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:	Bc. 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 + 51
Klíčová slova:	kruhové jednotky; kruhová čísla; abelovská tělesa; Ennolovy relace; modul relací; čtyři rozvětvená prvočísla

Bibliographic Entry

Author:	Bc. 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 + 51
Keywords:	circular units; circular numbers; abelian fields; Ennola relations; the module of relations; four ramified primes

Abstrakt

V této diplomové práci se zabýváme grupami kruhových čísel a kruhových jednotek v Sinnottově smyslu v reálných abelovských tělesech s právě čtyřmi rozvětvenými prvočísly za jistých speciálních předpokladů. Konkrétně se snažíme nalézt jejich $\mathbb{Z}$-báze a popsat příslušný modul relací. Práce navazuje na článek [5].

Abstract

In this thesis we study the groups of circular numbers and circular units in Sinnott's sense in real abelian fields with exactly four ramified primes under certain special conditions. More specifically, we are trying to find their $\mathbb{Z}$-bases and to describe the corresponding module of relations. The thesis builds upon the paper [5].

MASARYKOVA UNIVERZITA
Přírodovědecká fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Akademický rok: 2015/2016

Ústav:	Ústav matematiky a statistiky
Student:	Bc. Vladimír Sedláček
Program:	Matematika
Obor:	Algebra a diskrétní matematika

Ředitel *Ústavu matematiky a statistiky* PřF MU Vám ve smyslu Studijního a zkušebního řádu MU určuje diplomovou práci s tématem:

Téma práce:	Kruhové jednotky abelovských těles
Téma práce anglicky:	Circular units of abelian fields

Oficiální zadání:
Cílem diplomové práce je studium Ennolových relací pro nějakou zvolenou třídu abelovských těles. Kromě osmé a dvanácté kapitoly Washingtonovy učebnice je třeba využít vhodné články z odborných časopisů.

Literatura:
WASHINGTON, Lawrence C. *Introduction to cyclotomic fields*. 2nd ed. New York: Springer, 1997. xiv, 487 s. ISBN 0-387-94762-0.

Jazyk závěrečné práce: angličtina

Vedoucí práce:	prof. RNDr. Radan Kučera, DSc.
Datum zadání práce:	10. 9. 2015
V Brně dne:	27. 10. 2015

Souhlasím se zadáním (podpis, datum):

Sedláček	Radan Kučera	v.z. Pavel Horák
Bc. Vladimír Sedláček **student**	prof. RNDr. Radan Kučera, DSc. **vedoucí práce**	prof. RNDr. Jan Slovák, DrSc. **ředitel Ústavu matematiky a statistiky**

Poděkování

Na tomto místě bych chtěl upřímně poděkovat prof. RNDr. Radanu Kučerovi, DSc., za velkou ochotu, nadšení, vstřícnost, trpělivost a mnoho cenných rad a připomínek, které tuto práci výrazně vylepšily po odborné i didaktické stránce.

Prohlášení

Prohlašuji, že jsem svoji diplomovou 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 easier orientation we present here the basic notation used throughout the thesis.

$\mathbb{C}$	the set of complex numbers
$\mathbb{R}$	the set of real numbers
$\mathbb{Q}$	the set of rational numbers
$\mathbb{Z}$	the set of integers
$\mathbb{N}$	the set of natural numbers (without 0)
$\emptyset$	the empty set
$\lvert H\rvert$	the cardinality of the set H
$\gcd(a,b)$	the greatest common divisor of integers a,b
$\operatorname{lcm}(a,b)$	the least common multiple of integers a,b
$\det M$	the determinant of the matrix M
ζ_n	a primitive n-th rooth of unity
$\ker f$	the kernel of the map f
$f\vert_A$	the restriction of the map f to the subset A of the domain
$R^\times$	the subgroup of units of the ring R
$\langle\eta\rangle, \langle\eta\rangle_R$	the subgroup (resp. R-submodule) generated by η
$\mathbb{Z}[G]$	the integral group ring of the group G
$\prod_{i\in I} K_i$, KL	the compositum of all fields K_i, where $i \in I$ (resp. of K, L)
$\prod_{i\in I} T_i, T \times S$	the product of all groups (or modules) T_i, where $i \in I$ (resp. of T, S)
$\bigoplus_{i\in I} T_i, T \oplus S$	the sum of all groups (or modules) T_i, where $i \in I$ (resp. of T, S)
$T \cdot S, TS$	the subgroup (or submodule) generated by T and S
T/S	the quotient group (or module) of T by S
$[T : S]$	the index of the group (or module) S in the group (or module) T
K/L	extension of fields $K \subseteq L$
$[K : L]$	the degree of the field extension K/L
$\operatorname{Gal}(K/L)$	the Galois group of the Galois extension K/L
$\mathrm{N}_{K/L}$	the norm operator of the field extension K/L
$\eta^\sigma, \sigma\eta$	the result of the module action of σ on η (depending on the context)
$\operatorname{cond}(K)$	the conductor of an abelian field K

Introduction

The group of circular units is an important object of study in modern number theory. In contrast to the case of cyclotomic fields, there are several possible definitions of a group of circular units of a general number field. One of the most well known of these definitions is due to Sinnott and appeared in the paper [10], where he generalized the results from [9]. Sinnott's circular units generalize many previous groups of units due to Kummer, Hasse, Leopoldt, Gras, Gillard and others, and have proven to have many interesting applications; for example they have deep connections to class groups, appear in Iwasawa theory and form an example of an Euler system. In order to do calculations, sometimes it's useful to have an explicit $\mathbb{Z}$-basis of this group at hand. However, such a basis is known only in a few special cases, for example for cyclotomic fields, composita of quadratic fields, abelian fields ramified at at most two primes or certain abelian fields ramified at three primes (see [3], [4], [1], [2] and [5]).

The goal of this thesis is to construct explicit $\mathbb{Z}$-bases of the groups of circular numbers and circular units (in Sinnott's sense) in yet another case, namely that of a real abelian field ramified at exactly four primes and satisfying some additional conditions, as well as to study the Ennola relations that occur along the way, following the approach in [5].

The thesis is subdivided into four chapters. In the first of them, we recall the basic definitions and results about abelian fields and the groups of circular numbers and units, while in the second, we describe more precisely the class of fields we will study and we lay foundations for the work in the rest of the thesis.

The third chapter forms the core of the thesis. We describe here the general strategy we will use to find the $\mathbb{Z}$-bases, and then we do so in five different families of cases of increasing difficulty. Finally in the short fourth chapter, we explain how these constructions relate to the module of relations and discuss some partial results about the relevant Ennola relations.

The reader is assumed to know the basics of Galois theory, module theory and algebraic number theory, especially ramification theory. The knowledge of the theory of Dirichlet characters in the scope of [11], Chapter 3 is also welcome, although not strictly required. During Chapter 3 of the thesis, the reader is also strongly advised to draw pictures to get a better grasp of the exposition.

This thesis was created in the typographic system LaTeX. For some of the computations, the computer algebra system SAGE was used.

Chapter 1

Basic definitions and results

1.1 Preliminaries from the theory of abelian fields

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 $\mathbb{Q}(\zeta_n)$, where $n \in \mathbb{N}$ and ζ_n is an n-th primitive root of unity.*

Proof. See [11], page 321. □

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 $\operatorname{cond}(k)$.

Remark 1.4. Using ramification theory, it's not hard to see that for any abelian field k, $\mathbb{Q}(\zeta_{\operatorname{cond}}(k))$ is ramified exactly at the same primes as k. In other words, a prime divides $\operatorname{cond}(k)$ iff it ramifies in k.

Definition 1.5. The *genus field in the narrow sense* of an abelian field is its maximal field extension which is abelian over $\mathbb{Q}$ and unramified at all finite primes.

Usually, we will use Definition 1.5 only indirectly, thanks to the following lemma:

Lemma 1.6. *Let k be an abelian field, K be its genus field in the narrow sense, 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* $\operatorname{Gal}(K/\mathbb{Q})$ *corresponding to p. Moreover for any $p \in P$, let K_p be the maximal subfield of K ramified only at p. Then the following statements hold (the products denote the composita of fields):*

(i) $K = \prod_{p \in P} K_p$,

(ii) $K = k \prod_{p \in P \setminus \{q\}} K_p$ *for any* $q \in P$,

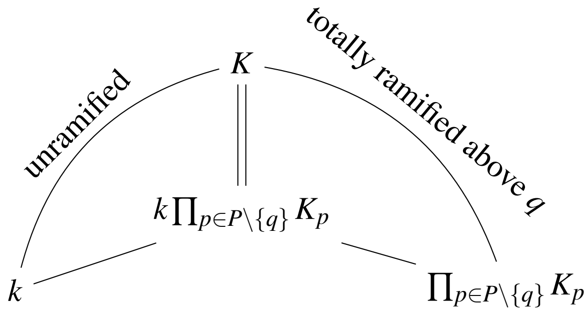
(iii) $\operatorname{Gal}(K/\mathbb{Q}) \cong \prod_{p \in P} T_p$ *and for any* $p \in P$,

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

(iv) *For any $p \in P$, we have $[K_p : \mathbb{Q}] = e_p$.*

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 [11], page 24 is used in the proof. $\square$

Remark 1.7. We will at least briefly outline the proof of (ii) in Lemma 1.6. 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 1.8. Note that for any odd $p \in P$, the field K_p in the statement of Lemma 1.6 is determined uniquely by the condition (iv) alone (together with the fact that it must be abelian), because by Remark 1.4,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, since p is odd. Thus if only odd primes ramify in k, the equalities (i) or (ii) in Lemma 1.6 can be used to construct K from k. In general though, this argument doesn't help us determine the field K_2 without prior knowledge of K (there could be up to three possibilities), and the "correct" choice of K_2 is given by the theory of Dirichlet characters. However, even in this case we can still construct K only from the data provided by k thanks to the equality (ii).

Definition 1.9. An element α of a real abelian field K is called *totally positive* if for any embedding $\sigma : K \to \mathbb{R}$, we have $\sigma(\alpha) > 0$.

1.2 The groups of circular numbers and circular units

Definition 1.10. 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.

For the remainder of this chapter, let $k \neq \mathbb{Q}$ be a real abelian field, K be its the genus field in the narrow sense, P be the set of ramified primes of k (note that the condition $k \neq \mathbb{Q}$ implies that $P \neq \emptyset$) 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 1.11. The group $D(k)$ of circular numbers of k is given as

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

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 1.12. 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 1.13. All the generators η_I of $D(k)$ are norms of nonzero elements from an imaginary abelian field to a real subfield. Hence for any I, we can write

$$\eta_I = (1-\zeta_{\mathrm{cond}(\prod_{i\in I} K_i)})^{\sum_{i=1}^{r}(\sigma_i+\overline{\sigma_i})}$$

for some $r\in\mathbb{N}$, where $\overline{\sigma_i}$ is the automorphism which is complex conjugate to σ_i. It follows that $\sigma(\eta_I)>0$ for any embedding $\sigma: k\to\mathbb{R}$, so that η_I so totally positive. 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 [6], it is proven that the previous definition of $C(k)$ gives the same group as Sinnott's original definition in [10]. One of the reasons that $C(k)$ is important is the following result, due to Sinnott:

Theorem 1.14. *The index $[E(k):C(k)]$ is finite.*

Proof. See [10], Theorem 4.1. □

Lemma 1.15. *Let $\emptyset \subsetneq I \subseteq P$.*

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

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

Proof. Let $n=\mathrm{cond}(\prod_{i\in I}K_i)$. Since η_I is a norm of the algebraic integer $1-\zeta_n$, it is also an algebraic integer, so it suffices to compute its absolute norm to prove (i). We have

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

using the computation in [8], page 29. Since $\mathbb{Q}(\zeta_n)$ is ramified at the same primes as $\prod_{i\in I}K_i$ by Remark 1.4, it follows that $\mathrm{N}_{\prod_{i\in I}K_i\cap k/\mathbb{Q}}(\eta_I)=1$ iff $|I|>1$.

As for (ii), note that for any $\sigma\in\mathrm{Gal}(K/\mathbb{Q})$, the commutitavity of $\mathrm{Gal}(K/\mathbb{Q})$ implies that $\eta_I^{1-\sigma}$ is a norm of $(1-\zeta_n)^{1-\sigma}$. But $(1-\zeta_n)^{1-\sigma}=\frac{1-\zeta_n}{1-\zeta_n^a}$ for some $a\in\mathbb{Z}$, $\gcd(a,n)=1$, and by Lemma 3.9 in [8], this is a unit. Since the norm of a unit is again a unit, we are done. □

Corollary 1.16. *We have*

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

and

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

Proposition 1.17. *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 1.14, 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 1.15, 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 $C^+(k)$ 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. □

Lemma 1.18. *If $L' \subset L$ are abelian fields, then for any $\varepsilon \in C(L)$ (resp. $C^+(L)$, resp. $D(L)$, resp. $D^+(L)$) we have $\mathrm{N}_{L/L'}(\varepsilon) \in C(L')$ (resp. $C^+(L')$, resp. $D(L')$, resp. $D^+(L')$).*

Proof. This is well known and can be proved easily using the original Sinnott's definition of $C(L)$. □

Chapter 2

The special case of four ramified primes

2.1 Notation

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 denote pairwise distinct integers satisfying $1 \leq i, j, l, h \leq 4$, 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 $\zeta_n = \mathrm{e}^{2\pi i/n}$).

Let K be the genus field in the narrow sense of k and let $G := \mathrm{Gal}(K/\mathbb{Q})$. Then by Lemma 1.6, 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 $\pi_i : G \to T_i$,
- $a_i := [T_i : \pi_i(H)]$,
- $r_i := |H \cap \ker \pi_i|$,
- $s_{ij} := |H \cap \ker(\pi_i \pi_j)|$,
- $n_i := \frac{m}{r_i}$,
- $\eta := \eta_{\{1,2,3,4\}}$,
- 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 1.6.)

2.2 Assumptions

In the remainder of the thesis, we will assume the following:

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

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

2.3 Auxiliary results

Lemma 2.1. *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 2.2. *We have*

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

and

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

Proof. Since

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

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

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

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

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

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 1.6, 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 we can consider the short exact sequence

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

where

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

by Lemma 1.6. Thus $|\pi_i\pi_j\pi_l(H)| = m$ and

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

(since Lemma 1.6 implies that $|H \cap T_h| = 1$).

□

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

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

Remark 2.3. Note that Proposition 2.2 implies that $a_i n_i \neq 1$, otherwise T_i would be trivial and p_i wouldn't ramify in k.

Corollary 2.4. *We have*

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

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

and

$$[k : \mathbb{Q}] = a_1 a_2 a_3 a_4 \frac{m^3}{r_1 r_2 r_3 r_4}.$$

Proof. This follows from the computations

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

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

and

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

□

Lemma 2.5. *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

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

Proof. It follows from Proposition 2.2 that $s_{ij} \mid r_i, s_{ij} \mid r_j$ and

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

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 can compute

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

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

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

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

Finally, using the first result, we have

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

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

Remark 2.6. If k is fixed, we have shown in Lemmas 2.2 and 2.5 and Remark 2.3 that

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

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

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

there exist infinitely many real abelian fields k ramified at exactly four primes satisfying the assumptions on page 6 (in particular, the family of fields we are studying is nonempty). The proof of this is analogous to the proof of a similar statement in [7] and we omit it.

Proposition 2.7. *We have*

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

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

Proof. First note that by Lemma 2.5, we have

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

and

$$a_2\frac{m}{r_2 s_{34}} \in \mathbb{N}$$

(this follows from $r_2 \mid m$, $s_{34} \mid m$ and $\gcd(r_2, s_{34}) = \gcd(r_2, r_3, r_4) = 1$), so the expressions make sense. By Corollary 2.4, the set on the right hand side has at most $|\mathrm{Gal}(k/\mathbb{Q})|$ elements. Now let ρ be any automorphism of k. If we can show that ρ 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.

$$
\begin{tikzcd}[column sep=large]
K_1K_2K_3K_4 = K \arrow[d, dash, "\langle \sigma_1 \rangle"'] \arrow[dr, dash] & \\
& k \arrow[d, dash, "a_1 \frac{m}{r_1}"] \\
K_2K_3K_4 \arrow[d, dash, "\langle \sigma_2|_{K_2K_3K_4} \rangle"'] \arrow[dr, dash] & k \cap K_2K_3K_4 \arrow[d, dash, "a_2 \frac{m}{r_2 s_{34}}"] \\
K_3K_4 \arrow[d, dash, "\langle \sigma_3|_{K_3K_4} \rangle"'] \arrow[dr, dash] & k \cap K_3K_4 \arrow[d, dash, "a_3 \frac{m}{r_3 r_4} s_{34}"] \\
K_4 \arrow[d, dash, "\langle \sigma_4|_{K_4} \rangle"'] \arrow[dr, dash] & k \cap K_4 \arrow[d, dash, "a_4"] \\
\mathbb{Q} \arrow[dr, dash] & \mathbb{Q} \\
\end{tikzcd}
$$

Since $\mathrm{Gal}(k \cap K_4/\mathbb{Q})$ is a cyclic group of order a_4 (by Lemma 2.2) 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 $\frac{[k\cap K_3K_4:\mathbb{Q}]}{[k\cap K_4:\mathbb{Q}]} = a_3 \frac{m}{r_3 r_4} s_{34}$ (by Corollary 2.4) 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 $x_3 \in \mathbb{Z}$ with $0 \le x_3 < a_3 \frac{m}{r_3 r_4} s_{34}$ 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

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

(by Corollary 2.4) 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 $x_2 \in \mathbb{Z}$, $0 \le x_2 < a_2 \frac{m}{r_2 s_{34}}$ such that $\rho \sigma_3^{-x_3} \sigma_4^{-x_4}\Big|_k$ and $\sigma_2^{x_2}$ have the same restriction to $k \cap K_2K_3K_4$. Therefore $\rho \sigma_2^{-x_2} \sigma_3^{-x_3} \sigma_4^{-x_4}\Big|_k \in \mathrm{Gal}(k/k \cap K_2K_3K_4)$.

Finally, we have

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

(using Lemma 1.6), 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.

$\square$

Chapter 3

The construction of bases of circular numbers and circular units

3.1 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^+). To achive this, we will build upon the results in [5]. 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 1.6 implies that

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

where the first isomorphism is given by restriction, hence R_iN_i also acts as the norm operator from k to $k \cap K_jK_lK_h$. If we denote the congruence corresponding to the canonical projection $\mathbb{Z}[G] \to \mathbb{Z}[G/H]$ by $\equiv$, then we have (using Lemma 2.1)

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

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

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

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

by $\sim$, where $(R_1N_1, R_2N_2, R_3N_3, R_4N_4)$ is the ideal generated in $\mathbb{Z}[G/H]$ by the images of the elements R_iN_i. 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 a subfield $k \cap K_iK_jK_l$ with less ramified primes. We will make use of this extensively, because an explicit $\mathbb{Z}$-basis of $D^+(k \cap K_iK_jK_l)$ and $C^+(k \cap K_iK_jK_l)$ has already been constructed in [5], as the following lemma shows.

Lemma 3.1. *The field $k \cap K_iK_jK_l$ satisfies the assumptions of [5]. In other words, if K' is the genus field of $k \cap K_iK_jK_l$, then $\mathrm{Gal}(K'/k \cap K_iK_jK_l)$ is cyclic and the inertia subgroups of $\mathrm{Gal}(K'/\mathbb{Q})$ are all cyclic.*

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

Now let K' be the genus field of k', and for any $u \in \{1, 2, 3\}$, let K'_u be the maximal subfield of K' ramified only at p_u and T'_u be the inertia subgroup of $\mathrm{Gal}(K'/\mathbb{Q})$ corresponding to p_u. Then by Lemma 1.6, we have $K'_u \subseteq K_u$ (using the alternate characterization of K_u), hence $T'_i \cong \mathrm{Gal}(K'_u/\mathbb{Q})$ 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 1.6, 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.

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

□

Using the results in [5], 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 1.17 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 (thanks to the discussion above Lemma 3.1.

We will always refer to the conjugates of η by their coordinates x_1, x_2, x_3, x_4 according to Proposition 2.7. This allows us to visualise $\mathrm{Gal}(k/\mathbb{Q})$ geometrically as a discrete (at most) four-dimensional cuboid.

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

In this case, we have

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

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

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

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 $\eta^{\sigma_1^{x_1}\sigma_2^{x_2}\sigma_3^{x_3}\sigma_4^{x_4}}$:

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

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

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

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

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

and

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

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

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

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

and

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

To continue, we need to define an auxiliary relation.

Let

$$\Gamma := \sigma_2^{a_2(m-2)} - \sum_{u=0}^{m-3}\sum_{v=1}^{u+1} \sigma_1^{a_1v}\sigma_2^{a_2u} \in \mathbb{Z}[G]. \tag{3.1}$$

Lemma 3.2. *We have*

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

Proof. We have

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

which implies

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

Using this repeatedly, we obtain

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

as needed. $\square$

Thanks to Lemma 3.2, we will recover all the cases

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

using the relation $\sigma_3^w R_1R_2R_4\Gamma\sum_{u=0}^{m-1}\sigma_3^{a_3 u} \sim 0$ for all $0 \leq w < a_3$, since we can already recover the conjugates of η corresponding to the summands in this relation arising from the double sum in (3.1) (their exponents of σ_2 are between 0 and $a_2(m-2)-1$) as well as the conjugates of η corresponding to the summands arising from the first summand in (3.1), except for precisely one.

Next, we will recover all the cases

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

using the relation $R_4\sum_{u=0}^{m-1}\sigma_1^{a_1 u}\sigma_2^{a_2 u}\sigma_3^{a_3 u}$, 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

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

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 a given $0 \le v < m-1$. 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 3.3. *Under the assumptions on page 6, 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^+.*

3.3 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 $\eta^{\sigma_1^{x_1}\sigma_2^{x_2}\sigma_3^{x_3}\sigma_4^{x_4}}$:

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

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

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

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

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

and

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

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

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

and

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

Next, we will recover all the cases

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

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 the exponents of σ_2 in this relation are pairwise congruent modulo a_2 (and we have already recovered all of them except exactly one). After this, we can recover the cases

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

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

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

and

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

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

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

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

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

using the relation $R_2 N_2 \sim 0$. Therefore the induction is complete and we have recovered all the conjugates of η.

Thus we have proven the following theorem:

Theorem 3.4. *Under the assumptions on page 6, 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^+.*

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

In this case, we have

$$\mathrm{Gal}(k/\mathbb{Q}) \cong \{\sigma_1^{x_1} \sigma_2^{x_2} \sigma_3^{x_3} \sigma_4^{x_4}\big|_k ;\ 0 \leq x_1 < n_1, 0 \leq x_2 < n_2, 0 \leq x_3 < a_3 m, 0 \leq x_4 < a_4\},$$
$$s_{12} = \gcd(r_1, r_2), s_{13} = s_{14} = s_{23} = s_{24} = s_{34} = 1$$

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

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

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

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

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

Next, we will recover the cases $x_4 = 0$, $a_3 < x_3 < a_3m$, $x_1 = n_1 - 1$ or $x_2 = n_2 - 1$ using the relations $N_1 \sim 0$, $N_2 \sim 0$. Now we can also recover the cases

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

using the relation $R_4 \sum_{u=0}^{m-1} \sigma_1^u \sigma_2^u \sigma_3^{a_3 u} \sim 0$, due to the fact that the exponents of σ_3 in this relation are pairwise congruent modulo a_3 (and we have already recovered all of them except exactly one).

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

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

so that Q' is generated by the class of η as a $\mathbb{Z}[G]$-module. Furthermore, let Q be the quotient $\mathbb{Z}$-module of Q' by the classes of conjugates we have already recovered, i.e.,

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

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

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

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 3.5. *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

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

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 3.6. *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 $0 \le v < \mathrm{lcm}(n_1,n_2)$, we have

$$\sigma_1^{u+v}\sigma_2^{v}\cdot\mu = 0 \tag{3.2}$$

and

$$\sigma_1^{v}\sigma_2^{v}\cdot\mu = \mu. \tag{3.3}$$

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 $0 \leq v < \mathrm{lcm}(n_1, n_2) - 1$. Then Lemma 3.5 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

$$\{0, 1, \ldots, \gcd(n_1, n_2)\} \times \{0, 1, \ldots, \mathrm{lcm}(n_1, n_2)\} \to \{0, 1, \ldots, n_1\} \times \{0, 1, \ldots, n_2\}$$

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 $0 \leq u, u' \leq \gcd(n_1, n_2)$, 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 $0 \leq v, v' \leq \mathrm{lcm}(n_1, n_2)$). 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 $0 \leq x_1 < n_1$, $0 \leq x_2 < n_2$, we can write

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

for unique $0 \leq u < \gcd(n_1, n_2)$ and $0 \leq v < \mathrm{lcm}(n_1, n_2)$, and the equalities (3.2) and (3.3) 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 3.7. *We have $\mu = 0$.*

Proof. Using the relation $N_1 \sim 0$ and Lemma 3.6 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 3.6, $\sigma_1^{v\cdot\gcd(n_1,n_2)+u}\cdot\mu$ 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 3.6, $\sigma_2^{v\cdot\gcd(n_1,n_2)+u}\cdot\mu$ 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 3.8. *Under the assumptions on page 6, 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^+.*

3.5 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

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

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

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 3.9. *For any $a,b,c\in\mathbb{N}$, 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

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

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

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

as needed. □

Lemma 3.10. *The following are equivalent:*

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

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

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

(iv) $\gcd(n_1, n_2) \mid n_3$.

Proof.

"(i) ⇔ (ii)": Using Lemma 3.9 together with Lemma 2.5, we get

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

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

"(i) $\Rightarrow$ (iv)": This is immediate, because $\gcd(n_1,n_2,n_3)$ is a divisor of n_3.

"(i) $\Leftarrow$ (iv)": The relation $\gcd(n_1,n_2,n_3) \mid \gcd(n_1,n_2)$ is true automatically. Conversely, if $\gcd(n_1,n_2) \mid n_3$, then $\gcd(n_1,n_2)$ is a common divisor of n_1,n_2,n_3, hence also $\gcd(n_1,n_2) \mid \gcd(n_1,n_2,n_3)$.

□

Therefore, using Lemma 3.10 together with Lemma 2.5, we get

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

(Note that $n_3 = a_3 n_3 > 1$ by Remark 2.3.)

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 $x_2 = x_3 = x_4 = 0$, $\gcd(n_1,n_3) \le x_1 < n_1$ and $x_3 = x_4 = 0$, $x_1 = 0, \gcd(n_2,n_3) \le x_2 < n_2$ using the relations $N_2 \sim 0$, $N_1 \sim 0$.

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

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

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

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

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

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

for any $x_1, x_2 \in \mathbb{Z}$, this is equivalent with showing that $\sigma_1^{x_1}\sigma_2^{x_2}\cdot\mu = 0$ for each $0 \le x_1 < n_1$, $0 \le x_2 < n_2$ (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 3.11. *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

$$0 \sim \sigma_1^{x_1}\sigma_2^{x_2}\left(R_4T\sum_{v=0}^{n_3-1}\sigma_1^v\sigma_2^v\sigma_3^v - \sigma_1\sigma_2N_3R_4T\right) = \sigma_1^{x_1}\sigma_2^{x_2}R_4T\sum_{v=0}^{n_3-1}\left(\sigma_1^v\sigma_2^v - \sigma_1\sigma_2\right)\sigma_3^v$$

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

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

Since all the summands in the expression

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

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

Lemma 3.12. *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 3.6, we can write

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

where $0 \le u < \gcd(n_1,n_2) = \gcd(\gcd(n_1,n_3),\gcd(n_2,n_3))$ (by Lemma 3.10) and $0 \le v < \operatorname{lcm}(n_1,n_2)$. Moreover, by Lemma 3.11, we have

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

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 3.10 The assertion now follows from the definition of Q, since

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

□

Proposition 3.13. *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 3.10. Using the relation $N_1 \sim 0$ and Lemma 3.6 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 3.6, $\sigma_1^{v\cdot\gcd(n_1,n_2)+u}\cdot\mu$ is zero for $u \neq 0$ and is 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 3.6, $\sigma_2^{v\cdot\gcd(n_1,n_2)+u}\cdot\mu$ is zero for $u \neq 0$ and is 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 3.14. *Under the assumptions on page 6, 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^+.

3.6 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 3.15. *Under the assumptions $s_{12} = s_{13} = s_{23} = 1$, the following are equivalent:*

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

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

(iii) $r_1 r_2 r_3 = m$,

(iv) $n_1 = r_2 r_3, n_2 = r_1 r_3, n_3 = r_1 r_2$,

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

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

Proof.

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

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

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

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

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

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

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

$\square$

Thus $\frac{n_1 n_2 n_3}{m} = m = r_2 n_2 = \gcd(n_1, n_3) n_2$ by Lemma 3.15 and using Lemma 2.5, we get

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

We will 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 $n_3 = r_1 r_2 > 1$, $n_1 - r_2 - 1 = r_2(r_3 - 1) - 1 > 0$ 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 $\overline{z} := z \pmod{r_3}$ for any $z \in \mathbb{Z}$, so that $\overline{z} \in \{0, 1, \ldots, r_3 - 1\}$. We will also define h to be the unique integer satisfying

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

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

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

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

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

(where we denote $\eta^\rho \in D^+$ and its class in Q' in the same way for any $\rho \in G$). We will write Q additively, denoting the class of η in Q by μ, hence denoting the class of η^ρ in Q

by $\rho \cdot \mu$ for any $\rho \in \mathrm{Gal}(k/\mathbb{Q})$ or $\rho \in G$. Showing that we have indeed chosen a basis now amounts to showing that Q is trivial. Since

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

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

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

Let

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

Lemma 3.16. *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 $0 \leq w < m$ can be uniquely written as $un_3 + v$, where $0 \leq u < r_3$, $0 \leq v < n_3$, 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

$$\begin{aligned}
0 &\sim \sigma_1^{x_1}\sigma_2^{x_2}\left(R_4 T \sum_{v=0}^{n_3-1} \sigma_1^v\sigma_2^v\sigma_3^v - \sigma_1\sigma_2 N_3 R_4 T\right) = \sigma_1^{x_1}\sigma_2^{x_2} R_4 T \sum_{v=0}^{n_3-1} \left(\sigma_1^v\sigma_2^v - \sigma_1\sigma_2\right)\sigma_3^v \\
&= \sigma_1^{x_1}\sigma_2^{x_2}(1-\sigma_1\sigma_2)R_4 T + \sigma_1^{x_1}\sigma_2^{x_2} R_4 T \sum_{v=2}^{n_3-1} \left(\sigma_1^v\sigma_2^v - \sigma_1\sigma_2\right)\sigma_3^v \\
&= \sigma_1^{x_1}\sigma_2^{x_2}(1-\sigma_1\sigma_2)T + \sigma_1^{x_1}\sigma_2^{x_2}(1-\sigma_1\sigma_2)T \sum_{u=1}^{a_4-1} \sigma_4^u + \sigma_1^{x_1}\sigma_2^{x_2} R_4 T \sum_{v=2}^{n_3-1} \left(\sigma_1^v\sigma_2^v - \sigma_1\sigma_2\right)\sigma_3^v.
\end{aligned}$$

Since all the summands in the expression

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

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. □

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

We will decompose our rectangle (of conjugates of η having $x_3 = x_4 = 0$) into $r_3 \times r_3$ rectangular blocks of height r_2 and width r_1 in the natural way. In the following, by a big row (resp. 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 $Y_u := \sigma_1^{r_2(r_3-1)-1}\sigma_2^u \cdot \mu$. By definition, X_u and Y_u are elements of Q. It will be convenient to allow any integers in the indices of the X's and Y's and regard them only modulo n_2 (to be more precise, as in the set $\{0, 1, \dots, n_2 - 1\}$). Moreover note that by definition, $Y_u = 0$ for $0 \le u < r_1 + r_3 - 2$.

Lemma 3.17. *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 $v = 0, 1, \dots, r_2 - 2$ that

$$\sigma_1^{n_1-2-v}\sigma_2^{u-v} \cdot \mu = X_u. \tag{3.4}$$

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

$$\left(\sigma_1^{n_1-2-v}\sigma_2^{u-v}(1-\sigma_1\sigma_2)\sum_{w=0}^{r_3-1}\sigma_1^{wn_3}\sigma_2^{wn_3}\right) \cdot \mu = 0, \tag{3.5}$$

which follows from Lemma 3.16, 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 $n_1 - r_2 \leq n_1 - 2 - v < n_1 - 2$ and $n_1 - r_2 + 1 \leq n_1 - 1 - v < n_1 - 1$, 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 (3.5) 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 (3.4) holds.

Now for any $0 \leq u < n_2$, we will take $v = r_2 - 1$ in (3.5). 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

$$\begin{aligned}
0 &= \left(\sigma_1^{n_1-r_2-1}\sigma_2^{u-r_2+1}(1-\sigma_1\sigma_2) + \sigma_1^{n_1-1}\sigma_2^{u-r_2+1+h\cdot r_1}(1-\sigma_1\sigma_2)\right)\cdot\mu \\
&= \underbrace{\sigma_1^{n_1-r_2-1}\sigma_2^{u-r_2+1}\cdot\mu}_{=Y_{u-r_2+1}} - \underbrace{\sigma_1^{n_1-r_2}\sigma_2^{u-r_2+2}\cdot\mu}_{=X_u \text{ due to (3.4)}} + \sigma_1^{n_1-1}\sigma_2^{u-r_2+1+h\cdot r_1}\cdot\mu \\
&\quad - \underbrace{\sigma_1^{n_1}\sigma_2^{u-r_2+1+h\cdot r_1+1}\cdot\mu}_{=0}.
\end{aligned}$$

Therefore

$$\sigma_1^{n_1-1}\sigma_2^{u-r_2+1+h\cdot r_1}\cdot\mu = X_u - Y_{u-r_2+1}. \tag{3.6}$$

Finally, for any $0 \leq u < n_2$, we will take $v = r_2$ in (3.5). 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

$$0 = \underbrace{\sigma_1^{n_1-r_2-2}\sigma_2^{u-r_2}\cdot\mu}_{=0} - \underbrace{\sigma_1^{n_1-r_2-1}\sigma_2^{u-r_2+1}\cdot\mu}_{=Y_{u-r_2+1}} + \underbrace{\sigma_1^{n_1-2}\sigma_2^{u-r_2+h\cdot r_1}\cdot\mu}_{=X_{u-r_2+h\cdot r_1}} - \underbrace{\sigma_1^{n_1-1}\sigma_2^{u-r_2+1+h\cdot r_1}\cdot\mu}_{=X_u - Y_{u-r_2+1} \text{ due to (3.6)}}.$$

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

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

and

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

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

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

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

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

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

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

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

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

we get $0 \leq v \leq r_2 - 2$ 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 $0 \leq x_2 < n_2$, denoting $u = x_2 + r_2 - 1 - h \cdot r_1$, the equality (3.6) 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 3.17, from now on we will regard the indices of the X's only modulo r_3. The lemma also implies the equality

$$\sigma_1^{n_1-1} \sigma_2^{x_2} \cdot \mu + \sigma_1^{n_1 - r_2 - 1} \sigma_2^{x_2 - h\cdot r_1} \cdot \mu = X_{x_2 - 1} - Y_{x_2 - h\cdot r_1} + Y_{x_2 - h\cdot r_1} = X_{x_2 - 1} \tag{3.7}$$

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

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

Let

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

and

$$\beta := X_0 + X_1 + \cdots + X_{r_3 - 1} \in Q. \tag{3.8}$$

Lemma 3.18. *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

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

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

Similarly, using Lemma 3.17 together with the relation $N_1 \sim 0$ and the equality (3.7), 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

$$\Gamma_q := \sum_{u=0}^{r_3-h'-1} \sum_{v=0}^{\overline{r_2}-1} X_{q+v-ur_2-1} \in Q. \tag{3.9}$$

Lemma 3.19. *For any* $0 \le q \le r_3 - 3$, *we have* $\Gamma_q = 0$.

Proof. Using Lemma 3.17, the relation $N_1 \sim 0$ and the equality (3.7), we get

$$\begin{aligned}
0 &= \sum_{u=0}^{r_3-h'-1} \sigma_2^{q-uhr_1} N_1 \cdot \mu \\
&= \sum_{u=0}^{r_3-h'-2} \underbrace{\left(\sigma_1^{n_1-1}\sigma_2^{q-uhr_1} + \sigma_1^{r_2(r_3-1)-1}\sigma_2^{q-(u+1)hr_1}\right)\cdot\mu}_{=X_{q-uhr_1-1} \text{ due to } (3.7)} \\
&\quad + \underbrace{\sigma_1^{r_2(r_3-1)-1}\sigma_2^{q}\cdot\mu}_{=Y_q} + \underbrace{\sigma_1^{n_1-1}\sigma_2^{q-(r_3-h'-1)hr_1}\cdot\mu}_{=X_{q-(r_3-h'-1)hr_1-1}-Y_{q+r_1}} \\
&\quad + \sum_{x_1=r_2(r_3-1)}^{n_1-2} \sum_{u=0}^{r_3-h'-1} \sigma_1^{x_1}\sigma_2^{q-uhr_1}\cdot\mu.
\end{aligned}$$

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 3.17, 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 3.18. □

Finally, let

$$\Delta := \sum_{u=0}^{r_3-1} u \cdot \sum_{v=0}^{\overline{r_2}-1} \sum_{w=0}^{\overline{r_1}-1} X_{v+w-ur_2-1} \in Q. \tag{3.10}$$

Lemma 3.20. *We have* $\Delta = 0$.

Proof. Using Lemma 3.17, the relation $N_1 \sim 0$ and the equality (3.7), we get

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

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

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

such that

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

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

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

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

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

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

After using the equality $\alpha = 0$ by Lemma 3.18 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 3.18. □

Now let $\mathscr{X}$ be the free $\mathbb{Z}$-module with generators $\widehat{X}_0, \widehat{X}_1, \dots, \widehat{X}_{r_3-1}$. Analogously to the definitions (3.8), (3.9), (3.10), we will define

$$
\begin{aligned}
\widehat{\beta} &:= X_0 + X_1 + \cdots + \widehat{X}_{r_3-1} \in \mathscr{X}, \\
\widehat{\Gamma}_q &:= \sum_{u=0}^{r_3-h'-1} \sum_{v=0}^{\overline{r_2}-1} \widehat{X}_{\overline{q+v-ur_2-1}} \in \mathscr{X}, \\
\widehat{\Delta} &:= \sum_{u=0}^{r_3-1} u \cdot \sum_{v=0}^{\overline{r_2}-1} \sum_{w=0}^{\overline{r_1}-1} \widehat{X}_{\overline{v+w-ur_2-1}} \in \mathscr{X}
\end{aligned}
$$

for all $0 \le q \le r_3 - 3$. Also let $\psi : \mathscr{X} \to Q$ be the $\mathbb{Z}$-module homomorphism satisfying $\psi(\widehat{X}_u) = X_u$ for all $0 \le u < r_3$ (since $\mathscr{X}$ is free, this is well defined and determines ψ uniquely). Then for all $0 \le q \le r_3 - 3$, it's clear by Lemmas 3.18, 3.19 and 3.20 that

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

hence

$$\widehat{\beta}, \widehat{\Gamma}_q, \widehat{\Delta} \in \ker \psi. \tag{3.11}$$

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

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

By the definition of M, we have

$$M \cdot \begin{pmatrix} \widehat{X}_0 \\ \widehat{X}_1 \\ \widehat{X}_2 \\ \widehat{X}_3 \\ \vdots \\ \widehat{X}_{r_3-2} \\ \widehat{X}_{r_3-1} \end{pmatrix} = \begin{pmatrix} \widehat{\beta} \\ \widehat{\Gamma}_0 \\ \widehat{\Gamma}_1 \\ \widehat{\Gamma}_2 \\ \vdots \\ \widehat{\Gamma}_{r_3-3} \\ \widehat{\Delta} \end{pmatrix} \tag{3.12}$$

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

Let

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

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

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

Lemma 3.21. *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

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

□

Lemma 3.22. *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

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

□

Now 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

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

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

Lemma 3.23. *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 3.21, we directly get $\beta(\zeta) = R(\zeta) = 0$. For the second assertion, we have

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

Similarly, using Lemma 3.22 with $y = \zeta^{-r_2}$ and $b = r_3 - 1$, we can see that

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

□

Proposition 3.24. *M is unimodular.*

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

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

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

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

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. □

Corollary 3.25. *We have $X_u = 0$ for all $0 \le q < r_3$.*

Proof. Let M^{-1} be the inverse matrix to M. By Proposition 3.24, it exists and it has integer entries. From the equation (3.12), it then follows that

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

which implies that $\widehat{\beta}, \widehat{\Gamma}_0, \widehat{\Gamma}_1, \dots, \widehat{\Gamma}_{r_3-3}, \widehat{\Delta}$ generate $\mathscr{X}$. But all of these elements lie in $\ker\psi$ by (3.11), hence $\ker\psi = \mathscr{X}$ and ψ is the zero homomorphism. On the other hand, we know that the image of ψ is generated by $X_0, X_1, \dots, X_{r_3-1}$ by the definition of ψ, so all of these must be zero as well. □

Corollary 3.26. *We have $Y_u = 0$ for all $r_1 + r_3 - 2 \le u < n_2$.*

Proof. By the Chinese remainder theorem, it suffices to show by induction with respect to $u = 0, 1, \dots, r_3 - 1$ 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 a given $0 \le u < r_3 - 1$. Then using $N_1 \sim 0$ and Lemma 3.17, we get

$$0 = \sigma_2^{v-uhr_1} N_1 \cdot \mu = \sum_{x_1 = r_2(r_3-1)-1}^{n_1-1} \sigma_1^{x_1} \sigma_2^{v-uhr_1} \cdot \mu$$

$$= \underbrace{Y_{v-uhr_1}}_{=0} - Y_{v-uhr_1-hr_1} + \sum_{x_1=r_2(r_3-1)}^{n_1-1} \underbrace{X_{v-uhr_1-x_1-2}}_{=0} = -Y_{v-(u+1)hr_1}$$

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

Bz Lemma 3.17, it now follows that Q is trivial, so we have proven the following theorem:

Theorem 3.27. *Under the assumptions on page 6, 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 4

The module of relations

In this chapter, we will try to study the relations between the generators of the group of circular numbers more abstractly, following the approach in [5]. Sometimes we will only state the results and omit the proofs, or just outline them.

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

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

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

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

and similarly

$$\eta_{ijl} := \eta_{\{i,j,l\}}, \eta_{ij} := \eta_{\{i,j\}}, \eta_i := \eta_{\{i\}}.$$

Therefore we have

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

and

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

Since

$$\eta\in k, \eta_{ijl}\in k\cap K_iK_jK_l, \eta_{ij}\in k\cap K_iK_j \text{ and } \eta_i\in k\cap K_i,$$

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

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

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

Lemma 1.18 implies that for any $\emptyset \subsetneq I \subseteq \{1,2,3,4\}$, $|I| \geq 2$ and $i \in I$, we have

$$\mathrm{N}_{k\cap\prod_{u\in I} K_u/k\cap\prod_{u\in I\setminus\{i\}} K_u}\eta_I \in D^+\left(k\cap \prod_{u\in I\setminus\{i\}} K_u\right),$$

hence there exists some

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

such that

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

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

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

Remark 4.1. In fact, the relation $N_{i,I}$ can be described much more explicitly using the Frobenius automorphisms, but we won't go into details here.

Now let M be the $\mathbb{Z}[G]$-submodule of $\ker\varphi$ generated by the norm relations $N_{i,I}$ for all possible $\emptyset \subsetneq I \subseteq \{1,2,3,4\}$, $|I| \geq 2$ and $i \in I$. Our goal will be to describe the quotient $\mathbb{Z}[G]$-module $\ker\varphi/M$. We will call *the module of Ennola relations*.

Let E_{ijl} be the Ennola relation described by Theorem 10 in [5] applied to the field $k \cap K_iK_jK_l$.

Proposition 4.2. *In all the cases described in Chapter 3, the* $\mathbb{Z}[G]$*-module* $\ker\varphi/M$ *is generated by the classes of* $E_{123}, E_{124}, E_{134}, E_{234}$ *and the action of* G *is trivial on it.*

Proof. For any case described in Chapter 3, let B be a $\mathbb{Z}$-basis of D^+. For any element of B, we will fix its preimage with respect to φ; let Y be the set of these fixed preimages. Then the elements of Y are $\mathbb{Z}$-linearly independent and we have $\mathscr{X} = \ker\varphi \oplus Y$. Recall that to construct B, we always used only norm relations together with the four implicit Ennola relations $E_{123}, E_{124}, E_{134}, E_{234}$ from [5]. This shows that $\ker\varphi$ is generated by $M \cup \{E_{123}, E_{124}, E_{134}, E_{234}\}$, which proves the first part of the proposition. The second part follows from the fact that the action of G on E_{ijl} is the same as the action of $\mathrm{Gal}(k\cap K_iK_jK_l/\mathbb{Q})$ on E_{ijl}, which is trivial by Theorem 19 in [5]. □

Remark 4.3. In the case $a_1 = a_2 = a_3 = a_4 = r_1 = r_2 = r_3 = r_4 = 1$ (which is a special case of the one in Section 3.2), it can be shown that $\ker\varphi/M \cong (\mathbb{Z}/m)^4$, which is a stronger result than in Proposition 4.2. The proof is too technical to include here, but essentialy it consists of constructing a $\mathbb{Z}$-module (not $\mathbb{Z}[G]$-module!) homomorphism from $\mathscr{X}$ to $\mathbb{Z}/m$ and showing that all the norm relations together three of the four Ennola relations lie in its kernel, while the fourth Ennola relation maps to the class of 1 modulo m.

Remark 4.4. A crucial part of the proof of Proposition 4.2 was the fact that in all of the cases studied in Chapter 3, we never encountered any new Ennola relation, i.e. an element of $\mathscr{X} \setminus M$ having a nonzero coefficient at x. This will not always be case though, because we have already found a new Ennola relation in the special case

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

(but the proof that it doesn't lie in M is again quite technical to describe here). Note that in this case, we have $N = 0$, but it is still possible to recover all the conjugates of η using this new Ennola relation.

In fact, it appears quite plausible that a new Ennola relation could arise whenever we have $a_i > 1$ and $r_i > 1$ at the same time. It is not a coincidence that this didn't happen in any of the cases studied in Chapter 3, because this will probably drastically increase the difficulty of construction of a $\mathbb{Z}$-basis of D^+ and C^+.

Conclusion

To summarize, we have managed to construct explicit $\mathbb{Z}$-bases of the groups of circular numbers and circular units (in Sinnott's sense) of a real abelian field with exactly four ramified primes in five different infinite families of cases. All of these are new results and they illustrate the power of the geometric approach, which is converted into algebraic notation afterwards.

However, even if there are some similarities in these five constructions, it seems that there is no easy way how to generalize all of them at the same time, so the general case remains open. It's quite probable that in order to solve it, we will first to fully understand new Ennola relations that will arise, unlike in our five cases. In this regard, it might also be useful to explore the relationship between all the Ennola relations, even those coming from the maximal subfields ramified at three primes. In the last chapter, we have briefly touched this subject, but the results here are much weaker than in Chapter 3, so this seems to be a promising topic for future research.

Bibliography

[1] K. DOHMAE, *On Bases of Groups of Circular Units of Some Imaginary Abelian Number Fields*, Journal of Number Theory, 61 (1996), pp. 343 – 364.

[2] K. DOHMAE, *A note on Sinnott's index formula*, Acta Arithmetica, 82 (1997), pp. 57–67.

[3] R. KUČERA, *On bases of the Stickelberger ideal and of the group of circular units of a cyclotomic field*, Journal of Number Theory, 40 (1992), pp. 284 – 316.

[4] R. KUČERA, *On the Stickelberger Ideal and Circular Units of a Compositum of Quadratic Fields*, Journal of Number Theory, 56 (1996), pp. 139 – 166.

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

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

[7] A. SALAMI, *Bases of the group of cyclotomic units of some real abelian extension*, PhD thesis, Université Laval Québec, 2014.

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

[9] W. SINNOTT, *On the Stickelberger Ideal and the Circular Units of a Cyclotomic Field*, Annals of Mathematics, 108 (1978), pp. 107–134.

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

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