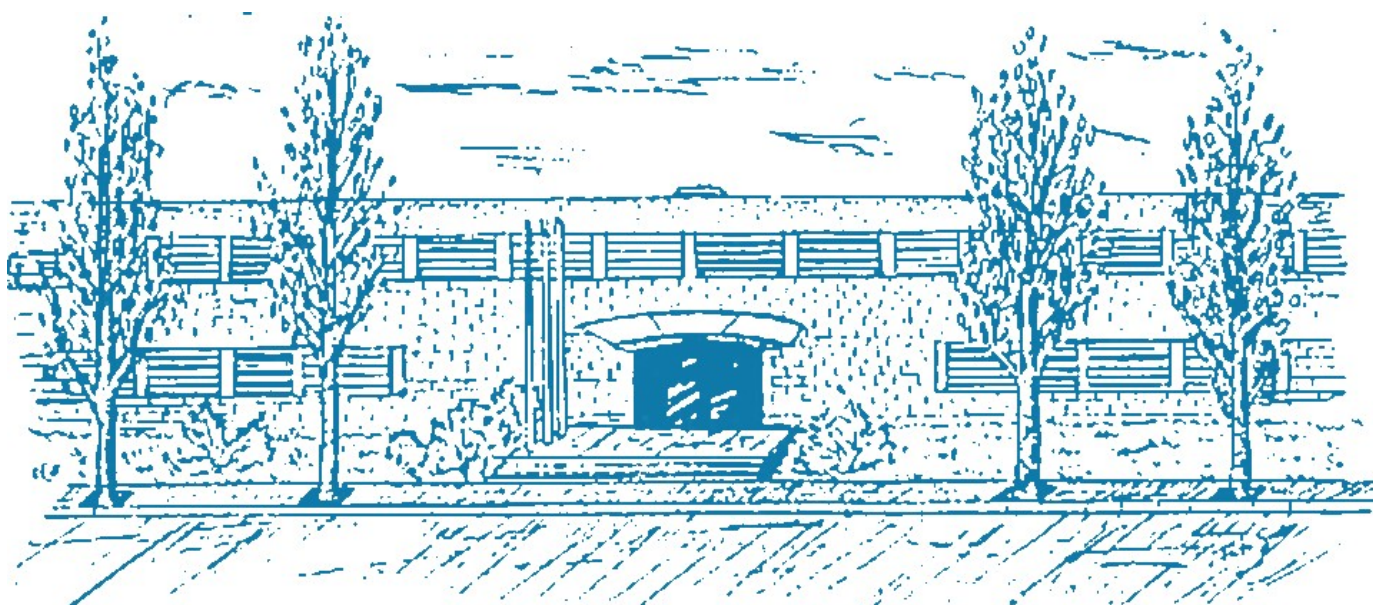


UNIVERSITAT POLITÈCNICA DE CATALUNYA - BarcelonaTech (UPC)
FME - FACULTAT DE MATEMÀTIQUES I ESTADÍSTICA

MASTER IN ADVANCED MATHEMATICS AND MATHEMATICAL ENGINEERING (MAMME)
MASTER'S THESIS

Conjugacy Problem for some extensions of the Heisenberg group



Author: Raül Agulló Pardo

Director: Enric Ventura

Department: Mathematics

Barcelona, (2026)



UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Facultat de Matemàtiques i Estadística



Universitat Politècnica de Catalunya
Facultat de Matemàtiques i Estadística

Master in Advanced Mathematics and Mathematical Engineering
Master's thesis

Conjugacy problem for some extensions of the Heisenberg group

Raúl Agulló Pardo

Supervised by Enric Ventura Capell

May, 2026

First of all, thanks to Enric Ventura, my tutor, who has helped me and supported me a lot through this journey. The subject of this Master's Thesis has been fascinating and I have been able to produce interesting results. This would not have been possible without your support.

I would also like to thank my parents, my sister and my aunt Carmen, who have supported me a lot from the distance and have put up with many phonecalls from me.

Abstract

This Master's thesis studies the Conjugacy Problem for extensions of Heisenberg groups from the perspective of Algorithmic Group Theory. After introducing the three-dimensional Heisenberg group H_3 , the work develops an explicit description of its endomorphisms and automorphisms, proving that $\text{Aut}(H_3) \cong \mathbb{Z}^2 \rtimes GL_2(\mathbb{Z})$. Using these structural results, the thesis solves both the Conjugacy Problem and the Twisted Conjugacy Problem for H_3 , and proves that $\text{Aut}(H_3)$, as well as every finitely generated subgroup containing the inner automorphism group, is orbit decidable. Applying the Bogopolski–Martino–Ventura theorem, this yields solvability results for the Conjugacy Problem in many extensions of H_3 . The thesis then generalizes these methods to higher-dimensional Heisenberg groups H_{k+2} , obtaining both positive and negative results on orbit decidability for subgroups of the automorphisms group as well as on the Conjugacy Problem in some of their extensions.

Keywords

Algorithmic Group Theory, Heisenberg group, Automorphisms, Conjugacy Problem, Twisted Conjugacy Problem, Orbit Decidability

Contents

1	Introduction	3
2	Heisenberg's group of dimension 3	6
2.1	Definition of Heisenberg's group	6
2.2	Endomorphisms of H_3	9
2.3	Automorphisms of H_3	11
2.4	Structure of $Aut(H_3)$	14
2.5	Conjugacy Problem and Twisted Conjugacy Problem	20
2.6	Orbit decidability	23
2.6.1	$OD(Aut(H_3))$	23
2.6.2	$OD(\langle \varphi_{M_1, \mathbf{p}^1}, \dots, \varphi_{M_n, \mathbf{p}^n} \rangle Inn(H_3))$	25
3	Heisenberg's group of higher dimensions	30
3.1	Definition of Heisenberg's group of higher dimensions	30
3.2	Endomorphisms of H_{k+2}	33
3.3	Automorphisms of H_{k+2}	36
3.4	Structure of $Aut(H_{k+2})$	39
3.5	Conjugacy Problem and Twisted Conjugacy Problem	42
3.6	Orbit decidability	44
3.6.1	$OD(Aut(H_{k+2}))$	44
3.6.2	$OD(\langle \varphi_{M_1, \mathbf{p}^1}, \dots, \varphi_{M_n, \mathbf{p}^n} \rangle Inn(H_{k+2}))$ (Positive and negative results)	49
4	Conclusions	53
	References	54
A	Some notes on symplectic matrices	56
B	Presentation of $Sp_4(\mathbb{Z})$ and $GSp_4(\mathbb{Z})$	60

1. Introduction

The study of Algorithmic Group Theory started more than a hundred years ago with the famous *three Dehn Problems* (see the seminal paper [12]), namely the *Word Problem*, the *Conjugacy Problem* and the *Isomorphism Problem*:

Word Problem, (WP(G)): For a finite presentation $G = \langle X \mid R \rangle$, given a word on the generators $w \in F(X)$, decide whether w represents the trivial element in G , $w =_G 1$.

Conjugacy Problem, (CP(G)): For a finite presentation $G = \langle X \mid R \rangle$, given two words on the generators $u, v \in F(X)$, decide whether u and v represent conjugate elements in G , $u \sim_G v$.

Isomorphism Problem, (IP): Given two finite presentations, $\langle X \mid R \rangle$ and $\langle Y \mid S \rangle$, decide whether they present isomorphic groups, $\langle X \mid R \rangle \simeq \langle Y \mid S \rangle$.

Although Dehn wrote his three problems with a clear intention to encourage the mathematical community to study and solve them as central points for the future theory, one of the first major developments was done by Novikov [18] in 1955 and Boone [4] in 1958, showing that the Word Problem, and so the Conjugacy Problem as well, are unsolvable in the sense that there does not exist any Turing machine able to solve them. Soon, Adian [1] and Rabin [20] got the same result for the Isomorphism Problem.

These negative results redirected the field towards identifying broad classes of groups where these problems remain solvable.

The present project aims to contribute in this direction, focusing on the Conjugacy Problem in close relation with two more modern algorithmic problems: the *Twisted Conjugacy Problem* and the *Orbit Decidability Problem*.

Let G be a group and $\varphi \in \text{Aut}(G)$, $g \mapsto g\varphi$, be an automorphism. Two elements $u, v \in G$ are said to be φ -twisted conjugated, denoted $u \sim_\varphi v$, if there exists $x \in G$ such that $v = (x\varphi)^{-1}ux$. It is easy to see that $\sim_\varphi$ is an equivalence relation on G (which coincides with the usual conjugation when $\varphi = \text{Id}$). This variation of standard conjugacy was first introduced by Reidemeister [21] back in 1936, with clear topological motivations related to Nielsen Fixed Point Theory. The corresponding algorithmic problem is the following generalization of the Conjugacy Problem:

Twisted Conjugacy Problem, (TCP(G)): For a finite presentation $G = \langle X \mid R \rangle$, given an automorphism $\varphi: G \rightarrow G$ (by the images of generators), and two words on the generators, $u, v \in F(X)$, decide whether u and v represent φ -twisted conjugate elements from G , i.e., $u \sim_\varphi v$.

Of course, CP coincides with the particular case of TCP with $\varphi = \text{Id}$; so, a positive solution to $TCP(G)$ immediately gives a positive solution to $CP(G)$ (which automatically gives a positive solution to $WP(G)$ as well). However, as one might expect, in an arbitrary group G , twisted conjugacy classes may be much more complicated to understand than standard conjugacy classes. For instance, in the case of free groups, $CP(F_n)$ is very easy both conceptually and computationally, while $TCP(F_n)$ is known to be solvable but much harder in both senses; see [6, Thm. 1.5]. Also, similarly to the classical result stating the existence of a finitely presented group G with solvable $WP(G)$ but unsolvable $CP(G)$ (see, for example, [16]), there is a more recent result stating the existence of a finitely presented group G with solvable $CP(G)$ but unsolvable $TCP(G)$; see [7, Cor. 4.9].

In [6], Bogopolski–Martino–Maslakova–Ventura solved the Conjugacy Problem for free-by-cyclic groups, $CP(F_n \rtimes_\varphi \mathbb{Z})$. The proof had two clearly separate ingredients: firstly a positive solution to the Twisted Conjugacy Problem for free groups, $TCP(F_n)$, and, secondly, a result from Brinkmann [8] providing an algorithm to decide, given an automorphism $\varphi \in \text{Aut}(F_n)$, and two elements $u, v \in F_n$, whether v is

conjugate to some iterated image of u , i.e., $v \sim u\varphi^k$, for some $k \in \mathbb{Z}$. On the other hand, more than 30 years earlier, Miller [16] already studied the much bigger family of free-by-free groups, and showed that the Conjugacy Problem is unsolvable within that framework.

Few years after the publication of [6], Bogopolski–Martino–Ventura [7] realized that, in their solution to $CP(F_n \rtimes_{\varphi} \mathbb{Z})$, the case where the two inputs belonged to outside the normal subgroup F_n (i.e., $u, v \notin F_n$) boils down to $TCP(F_n)$, while the opposite case ($u, v \in F_n$) corresponded directly to Brinkmann's result (note that if $u \in F_n$ and $v \notin F_n$, or viceversa, then they automatically cannot be conjugate to each other). This pattern happened to be much more general: in the free-by-free group $G = F_n \rtimes_{\varphi_1, \dots, \varphi_m} F_m$, the decision on whether two elements $u, v \notin F_n$ are conjugated to each other in G boils down to $TCP(F_n)$, while deciding whether two elements $u, v \in F_n$ are conjugated to each other in G , becomes a much harder problem than Brinkmann's one (and mandatorily sometimes unsolvable, according to Miller's result [16]). Much beyond this family, the main result in [7] is the following one, exactly in the same spirit, but applying to any (non necessarily split) algorithmic short exact sequence of groups:

Theorem 1.1 (Bogopolski–Martino–Ventura, [7]). *Let $1 \rightarrow F \xrightarrow{\alpha} G \xrightarrow{\beta} H \rightarrow 1$ be an algorithmic short exact sequence of groups such that (i) F has solvable twisted conjugacy problem; (ii) H has solvable conjugacy problem; and (iii) for every $1 \neq h \in H$, the subgroup $\langle h \rangle$ has finite index on its centralizer $C_H(h)$, and there is an algorithm which computes a finite set of coset representatives, $z_{h,1}, \dots, z_{h,t_h} \in H$, $C_H(h) = \langle h \rangle z_{h,1} \sqcup \dots \sqcup \langle h \rangle z_{h,t_h}$. Then, the following are equivalent:*

- (a) *the conjugacy problem for G is solvable;*
- (b) *the conjugacy problem for G restricted to F is solvable;*
- (c) *the action subgroup $A_G = \{\varphi_g \mid g \in G\} \leq \text{Aut}(F)$ is orbit decidable.*

Here, the *action subgroup* associated to a short exact sequence, A_G , is just the set of restrictions to $F \trianglelefteq G$, namely $\varphi_g: F \rightarrow F$, of the inner automorphisms of G , namely $\gamma_g: G \rightarrow G$, $x \mapsto g^{-1}xg$ (note that φ_g is not, in general, inner as automorphism of F ; we can only say that $A_G \leq \text{Aut}(F)$). Finally, the notion of *Orbit Decidability* is crucial:

Orbit Decidability Problem, OD(A): For a finite presentation $G = \langle X \mid R \rangle$ and a group of automorphisms $A \leq \text{Aut}(G)$, given two words on the generators $u, v \in F(X)$, decide whether the corresponding elements $u, v \in G$ can be mapped to each other by some automorphism in A , i.e., whether there exists $\alpha \in A$ such that $u\alpha = v$.

A subgroup $A \leq \text{Aut}(G)$ is said to be *orbit decidable* if $OD(A)$ is solvable. Particularizing to the case where both F and H are free groups (hypotheses (i), (ii) and (iii) do hold), the group G sitting in the middle of the short exact sequence is free-by-free, and Theorem 1.1 states that $CP(G)$ is solvable if and only if the corresponding action subgroup is orbit decidable: sometimes this is the case (for example, when $H = \mathbb{Z}$, in which case $A_G/(A_G \cap \text{Inn}(F))$ is cyclic and $OD(A_G)$ is, precisely, Brinkmann's problem), and sometimes it is not (like in the classical Miller's examples of free-by-free groups with unsolvable Conjugacy Problem); see [7] for more details.

After the publication of [7], several research papers have appeared following the same strategy but in other situations and groups: anytime we have a family of groups (to put in place of F) for which we can solve the Twisted Conjugacy Problem, it becomes interesting to study Orbit Decidability for (all, certain) subgroups of automorphisms $A \leq \text{Aut}(F)$, and deduce from it the solvability or unsolvability of the Conjugacy Problem for extensions of F by families of groups H satisfying (ii) and (iii) (for example, torsion-free hyperbolic groups; see [7]). In particular, we have the following result, which proves that torsion-free hyperbolic groups verify (iii) (and (ii) is a well-known result):

Theorem 1.2 (Bogopolski–Martino–Ventura, Proposition 4.11, [7]). *Let H be a finitely generated hyperbolic group given by a finite presentation, and let h be an element of H .*

1. *There is an algorithm to determine whether or not the centralizer $C_H(h)$ is finite and, if it is so, to list all its elements.*
2. *If h has infinite order in H , then $\langle h \rangle$ has finite index in $C_H(h)$ and there is an algorithm which computes a set of coset representatives for $\langle h \rangle$ in $C_H(h)$.*

This strategy was followed in [7] itself to study the Conjugacy Problem within the family of free-by-free-abelian groups, where the authors positively solved it for all groups of the form $\mathbb{Z}^2 \rtimes F_m$, and $\mathbb{Z}^n \rtimes_A F_m$ with virtually solvable action subgroup $A \leq GL_n(\mathbb{Z})$; and provided the first known examples of groups of the form $\mathbb{Z}^4 \rtimes F_n$ with unsolvable Conjugacy Problem. Similarly, Šunić–Ventura [23] constructed the first known examples of automaton groups with unsolvable Conjugacy Problem. González-Meneses–Ventura [13] followed the same project for Braid groups, showing that all Braid-by-hyperbolic groups have solvable Conjugacy Problem. Burillo–Matucci–Ventura [9] did the same for Thompson’s group F , proving in this case the existence of Thomson-by-hyperbolic groups with unsolvable Conjugacy Problem. Recently, Blufstein–Valiunas [5], Crowe [10, 11], and Mitra–Roy–Ventura [17] have followed similar projects for certain large-type Artin groups, for dihedral Artin groups, and for Baumslag–Solitar groups $BS(n, 1)$, respectively.

In the present Master’s thesis, we propose to follow a similar project for the Heisenberg’s group H_3 . In particular, we will begin introducing the definition of this group. Next, we will study the automorphisms of the group, so as to solve $TCP(H_3)$. Once we have this, we will prove that the whole group of automorphisms of H_3 is orbit decidable, as well as every finitely generated subgroup of $Aut(H_3)$ containing $Inn(H_3)$. A direct application of Theorem 1.1 will prove the solvability of CP for many extensions of Heisenberg’s group. In particular, the new results we will prove are

- $TCP(H_3)$ is solvable.
- $Aut(H_3)$ is orbit decidable.
- Every finitely generated subgroup A such that $Inn(H_3) \leq A \leq Aut(H_3)$ is orbit decidable.

Once we have this, we will extend the results of this section to higher dimensional Heisenberg’s groups. We will begin by defining these groups, and studying their automorphisms’ group, so as to solve $TCP(H_{k+2})$. In this scenario, however, we will find that some of the finitely generated subgroups of $Aut(H_{k+2})$ containing $Inn(H_{k+2})$ are orbit undecidable, which will lead to negative results of the conjugacy problem for some extensions of the higher dimensional Heisenberg’s groups. In particular, the new results we will prove are

- $TCP(H_{k+2})$ is solvable.
- $Aut(H_{k+2})$ is orbit decidable.
- The orbit decidability of a finitely generated subgroup A such that $Inn(H_{k+2}) \leq A \leq Aut(H_{k+2})$ is equivalent to the orbit decidability of the subgroup of matrices associated to those automorphisms intersected with $Sp_{2k}(\mathbb{Z})$. In particular, this yields results of orbit undecidability for some of these subgroups if $k \geq 4$.

2. Heisenberg's group of dimension 3

2.1 Definition of Heisenberg's group

Consider

$$H_3 = \langle a, b, c \mid [a, b]c, [a, c], [b, c] \rangle.$$

Theorem 2.1. *Given $w \in F(a, b, c)$ a word, it can be written in H_3 in its normal form as $w =_{H_3} a^m b^n c^p$ with $m, n, p \in \mathbb{Z}$.*

Proof. Let $w \in F(a, b, c)$ be a word on the generators of H_3 . We want to prove that w can be rewritten as $w =_{H_3} a^m b^n c^p$ with $m, n, p \in \mathbb{Z}$.

First, we see, that we can always move c to the right of the word by multiplying by conjugators of the relations:

Note that $[d, c] \in R$ is a relation for $d = a, b$. So, $dc[d, c]c^{-1}d^{-1} = dcd^{-1}c^{-1}dcc^{-1}d^{-1} = [d^{-1}, c^{-1}] \in \langle\langle R \rangle\rangle$. Furthermore, $d[d, c]^{-1}d^{-1} = dc^{-1}d^{-1}cdd^{-1} = dc^{-1}d^{-1}c = [d^{-1}, c] \in \langle\langle R \rangle\rangle$ and also, $c[d, c]^{-1}c^{-1} = [d, c^{-1}] \in \langle\langle R \rangle\rangle$.

If $w = uc^{\varepsilon_1}d^{\varepsilon_2}v$ with $u, v \in F(a, b, c)$, $d = a$ or $d = b$, $\varepsilon_1, \varepsilon_2 \in \{-1, 1\}$, then

$$w = uc^{\varepsilon_1}d^{\varepsilon_2}v =_{H_3} uc^{\varepsilon_1}d^{\varepsilon_2}vv^{-1}[d^{\varepsilon_2}, c^{\varepsilon_1}]v = ud^{\varepsilon_2}c^{\varepsilon_1}v$$

Now, we see that if we have a b followed by an a in w , we can always exchange them at the price of including c 's in the word.

Note that $[a, b]c = a^{-1}b^{-1}abc \in R$, so $ba([a^{-1}, b^{-1}]c^{-1})a^{-1}b^{-1} = abca^{-1}b^{-1} \in \langle\langle R \rangle\rangle$. In addition to this, $ba([a, b]c)a^{-1}b^{-1}b([a^{-1}, c])b^{-1}([b^{-1}, c]) = baa^{-1}b^{-1}abca^{-1}b^{-1}bac^{-1}a^{-1}cb^{-1}bc^{-1}b^{-1}c = aba^{-1}b^{-1}c \in \langle\langle R \rangle\rangle$.

We can also see that $a^{-1}ba([b, c]([a, b]c)^{-1})a^{-1}b^{-1}a = a^{-1}bab^{-1}c^{-1}bcc^{-1}b^{-1}a^{-1}baa^{-1}b^{-1}a = a^{-1}bab^{-1}c^{-1} \in \langle\langle R \rangle\rangle$ and $ab^{-1}a^{-1}([b^{-1}, c](aba^{-1}b^{-1}c)^{-1})aba^{-1} = ab^{-1}a^{-1}bc^{-1}b^{-1}cc^{-1}bab^{-1}a^{-1}aba^{-1} = ab^{-1}a^{-1}bc^{-1} \in \langle\langle R \rangle\rangle$.

If $w = ubav$, then $w = ubav =_{H_3} ubavv^{-1}a^{-1}b^{-1}abcv = uabcv$.

If $w = ub^{-1}a^{-1}v$, then $w = ub^{-1}a^{-1}v =_{H_3} ub^{-1}a^{-1}vv^{-1}aba^{-1}b^{-1}cv = ua^{-1}b^{-1}cv$.

If $w = ub^{-1}av$, then $w = ub^{-1}av =_{H_3} ub^{-1}avv^{-1}a^{-1}bab^{-1}c^{-1}v = uab^{-1}c^{-1}v$.

If $w = uba^{-1}v$, then $w = uba^{-1}v =_{H_3} uba^{-1}vv^{-1}ab^{-1}a^{-1}bc^{-1}v = ua^{-1}bc^{-1}v$.

It is easy to see that if we keep doing these changes to the word a finite number of times, we get to $w =_{H_3} a^m b^n c^p$. $\square$

Theorem 2.2. *H_3 is isomorphic to the following matrices subgroup:*

$$H_3 \cong \left\{ \begin{pmatrix} 1 & n & p \\ 0 & 1 & m \\ 0 & 0 & 1 \end{pmatrix} \mid m, n, p \in \mathbb{Z} \right\} \leq SL_3(\mathbb{Z}).$$

Proof. Let $G = \left\{ \begin{pmatrix} 1 & n & p \\ 0 & 1 & m \\ 0 & 0 & 1 \end{pmatrix} \mid m, n, p \in \mathbb{Z} \right\} \leq SL_3(\mathbb{Z})$.

We define

$$\begin{aligned}\Phi : H_3 &\rightarrow G \\ a &\mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \\ b &\mapsto \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ c &\mapsto \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.\end{aligned}$$

Let's see that Φ is well-defined:

$$\begin{aligned}([a, b]c)\Phi &= (a^{-1}b^{-1}abc)\Phi = ((a)\Phi)^{-1}((b)\Phi)^{-1}((a)\Phi)((b)\Phi)((c)\Phi) \\ &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & -1 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.\end{aligned}$$

$$\begin{aligned}([a, c])\Phi &= (a^{-1}c^{-1}ac)\Phi = ((a)\Phi)^{-1}((c)\Phi)^{-1}((a)\Phi)((c)\Phi) \\ &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\end{aligned}$$

$$= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

$$\begin{aligned} ([b, c])\Phi &= (b^{-1}c^{-1}bc)\Phi = ((b)\Phi)^{-1}((c)\Phi)^{-1}((b)\Phi)((c)\Phi) \\ &= \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & -1 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \end{aligned}$$

So, Φ is well-defined.

Let's see that Φ is onto. Let $\begin{pmatrix} 1 & n & p \\ 0 & 1 & m \\ 0 & 0 & 1 \end{pmatrix} \in G$, and consider $u = a^m b^n c^p \in H_3$, then, we have that

$$\begin{aligned} (u)\Phi &= (a^m b^n c^p)\Phi = ((a)\Phi)^m ((b)\Phi)^n ((c)\Phi)^p \\ &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & m \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & n & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & p \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & n & 0 \\ 0 & 1 & m \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & p \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & n & p \\ 0 & 1 & m \\ 0 & 0 & 1 \end{pmatrix}. \end{aligned}$$

So, Φ is onto.

Let's see that Φ is injective. Let $u \in H_3$, then, by Theorem 2.1, $u = a^m b^n c^p \in H_3$ and we have that

$$(u)\Phi = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \Leftrightarrow \begin{pmatrix} 1 & n & p \\ 0 & 1 & m \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \Leftrightarrow m = n = p = 0 \Rightarrow u = 1.$$

So, $\text{Ker}(\Phi) = 1$ and Φ is injective. □

Corollary 2.3. Given $w \in H_3$, w can be written in a uniquely way in its normal form as $w =_{H_3} a^m b^n c^p$ with $m, n, p \in \mathbb{Z}$.

Proof. Let $w = a^m b^n c^p = a^{m'} b^{n'} c^{p'}$, then applying the isomorphism Φ , we get

$$a^m b^n c^p = a^{m'} b^{n'} c^{p'} \Leftrightarrow \begin{pmatrix} 1 & n & p \\ 0 & 1 & m \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n' & p' \\ 0 & 1 & m' \\ 0 & 0 & 1 \end{pmatrix} \Leftrightarrow p = p', n = n', m = m'.$$

This finishes the proof. □

We also have the following property:

Corollary 2.4. H_3 is torsion-free, that is, the only element with finite order is the trivial one. □

2.2 Endomorphisms of H_3

Lemma 2.5. In H_3 , we have

$$\begin{aligned} b^n a^m &= a^m b^n c^{mn} \\ (a^m b^n c^p)^{-1} &= a^{-m} b^{-n} c^{mn-p}. \end{aligned}$$

Proof.

$$\begin{aligned} (b^n a^m)\Phi &= ((b)\Phi)^n((a)\Phi)^m \\ &= \begin{pmatrix} 1 & n & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & m \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & n & nm \\ 0 & 1 & m \\ 0 & 0 & 1 \end{pmatrix} \\ &= (a^m b^n c^{mn})\Phi. \end{aligned}$$

And we conclude by the injectivity of Φ .

$$\begin{aligned} &((a^m b^n c^p)(a^{-m} b^{-n} c^{mn-p}))\Phi \\ &= ((a^m b^n c^p)\Phi)((a^{-m} b^{-n} c^{mn-p})\Phi) \\ &= \begin{pmatrix} 1 & n & p \\ 0 & 1 & m \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -n & mn-p \\ 0 & 1 & -m \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = (1)\Phi. \end{aligned}$$

So, by the injectivity of Φ , $(a^m b^n c^p)(a^{-m} b^{-n} c^{mn-p}) = 1$ and $(a^m b^n c^p)^{-1} = a^{-m} b^{-n} c^{mn-p}$.

This finishes the proof. □

Theorem 2.6. The center of H_3 is $Z(H_3) = \langle c \rangle \cong \mathbb{Z}$.

Proof. Let $u = a^{m'} b^{n'} c^{p'} \in Z(H_3)$ and $v = a^m b^n c^p \in H_3$, then

$$uv = a^{m'} b^{n'} c^{p'} a^m b^n c^p = a^{m'} b^{n'} a^m b^n c^{p'+p} = a^{m'} a^m b^{n'} b^n c^{p'+p} = a^{m'+m} b^{n'+n} c^{p'+p+n'm},$$

and, similarly $vu = a^{m+m'} b^{n+n'} c^{p+p'+nm'}$. Then, by Corollary 2.3, we have

$$uv = vu, \forall v \in H_3 \Leftrightarrow n'm = nm', \forall m, n \in \mathbb{Z} \Leftrightarrow m' = n' = 0.$$

This finishes the proof. $\square$

Theorem 2.7. *The derived subgroup of H_3 is $H'_3 = \langle c \rangle \cong \mathbb{Z}$.*

Proof. Let $[a^m b^n c^p, a^{m'} b^{n'} c^{p'}]$ be a commutator. Then,

$$\begin{aligned} [a^m b^n c^p, a^{m'} b^{n'} c^{p'}] &= (a^m b^n c^p)^{-1} (a^{m'} b^{n'} c^{p'})^{-1} (a^m b^n c^p) (a^{m'} b^{n'} c^{p'}) \\ &= a^{-m} b^{-n} c^{mn-p} a^{-m'} b^{-n'} c^{m'n'-p'} a^m b^n c^p a^{m'} b^{n'} c^{p'} \\ &= a^{-m} b^{-n} a^{-m'} b^{-n'} a^m b^n a^{m'} b^{n'} c^{mn+m'n'} \\ &= a^{-m} a^{-m'} b^{-n} b^{-n'} a^m a^{m'} b^n b^{n'} c^{mn+m'n'} \\ &= a^{-m-m'} b^{-n-n'} a^{m+m'} b^{n+n'} c^{mn+m'n'+2m'n} \\ &= a^{-m-m'} a^{m+m'} b^{-n-n'} c^{-mn-m'n-mn'-m'n'} b^{n+n'} c^{mn+m'n'+2m'n} \\ &= c^{m'n-mn'}. \end{aligned}$$

This proves that $H'_3 \subseteq \langle c \rangle$. To see $H'_3 \supseteq \langle c \rangle$, since H'_3 is a subgroup, it suffices to show that $c \in H'_3$. Taking $m' = 1, n = 1, m = 0, n' = 0$, we have that $[b, a] = c$, and this finishes the proof. $\square$

Observe that G' is fully-characteristic in G , which means that for every $\varphi \in \text{End}(G)$, $(G')\varphi \subseteq G'$.

In the case of Heisenberg's group, this means that if $\varphi \in \text{End}(H_3)$, then $(c)\varphi = c^\varepsilon$ for $\varepsilon \in \mathbb{Z}$.

Now, let $\varphi \in \text{End}(H_3)$, we can suppose that

$$\begin{aligned} \varphi : H_3 &\rightarrow H_3 \\ a &\mapsto a^{m_{11}} b^{m_{12}} c^{p_1} \\ b &\mapsto a^{m_{21}} b^{m_{22}} c^{p_2} \\ c &\mapsto c^\varepsilon. \end{aligned}$$

Then, φ must be well-defined, so

$$\begin{aligned} 1 &= ([a, b]c)\varphi = (a^{-1}b^{-1}abc)\varphi = ((a)\varphi)^{-1}((b)\varphi)^{-1}((a)\varphi)((b)\varphi)((c)\varphi) \\ &= (a^{m_{11}} b^{m_{12}} c^{p_1})^{-1} (a^{m_{21}} b^{m_{22}} c^{p_2})^{-1} a^{m_{11}} b^{m_{12}} c^{p_1} a^{m_{21}} b^{m_{22}} c^{p_2} c^\varepsilon \\ &= a^{-m_{11}} b^{-m_{12}} c^{m_{11}m_{12}-p_1} a^{-m_{21}} b^{-m_{22}} c^{m_{21}m_{22}-p_2} a^{m_{11}} b^{m_{12}} c^{p_1} a^{m_{21}} b^{m_{22}} c^{p_2} c^\varepsilon \\ &= a^{-m_{11}} b^{-m_{12}} a^{-m_{21}} b^{-m_{22}} a^{m_{11}} b^{m_{12}} a^{m_{21}} b^{m_{22}} c^{m_{11}m_{12}+m_{21}m_{22}+\varepsilon} \\ &= a^{-m_{11}} b^{-m_{12}} a^{-m_{21}} b^{-m_{22}} a^{m_{11}} a^{m_{21}} b^{m_{12}} b^{m_{22}} c^{m_{11}m_{12}+m_{21}m_{22}+\varepsilon} \\ &= a^{-m_{11}} b^{-m_{12}} a^{-m_{21}} b^{-m_{22}} a^{m_{11}+m_{21}} b^{m_{12}+m_{22}} c^{m_{11}m_{12}+m_{21}m_{22}+\varepsilon} \\ &= a^{-m_{11}} b^{-m_{12}} a^{-m_{21}} a^{m_{11}+m_{21}} b^{-m_{22}} c^{-m_{22}m_{11}-m_{22}m_{21}} b^{m_{12}+m_{22}} c^{m_{11}m_{12}+m_{21}m_{12}+m_{21}m_{22}+\varepsilon} \\ &= a^{-m_{11}} b^{-m_{12}} a^{m_{11}} b^{m_{12}} c^{-m_{22}m_{11}+m_{12}m_{21}+m_{11}m_{12}+\varepsilon} \\ &= a^{-m_{11}} a^{m_{11}} b^{-m_{12}} c^{-m_{12}m_{11}} b^{m_{12}} c^{-m_{22}m_{11}+m_{12}m_{21}+m_{11}m_{12}+\varepsilon} \\ &= c^{\varepsilon-m_{11}m_{22}+m_{12}m_{21}}. \end{aligned}$$

This implies that $\begin{vmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{vmatrix} = m_{11}m_{22} - m_{21}m_{12} = \varepsilon$.

The other 2 relations are trivially sent to 1 by the choice of $(c)\varphi$.

We can associate to $\varphi \in \text{End}(H_3)$, a matrix $M = \begin{bmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{bmatrix}$ and a vector $\mathbf{p} = [p_1, p_2]$. Then, given the image of a and b by φ , the image of c is already determined ($(c)\varphi = c^{\det(M)}$).

Theorem 2.8. *Every endomorphism $\varphi \in \text{End}(H_3)$ has the form*

$$\begin{aligned} \varphi : H_3 &\rightarrow H_3 \\ a &\mapsto a^{m_{11}} b^{m_{12}} c^{p_1} \\ b &\mapsto a^{m_{21}} b^{m_{22}} c^{p_2} \\ c &\mapsto c^{\det(M)}. \end{aligned}$$

Reciprocally, given a matrix $M = \begin{bmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{bmatrix} \in \mathcal{M}_2(\mathbb{Z})$ and a vector $\mathbf{p} = [p_1, p_2] \in \mathbb{Z}^2$, we can define an endomorphism of H_3 with the earlier form.

2.3 Automorphisms of H_3

Now, we focus our attention on automorphisms, that is, bijective endomorphisms. We introduce a lemma that will be useful for the computations.

Lemma 2.9. *In H_3 ,*

$$(a^m b^n)^k = a^{km} b^{kn} c^{\frac{k(k-1)}{2} mn}.$$

Proof. It is trivially true for $k = 0$.

By induction on k , if $k > 0$:

If $k = 1$, then $(a^m b^n)^1 = a^m b^n$.

Suppose it is true for k , let's see for $k + 1$:

$$\begin{aligned} (a^m b^n)^{k+1} &= a^m b^n (a^m b^n)^k =_{IH} a^m b^n a^{km} b^{kn} c^{\frac{k(k-1)}{2} mn} \\ &= a^m a^{km} b^n b^{kn} c^{kmn} c^{\frac{k(k-1)}{2} mn} \\ &= a^{(k+1)m} b^{(k+1)n} c^{(\frac{k(k-1)}{2} + \frac{2k}{2}) mn} \\ &= a^{(k+1)m} b^{(k+1)n} c^{\frac{k(k+1)}{2} mn}. \end{aligned}$$

If $k < 0$, let $l = -k$. Then,

$$\begin{aligned}
(a^m b^n)^k &= ((a^m b^n)^{-1})^l = (b^{-n} a^{-m})^l \\
&= (a^{-m} b^{-n} c^{mn})^l = (a^{-m} b^{-n})^l c^{lmn} \\
&= a^{-lm} b^{-ln} c^{\frac{l(l-1)}{2} mn} c^{lmn} \\
&= a^{-lm} b^{-ln} c^{\frac{l(l+1)}{2} mn} \\
&= a^{-lm} b^{-ln} c^{\frac{-l(-l-1)}{2} mn} \\
&= a^{km} b^{kn} c^{\frac{k(k-1)}{2} mn}.
\end{aligned}$$

This finishes the proof. $\square$

Now, given φ an endomorphism, we check under which conditions φ is also injective. If it is injective, that means that $\text{Ker}(\varphi) = 1$, so if $(a^m b^n c^p)\varphi = 1$, then $m = n = p = 0$. We denote $\varepsilon = \det(M)$.

$$\begin{aligned}
1 &= (a^m b^n c^p)\varphi = ((a)\varphi)^m ((b)\varphi)^n ((c)\varphi)^p \\
&= (a^{m_{11}} b^{m_{12}} c^{p_1})^m (a^{m_{21}} b^{m_{22}} c^{p_2})^n c^{\varepsilon p} \\
&= (a^{m_{11}} b^{m_{12}})^m (a^{m_{21}} b^{m_{22}})^n c^{mp_1 + np_2 + \varepsilon p} \\
&= a^{mm_{11}} b^{mm_{12}} c^{\frac{m(m-1)}{2} m_{11} m_{12}} a^{nm_{21}} b^{nm_{22}} c^{\frac{n(n-1)}{2} m_{21} m_{22}} c^{mp_1 + np_2 + \varepsilon p} \\
&= a^{mm_{11}} b^{mm_{12}} a^{nm_{21}} b^{nm_{22}} c^{\frac{m(m-1)}{2} m_{11} m_{12} + \frac{n(n-1)}{2} m_{21} m_{22} + mp_1 + np_2 + \varepsilon p} \\
&= a^{mm_{11}} a^{nm_{21}} b^{mm_{12}} b^{nm_{22}} c^{mn m_{12} m_{21}} c^{\frac{m(m-1)}{2} m_{11} m_{12} + \frac{n(n-1)}{2} m_{21} m_{22} + mp_1 + np_2 + \varepsilon p} \\
&= a^{mm_{11} + nm_{21}} b^{mm_{12} + nm_{22}} c^{\frac{m(m-1)}{2} m_{11} m_{12} + mn m_{12} m_{21} + \frac{n(n-1)}{2} m_{21} m_{22} + mp_1 + np_2 + \varepsilon p}.
\end{aligned}$$

This gives us the equations:

$$\begin{cases}
mm_{11} + nm_{21} &= 0 \\
mm_{12} + nm_{22} &= 0 \\
p\varepsilon + mp_1 + np_2 + \frac{m(m-1)}{2} m_{11} m_{12} + \frac{n(n-1)}{2} m_{21} m_{22} + nm m_{12} m_{21} &= 0
\end{cases}$$

If we consider the first two equations, they form a linear system on variables m, n whose coefficient matrix has determinant:

$$\begin{vmatrix} m_{11} & m_{21} \\ m_{12} & m_{22} \end{vmatrix} = m_{11} m_{22} - m_{21} m_{12} = \varepsilon.$$

So, this linear system has a non trivial rational solution (and therefore a non trivial integer solution because it is homogeneous), if and only if, $\varepsilon = 0$.

Assuming $\varepsilon \neq 0$, necessarily, $m = n = 0$, and substituting in the third equation, we get $p\varepsilon = 0 \Rightarrow p = 0$. This implies that our φ is injective, if and only if, $\det(M) \neq 0$.

Since we want to focus on automorphisms, to see which endomorphisms are actually automorphisms, we are going to use the fact that G' is characteristic in G . This implies that, actually, if $\varphi \in \text{End}(H_3)$ is an automorphism, then $(c)\varphi = c$ or $(c)\varphi = c^{-1}$, so $\det(M) = \pm 1$ and $M \in GL_2(\mathbb{Z})$.

We check that this condition is not only necessary, but also sufficient for $\varphi \in \text{End}(H_3)$ to be an automorphism.

Let

$$\begin{aligned}\varphi : H_3 &\rightarrow H_3 \\ a &\mapsto a^{m_{11}} b^{m_{12}} c^{p_1} \\ b &\mapsto a^{m_{21}} b^{m_{22}} c^{p_2} \\ c &\mapsto c^\varepsilon,\end{aligned}$$

where $\varepsilon = \det(M) = \pm 1$.

Notice that $\text{Im}(\varphi) = \langle a^{m_{11}} b^{m_{12}} c^{p_1}, a^{m_{21}} b^{m_{22}} c^{p_2}, c \rangle$. Since $(a^{m_{11}} b^{m_{12}} c^{p_1})^{m_{22}} (a^{m_{21}} b^{m_{22}} c^{p_2})^{-m_{12}} \in \text{Im}(\varphi)$. Developing this expression:

$$\begin{aligned}(a^{m_{11}} b^{m_{12}} c^{p_1})^{m_{22}} (a^{m_{21}} b^{m_{22}} c^{p_2})^{-m_{12}} &= a^{m_{11}m_{22}} b^{m_{12}m_{22}} c^{\frac{m_{22}(m_{22}-1)}{2} m_{11}m_{12}} c^{m_{22}p_1} \\ &a^{-m_{21}m_{12}} b^{-m_{22}m_{12}} c^{\frac{-m_{12}(-m_{12}-1)}{2} m_{21}m_{22}} c^{-m_{12}p_2} \\ &= a^{m_{11}m_{22}} b^{m_{12}m_{22}} a^{-m_{21}m_{12}} b^{-m_{22}m_{12}} \\ &c^{\frac{m_{22}(m_{22}-1)}{2} m_{11}m_{12} + \frac{m_{12}(m_{12}+1)}{2} m_{21}m_{22} + m_{22}p_1 - m_{12}p_2} \\ &= a^{m_{11}m_{22}} a^{-m_{21}m_{12}} b^{m_{12}m_{22}} c^{-m_{12}^2 m_{21}m_{22}} b^{-m_{22}m_{12}} \\ &c^{\frac{m_{22}(m_{22}-1)}{2} m_{11}m_{12} + \frac{m_{12}(m_{12}+1)}{2} m_{21}m_{22} + m_{22}p_1 - m_{12}p_2} \\ &= a^\varepsilon c^{\frac{m_{22}(m_{22}-1)}{2} m_{11}m_{12} - m_{22}m_{12}^2 m_{21} + \frac{m_{12}(m_{12}+1)}{2} m_{21}m_{22} + m_{22}p_1 - m_{12}p_2} \\ &= a^\varepsilon c^{\frac{m_{22}(m_{22}-1)}{2} m_{11}m_{12} + \frac{m_{12}^2 + m_{12} - 2m_{12}^2}{2} m_{21}m_{22} + m_{22}p_1 - m_{12}p_2} \\ &= a^\varepsilon c^{\frac{m_{22}(m_{22}-1)}{2} m_{11}m_{12} + \frac{m_{12} - m_{12}^2}{2} m_{21}m_{22} + m_{22}p_1 - m_{12}p_2} \\ &= a^\varepsilon c^{\frac{m_{22}(m_{22}-1)}{2} m_{11}m_{12} - \frac{m_{12}(m_{12}-1)}{2} m_{21}m_{22} + m_{22}p_1 - m_{12}p_2}.\end{aligned}$$

So, this implies that $a \in \text{Im}(\varphi)$.

In particular, we can see that

$$(a^{m_{22}\varepsilon} b^{-m_{12}\varepsilon} c^{\varepsilon \left(\frac{m_{12}(m_{12}-1)}{2} m_{21}m_{22} - \frac{m_{22}(m_{22}-1)}{2} m_{11}m_{12} - m_{22}p_1 + m_{12}p_2 \right)})_\varphi = a$$

Analogously, $(a^{m_{11}} b^{m_{12}} c^{p_1})^{-m_{21}} (a^{m_{21}} b^{m_{22}} c^{p_2})^{m_{11}} \in \text{Im}(\varphi)$ and developing, we get:

$$(a^{m_{11}} b^{m_{12}} c^{p_1})^{-m_{21}} (a^{m_{21}} b^{m_{22}} c^{p_2})^{m_{11}} = b^\varepsilon c^{-\frac{m_{21}(m_{21}-1)}{2} m_{11}m_{12} + \frac{m_{11}(m_{11}-1)}{2} m_{21}m_{22} - m_{21}p_1 + m_{11}p_2}$$

So, this implies that $b \in \text{Im}(\varphi)$.

In particular, we can see that

$$(a^{-m_{21}\varepsilon} b^{m_{11}\varepsilon} c^{\varepsilon \left(\frac{m_{21}(m_{21}-1)}{2} m_{11}m_{12} - \frac{m_{11}(m_{11}-1)}{2} m_{21}m_{22} + m_{21}p_1 - m_{11}p_2 \right)})_\varphi = b$$

We have proven that $\text{Im}(\varphi) = \langle a, b, c \rangle = H_3$.

And, in particular, given φ , we have that:

$$\begin{aligned}
\varphi^{-1} : H_3 &\rightarrow H_3 \\
a &\mapsto a^{m_{22}\varepsilon} b^{-m_{12}\varepsilon} c^{\varepsilon \left(\frac{m_{12}(m_{12}-1)}{2} m_{21} m_{22} - \frac{m_{22}(m_{22}-1)}{2} m_{11} m_{12} - m_{22} p_1 + m_{12} p_2 \right)} \\
b &\mapsto a^{-m_{21}\varepsilon} b^{m_{11}\varepsilon} c^{\varepsilon \left(\frac{m_{21}(m_{21}-1)}{2} m_{11} m_{12} - \frac{m_{11}(m_{11}-1)}{2} m_{21} m_{22} + m_{21} p_1 - m_{11} p_2 \right)} \\
c &\mapsto c^{\varepsilon}
\end{aligned}$$

The conclusion of this section is the following:

Theorem 2.10. *Let $\varphi \in \text{Aut}(H_3)$, then*

$$\begin{aligned}
\varphi : H_3 &\rightarrow H_3 \\
a &\mapsto a^{m_{11}} b^{m_{12}} c^{p_1} \\
b &\mapsto a^{m_{21}} b^{m_{22}} c^{p_2} \\
c &\mapsto c^{\det(M)}
\end{aligned}$$

with $M = \begin{bmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{bmatrix} \in GL_2(\mathbb{Z})$.

Reciprocally, an invertible matrix $M \in GL_2(\mathbb{Z})$ and a vector $\mathbf{p} = [p_1, p_2] \in \mathbb{Z}^2$ define an automorphism of H_3 with the earlier form. $\square$

From now on, we will denote $\varphi_{M,\mathbf{p}}$ the automorphism with associated matrix M and vector $\mathbf{p}$.

2.4 Structure of $\text{Aut}(H_3)$

Now, once we have Theorem 2.10, we want to deduce the exact structure of $\text{Aut}(H_3)$. We start computing how the composition of automorphisms works. Let $\varphi_{M,\mathbf{p}}, \varphi_{N,\mathbf{q}} \in \text{Aut}(H_3)$, then, denoting $\varepsilon_M = \det(M)$ and $\varepsilon_N = \det(N)$,

$$\begin{aligned}
\varphi_{M,\mathbf{p}} : H_3 &\rightarrow H_3 \\
a &\mapsto a^{m_{11}} b^{m_{12}} c^{p_1} \\
b &\mapsto a^{m_{21}} b^{m_{22}} c^{p_2} \\
c &\mapsto c^{\varepsilon_M},
\end{aligned}$$

$$\begin{aligned}
\varphi_{N,\mathbf{q}} : H_3 &\rightarrow H_3 \\
a &\mapsto a^{n_{11}} b^{n_{12}} c^{q_1} \\
b &\mapsto a^{n_{21}} b^{n_{22}} c^{q_2} \\
c &\mapsto c^{\varepsilon_N}.
\end{aligned}$$

Now, we compute $\varphi_{M,\mathbf{p}}\varphi_{N,\mathbf{q}}$:

$$\begin{aligned}
(a)\varphi_{M,\mathbf{p}}\varphi_{N,\mathbf{q}} &= (a^{m_{11}}b^{m_{12}}c^{p_1})\varphi_{N,\mathbf{q}} = ((a)\varphi_{N,\mathbf{q}})^{m_{11}}((b)\varphi_{N,\mathbf{q}})^{m_{12}}((c)\varphi_{N,\mathbf{q}})^{p_1} \\
&= (a^{n_{11}}b^{n_{12}}c^{q_1})^{m_{11}}(a^{n_{21}}b^{n_{22}}c^{q_2})^{m_{12}}c^{p_1\varepsilon_N} \\
&= (a^{n_{11}}b^{n_{12}})^{m_{11}}(a^{n_{21}}b^{n_{22}})^{m_{12}}c^{m_{11}q_1+m_{12}q_2+p_1\varepsilon_N} \\
&= a^{m_{11}n_{11}}b^{m_{11}n_{12}}c^{\frac{m_{11}(m_{11}-1)}{2}n_{11}n_{12}}a^{m_{12}n_{21}}b^{m_{12}n_{22}}c^{\frac{m_{12}(m_{12}-1)}{2}n_{21}n_{22}}c^{m_{11}q_1+m_{12}q_2+p_1\varepsilon_N} \\
&= a^{m_{11}n_{11}}a^{m_{12}n_{21}}b^{m_{11}n_{12}}c^{m_{11}m_{12}n_{12}n_{21}}b^{m_{12}n_{22}} \\
&= c^{\frac{m_{12}(m_{12}-1)}{2}n_{21}n_{22}+\frac{m_{11}(m_{11}-1)}{2}n_{11}n_{12}+m_{11}q_1+m_{12}q_2+p_1\varepsilon_N} \\
&= a^{m_{11}n_{11}+m_{12}n_{21}}b^{m_{11}n_{12}+m_{12}n_{22}} \\
&= c^{\frac{m_{12}(m_{12}-1)}{2}n_{21}n_{22}+\frac{m_{11}(m_{11}-1)}{2}n_{11}n_{12}+m_{11}m_{12}n_{12}n_{21}+m_{11}q_1+m_{12}q_2+p_1\varepsilon_N},
\end{aligned}$$

$$\begin{aligned}
(b)\varphi_{M,\mathbf{p}}\varphi_{N,\mathbf{q}} &= (a^{m_{21}}b^{m_{22}}c^{p_2})\varphi_{N,\mathbf{q}} = ((a)\varphi_{N,\mathbf{q}})^{m_{21}}((b)\varphi_{N,\mathbf{q}})^{m_{22}}((c)\varphi_{N,\mathbf{q}})^{p_2} \\
&= (a^{n_{11}}b^{n_{12}}c^{q_1})^{m_{21}}(a^{n_{21}}b^{n_{22}}c^{q_2})^{m_{22}}c^{p_2\varepsilon_N} \\
&= (a^{n_{11}}b^{n_{12}})^{m_{21}}(a^{n_{21}}b^{n_{22}})^{m_{22}}c^{m_{21}q_1+m_{22}q_2+p_2\varepsilon_N} \\
&= a^{m_{21}n_{11}}b^{m_{21}n_{12}}c^{\frac{m_{21}(m_{21}-1)}{2}n_{11}n_{12}}a^{m_{22}n_{21}}b^{m_{22}n_{22}}c^{\frac{m_{22}(m_{22}-1)}{2}n_{21}n_{22}}c^{m_{21}q_1+m_{22}q_2+p_2\varepsilon_N} \\
&= a^{m_{21}n_{11}}a^{m_{22}n_{21}}b^{m_{21}n_{12}}c^{m_{21}m_{22}n_{12}n_{21}}b^{m_{22}n_{22}} \\
&= c^{\frac{m_{22}(m_{22}-1)}{2}n_{21}n_{22}+\frac{m_{21}(m_{21}-1)}{2}n_{11}n_{12}+m_{21}q_1+m_{22}q_2+p_2\varepsilon_N} \\
&= a^{m_{21}n_{11}+m_{22}n_{21}}b^{m_{21}n_{12}+m_{22}n_{22}} \\
&= c^{\frac{m_{22}(m_{22}-1)}{2}n_{21}n_{22}+\frac{m_{21}(m_{21}-1)}{2}n_{11}n_{12}+m_{21}m_{22}n_{12}n_{21}+m_{21}q_1+m_{22}q_2+p_2\varepsilon_N},
\end{aligned}$$

$$(c)\varphi_{M,\mathbf{p}}\varphi_{N,\mathbf{q}} = (c^{\varepsilon_M})\varphi_{N,\mathbf{q}} = c^{\varepsilon_M\varepsilon_N}.$$

We can see that the matrix associated to $\varphi_{M,\mathbf{p}}\varphi_{N,\mathbf{q}}$ is MN , so we can define an epimorphism:

$$\begin{aligned}
\beta : \text{Aut}(H_3) &\rightarrow GL_2(\mathbb{Z}) \\
\varphi_{M,\mathbf{p}} &\mapsto \det(M)M
\end{aligned}$$

In fact, we have the following short exact sequence:

$$1 \rightarrow \mathbb{Z}^2 \xrightarrow{\alpha} \text{Aut}(H_3) \xrightarrow{\beta} GL_2(\mathbb{Z}) \rightarrow 1$$

where $\mathbf{p}\alpha = \varphi_{I,\mathbf{p}}$ and $\varphi_{M,\mathbf{p}}\beta = \det(M)M$.

By [19], this short exact sequence splits. So, in fact, $\text{Aut}(H_3) \cong \mathbb{Z}^2 \rtimes GL_2(\mathbb{Z})$. Adapting the results of the article to our notation, it splits as follows:

First, take the presentation $GL_2(\mathbb{Z}) = \langle \rho, \tau, \kappa \mid \rho\tau\rho = \tau\rho\tau, (\rho\tau\rho)^4 = 1, \kappa\tau\kappa^{-1} = \tau^{-1}, \kappa\rho\kappa^{-1} =$

$\rho^{-1}, \kappa^2 = 1\rangle$, where

$$\begin{aligned}\rho \text{ corresponds to } T &:= \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \\ \tau \text{ corresponds to } U &:= \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}, \text{ and} \\ \kappa \text{ corresponds to } J &:= \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}.\end{aligned}$$

Define

$$\begin{aligned}s : GL_2(\mathbb{Z}) &\rightarrow Aut(H_3) \\ \rho &\mapsto \varphi_{T, \mathbf{0}_2} \\ \tau &\mapsto \varphi_{U, \mathbf{0}_2} \\ \kappa &\mapsto \varphi_{-J, [-1, 0]}.\end{aligned}$$

See that s is well-defined:

- We check that the first relation $(\rho\tau\rho = \tau\rho\tau)$ is kept by s :

$$\begin{aligned}(a)(\rho\tau\rho)s &= (a)\varphi_{T, \mathbf{0}_2}\varphi_{U, \mathbf{0}_2}\varphi_{T, \mathbf{0}_2} \\ &= (ab)\varphi_{U, \mathbf{0}_2}\varphi_{T, \mathbf{0}_2} \\ &= (aa^{-1}b)\varphi_{T, \mathbf{0}_2} \\ &= b \\ (a)(\tau\rho\tau)s &= (a)\varphi_{U, \mathbf{0}_2}\varphi_{T, \mathbf{0}_2}\varphi_{U, \mathbf{0}_2} \\ &= (a)\varphi_{T, \mathbf{0}_2}\varphi_{U, \mathbf{0}_2} \\ &= (ab)\varphi_{U, \mathbf{0}_2} \\ &= aa^{-1}b \\ &= b\end{aligned}$$

So, the images of a coincide.

$$\begin{aligned}(b)(\rho\tau\rho)s &= (b)\varphi_{T, \mathbf{0}_2}\varphi_{U, \mathbf{0}_2}\varphi_{T, \mathbf{0}_2} \\ &= (b)\varphi_{U, \mathbf{0}_2}\varphi_{T, \mathbf{0}_2} \\ &= (a^{-1}b)\varphi_{T, \mathbf{0}_2} \\ &= (ab)^{-1}b \\ &= a^{-1}c \\ (b)(\tau\rho\tau)s &= (b)\varphi_{U, \mathbf{0}_2}\varphi_{T, \mathbf{0}_2}\varphi_{U, \mathbf{0}_2} \\ &= (a^{-1}b)\varphi_{T, \mathbf{0}_2}\varphi_{U, \mathbf{0}_2} \\ &= ((ab)^{-1}b)\varphi_{U, \mathbf{0}_2} \\ &= (a^{-1}c)\varphi_{U, \mathbf{0}_2} \\ &= a^{-1}c\end{aligned}$$

So, the images of b coincide.

So, $(\rho\tau\rho)s = (\tau\rho\tau)s$.

- We check that the second relation $((\rho\tau\rho)^4 = 1)$ is kept by s :

From previous computations, we already know that $(\rho\tau\rho)s$ acts as: $a \mapsto b$ and $b \mapsto a^{-1}c$.

$$\begin{aligned}
 (a)((\rho\tau\rho)^4)s &= (a)((\rho\tau\rho)s)^4 \\
 &= (b)((\rho\tau\rho)s)^3 \\
 &= (a^{-1}c)((\rho\tau\rho)s)^2 \\
 &= (((a)(\rho\tau\rho)s)^{-1}(c)(\rho\tau\rho)s)((\rho\tau\rho)s) \\
 &= (b^{-1}c)((\rho\tau\rho)s) \\
 &= ((b)(\rho\tau\rho)s)^{-1}(c)(\rho\tau\rho)s \\
 &= (a^{-1}c)^{-1}c \\
 &= (c^{-1}a)c \\
 &= a(c^{-1}c) \\
 &= a
 \end{aligned}$$

It leaves fixed a .

$$\begin{aligned}
 (b)((\rho\tau\rho)^4)s &= (b)((\rho\tau\rho)s)^4 \\
 &= (a^{-1}c)((\rho\tau\rho)s)^3 \\
 &= (((a)(\rho\tau\rho)s)^{-1}(c)(\rho\tau\rho)s)((\rho\tau\rho)s)^2 \\
 &= (b^{-1}c)((\rho\tau\rho)s)^2 \\
 &= (((b)(\rho\tau\rho)s)^{-1}(c)(\rho\tau\rho)s)((\rho\tau\rho)s) \\
 &= ((a^{-1}c)^{-1}c)((\rho\tau\rho)s) \\
 &= (c^{-1}ac)((\rho\tau\rho)s) \\
 &= (a)((\rho\tau\rho)s) \\
 &= b
 \end{aligned}$$

It leaves fixed b .

So, $((\rho\tau\rho)^4)s$ is the identity.

- We check that the third relation $(\kappa\tau\kappa^{-1} = \tau^{-1})$ is kept by s :

First, we verify the relation on a :

$$\begin{aligned}
(a)(\kappa\tau\kappa^{-1})s &= (a)(\kappa s)(\tau s)(\kappa s)^{-1} \\
&= (ac^{-1})(\tau s)(\kappa s)^{-1} \\
&= ((a)(\tau s)((c)(\tau s))^{-1})(\kappa s)^{-1} \\
&= (ac^{-1})(\kappa s)^{-1} \\
&= (a)(\kappa s)^{-1}((c)(\kappa s)^{-1})^{-1} \\
&= (ac^{-1})(c^{-1})^{-1} \\
&= ac^{-1}c \\
&= a \\
(a)(\tau^{-1})s &= a
\end{aligned}$$

Next, we verify the relation on b :

$$\begin{aligned}
(b)(\kappa\tau\kappa^{-1})s &= (b)(\kappa s)(\tau s)(\kappa s)^{-1} \\
&= (b^{-1})(\tau s)(\kappa s)^{-1} \\
&= (((b)(\tau s))^{-1})(\kappa s)^{-1} \\
&= (a^{-1}b)^{-1}(\kappa s)^{-1} \\
&= (b^{-1}a)(\kappa s)^{-1} \\
&= (b^{-1})(\kappa s)^{-1}(a)(\kappa s)^{-1} \\
&= b(ac^{-1}) \\
&= bac^{-1} \\
&= (abc)c^{-1} \\
&= ab \\
(b)(\tau^{-1})s &= ab
\end{aligned}$$

- We check that the fourth relation $(\kappa\rho\kappa^{-1} = \rho^{-1})$ is kept by s :

First, we verify the relation on a :

$$\begin{aligned}
(a)(\kappa\rho\kappa^{-1})s &= (a)(\kappa s)(\rho s)(\kappa s)^{-1} \\
&= (ac^{-1})(\rho s)(\kappa s)^{-1} \\
&= ((a)(\rho s)((c)(\rho s))^{-1})(\kappa s)^{-1} \\
&= (abc^{-1})(\kappa s)^{-1} \\
&= (a)(\kappa s)^{-1}(b)(\kappa s)^{-1}((c)(\kappa s)^{-1})^{-1} \\
&= (ac^{-1})(b^{-1})(c^{-1})^{-1} \\
&= ac^{-1}b^{-1}c \\
&= ab^{-1} \\
(a)(\rho^{-1})s &= ab^{-1}
\end{aligned}$$

Next, we verify the relation on b :

$$\begin{aligned}
(b)(\kappa\rho\kappa^{-1})s &= (b)(\kappa s)(\rho s)(\kappa s)^{-1} \\
&= (b^{-1})(\rho s)(\kappa s)^{-1} \\
&= (((b)(\rho s))^{-1})(\kappa s)^{-1} \\
&= (b^{-1})(\kappa s)^{-1} \\
&= (((b)(\kappa s)^{-1})^{-1}) \\
&= (b^{-1})^{-1} \\
&= b \\
(b)(\rho^{-1})s &= b
\end{aligned}$$

- We check the fifth relation ($\kappa^2 = 1$) is kept by s :

First, we verify the relation on a :

$$\begin{aligned}
(a)(\kappa^2)s &= (a)(\kappa s)^2 \\
&= (ac^{-1})(\kappa s) \\
&= (a)(\kappa s)((c)(\kappa s))^{-1} \\
&= (ac^{-1})(c^{-1})^{-1} \\
&= ac^{-1}c \\
&= a
\end{aligned}$$

κ^2 leaves a fixed.

$$\begin{aligned}
(b)(\kappa^2)s &= (b)(\kappa s)^2 \\
&= (b^{-1})(\kappa s) \\
&= (((b)(\kappa s))^{-1}) \\
&= (b^{-1})^{-1} \\
&= b
\end{aligned}$$

κ^2 leaves b fixed.

So, κ^2 is the identity.

And it is clear that $s\beta = Id_{GL_2(\mathbb{Z})}$.

As a result, we obtain the following result:

Theorem 2.11. *The group of automorphisms of H_3 is isomorphic to the following group:*

$$Aut(H_3) \cong \mathbb{Z}^2 \rtimes GL_2(\mathbb{Z}).$$

□

2.5 Conjugacy Problem and Twisted Conjugacy Problem

Before studying the twisted conjugacy problem, we solve the conjugacy problem in H_3 .

Given $a^r b^s c^t, a^u b^v c^w \in H_3$, we want to see if there exists $a^{x_1} b^{x_2} c^{x_3} \in H_3$ such that $a^r b^s c^t = (a^{x_1} b^{x_2} c^{x_3})^{-1} a^u b^v c^w a^{x_1} b^{x_2} c^{x_3}$. Developing, we get the following:

$$\begin{aligned}
 a^r b^s c^t &= (a^{x_1} b^{x_2} c^{x_3})^{-1} a^u b^v c^w a^{x_1} b^{x_2} c^{x_3} \\
 &= a^{-x_1} b^{-x_2} c^{-x_1 x_2 - x_3} a^u b^v c^w a^{x_1} b^{x_2} c^{x_3} \\
 &= a^{-x_1} b^{-x_2} a^u b^v a^{x_1} b^{x_2} c^{w+x_1 x_2} \\
 &= a^{-x_1} a^u b^{-x_2} c^{-u x_2} b^v a^{x_1} b^{x_2} c^{w+x_1 x_2} \\
 &= a^{-x_1+u} b^{-x_2+v} a^{x_1} b^{x_2} c^{w+x_1 x_2 - u x_2} \\
 &= a^{-x_1+u} a^{x_1} b^{-x_2+v} c^{-x_1 x_2 + v x_1} b^{x_2} c^{w+x_1 x_2 - u x_2} \\
 &= a^u b^v c^{w+v x_1 - u x_2}
 \end{aligned}$$

Therefore, $a^r b^s c^t \sim a^u b^v c^w$, if and only if, $r = u$, $s = v$ and there exist $x_1, x_2 \in \mathbb{Z}$ such that $t = w + v x_1 - u x_2$. This is equivalent to $r = u$, $s = v$ and $t \equiv w \pmod{g}$ where $g = \gcd(u, v) = \gcd(r, s)$.

Now, we go to the twisted conjugacy problem. Given $a^r b^s c^t, a^u b^v c^w \in H_3$ and $\varphi_{M,p} \in \text{Aut}(H_3)$,

$$\begin{aligned}
 \varphi_{M,p} : H_3 &\rightarrow H_3 \\
 a &\mapsto a^{m_{11}} b^{m_{12}} c^{p_1} \\
 b &\mapsto a^{m_{21}} b^{m_{22}} c^{p_2} \\
 c &\mapsto c^{\varepsilon_M},
 \end{aligned}$$

we want to see if $a^r b^s c^t \sim_{\varphi_{M,p}} a^u b^v c^w$. That is, if there exists $a^{x_1} b^{x_2} c^{x_3} \in H_3$ such that $a^r b^s c^t = ((a^{x_1} b^{x_2} c^{x_3}) \varphi_{M,p})^{-1} a^u b^v c^w a^{x_1} b^{x_2} c^{x_3}$. Developing, we get

$$\begin{aligned}
 a^r b^s c^t &= ((a^{x_1} b^{x_2} c^{x_3}) \varphi_{M,p})^{-1} a^u b^v c^w a^{x_1} b^{x_2} c^{x_3} \\
 &= ((c) \varphi_{M,p})^{-x_3} ((b) \varphi_{M,p})^{-x_2} ((a) \varphi_{M,p})^{-x_1} a^u b^v c^w a^{x_1} b^{x_2} c^{x_3} \\
 &= c^{-x_3 \varepsilon_M} (a^{m_{21}} b^{m_{22}} c^{p_2})^{-x_2} (a^{m_{11}} b^{m_{12}} c^{p_1})^{-x_1} a^u b^v c^w a^{x_1} b^{x_2} c^{x_3} \\
 &= (a^{m_{21}} b^{m_{22}})^{-x_2} (a^{m_{11}} b^{m_{12}})^{-x_1} a^u b^v a^{x_1} b^{x_2} c^{-x_1 p_1 - x_2 p_2 + (1-\varepsilon_M)x_3 + w} \\
 &= a^{-x_2 m_{21}} b^{-x_2 m_{22}} c^{\frac{x_2(x_2+1)}{2} m_{21} m_{22}} a^{-x_1 m_{11}} b^{-x_1 m_{12}} c^{\frac{x_1(x_1+1)}{2} m_{11} m_{12}} a^u b^v a^{x_1} b^{x_2} c^{-x_1 p_1 - x_2 p_2 + (1-\varepsilon_M)x_3 + w} \\
 &= a^{-x_2 m_{21}} b^{-x_2 m_{22}} a^{-x_1 m_{11}} b^{-x_1 m_{12}} a^u b^v a^{x_1} b^{x_2} \\
 &= c^{\frac{x_2(x_2+1)}{2} m_{21} m_{22} + \frac{x_1(x_1+1)}{2} m_{11} m_{12} - x_1 p_1 - x_2 p_2 + (1-\varepsilon_M)x_3 + w} \\
 &= a^{-x_2 m_{21}} a^{-x_1 m_{11}} b^{-x_2 m_{22}} c^{x_1 x_2 m_{11} m_{22}} b^{-x_1 m_{12}} a^u a^{x_1} b^v c^{v x_1} b^{x_2} \\
 &= c^{\frac{x_2(x_2+1)}{2} m_{21} m_{22} + \frac{x_1(x_1+1)}{2} m_{11} m_{12} - x_1 p_1 - x_2 p_2 + (1-\varepsilon_M)x_3 + w} \\
 &= a^{-x_2 m_{21} - x_1 m_{11}} b^{-x_2 m_{22} - x_1 m_{12}} a^{u+x_1} b^{v+x_2} \\
 &= c^{\frac{x_2(x_2+1)}{2} m_{21} m_{22} + x_1 x_2 m_{11} m_{22} + \frac{x_1(x_1+1)}{2} m_{11} m_{12} - x_1 p_1 + v x_1 - x_2 p_2 + (1-\varepsilon_M)x_3 + w} \\
 &= a^{-x_2 m_{21} - x_1 m_{11}} a^{u+x_1} b^{-x_2 m_{22} - x_1 m_{12}} c^{-u x_2 m_{22} - u x_1 m_{12} - x_1 x_2 m_{22} - x_1^2 m_{12}} b^{v+x_2} \\
 &= c^{\frac{x_2(x_2+1)}{2} m_{21} m_{22} + x_1 x_2 m_{11} m_{22} + \frac{x_1(x_1+1)}{2} m_{11} m_{12} - x_1 p_1 + v x_1 - x_2 p_2 + (1-\varepsilon_M)x_3 + w}
 \end{aligned}$$

$$= a^{(1-m_{11})x_1 - m_{21}x_2 + u} b^{-m_{12}x_1 + (1-m_{22})x_2 + v} c^{\frac{x_2(x_2+1)}{2}m_{21}m_{22} + x_1x_2m_{11}m_{22} - ux_2m_{22} - ux_1m_{12} - x_1x_2m_{22} - x_1^2m_{12} + \frac{x_1(x_1+1)}{2}m_{11}m_{12} - x_1p_1 + vx_1 - x_2p_2 + (1-\varepsilon_M)x_3 + w}.$$

If we compare the two sides of the equality, this gives us

$$\begin{cases} (1-m_{11})x_1 - m_{21}x_2 = r-u \\ -m_{12}x_1 + (1-m_{22})x_2 = s-v, \end{cases} \quad (1)$$

and after solving this linear equation $[x_1, x_2](I-M) = [r-u, s-v]$, if it has an integer solution, we have to check the last equation:

$$\begin{aligned} \frac{x_2(x_2+1)}{2}m_{21}m_{22} + x_1x_2(m_{11}m_{22} - m_{22}) - x_1^2m_{12} + \frac{x_1(x_1+1)}{2}m_{11}m_{12} \\ + (v - um_{12} - p_1)x_1 + (-um_{22} - p_2)x_2 + (1 - \varepsilon_M)x_3 = t - w, \end{aligned}$$

which can be rewritten as

$$\begin{aligned} \frac{1}{2}x_1^2(m_{11} - 2)m_{12} + x_1x_2m_{22}(m_{11} - 1) + \frac{1}{2}x_2^2m_{21}m_{22} \\ + (v - um_{12} - p_1 + \frac{1}{2}m_{11}m_{12})x_1 + (-um_{22} - p_2 + \frac{1}{2}m_{21}m_{22})x_2 + (1 - \varepsilon_M)x_3 = t - w. \end{aligned} \quad (2)$$

An algorithm deciding whether two elements are twisted conjugated must first solve the linear system (1). We distinguish the following cases:

- **Incompatible System:** The system has no solution. Therefore, the algorithm must answer no.
- **Compatible Determined System:** The system has a unique solution. We have two subcases:
 - The system has a solution over the integers. We substitute the values of x_1, x_2 in (2).
 - * If $\varepsilon_M = 1$, the value of x_3 doesn't matter, we just check if (2) is verified. If it is verified, the algorithm must answer yes (Our possible conjugator is $a^{x_1}b^{x_2}$). Otherwise, the algorithm must answer no.
 - * If $\varepsilon_M = -1$, we leave $2x_3$ on one side of the equality and check if the other side of the equality is even. If it is even, dividing by 2, we get the value of x_3 , and the algorithm must answer yes (Our possible conjugator is $a^{x_1}b^{x_2}c^{x_3}$). Otherwise, it must answer no.
 - The system has no solution over the integers (the solution is rational). The algorithm must answer no.
- **Compatible Undetermined System:** The system has an infinite number of solutions. We distinguish two subcases:
 - The freedom degree of the system is 2. This means $M = I$, $r = u$ and $s = v$. Then (2) is reduced to

$$(v - p_1)x_1 + (-u - p_2)x_2 = t - w.$$

If $\gcd(v - p_1, -u - p_2) \mid t - w$, then there exist $x_1, x_2 \in \mathbb{Z}$ solutions of this equation, and the algorithm must answer yes (Our conjugator is $a^{x_1}b^{x_2}$ for x_1, x_2 a solution of this equation, which can be computed using Bezout's identity and Euclides' extended algorithm).

Otherwise, the algorithm must answer no.

- The freedom degree of the system is 1. Then, one of the two equations of the system is a linear combination of the other. The system [1](#) reduces to $\alpha x_1 + \beta x_2 = \gamma$ with $\gcd(\alpha, \beta, \gamma) = 1$. We know this equation has solution over the integers, if and only if, $\gcd(\alpha, \beta) \mid \gamma$. If this is not the case, the algorithm must answer no. Otherwise, we denote $g = \gcd(\alpha, \beta)$, and let $y_1, y_2 \in \mathbb{Z}$ such that $\alpha y_1 + \beta y_2 = g$. Then $x_1 = y_1 \frac{\gamma}{g}$, $x_2 = y_2 \frac{\gamma}{g}$ is a particular solution of $\alpha x_1 + \beta x_2 = \gamma$. The general solution of this equation (over the integers) is $x_1 = y_1 \frac{\gamma}{g} + \lambda \frac{\beta}{g}$, $x_2 = y_2 \frac{\gamma}{g} - \lambda \frac{\alpha}{g}$ with $\lambda \in \mathbb{Z}$.

It is left to check whether equation [\(2\)](#) is verified for some $\lambda \in \mathbb{Z}$ or not. Substituting the general value of x_1 and x_2 on the equation, the only variables are λ and x_3 . We distinguish two cases:

- * If $\varepsilon_M = 1$, then the value of x_3 doesn't matter. Equation [\(2\)](#) reduces to a degree two equation on λ . We can compute the solutions of this equation over $\mathbb{C}$ and check if any of the two solutions is integer. If yes, the algorithm must answer yes, substitute the value of λ on the expressions of x_1 and x_2 and return $a^{x_1} b^{x_2}$ as a possible conjugator. If no, the algorithm must answer no.
- * If $\varepsilon_M = -1$, then what we can do is to leave $2x_3$ on the right-hand side of the equality, and the two-degree polynomial on λ on the left-hand side. After multiplying by 2 if there are any denominators on the coefficients of the two-degree polynomial on λ , we can reduce the equation modulo 2 or 4, and check for $\lambda \in \{0, 1\}$ ($\{0, 1, 2, 3\}$ if we have reduced the equation modulo 4) if the equation has a solution modulo 2 (or 4). If it has no solution, the algorithm must answer no. If it has a solution, the algorithm must answer yes. In order to give a possible conjugator, it must substitute the value of λ on x_1 and x_2 , and also on [\(2\)](#) and solve the equation for x_3 . Then, our possible conjugator would be $a^{x_1} b^{x_2} c^{x_3}$.

As a result of this section, we obtain the following theorem:

Theorem 2.12. *The Twisted Conjugacy Problem is solvable in H_3 .* □

Now, we give an example of this. Suppose

$$M = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}, \quad \mathbf{p} = [2, 3].$$

We want to check whether $abc^2 \sim_{\varphi_{M, \mathbf{p}}} ab^3c^5$. This is, $r = 1, s = 1, t = 2, u = 1, v = 3, w = 5$. We start with the linear system [\(1\)](#):

$$[0, -2] = [x_1, x_2](I - M) = [x_1, x_2] \begin{bmatrix} 0 & -1 \\ 0 & 2 \end{bmatrix} = [0, -x_1 + 2x_2]$$

This is a compatible undetermined system with freedom degree 1. Our equation is $-x_1 + 2x_2 = -2$. We can see that $x_1 = 2 + 2\lambda$ and $x_2 = \lambda$ for $\lambda \in \mathbb{Z}$ is the general solution of this equation (over the integers).

We substitute these values on equation (2):

$$\begin{aligned} 2 - 5 &= \frac{1}{2}(2\lambda + 2)^2(-1) \cdot 1 + \lambda(2\lambda + 2) \cdot 0 \cdot (-1) + \frac{\lambda^2}{2} \cdot 0 \cdot (-1) \\ &\quad + \left(\frac{1}{2} \cdot 1 \cdot 1 - 1 \cdot 1 + 3 - 2 \right) (2\lambda + 2) \\ &\quad + \left(\frac{1}{2} \cdot 0 \cdot (-1) + 1 - 3 \right) \lambda + 2x_3, \end{aligned}$$

$$-3 = -2(\lambda^2 + 2\lambda + 1) + \lambda + 1 - 2\lambda + 2x_3,$$

$$-2x_3 = -2\lambda^2 - 5\lambda + 2.$$

Reducing this last equation modulo 2, we get $\lambda \equiv 0 \pmod{2}$. Substituting $\lambda = 0$, we get $x_1 = 2, x_2 = 0, x_3 = -1$. Therefore, a $\varphi_{M,p}$ -twisted conjugator is a^2c^{-1} .

We verify it:

$$\begin{aligned} abc^2 &\stackrel{?}{=} ((c)\varphi_{M,p})((a)\varphi_{M,p})^{-2}(ab^3c^5)(a^2c^{-1}) \\ &= (abc^2)^{-2}ab^3a^2c^{-1+5-1} \\ &= b^{-1}a^{-1}b^{-1}a^{-1}ab^3a^2c^{-1} \\ &= a^{-1}b^{-1}b^2a^2 \\ &= a^{-1}a^2bc^2 \\ &= abc^2 \end{aligned}$$

2.6 Orbit decidability

For a finite presentation $G = \langle X \mid R \rangle$ and a group of automorphisms $A \leq \text{Aut}(G)$, given two words on the generators $u, v \in F(X)$, the **orbit decidability problem**, $OD(A)$, consists on deciding whether the corresponding elements $u, v \in G$ can be mapped to each other by some automorphism in A , i.e., whether there exists $\varphi \in A$ such that $(u)\varphi = v$.

In this section, we study the orbit decidability of subgroups of the Heisenberg automorphism group.

2.6.1 $OD(\text{Aut}(H_3))$

We start with the full automorphism group, which is orbit decidable.

Given $u, v \in H_3$, we want to decide whether there exists $\varphi_{M,p} \in \text{Aut}(H_3)$ such that $(u)\varphi_{M,p} = v$.

We consider $u = a^{u_1}b^{u_2}c^{u_3}$ and $v = a^{v_1}b^{v_2}c^{v_3}$. For these two elements to be in the same orbit, a necessary condition is that there exists an invertible matrix M such that $[u_1, u_2]M = [v_1, v_2]$, which means $m_{1j}u_1 + m_{2j}u_2 = v_j$, so $\gcd(u_1, u_2) \mid v_j$, and furthermore, since M is invertible, $\gcd(v_1, v_2) \mid u_i$. This means we must have $\gcd(u_1, u_2) = \gcd(v_1, v_2) = g$.

Therefore, a possible algorithm that checks whether u and v are in the same orbit, must first compute $\gcd(u_1, u_2)$ and $\gcd(v_1, v_2)$. If they are not equal, it must answer no.

Suppose now $\gcd(u_1, u_2) = \gcd(v_1, v_2) = g$. Using Bezout's identity, there exist $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ such that $a_1 u_1 + a_2 u_2 = g = b_1 v_1 + b_2 v_2$, computable using Euclides' extended algorithm. We define $c_1 = \frac{u_1}{g}, c_2 = \frac{u_2}{g}, d_1 = \frac{v_1}{g}, d_2 = \frac{v_2}{g}$.

Integer solutions of the equations $u_1 x_1 + u_2 x_2 = 0$ are of the form $x_1 = -\alpha c_2, x_2 = \alpha c_1$ where $\alpha \in \mathbb{Z}$.

A particular solution of $u_1 x_1 + u_2 x_2 = v_j$ is $x_1 = d_j a_1, x_2 = d_j a_2$.

Therefore, the coefficients of a possible matrix M must be of the form $m_{ij} = d_j a_i + (-1)^i \alpha_j c_{3-i}$ for $i, j = 1, 2$ and $\alpha_j \in \mathbb{Z}$ a free parameter.

$$M = \begin{bmatrix} d_1 a_1 - \alpha_1 c_2 & d_2 a_1 - \alpha_2 c_2 \\ d_1 a_2 + \alpha_1 c_1 & d_2 a_2 + \alpha_2 c_1 \end{bmatrix}$$

We compute $\det(M)$:

$$\begin{aligned} \det(M) &= \begin{vmatrix} d_1 a_1 & d_2 a_1 \\ d_1 a_2 & d_2 a_2 \end{vmatrix} + \begin{vmatrix} -\alpha_1 c_2 & d_2 a_1 \\ \alpha_1 c_1 & d_2 a_2 \end{vmatrix} + \begin{vmatrix} d_1 a_1 & -\alpha_2 c_2 \\ d_1 a_2 & \alpha_2 c_1 \end{vmatrix} + \begin{vmatrix} -\alpha_1 c_2 & -\alpha_2 c_2 \\ \alpha_1 c_1 & \alpha_2 c_1 \end{vmatrix} \\ &= \alpha_1 d_2 \begin{vmatrix} -c_2 & a_1 \\ c_1 & a_2 \end{vmatrix} + \alpha_2 d_1 \begin{vmatrix} a_1 & -c_2 \\ a_2 & c_1 \end{vmatrix} = (\alpha_2 d_1 - \alpha_1 d_2) \begin{vmatrix} a_1 & -c_2 \\ a_2 & c_1 \end{vmatrix} \\ &= \alpha_2 d_1 - \alpha_1 d_2 = \varepsilon \end{aligned}$$

We want $\varepsilon = \pm 1$, so $\alpha_j = (-1)^j \varepsilon b_{3-j} + \beta d_j$ for $j = 1, 2$ and $\beta \in \mathbb{Z}$.

Now, if $a^{v_1} b^{v_2} c^{v_3} = (a^{u_1} b^{u_2} c^{u_3}) \varphi_{M,p}$, then M must have the form we just computed and the exponents of c must verify the following:

$$a^{v_1} b^{v_2} c^{v_3} = (a^{u_1} b^{u_2} c^{u_3}) \varphi_{M,p} = a^{u_1 m_{11} + u_2 m_{21}} b^{u_1 m_{12} + u_2 m_{22}} c^{\frac{u_2(u_2-1)}{2} m_{21} m_{22} + \frac{u_1(u_1-1)}{2} m_{11} m_{12} + u_1 u_2 m_{12} m_{21} + u_1 p_1 + u_2 p_2 + \varepsilon u_3}$$

$$v_3 - \varepsilon u_3 = \frac{u_2(u_2-1)}{2} m_{21} m_{22} + \frac{u_1(u_1-1)}{2} m_{11} m_{12} + u_1 u_2 m_{12} m_{21} + u_1 p_1 + u_2 p_2$$

The equation $u_1 x_1 + u_2 x_2 = K$ has a solution over the integers if and only if $g = \gcd(u_1, u_2) \mid K$.

In our case, if $2 \nmid g$ (if u_1 and u_2 are not both even), then this last equation has a solution, if and only if, $v_3 \equiv \pm u_3 \pmod{g}$, since $g \mid \frac{u_i(u_i-1)}{2}$ and $g \mid u_1 u_2$.

Otherwise, if u_1 and u_2 are both even, it could happen that $g \nmid \frac{u_i(u_i-1)}{2}$. In order to check whether this equation has solutions or not, we can substitute m_{ij} by the value we computed earlier and check whether

$$\frac{u_2(u_2-1)}{2} m_{21} m_{22} + \frac{u_1(u_1-1)}{2} m_{11} m_{12} + \varepsilon u_3 - v_3 \equiv 0 \pmod{g}$$

which can be reduced to

$$\underbrace{-\frac{g}{2} \left(\frac{u_2}{g} m_{21} m_{22} + \frac{u_1}{g} m_{11} m_{12} \right)}_D + \varepsilon u_3 - v_3 \equiv 0 \pmod{g} \quad (3)$$

According to Lemma 2.16, which we will see in the following section, in this case, the value of D modulo g does not depend on β or ε , which are the free parameters we can choose to determine a possible matrix.

Therefore, we just compute D modulo g for $\beta = 0$ and check if equation (3) is verified for $\varepsilon \in \{-1, 1\}$. So, checking a finite number of possibilities, we can decide whether u and v are in the same orbit or not.

As a result, we obtain the following theorem:

Theorem 2.13. *The full group of automorphisms of H_3 is Orbit Decidable.* $\square$

A direct application of Theorem 1.1 gives us the following corollary:

Corollary 2.14. *Let H be a torsion-free hyperbolic group (with n generators) and let $\varphi_{M_1, p^1}, \dots, \varphi_{M_n, p^n} \in \text{Aut}(H_3)$ be automorphisms such that $\langle \varphi_{M_1, p^1}, \dots, \varphi_{M_n, p^n} \rangle = \text{Aut}(H_3)$. Then the Conjugacy Problem is solvable in any group of the form $H_3 \rtimes_{\varphi_{M_1, p^1}, \dots, \varphi_{M_n, p^n}} H$.* $\square$

2.6.2 $\text{OD}(\langle \varphi_{M_1, p^1}, \dots, \varphi_{M_n, p^n} \rangle \text{Inn}(H_3))$

Now, we study the orbit decidability of any finitely generated subgroup A such that $\text{Inn}(H_3) \leq A \leq \text{Aut}(H_3)$.

For this purpose, we will use the following result:

Theorem 2.15 (Bogopolski–Martino–Ventura, [7]). *Every finitely generated subgroup of $\text{Aut}(\mathbb{Z}^2) = \text{GL}_2(\mathbb{Z})$ is orbit decidable, i.e., there exists an algorithm deciding whether there exists $N \in \langle M_1, \dots, M_n \rangle$ such that $[u_1, u_2]N = [v_1, v_2]$ and computing such N in the case it exists given $[u_1, u_2], [v_1, v_2] \in \mathbb{Z}^2$ and $\langle M_1, \dots, M_n \rangle \leq \text{GL}_2(\mathbb{Z})$.*

Given $u = a^{u_1} b^{u_2} c^{u_3}$, $v = a^{v_1} b^{v_2} c^{v_3} \in H_3$, we want to find out if there exists $\psi \in \langle \varphi_{M_1, p^1}, \dots, \varphi_{M_n, p^n} \rangle \text{Inn}(H_3)$, such that $(u)\psi = v$.

The algorithm solving this problem must first check whether there exists $N \in \langle M_1, \dots, M_n \rangle$ such that $[u_1, u_2]N = [v_1, v_2]$. If no, it must answer no.

Otherwise, suppose we have $N = M_{i_1}^{k_1} \dots M_{i_l}^{k_l}$ such that $[u_1, u_2]N = [v_1, v_2]$ ($\gcd(u_1, u_2) = \gcd(v_1, v_2) = g$ in this case). We can compute $\varphi_{N, r} = \varphi_{M_{i_1}, p^{i_1}}^{k_1} \dots \varphi_{M_{i_l}, p^{i_l}}^{k_l}$. Then, we have

$$(u)\varphi_{N, r} = a^{v_1} b^{v_2} c^{u_3 \varepsilon_N + \frac{u_1(u_1-1)}{2} n_{11} n_{12} + u_1 u_2 n_{12} n_{21} + \frac{u_2(u_2-1)}{2} n_{21} n_{22} + u_1 r_1 + u_2 r_2}$$

Let us call C the exponent of c in the last expression.

Recall that in this case, $(u)\varphi_{N, r} \sim v$ ($\sim$ meaning they are conjugated), if and only if, $v_3 \equiv C \pmod{g}$.

We can simplify C a lot modulo g . If $2 \nmid g$, we have

$$C \equiv u_3 \varepsilon_N \pmod{g} \quad (4)$$

If $2 \mid g$, we have

$$C \equiv u_3 \varepsilon_N - \frac{g}{2} \left(\frac{u_1}{g} n_{11} n_{12} + \frac{u_2}{g} n_{21} n_{22} \right) \pmod{g} \quad (5)$$

First, we will prove the following lemma:

Lemma 2.16. *In the case $2 \mid g$, if N, N' are two matrices such that $[u_1, u_2]N = [u_1, u_2]N' = [v_1, v_2]$, then*

$$\frac{g}{2} \left(\frac{u_1}{g} n_{11} n_{12} + \frac{u_2}{g} n_{21} n_{22} \right) \equiv \frac{g}{2} \left(\frac{u_1}{g} n'_{11} n'_{12} + \frac{u_2}{g} n'_{21} n'_{22} \right) \pmod{g} \quad (6)$$

Proof. First, we see that (6) is equivalent to

$$\frac{u_1}{g} n_{11} n_{12} + \frac{u_2}{g} n_{21} n_{22} \equiv \frac{u_1}{g} n'_{11} n'_{12} + \frac{u_2}{g} n'_{21} n'_{22} \pmod{2} \quad (7)$$

To see this, notice that if $[u_1, u_2]N = [u_1, u_2]N' = [v_1, v_2]$, then $[v_1, v_2]N^{-1}N' = [v_1, v_2]$, that is, $Q = N^{-1}N' \in \text{Fix}([v_1, v_2])$.

$$N' = NQ = \begin{bmatrix} n_{11} & n_{12} \\ n_{21} & n_{22} \end{bmatrix} \begin{bmatrix} q_{11} & q_{12} \\ q_{21} & q_{22} \end{bmatrix} = \begin{bmatrix} n_{11}q_{11} + n_{12}q_{21} & n_{11}q_{12} + n_{12}q_{22} \\ n_{21}q_{11} + n_{22}q_{21} & n_{21}q_{12} + n_{22}q_{22} \end{bmatrix}$$

We have then

$$\begin{aligned} \frac{u_1}{g} n'_{11} n'_{12} + \frac{u_2}{g} n'_{21} n'_{22} &= \frac{u_1}{g} (n_{11}q_{11} + n_{12}q_{21})(n_{11}q_{12} + n_{12}q_{22}) \\ &\quad + \frac{u_2}{g} (n_{21}q_{11} + n_{22}q_{21})(n_{21}q_{12} + n_{22}q_{22}) \\ &= \frac{u_1}{g} n_{11}^2 q_{11} q_{12} + \frac{u_1}{g} n_{11} n_{12} (q_{11} q_{22} + q_{21} q_{12}) + \frac{u_1}{g} n_{12}^2 q_{21} q_{22} \\ &\quad + \frac{u_2}{g} n_{21}^2 q_{11} q_{12} + \frac{u_2}{g} n_{21} n_{22} (q_{11} q_{22} + q_{21} q_{12}) + \frac{u_2}{g} n_{22}^2 q_{21} q_{22} \\ &= \frac{u_1}{g} n_{11}^2 q_{11} q_{12} + \frac{u_1}{g} n_{11} n_{12} (\varepsilon_Q + 2q_{21} q_{12}) + \frac{u_1}{g} n_{12}^2 q_{21} q_{22} \\ &\quad + \frac{u_2}{g} n_{21}^2 q_{11} q_{12} + \frac{u_2}{g} n_{21} n_{22} (\varepsilon_Q + 2q_{21} q_{12}) + \frac{u_2}{g} n_{22}^2 q_{21} q_{22} \\ &\equiv \frac{u_1}{g} n_{11} n_{12} + \frac{u_2}{g} n_{21} n_{22} + \left(\frac{u_1}{g} n_{11}^2 + \frac{u_2}{g} n_{21}^2 \right) q_{11} q_{12} \\ &\quad + \left(\frac{u_1}{g} n_{12}^2 + \frac{u_2}{g} n_{22}^2 \right) q_{21} q_{22} \pmod{2} \end{aligned}$$

Therefore, in order to prove (7), we just have to prove that

$$\left(\frac{u_1}{g} n_{11}^2 + \frac{u_2}{g} n_{21}^2 \right) q_{11} q_{12} + \left(\frac{u_1}{g} n_{12}^2 + \frac{u_2}{g} n_{22}^2 \right) q_{21} q_{22} \equiv 0 \pmod{2}$$

In addition, since an expression squared stays the same modulo 2, we can reduce it to

$$\left(\frac{u_1}{g} n_{11} + \frac{u_2}{g} n_{21} \right) q_{11} q_{12} + \left(\frac{u_1}{g} n_{12} + \frac{u_2}{g} n_{22} \right) q_{21} q_{22} \equiv 0 \pmod{2} \quad (8)$$

We note that $[u_1, u_2]N = [v_1, v_2] = [v_1, v_2]Q$, which results, dividing by g , in the equations:

$$\frac{u_1}{g} n_{11} + \frac{u_2}{g} n_{21} = \frac{v_1}{g} = \frac{v_1}{g} q_{11} + \frac{v_2}{g} q_{21} \quad (9)$$

$$\frac{u_1}{g} n_{12} + \frac{u_2}{g} n_{22} = \frac{v_2}{g} = \frac{v_1}{g} q_{12} + \frac{v_2}{g} q_{22} \quad (10)$$

We also note that since $\gcd(\frac{u_1}{g}, \frac{u_2}{g}) = \gcd(\frac{v_1}{g}, \frac{v_2}{g}) = 1$ and N, Q have determinant ± 1 , we know that $\frac{u_1}{g}$ and $\frac{u_2}{g}$ cannot be both even, $\frac{v_1}{g}$ and $\frac{v_2}{g}$ cannot be both even and the two elements of the same row (or the same column) of N or Q cannot be both even.

Taking all this into account, if we assume $\frac{v_1}{g}$ is even, then $\frac{v_2}{g}$ is odd, and reducing (9) modulo 2, we obtain

$$\frac{u_1}{g}n_{11} + \frac{u_2}{g}n_{21} \equiv 0 \equiv q_{21} \pmod{2}$$

Therefore, (8) is true in this case.

Analogously, if we assume $\frac{v_2}{g}$ is even, then $\frac{v_1}{g}$ is odd, and reducing (10) modulo 2, we obtain

$$\frac{u_1}{g}n_{12} + \frac{u_2}{g}n_{22} \equiv 0 \equiv q_{12} \pmod{2}$$

Therefore, (8) is true in this case.

We just have to check what happens in the case $\frac{v_1}{g}$ and $\frac{v_2}{g}$ are both odd. In this case, substituting in (9) and (10), we get

$$\frac{u_1}{g}n_{11} + \frac{u_2}{g}n_{21} \equiv 1 \equiv q_{11} + q_{21} \pmod{2} \quad (11)$$

$$\frac{u_1}{g}n_{12} + \frac{u_2}{g}n_{22} \equiv 1 \equiv q_{12} + q_{22} \pmod{2} \quad (12)$$

The equation (8) is reduced to

$$q_{11}q_{12} + q_{21}q_{22} \equiv 0 \pmod{2} \quad (13)$$

We know that $q_{11} + q_{21}$ is odd, therefore, we have two possible cases:

- q_{11} even and q_{21} odd.
- q_{11} odd and q_{21} even.

We know that $q_{12} + q_{22}$ is odd, therefore, we have two possible cases:

- q_{12} even and q_{22} odd.
- q_{12} odd and q_{22} even.

We have a total of 4 possible cases:

- q_{11} even, q_{21} odd, q_{12} even and q_{22} odd. This case is not possible because row 1 of Q would have 2 as common factor.
- q_{11} even, q_{21} odd, q_{12} odd and q_{22} even. In this case, (13) is true.
- q_{11} odd, q_{21} even, q_{12} even and q_{22} odd. In this case, (13) is true.
- q_{11} odd, q_{21} even, q_{12} odd and q_{22} even. This case is not possible because row 2 of Q would have 2 as common factor.

In all cases, (13) and therefore, (8) is true. So this finishes the proof of (6). □

Notice that there could be more than one $N \in \langle M_1, \dots, M_n \rangle$ verifying $[u_1, u_2]N = [v_1, v_2]$ and also each of these N could be rewritten in different ways as a word on $M_1, \dots, M_n$ (what could change r). However, by Lemma 2.16, in the case $2 \mid g$, the second addend of the expression (5) does not depend on the choice of N among all matrices N such that $[u_1, u_2]N = [v_1, v_2]$ and, in addition, neither (4) nor (5) depend on r .

The only thing that depends on the choice of N in both expressions (4) and (5) is ε_N .

If we want to decide whether there exists $\psi \in \langle \varphi_{M_1, \mathbf{p}^1}, \dots, \varphi_{M_n, \mathbf{p}^n} \rangle \text{Inn}(H_3)$ such that $(u)\psi = v$, after making all these computations, if $2 \nmid g$, we check whether

$$v_3 \equiv u_3 \varepsilon_N \pmod{g} \quad (14)$$

or if $2 \mid g$, we check whether

$$v_3 \equiv u_3 \varepsilon_N - \frac{g}{2} \left(\frac{u_1}{g} n_{11} n_{12} + \frac{u_2}{g} n_{21} n_{22} \right) \pmod{g} \quad (15)$$

If yes, the algorithm answers yes.

If not, but we have, in the case $2 \nmid g$, that

$$v_3 \equiv -u_3 \varepsilon_N \pmod{g} \quad (16)$$

or, in the case $2 \mid g$, that

$$v_3 \equiv -u_3 \varepsilon_N - \frac{g}{2} \left(\frac{u_1}{g} n_{11} n_{12} + \frac{u_2}{g} n_{21} n_{22} \right) \pmod{g}, \quad (17)$$

there exists ψ if and only if there exists $Q \in \langle M_1, \dots, M_n \rangle$ such that $\det(Q) = -1$ and $[v_1, v_2]Q = [v_1, v_2]$.

This is because if such Q exists, then $NQ \in \langle M_1, \dots, M_n \rangle$ and $[u_1, u_2]NQ = [v_1, v_2]$, so substituting N by $N' = NQ$, the condition (14) transforms to (16) ($\varepsilon_{N'} = -\varepsilon_N$) and the condition (15) transforms to (17) ($\varepsilon_{N'} = -\varepsilon_N$ and Lemma 2.16 tells us the second addend does not change modulo g).

If we are not in any of these two cases, the algorithm must answer no.

It remains to prove the following lemma in order to conclude the orbit decidability:

Lemma 2.17. *There exists an algorithm determining whether there exists $Q \in \langle M_1, \dots, M_n \rangle$ such that $\det(Q) = -1$ and $[v_1, v_2]Q = [v_1, v_2]$.*

Proof. If all M_i 's have determinant 1, the answer is no.

Otherwise, assume without any loss of generality that M_1 has determinant -1. If there are other matrices with determinant -1, for instance, M_2 , we can substitute them by $M_1 M_2$. Then $M_1 M_2$ has determinant 1 and $\langle M_1, M_2, \dots, M_n \rangle = \langle M_1, M_1 M_2, \dots, M_n \rangle$.

Therefore, we can assume without any loss of generality that M_1 is the only matrix with determinant -1 and all other matrices have determinant 1.

We will prove that, in this case,

$$SL_2(\mathbb{Z}) \cap \langle M_1, M_2, \dots, M_n \rangle = \langle M_1^2, M_2, \dots, M_n, M_1^{-1} M_2 M_1, \dots, M_1^{-1} M_n M_1 \rangle$$

Clearly, we have the inclusion $\supseteq$.

Then, to prove the inclusion $\leq$, given $N \in SL_2(\mathbb{Z}) \cap \langle M_1, M_2, \dots, M_n \rangle$, we know that

$$N = \prod_{j=1}^k M_{i_j}^{\varepsilon_j} = M_{i_1}^{\varepsilon_1} M_{i_2}^{\varepsilon_2} \dots M_{i_k}^{\varepsilon_k} \quad (18)$$

with $i_j \in \{1, \dots, n\}$ and $\varepsilon_j \in \{-1, 1\}$ for $j = 1, \dots, k$.

Since $N \in SL_2(\mathbb{Z})$, we know that the number of appearances of M_1 is even. We will prove that $N \in \langle M_1^2, M_2, \dots, M_n, M_1^{-1}M_2M_1, \dots, M_1^{-1}M_nM_1 \rangle$ by induction on the number of appearances of M_1 .

If N has no appearances of M_1 , then clearly, $N \in \langle M_2, \dots, M_n \rangle \leq \langle M_1^2, M_2, \dots, M_n, M_1^{-1}M_2M_1, \dots, M_1^{-1}M_nM_1 \rangle$.

Now, suppose M_1 appears at least two times:

We look for the first and the second appearance of M_1 in (18). If the second appearance of M_1 has the same exponent as the first appearance, we have

$$N = PM_1^\varepsilon QM_1^\varepsilon R$$

where $P, Q \in \langle M_2, \dots, M_n \rangle$ and $R \in \langle M_1, M_2, \dots, M_n \rangle$. We can rearrange the expression as

$$N = P(M_1^2)^\varepsilon M_1^{-\varepsilon} QM_1^\varepsilon R$$

If the second appearance of M_1 has the opposite exponent as the first appearance, we have

$$N = PM_1^{-\varepsilon} QM_1^\varepsilon R$$

where $P, Q \in \langle M_2, \dots, M_n \rangle$ and $R \in \langle M_1, M_2, \dots, M_n \rangle$. If $\varepsilon = -1$, we can rewrite the expression as

$$N = PM_1 QM_1^{-1} R = PM_1^2 M_1^{-1} QM_1 M_1^{-2} R$$

Otherwise,

$$N = PM_1^{-1} QM_1 R$$

Given $M_1^{-1}QM_1$ with $Q \in \langle M_2, \dots, M_n \rangle$, clearly we have that $M_1^{-1}QM_1 \in \langle M_1^{-1}M_2M_1, \dots, M_1^{-1}M_nM_1 \rangle$.

In all of these cases, we have rewritten

$$N = SR$$

where $S \in \langle M_1^2, M_2, \dots, M_n, M_1^{-1}M_2M_1, \dots, M_1^{-1}M_nM_1 \rangle$, $R \in \langle M_1, M_2, \dots, M_n \rangle$ and both S and R have determinant 1.

Applying the inductive hypothesis to R , which has strictly less appearances of M_1 than N , we have that $R \in \langle M_1^2, M_2, \dots, M_n, M_1^{-1}M_2M_1, \dots, M_1^{-1}M_nM_1 \rangle$. So, $N \in \langle M_1^2, M_2, \dots, M_n, M_1^{-1}M_2M_1, \dots, M_1^{-1}M_nM_1 \rangle$.

Once we have this, since $SL_2(\mathbb{Z}) \triangleleft_2 GL_2(\mathbb{Z})$, we know that $H := SL_2(\mathbb{Z}) \cap \langle M_1, M_2, \dots, M_n \rangle \triangleleft_2 \langle M_1, M_2, \dots, M_n \rangle =: G$.

The quotient G/H will have only the elements H (matrices of G with determinant 1) and M_1H (matrices of G with determinant -1). Since H is normal in G , we have that $M_1H = HM_1$.

Therefore, if there exists $Q \in G$ such that $[v_1, v_2]Q = [v_1, v_2]$ and $\det(Q) = -1$, then $Q \in M_1H$ and $Q = M_1T$ where $T \in \langle M_1^2, M_2, \dots, M_n, M_1^{-1}M_2M_1, \dots, M_1^{-1}M_nM_1 \rangle$.

The algorithm determining the existence or inexistence of Q must first compute $[w_1, w_2] := [v_1, v_2]M_1$ and then apply the algorithm of Theorem 2.15 with inputs $[w_1, w_2], [v_1, v_2] \in \mathbb{Z}^2$ and see whether there exists $T \in \langle M_1^2, M_2, \dots, M_n, M_1^{-1}M_2M_1, \dots, M_1^{-1}M_nM_1 \rangle$ such that $[w_1, w_2]T = [v_1, v_2]$. If T exists, the algorithm must answer yes and $Q = M_1T$.

If T does not exist, then Q cannot exist and the algorithm must answer no. $\square$

As a result, we obtain the following theorem:

Theorem 2.18. *Every finitely generated subgroup A of automorphisms such that $\text{Inn}(H_3) \leq A \leq \text{Aut}(H_3)$ is Orbit Decidable.* $\square$

A direct application of Theorem 1.1 gives us the following corollary:

Corollary 2.19. *Let H be a torsion-free hyperbolic group (with n generators) and let $\varphi_{M_1, \mathbf{p}^1}, \dots, \varphi_{M_n, \mathbf{p}^n} \in \text{Aut}(H_3)$ be automorphisms. Then the Conjugacy Problem is solvable in any group of the form $H_3 \rtimes_{\varphi_{M_1, \mathbf{p}^1}, \dots, \varphi_{M_n, \mathbf{p}^n}} H$.* $\square$

3. Heisenberg's group of higher dimensions

3.1 Definition of Heisenberg's group of higher dimensions

Consider

$$H_{k+2} = \langle a_1, a_2, \dots, a_k, b_1, b_2, \dots, b_k, c \mid [a_i, a_j] \forall i < j, \\ [b_i, b_j] \forall i < j, [a_i, b_j] \forall i \neq j, [a_i, b_i]c \forall i, [a_i, c] \forall i, [b_i, c] \forall i \rangle$$

Theorem 3.1. *Given $w \in F(a_1, a_2, \dots, a_k, b_1, b_2, \dots, b_k, c)$ a word, then it can be written in H_{k+2} in its normal form as $w =_{H_{k+2}} a_1^{m_1} a_2^{m_2} \dots a_k^{m_k} b_1^{n_1} b_2^{n_2} \dots b_k^{n_k} c^p$ with $m_1, m_2, \dots, m_k, n_1, n_2, \dots, n_k, p \in \mathbb{Z}$.*

In order to simplify notation, we will write an element $w \in H_{k+2}$ in its normal form as $a^{\mathbf{m}} b^{\mathbf{n}} c^p$, where $a^{\mathbf{m}}$ is short for $a_1^{m_1} a_2^{m_2} \dots a_k^{m_k}$ and the same for $b^{\mathbf{n}}$. Therefore, $\mathbf{m}, \mathbf{n} \in \mathbb{Z}^k$ with this notation.

Theorem 3.2. *H_{k+2} is isomorphic to the following matrices subgroup:*

$$H_{k+2} \cong \left\{ \begin{pmatrix} 1 & \mathbf{n} & p \\ \mathbf{0}_k^T & I_k & \mathbf{m}^T \\ 0 & \mathbf{0}_k & 1 \end{pmatrix} = \begin{pmatrix} 1 & n_1 & n_2 & \dots & n_k & p \\ 0 & 1 & 0 & \dots & 0 & m_1 \\ 0 & 0 & 1 & \dots & 0 & m_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & m_k \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix} \mid m_1, m_2, \dots, m_k, n_1, n_2, \dots, n_k, p \in \mathbb{Z} \right\} \leq SL_{k+2}(\mathbb{Z}).$$

Proof. Let G denote the above subgroup of invertible integer matrices.

Denoting the canonical vectors by $\mathbf{e}_i = [0, \dots, 0, 1, 0, \dots, 0] \in \mathbb{Z}^{k+2}$ where the 1 is at the i -th position, we define

$$\begin{aligned} \Phi : H_{k+2} &\rightarrow G \\ a_i &\mapsto I + A_i \quad \text{for } i = 1, \dots, k \\ b_i &\mapsto I + B_i \quad \text{for } i = 1, \dots, k \\ c &\mapsto I + C \end{aligned}$$

with

$$A_i = [\mathbf{0}^T \quad \mathbf{0}^T \quad \cdots \quad \mathbf{0}^T \quad \mathbf{e}_{i+1}^T] = \begin{bmatrix} \mathbf{0} \\ \vdots \\ \mathbf{0} \\ \mathbf{e}_{k+2} \\ \mathbf{0} \\ \vdots \\ \mathbf{0} \end{bmatrix},$$

where the vector $\mathbf{e}_{k+2}$ is in the $(i+1)$ -th row;

$$B_i = [\mathbf{0}^T \quad \cdots \quad \mathbf{0}^T \quad \mathbf{e}_1^T \quad \mathbf{0}^T \quad \cdots \quad \mathbf{0}^T] = \begin{bmatrix} \mathbf{e}_{i+1} \\ \mathbf{0} \\ \vdots \\ \mathbf{0} \end{bmatrix},$$

where the vector $\mathbf{e}_1^T$ is in the $(i+1)$ -th column; and

$$C = \begin{bmatrix} \mathbf{0} & 1 \\ O & \mathbf{0}^T \end{bmatrix}.$$

It is easy to check that

$$\begin{aligned} A_i B_i &= O, \\ B_i A_i &= \begin{bmatrix} \mathbf{0} & 1 \\ O & \mathbf{0}^T \end{bmatrix} = C, \\ B_i A_j &= O = A_j B_i, \quad \text{if } i \neq j, \\ A_i C &= C A_i = B_i C = C B_i = C C = O, \\ A_i A_j &= O = B_i B_j. \end{aligned}$$

Furthermore, every element $M = \begin{pmatrix} 1 & n_1 & n_2 & \cdots & n_k & p \\ 0 & 1 & 0 & \cdots & 0 & m_1 \\ 0 & 0 & 1 & \cdots & 0 & m_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & m_k \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix} \in G$ can be written as

$$M = I + \sum_{i=1}^k (m_i A_i + n_i B_i) + p C.$$

Let's see that Φ is well-defined:

$$\begin{aligned} ([a_i, a_j])\Phi &= [I + A_i, I + A_j] = (I - A_i)(I - A_j)(I + A_i)(I + A_j) \\ &= (I - A_i - A_j)(I + A_i)(I + A_j) \\ &= (I - A_j)(I + A_j) \\ &= I; \end{aligned}$$

$$\begin{aligned}
([b_i, b_j])\Phi &= [I + B_i, I + B_j] = (I - B_i)(I - B_j)(I + B_i)(I + B_j) \\
&= (I - B_i - B_j)(I + B_i)(I + B_j) \\
&= (I - B_j)(I + B_j) \\
&= I;
\end{aligned}$$

$$\begin{aligned}
([a_i, b_j])\Phi &= [I + A_i, I + B_j] = (I - A_i)(I - B_j)(I + A_i)(I + B_j) \\
&= (I - A_i - B_j)(I + A_i)(I + B_j) \\
&= (I - B_j)(I + B_j) \\
&= I,
\end{aligned}$$

where $i \neq j$, so $A_i B_j = O = B_j A_i$;

$$\begin{aligned}
([a_i, b_i]c)\Phi &= [I + A_i, I + B_i](I + C) = (I - A_i)(I - B_i)(I + A_i)(I + B_i)(I + C) \\
&= (I - A_i - B_i)(I + A_i)(I + B_i)(I + C) \\
&= (I - B_i - C)(I + B_i)(I + C) \\
&= (I - C)(I + C) \\
&= I;
\end{aligned}$$

$$\begin{aligned}
([a_i, c])\Phi &= [I + A_i, I + C] = (I - A_i)(I - C)(I + A_i)(I + C) \\
&= (I - A_i - C)(I + A_i)(I + C) \\
&= (I - C)(I + C) \\
&= I;
\end{aligned}$$

$$\begin{aligned}
([b_i, c])\Phi &= [I + B_i, I + C] = (I - B_i)(I - C)(I + B_i)(I + C) \\
&= (I - B_i - C)(I + B_i)(I + C) \\
&= (I - C)(I + C) \\
&= I.
\end{aligned}$$

So, Φ is well-defined.

Let's see that Φ is onto. Let $M = \begin{pmatrix} 1 & n_1 & n_2 & \cdots & n_k & p \\ 0 & 1 & 0 & \cdots & 0 & m_1 \\ 0 & 0 & 1 & \cdots & 0 & m_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & m_k \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix} \in G$ and consider $u = a^{\mathbf{m}} b^{\mathbf{n}} c^p \in H_{k+2}$

where $\mathbf{m} = [m_1, m_2, \dots, m_k] \in \mathbb{Z}^k$ and $\mathbf{n} = [n_1, n_2, \dots, n_k] \in \mathbb{Z}^k$. Then, it can be checked that

$$(u)\Phi = I + \sum_{i=1}^k (m_i A_i + n_i B_i) + pC = M.$$

So, Φ is onto.

Let's see that Φ is injective. Let $u \in H_{k+2}$, then, by Theorem 3.1, $u = a^{\mathbf{m}}b^{\mathbf{n}}c^p \in H_{k+2}$ and we have that

$$(u)\Phi = I \Leftrightarrow \begin{pmatrix} 1 & n_1 & n_2 & \cdots & n_k & p \\ 0 & 1 & 0 & \cdots & 0 & m_1 \\ 0 & 0 & 1 & \cdots & 0 & m_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & m_k \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix} = I$$

$$\Leftrightarrow m_1 = m_2 = \cdots = m_k = n_1 = n_2 = \cdots = n_k = p = 0 \Leftrightarrow u = 1.$$

So, $\text{Ker}(\Phi) = 1$ and Φ is injective. □

Corollary 3.3. *Given $w \in H_{k+2}$, then w can be written in a uniquely way in its normal form as $w = a^{\mathbf{m}}b^{\mathbf{n}}c^p$ with $\mathbf{m}, \mathbf{n} \in \mathbb{Z}^k$ and $p \in \mathbb{Z}$.* □

The proof of this corollary is done exactly as in the three-dimensional case. We also have the following property:

Corollary 3.4. *H_{k+2} is torsion-free, that is, the only element with finite order is the trivial one.* □

3.2 Endomorphisms of H_{k+2}

Most of the results for the three dimensional Heisenberg group H_3 generalize to higher dimensions. As a result, we have the following analogous results:

Lemma 3.5. *In H_{k+2} , we have $b^{\mathbf{n}}a^{\mathbf{m}} = a^{\mathbf{m}}b^{\mathbf{n}}c^{\mathbf{m}\mathbf{n}^T}$ and $(a^{\mathbf{m}}b^{\mathbf{n}}c^p)^{-1} = a^{-\mathbf{m}}b^{-\mathbf{n}}c^{\mathbf{m}\mathbf{n}^T - p}$.* □

Theorem 3.6. *The center of H_{k+2} is $Z(H_{k+2}) = \langle c \rangle \cong \mathbb{Z}$.* □

Theorem 3.7. *The derived subgroup of H_{k+2} is $H'_{k+2} = \langle c \rangle \cong \mathbb{Z}$.* □

We omit the proof of these results, since the proof is exactly the same as in H_3 bearing in mind that $\mathbf{m}, \mathbf{n}$ are vectors instead of scalars.

Since the derived subgroup is fully-characteristic, we have that if $\varphi \in \text{End}(H_{k+2})$, then $(c)\varphi = c^\mu$ for $\mu \in \mathbb{Z}$.

Now, let $\varphi \in \text{End}(H_{k+2})$, then writing the images of generators in normal form we have

$$\begin{aligned} \varphi : H_{k+2} &\rightarrow H_{k+2} \\ a_1 &\mapsto a^{\mathbf{m}_1^{11}}b^{\mathbf{m}_1^{12}}c^{p_1^{(1)}} \\ a_2 &\mapsto a^{\mathbf{m}_2^{11}}b^{\mathbf{m}_2^{12}}c^{p_2^{(1)}} \\ &\vdots \end{aligned}$$

$$\begin{aligned}
a_k &\mapsto a^{\mathbf{m}_k^{11}} b^{\mathbf{m}_k^{12}} c^{\rho_k^{(1)}} \\
b_1 &\mapsto a^{\mathbf{m}_1^{21}} b^{\mathbf{m}_1^{22}} c^{\rho_1^{(2)}} \\
b_2 &\mapsto a^{\mathbf{m}_2^{21}} b^{\mathbf{m}_2^{22}} c^{\rho_2^{(2)}} \\
&\vdots \\
b_k &\mapsto a^{\mathbf{m}_k^{21}} b^{\mathbf{m}_k^{22}} c^{\rho_k^{(2)}} \\
c &\mapsto c^\mu.
\end{aligned}$$

Since φ must be well-defined, $([a_i, a_j])\varphi = ([b_i, b_j])\varphi = ([a_i, b_j])\varphi = 1$ for $i \neq j$. To reduce computations, note that these commutators are sent to $[a^{\mathbf{m}_i^{\bullet 1}} b^{\mathbf{m}_i^{\bullet 2}} c^{\rho_i^{(\bullet)}} , a^{\mathbf{m}_j^{\blacktriangle 1}} b^{\mathbf{m}_j^{\blacktriangle 2}} c^{\rho_j^{(\blacktriangle)}}]$ where $\bullet, \blacktriangle \in \{1, 2\}$ can be equal or different and $i \neq j$. Therefore, we have

$$\begin{aligned}
1 &= [a^{\mathbf{m}_i^{\bullet 1}} b^{\mathbf{m}_i^{\bullet 2}} c^{\rho_i^{(\bullet)}} , a^{\mathbf{m}_j^{\blacktriangle 1}} b^{\mathbf{m}_j^{\blacktriangle 2}} c^{\rho_j^{(\blacktriangle)}}] \\
&= (a^{\mathbf{m}_i^{\bullet 1}} b^{\mathbf{m}_i^{\bullet 2}} c^{\rho_i^{(\bullet)}})^{-1} (a^{\mathbf{m}_j^{\blacktriangle 1}} b^{\mathbf{m}_j^{\blacktriangle 2}} c^{\rho_j^{(\blacktriangle)}})^{-1} (a^{\mathbf{m}_i^{\bullet 1}} b^{\mathbf{m}_i^{\bullet 2}} c^{\rho_i^{(\bullet)}}) (a^{\mathbf{m}_j^{\blacktriangle 1}} b^{\mathbf{m}_j^{\blacktriangle 2}} c^{\rho_j^{(\blacktriangle)}}) \\
&= a^{-\mathbf{m}_i^{\bullet 1}} b^{-\mathbf{m}_i^{\bullet 2}} c^{\mathbf{m}_i^{\bullet 1}(\mathbf{m}_i^{\bullet 2})^T - \rho_i^{(\bullet)}} a^{-\mathbf{m}_j^{\blacktriangle 1}} b^{-\mathbf{m}_j^{\blacktriangle 2}} c^{\mathbf{m}_j^{\blacktriangle 1}(\mathbf{m}_j^{\blacktriangle 2})^T - \rho_j^{(\blacktriangle)}} a^{\mathbf{m}_i^{\bullet 1}} b^{\mathbf{m}_i^{\bullet 2}} c^{\rho_i^{(\bullet)}} a^{\mathbf{m}_j^{\blacktriangle 1}} b^{\mathbf{m}_j^{\blacktriangle 2}} c^{\rho_j^{(\blacktriangle)}} \\
&= a^{-\mathbf{m}_i^{\bullet 1}} b^{-\mathbf{m}_i^{\bullet 2}} a^{-\mathbf{m}_j^{\blacktriangle 1}} b^{-\mathbf{m}_j^{\blacktriangle 2}} a^{\mathbf{m}_i^{\bullet 1}} b^{\mathbf{m}_i^{\bullet 2}} a^{\mathbf{m}_j^{\blacktriangle 1}} b^{\mathbf{m}_j^{\blacktriangle 2}} c^{\mathbf{m}_i^{\bullet 1}(\mathbf{m}_i^{\bullet 2})^T + \mathbf{m}_j^{\blacktriangle 1}(\mathbf{m}_j^{\blacktriangle 2})^T} \\
&= a^{-\mathbf{m}_i^{\bullet 1} - \mathbf{m}_j^{\blacktriangle 1}} b^{-\mathbf{m}_i^{\bullet 2} - \mathbf{m}_j^{\blacktriangle 2}} a^{\mathbf{m}_i^{\bullet 1}} b^{\mathbf{m}_i^{\bullet 2}} a^{\mathbf{m}_j^{\blacktriangle 1}} b^{\mathbf{m}_j^{\blacktriangle 2}} \\
&\quad c^{\mathbf{m}_i^{\bullet 1}(\mathbf{m}_i^{\bullet 2})^T + \mathbf{m}_j^{\blacktriangle 1}(\mathbf{m}_j^{\blacktriangle 2})^T} c^{\mathbf{m}_i^{\bullet 2}(\mathbf{m}_j^{\blacktriangle 1})^T} \\
&= a^{-\mathbf{m}_j^{\blacktriangle 1}} b^{-\mathbf{m}_j^{\blacktriangle 2}} a^{\mathbf{m}_j^{\blacktriangle 1}} b^{\mathbf{m}_j^{\blacktriangle 2}} \\
&\quad c^{\mathbf{m}_i^{\bullet 1}(\mathbf{m}_i^{\bullet 2})^T + \mathbf{m}_j^{\blacktriangle 1}(\mathbf{m}_j^{\blacktriangle 2})^T} c^{\mathbf{m}_i^{\bullet 2}(\mathbf{m}_j^{\blacktriangle 1})^T} c^{-\mathbf{m}_i^{\bullet 1}(\mathbf{m}_i^{\bullet 2})^T - \mathbf{m}_i^{\bullet 1}(\mathbf{m}_j^{\blacktriangle 2})^T} \\
&= c^{\mathbf{m}_i^{\bullet 2}(\mathbf{m}_j^{\blacktriangle 1})^T - \mathbf{m}_i^{\bullet 1}(\mathbf{m}_j^{\blacktriangle 2})^T}.
\end{aligned}$$

Therefore, we have that

$$\mathbf{m}_i^{\bullet 2} (\mathbf{m}_j^{\blacktriangle 1})^T - \mathbf{m}_i^{\bullet 1} (\mathbf{m}_j^{\blacktriangle 2})^T = 0$$

for $i \neq j$.

In addition to this, we must have $([a_i, b_i]c)\varphi = 1$. This results in:

$$\begin{aligned}
1 &= ([a_i, b_i]c)\varphi = [a^{\mathbf{m}_i^{11}} b^{\mathbf{m}_i^{12}} c^{\rho_i^{(1)}} , a^{\mathbf{m}_i^{21}} b^{\mathbf{m}_i^{22}} c^{\rho_i^{(2)}}] c^\mu \\
&= c^{\mathbf{m}_i^{12}(\mathbf{m}_i^{21})^T - \mathbf{m}_i^{11}(\mathbf{m}_i^{22})^T + \mu}.
\end{aligned}$$

Therefore, we have that

$$\mathbf{m}_i^{11} (\mathbf{m}_i^{22})^T - \mathbf{m}_i^{12} (\mathbf{m}_i^{21})^T = \mu.$$

The relations $[a_i, c]$, $[b_i, c]$ are trivially sent to trivial.

We can define the $2k \times 2k$ matrix

$$M = \left[\begin{array}{c|c} M^{11} & M^{12} \\ \hline M^{21} & M^{22} \end{array} \right] = \left[\begin{array}{c|c} \mathbf{m}_1^{11} & \mathbf{m}_1^{12} \\ \vdots & \vdots \\ \mathbf{m}_k^{11} & \mathbf{m}_k^{12} \\ \hline \mathbf{m}_1^{21} & \mathbf{m}_1^{22} \\ \vdots & \vdots \\ \mathbf{m}_k^{21} & \mathbf{m}_k^{22} \end{array} \right]$$

Then, all these relations can be summarized as:

$$MJM^T = \mu J$$

with

$$J = \begin{bmatrix} O & I_k \\ -I_k & O \end{bmatrix}.$$

Let's check this:

$$\begin{aligned} MJM^T &= \left[\begin{array}{c|c} \mathbf{m}_1^{11} & \mathbf{m}_1^{12} \\ \vdots & \vdots \\ \mathbf{m}_k^{11} & \mathbf{m}_k^{12} \\ \hline \mathbf{m}_1^{21} & \mathbf{m}_1^{22} \\ \vdots & \vdots \\ \mathbf{m}_k^{21} & \mathbf{m}_k^{22} \end{array} \right] \begin{bmatrix} O & I_k \\ -I_k & O \end{bmatrix} M^T \\ &= \left[\begin{array}{c|c} -\mathbf{m}_1^{12} & \mathbf{m}_1^{11} \\ \vdots & \vdots \\ -\mathbf{m}_k^{12} & \mathbf{m}_k^{11} \\ \hline -\mathbf{m}_1^{22} & \mathbf{m}_1^{21} \\ \vdots & \vdots \\ -\mathbf{m}_k^{22} & \mathbf{m}_k^{21} \end{array} \right] \left[\begin{array}{c|c} (\mathbf{m}_1^{11})^T & \dots & (\mathbf{m}_k^{11})^T \\ \hline (\mathbf{m}_1^{12})^T & \dots & (\mathbf{m}_k^{12})^T \end{array} \right] \\ &= \begin{bmatrix} N^{11} & N^{12} \\ N^{21} & N^{22} \end{bmatrix}, \end{aligned}$$

where

$$\begin{aligned} N^{11} &= \left[\mathbf{m}_i^{11} (\mathbf{m}_j^{12})^T - \mathbf{m}_i^{12} (\mathbf{m}_j^{11})^T \right]_{i,j} = [0]_{i,j} = O; \\ N^{12} &= \left[\mathbf{m}_i^{11} (\mathbf{m}_j^{22})^T - \mathbf{m}_i^{12} (\mathbf{m}_j^{21})^T \right]_{i,j} = [\mu \delta_{ij}]_{i,j} = \mu I_k; \\ N^{21} &= \left[\mathbf{m}_i^{21} (\mathbf{m}_j^{12})^T - \mathbf{m}_i^{22} (\mathbf{m}_j^{11})^T \right]_{i,j} = [-\mu \delta_{ij}]_{i,j} = -\mu I_k; \\ N^{22} &= \left[\mathbf{m}_i^{21} (\mathbf{m}_j^{22})^T - \mathbf{m}_i^{22} (\mathbf{m}_j^{21})^T \right]_{i,j} = [0]_{i,j} = O. \end{aligned}$$

So, $MJM^T = \mu J$ and this summarizes all the relations the matrix M must satisfy in order to be the matrix associated to the endomorphism φ .

3.3 Automorphisms of H_{k+2}

Now, we focus our attention on automorphisms in H_{k+2} , that is, bijective endomorphisms. We have the same lemma as in H_3 , which will make computations easier and whose proof is analogous:

Lemma 3.8. In H_{k+2} , $(a^{\mathbf{m}}b^{\mathbf{n}})^l = a^{\mathbf{m}}b^{\mathbf{n}}c^{\frac{l(l-1)}{2}\mathbf{m}\mathbf{n}^T}$.

Now, given φ an endomorphism, we check under which conditions, φ is also injective. If it is injective, that means that $\text{Ker}(\varphi) = 1$, so if $(a^{\mathbf{m}}b^{\mathbf{n}}c^{\mathbf{p}})\varphi = 1$, then $\mathbf{m} = \mathbf{n} = \mathbf{0}_k$ and $\mathbf{p} = 0$.

$$\begin{aligned}
1 &= (a^{\mathbf{m}}b^{\mathbf{n}}c^{\mathbf{p}})\varphi = ((a_1)\varphi)^{m_1}((a_2)\varphi)^{m_2} \dots ((a_k)\varphi)^{m_k}((b_1)\varphi)^{n_1}((b_2)\varphi)^{n_2} \dots ((b_k)\varphi)^{n_k}((c)\varphi)^{\mathbf{p}} \\
&= \left(a^{m_1^{11}}b^{m_1^{12}}c^{p_1^{(1)}}\right)^{m_1} \left(a^{m_2^{11}}b^{m_2^{12}}c^{p_2^{(1)}}\right)^{m_2} \dots \left(a^{m_k^{11}}b^{m_k^{12}}c^{p_k^{(1)}}\right)^{m_k} \\
&\quad \left(a^{m_1^{21}}b^{m_1^{22}}c^{p_1^{(2)}}\right)^{n_1} \left(a^{m_2^{21}}b^{m_2^{22}}c^{p_2^{(2)}}\right)^{n_2} \dots \left(a^{m_k^{21}}b^{m_k^{22}}c^{p_k^{(2)}}\right)^{n_k} c^{\mu\mathbf{p}} \\
&= \left(a^{m_1m_1^{11}}b^{m_1m_1^{12}}c^{\frac{m_1(m_1-1)}{2}m_1^{11}(m_1^{12})^T + m_1p_1^{(1)}}\right) \left(a^{m_2m_2^{11}}b^{m_2m_2^{12}}c^{\frac{m_2(m_2-1)}{2}m_2^{11}(m_2^{12})^T + m_2p_2^{(1)}}\right) \\
&\quad \dots \left(a^{m_km_k^{11}}b^{m_km_k^{12}}c^{\frac{m_k(m_k-1)}{2}m_k^{11}(m_k^{12})^T + m_kp_k^{(1)}}\right) \\
&\quad \left(a^{n_1m_1^{21}}b^{n_1m_1^{22}}c^{\frac{n_1(n_1-1)}{2}m_1^{21}(m_1^{22})^T + n_1p_1^{(2)}}\right) \left(a^{n_2m_2^{21}}b^{n_2m_2^{22}}c^{\frac{n_2(n_2-1)}{2}m_2^{21}(m_2^{22})^T + n_2p_2^{(2)}}\right) \\
&\quad \dots \left(a^{n_km_k^{21}}b^{n_km_k^{22}}c^{\frac{n_k(n_k-1)}{2}m_k^{21}(m_k^{22})^T + n_kp_k^{(2)}}\right) c^{\mu\mathbf{p}} \\
&= a^{\sum_{i=1}^k m_i m_i^{11} + \sum_{i=1}^k n_i m_i^{21}} b^{\sum_{i=1}^k m_i m_i^{12} + \sum_{i=1}^k n_i m_i^{22}} \\
&\quad c^{\mu\mathbf{p} + \sum_{i=1}^k \frac{m_i(m_i-1)}{2} m_i^{11} (m_i^{12})^T + \sum_{i=1}^k \frac{n_i(n_i-1)}{2} m_i^{21} (m_i^{22})^T} \\
&\quad c^{\sum_{i=1}^{k-1} \sum_{j=i+1}^k m_i m_i^{12} (m_j m_j^{11})^T + \sum_{i=1}^{k-1} \sum_{j=i+1}^k n_i m_i^{22} (n_j m_j^{21})^T} \\
&\quad c^{(\sum_{i=1}^k m_i m_i^{12}) \cdot (\sum_{i=1}^k n_i m_i^{21})^T + \sum_{i=1}^k m_i p_i^{(1)} + \sum_{i=1}^k n_i p_i^{(2)}}
\end{aligned}$$

If we want this last expression to be equal to 1, all the exponents must be necessarily equal to 0. Looking at the exponents of a and b , we get the following linear system:

$$\begin{aligned}
\sum_{i=1}^k m_i m_{ij}^{11} + \sum_{i=1}^k n_i m_{ij}^{21} &= 0 & \text{for } j = 1, 2, \dots, k; \\
\sum_{i=1}^k m_i m_{ij}^{12} + \sum_{i=1}^k n_i m_{ij}^{22} &= 0 & \text{for } j = 1, 2, \dots, k;
\end{aligned}$$

where $m_{ij}^{\bullet\blacktriangle}$ denotes the (i, j) element of the matrix $M^{\bullet\blacktriangle}$ for $\bullet, \blacktriangle \in \{1, 2\}$.

This system can be written in matricial form as

$$[\mathbf{m}, \mathbf{n}]M = \mathbf{0}_{2k},$$

where M is the matrix associated to the endomorphism φ defined in the previous section.

This linear system has a non trivial rational solution (and therefore a non trivial integer solution because it is homogeneous), if and only if, $\det(M) = 0$.

Assuming $\det(M) \neq 0$, we have that $m_1 = m_2 = \dots = m_k = n_1 = n_2 = \dots = n_k = 0$ and the exponent of c is reduced to $p\mu$; moreover, $p\mu = 0 \Leftrightarrow \mu = 0$ or $p = 0$. So, in order to force $p = 0$, we must assume $\mu \neq 0$.

Furthermore, using the fact that G' is characteristic in G , we have that, in fact, $(c)\varphi = c$ or $(c)\varphi = c^{-1}$. So, in fact, $\mu = \pm 1$.

Using this, together with the results obtained in the endomorphisms section, we can conclude that $M \in GSp_{2k}(\mathbb{Z})$ (See Appendix A).

It remains to check whether this condition is sufficient for φ to be an automorphism. In particular, we have to check if φ is onto with these conditions.

By the previous section, since $M \in GSp_{2k}(\mathbb{Z})$, we know that M is invertible. Let us denote $N = M^{-1}$

and write $N = \begin{bmatrix} N^{11} & N^{12} \\ N^{21} & N^{22} \end{bmatrix}$, where $N^{\bullet\blacktriangle} = \begin{bmatrix} \mathbf{n}_1^{\bullet\blacktriangle} \\ \mathbf{n}_2^{\bullet\blacktriangle} \\ \vdots \\ \mathbf{n}_k^{\bullet\blacktriangle} \end{bmatrix} \in \mathcal{M}_k(\mathbb{Z})$ for $\bullet, \blacktriangle \in \{1, 2\}$. Then, $[\mathbf{n}_i^{11}, \mathbf{n}_i^{12}]M = \mathbf{e}_i$

and $[\mathbf{n}_i^{21}, \mathbf{n}_i^{22}]M = \mathbf{e}_{k+i}$ for $i = 1, 2, \dots, k$. Consider $a^{\mathbf{n}_i^{11}} b^{\mathbf{n}_i^{12}}$, then we have that

$$(a^{\mathbf{n}_i^{11}} b^{\mathbf{n}_i^{12}})\varphi = a_i c^{\gamma_{1i}},$$

where

$$\begin{aligned} \gamma_{1i} = & \sum_{j=1}^k \frac{n_{ij}^{11}(n_{ij}^{11} - 1)}{2} \mathbf{m}_j^{11} (\mathbf{m}_j^{12})^T + \sum_{j=1}^k \frac{n_{ij}^{12}(n_{ij}^{12} - 1)}{2} \mathbf{m}_j^{21} (\mathbf{m}_j^{22})^T \\ & + \sum_{j=1}^{k-1} \sum_{l=j+1}^k n_{ij}^{11} \mathbf{m}_j^{12} (n_{il}^{11} \mathbf{m}_l^{11})^T + \sum_{j=1}^{k-1} \sum_{l=j+1}^k n_{ij}^{12} \mathbf{m}_j^{22} (n_{il}^{12} \mathbf{m}_l^{21})^T \\ & + \left(\sum_{j=1}^k n_{ij}^{11} \mathbf{m}_j^{12} \right) \cdot \left(\sum_{j=1}^k n_{ij}^{12} \mathbf{m}_j^{21} \right)^T \\ & + \sum_{j=1}^k n_{ij}^{11} p_j^{(1)} + \sum_{j=1}^k n_{ij}^{12} p_j^{(2)}. \end{aligned}$$

We can see that $(a^{\mathbf{n}_i^{11}} b^{\mathbf{n}_i^{12}} c^{-\mu(M)\gamma_{1i}})\varphi = a_i$.

Analogously,

$$(a^{\mathbf{n}_i^{21}} b^{\mathbf{n}_i^{22}})\varphi = b_i c^{\gamma_{2i}},$$

where

$$\begin{aligned} \gamma_{2i} = & \sum_{j=1}^k \frac{n_{ij}^{21}(n_{ij}^{21} - 1)}{2} \mathbf{m}_j^{11} (\mathbf{m}_j^{12})^T + \sum_{j=1}^k \frac{n_{ij}^{22}(n_{ij}^{22} - 1)}{2} \mathbf{m}_j^{21} (\mathbf{m}_j^{22})^T \\ & + \sum_{j=1}^{k-1} \sum_{l=j+1}^k n_{ij}^{21} \mathbf{m}_j^{12} (n_{il}^{21} \mathbf{m}_l^{11})^T + \sum_{j=1}^{k-1} \sum_{l=j+1}^k n_{ij}^{22} \mathbf{m}_j^{22} (n_{il}^{22} \mathbf{m}_l^{21})^T \end{aligned}$$

$$\begin{aligned}
& + \left(\sum_{j=1}^k n_{ij}^{21} \mathbf{m}_j^{12} \right) \cdot \left(\sum_{j=1}^k n_{ij}^{22} \mathbf{m}_j^{21} \right)^T \\
& + \sum_{j=1}^k n_{ij}^{21} p_j^{(1)} + \sum_{j=1}^k n_{ij}^{22} p_j^{(2)}.
\end{aligned}$$

We can see that $(a^{\mathbf{n}_i^{21}} b^{\mathbf{n}_i^{22}} c^{-\mu(M)\gamma_{2i}})\varphi = b_i$.

And we clearly have that $(c^{\mu(M)})\varphi = c$.

Therefore,

$$\begin{aligned}
\varphi^{-1} : H_{k+2} &\rightarrow H_{k+2} \\
a_1 &\mapsto a^{\mathbf{n}_1^{11}} b^{\mathbf{n}_1^{12}} c^{-\mu(M)\gamma_{11}} \\
a_2 &\mapsto a^{\mathbf{n}_2^{11}} b^{\mathbf{n}_2^{12}} c^{-\mu(M)\gamma_{12}} \\
&\vdots \\
a_k &\mapsto a^{\mathbf{n}_k^{11}} b^{\mathbf{n}_k^{12}} c^{-\mu(M)\gamma_{1k}} \\
b_1 &\mapsto a^{\mathbf{n}_1^{21}} b^{\mathbf{n}_1^{22}} c^{-\mu(M)\gamma_{21}} \\
b_2 &\mapsto a^{\mathbf{n}_2^{21}} b^{\mathbf{n}_2^{22}} c^{-\mu(M)\gamma_{22}} \\
&\vdots \\
b_k &\mapsto a^{\mathbf{n}_k^{21}} b^{\mathbf{n}_k^{22}} c^{-\mu(M)\gamma_{2k}} \\
c &\mapsto c^{\mu(M)}.
\end{aligned}$$

Theorem 3.9. Let $\varphi \in \text{Aut}(H_{k+2})$, then

$$\begin{aligned}
\varphi : H_{k+2} &\rightarrow H_{k+2} \\
a_1 &\mapsto a^{\mathbf{m}_1^{11}} b^{\mathbf{m}_1^{12}} c^{p_1^{(1)}} \\
a_2 &\mapsto a^{\mathbf{m}_2^{11}} b^{\mathbf{m}_2^{12}} c^{p_2^{(1)}} \\
&\vdots \\
a_k &\mapsto a^{\mathbf{m}_k^{11}} b^{\mathbf{m}_k^{12}} c^{p_k^{(1)}} \\
b_1 &\mapsto a^{\mathbf{m}_1^{21}} b^{\mathbf{m}_1^{22}} c^{p_1^{(2)}} \\
b_2 &\mapsto a^{\mathbf{m}_2^{21}} b^{\mathbf{m}_2^{22}} c^{p_2^{(2)}} \\
&\vdots \\
b_k &\mapsto a^{\mathbf{m}_k^{21}} b^{\mathbf{m}_k^{22}} c^{p_k^{(2)}} \\
c &\mapsto c^{\mu(M)},
\end{aligned}$$

with $M = \begin{bmatrix} M^{11} & M^{12} \\ M^{21} & M^{22} \end{bmatrix} \in GSp_{2k}(\mathbb{Z}) = \{B \in GL_{2k}(\mathbb{Z}) \mid BJB^T = \mu(B)J \text{ with } \mu(B) \in \{-1, 1\}\}$, where

$$M^{\bullet\blacktriangle} = \begin{bmatrix} \mathbf{m}_1^{\bullet\blacktriangle} \\ \mathbf{m}_2^{\bullet\blacktriangle} \\ \vdots \\ \mathbf{m}_k^{\bullet\blacktriangle} \end{bmatrix} \in \mathcal{M}_k(\mathbb{Z}) \text{ for } \bullet, \blacktriangle \in \{1, 2\} \text{ and } J = \begin{bmatrix} O & I_k \\ -I_k & O \end{bmatrix}.$$

Reciprocally, given $M \in GSp_{2k}(\mathbb{Z})$ and $\mathbf{p} = [\mathbf{p}^{(1)}, \mathbf{p}^{(2)}] \in \mathbb{Z}^{2k}$, we can define an automorphism of H_{k+2} with the earlier form.

From now on, we will denote $\varphi_{M,\mathbf{p}}$ the automorphism with associated matrix $M \in GSp_{2k}(\mathbb{Z})$ and associated vector $\mathbf{p} \in \mathbb{Z}^{2k}$.

3.4 Structure of $Aut(H_{k+2})$

We compute how the composition of automorphisms works. Let $\varphi_{M,\mathbf{p}}, \varphi_{N,\mathbf{q}} \in Aut(H_{k+2})$, then

$$\begin{aligned} \varphi_{M,\mathbf{p}} : H_{k+2} &\rightarrow H_{k+2} \\ a_1 &\mapsto a^{\mathbf{m}_1^{11}} b^{\mathbf{m}_1^{12}} c^{\rho_1^{(1)}} \\ a_2 &\mapsto a^{\mathbf{m}_2^{11}} b^{\mathbf{m}_2^{12}} c^{\rho_2^{(1)}} \\ &\vdots \\ a_k &\mapsto a^{\mathbf{m}_k^{11}} b^{\mathbf{m}_k^{12}} c^{\rho_k^{(1)}} \\ b_1 &\mapsto a^{\mathbf{m}_1^{21}} b^{\mathbf{m}_1^{22}} c^{\rho_1^{(2)}} \\ b_2 &\mapsto a^{\mathbf{m}_2^{21}} b^{\mathbf{m}_2^{22}} c^{\rho_2^{(2)}} \\ &\vdots \\ b_k &\mapsto a^{\mathbf{m}_k^{21}} b^{\mathbf{m}_k^{22}} c^{\rho_k^{(2)}} \\ c &\mapsto c^{\mu(M)}, \end{aligned}$$

$$\begin{aligned} \varphi_{N,\mathbf{q}} : H_{k+2} &\rightarrow H_{k+2} \\ a_1 &\mapsto a^{\mathbf{n}_1^{11}} b^{\mathbf{n}_1^{12}} c^{\rho_1^{(1)}} \\ a_2 &\mapsto a^{\mathbf{n}_2^{11}} b^{\mathbf{n}_2^{12}} c^{\rho_2^{(1)}} \\ &\vdots \\ a_k &\mapsto a^{\mathbf{n}_k^{11}} b^{\mathbf{n}_k^{12}} c^{\rho_k^{(1)}} \\ b_1 &\mapsto a^{\mathbf{n}_1^{21}} b^{\mathbf{n}_1^{22}} c^{\rho_1^{(2)}} \\ b_2 &\mapsto a^{\mathbf{n}_2^{21}} b^{\mathbf{n}_2^{22}} c^{\rho_2^{(2)}} \\ &\vdots \end{aligned}$$

$$b_k \mapsto a^{\mathbf{n}_k^{21}} b^{\mathbf{n}_k^{22}} c^{q_k^{(2)}}$$

$$c \mapsto c^{\mu(N)}.$$

Now, we compute $\varphi_{M,\mathbf{p}}\varphi_{N,\mathbf{q}}$:

$$\begin{aligned} (a_i)\varphi_{M,\mathbf{p}}\varphi_{N,\mathbf{q}} &= (a^{\mathbf{m}_i^{11}} b^{\mathbf{m}_i^{12}} c^{p_i^{(1)}})\varphi_{N,\mathbf{q}} \\ &= ((a_1)\varphi_{N,\mathbf{q}})^{m_{i1}^{11}} \dots ((a_k)\varphi_{N,\mathbf{q}})^{m_{ik}^{11}} ((b_1)\varphi_{N,\mathbf{q}})^{m_{i1}^{12}} \dots ((b_k)\varphi_{N,\mathbf{q}})^{m_{ik}^{12}} ((c)\varphi_{N,\mathbf{q}})^{p_i^{(1)}} \\ &= \left(a^{\mathbf{n}_1^{11}} b^{\mathbf{n}_1^{12}} c^{q_1^{(1)}}\right)^{m_{i1}^{11}} \dots \left(a^{\mathbf{n}_k^{11}} b^{\mathbf{n}_k^{12}} c^{q_k^{(1)}}\right)^{m_{ik}^{11}} \left(a^{\mathbf{n}_1^{21}} b^{\mathbf{n}_1^{22}} c^{q_1^{(2)}}\right)^{m_{i1}^{12}} \dots \left(a^{\mathbf{n}_k^{21}} b^{\mathbf{n}_k^{22}} c^{q_k^{(2)}}\right)^{m_{ik}^{12}} c^{\mu(N)p_i^{(1)}} \\ &= \left(a^{m_{i1}^{11}\mathbf{n}_1^{11}} b^{m_{i1}^{11}\mathbf{n}_1^{12}} c^{\frac{m_{i1}^{11}(m_{i1}^{11}-1)}{2}\mathbf{n}_1^{11}(\mathbf{n}_1^{12})^T + m_{i1}^{11}q_1^{(1)}}\right) \dots \left(a^{m_{ik}^{11}\mathbf{n}_k^{11}} b^{m_{ik}^{11}\mathbf{n}_k^{12}} c^{\frac{m_{ik}^{11}(m_{ik}^{11}-1)}{2}\mathbf{n}_k^{11}(\mathbf{n}_k^{12})^T + m_{ik}^{11}q_k^{(1)}}\right) \\ &\quad \left(a^{m_{i1}^{12}\mathbf{n}_1^{21}} b^{m_{i1}^{12}\mathbf{n}_1^{22}} c^{\frac{m_{i1}^{12}(m_{i1}^{12}-1)}{2}\mathbf{n}_1^{21}(\mathbf{n}_1^{22})^T + m_{i1}^{12}q_1^{(2)}}\right) \dots \left(a^{m_{ik}^{12}\mathbf{n}_k^{21}} b^{m_{ik}^{12}\mathbf{n}_k^{22}} c^{\frac{m_{ik}^{12}(m_{ik}^{12}-1)}{2}\mathbf{n}_k^{21}(\mathbf{n}_k^{22})^T + m_{ik}^{12}q_k^{(2)}}\right) c^{\mu(N)p_i^{(1)}} \\ &= a^{\sum_{j=1}^k m_{ij}^{11}\mathbf{n}_j^{11} + \sum_{j=1}^k m_{ij}^{12}\mathbf{n}_j^{21}} b^{\sum_{j=1}^k m_{ij}^{11}\mathbf{n}_j^{12} + \sum_{j=1}^k m_{ij}^{12}\mathbf{n}_j^{22}} c^{\mu(N)p_i^{(1)} + \gamma_{1i}}, \end{aligned}$$

where

$$\begin{aligned} \gamma_{1i} &= \sum_{j=1}^k \frac{m_{ij}^{11}(m_{ij}^{11}-1)}{2} \mathbf{n}_j^{11} (\mathbf{n}_j^{12})^T + \sum_{j=1}^k \frac{m_{ij}^{12}(m_{ij}^{12}-1)}{2} \mathbf{n}_j^{21} (\mathbf{n}_j^{22})^T \\ &\quad + \sum_{j=1}^{k-1} \sum_{l=j+1}^k m_{ij}^{11}\mathbf{n}_j^{12} (m_{il}^{11}\mathbf{n}_l^{11})^T + \sum_{j=1}^{k-1} \sum_{l=j+1}^k m_{ij}^{12}\mathbf{n}_j^{22} (m_{il}^{12}\mathbf{n}_l^{21})^T \\ &\quad + \left(\sum_{j=1}^k m_{ij}^{11}\mathbf{n}_j^{12}\right) \cdot \left(\sum_{j=1}^k m_{ij}^{12}\mathbf{n}_j^{21}\right)^T \\ &\quad + \sum_{j=1}^k m_{ij}^{11}q_j^{(1)} + \sum_{j=1}^k m_{ij}^{12}q_j^{(2)}. \end{aligned}$$

$$\begin{aligned} (b_i)\varphi_{M,\mathbf{p}}\varphi_{N,\mathbf{q}} &= (a^{\mathbf{m}_i^{21}} b^{\mathbf{m}_i^{22}} c^{p_i^{(2)}})\varphi_{N,\mathbf{q}} \\ &= ((a_1)\varphi_{N,\mathbf{q}})^{m_{i1}^{21}} \dots ((a_k)\varphi_{N,\mathbf{q}})^{m_{ik}^{21}} ((b_1)\varphi_{N,\mathbf{q}})^{m_{i1}^{22}} \dots ((b_k)\varphi_{N,\mathbf{q}})^{m_{ik}^{22}} ((c)\varphi_{N,\mathbf{q}})^{p_i^{(2)}} \\ &= \left(a^{\mathbf{n}_1^{11}} b^{\mathbf{n}_1^{12}} c^{q_1^{(1)}}\right)^{m_{i1}^{21}} \dots \left(a^{\mathbf{n}_k^{11}} b^{\mathbf{n}_k^{12}} c^{q_k^{(1)}}\right)^{m_{ik}^{21}} \left(a^{\mathbf{n}_1^{21}} b^{\mathbf{n}_1^{22}} c^{q_1^{(2)}}\right)^{m_{i1}^{22}} \dots \left(a^{\mathbf{n}_k^{21}} b^{\mathbf{n}_k^{22}} c^{q_k^{(2)}}\right)^{m_{ik}^{22}} c^{\mu(N)p_i^{(2)}} \\ &= \left(a^{m_{i1}^{21}\mathbf{n}_1^{11}} b^{m_{i1}^{21}\mathbf{n}_1^{12}} c^{\frac{m_{i1}^{21}(m_{i1}^{21}-1)}{2}\mathbf{n}_1^{11}(\mathbf{n}_1^{12})^T + m_{i1}^{21}q_1^{(1)}}\right) \dots \left(a^{m_{ik}^{21}\mathbf{n}_k^{11}} b^{m_{ik}^{21}\mathbf{n}_k^{12}} c^{\frac{m_{ik}^{21}(m_{ik}^{21}-1)}{2}\mathbf{n}_k^{11}(\mathbf{n}_k^{12})^T + m_{ik}^{21}q_k^{(1)}}\right) \\ &\quad \left(a^{m_{i1}^{22}\mathbf{n}_1^{21}} b^{m_{i1}^{22}\mathbf{n}_1^{22}} c^{\frac{m_{i1}^{22}(m_{i1}^{22}-1)}{2}\mathbf{n}_1^{21}(\mathbf{n}_1^{22})^T + m_{i1}^{22}q_1^{(2)}}\right) \dots \left(a^{m_{ik}^{22}\mathbf{n}_k^{21}} b^{m_{ik}^{22}\mathbf{n}_k^{22}} c^{\frac{m_{ik}^{22}(m_{ik}^{22}-1)}{2}\mathbf{n}_k^{21}(\mathbf{n}_k^{22})^T + m_{ik}^{22}q_k^{(2)}}\right) c^{\mu(N)p_i^{(2)}} \\ &= a^{\sum_{j=1}^k m_{ij}^{21}\mathbf{n}_j^{11} + \sum_{j=1}^k m_{ij}^{22}\mathbf{n}_j^{21}} b^{\sum_{j=1}^k m_{ij}^{21}\mathbf{n}_j^{12} + \sum_{j=1}^k m_{ij}^{22}\mathbf{n}_j^{22}} c^{\mu(N)p_i^{(2)} + \gamma_{2i}}, \end{aligned}$$

where

$$\begin{aligned}
\gamma_{2i} = & \sum_{j=1}^k \frac{m_{ij}^{21}(m_{ij}^{21} - 1)}{2} \mathbf{n}_j^{11} (\mathbf{n}_j^{12})^T + \sum_{j=1}^k \frac{m_{ij}^{22}(m_{ij}^{22} - 1)}{2} \mathbf{n}_j^{21} (\mathbf{n}_j^{22})^T \\
& + \sum_{j=1}^{k-1} \sum_{l=j+1}^k m_{ij}^{21} \mathbf{n}_j^{12} (m_{il}^{21} \mathbf{n}_l^{11})^T + \sum_{j=1}^{k-1} \sum_{l=j+1}^k m_{ij}^{22} \mathbf{n}_j^{22} (m_{il}^{22} \mathbf{n}_l^{21})^T \\
& + \left(\sum_{j=1}^k m_{ij}^{21} \mathbf{n}_j^{12} \right) \cdot \left(\sum_{j=1}^k m_{ij}^{22} \mathbf{n}_j^{21} \right)^T \\
& + \sum_{j=1}^k m_{ij}^{21} q_j^{(1)} + \sum_{j=1}^k m_{ij}^{22} q_j^{(2)}.
\end{aligned}$$

$$(c)\varphi_{M,\mathbf{p}}\varphi_{N,\mathbf{q}} = ((c)\varphi_{N,\mathbf{q}})^{\mu(M)} = c^{\mu(M)\mu(N)}.$$

We can see that the matrix associated to $\varphi_{M,\mathbf{p}}\varphi_{N,\mathbf{q}}$ is MN , so we can define an epimorphism:

$$\begin{aligned}
\beta : \text{Aut}(H_{k+2}) &\rightarrow \text{GSp}_{2k}(\mathbb{Z}) \\
\varphi_{M,\mathbf{p}} &\mapsto \mu(M)M.
\end{aligned}$$

In fact, we have the following short exact sequence:

$$1 \rightarrow \mathbb{Z}^{2k} \xrightarrow{\alpha} \text{Aut}(H_{k+2}) \xrightarrow{\beta} \text{GSp}_{2k}(\mathbb{Z}) \rightarrow 1,$$

where $\mathbf{p}\alpha = \varphi_{I,\mathbf{p}}$ and $\varphi_{M,\mathbf{p}}\beta = \mu(M)M$.

In an attempt to generalize the result in Section 2.4, we have done the computations to determine whether this short exact sequence splits.

In order to do this, we have found in the literature (see [3] for $\text{Sp}_4(\mathbb{Z})$ and [15] for $\text{Sp}_{2k}(\mathbb{Z})$ with $k \geq 3$) the presentation of $\text{Sp}_{2k}(\mathbb{Z})$.

To compute a presentation of $\text{GSp}_{2k}(\mathbb{Z})$, once we have the presentation of $\text{Sp}_{2k}(\mathbb{Z})$, we can add as generator the antisymplectic matrix $H = \begin{bmatrix} -I_k & O \\ O & I_k \end{bmatrix}$, which has order 2 and compute the result of conjugating every other generator by H , adding this as relation as well as $H^2 = I_{2k}$. Like this, we have a presentation of $\text{GSp}_{2k}(\mathbb{Z})$. To illustrate this, we add Appendix B as an example of this process for $k = 2$.

After computing a presentation of $\text{GSp}_{2k}(\mathbb{Z})$, the idea is to map the generators $E_{ij} \in \text{GSp}_{2k}(\mathbb{Z})$ to $\varphi_{E_{ij},\mathbf{x}}(E_{ij})$, where $\mathbf{x}(E_{ij})$ is a $2k$ -dimensional vector of unknowns. This map must be a homomorphism for the short exact sequence to split, so imposing that the relations are kept by the map, we get a set of linear equations on the unknowns.

After computing all this (using a computer) and solving the linear equations, we got a compatible undetermined system where some of the unknowns had to be rational numbers with 2 on the denominator. So, the short exact sequence should not split if these computations are correct.

We have omitted all the details of these computations or the script in this thesis, since it was a negative result that was not aligned either to the main objective of this Master Thesis, which is to solve the CP for certain extensions of Heisenberg group.

3.5 Conjugacy Problem and Twisted Conjugacy Problem

Before studying the twisted conjugacy problem, we solve the conjugacy problem in H_{k+2} .

Given $a^r b^s c^t, a^u b^v c^w \in H_{k+2}$, we want to see if there exists $a^x b^y c^z \in H_3$ such that $a^r b^s c^t = (a^x b^y c^z)^{-1} a^u b^v c^w a^x b^y c^z$. Developing, we get the following:

$$\begin{aligned} a^r b^s c^t &= (a^x b^y c^z)^{-1} a^u b^v c^w a^x b^y c^z \\ &= a^{-x} b^{-y} c^{xy^T - z} a^{u+x} b^{v+y} c^{z+w+vx^T} \\ &= a^u b^v c^{w+vx^T - uy^T}. \end{aligned}$$

Therefore, $a^r b^s c^t \sim a^u b^v c^w$, if and only if, $\mathbf{r} = \mathbf{u}$, $\mathbf{s} = \mathbf{v}$ and there exist $\mathbf{x}, \mathbf{y} \in \mathbb{Z}^k$ such that $t = w + \mathbf{v}\mathbf{x}^T - \mathbf{u}\mathbf{y}^T$. This is equivalent to $\mathbf{r} = \mathbf{u}$, $\mathbf{s} = \mathbf{v}$ and $t \equiv w \pmod{g}$ where $g = \gcd(r_i, s_i)_{i=1, \dots, k}$.

Now, we go to the twisted conjugacy problem:

Given $a^r b^s c^t, a^u b^v c^w \in H_{k+2}$ and $\varphi_{M, \mathbf{p}} \in \text{Aut}(H_{k+2})$,

$$\begin{aligned} \varphi : H_{k+2} &\rightarrow H_{k+2} \\ a_1 &\mapsto a^{\mathbf{m}_1^{11}} b^{\mathbf{m}_1^{12}} c^{p_1^{(1)}} \\ a_2 &\mapsto a^{\mathbf{m}_2^{11}} b^{\mathbf{m}_2^{12}} c^{p_2^{(1)}} \\ &\vdots \\ a_k &\mapsto a^{\mathbf{m}_k^{11}} b^{\mathbf{m}_k^{12}} c^{p_k^{(1)}} \\ b_1 &\mapsto a^{\mathbf{m}_1^{21}} b^{\mathbf{m}_1^{22}} c^{p_1^{(2)}} \\ b_2 &\mapsto a^{\mathbf{m}_2^{21}} b^{\mathbf{m}_2^{22}} c^{p_2^{(2)}} \\ &\vdots \\ b_k &\mapsto a^{\mathbf{m}_k^{21}} b^{\mathbf{m}_k^{22}} c^{p_k^{(2)}} \\ c &\mapsto c^{\mu(M)}, \end{aligned}$$

we want to see if $a^r b^s c^t \sim_{\varphi_{M, \mathbf{p}}} a^u b^v c^w$. That is, if there exists $a^x b^y c^z \in H_{k+2}$ such that $a^r b^s c^t = ((a^x b^y c^z)\varphi_{M, \mathbf{p}})^{-1} a^u b^v c^w a^x b^y c^z$. Developing, we get

$$\begin{aligned} a^r b^s c^t &= ((a^x b^y c^z)\varphi_{M, \mathbf{p}})^{-1} a^u b^v c^w a^x b^y c^z \\ &= (d^{[\mathbf{x}, \mathbf{y}]M} c^{\mu(M)z+\gamma})^{-1} a^{u+\mathbf{x}} b^{v+\mathbf{y}} c^{w+z+\mathbf{v}\mathbf{x}^T} \\ &= (a^{-\hat{\mathbf{x}}} b^{-\hat{\mathbf{y}}} c^{-\mu(M)z-\gamma+\hat{\mathbf{x}}\hat{\mathbf{y}}^T}) a^{u+\mathbf{x}} b^{v+\mathbf{y}} c^{w+z+\mathbf{v}\mathbf{x}^T} \\ &= d^{[\mathbf{u}, \mathbf{v}]+[\mathbf{x}, \mathbf{y}](I-M)} c^{w+(1-\mu(M))z-\gamma+(\hat{\mathbf{x}}-\mathbf{x}-\mathbf{u})\hat{\mathbf{y}}^T+\mathbf{v}\mathbf{x}^T}, \end{aligned}$$

where

$$\begin{aligned} \hat{\mathbf{x}} &= ([\mathbf{x}, \mathbf{y}]M) [1..k] = \mathbf{x}M^{11} + \mathbf{y}M^{21}, \\ \hat{\mathbf{y}} &= ([\mathbf{x}, \mathbf{y}]M) [k+1..2k] = \mathbf{x}M^{12} + \mathbf{y}M^{22}, \end{aligned}$$

$$\begin{aligned}
\gamma = & \sum_{i=1}^k \frac{x_i(x_i - 1)}{2} \mathbf{m}_i^{11} (\mathbf{m}_i^{12})^T + \sum_{i=1}^k \frac{y_i(y_i - 1)}{2} \mathbf{m}_i^{21} (\mathbf{m}_i^{22})^T \\
& + \sum_{i=1}^{k-1} \sum_{j=i+1}^k x_i \mathbf{m}_i^{12} (x_j \mathbf{m}_j^{11})^T + \sum_{i=1}^{k-1} \sum_{j=i+1}^k y_i \mathbf{m}_i^{22} (y_j \mathbf{m}_j^{21})^T \\
& + \left(\sum_{i=1}^k x_i \mathbf{m}_i^{12} \right) \cdot \left(\sum_{i=1}^k y_i \mathbf{m}_i^{21} \right)^T \\
& + \sum_{i=1}^k x_i p_i^{(1)} + \sum_{i=1}^k y_i p_i^{(2)}.
\end{aligned}$$

After making the substitutions of $\hat{\mathbf{x}}, \hat{\mathbf{y}}$, we get that the exponent of c is

$$\begin{aligned}
C = & w + (1 - \mu(M))z - \gamma + (\hat{\mathbf{x}} - \mathbf{x} - \mathbf{u})\hat{\mathbf{y}}^T + \mathbf{v}\mathbf{x}^T \\
= & w + (1 - \mu(M))z - \gamma + (\mathbf{x}(M^{11} - I) + \mathbf{y}M^{21} - \mathbf{u})(\mathbf{x}M^{12} + \mathbf{y}M^{22})^T + \mathbf{v}\mathbf{x}^T \\
= & w + (1 - \mu(M))z - \gamma + \mathbf{x}(M^{11} - I)(M^{12})^T \mathbf{x}^T + \mathbf{x}(M^{11} - I)(M^{22})^T \mathbf{y}^T \\
& + \mathbf{y}M^{21}(M^{12})^T \mathbf{x}^T + \mathbf{y}M^{21}(M^{22})^T \mathbf{y}^T - \mathbf{u}(M^{12})^T \mathbf{x}^T - \mathbf{u}(M^{22})^T \mathbf{y}^T + \mathbf{v}\mathbf{x}^T \\
= & w + (1 - \mu(M))z - \gamma + \mathbf{x}M^{11}(M^{12})^T \mathbf{x}^T - \mathbf{x}(M^{12})^T \mathbf{x}^T + \mathbf{x}M^{11}(M^{22})^T \mathbf{y}^T - \mathbf{x}(M^{22})^T \mathbf{y}^T \\
& + \mathbf{x}M^{12}(M^{21})^T \mathbf{y}^T + \mathbf{y}M^{21}(M^{22})^T \mathbf{y}^T - \mathbf{u}(M^{12})^T \mathbf{x}^T - \mathbf{u}(M^{22})^T \mathbf{y}^T + \mathbf{v}\mathbf{x}^T.
\end{aligned}$$

An algorithm deciding whether two elements are twisted conjugated must first solve the linear system $[\mathbf{x}, \mathbf{y}](I - M) = [\mathbf{r} - \mathbf{u}, \mathbf{s} - \mathbf{v}]$. We distinguish the following cases:

- **Incompatible System:** The system has no solution. Therefore, the algorithm must answer no.
- **Compatible Determined System:** The system has a unique solution. We have two subcases:
 - The system has a solution over the integers. We substitute the values of $\mathbf{x}, \mathbf{y}$ in the equation $C = t$.
 - * If $\mu(M) = 1$, the value of z doesn't matter, we just check if $C = t$ is verified. If it is verified, the algorithm must answer yes (Our possible conjugator is $a^x b^y$). Otherwise, the algorithm must answer no.
 - * If $\mu(M) = -1$, we must leave $2z$ on one side of the equality and check if the other side of the equality is even. If it is even, dividing by 2, we get the value of z , and the algorithm must answer yes (Our possible conjugator is $a^x b^y c^z$). Otherwise, it must answer no.
 - The system has no solution over the integers (The solution is rational). The algorithm must answer no.
- **Compatible Undetermined System:** The system has an infinite number of solutions.

Let h be the freedom degree of the system. Then, we can write $\mathbf{x}, \mathbf{y}$ in terms of $\lambda_1, \dots, \lambda_h$, where λ_i are free parameters over the integers. We substitute the values of $\mathbf{x}, \mathbf{y}$ in $C = t$. We distinguish two cases:

- If $\mu(M) = 1$, then the value of z doesn't matter. The equation $C = t$ reduces to a quadratic equation of the form

$$\sum_{i,j=1}^h \alpha_{ij} \lambda_i \lambda_j + \sum \beta_j \lambda_j = \hat{\gamma}$$

where the $\alpha_{ij}, \beta_j, \hat{\gamma}$ are integers, or at worst, some of them are rational numbers with denominator 2.

By reference [14], there exists an algorithm determining whether this type of equation has a solution over the integers.

After applying this algorithm, if the equation has a solution over the integers, we answer yes, we substitute the values of λ_i obtained in $\mathbf{x}$ and $\mathbf{y}$ and obtain $a^x b^y$ as a possible conjugator.

If the equation has no solution over the integers for λ_i , our algorithm must answer no.

- If $\mu(M) = -1$, then what we can do is to leave $2z$ on one side of the equality, and the quadratic equation on λ_i on the other side. After multiplying by 2 if there are any denominators on the coefficients of the quadratic equation on λ_i , we can reduce the equation modulo 2 or 4, and check for $\lambda_i \in \{0, 1\}$ ($\{0, 1, 2, 3\}$ if we have reduced the equation modulo 4) if the equation has a solution modulo 2 (or 4). After checking a finite number of possibilities, the algorithm will determine if this equation has a solution modulo 2 (or 4). If it has no solution, the algorithm must answer no. If it has a solution, the algorithm must answer yes. In order to give a possible conjugator, it must substitute the value of λ_i on $\mathbf{x}$ and $\mathbf{y}$, and also on $C = t$ and solve the equation for z . Then, our possible conjugator would be $a^x b^y c^z$.

As a result of this section, we obtain the following theorem:

Theorem 3.10. *The Twisted Conjugacy Problem is solvable in H_{k+2} for all $k \geq 1$.* □

3.6 Orbit decidability

In this section, we will study the orbit decidability of the full automorphism group of the higher dimensional Heisenberg group. In the general case of $k + 2$ dimensions, not every finitely generated subgroup of automorphisms containing the inner ones will be orbit decidable. However, we will be able to connect the orbit decidability of a finitely generated subgroup of automorphisms (containing the inner ones) with the orbit decidability of the finitely generated matrices subgroup formed by the matrices associated to these automorphisms.

3.6.1 OD(Aut(H_{k+2}))

We start with the full automorphism group, which is orbit decidable.

We will use the following transitivity property of $Sp_{2k}(\mathbb{Z})$ over the unimodular vectors:

Theorem 3.11 (Sierra–Wahl, Proposition 2.25(ii) adapted, [22]). *The group $Sp_{2k}(\mathbb{Z})$ acts transitively on the set of unimodular vectors of $\mathbb{Z}^{2k}$, that is, given two vectors $\mathbf{u}, \mathbf{v} \in \mathbb{Z}^{2k}$ such that $\gcd(u_i)_{i=1, \dots, 2k} = \gcd(v_i)_{i=1, \dots, 2k} = 1$, then there exists $M \in Sp_{2k}(\mathbb{Z})$ such that $\mathbf{u}M = \mathbf{v}$.*

Notice that the statement of this Theorem automatically implies that $Sp_{2k}(\mathbb{Z}) \leq GL_{2k}(\mathbb{Z}) = Aut(\mathbb{Z}^{2k})$ is orbit decidable. In fact, given $\mathbf{u}, \mathbf{v} \in \mathbb{Z}^{2k}$, there exists $M \in Sp_{2k}(\mathbb{Z})$ such that $\mathbf{u}M = \mathbf{v}$, if and only if,

$\gcd(u_i)_{i=1,\dots,2k} = \gcd(v_i)_{i=1,\dots,2k}$. The sufficiency comes from Theorem 3.11: if $g = \gcd(u_i)_{i=1,\dots,2k} = \gcd(v_i)_{i=1,\dots,2k}$, then dividing $\mathbf{u}, \mathbf{v}$ by g , we get unimodular vectors which are on the same orbit, and therefore, the original $\mathbf{u}, \mathbf{v}$ are also on the same orbit. The necessity is clear, since the existence of an integer invertible matrix M sending $\mathbf{u}$ to $\mathbf{v}$ implies that the elements of both vectors must have the same gcd.

Given $a^{\mathbf{u}}b^{\mathbf{v}}c^w, a^{\mathbf{r}}b^{\mathbf{s}}c^t \in H_{k+2}$, we want to decide whether there exists $\varphi_{M,\mathbf{p}} \in \text{Aut}(H_{k+2})$ such that $a^{\mathbf{u}}b^{\mathbf{v}}c^w = (a^{\mathbf{r}}b^{\mathbf{s}}c^t)\varphi_{M,\mathbf{p}}$. After making computations, we get

$$a^{\mathbf{u}}b^{\mathbf{v}}c^w = (a^{\mathbf{r}}b^{\mathbf{s}}c^t)\varphi_{M,\mathbf{p}} = d^{[\mathbf{r},\mathbf{s}]M} c^{\mu(M)t+\gamma}, \quad (19)$$

where

$$\begin{aligned} \gamma = & \sum_{i=1}^k \frac{r_i(r_i-1)}{2} \mathbf{m}_i^{11} (\mathbf{m}_i^{12})^T + \sum_{i=1}^k \frac{s_i(s_i-1)}{2} \mathbf{m}_i^{21} (\mathbf{m}_i^{22})^T \\ & + \sum_{i=1}^{k-1} \sum_{j=i+1}^k r_i \mathbf{m}_i^{12} (r_j \mathbf{m}_j^{11})^T + \sum_{i=1}^{k-1} \sum_{j=i+1}^k s_i \mathbf{m}_i^{22} (s_j \mathbf{m}_j^{21})^T \\ & + \left(\sum_{i=1}^k r_i \mathbf{m}_i^{12} \right) \cdot \left(\sum_{i=1}^k s_i \mathbf{m}_i^{21} \right)^T \\ & + \sum_{i=1}^k r_i p_i^{(1)} + \sum_{i=1}^k s_i p_i^{(2)}. \end{aligned}$$

For (19) to be verified, we need first of all that $[\mathbf{u}, \mathbf{v}] = [\mathbf{r}, \mathbf{s}]M$. By Theorem 3.11, this is verified if and only if $\gcd(u_i, v_i)_{i=1,\dots,k} = \gcd(r_i, s_i)_{i=1,\dots,k}$.

Our decision algorithm would start computing $\gcd(u_i, v_i)_{i=1,\dots,k}$ and $\gcd(r_i, s_i)_{i=1,\dots,k}$. If they are different, there cannot exist $\varphi_{M,\mathbf{p}} \in \text{Aut}(H_{k+2})$ such that $a^{\mathbf{u}}b^{\mathbf{v}}c^w = (a^{\mathbf{r}}b^{\mathbf{s}}c^t)\varphi_{M,\mathbf{p}}$ since there cannot exist $M \in \text{GSp}_{2k}(\mathbb{Z})$ sending $[\mathbf{r}, \mathbf{s}]$ to $[\mathbf{u}, \mathbf{v}]$. The answer should then be no.

If $g = \gcd(u_i, v_i)_{i=1,\dots,k} = \gcd(r_i, s_i)_{i=1,\dots,k}$, we know the existence of $M \in \text{Sp}_{2k}(\mathbb{Z})$ such that $[\mathbf{u}, \mathbf{v}] = [\mathbf{r}, \mathbf{s}]M$ and we can compute such an M . In general, it is not unique.

Now, we look at the exponent of c . We haven't made yet any imposition on the vector $\mathbf{p}$ associated to our possible automorphism. From the expression of γ , we see that the last two addends can be equal to any multiple of g by choosing $\mathbf{p}$ appropriately.

We distinguish two cases:

- $2 \nmid g$. In this case, we notice that all the other terms in the expression of γ are divisible by g . If $w \equiv t \pmod{g}$, then we can choose the vector $\mathbf{p}$ such that the exponents of c coincide. We answer yes.

If $w \equiv -t \pmod{g}$, we can also do this, changing our M by HN where $H = \begin{bmatrix} -I_k & O \\ O & I_k \end{bmatrix}$ and N is a symplectic matrix such that $[\mathbf{u}, \mathbf{v}] = [-\mathbf{r}, \mathbf{s}]N$. Then, M will be antisymplectic ($\mu(M) = -1$) and the exponent of c in (19) will be $-t + \gamma$. We answer yes.

If none of this congruences is verified, we can conclude that there is no automorphism verifying (19). We answer no.

- $2 \mid g$. In this case, we have to work a little more, since the first two summands of γ are not necessarily multiples of g (but only of $\frac{g}{2}$). Choosing an adequate value for the vector $\mathbf{p}$, we can make the exponents of c in (19) coincide, if and only if,

$$w \equiv \mu(M)t - \frac{g}{2} \sum_{i=1}^k \left(\frac{r_i}{g} \mathbf{m}_i^{11} (\mathbf{m}_i^{12})^T + \frac{s_i}{g} \mathbf{m}_i^{21} (\mathbf{m}_i^{22})^T \right) \pmod{g}. \quad (20)$$

By Lemma 3.12, regardless of the choice of M provided that $[\mathbf{r}, \mathbf{s}]M = [\mathbf{u}, \mathbf{v}]$, the second part of the right hand-side term of (20) doesn't change modulo g . Therefore, we can compute it for a particular M symplectic and check whether

$$w \equiv t - \frac{g}{2} \sum_{i=1}^k \left(\frac{r_i}{g} \mathbf{m}_i^{11} (\mathbf{m}_i^{12})^T + \frac{s_i}{g} \mathbf{m}_i^{21} (\mathbf{m}_i^{22})^T \right) \pmod{g}$$

If this is the case, the algorithm must answer yes. Otherwise, check whether

$$w \equiv -t - \frac{g}{2} \sum_{i=1}^k \left(\frac{r_i}{g} \mathbf{m}_i^{11} (\mathbf{m}_i^{12})^T + \frac{s_i}{g} \mathbf{m}_i^{21} (\mathbf{m}_i^{22})^T \right) \pmod{g}.$$

In the affirmative case, answer yes, using a similar argument as in the case $2 \nmid g$, changing M by HN as described there; otherwise, answer no.

To finish the proof, let us see the already used result:

Lemma 3.12. *In the case $2 \mid g$, if M, N are both matrices such that $[\mathbf{r}, \mathbf{s}]M = [\mathbf{r}, \mathbf{s}]N = [\mathbf{u}, \mathbf{v}]$, then*

$$\frac{g}{2} \sum_{i=1}^k \left(\frac{r_i}{g} \mathbf{m}_i^{11} (\mathbf{m}_i^{12})^T + \frac{s_i}{g} \mathbf{m}_i^{21} (\mathbf{m}_i^{22})^T \right) \equiv \frac{g}{2} \sum_{i=1}^k \left(\frac{r_i}{g} \mathbf{n}_i^{11} (\mathbf{n}_i^{12})^T + \frac{s_i}{g} \mathbf{n}_i^{21} (\mathbf{n}_i^{22})^T \right) \pmod{g}. \quad (21)$$

Proof. To see this, notice that if $[\mathbf{r}, \mathbf{s}]M = [\mathbf{r}, \mathbf{s}]N = [\mathbf{u}, \mathbf{v}]$, then $[\mathbf{u}, \mathbf{v}]N^{-1}M = [\mathbf{u}, \mathbf{v}]$, that is, $Q = N^{-1}M \in \text{Fix}([\mathbf{u}, \mathbf{v}])$.

$$M = NQ = \begin{bmatrix} N^{11} & N^{12} \\ N^{21} & N^{22} \end{bmatrix} \begin{bmatrix} Q^{11} & Q^{12} \\ Q^{21} & Q^{22} \end{bmatrix} = \begin{bmatrix} N^{11}Q^{11} + N^{12}Q^{21} & N^{11}Q^{12} + N^{12}Q^{22} \\ N^{21}Q^{11} + N^{22}Q^{21} & N^{21}Q^{12} + N^{22}Q^{22} \end{bmatrix}.$$

We have the following equalities:

$$\mathbf{m}_i^{11} = \mathbf{n}_i^{11}Q^{11} + \mathbf{n}_i^{12}Q^{21} \quad (22)$$

$$\mathbf{m}_i^{12} = \mathbf{n}_i^{11}Q^{12} + \mathbf{n}_i^{12}Q^{22} \quad (23)$$

$$\mathbf{m}_i^{21} = \mathbf{n}_i^{21}Q^{11} + \mathbf{n}_i^{22}Q^{21} \quad (24)$$

$$\mathbf{m}_i^{22} = \mathbf{n}_i^{21}Q^{12} + \mathbf{n}_i^{22}Q^{22}. \quad (25)$$

Since Q is general symplectic, we also have the following equalities:

$$Q^{11} (Q^{12})^T = Q^{12} (Q^{11})^T \quad (26)$$

$$Q^{21} (Q^{22})^T = Q^{22} (Q^{21})^T \quad (27)$$

$$Q^{11} (Q^{22})^T - Q^{12} (Q^{21})^T = \mu(Q)I_k. \quad (28)$$

Using (22) and (23), we get

$$\begin{aligned}
\mathbf{m}_i^{11} (\mathbf{m}_i^{12})^T &= (\mathbf{n}_i^{11} Q^{11} + \mathbf{n}_i^{12} Q^{21}) (\mathbf{n}_i^{11} Q^{12} + \mathbf{n}_i^{12} Q^{22})^T = \\
&= \mathbf{n}_i^{11} Q^{11} (Q^{12})^T (\mathbf{n}_i^{11})^T + \mathbf{n}_i^{12} Q^{21} (Q^{12})^T (\mathbf{n}_i^{11})^T + \mathbf{n}_i^{11} Q^{11} (Q^{22})^T (\mathbf{n}_i^{12})^T + \mathbf{n}_i^{12} Q^{21} (Q^{22})^T (\mathbf{n}_i^{12})^T = \\
&= \mathbf{n}_i^{11} Q^{11} (Q^{12})^T (\mathbf{n}_i^{11})^T + 2\mathbf{n}_i^{12} Q^{21} (Q^{12})^T (\mathbf{n}_i^{11})^T + \mu(Q) \mathbf{n}_i^{11} (\mathbf{n}_i^{12})^T + \mathbf{n}_i^{12} Q^{21} (Q^{22})^T (\mathbf{n}_i^{12})^T,
\end{aligned} \tag{29}$$

where, in the last line, we have used (28) in the third term of the second line and we have transposed the scalar $\mathbf{n}_i^{11} Q^{12} (Q^{21})^T (\mathbf{n}_i^{12})^T$.

Similarly, using (24) and (25), we get

$$\begin{aligned}
\mathbf{m}_i^{21} (\mathbf{m}_i^{22})^T &= (\mathbf{n}_i^{21} Q^{11} + \mathbf{n}_i^{22} Q^{21}) (\mathbf{n}_i^{21} Q^{12} + \mathbf{n}_i^{22} Q^{22})^T = \\
&= \mathbf{n}_i^{21} Q^{11} (Q^{12})^T (\mathbf{n}_i^{21})^T + \mathbf{n}_i^{22} Q^{21} (Q^{12})^T (\mathbf{n}_i^{21})^T + \mathbf{n}_i^{21} Q^{11} (Q^{22})^T (\mathbf{n}_i^{22})^T + \mathbf{n}_i^{22} Q^{21} (Q^{22})^T (\mathbf{n}_i^{22})^T = \\
&= \mathbf{n}_i^{21} Q^{11} (Q^{12})^T (\mathbf{n}_i^{21})^T + 2\mathbf{n}_i^{22} Q^{21} (Q^{12})^T (\mathbf{n}_i^{21})^T + \mu(Q) \mathbf{n}_i^{21} (\mathbf{n}_i^{22})^T + \mathbf{n}_i^{22} Q^{21} (Q^{22})^T (\mathbf{n}_i^{22})^T,
\end{aligned} \tag{30}$$

where, in the last line, we have used (28) in the third term of the second line and we have transposed the scalar $\mathbf{n}_i^{21} Q^{12} (Q^{21})^T (\mathbf{n}_i^{22})^T$.

Notice that (21) is equivalent to

$$\sum_{i=1}^k \left(\frac{r_i}{g} \mathbf{m}_i^{11} (\mathbf{m}_i^{12})^T + \frac{s_i}{g} \mathbf{m}_i^{21} (\mathbf{m}_i^{22})^T \right) \equiv \sum_{i=1}^k \left(\frac{r_i}{g} \mathbf{n}_i^{11} (\mathbf{n}_i^{12})^T + \frac{s_i}{g} \mathbf{n}_i^{21} (\mathbf{n}_i^{22})^T \right) \pmod{2}. \tag{31}$$

Using (29) and (30), the left hand-side of the equality is equivalent modulo 2 to

$$\begin{aligned}
&\sum_{i=1}^k \left(\frac{r_i}{g} \mathbf{m}_i^{11} (\mathbf{m}_i^{12})^T + \frac{s_i}{g} \mathbf{m}_i^{21} (\mathbf{m}_i^{22})^T \right) \equiv_2 \\
&\sum_{i=1}^k \left(\frac{r_i}{g} \left(\mathbf{n}_i^{11} Q^{11} (Q^{12})^T (\mathbf{n}_i^{11})^T + \mathbf{n}_i^{11} (\mathbf{n}_i^{12})^T + \mathbf{n}_i^{12} Q^{21} (Q^{22})^T (\mathbf{n}_i^{12})^T \right) \right. \\
&\quad \left. + \frac{s_i}{g} \left(\mathbf{n}_i^{21} Q^{11} (Q^{12})^T (\mathbf{n}_i^{21})^T + \mathbf{n}_i^{21} (\mathbf{n}_i^{22})^T + \mathbf{n}_i^{22} Q^{21} (Q^{22})^T (\mathbf{n}_i^{22})^T \right) \right).
\end{aligned}$$

Now, for (31) to be true, we need to prove

$$\begin{aligned}
&\sum_{i=1}^k \left(\frac{r_i}{g} \left(\mathbf{n}_i^{11} Q^{11} (Q^{12})^T (\mathbf{n}_i^{11})^T + \mathbf{n}_i^{12} Q^{21} (Q^{22})^T (\mathbf{n}_i^{12})^T \right) \right. \\
&\quad \left. + \frac{s_i}{g} \left(\mathbf{n}_i^{21} Q^{11} (Q^{12})^T (\mathbf{n}_i^{21})^T + \mathbf{n}_i^{22} Q^{21} (Q^{22})^T (\mathbf{n}_i^{22})^T \right) \right) \equiv 0 \pmod{2}.
\end{aligned} \tag{32}$$

We also have the relations

$$[\mathbf{u}, \mathbf{v}] = [\mathbf{u}, \mathbf{v}] \begin{bmatrix} Q^{11} & Q^{12} \\ Q^{21} & Q^{22} \end{bmatrix} = [\mathbf{u}Q^{11} + \mathbf{v}Q^{21}, \mathbf{u}Q^{12} + \mathbf{v}Q^{22}], \tag{33}$$

$$[\mathbf{r}, \mathbf{s}] = [\mathbf{r}, \mathbf{s}] \begin{bmatrix} N^{11} & N^{12} \\ N^{21} & N^{22} \end{bmatrix} = [\mathbf{r}N^{11} + \mathbf{s}N^{21}, \mathbf{r}N^{12} + \mathbf{s}N^{22}]. \tag{34}$$

Using (26) and (27), we know that the matrices $Q^{11} (Q^{12})^T$ and $Q^{21} (Q^{22})^T$ are symmetric. This means that the terms of the sum in (32) are quadratic forms applied to the vectors $\mathbf{n}_i^{\bullet\blacktriangle}$. Given a vector $\mathbf{x} \in \mathbb{Z}^k$ and a symmetric matrix $A \in \mathcal{M}_k(\mathbb{Z})$, we have that:

$$\mathbf{x}A\mathbf{x}^T = 2 \sum_{j=1}^{k-1} \sum_{l=j+1}^k x_j a_{jl} x_l + \sum_{j=1}^k x_j^2 a_{jj}$$

In modulo 2, the term multiplied by 2 disappears and squaring 0 or 1 leaves the number unchanged, so in fact,

$$\mathbf{x}A\mathbf{x}^T \equiv_2 \sum_{j=1}^k x_j a_{jj}$$

Translating this for $A = Q^{11} (Q^{12})^T$ and $A = Q^{21} (Q^{22})^T$, the expression (32) changes modulo 2 to

$$\begin{aligned} & \sum_{i=1}^k \left(\frac{r_i}{g} \sum_{j=1}^k n_{ij}^{11} \sum_{l=1}^k q_{jl}^{11} q_{jl}^{12} + \frac{s_i}{g} \sum_{j=1}^k n_{ij}^{21} \sum_{l=1}^k q_{jl}^{11} q_{jl}^{12} \right. \\ & \quad \left. + \frac{r_i}{g} \sum_{j=1}^k n_{ij}^{12} \sum_{l=1}^k q_{jl}^{21} q_{jl}^{22} + \frac{s_i}{g} \sum_{j=1}^k n_{ij}^{22} \sum_{l=1}^k q_{jl}^{21} q_{jl}^{22} \right) \\ &= \sum_{j=1}^k \left[\left(\sum_{i=1}^k \left(\frac{r_i}{g} n_{ij}^{11} + \frac{s_i}{g} n_{ij}^{21} \right) \right) \cdot \sum_{l=1}^k q_{jl}^{11} q_{jl}^{12} \right. \\ & \quad \left. + \left(\sum_{i=1}^k \left(\frac{r_i}{g} n_{ij}^{12} + \frac{s_i}{g} n_{ij}^{22} \right) \right) \cdot \sum_{l=1}^k q_{jl}^{21} q_{jl}^{22} \right] \\ &= \sum_{j=1}^k \left(\frac{u_j}{g} \sum_{l=1}^k q_{jl}^{11} q_{jl}^{12} + \frac{v_j}{g} \sum_{l=1}^k q_{jl}^{21} q_{jl}^{22} \right), \end{aligned}$$

where the last equality comes from (34).

Now, we do the opposite, transforming the sums into quadratic forms:

$$\begin{aligned} & \sum_{j=1}^k \left(\frac{u_j}{g} \sum_{l=1}^k q_{jl}^{11} q_{jl}^{12} + \frac{v_j}{g} \sum_{l=1}^k q_{jl}^{21} q_{jl}^{22} \right) \\ & \equiv_2 \frac{\mathbf{u}}{g} Q^{11} (Q^{12})^T \left(\frac{\mathbf{u}}{g} \right)^T + \frac{\mathbf{v}}{g} Q^{21} (Q^{22})^T \left(\frac{\mathbf{v}}{g} \right)^T. \end{aligned}$$

Using (33), we can rewrite the following scalar product as follows:

$$\begin{aligned} \frac{\mathbf{u}}{g} \left(\frac{\mathbf{v}}{g} \right)^T &= \left(\frac{\mathbf{u}}{g} Q^{11} + \frac{\mathbf{v}}{g} Q^{21} \right) \left(\frac{\mathbf{u}}{g} Q^{12} + \frac{\mathbf{v}}{g} Q^{22} \right)^T \\ &= \frac{\mathbf{u}}{g} Q^{11} (Q^{12})^T \left(\frac{\mathbf{u}}{g} \right)^T + \frac{\mathbf{u}}{g} Q^{11} (Q^{22})^T \left(\frac{\mathbf{v}}{g} \right)^T \\ & \quad + \frac{\mathbf{v}}{g} Q^{21} (Q^{12})^T \left(\frac{\mathbf{u}}{g} \right)^T + \frac{\mathbf{v}}{g} Q^{21} (Q^{22})^T \left(\frac{\mathbf{v}}{g} \right)^T \end{aligned}$$

$$\equiv_2 \frac{\mathbf{u}}{g} Q^{11} (Q^{12})^T \left(\frac{\mathbf{u}}{g} \right)^T + \frac{\mathbf{u}}{g} \left(\frac{\mathbf{v}}{g} \right)^T + \frac{\mathbf{v}}{g} Q^{21} (Q^{22})^T \left(\frac{\mathbf{v}}{g} \right)^T,$$

where in the last equality we have used (28) (substituting $Q^{11} (Q^{22})^T$) and we have transposed the scalar $\frac{\mathbf{v}}{g} Q^{21} (Q^{12})^T \left(\frac{\mathbf{u}}{g} \right)^T$.

Therefore,

$$\frac{\mathbf{u}}{g} Q^{11} (Q^{12})^T \left(\frac{\mathbf{u}}{g} \right)^T + \frac{\mathbf{v}}{g} Q^{21} (Q^{22})^T \left(\frac{\mathbf{v}}{g} \right)^T \equiv 0 \pmod{2}.$$

This finishes the proof of the lemma. $\square$

As a result, we obtain the following theorem:

Theorem 3.13. *The full group of automorphisms of H_{k+2} is Orbit Decidable.* $\square$

A direct application of Theorem 1.1 gives us the following corollary:

Corollary 3.14. *Let H be a torsion-free hyperbolic group (with n generators) and let $\varphi_{M_1, \mathbf{p}^1}, \dots, \varphi_{M_n, \mathbf{p}^n} \in \text{Aut}(H_{k+2})$ be automorphisms such that $\langle \varphi_{M_1, \mathbf{p}^1}, \dots, \varphi_{M_n, \mathbf{p}^n} \rangle = \text{Aut}(H_{k+2})$. Then the Conjugacy Problem is solvable in any group of the form $H_{k+2} \rtimes_{\varphi_{M_1, \mathbf{p}^1}, \dots, \varphi_{M_n, \mathbf{p}^n}} H$.* $\square$

3.6.2 $\text{OD}(\langle \varphi_{M_1, \mathbf{p}^1}, \dots, \varphi_{M_n, \mathbf{p}^n} \rangle \text{Inn}(H_{k+2}))$ (Positive and negative results)

Now, we will relate the orbit decidability of this subgroup with the orbit decidability of the subgroup generated by the associated matrices.

Theorem 3.15. *Let $\mathbf{p}^1, \dots, \mathbf{p}^n \in \mathbb{Z}^{2k}$. Then, $Sp_{2k}(\mathbb{Z}) \cap \langle M_1, \dots, M_n \rangle \leq \text{Aut}(\mathbb{Z}^{2k})$ is Orbit Decidable, if and only if, $\langle \varphi_{M_1, \mathbf{p}^1}, \dots, \varphi_{M_n, \mathbf{p}^n} \rangle \text{Inn}(H_{k+2}) \leq \text{Aut}(H_{k+2})$ is Orbit Decidable.*

Proof. ($\Rightarrow$) Since $Sp_{2k}(\mathbb{Z}) \cap \langle M_1, \dots, M_n \rangle \triangleleft_2 \langle M_1, \dots, M_n \rangle$ or $Sp_{2k}(\mathbb{Z}) \cap \langle M_1, \dots, M_n \rangle = \langle M_1, \dots, M_n \rangle$, we know that $\langle M_1, \dots, M_n \rangle$ is also Orbit Decidable.

Let $a^{\mathbf{u}} b^{\mathbf{v}} c^{\mathbf{w}}, a^{\mathbf{r}} b^{\mathbf{s}} c^{\mathbf{t}} \in H_{k+2}$. If there is no matrix $M \in \langle M_1, \dots, M_n \rangle$ such that $[\mathbf{r}, \mathbf{s}]M = [\mathbf{u}, \mathbf{v}]$, then we must answer no.

If $\exists M \in \langle M_1, \dots, M_n \rangle$ such that $[\mathbf{r}, \mathbf{s}]M = [\mathbf{u}, \mathbf{v}]$ and $M = M_{i_1}^{\varepsilon_1} \dots M_{i_l}^{\varepsilon_l}$, we can compute $\varphi_{M, \mathbf{p}} = \varphi_{M_{i_1}, \mathbf{p}^{i_1}}^{\varepsilon_1} \dots \varphi_{M_{i_l}, \mathbf{p}^{i_l}}^{\varepsilon_l}$. Then, we have

$$(a^{\mathbf{x}} b^{\mathbf{y}})^{-1} (a^{\mathbf{r}} b^{\mathbf{s}} c^{\mathbf{t}}) \varphi_{M, \mathbf{p}} a^{\mathbf{x}} b^{\mathbf{y}} = a^{\mathbf{u}} b^{\mathbf{v}} c^{\mu(M)\mathbf{t} + \gamma + \mathbf{v}\mathbf{x}^T - \mathbf{u}\mathbf{y}^T},$$

where

$$\begin{aligned}
\gamma = & \sum_{i=1}^k \frac{r_i(r_i-1)}{2} \mathbf{m}_i^{11} (\mathbf{m}_i^{12})^T + \sum_{i=1}^k \frac{s_i(s_i-1)}{2} \mathbf{m}_i^{21} (\mathbf{m}_i^{22})^T \\
& + \sum_{i=1}^{k-1} \sum_{j=i+1}^k r_i \mathbf{m}_i^{12} (r_j \mathbf{m}_j^{11})^T + \sum_{i=1}^{k-1} \sum_{j=i+1}^k s_i \mathbf{m}_i^{22} (s_j \mathbf{m}_j^{21})^T \\
& + \left(\sum_{i=1}^k r_i \mathbf{m}_i^{12} \right) \cdot \left(\sum_{i=1}^k s_i \mathbf{m}_i^{21} \right)^T \\
& + \sum_{i=1}^k r_i p_i^{(1)} + \sum_{i=1}^k s_i p_i^{(2)}.
\end{aligned}$$

Since we can choose $\mathbf{x}, \mathbf{y} \in \mathbb{Z}^k$, the equation $w = \mu(M)t + \gamma + \mathbf{v}\mathbf{x}^T - \mathbf{u}\mathbf{y}^T$ has a solution over the integers, if and only if,

- In the case $2 \nmid g$, $w \equiv \mu(M)t \pmod{g}$, where $g = \gcd(u_i, v_i)_{i=1, \dots, k} = \gcd(r_i, s_i)_{i=1, \dots, k}$; or $w \equiv -\mu(M)t \pmod{g}$ and there exists $Q \in \langle M_1, \dots, M_n \rangle$ with $\mu(Q) = -1$ such that $[\mathbf{u}, \mathbf{v}]Q = [\mathbf{u}, \mathbf{v}]$.

This last problem (deciding the existence of Q) can be reduced to:

If $M_1, \dots, M_n$ are all symplectic, Q does not exist.

If, without any loss of generality, M_1 is antisymplectic and $M_2, \dots, M_n$ are symplectic, then, we just have to decide if $\exists R \in Sp_{2k}(\mathbb{Z}) \cap \langle M_1, \dots, M_n \rangle = \langle M_1^2, M_2, \dots, M_n, M_1^{-1}M_2M_1, \dots, M_1^{-1}M_nM_1 \rangle$ such that $([\mathbf{u}, \mathbf{v}]M_1) \cdot R = [\mathbf{u}, \mathbf{v}]$. (Here we use the same arguments as in Lemma 2.17, changing SL by Sp and GL by GSp , as well as determinants by multipliers. It is similar because $Sp_{2k}(\mathbb{Z}) \triangleleft_2 GSp_{2k}(\mathbb{Z})$).

So, if $Sp_{2k}(\mathbb{Z}) \cap \langle M_1, \dots, M_n \rangle$ is orbit decidable, this decisional problem can be solved.

- In the case $2 \mid g$, after computing $\alpha = \sum_{i=1}^k \left(\frac{r_i}{g} \mathbf{m}_i^{11} (\mathbf{m}_i^{12})^T + \frac{s_i}{g} \mathbf{m}_i^{21} (\mathbf{m}_i^{22})^T \right) \pmod{2}$ (by Lemma 3.12, α does not depend on the choice of M), $w \equiv \mu(M)t + \alpha \frac{g}{2} \pmod{g}$; or $w \equiv -\mu(M)t + \alpha \frac{g}{2} \pmod{g}$ and there exists $Q \in \langle M_1, \dots, M_n \rangle$ with $\mu(Q) = -1$ such that $[\mathbf{u}, \mathbf{v}]Q = [\mathbf{u}, \mathbf{v}]$, where this last decisional problem can be solved (it is the same problem as in the case $2 \nmid g$).

So, $\langle \varphi_{M_1, \mathbf{p}^1}, \dots, \varphi_{M_n, \mathbf{p}^n} \rangle \text{Inn}(H_{k+2}) \leq \text{Aut}(H_{k+2})$ is Orbit Decidable.

($\Leftarrow$) Let $[\mathbf{u}, \mathbf{v}], [\mathbf{r}, \mathbf{s}] \in \mathbb{Z}^{2k}$. We want to decide if $\exists M \in Sp_{2k}(\mathbb{Z}) \cap \langle M_1, \dots, M_n \rangle$ such that $[\mathbf{r}, \mathbf{s}]M = [\mathbf{u}, \mathbf{v}]$.

If $\gcd(u_i, v_i)_{i=1, \dots, k} \neq \gcd(r_i, s_i)_{i=1, \dots, k}$, then M cannot exist, because there is no $M \in GL_{2k}(\mathbb{Z})$ doing this.

Therefore, we can assume that $g = \gcd(u_i, v_i)_{i=1, \dots, k} = \gcd(r_i, s_i)_{i=1, \dots, k}$. After multiplying by $\frac{3}{g}$ if necessary, we may assume without any loss of generality that $\gcd(u_i, v_i)_{i=1, \dots, k} = \gcd(r_i, s_i)_{i=1, \dots, k} = 3$.

Now, since $\langle \varphi_{M_1, \mathbf{p}^1}, \dots, \varphi_{M_n, \mathbf{p}^n} \rangle \text{Inn}(H_{k+2}) \leq \text{Aut}(H_{k+2})$ is Orbit Decidable, we have an algorithm deciding if given two elements of H_{k+2} , there is a ψ in this subgroup of automorphisms such that ψ sends one of the elements to the other.

We give to this algorithm the elements $a^u b^v c, a^r b^s c \in H_{k+2}$. If the algorithm answers yes, then there is $\psi = \varphi_{M, \mathbf{p}} \xi_{a^x b^y c^z} \in \langle \varphi_{M_1, \mathbf{p}^1}, \dots, \varphi_{M_n, \mathbf{p}^n} \rangle \text{Inn}(H_{k+2})$ such that

$$a^u b^v c = (a^r b^s c) \varphi_{M, \mathbf{p}} \xi_{a^x b^y c^z} = (a^x b^y c^z)^{-1} (a^r b^s c) \varphi_{M, \mathbf{p}} (a^x b^y c^z) = a^{\tilde{u}} b^{\tilde{v}} c^{\mu(M) + \gamma + \tilde{\mathbf{v}} \mathbf{x}^T - \tilde{\mathbf{u}} \mathbf{y}^T},$$

where $[\mathbf{r}, \mathbf{s}]M = [\tilde{\mathbf{u}}, \tilde{\mathbf{v}}]$ and

$$\begin{aligned} \gamma = & \sum_{i=1}^k \frac{r_i(r_i-1)}{2} \mathbf{m}_i^{11} (\mathbf{m}_i^{12})^T + \sum_{i=1}^k \frac{s_i(s_i-1)}{2} \mathbf{m}_i^{21} (\mathbf{m}_i^{22})^T \\ & + \sum_{i=1}^{k-1} \sum_{j=i+1}^k r_i \mathbf{m}_i^{12} (r_j \mathbf{m}_j^{11})^T + \sum_{i=1}^{k-1} \sum_{j=i+1}^k s_i \mathbf{m}_i^{22} (s_j \mathbf{m}_j^{21})^T \\ & + \left(\sum_{i=1}^k r_i \mathbf{m}_i^{12} \right) \cdot \left(\sum_{i=1}^k s_i \mathbf{m}_i^{21} \right)^T \\ & + \sum_{i=1}^k r_i p_i^{(1)} + \sum_{i=1}^k s_i p_i^{(2)}; \end{aligned}$$

but this implies that $[\mathbf{r}, \mathbf{s}]M = [\mathbf{u}, \mathbf{v}]$ ($[\tilde{\mathbf{u}}, \tilde{\mathbf{v}}] = [\mathbf{u}, \mathbf{v}]$) and the exponents of c must coincide:

$$1 = \mu(M) + \gamma + \tilde{\mathbf{v}} \mathbf{x}^T - \tilde{\mathbf{u}} \mathbf{y}^T.$$

Since $3 \mid \gamma + \mathbf{v} \mathbf{x}^T - \mathbf{u} \mathbf{y}^T$, reducing modulo 3 we have

$$\mu(M) \equiv 1 \pmod{3},$$

and since $\mu(M) \in \{-1, 1\}$, the only possibility is $\mu(M) = 1$ ($M \in Sp_{2k}(\mathbb{Z})$).

So we have that $\exists M \in Sp_{2k}(\mathbb{Z}) \cap \langle M_1, \dots, M_n \rangle$ such that $[\mathbf{r}, \mathbf{s}]M = [\mathbf{u}, \mathbf{v}]$.

Conversely, if $\exists M \in Sp_{2k}(\mathbb{Z}) \cap \langle M_1, \dots, M_n \rangle$ such that $[\mathbf{r}, \mathbf{s}]M = [\mathbf{u}, \mathbf{v}]$ and $M = M_{i_1}^{\varepsilon_1} \dots M_{i_l}^{\varepsilon_l}$, then we can construct $\psi = \varphi_{M, \mathbf{p}} \xi_{a^x b^y} \in \langle \varphi_{M_1, \mathbf{p}^1}, \dots, \varphi_{M_n, \mathbf{p}^n} \rangle \text{Inn}(H_{k+2})$ with $\varphi_{M, \mathbf{p}} = \varphi_{M_{i_1}, \mathbf{p}^{i_1}}^{\varepsilon_1} \dots \varphi_{M_{i_l}, \mathbf{p}^{i_l}}^{\varepsilon_l}$ so that

$$(a^r b^s c) \psi = a^u b^v c^{1 + \gamma + \mathbf{v} \mathbf{x}^T - \mathbf{u} \mathbf{y}^T},$$

where

$$\begin{aligned} \gamma = & \sum_{i=1}^k \frac{r_i(r_i-1)}{2} \mathbf{m}_i^{11} (\mathbf{m}_i^{12})^T + \sum_{i=1}^k \frac{s_i(s_i-1)}{2} \mathbf{m}_i^{21} (\mathbf{m}_i^{22})^T \\ & + \sum_{i=1}^{k-1} \sum_{j=i+1}^k r_i \mathbf{m}_i^{12} (r_j \mathbf{m}_j^{11})^T + \sum_{i=1}^{k-1} \sum_{j=i+1}^k s_i \mathbf{m}_i^{22} (s_j \mathbf{m}_j^{21})^T \\ & + \left(\sum_{i=1}^k r_i \mathbf{m}_i^{12} \right) \cdot \left(\sum_{i=1}^k s_i \mathbf{m}_i^{21} \right)^T \\ & + \sum_{i=1}^k r_i p_i^{(1)} + \sum_{i=1}^k s_i p_i^{(2)}. \end{aligned}$$

Since $\gcd(u_i, v_i)_{i=1, \dots, k} = \gcd(r_i, s_i)_{i=1, \dots, k} = 3$, $3 \mid \gamma$ and we can choose $\mathbf{x}, \mathbf{y} \in \mathbb{Z}^k$ such that

$$\mathbf{v}\mathbf{x}^T - \mathbf{u}\mathbf{y} = -\gamma,$$

and, therefore,

$$(a^r b^s c)\psi = a^u b^v c.$$

This means, that the algorithm answers yes on inputs $a^u b^v c, a^r b^s c \in H_{k+2}$, if and only if, $\exists M \in Sp_{2k}(\mathbb{Z}) \cap \langle M_1, \dots, M_n \rangle$ such that $[\mathbf{r}, \mathbf{s}]M = [\mathbf{u}, \mathbf{v}]$. So, $Sp_{2k}(\mathbb{Z}) \cap \langle M_1, \dots, M_n \rangle \leq GL_{2k}(\mathbb{Z})$ is Orbit Decidable.

This finishes the proof. $\square$

We have the following corollaries:

Corollary 3.16. *Every subgroup of the form $\langle \varphi_{M, \mathbf{p}} \rangle Inn(H_{k+2}) \leq Aut(H_{k+2})$ is Orbit Decidable.*

Proof. For any invertible matrix $M \in GL_{2k}(\mathbb{Z})$, it is a well-known result that $\langle M \rangle \leq Aut(\mathbb{Z}^{2k}) = GL_{2k}(\mathbb{Z})$ is Orbit Decidable.

If M is antisymplectic, then $\langle M \rangle \cap Sp_{2k}(\mathbb{Z}) = \langle M^2 \rangle$; and if M is symplectic, then $\langle M \rangle \cap Sp_{2k}(\mathbb{Z}) = \langle M \rangle$. In any case, the corresponding subgroup is cyclic and, therefore, Orbit Decidable. Applying Theorem 3.15, we get the result we want. $\square$

A direct application of Theorem 1.1 gives us the following corollary:

Corollary 3.17. *The Conjugacy Problem is solvable in any group of the form $H_{k+2} \rtimes \mathbb{Z}$.* $\square$

By [7, Proposition 7.5], we have that

Lemma 3.18. *For $k \geq 4$, there exist 14 matrices $A_1, \dots, A_{14} \in GL_k(\mathbb{Z})$ such that $\langle A_1, \dots, A_{14} \rangle \leq GL_k(\mathbb{Z})$ is Orbit Undecidable.*

This [7, Proposition 7.5] just claims the existence of orbit undecidable subgroups of $GL_k(\mathbb{Z})$ for $k \geq 4$, but we can be more precise and get a 14-generated such subgroup using the argument in the paragraph immediately before [7, Corollary 7.2] based on Borisov's example of a 2-generated 12-related group with unsolvable Word Problem.

For a fixed $k \geq 4$, we can now define the matrices

$$G_i = \begin{bmatrix} A_i & O \\ O & (A_i^T)^{-1} \end{bmatrix} \in Sp_{2k}(\mathbb{Z})$$

for $i = 1, \dots, 14$.

As a result, we have

Corollary 3.19. *For $k \geq 4$, the subgroup $\langle \varphi_{G_1, \mathbf{p}^1}, \dots, \varphi_{G_{14}, \mathbf{p}^{14}} \rangle Inn(H_{k+2}) \leq Aut(H_{k+2})$ for any $\mathbf{p}^1, \dots, \mathbf{p}^{14} \in \mathbb{Z}^{2k}$ is Orbit Undecidable.*

Proof. We will prove that $\langle G_1, \dots, G_{14} \rangle \cap Sp_{2k}(\mathbb{Z}) = \langle G_1, \dots, G_{14} \rangle$ is Orbit Undecidable.

If it was Orbit Decidable, then taking as inputs $[\mathbf{u}, \mathbf{0}_k], [\mathbf{v}, \mathbf{0}_k] \in \mathbb{Z}^{2k}$, we can determine if there exists $A \in \langle A_1, \dots, A_{14} \rangle$ such that $\mathbf{u} = \mathbf{v}A$, but by Lemma 3.18, this is impossible. Therefore, $\langle G_1, \dots, G_{14} \rangle$ is Orbit Undecidable.

Applying Theorem 3.15, we conclude. $\square$

A direct application of Theorem 1.1 gives us the following corollary:

Corollary 3.20. *For $k \geq 4$, there exist H_{k+2} -by-free groups of the form $H_{k+2} \rtimes F_{14}$ with unsolvable Conjugacy Problem.* $\square$

An open question arises: For $k = 2, 3$, can we find examples of subgroups of matrices from $Sp_{2k}(\mathbb{Z})$ which are orbit undecidable? The answer to this question would allow us to determine if there are H_{k+2} -by-torsion-free-hyperbolic groups with unsolvable Conjugacy Problem for $k = 2, 3$.

4. Conclusions

The aim of this Master's Thesis was to find applications of Theorem 1.1 with $F = H_{k+2}$ for $k \geq 1$. From some previous results, i.e., the structure of the group of automorphisms of the Heisenberg group (see [19]); the aim was to check that the conditions of Theorem 1.1 were satisfied, and then apply the theorem. In particular, we proved:

- The Twisted Conjugacy Problem is solvable in H_3 (Theorem 2.12) and, more generally in H_{k+2} (Theorem 3.10).
- The full group of automorphisms $Aut(H_3)$ (Theorem 2.13), and more generally, $Aut(H_{k+2})$ (Theorem 3.13) is Orbit Decidable. As a result, we obtained corollaries 2.14 and 3.14.
- Every finitely generated subgroup A such that $Inn(H_3) \leq A \leq Aut(H_3)$ is Orbit Decidable (Theorem 2.18), obtaining the corresponding application: Corollary 2.19.
- Every subgroup of the form $\langle \varphi_{M,p} \rangle Inn(H_{k+2}) \leq Aut(H_{k+2})$ is Orbit Decidable (Corollary 3.16), obtaining the corresponding application: Corollary 3.17.
- For $k \geq 4$, there are finitely generated subgroups A such that $Inn(H_{k+2}) \leq A \leq Aut(H_{k+2})$ which are Orbit Undecidable (Corollary 3.19), obtaining the subsequent negative result regarding the CP of some particular extensions (Corollary 3.20).

All these results were new contributions to the field. We believe that the aim of the Master's Thesis has been fulfilled with these results.

References

- [1] S.I. Adyan, “Algorithmic unsolvability of problems of recognition of certain properties of groups” (in Russian) *Doklady Akademii Nauk SSSR* **103** (1955), 533–535. C.F. Nyberg-Brodda, “The Adyan-Rabin theorem: an English translation”, (2022).
- [2] A. Andrianov, “Introduction to Siegel Modular Forms and Dirichlet Series”, *Springer*, (2009).
- [3] P. Bender, “Eine Präsentation der symplektischen Gruppe $Sp(4, \mathbb{Z})$ mit 2 Erzeugenden und 8 definierenden Relationen”, *Journal of Algebra*, **65**, 328–331, (1980).
- [4] W. Boone, “The word problem”, *Proceedings of the National Academy of Sciences* **44**(10) (1958), 1061–1065.
- [5] M. Blufstein, M. Valiunas, “On the twisted conjugacy problem for large-type Artin groups”, preprint available at <https://arxiv.org/pdf/2411.05493>.
- [6] O. Bogopolski, A. Martino, O. Maslakova, E. Ventura, “Free-by-cyclic groups have solvable conjugacy problem”, *Bulletin of the London Mathematical Society* **38**(5) (2006), 787–794.
- [7] O. Bogopolski, A. Martino, E. Ventura, “Orbit decidability and the conjugacy problem for some extensions of groups”, *Transactions of the AMS* **362**(4) (2010), 2003–2036.
- [8] P. Brinkmann, “Detecting automorphic orbits in free groups”, *Journal of Algebra* **324** (2010), 1083–1097.
- [9] J. Burillo, F. Matucci, E. Ventura, “The conjugacy problem in extensions of Thompson’s group F ”, *Israel Journal of Mathematics* **216**(1) (2016), 15–59.
- [10] G. Crowe, “Twisted conjugacy in dihedral Artin groups I: Torus Knot groups”, *Journal of Groups, Complexity, Cryptology* **17**(1) (2025).
- [11] G. Crowe, “Twisted conjugacy in dihedral Artin groups II: Baumslag–Solitar groups $BS(n, n)$ ”, to appear in *International Journal of Algebra and Computation*, available at <https://arxiv.org/abs/2404.04705>.
- [12] M. Dehn, “Über unendliche diskontinuierliche Gruppen”, *Math. Ann.* **71** (1911). Translated by J. Stillwell: “On Infinite Discontinuous Groups”, in *Papers on Group Theory and Topology* 133–178, Springer-Verlag, 1987.
- [13] J. González-Meneses, E. Ventura, “Twisted conjugacy in the braid group”, *Israel Journal of Mathematics* **201** (2014), 455–476.
- [14] Grunewald FJ, Segal D. “How to solve a quadratic equation in integers”. *Mathematical Proceedings of the Cambridge Philosophical Society*, (1981); **89**(1):1–5.
- [15] A.J. Hahn, O.T. O’Meara, “The Classical Groups and K-Theory”, *Springer*, (1989).
- [16] C.F. Miller III, “On group-theoretic decision problems and their classification”, *Annals of Math. Studies* **68** (1971).

- [17] O. Mitra, M. Roy, E. Ventura, "On the twisted conjugacy problem for Baumslag–Solitar groups", preprint available at <https://arxiv.org/pdf/2508.04397>.
- [18] P.S. Novikov, "On the algorithmic unsolvability of the word problem in group theory", *Proceedings of the Steklov Institute of Mathematics* (in Russian) **44** (1955), 1–143.
- [19] D.V. Osipov, "Discrete Heisenberg group and its automorphism group", *Mathematical Notes*, (2015). Available at <https://arxiv.org/abs/1505.00348v1>.
- [20] M.O. Rabin, "Recursive unsolvability of group theoretic problems", *Annals of Mathematics* (2) **67** (1958), 172–194.
- [21] K. Reidemeister, "Automorphismen von homotopiekettenringen", *Math. Ann.* **112** (1936), 586–593.
- [22] I. Sierra and N. Wahl, "Homological stability for symplectic groups via algebraic arc complexes", (2025). Available at <https://arxiv.org/abs/2411.07895>
- [23] Z. Sunic, E. Ventura, "The conjugacy problem in automaton groups is not solvable", *Journal of Algebra* **364** (2012), 148–154.

A. Some notes on symplectic matrices

In Section 3.2, we encountered a very concrete type of matrices. We will introduce in this appendix some useful definitions and properties related to these matrices. In particular, we will define **general symplectic matrices** and some properties of them.

Given a commutative ring with unity R and a matrix $M \in \mathcal{M}_{2k}(R)$, we say that M is general symplectic if it satisfies the relation

$$M^T J M = \mu(M) J \text{ with } J = J_k = \begin{bmatrix} O & I_k \\ -I_k & O \end{bmatrix}$$

and a unit scalar $\mu(M)$ called the multiplier of M .

Lemma A.1. *The product of two general symplectic matrices is again a general symplectic matrix and the multiplier of a product is the product of multipliers of the factors.*

Proof. Given M, N general symplectic matrices over a ring R , we have

$$\begin{aligned} (MN)^T J (MN) &= N^T (M^T J M) N = N^T (\mu(M) J) N \\ &= \mu(M) N^T J N = \mu(M) \mu(N) J \\ &= \mu(MN) J. \end{aligned}$$

Therefore, MN is again a general symplectic matrix with multiplier $\mu(MN) = \mu(M)\mu(N)$. $\square$

Lemma A.2 (Andrianov, [2]). *Let $M = \begin{bmatrix} M^{11} & M^{12} \\ M^{21} & M^{22} \end{bmatrix}$ where the blocks $M^{11}, M^{12}, M^{21}, M^{22}$ are square matrices of order k , and let μ be a unit in R . Then, the following conditions are equivalent:*

1. M is general symplectic with the multiplier $\mu(M) = \mu$;
2. M^T is general symplectic with the multiplier $\mu(M^T) = \mu$;
3. M is invertible, and

$$M^{-1} = \mu^{-1} \begin{bmatrix} (M^{22})^T & -(M^{12})^T \\ -(M^{21})^T & (M^{11})^T \end{bmatrix};$$

4. The blocks $M^{11}, M^{12}, M^{21}, M^{22}$ satisfy the conditions

$$(M^{11})^T M^{21} = (M^{21})^T M^{11}, \quad (M^{12})^T M^{22} = (M^{22})^T M^{12}, \quad (35)$$

$$\text{and } (M^{11})^T M^{22} - (M^{21})^T M^{12} = \mu I_k$$

or the conditions

$$M^{11} (M^{12})^T = M^{12} (M^{11})^T, \quad M^{21} (M^{22})^T = M^{22} (M^{21})^T, \quad (36)$$

$$\text{and } M^{11} (M^{22})^T - M^{12} (M^{21})^T = \mu I_k.$$

Proof. (1) $\Rightarrow$ (3). Suppose M is general symplectic with $\mu(M) = \mu$. Then,

$$\begin{aligned}
M^T J M &= \begin{bmatrix} (M^{11})^T & (M^{21})^T \\ (M^{12})^T & (M^{22})^T \end{bmatrix} \begin{bmatrix} O & I_k \\ -I_k & O \end{bmatrix} \begin{bmatrix} M^{11} & M^{12} \\ M^{21} & M^{22} \end{bmatrix} \\
&= \begin{bmatrix} -(M^{21})^T & (M^{11})^T \\ -(M^{22})^T & (M^{12})^T \end{bmatrix} \begin{bmatrix} M^{11} & M^{12} \\ M^{21} & M^{22} \end{bmatrix} \\
&= \begin{bmatrix} (M^{11})^T M^{21} - (M^{21})^T M^{11} & (M^{11})^T M^{22} - (M^{21})^T M^{12} \\ (M^{12})^T M^{21} - (M^{22})^T M^{11} & (M^{12})^T M^{22} - (M^{22})^T M^{12} \end{bmatrix} \\
&= \mu J \\
&= \begin{bmatrix} O & \mu I_k \\ -\mu I_k & O \end{bmatrix}.
\end{aligned}$$

So, we have

$$\begin{aligned}
(M^{11})^T M^{21} &= (M^{21})^T M^{11}, \quad (M^{12})^T M^{22} = (M^{22})^T M^{12}, \\
\text{and } (M^{11})^T M^{22} - (M^{21})^T M^{12} &= \mu I_k.
\end{aligned}$$

which coincides with (35).

Now, multiplying

$$\begin{aligned}
&\mu^{-1} \begin{bmatrix} (M^{22})^T & -(M^{12})^T \\ -(M^{21})^T & (M^{11})^T \end{bmatrix} \begin{bmatrix} M^{11} & M^{12} \\ M^{21} & M^{22} \end{bmatrix} \\
&= \mu^{-1} \begin{bmatrix} (M^{22})^T M^{11} - (M^{12})^T M^{21} & (M^{22})^T M^{12} - (M^{12})^T M^{22} \\ (M^{11})^T M^{21} - (M^{21})^T M^{11} & (M^{11})^T M^{22} - (M^{21})^T M^{12} \end{bmatrix} \\
&= \mu^{-1} \begin{bmatrix} \mu I_k & O \\ O & \mu I_k \end{bmatrix} \\
&= I_{2k}.
\end{aligned}$$

So, M is invertible and

$$M^{-1} = \mu^{-1} \begin{bmatrix} (M^{22})^T & -(M^{12})^T \\ -(M^{21})^T & (M^{11})^T \end{bmatrix}.$$

(3) $\Rightarrow$ (1). Reciprocally, assuming M is invertible and

$$M^{-1} = \mu^{-1} \begin{bmatrix} (M^{22})^T & -(M^{12})^T \\ -(M^{21})^T & (M^{11})^T \end{bmatrix},$$

and using the fact that $M^{-1}M = I_{2k}$, we get the conditions (35), which imply that M is general symplectic.

(1) $\Rightarrow$ (2). M^T is general symplectic with $\mu(M^T) = \mu$, if and only if,

$$\begin{aligned}
 MJM^T &= \begin{bmatrix} M^{11} & M^{12} \\ M^{21} & M^{22} \end{bmatrix} \begin{bmatrix} O & I_k \\ -I_k & O \end{bmatrix} \begin{bmatrix} (M^{11})^T & (M^{21})^T \\ (M^{12})^T & (M^{22})^T \end{bmatrix} \\
 &= \begin{bmatrix} -M^{12} & M^{11} \\ -M^{22} & M^{21} \end{bmatrix} \begin{bmatrix} (M^{11})^T & (M^{21})^T \\ (M^{12})^T & (M^{22})^T \end{bmatrix} \\
 &= \begin{bmatrix} M^{11} (M^{12})^T - M^{12} (M^{11})^T & M^{11} (M^{22})^T - M^{12} (M^{21})^T \\ M^{21} (M^{12})^T - M^{22} (M^{11})^T & M^{21} (M^{22})^T - M^{22} (M^{21})^T \end{bmatrix} \\
 &= \mu J \\
 &= \begin{bmatrix} O & \mu I_k \\ -\mu I_k & O \end{bmatrix},
 \end{aligned}$$

which is verified, if and only if,

$$\begin{aligned}
 M^{11} (M^{12})^T &= M^{12} (M^{11})^T, \quad M^{21} (M^{22})^T = M^{22} (M^{21})^T, \\
 \text{and } M^{11} (M^{22})^T - M^{12} (M^{21})^T &= \mu I_k.
 \end{aligned}$$

which coincides with (36).

Assuming (1), we have proved that (3) also holds. Therefore,

$$\begin{aligned}
 \mu I_{2k} &= M \mu M^{-1} = \begin{bmatrix} M^{11} & M^{12} \\ M^{21} & M^{22} \end{bmatrix} \begin{bmatrix} (M^{22})^T & -(M^{12})^T \\ -(M^{21})^T & (M^{11})^T \end{bmatrix} \\
 &= \begin{bmatrix} M^{11} (M^{22})^T - M^{12} (M^{21})^T & M^{12} (M^{11})^T - M^{11} (M^{12})^T \\ M^{21} (M^{22})^T - M^{22} (M^{21})^T & M^{22} (M^{11})^T - M^{21} (M^{12})^T \end{bmatrix}
 \end{aligned}$$

And these relations coincide with (36), which proves that M^T is general symplectic.

(2) $\Rightarrow$ (1) It is immediate using (1) $\Rightarrow$ (2) and the fact that $(M^T)^T = M$.

Finally, we have already seen that (1) implies (35). Therefore, clearly (1) $\Rightarrow$ (4).

Reciprocally, if (35) is verified, then (1) is verified. If (36) is verified, then (2), and therefore (1), is verified. This proves (4) $\Rightarrow$ (1). $\square$

Lemma A.3. *If M is general symplectic with multiplier $\mu(M) = \mu$, then M^{-1} is also general symplectic with multiplier $\mu(M^{-1}) = \mu^{-1}$.*

Proof. Suppose M is general symplectic with multiplier $\mu(M) = \mu$. Then,

$$M^T J M = \mu J$$

and we have that

$$\mu^{-1} J = (M^{-1})^T J M^{-1},$$

which finishes the proof. $\square$

These lemmas prove immediately the following result:

Theorem A.4. *The set of general symplectic matrices of order $2k$ over a ring R , which we will denote from now on as $GS_{p_{2k}}(R)$, is a subgroup of $GL_{2k}(R)$. Therefore,*

$$GS_{p_{2k}}(R) = \{M \in GL_{2k}(R) \mid M^T JM = \mu(M)J \text{ with } \mu(M) \in R^*\},$$

where

$$J = \begin{bmatrix} O & I_k \\ -I_k & O \end{bmatrix}.$$

This group is called in the literature **general symplectic group**. □

We will say that M is a **symplectic** matrix if M is a general symplectic matrix with multiplier $\mu(M) = 1$.

It is also worth defining the subgroup of **symplectic matrices** $Sp_{2k}(R)$ of $GS_{p_{2k}}(R)$, which is defined as the set general symplectic matrices which have multiplier $\mu = 1$; that is:

$$Sp_{2k}(R) = \{M \in GL_{2k}(R) \mid M^T JM = J\}.$$

For our purposes, we will consider that $R = \mathbb{Z}$ and, therefore, $R^* = \{-1, 1\}$. This means that

$$GS_{p_{2k}}(\mathbb{Z}) = \{M \in GL_{2k}(\mathbb{Z}) \mid M^T JM = \mu(M)J \text{ with } \mu(M) \in \{-1, 1\}\}.$$

We will say that $M \in GS_{p_{2k}}(\mathbb{Z})$ is **antisymplectic** if M is a general symplectic matrix over the integers such that $\mu(M) = -1$.

B. Presentation of $Sp_4(\mathbb{Z})$ and $GSp_4(\mathbb{Z})$

By [3], we have that $Sp_4(\mathbb{Z})$ is generated by

$$\begin{aligned}
 x_\alpha &= \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 1 \end{bmatrix}, & x_\beta &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, & x_{\alpha+\beta} &= \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \\
 x_{2\alpha+\beta} &= \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, & w_\alpha &= \begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, & w_\beta &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix},
 \end{aligned}$$

subject to relations:

$$x_\alpha x_\beta x_\alpha^{-1} x_\beta^{-1} = x_{\alpha+\beta} x_{2\alpha+\beta}, \quad (37)$$

$$x_\alpha x_{\alpha+\beta} x_\alpha^{-1} x_{\alpha+\beta}^{-1} = x_{2\alpha+\beta}^2, \quad (38)$$

$$x_\alpha x_{2\alpha+\beta} x_\alpha^{-1} x_{2\alpha+\beta}^{-1} = 1, \quad (39)$$

$$x_\beta x_{\alpha+\beta} x_\beta^{-1} x_{\alpha+\beta}^{-1} = 1, \quad (40)$$

$$x_\beta x_{2\alpha+\beta} x_\beta^{-1} x_{2\alpha+\beta}^{-1} = 1, \quad (41)$$

$$x_{\alpha+\beta} x_{2\alpha+\beta} x_{\alpha+\beta}^{-1} x_{2\alpha+\beta}^{-1} = 1, \quad (42)$$

$$w_\alpha w_\beta^2 w_\alpha = w_\beta^2, \quad (43)$$

$$w_\beta w_\alpha^2 w_\beta^{-1} = w_\alpha^2, \quad (44)$$

$$(w_\alpha w_\beta)^2 = (w_\beta w_\alpha)^2, \quad (45)$$

$$w_\beta^4 = 1, \quad (46)$$

$$w_\alpha x_\beta w_\alpha^{-1} = x_{2\alpha+\beta}, \quad (47)$$

$$w_\alpha x_{2\alpha+\beta} w_\alpha^{-1} = x_\beta, \quad (48)$$

$$w_\alpha x_{\alpha+\beta} w_\alpha^{-1} = x_{\alpha+\beta}^{-1}, \quad (49)$$

$$w_\beta x_\alpha w_\beta^{-1} = x_{\alpha+\beta}, \quad (50)$$

$$w_\beta x_{\alpha+\beta} w_\beta^{-1} = x_\alpha^{-1}, \quad (51)$$

$$w_\beta x_{2\alpha+\beta} w_\beta^{-1} = x_{2\alpha+\beta}, \quad (52)$$

$$w_\alpha x_\alpha w_\alpha^{-1} = x_\alpha^{-1} w_\alpha^{-1} x_\alpha^{-1}, \quad (53)$$

$$w_\beta x_\beta w_\beta^{-1} = x_\beta^{-1} w_\beta^{-1} x_\beta^{-1}. \quad (54)$$

We see that the “elementary matrices” (here we tried to rewrite the presentation in terms of “elementary matrices” as they are defined in [15]) generating $Sp_4(\mathbb{Z})$ of dimension 4 are

$$\begin{aligned}
E_{1,1} &= \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, & E_{1,3} &= \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \\
E_{1,4} &= \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 1 \end{bmatrix}, & E_{2,2} &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \\
E_{2,3} &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{bmatrix}, & E_{2,4} &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}, \\
E_{3,3} &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, & E_{4,4} &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}.
\end{aligned}$$

We want to write $x_\alpha, x_{\alpha+\beta}, x_{2\alpha+\beta}, x_\beta, w_\alpha, w_\beta$ in terms of these elementary matrices. We see that

$$\begin{aligned}
x_\alpha &= E_{1,4}, \\
x_{\alpha+\beta} &= E_{1,3}, \\
x_{2\alpha+\beta} &= E_{1,1}, \\
x_\beta &= E_{3,3}, \\
w_\alpha &= E_{1,4}^{-1} E_{2,3} E_{1,4}, \\
w_\beta &= E_{3,3}^{-1} E_{4,4} E_{3,3},
\end{aligned}$$

and conversely,

$$\begin{aligned}
E_{2,2} &= x_{2\alpha+\beta} w_\alpha w_\beta x_\beta w_\alpha^{-1}, \\
E_{2,3} &= x_\alpha w_\alpha x_\alpha, \\
E_{2,4} &= x_{\alpha+\beta} w_\beta w_\alpha x_\alpha w_\beta^{-1}, \\
E_{4,4} &= x_\beta w_\beta x_\beta.
\end{aligned}$$

Making these substitutions, we get that $Sp_4(\mathbb{Z})$ is generated by

$$E_{1,1}, E_{1,3}, E_{1,4}, E_{2,2}, E_{2,3}, E_{2,4}, E_{3,3}, E_{4,4},$$

subject to relations

$$E_{1,4} E_{3,3} E_{1,4}^{-1} E_{3,3}^{-1} = E_{1,3} E_{1,1}, \quad (55)$$

$$E_{1,4}E_{1,3}E_{1,4}^{-1}E_{1,3}^{-1} = E_{1,1}^2, \quad (56)$$

$$E_{1,4}E_{1,1}E_{1,4}^{-1}E_{1,1}^{-1} = 1, \quad (57)$$

$$E_{3,3}E_{1,3}E_{3,3}^{-1}E_{1,3}^{-1} = 1, \quad (58)$$

$$E_{3,3}E_{1,1}E_{3,3}^{-1}E_{1,1}^{-1} = 1, \quad (59)$$

$$E_{1,3}E_{1,1}E_{1,3}^{-1}E_{1,1}^{-1} = 1, \quad (60)$$

$$E_{1,4}^{-1}E_{2,3}E_{1,4}^{-1}(E_{3,3}^{-1}E_{4,4}E_{3,3}^{-1})^2E_{1,4}^{-1}E_{2,3}E_{1,4}^{-1} = (E_{3,3}^{-1}E_{4,4}E_{3,3}^{-1})^2, \quad (61)$$

$$E_{3,3}^{-1}E_{4,4}E_{3,3}^{-1}(E_{1,4}^{-1}E_{2,3}E_{1,4}^{-1})^2(E_{3,3}^{-1}E_{4,4}E_{3,3}^{-1})^{-1} = (E_{1,4}^{-1}E_{2,3}E_{1,4}^{-1})^2, \quad (62)$$

$$(E_{1,4}^{-1}E_{2,3}E_{1,4}^{-1}E_{3,3}^{-1}E_{4,4}E_{3,3}^{-1})^2 = (E_{3,3}^{-1}E_{4,4}E_{3,3}^{-1}E_{1,4}^{-1}E_{2,3}E_{1,4}^{-1})^2, \quad (63)$$

$$(E_{3,3}^{-1}E_{4,4}E_{3,3}^{-1})^4 = 1, \quad (64)$$

$$E_{1,4}^{-1}E_{2,3}E_{1,4}^{-1}E_{3,3}(E_{1,4}^{-1}E_{2,3}E_{1,4}^{-1})^{-1} = E_{1,1}, \quad (65)$$

$$E_{1,4}^{-1}E_{2,3}E_{1,4}^{-1}E_{1,1}(E_{1,4}^{-1}E_{2,3}E_{1,4}^{-1})^{-1} = E_{3,3}, \quad (66)$$

$$E_{1,4}^{-1}E_{2,3}E_{1,4}^{-1}E_{1,3}(E_{1,4}^{-1}E_{2,3}E_{1,4}^{-1})^{-1} = E_{1,3}^{-1}, \quad (67)$$

$$E_{3,3}^{-1}E_{4,4}E_{3,3}^{-1}E_{1,4}(E_{3,3}^{-1}E_{4,4}E_{3,3}^{-1})^{-1} = E_{1,3}, \quad (68)$$

$$E_{3,3}^{-1}E_{4,4}E_{3,3}^{-1}E_{1,3}(E_{3,3}^{-1}E_{4,4}E_{3,3}^{-1})^{-1} = E_{1,4}^{-1}, \quad (69)$$

$$E_{3,3}^{-1}E_{4,4}E_{3,3}^{-1}E_{1,1}(E_{3,3}^{-1}E_{4,4}E_{3,3}^{-1})^{-1} = E_{1,1}, \quad (70)$$

$$E_{1,4}^{-1}E_{2,3}(E_{1,4}^{-1}E_{2,3}E_{1,4}^{-1})^{-1} = E_{1,4}^{-1}(E_{1,4}^{-1}E_{2,3}E_{1,4}^{-1})^{-1}E_{1,4}^{-1}, \quad (71)$$

$$E_{3,3}^{-1}E_{4,4}(E_{3,3}^{-1}E_{4,4}E_{3,3}^{-1})^{-1} = E_{3,3}^{-1}(E_{3,3}^{-1}E_{4,4}E_{3,3}^{-1})^{-1}E_{3,3}^{-1}, \quad (72)$$

$$E_{2,2} = E_{1,1}E_{1,4}^{-1}E_{2,3}E_{1,4}^{-1}E_{3,3}^{-1}E_{4,4}(E_{1,4}^{-1}E_{2,3}E_{1,4}^{-1})^{-1}, \quad (73)$$

$$E_{2,4} = E_{1,3}E_{3,3}^{-1}E_{4,4}E_{3,3}^{-1}E_{1,4}^{-1}E_{2,3}(E_{3,3}^{-1}E_{4,4}E_{3,3}^{-1})^{-1}. \quad (74)$$

Notice that we can eliminate $E_{2,2}$ and $E_{2,4}$ from this presentation, eliminating also the last two relations.

In order to get a presentation of $GSp_4(\mathbb{Z})$ from this presentation, since $Sp_4(\mathbb{Z}) \triangleleft_2 GSp_4(\mathbb{Z})$, we just need to add as generator an anti-symplectic matrix (a general symplectic matrix with multiplier -1), such as

$$H = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} -I_2 & O \\ O & I_2 \end{bmatrix},$$

which verifies $H^2 = I_4$, and add as relations $H^{-1}E_{i,j}H = E_{i,j}$ if the parity of i is different from the parity of j and $H^{-1}E_{i,j}H = E_{i,j}^{-1}$ if i and j have the same parity.

This gives as the presentation of $GSp_4(\mathbb{Z})$ with generators

$$H, E_{1,1}, E_{1,3}, E_{1,4}, E_{2,3}, E_{3,3}, E_{4,4},$$

subject to relations (55) - (72) and relations:

$$H^2 = 1, \tag{75}$$

$$H^{-1}E_{1,1}H = E_{1,1}^{-1}, \tag{76}$$

$$H^{-1}E_{1,3}H = E_{1,3}^{-1}, \tag{77}$$

$$H^{-1}E_{1,4}H = E_{1,4}, \tag{78}$$

$$H^{-1}E_{2,3}H = E_{2,3}, \tag{79}$$

$$H^{-1}E_{3,3}H = E_{3,3}^{-1}, \tag{80}$$

$$H^{-1}E_{4,4}H = E_{4,4}^{-1}. \tag{81}$$