Congruence Subgroups of the Automorphism Group of a Free Group

Daniel W. Appel

Technical Report

RHUL–MA–2010–13

30 Ocotber 2010

Department of Mathematics
Royal Holloway, University of London
Egham, Surrey TW20 0EX, England

http://www.rhul.ac.uk/mathematics/techreports

Congruence Subgroups of the Automorphism Group of a Free Group

Daniel W. Appel

Thesis submitted to the University of London
for the degree of Doctor of Philosophy

Department of Mathematics
Royal Holloway
University of London

April 2010

Declaration

These doctoral studies were conducted under the supervision of Doctor Benjamin Klopsch.

The work presented in this thesis is of original research carried out by myself, in collaboration with others, whilst enrolled in the Department of Mathematics as a candidate for the degree of Doctor of Philosophy. The following results, which have been obtained in a collaboration with E. Ribnere, have been published in a joint paper:

- Theorem B, parts (i), (ii), (iii), respectively Theorem 4.5 for the special case $n = 2$.
- Theorem D, (i), (ii), (iii), (iv), respectively Theroem 4.12.
- Corollary E, respectively Corollaries 4.13 and 4.14.
- The presentation of $\mathrm{Aut}^+(F_2)$ given in Section 2.2.
- Proposition 3.1 for the special case $n = 2$.
- The discussion in Section 4.1.3.
- Corollary 4.6.
- Lemmas 4.16 and 4.17.

This work has not been submitted for any other degree or award in any other university or educational establishment.

Daniel W. Appel, April 2010

Abstract

Let $n \geq 2$ and F_n be the free group of rank n. Its automorphism group $\mathrm{Aut}(F_n)$ has a well-known surjective linear representation

$$\rho : \mathrm{Aut}(F_n) \longrightarrow \mathrm{Aut}(F_n/F_n') = \mathrm{GL}_n(\mathbb{Z})$$

where F_n' denotes the commutator subgroup of F_n. By $\mathrm{Aut}^+(F_n) := \rho^{-1}(\mathrm{SL}_n(\mathbb{Z}))$ we denote the special automorphism group of F_n.

For an epimorphism $\pi : F_n \to G$ of F_n onto a finite group G we call

$$\Gamma^+(G,\pi) := \{\varphi \in \mathrm{Aut}^+(F_n) \mid \pi\varphi = \pi\}$$

the *standard congruence subgroup of* $\mathrm{Aut}^+(F_n)$ *associated to* G *and* π. These groups are the objects of our study, where we mainly focus on the case $n = 2$. Our most important results are the following.

We fully describe the abelianization of $\Gamma^+(G,\pi) \leq \mathrm{Aut}^+(F_2)$ for abelian and dihedral groups G. We also show that standard congruence subgroups of $\mathrm{Aut}^+(F_2)$ associated to dihedral groups provide a family of subgroups of $\mathrm{Aut}^+(F_2)$ of increasing finite index while each is generated by four elements. This implies that finite index subgroups of $\mathrm{Aut}(F_2)$ cannot be written as free products. Furthermore, we prove that standard congruence subgroups of $\mathrm{Aut}^+(F_2)$ associated to finite non-perfect groups have infinite abelianization.

We are also interested in the images of standard congruence subgroups of $\mathrm{Aut}^+(F_2)$ under the representation ρ. For these we show that $\rho(\Gamma^+(G,\pi)) \leq \mathrm{SL}_2(\mathbb{Z})$ is a congruence subgroup, i.e., it contains a group of the form $\ker(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}))$, whenever G is a finite metacyclic group.

In the last chapter we discuss some open problems on standard congruence subgroups of $\mathrm{Aut}^+(F_2)$ and give suggestions for further research.

Acknowledgements

First of all, I would like to thank my supervisor Dr. Benjamin Klopsch for his valuable support and many inspiring conversations. His very insightful feedback on my work has been a great help to me.

I am also very grateful to my most influential academic teacher, Professor Dr. Fritz Grunewald, who I already met at the very beginning of my undergraduate studies and who still had a strong influence on my work during my doctoral studies. It is very well possible that I would not have been motivated to continue my studies after having finished my Master's degree if he had not been. Professor Grunewald unexpectedly passed away only weeks before I finished my thesis.

I would like to thank my fellow student Dr. Marc Siegmund for many motivating discussions at the early stages of my doctoral studies.

I would also like to thank Dr. Evija Ribnere for a very fruitful collaboration which let to my very first mathematical publication.

I am very grateful to my fellow students Chistian Löffelsend and Dr. Rolf Bienert for proof-reading my thesis and giving critical remarks.

Finally, I would like to thank my family for their non-mathematical support at all stages of my studies.

My doctoral studies were supported by a Thomas Holloway Scholarship.

This work is dedicated to the memory of

Professor Dr. Fritz J. Grunewald
1949 – 2010.

Contents

Declaration **2**

Abstract **3**

Acknowledgements **4**

1 Introduction **8**

1.1 The Notion of Congruence Subgroups of $\mathrm{Aut}(F_n)$ 8

1.2 Main Results 10

1.3 Motivation and Related Results 15

2 Preliminaries **19**

2.1 A Brief Introduction to Presentations 19

2.2 Some Facts on the Automorphism Group of a Free Group 21

2.3 The Product Replacement Graph 22

2.4 A Lemma on Finite Index Subgroups 25

2.5 Some Results on Free Products 26

3 Congruence Subgroups of $\mathrm{SL}_n(\mathbb{Z})$ **31**

3.1 Introduction 31

3.2 The Index of Congruence Subgroups 32

3.3 Free Congruence Subgroups of $\mathrm{SL}_2(\mathbb{Z})$ 36

4 Congruence Subgroups of $\mathrm{Aut}(F_n)$ **40**

4.1 Preliminary Results on Congruence Subgroups of $\mathrm{Aut}(F_n)$ 40

4.1.1 A Reduction Step 41

4.1.2 Connection to the Product Replacement Graph and Dependence on the Presentation 42
4.1.3 First Remarks on the Index 43
4.2 Congruence Subgroups associated to Abelian Groups . . 44
4.2.1 The Index of Congruence Subgroups associated to Abelian Groups 44
4.2.2 Product Replacement Graphs of Abelian Groups . 49
4.2.3 The Abelianization of Congruence Subgroups associated to Abelian Groups 50
4.3 Congruence Subgroups associated to Dihedral Groups . . 52
4.3.1 Index and Generation of Congruence Subgroups associated to Dihedral Groups 52
4.3.2 Product Replacement Graphs of Dihedral Groups 60
4.3.3 The Abelianization of Congruence Subgroups associated to Dihedral Groups 60
4.4 Congruence Subgroups associated to Semidirect Products of Cyclic Groups 68
4.4.1 Index in $\mathrm{Aut}^+(F_2)$ and Image in $\mathrm{SL}_2(\mathbb{Z})$ 69
4.4.2 Product Replacement Graphs of Semidirect Products of Cyclic Groups 85
4.5 Congruence Subgroups associated to Certain Wreath Products 87
4.5.1 Wreath Products of the Form $\mathbb{Z}/m\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}$ . . . 87
4.5.2 Wreath Products of the Form $\mathbb{Z}/p\mathbb{Z} \wr \mathbb{Z}/p\mathbb{Z}$ 94
4.5.3 Product Replacement Graphs of Certain Wreath Products 100
4.6 The Abelianization of Congruence Subgroups associated to Non-Perfect Groups 101

5 Suggestions for Further Research **103**

Chapter 1

Introduction

In this chapter we introduce standard congruence subgroups of the automorphism group of a free group, which are the main objects of our interest. We also briefly describe their connection to congruence subgroups of the special linear group. Then we state our main results and point out connections to results by other authors.

1.1 The Notion of Congruence Subgroups of $\mathrm{Aut}(F_n)$

Let $F_n = \langle x_1, \ldots, x_n \rangle$ be the free group on $n \geq 2$ generators and $\pi : F_n \to G$ be an epimorphism of F_n onto a finite group G. Let R be the kernel of π and

$$\Gamma(R) := \{\varphi \in \mathrm{Aut}(F_n) \mid \varphi(R) = R\}$$

be the subgroup of $\mathrm{Aut}(F_n)$ consisting of those automorphisms that send the kernel of π onto itself. Every $\varphi \in \Gamma(R)$ induces an automorphism of $F_n/R \cong G$. We set

$$\begin{aligned}\Gamma(G,\pi) :=& \{\varphi \in \Gamma(R) \mid \varphi \text{ induces the identity on } F_n/R\} \\ =& \ker(\Gamma(R) \to \mathrm{Aut}(G)).\end{aligned}$$

This is a finite index subgroup of $\mathrm{Aut}(F_n)$. (See Section 4.1.2.) Groups of the form $\Gamma(G,\pi)$ are called *standard congruence subgroups of* $\mathrm{Aut}(F_n)$. A subgroup of $\mathrm{Aut}(F_n)$ containing a standard congruence subgroup is called a *congruence subgroup of* $\mathrm{Aut}(F_n)$.

Note that, by definition, $\Gamma(G,\pi)$ only depends on the kernel of π but not on the particular choice of the epimorphism. It is easily verified that

$$\Gamma(G,\pi) = \{\varphi \in \mathrm{Aut}(F_n) \mid \varphi\pi = \pi\}.$$

Let F_n' be the commutator subgroup of F_n. The automorphism group $\mathrm{Aut}(F_n)$ has a well-known representation

$$\rho : \mathrm{Aut}(F_n) \to \mathrm{Aut}(F_n/F_n') = \mathrm{GL}_n(\mathbb{Z}).$$

See for example [19, Sec. 3.5]. We remark that ρ is onto. The kernel of this representation is denoted by IA_n and called the group of IA_n-*automorphisms* or sometimes also the *classical Torelli group*. (For an interesting generalization see [24].) By a famous result of Nielsen, IA_n is a finitely generated group. Moreover, in the special case $n = 2$, we have

$$\mathrm{IA}_2 = \mathrm{Inn}(F_2).$$

For $n \geq 3$, however, $\mathrm{Inn}(F_n)$ is properly contained in IA_n.

By $\mathrm{Aut}^+(F_n) := \rho^{-1}(\mathrm{SL}_n(\mathbb{Z}))$ we denote the *special automorphism group of* F_n. This is a subgroup of index 2 in $\mathrm{Aut}(F_n)$. We also set

$$\Gamma^+(G, \pi) := \Gamma(G, \pi) \cap \mathrm{Aut}^+(F_n).$$

Groups of this form are called *standard congruence subgroups of* $\mathrm{Aut}^+(F_n)$. Accordingly, a subgroup of $\mathrm{Aut}^+(F_n)$ containing a standard congruence subgroup is called a *congruence subgroup of* $\mathrm{Aut}^+(F_n)$.

If $K \leq F_n$ is a characteristic subgroup of F_n and $\pi : F_n \to F_n/K$ the natural projection, we call

$$\ker(\mathrm{Aut}(F_n) \to \mathrm{Aut}(F_n/K)) = \Gamma(F_n/K, \pi)$$

a *principal congruence subgroup of* $\mathrm{Aut}(F_n)$. If we consider $\mathrm{Aut}^+(F_n)$ instead of $\mathrm{Aut}(F_n)$, we only assume that K is fixed by $\mathrm{Aut}^+(F_n)$. One easily sees that every (standard) congruence subgroup of $\mathrm{Aut}(F_n)$, respectively $\mathrm{Aut}^+(F_n)$, contains a principal congruence subgroup. (See also the discussion in Chapter 5.)

Now we see the analogy to $\mathrm{SL}_n(\mathbb{Z})$: a *principal congruence subgroup of* $\mathrm{SL}_n(\mathbb{Z})$ is a subgroup of the form

$$\ker(\mathrm{SL}_n(\mathbb{Z}) \to \mathrm{SL}_n(\mathbb{Z}/m\mathbb{Z}))$$

and a *congruence subgroup of* $\mathrm{SL}_n(\mathbb{Z})$ is a subgroup containing a principal congruence subgroup. Observe that congruence subgroups of $\mathrm{SL}_n(\mathbb{Z})$ are of finite index.

A classical question is whether every finite index subgroup of $\mathrm{SL}_n(\mathbb{Z})$ is a congruence subgroup. In the 1890's Fricke-Klein [11] showed that the answer is no for $n = 2$. In the 1960's it was proved by Bass-Lazard-Serre [5] and independently by Mennicke [18] that for $n \geq 3$ the answer is yes. More recently it has been shown that every finite index subgroup of $\mathrm{Aut}(F_2)$ is a congruence subgroup, see [4] and [6]. The question whether for $n \geq 3$ every finite index subgroup of $\mathrm{Aut}(F_n)$ is a congruence subgroup is still open.

1.2 Main Results

Let us now state the main results of this thesis. It is our aim to understand the algebraic structure of the standard congruence subgroups of $\mathrm{Aut}^+(F_n)$ and also their images in $\mathrm{SL}_n(\mathbb{Z})$ under the representation $\rho : \mathrm{Aut}(F_n) \to \mathrm{GL}_n(\mathbb{Z})$. Although we prove some results for general $n \in \mathbb{N}$, we mainly focus on the case $n = 2$.

A quite general result that we prove (see Section 4.6) is

Theorem A. [1] *Let G be a finite non-perfect group, i.e., G has non-trivial abelianization and $\pi : F_2 \to G$ be an epimorphism. Then $\Gamma^+(G, \pi)$ has infinite abelianization.*

For certain families of standard congruence subgroups we can, of course, prove more detailed results.

The first family of standard congruence subgroups we consider consists of the ones associated to finite abelian groups, see Section 4.2. For these we prove

Theorem B. [2] *Let G be a finite abelian group.*

(i) Up to conjugation, $\Gamma^+(G, \pi)$ only depends on G but not on the particular epimorphism $\pi : F_n \to G$.

(ii) $[\mathrm{Aut}^+(F_n) : \Gamma^+(G, \pi)] = [\mathrm{SL}_n(\mathbb{Z}) : \rho(\Gamma^+(G, \pi))]$.

[1] This is Theorem 4.55 in Section 4.6.

[2] Parts (i), (ii), (iii) correspond to Theorem 4.5 in Section 4.2.1. Part (iv) is given by Theorem 4.11 in Section 4.2.3.

(iii) *Writing* $G \cong \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z}$ *with* $m_{i+1} \mid m_i$ *for* $1 \leq i \leq n-1$, *the index of* $\Gamma^+(G,\pi)$ *in* $\mathrm{Aut}^+(F_n)$ *is given by*

$$m_1^n \cdots m_{n-1}^n m_n^{n-1} \prod_{j=1}^{n-1} \prod_{p \mid m_j} \left(1 - p^{j-n-1}\right)$$

where the second product runs over all primes p *dividing* m_j.

(iv) *Suppose that* $n = 2$ *and let* $m_1, m_2 \in \mathbb{N}$ *such that* $m_1 \geq 3$, $m_2 \mid m_1$ *and* $(m_1, m_2) \neq (3,1)$. *Moreover, let* $G \cong \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$ *and* $\pi : F_2 \to G$ *be an epimorphism. Then*

$$\Gamma^+(G,\pi)^{\mathrm{ab}} \cong G \times \mathbb{Z}^{1+12^{-1}m_2m_1^2\prod_{p\mid m_1}(1-p^{-2})}$$

where the product runs over all primes p *dividing* m_1.

Furthermore, we have

$$\begin{aligned}
\Gamma^+(\mathbb{Z}/2\mathbb{Z},\pi)^{\mathrm{ab}} &\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}, \\
\Gamma^+(\mathbb{Z}/3\mathbb{Z},\pi)^{\mathrm{ab}} &\cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}, \\
\Gamma^+(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},\pi)^{\mathrm{ab}} &\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^2.
\end{aligned}$$

For $m_1, m_2 \in \mathbb{N}$ let

$$\Gamma(m_1,m_2) := \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \mid a \equiv_{m_1} 1, b \equiv_{m_1} 0,\ c \equiv_{m_2} 0, d \equiv_{m_2} 1\}.$$

This is a finite index subgroup of $\mathrm{SL}_2(\mathbb{Z})$. In fact, it is a congruence subgroup.

A very important tool in the proof of part (iv) is the following generalization of a result of Frasch [10], which we prove in Section 3.3.

Proposition C. [3] *Let* $m_1, m_2 \in \mathbb{N}$ *such that* $m_1 \geq 3$, $m_2 \mid m_1$ *and* $(m_1, m_2) \neq (3,1)$. *Then* $\Gamma(m_1,m_2)$ *is free of rank*

$$1 + \frac{m_2 m_1^2}{12} \prod_{\substack{p \mid m_1 \\ p \text{ prime}}} \left(1 - p^{-2}\right).$$

[3] This is Proposition 3.4 in Section 3.3.

In part (iv) of Theorem B we only consider the case that $n = 2$. Besides the fact that we use Proposition C to prove part (iv), one reason is that, in this case, $\mathrm{IA}_2 = \mathrm{Inn}(F_2) \cong F_2$ so that it is very convenient to use the exact sequence

$$1 \longrightarrow \mathrm{IA}_2 \cap \Gamma^+(G,\pi) \longrightarrow \Gamma^+(G,\pi) \longrightarrow \rho(\Gamma^+(G,\pi)) \longrightarrow 1$$

for our computations. For the same reason, in what follows, we restrict ourselves to considering standard congruence subgroups of $\mathrm{Aut}^+(F_2)$.

As a generalization of abelian groups, one might wish to consider solvable groups. As a first step in this direction, in Section 4.3, we consider dihedral groups.

Theorem D. [4] *Let $n \geq 3$ and D_n be the dihedral group of order $2n$.*

(i) Up to conjugation, $\Gamma^+(D_n,\pi)$ only depends on n, but not on the epimorphism $\pi : F_2 \to D_n$.

(ii) The index of $\Gamma^+(D_n,\pi)$ in $\mathrm{Aut}^+(F_2)$ is $6n$.

(iii) The image $\rho(\Gamma^+(D_n,\pi)) \leq \mathrm{SL}_2(\mathbb{Z})$ is conjugate to $\Gamma(2,1)$ if n is odd and to $\Gamma(2,2)$ if n is even.

(iv) The group $\Gamma^+(D_n,\pi)$ is generated by four elements.

(v) $$\Gamma^+(D_n,\pi)^{\mathrm{ab}} \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^2, & n \text{ odd} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^3, & n \text{ even.} \end{cases}$$

An interesting consequence is

Corollary E. [5] *The special automorphism group $\mathrm{Aut}^+(F_2)$, and hence also $\mathrm{Aut}(F_2)$, has subgroups of arbitrarily large index, generated by four elements. This implies that finite-index subgroups of $\mathrm{Aut}(F_2)$ cannot be written as free products.*

A more general family of finite groups is the one of semidirect products of finite cyclic groups. This is the next class of groups we are going to consider.

[4] Parts (i), (ii), (iii), (iv) correspond to Theorem 4.12 in Section 4.3.1. Part (v) is given by Theorem 4.19 in Section 4.3.3.

[5] This corresponds to Corollary 4.13 and part (ii) of Corollary 4.14 in Section 4.3.1.

We remark that an important ingredient in the proof of parts (iv) and (v) of Theorem D is that, essentially, the image $\rho(\Gamma^+(D_n, \pi))$ in $\mathrm{SL}_2(\mathbb{Z})$ does not depend on n, so that we can determine a presentation for it. When we try to generalize our results to standard congruence subgroups of $\mathrm{Aut}^+(F_2)$ associated to semidirect products of finite cyclic groups, we see that, in this case, the image in $\mathrm{SL}_2(\mathbb{Z})$ can have arbitrarily large index. For this reason the method that we use in the proof of Theorem D does not apply in this case.

Theorem F. [6] *Let $a \in \mathbb{N}$ and $\alpha \in (\mathbb{Z}/a\mathbb{Z})^*$. Consider the group $G := \mathbb{Z}/a\mathbb{Z} \rtimes \langle g \rangle$ where the finite cyclic group $\langle g \rangle$ acts on $\mathbb{Z}/a\mathbb{Z}$ via $\langle g \rangle \to \langle \alpha \rangle$, $g \mapsto \alpha$. Let $a = \prod p^{n_p}$ be the prime factorization of a and let k_p such that $\alpha \in 1 + \prod p^{k_p}(\mathbb{Z}/a\mathbb{Z})^*$. Moreover, let $\pi : F_2 \to G$ be an epimorphism. Then the following holds.*

(i) Up to conjugation, $\Gamma^+(G, \pi)$ only depends on G, but not on the choice of the epimorphism $\pi : F_2 \to G$.

(ii) The index of $\Gamma^+(G, \pi)$ in $\mathrm{Aut}^+(F_2)$ is

$$\frac{a \cdot \mathrm{ord}(\alpha) \cdot \mathrm{ord}(g)^2 \cdot \prod p^{k_p}}{\gcd(\mathrm{ord}(g), \prod p^{k_p})} \cdot \prod (1 - q^{-2})$$

where the very last product runs over all prime numbers q dividing $\mathrm{lcm}(\mathrm{ord}(g), \prod p^{k_p})$.

(iii) The image $\rho(\Gamma^+(G, \pi)) \leq \mathrm{SL}_2(\mathbb{Z})$ is conjugate to $\Gamma(\mathrm{ord}(g), \prod p^{k_p})$. In particular, it is a congruence subgroup.

A nice consequence is given by

Corollary G. [7] *Let G be a finite metacyclic group and $\pi : F_2 \to G$ be an epimorphism. Then $\rho(\Gamma^+(G, \pi))$ is a congruence subgroup.*

This is the most general situation for which we know that the image of a standard congruence subgroup in $\mathrm{SL}_2(\mathbb{Z})$ is congruence. One might wish to generalize this result to metabelian groups. Indeed, computer experiments indicate that it also holds for standard congruence subgroups

[6] This is Theorem 4.24 in Section 4.4.1.

[7] This is Corollary 4.26 in Section 4.4.1

associated to these. As an example, in Section 4.5, we consider certain wreath products of finite cyclic groups. We shall see, however, that, so far, it is not always clear, whether the image in $\mathrm{SL}_2(\mathbb{Z})$ is a congruence subgroup.

Theorem H. [8] *Let m be odd and $m = \prod p^{k_p}$ be its prime factorization.*

(i) Up to conjugation, $\Gamma^+(\mathbb{Z}/m\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}, \pi)$ only depends on m, but not on the particular epimorphism $\pi : F_2 \to \mathbb{Z}/m\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}$.

(ii) The index of $\Gamma^+(\mathbb{Z}/m\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}, \pi)$ in $\mathrm{Aut}^+(F_2)$ is $6m^3 \prod_{p|m}(1-p^{-2})$.

(iii) The image $\rho(\Gamma^+(\mathbb{Z}/m\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}, \pi)) \leq \mathrm{SL}_2(\mathbb{Z})$ is conjugate to $\Gamma(m, 2)$. In particular, it is a congruence subgroup.

The case that m is even is excluded in the above theorem. However, we will show the following.

Theorem I. [9] *Let $k \geq 2$. Then the following holds.*

(i) Up to conjugation, $\Gamma^+(\mathbb{Z}/2^k\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}, \pi)$ only depends on k, but not on the particular epimorphism $\pi : F_2 \to \mathbb{Z}/2^k\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}$.

(ii) The index of $\Gamma^+(\mathbb{Z}/2^k\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}, \pi)$ in $\mathrm{Aut}^+(F_2)$ is $3 \cdot 2^{3k+1}$.

(iii) The image $\rho(\Gamma^+(\mathbb{Z}/2^k\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}, \pi)) \leq \mathrm{SL}_2(\mathbb{Z})$ is conjugate to a subgroup of index 2 in $\Gamma(2^k, 2)$.

Here the case $k = 1$ is excluded. However, in this case, we have $\mathbb{Z}/2\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z} \cong D_4$ so that we can refer to Theorem D.

Moreover, we show

Theorem J. [10] *Let p be an odd prime.*

(i) Up to conjugation, $\Gamma^+(\mathbb{Z}/p\mathbb{Z} \wr \mathbb{Z}/p\mathbb{Z}, \pi)$ only depends on p, but not on the particular epimorphism $\pi : F_2 \to \mathbb{Z}/p\mathbb{Z} \wr \mathbb{Z}/p\mathbb{Z}$.

(ii) The index of $\Gamma^+(\mathbb{Z}/p\mathbb{Z} \wr \mathbb{Z}/p\mathbb{Z}, \pi)$ in $\mathrm{Aut}^+(F_2)$ is $p^{p+2}(p^2+1)$.

[8] This is Theorem 4.43 in Section 4.5.1.
[9] This is Theorem 4.44 in Section 4.5.1.
[10] This is Theorem 4.49 in Section 4.5.2.

(iii) *The image* $\rho(\Gamma^+(\mathbb{Z}/p\mathbb{Z} \wr \mathbb{Z}/p\mathbb{Z}, \pi)) \leq \mathrm{SL}_2(\mathbb{Z})$ *is a subgroup of index* p *in* $\Gamma(p)$.

For all families of finite groups that we consider we also describe the product replacement graphs in terms of the numbers of their connected components and the sizes of these. We remark that for finite abelian groups this is also done by Diaconis and Graham in [7]. However, they use a very different method to find a formula for the size of the product replacement graph. To be concrete, they use abstract Möbius inversion, which was introduced by Hall [13]. We note that our formula for the number of generating n-tuples seems to be much easier to evaluate.

We also prove

Theorem K. *The following classes of finite groups have a unique* T_2*-system.*

- *Semidirect products of two finite cyclic groups.*
- *Wreath products of the form* $\mathbb{Z}/m\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}$ *with* $m \in \mathbb{N}$ *odd.*
- *Wreath products of the form* $\mathbb{Z}/2^k\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}$ *with* $k \geq 2$.
- *Wreath products of the form* $\mathbb{Z}/p\mathbb{Z} \wr \mathbb{Z}/p\mathbb{Z}$ *with* p *an odd prime.*

For details we refer to Sections 4.2.2, 4.3.2, 4.4.2 and 4.5.3. These results imply the uniqueness of $\Gamma^+(G, \pi)$ up to conjugation for the considered classes of finite groups. See Lemma 4.2 in Section 4.1.2.

1.3 Motivation and Related Results

The automorphism group of the free group is a much studied group. For example, the question whether $\mathrm{Aut}(F_n)$ is linear is a very classical problem, which was finally solved in 2002.

The automorphism group $\mathrm{Aut}(F_2)$ is linear. This is, however, not easy to see. In [8] Dyer, Formanek and Grossmann prove that $\mathrm{Aut}(F_2)$ has a faithful representation over $\mathbb{C}$ if and only if the braid group B_4 on four strings does. Krammer shows in [15] that the braid groups B_n indeed have faithful representations over $\mathbb{C}$. In contrast to that, we have the following famous result of Formanek and Procesi, see [9].

G	$[\mathrm{Aut}^+(F_2) : \Delta]$	Δ^{ab}
C_2	3	$\mathbb{Z}^2 \times C_2 \times C_4$
C_3	8	$\mathbb{Z} \times C_3 \times C_3$
C_4	12	$\mathbb{Z}^2 \times C_4$
$C_2 \times C_2$	6	$\mathbb{Z}^2 \times C_2 \times C_2 \times C_2$
C_5	24	$\mathbb{Z}^3 \times C_5$
C_6	24	$\mathbb{Z}^3 \times C_6$
C_7	48	$\mathbb{Z}^5 \times C_7$
D_3	18	$\mathbb{Z}^2 \times C_2$
D_4	24	$\mathbb{Z}^3 \times C_2$
D_5	30	$\mathbb{Z}^2 \times C_2$

Table 1.1: Computational Results by Grunewald and Lubotzky.

Theorem (Formanek, Procesi)**.** *Let F_n be the free group of rank $n \geq 3$ and let $\mathrm{Aut}(F_n)$ be its automorphism group. Then there is no faithful linear representation $\mathrm{Aut}(F_n) \to \mathrm{GL}_m(k)$ for any $m \in \mathbb{Z}$ over any field k.*

The groups $\Gamma(G, \pi)$ have been studied by various authors. For instance, in [12] Grunewald and Lubotzky use the groups $\Gamma(G, \pi)$ to construct linear representations of the automorphism group $\mathrm{Aut}(F_n)$. An interesting result they obtain is that for any two natural numbers $n \geq 2$, $k \geq 1$, there is a finite index subgroup $\Gamma \leq \mathrm{Aut}(F_n)$ and a representation $\Gamma \to \prod_{i=1}^{k} \mathrm{SL}_{(n-1)i}(\mathbb{Z})$ whose image has finite index in $\prod_{i=1}^{k} \mathrm{SL}_{(n-1)i}(\mathbb{Z})$.

In [12, Sec. 9.4] Grunewald and Lubotzky present, for some explicit G of small order and $2 \leq n \leq 4$, the indices of the groups $\Gamma^+(G, \pi)$ in $\mathrm{Aut}^+(F_n)$ and also the abelianizations of the groups $\Gamma^+(G, \pi)$ which they obtain by MAGMA [17] computations. To be precise, they do the following. By a random process they generate elements of $\Gamma^+(G, \pi)$ and collect these in a set until it generates a finite index subgroup Δ of $\mathrm{Aut}^+(F_n)$. The group $\Delta \leq \Gamma^+(G, \pi)$ can be seen as an approximation of $\Gamma^+(G, \pi)$. See Table 1.1 for some of their results in the case $n = 2$. By Theorems B and D we fully explain their experimental results for finite abelian and dihedral groups.

Actually, Grunewald and Lubotzky present computational results for some more finite groups G, e.g., $G = A_5$. In all considered cases $\Gamma^+(G, \pi)$

has infinite abelianization if $n = 2$. For G non-perfect we now know by Theorem A that $\Gamma^+(G,\pi)^{\mathrm{ab}}$ is infinite for every epimorphism $\pi : F_2 \to G$. However, our proof does not work for perfect groups G. Hence we state the following problem.

Does $\Gamma^+(G,\pi) \leq \mathrm{Aut}^+(F_2)$ *have infinite abelianization for every epimorphism* $\pi : F_2 \to G$ *onto a non-trivial finite group* G*?*

The situation in the case $n \geq 3$ looks different. Indeed, Grunewald and Lubotzky show that for every epimorphism $\pi : F_n \to G$ of F_n, $n \geq 3$, onto a finite abelian group G, the group $\Gamma(G,\pi) \leq \mathrm{Aut}(F_n)$ has finite abelianization. This is Proposition 8.5 in [12]. Computational results [12, Sec. 9.4] indicate that $\Gamma^+(G,\pi)$ always has finite abelianization if $n \geq 3$. This leads to the following question.

Does $\Gamma^+(G,\pi) \leq \mathrm{Aut}^+(F_n)$, $n \geq 3$, *have finite abelianization for every epimorphism* $\pi : F_n \to G$ *onto a non-trivial finite group* G*?*

Some results in this thesis are related to results of Satoh [25, 26]. In his papers Satoh considers the kernel $T_{n,m}$ of the composition

$$\mathrm{Aut}(F_n) \xrightarrow{\rho} \mathrm{GL}_n(\mathbb{Z}) \longrightarrow \mathrm{GL}_n(\mathbb{Z}/m\mathbb{Z}).$$

One easily sees that for $m \geq 3$ we have $T_{n,m} = \Gamma^+((\mathbb{Z}/m\mathbb{Z})^n, \pi)$ where $\pi : F_n \to (\mathbb{Z}/m\mathbb{Z})^n$ is the obvious epimorphism. Satoh shows that for $n, m \geq 2$ one has

$$T_{n,m}^{\mathrm{ab}} \cong (\mathrm{IA}_n^{\mathrm{ab}} \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z}) \times \Gamma_n(m)^{\mathrm{ab}}$$

where $\Gamma_n(m)$ denotes the kernel of the natural epimorphism $\mathrm{GL}_n(\mathbb{Z}) \to \mathrm{GL}_n(\mathbb{Z}/m\mathbb{Z})$. Since $\mathrm{IA}_2 = \mathrm{Inn}(F_2)$ is free of rank 2, for $n = 2$ this reads

$$T_{2,m}^{\mathrm{ab}} \cong (\mathbb{Z}/m\mathbb{Z})^2 \times \Gamma_2(m)^{\mathrm{ab}}.$$

Observe that for $m \geq 3$ we have $\Gamma_2(m) = \Gamma(m,m)$. Recalling Proposition C, we see that this result corresponds to our result in Theorem B (iv) for the special case $G = (\mathbb{Z}/m\mathbb{Z})^2$. Satoh also gives the integral homology groups of $T_{2,p}$ for odd primes p. In particular, he shows that

$$\mathrm{H}_1(T_{2,p}, \mathbb{Z}) = (\mathbb{Z}/p\mathbb{Z})^2 \times \mathbb{Z}^{1+12^{-1}p^3(1-p^{-2})}.$$

Since the first integral homology group is actually the abelianization, this corresponds to our result in Theorem B (iv) for the special case $G = (\mathbb{Z}/p\mathbb{Z})^2$.

Finally we remark that some results that were obtained in a collaboration of Ribnere and the author have been published in the joint paper [3].

Chapter 2

Preliminaries

In this chapter we provide background material and results that we need later on. In particular, in Section 2.5 we prove some combinatorial results on the minimal number of generators of finite-index subgroups of free products, which we use to prove Corollary E.

2.1 A Brief Introduction to Presentations

In this thesis we frequently make use of presentations of groups, that is, describing a group in terms of generators and relations. We therefore give a brief introduction to these methods.

Let G be a group. Then there exist a free group F and an epimorphism $\pi : F \to G$. Such an epimorphism is called a *presentation* of the group G. By R we denote the kernel of π so that $F/R \cong G$. The elements of R are called *relators* of the presentation π. Let $Y \subseteq F$ be a set of free generators of F. Moreover, let $S \subseteq R$ be a subset of R such that $\langle S \rangle^F = R$, where $\langle S \rangle^F$ denotes the normal closure of S in F. Note that $\pi(Y)$ generates the group G. The sets Y and S now provide sets of *generators* and *defining relators*, respectively. We write this as

$$G = \langle Y \mid S \rangle.$$

We can thus think of G as the group consisting of all words in the elements of Y and their inverses where a word represents the identity element of G if and only if it can be written as a product of conjugates of the elements of S and their inverses.

Very often it is more convenient to list the elements of $X := \pi(Y) \subseteq G$ rather than the ones of $Y \subseteq F$. Instead of the set S we then use the set of words $\{s(X) \mid s \in S\}$, obtained by formally replacing the generators

of F by their images under π, that is, if $s = \prod_{i=1}^{n} y_i^{\varepsilon_i}$ where $y_i \in Y$ and $\varepsilon_i \in \{-1, 1\}$, then $s(X)$ is the word $\prod_{i=1}^{n} \pi(y_i)^{\varepsilon_i}$. Sometimes we also write $s(X) = 1$ instead of just $s(X)$. An expression of the form $s(X) = 1$ is called a *defining relation* of G. More generally, if $a, b \in X$, then the expression $a = b$ is called a (defining) relation of G if ab^{-1} is a (defining) relator of G.

A group G is called *finitely generated* if there exists a presentation $G = \langle Y \mid S \rangle$ with Y finite, that is, there exists an epimorphism of a free group of finite rank onto G. If G admits a presentation $G = \langle Y \mid S \rangle$ where Y and S are finite, we say that G is *finitely presented*. Note that subgroups and quotients of a finitely presented group need not necessarily be finitely presented. However, the class of finitely presented groups is closed under taking finite index subgroups and under taking extensions. In the former case one can use the Reidemeister-Schreier method [19, Sec. 2.3] to obtain a presentation, in the latter case one can use the following

Proposition 2.1 (Hall)**.** *Let G be a group such that G is an extension of H by N, that is, we have an exact sequence of groups*

$$1 \longrightarrow N \longrightarrow G \xrightarrow{\pi} H \longrightarrow 1.$$

Suppose we have finite presentations of N and H given by

$$N = \langle n_1, \ldots, n_r \mid R_1(\boldsymbol{n}), \ldots, R_k(\boldsymbol{n}) \rangle,$$
$$H = \langle h_1, \ldots, h_s \mid W_1(\boldsymbol{h}), \ldots, W_l(\boldsymbol{h}) \rangle.$$

For $1 \leq i \leq s$ let $g_i \in \pi^{-1}(h_i)$. Then there are words V_{ij} and $\widetilde{W}_i$ for $1 \leq i \leq s$, $1 \leq j \leq r$ such that $g_i n_j g_i^{-1} = V_{ij}(\boldsymbol{n})$ and $W_i(\boldsymbol{g}) = \widetilde{W}_i(\boldsymbol{n})$. Moreover, a presentation of G is given by

$$\begin{aligned} G = \langle n_1, \ldots, n_r, g_1, \ldots, g_s \mid & R_1(\boldsymbol{n}), \ldots, R_k(\boldsymbol{n}), \\ & g_i n_j g_i^{-1} = V_{ij}(\boldsymbol{n}), \\ & W_i(\boldsymbol{g}) = \widetilde{W}_i(\boldsymbol{n}) \rangle. \end{aligned}$$

This result can be found in [14, Chap. 13].

Let us mention a warning which can also be found there. Suppose we have a finite presentation $G = \langle x_1, \ldots, x_n \mid \boldsymbol{R}(x_1, \ldots, x_n) = 1 \rangle$ where $\boldsymbol{R}$

is a collection of defining relators. If we have another set of generators $y_1, \ldots, y_m$ such that we can express $x_i = w_i(\boldsymbol{y})$, then it is a common error to conclude that $G = \langle y_1, \ldots, y_m \mid \boldsymbol{R}(w_1(\boldsymbol{y}), \ldots, w_n(\boldsymbol{y})) = 1\rangle$. The following lemma, which can be proved through Tietze transformations, gives the correct presentation.

Lemma 2.2. *Let $G = \langle x_1, \ldots, x_n \mid \boldsymbol{R}(x_1, \ldots, x_n) = 1\rangle$ be a finite presentation of the group G. Suppose that $y_1, \ldots, y_m$ yields a set of generators of G such that*

$$x_i = w_i(y_1, \ldots, y_m),$$
$$y_j = v_j(x_1, \ldots, x_n).$$

Then G admits a presentation

$$G = \langle y_1, \ldots, y_m \mid \boldsymbol{R}(w_1(\boldsymbol{y}), \ldots, w_n(\boldsymbol{y})) = 1,\ y_j = v_j(w_1(\boldsymbol{y}), \ldots, w_n(\boldsymbol{y}))\rangle.$$

2.2 Some Facts on the Automorphism Group of a Free Group

Let $n \geq 2$ and $F_n = \langle x_1, \ldots, x_n\rangle$ be the free group on n generators. Following the notation of [19, Sec. 3.5], we consider the elementary automorphisms

$$U_{i,k} = \Big\{ x_i \mapsto x_i x_k \qquad\qquad V_{i,k} = \Big\{ x_i \mapsto x_k x_i$$

$$P_{i,k} = \begin{cases} x_i \mapsto x_k \\ x_k \mapsto x_i \end{cases} \qquad\qquad \sigma_i = \Big\{ x_i \mapsto x_i^{-1}$$

where $1 \leq i, k \leq n,\ i \neq k$ and values not given are identical to the argument, e.g., $\sigma_i(x_k) = x_k$.

It is a well-known result of Nielsen that $\mathrm{Aut}(F_n)$ is generated by these elementary automorphisms. See for example [19, Sec. 3.5]. Moreover, $\mathrm{Aut}^+(F_n)$ is generated by the automorphisms $U_{i,k}$ and $V_{i,k}$.

For an element $w \in F_n$ we let $\alpha_w \in \mathrm{Inn}(F_n)$ be the inner automorphism of F_n given by conjugation with w, that is, $\alpha_w(z) = wzw^{-1}$ for all $z \in F_n$. Note that $\mathrm{Inn}(F_n) \cong F_n$ is free on $\alpha_{x_1}, \ldots, \alpha_{x_n}$.

We now use the fact that the group $\mathrm{Aut}^+(F_2)$ is an extension of $\mathrm{IA}_2 = \mathrm{Inn}(F_2)$ by $\mathrm{SL}_2(\mathbb{Z})$, i.e., we use the exact sequence

$$1 \longrightarrow \mathrm{IA}_2 \longrightarrow \mathrm{Aut}^+(F_2) \xrightarrow{\rho} \mathrm{SL}_2(\mathbb{Z}) \longrightarrow 1$$

to determine a finite presentation of $\mathrm{Aut}^+(F_2)$. The group IA_2 is free on α_x and α_y. The group $\mathrm{SL}_2(\mathbb{Z})$ has the well-known presentation

$$\mathrm{SL}_2(\mathbb{Z}) = \langle a, b \mid a^4 = 1, a^2 = b^3 \rangle$$

as an amalgamated product. Here we can identify a with $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ and b with $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 1 \end{smallmatrix}\right)$. For our purpose, however, it is more convenient to have a presentation in the generators $e_1 = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ and $e_2 = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Using Tietze transformations, one finds the presentation

$$\mathrm{SL}_2(\mathbb{Z}) = \langle e_1, e_2 \mid e_2 e_1^{-1} e_2 e_1 e_2^{-1} e_1, (e_2 e_1^{-1} e_2)^4 \rangle.$$

These transformations are carried out in [24, Prop. 1.2]. Observe that preimages of e_1 and e_2 under ρ are given by

$$u = \begin{cases} x \mapsto xy \\ y \mapsto y \end{cases} \quad \text{and} \quad v = \begin{cases} x \mapsto x \\ y \mapsto xy \end{cases},$$

respectively. Using Proposition 2.1 of Hall, we compute the following presentation.

$$\begin{aligned} \mathrm{Aut}^+(F_2) = \langle \alpha_x, \alpha_y, u, v \mid \quad & u\alpha_x u^{-1} = \alpha_x \alpha_y, \quad u\alpha_y u^{-1} = \alpha_y, \\ & v\alpha_x v^{-1} = \alpha_x, \qquad v\alpha_y v^{-1} = \alpha_x \alpha_y, \\ & vu^{-1} vuv^{-1} u = 1, \\ & (vu^{-1} v)^4 = \alpha_x \alpha_y^{-1} \alpha_x^{-1} \alpha_y \qquad \rangle. \end{aligned}$$

This presentation is used in our MAGMA computations.

2.3 The Product Replacement Graph

Standard congruence subgroups of $\mathrm{Aut}^+(F_n)$ are closely connected to product replacement graphs of finite groups. We shall describe this connection in Section 4.1.2. Let us now explain the construction of these graphs and present some facts that we need later. A good survey on the product replacement graph is given by [21].

For a finitely generated group G we denote by $\mathrm{d}(G)$ the minimal number of generators of G.

Let G be a finite group, $n \geq \mathrm{d}(G)$ and

$$\mathbf{V}_n(G) := \{(g_1, \ldots, g_n) \in G \times \cdots \times G \mid \langle g_1, \ldots, g_n \rangle = G\}$$

be the set of all generating n-tuples of G. On the set $\mathbf{V}_n(G)$ one defines the so called *elementary Nielsen moves*, given by

$$(g_1, \ldots, g_i, \ldots, g_n) \longrightarrow (g_1, \ldots, g_{i-1}, g_i g_j^{\pm 1}, g_{i+1}, \ldots, g_n)$$
$$(g_1, \ldots, g_i, \ldots, g_n) \longrightarrow (g_1, \ldots, g_{i-1}, g_j^{\pm 1} g_i, g_{i+1}, \ldots, g_n)$$

with $1 \leq i, j \leq n$, $i \neq j$. (Comparing these with the generators of $\mathrm{Aut}^+(F_n)$ given in Section 2.2, one already sees a connection between the product replacement graph and $\mathrm{Aut}^+(F_n)$.) The product replacement graph of G is the graph with vertex set $\mathbf{V}_n(G)$ where two vertices are connected by an edge if and only if one can be obtained from the other through an elementary Nielsen move. By a *Nielsen move* we refer to a finite sequence of elementary Nielsen moves. For brevity, we also denote the product replacement graph by $\mathbf{V}_n(G)$.

It is a natural problem to consider the number and the sizes of the connected components of $\mathbf{V}_n(G)$. For this purpose, an important and classical tool is given by

Proposition 2.3 (Higman)**.** *Let G be a group such that $\mathrm{d}(G) \leq 2$. If (g, h) and $(g', h') \in \mathbf{V}_2(G)$ lie in the same connected component of $\mathbf{V}_2(G)$, then the commutators $[g, h]$ and $[g', h']$ are conjugate.*

In other words, the conjugacy class of $[g, h]$ is invariant under Nielsen moves. This result can quickly be verified by considering the elementary Nielsen moves. Using this, we may formulate the following

Definition 2.4. Let G be a group such that $\mathrm{d}(G) \leq 2$. The *Higman invariant* of the connected component of $\mathbf{V}_2(G)$ containing the pair (g, h) is given by the conjugacy class of $[g, h]$ in G. ◇

Another important result is

Theorem 2.5 (Lubotzky, Pak)**.** *If $\alpha : G \to H$ is an epimorphism between finite groups, then for every $n \geq \mathrm{d}(G)$ the induced map $\mathbf{V}_n(G) \to \mathbf{V}_n(H)$ given by $(g_1, \ldots, g_n) \mapsto (\alpha(g_1), \ldots, \alpha(g_n))$ is a surjective graph projection. In particular, the number of connected components of $\mathbf{V}_n(H)$ is bounded by that of $\mathbf{V}_n(G)$.*

This is Theorem 2.1.4 in [21]. It is an immediate consequence of the following result, which is Lemma 2.1.5 in [21].

Lemma 2.6 (Gaschütz-Lemma)**.** *Let $\alpha : G \to H$ be an epimorphism between finite groups, $n \geq \mathrm{d}(G)$ and let $(h_1, \ldots, h_n)$ be a generating n-tuple of H. Then there exists a generating n-tuple $(g_1, \ldots, g_n)$ of G with $\alpha(g_i) = h_i$ for $1 \leq i \leq n$.*

In the above situation we call $(g_1, \ldots, g_n)$ a *lift* of $(h_1, \ldots, h_n)$. Using this lemma, we also find

Lemma 2.7. *Let $\alpha : G \to H$ be an epimorphism between finite groups. Moreover, let $n \geq \mathrm{d}(G)$ and $(h_1, \ldots, h_n)$, $(h'_1, \ldots, h'_n) \in \mathbf{V}_n(H)$. If the tuples $(h_1, \ldots, h_n)$ and $(h'_1, \ldots, h'_n)$ lie in the same connected component of $\mathbf{V}_n(H)$, then both tuples have the same number of lifts to $\mathbf{V}_n(G)$.*

Proof. It suffices to show that if the tuple $(h'_1, \ldots, h'_n)$ can be obtained from $(h_1, \ldots, h_n)$ by an elementary Nielsen move, both tuples have the same number of lifts to $\mathbf{V}_n(G)$. Then the lemma follows by induction. Let us consider the case that

$$(h'_1, \ldots, h'_i, \ldots h'_n) = (h_1, \ldots, h_{i-1}, h_i h_j, h_{i+1} \ldots, h_n).$$

The argument for the other elementary Nielsen moves is the same. If $(g_1, \ldots, g_n) \in \mathbf{V}_n(G)$ is a lift of $(h_1, \ldots, h_n)$, then $(g_1, \ldots, g_i g_j, \ldots, g_n)$ is a lift of $(h'_1, \ldots, h'_n)$. Conversely, if $(g'_1, \ldots, g'_n)$ is a lift of $(h'_1, \ldots, h'_n)$, then $(g'_1, \ldots, g'_i g'^{-1}_j, \ldots, g'_n)$ is a lift of $(h_1, \ldots, h_n)$. We thus obtain a bijection between the sets of lifts of $(h_1, \ldots, h_n)$ and those of $(h'_1, \ldots, h'_n)$. □

A notion which is closely connected to the product replacement graph is the notion of *T_n-systems*. One way to introduce T_n-systems is the following. Let G be a finite group and $n \geq \mathrm{d}(G)$. Moreover, let $(g_1, \ldots, g_n) \in$

$\mathbf{V}_n(G)$. Then the T_n-system of G, represented by $(g_1, \ldots, g_n)$, is the set of all n-tuples

$$(\alpha(g_1'), \ldots, \alpha(g_n')) \in \mathbf{V}_n(G)$$

where $(g_1', \ldots, g_n')$ runs through the connected component of $(g_1, \ldots, g_n)$ in $\mathbf{V}_n(G)$ and α runs through $\mathrm{Aut}(G)$. The following is easily verified.

Lemma 2.8. *Let G be a finite group and $n \geq \mathrm{d}(G)$. If G has only one T_n-system, then all connected components of $\mathbf{V}_n(G)$ have the same size.*

2.4 A Lemma on Finite Index Subgroups

The following result is well-known.

Lemma 2.9. *Let G be a group and $H, N \leq G$ subgroups of G such that N is normal in G. If H has finite index in G, then we have*

$$[G : H] = [N : N \cap H] \cdot [G/N : HN/N].$$

Proof. Clearly we have $[G : N] = [G : HN] \cdot [HN : N]$ so that

$$[G : HN] = \frac{[G : N]}{[HN : N]} = [G/N : HN/N].$$

Furthermore, one easily sees that the map $N/(H \cap N) \to HN/H$ induced by the inclusion $N \hookrightarrow HN$ is bijective. Hence

$$[N : H \cap N] = [HN : H].$$

Finally, observe that $[G : H] = [G : HN] \cdot [HN : H]$. From the above we now obtain the desired result. □

One can visualize this result by the diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \longrightarrow & G & \longrightarrow & G/N & \longrightarrow & 1 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 1 & \longrightarrow & N \cap H & \longrightarrow & H & \longrightarrow & HN/N & \longrightarrow & 1 \end{array}$$

where all homomorphisms are the obvious ones. The lemma says that if H has finite index in G, then this index is just the product of the index on the left and the index on the right.

2.5 Some Results on Free Products

Let us state two useful results on free products of groups. A good reference is given by [23, Chap. 6].

Theorem 2.10 (Grushko-Neumann Theorem)**.** *If F is a finitely generated free group and π is an epimorphism from F onto the free product of groups G_i where i runs over an index set I, then F is the free product of groups F_i, $i \in I$, such that $\pi(F_i) = G_i$.*

As before, for a finitely generated group G let $\mathrm{d}(G)$ denote the minimal number of generators of G. Using the above result, we prove

Lemma 2.11. *Let $G = G_1 * \cdots * G_k$ be the free product of the non-trivial groups G_i.*

(i) If the groups G_i are finitely generated, then $\mathrm{d}(G) = \mathrm{d}(G_1) + \cdots + \mathrm{d}(G_k)$. In particular, $\mathrm{d}(G) \geq k$.

(ii) If G is finitely generated, then so is each group G_i.

Proof. Let us consider part (i). Certainly it is true for free products of free groups. The group G is the homomorphic image of a free group F of rank $\mathrm{d}(G)$, say $\pi(F) = G$. By Theorem 2.10, $F = F_1 * \cdots * F_k$, where $\pi(F_i) = G_i$. Hence $\mathrm{d}(G_1) + \cdots + \mathrm{d}(G_k) \leq \mathrm{d}(G)$. On the other hand, the disjoint union of minimal generating sets of the G_i forms a generating set of G of size $\mathrm{d}(G_1) + \cdots + \mathrm{d}(G_k)$ so that $\mathrm{d}(G) \leq \mathrm{d}(G_1) + \cdots + \mathrm{d}(G_k)$. This proves part (i).

Part (ii) follows since each factor of G is a homomorphic image of G. □

Sometimes part (i) of the above lemma is also referred to as the Grushko Theorem.

Theorem 2.12 (Kurosh Subgroup Theorem)**.** *Let G be the free product of groups G_i, where i runs over an index set I. Let H be a subgroup of G. Then H is the free product of a (possibly trivial) free group F together with the factors $H \cap (d_i G_i d_i^{-1})$ where i varies over I and d_i varies over an (H, G_i)-double coset representative system of G.*

Furthermore, if H has finite index m in G, then the rank of F is $\sum_{i\in I}(m-m_i)+1-m$ where m_i is the number of (H,G_i)-double cosets in G.

From this we obtain

Proposition 2.13. *Let G be the free product of finitely generated non-trivial groups*

$$G = G_1 * \cdots * G_n * G_{n+1} * \cdots * G_k$$

where for $1 \le j \le n$ the groups G_j are of finite order g_j, respectively, and for $n+1 \le j \le k$ the groups G_j are infinite. Suppose that $H \le G$ is a subgroup of finite index m in G. Then $\mathrm{d}(H) \ge (k-1-\sum_{j=1}^{n} g_j^{-1})m+1$.

Proof. Let $R = \{r_1, \ldots, r_m\}$ be a set of representatives for $H\backslash G$. For each j we wish to determine the cardinality of a set $D_j \subseteq R$ of (H,G_j)-double coset representatives in G, i.e., we wish to determine the cardinality of $(H\backslash G)/G_j$. Thus we need to consider the action of G_j on $H\backslash G$ by multiplication from the right and find the number of orbits.

First we consider the finite groups G_j, $1 \le j \le n$. Note that each G_j-orbit in $H\backslash G$ has length dividing g_j. For $1 \le j \le n$ and $l \mid g_j$ we thus set

$$D_j^l := \{r_i \in R \mid Hr_i \text{ has } G_j\text{-orbit length } l\}.$$

We can now obtain an (H,G_j)-double coset representative system D_j by choosing exactly $|D_j^l|/l$ elements from each set D_j^l, namely one representative for each G_j-orbit. Hence we have

$$|D_j| = \sum_{l\mid g_j} |D_j^l|/l. \tag{2.1}$$

Observe that

$$\begin{aligned} & d_j \in D_j^l \text{ with } l \ne g_j \\ \Leftrightarrow\quad & Hd_j \cdot g = Hd_j \text{ for some } g \in G_j \setminus \{1\} \\ \Leftrightarrow\quad & d_j g d_j^{-1} \in H \text{ for some } g \in G_j \setminus \{1\} \\ \Leftrightarrow\quad & H \cap d_j G_j d_j^{-1} \ne 1. \end{aligned}$$

Hence, as d_j varies over D_j, we obtain exactly

$$\sum_{\substack{l\mid g_j \\ l\ne g_j}} |D_j^l|/l$$

non-trivial groups of the form $H \cap d_j G_j d_j^{-1}$ for $1 \leq j \leq n$.

Now we consider the infinite groups G_j, $n+1 \leq j \leq k$. For each j we choose a set D_j of (H, G_j)-double coset representatives. Let $d_j \in D_j$. Since G_j is infinite, but Hd_j has orbit length at most m, we see that there is some non-trivial $g \in G_j$ such that $Hd_j \cdot g = Hd_j$, that is, $d_j g d_j^{-1} \in H$. Hence $H \cap d_j G_j d_j^{-1}$ is non-trivial for every $d_j \in D_j$. So the number of non-trivial groups of the form $H \cap d_j G_j d_j^{-1}$ as d_j varies over D_j is just $|D_j|$ for $n+1 \leq j \leq k$.

By the Kurosh Subgroup Theorem, H is the free product of a free group of rank $\sum_{j=1}^{k}(m - |D_j|) + 1 - m$ and the factors $H \cap (d_j G_j d_j^{-1})$ where $1 \leq j \leq k$ and d_j varies over D_j. By part (i) of Lemma 2.11, we have $\mathrm{d}(H) \geq N$ where

$$N = \sum_{j=1}^{k}(m - |D_j|) + 1 - m + \sum_{j=1}^{n} \sum_{\substack{l | g_j \\ l \neq g_j}} |D_j^l|/l + \sum_{j=n+1}^{k} |D_j|$$

$$= (k-1)m + 1 + \sum_{j=1}^{n}(-|D_j| + \sum_{\substack{l | g_j \\ l \neq g_j}} |D_j^l|/l).$$

Since $D_j^l \subseteq R$ and $|R| = m$, we find for $1 \leq j \leq n$ that

$$-|D_j| + \sum_{\substack{l | g_j \\ l \neq g_j}} |D_j^l|/l \overset{(2.1)}{=} -g_j^{-1}|D_j^{g_j}| \geq -g_j^{-1}m.$$

Hence

$$N \geq (k - 1 - \sum_{j=1}^{n} g_j^{-1})m + 1$$

as we have claimed. □

With the above notation we have

$$k - 1 - \sum_{j=1}^{n} g_j^{-1} = (k-n) + n - 1 - \sum_{j=1}^{n} g_j^{-1} \geq k - n - 1 + \sum_{j=1}^{n} \left(1 - g_j^{-1}\right).$$

One easily verifies that this expression is positive whenever G is a free product with at least two non-trivial factors such that $G \ncong C_2 * C_2$.

Indeed, we then have

$$k - n - 1 + \sum_{j=1}^{n} \left(1 - g_j^{-1}\right) \geq \frac{1}{6}.$$

This leads to

Corollary 2.14. *Let G be a free product of finitely generated groups with at least two non-trivial factors such that $G \ncong C_2 * C_2$. Then there is some $c = c(G) \geq 1/6$ such that if $H \leq G$ is a subgroup of finite index m in G, then $\mathrm{d}(H) \geq cm + 1$.*

Note that the group $C_2 * C_2 \cong D_\infty \cong \mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$, which is excluded in the above result, indeed behaves differently: for $m \in \mathbb{N}$, it contains the subgroup $m\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ of index m, generated by two elements.

For specific free products we can, of course, find a better bound. Using the well-known fact that $\mathrm{PSL}_2(\mathbb{Z}) \cong C_2 * C_3$, Proposition 2.13 yields

Example 2.15. If H is a subgroup of finite index m in $\mathrm{PSL}_2(\mathbb{Z})$, then $\mathrm{d}(H) \geq m/5 + 1$.

We can generalize Proposition 2.13 as follows.

Corollary 2.16. *Let G be the free product as in Proposition 2.13. Suppose that $\widetilde{G}$ is a group such that there is an epimorphism of $\widetilde{G}$ onto G with finite kernel K. If $H \leq \widetilde{G}$ is a subgroup of finite index m in $\widetilde{G}$, then $\mathrm{d}(H) \geq (k - 1 - \sum_{j=1}^{n} g_j^{-1})m/|K| + 1$.*

Proof. Let $\varepsilon : \widetilde{G} \to G$ be an epimorphism with finite kernel K. Then we have the following commutative diagram with exact rows.

$$\begin{array}{ccccccccc}
1 & \longrightarrow & K & \longrightarrow & \widetilde{G} & \xrightarrow{\varepsilon} & G & \longrightarrow & 1 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
1 & \longrightarrow & H \cap K & \longrightarrow & H & \xrightarrow{\varepsilon} & \varepsilon(H) & \longrightarrow & 1
\end{array}$$

Let $c := [K : H \cap K]$. Then clearly $c \leq |K|$. By Lemma 2.9 we see that $[G : \varepsilon(H)] = m/c$. By Proposition 2.13 it follows that the minimal number of generators for $\varepsilon(H)$ is at least $(n - 1 - \sum_{j=1}^{n} g_j^{-1})m/c + 1 \geq (n - 1 - \sum_{j=1}^{n} g_j^{-1})m/|K| + 1$. Since H maps onto $\varepsilon(H)$, the same lower bound for the number of generators also holds for H. □

Here we give the following application.

Example 2.17. If H is a subgroup of finite index m in $\mathrm{SL}_2(\mathbb{Z})$, then $\mathrm{d}(H) \geq m/10 + 1$.

Corollary 2.18. *For a fixed number of generators we cannot obtain subgroups of arbitrary large finite index in* $\mathrm{SL}_2(\mathbb{Z})$.

The above result also implies that for every $n \in \mathbb{N}$ the set

$$\{H \leq \mathrm{SL}_2(\mathbb{Z}) \mid [\mathrm{SL}_2(\mathbb{Z}) : H] < \infty,\ \mathrm{d}(H) \leq n\}$$

is finite.

Chapter 3

Congruence Subgroups of $\mathrm{SL}_n(\mathbb{Z})$

In this chapter we consider the congruence subgroups $\Gamma_n(m_1, \ldots, m_n)$ of $\mathrm{SL}_n(\mathbb{Z})$ to be defined below and determine their indices in $\mathrm{SL}_n(\mathbb{Z})$. In the special case $n = 2$ we also determine their algebraic structure.

3.1 Introduction

Let $n, m_1, \ldots, m_n \in \mathbb{N}$. Then we write

$$\Gamma_n(m_1, \ldots, m_n) := \{(a_{ij}) \in \mathrm{SL}_n(\mathbb{Z}) \mid a_{ij} \equiv \delta_{i,j} \mod m_i\}$$

where $\delta_{i,j}$ denotes the Kronecker symbol, i.e., $\delta_{i,j} = 1$ if $i = j$ and $\delta_{i,j} = 0$ otherwise. It is an easy exercise to show that this defines a subgroup of $\mathrm{SL}_n(\mathbb{Z})$. For $m \in \mathbb{N}$, the group $\Gamma_n(m, \ldots, m)$ is called the *principal congruence subgroup of level m in* $\mathrm{SL}_n(\mathbb{Z})$. It is the kernel of the natural epimorphism $\mathrm{SL}_n(\mathbb{Z}) \to \mathrm{SL}_n(\mathbb{Z}/m\mathbb{Z})$.

In the case $n = 2$ we shall write $\Gamma(m_1, m_2)$ instead of $\Gamma_2(m_1, m_2)$. Moreover, it is common to use the following notation. For $m \in \mathbb{N}$ let

$$\begin{aligned}
\Gamma^0(m) &:= \{A \in \mathrm{SL}_2(\mathbb{Z}) \mid A \equiv \left(\begin{smallmatrix} * & 0 \\ * & * \end{smallmatrix}\right) \mod m\},\\
\Gamma^1(m) &:= \Gamma(m,1) = \{A \in \mathrm{SL}_2(\mathbb{Z}) \mid A \equiv \left(\begin{smallmatrix} 1 & 0 \\ * & * \end{smallmatrix}\right) \mod m\},\\
\Gamma(m) &:= \Gamma(m,m) = \{A \in \mathrm{SL}_2(\mathbb{Z}) \mid A \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \mod m\}.
\end{aligned}$$

Note that actually

$$\Gamma^1(m) = \{A \in \mathrm{SL}_2(\mathbb{Z}) \mid A \equiv \left(\begin{smallmatrix} 1 & 0 \\ * & 1 \end{smallmatrix}\right) \mod m\}.$$

One also considers the congruence subgroups

$$\begin{aligned}
\Gamma_0(m) &:= \{A \in \mathrm{SL}_2(\mathbb{Z}) \mid A \equiv \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \mod m\},\\
\Gamma_1(m) &:= \Gamma(1,m) = \{A \in \mathrm{SL}_2(\mathbb{Z}) \mid A \equiv \left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right) \mod m\}
\end{aligned}$$

which are conjugate to $\Gamma^0(m)$ and $\Gamma^1(m)$ in $\mathrm{SL}_2(\mathbb{Z})$ via the matrix $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, respectively.

We shall write $\mathrm{P}\Gamma^0(m)$, $\mathrm{P}\Gamma^1(m)$, $\mathrm{P}\Gamma(m)$, $\mathrm{P}\Gamma_0(m)$ and $\mathrm{P}\Gamma_1(m)$ for the images of $\Gamma^0(m)$, $\Gamma^1(m)$, $\Gamma(m)$, $\Gamma_0(m)$ and $\Gamma_1(m)$, respectively, in $\mathrm{PSL}_2(\mathbb{Z})$ under the natural projection $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{PSL}_2(\mathbb{Z})$.

The above congruence subgroups are very useful for our purpose, since, as one easily verifies, for the obvious epimorphism $\pi : F_n \to \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z}$, we have

$$\rho(\Gamma^+(\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z}, \pi)) = \Gamma_n(m_1, \ldots, m_n)$$

where $\rho : \mathrm{Aut}(F_n) \to \mathrm{GL}_n(\mathbb{Z})$ is the representation introduced in Section 1.1. Conversely, since $\mathrm{IA}_n \leq \Gamma^+(\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z}, \pi)$, we have

$$\rho^{-1}(\Gamma_n(m_1, \ldots, m_n)) = \Gamma^+(\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z}, \pi).$$

3.2 The Index of Congruence Subgroups

It is our aim to prove the following formula.

Proposition 3.1. *Let $n, m_1, \ldots, m_n \in \mathbb{N}$ such that $m_{i+1} \mid m_i$ for all $1 \leq i \leq n-1$. Then*

$$[\mathrm{SL}_n(\mathbb{Z}) : \Gamma_n(m_1, \ldots, m_n)] = m_1^n \cdots m_{n-1}^n m_n^{n-1} \prod_{j=1}^{n-1} \prod_{p \mid m_j} \left(1 - p^{j-n-1}\right)$$

where the second product runs over all primes p dividing m_j.

Note that some of the m_i in the above proposition may very well be equal to 1. In Section 4.2 we will also give a formula for the index of $\Gamma(m_1, m_2)$ in $\mathrm{SL}_2(\mathbb{Z})$ without assuming that $m_2 \mid m_1$.

Before we prove this result, we need to show the following.

Lemma 3.2. *Let $n, m \in \mathbb{N}$. Then*

$$|\operatorname{GL}_n(\mathbb{Z}/m\mathbb{Z})| = m^{n^2} \prod_{\substack{p \mid m \\ p \text{ prime}}} \prod_{j=1}^{n} \left(1 - p^{-j}\right)$$

$$\textit{and} \quad |\operatorname{SL}_n(\mathbb{Z}/m\mathbb{Z})| = m^{n^2-1} \prod_{\substack{p \mid m \\ p \text{ prime}}} \prod_{j=2}^{n} \left(1 - p^{-j}\right).$$

Proof. If $m = p_1^{e_1} \cdots p_k^{e_k}$ is the prime factorization of m, we have

$$\operatorname{GL}_n(\mathbb{Z}/m\mathbb{Z}) \cong \operatorname{GL}_n(\mathbb{Z}/p_1^{e_1}\mathbb{Z}) \times \cdots \times \operatorname{GL}_n(\mathbb{Z}/p_k^{e_k}\mathbb{Z})$$

and the analogous result also holds for $\operatorname{SL}_n(\mathbb{Z}/m\mathbb{Z})$. Hence is suffices to consider the case where $m = p^e$ is a prime power. We first prove the result for $\operatorname{GL}_n(\mathbb{Z}/p^e\mathbb{Z})$, using induction on e.

Since $\mathbb{Z}/p\mathbb{Z}$ is a field, we easily see

$$|\operatorname{GL}_n(\mathbb{Z}/p\mathbb{Z})| = \prod_{j=1}^{n} (p^n - p^{n-j}) = p^{n^2} \prod_{j=1}^{n} \left(1 - p^{-j}\right).$$

Now suppose we already know that

$$|\operatorname{GL}_n(\mathbb{Z}/p^e\mathbb{Z})| = p^{en^2} \prod_{j=1}^{n} \left(1 - p^{-j}\right).$$

Consider the exact sequence

$$1 \longrightarrow K_e \longrightarrow \operatorname{GL}_n(\mathbb{Z}/p^{e+1}\mathbb{Z}) \longrightarrow \operatorname{GL}_n(\mathbb{Z}/p^e\mathbb{Z}) \longrightarrow 1$$

induced by the natural projection $\mathbb{Z}/p^{e+1}\mathbb{Z} \to \mathbb{Z}/p^e\mathbb{Z}$. We claim that

$$K_e = \{\mathbf{I}_n + p^e(a_{ij}) \mid (a_{ij}) \in \operatorname{Mat}_n(\mathbb{Z}/p^{e+1}\mathbb{Z})\}.$$

The inclusion $\subseteq$ is clear. Conversely, let $A = \mathbf{I}_n + p^e(a_{ij})$ with some matrix $(a_{ij}) \in \operatorname{Mat}_n(\mathbb{Z}/p^{e+1}\mathbb{Z})$. Then $A \equiv \mathbf{I}_n \mod p$ so that $\det A \equiv 1 \mod p$. Hence $\det A$ is a unit modulo p^e. It follows that A is invertible, i.e., $A \in \operatorname{GL}_n(\mathbb{Z}/p^{e+1}\mathbb{Z})$. This proves the inclusion $\supseteq$. In particular, we now see that K_e has exactly p^{n^2} elements, namely $\mathbf{I}_n + p^e(a_{ij})$ with $a_{ij} \in \{0, 1, \ldots, p-1\}$. So we find that

$$|\operatorname{GL}_n(\mathbb{Z}/p^{e+1}\mathbb{Z})| = p^{n^2} |\operatorname{GL}_n(\mathbb{Z}/p^e\mathbb{Z})| = p^{(e+1)n^2} \prod_{j=1}^{n} \left(1 - p^{-j}\right)$$

and the proof for $\mathrm{GL}_n(\mathbb{Z}/p^e\mathbb{Z})$ is complete.

By the exact sequence

$$1 \longrightarrow \mathrm{SL}_n(\mathbb{Z}/p^e\mathbb{Z}) \longrightarrow \mathrm{GL}_n(\mathbb{Z}/p^e\mathbb{Z}) \xrightarrow{\det} (\mathbb{Z}/p^e\mathbb{Z})^* \longrightarrow 1$$

we find that $|\mathrm{GL}_n(\mathbb{Z}/p^e\mathbb{Z})|/|\mathrm{SL}_n(\mathbb{Z}/p^e\mathbb{Z})| = |(\mathbb{Z}/p^e\mathbb{Z})^*|$, that is,

$$|\mathrm{SL}_n(\mathbb{Z}/p^e\mathbb{Z})| = \frac{|\mathrm{GL}_n(\mathbb{Z}/p^e\mathbb{Z})|}{p^e(1-p^{-1})} = p^{e(n^2-1)} \prod_{j=2}^{n} \left(1-p^{-j}\right)$$

which completes the proof. □

For the proof of Proposition 3.1 the following notation will be useful. Let $k, m, n \in \mathbb{N}$ such that $k \leq n$. Then we write

$$\Delta_{n,k}(m) := \left\{ A \in \mathrm{SL}_n(\mathbb{Z}/m\mathbb{Z}) \;\middle|\; A = \left(\begin{array}{c|c} \mathbf{I}_k & 0 \\ \hline * & * \end{array}\right) \right\}.$$

By considering determinants, one easily sees that for $1 \leq k \leq n-1$ we have

$$\Delta_{n,k}(m) = \left\{ A \in \mathrm{SL}_n(\mathbb{Z}/m\mathbb{Z}) \;\middle|\; A = \left(\begin{array}{c|c} \mathbf{I}_k & 0 \\ \hline * & A' \end{array}\right), A' \in \mathrm{SL}_{n-k}(\mathbb{Z}/m\mathbb{Z}) \right\}.$$

Hence for $1 \leq k \leq n-1$ we find

$$\begin{aligned} |\Delta_{n,k}(m)| &= m^{k(n-k)} |\mathrm{SL}_{n-k}(\mathbb{Z}/m\mathbb{Z})| \\ &= m^{n^2-nk-1} \prod_{\substack{p \mid m \\ p \text{ prime}}} \prod_{j=2}^{n-k} \left(1-p^{-j}\right), \text{ by Lem. 3.2.} \end{aligned}$$

Moreover $\Delta_{n,n}(m) = \{\mathbf{I}_n\}$. Let us write

$$\phi_m : \mathrm{SL}_n(\mathbb{Z}) \longrightarrow \mathrm{SL}_n(\mathbb{Z}/m\mathbb{Z})$$

for the natural epimorphism. Then

$$\Gamma_n(\underbrace{m, \ldots, m}_{k \text{ times}}, 1, \ldots, 1) = \phi_m^{-1}(\Delta_{n,k}(m)).$$

We are now ready to prove the proposition.

Proof of Proposition 3.1. We prove this result by induction, i.e., we first determine the index of $\Gamma_n(m_1, 1, \ldots, 1)$ in $\mathrm{SL}_n(\mathbb{Z})$ and then the index of $\Gamma_n(m_1, \ldots, m_k, m_{k+1}, 1, \ldots, 1)$ in $\Gamma_n(m_1, \ldots, m_k, 1, \ldots, 1)$ for $1 \leq k \leq n-1$. Accordingly, we shall start by showing that

$$[\mathrm{SL}_n(\mathbb{Z}) : \Gamma_n(m_1, 1, \ldots, 1)] = m_1^n \prod_{p|m_1} \left(1 - p^{-n}\right). \tag{3.1}$$

To this end, consider the following commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \Gamma_n(m_1) & \longrightarrow & \mathrm{SL}_n(\mathbb{Z}) & \xrightarrow{\phi_{m_1}} & \mathrm{SL}_n(\mathbb{Z}/m_1\mathbb{Z}) & \longrightarrow & 1 \\ & & \| & & \uparrow & & \uparrow & & \\ 1 & \longrightarrow & \Gamma_n(m_1) & \longrightarrow & \Gamma_n(m_1, 1, \ldots, 1) & \longrightarrow & \Delta_{n,1}(m_1) & \longrightarrow & 1 \end{array}$$

From Lemma 2.9 we obtain

$$[\mathrm{SL}_n(\mathbb{Z}) : \Gamma_n(m_1, 1, \ldots, 1)] = [\mathrm{SL}_n(\mathbb{Z}/m_1\mathbb{Z}) : \Delta_{n,1}(m_1)].$$

By Lemma 3.2 and the above remarks, the right hand side is given by

$$\frac{m_1^{n^2-1} \prod_{p|m_1} \prod_{j=2}^{n} (1 - p^{-j})}{m_1^{n^2-n-1} \prod_{p|m_1} \prod_{j=2}^{n-1} (1 - p^{-j})} = m_1^n \prod_{p|m_1} \left(1 - p^{-n}\right)$$

which proves (3.1).

Let us now suppose we already know that

$$[\mathrm{SL}_n(\mathbb{Z}) : \Gamma_n(m_1, \ldots, m_k, 1, \ldots, 1)] = m_1^n \cdots m_k^n \prod_{j=1}^{k} \prod_{p|m_j} \left(1 - p^{j-n-1}\right)$$

for some $1 \leq k \leq n-2$. Again we consider a commutative diagram. Here we abbreviate $\Gamma_n(m_1, \ldots, m_k) := \Gamma_n(m_1, \ldots, m_k, 1, \ldots, 1)$ and similarly $\Gamma_n(m_1, \ldots, m_{k+1}) := \Gamma_n(m_1, \ldots, m_k, m_{k+1}, 1, \ldots, 1)$.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K_{k+1} & \longrightarrow & \Gamma_n(m_1, \ldots, m_k) & \xrightarrow{\phi_{m_{k+1}}} & \Delta_{n,k}(m_{k+1}) & \longrightarrow & 1 \\ & & \| & & \uparrow & & \uparrow & & \\ 1 & \longrightarrow & K_{k+1} & \longrightarrow & \Gamma_n(m_1, \ldots, m_{k+1}) & \longrightarrow & \Delta_{n,k+1}(m_{k+1}) & \longrightarrow & 1 \end{array}$$

We have

$$K_{k+1} = \Gamma_n(m_1, \ldots, m_k, m_{k+1}, m_{k+1}, \ldots, m_{k+1}).$$

By Lemmas 2.9 and 3.2 we find that

$$\begin{aligned} & [\Gamma_n(m_1,\ldots,m_k,1,\ldots,1):\Gamma_n(m_1,\ldots,m_k,m_{k+1}1,\ldots,1)] \\ = \quad & \frac{|\Delta_{n,k}(m_{k+1})|}{|\Delta_{n,k+1}(m_{k+1})|} \\ = \quad & \frac{m_{k+1}^{n^2-nk-1}\prod_{p|m_{k+1}}\prod_{j=2}^{n-k}(1-p^{-j})}{m_{k+1}^{n^2-n(k+1)-1}\prod_{p|m_{k+1}}\prod_{j=2}^{n-k-1}(1-p^{-j})} \\ = \quad & m_{k+1}^n \prod_{p|m_{k+1}} \left(1-p^{k-n}\right). \end{aligned}$$

By induction we obtain

$$[\mathrm{SL}_n(\mathbb{Z}):\Gamma_n(m_1,\ldots,m_{n-1},1)] = m_1^n\cdots m_{n-1}^n \prod_{j=1}^{n-1}\prod_{p|m_j}\left(1-p^{j-n-1}\right).$$

Finally the exact sequence

$$1 \longrightarrow \Gamma_n(m_1,\ldots,m_n) \longrightarrow \Gamma_n(m_1,\ldots,m_{n-1},1) \xrightarrow{\phi_{m_n}} \Delta_{n,n-1}(m_n) \longrightarrow 1$$

yields

$$[\Gamma_n(m_1,\ldots,m_{n-1},1):\Gamma_n(m_1,\ldots,m_{n-1},m_n)] = |\Delta_{n,n-1}(m_n)| = m_n^{n-1}.$$

This completes the proof. □

3.3 Free Congruence Subgroups of $\mathrm{SL}_2(\mathbb{Z})$

We wish to describe the algebraic structure of the congruence subgroups $\mathrm{P}\Gamma(m,n) \leq \mathrm{PSL}_2(\mathbb{Z})$ and also of $\Gamma(m,n) \leq \mathrm{SL}_2(\mathbb{Z})$ for $n \mid m$. It is well-known that $\mathrm{PSL}_2(\mathbb{Z})$ is the free product

$$\mathrm{PSL}_2(\mathbb{Z}) = \left\langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle * \left\langle \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \right\rangle$$

where the first factor has order 2 and the second one has order 3. From the Kurosh Subgroup Theorem, see Section 2.5, it follows that every subgroup of $\mathrm{PSL}_2(\mathbb{Z})$ is the free product of a (possibly trivial) free group, and certain numbers of copies of the cyclic groups C_2 and C_3. As we

shall see, up to a few special cases, the groups $\mathrm{P}\Gamma(m,n)$ and $\Gamma(m,n)$ are actually free.

In [10] Frasch gives the following description of the groups $\mathrm{P}\Gamma(p)$ for p prime.

Theorem 3.3 (Frasch)**.** *Let $p \geq 3$ be a prime. Then $\mathrm{P}\Gamma(p)$ is free of rank $1 + p^3(1-p^{-2})/12$. Moreover, $\mathrm{P}\Gamma(2)$ is free of rank 2.*

We shall now generalize his result to

Proposition 3.4. *Let $m, n \in \mathbb{N}$ such that $m \geq 3$, $n \mid m$ and $(m,n) \neq (3,1)$. Then $\Gamma(m,n)$ and $\mathrm{P}\Gamma(m,n)$ are free of rank*

$$1 + \frac{nm^2}{12} \prod_{\substack{p \mid m \\ p \text{ prime}}} \left(1 - p^{-2}\right).$$

In particular, for primes $p \geq 5$, the groups $\Gamma(p,1)$ are free of rank $1 + p^2(1-p^{-2})/12$ so that the rank of $\Gamma(p,1)$ grows quadratically in p. In contrast, for $r \geq 3$ one can show that the corresponding subgroups $\Gamma_r(p,1,\ldots,1)$ in $\mathrm{SL}_r(\mathbb{Z})$ can always be generated by $r(r-1)$ matrices. See also [12, Lem. 6.1] or [1, Prop. 2.15].

Let us now prove the above proposition. Consider the natural projection $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{PSL}_2(\mathbb{Z})$. By definition, it maps $\Gamma(m)$ onto $\mathrm{P}\Gamma(m)$. For $m \geq 3$ the kernel $\langle \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \rangle$ of this projection has trivial intersection with $\Gamma(m)$. Hence we obtain an isomorphism

$$\Gamma(m) \xrightarrow{\sim} \mathrm{P}\Gamma(m).$$

Note that this argument does not work in the case $m = 2$. Indeed, applying Proposition 2.1 to the exact sequence

$$1 \longrightarrow \langle \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \rangle \longrightarrow \Gamma(2) \longrightarrow \mathrm{P}\Gamma(2) \longrightarrow 1$$

one finds that, in contrast to $\mathrm{P}\Gamma(2)$, the group $\Gamma(2)$ is not free but the direct product of a rank two free group and a cyclic group of order two. Furthermore, in [22] Rademacher considers the groups $\mathrm{P}\Gamma^0(p)$ for primes p. In particular, he shows that

$$\mathrm{P}\Gamma^0(2) \cong \mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$$
$$\mathrm{P}\Gamma^0(3) \cong \mathbb{Z} * \mathbb{Z}/3\mathbb{Z}.$$

Noting that $\mathrm{P}\Gamma^1(2) = \mathrm{P}\Gamma^0(2)$ and $\mathrm{P}\Gamma^1(3) = \mathrm{P}\Gamma^0(3)$, we see that $\mathrm{P}\Gamma^1(2)$ and $\mathrm{P}\Gamma^1(3)$ are not free. So the cases which are excluded in the proposition indeed behave differently.

Lemma 3.5. *Let $m \geq 3$. Then $\Gamma(m) \cong \mathrm{P}\Gamma(m)$ is free of rank*

$$1 + \frac{m^3}{12} \prod_{p|m} \left(1 - p^{-2}\right)$$

where the product runs over all primes p dividing m.

Proof. Observe that for $m_1, m_2 \in \mathbb{N}$ such that $m_1 \mid m_2$ we have $\Gamma(m_2) \leq \Gamma(m_1)$. Accordingly the main point in our proof is that subgroups of free groups are again free and the rank is given by the Schreier formula [19, Thm. 2.10]. Since $\Gamma(2)$ is not free, we consider two cases.

Case 1: We have $m = 2^a$ for some $a \geq 2$. One can verify that $\mathrm{P}\Gamma(4)$ has index 4 in $\mathrm{P}\Gamma(2)$. Since the latter group is free of rank 2, we find that $\mathrm{P}\Gamma(4)$ is free of rank 5. From Proposition 3.1 we know that $\Gamma(2^a)$ has index 2^{3a-6} in $\Gamma(4)$. We thus find that the group $\Gamma(2^a)$ is free of rank $1 + 2^{3a}(1 - 2^{-2})/12$, as claimed.

Case 2: We have $p_0 \mid m$ for some prime $p_0 > 2$. Again by Proposition 3.1, we see that

$$[\Gamma(p_0) : \Gamma(m)] = \frac{m^3}{p_0^3} \prod_{\substack{p|m \\ p \neq p_0}} \left(1 - p^{-2}\right).$$

Since, by Proposition 3.3, the group $\Gamma(p_0)$ is free of rank $1 + p_0^3(1 - p_0^{-2})/12$, we obtain the desired result. □

We next wish to generalize this result to the groups $\Gamma(m, n)$ and $\mathrm{P}\Gamma(m, n)$ where $m \geq 3$, $n \mid m$ and $(m, n) \neq (3, 1)$. The first step is, of course, to show that these groups are free. Observe that in this case, the natural projection $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{PSL}_2(\mathbb{Z})$ again leads to an isomorphism

$$\Gamma(m, n) \xrightarrow{\sim} \mathrm{P}\Gamma(m, n).$$

Lemma 3.6. *Let $m \geq 4$, then $\Gamma^1(m) \cong \mathrm{P}\Gamma^1(m)$ is a free group.*

Proof. Let us first consider the case that m has a prime factor $p \geq 5$. We show that $\mathrm{P}\Gamma^1(p)$ does not contain a non-trivial element of finite

order. Then the Kurosh Subgroup Theorem yields that $\mathrm{P}\Gamma^1(p)$ is free. To this end assume that $A \in \mathrm{P}\Gamma^1(p)$ is a non-trivial element of finite order. Observe that, again by the Kurosh Subgroup Theorem, A has either order 2 or 3. By definition of $\mathrm{P}\Gamma^1(p)$ we have

$$A \equiv \begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix} \mod p$$

for some $0 \leq k \leq p-1$. It follows that

$$A^p \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod p.$$

Now we consider two cases.

Case 1: $A^p = 1$. Then the order of A divides p and we have a contradiction, since A has either order 2 or 3.

Case 2: $A^p \neq 1$. Then A^p is a non-trivial element of $\mathrm{P}\Gamma(p)$, which is, by Theorem 3.3, a free group. Hence A^p does not have finite order, contradiction.

For the remaining cases, that is, for the cases $m = 2^i 3^j$ with suitable $i, j \in \mathbb{N} \cup \{0\}$, one verifies by an explicit computation using the Reidemeister-Schreier method that $\mathrm{P}\Gamma^1(m)$ is also free for $m = 4, 6, 9$. Hence the lemma follows. □

From the above lemma together with Lemma 3.5, the formulas in Proposition 3.1 and the Schreier formula, we now obtain Proposition 3.4.

Remark 3.7. There is a nice alternative argument to show that the groups $\mathrm{P}\Gamma^1(m)$ are free for $m \geq 4$ which works as follows. Let $p \geq 5$ be a prime. In [22] Rademacher gives a very concrete description of the group $\mathrm{P}\Gamma^0(p)$. He shows that $\mathrm{P}\Gamma^0(p)$ is the free product of a non-trivial free group and

- $\langle V_{x_1} \mid V_{x_1}^2 = 1 \rangle * \langle V_{x_2} \mid V_{x_2}^2 = 1 \rangle$ if $p \equiv 1 \mod 4$
- $\langle V_{\lambda_1} \mid V_{\lambda_1}^3 = 1 \rangle * \langle V_{\lambda_2} \mid V_{\lambda_2}^3 = 1 \rangle$ if $p \equiv 1 \mod 3$

where x_i, λ_i are defined by $x^2 \equiv -1$ and $(2\lambda - 1)^2 \equiv -3 \mod p$, respectively, and

$$V_k = \left(\begin{smallmatrix} k & -kk_*-1 \\ 1 & -k_* \end{smallmatrix}\right) \text{ with } 1 \leq k_* \leq p-1,\ kk_* \equiv -1 \mod p.$$

One can easily verify that a non-trivial element of $\mathrm{P}\Gamma^1(p)$ can neither be conjugated into $\langle V_{x_i} \rangle$ nor $\langle V_{\lambda_i} \rangle$. Hence the Kurosh Subgroup Theorem (and again checking $m = 4, 6, 9$ separately) implies that for $m \geq 4$ the group $\mathrm{P}\Gamma^1(m)$ is free. $\diamond$

Chapter 4

Congruence Subgroups of $\mathrm{Aut}(F_n)$

This chapter is the main part of the thesis. We first make a few observations on congruence subgroups of $\mathrm{Aut}^+(F_n)$ and then consider standard congruence subgroups associated to certain families of finite groups, i.e., finite abelian groups, dihedral groups, semidirect products of finite cyclic groups and some wreath products of finite cyclic groups. For all these finite groups we also describe the product replacement graph in terms of the number and the sizes of its connected components. Finally, we show that the abelianization of a standard congruence subgroup of $\mathrm{Aut}^+(F_2)$ associated to a finite non-perfect group is infinite.

4.1 Preliminary Results on Congruence Subgroups of $\mathrm{Aut}(F_n)$

Let us briefly recall our notation from Section 1.1, which we will need throughout the whole chapter.

By $F_n = \langle x_1, \ldots, x_n \rangle$ we denote the free group on $n \geq 2$ generators. For $n = 2$ we usually write $F_2 = \langle x, y \rangle$. For an epimorphism $\pi : F_n \to G$ of F_n onto a finite group G we define

$$\begin{aligned}\Gamma(G, \pi) :=& \{\varphi \in \mathrm{Aut}(F_n) \mid \varphi(\ker(\pi)) = \ker(\pi),\ \varphi \text{ induces } \mathrm{id}_{F_n/\ker(\pi)}\} \\ =& \{\varphi \in \mathrm{Aut}(F_n) \mid \pi\varphi = \pi\}.\end{aligned}$$

We have a surjective representation

$$\rho : \mathrm{Aut}(F_n) \to \mathrm{Aut}(F_n/F_n') = \mathrm{GL}_n(\mathbb{Z})$$

and define $\mathrm{Aut}^+(F_n) := \rho^{-1}(\mathrm{SL}_n(\mathbb{Z}))$. Moreover, we set $\Gamma^+(G, \pi) := \Gamma(G, \pi) \cap \mathrm{Aut}^+(F_n)$.

4.1.1 A Reduction Step

As before, let G be a finite group and $\pi : F_n \to G$ an epimorphism. Suppose that $\bar{G}$ is a group such that there is an epimorphism $G \to \bar{G}$. Observe that we naturally obtain an epimorphism $\bar{\pi} : F_n \xrightarrow{\pi} G \to \bar{G}$. If we have $\pi\varphi = \pi$ for some $\varphi \in \mathrm{Aut}(F_n)$, then clearly $\bar{\pi}\varphi = \bar{\pi}$. Hence

$$\Gamma(G, \pi) \leq \Gamma(\bar{G}, \bar{\pi}).$$

In particular, we may choose $\bar{G} = G^{\mathrm{ab}}$, the abelianization of G. With the above notation we have

$$\rho(\Gamma(G, \pi)) \leq \rho(\Gamma(G^{\mathrm{ab}}, \bar{\pi})).$$

This will be helpful, since the image $\rho(\Gamma(G, \pi))$ is easy to understand if G is abelian: as mentioned before if $\pi : F_n \to \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z}$ is the obvious epimorphism, then

$$\rho(\Gamma^+(\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z}, \pi)) = \Gamma_n(m_1, \ldots, m_n).$$

A similar observation is given by the following result.

Lemma 4.1. *Let $\pi : F_n \to G$ be an epimorphism of F_n onto a finite group. Moreover, let $\pi_i : G \to G_i$, $1 \leq i \leq m$, be epimorphisms with $\bigcap_{1 \leq i \leq m} \ker(\pi_i) = 1$. Then*

$$\Gamma^+(G, \pi) = \bigcap_{1 \leq i \leq m} \Gamma^+(G_i, \pi_i\pi).$$

Proof. By the above discussion, we have $\Gamma^+(G, \pi) \leq \Gamma^+(G_i, \pi_i\pi)$ for $1 \leq i \leq m$. Hence the inclusion $\leq$ is already clear.

Now let $\varphi \in \bigcap \Gamma^+(G_i, \pi_i\pi)$. Then we have $\varphi(\ker(\pi_i\pi)) = \ker(\pi_i\pi)$ and $\varphi(w) \equiv w \mod \ker(\pi_i\pi)$ for all $1 \leq i \leq m$ and $w \in F_n$. Hence

$$\varphi(\bigcap \ker(\pi_i\pi)) = \bigcap \ker(\pi_i\pi)$$

and also

$$\varphi(w) \equiv w \mod \bigcap \ker(\pi_i\pi)$$

for all $w \in F_n$. It thus suffices to show that $\bigcap \ker(\pi_i\pi) = \ker(\pi)$. Here the inclusion $\geq$ is obvious. Conversely, if $w \in \bigcap \ker(\pi_i\pi)$, then $\pi_i(\pi(w)) = 1$ for $1 \leq i \leq m$ so that $\pi(w) \in \bigcap \ker(\pi_i) = 1$, that is, $w \in \ker(\pi)$. □

4.1.2 Connection to the Product Replacement Graph and Dependence on the Presentation

For a finite group G with $\mathrm{d}(G) \leq n$ we set

$$\mathbf{E}_n(G) := \{\pi : F_n \to G \mid \pi \text{ is an epimorphism}\}.$$

Note that $\mathbf{E}_n(G)$ is a finite set. The automorphism group $\mathrm{Aut}(F_n)$ acts on $\mathbf{E}_n(G)$ from the right by

$$\pi \cdot \varphi := \pi\varphi, \quad \varphi \in \mathrm{Aut}(F_n),\, \pi \in \mathbf{E}_n(G).$$

If we fix an epimorphism $\pi \in \mathbf{E}_n(G)$, then $\Gamma(G, \pi)$ is exactly the stabilizer of π under this action. By the orbit-stabilizer theorem we have

$$[\mathrm{Aut}(F_n) : \Gamma(G, \pi)] = |\pi \cdot \mathrm{Aut}(F_n)|.$$

In particular, $\Gamma(G, \pi)$ has finite index in $\mathrm{Aut}(F_n)$. Note that

$$\Gamma(G, \pi \cdot \varphi) = \varphi^{-1}\Gamma(G, \pi)\varphi, \quad \varphi \in \mathrm{Aut}(F_n). \tag{4.1}$$

Hence, up to conjugation, $\Gamma(G, \pi)$ only depends on the orbit of π under the action of $\mathrm{Aut}(F_n)$. The automorphism group $\mathrm{Aut}(G)$ acts on $\mathbf{E}_n(G)$ from the left by

$$\alpha \cdot \pi := \alpha\pi, \quad \alpha \in \mathrm{Aut}(G), \pi \in \mathbf{E}_n(G).$$

Obviously, we have

$$\Gamma(G, \pi) = \Gamma(G, \alpha \cdot \pi).$$

We may naturally identify $\mathbf{E}_n(G)$ with the set $\mathbf{V}_n(G)$ of generating n-tuples of G, which we have considered in Section 2.3, through the correspondence

$$\mathbf{E}_n(G) \ni \pi \quad \longleftrightarrow \quad (\pi(x_1), \ldots, \pi(x_n)) \in \mathbf{V}_n(G).$$

Now the action of $\mathrm{Aut}^+(F_n)$ on $\mathbf{E}_n(G)$ leads to the Nielsen moves that define the product replacement graph of G.

Under this identification, the orbit $\pi \cdot \mathrm{Aut}^+(F_n)$ corresponds to the connected component of $\mathbf{V}_n(G)$ containing $(\pi(x_1), \ldots, \pi(x_n))$ and the

orbit $\mathrm{Aut}(G) \cdot \pi \cdot \mathrm{Aut}^+(F_n)$ corresponds to the T_n-system containing this tuple.

In particular, the index of $\Gamma^+(G,\pi)$ in $\mathrm{Aut}^+(F_n)$ is the size of the connected component of $\mathbf{V}_n(G)$ containing the tuple $(\pi(x_1),\dots,\pi(x_n))$. Moreover, up to conjugation, $\Gamma^+(G,\pi)$ only depends on the connected component of $(\pi(x_1),\dots,\pi(x_n))$ and, more generally, only on the T_n-system of this tuple. Hence, if G has only one T_n-system, then, up to conjugation, $\Gamma^+(G,\pi)$ does not depend on the particular choice of the epimorphism π. In particular, we have

Lemma 4.2. *If the finite group G has only one T_2-system, then, up to conjugation, $\Gamma^+(G,\pi)$ does not depend on the choice of π.*

4.1.3 First Remarks on the Index

Let us consider the following commutative diagram.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{IA}_n & \longrightarrow & \mathrm{Aut}^+(F_n) & \xrightarrow{\rho} & \mathrm{SL}_n(\mathbb{Z}) & \longrightarrow & 1 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 1 & \longrightarrow & \mathrm{IA}_n \cap \Gamma^+(G,\pi) & \longrightarrow & \Gamma^+(G,\pi) & \xrightarrow{\rho} & \rho(\Gamma^+(G,\pi)) & \longrightarrow & 1 \end{array}$$

The rows of this diagram are exact and the homomorphisms from the second row to the first one are simply the inclusions. Before we apply Lemma 2.9 to this diagram, we note the following result for the special case $n = 2$. Recall that, in this case, $\mathrm{IA}_2 = \mathrm{Inn}(F_2)$. Moreover, for $z \in F_2$, we write $\alpha_z \in \mathrm{IA}_2$ for the inner automorphism given by $\alpha_z(w) = zwz^{-1}$. Similarly, for $g \in G$ we define $c_g \in \mathrm{Inn}(G)$ by $c_g(h) := ghg^{-1}$ for all $h \in G$.

Lemma 4.3. *The homomorphism $\Phi : \mathrm{IA}_2 \to \mathrm{Inn}(G)$ given by $\Phi(\alpha_z) := c_{\pi(z)}$ leads to an exact sequence*

$$1 \longrightarrow \mathrm{IA}_2 \cap \Gamma^+(G,\pi) \longrightarrow \mathrm{IA}_2 \xrightarrow{\Phi} \mathrm{Inn}(G) \longrightarrow 1.$$

In particular $[\mathrm{IA}_2 : \mathrm{IA}_2 \cap \Gamma^+(G,\pi)] = |\mathrm{Inn}(G)| = [G : \mathrm{Z}(G)]$.

Proof. Since $\pi : F_2 \to G$ is onto, it follows that Φ is onto. We now show that $\ker \Phi = \mathrm{IA}_2 \cap \Gamma^+(G,\pi)$.

Let $\alpha_z \in \ker \Phi$. Then $c_{\pi(z)} = \mathrm{id}_G$, i.e., $\pi(z)g\pi(z)^{-1} = g$ for all $g \in G$. Hence $\pi\alpha_z(w) = \pi(z)\pi(w)\pi(z)^{-1} = \pi(w)$ for all $w \in F_2$ so that $\pi\alpha_z = \pi$. This shows that $\alpha_z \in \mathrm{IA}_2 \cap \Gamma^+(G, \pi)$.

Conversely, suppose that $\alpha_z \in \mathrm{IA}_2 \cap \Gamma^+(G, \pi)$. Then $\pi\alpha_z = \pi$ so that $\pi(z)\pi(w)\pi(z)^{-1} = \pi(w)$ for all $w \in F_2$. Since π is onto, it follows that $\pi(z) \in \mathrm{Z}(G)$. Hence $c_{\pi(z)} = \mathrm{id}_G$, i.e., $\alpha_z \in \ker \Phi$. □

Now we apply Lemma 2.9 to the above diagram to obtain

Corollary 4.4. *We have*

$$[\mathrm{Aut}^+(F_n) : \Gamma^+(G, \pi)] = [\mathrm{SL}_n(\mathbb{Z}) : \rho(\Gamma^+(G, \pi))] \cdot [\mathrm{IA}_n : \mathrm{IA}_n \cap \Gamma^+(G, \pi)].$$

For $n = 2$ this implies

$$[\mathrm{Aut}^+(F_2) : \Gamma^+(G, \pi)] = [\mathrm{SL}_2(\mathbb{Z}) : \rho(\Gamma^+(G, \pi))] \cdot |\mathrm{Inn}(G)|.$$

Note that if $\pi : F_n \to G$ is an epimorphism onto an abelian group, we have $\mathrm{IA}_n \leq \Gamma^+(G, \pi)$. Hence, in this case

$$[\mathrm{Aut}^+(F_n) : \Gamma^+(G, \pi)] = [\mathrm{SL}_n(\mathbb{Z}) : \rho(\Gamma^+(G, \pi))].$$

This observation will be used in the next section.

4.2 Congruence Subgroups associated to Abelian Groups

In this section we consider congruence subgroups of $\mathrm{Aut}^+(F_n)$ associated to finite abelian groups. Our aim is to prove Theorem B. We first determine their indices in $\mathrm{Aut}^+(F_n)$. Using this, we obtain a nice description of the product replacement graphs of finite abelian groups. Using our results on congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ in Section 3.3, we also determine the abelianizations of congruence subgroups of $\mathrm{Aut}^+(F_2)$ associated to finite abelian groups.

4.2.1 The Index of Congruence Subgroups associated to Abelian Groups

Our aim in this section is to prove

Theorem 4.5. *Let G be a finite abelian group. Then, up to conjugation, $\Gamma^+(G,\pi)$ only depends on G but not on the particular epimorphism $\pi : F_n \to G$. We have*

$$[\mathrm{Aut}^+(F_n) : \Gamma^+(G,\pi)] = [\mathrm{SL}_n(\mathbb{Z}) : \rho(\Gamma^+(G,\pi))].$$

Writing $G \cong \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z}$ with $m_{i+1} \mid m_i$ for $1 \leq i \leq n-1$, the index of $\Gamma^+(G,\pi)$ in $\mathrm{Aut}^+(F_n)$ is given by

$$m_1^n \cdots m_{n-1}^n m_n^{n-1} \prod_{j=1}^{n-1} \prod_{p \mid m_j} \left(1 - p^{j-n-1}\right)$$

where the second product runs over all primes p dividing m_j.

We note that this result for the special case $n = 2$ can be found in the joint paper [3] of Ribnere and the author.

Before we prove this, let us state a consequence of this theorem which can also be found in [3].

Corollary 4.6. *Let $m_1, m_2 \in \mathbb{N}$ (where not necessarily $m_2 \mid m_1$). Then*

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(m_1,m_2)] = \mathrm{lcm}(m_1,m_2)^2 \gcd(m_1,m_2) \prod (1 - p^{-2}).$$

where the product runs over all primes p dividing $\mathrm{lcm}(m_1,m_2)$.

Proof. We have $\Gamma(m_1,m_2) = \rho(\Gamma^+(\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}, \pi))$ where $\pi : F_2 \to \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$ is the obvious epimorphism. Observe that there is an isomorphism

$$\alpha : \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/\mathrm{lcm}(m_1,m_2)\mathbb{Z} \times \mathbb{Z}/\gcd(m_1,m_2)\mathbb{Z}.$$

Now

$$\Gamma^+(\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}, \pi) = \Gamma^+(\mathbb{Z}/\mathrm{lcm}(m_1,m_2)\mathbb{Z} \times \mathbb{Z}/\gcd(m_1,m_2)\mathbb{Z}, \alpha\pi).$$

Since, up to conjugation, $\Gamma^+(\mathbb{Z}/\mathrm{lcm}(m_1,m_2)\mathbb{Z} \times \mathbb{Z}/\gcd(m_1,m_2)\mathbb{Z}, \alpha\pi)$ does not depend on $\alpha\pi$, we find that

$$\rho(\Gamma^+(\mathbb{Z}/\mathrm{lcm}(m_1,m_2)\mathbb{Z} \times \mathbb{Z}/\gcd(m_1,m_2)\mathbb{Z}, \alpha\pi)) = \Gamma(m_1,m_2)$$

is conjugate to $\Gamma(\mathrm{lcm}(m_1,m_2), \gcd(m_1,m_2))$. By Proposition 3.1, the result follows. □

Our first step towards proving the theorem is

Lemma 4.7. *Let $m, n \in \mathbb{N}$ and $a_1, \ldots, a_n \in (\mathbb{Z}/m\mathbb{Z})^n$. Then, writing the a_i as column vectors, we have*

$$\langle a_1, \ldots, a_n \rangle = (\mathbb{Z}/m\mathbb{Z})^n \iff (a_1 \cdots a_n) \in \mathrm{GL}_n(\mathbb{Z}/m\mathbb{Z}).$$

In particular $|\mathbf{V}_n((\mathbb{Z}/m\mathbb{Z})^n)| = |\mathrm{GL}_n(\mathbb{Z}/m\mathbb{Z})|$.

Proof. We have

$$\langle a_1, \ldots, a_n \rangle = (\mathbb{Z}/m\mathbb{Z})^n.$$

$$\Leftrightarrow \quad \text{There are } \lambda_{ij} \in \mathbb{Z}/m\mathbb{Z}, 1 \le i, j \le n, \text{ such that}$$
$$\lambda_{11}a_1 + \cdots + \lambda_{n1}a_n = (1\ 0 \cdots 0\ 0)^t, \ldots,$$
$$\lambda_{1n}a_1 + \cdots + \lambda_{nn}a_n = (0\ 0 \cdots 0\ 1)^t.$$

$$\Leftrightarrow \quad \text{There are } \lambda_{ij} \in \mathbb{Z}/m\mathbb{Z}, 1 \le i, j \le n, \text{ such that}$$
$$(a_1 \cdots a_n) \begin{pmatrix} \lambda_{11} & \cdots & \lambda_{1n} \\ \vdots & \ddots & \vdots \\ \lambda_{n1} & \cdots & \lambda_{nn} \end{pmatrix} = \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix}.$$

$$\Leftrightarrow \quad (a_1 \cdots a_n) \in \mathrm{GL}_n(\mathbb{Z}/m\mathbb{Z}).$$

This proves the lemma. □

By the above lemma, we can identify $\mathbf{V}_n((\mathbb{Z}/m\mathbb{Z})^n)$ with $\mathrm{GL}_n(\mathbb{Z}/m\mathbb{Z})$ in a natural way. We shall use this identification in the proof of the following lemma. By ϕ we denote the Euler ϕ-function.

Lemma 4.8. *The product replacement graph $\mathbf{V}_n((\mathbb{Z}/m\mathbb{Z})^n)$ has exactly $\phi(m)$ connected components. Identifying $\mathbf{V}_n((\mathbb{Z}/m\mathbb{Z})^n)$ with $\mathrm{GL}_n(\mathbb{Z}/m\mathbb{Z})$, the connected components are characterized by the determinant.*

Proof. Observe that, under our identification of the graph $\mathbf{V}_n((\mathbb{Z}/m\mathbb{Z})^n)$ with $\mathrm{GL}_n(\mathbb{Z}/m\mathbb{Z})$, the Nielsen moves correspond to certain column operations. To be precise, an elementary Nielsen move corresponds to the addition of a column to another one. Hence it is clear that the determinant is an invariant for the connected components so that $\mathbf{V}_n((\mathbb{Z}/m\mathbb{Z})^n)$ has at least $\phi(m)$ components.

Suppose that $\det(a_1 \cdots a_n) = \varepsilon$. We shall now show that $(a_1, \ldots, a_n)$ is in the same connected component as

$$\left(\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}, \ldots, \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ \varepsilon \end{pmatrix} \right) \tag{4.2}$$

thereby proving that $\mathbf{V}_n((\mathbb{Z}/m\mathbb{Z})^n)$ has exactly $\phi(m)$ connected components and that these are characterized by the determinant. Observe that, since the determinant of $(a_1 \cdots a_n)$ is a unit modulo m, so must be the greatest common divisor of the entries in the first row. Using Nielsen moves, we can apply an Euclidean algorithm to the first row to obtain a matrix of the form

$$\left(\begin{array}{c|ccc} 1 & 0 & \cdots & 0 \\ \hline * & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ * & a_{n2} & \cdots & a_{nn} \end{array} \right).$$

Now the determinant of the $(n-1) \times (n-1)$-submatrix at the bottom right must again be a unit. So we can apply a Euclidean algorithm to its first row $(a_{22} \cdots a_{2n})$ to obtain $(1\ 0 \cdots 0)$. Adding a suitable multiple of the second column of the $n \times n$-matrix to its first column, we obtain

$$\left(\begin{array}{cc|ccc} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \hline * & * & * & \cdots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ * & * & * & \cdots & * \end{array} \right).$$

Proceeding inductively we get a matrix of the form

$$\left(\begin{array}{c|c} \mathbf{I}_{n-1} & 0 \\ \hline * & a \end{array} \right).$$

Now a has to be a unit. Indeed, we must have $a = \varepsilon$. So, by adding suitable multiples of the last column to the others, we obtain the desired matrix corresponding to (4.2). □

Lemma 4.9. *Let $G := \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z}$ with $m_{i+1} \mid m_i$ for $1 \leq i \leq n-1$. Then $\mathbf{V}_n(G)$ has exactly $\phi(m_n)$ connected components. Moreover, G has only one T_n-system.*

Proof. Let us first consider the case that $m_n > 1$. Observe that for every $\varepsilon \in (\mathbb{Z}/m_n\mathbb{Z})^*$ we have a generating n-tuple of G of the form (4.2). We show that these $\phi(m_n)$ tuples represent the connected components. To this end let

$$A = \left(\begin{pmatrix} a_{11} \\ \vdots \\ a_{n1} \end{pmatrix}, \ldots, \begin{pmatrix} a_{1n} \\ \vdots \\ a_{nn} \end{pmatrix} \right)$$

be an arbitrary generating n-tuple of G. We shall assign two matrices to this tuple as follows. On the one hand, via the natural projection $G \twoheadrightarrow (\mathbb{Z}/m_n\mathbb{Z})^n$, we can map A onto a generating n-tuple of $(\mathbb{Z}/m_n\mathbb{Z})^n$. By Lemma 4.7, we can identify this tuple with a matrix $A_n \in \mathrm{GL}_n(\mathbb{Z}/m_n\mathbb{Z})$. On the other hand, by Lemma 2.6 of Gaschütz, the tuple A lifts via $(\mathbb{Z}/m_1\mathbb{Z})^n \twoheadrightarrow G$ to a generating n-tuple of $(\mathbb{Z}/m_1\mathbb{Z})^n$ which we can identify with a matrix $A_1 \in \mathrm{GL}_n(\mathbb{Z}/m_1\mathbb{Z})$. Now, if we apply a Nielsen move to A, the matrix we obtain maps onto the matrix obtained from A_n by applying the same move. Since $\det(A_n) \in (\mathbb{Z}/m_n\mathbb{Z})^*$ is invariant under Nielsen moves, we find that the generating tuples (4.2) lie in distinct connected components of $\mathbf{V}_n(G)$. It now remains to verify that A lies in the same connected component as

$$\left(\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ 0 \\ 0 \end{pmatrix}, \cdots, \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ \det(A_n) \end{pmatrix} \right).$$

From Lemma 4.8 we know that we can apply a Nielsen move to A_1 such that we obtain

$$\begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & \det(A_1) \end{pmatrix} \in \mathrm{GL}_n(\mathbb{Z}/m_1\mathbb{Z}). \tag{4.3}$$

Since $\det(A_1) \equiv \det(A_n) \mod m_n$, we now just have to apply the same Nielsen move to A to obtain the desired result.

To see that G has only one T_n-system, we note that each of the generating tuples (4.2) can be mapped onto the canonical one by an automorphism of G.

Let us now consider the case $m_n = 1$. Suppose that $m_1, \ldots, m_{k-1} \neq 1$ and $m_k, \ldots, m_n = 1$. As before we can lift an arbitrary generating tuple

$A \in \mathbf{V}_n(G)$ to some $A_1 \in \mathbf{V}_n((\mathbb{Z}/m_1\mathbb{Z})^n)$. By applying Nielsen moves such that A_1 is transformed to a matrix as in (4.3), we get that, by the same moves, A is transformed to

$$\left(\begin{array}{c|c} \mathbf{I}_k & 0 \\ \hline 0 & 0 \end{array}\right).$$

Hence, in the case $m_n = 1$, the graph $\mathbf{V}_n(G)$ is connected. In particular, G has only one T_n-system. □

Now we complete the proof of the main result.

Proof of Theorem 4.5. The fact that

$$[\mathrm{Aut}^+(F_n) : \Gamma^+(G,\pi)] = [\mathrm{SL}_n(\mathbb{Z}) : \rho(\Gamma^+(G,\pi))]. \tag{4.4}$$

follows from Corollary 4.4. We know by Lemma 4.9 that the index of $\Gamma^+(G,\pi)$, with G as in the theorem, does not depend on the choice of π. If one thus chooses the canonical epimorphism $\pi : F_n \to G$, then $\rho(\Gamma^+(G,\pi)) = \Gamma(m_1,\ldots,m_n)$. The index of this group in $\mathrm{SL}_n(\mathbb{Z})$ is given in Proposition 3.1. □

4.2.2 Product Replacement Graphs of Abelian Groups

The above results enable us to prove some facts about the product replacement graph of a finite abelian group. Indeed, we can find the number of its vertices and the number and the sizes of its connected components. Note that formulas for these numbers are also given by Diaconis and Graham in [7]. However, they use a very different method to find a formula for the size of the product replacement graph. To be concrete, they use abstract Möbius inversion, which was introduced by Hall [13]. We note that our formula for the number of generating n-tuples seems to be much easier to evaluate.

Proposition 4.10. *Let* $G := \mathbb{Z}/m_1\mathbb{Z}\times\cdots\times\mathbb{Z}/m_n\mathbb{Z}$ *where* $m_{i+1} \mid m_i$. *The number of connected components of* $\mathbf{V}_n(G)$ *is* $\phi(m_n)$ *and each component has exactly*

$$m_1^n \cdots m_{n-1}^n m_n^{n-1} \prod_{j=1}^{n-1} \prod_{\substack{p \mid m_j \\ p \text{ prime}}} (1 - p^{j-n-1})$$

vertices. Moreover, G has only one T_n-system.

In particular, G has exactly

$$m_1^n \cdots m_n^n \prod_{j=1}^{n} \prod_{\substack{p \mid m_j \\ p \text{ prime}}} (1 - p^{j-n-1})$$

generating n-tuples and if $m_n \leq 2$, then $\mathbf{V}_n(G)$ is connected.

Proof. Since, by Lemma 4.9, the group G has only one T_n-system, we see that all connected components of $\mathbf{V}_n(G)$ have the same size. Now the size of such a component is just the index of $\Gamma^+(G, \pi)$ in $\mathrm{Aut}^+(F_n)$ and, by Lemma 4.9, the number of connected components is $\phi(m_n)$. We thus obtain the desired result. □

4.2.3 The Abelianization of Congruence Subgroups associated to Abelian Groups

Using the results of the preceding sections and the facts we know about congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$, we can determine the abelianization of $\Gamma^+(G, \pi)$ for an abelian group G in the case $n = 2$. Note that our result covers all possible choices for G abelian.

Theorem 4.11. *Let $m, n \in \mathbb{N}$ such that $m \geq 3$, $n \mid m$ and $(m, n) \neq (3, 1)$. Moreover, let $G := \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ and $\pi : F_2 \to G$ be an epimorphism. Then*

$$\Gamma^+(G, \pi)^{\mathrm{ab}} \cong G \times \mathbb{Z}^{1+12^{-1}nm^2 \prod_{p \mid m}(1-p^{-2})}$$

where the product runs over all primes p dividing m.

Furthermore, we have

$$\begin{aligned} \Gamma^+(\mathbb{Z}/2\mathbb{Z}, \pi)^{\mathrm{ab}} &\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}, \\ \Gamma^+(\mathbb{Z}/3\mathbb{Z}, \pi)^{\mathrm{ab}} &\cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}, \\ \Gamma^+(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \pi)^{\mathrm{ab}} &\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^2. \end{aligned}$$

Proof. By Theorem 4.5, up to conjugation, the group $\Gamma^+(G, \pi)$ only depends on G but not on the particular choice of the epimorphism $\pi : F_2 \to G$. We may thus suppose that $\pi(x) = (1, 0)$ and $\pi(y) = (0, 1)$.

Note that, since G is abelian, we have $\mathrm{IA}_2 \leq \Gamma^+(G,\pi)$. Hence there is an exact sequence

$$1 \longrightarrow \mathrm{IA}_2 \longrightarrow \Gamma^+(G,\pi) \xrightarrow{\rho} \Gamma(m,n) \longrightarrow 1.$$

By Proposition 3.4, the group $\Gamma(m,n)$ is free of rank

$$r := 1 + \frac{nm^2}{12} \prod_{p|m} \left(1 - p^{-2}\right).$$

Let $\{M_i = \left(\begin{smallmatrix} a_i & b_i \\ c_i & d_i \end{smallmatrix}\right) \mid 1 \leq i \leq r\}$ be a set of free generators of $\Gamma(m,n)$. Moreover, let $\varphi_i \in \mathrm{Aut}^+(F_2)$ such that $\rho(\varphi_i) = M_i$, that is,

$$\varphi_i(x) \equiv a_i x + c_i y, \quad \varphi_i(y) \equiv b_i x + d_i y \mod F_2' \tag{4.5}$$

where F_2' denotes the commutator subgroup of F_2. Recall that the group IA_2 is free on α_x, α_y, the inner automorphisms given by conjugation with x and y, respectively (see Section 2.2). Now Proposition 2.1 of Hall yields that $\Gamma^+(G,\pi)$ admits a presentation

$$\langle \alpha_x, \alpha_y, \varphi_1, \ldots, \varphi_r \mid \varphi_i \alpha_x \varphi_i^{-1} = w_i,\ \varphi_i \alpha_y \varphi_i^{-1} = v_i \text{ for } 1 \leq i \leq r \rangle$$

where the w_i and v_i are suitable words in α_x, α_y. We have

$$\varphi_i \alpha_x \varphi_i^{-1} = \alpha_{\varphi_i(x)}, \quad \varphi_i \alpha_y \varphi_i^{-1} = \alpha_{\varphi_i(y)}$$

for all i. Hence, from (4.5) it follows that

$$\overline{\alpha_x} = a_i \overline{\alpha_x} + c_i \overline{\alpha_y}, \quad \overline{\alpha_y} = b_i \overline{\alpha_x} + d_i \overline{\alpha_y} \tag{4.6}$$

in the abelianization of $\Gamma^+(G,\pi)$. This yields that $\Gamma^+(G,\pi)^{\mathrm{ab}}$ is the abelian group generated by $\overline{\alpha_x}, \overline{\alpha_y}$ and $\overline{\varphi_i}, 1 \leq i \leq r$, subject to the relations (4.6). Observe that $\left(\begin{smallmatrix} 1 & 0 \\ n & 1 \end{smallmatrix}\right) \in \Gamma(m,n)$. Hence this matrix is a product of the M_i and one consequence of the relations (4.6) is

$$\overline{\alpha_x} = \overline{\alpha_x} + n\overline{\alpha_y}.$$

We thus find that $n\overline{\alpha_y} = 0$. Similarly we find that $m\overline{\alpha_x} = 0$. Obviously we can rewrite the defining relations (4.6) as

$$(a_i - 1)\overline{\alpha_x} = c_i \overline{\alpha_y}, \quad (1 - d_i)\overline{\alpha_y} = b_i \overline{\alpha_x}. \tag{4.7}$$

By definition of $\Gamma(m,n)$, we have

$$(a_i - 1) \equiv b_i \equiv 0 \mod m, \quad (1 - d_i) \equiv c_i \equiv 0 \mod n$$

for all i so that all relations in (4.7) are consequences of $m\overline{\alpha_x} = 0$ and $n\overline{\alpha_y} = 0$. Hence we obtain a presentation

$$\Gamma^+(G,\pi)^{\mathrm{ab}} = \langle \overline{\alpha_x}, \overline{\alpha_y}, \overline{\varphi_1}, \ldots, \overline{\varphi_r} \mid \text{abelian}, \ m\overline{\alpha_x} = 0, \ n\overline{\alpha_y} = 0 \rangle.$$

This proves $\Gamma^+(G,\pi)^{\mathrm{ab}} \cong G \times \mathbb{Z}^r$. The three special cases can be obtained by an explicit computation. One can also refer to Table 1.1 in Section 1.3: by Theorem 4.5 one sees that the groups Δ obtained in the computation, are actually equal to $\Gamma^+(G,\pi)$ in these cases, since they have the same index in $\mathrm{Aut}^+(F_2)$. □

4.3 Congruence Subgroups associated to Dihedral Groups

In this section we prove Theorem D on standard congruence subgroups of $\mathrm{Aut}^+(F_2)$ associated to dihedral groups. Again, we determine the indices of these groups in $\mathrm{Aut}^+(F_2)$. We also determine, up to conjugation, their images in $\mathrm{SL}_2(\mathbb{Z})$ under the standard representation. Using this, we obtain the somewhat surprising fact that congruence subgroups of $\mathrm{Aut}^+(F_2)$ associated to dihedral groups are always generated by four elements. From this we draw some interesting conclusions about finite-index subgroups of $\mathrm{Aut}^+(F_2)$.

4.3.1 Index and Generation of Congruence Subgroups associated to Dihedral Groups

Our aim in this section is to prove

Theorem 4.12. *Let $n \geq 3$ and D_n be the dihedral group of order $2n$.*

(i) Up to conjugation, $\Gamma^+(D_n,\pi)$ only depends on n, but not on the epimorphism $\pi : F_2 \to D_n$.

(ii) The index of $\Gamma^+(D_n,\pi)$ in $\mathrm{Aut}^+(F_2)$ is $6n$.

(iii) *The image* $\rho(\Gamma^+(D_n,\pi)) \leq \mathrm{SL}_2(\mathbb{Z})$ *is conjugate to* $\Gamma_1(2)$ *if* n *is odd and to* $\Gamma(2)$ *if* n *is even.*

(iv) *The group* $\Gamma^+(D_n,\pi)$ *is generated by four elements.*

This result is also contained in the joint work [3] of Ribnere and the author. There one also finds the following interesting observation.

Corollary 4.13. *The special automorphism group* $\mathrm{Aut}^+(F_2)$*, and hence also* $\mathrm{Aut}(F_2)$*, has subgroups of arbitrary large index, generated by four elements.*

Comparing this to Corollary 2.18, we see that $\mathrm{Aut}^+(F_2)$ behaves in this respect very different than $\mathrm{SL}_2(\mathbb{Z})$. Furthermore, $\mathrm{SL}_2(\mathbb{Z})$ contains free finite index subgroups, e.g., $\Gamma(5)$. In contrast to that, we have

Corollary 4.14. *(i) Let* $U \leq \mathrm{Aut}(F_2)$ *be a subgroup of finite index* m *in* $\mathrm{Aut}(F_2)$*. Then* U *has subgroups of arbitrary large finite index, generated by* $3m+1$ *elements.*

(ii) *Finite index subgroups of* $\mathrm{Aut}(F_2)$ *cannot be written as non-trivial free products.*

(iii) *The special automorphism group* $\mathrm{Aut}^+(F_2)$ *does not have an epimorphism with finite kernel onto a non-trivial free product.*

Proof. For part (i) we observe that, as n increases, the subgroups $U \cap \Gamma^+(D_n,\pi) \leq U$ have arbitrary large finite index in U. Since U has index m in $\mathrm{Aut}(F_2)$, we find that $[\Gamma^+(D_n,\pi) : U \cap \Gamma^+(D_n,\pi)] \leq m$. The Schreier formula and the fact that $\Gamma^+(D_n,\pi)$ is generated by four elements yield part (i).

Now we consider part (ii). Let $U \leq \mathrm{Aut}(F_2)$ be a subgroup of finite index m in $\mathrm{Aut}(F_2)$. Assume that U can be written as a free product, say $U \cong G_1 * \cdots * G_k$, $k \geq 2$, with non-trivial groups G_i. Since U is finitely generated, so are all the G_i, by Lemma 2.11. By part (i), U has a subgroup V of arbitrary large index n such that $\mathrm{d}(V) \leq 3m+1$. However, unless $U \cong C_2 * C_2$, Corollary 2.14 yields that $\mathrm{d}(V) \geq cn+1$ with $c > 0$. Hence we only need to show that $U \ncong C_2 * C_2$. To this end, assume $U \cong C_2 * C_2$. Note that in this case $U \cong D_\infty$ is solvable. Since

U has finite index in $\mathrm{Aut}(F_2)$, it follows that $U \cap \mathrm{IA}_2$ is non-trivial. Now on the one hand $U \cap \mathrm{IA}_2$ is solvable, but on the other hand $U \cap \mathrm{IA}_2$ is also free, contradiction. This proves part (ii).

For part (iii) we first recall that $\mathrm{Aut}^+(F_2)$ is finitely generated. Therefore, by part (ii) of Lemma 2.11, it suffices to show that $\mathrm{Aut}^+(F_2)$ does not have an epimorphism with finite kernel onto a non-trivial free product of finitely generated groups. Moreover, by Corollary 2.16, it suffices to show that there is no epimorphism $\mathrm{Aut}^+(F_2) \to C_2 * C_2$ with finite kernel. Suppose there is such an epimorphism. From the presentation of $\mathrm{Aut}^+(F_2)$ given in Section 2.2, we obtain $(\mathrm{Aut}^+(F_2))^{\mathrm{ab}} \cong C_{12}$. So this epimorphism induces an epimorphism $C_{12} \cong (\mathrm{Aut}^+(F_2))^{\mathrm{ab}} \to (C_2 * C_2)^{\mathrm{ab}} \cong C_2 \times C_2$, which is clearly impossible. □

Let us now prove Theorem 4.12. A presentation of the dihedral group D_n is given by

$$D_n = \langle r, s \mid r^n = 1,\ s^2 = 1,\ rs = sr^{-1} \rangle.$$

The group contains exactly $2n$ elements, namely

$$1, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}.$$

If n is odd, the center $\mathrm{Z}(D_n)$ of D_n is trivial. For even n its center has order 2 and we have $\mathrm{Z}(D_n) = \langle r^{\frac{n}{2}} \rangle$.

Statement (i) of Theorem 4.12 follows from

Lemma 4.15. *Let $n \geq 3$ and D_n be the dihedral group of order $2n$. The group D_n has only one T_2-system. Moreover, D_n has exactly $3\phi(n)n$ generating pairs.*

Proof. First we show that the elements $sr^a, r^b \in D_n$, $a, b \in \mathbb{Z}$, generate D_n if and only if $\langle r^b \rangle = \langle r \rangle$, i.e., $\gcd(n, b) = 1$.

Suppose that $\langle sr^a, r^b \rangle = D_n$. Observe that sr^a has order 2 and r^b has order dividing n. Moreover, since $sr^a \cdot r^b \cdot (sr^a)^{-1} = r^{-b}$, the subgroup $\langle r^b \rangle \leq D_n$ is normal. Hence every element of D_n can be written as $(sr^a)^c (r^b)^d$ with suitable $0 \leq c \leq 1$ and $0 \leq d \leq \mathrm{ord}(r^b) - 1$. It follows that $\mathrm{ord}(r^b) = n$, that is, $\langle r^b \rangle = \langle r \rangle$. The converse implication is clear.

Now consider the exact sequence

$$1 \longrightarrow \langle r \rangle \longrightarrow D_n \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 1.$$

By Proposition 4.10, the graph $\mathbf{V}_2(\mathbb{Z}/2\mathbb{Z})$ is connected. Therefore, every connected component of $\mathbf{V}_2(D_n)$ contains a lift of the generating pair $(1,0)$ of $\mathbb{Z}/2\mathbb{Z}$, that is, a pair of the form (sr^a, r^b) with $\gcd(n,b) = 1$. The same orbit also contains (s, r^b). One easily verifies that the map induced by $s \mapsto s$, $r \mapsto r^b$ yields an automorphism of D_n. Hence D_n has only one T_2-system.

Since $\mathbf{V}_2(\mathbb{Z}/2\mathbb{Z})$ is connected, we know, by Lemma 2.7, that each generating pair of $\mathbb{Z}/2\mathbb{Z}$ has the same number of lifts to D_n. Finally, since the generating pair $(1,0)$ has exactly $\phi(n)n$ lifts, namely (sr^a, r^b) with $1 \leq a, b \leq n$, $\gcd(b,n) = 1$, and $\mathbb{Z}/2\mathbb{Z}$ has exactly 3 generating pairs, the proof is complete. □

Next we show that the image $\rho(\Gamma^+(D_n, \pi))$ is conjugate to $\Gamma_1(2)$ if n is odd and to $\Gamma(2)$ if n is even. Since we already know that, up to conjugation, $\Gamma^+(D_n, \pi)$ does not depend on π, it suffices to consider the epimorphism $\pi_0 : F_2 \to D_n$ given by $\pi_0(x) = r$ and $\pi_0(y) = s$.

We know from Subsection 4.1.1 that $\rho(\Gamma^+(D_n, \pi_0))$ is a subgroup of $\rho(\Gamma^+(D_n^{\mathrm{ab}}, \bar{\pi}_0))$, where $\bar{\pi}_0$ is the epimorphism π_0 followed by the natural projection onto the abelian quotient $D_n^{\mathrm{ab}} = D_n/D_n'$. We have

$$\begin{aligned} D_n^{\mathrm{ab}} &= \langle \bar{s} \mid 2\bar{s} = 0 \rangle \cong \mathbb{Z}/2\mathbb{Z}, && \text{for } n \text{ odd}, \\ D_n^{\mathrm{ab}} &= \langle \bar{r}, \bar{s} \mid 2\bar{r} = 0, 2\bar{s} = 0, \bar{r} + \bar{s} = \bar{s} + \bar{r} \rangle \cong (\mathbb{Z}/2\mathbb{Z})^2 && \text{for } n \text{ even} \end{aligned}$$

where $\bar{r}$ and $\bar{s}$ are the images of r and s in D_n^{ab}, respectively. Hence

$$\rho(\Gamma^+(D_n, \pi_0)) \leq \begin{cases} \Gamma_1(2) \text{ if } n \text{ is odd} \\ \Gamma(2) \text{ if } n \text{ is even.} \end{cases} \tag{4.8}$$

Observe that the following automorphisms are in $\Gamma^+(D_n, \pi_0)$.

$$\gamma_1 = \begin{cases} x \mapsto yx^{-1}y \\ y \mapsto y^{-1} \end{cases} \qquad \gamma_2 = \begin{cases} x \mapsto x \\ y \mapsto xyx \end{cases}$$

$$\gamma_3 = \begin{cases} x \mapsto y^2x \\ y \mapsto y \end{cases} \qquad \gamma_4 = \begin{cases} x \mapsto x \\ y \mapsto x^n y \end{cases}$$

For the reader's convenience we include their inverses.

$$\gamma_1^{-1} = \begin{cases} x \mapsto y^{-1}x^{-1}y^{-1} \\ y \mapsto y^{-1} \end{cases} \qquad \gamma_2^{-1} = \begin{cases} x \mapsto x \\ y \mapsto x^{-1}yx^{-1} \end{cases}$$

$$\gamma_3^{-1} = \begin{cases} x \mapsto y^{-2}x \\ y \mapsto y \end{cases} \qquad \gamma_4^{-1} = \begin{cases} x \mapsto x \\ y \mapsto x^{-n}y \end{cases}$$

The images of the automorphisms $\gamma_1, \ldots, \gamma_4$ under ρ are given by $\left(\begin{smallmatrix} -1 & 0 \\ 2 & -1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 0 \\ 2 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$, respectively. For odd n these matrices generate $\Gamma_1(2)$ and for even n they generate $\Gamma(2)$. Therefore equality holds in (4.8), which proves statement (iii) of Theorem 4.12.

By Proposition 3.1, we know that $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_1(2)] = 3$ and that $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(2)] = 6$. Hence Corollary 4.4 yields that the index of $\Gamma^+(D_n, \pi)$ in $\mathrm{Aut}^+(F_2)$ is given by

$$[\mathrm{SL}_2(\mathbb{Z}) : \rho(\Gamma^+(D_n, \pi))] \cdot |\operatorname{Inn}(D_n)| = \begin{cases} 3 \cdot 2n = 6n, & \text{for } n \text{ odd} \\ 6 \cdot n = 6n, & \text{for } n \text{ even.} \end{cases}$$

So statement (ii) of Theorem 4.12 is proved.

To prove statement (iv), we show that the automorphisms $\gamma_1, \ldots, \gamma_4$ introduced above generate $\Gamma^+(D_n, \pi_0)$. Considering the sequence

$$1 \longrightarrow \mathrm{IA}_2 \cap \Gamma^+(D_n, \pi_0) \longrightarrow \Gamma^+(D_n, \pi_0) \xrightarrow{\rho} \rho(\Gamma^+(D_n, \pi_0)) \longrightarrow 1$$

we see that $\Gamma^+(D_n, \pi_0)$ is generated by the generators of $\mathrm{IA}_2 \cap \Gamma^+(D_n, \pi_0)$ together with preimages of the generators of $\rho(\Gamma^+(D_n, \pi_0))$. Therefore we compute generators of $\mathrm{IA}_2 \cap \Gamma^+(D_n, \pi_0)$ and of $\rho(\Gamma^+(D_n, \pi_0))$, using the

Reidemeister method [19, Thm. 2.7], and then show that each generator can be written as a product of $\gamma_1^{\pm 1}, \ldots, \gamma_4^{\pm 1}$.

We first focus on the case that n is odd. In this case the center of D_n is trivial. So Lemma 4.3 yields an isomorphism

$$\mathrm{IA}_2 \cap \Gamma^+(D_n, \pi_0) \backslash \mathrm{IA}_2 \xrightarrow{\sim} D_n, \quad [\alpha_w] \mapsto \pi_0(w).$$

Hence a set of right coset representatives of $\mathrm{IA}_2 \cap \Gamma^+(D_n, \pi_0)$ in IA_2 is given by

$$\mathrm{id}_{F_2}, \alpha_x, \alpha_{x^2}, \ldots, \alpha_{x^{n-1}}, \alpha_y, \alpha_{yx}, \ldots, \alpha_{yx^{n-1}}.$$

For an automorphism $\alpha_w \in \mathrm{IA}_2 = \mathrm{Inn}(F_2)$, we write $\overline{\alpha_w}$ for its representative, taken from the above list. The Reidemeister method says that $\mathrm{IA}_2 \cap \Gamma^+(D_n, \pi_0)$ is generated by

$$K\alpha_x \overline{K\alpha_x}^{-1} \quad \text{and} \quad K\alpha_y \overline{K\alpha_y}^{-1}$$

where K runs through the above list of representatives. We first compute the elements that are given by $K\alpha_x \overline{K\alpha_x}^{-1}$. For $0 \leq k \leq n-2$ we have

$$\alpha_{x^k} \alpha_x \overline{\alpha_{x^k} \alpha_x}^{-1} = \alpha_{x^{k+1}} \alpha_{x^{k+1}}^{-1} = \mathrm{id}_{F_2}.$$

For $k = n-1$ we find

$$\alpha_{x^{n-1}} \alpha_x \overline{\alpha_{x^{n-1}} \alpha_x}^{-1} = \alpha_{x^n} \, \mathrm{id}_{F_2} = \alpha_{x^n}.$$

Again for $0 \leq k \leq n-2$ we have

$$\alpha_{yx^k} \alpha_x \overline{\alpha_{yx^k} \alpha_x}^{-1} = \alpha_{yx^{k+1}} \alpha_{yx^{k+1}}^{-1} = \mathrm{id}_{F_2}.$$

For $k = n-1$ we have

$$\alpha_{yx^{n-1}} \alpha_x \overline{\alpha_{yx^{n-1}} \alpha_x}^{-1} = \alpha_{yx^n} \alpha_y^{-1} = \alpha_{yx^n y^{-1}}.$$

Let us now consider $K\alpha_y \overline{K\alpha_y}^{-1}$. Clearly we have

$$\mathrm{id}_{F_2} \, \alpha_y \overline{\mathrm{id}_{F_2} \, \alpha_y}^{-1} = \mathrm{id}_{F_2}.$$

For $1 \leq k \leq n-1$ we find

$$\alpha_{x^k} \alpha_y \overline{\alpha_{x^k} \alpha_y}^{-1} = \alpha_{x^k y} \alpha_{yx^{n-k}}^{-1} = \alpha_{x^k y x^{k-n} y^{-1}}.$$

Next we find

$$\alpha_y \alpha_y \overline{\alpha_y \alpha_y}^{-1} = \alpha_{y^2} \,\mathrm{id}_{F_2} = \alpha_{y^2}.$$

Finally, for $1 \le k \le n-1$ we have

$$\alpha_{yx^k} \alpha_y \overline{\alpha_{yx^k} \alpha_y}^{-1} = \alpha_{yx^k y} \alpha_{x^{n-k}}^{-1} = \alpha_{yx^k yx^{k-n}}.$$

We collect and rewrite the set of generators that we have found as

$$\alpha_{x^n},\ \alpha_{y^2},\ \alpha_{yx^n y^{-1}},\ \alpha_{x^k yx^{k-n} y},\ \alpha_{yx^k yx^{k-n}}\ (1 \le k \le n-1).$$

Since IA_2 is free of rank 2 and $\mathrm{IA}_2 \cap \Gamma^+(D_n, \pi_0)$ is a subgroup of index $2n$, the Schreier formula yields that $\mathrm{IA}_2 \cap \Gamma^+(D_n, \pi_0)$ is free of rank $2n+1$. The above set of generators contains exactly $2n+1$ elements so that $\mathrm{IA}_2 \cap \Gamma^+(D_n, \pi_0)$ is freely generated by these. We have

$$\rho(\Gamma^+(D_n, \pi_0)) = \Gamma_1(2) = \left\langle \left(\begin{smallmatrix} 1 & 0 \\ 2 & 1 \end{smallmatrix}\right),\ \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \right\rangle.$$

Let

$$\varphi_1 = \begin{cases} x \mapsto xy^2 \\ y \mapsto y \end{cases} \qquad \text{and} \quad \varphi_2 = \begin{cases} x \mapsto x \\ y \mapsto x^{\frac{1-n}{2}} y x^{\frac{n+1}{2}} \end{cases}$$

so that $\rho(\varphi_1) = \left(\begin{smallmatrix} 1 & 0 \\ 2 & 1 \end{smallmatrix}\right)$ and $\rho(\varphi_2) = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. An easy computation shows that these are elements of $\Gamma^+(D_n, \pi_0)$. Hence $\Gamma^+(D_n, \pi_0)$ is generated by

$$\begin{aligned} &\varphi_1,\ \varphi_2,\ \alpha_{x^n},\ \alpha_{y^2},\ \alpha_{yx^n y^{-1}}, \\ &\alpha_{x^k yx^{k-n} y},\ \alpha_{yx^k yx^{k-n}}\ (1 \le k \le n-1). \end{aligned}$$

The following formulas can be verified by elementary computations.

Lemma 4.16. *The following identities hold.*

$$\begin{aligned} \varphi_1 &= \gamma_3^{-2} \gamma_1^{-2} \gamma_3 \\ \varphi_2 &= \gamma_2^{n+1} \gamma_4^{-1} \gamma_2^{-\frac{n+1}{2}} \\ \alpha_{x^n} &= \gamma_4^2 \gamma_2^{-n} \\ \alpha_{y^2} &= \gamma_1^2 \gamma_3^2 \\ \alpha_{yx^n y^{-1}} &= \gamma_1^{-1} \gamma_3^{-1} \gamma_4^{-2} \gamma_2^n \gamma_1^{-1} \gamma_3^{-1} \\ \alpha_{yx^k yx^{k-n}} &= \gamma_3 \gamma_1 \gamma_4^{-1} \gamma_2^k \gamma_3^{-1} \gamma_1^{-1} \gamma_4 \gamma_2^{n-k} \gamma_4^{-2} \\ \alpha_{x^k yx^{k-n} y} &= \gamma_4^2 \gamma_2^{-n} \gamma_4^{-1} \gamma_2^k \gamma_3 \gamma_1 \gamma_4 \gamma_2^{-k} \gamma_3^{-1} \gamma_1^{-1} \end{aligned}$$

for $1 \le k \le n-1$.

Now we consider the case where n is even. Note that, in this case, D_n has center $\langle r^{\frac{n}{2}} \rangle$ and $\mathrm{Inn}(D_n) \cong D_{\frac{n}{2}}$. By a similar computation as above, we find that $\mathrm{IA}_2 \cap \Gamma^+(D_n, \pi_0)$ is free on

$$\alpha_{x^{\frac{n}{2}}},\ \alpha_{y^2},\ \alpha_{yx^{\frac{n}{2}}y^{-1}},\ \alpha_{yx^kyx^{k-\frac{n}{2}}},\ \alpha_{x^kyx^{k-\frac{n}{2}}y}\ (1 \le k \le n/2-1).$$

Furthermore,

$$\rho(\Gamma^+(D_n, \pi_0)) = \Gamma(2) = \left\langle \left(\begin{smallmatrix} 1 & 0 \\ 2 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \right\rangle.$$

The automorphisms

$$\psi_1 = \begin{cases} x \mapsto xy^2 \\ y \mapsto y \end{cases}, \quad \psi_2 = \begin{cases} x \mapsto x \\ y \mapsto xyx \end{cases} \quad \text{and} \quad \psi_3 = \begin{cases} x \mapsto y^{-1}x^{-1}y \\ y \mapsto y^{-1} \end{cases}$$

are in $\Gamma^+(D_n, \pi_0)$ and also preimages of the generators of $\Gamma(2)$. So $\Gamma^+(D_n, \pi_0)$ is generated by

$$\psi_1,\ \psi_2,\ \psi_3,\ \alpha_{x^{\frac{n}{2}}},\ \alpha_{y^2},\ \alpha_{yx^{\frac{n}{2}}y^{-1}},$$
$$\alpha_{x^kyx^{k-\frac{n}{2}}y},\ \alpha_{yx^kyx^{k-\frac{n}{2}}}\ (1 \le k \le n/2-1).$$

As before, we show that all generators of $\Gamma^+(D_n, \pi_0)$ can be expressed as products of $\gamma_1^{\pm 1}, \ldots, \gamma_4^{\pm 1}$.

Lemma 4.17. *We have*

$$\begin{aligned}
\psi_1 &= \gamma_3^{-2}\gamma_1^{-2}\gamma_3 \\
\psi_2 &= \gamma_2 \\
\psi_3 &= \gamma_1^{-1}\gamma_3\gamma_1^2 \\
\alpha_{x^{\frac{n}{2}}} &= \gamma_4\gamma_2^{-\frac{n}{2}} \\
\alpha_{y^2} &= \gamma_1^2\gamma_3^2 \\
\alpha_{yx^{\frac{n}{2}}y^{-1}} &= \gamma_1^{-1}\gamma_3^{-1}\gamma_4^{-1}\gamma_2^{\frac{n}{2}}\gamma_1^{-1}\gamma_3^{-1} \\
\alpha_{yx^kyx^{k-\frac{n}{2}}} &= \gamma_3\gamma_1\gamma_2^k\gamma_3^{-2}\gamma_1^{-2}\gamma_3\gamma_1\gamma_2^{\frac{n}{2}-k}\gamma_4^{-1} \\
\alpha_{x^kyx^{k-\frac{n}{2}}y} &= \gamma_2^k\gamma_3^{-2}\gamma_1^{-2}\gamma_3\gamma_1\gamma_3^{-2}\gamma_1^{-2}\gamma_4\gamma_2^{-\frac{n}{2}-k}\gamma_3^{-2}\gamma_1^{-2}\gamma_3\gamma_1
\end{aligned}$$

for $1 \le k \le n/2-1$.

This completes the proof of statement (iv) of Theorem 4.12.

We remark that our proof of Theorem 4.12 (iv) is a very direct one. It would be interesting to see if there is also a more conceptual way to prove this statement. (See also the remarks after Theorem 4.24 about a generalization of this result.)

4.3.2 Product Replacement Graphs of Dihedral Groups

From our results in the previous section we obtain the following description of the product replacement graph of a dihedral group.

Corollary 4.18. *Let $n \geq 3$ and D_n be the dihedral group of order $2n$. Then D_n has exactly $3\phi(n)n$ generating pairs and $\mathbf{V}_2(D_n)$ has exactly $\phi(n)/2$ connected components, each of size $6n$. Moreover, D_n has only one T_2-system.*

Proof. The number of generating pairs of D_n and the fact that D_n has only one T_2-system was already shown in Lemma 4.15. Since the size of the components is just the index of $\Gamma^+(D_n, \pi)$ in $\mathrm{Aut}^+(F_2)$ for the corresponding π, part (ii) of Theorem 4.12 completes the proof. □

4.3.3 The Abelianization of Congruence Subgroups associated to Dihedral Groups

The aim of this section is to prove

Theorem 4.19. *Let $n \geq 3$ and $\pi : F_2 \to D_n$ be an epimorphism. Then*

$$\Gamma^+(D_n, \pi)^{\mathrm{ab}} \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^2, & n \text{ odd} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^3, & n \text{ even.} \end{cases}$$

Our first step to prove this result is to use the exact sequence

$$1 \longrightarrow \mathrm{IA}_2 \cap \Gamma^+(D_n, \pi_0) \longrightarrow \Gamma^+(D_n, \pi_0) \xrightarrow{\rho} \rho(\Gamma^+(D_n, \pi_0)) \longrightarrow 1$$

to determine a presentation of $\Gamma^+(D_n, \pi_0)$. We point out that we do not intend to simplify this presentation. We only use it as a tool to prove the desired result.

Let us first focus on the case that n is odd. We have already seen that, in this case, $\Gamma^+(D_n, \pi_0)$ is generated by

$$\varphi_1,\ \varphi_2,\ \alpha_{x^n},\ \alpha_{y^2},\ \alpha_{yx^ny^{-1}},\ \alpha_{x^kyx^{k-n}y},\ \alpha_{yx^kyx^{k-n}}\ (1 \leq k \leq n-1)$$

where

$$\varphi_1 = \begin{cases} x \mapsto xy^2 \\ y \mapsto y \end{cases} \quad \text{and} \quad \varphi_2 = \begin{cases} x \mapsto x \\ y \mapsto x^{\frac{1-n}{2}} y x^{\frac{n+1}{2}}. \end{cases}$$

Using the Reidemeister-Schreier method [19, Sec. 2.3] one can compute a presentation of $\rho(\Gamma^+(D_n, \pi_0)) = \Gamma_1(2)$. We have

$$\Gamma_1(2) = \langle M_1 = \left(\begin{smallmatrix} 1 & 0 \\ 2 & 1 \end{smallmatrix}\right), M_2 = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \mid (M_1 M_2^{-1})^4, M_1 M_2^{-1} M_1^2 M_2^{-1} M_1 M_2^{-2} \rangle.$$

Observe that $\rho(\varphi_1) = M_1$ and $\rho(\varphi_2) = M_2$. To ease notation a bit we write

$$\begin{aligned} &a_1 := \alpha_{x^n}, \quad a_2 := \alpha_{y^2}, \quad a_3 := \alpha_{yx^n y^{-1}}, \\ &b_k := \alpha_{yx^k yx^{k-n}}, \quad c_k := \alpha_{x^k yx^{k-n} y}, \quad 1 \le k \le n-1. \end{aligned}$$

By Proposition 2.1, in order to obtain a presentation of $\Gamma^+(D_n, \pi_0)$, we have to express the elements $(\varphi_1\varphi_2^{-1})^4$, $\varphi_1\varphi_2^{-1}\varphi_1^2\varphi_2^{-1}\varphi_1\varphi_2^{-2}$ and $\varphi_i a_j \varphi_i^{-1}$, $\varphi_i b_j \varphi_i^{-1}$, $\varphi_i c_j \varphi_i^{-1}$ as words in a_1, a_2, a_3, b_k, c_k. It is an elementary (though rather long) computation to verify the following result. To avoid case distinctions, we omit the cases $n = 3$ or 5. In these cases, one can refer to Table 1.1 in Section 1.3.

Proposition 4.20. *For odd $n \ge 7$, the group $\Gamma^+(D_n, \pi_0)$ is generated by the elements $\varphi_1, \varphi_2, a_1, a_2, a_3$ and b_k, c_k $(1 \le k \le n-1)$ subject to the following relations.*

(A)

$$\begin{aligned} \varphi_1 a_1 \varphi_1^{-1} &= c_1 a_2^{-1} b_{n-1} \cdots c_l a_2^{-1} b_{n-l} \cdots c_{n-1} a_2^{-1} b_1 \cdot a_1 a_2 \\ \varphi_2 a_1 \varphi_2^{-1} &= a_1 \\ \varphi_1 a_2 \varphi_1^{-1} &= a_2 \\ \varphi_2 a_2 \varphi_2^{-1} &= a_1^{-1} c_{\frac{n+1}{2}} a_2^{-1} b_{\frac{n+1}{2}} a_1 \\ \varphi_1 a_3 \varphi_1^{-1} &= b_1 c_{n-1} a_2^{-1} \cdots b_l c_{n-l} a_2^{-1} \cdots b_{n-1} c_1 a_2^{-1} \cdot a_3 a_2 \\ \varphi_2 a_3 \varphi_2^{-1} &= a_1^{-1} c_{\frac{n+1}{2}} a_2^{-1} a_3 a_2 c_{\frac{n+1}{2}}^{-1} a_1 \end{aligned}$$

(B)

$$\begin{aligned} \varphi_1 b_k \varphi_1^{-1} &= b_1 c_{n-1} a_2^{-1} \cdots b_l c_{n-l} a_2^{-1} \cdots b_{k-1} c_{n-k+1} a_2^{-1} \\ &\quad \cdot b_k \cdot b_{k+1}^{-1} a_2 c_{n-k-1}^{-1} \cdots b_l^{-1} a_2 c_{n-l}^{-1} \cdots b_{n-1}^{-1} a_2 c_1^{-1} \\ \varphi_2 b_k \varphi_2^{-1} &= \begin{cases} a_1^{-1} c_{\frac{n+1}{2}} a_2^{-1} b_{\frac{n+1}{2}+k}, & 1 \le k \le \frac{n-3}{2} \\ a_1^{-1} c_{\frac{n+1}{2}} a_2^{-1} a_3 a_2, & k = \frac{n-1}{2} \\ a_1^{-1} c_{\frac{n+1}{2}} a_2^{-1} a_3 b_{k-\frac{n-1}{2}} a_1, & \frac{n+1}{2} \le k \le n-1 \end{cases} \end{aligned}$$

(C)

$$\begin{aligned}
\varphi_1 c_k \varphi_1^{-1} &= c_1 \cdot a_2^{-1} b_{n-1} c_2 \cdots a_2^{-1} b_l c_{n-l+1} \cdots a_2^{-1} b_{n-k+1} c_k \\
&\quad \cdot c_{k+1}^{-1} b_{n-k-1}^{-1} a_2 \cdots c_l^{-1} b_{n-l}^{-1} a_2 \cdots c_{n-1}^{-1} b_1^{-1} a_2 \\
\varphi_2 c_k \varphi_2^{-1} &= \begin{cases} a_1^{-1} c_{\frac{n+1}{2}+k} a_2^{-1} a_3^{-1} b_{\frac{n+1}{2}} a_1, & 1 \le k \le \frac{n-3}{2} \\ a_3^{-1} b_{\frac{n+1}{2}} a_1, & k = \frac{n-1}{2} \\ c_{k-\frac{n-1}{2}} a_2^{-1} b_{\frac{n+1}{2}} a_1, & \frac{n+1}{2} \le k \le n-1 \end{cases}
\end{aligned}$$

(D)

$$\begin{aligned}
(\varphi_1 \varphi_2^{-1})^4 &= c_1 a_2^{-1} b_{n-1} \cdots c_l a_2^{-1} b_{n-l} \cdots c_{\frac{n-1}{2}} a_2^{-1} b_{\frac{n+1}{2}} \\
&\quad \cdot c_{\frac{n+1}{2}} a_2^{-1} a_3^{-1} \\
&\quad \cdot a_2 c_1^{-1} b_{n-1}^{-1} \cdots a_2 c_l^{-1} b_{n-l}^{-1} \cdots a_2 c_{\frac{n-1}{2}}^{-1} b_{\frac{n+1}{2}}^{-1} \\
&\quad \cdot a_2 c_{\frac{n+1}{2}}^{-1} a_1 \\
\varphi_1 \varphi_2^{-1} \varphi_1^2 \varphi_2^{-1} \varphi_1 \varphi_2^{-2} &= c_1 a_2^{-1} b_{n-1} \cdots c_l a_2^{-1} b_{n-l} \cdots c_{\frac{n-1}{2}} a_2^{-1} b_{\frac{n+1}{2}} \\
&\quad \cdot c_{\frac{n+1}{2}} \\
&\quad \cdot c_{\frac{n+3}{2}}^{-1} b_{\frac{n-1}{2}}^{-1} a_2 \cdots c_l^{-1} b_{n-l+1}^{-1} a_2 \cdots c_{n-2}^{-1} b_3^{-1} a_2 \\
&\quad \cdot c_{n-1}^{-1} b_2^{-1} a_1^{-1} b_1^{-1} a_3^{-1} a_2 c_1^{-1} a_1
\end{aligned}$$

Recall that, in Section 4.3.1, we have introduced the following elements of $\Gamma^+(D_n, \pi_0)$.

$$\gamma_1 = \begin{cases} x \mapsto y x^{-1} y \\ y \mapsto y^{-1} \end{cases} \qquad \gamma_2 = \begin{cases} x \mapsto x \\ y \mapsto xyx \end{cases}$$

$$\gamma_3 = \begin{cases} x \mapsto y^2 x \\ y \mapsto y \end{cases} \qquad \gamma_4 = \begin{cases} x \mapsto x \\ y \mapsto x^n y \end{cases}$$

In Lemma 4.16 we have written the elements φ_1, φ_2, a_1, a_2, a_3, b_k and c_k as words in $\gamma_1^{\pm 1}, \ldots, \gamma_4^{\pm 1}$. Conversely, we have

Lemma 4.21. *The following identities hold.*

$$\gamma_1 = \varphi_2^{-1}\varphi_1\varphi_2^{-1}a_1^{-1}c_{\frac{n+1}{2}} \cdot a_2^{-1}b_{\frac{n+1}{2}}c_{\frac{n-1}{2}} \cdot a_2^{-1}b_{\frac{n+3}{2}}c_{\frac{n-3}{2}} \cdots a_2^{-1}b_{n-1}c_1 \cdot a_2^{-1}a_3a_2$$
$$\gamma_2 = a_1\varphi_2^2$$
$$\gamma_3 = a_2\varphi_1$$
$$\gamma_4 = (a_1\varphi_2^2)^{-\frac{n+1}{2}}\varphi_2^{-1}(a_1\varphi_2^2)^{n+1}$$

We now turn to the case that n is even. We already know that, in this case, $\Gamma^+(D_n, \pi_0)$ is generated by

$$\psi_1,\ \psi_2,\ \psi_3,\ \alpha_{x^{\frac{n}{2}}},\ \alpha_{y^2},\ \alpha_{yx^{\frac{n}{2}}y^{-1}},\ \alpha_{yx^kyx^{k-\frac{n}{2}}},\ \alpha_{x^kyx^{k-\frac{n}{2}}y}\ (1 \le k \le n/2-1)$$

where

$$\psi_1 = \begin{cases} x \mapsto xy^2 \\ y \mapsto y \end{cases}, \quad \psi_2 = \begin{cases} x \mapsto x \\ y \mapsto xyx \end{cases} \quad \text{and} \quad \psi_3 = \begin{cases} x \mapsto y^{-1}x^{-1}y \\ y \mapsto y^{-1}. \end{cases}$$

In order not to get confused with the above notation, we shall use other names in this computation, even if some automorphisms coincide with some from the case that n is odd. We therefore write

$$d_1 := \alpha_{x^{\frac{n}{2}}}, \quad d_2 := \alpha_{y^2}, \quad d_3 := \alpha_{yx^{\frac{n}{2}}y^{-1}},$$
$$e_k := \alpha_{yx^kyx^{k-\frac{n}{2}}}, \quad f_k := \alpha_{x^kyx^{k-\frac{n}{2}}y}\ (1 \le k \le n/2-1).$$

The image $\rho(\Gamma^+(D_n, \pi_0)) = \Gamma(2)$ is generated by $N_1 := \rho(\psi_1) = \left(\begin{smallmatrix} 1 & 0 \\ 2 & 1 \end{smallmatrix}\right)$, $N_2 := \rho(\psi_2) = \left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right)$ and $N_3 := \rho(\psi_3) = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ and admits the presentation

$$\Gamma(2) = \langle N_1, N_2, N_3 \mid N_3^2 = 1,\ N_1N_3N_1^{-1}N_3^{-1} = 1,\ N_2N_3N_2^{-1}N_3^{-1} = 1\rangle.$$

This leads us to the following result.

Proposition 4.22. *For even $n \ge 4$, the group $\Gamma^+(D_n, \pi_0)$ is generated by the elements $\psi_1, \psi_2, \psi_3, d_1, d_2, d_3$ and e_k, f_k $(1 \le k \le n/2-1)$, subject to the following relations.*

(A)

$$\begin{aligned}
\psi_1 d_1 \psi_1^{-1} &= f_1 d_2^{-1} e_{\frac{n}{2}-1} \cdots f_l d_2^{-1} e_{\frac{n}{2}-l} \cdots f_{\frac{n}{2}-1} d_2^{-1} e_1 \cdot d_1 d_2 \\
\psi_2 d_1 \psi_2^{-1} &= d_1 \\
\psi_3 d_1 \psi_3^{-1} &= d_2^{-1} d_3^{-1} d_2 \\
\psi_1 d_2 \psi_1^{-1} &= d_2 \\
\psi_2 d_2 \psi_2^{-1} &= f_1 d_2^{-1} d_3 e_1 d_1 \\
\psi_3 d_2 \psi_3^{-1} &= d_2^{-1} \\
\psi_1 d_3 \psi_1^{-1} &= e_1 f_{\frac{n}{2}-1} d_2^{-1} \cdots e_l f_{\frac{n}{2}-l} d_2^{-1} \cdots e_{\frac{n}{2}-1} f_1 d_2^{-1} \cdot d_3 d_2 \\
\psi_2 d_3 \psi_2^{-1} &= f_1 d_2^{-1} d_3 d_2 f_1^{-1} \\
\psi_3 d_3 \psi_3^{-1} &= d_2^{-1} d_1^{-1} d_2
\end{aligned}$$

(B)

$$\begin{aligned}
\psi_1 e_k \psi_1^{-1} &= e_1 \cdot f_{\frac{n}{2}-1} d_2^{-1} e_2 \cdots f_l d_2^{-1} e_{\frac{n}{2}+1-l} \cdots f_{\frac{n}{2}+1-k} d_2^{-1} e_k \\
&\quad \cdot e_{k+1}^{-1} d_2 f_{\frac{n}{2}-1-k}^{-1} \cdots e_l^{-1} d_2 f_{\frac{n}{2}-l}^{-1} \cdots e_{\frac{n}{2}-1}^{-1} d_2 f_1^{-1} \\
\psi_2 e_k \psi_2^{-1} &= \begin{cases} f_1 d_2^{-1} d_3 e_{k+1}, & 1 \le k \le \frac{n}{2} - 2 \\ f_1 d_2^{-1} d_3^2 d_2, & k = \frac{n}{2} - 1 \end{cases} \\
\psi_3 e_k \psi_3^{-1} &= d_2^{-1} d_1^{-1} e_k^{-1} d_3 d_2
\end{aligned}$$

(C)

$$\begin{aligned}
\psi_1 f_k \psi_1^{-1} &= f_1 \cdot d_2^{-1} e_{\frac{n}{2}-1} f_2 \cdots d_2^{-1} e_{\frac{n}{2}-l+1} f_l \cdots d_2^{-1} e_{\frac{n}{2}-k+1} f_k \\
&\quad \cdot f_{k+1}^{-1} e_{\frac{n}{2}-k-1}^{-1} d_2 \cdots f_{\frac{n}{2}-l}^{-1} e_l^{-1} d_2 \cdots f_{\frac{n}{2}-1}^{-1} e_1^{-1} d_2 \\
\psi_2 f_k \psi_2^{-1} &= \begin{cases} f_{k+1} d_2^{-1} e_1 d_1, & 1 \le k \le \frac{n}{2} - 2 \\ d_1 e_1 d_1, & k = \frac{n}{2} - 1 \end{cases} \\
\psi_3 f_k \psi_3^{-1} &= d_2^{-1} d_3^{-1} d_2 f_k^{-1} d_1
\end{aligned}$$

(D)

$$\begin{aligned} \psi_1\psi_3\psi_1^{-1}\psi_3^{-1} &= d_2^{-1} \\ \psi_2\psi_3\psi_2^{-1}\psi_3^{-1} &= d_1^{-1}e_1^{-1}d_2 \\ \psi_3^2 &= 1 \end{aligned}$$

In Lemma 4.17 we have expressed the above generators of the group $\Gamma^+(D_n, \pi_0)$ as words in $\gamma_1^{\pm 1}, \ldots, \gamma_4^{\pm 1}$. Again, we also give the converse result.

Lemma 4.23. *The following holds.*

$$\begin{aligned} \gamma_1 &= \psi_1^{-1}\psi_3 & \gamma_2 &= \psi_2 \\ \gamma_3 &= d_2\psi_1 & \gamma_4 &= d_1\psi_2^{\frac{n}{2}} \end{aligned}$$

Let us give an outline of our strategy for the remaining computations. For brevity we only describe it for the case that n is odd. In Proposition 4.20 we have found a presentation of $\Gamma^+(D_n, \pi_0)$ in terms of the generators φ_i, and a_j, b_k, c_k where $1 \leq i \leq 2$, $1 \leq j \leq 3$ and $1 \leq k \leq n-1$, say

$$\Gamma^+(D_n, \pi_0) = \langle \varphi_i, a_j, b_k, c_k \mid \boldsymbol{R}(\varphi_i, a_j, b_k, c_k) = 1 \rangle.$$

Moreover, in Lemma 4.16 we have written these generators as words in $\gamma_1^{\pm 1}, \ldots, \gamma_4^{\pm 1}$, say

$$\varphi_i = w_{\varphi_i}(\boldsymbol{\gamma}), \quad a_j = w_{a_j}(\boldsymbol{\gamma}), \quad b_k = w_{b_k}(\boldsymbol{\gamma}), \quad c_k = w_{c_k}(\boldsymbol{\gamma}).$$

Conversely, Lemma 4.21 gives us the elements $\gamma_1, \ldots, \gamma_4$ as words in the original generators, i.e.,

$$\gamma_l = v_l(\varphi_i, a_j, b_k, c_k).$$

By Lemma 2.2 we can thus obtain a new presentation of $\Gamma^+(D_n, \pi_0)$ by

$$\begin{aligned} \Gamma^+(D_n, \pi_0) = \langle \gamma_1, \ldots, \gamma_4 \mid & \boldsymbol{R}(w_{\varphi_i}(\boldsymbol{\gamma}), w_{a_j}(\boldsymbol{\gamma}), w_{b_k}(\boldsymbol{\gamma}), w_{c_k}(\boldsymbol{\gamma})) = 1, \\ & \gamma_l = v_l(w_{\varphi_i}(\boldsymbol{\gamma}), w_{a_j}(\boldsymbol{\gamma}), w_{b_k}(\boldsymbol{\gamma}), w_{c_k}(\boldsymbol{\gamma})) \rangle. \end{aligned}$$

We shall use this presentation to obtain one of $\Gamma^+(D_n, \pi_0)^{\mathrm{ab}}$. However, we will not immediately plug in the words $w_{\varphi_i}(\boldsymbol{\gamma})$, $w_{a_j}(\boldsymbol{\gamma})$, $w_{b_k}(\boldsymbol{\gamma})$ and $w_{c_k}(\boldsymbol{\gamma})$ in the relations $\boldsymbol{R}$. Instead, we first try to simplify these relations, that is, we proceed as follows.

(1) We compute the images of $w_{\varphi_i}(\boldsymbol{\gamma})$, $w_{a_j}(\boldsymbol{\gamma})$, $w_{b_k}(\boldsymbol{\gamma})$ and $w_{c_k}(\boldsymbol{\gamma})$ in $\Gamma^+(D_n, \pi_0)^{\mathrm{ab}}$ to find some additional relations between the generators φ_i, a_j, b_k and c_k in the abelianization and to thus ease notation. (As we shall see a lot will cancel out, if we proceed this way.)

(2) We consider the relations in $\Gamma^+(D_n, \pi_0)^{\mathrm{ab}}$ imposed by $\boldsymbol{R}(\varphi_i, a_j, b_k, c_k)$ and simplify them by using our results from step 1. After that we replace the generators φ_i, a_j, b_k, and c_k by $w_{\varphi_i}(\boldsymbol{\gamma}), w_{a_j}(\boldsymbol{\gamma})$ and $w_{b_k}(\boldsymbol{\gamma}), w_{c_k}(\boldsymbol{\gamma})$, respectively.

(3) We consider the relations imposed by

$$\gamma_l = v_l(w_{\varphi_i}(\boldsymbol{\gamma}), w_{a_j}(\boldsymbol{\gamma}), w_{b_k}(\boldsymbol{\gamma}), w_{c_k}(\boldsymbol{\gamma})).$$

Computation for the Odd Case

The relations in Lemma 4.16 say that, in the abelianization of $\Gamma^+(D_n, \pi_0)$, we have

$$\begin{aligned}
\varphi_1 &= -2\gamma_1 - \gamma_3, \\
\varphi_2 &= \frac{n+1}{2}\gamma_2 - \gamma_4, \\
a_1 &= -n\gamma_2 + 2\gamma_4, \\
a_2 &= 2\gamma_1 + 2\gamma_3, \\
a_3 &= -2\gamma_1 + n\gamma_2 - 2\gamma_3 - 2\gamma_4, \\
b_k &= n\gamma_2 - 2\gamma_4, \\
c_k &= -n\gamma_2 + 2\gamma_4.
\end{aligned}$$

We can thus ease our computation by noting that $a_1 = c_k = -b_k$ for $1 \leq k \leq n-1$ and $a_3 = -a_1 - a_2$. Next we consider the relations in Proposition 4.20. From the ones in part (A), we find

$$\begin{aligned}
a_1 = a_1 + (2-n)a_2 \quad &\Leftrightarrow \quad (2-n)a_2 = 0 \\
a_2 = -a_2 \quad &\Leftrightarrow \quad 2a_2 = 0
\end{aligned}$$

from which we obtain $a_2 = 0$. Considering the above relations once more, this also implies $a_3 = -a_1$. One easily sees that all relations imposed by (B) and (C) are now already redundant, that is, they are consequences

of $a_2 = 0$, $a_3 = -a_1$ and $a_1 = c_k = -b_k$. The only additional relation we get comes from (D) and says $4\varphi_1 - 4\varphi_2 = 2a_1$. Hence steps 1 and 2 have led to the relations

$$\begin{array}{lllll} a_2 & = 0 & \Leftrightarrow & 2\gamma_1 + 2\gamma_3 & = 0 \\ 4\varphi_1 - 4\varphi_2 & = 2a_1 & \Leftrightarrow & 8\gamma_1 + 2(n+1)\gamma_2 + 4\gamma_3 - 4\gamma_4 & = 2n\gamma_2 - 4\gamma_4 \end{array}$$

which we can simplify to

$$\begin{aligned} 2\gamma_1 + 2\gamma_3 &= 0 \\ 4\gamma_1 + 2\gamma_2 &= 0. \end{aligned}$$

Now we consider the relations $\gamma_l = v_l(w_{\varphi_i}(\boldsymbol{\gamma}), w_{a_j}(\boldsymbol{\gamma}), w_{b_k}(\boldsymbol{\gamma}), w_{c_k}(\boldsymbol{\gamma}))$, where the v_l can be found in Lemma 4.21. One easily sees that the only new relation comes from the expression for γ_1. We obtain $\gamma_1 = -2\gamma_1 - \gamma_2 - \gamma_3$, which means

$$3\gamma_1 + \gamma_2 + \gamma_3 = 0.$$

Hence $\Gamma^+(D_n, \pi_0)^{\mathrm{ab}}$ is the abelian group, generated by $\gamma_1, \ldots, \gamma_4$, subject to the relations

$$\begin{aligned} 2\gamma_1 + 2\gamma_3 &= 0 \\ 4\gamma_1 + 2\gamma_2 &= 0 \\ 3\gamma_1 + \gamma_2 + \gamma_3 &= 0. \end{aligned}$$

By the last relation we can eliminate γ_3. We thus have the generators γ_1, γ_2 and γ_4 and the defining relations reduce to

$$4\gamma_1 + 2\gamma_2 = 0.$$

If we set $\delta := 2\gamma_1 + \gamma_2$, we finally obtain a presentation

$$\Gamma^+(D_n, \pi_0)^{\mathrm{ab}} = \langle \gamma_1, \gamma_4, \delta \mid 2\delta = 0 \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^2.$$

Computation for the Even Case

Here the relations in Lemma 4.17 say

$$\begin{aligned}
\psi_1 &= -2\gamma_1 - \gamma_3 \\
\psi_2 &= \gamma_2 \\
\psi_3 &= \gamma_1 + \gamma_3 \\
d_1 &= -\frac{n}{2}\gamma_2 + \gamma_4 \\
d_2 &= 2\gamma_1 + 2\gamma_3 \\
d_3 &= -2\gamma_1 + \frac{n}{2}\gamma_2 - 2\gamma_3 - \gamma_4 \\
e_k &= \frac{n}{2}\gamma_2 - \gamma_4 \\
f_k &= -4\gamma_1 - \frac{n}{2}\gamma_2 - 4\gamma_3 + \gamma_4
\end{aligned}$$

for $1 \leq k \leq n/2 - 1$. In particular $d_1 = f_k - 2d_2 = -e_k$ for all k and $d_3 = e_k - d_2$, $d_2 = 2\psi_3$. This simplifies the relations we obtain from Proposition 4.22 very much. From (D) we obtain $d_2 = 0$. Indeed, one can now verify, that all relations from (A), (B) and (C) are redundant, that is, they are consequences of $d_2 = 0$ and the ones we have found above. Hence we only obtain the single relation

$$2\gamma_1 + 2\gamma_3 = 0.$$

In the next step, we have to consider the relations that come from Lemma 4.23. But also these relations are easily seen to be redundant. Hence we have

$$\begin{aligned}
\Gamma^+(D_n, \pi_0)^{\mathrm{ab}} &= \langle \gamma_1, \gamma_2, \gamma_3, \gamma_4 \mid 2\gamma_1 + 2\gamma_3 = 0 \rangle \\
&= \langle \gamma_1, \gamma_2, \gamma_4, \delta \mid 2\delta = 0 \rangle, \quad \text{where } \delta = \gamma_1 + \gamma_3 \\
&\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^3.
\end{aligned}$$

4.4 Congruence Subgroups associated to Semidirect Products of Cyclic Groups

As a generalization of congruence subgroups of $\mathrm{Aut}^+(F_2)$ associated to abelian or dihedral groups, we consider in this section congruence subgroups associated to semidirect products of two finite cyclic groups and

prove Theorem F.

Even more generally, one might consider congruence subgroups associated to finite metacyclic groups. The class of finite metacyclic groups, however, is very large and semidirect products of two finite cyclic groups can be considered as the easiest examples of finite metacyclic groups. Anyway, we also have an interesting result on congruence subgroups associated to finite metacyclic groups, see Corollary 4.26.

4.4.1 Index in $\mathrm{Aut}^+(F_2)$ and Image in $\mathrm{SL}_2(\mathbb{Z})$

Let G be a semidirect product of two finite cyclic groups, that is, we can write G as

$$G = \mathbb{Z}/a\mathbb{Z} \rtimes \langle g \rangle$$

where the action of $\langle g \rangle$ on $\mathbb{Z}/a\mathbb{Z}$ is induced by a homomorphism $\langle g \rangle \to \mathrm{Aut}(\mathbb{Z}/a\mathbb{Z}) \cong (\mathbb{Z}/a\mathbb{Z})^*$. Hence g acts on $\mathbb{Z}/a\mathbb{Z}$ by multiplication with an element $\alpha \in (\mathbb{Z}/a\mathbb{Z})^*$, that is, the multiplication in G is given by $(r, g^k) \cdot (s, g^l) = (r + \alpha^k s, g^{k+l})$ for all (r, g^k), $(s, g^l) \in G$. We shall keep this notation throughout the whole section. Our main result in this section is

Theorem 4.24. *Let $a \in \mathbb{N}$ and $\alpha \in (\mathbb{Z}/a\mathbb{Z})^*$. Consider the group $G := \mathbb{Z}/a\mathbb{Z} \rtimes \langle g \rangle$ where the finite cyclic group $\langle g \rangle$ acts on $\mathbb{Z}/a\mathbb{Z}$ via $\langle g \rangle \to \langle \alpha \rangle$, $g \mapsto \alpha$. Let $a = \prod p^{n_p}$ be the prime factorization of a and let k_p such that $\alpha \in 1 + \prod p^{k_p}(\mathbb{Z}/a\mathbb{Z})^*$. Moreover, let $\pi : F_2 \to G$ be an epimorphism. Then the following holds.*

(i) Up to conjugation, $\Gamma^+(G, \pi)$ only depends on G, but not on the choice of the epimorphism $\pi : F_2 \to G$.

(ii) The index of $\Gamma^+(G, \pi)$ in $\mathrm{Aut}^+(F_2)$ is

$$\frac{a \cdot \mathrm{ord}(\alpha) \cdot \mathrm{ord}(g)^2 \cdot \prod p^{k_p}}{\gcd(\mathrm{ord}(g), \prod p^{k_p})} \cdot \prod (1 - q^{-2})$$

where the very last product runs over all prime numbers q dividing $\mathrm{lcm}(\mathrm{ord}(g), \prod p^{k_p})$.

(iii) The image $\rho(\Gamma^+(G, \pi)) \leq \mathrm{SL}_2(\mathbb{Z})$ is conjugate to $\Gamma(\mathrm{ord}(g), \prod p^{k_p})$. In particular, it is a congruence subgroup.

Remark 4.25. Choosing $\langle g \rangle$ of order 2 and $\alpha := -1$, one obtains again parts (i), (ii) and (iii) of Theorem 4.12. We note, however, that in the proof of the above theorem (to be precise, in the proof of Lemma 4.39), we make use of our results on dihedral groups. Therefore parts (i), (ii) and (iii) of Theorem 4.12 are not logical consequences of the above result. ◇

Recall that Theorem 4.12 (iv) says that $\mathrm{d}(\Gamma^+(D_n, \pi)) \leq 4$ for every epimorphism $\pi : F_2 \to D_n$. At this point it is not clear to us how this generalizes to congruence subgroups associated to semidirect products of two finite cyclic groups. By Theorem 4.24 (iii), the congruence subgroup $\Gamma^+(\mathbb{Z}/a\mathbb{Z} \rtimes \langle g \rangle, \pi)$ maps onto a conjugate of $\Gamma(\mathrm{ord}(g), \prod p^{k_p})$, which is, in almost all cases, a free group whose rank depends on $\mathrm{ord}(g)$ and $\prod p^{k_p}$, see Proposition 3.4. It is thus clear that $\mathrm{d}(\Gamma^+(\mathbb{Z}/a\mathbb{Z} \rtimes \langle g \rangle, \pi))$ is not bounded by a constant. However, it is possible that $\mathrm{d}(\Gamma^+(\mathbb{Z}/a\mathbb{Z} \rtimes \langle g \rangle, \pi))$ only depends on the (rank of the) image $\rho(\Gamma^+(\mathbb{Z}/a\mathbb{Z} \rtimes \langle g \rangle, \pi))$. It seems unlikely that, in this case, one can use the same method that we have used in the case of dihedral groups to prove the statement. Using, for instance, the results of Rademacher [22] and the Reidemeister method, one can find a set of generators of $\Gamma(\mathrm{ord}(g), \prod p^{k_p})$ for given values of $\mathrm{ord}(g)$ and $\prod p^{k_p}$. But it seems impossible to write down a generating set of $\Gamma(\mathrm{ord}(g), \prod p^{k_p})$ for the general case in a closed form, let alone to find the corresponding elements in $\mathrm{Aut}^+(F_2)$.

A nice consequence of Theorem 4.24 is given by

Corollary 4.26. *Let G be a finite metacyclic group and $\pi : F_2 \to G$ be an epimorphism. Then $\rho(\Gamma^+(G, \pi))$ is a congruence subgroup.*

This result follows easily from the above theorem using

Lemma 4.27. *Let G be a finite metacyclic group. Then G is a homomorphic image of a semidirect product of two finite cyclic groups.*

Proof. Since G is a finite metacyclic group, it fits into an exact sequence of the form

$$1 \longrightarrow C_l \longrightarrow G \longrightarrow C_m \longrightarrow 1$$

with suitable $l, m \in \mathbb{N}$. By Proposition 2.1, the group G thus admits a presentation

$$G = \langle g, h \mid h^l = 1,\ g^m = h^x,\ ghg^{-1} = h^y \rangle$$

where $\gcd(y, l) = 1$. Let us write $x = x_1 \cdot x_2$ such that $\gcd(x_2, l) = 1$. Then G is generated by g, h^{x_2} and one easily verifies that G admits the following presentation.

$$G = \langle g, h^{x_2} \mid (h^{x_2})^l = 1,\ g^m = (h^{x_2})^{x_1},\ gh^{x_2}g^{-1} = (h^{x_2})^y \rangle$$

Therefore we may, without loss of generality, assume that every prime divisor of x is also one of l. Let $k := \mathrm{lcm}(x, l)$. Observe that $\gcd(y, k) = 1$ and define

$$\widetilde{G} := \langle g, h \mid h^k = 1,\ g^m = h^x,\ ghg^{-1} = h^y \rangle.$$

Clearly $\widetilde{G}$ maps onto G. Now we define

$$\widehat{G} := \langle g, h \mid h^k = 1,\ g^{mk/x} = 1,\ ghg^{-1} = h^y \rangle \cong C_k \rtimes C_{mk/x}.$$

Now the group $\widehat{G}$ maps onto

$$\langle g, h \mid h^k = 1,\ g^{mk/x} = 1,\ ghg^{-1} = h^y,\ g^m = h^x \rangle.$$

From the relation $g^m = h^x$ we obtain $g^{mk/x} = h^k = 1$. Therefore the relation $g^{mk/x} = 1$ is redundant so that $\widehat{G}$ maps onto

$$\langle g, h \mid h^k = 1,\ g^m = h^x,\ ghg^{-1} = h^y \rangle = \widetilde{G}.$$

Altogether we find that $\widehat{G}$ maps onto G, as desired. □

Proof of Cor. 4.26. By the above lemma, there exists a semidirect product H of two finite cyclic groups having an epimorphism $\varepsilon : H \to G$. Now the Gaschütz-Lemma 2.6 yields that there is an epimorphism $\pi' : F_2 \to H$ such that $\pi = \varepsilon\pi'$. By our discussion in Section 4.1.1, we have $\rho(\Gamma^+(H, \pi')) \leq \rho(\Gamma^+(G, \pi))$. Theorem 4.24 (iii) says that $\rho(\Gamma^+(H, \pi'))$ is a congruence subgroup and hence so is $\rho(\Gamma^+(G, \pi))$. □

Let us now turn to the proof of Theorem 4.24.

Lemma 4.28. *Let p be a prime, $n \in \mathbb{N}$ and $\alpha \in (\mathbb{Z}/p^n\mathbb{Z})^*$. Then the following statements are equivalent.*

(i) The order $\mathrm{ord}(\alpha)$ of α in $(\mathbb{Z}/p^n\mathbb{Z})^*$ is a power of p.

(ii) $\alpha \equiv 1 \mod p$.

In particular, if $\alpha \equiv 1 \mod p$ and $\alpha \neq 1$, then $p \mid \mathrm{ord}(\alpha)$.

Proof. From the natural epimorphism we obtain an exact sequence

$$1 \longrightarrow K \longrightarrow (\mathbb{Z}/p^n\mathbb{Z})^* \longrightarrow (\mathbb{Z}/p\mathbb{Z})^* \longrightarrow 1.$$

Observe that K consists exactly of those elements in $(\mathbb{Z}/p^n\mathbb{Z})^*$ that are congruent to 1 modulo p.

Since $|(\mathbb{Z}/p^n\mathbb{Z})^*| = (p-1)p^{n-1}$ and $|(\mathbb{Z}/p\mathbb{Z})^*| = (p-1)$, we see that $|K| = p^{n-1}$. In particular, K is a p-group and the implication (ii) $\Rightarrow$ (i) is clear. To prove that (i) implies (ii) let us suppose that $\alpha \not\equiv 1 \mod p$. Then αK is a non-trivial element of $(\mathbb{Z}/p^n\mathbb{Z})^*/K$, a group of order $(p-1)$. Now, if $\mathrm{ord}(\alpha)$ is a power of p, say $\mathrm{ord}(\alpha) = p^e$, then also $(\alpha K)^{p^e} = K$ so that $\mathrm{ord}(\alpha K) \mid p^e$. Hence $\mathrm{ord}(\alpha K)$ is also a power of p. But since $\mathrm{ord}(\alpha K) \mid (p-1)$ this is impossible. □

We now describe the order of an element $1 \neq \alpha \in (\mathbb{Z}/p^n\mathbb{Z})^*$ in the case $\alpha \equiv 1 \mod p$ more precisely, depending on the maximal k such that $\alpha \equiv 1 \mod p^k$.

Lemma 4.29. *Let $a \in \mathbb{Z}$ and p be an odd prime. If $a \equiv 1 + p^k b \mod p^{k+1}$ for some $b \in \mathbb{Z}$ and $k \geq 1$, then*

$$a^{p^e} \equiv 1 + p^{k+e}b \mod p^{k+e+1}$$

for all $e \in \mathbb{N}$. Moreover, if $n \geq k$ and $p \nmid b$, then the smallest $e \in \mathbb{N}$ with $a^{p^e} \equiv 1 \mod p^n$ is given by $e = n - k$.

Proof. Since $a \equiv 1 + p^k b \mod p^{k+1}$, we have $a = 1 + p^k b + p^{k+1}c =$

$1 + p^k(b + pc)$ with some $c \in \mathbb{Z}$. Hence

$$\begin{aligned} a^p &= (1 + p^k(b + pc))^p \\ &= \sum_{i=0}^{p} \binom{p}{i} p^{ki}(b + pc)^i \\ &= 1 + p \cdot p^k(b + pc) + p^{kp}(b + pc)^p + \sum_{i=2}^{p-1} \binom{p}{i} p^{ki}(b + pc)^i. \end{aligned}$$

For $2 \leq i \leq p - 1$ we have $p \mid \binom{p}{i}$ and therefore

$$\sum_{i=2}^{p-1} \binom{p}{i} p^{ki}(b + pc)^i \equiv 0 \mod p^{2k+1}.$$

Observe that $2k + 1 \geq k + 2$ so that this sum also vanishes modulo p^{k+2}. Moreover, we also have $kp \geq k + 2$ so that $p^{kp}(b + pc)^p \equiv 0 \mod p^{k+2}$. Hence

$$a^p \equiv 1 + p^{k+1}(b + pc) \equiv 1 + p^{k+1}b \mod p^{k+2}.$$

The first part of the lemma now follows by induction.

The rest follows, since if $p \nmid b$, then the greatest power of p dividing $a^{p^e} - 1$ is given by p^{k+e}. □

The case $p = 2$ needs some special consideration.

Lemma 4.30. *Let $a \in \mathbb{Z}$.*

(i) If $a \equiv 1 + 2^k b \mod 2^{k+1}$ for some $b \in \mathbb{Z}$ and $k \geq 2$, then

$$a^{2^e} \equiv 1 + 2^{k+e}b \mod 2^{k+e+1}$$

for all $e \in \mathbb{N}$. Moreover, if $n \geq k$ and $2 \nmid b$, then the smallest $e \in \mathbb{N}$ with $a^{2^e} \equiv 1 \mod 2^n$ is given by $e = n - k$.

(ii) If $a \equiv -1 + 2^m c \mod 2^{m+1}$ for some $c \in \mathbb{Z}$ and $m \geq 2$, then

$$a^{2^e} \equiv 1 - 2^{m+e}c \mod 2^{m+e+1}$$

for all $e \in \mathbb{N}$. Moreover, if $n \geq m + 1$ and $2 \nmid c$, then the smallest $e \in \mathbb{N}$ with $a^{2^e} \equiv 1 \mod 2^n$ is given by $e = n - m$. If $n = m$, then the smallest such e is given by $e = 2$.

(iii) The following two statements are equivalent

(a) $a = 1 + 2b$ *with* $2 \nmid b$.

(b) $a = -1 + 2^m c$ *with* $2 \nmid c$ *and* $m \geq 2$.

Proof. Part (i) can be proved in the same way as Lemma 4.29.

Consider part (ii). We write $a = -1 + 2^m c + 2^{m+1} c'$ with suitable $c' \in \mathbb{Z}$. Then

$$a^2 = 1 - 2^{m+1} c - 2^{m+2} c' + 2^{2m} (c + 2c')^2.$$

Since $m \geq 2$, we have

$$a^2 \equiv 1 - 2^{m+1} c \mod 2^{m+2}.$$

Using (i), we easily obtain the rest of part (ii).

Let us now verify part (iii). Suppose that (a) holds. Then we find $a = -1 + 2(b+1)$. Since $2 \nmid b$ we have $2 \mid (b+1)$ so that (b) holds. Conversely, suppose that (b) holds. Then $a = 1 + 2(2^{m-1} c - 1)$ where $2 \nmid (2^{m-1} c - 1)$. Hence (a) holds. □

Corollary 4.31. *Let* p *be a prime,* $n \in \mathbb{N}$ *and* $\alpha \in (\mathbb{Z}/p^n\mathbb{Z})^*$ *such that* $\alpha \equiv 1 \mod p$.

(i) Suppose that p *is odd. Then for* $1 \leq k \leq n$ *the following two statements are equivalent*

(a) $\alpha \in 1 + p^k (\mathbb{Z}/p^n\mathbb{Z})^*$.

(b) $\mathrm{ord}(\alpha) = p^{n-k}$.

(ii) Suppose that $p = 2$.
If $\alpha \in 1 + 2^k (\mathbb{Z}/2^n\mathbb{Z})^*$ *with* $2 \leq k \leq n$, *then* $\mathrm{ord}(\alpha) = 2^{n-k}$.
If $\alpha \in -1 + 2^m (\mathbb{Z}/2^n\mathbb{Z})^*$ *with* $2 \leq m \leq n-1$, *then* $\mathrm{ord}(\alpha) = 2^{n-m}$.
If $\alpha = -1$, *then* $\mathrm{ord}(\alpha) = 2$.

Proof. Since $\alpha \equiv 1 \mod p$, we know, by Lemma 4.28 that the order of α is a power of p. The result thus follows from Lemmas 4.29 and 4.30. □

Observe that, by Lemma 4.30 (iii), part (ii) of the above corollary covers all possible cases.

Lemma 4.32. *Let $a = \prod p^{n_p}$ be the prime factorization of $a \in \mathbb{N}$. Moreover, let $0 \leq k_p \leq n_p$ such that $\alpha \in 1 + \prod p^{k_p}(\mathbb{Z}/a\mathbb{Z})^*$. Then*

$$|\operatorname{Inn}(\mathbb{Z}/a\mathbb{Z} \rtimes \langle g \rangle)| = \operatorname{ord}(\alpha) \cdot \prod p^{n_p - k_p}.$$

Proof. An element $(r, g^m) \in \mathbb{Z}/a\mathbb{Z} \rtimes \langle g \rangle$ is in the center of $\mathbb{Z}/a\mathbb{Z} \rtimes \langle g \rangle$ if and only if

$$(r, g^m) = (1,1)(r, g^m)(1,1)^{-1} = (1 + r - \alpha^m, g^m)$$

and

$$(r, g^m) = (0, g)(r, g^m)(0, g)^{-1} = (\alpha r, g^m).$$

The first equation is equivalent to $\alpha^m = 1$, that is, $\operatorname{ord}(\alpha) \mid m$ and the second one is equivalent to $\alpha r = r$. Therefore the center of $\mathbb{Z}/a\mathbb{Z} \rtimes \langle g \rangle$ is given by

$$\mathrm{Z}(\mathbb{Z}/a\mathbb{Z} \rtimes \langle g \rangle) = \{(r, g^m) \in \mathbb{Z}/a\mathbb{Z} \rtimes \langle g \rangle \mid \alpha r = r,\ \operatorname{ord}(\alpha) \mid m\}.$$

Consider the (additive) subgroup

$$\{r \in \mathbb{Z}/a\mathbb{Z} \mid r\alpha = r\}$$

of $\mathbb{Z}/a\mathbb{Z}$. Clearly $r\alpha = r \Leftrightarrow r(\alpha - 1) = 0$. We have $\alpha - 1 \in \prod p^{k_p}(\mathbb{Z}/a\mathbb{Z})^*$. Hence $r\alpha = r \Leftrightarrow r \prod p^{k_p} = 0 \Leftrightarrow r \in \langle \prod p^{n_p - k_p} \rangle$. So the above subgroup is generated by $\prod p^{n_p - k_p}$. In particular, it contains exactly $\prod p^{k_p}$ elements. It follows that the center of $\mathbb{Z}/a\mathbb{Z} \rtimes \langle g \rangle$ has exactly $\prod p^{k_p} \cdot \frac{\operatorname{ord}(g)}{\operatorname{ord}(\alpha)}$ elements, which completes the proof. □

Let us consider the sets of generating pairs of $\mathbb{Z}/p^n\mathbb{Z} \rtimes \langle g \rangle$ and then, more generally, of $\mathbb{Z}/a\mathbb{Z} \rtimes \langle g \rangle$.

Lemma 4.33. *Let p be a prime. Then for $r, s \in \mathbb{Z}/p^n\mathbb{Z}$ the following two statements are equivalent.*

(a) $\langle (r, g), (s, 1) \rangle = \mathbb{Z}/p^n\mathbb{Z} \rtimes \langle g \rangle$.

(b) $s \in (\mathbb{Z}/p^n\mathbb{Z})^*$.

Proof. For brevity we write $H := \mathbb{Z}/p^n\mathbb{Z} \rtimes \langle \alpha \rangle$. Then we have an obvious epimorphism $\mathbb{Z}/p^n\mathbb{Z} \rtimes \langle g \rangle \to H$.

Assume that (a) holds. From the above epimorphism we obtain that (r, α) and $(s, 1)$ generate H.

Let us first consider the case that $\alpha \equiv 1 \mod p$. We have a natural epimorphism

$$H \to \mathbb{Z}/p\mathbb{Z} \rtimes \langle \alpha \rangle, \quad (z, \alpha^k) \mapsto (\overline{z}, \alpha^k).$$

Since $\alpha \equiv 1 \mod p$, the action of $\langle \alpha \rangle$ on $\mathbb{Z}/p\mathbb{Z}$ is trivial. Hence

$$\mathbb{Z}/p\mathbb{Z} \rtimes \langle \alpha \rangle = \mathbb{Z}/p\mathbb{Z} \times \langle \alpha \rangle$$

is a direct product. Moreover, by Lemma 4.28, the element α has p-power order so that we obtain an epimorphism

$$\langle \alpha \rangle \to \mathbb{Z}/p\mathbb{Z}, \quad \alpha^k \mapsto \overline{k}.$$

This leads to an epimorphism

$$H \to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}, \quad (z, \alpha^k) \mapsto (\overline{z}, \overline{k}).$$

Now $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ is generated by the images of (r, α) and $(s, 1)$, which are given by $(\overline{r}, \overline{1})$ and $(\overline{s}, \overline{0})$, respectively. Since $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ is not cyclic, it follows that $s \not\equiv 0 \mod p$, i.e., $s \in (\mathbb{Z}/p^n\mathbb{Z})^*$.

Now we consider the case $\alpha \not\equiv 1 \mod p$, that is, $\alpha - 1 \in (\mathbb{Z}/p^n\mathbb{Z})^*$. Clearly we have $\mathrm{ord}((r, \alpha)) \geq \mathrm{ord}(\alpha)$. We show that equality holds. To this end, let $m := \mathrm{ord}(\alpha)$. Then

$$(r, \alpha)^m = (r(1 + \alpha + \cdots + \alpha^{m-1}), 1).$$

Moreover

$$0 = \alpha^m - 1 = (1 + \alpha + \cdots + \alpha^{m-1})(\alpha - 1).$$

Since $\alpha - 1 \in (\mathbb{Z}/p^n\mathbb{Z})^*$ this implies $(1 + \alpha + \cdots + \alpha^{m-1}) = 0$. Hence $(r, \alpha)^m = (0, 1)$ so that $\mathrm{ord}((r, \alpha)) = \mathrm{ord}(\alpha)$. Now observe that, since $H = \langle (r, \alpha), (s, 1) \rangle$ and $(r, \alpha)(s, 1)(r, \alpha)^{-1} = (\alpha s, 1)$, the subgroup of H generated by $(s, 1)$ is normal. We can thus write every element of H as $(r, \alpha)^i (s, 1)^j$ with $1 \leq i \leq \mathrm{ord}(\alpha)$ and $1 \leq j \leq \mathrm{ord}((s, 1))$. In particular,

$$p^n \cdot \mathrm{ord}(\alpha) = |H| = \mathrm{ord}((s, 1)) \cdot \mathrm{ord}((\alpha))$$

so that $\mathrm{ord}((s,1)) = p^n$. This shows that $\mathrm{ord}(s) = p^n$, i.e., $s \in (\mathbb{Z}/p^n\mathbb{Z})^*$, as desired.

The fact that (b) implies (a) easily follows from the exact sequence

$$1 \longrightarrow \mathbb{Z}/p^n\mathbb{Z} \longrightarrow H \longrightarrow \langle g \rangle \longrightarrow 1.$$

Hence the lemma follows. □

We now generalize the above result on $\mathbb{Z}/p^n\mathbb{Z} \rtimes \langle g \rangle$ to the group $\mathbb{Z}/a\mathbb{Z} \rtimes \langle g \rangle$.

Corollary 4.34. *Let $\tilde{a} \mid a$ be the greatest divisor of a satisfying $\alpha \equiv 1 \mod \tilde{a}$ and $\gcd(\mathrm{ord}(g), \tilde{a}) = 1$. Moreover let $r, s \in \mathbb{Z}/a\mathbb{Z}$ such that s is a unit modulo $\tilde{a}$. Then the following two statements are equivalent.*

(a) $\langle (r,g), (s,1) \rangle = \mathbb{Z}/a\mathbb{Z} \rtimes \langle g \rangle$.

(b) $s \in (\mathbb{Z}/a\mathbb{Z})^*$.

Proof. Let us write $G = \mathbb{Z}/a\mathbb{Z} \rtimes \langle g \rangle$.

Suppose that (a) holds. It suffices to show that $s \not\equiv 0 \mod p$ for every prime p dividing a. Let $a = \prod p^{n_p}$ be the prime factorization of a. We consider two cases.

Case 1: We have $\alpha \equiv 1 \mod p^{n_p}$. If $p \nmid \mathrm{ord}(g)$, then, by definition of $\tilde{a}$, we have $p \mid \tilde{a}$. Since s is a unit modulo $\tilde{a}$, it then follows that it is also a unit modulo p so that $s \not\equiv 0 \mod p$. If $p \mid \mathrm{ord}(g)$, we have a natural epimorphism

$$G \to \mathbb{Z}/p\mathbb{Z} \times \langle g \rangle \to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$

mapping (r,g) onto $(\overline{r}, \overline{1})$ and $(s,1)$ onto $(\overline{s}, \overline{0})$. Since $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ is not cyclic, it now follows that $s \not\equiv 0 \mod p$.

Case 2: We have $\alpha \not\equiv 1 \mod p^{n_p}$. Then we obtain an epimorphism

$$G \to \mathbb{Z}/p^{n_p}\mathbb{Z} \rtimes \langle g \rangle$$

with $\langle g \rangle$ acting non-trivially on $\mathbb{Z}/p^{n_p}\mathbb{Z}$. Now Lemma 4.33 yields that s is a unit modulo p^{n_p}.

The fact that (b) implies (a) follows from the exact sequence

$$1 \longrightarrow \mathbb{Z}/a\mathbb{Z} \longrightarrow G \longrightarrow \langle g \rangle \longrightarrow 1.$$

This completes the proof. □

We now use Lemma 2.6 to determine the number of generating pairs of $\mathbb{Z}/a\mathbb{Z} \rtimes \langle g \rangle$. As usual, we write ϕ for the Euler ϕ-function.

Corollary 4.35. *Let $\tilde{a} \mid a$ be the greatest divisor of a satisfying $\alpha \equiv 1 \mod \tilde{a}$ and $\gcd(\mathrm{ord}(g), \tilde{a}) = 1$. The number of generating pairs of $\mathbb{Z}/a\mathbb{Z} \rtimes \langle g \rangle$ is*

$$\frac{\phi(a) \cdot a}{\phi(\tilde{a})} \cdot \tilde{a} \cdot \mathrm{ord}(g)^2 \cdot \prod (1 - q^{-2})$$

where the product runs over all primes q dividing $\tilde{a} \cdot \mathrm{ord}(g)$. In particular, the group $\mathbb{Z}/p^n\mathbb{Z} \rtimes \langle g \rangle$ with p prime and $\langle g \rangle$ acting non-trivially has exactly

$$\phi(p^n) \cdot p^n \cdot \mathrm{ord}(g)^2 \cdot \prod_{\substack{q \mid \mathrm{ord}(g) \\ q \text{ prime}}} (1 - q^{-2}) = \phi(p^n) \cdot p^n \cdot [\mathrm{SL}_2(\mathbb{Z}) : \Gamma^1(\mathrm{ord}(g))]$$

generating pairs.

Proof. We write $G = \mathbb{Z}/a\mathbb{Z} \rtimes \langle g \rangle$ and consider the natural epimorphism $G \to \mathbb{Z}/\tilde{a}\mathbb{Z} \times \langle g \rangle$. Observe that $\mathbb{Z}/\tilde{a}\mathbb{Z} \times \langle g \rangle$ is cyclic. Therefore, by Proposition 4.10, the product replacement graph $\mathbf{V}_2(\mathbb{Z}/\tilde{a}\mathbb{Z} \times \langle g \rangle)$ is connected. By Lemma 2.7, it follows that all generating pairs of $\mathbb{Z}/\tilde{a}\mathbb{Z} \times \langle g \rangle$ have the same number of lifts to G.

Consider the generating pair $((0, g), (1, 1))$ of $\mathbb{Z}/\tilde{a}\mathbb{Z} \times \langle g \rangle$. By Corollary 4.34, the lifts of this pair are precisely the pairs $((r, g), (s, 1))$ with $r \in \ker(\mathbb{Z}/a\mathbb{Z} \to \mathbb{Z}/\tilde{a}\mathbb{Z})$ and $s \in \ker((\mathbb{Z}/a\mathbb{Z})^* \to (\mathbb{Z}/\tilde{a}\mathbb{Z})^*)$. Hence we have $a/\tilde{a}$ choices for r and $\phi(a)/\phi(\tilde{a})$ choices for s so that this pair has exactly $\frac{\phi(a) \cdot a}{\phi(\tilde{a}) \cdot \tilde{a}}$ lifts to $\mathbb{Z}/a\mathbb{Z} \rtimes \langle g \rangle$.

Since $\mathbb{Z}/\tilde{a}\mathbb{Z} \times \langle g \rangle$ is cyclic of order $\tilde{a} \cdot \mathrm{ord}(g)$, we know from Proposition 4.10 that the number of generating pairs of $\mathbb{Z}/\tilde{a}\mathbb{Z} \times \langle g \rangle$ is exactly

$$\tilde{a}^2 \cdot \mathrm{ord}(g)^2 \cdot \prod (1 - q^{-2})$$

where the product runs over all primes q dividing $\tilde{a} \cdot \mathrm{ord}(g)$. This leads to the desired number of generating pairs of $\mathbb{Z}/a\mathbb{Z} \rtimes \langle g \rangle$.

Now suppose that $a = p^n$ is a prime power and g acts by $\alpha \neq 1$. We claim that $\tilde{a} = 1$. Assume that $\tilde{a} \neq 1$, i.e., $\tilde{a}$ is a non-trivial power of p. Since $\alpha \equiv 1 \mod \tilde{a}$, we have $\alpha \equiv 1 \mod p$ so that, by Lemma 4.28, we obtain $p \mid \mathrm{ord}(\alpha)$ and hence $p \mid \mathrm{ord}(g)$. But $\gcd(\mathrm{ord}(g), \tilde{a}) = 1$,

contradiction. This proves the second formula. The last equality holds by Proposition 3.1. □

Lemma 4.36. *Let $G = \mathbb{Z}/a\mathbb{Z} \rtimes \langle g \rangle$ be a semidirect product of two finite cyclic groups. Then G has only one T_2-system.*

Proof. As above, let $\tilde{a} \mid a$ be the greatest divisor of a satisfying $\alpha \equiv 1 \mod \tilde{a}$ and $\gcd(\mathrm{ord}(g), \tilde{a}) = 1$. Recall that we have an epimorphism $G \to \mathbb{Z}/\tilde{a}\mathbb{Z} \times \langle g \rangle$ and that $\mathbf{V}_2(\mathbb{Z}/\tilde{a}\mathbb{Z} \times \langle g \rangle)$ is connected. Therefore we can move every generating pair of G to a lift of $((0,g),(1,1)) \in \mathbf{V}_2(\mathbb{Z}/\tilde{a}\mathbb{Z} \rtimes \langle g \rangle)$, that is, by Corollary 4.34, a pair $((r,g),(s,1)) \in \mathbf{V}_2(\mathbb{Z}/a\mathbb{Z} \rtimes \langle g \rangle)$ with $r \in \ker(\mathbb{Z}/a\mathbb{Z} \to \mathbb{Z}/\tilde{a}\mathbb{Z})$ and $s \in \ker((\mathbb{Z}/a\mathbb{Z})^* \to (\mathbb{Z}/\tilde{a}\mathbb{Z})^*)$. Since $s \in (\mathbb{Z}/a\mathbb{Z})^*$, we find some $k \in \mathbb{Z}$ such that $k \equiv -rs^{-1}\alpha^{-1} \mod a$. We now obtain

$$((r,g)(s,1)^k, (s,1)) = ((0,g),(s,1)).$$

Finally, we have an automorphism of G induced by $(0,g) \mapsto (0,g)$ and $(s,1) \mapsto (1,1)$, which shows that G indeed has only one T_2-system. □

Lemma 4.37. *Consider the semidirect product $\mathbb{Z}/p^n\mathbb{Z} \rtimes \langle g \rangle$ with p prime and g acting by $\alpha \in (\mathbb{Z}/p^n\mathbb{Z})^*$. If $\alpha \not\equiv 1 \mod p$, then $\mathbf{V}_2(\mathbb{Z}/p^n\mathbb{Z} \rtimes \langle g \rangle)$ has exactly $\phi(p^n) \cdot \mathrm{ord}(\alpha)^{-1}$ connected components, each of size*

$$|\operatorname{Inn}(\mathbb{Z}/p^n\mathbb{Z} \rtimes \langle g \rangle)| \cdot [\mathrm{SL}_2(\mathbb{Z}) : \Gamma^1(\mathrm{ord}(g))].$$

Proof. As seen in the proof of Lemma 4.36, each connected component of $\mathbf{V}_2(\mathbb{Z}/p^n\mathbb{Z} \rtimes \langle g \rangle)$ contains a pair of the form

$$((0,g),(s,1)).$$

For every $0 \leq e \leq \mathrm{ord}(\alpha) - 1$, this pair is in the same component as

$$((0,g),(0,g)^e(s,1)(0,g)^{-e}) = ((0,g),(\alpha^e s,1)).$$

Hence $\mathbf{V}_2(\mathbb{Z}/p^n\mathbb{Z} \rtimes \langle g \rangle)$ has at most $\phi(p^n) \cdot \mathrm{ord}(\alpha)^{-1}$ connected components.

To determine a lower bound for the number of connected components consider the commutator

$$[(0,g),(s,1)] = ((\alpha - 1)s, 1)$$

whose conjugates are $(\alpha^e(\alpha-1)s, 1)$, $0 \leq e \leq \mathrm{ord}(\alpha)-1$. Hence, if $((0,g),(s',1))$ is in the same connected component as $((0,g),(s,1))$, then $\alpha^e(\alpha-1)s = (\alpha-1)s'$ for some e. Furthermore, since $\alpha \not\equiv 1 \mod p$ this implies $\alpha^e s = s'$. So we see that the number of connected components is exactly $\phi(p^n)\cdot \mathrm{ord}(\alpha)^{-1}$.

Since, as a consequence of Lemma 4.36, all components have the same size, each of them must have exactly

$$\begin{aligned}
&|\mathbf{V}_2(\mathbb{Z}/p^n\mathbb{Z} \rtimes \langle g\rangle)| \cdot \phi(p^n)^{-1} \cdot \mathrm{ord}(\alpha)\\
=&p^n \cdot \mathrm{ord}(\alpha) \cdot [\mathrm{SL}_2(\mathbb{Z}) : \Gamma^1(\mathrm{ord}(g))], \quad \text{by Cor. 4.35}\\
=&|\operatorname{Inn}(\mathbb{Z}/p^n\mathbb{Z} \rtimes \langle g\rangle)| \cdot [\mathrm{SL}_2(\mathbb{Z}) : \Gamma^1(\mathrm{ord}(g))], \quad \text{by Lem. 4.32}
\end{aligned}$$

vertices. This completes the proof. □

By similar computations one can also determine upper and lower bounds for the number of connected components of $\mathbf{V}_2(\mathbb{Z}/p^n\mathbb{Z} \rtimes \langle g\rangle)$ in the case $\alpha \equiv 1 \mod p$. However, the following computation is more convenient.

We note that we first determine a lower bound for the number of connected components of $\mathbf{V}_2(\mathbb{Z}/p^n\mathbb{Z} \rtimes \langle g\rangle)$ in the case $\alpha \equiv 1 \mod p$. Later on we will get the exact number.

Lemma 4.38. *Suppose that $\alpha \in 1 + p^k(\mathbb{Z}/p^n\mathbb{Z})^*$ for some $1 \leq k \leq n-1$. Then $\mathbf{V}_2(\mathbb{Z}/p^n\mathbb{Z} \rtimes \langle g\rangle)$ has at least $\phi(\gcd(p^k, \mathrm{ord}(g)))$ connected components. Moreover, all components have the same size and this size is less than or equal to*

$$\frac{p^{2n}}{\gcd(p^k, \mathrm{ord}(g))} \cdot [\mathrm{SL}_2(\mathbb{Z}) : \Gamma^1(\mathrm{ord}(g))].$$

Proof. Since the action of $\langle g\rangle$ on $\mathbb{Z}/p^k\mathbb{Z}$ is trivial, we have an epimorphism

$$\mathbb{Z}/p^n\mathbb{Z} \rtimes \langle g\rangle \to \mathbb{Z}/p^k\mathbb{Z} \times \langle g\rangle.$$

Observe that

$$\mathbb{Z}/p^k\mathbb{Z} \times \langle g\rangle \cong \mathbb{Z}/\operatorname{lcm}(p^k, \mathrm{ord}(g))\mathbb{Z} \times \mathbb{Z}/\gcd(p^k, \mathrm{ord}(g))\mathbb{Z}.$$

From Proposition 4.10 we thus know that $\mathbf{V}_2(\mathbb{Z}/p^k\mathbb{Z} \times \langle g\rangle)$ has exactly $\phi(\gcd(p^k, \mathrm{ord}(g)))$ connected components. By Theorem 2.5, this proves

the first result. We know from Lemma 4.36 that all connected components of $\mathbf{V}_2(\mathbb{Z}/p^n\mathbb{Z} \rtimes \langle g \rangle)$ have the same size. Furthermore, Corollary 4.35 yields that $\mathbf{V}_2(\mathbb{Z}/p^n\mathbb{Z} \rtimes \langle g \rangle)$ has exactly $p^{2n}(1-p^{-1}) \cdot [\mathrm{SL}_2(\mathbb{Z}) : \Gamma^1(\mathrm{ord}(g))]$ elements. Note that, by Lemma 4.28, we have $p \mid \mathrm{ord}(\alpha)$ and hence also $p \mid \mathrm{ord}(g)$. This shows that $\gcd(p^k, \mathrm{ord}(g)) = p^e$ for some $1 \leq e \leq k$ and therefore

$$\phi(\gcd(p^k, \mathrm{ord}(g))) = \gcd(p^k, \mathrm{ord}(g)) \cdot (1 - p^{-1}).$$

We now see that each connected component has at most

$$\frac{|\mathbf{V}_2(\mathbb{Z}/p^n\mathbb{Z} \rtimes \langle g \rangle)|}{\phi(\gcd(p^k, \mathrm{ord}(g)))} = \frac{p^{2n}(1 - p^{-1}) \cdot [\mathrm{SL}_2(\mathbb{Z}) : \Gamma^1(\mathrm{ord}(g))]}{\gcd(p^k, \mathrm{ord}(g)) \cdot (1 - p^{-1})}$$

vertices, which proves the rest of the lemma. □

If $p = 2$ and $\alpha \in 1 + 2(\mathbb{Z}/2^n\mathbb{Z})^*$, $n \geq 2$, the above lemma only yields that $\mathbf{V}_2(\mathbb{Z}/2^n\mathbb{Z} \rtimes \langle g \rangle)$ has at least one connected component, which is obvious. To prove our main result we need a better bound in this very special case and we provide it in the next lemma. Recall that, in this case, $\alpha \in -1 + 2^m(\mathbb{Z}/2^n\mathbb{Z})^*$ for some $2 \leq m \leq n$.

Lemma 4.39. *Suppose that $p = 2$ and $\alpha \in 1 + 2(\mathbb{Z}/2^n\mathbb{Z})^*$, $n \geq 2$.*

(i) If $\alpha \in -1 + 2^m(\mathbb{Z}/2^n\mathbb{Z})^*$, $2 \leq m \leq n-1$, then the product replacement graph $\mathbf{V}_2(\mathbb{Z}/2^n\mathbb{Z} \rtimes \langle g \rangle)$ has at least 2^{m-1} connected components. Moreover, each component has size less than or equal to

$$2^{2n-m} \cdot [\mathrm{SL}_2(\mathbb{Z}) : \Gamma^1(\mathrm{ord}(g))].$$

(ii) If $\alpha = -1$, then $\mathbf{V}_2(\mathbb{Z}/2^n\mathbb{Z} \rtimes \langle g \rangle)$ has at least 2^{n-2} connected components, each of size less than or equal to

$$2^{n+1} \cdot [\mathrm{SL}_2(\mathbb{Z}) : \Gamma^1(\mathrm{ord}(g))].$$

Proof. Note that, by Corollary 4.35, the graph $\mathbf{V}_2(\mathbb{Z}/2^n\mathbb{Z} \rtimes \langle g \rangle)$ has exactly

$$\phi(2^n) \cdot 2^n \cdot [\mathrm{SL}_2(\mathbb{Z}) : \Gamma^1(\mathrm{ord}(g))] = 2^{2n-1} \cdot [\mathrm{SL}_2(\mathbb{Z}) : \Gamma^1(\mathrm{ord}(g))]$$

vertices.

To prove part (i) we make use of the Higman invariant. As we already know, for $s \in (\mathbb{Z}/2^n\mathbb{Z})^*$, the pair $((0,g),(s,1))$ generates $\mathbb{Z}/2^n\mathbb{Z} \rtimes \langle g\rangle$. Observe that the conjugacy class of $[(0,g),(s,1)] = (s(\alpha-1),1)$ is

$$C(s) := \{(s(\alpha-1)\alpha^e, 1) \in \mathbb{Z}/2^n\mathbb{Z} \rtimes \langle g\rangle \mid 0 \le e \le \mathrm{ord}(\alpha)-1\}.$$

We now show that, as s runs through $(\mathbb{Z}/2^n\mathbb{Z})^*$, we obtain at least 2^{m-1} distinct conjugacy classes $C(s)$. Since for each conjugacy class there is at least one connected component in $\mathbf{V}_2(\mathbb{Z}/2^n\mathbb{Z} \rtimes \langle g\rangle)$, this implies the desired result.

Since $\alpha \in -1+2^m(\mathbb{Z}/2^n\mathbb{Z})^*$, Lemma 4.30 (iii) yields $\alpha-1 \in 2(\mathbb{Z}/2^n\mathbb{Z})^*$. Hence for $s, s' \in (\mathbb{Z}/2^n\mathbb{Z})^*$, we find

$$C(s) = C(s') \quad \Longleftrightarrow \quad 2s = 2s'\alpha^e \text{ for some } 0 \le e \le \mathrm{ord}(\alpha)-1.$$

Therefore we need to consider the action of $\langle\alpha\rangle$ on the set $2(\mathbb{Z}/2^n\mathbb{Z})^*$ by multiplication. To be precise, we need to show that there are at least 2^{m-1} orbits under this action. The set $2(\mathbb{Z}/2^n\mathbb{Z})^*$ contains exactly 2^{n-2} elements. Indeed, for $s, s' \in (\mathbb{Z}/2^n\mathbb{Z})^*$ we have $2s = 2s'$ if and only if $s = s'$ or $s' = s+2^{n-1}$. For $s \in (\mathbb{Z}/2^n\mathbb{Z})^*$, the orbit length of $2s$ in $2(\mathbb{Z}/2^n\mathbb{Z})^*$ is given by the index $[\langle\alpha\rangle : \mathrm{Stab}(2s)]$. By Lemma 4.30 we have $\alpha^{2^{n-m-1}} = 1-2^{n-1}\beta$ for some $\beta \in (\mathbb{Z}/2^n\mathbb{Z})^*$ so that $1 \neq \alpha^{2^{n-m-1}} \in \mathrm{Stab}(2s)$ and $|\mathrm{Stab}(2s)| \ge 2$. Moreover, by Corollary 4.31 we have $\mathrm{ord}(\alpha) = 2^{n-m}$. Therefore

$$[\langle\alpha\rangle : \mathrm{Stab}(2s)] \le \frac{\mathrm{ord}(\alpha)}{2} = 2^{n-m-1}.$$

Since each orbit has length at most 2^{n-m-1}, there must be at least $2^{n-2}/2^{n-m-1} = 2^{m-1}$ orbits in $2(\mathbb{Z}/2^n\mathbb{Z})^*$, as desired.

To prove part (ii) observe that we have an epimorphism

$$\mathbb{Z}/2^n\mathbb{Z} \rtimes \langle g\rangle \to \mathbb{Z}/2^n\mathbb{Z} \rtimes \langle -1\rangle \cong D_{2^n}.$$

By Corollary 4.18 we know that $\mathbf{V}_2(D_{2^n})$ has exactly $\phi(2^n)/2 = 2^{n-2}$ connected components. By Theorem 2.5, the lemma follows. □

Let us reformulate the above results as

Corollary 4.40. *Suppose that $\alpha \neq 1$. Then the following holds.*

(i) If $\alpha \not\equiv 1 \mod p$, *then*

$$[\mathrm{SL}_2(\mathbb{Z}) : \rho(\Gamma^+(\mathbb{Z}/p^n\mathbb{Z} \rtimes \langle g\rangle, \pi))] = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma^1(\mathrm{ord}(g)).]$$

(ii) If $\alpha \in 1 + p^k(\mathbb{Z}/p^n\mathbb{Z})^*$ *where* $1 \leq k \leq n-1$, *then the index of* $\rho(\Gamma^+(\mathbb{Z}/p^n\mathbb{Z} \rtimes \langle g\rangle, \pi))$ *in* $\mathrm{SL}_2(\mathbb{Z})$ *is less than or equal to*

$$\frac{p^{2k}}{\gcd(p^k, \mathrm{ord}(g))} \cdot [\mathrm{SL}_2(\mathbb{Z}) : \Gamma^1(\mathrm{ord}(g))].$$

Proof. By Lemma 4.4, the index $[\mathrm{Aut}^+(F_2) : \Gamma^+(\mathbb{Z}/p^n\mathbb{Z} \rtimes \langle g\rangle, \pi)]$ is equal to

$$|\operatorname{Inn}(\mathbb{Z}/p^n\mathbb{Z} \rtimes \langle g\rangle)| \cdot [\mathrm{SL}_2(\mathbb{Z}) : \rho(\Gamma^+(\mathbb{Z}/p^n\mathbb{Z} \rtimes \langle g\rangle, \pi))].$$

Recall that $[\mathrm{Aut}^+(F_2) : \Gamma^+(\mathbb{Z}/p^n\mathbb{Z} \rtimes \langle g\rangle, \pi)]$ also coincides with the size of the connected component containing $(\pi(x), \pi(y))$ in $\mathbf{V}_2(\mathbb{Z}/p^n\mathbb{Z} \rtimes \langle g\rangle)$. Hence part (i) follows directly from Lemma 4.37.

Let us now consider part (ii). For p odd we can use the results on the connected components of $\mathbf{V}_2(\mathbb{Z}/p^n\mathbb{Z} \rtimes \langle g\rangle)$ given by Lemma 4.38 together with the fact that, by Corollary 4.31 and Lemma 4.32, we have $|\operatorname{Inn}(\mathbb{Z}/p^n\mathbb{Z} \rtimes \langle g\rangle)| = p^{n-k} \cdot \mathrm{ord}(\alpha) = p^{2(n-k)}$. For $p = 2$ we consider two cases.

If $\alpha \in 1 + 2^k(\mathbb{Z}/2^n\mathbb{Z})^*$, $2 \leq k \leq n-1$, we have $|\operatorname{Inn}(\mathbb{Z}/2^n\mathbb{Z} \rtimes \langle g\rangle)| = 2^{n-k} \cdot \mathrm{ord}(\alpha) = 2^{2(n-k)}$ and can argue as before.

If $\alpha \in 1 + 2(\mathbb{Z}/2^n\mathbb{Z})^*$, then $\alpha \in -1 + 2^m(\mathbb{Z}/2^n\mathbb{Z})^*$ with $2 \leq m \leq n$. Note that we have to show that the index of $\rho(\Gamma^+(\mathbb{Z}/2^n\mathbb{Z} \rtimes \langle g\rangle, \pi))$ in $\mathrm{SL}_2(\mathbb{Z})$ is less than or equal to

$$2 \cdot [\mathrm{SL}_2(\mathbb{Z}) : \Gamma^1(\mathrm{ord}(g))].$$

For $2 \leq m \leq n-1$ we use Lemma 4.39 (i) and the fact that, by Corollary 4.31 and Lemma 4.32, we have

$$\operatorname{Inn}(\mathbb{Z}/2^n\mathbb{Z} \rtimes \langle g\rangle) = 2^{n-1} \cdot \mathrm{ord}(\alpha) = 2^{2n-m-1}.$$

For $m = n$, we have $\alpha = -1$ and use Lemma 4.39 (ii) together with the fact that, again by Corollary 4.31 and Lemma 4.32, we have

$$\operatorname{Inn}(\mathbb{Z}/2^n\mathbb{Z} \rtimes \langle g\rangle) = 2^{n-1} \cdot \mathrm{ord}(\alpha) = 2^{2n}.$$

This completes the proof. □

With these results we now determine the image of $\Gamma^+(\mathbb{Z}/p^n\mathbb{Z} \rtimes \langle g \rangle)$ in $\mathrm{SL}_2(\mathbb{Z})$ up to conjugation.

Lemma 4.41. *Let $\pi : F_2 \to \mathbb{Z}/p^n\mathbb{Z} \rtimes \langle g \rangle$ be the epimorphism given by $\pi(x) = (0, g)$ and $\pi(y) = (1, 1)$. If $0 \leq k \leq n$ such that $\alpha \in 1 + p^k(\mathbb{Z}/p^n\mathbb{Z})^*$, then*

$$\rho(\Gamma^+(\mathbb{Z}/p^n\mathbb{Z} \rtimes \langle g \rangle, \pi)) = \Gamma(\mathrm{ord}(g), p^k).$$

Proof. We have a natural epimorphism $\mathbb{Z}/p^n\mathbb{Z} \rtimes \langle g \rangle \to \mathbb{Z}/p^k\mathbb{Z} \times \langle g \rangle$, so that, by our discussion in Section 4.1.1, we find

$$\rho(\Gamma^+(\mathbb{Z}/p^n\mathbb{Z} \rtimes \langle g \rangle, \pi)) \leq \Gamma(\mathrm{ord}(g), p^k).$$

We show that equality holds by considering the indices of these two groups in $\mathrm{SL}_2(\mathbb{Z})$.

If $\alpha \not\equiv 1 \mod p$, we can use Corollary 4.40 (i) to obtain the desired result.

Consider the case $1 \leq k \leq n-1$. We have

$$\begin{aligned}
&[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(\mathrm{ord}(g), p^k)] \\
&= \mathrm{lcm}(\mathrm{ord}(g), p^k)^2 \cdot \gcd(\mathrm{ord}(g), p^k) \cdot \prod (1 - q^{-2}), \quad \text{by Cor. 4.6} \\
&= \frac{\mathrm{ord}(g)^2 \cdot p^{2k}}{\gcd(\mathrm{ord}(g), p^k)} \cdot \prod (1 - q^{-2})
\end{aligned}$$

where the product runs over all primes q dividing $\mathrm{lcm}(\mathrm{ord}(g), p^k)$. Since, by Lemma 4.28, we have $p \mid \mathrm{ord}(\alpha)$ and hence also $p \mid \mathrm{ord}(g)$, this is equivalent to saying that the product runs over all primes q dividing $\mathrm{ord}(g)$. Therefore the above expression is equal to

$$\frac{p^{2k}}{\gcd(\mathrm{ord}(g), p^k)} \cdot [\mathrm{SL}_2(\mathbb{Z}) : \Gamma^1(\mathrm{ord}(g)].$$

Now we apply part (ii) of Corollary 4.40.

Finally, if $k = n$, then $\mathbb{Z}/p^n\mathbb{Z} \rtimes \langle g \rangle = \mathbb{Z}/p^n\mathbb{Z} \times \langle g \rangle$ is abelian so that the result follows immediately. □

Note that, in particular, we now know the exact index of the image $\rho(\Gamma^+(\mathbb{Z}/p^n\mathbb{Z} \rtimes \langle g \rangle, \pi))$ in $\mathrm{SL}_2(\mathbb{Z})$.

Now we have all results we need to complete the proof of our theorem.

Proof of Theorem 4.24. The fact that, up to conjugation, $\Gamma^+(G,\pi)$ does not depend on the epimorphism follows from Lemma 4.36. For simplicity we may thus assume that $\pi(x) = (0, g)$ and $\pi(y) = (1, 1)$.

Let $a = \prod p^{n_p}$ be the prime factorization of a. Then for each prime p dividing a we have an obvious epimorphism

$$\pi_p : \mathbb{Z}/a\mathbb{Z} \rtimes \langle g\rangle \longrightarrow \mathbb{Z}/p^{n_p}\mathbb{Z} \rtimes \langle g\rangle$$

where the action of $\langle g\rangle$ on $\mathbb{Z}/p^{n_p}\mathbb{Z}$ is given by $g \mapsto \overline{\alpha}$ with $\overline{\alpha}$ denoting the image of α in $(\mathbb{Z}/p^{n_p}\mathbb{Z})^*$. Clearly we have $\bigcap \ker(\pi_p) = 1$ so that Lemma 4.1 yields

$$\Gamma^+(\mathbb{Z}/a\mathbb{Z} \rtimes \langle g\rangle, \pi) = \bigcap \Gamma^+(\mathbb{Z}/p^{n_p}\mathbb{Z} \rtimes \langle g\rangle, \pi_p\pi).$$

If $\overline{\alpha} \in 1 + p^{k_p}(\mathbb{Z}/p^{n_p}\mathbb{Z})^*$ with $0 \le k_p \le n_p$, Lemma 4.41 yields that

$$\rho(\Gamma^+(\mathbb{Z}/p^{n_p}\mathbb{Z} \rtimes \langle g\rangle, \pi_p\pi)) = \Gamma(\mathrm{ord}(g), p^{k_p}).$$

Hence we obtain

$$\rho(\Gamma^+(\mathbb{Z}/a\mathbb{Z} \rtimes \langle g\rangle, \pi)) = \bigcap \Gamma(\mathrm{ord}(g), p^{k_p}) = \Gamma(\mathrm{ord}(g), \prod p^{k_p}).$$

Finally, we know by Lemma 4.4 that the index of $\Gamma^+(G,\pi)$ in $\mathrm{Aut}^+(F_2)$ is given by

$$|\operatorname{Inn}(G)| \cdot [\mathrm{SL}_2(\mathbb{Z}) : \rho(\Gamma^+(G,\pi))].$$

By Lemma 4.32 we have $|\operatorname{Inn}(G)| = \prod p^{n_p - k_p} \cdot \mathrm{ord}(\alpha)$ where the k_p are given by $\alpha \in 1 + \prod p^{k_p}(\mathbb{Z}/a\mathbb{Z})^*$. Moreover, by Corollary 4.6 we have

$$\begin{aligned}
&[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(\mathrm{ord}(g), \prod p^{k_p})] \\
=&\,\mathrm{lcm}(\mathrm{ord}(g), \prod p^{k_p})^2 \cdot \gcd(\mathrm{ord}(g), \prod p^{k_p}) \cdot \prod (1 - q^{-2}) \\
=&\,\frac{\mathrm{ord}(g)^2 \cdot \prod p^{2k_p}}{\gcd(\mathrm{ord}(g), \prod p^{k_p})} \cdot \prod (1 - q^{-2})
\end{aligned}$$

where q runs through all primes dividing $\mathrm{lcm}(\mathrm{ord}(g), \prod p^{k_p})$. □

4.4.2 Product Replacement Graphs of Semidirect Products of Cyclic Groups

Using our above results, we find

Theorem 4.42. *Let $a \in \mathbb{N}$ and $\alpha \in (\mathbb{Z}/a\mathbb{Z})^*$. Consider the group $G := \mathbb{Z}/a\mathbb{Z} \rtimes \langle g \rangle$ where the finite cyclic group $\langle g \rangle$ acts on $\mathbb{Z}/a\mathbb{Z}$ via $\langle g \rangle \to \langle \alpha \rangle$, $g \mapsto \alpha$. Let $a = \prod p^{n_p}$ be the prime factorization of a and let k_p such that $\alpha \in 1 + \prod p^{k_p}(\mathbb{Z}/a\mathbb{Z})^*$. Moreover, let $\tilde{a} \mid a$ be the greatest divisor of a satisfying $\alpha \equiv 1 \mod \tilde{a}$ and $\gcd(\mathrm{ord}(g), \tilde{a}) = 1$. Then the following holds.*

(i) The group G has only one T_2-system.

(ii) The graph $\mathbf{V}_2(G)$ has exactly

$$\phi(a) \cdot a \cdot \phi(\tilde{a})^{-1} \cdot \tilde{a} \cdot \mathrm{ord}(g)^2 \prod (1 - q^{-2})$$

vertices, where the product runs over all primes q dividing $\tilde{a} \cdot \mathrm{ord}(g)$.

(iii) The number of connected components of $\mathbf{V}_2(G)$ is

$$\frac{\tilde{a} \cdot \mathrm{ord}(g) \cdot \phi(a)}{\phi(\tilde{a}) \cdot \mathrm{ord}(\alpha) \cdot \mathrm{lcm}(\mathrm{ord}(g), \prod p^{k_p})}.$$

(iv) The number of vertices of each connected component of $\mathbf{V}_2(G)$ is

$$\frac{a \cdot \mathrm{ord}(\alpha) \cdot \mathrm{ord}(g)^2 \cdot \prod p^{k_p}}{\gcd(\mathrm{ord}(g), \prod p^{k_p})} \cdot \prod (1 - q^{-2})$$

where the very last product runs over all prime numbers q dividing $\mathrm{lcm}(\mathrm{ord}(g), \prod p^{k_p})$.

Proof. Part (i) is given by Lemma 4.36, part (ii) is given by Corollary 4.35 and part (iv) follows from Theorem 4.24 (ii). So we only have to verify part (iii). Using (ii) and (iv), we find that the size of each connected component of $\mathbf{V}_2(G)$ is

$$\frac{\phi(a) \cdot \tilde{a} \cdot \gcd(\mathrm{ord}(g), \prod p^{k_p})}{\phi(\tilde{a}) \cdot \mathrm{ord}(\alpha) \cdot \prod p^{k_p}} \cdot \prod (1 - q^{-2})$$

where the last product runs over all primes q dividing $\tilde{a} \cdot \mathrm{ord}(g)$, but not $\mathrm{lcm}(\mathrm{ord}(g), \prod p^{k_p})$. Since $\gcd(\mathrm{ord}(g), \tilde{a}) = 1$, this is equivalent to saying that $q \mid \tilde{a}$, but $q \nmid \prod p^{k_p}$. However, if $q \mid \tilde{a}$, then $\alpha \equiv 1 \mod q$ so that $k_q \geq 1$ and $q \mid \prod p^{k_p}$. So such q does not exist. Therefore the last product is empty and one can easily rewrite the above fraction to obtain the desired result. □

4.5 Congruence Subgroups associated to Certain Wreath Products

The last family of standard congruence subgroups of $\mathrm{Aut}^+(F_2)$ we consider consists of congruence subgroups associated to certain wreath products of finite cyclic groups. We shall prove Theorems H, I and J in this section. We note that this is the first family of congruence subgroups whose image in $\mathrm{SL}_2(\mathbb{Z})$ is not quite understood. In particular, it is not yet clear if it is always a congruence subgroup.

4.5.1 Wreath Products of the Form $\mathbb{Z}/m\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}$

In this section we consider the case that

$$G = \mathbb{Z}/m\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z} = (\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}.$$

Throughout the whole section we assume that $m = \prod p^{k_p}$ is the prime factorization of m.

Our aim is to prove

Theorem 4.43. *Let m be odd and $m = \prod p^{k_p}$ be its prime factorization.*

(i) Up to conjugation, $\Gamma^+(\mathbb{Z}/m\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}, \pi)$ only depends on m, but not on the particular epimorphism $\pi : F_2 \to \mathbb{Z}/m\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}$.

(ii) The index of $\Gamma^+(\mathbb{Z}/m\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}, \pi)$ in $\mathrm{Aut}^+(F_2)$ is $6m^3 \prod_{p|m}(1-p^{-2})$.

(iii) The image $\rho(\Gamma^+(\mathbb{Z}/m\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}, \pi)) \leq \mathrm{SL}_2(\mathbb{Z})$ is conjugate to $\Gamma(m, 2)$. In particular, it is a congruence subgroup.

The case that m is even is excluded from the above theorem. However, we will show

Theorem 4.44. *Let $k \geq 2$. Then the following holds.*

(i) Up to conjugation, $\Gamma^+(\mathbb{Z}/2^k\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}, \pi)$ only depends on k, but not on the particular epimorphism $\pi : F_2 \to \mathbb{Z}/2^k\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}$.

(ii) The index of $\Gamma^+(\mathbb{Z}/2^k\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}, \pi)$ in $\mathrm{Aut}^+(F_2)$ is $3 \cdot 2^{3k+1}$.

(iii) *For $k \geq 2$, the image $\rho(\Gamma^+(\mathbb{Z}/2^k\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}, \pi)) \leq \mathrm{SL}_2(\mathbb{Z})$ is conjugate to a subgroup of index 2 in $\Gamma(2^k, 2)$.*

Here the case $k = 1$ is excluded. Observe that, $\mathbb{Z}/2\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z} \cong D_4$ so that we can refer to Theorem 4.12. We thus see that part (i) is still true in this case. However, we find that the index of $\Gamma^+(\mathbb{Z}/2\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}, \pi)$ in $\mathrm{Aut}^+(F_2)$ is $24 = 3 \cdot 2^3$ and that $\rho(\Gamma^+(\mathbb{Z}/2\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}, \pi)) = \Gamma(2, 2)$.

Let us now prove the main results of this section. We start by determining the numbers of generating pairs of the groups $\mathbb{Z}/m\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/2^k\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}$.

Lemma 4.45. *Let m be odd and $m = \prod p^{k_p}$ be its prime factorization. Then*

$$|\mathbf{V}_2(\mathbb{Z}/m\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z})| = 3m^4 \prod_{p|m} (1 - p^{-1})(1 - p^{-2}).$$

Moreover, for $k \in \mathbb{N}$, we have

$$|\mathbf{V}_2(\mathbb{Z}/2^k\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z})| = 3 \cdot 2^{4k-1}.$$

Proof. Let $G := \mathbb{Z}/m\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}$. We have an exact sequence

$$1 \longrightarrow [G, G] \longrightarrow G \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \longrightarrow 1 \tag{4.9}$$

where the epimorphism $G \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ of G onto its abelianization is given by $((a, b), c) \mapsto (a + b, c)$. Accordingly, $[G, G] = \langle((b, -b), 0)\rangle$ for any $b \in (\mathbb{Z}/m\mathbb{Z})^*$. The group $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is generated by $(1, 1)$ and this element lifts to $((0, 1), 1) \in G$. Hence, every pair of the form

$$((b, -b), 0),\ ((0, 1), 1),\ b \in (\mathbb{Z}/m\mathbb{Z})^*$$

generates G.

We know by Theorem 4.10 that $\mathbf{V}_2(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ is connected. Therefore, by Lemma 2.7, all generating pairs of $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ have the same number of lifts. For simplicity, we consider

$$((1, 1),\ (0, 0)) \in \mathbf{V}_2(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}).$$

Preimages of this pair have the form

$$(((a, 1 - a), 1),\ ((b, -b), 0)). \tag{4.10}$$

For every prime $p \mid m$ we have a natural epimorphism $\mathbb{Z}/m\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}$. Note that $\mathbb{Z}/p\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}$ is not cyclic. Hence, if the pair (4.10) generates G, we have $b \not\equiv 0 \mod p$ for all $p \mid m$ so that $b \in (\mathbb{Z}/m\mathbb{Z})^*$. Conversely, if $b \in (\mathbb{Z}/m\mathbb{Z})^*$, sequence (4.9) implies that the pair (4.10) generates G. It follows that every generating pair of $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ has exactly $m \cdot \phi(m)$ lifts to G. By Proposition 4.10, we know that

$$|\mathbf{V}_2(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})| = 3m^2 \prod_{p|m} (1 - p^{-2})$$

which completes the proof for the first formula.

Let $H := \mathbb{Z}/2^k\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}$. We use the fact that a subset of a group generates the group if and only if it generates the group modulo its Frattini subgroup, see [23, Sec. 5.2], and that the Frattini subgroup of a finite p-group can easily be described. To be concrete, in our case, the Frattini subgroup of H is given by $\Phi(H) = H^2[H, H]$. Consider the natural projections

$$H \longrightarrow H/[H, H] \longrightarrow H/\Phi(H).$$

If $\langle g, h \rangle = H$, then, clearly, $\langle g, h \mod [H, H] \rangle = H/[H, H]$. Conversely, suppose that $\langle g, h \mod [H, H] \rangle = H/[H, H]$. Then $\langle g, h \mod \Phi(H) \rangle = H/\Phi(H)$. So, by the above mentioned result, we find $\langle g, h \rangle = H$ for every lift (g, h) of $(g, h \mod [H, H])$. Since $|[H, H]| = 2^k$, every generating pair $(g, h \mod [H, H])$ has exactly 2^{2k} lifts to H. Since, by Proposition 4.10, we have $|\mathbf{V}_2(\mathbb{Z}/2^k\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})| = 3 \cdot 2^{2k-1}$, the proof is complete. □

Lemma 4.46. *For m odd, the number of connected components of the graph $\mathbf{V}_2(\mathbb{Z}/m\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z})$ is $\phi(m)/2$. For $k \geq 2$, the number of connected components of $\mathbf{V}_2(\mathbb{Z}/2^k\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z})$ is 2^{k-2}.*

Proof. Let us write $G := \mathbb{Z}/m\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}$. As above, we use the epimorphism $G \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ given by $((a, b), c) \mapsto (a + b, c)$. Since $\mathbf{V}_2(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ is connected, every connected component of $\mathbf{V}_2(G)$ contains a lift of the pair $((1, 1),\ (0, 0))$, that is, as seen in the proof of Lemma 4.45, a pair of the form

$$(((a, 1 - a), 1),\ ((b, -b), 0)),\ b \in (\mathbb{Z}/m\mathbb{Z})^*.$$

Choose $k \in \mathbb{N}$ such that $kb \equiv -a \mod m$. Then

$$((b,-b),0)^k \cdot ((a,1-a),1) = ((0,1),1).$$

So every connected component contains a pair of the form

$$(((0,1),1),\ ((b,-b),0)),\ b \in (\mathbb{Z}/m\mathbb{Z})^*.$$

Conjugating this pair with $((0,1),1)$, we obtain the pair

$$(((0,1),1),\ ((-b,b),0))$$

which is therefore contained in the same component. Hence there are at most $\phi(m)/2$ connected components in $\mathbf{V}_2(G)$.

For a lower bound, consider the commutator

$$[((0,1),1),\ ((-b,b),0)] = ((-2b,2b),0).$$

This element has itself and its inverse as only conjugates. So we see that there must be at least $\phi(m)/2$ connected components, which completes the proof for m odd.

Let $H := \mathbb{Z}/2^k\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}$ with $k \geq 2$. Again we consider the epimorphism $H \to \mathbb{Z}/2^k\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ onto the abelianization. Also the graph $\mathbf{V}_2(\mathbb{Z}/2^k\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ is connected so that every component of $\mathbf{V}_2(H)$ contains a lift of the pair $((1,0),\ (0,1))$, that is, a pair of the form

$$(((a,1-a),0),\ ((b,-b),1)),\ b \in (\mathbb{Z}/2^k\mathbb{Z})^*.$$

Since $\gcd(2a-1,2) = 1$, we can find $l \in \mathbb{N}$ such that $l(2a-1) \equiv -b \mod 2^k$. Now

$$((a,1-a),0)^l \cdot ((b,-b),1) \cdot ((a,1-a),0)^{-l} = ((0,0),1)$$

so that every component of $\mathbf{V}_2(H)$ contains a pair of the form

$$(((a,1-a),0),\ ((0,0),1)).$$

Conjugating this pair with $((0,0),1)$, we see that the same orbit also contains

$$(((1-a,a),0),\ ((0,0),1)).$$

Applying the Nielsen move corresponding to the automorphism $x \mapsto x^{-1},\ y \mapsto y^{-1}$, we see that, besides the two pairs we have already found, also the pairs

$$(((-a, a-1), 0),\ ((0,0),1)) \quad \text{and} \quad (((a-1, -a), 0),\ ((0,0),1))$$

are in the same connected component. One easily verifies that for every $a \in \mathbb{Z}/2^k\mathbb{Z}$ these four pairs are pairwise distinct. Hence there are at most 2^{k-2} orbits.

For a lower bound, we consider the Higman invariant again. Also in this case the commutator

$$[((a, 1-a), 0),\ ((0,0),1)] = ((2a-1, 1-2a), 0)$$

has itself and its inverse as only conjugates. Since we have 2^k choices for a, we have 2^{k-1} choices for $2a$ and so, finally, 2^{k-2} different Higman invariants. □

Lemma 4.47. *For m odd the group $\mathbb{Z}/m\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}$ admits a presentation*

$$\langle A, B \mid A^m = B^{2m} = 1, BAB^{-1} = A^{-1} \rangle$$

where A and B can be identified with $((1,-1),0)$ and $((0,1),1)$, respectively.

The group $\mathbb{Z}/2^k\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}$ admits a presentation

$$\langle C, D \mid C^{2^k} = D^2 = [C,D]^{2^k} = 1, [C, DCD^{-1}] = 1 \rangle$$

where C and D can be identified with $((1,0),0)$ and $((0,0),1)$, respectively.

Proof. The first presentation can easily be obtained from the exact sequence

$$1 \longrightarrow \langle((1,-1),0)\rangle \longrightarrow \mathbb{Z}/m\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \longrightarrow 1$$

together with Proposition 2.1.

We now consider the group $\mathbb{Z}/2^k\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}$. Also here we use the exact sequence

$$1 \longrightarrow \langle((1,-1),0)\rangle \longrightarrow \mathbb{Z}/2^k\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/2^k\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \longrightarrow 1$$

together with Proposition 2.1. In this case, however, the group on the right is not cyclic, but generated by $(1,0)$ and $(0,1)$. The first element has order 2^k and lifts to $((1,0),0) = C$, the second element has order 2 and lifts to $((0,0),1) = D$. Setting $K := ((1,-1),0)$ we now obtain the following presentation.

$$\langle C, D, K \mid C^{2^k} = D^2 = K^{2^k} = 1, CDC^{-1}D^{-1} = K, \\ CKC^{-1} = K, DKD^{-1} = K^{-1}\rangle$$

We see that we can replace K by $CDC^{-1}D^{-1} = [C,D]$ and delete K from the list of generators to obtain

$$\langle C, D \mid C^{2^k} = D^2 = [C,D]^{2^k} = 1, \\ CDC^{-1}D^{-1}C^{-1} = DC^{-1}D^{-1}, DC^{-1}D^{-2} = D^{-1}C^{-1}\rangle.$$

The last relation is equivalent to $D^2CD^{-2} = C$ and thus redundant, because $D^2 = 1$. So, deleting this relation and rewriting the second last relation as $[C, DCD^{-1}] = 1$, we obtain the desired result. □

Corollary 4.48. *Let m be odd and $k \geq 2$. The groups $\mathbb{Z}/m\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/2^k\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}$ both have only one T_2-System. In particular, all connected components of $\mathbf{V}_2(\mathbb{Z}/m\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z})$ and of $\mathbf{V}_2(\mathbb{Z}/2^k\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z})$ have the same size.*

Proof. We have already seen that every connected component of the graph $\mathbf{V}_2(\mathbb{Z}/m\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z})$ contains a pair of the form

$$(((0,1),1),\ ((b,-b),0)),\ b \in (\mathbb{Z}/m\mathbb{Z})^*.$$

Using the presentation given in Lemma 4.47, one easily verifies that

$$((0,1),1) \mapsto ((0,1),1),\ ((b,-b),0) \mapsto ((1,-1),0)$$

induces an automorphism of $\mathbb{Z}/m\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}$.

Similarly, we know that every orbit of $\mathbf{V}_2(\mathbb{Z}/2^k\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z})$ contains a pair of the form

$$(((1-a,a),0),\ ((0,0),1)).$$

Here one can verify, using the above presentation, that

$$((1-a,a),0) \mapsto ((1,0),0),\ ((0,0),1) \mapsto ((0,0),1)$$

induces an automorphism of $\mathbb{Z}/2^k\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}$. □

Proof of Theorem 4.43. The fact that, up to conjugation, $\Gamma^+(\mathbb{Z}/m\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}, \pi)$ does not depend on π follows from Corollary 4.48. We may thus assume that

$$\pi : F_2 \to \mathbb{Z}/m\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}, \quad x \mapsto ((1,0),0), \quad y \mapsto ((0,0),1).$$

Composing this epimorphism with the projection onto the abelianization of $\mathbb{Z}/m\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}$, we obtain

$$\bar{\pi} : F_2 \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \quad x \mapsto (1,0), \quad y \mapsto (0,1).$$

This implies that $\rho(\Gamma^+(\mathbb{Z}/m\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}, \pi)) \leq \Gamma(m,2)$.

By Lemmas 4.45, 4.46 and Corollary 4.48, we find that each connected component has exactly $6m^3 \prod(1-p^{-2})$ vertices, which proves the result on the index of $\Gamma^+(\mathbb{Z}/m\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}, \pi)$ in $\mathrm{Aut}^+(F_2)$.

We have

$$\mathrm{Z}(\mathbb{Z}/m\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}) = \{((a,a),0) \in \mathbb{Z}/m\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z} \mid a \in \mathbb{Z}/m\mathbb{Z}\}$$

so that $|\,\mathrm{Z}(G)| = m$ and $|\,\mathrm{Inn}(\mathbb{Z}/m\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z})| = 2m$. This shows, by Corollary 4.4, that

$$[\mathrm{SL}_2(\mathbb{Z}) : \rho(\Gamma^+(\mathbb{Z}/m\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}, \pi))] = 3m^2 \prod_{p|m}(1-p^{-2}).$$

Since, by Proposition 3.1, this corresponds to the index of $\Gamma(m,2)$ in $\mathrm{SL}_2(\mathbb{Z})$, we obtain the desired result. □

Proof of Theorem 4.44. The fact that, up to conjugation, $\Gamma^+(\mathbb{Z}/2^k\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}, \pi)$ does not depend on π follows from Corollary 4.48. So we may assume that

$$\pi : F_2 \to \mathbb{Z}/2^k\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}, \quad x \mapsto ((1,0),0), \quad y \mapsto ((0,0),1).$$

We compose this epimorphism with the projection onto the abelianization of $\mathbb{Z}/2^k\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}$ to obtain

$$\bar{\pi} : F_2 \to \mathbb{Z}/2^k\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \quad x \mapsto (1,0), \quad y \mapsto (0,1).$$

Hence $\rho(\Gamma^+(\mathbb{Z}/2^k\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}, \pi)) \leq \Gamma(2^k,2)$.

Suppose that $k \geq 2$. By Lemmas 4.45, 4.46 and Corollary 4.48, we know that each connected component of $\mathbf{V}_2(\mathbb{Z}/2^k\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z})$ has exactly $3 \cdot 2^{3k+1}$ vertices. Moreover, we have $|\operatorname{Inn}(\mathbb{Z}/2^k\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z})| = 2^{k+1}$, so that the index of $\rho(\Gamma^+(\mathbb{Z}/2^k\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}, \pi))$ in $\mathrm{SL}_2(\mathbb{Z})$ is $3 \cdot 2^{2k}$, while, by Proposition 3.1, we have $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(2^k, 2)] = 3 \cdot 2^{2k-1}$. □

Let us point out the following observation. Suppose that $k \geq 2$ and consider the matrix

$$\begin{pmatrix} 1 + 2^k & -2^k \\ 2^k & 1 - 2^k \end{pmatrix} \in \Gamma(2^k).$$

One easily sees that

$$\varphi = \begin{cases} x \mapsto (xy)^{2^k} x \\ y \mapsto x^{-1}(xy)^{1-2^k}. \end{cases}$$

induces an automorphism of F_2, which is mapped onto the above matrix by ρ. Now the preimages of this matrix under ρ are exactly the automorphisms $\alpha\varphi$ with $\alpha \in \operatorname{Inn}(F_2)$. Following the notation in Lemma 4.47, let $\pi : F_2 \to \mathbb{Z}/2^k\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}$ be the epimorphism given by $\pi(x) := C$ and $\pi(y) := D$. Now

$$\pi(\varphi(x)) = (CD)^{2^k} C = ((2^{k-1} + 1, 2^{k-1}), 0).$$

The only conjugates of $C = ((1, 0), 0)$ in $\mathbb{Z}/2^k\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}$ are C itself and $((0, 1), 0)$. Hence, there exists no $\alpha \in \operatorname{Inn}(F_2)$ such that $\alpha\varphi \in \Gamma^+(\mathbb{Z}/2^k\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}, \pi)$. It follows that the above matrix is not contained in $\rho(\Gamma^+(\mathbb{Z}/2^k\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}, \pi))$. Hence $\rho(\Gamma^+(\mathbb{Z}/2^k\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}, \pi))$ does not contain the principal congruence subgroup $\Gamma(2^k)$. Computer experiments, however, indicate that $\rho(\Gamma^+(\mathbb{Z}/2^k\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}, \pi))$ contains $\Gamma(2^{k+1})$.

We will make a similar observation for the group $\mathbb{Z}/p\mathbb{Z} \wr \mathbb{Z}/p\mathbb{Z}$ with p prime at the end of the following section.

4.5.2 Wreath Products of the Form $\mathbb{Z}/p\mathbb{Z} \wr \mathbb{Z}/p\mathbb{Z}$

Let us now consider the case that

$$G = (\mathbb{Z}/p\mathbb{Z}) \wr (\mathbb{Z}/p\mathbb{Z}) = (\mathbb{Z}/p\mathbb{Z})^p \rtimes \mathbb{Z}/p\mathbb{Z}$$

where p is an odd prime and $\mathbb{Z}/p\mathbb{Z}$ acts on $(\mathbb{Z}/p\mathbb{Z})^p$ by a cyclic shift of the coordinates. For these groups, we prove

Theorem 4.49. *Let p be an odd prime.*

(i) Up to conjugation, $\Gamma^+(\mathbb{Z}/p\mathbb{Z} \wr \mathbb{Z}/p\mathbb{Z}, \pi)$ only depends on p, but not on the particular epimorphism $\pi : F_2 \to \mathbb{Z}/p\mathbb{Z} \wr \mathbb{Z}/p\mathbb{Z}$.

(ii) The index of $\Gamma^+(\mathbb{Z}/p\mathbb{Z} \wr \mathbb{Z}/p\mathbb{Z}, \pi)$ in $\mathrm{Aut}^+(F_2)$ is $p^{p+2}(p^2+1)$.

(iii) The image $\rho(\Gamma^+(\mathbb{Z}/p\mathbb{Z} \wr \mathbb{Z}/p\mathbb{Z}, \pi)) \leq \mathrm{SL}_2(\mathbb{Z})$ is a subgroup of index p in $\Gamma(p)$.

For the corresponding results for $p = 2$ see the remarks after Theorem 4.44.

Throughout the whole section we shall assume that p is an odd prime.

Observe that G admits a presentation

$$\langle A_1, \ldots, A_p, B \mid A_i A_j = A_j A_i,\ A_i^p = B^p = 1,\ BA_iB^{-1} = A_{i+1} \rangle \quad (4.11)$$

where the element B can be identified with $((0, \ldots, 0), 1)$, the element A_1 with $((1, 0, \ldots, 0), 0)$ and, accordingly, A_i with $((0, \ldots, 1, \ldots, 0), 0)$ where the 1 is on the i-th position. The indices in the presentation should be read modulo p. We have

$$G^{\mathrm{ab}} = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$

and the projection from G onto its abelianization is given by

$$((a_1, \ldots, a_p), k) \longmapsto (a_1 + \cdots + a_p, k).$$

Note that $|[G, G]| = p^{p-1}$.

For $((a_1, \ldots, a_p), k)$, $((b_1, \ldots, b_p), l) \in G$ we have

$$((a_1, \ldots, a_p), k) \cdot ((b_1, \ldots, b_p), l) = ((a_1 + b_{1-k}, \ldots, a_p + b_{p-k}), k + l)$$

and

$$[((a_i), k), ((b_i), l)] = ((a_i - a_{i-l} + b_{i-k} - b_i), 0).$$

Note that the entries $(a_i - a_{i-l} + b_{i-k} - b_i)$ sum up to 0 as i runs through $1, \ldots, p$. Therefore

$$[G, G] \leq \{((a_i), 0) \in G \mid a_1 + \cdots + a_p = 0\}.$$

Since the group on the right hand side has exactly p^{p-1} elements, we see that $[G,G]$ is actually equal to that group.

By the same argument on generating sets using the the Frattini subgroup of finite p-groups as in the proof of Lemma 4.45, we see that every generating pair $(g, h \mod [G,G])$ of G^{ab} has exactly p^{2p-2} lifts to $\mathbf{V}_2(G)$. Since $G^{\mathrm{ab}} = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ has exactly $(p^2-1)(p^2-p)$ generating pairs, we obtain

Lemma 4.50. *The group $\mathbb{Z}/p\mathbb{Z} \wr \mathbb{Z}/p\mathbb{Z}$ has exactly $p^{2p-1}(p^2-1)(p-1)$ generating pairs.*

The next result implies part (i) of Theorem 4.49.

Lemma 4.51. *The group $\mathbb{Z}/p\mathbb{Z} \wr \mathbb{Z}/p\mathbb{Z}$ has only one T_2-system.*

Proof. By our discussion in Section 4.2.2, we find that every generating pair of $G = \mathbb{Z}/p\mathbb{Z} \wr \mathbb{Z}/p\mathbb{Z}$ lies in the connected component of a lift of $((a,0),\ (0,1)) \in \mathbf{V}_2(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z})$, where $a \neq 0$, that is, in the component of a pair

$$((a_i),0),\ ((b_i),1)), \quad a_1 + \cdots + a_p = a,\ b_1 + \cdots + b_p = 0.$$

We are now going to verify that

$$((a_i),0) \mapsto ((1,0,\ldots,0),0), \quad ((b_i),1) \mapsto ((0,0,\ldots,0),1) \tag{4.12}$$

induces an automorphism of G. To this end, we only need to show that the above map respects the defining relations of G. Since $a_1 + \cdots + a_p \neq 0$, we find that not all a_i are identical. Therefore $((a_i),0)$ has exactly p conjugates in G, namely

$$((b_i),1)^k \cdot ((a_i),0) \cdot ((b_i),1)^{-k}.$$

Observe that, since all these conjugates have a zero at the second position, they commute with each other. Furthermore, they all have order p. Hence

$$\langle((a_i),0)\rangle^G \cong (\mathbb{Z}/p\mathbb{Z})^k,\ k \leq p.$$

Since, by assumption, G is generated by $((a_i),0)$ and $((b_i),1)$, the quotient $G/\langle((a_i),0)\rangle^G$ is generated by the image of $((b_i),1)$ and thus has order p. Considering

$$1 \longrightarrow \langle((a_i),0)\rangle^G \longrightarrow G \longrightarrow G/\langle((a_i),0)\rangle^G \longrightarrow 1$$

and counting elements, we find that $\langle((a_i),0)\rangle^G \cong (\mathbb{Z}/p\mathbb{Z})^p$. Applying Proposition 2.1, we obtain the following presentation.

$$G = \langle C_0, \ldots, C_{p-1}, D \mid C_iC_j = C_jC_i,\ C_i^p = 1,\ D^p = 1,\ DC_iD^{-1} = C_{i+1}\rangle$$

where

$$C_j := ((b_i),1)^j \cdot ((a_i),0) \cdot ((b_i),1)^{-j}, \quad D := ((b_i),1).$$

Comparing this with the presentation given by (4.11), we see that (4.12) indeed induces an automorphism of G. Hence the lemma follows. □

Lemma 4.52. *The group $G = \mathbb{Z}/p\mathbb{Z} \wr \mathbb{Z}/p\mathbb{Z}$ has exactly $p^{p-3}(p-1)$ Higman invariants.*

Proof. As argued in the proof of Lemma 4.51, each connected component of $\mathbf{V}_2(G)$ contains a pair of the form

$$((a_i),0),\ ((b_i),1), \quad a_1 + \cdots + a_p \neq 0,\ b_1 + \cdots + b_p = 0.$$

Hence, the Higman invariants of G are the conjugacy classes of the commutators

$$[((a_i),0),((b_i),1)] = ((a_i - a_{i-1}),0), \quad a_1 + \cdots + a_p \neq 0.$$

We now verify that such a commutator has exactly p conjugates. To see this, it suffices to show that the entries $a_i - a_{i-1}$ for $1 \leq i \leq p$ are not all identical. For a contradiction, we thus assume that $a_i - a_{i-1} = \lambda$ for $1 \leq i \leq p$ with some $\lambda \in \mathbb{Z}/p\mathbb{Z}$. This is equivalent to $a_i = \lambda + a_{i-1}$, so that, inductively, we find $a_i = (i-1)\lambda + a_1$. Now we have

$$\begin{aligned} a_1 + a_2 + \cdots + a_p &= a_1 + (p-1)a_1 + (1 + 2 + \cdots + (p-1))\lambda \\ &= p \cdot a_1 + 0 \cdot \lambda \\ &= 0, \end{aligned}$$

contradiction. Hence the above commutator indeed has exactly p conjugates.

To complete the proof, it remains to verify that in $(\mathbb{Z}/p\mathbb{Z})^p$ there are exactly $p^{p-2}(p-1)$ vectors of the form $(a_i - a_{i-1})$ with $a_1 + \cdots + a_p \neq 0$.

To this end, let M be the circulant $p \times p$-matrix over $\mathbb{Z}/p\mathbb{Z}$, given by

$$M := \begin{pmatrix} 1 & -1 & & & \\ & 1 & -1 & & \\ & & \ddots & \ddots & \\ & & & 1 & -1 \\ -1 & & & & 1 \end{pmatrix}.$$

Then $(a_i - a_{i-1}) = M \cdot (a_i)$. Setting

$$A := \{(a_i) \in (\mathbb{Z}/p\mathbb{Z})^p \mid a_1 + \cdots + a_p = 0\}$$

we thus have to determine $|M \cdot ((\mathbb{Z}/p\mathbb{Z})^p \setminus A)|$.

We should point out that a priori it is not clear, if $M \cdot ((\mathbb{Z}/p\mathbb{Z})^p \setminus A)$ is equal to $M \cdot (\mathbb{Z}/p\mathbb{Z})^p \setminus M \cdot A$, since M does not have full rank so that $v \mapsto Mv$ is not bijective.

One easily sees that the rank of M is $p - 1$ and

$$\ker(M) = (\mathbb{Z}/p\mathbb{Z}) \cdot \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}.$$

Observe that $\ker(M) \leq A$. Moreover, $M \cdot (\mathbb{Z}/p\mathbb{Z})^p \leq A$. Since $\dim(A) = p-1$, we actually have $A = M \cdot (\mathbb{Z}/p\mathbb{Z})^p$. So the set that we are interested in can be written as

$$M \cdot ((\mathbb{Z}/p\mathbb{Z})^p \setminus A) = M \cdot ((\mathbb{Z}/p\mathbb{Z})^p \setminus M \cdot (\mathbb{Z}/p\mathbb{Z})^p).$$

Observe that

$$M \cdot (\mathbb{Z}/p\mathbb{Z})^p \setminus M^2 \cdot (\mathbb{Z}/p\mathbb{Z})^p \subseteq M \cdot ((\mathbb{Z}/p\mathbb{Z})^p \setminus M \cdot (\mathbb{Z}/p\mathbb{Z})^p).$$

We want to show that equality holds. Let $v \in M^2 \cdot (\mathbb{Z}/p\mathbb{Z})^p$, say $v = M \cdot (M \cdot u)$, $u \in (\mathbb{Z}/p\mathbb{Z})^p$. If also $w \in (\mathbb{Z}/p\mathbb{Z})^p$ with $M \cdot w = v$, then

$$\begin{aligned} w &\in M \cdot u + \ker(M) \\ &\subseteq M \cdot u + M \cdot (\mathbb{Z}/p\mathbb{Z})^p, \text{ since } \ker(M) \leq M \cdot (\mathbb{Z}/p\mathbb{Z})^p \\ &= M \cdot (\mathbb{Z}/p\mathbb{Z})^p. \end{aligned}$$

Hence we find that if $M \cdot w \in M^2 \cdot (\mathbb{Z}/p\mathbb{Z})^p$, then $w \in M \cdot (\mathbb{Z}/p\mathbb{Z})^p$. So

$$M \cdot w \in M^2 \cdot (\mathbb{Z}/p\mathbb{Z})^p \Longleftrightarrow w \in M \cdot (\mathbb{Z}/p\mathbb{Z})^p.$$

It follows that

$$M \cdot (\mathbb{Z}/p\mathbb{Z})^p \setminus M^2 \cdot (\mathbb{Z}/p\mathbb{Z})^p = M \cdot ((\mathbb{Z}/p\mathbb{Z})^p \setminus M \cdot (\mathbb{Z}/p\mathbb{Z})^p).$$

Finally, one verifies that

$$M^2 = \begin{pmatrix} 1 & -2 & 1 & & & & & \\ & 1 & -2 & 1 & & & & \\ & & 1 & -2 & 1 & & & \\ & & & 1 & -2 & 1 & & \\ & & & & \ddots & \ddots & \ddots & \\ & & & & & 1 & -2 & 1 \\ 1 & & & & & & 1 & -2 \\ -2 & 1 & & & & & & 1 \end{pmatrix}$$

has rank $p-2$. So we find

$$|M \cdot ((\mathbb{Z}/p\mathbb{Z})^p \setminus A)| = p^{p-1} - p^{p-2} = p^{p-2}(p-1).$$

This completes the proof. □

Remark 4.53. As indicated in the above proof, generating sets of wreath products of finite cyclic groups are connected to circulant matrices. Motivated by this, in [2], the author considers the groups of regular circulant matrices over finite fields and integer residue class rings. More precisely, he determines the orders of these groups and makes a first step towards finding the algebraic structure of them. ◇

From the above result, it follows that $\mathbf{V}_2(G)$ has at least $p^{p-3}(p-1)$ connected components. Since, as a consequence of Lemma 4.51, they all have the same size, each component has at most $|\mathbf{V}_2(G)|/(p^{p-3}(p-1)) = p^{p+2}(p^2-1)$ vertices. Hence

$$[\mathrm{Aut}^+(F_2) : \Gamma^+(G,\pi)] \leq p^{p+2}(p^2-1).$$

We have

$$\mathrm{Z}(G) = \{((a,\ldots,a),0) \in G \mid a \in \mathbb{Z}/p\mathbb{Z}\}.$$

So, in particular $|\,\mathrm{Z}(G)| = p$ and $|\,\mathrm{Inn}(G)| = p^p$. By Corollary 4.4, we obtain

$$[\mathrm{SL}_2(\mathbb{Z}) : \rho(\Gamma^+(G,\pi))] \leq p^{p+2}(p^2-1)/p^p = p^4(1-p^{-2}).$$

Moreover, by our discussion in Section 4.1.1, we have

$$\rho(\Gamma^+(G,\pi)) \leq \Gamma(p).$$

By Proposition 3.1, the group $\Gamma(p)$ has index $p^3(1-p^{-2})$ in $\mathrm{SL}_2(\mathbb{Z})$. Hence, $\rho(\Gamma^+(G,\pi))$ is either equal to $\Gamma(p)$ or a subgroup of index p in $\Gamma(p)$. We claim that the latter holds. To prove this, it suffices to find an element of $\Gamma(p)$ which is not contained in $\rho(\Gamma^+(G,\pi))$. Note that, by Lemma 4.51, up to conjugation, $\rho(\Gamma^+(G,\pi))$ does not depend on π. We may thus assume that

$$\pi(x) = ((1,0,\ldots,0),0), \quad \pi(y) = ((0,0,\ldots,0),1).$$

Consider the matrix

$$\begin{pmatrix} 1+p & -p \\ p & 1-p \end{pmatrix} \in \Gamma(p).$$

If $\varphi \in \mathrm{Aut}^+(F_2)$ is a preimage under ρ of this matrix, then $\varphi = \alpha\varphi_p$ with some $\alpha \in \mathrm{Inn}(F_2)$ and

$$\varphi_p = \begin{cases} x \mapsto (xy)^p x \\ y \mapsto x^{-1}(xy)^{1-p}. \end{cases}$$

Assume, for a contradiction, that $\varphi \in \Gamma^+(G,\pi)$. Then, in particular,

$$\pi(x) = \pi(w)\cdot\pi((xy)^p x)\cdot\pi(w)^{-1} = \pi(w)\cdot((2,1,\ldots,1),0)\cdot\pi(w)^{-1}.$$

But $\pi(x) = ((1,0,\ldots,0),0)$ and $((2,1,\ldots,1),0)$ are not conjugate in G, contradiction. Hence $\varphi \notin \Gamma^+(G,\pi)$ and $\rho(\Gamma^+(G,\pi))$ is properly contained in $\Gamma(p)$. From this, we obtain parts (ii) and (iii) of Theorem 4.49.

4.5.3 Product Replacement Graphs of Certain Wreath Products

From our discussion in this section, we obtain

Corollary 4.54. *(i) Let $m \in \mathbb{N}$ be odd. Then the product replacement graph $\mathbf{V}_2(\mathbb{Z}/m\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z})$ has exactly $\phi(m)/2$ connected components, each of which has exactly $6m^3 \prod_{p|m}(1-p^{-2})$ vertices.*

(ii) Let $k \geq 2$. Then the graph $\mathbf{V}_2(\mathbb{Z}/2^k\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z})$ has exactly 2^{k-2} connected components, each of which has exactly $3 \cdot 2^{3k+1}$ vertices.

(iii) Let p be an odd prime. Then the graph $\mathbf{V}_2(\mathbb{Z}/p\mathbb{Z} \wr \mathbb{Z}/p\mathbb{Z})$ has exactly $p^{p-3}(p-1)$ connected components, each of which has exactly $p^{p+2}(p^2-1)$ vertices.

In each case, the Higman invariants characterize the connected components. Furthermore, all considered groups have only one T_2-system.

4.6 The Abelianization of Congruence Subgroups associated to Non-Perfect Groups

In this section we show

Theorem 4.55. *Let G be a finite non-perfect group, i.e., G has non-trivial abelianization. Then $\Gamma^+(G,\pi)$ has infinite abelianization.*

Proof. First we consider the case that $G/G' \cong \mathbb{Z}/2\mathbb{Z}$ where G' denotes the commutator subgroup of G. Then we naturally obtain an epimorphism

$$\bar{\pi} : F_2 \xrightarrow{\pi} G \longrightarrow \mathbb{Z}/2\mathbb{Z}.$$

By our discussion in Section 4.1.1, we have

$$\Gamma^+(G,\pi) \leq \Gamma^+(\mathbb{Z}/2\mathbb{Z},\bar{\pi}). \tag{4.13}$$

By Theorem 4.5, we may assume that $\bar{\pi}(x) = 1$ and $\bar{\pi}(y) = 0$. We set

$$\bar{\rho} : \mathrm{Aut}^+(F_2) \xrightarrow{\rho} \mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{PSL}_2(\mathbb{Z})$$

where the second epimorphism is the natural projection. Note that $\bar{\rho}$ is onto. Since $\bar{\rho}$ induces an epimorphism $\Gamma^+(G,\pi)^{\mathrm{ab}} \to \bar{\rho}(\Gamma^+(G,\pi))^{\mathrm{ab}}$, it suffices to show that $\bar{\rho}(\Gamma^+(G,\pi))$ has infinite abelianization. By (4.13) we have

$$\bar{\rho}(\Gamma^+(G,\pi)) \leq \bar{\rho}(\Gamma^+(\mathbb{Z}/2\mathbb{Z},\bar{\pi})) = \mathrm{P}\Gamma^1(2).$$

Hence $\bar{\rho}(\Gamma^+(G,\pi))$ is a finite index subgroup of $\mathrm{P}\Gamma^1(2)$. Note that $\mathrm{P}\Gamma^1(2) = \mathrm{P}\Gamma^0(2)$. By an example of Rademacher [22, Sec. 8], we have

$$\mathrm{P}\Gamma^0(2) = \left\langle \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \right\rangle * \left\langle \begin{pmatrix} 1 & -2 \\ 1 & -1 \end{pmatrix} \right\rangle$$

where the first factor is infinite cyclic and the second one has order 2. The Kurosh Subgroup Theorem yields that $\bar{\rho}(\Gamma^+(G,\pi))$ is the free product of

(i) a possibly trivial free group,

(ii) certain subgroups of conjugates of $\langle \left(\begin{smallmatrix} 1 & 0 \\ -1 & 1 \end{smallmatrix}\right) \rangle$,

(iii) certain conjugates of $\left\langle \left(\begin{smallmatrix} 1 & -2 \\ 1 & -1 \end{smallmatrix}\right) \right\rangle$.

We shall prove that a factor of type (i) or (ii) actually appears. To this end let us assume that $\bar{\rho}(\Gamma^+(G,\pi))$ is the free product of factors of type (iii) only. Then $\bar{\rho}(\Gamma^+(G,\pi))$ is generated by elements of order 2 and $\bar{\rho}(\Gamma^+(G,\pi))^{\mathrm{ab}} \cong (\mathbb{Z}/2\mathbb{Z})^m$ for some $m \in \mathbb{N}$. Let k be the order of G. Then the automorphism $\varphi \in \mathrm{Aut}^+(F_2)$ given by

$$\varphi(x) = xy^k,\ \varphi(y) = y$$

is an element of $\Gamma^+(G,\pi)$. Hence

$$M := \begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix} \in \bar{\rho}(\Gamma^+(G,\pi)).$$

Since $M \in \langle \left(\begin{smallmatrix} 1 & 0 \\ -1 & 1 \end{smallmatrix}\right) \rangle$, one easily sees that the image of M in $\mathrm{P}\Gamma^0(2)^{\mathrm{ab}}$ has infinite order. On the other hand, the image of M in $\bar{\rho}(\Gamma^+(G,\pi))^{\mathrm{ab}}$ must have finite order. Observe that the inclusion $\bar{\rho}(\Gamma^+(G,\pi)) \hookrightarrow \mathrm{P}\Gamma^0(2)$ induces a homomorphism $\bar{\rho}(\Gamma^+(G,\pi))^{\mathrm{ab}} \to \mathrm{P}\Gamma^0(2)^{\mathrm{ab}}$ such that the following diagram commutes.

$$\begin{array}{ccc} \bar{\rho}(\Gamma^+(G,\pi)) & \longrightarrow & \mathrm{P}\Gamma^0(2) \\ \downarrow & & \downarrow \\ \bar{\rho}(\Gamma^+(G,\pi))^{\mathrm{ab}} & \longrightarrow & \mathrm{P}\Gamma^0(2)^{\mathrm{ab}} \end{array}$$

This implies that the image of M in $\mathrm{P}\Gamma^0(2)^{\mathrm{ab}}$ has finite order, contradiction.

The proof for $G^{\mathrm{ab}} = \mathbb{Z}/3\mathbb{Z}$ is almost the same. In the remaining cases, we find, by Proposition 3.4, that $\bar{\rho}(\Gamma^+(G,\pi))$ is a finite index subgroup of a free subgroup of $\mathrm{PSL}_2(\mathbb{Z})$. In particular, it has infinite abelianization and so must have $\Gamma^+(G,\pi)$. □

Chapter 5

Suggestions for Further Research

Motivated by Theorem 4.55, the first open problem we mention is

Problem 1. *Does $\Gamma^+(G,\pi)$ have infinite abelianization for all epimorphisms $\pi : F_2 \to G$ of F_2 onto a non-trivial finite group?*

We have seen in Theorem 4.55 that this problem is, in fact, only open for perfect groups G. One can reduce it further to finite simple groups using the following observation.

Suppose that $\pi : F_2 \to G$ is an epimorphism of F_2 onto a finite group. Further suppose that $\alpha : G \to H$ is an epimorphism such that $\Gamma^+(H,\alpha\pi)$ has infinite abelianization, that is, it maps onto $\mathbb{Z}$. Now $\Gamma^+(G,\pi)$ is a finite index subgroup of $\Gamma^+(H,\alpha\pi)$ so that it maps onto a finite index subgroup of $\mathbb{Z}$, that is, it maps onto $\mathbb{Z}$. Hence also $\Gamma^+(G,\pi)$ has infinite abelianization.

Instead of considering standard congruence subgroups of $\mathrm{Aut}^+(F_2)$ and their abelianizations, it might be easier to consider principal congruence subgroups. Let us recall the definition.

Let $K \leq F_2$ be a finite index subgroup of F_2, fixed by all automorphisms in $\mathrm{Aut}^+(F_2)$. Note that, since $\mathrm{Inn}(F_2) \leq \mathrm{Aut}^+(F_2)$, the subgroup K is then normal in F_2. We call

$$\ker(\mathrm{Aut}^+(F_2) \to \mathrm{Aut}(F_2/K))$$

the *principal congruence subgroup of* $\mathrm{Aut}^+(F_2)$ *associated to* K. Observe that if $\pi : F_2 \to F_2/K$ is the natural projection, then

$$\ker(\mathrm{Aut}^+(F_2) \to \mathrm{Aut}(F_2/K)) = \Gamma^+(F_2/K,\pi).$$

Given an arbitrary epimorphism $\pi : F_2 \to G$ of F_2 onto a finite group G, one can associate a principal congruence subgroup as follows. Let $R :=$

$\ker(\pi)$. For $\varphi \in \mathrm{Aut}^+(F_2)$ we have $\ker(\pi\varphi^{-1}) = \varphi(R)$. Let

$$\widetilde{R} := \bigcap_{\varphi \in \mathrm{Aut}^+(F_2)} \ker(\pi\varphi^{-1}) = \bigcap_{\varphi \in \mathrm{Aut}^+(F_2)} \varphi(R).$$

Then $\widetilde{R} \leq F_2$ is invariant under $\mathrm{Aut}^+(F_2)$. Moreover, since R has finite index in F_2 and π has finite orbit in $\mathbf{E}_2(G)$, the subgroup $\widetilde{R}$ has finite index in F_2. Define

$$\widetilde{\pi} : F_2 \longrightarrow F_2/\widetilde{R}$$

as the natural projection. Then

$$\Gamma^+(F_2/\widetilde{R}, \widetilde{\pi}) = \ker(\mathrm{Aut}^+(F_2) \to \mathrm{Aut}(F_2/\widetilde{R}))$$

is a principal congruence subgroup. It is contained in $\Gamma^+(G, \pi)$, as one easily verifies.

Recall that if $B \leq A$ are groups, then the *core of B in A* is defined as the intersection of all conjugates of B in A, that is, $\mathrm{core}(B, A) = \bigcap_{a \in A} aBa^{-1}$. It is the largest normal subgroup of A, contained in B. The following is easily verified.

Lemma 5.1. *Given an epimorphism $\pi : F_2 \to G$ of F_2 onto a finite group G, let $\widetilde{R} := \bigcap_{\varphi \in \mathrm{Aut}^+(F_2)} \ker(\pi\varphi^{-1})$ and $\widetilde{\pi} : F_2 \to F_2/\widetilde{R}$ be the natural projection. Then $\Gamma^+(F_2/\widetilde{R}, \widetilde{\pi}) = \mathrm{core}(\Gamma^+(G, \pi), \mathrm{Aut}^+(F_2))$.*

In the above situation, we shall call $\Gamma^+(F_2/\widetilde{R}, \widetilde{\pi})$ the *principal congruence subgroup of* $\mathrm{Aut}^+(F_2)$ *associated to* π.

In what follows let

$$\bar{\rho} : \mathrm{Aut}^+(F_2) \to \mathrm{PSL}_2(\mathbb{Z})$$

be the standard representation of $\mathrm{Aut}^+(F_2)$ followed by the natural projection of $\mathrm{SL}_2(\mathbb{Z})$ onto $\mathrm{PSL}_2(\mathbb{Z})$.

Lemma 5.2. *Let $\pi : F_2 \to G$ be an epimorphism onto a finite group such that $\pi(x)$ is not conjugate to $\pi(y)^{\pm 1}$ in G, that is, $\pi(x)$ is neither conjugate to $\pi(y)$ nor to $\pi(y)^{-1}$. Then $\bar{\rho}(\Gamma^+(G, \pi))$ does not contain the elements $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right)$.*

Proof. One has to verify that $\pm\left(\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right)$ and $\pm\left(\begin{smallmatrix}0 & -1\\ 1 & 1\end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ are not contained in $\rho(\Gamma^+(G,\pi))$. Assume that $\left(\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right) \in \rho(\Gamma^+(G,\pi))$. Since $\ker(\rho) = \mathrm{Inn}(F_2)$, there is some $w \in F_2$ such that the automorphism $\varphi \in \mathrm{Aut}^+(F_2)$ induced by $\varphi(x) = wyw^{-1}$, $\varphi(y) = wx^{-1}w^{-1}$ is in $\Gamma^+(G,\pi)$. Hence $\pi(x) = \pi(w)\pi(y)\pi(w)^{-1}$, contradiction. The other cases are similar. □

Recall that $\mathrm{PSL}_2(\mathbb{Z}) = \langle\left(\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right)\rangle * \langle\left(\begin{smallmatrix}0 & -1\\ 1 & 1\end{smallmatrix}\right)\rangle$. An immediate consequence of the Kurosh Subgroup Theorem is that if $H \leq \mathrm{PSL}_2(\mathbb{Z})$ is a subgroup, not containing any conjugate of $\left(\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}0 & -1\\ 1 & 1\end{smallmatrix}\right)$, then H is free. This leads to

Corollary 5.3. *Let $\pi : F_2 \to G$ be an epimorphism onto a finite group G such that $\pi(x)$ is not conjugate to $\pi(y)^{\pm 1}$ in G. Then the principal congruence subgroup associated to π maps onto a free group. In particular, it has infinite abelianization.*

Proof. Recall that the principal congruence subgroup associated to π is given by $\mathrm{core}(\Gamma^+(G,\pi), \mathrm{Aut}^+(F_2))$. We show that the image

$$H := \bar{\rho}(\mathrm{core}(\Gamma^+(G,\pi), \mathrm{Aut}^+(F_2)))$$

is free. Assume that H contains a conjugate of $\left(\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right)$. Since H is normal in $\mathrm{PSL}_2(\mathbb{Z})$, it also contains $\left(\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right)$ itself. But since $H \leq \bar{\rho}(\Gamma^+(G,\pi))$ we know from Lemma 5.2 that this cannot be true. Similarly, H does not contain any conjugate of $\left(\begin{smallmatrix}0 & -1\\ 1 & 1\end{smallmatrix}\right)$ and we thus see that H is free. □

Corollary 5.4. *For every finite group G there is some $\pi : F_2 \to G$ such that the associated principal congruence subgroup maps onto a free group and thus has infinite abelianization.*

Proof. As a consequence of the classification of finite simple groups, every finite simple group H can be generated by two elements h_1, h_2 where $\mathrm{ord}(h_1) \neq \mathrm{ord}(h_2)$. So, in particular, h_1 is not conjugate to $h_2^{\pm 1}$ in H. Now let H be a simple quotient of G and h_1, h_2 as above. Define an epimorphism $\pi' : F_2 \to H$ by $\pi'(x) := h_1$ and $\pi'(y) := h_2$. By Lemma 2.6 there are lifts $g_1, g_2 \in G$ of h_1, h_2, respectively, such that $\langle g_1, g_2\rangle = G$.

Set $\pi(x) := g_1$ and $\pi(y) := g_2$. Then $\Gamma^+(G,\pi) \leq \Gamma^+(H,\pi')$. As seen above, $\bar{\rho}(\mathrm{core}(\Gamma^+(H,\pi'),\mathrm{Aut}^+(F_2)))$ is free and hence so is

$$\bar{\rho}(\mathrm{core}(\Gamma^+(G,\pi),\mathrm{Aut}^+(F_2))) \leq \bar{\rho}(\mathrm{core}(\Gamma^+(H,\pi'),\mathrm{Aut}^+(F_2))).$$

This completes the proof. □

Since, by construction, the principal congruence subgroup associated to an epimorphism $\pi : F_2 \to G$ only depends on the connected component of $(\pi(x),\pi(y))$ in $\mathbf{V}_2(G)$, we also get

Corollary 5.5. *Let G be a finite group with the property that every connected component of $\mathbf{V}_2(G)$ contains a pair (g,h) such that g is not conjugate to $h^{\pm 1}$ in G. Then for every epimorphism $\pi : F_2 \to G$, the associated principal congruence subgroup maps onto a free group and thus has infinite abelianization.*

This leads to

Problem 2. *For which finite (non-abelian) groups G does the following hold? Every connected component of $\mathbf{V}_2(G)$ contains a pair (g,h) such that g is not conjugate to $h^{\pm 1}$.*

We formulate the problem in this way, since Proposition 5.8 below gives an interesting example for a group G which does not satisfy the property in question. To understand this, we need two lemmas.

Lemma 5.6. *Let $G = \langle g,h\rangle$ be a finite group. Suppose that each of the pairs (g,hg) and (gh,h) is conjugate to (g,h). Then every pair $(g',h') \in \mathbf{V}_2(G)$ in the connected component of (g,h) is conjugate to (g,h).*

Proof. Inductively one finds that the pairs (g,hg^k) and (gh^k,h) are conjugate to (g,h) for $k \in \mathbb{N}$. Since g and h have finite order, the same is still true for $k \in \mathbb{Z}$. In particular, (g,hg^{-1}) and (gh^{-1},h) are also conjugate to (g,h). By conjugation with g and h we now find that all pairs

$$(gh^{\pm 1},h),\ (h^{\pm 1}g,h),\ (g,g^{\pm 1}h),\ (g,hg^{\pm 1})$$

which are obtained from (g,h) by an elementary Nielsen move are conjugate to (g,h). Since every pair in the connected component of (g,h) is obtained from (g,h) by a Nielsen move, the lemma follows. □

Lemma 5.7. *Let $G = \langle g, h\rangle$ be a finite group.*

(a) The following two properties are equivalent.

(1) There exist $a, b \in G$ such that

$$g = aha^{-1}, \qquad g = bhb^{-1},$$
$$h = ag^{-1}a^{-1}, \qquad h = bg^{-1}hb^{-1}.$$

(2) For $\pi : F_2 \to G$, with $\pi(x) = g$ and $\pi(y) = h$, we have

$$\rho(\Gamma^+(G, \pi)) = \mathrm{SL}_2(\mathbb{Z}),$$

that is, $\mathrm{Inn}(F_2) \cdot \Gamma^+(G, \pi) = \mathrm{Aut}^+(F_2)$.

(b) If one (and thus both) of the properties (1), (2) is satisfied, then for every pair $(g', h') \in \mathbf{V}_2(G)$ in the connected component of (g, h) we have that g' and h' are conjugate.

(c) If one (and thus both) of the properties (1), (2) is satisfied, then $\ker(\pi) \leq F_2$ is fixed by all elements of $\mathrm{Aut}^+(F_2)$, that is, $\Gamma^+(G, \pi)$ is a principal congruence subgroup.

Proof. Let us first assume that (1) holds. Let $w \in \pi^{-1}(a)$ and $\varphi \in \mathrm{Aut}^+(F_2)$ be the automorphism induced by $\varphi(x) = wyw^{-1}$, $\varphi(y) = wx^{-1}w^{-1}$. Then one verifies that $\pi(\varphi(x)) = g = \pi(x)$ and $\pi(\varphi(y)) = h = \pi(y)$. Hence $\varphi \in \Gamma^+(G, \pi)$. It follows that $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \in \rho(\Gamma^+(G, \pi))$. Similarly, one also shows that $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right) \in \rho(\Gamma^+(G, \pi))$. This implies (2).

The argument for (2) $\Rightarrow$ (1) is very similar.

Now assume that (1) and (2) hold. Suppose that $(g', h') \in \mathbf{V}_2(G)$ is in the connected component of (g, h). Then $\Gamma^+(G, \pi)$ and $\Gamma^+(G, \pi')$ with $\pi'(x) = g'$, $\pi'(y) = h'$ are conjugate. Hence so are their images under the representation ρ. It follows that $\rho(\Gamma^+(G, \pi')) = \mathrm{SL}_2(\mathbb{Z})$. Now the equivalence of (1) and (2) yields that, in particular, there is some $a' \in G$ such that $g' = a'h'a'^{-1}$. So g' and h' are conjugate and (b) is proved.

To prove (c), suppose that $w \in \ker(\pi)$ and $\varphi \in \mathrm{Aut}^+(F_2)$. By (2) we have $\varphi = \alpha_u \cdot \gamma$ with $\alpha_u \in \mathrm{Inn}(F_2)$ and $\gamma \in \Gamma^+(G, \pi)$. Now

$$\pi(\alpha_u(\gamma(w))) = \pi(u) \cdot \pi(\gamma(w)) \cdot \pi(u)^{-1} = \pi(u) \cdot \pi(w) \cdot \pi(u^{-1}) = 1.$$

So $\varphi(w) = \alpha_u\gamma(w) \in \ker(\pi)$. This completes the proof. □

The above result leads to

Problem 3. *If for every pair $(g', h') \in \mathbf{V}_2(G)$ in the connected component of (g, h) we have that g' and h' are conjugate, does it follow that there exist a and b as in (1)?*

A priori it is not clear if there exist finite groups satisfying the properties considered above. The following result gives an example. It is interesting that, in this example, $\ker(\pi)$ is not only fixed by $\mathrm{Aut}^+(F_2)$ but also by $\mathrm{Aut}(F_2)$, i.e., it is a characteristic subgroup of F_2.

Proposition 5.8. *Let $\pi : F_2 \to \mathrm{SL}_3(11)$ be the epimorphism given by $\pi(x) = g$, $\pi(y) = h$ with*

$$g := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 2 \end{pmatrix} \quad \textit{and} \quad h := \begin{pmatrix} 9 & 0 & 1 \\ 8 & 0 & 2 \\ 0 & 1 & 0 \end{pmatrix}.$$

Then every pair $(g', h') \in \mathbf{V}_2(\mathrm{SL}_3(11))$ in the connected component of (g, h) has the property that g' is conjugate to h'. Moreover

$$\rho(\Gamma^+(\mathrm{SL}_3(11), \pi)) = \mathrm{SL}_2(\mathbb{Z})$$

and $\ker(\pi) \leq F_2$ is a characteristic subgroup.

Proof. Let

$$c := \begin{pmatrix} 8 & 0 & 0 \\ 0 & 8 & 0 \\ 0 & 0 & 5 \end{pmatrix}, \quad d := \begin{pmatrix} 6 & 10 & 5 \\ 7 & 3 & 9 \\ 3 & 3 & 3 \end{pmatrix}.$$

Then $c(g, hg)c^{-1} = (g, h)$ and $d(gh, h)d^{-1} = (g, h)$. By Lemma 5.6, it follows that every pair (g', h') in the connected component of (g, h) is conjugate to (g, h). Since

$$\begin{pmatrix} 2 & 9 & 9 \\ 2 & 2 & 1 \\ 8 & 4 & 8 \end{pmatrix} h \begin{pmatrix} 2 & 9 & 9 \\ 2 & 2 & 1 \\ 8 & 4 & 8 \end{pmatrix}^{-1} = g$$

the first part of the proposition follows.

For the second part, let

$$a := \begin{pmatrix} 8 & 3 & 3 \\ 2 & 2 & 1 \\ 2 & 1 & 2 \end{pmatrix} \quad \text{and} \quad b := \begin{pmatrix} 9 & 2 & 2 \\ 5 & 5 & 8 \\ 10 & 5 & 10 \end{pmatrix}.$$

Then property (1) in Lemma 5.7 is satisfied, so that $\rho(\Gamma^+(\mathrm{SL}_3(11), \pi)) = \mathrm{SL}_2(\mathbb{Z})$. To see that $\ker(\pi) \leq F_2$ is a characteristic subgroup, we recall that $\mathrm{Aut}^+(F_2)$ is a subgroup of index 2 in $\mathrm{Aut}(F_2)$. Since we already know that $\ker(\pi)$ is fixed by $\mathrm{Aut}^+(F_2)$, it thus suffices to show that $\ker(\pi)$ is also fixed by one specific automorphism of F_2 which is not contained in $\mathrm{Aut}^+(F_2)$. We choose the one induced by $x \mapsto x$ and $y \mapsto y^{-1}$. Let

$$e := \begin{pmatrix} 8 & 0 & 0 \\ 0 & 0 & 9 \\ 0 & 9 & 0 \end{pmatrix}.$$

Then

$$eg^{-\mathrm{tr}}e^{-1} = g \quad \text{and} \quad eh^{-\mathrm{tr}}e^{-1} = h^{-1}.$$

Note that the map from $\mathrm{SL}_3(11)$ onto itself which sends an element to the transpose of its inverse is an automorphism of $\mathrm{SL}_3(11)$. Composing it with the inner automorphism given by conjugation with e, we see that $g \mapsto g$, $h \mapsto h^{-1}$ induces an automorphism of $\mathrm{SL}_3(11)$. In particular, if a word $w(x, y) \in F_2$ lies in the kernel of π, then so does $w(x, y^{-1})$. In other words, $\ker(\pi)$ is fixed by $x \mapsto x$, $y \mapsto y^{-1}$, as desired. □

We note that this is just the first example in an infinite family found by B. Klopsch in an unpublished work.

The example given in Proposition 5.8 leads to the following very concrete question

Problem 4. *Does $\Gamma^+(\mathrm{SL}_3(11), \pi)$ with $\pi(x) = g$, $\pi(y) = h$ have infinite abelianization?*

It also leads to

Problem 5. *For which epimorphisms $\pi : F_2 \to G$ of F_2 onto a finite group G do we have $\rho(\Gamma^+(G, \pi)) = \mathrm{SL}_2(\mathbb{Z})$?*

The following problem is not directly connected to congruence subgroups of $\mathrm{Aut}^+(F_2)$, but, noting that $\mathrm{PSL}_3(11) = \mathrm{SL}_3(11)$, also motivated by Proposition 5.8.

Problem 6. *For which prime powers q is there an epimorphism $\pi : F_2 \to \mathrm{PSL}_3(q)$ such that $\ker(\pi) \leq F_2$ is a characteristic subgroup?*

Of course, one can generalize the question by considering $\mathrm{PSL}_n(q)$, $n \geq 3$, instead of $\mathrm{PSL}_3(q)$. Even more general, one might also consider epimorphisms $F_r \to \mathrm{PSL}_n(q)$, $r \geq 2$. This leads to an interesting connection to Wiegold's conjecture, which says that for every $r \geq 3$ and every non-abelian finite group G, there is only one T_r-system. (See for example [21, Conj. 2.5.4].) Indeed, if Wiegold's conjecture holds, then, for every $r \geq 3$, there exists no epimorphism from F_r onto a non-abelian finite simple group G such that its kernel is characteristic in F_r. This can be seen as follows.

Suppose that Wiegold's conjecture holds and that we have an epimorphism $\pi : F_r \to G$, $r \geq 3$, onto a non-abelian finite simple group such that $\ker(\pi)$ is characteristic in F_r. Now, since G has only one T_r-system, every epimorphism from F_r onto G is of the form $\alpha\pi\varphi$ with $\alpha \in \mathrm{Aut}(G)$ and $\varphi \in \mathrm{Aut}^+(F_r)$. Observe that

$$\ker(\alpha\pi\varphi) = \ker(\pi\varphi) = \varphi^{-1}(\ker(\pi)) = \ker(\pi)$$

where the last equality holds, since $\ker(\pi)$ is characteristic in F_r. It follows that $\ker(\pi)$ is the only normal subgroup of F_r such that the corresponding quotient is isomorphic to G. By the classification of finite simple groups, G is generated by two elements. Therefore, for every $1 \leq i \leq r$, there is some epimorphism $\pi_i : F_r \to G$ such that $x_i \in \ker(\pi_i)$. Since $\ker(\pi_i) = \ker(\pi)$, it follows that $\ker(\pi) = F_r$, contradiction.

Another, very natural question is

Problem 7. *For which epimorphisms $\pi : F_2 \to G$ of F_2 onto a finite group G is the image $\rho(\Gamma^+(G, \pi))$ a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$?*

The most general result, we have obtained so far is that for metacyclic groups G it always is, see Corollary 4.26. Also for $G = \mathbb{Z}/m\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}$ with m odd this is true, see Theorem 4.43. A counterexample is given by

$G = A_5$, the alternating group of degree 5. Moreover, A_5 is the smallest group with this property.

As a generalization, one might expect that $\rho(\Gamma^+(G,\pi))$ is always a congruence subgroup, if G is solvable. This turns out to be false. There is a solvable group G of order 128 for which $\rho(\Gamma^+(G,\pi))$ is not a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$, see [3, Section 5] for details. Computational results indicate that $\rho(\Gamma^+(G,\pi))$ is always a congruence subgroup if G is metabelian.

Part (iii) of Theorem 4.49 leads us to a concrete case of the above problem, namely:

Problem 8. *Is the the image* $\rho(\Gamma^+(\mathbb{Z}/p\mathbb{Z} \wr \mathbb{Z}/p\mathbb{Z}, \pi)) \leq \mathrm{SL}_2(\mathbb{Z})$ *a congruence subgroup?*

We have

Example 5.9. The image $\rho(\Gamma^+(\mathbb{Z}/5\mathbb{Z} \wr \mathbb{Z}/5\mathbb{Z}, \pi)) \leq \mathrm{SL}_2(\mathbb{Z})$ contains $\Gamma(25)$ and thus is a congruence subgroup.

We have verified this example by using a Reidemeister rewriting process to obtain generators of $\Gamma(25)$ from the ones of $\Gamma(5)$ which are provided by Frasch [10]. One can, basically, do the same for any given p, but it seems unlikely that this procedure can be used to show that $\rho(\Gamma^+(\mathbb{Z}/p\mathbb{Z} \wr \mathbb{Z}/p\mathbb{Z}, \pi))$ always contains $\Gamma(p^2)$: using Frasch's results, it is easy to write down generators of $\Gamma(p)$ for a concrete prime p, but the arithmetic modulo p used in the computation of these generators and the Reidemeister rewriting process seems to make it impossible to extend this method to a general proof.

Finally, we have the popular congruence subgroup problem.

Problem 9. *Is every finite index subgroup of* $\mathrm{Aut}^+(F_n)$ *a congruence subgroup?*

For $\mathrm{SL}_n(\mathbb{Z})$ this problem is already solved. The answer is yes for $n \geq 3$ (see [5], [18]) and no for $n = 2$ (see [11]). More recently it has been shown that, in the case $n = 2$, every finite index subgroup of $\mathrm{Aut}(F_2)$ is a congruence subgroup. See [4] and [6]. For $n \geq 3$ this problem is still open.

Bibliography

[1] D. Appel, *Linear Representations of the Automorphism Group of a Free Group.* Master Thesis (Heinrich-Heine-Universität Düsseldorf, Germany, 2006).

[2] D. Appel, *Regular Circulant Matrices.* arXiv:0909.3507v1, (2009).

[3] D. Appel, E. Ribnere, *On the index of congruence subgroups of* $\mathrm{Aut}(F_n)$., J. Alg. **321** (2009), 2875–2889.

[4] M. Asada, *The faithfulness of the monodromy representations associated with certain families of algebraic curves.* J. Pure Appl. Algebra **159** (2001), no. 2–3, 123–147.

[5] H. Bass, M. Lazard, J-P. Serre, *Sous-groupes d'indicis finis dans* $\mathrm{SL}(n, \mathbb{Z})$. Bull. Am. Math. Soc. **70** (1964), 385–392.

[6] K.-U. Bux, M. V. Ershov, A. S. Rapinchuk, *The congruence subgroup property of* $\mathrm{Aut}(F_2)$*: A group-theoretic proof of Asada's theorem* arXiv:0909.0304v1 (2009).

[7] P. Diaconis, R. Graham, *The graph of generating sets of an abelian group.* Colloq. Math. **80** (1999), 31–38.

[8] J. L. Dyer, E. Formanek, E. K. Grossman, *On the linearity of automorphism groups of free groups.* Arch. Math., **38**, (1982), 404–409.

[9] E. Formanek, C. Procesi, *The automorphism group of a free group is not linear.* J. Alg., **149**, (1992), 494–499.

[10] H. Frasch, *Die Erzeugenden der Hauptkongruenzuntergruppen für Primzahlstufen.* Math. Ann., **108**, (1933), 229–252.

[11] R. Fricke, F. Klein, *Vorlesungen über die Thoerie der automorphen Funktionen.* B. G. Teubner Verlagsgesellschaft, Stuttgart, 1890–1892.

[12] F. Grunewald, A. Lubotzky, *Linear Representations of the Automorphism Group of a Free Group.* Geom. Funct. Anal. **18** (2009), 1564–1608.

[13] P. Hall, *The Eulerian functions of a group.* Quart. J. Math., **7** (1936), 134–151.

[14] D. L. Johnson, *Presentations of Groups.* Cambridge University Press, Cambridge, 1976.

[15] D. Krammer, *Braid groups are linear.* Ann. Math., **155**, (2002), 131–156.

[16] R. C. Lyndon, P. E. Schupp, *Combinatorial Group Theory* (Springer Verlag, New York - Heidelberg - Berlin, 1977).

[17] Web page of the computer algebra system MAGMA: http://magma.maths.usyd.edu.au/magma/

[18] J. L. Mennicke, *Finite factor groups of the unimodular group.* Ann. Math. (2) **81** (1965), 31–37.

[19] W. Magnus, A. Karrass, D. Solitar, *Combinatorial Group Theory* (John Wiley & Sons, Inc., New York, 1966).

[20] B. H. Neumann, H. Neumann, *Zwei Klassen charakteristischer Untergruppen und ihre Faktorgruppen.* Math. Nachr. **4** (1951) 106–125.

[21] I. Pak, *What do we know about the product replacement algorithm?* Groups and Computation III (Columbus, Ohio, 1999), Ohio State Univ. Math. Res. Inst. Publ. **8**, de Gruyter, Berlin, (2001), 301–347.

[22] H. Rademacher, *Über die Erzeugenden von Kongruenzuntergruppe der Modulgruppe.* Abhandlungen Hamburg, **7**, (1929), 134–148.

[23] D. J. S. Robinson, *A Course in the Theory of Groups* (Springer Verlag, New York - Heidelberg - Berlin, 1982).

[24] M. Siegmund, *Generalized Torelli Groups.* Dissertation (Heinrich-Heine-Universität Düsseldorf, Germany, 2007).

[25] T. Satoh, *The abelianization of the congruence IA-automorphism group of a free group.* Math. Proc. Camb. Phil. Soc. **142** (2007), 239–248.

[26] T. Satoh, *Corrigendum: The abelianization of the congruence IA-automorphism group of a free group.* Math. Proc. Camb. Phil. Soc. **143** (2007), 255–256.