MASARYKOVA UNIVERZITA
PŘÍRODOVĚDECKÁ FAKULTA
ÚSTAV MATEMATIKY A STATISTIKY

Diplomová práce

BRNO 2017 VLADIMÍR SEDLÁČEK

MASARYKOVA UNIVERZITA
PŘÍRODOVĚDECKÁ FAKULTA
ÚSTAV MATEMATIKY A STATISTIKY

Kruhové jednotky abelovských těles

Diplomová práce

Vladimír Sedláček

Vedoucí práce: prof. RNDr. Radan Kučera, DSc. **Brno 2017**

Bibliografický záznam

Autor:	Vladimír Sedláček Přírodovědecká fakulta, Masarykova univerzita Ústav matematiky a statistiky
Název práce:	Kruhové jednotky abelovských těles
Studijní program:	Matematika
Studijní obor:	Algebra a diskrétní matematika
Vedoucí práce:	prof. RNDr. Radan Kučera, DSc.
Akademický rok:	2016/2017
Počet stran:	ix + ??
Klíčová slova:	kruhové jednotky; kruhová čísla, abelovská tělesa, Ennolovy relace, čtyři rozvětvená prvočísla

Bibliographic Entry

Author:	Vladimír Sedláček Faculty of Science, Masaryk University Department of Mathematics and Statistics
Title of Thesis:	Circular units of abelian fields
Degree Programme:	Mathematics
Field of Study:	Algebra and Discrete Mathematics
Supervisor:	prof. RNDr. Radan Kučera, DSc.
Academic Year:	2016/2017
Number of Pages:	ix + ??
Keywords:	circular units; circular numbers; abelian fields, Ennola relations, four ramified primes

Abstrakt

V této diplomové práci se zabýváme....

Abstract

In this thesis we study...

Místo tohoto listu vložte kopii oficiálního (podepsaného) zadání práce.

Poděkování

Prohlášení

Prohlašuji, že jsem svoji bakalářskou práci vypracoval samostatně pod vedením prof. RNDr. Radana Kučery, DSc. s využitím informačních zdrojů, které jsou v práci citovány.

Brno 15. května 2017 . . . .

Vladimír Sedláček

Contents

Overview of the used notation

For an easier orientation in the text, we present here the basic notation used throughout the thesis.

$\mathbb{C}$	množina všech komplexních čísel
$\mathbb{R}$	množina všech reálných čísel
$\mathbb{Z}$	množina všech celých čísel
$\mathbb{N}$	množina všech přirozených čísel

Introduction

Test interpunkce:

Žluťoučký kůň úpěl ďábelské ódy
ěščřžýáíéľťňďúů

Toto je nějaký úvodní text, ve kterém se obvykle popisuje struktura práce, cíle a případně i výsledky. Toto je nějaký úvodní text, ve kterém se obvykle popisuje struktura práce, cíle a případně i výsledky. Toto je nějaký úvodní text, ve kterém se obvykle popisuje struktura práce, cíle a případně i výsledky. Toto je nějaký úvodní text, ve kterém se obvykle popisuje struktura práce, cíle a případně i výsledky. Toto je nějaký úvodní text, ve kterém se obvykle popisuje struktura práce, cíle a případně i výsledky. Toto je nějaký úvodní text, ve kterém se obvykle popisuje struktura práce, cíle a případně i výsledky.

Toto je nějaký úvodní text, ve kterém se obvykle popisuje struktura práce, cíle a případně i výsledky. Toto je nějaký úvodní text, ve kterém se obvykle popisuje struktura práce, cíle a případně i výsledky. Toto je nějaký úvodní text, ve kterém se obvykle popisuje struktura práce, cíle a případně i výsledky. Toto je nějaký úvodní text, ve kterém se obvykle popisuje struktura práce, cíle a případně i výsledky. Toto je nějaký úvodní text, ve kterém se obvykle popisuje struktura práce, cíle a případně i výsledky. Toto je nějaký úvodní text, ve kterém se obvykle popisuje struktura práce, cíle a případně i výsledky. Toto je nějaký úvodní text, ve kterém se obvykle popisuje struktura práce, cíle a případně i výsledky.

Chapter 1

Preliminaries

1.1 Basic definitions and results

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

Theorem 1.2 (Kronecker-Weber)**.** *Every abelian field is a subfield of some cyclotomic field.*

Proof. See [5], page 321. $\square$

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. 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.

Because Definition 1.4 is not constructive, it will prove useful to have an alternate characterization.

Lemma 1.5. *Let $k \subseteq K$ be abelian fields, P be the set of ramified primes of k and for any $p \in P$, let e_p be ramification index of p in k and let T_p be the inertia subgroup of $\mathrm{Gal}(K/\mathbb{Q})$ corresponding to p. Assume that all the inertia subgroups of $\mathrm{Gal}(K/\mathbb{Q})$ are cyclic and for any $p \in P$, let K_p be the unique abelian field of degree $[K_p : \mathbb{Q}] = e_p$ ramified only at p. Then the following are equivalent (the products denote the composita of fields):*

1. *K is the genus field in the narrow sense of k (using Definition 1.4),*
2. *$K = \prod_{p\in P} K_p$,*
3. *$K = k\prod_{p\in P\setminus\{q\}} K_p$ for any $q \in P$,*
4. *$\mathrm{Gal}(K/\mathbb{Q}) \cong \prod_{p\in P} T_p$ and*

$$T_p = \mathrm{Gal}\left(K/\prod_{q\in P\setminus\{p\}} K_p\right) \cong \mathrm{Gal}\left(k/k\cap\prod_{q\in P\setminus\{p\}} K_p\right) \cong \mathrm{Gal}(K_p/\mathbb{Q})$$

for any $p \in P$.

5. *For any $p \in P$, K_p is the maximal subfield of K ramified only at p.*

Proof. The lemma is well known and follows from the isomorphism of the lattice of all abelian fields and the lattice of all finite subgroups of the group of all Dirichlet characters. More specifically, Theorem 3.5 from [5], page 24 is used here. We will briefly outline at least some of the implications that do not use Dirichlet characters directly.

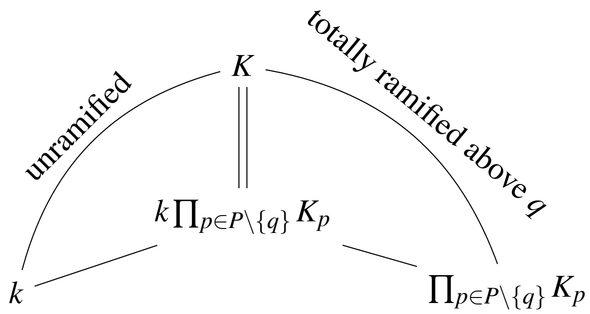
"(ii)+(iii) $\Leftrightarrow$ (iv)": This follows by elementary Galois theory, since $K_p \cap K_q = \mathbb{Q}$ for any $p, q \in P$.

"(ii) $\Leftrightarrow$ (v)": This is clear from the definition of ramification.

"(i) $\Rightarrow$ (iii)": Let $q \in P$ be fixed. The extension $K/\prod_{p\in P\setminus\{q\}} K_p$ is totally ramified at the prime ideals above q, so the same must be true for the extension

$$K/k \prod_{p\in P\setminus\{q\}} K_p.$$

But since the extension K/k is unramified by the definition of K, so is $K/k\prod_{p\in P\setminus\{q\}} K_p$. Therefore $[K : k\prod_{p\in P\setminus\{q\}} K_p] = 1$.



□

Remark 1.6. Note that for any $p \in P$, the field K_p in the statement of Lemma 1.5 is really determined uniquely, because by the ramification requirement, it must be a subfield of the cyclotomic field $\mathbb{Q}(\zeta_{p^f})$ for some $f \in \mathbb{N}$, whose absolute Galois group is isomorphic to $(\mathbb{Z}/p^f\mathbb{Z})^\times$, which is cyclic iff $p \geq 3$ or $f \leq 2$, and cyclic groups have at exactly one quotient group of any possible order. The assumption of the cyclicity of all inertia groups in the statement of the lemma is thus not required for $p \geq 3$ or $f \leq 2$, and can be also be removed for the other cases (but then there are three possible choices for K_2, so we must slightly change the statement).

Definition 1.7. 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 1.8. An element α of a totally real number field K is called totally positive if for any embedding $\sigma : K \to \mathbb{R}$, we have $\sigma(\alpha) > 0$.

1.2 The group of circular numbers

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

The following definition is equivalent to Lettl's modification of Sinnott's definition:

Definition 1.9. The group $D(k)$ of circular numbers of k is given as

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

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

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

where N denotes the norm operator and the product of fields denotes their compositum. The subgroup of totally positive elements of $D(k)$ will be denoted by $D^+(k)$.

Definition 1.10. The group $C(k)$ of circular numbers of k is $E(k) \cap D(k)$, where $E(k)$ is the group of units of the ring of algebraic integers of k. The subgroup of totally positive elements of $C(k)$ will be denoted by $C^+(k)$.

Remark 1.11. All the generators η_I of D are totally positive, because they are defined as norms of elements from an imaginary field to a real field. Hence they are images of a product of pairs of complex conjugate automorphisms, and as such they must become positive upon fixing an embedding $\sigma : k \to \mathbb{R}$. On the other hand, -1 is not totally positive and its product with any totally positive element is also not totally positive. This shows that

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

which is canonically isomorphic to the to torsion-free part of $D(k)$. Since $\mathbb{Z}$ is a principal ideal domain and $D(k)$ is finitely generated, this implies that $D^+(k)$ and consequently also $C^+(k)$ are free $\mathbb{Z}$-modules.

In [2], it is proven that the previous definition of $C(k)$ gives the same group as Sinnott's original definition in [4]. One of the reasons that $C(k)$ is important is the following result, due to Sinnott:

Theorem 1.12. *The index $[E(k) : C(k)]$ is finite.*

Proof. See [4], Theorem 4.1. □

Lemma 1.13.

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

Proof. Since all η_I are algebraic integers, it suffices to compute their absolute norm. We have

$$\begin{aligned} \mathrm{N}_{\prod_{i\in I} K_i \cap k/\mathbb{Q}}(\eta_I) &= \mathrm{N}_{\mathbb{Q}(\zeta_{\mathrm{cond}(\prod_{i\in I} K_i)})/\mathbb{Q}}(1-\zeta_{\mathrm{cond}(\prod_{i\in I} K_i)}) \\ &= \begin{cases} p & \text{if } \mathrm{cond}\left(\prod_{i\in I} K_i\right) \text{ is a power of a prime } p, \\ 1 & \text{otherwise} \end{cases} \end{aligned}$$

using the computation in [3], page 29. Now, we know that $\mathbb{Q}(\mathrm{cond}\left(\prod_{i\in I} K_i\right))$ is ramified at the same primes as $\prod_{i\in I} K_i$ (this follows from the fact that the intersection of cyclotomic fields is again a cyclotomic field), hence $\mathrm{N}_{\prod_{i\in I} K_i \cap k/\mathbb{Q}}(\eta_I) = 1$ iff $|I| > 1$. Moreover, for any I and any $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, we have $\mathrm{N}_{\prod_{i\in I} K_i \cap k/\mathbb{Q}}(\eta_I) = \mathrm{N}_{\prod_{i\in I} K_i \cap k/\mathbb{Q}}(\sigma(\eta_I))$, hence $\mathrm{N}_{\prod_{i\in I} K_i \cap k/\mathbb{Q}}(\eta_I^{1-\sigma}) = 1$, which proves the rest of the assertion. □

Corollary 1.14. *We have*

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

and

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

Proposition 1.15. *The $\mathbb{Z}$-rank of $D^+(k)$ is $[k:\mathbb{Q}] + |P| - 1$ and the $\mathbb{Z}$-rank of $C^+(k)$ is $[k:\mathbb{Q}] - 1$.*

Proof. By Dirichlet's unit theorem, the $\mathbb{Z}$-rank of $E(k)$ is $[k:\mathbb{Q}]-1$, since all the embeddings of k are real. Since the index $[E(k):C(k)]$ is finite by Theorem 1.12, the $\mathbb{Z}$-rank of $C(k)$ must be $[k:\mathbb{Q}]-1$ as well. Since $C^+(k)$ is isomorphic to the torsion-free part of $C(k)$, its $\mathbb{Z}$-rank must also be $[k:\mathbb{Q}]-1$

Now consider the quotient module $D^+(k)/C^+(k)$. By Lemma 1.13, it is generated as a $\mathbb{Z}$-module by the images of η_I for $|I| = 1$, hence it has exactly $|P|$ generators. Since the absolute norm of $\eta_{\{p\}}$ is a power of p, the elements η_I with $|I| = 1$ are multiplicatively independent (any nontrivial relation between them would give us a nontrivial multiplicative relation between powers of different primes, which is not possible). Moreover, since the absolute norm of all elements in C^+ is 1, the images of η_I remain multiplicatively independent in $D^+(k)/C^+(k)$. Thefore this quotient module has $\mathbb{Z}$-rank $|P|$, which implies that the $\mathbb{Z}$-rank of D^+ is $[k:\mathbb{Q}] + |P| - 1$ by the first part. □

1.3 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^+. We will also 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. Finally, for any $n \in \mathbb{N}$, ζ_n will denote a primitive n-th root of unity (WLOG we can take $\zeta_n = e^{2\pi i/n}$).

Let K be the genus field in the narrow sense of k and let $G := \mathrm{Gal}(K/\mathbb{Q})$. Then by Lemma 1.5, 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

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

by Lemma 1.5.)

We will assume the following:

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

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

1.4 Auxiliary results

Lemma 1.16. *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. $\square$

Proposition 1.17. *We have*

$$a_i = [k \cap K_i : \mathbb{Q}],$$

$$r_i = [K : kK_i],$$

$$|T_i| = a_i n_i,$$

$$s_{ij} = [K : kK_iK_j],$$
$$[K_i : k \cap K_i] = n_i,$$
$$[K_iK_j : k \cap K_iK_j] = \frac{m}{s_{ij}}$$

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 1.5, 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 1.5 implies that $|H\cap T_h| = 1$). $\square$

$$\begin{tikzcd}
 & K \arrow[d, dash, "r_i"'] & \\
 & kK_i \arrow[dl, dash, "n_i"'] \arrow[dr, dash, "\frac{|T_j\times T_l\times T_h|}{r_i}"] & \\
k \arrow[dr, dash] & & K_i \arrow[dl, dash, "|\pi_i(H)|"] \\
 & k\cap K_i \arrow[d, dash, "a_i"'] & \\
 & \mathbb{Q} &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & K \arrow[d, dash, "s_{ij}"'] & \\
 & kK_iK_j \arrow[dl, dash, "\frac{m}{s_{ij}}"'] \arrow[dr, dash, "\frac{|T_l\times T_h|}{s_{ij}}"] & \\
k \arrow[dr, dash] & & K_iK_j \arrow[dl, dash, "|\pi_i\pi_j(H)|"] \\
 & k\cap K_iK_j \arrow[d, dash, "\frac{|T_i\times T_j|}{|\pi_i\pi_j(H)|}"'] & \\
 & \mathbb{Q} &
\end{tikzcd}$$

$$\begin{tikzcd}
 & K = kK_iK_jK_l \arrow[dl, dash, "m"'] \arrow[dr, dash, "|T_h|"] & \\
k \arrow[dr, dash] & & K_iK_jK_l \arrow[dl, dash, "|\pi_i\pi_j\pi_h(H)|"] \\
 & k\cap K_iK_jK_l \arrow[d, dash, "\frac{|T_i\times T_j\times T_l|}{|\pi_i\pi_j\pi_l(H)|}"'] & \\
 & \mathbb{Q} &
\end{tikzcd}$$

Corollary 1.18. *We have*

$$[k \cap K_i K_j : \mathbb{Q}] = a_i a_j \frac{m}{r_i r_j} s_{ij},$$

$$[k \cap K_i K_j K_l : \mathbb{Q}] = a_i a_j a_l \frac{m^2}{r_i r_j r_l}$$

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

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

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

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 1.19. *We have*

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

and

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

Proof. It follows from Proposition 1.17 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

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

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

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

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

Similarly, we have

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

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

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

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

Finally, using the first result, we have

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

which clearly divides both $\frac{m}{r_i} = n_i$ and $\frac{m}{r_j} = n_j$. Moreover, if t is any common divisor of $n_i = \frac{m}{r_i}$ and $n_j = \frac{m}{r_j}$, then both r_it and r_jt divide m, hence $t \cdot \operatorname{lcm}(r_i, r_j) = \operatorname{lcm}(r_it, r_jt) \mid m$. Thus $t \mid \frac{m}{\operatorname{lcm}(r_i, r_j)}$ and we are done. □

Proposition 1.20. *We have*

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

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

Proof. First note that by Lemma 1.19, we have

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

and

$$a_2\frac{m}{r_2s_{34}} = a_2\operatorname{lcm}(r_3, r_4)\frac{m}{r_2r_3r_4} \in \mathbb{N}$$

(this follows from $r_i \mid m$ and $\gcd(r_2, r_3, r_4) = 1$), so the expressions make sense. By Corollary 1.18, 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.

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

Since $\mathrm{Gal}(k\cap K_4/\mathbb{Q})$ is a cyclic group of order a_4 (by Lemma 1.17) generated by $\sigma_4|_{k\cap K_4}$ (as a quotient of $\mathrm{Gal}(K_4/\mathbb{Q}) = \langle\sigma_4|_{K_4}\rangle$), there must exist a unique $x_4 \in \mathbb{Z}$, $0 \le x_4 < a_4$ such that ρ and $\sigma_4^{x_4}$ have the same restrictions to $k\cap K_4$. Therefore $\rho\sigma_4^{-x_4}\big|_k \in \mathrm{Gal}(k/k\cap K_4)$.

Next, $\mathrm{Gal}(k\cap K_3K_4/k\cap K_4)$ is a cyclic group of order $\frac{[k\cap K_3K_4:\mathbb{Q}]}{[k\cap K_4:\mathbb{Q}]} = a_3\frac{m}{r_3r_4}s_{34}$ (by Corollary 1.18) generated by $\sigma_3|_{k\cap K_3K_4}$ (as it is isomorphic by restriction to

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

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

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

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

(by Corollary 1.18) generated by $\sigma_2|_{k\cap K_2K_3K_4}$ (as it is isomorphic by restriction to

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

which is a quotient of

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

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

Finally, we have

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

(using Lemma 1.5), 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 $\rho = \sigma_1^{x_1}\sigma_2^{x_2}\sigma_3^{x_3}\sigma_4^{x_4}\big|_k$ and the proof is finished.

□

Chapter 2

The construction of bases of circular numbers and circular units

2.1 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 C^+). The generators of D^+ are subject to norm relations that correspond to the sum of all elements of the respective inertia groups T_i. Namely, let

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

Then the norm operator from K to $K_jK_lK_h$ can be given as R_iN_i, because both are equal to the sum of all elements from T_i. Moreover, Lemma 1.5 implies that

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

where the first isomorphism is given by restriction, hence R_iN_i also acts as the norm operator from k to $k \cap K_1K_2K_3$. If we denote the congruence corresponding to the canonical projection $\mathbb{Z}[G] \to \mathbb{Z}[G/H]$ by $\equiv$, then we have (using Lemma 1.16)

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

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 2.1. *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. It's clear that these fields are all real, abelian (their absolute Galois groups are quotients of G) and ramified at three primes. By symmetry, it suffices to prove the rest of the statement only for the field $k' := k\cap K_1K_2K_3$.

Now let K' be the genus field of k', and for any $i\in\{1,2,3\}$, let K'_i be the maximal subfield of K' ramified only at p_i and T'_i be the inertia subgroup of $\mathrm{Gal}(K'/\mathbb{Q})$ corresponding to p_i Then by Lemma 1.5, we have $K'_i\subseteq K_i$ (using the alternate characterization of K_i), hence $T'_i\cong\mathrm{Gal}(K'_i/\mathbb{Q})$ is isomorphic to a quotient of the cyclic group $\mathrm{Gal}(K/\mathbb{Q})\cong T_i$, so it must also be cyclic.

Finally note that by Lemma 1.5, we have $K' = K'_1K'_2K'_3\subseteq K_1K_2K_3$ and $kK_1K_2K_3 = K$, hence $\mathrm{Gal}(K'/k') = \mathrm{Gal}(K'_1K'_2K'_3/k\cap K_1K_2K_3)$ is a quotient of

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

which is cyclic. This concludes the proof.

$$\begin{tikzcd}
 & K = kK_1K_2K_3 \arrow[dl, dash] \arrow[dr, dash] & \\
k \arrow[ddr, dash] & & K_1K_2K_3 \arrow[d, dash] \\
 & & K' = K'_1K'_2K'_3 \arrow[dl, dash] \\
 & k' = k\cap K_1K_2K_3 \arrow[d, dash] & \\
 & \mathbb{Q} &
\end{tikzcd}$$

□

Using the results in [1], we can thus take the bases of

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

and we will denote their union by B_D. Analogously, we can take bases of

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

and denote their union by B_C.

To construct a basis of D^+ (resp. C^+), we will take the union of B_D (resp. B_C) with a set of suitably chosen conjugates of the highest generator η. In order to have a chance to obtain a basis, this set should contain

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

by Proposition 1.15 and using the principle of inclusion and exclusion (due to the fact that these bases were constructed "inductively").

We cannot guarantee at the moment that the union of all these conjugates is not linearly dependent, but if we will show how to obtain all the missing conjugates of η using the relations

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

it will follow that we really have a basis.

We will always refer to the conjugates of η by their coordinates x_1,x_2,x_3,x_4 according to Proposition 1.20. This allows us to visualise $\mathrm{Gal}(k/\mathbb{Q})$ geometrically as a discrete (at most) four-dimensional cuboid.

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

In this case, we have

$$\mathrm{Gal}(k/\mathbb{Q})\cong\{\sigma_1^{x_1}\sigma_2^{x_2}\sigma_3^{x_3}\sigma_4^{x_4}\big|_k;\ 0\le x_1<a_1m, 0\le x_2<a_2m, 0\le x_3<a_3m, 0\le x_4<a_4\},$$

$$s_{12}=s_{13}=s_{14}=s_{23}=s_{24}=s_{34}=1,$$

$$R_1N_1\sim 0, R_2N_2\sim 0, R_3N_3\sim 0, R_4\sum_{u=0}^{m-1}\sigma_1^{a_1u}\sigma_2^{a_2u}\sigma_3^{a_3u}\sim 0$$

and

$$\begin{aligned}N &= a_1a_2a_3a_4m^3-(a_1a_2a_3+a_1a_2a_4+a_1a_3a_4+a_2a_3a_4)m^2\\ &\quad +(a_1a_2+a_1a_3+a_1a_4+a_2a_3+a_2a_4+a_3a_4)m-a_1-a_2-a_3-a_4+1.\\ &= (a_1m-1)(a_2m-1)(a_3m-1)(a_4-1)+(a_1m-1)(a_2m-1)(a_3m-1)\\ &\quad -a_1a_2a_3m^2+(a_1a_2+a_1a_3+a_2a_3)m-a_1-a_2-a_3+1\\ &= (a_1m-1)(a_2m-1)(a_3m-1)(a_4-1)+(a_1m-1)(a_2(m-1)-1)(a_3m-1)\\ &\quad +(a_1-1)(a_3m-1)+a_3(m-1)\end{aligned}$$

We will define B_1 as the set of the following N conjugates $\eta^{\sigma_1^{x_1}\sigma_2^{x_2}\sigma_3^{x_3}\sigma_4^{x_4}}$:

- $0 \leq x_1 < a_1m-1, 0 \leq x_2 < a_2m-1, 0 \leq x_3 < a_3m-1, 1 \leq x_4 < a_4$,
- $0 \leq x_1 < a_1m-1, 0 \leq x_2 < a_2(m-1)-1, 0 \leq x_3 < a_3m-1, x_4 = 0$,
- $0 \leq x_1 < a_1-1, x_2 = a_2(m-1)-1, 0 \leq x_3 < a_3m-1, x_4 = 0$,
- $x_1 = a_1-1, x_2 = a_2(m-1)-1, 0 \leq x_3 < a_3(m-1), x_4 = 0$.

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

$$x_1 = a_1m-1, 0 \leq x_2 < a_2(m-1)-1, 0 \leq x_3 < a_3m-1$$

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

$$0 \leq x_1 < a_1m, 0 \leq x_2 < a_2(m-1)-1, x_3 = a_3m-1$$

and

$$0 \leq x_1 < a_1-1, x_2 = a_2(m-1)-1, x_3 = a_3m-1$$

using the relation $R_3N_3 \sim 0$.

At this moment, we are only missing the conjugates $\eta^{\sigma_1^{x_1}\sigma_2^{x_2}\sigma_3^{x_3}}$ with

$$a_1 \leq x_1 < a_1m, x_2 = a_2(m-1)-1, 0 \leq x_3 < a_3m,$$

$$0 \leq x_1 < a_1m, a_2(m-1) \leq x_2 < a_2m, 0 \leq x_3 < a_3m$$

and

$$x_1 = a_1-1, x_2 = a_2(m-1)-1, a_3(m-1) \leq x_3 < a_3m.$$

To continue, we need to define an auxiliary relation.

Let

$$\Gamma := \sigma_2^{a_2(m-2)} - \sum_{u=0}^{m-3}\sum_{v=1}^{u+1} \sigma_1^{a_1v}\sigma_2^{a_2u} \in \mathbb{Z}[G].$$

Lemma 2.2. *We have*

$$R_1R_2R_4\Gamma\sum_{u=0}^{m-1}\sigma_3^{a_3u} \sim 0.$$

Proof. We have

$$\begin{aligned}
\sigma_1^{a_1}\sigma_2^{a_2}\Gamma &= \sigma_1^{a_1}\sigma_2^{a_2(m-1)} - \sum_{u=1}^{m-2}\sum_{v=2}^{u+1}\sigma_1^{a_1v}\sigma_2^{a_2u} \\
&= \sigma_1^{a_1}N_2 - \sigma_1^{a_1}\sum_{u=0}^{m-2}\sigma_2^{a_2u} - \sum_{u=0}^{m-2}\sum_{v=2}^{u+1}\sigma_1^{a_1v}\sigma_2^{a_2u} \\
&= \sigma_1^{a_1}N_2 - \sum_{u=0}^{m-2}\sum_{v=1}^{u+1}\sigma_1^{a_1v}\sigma_2^{a_2u} \\
&= \sigma_1^{a_1}N_2 - \sigma_2^{a_2(m-2)} + \Gamma - \sum_{v=1}^{m-1}\sigma_1^{a_1v}\sigma_2^{a_2(m-2)} \\
&= \sigma_1^{a_1}N_2 - \sigma_2^{a_2}N_1 + \Gamma,
\end{aligned}$$

which implies

$$\sigma_1^{a_1}\sigma_2^{a_2}R_1R_2\Gamma \sim R_1R_2\Gamma.$$

Using this repeatedly, we obtain

$$R_1R_2R_4\Gamma\sum_{u=0}^{m-1}\sigma_3^{a_3} \sim R_1R_2\Gamma\left(R_4\sum_{u=0}^{m-1}\sigma_1^{a_1}\sigma_2^{a_2}\sigma_3^{a_3}\right) \sim 0,$$

as needed. □

Thanks to Lemma 2.2, we will recover all the cases

$$x_1 = a_1-1, x_2 = a_2(m-1)-1, a_3(m-1) \le x_3 < a_3m, x_4 = 0$$

using the relation $R_1R_2R_4\Gamma\sum_{u=0}^{m-1}\sigma_3^{a_3u}$.

Next, we will recover all the cases

$$0 \le x_1 < a_1m, a_2(m-1) \le x_2 < a_2m-1, 0 \le x_3 < a_3m, x_4 = 0$$

using the relation $R_4\sum_{u=0}^{m-1}\sigma_1^{a_1u}\sigma_2^{a_2u}\sigma_3^{a_3u}$, due to the fact that for any two different conjugates of η used in this relation, the difference of their exponents of σ_2 is divisible by a_2 (and we have already recovered all of them except exactly one). After this, we can recover the cases

$$0 \le x_1 < a_1, x_2 = a_2m-1, 0 \le x_3 < a_3m, x_4 = 0$$

using the relation $R_2N_2 \sim 0$.

Finally, we will use induction with respect to $v = 0,1,\ldots,m-1$ to show that we can recover the conjugates $\eta^{\sigma_1^{x_1}\sigma_2^{x_2}\sigma_3^{x_3}}$ with

$$va_1 \le x_1 < (v+1)a_1, x_2 = a_2(m-1)-1, 0 \le x_3 < a_3m, x_4 = 0$$

and

$$va_1 \le x_1 < (v+1)a_1, x_2 = a_2m-1, 0 \le x_3 < a_3m, x_4 = 0.$$

The basis step $v=0$ has already been done. Now suppose that the statement is true for $0<v<m-1$. Then we can recover the conjugates with

$$(v+1)a_1 \le x_1 < (v+2)a_1, x_2 = a_2m-1, 0 \le x_3 < a_3m, x_4 = 0$$

using the relation $R_4\sum_{u=0}^{m-1}\sigma_1^{a_1u}\sigma_2^{a_2u}\sigma_3^{a_3u}$, again due to the fact that for any two different conjugates of η used in this relation, the difference of their exponents of σ_2 is divisible by a_2 (and we have already recovered all of them except exactly one) and subsequently the conjugates with

$$(v+1)a_1 \le x_1 < (v+2)a_1, x_2 = a_2(m-1)-1, 0 \le x_3 < a_3m, x_4 = 0$$

using the relation $R_2N_2 \sim 0$. Therefore the induction is complete and we have recovered all the conjugates of η.

Thus we have proven the following theorem:

Theorem 2.3. *Under the assumptions on page 5, if $r_1=r_2=r_3=r_4=1$, then the set $B_1\cup B_D$ forms a basis of D^+ and the set $B_1\cup B_C$ forms a basis of C^+.*

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

In this case, we have

$$\mathrm{Gal}(k/\mathbb{Q}) \cong \{\sigma_1^{x_1}\sigma_2^{x_2}\sigma_3^{x_3}\sigma_4^{x_4}\big|_k;\ 0\le x_1<a_1m, 0\le x_2<a_2m, 0\le x_3<n_3, 0\le x_4<a_4\},$$
$$s_{12}=s_{13}=s_{14}=s_{23}=s_{24}=s_{34}=1,$$
$$R_1N_1\sim 0, R_2N_2\sim 0, N_3\sim 0, R_4\sum_{u=0}^{m-1}\sigma_1^{a_1u}\sigma_2^{a_2u}\sigma_3^{u}\sim 0$$

and

$$\begin{aligned}
N &= a_1a_2a_4\frac{m^3}{r_3} - a_1a_2a_4m^2 - (a_1a_2+a_1a_4+a_2a_4)\frac{m^2}{r_3}\\
&\quad + (a_1a_2+a_1a_4+a_2a_4)m + (a_1+a_2+a_4)\frac{m}{r_3} - a_1 - a_2 - a_4\\
&= (n_3-1)(a_1a_2a_4m^2 - (a_1a_2+a_1a_4+a_2a_4)m + a_1+a_2+a_4)\\
&= (n_3-1)(a_1a_2m^2 - (a_1a_2+a_1+a_2)m + a_1+a_2+1)\\
&\quad + (n_3-1)(a_4-1)(a_1a_2m^2 - a_1m - a_2m + 1)\\
&= (n_3-1)(a_4-1)(a_1m-1)(a_2m-1) + (n_3-1)(a_1m-1)(a_2(m-1)-1)\\
&\quad + (n_3-1)a_1
\end{aligned}$$

We will define B_2 as the set of the following N conjugates $\eta^{\sigma_1^{x_1}\sigma_2^{x_2}\sigma_3^{x_3}\sigma_4^{x_4}}$:

- $0\le x_1<a_1m-1, 0\le x_2<a_2m-1, 0\le x_3<n_3-1, 1\le x_4<a_4$,
- $0\le x_1<a_1m-1, 0\le x_2<a_2(m-1)-1, 1\le x_3<n_3, x_4=0$,
- $0\le x_1<a_1, x_2=a_2(m-1)-1, 1\le x_3<n_3, x_4=0$.

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 $R_1N_1\sim 0, R_2N_2\sim 0, N_3\sim 0$. From now on, we only need to deal with the cases where $x_4=0$.

Next, we will recover the cases

$$x_1 = a_1m-1, 0 \le x_2 < a_2(m-1)-1, 1 \le x_3 < n_3, x_4 = 0$$

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

$$0 \le x_1 < a_1m, 0 \le x_2 < a_2(m-1)-1, x_3 = x_4 = 0$$

and

$$0 \le x_1 < a_1, x_2 = a_2(m-1)-1, x_3 = x_4 = 0$$

using the relation $N_3 \sim 0$.

At this moment, we are only missing the conjugates $\eta^{\sigma_1^{x_1}\sigma_2^{x_2}\sigma_3^{x_3}}$ with

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

and

$$a_1 \le x_1 < a_1m, x_2 = a_2(m-1)-1, 0 \le x_3 < n_3.$$

Next, we will recover all the cases

$$0 \le x_1 < a_1m, a_2(m-1) \le x_2 < a_2m-1, 0 \le x_3 < n_3, x_4 = 0$$

using the relation $R_4 \sum_{u=0}^{m-1} \sigma_1^{a_1u}\sigma_2^{a_2u}\sigma_3^{u}$, due to the fact that for any two different conjugates of η used in this relation, the difference of their exponents of σ_2 is divisible by a_2 (and we have already recovered all of them except exactly one). After this, we can recover the cases

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

using the relation $R_2N_2 \sim 0$.

Finally, we will use induction with respect to $v = 0, 1, \dots, m-1$ to show that we can recover the conjugates $\eta^{\sigma_1^{x_1}\sigma_2^{x_2}\sigma_3^{x_3}}$ with

$$va_1 \le x_1 < (v+1)a_1, x_2 = a_2(m-1)-1, 0 \le x_3 < n_3, x_4 = 0$$

and

$$va_1 \le x_1 < (v+1)a_1, x_2 = a_2m-1, 0 \le x_3 < n_3, x_4 = 0.$$

The basis step $v = 0$ has already been done. Now suppose that the statement is true for $0 < v < m-1$. Then we can recover the conjugates with

$$(v+1)a_1 \le x_1 < (v+2)a_1, x_2 = a_2m-1, 0 \le x_3 < n_3, x_4 = 0$$

using the relation $R_4 \sum_{u=0}^{m-1} \sigma_1^{a_1u}\sigma_2^{a_2u}\sigma_3^{u}$, again due to the fact that for any two different conjugates of η used in this relation, the difference of their exponents of σ_2 is divisible by a_2 (and we have already recovered all of them except exactly one) and subsequently the conjugates with

$$(v+1)a_1 \le x_1 < (v+2)a_1, x_2 = a_2(m-1)-1, 0 \le x_3 < n_3, x_4 = 0$$

using the relation $R_2N_2 \sim 0$. Therefore the induction is complete and we have recovered all the conjugates of η.

Thus we have proven the following theorem:

Theorem 2.4. *Under the assumptions on page 5, if $r_1 = r_2 = a_3 = r_4 = 1$, then the set $B_2 \cup B_D$ forms a basis of D^+ and the set $B_2 \cup B_C$ forms a basis of C^+.*

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

In this case, we have

$$\mathrm{Gal}(k/\mathbb{Q}) \cong \{\sigma_1^{x_1}\sigma_2^{x_2}\sigma_3^{x_3}\sigma_4^{x_4}\big|_k;\ 0 \le x_1 < n_1, 0 \le x_2 < n_2, 0 \le x_3 < a_3 m, 0 \le x_4 < a_4\},$$

$$s_{12} = \gcd(r_1, r_2), s_{13} = s_{14} = s_{23} = s_{24} = s_{34} = 1$$

and

$$N_1 \sim 0, N_2 \sim 0, R_3 N_3 \sim 0, R_4 \sum_{u=0}^{m-1} \sigma_1^u \sigma_2^u \sigma_3^{a_3 u} \sim 0.$$

Moreover, by Lemma 1.19, we have $s_{12}\frac{m}{r_1 r_2} = \gcd(n_1, n_2)$, hence

$$\begin{aligned}
N &= a_3 a_4 \frac{m^3}{r_1 r_2} - a_3 \frac{m^2}{r_1 r_2} - a_4 \frac{m^2}{r_1 r_2} - a_3 a_4 \left(\frac{m^2}{r_1} + \frac{m^2}{r_2}\right) + s_{12}\frac{m}{r_1 r_2} \\
&+ a_3(n_1+n_2) + a_4(n_1+n_2) + a_3 a_4 m - a_3 - a_4 - 1 \\
&= a_3\left(m n_1 n_2 - n_1 n_2 - m n_1 - m n_2 + n_1 + n_2 + m - 1\right) - n_1 n_2 + n_1 + n_2 - 1 \\
&+ (a_4 - 1)(a_3\left(m n_1 n_2 - m n_1 - m n_2 + m\right) - n_1 n_2 + n_1 + n_2 - 1) + \gcd(n_1, n_2) - 1 \\
&= a_3(m-1)(n_1-1)(n_2-1) - (n_1-1)(n_2-1) \\
&+ (a_4-1)\left(a_3 m (n_1-1)(n_2-1) - (n_1-1)(n_2-1)\right) + \gcd(n_1,n_2) - 1 \\
&= (n_1-1)(n_2-1)(a_3(m-1)-1) \\
&+ (a_4-1)(n_1-1)(n_2-1)(a_3 m - 1) + \gcd(n_1,n_2) - 1.
\end{aligned}$$

We will define B_3 as the set of the following N conjugates $\eta^{\sigma_1^{x_1}\sigma_2^{x_2}\sigma_3^{x_3}\sigma_4^{x_4}}$:

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

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 $N_1 \sim 0, N_2 \sim 0, R_3 N_3 \sim 0$. From now on, we only need to deal with the cases where $x_4 = 0$.

Next, we will recover the cases $x_4 = 0, a_3 < x_3 < a_3 m$, $x_1 = n_1 - 1$ or $x_2 = n_2 - 1$ using the relations $N_1 \sim 0, N_2 \sim 0$. Now note that the exponents of σ_3 in $R_4 \sum_{u=0}^{m-1} \sigma_1^u \sigma_2^u \sigma_3^{a_3 u} \sim 0$ are pairwise congruent modulo a_3. Since for any $1 \le v < a_3$, we have already recovered all the conjugates with $x_3 \equiv v \pmod{a_3}$ except for one, we can also use the relation $R_4 \sum_{u=0}^{m-1} \sigma_1^u \sigma_2^u \sigma_3^{a_3 u} \sim 0$ several times to recover the cases

$$0 \le x_1 < n_1, 0 \le x_2 < n_2, 1 \le x_3 < a_3, x_4 = 0$$

as well.

At this moment, we are only missing the conjugates $\eta^{\sigma_1^{x_1}\sigma_2^{x_2}\sigma_3^{a_3}}$ for all

$$0 \le x_1 < n_1, 0 \le x_2 < n_2$$

and among the conjugates $\eta^{\sigma_1^{x_1}\sigma_2^{x_2}}$ we have only those with $0 < x_1 < gcd(n_1,n_2), x_2 = 0$ We will focus on recovering the remaining conjugates $\eta^{\sigma_1^{x_1}\sigma_2^{x_2}}$, because once we have those, we can recover those with $x_3 = a_3, x_4 = 0$ just by using the relation $R_3N_3 \sim 0$.

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

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

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

$$\begin{aligned} Q := Q'/\langle\{\eta^{\sigma_1^{x_1}\sigma_2^{x_2}\sigma_3^{x_3}\sigma_4^{x_4}};\quad & 0 \le x_1 < n_1, 0 \le x_2 < n_2, 0 \le x_3 < a_3m, 0 < x_4 < a_4,\\ & \text{or } 0 \le x_1 < n_1, 0 \le x_2 < n_2, 1 \le x_3 < a_3m, x_3 \ne a_3, x_4 = 0,\\ & \text{or } 1 \le x_1 < \gcd(n_1,n_2), x_2 = x_3 = x_4 = 0\}\rangle_{\mathbb{Z}}. \end{aligned}$$

We will write Q additively, denoting the class of η by μ, hence for any $\rho \in \mathrm{Gal}(k/\mathbb{Q})$ or $\rho \in \mathrm{Gal}(K/\mathbb{Q})$, 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. Since

$$0 = \sigma_1^{x_1}\sigma_2^{x_2}R_3N_3 \cdot \mu = \sigma_1^{x_1}\sigma_2^{x_2} \cdot \mu + \sigma_1^{x_1}\sigma_2^{x_2}\sigma_3^{a_3} \cdot \mu$$

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

Lemma 2.5. *In Q, we have*

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

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

Proof. Using the fact that the order of σ_3 is a_3m, we have

$$\begin{aligned} 0 &\sim \sigma_1^{x_1}\sigma_2^{x_2}\left(R_3R_4\sum_{u=0}^{m-1}\sigma_1^u\sigma_2^u\sigma_3^{a_3u} - \sigma_1\sigma_2R_4R_3N_3\right)\\ &= \sigma_1^{x_1}\sigma_2^{x_2}R_3R_4\sum_{u=0}^{m-1}\left(\sigma_1^u\sigma_2^u - \sigma_1\sigma_2\right)\sigma_3^{a_3u}\\ &= \sigma_1^{x_1}\sigma_2^{x_2}(1-\sigma_1\sigma_2)R_3R_4 + \sigma_1^{x_1}\sigma_2^{x_2}R_3R_4\sum_{u=2}^{m-1}\left(\sigma_1^u\sigma_2^u - \sigma_1\sigma_2\right)\sigma_3^{a_3u}\\ &= \sigma_1^{x_1}\sigma_2^{x_2}(1-\sigma_1\sigma_2) + \sigma_1^{x_1}\sigma_2^{x_2}(1-\sigma_1\sigma_2)R_3\sum_{u=1}^{a_4-1}\sigma_4^u\\ &\quad + \sigma_1^{x_1}\sigma_2^{x_2}(1-\sigma_1\sigma_2)\sum_{u=1}^{a_3-1}\sigma_3^u + \sigma_1^{x_1}\sigma_2^{x_2}R_3R_4\sum_{u=2}^{m-1}\left(\sigma_1^u\sigma_2^u - \sigma_1\sigma_2\right)\sigma_3^{a_3u} \end{aligned}$$

Since all the summands in the expression

$$\sigma_1^{x_1}\sigma_2^{x_2}(1-\sigma_1\sigma_2)R_3\sum_{u=1}^{a_4-1}\sigma_4^u+\sigma_1^{x_1}\sigma_2^{x_2}(1-\sigma_1\sigma_2)\sum_{u=1}^{a_3-1}\sigma_3^u$$
$$+\sigma_1^{x_1}\sigma_2^{x_2}R_3R_4\sum_{u=2}^{m-1}(\sigma_1^u\sigma_2^u-\sigma_1\sigma_2)\,\sigma_3^{a_3u}$$

have either $x_4>0$ or $1\le x_3<a_3m, x_3\ne a_3$ (where x_3 and x_4 denote the respective exponents of σ_3 and σ_4 in each term), the result of their action on μ becomes trivial in Q, which yields the result. □

Lemma 2.6. *For any $0\le x_1<n_1, 0\le x_2<n_2$, we have*

$$\sigma_1^{x_1}\sigma_2^{x_2}\cdot\mu=\begin{cases}\mu & \text{if } x_1\equiv x_2 \pmod{\gcd(n_1,n_2)}\\ 0 & \text{otherwise.}\end{cases}$$

Proof. First we will prove that for any $1\le u<\gcd(n_1,n_2)$ and $0\le v<\operatorname{lcm}(n_1,n_2)$, we have

$$\sigma_1^{u+v}\sigma_2^v\cdot\mu=0 \tag{2.1}$$

and

$$\sigma_1^v\sigma_2^v\cdot\mu=\mu. \tag{2.2}$$

We will do so simultaneously by induction on v. For $v=0$, this follows directly from the definitions of Q and μ. Now suppose that the statements hold for $0\le v<\operatorname{lcm}(n_1,n_2)-1$. Then Lemma 2.5 implies that

$$\sigma_1^{u+(v+1)}\sigma_2^{v+1}\cdot\mu=\sigma_1^{u+v}\sigma_2^v\cdot\mu=0$$

and

$$\sigma_1^{v+1}\sigma_2^{v+1}\cdot\mu=\sigma_1^v\sigma_2^v\cdot\mu=\mu$$

by the induction hypothesis, so both statements also hold for $v+1$ and we are done with the induction.

Now consider the map

$$\{0,1,\dots,\gcd(n_1,n_2)\}\times\{0,1,\dots,\operatorname{lcm}(n_1,n_2)\}\to\{0,1,\dots,n_1\}\times\{0,1,\dots,n_2\}$$

given by $(u,v)\mapsto(u+v \pmod{n_1}, v \pmod{n_2})$. Suppose that both (u,v) and (u',v') map to the same element. Then, for suitable $q,q'\in\mathbb{Z}$,

$$(u-u')+(v-v')=qn_1$$

and

$$v-v'=q'n_2,$$

hence

$$(u-u')=qn_1-q'n_2\equiv 0 \pmod{\gcd(n_1,n_2)}.$$

Since $0 \le u, u' \le \gcd(n_1,n_2)$, this implies $u = u'$. Consequently both n_1 and n_2 divide $v - v'$, hence so does $\mathrm{lcm}(n_1,n_2)$ and $v = v'$ (using that $0 \le v, v' \le \mathrm{lcm}(n_1,n_2)$). Thus we have shown that the above map is injective, and since both sets have cardinality $n_1 n_2$, it must be a bijection. Therefore for any $0 \le x_1 < n_1$, $0 \le x_2 < n_2$, we can write

$$\sigma_1^{x_1}\sigma_2^{x_2} \cdot \mu = \sigma_1^{u+v}\sigma_2^{v} \cdot \mu$$

for unique $0 \le u < \gcd(n_1,n_2)$ and $0 \le v < \mathrm{lcm}(n_1,n_2)$, and the equalities (2.1) and (2.2) imply that $\sigma_1^{x_1}\sigma_2^{x_2} \cdot \mu = 0$ unless $u = 0$, in which case $\sigma_1^{x_1}\sigma_2^{x_2} \cdot \mu = \mu$. But the congruences

$$x_1 \equiv u + v \pmod{n_1}$$

and

$$x_2 \equiv v \pmod{n_2}$$

imply that

$$x_1 - x_2 \equiv u \pmod{(\gcd(n_1,n_2))},$$

so the condition $u = 0$ is equivalent to

$$x_1 \equiv x_2 \pmod{(\gcd(n_1,n_2))},$$

as needed.

□

Proposition 2.7. *We have $\mu = 0$.*

Proof. Using the relation $N_1 \sim 0$ and Lemma 2.6 together with the bijection

$$\{0,1,\ldots,\gcd(n_1,n_2)-1\} \times \{0,1,\ldots,\frac{n_1}{\gcd(n_1,n_2)}-1\} \to \{0,1,\ldots,n_1-1\}$$

given by $(u,v) \mapsto v \cdot \gcd(n_1,n_2) + u$, we get

$$0 = N_1 \cdot \mu = \sum_{w=0}^{n_1-1} \sigma_1^{w} \cdot \mu = \sum_{u=0}^{\gcd(n_1,n_2)-1} \sum_{v=0}^{\frac{n_1}{\gcd(n_1,n_2)}-1} \sigma_1^{v\cdot\gcd(n_1,n_2)+u} \cdot \mu = \frac{n_1}{\gcd(n_1,n_2)} \cdot \mu,$$

since by Lemma 2.6, $\sigma_1^{v\cdot\gcd(n_1,n_2)+u} \cdot \mu$ is zero for $u \neq 0$ and equal to μ otherwise.

Analogously, we get

$$0 = N_2 \cdot \mu = \sum_{w=0}^{n_2-1} \sigma_2^{w} \cdot \mu = \sum_{u=0}^{\gcd(n_1,n_2)-1} \sum_{v=0}^{\frac{n_2}{\gcd(n_1,n_2)}-1} \sigma_2^{v\cdot\gcd(n_1,n_2)+u} \cdot \mu = \frac{n_2}{\gcd(n_1,n_2)} \cdot \mu,$$

since by Lemma 2.6, $\sigma_2^{v\cdot\gcd(n_1,n_2)+u} \cdot \mu$ is zero for $u \neq 0$ and equal to μ otherwise.

Due to the fact that $\frac{n_1}{\gcd(n_1,n_2)}$ and $\frac{n_2}{\gcd(n_1,n_2)}$ are coprime, this implies $\mu = 0$ by Bézout's identity. □

It now follows that Q is trivial, so we have proven the following theorem:

Theorem 2.8. *Under the assumptions on page 5, if $a_1 = a_2 = r_3 = r_4 = 1$, then the set $B_3 \cup B_D$ forms a basis of D^+ and the set $B_3 \cup B_C$ forms a basis of C^+.*

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

In this case, we have

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

$$s_{12} = \gcd(r_1, r_2), s_{13} = \gcd(r_1, r_3), s_{23} = \gcd(r_2, r_3), s_{14} = s_{24} = s_{34} = 1$$

and

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

Lemma 2.9. *For any $a, b, c \in \mathbb{Z}$, we have*

$$\mathrm{lcm}(a,b,c) = \frac{abc \cdot \gcd(a,b,c)}{\gcd(a,b) \cdot \gcd(a,c) \cdot \gcd(b,c)}.$$

Proof. Let $d := \gcd(a,b,c)$. Then there exist $a', b', c' \in \mathbb{Z}$ such that $a = da', b = db', c = dc'$ and $\gcd(a', b', c') = 1$. Letting $e := \gcd(a,b), f := \gcd(a,c), g := \gcd(b,c)$, we get that there must exist $a'', b'', c'' \in \mathbb{Z}$ such that $a = defa'', b = degb'', c = dfgc''$ and

$$\gcd(a'', b'') = \gcd(a'', c'') = \gcd(b'', c'') = 1.$$

Also the condition $\gcd(a', b', c') = 1$ can be reformulated as

$$\gcd(e, f) = \gcd(e, g) = \gcd(f, g) = 1.$$

Thus we get

$$\mathrm{lcm}(a,b,c) = defga''b''c'' = \frac{abcdefg}{d^3e^2f^2g^2} = \frac{abc \cdot d}{de \cdot df \cdot dg} = \frac{abc \cdot \gcd(a,b,c)}{\gcd(a,b) \cdot \gcd(a,c) \cdot \gcd(b,c)},$$

as needed. □

Lemma 2.10. *The following are equivalent:*

1. $\gcd(n_1, n_2, n_3) = \gcd(n_1, n_2)$,
2. $\frac{n_1 n_2 n_3}{m} = \gcd(n_1, n_3) \cdot \gcd(n_2, n_3)$,
3. $\gcd(n_1, n_2) = \gcd(\gcd(n_1, n_3), \gcd(n_2, n_3))$.

Proof.

"(i) ⇔ (ii)": Using Lemma 2.9 together with Lemma 1.19, we get

$$m = \mathrm{lcm}(n_1, n_2, n_3) = \frac{n_1 n_2 n_3 \cdot \gcd(n_1 n_2 n_3)}{\gcd(n_1, n_2) \cdot \gcd(n_1, n_3) \cdot \gcd(n_2, n_3)},$$

hence

$$\frac{n_1 n_2 n_3}{m} = \frac{\gcd(n_1, n_2) \cdot \gcd(n_1, n_3) \cdot \gcd(n_2, n_3)}{\gcd(n_1 n_2 n_3)}$$

and this equals $\gcd(n_1, n_3) \cdot \gcd(n_2, n_3)$ iff $\gcd(n_1, n_2, n_3) = \gcd(n_1, n_2)$.

"(i) ⇔ (iii)": It suffices to show that $\gcd(n_1,n_2,n_3) = \gcd(\gcd(n_1,n_3),\gcd(n_2,n_3))$. This is true in general, because any integer is a common divisor of n_1,n_2,n_3 iff it is a common divisor of n_1,n_3 and a common divisor of n_2,n_3 iff it is a common divisor of $\gcd(n_1,n_3)$ and $\gcd(n_2,n_3)$ iff it is a common divisor of $\gcd(\gcd(n_1,n_3),\gcd(n_2,n_3))$.

□

Therefore, using Lemma 2.10 together with Lemma 1.19, we get

$$N = a_4n_1n_2n_3 - \frac{n_1n_2n_3}{m} - a_4(n_1n_2+n_1n_3+n_2n_3) - a_4 - 2 + a_4(n_1+n_2+n_3)$$
$$+\gcd(n_1,n_2)+\gcd(n_1,n_3)+\gcd(n_2,n_3)$$
$$=(a_4-1)(n_1-1)(n_2-1)(n_3-1)+(n_1-1)(n_2-1)(n_3-2)+(n_1-1)(n_2-1)-2$$
$$-\gcd(n_1,n_3)\cdot\gcd(n_2,n_3)+\gcd(n_1,n_2)+\gcd(n_1,n_3)+\gcd(n_2,n_3)$$
$$=(a_4-1)(n_1-1)(n_2-1)(n_3-1)+(n_1-1)(n_2-1)(n_3-2)$$
$$+(n_1-1)(n_2-\gcd(n_2,n_3)+(n_1-\gcd(n_1,n_3))\cdot(\gcd(n_2,n_3)-1)+\gcd(n_1,n_2)-1$$

We will define B_4 as the set of the following N conjugates $\eta^{\sigma_1^{x_1}\sigma_2^{x_2}\sigma_3^{x_3}\sigma_4^{x_4}}$:

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

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

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

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

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

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

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

We will write Q additively, denoting the class of η by μ, hence for any $\rho \in \mathrm{Gal}(k/\mathbb{Q})$ or $\rho \in \mathrm{Gal}(K/Q)$, 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. Since

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

for any $x_1, x_2 \in \mathbb{Z}$, this is equivalent with showing that $\sigma_1^{x_1}\sigma_2^{x_2} \cdot \mu = 0$ for each $0 \le x_1 < n_1$, $0 \le x_2 < n_2$ (and because of the definition of Q, it suffices to show this only for each $0 \le x_1 < \gcd(n_1,n_3)$, $0 \le x_2 < \gcd(n_2,n_3)$).

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 (and in this case, it can be seen geometrically that these form a regular grid). We will now describe the sum of these.

Let

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

Lemma 2.11. *In Q, we have*

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

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

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

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

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

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

Since all the summands in the expression

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

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

Lemma 2.12. *For any* $0\le x_1<\gcd(n_1,n_3), 0\le x_2<\gcd(n_2,n_3)$, *we have*

$$\sigma_1^{x_1}\sigma_2^{x_2}\cdot\mu=\begin{cases}\mu & \text{if } x_1\equiv x_2 \pmod{\gcd(n_1,n_2)}\\ 0 & \text{otherwise.}\end{cases}$$

Proof. Let $0\le x_1<\gcd(n_1,n_3), 0\le x_2<\gcd(n_2,n_3)$ be arbitrary. For the same reasons as in the proof of Lemma 2.6, we can write

$$\sigma_1^{x_1}\sigma_2^{x_2}\cdot\mu=\sigma_1^{u+v}\sigma_2^{v}\cdot\mu,$$

where $0\le u<\gcd(n_1,n_2)$ (by Lemma 2.10) and $0\le v<\operatorname{lcm}(n_1,n_2)$. Moreover, by Lemma 2.11, we have

$$\begin{aligned}\sigma_1^{u+v}\sigma_2^{v}T\cdot\mu&=\sigma_1^{u+v-1}\sigma_2^{v-1}T\cdot\mu=\cdots=\sigma_1^{u+1}\sigma_2T\cdot\mu=\sigma_1^uT\cdot\mu\\&=\sum_{w=0}^{r_3-1}\sigma_1^{wn_3+u}\sigma_2^{wn_3}\cdot\mu=\sigma_1^u\cdot\mu,\end{aligned}$$

where we used the definition of Q and the fact that n_3 is divisible by

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

by Lemma 2.10 The assertion now follows from the definition of Q, since

$$u\equiv x_1-x_2 \pmod{\gcd(n_1,n_2)}.$$

□

Proposition 2.13. *We have* $\mu=0$.

Proof. Recall that we have

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

by Lemma 2.10. Using the relation $N_1\sim 0$ and Lemma 2.6 together with the bijection

$$\{0,1,\dots,\gcd(n_1,n_2)-1\}\times\{0,1,\dots,\frac{\gcd(n_1,n_3)}{\gcd(n_1,n_2)}-1\}\to\{0,1,\dots,\gcd(n_1,n_3)-1\}$$

given by $(u,v)\mapsto v\cdot\gcd(n_1,n_2)+u$, we get

$$0=N_1\cdot\mu=\sum_{w=0}^{\gcd(n_1,n_3)-1}\sigma_1^w\cdot\mu=\sum_{u=0}^{\gcd(n_1,n_2)-1}\sum_{v=0}^{\frac{\gcd(n_1,n_3)}{\gcd(n_1,n_2)}-1}\sigma_1^{v\cdot\gcd(n_1,n_2)+u}\cdot\mu=\frac{\gcd(n_1,n_3)}{\gcd(n_1,n_2)}\cdot\mu,$$

since by Lemma 2.6, $\sigma_1^{v\cdot\gcd(n_1,n_2)+u}\cdot\mu$ is zero for $u\neq 0$ and equal to μ otherwise.

Analogously, we get

$$0 = N_2\cdot\mu = \sum_{w=0}^{\gcd(n_2,n_3)-1}\sigma_2^w\cdot\mu = \sum_{u=0}^{\gcd(n_1,n_2)-1}\sum_{v=0}^{\frac{\gcd(n_2,n_3)}{\gcd(n_1,n_2)}-1}\sigma_2^{v\cdot\gcd(n_1,n_2)+u}\cdot\mu = \frac{\gcd(n_2,n_3)}{\gcd(n_1,n_2)}\cdot\mu,$$

since by Lemma 2.6, $\sigma_2^{v\cdot\gcd(n_1,n_2)+u}\cdot\mu$ is zero for $u\neq 0$ and equal to μ otherwise.

Due to the fact that $\frac{\gcd(n_1,n_3)}{\gcd(n_1,n_2)}$ and $\frac{\gcd(n_2,n_3)}{\gcd(n_1,n_2)}$ are coprime, this implies $\mu = 0$ by Bézout's identity. □

It now follows that Q is trivial, so we have proven the following theorem:

Theorem 2.14. *Under the assumptions on page 5, if*

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

then the set $B_4\cup B_D$ forms a basis of D^+ and the set $B_4\cup B_C$ forms a basis of C^+.

2.6 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

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

$$s_{12} = s_{13} = s_{14} = s_{23} = s_{24} = s_{34} = 1$$

and

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

Note that the condition $r_1\neq 1, r_2\neq 1, r_3\neq 1$ is actually not restrictive, since we have already discussed the cases where it is not true earlier in this chapter.

Lemma 2.15. *Under the assumptions $s_{12} = s_{13} = s_{23} = 1$, the following are equivalent:*

1. $\gcd(n_1,n_2,n_3) = 1$,
2. $\mathrm{lcm}(r_1,r_2,r_3) = m$,
3. $r_1r_2r_3 = m$,
4. $n_1 = r_2r_3, n_2 = r_1r_3, n_3 = r_1r_2$,
5. $\frac{n_1n_2n_3}{m} = m$,
6. $\gcd(n_1,n_2) = r_3, \gcd(n_1,n_3) = r_2, \gcd(n_2,n_3) = r_1$.

Proof.

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

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

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

"(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 $r_1r_2r_3$, hence $\operatorname{lcm}(r_1,r_2,r_3) = r_1r_2r_3$.

"(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.

$\square$

Thus $\frac{n_1n_2n_3}{m} = m = r_2n_2 = \gcd(n_1,n_3)n_2$ by Lemma 2.15 and using Lemma 1.19, we get

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

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

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

(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 $x_2 = n_2-1$ (and always $x_4 = 0$) using the relations $N_1 \sim 0, N_2 \sim 0$ and the cases $x_3 = x_4 = 0$, $0 \le x_1 < n_1-r_2-1$, $x_2 = n_2-1$ using the relation $N_2 \sim 0$.

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

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

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

and similarly h' to be the unique integer satisfying

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

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

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

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

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

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

We will write Q additively, denoting the class of η by μ, hence for any $\rho \in \mathrm{Gal}(k/\mathbb{Q})$ or $\rho \in \mathrm{Gal}(K/Q)$, 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. Since

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

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

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

Let

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

Lemma 2.16. *In Q, we have*

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

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

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

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

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

$$0 \sim \sigma_1^{x_1} \sigma_2^{x_2} \left(R_4 T \sum_{v=0}^{n_3-1} \sigma_1^v \sigma_2^v \sigma_3^v - \sigma_1 \sigma_2 N_3 R_4 T \right) = \sigma_1^{x_1} \sigma_2^{x_2} R_4 T \sum_{v=0}^{n_3-1} \left(\sigma_1^v \sigma_2^v - \sigma_1 \sigma_2 \right) \sigma_3^v$$

$$= \sigma_1^{x_1} \sigma_2^{x_2} (1 - \sigma_1 \sigma_2) R_4 T + \sigma_1^{x_1} \sigma_2^{x_2} R_4 T \sum_{v=2}^{n_3-1} \left(\sigma_1^v \sigma_2^v - \sigma_1 \sigma_2 \right) \sigma_3^v$$

$$= \sigma_1^{x_1} \sigma_2^{x_2} (1 - \sigma_1 \sigma_2) T + \sigma_1^{x_1} \sigma_2^{x_2} (1 - \sigma_1 \sigma_2) T \sum_{u=1}^{a_4-1} \sigma_4^u + \sigma_1^{x_1} \sigma_2^{x_2} R_4 T \sum_{v=2}^{n_3-1} \left(\sigma_1^v \sigma_2^v - \sigma_1 \sigma_2 \right) \sigma_3^v.$$

Since all the summands in the expression

$$\sigma_1^{x_1} \sigma_2^{x_2} (1 - \sigma_1 \sigma_2) T \sum_{u=1}^{a_4-1} \sigma_4^u + \sigma_1^{x_1} \sigma_2^{x_2} R_4 T \sum_{v=2}^{n_3-1} \left(\sigma_1^v \sigma_2^v - \sigma_1 \sigma_2 \right) \sigma_3^v$$

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

The rest of the proof will be carried out purely algebraically, but perhaps it is helpful (although not strictly required) to see some of its parts geometrically.

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

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

Lemma 2.17. *We have $X_q = X_{q'}$ for any $q \equiv q' \pmod{r_3}$. Moreover, for any $0 \le x_1 < n_1$, $0 \le x_2 < n_2$, we have*

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

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

Now for every $0 \le u < n_2$, we will prove by induction with respect to $v = 0,1,\ldots,r_2-2$ that

$$\sigma_1^{n_1-2-v}\sigma_2^{u-v} \cdot \mu = X_u. \tag{2.3}$$

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

$$\left(\sigma_1^{n_1-2-v}\sigma_2^{u-v}(1-\sigma_1\sigma_2)\sum_{w=0}^{r_3-1}\sigma_1^{wn_3}\sigma_2^{wn_3}\right) \cdot \mu = 0, \tag{2.4}$$

which follows from Lemma 2.16, we claim that all the terms with $w > 0$ do not contribute anything to the sum. Indeed, all the exponents of σ_1 are pairwise congruent modulo r_2 (since $r_2 \mid n_3$), and since $n_1-r_2 \le n_1-2-v < n_1-2$ and $n_1-r_2+1 \le n_1-1-v < n_1-1$, we have

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

for any $w > 0$, because r_3 does not divide wn_3 in this case. Hence (2.4) implies that

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

therefore $\sigma_1^{n_1-2-v}\sigma_2^{u-v} \cdot \mu = X_u$ by the induction hypothesis. This completes the induction, so (2.3) holds.

Now for any $0 \le u < n_2$, we will take $v = r_2-1$ in (2.4). Again, since all the exponents of σ_1 are pairwise congruent modulo r_2 (since $r_2 \mid n_3$) in this sum, the only terms which could be nonzero are those arising from $w = 0$ and from w satisfying

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

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

Thus we have

$$\begin{aligned}
0 &= \left(\sigma_1^{n_1-r_2-1}\sigma_2^{u-r_2+1}(1-\sigma_1\sigma_2)+\sigma_1^{n_1-1}\sigma_2^{u-r_2+1+h\cdot r_1}(1-\sigma_1\sigma_2)\right)\cdot\mu \\
&= \underbrace{\sigma_1^{n_1-r_2-1}\sigma_2^{u-r_2+1}\cdot\mu}_{=Y_{u-r_2+1}} - \underbrace{\sigma_1^{n_1-r_2}\sigma_2^{u-r_2+2}\cdot\mu}_{=X_u \text{ due to (2.3)}} + \sigma_1^{n_1-1}\sigma_2^{u-r_2+1+h\cdot r_1}\cdot\mu \\
&\quad - \underbrace{\sigma_1^{n_1}\sigma_2^{u-r_2+1+h\cdot r_1+1}\cdot\mu}_{=0}.
\end{aligned}$$

Therefore

$$\sigma_1^{n_1-1}\sigma_2^{u-r_2+1+h\cdot r_1}\cdot\mu = X_u - Y_{u-r_2+1}. \tag{2.5}$$

Finally, for any $0\le u<n_2$, we will take $v=r_2$ in (2.4). Again, since all the exponents of σ_1 are pairwise congruent modulo r_2 in this sum, we only get nonzero terms for $w=0$ and for w satisfying

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

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

Thus we have

$$0=\underbrace{\sigma_1^{n_1-r_2-2}\sigma_2^{u-r_2}\cdot\mu}_{=0}-\underbrace{\sigma_1^{n_1-r_2-1}\sigma_2^{u-r_2+1}\cdot\mu}_{=Y_{u-r_2+1}}+\underbrace{\sigma_1^{n_1-2}\sigma_2^{u-r_2+h\cdot r_1}\cdot\mu}_{=X_{u-r_2+h\cdot r_1}}-\underbrace{\sigma_1^{n_1-1}\sigma_2^{u-r_2+1+h\cdot r_1}\cdot\mu}_{=X_u-Y_{u-r_2+1}\text{ due to (2.5)}}.$$

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

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

and

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

Since $\gcd(-r_2,r_1)=1$ and $n_2=r_1r_3$, this means that for all $q,q'\in\mathbb{Z}$ satisfying

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

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

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

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

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

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

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

we get $0 \le v \le r_2 - 2$ and the equality (1) implies

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

because $r_3 \mid n_1$.

Similarly, for $x_1 = n_1 - 1$ and any $0 \le x_2 < n_2$, denoting $u = x_2 + r_2 - 1 - h \cdot r_1$, the equality (2.5) implies that

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

since

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

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

This concludes the proof. □

Thanks to Lemma 2.17, from now on we will regard the indices of the X's only modulo r_3. The lemma also implies the equality

$$\sigma_1^{n_1-1}\sigma_2^{x_2} \cdot \mu + \sigma_1^{n_1-r_2-1}\sigma_2^{x_2-h\cdot r_1} \cdot \mu = X_{x_2-1} - Y_{x_2-h\cdot r_1} + Y_{x_2-h\cdot r_1} = X_{x_2-1} \tag{2.6}$$

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

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

Let $\alpha := Y_{r_1+r_3-2} + Y_{r_1+r_3-1} + \cdots + Y_{n_2-1} \in Q$ and $\beta := X_0 + X_1 + \cdots + X_{r_3-1} \in Q$.

Lemma 2.18. *We have $\alpha = \beta = 0$.*

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

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

and

$$\begin{aligned} 0 = \sigma_1^{r_2(r_3-1)} N_2 \cdot \mu &= \sum_{x_2=0}^{n_2-1} \sigma_1^{r_2(r_3-1)}\sigma_2^{x_2} \cdot \mu = \sum_{x_2=0}^{n_2-1} X_{x_2-r_2(r_3-1)-2} \\ &= \sum_{x_2=0}^{r_1r_3-1} X_{x_2+r_2-2} = \sum_{u=0}^{r_1-1}\sum_{v=0}^{r_3-1} X_{ur_3+v+r_2-2} = r_1 \cdot \sum_{v=0}^{r_3-1} X_{v+r_2-2} = r_1 \cdot \beta, \end{aligned}$$

since each $x_2 \in \{0,1,\dots,r_1r_3-1\}$ can be uniquely written as ur_3+v, where $0 \le u < r_1$, $0 \le v < r_3$.

Similarly, using Lemma 2.17 together with the relation $N_1 \sim 0$ and the equality (2.6), we get

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

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

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

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

Lemma 2.19. *For any $0 \le q \le r_3-3$, we have $\Gamma_q = 0$.*

Proof. Using Lemma 2.17, the relation $N_1 \sim 0$ and the equality (2.6), we get

$$\begin{aligned}
0 &= \sum_{u=0}^{r_3-h'-1} \sigma_2^{q-uhr_1} N_1 \cdot \mu \\
&= \sum_{u=0}^{r_3-h'-2} \underbrace{\left(\sigma_1^{n_1-1}\sigma_2^{q-uhr_1} + \sigma_1^{r_2(r_3-1)-1}\sigma_2^{q-(u+1)hr_1}\right)\cdot \mu}_{=X_{q-uhr_1-1} \text{ due to (2.6)}} \\
&+ \underbrace{\sigma_1^{r_2(r_3-1)-1}\sigma_2^{q}\cdot\mu}_{=Y_q} + \underbrace{\sigma_1^{n_1-1}\sigma_2^{q-(r_3-h'-1)hr_1}\cdot\mu}_{=X_{q-(r_3-h'-1)hr_1-1}-Y_{q+r_1}} \\
&+ \sum_{x_1=r_2(r_3-1)}^{n_1-2} \sum_{u=0}^{r_3-h'-1} \sigma_1^{x_1}\sigma_2^{q-uhr_1} \cdot \mu.
\end{aligned}$$

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

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

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

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

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

Continuing with the previous equality and using the congruence $hr_1 \equiv r_2 \pmod{r_3}$ and Lemma 2.17, we thus have

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

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

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

since $\beta = 0$ by Lemma 2.18. □

Finally, let

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

Lemma 2.20. *We have $\Delta = 0$.*

Proof. Using Lemma 2.17, the relation $N_1 \sim 0$ and the equality (2.6), we get

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

where we used the fact that

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

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

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

such that

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

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

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

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

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

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

After using the equality $\alpha = 0$ by Lemma 2.18 and the substitutions $v = n_1 - 1 - x_1$, $w = x_2$. this becomes

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

since $\beta = 0$ by Lemma 2.18. $\square$

For any linear combination of the X_u's, we can take the indices of all X_u in the set $\{0,1,\ldots,r_3-1\}$ (since $X_u = X_{\overline{u}}$ by Lemma 2.17) and write the linear combination as $\sum_{c=0}^{r_3-1} c_u X_u$. By definition, β, Γ_q and Δ are such linear combinations, and thus correspond to the r_3-tuples of integer coefficients $(c_1, c_2, \ldots, c_{r_3})$. Using this correspondence, we will now construct a matrix M of size $r_3 \times r_3$ (indexing its dimensions from 0 to $r_3 - 1$) as follows:

- The 0-th row will correspond to β (i.e., it will consist of all 1's).
- The q-th row for $1 \le q \le r_3 - 2$ will correspond to Γ_{q-1}.
- The $r_3 - 1$-th row will correspond to Δ.

Since the rows of M are coefficients of valid equalities in Q, we have $M \cdot X' = 0$, where $X = (X_0, X_1, \ldots, X_{r_3-1})$ 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 study the effect of multiplying M by a character matrix (i.e., basically performing the discrete Fourier transform).

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

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

Lemma 2.21. *Let $\zeta \neq 1$ be any r_3-th root of unity. Then we have $R(\zeta) = 0$ and*

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

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

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

□

Now let $\mathscr{X}$ be the free $\mathbb{Z}$-module with generators $\widehat{X_0}, \widehat{X_1}, \ldots, \widehat{X_{r_3-1}}$. By abuse of notation, we can consider $\widehat{\beta}, \widehat{\Gamma_q}, \widehat{\Delta} \in \mathscr{X}$ for $0 \leq q \leq r_3 - 3$, which formally look the same as β, Γ_q, Δ (except for the hats). Moreover let ζ be any r_3-th root of unity and consider the $\mathbb{Z}$-module homomorphism from $\mathscr{X}$ to the cyclotomic field $\mathbb{Q}(\zeta)$ given by

$$\sum_{u=0}^{r_3-1} c_u X_u \mapsto \sum_{u=0}^{r_3-1} c_u \zeta^u.$$

We can apply this homomorphism to $\widehat{\beta}, \widehat{\Gamma_q}, \widehat{\Delta}$, and we will denote its respective values by $\beta(\zeta), \Gamma_q(\zeta), \Delta(\zeta) \in \mathbb{Q}(\zeta)$. Note that since $\zeta^{r_3} = 1$, these values depend on the indices of X_u only modulo r_3, so it doesn't matter whether we regard these indices as in the set $\{0, 1, \ldots, r_3 - 1\}$ or just as integers. This will allow us to use the original definitions of β, Γ_q, Δ for their computation and switch between these two viewpoints liberally.

Lemma 2.22. *For any $b \in \mathbb{N}$ and $y \in \mathbb{C}$, we have the equality*

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

Proof. We have

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

□

Lemma 2.23. *Let $\zeta \neq 1$ be any r_3-th root of unity. Then for all $0 \leq q < r_3 - 3$, we have*

$$\beta(\zeta) = 0,$$

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

and

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

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

From the definitions and Lemma 2.21, we directly get $\beta(\zeta) = R(\zeta) = 0$. For the second assertion, we have

$$\begin{aligned}
\Gamma_q(\zeta) &= \sum_{u=0}^{r_3-h'-1} \sum_{v=0}^{\overline{r_2}-1} \zeta^{q+v-ur_2-1} \\
&= \zeta^{q-1} \cdot \sum_{v=0}^{\overline{r_2}-1} \zeta^{v} \sum_{u=0}^{r_3-h'-1} \zeta^{-ur_2} \\
&= \zeta^{q-1} \cdot (1+\zeta+\cdots+\zeta^{\overline{r_2}-1})(1+\zeta^{-r_2}+\zeta^{-2r_2}+\cdots+\zeta^{-(r_3-h'-1)r_2}) \\
&= \zeta^{q-1} \cdot \frac{\zeta^{\overline{r_2}}-1}{\zeta-1} \cdot \frac{\zeta^{-(r_3-h')r_2}-1}{\zeta^{-r_2}-1} \\
&= \zeta^{q-1} \cdot \frac{\zeta^{r_2}-1}{\zeta^{-r_2}-1} \cdot \frac{\zeta^{r_1}-1}{\zeta-1} \\
&= -\zeta^{q} \cdot \zeta^{r_2-1} \cdot (1+\zeta+\zeta^2+\cdots+\zeta^{r_1-1}) \\
&= \zeta^{q} \cdot P(\zeta).
\end{aligned}$$

Similarly, using Lemma 2.22 with $y = \zeta^{-r_2}$ and $b = r_3 - 1$, we can see that

$$\begin{aligned}
\Delta(\zeta) &= \sum_{u=0}^{r_3-1} u \cdot \sum_{v=0}^{\overline{r_2}-1} \sum_{w=0}^{\overline{r_1}-1} \zeta^{v+w-ur_2-1} \\
&= \zeta^{-1} \cdot \sum_{v=0}^{\overline{r_2}-1} \zeta^{v} \sum_{w=0}^{\overline{r_1}-1} \zeta^{w} \sum_{u=0}^{r_3-1} u \cdot \zeta^{-ur_2} \\
&= \zeta^{-1}(1+\zeta+\ldots+\zeta^{\overline{r_2}-1}) \\
&\quad \cdot (1+\zeta+\cdots+\zeta^{\overline{r_1}-1})(\zeta^{-r_2}+2\zeta^{-2r_2}+\cdots+(r_3-1)\zeta^{-(r_3-1)r_2}) \\
&= \zeta^{-1} \cdot \frac{\zeta^{\overline{r_2}}-1}{\zeta-1} \cdot \frac{\zeta^{\overline{r_1}}-1}{\zeta-1} \cdot \frac{r_3\zeta^{-r_2r_3} - \sum_{u=0}^{r_3-1} \zeta^{-r_2(u+1)}}{\zeta^{-r_2}-1} \\
&= \zeta^{-1} \cdot \frac{\zeta^{\overline{r_2}}-1}{\zeta-1} \cdot \frac{\zeta^{\overline{r_1}}-1}{\zeta-1} \cdot \frac{r_3(\zeta^{r_3})^{r_2} - \zeta^{-r_2} \cdot R(\zeta^{-r_2})}{\zeta^{-r_2}-1} \\
&= \zeta^{-1} \cdot \frac{\zeta^{r_2}-1}{\zeta-1} \cdot \frac{\zeta^{r_1}-1}{\zeta-1} \cdot \frac{r_3}{\zeta^{-r_2}-1} \\
&= \zeta^{-1} \cdot \frac{r_3}{\zeta-1} \cdot \frac{\zeta^{r_2}-1}{\zeta^{-r_2}-1} \cdot \frac{\zeta^{r_1}-1}{\zeta-1} \\
&= -D(\zeta) \cdot \zeta^{r_2-1} \cdot (1+\zeta+\zeta^2+\cdots+\zeta^{r_1-1}) \\
&= D(\zeta) \cdot P(\zeta).
\end{aligned}$$

□

Proposition 2.24. *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. $C = (\zeta_{r_3}^{r \cdot c})_{0 \le r,c < r_3}$. We will use the two previous lemmas together with the fact that multiplying a column of successive powers of ζ_{r_3} by a row of M from the left corresponds to evaluating the polynomial obtained from this row at ζ_{r_3}. Hence we have $M \cdot C = C'$, where $C'_{0,0} = R(1) = r_3$ and the $c-th$ column of C' is

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

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

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

where

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

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

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

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

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

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

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

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

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

(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 2.25. *We have $Y_q = 0$ for all $r_1 + r_3 - 2 \le q \le n_2 - 1$.*

Proof. By the Chinese remainder theorem, it suffices to show by induction with respect to $u = 0, 1, \ldots, r_3 - 1$ that for any $0 \le v < r_1$, we have $Y_{v-uhr_1} = 0$. The base case $u = 0$ follows directly from the definition of Y_u. Now suppose the statement is true for $0 \le u < r_3 - 1$. Then using $N_1 \sim 0$ and Lemma 2.17, we get

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

by the induction hypothesis and the fact that $X = 0$. This completes the induction. $\square$

It now follows that Q is trivial, so we have proven the following theorem:

Theorem 2.26. *Under the assumptions on page 5, if*

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

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

Chapter 3

Additional topics

3.1 The module of relations

3.2 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

$$m > 1, r_i \mid m, \gcd(r_i, r_j, r_l) = 1, a_i n_i \neq 1,$$

where $n_i = \frac{m}{r_i}$. 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 $p_i \equiv 1 \pmod{2a_i n_i}$ (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 $[K : \mathbb{Q}] = a_1 a_2 a_3 a_4 \frac{m^4}{r_1 r_2 r_3 r_4}$. 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, thanks to Lemma 1.5.

Theorem 3.1. *In the above notation, we have $[K : k] = m$, $[K : kK_i] = r_i$, $[k \cap K_i : \mathbb{Q}] = a_i$ and $kK_iK_jK_l = K$.*

Proof. Using Lemma 1.19 several times, we can compute

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

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

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

and

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

$\square$

Conclusion

Zde můžete napsat závěr. Zde můžete napsat závěr. Zde můžete napsat závěr. Zde můžete napsat závěr. Zde můžete napsat závěr. Zde můžete napsat závěr. Zde můžete napsat závěr. Zde můžete napsat závěr. Zde můžete napsat závěr. Zde můžete napsat závěr. Zde můžete napsat závěr. Zde můžete napsat závěr. Zde můžete napsat závěr. Zde můžete napsat závěr. Zde můžete napsat závěr. Zde můžete napsat závěr.

Zde můžete napsat závěr. Zde můžete napsat závěr. Zde můžete napsat závěr. Zde můžete napsat závěr. Zde můžete napsat závěr. Zde můžete napsat závěr. Zde můžete napsat závěr. Zde můžete napsat závěr. Zde můžete napsat závěr. Zde můžete napsat závěr. Zde můžete napsat závěr. Zde můžete napsat závěr. Zde můžete napsat závěr. Zde můžete napsat závěr. Zde můžete napsat závěr. Zde můžete napsat závěr. Zde můžete napsat závěr. Zde můžete napsat závěr. Zde můžete napsat závěr.

Bibliography

[1] R. KUČERA AND A. SALAMI, *Circular units of an abelian field ramified at three primes*, Journal of Number Theory, 163 (2016), pp. 296 – 315.

[2] G. LETTL, *A note on Thaine's circular units*, Journal of Number Theory, 35 (1990), pp. 224 – 226.

[3] V. SEDLÁČEK, *Úvod do teorie kruhových jednotek [online]*, 2015 [cit. 2017-05-06].

[4] W. SINNOTT, *On the Stickelberger Ideal and the Circular Units of an Abelian Field.*, Inventiones mathematicae, 62 (1980/81), pp. 181–234.

[5] L. C. WASHINGTON, *Introduction to cyclotomic fields*, Graduate texts in mathematics, Springer-Verlag, 1997.