1) \cdot x^q - \sum_{q=1}^{t-1} q \cdot x^q \\
&= t \cdot x^t - x^t - \sum_{q=1}^{t-1} x^q \\
&= t - \sum_{q=0}^{t-1} x^q \\
&= t.
\end{aligned}$$

□

Lemma 20. *The coefficients of Γ_q are (up to a multiple of β) the coefficients of the polynomial $x^q \cdot P(x)$ and the coefficients of Δ are (up to a multiple of β) the coefficients of the polynomial $D \cdot P(x)$, where*

$$P(x) := -x^{\overline{u}} \cdot (1 + x + x^2 + \cdots + x^{\overline{v}-1}) \in L$$

(where the coefficient at X_{q+1} corresponds to the coefficient at x^q).

Proof. Since a cyclic shift of the indices of X_q corresponds to multiplication by x in L and $x^t = 1$ in L, the coefficients of Γ_q (up to a multiple of β) are

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

Similarly, using the substitution $y = x^{t-\overline{u}}$ (so that $y^m = 1$ in L), we can see that the coefficients of Δ (up to a multiple of β) are

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

□

Theorem 21. *M is unimodular, hence $X = 0$.*

Proof. Let ζ_t be a primitive t-th root of unity and let C be the corresponding $t \times t$ character matrix, i.e. $C = (\zeta_t^{r \cdot c})_{0 \le r,c < t}$. Then (after reindexing the dimensions of M from 0 to $t-1$)

we have $M \cdot C = C'$, where $C_{0,0} = t$ and the $c-th$ column of C' is

$$\begin{pmatrix} 0 \\ P(\zeta_t^c) \\ \zeta_t^c \cdot P(\zeta_t^c) \\ \zeta_t^{2c} \cdot P(\zeta_t^c) \\ \vdots \\ \zeta_t^{(t-3)c} \cdot P(\zeta_t^c) \\ D(\zeta_t^c) \cdot P(\zeta_t^c) \end{pmatrix}$$

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 $P(\zeta_t^c)$ from each of these columns, we get (since multiplication by $\overline{v}$ is an automorphism of $\mathbb{Z}/t$)

$$|\det C'| = |\det C''| \cdot \left| \prod_{0<c<t} P(\zeta_t^c) \right| = |\det C''| \cdot \left| \prod_{0<c<t} -\zeta_t^{c\overline{u}} \right| \cdot \left| \prod_{0<c<t} \frac{\zeta_t^{c\overline{v}} - 1}{\zeta_t^c - 1} \right| = |\det C''|,$$

where

$$C'' = \begin{pmatrix} t & 0 & \dots & 0 & \dots & 0 \\ * & 1 & \dots & 1 & \dots & 1 \\ * & \zeta_t & \dots & \zeta_t^c & \dots & \zeta_t^{t-1} \\ * & \zeta_t^2 & \dots & \zeta_t^{2c} & \dots & \zeta_t^{2(t-1)} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ * & \zeta_t^{t-3} & \dots & \zeta_t^{(t-3)c} & \dots & \zeta_t^{(t-3)(t-1)} \\ * & D(\zeta_t) & \dots & D(\zeta_t^c) & \dots & D(\zeta_t^{t-1}) \end{pmatrix}.$$

On the other hand, if we take the matrix C, add all of its rows to the last one (thus creating $\begin{pmatrix} t & 0 & 0 & \dots & 0 \end{pmatrix}$ there) and then add a suitable linear combination of rows $0, 1, \dots, t-3$ to the $t-2$-th row times -1 using the equality

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

so that the $t-2$-th row will become $\begin{pmatrix} * & D(\zeta_t) & \dots & D(\zeta_t^c) & \dots & D(\zeta_t^{t-1}) \end{pmatrix}$, 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

$$|\det C| = |\det C''| = |\det C'|,$$

which together with the invertibility of C (in fact it is well known that $\det C = \pm\sqrt{t^t}$) implies that $|\det M| = 1$, as needed. □

Corollary 22. *We have $Y_q = 0$ for all $v + t - 2 \leq q \leq tv - 1$.*

Proof. Take the sum of all conjugates with $x_2 = r \cdot \overline{u}/\overline{v} \cdot v$ for $r = 1$, then for $r = 2$, and so on. In each sum all the conjugates are 0 except the corresponding Y_q, so it must be zero as well. The result then follows by repeating the same procedure, only increasing x_2 in each of the sums by 1 each time. □

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 $\mathrm{Gal}(K_i/\mathbb{Q})$ is cyclic of order $a_i n_i$, 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 8 and Proposition 9 as definitions instead).

Theorem 23. *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 11 several times, we can compute

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

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

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

and

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

□