

Free Groups and the Axiom of Choice



Philipp Kleppmann

University of Cambridge

Department of Pure Mathematics and Mathematical Statistics

Corpus Christi College

August 2015

This dissertation is submitted for the degree of

Doctor of Philosophy

Declaration

This dissertation is the result of my own work and includes nothing which is the outcome of work done in collaboration except as declared in the Acknowledgements and specified in the text. Chapters 1 and 2, and sections 4.1 and 4.2 consist of review material. Chapter 3, section 4.3, and chapters 5 and 6 are original work.

This dissertation is not substantially the same as any that I have submitted, or, is being concurrently submitted for a degree or diploma or other qualification at the University of Cambridge or any other University or similar institution except as declared in the Acknowledgements and specified in the text. I further state that no substantial part of my dissertation has already been submitted, or, is being concurrently submitted for any such degree, diploma or other qualification at the University of Cambridge or any other University of similar institution except as declared in the Acknowledgements and specified in the text

Philipp Kleppmann

Acknowledgments

I would like to express my gratitude to my supervisor, Thomas Forster, for asking about the Nielsen–Schreier theorem and for his advice and guidance over the last three years.

My thanks also go to John Truss and Benedikt Löwe for finding an error and suggesting a correction in the proof of proposition 5.13, to Thomas Forster for finding a simplification in the proof of proposition 5.13, to Vu Dang for spotting a gap in the proof of theorem 5.23, and to Alex Kruckman for providing the example 6.1. I would like to thank: Zachiri McKenzie, David Matthai, and Adam Lewicki for fruitful discussions; Debbie and Randall Holmes for hosting me in Boise for three weeks; the logic group in Leeds for informative and entertaining meetings; and Thomas Forster, Nicola Kleppmann, and Martin Kleppmann for proofreading my manuscript.

I am grateful to Corpus Christi College and the Department of Pure Mathematics and Mathematical Statistics for providing me with financial support which allowed me to complete my studies.

None of this would have been possible without my family's constant support and encouragement. It means a lot to me.

Free Groups and the Axiom of Choice

Philipp Kleppmann

Summary

The Nielsen–Schreier theorem states that subgroups of free groups are free. As all of its proofs use the Axiom of Choice, it is natural to ask whether the theorem is equivalent to the Axiom of Choice. Other questions arise in this context, such as whether the same is true for free abelian groups, and whether free groups have a notion of dimension in the absence of Choice.

In chapters 1 and 2 we define basic concepts and introduce Fraenkel–Mostowski models.

In chapter 3 the notion of dimension in free groups is investigated. We prove, without using the full Axiom of Choice, that all bases of a free group have the same cardinality. In contrast, a closely related statement is shown to be equivalent to the Axiom of Choice.

Schreier graphs are used to prove the Nielsen–Schreier theorem in chapter 4. For later reference, we also classify Schreier graphs of (normal) subgroups of free groups.

Chapter 5 starts with an analysis of the use of the Axiom of Choice in the proof of the Nielsen–Schreier theorem. Then we introduce *representative functions* – a tool for constructing choice functions from bases. They are used to deduce the finite Axiom of Choice from Nielsen–Schreier, and to prove the equivalence of a strong form of Nielsen–Schreier and the Axiom of Choice. Using Fraenkel–Mostowski models, we show that Nielsen–Schreier cannot be deduced from the Boolean Prime Ideal Theorem.

Chapter 6 explores properties of free abelian groups that are similar to those considered in chapter 5. However, the commutative setting requires new ideas and different proofs. Using representative functions, we deduce the Axiom of Choice for pairs from the abelian version of the Nielsen–Schreier theorem. This implication is shown to be strict by proving that it doesn't follow from the Boolean Prime Ideal Theorem. We end with a section on potential applications to vector spaces.

Contents

1 Preliminaries	7
1.1 Introduction	7
1.2 Sets	8
1.3 Free groups	11
1.4 Free abelian groups	13
1.5 Choice principles	13
2 Fraenkel–Mostowski models	16
2.1 Setup	16
2.2 An example	20
2.3 Two models	22
2.4 A transfer theorem	24
3 The size of bases	27
3.1 Bases of isomorphic free groups	28
3.2 Bases of equipollent free groups	31

4 Nielsen–Schreier	34
4.1 Schreier graphs	34
4.2 A proof of the Nielsen–Schreier theorem	38
4.3 Classifying Schreier graphs	42
5 Nielsen–Schreier and the Axiom of Choice	46
5.1 A brief history	47
5.2 The use of the Axiom of Choice	49
5.3 Does Nielsen–Schreier imply the Axiom of Choice?	52
5.4 Nielsen–Schreier implies the finite Axiom of Choice	56
5.5 Nielsen–Schreier doesn’t follow from the Prime Ideal Theorem	63
5.6 Reduced Nielsen–Schreier implies the Axiom of Choice	66
6 Free abelian groups	74
6.1 Abelian Nielsen–Schreier implies AC_2	75
6.2 The implication is strict	78
6.3 More on representative functions	81
Bibliography	86

Chapter 1

Preliminaries

1.1 Introduction

The Axiom of Choice was formulated in 1904 by Zermelo [41] in order to prove the well-ordering theorem. It is the only axiom of set theory that asserts the existence of a set without also defining it. Although it was disputed in its early days, it is now a well established axiom of set theory. In 1964, Mendelson [32] (p. 201) wrote:

The status of the Axiom of Choice has become less controversial in recent years. To most mathematicians it seems quite plausible and it has so many important applications in practically all branches of mathematics that not to accept it would seem to be a wilful hobbling of the practicing mathematician.

The controversy has led to the Axiom of Choice occupying a distinguished position among the axioms of Zermelo–Fraenkel set theory with Choice (ZFC). As many general and powerful theorems are among its consequences, its use in proofs of such results has been studied. Theorems of ZFC can be viewed as choice principles ordered by implication over Zermelo–Fraenkel set theory (ZF), i.e. $\phi \geq \psi$ iff $\text{ZF} \vdash \phi \Rightarrow \psi$. This gives rise to a hierarchy of statements which is the subject of several reference books – including

Howard and Rubin [19], Herrlich [14], and Jech [22] – and the numerous papers cited in them.

One choice principle that stands out is the Nielsen–Schreier theorem, which states that subgroups of free groups are free. Although the theorem is elegant and simple to state, little is known about its deductive strength. No progress has been made on this problem since the 1980s (Howard [16], Howard [17]). This gap in our knowledge is the starting point of this dissertation. We will improve the known results and prove some new theorems about subgroups of free groups and the Axiom of Choice.

The relation between bases of vector spaces and the Axiom of Choice has been studied in many articles. Vector spaces share some properties with free groups, and free abelian groups act as a bridge between them. This allows an exchange of questions and solutions to take place between free groups and vector spaces. We will analyse the notion of dimension, which is important in linear algebra, in the new context of free groups. In the last chapter, we also translate the technique of using representative functions, originally developed for free groups, to the new context of free abelian groups.

In the remainder of this chapter we give definitions, fix conventions, and review some basic results. Section 1.2 describes the set theories ZF and ZFA and introduces some notation. In section 1.3 we define free groups and review some of their elementary properties. Free abelian groups are defined in section 1.4. In this thesis we investigate the relationship between free groups and the Axiom of Choice. A list of choice principles considered in later chapters is given in section 1.5.

1.2 Sets

We shall be working with two different kinds of set theory: The usual Zermelo–Fraenkel set theory with the Axiom of Choice (ZFC) or without it (ZF), and set theory with atoms (ZFA). The following list of ZF-axioms is taken from chapter 1 of Jech’s textbook [21].

1. *Axiom of Extensionality.* If X and Y have the same elements, then $X = Y$.

2. *Axiom of Pairing.* For any a and b there exists a set $\{a, b\}$ that contains exactly a and b .
3. *Axiom Schema of Separation.* If P is a property (with parameter p), then for any X and p there exists a set $Y = \{u \in X : P(u, p)\}$ that contains all those $u \in X$ that have property P .
4. *Axiom of Union.* For any X there exists a set $Y = \bigcup X$, the union of all elements of X .
5. *Axiom of Power Set.* For any X there exists a set $Y = \mathcal{P}(X)$, the set of all subsets of X .
6. *Axiom of Infinity.* There exists an infinite set.
7. *Axiom Schema of Replacement.* If a class F is a function, then for any X there exists a set $Y = F(X) = \{F(x) : x \in X\}$.
8. *Axiom of Regularity.* Every nonempty set has an \in -minimal element.

Adding the Axiom of Choice, we obtain ZFC:

Axiom of Choice. Every family of nonempty sets has a choice function.

ZFA is a close relative of ZF. It differs in that it allows for a set of *atoms*. In essence, an atom is an empty object that is indistinguishable from other atoms. In addition to the binary relation symbol \in , ZFA has two constant symbols: A for the set of atoms, and \emptyset for the empty set. The axioms of ZFA are the same as those of ZF, except for the following changes:

We say that x is a *set* if $x \notin A$, and that x is an *atom* if $x \in A$. The ZF-axioms of Extensionality and Regularity are weakened to apply to sets only:

1. *Axiom of Extensionality.* If X and Y are two *sets* with the same elements, then $X = Y$.
8. *Axiom of Regularity.* Every nonempty *set* has an ϵ -minimal element.

And there are two new axioms:

9. \emptyset has no members.
10. *Atoms have no members.*

Ordered pairs are written in angle brackets: $\langle x, y \rangle$. They are taken to be Kuratowski ordered pairs, i.e. $\langle x, y \rangle = \{\{x\}, \{x, y\}\}$. Ordered n -tuples are also written in angle brackets: $\langle x_1, \dots, x_n \rangle$. They are inductively defined by $\langle x_1, \dots, x_n \rangle = \langle x_1, \langle x_2, \dots, x_n \rangle \rangle$.

Functions $f : X \rightarrow Y$ are implemented as subsets of $X \times Y$. Given the function f , we may choose to apply it to subsets of X instead of elements of X : We define, for any $A \subseteq X$,

$$f''A = \{f(a) : a \in A\}.$$

If $A \subseteq X$, then the *restriction* of f to A is $f|_A : A \rightarrow Y : a \mapsto f(a)$.

Let X be a set. The cardinality of X is written $|X|$. An *aleph* is the cardinality of a well-ordered set. The *Hartogs aleph* of X , written $\aleph(X)$ is the least aleph with $\aleph(X) \not\leq |X|$.

The *von Neumann hierarchy* is defined by

$$\begin{aligned} V_0 &= \emptyset \\ V_{\alpha+1} &= \mathcal{P}(V_\alpha) \\ V_\lambda &= \bigcup_{\alpha < \lambda} V_\alpha \text{ for } \lambda \text{ a non-zero limit ordinal} \end{aligned}$$

We can overload the V_α as an operation on sets. If X is a set, then we let

$$\begin{aligned} V_0(X) &= X \\ V_{\alpha+1}(X) &= \mathcal{P}(V_\alpha(X)) \cup V_\alpha(X) \\ V_\lambda(X) &= \bigcup_{\alpha < \lambda} V_\alpha(X) \text{ for } \lambda \text{ a non-zero limit ordinal} \end{aligned}$$

1.3 Free groups

Let X be any set. Before defining the free group $F(X)$ on X , we must introduce some vocabulary.

Definition 1.1. $X^{-1} = \{x^{-1} : x \in X\}$ is a set of formal inverses of members of X . X^{-1} is always assumed to be disjoint from X . For brevity, we write X^\pm for $X \cup X^{-1}$.

Elements of X^\pm are X -letters.

X -words are products $x_1 \cdots x_n$, where $n \geq 0$ and $x_i \in X^\pm$ for $i = 1, \dots, n$. Sometimes it is more convenient to write them as $x_1^{\epsilon_1} \cdots x_n^{\epsilon_n}$, where $n \geq 0$, and, for $i = 1, \dots, n$, $x_i \in X$ and $\epsilon_i \in \{1, -1\}$. They are implemented as finite sequences $\langle x_1, \dots, x_n \rangle$ of elements of X^\pm .

The process of removing a pair $x^\epsilon x^{-\epsilon}$ from the X -word $x_1^{\epsilon_1} \cdots x^\epsilon x^{-\epsilon} \cdots x_n^{\epsilon_n}$ is called *cancellation*.

An X -word is X -reduced if no cancellation is possible.

The X -reduction of an X -word α is the result of performing all possible cancellations in α . It is independent of the order in which the cancellations are performed.

Two X -words are *equivalent* if they have the same X -reductions.

The X -length of an X -word α , written $\ell_X(\alpha)$ is the number of letters in the X -reduction of α .

When there is no danger of confusion, we may omit references to X .

Definition 1.2. The *free group* $F(X)$ consists of the set of all reduced X -words, together with a binary operation $*$ defined to be concatenation followed by X -reduction. The identity element of $F(X)$ is the empty word, written $\mathbf{1}$.

This means that, if $\alpha = x_1 \cdots x_n$ and $\beta = y_1 \cdots y_m$ are reduced X -words with $x_i, y_i \in X^\pm$, then $\alpha * \beta$ is the X -reduction of $x_1 \cdots x_n y_1 \cdots y_m$. For notational simplicity we often don't

make a distinction between an X -word and its X -reduction, and we may colloquially take $F(X)$ to be the set of *all* X -words together with the binary operation of concatenation.

Definition 1.3. Let F be a group. F is a *free group* if there is $X \subseteq F$ such that $F \cong F(X)$. If this is the case, we say that F is *free* on X , and that X is a *basis* for F . This means that a group F is free if there is $X \subseteq F$ such that every element $\alpha \in F$ can be written as a unique reduced product $x_1 \cdots x_n$ of X -letters.

Free groups are characterised by a universal property: Let F be a free group with basis X . If G is a group and $f : X \rightarrow G$ is any function, then f has a unique extension to a homomorphism $\phi : F \rightarrow G$, defined by:

$$\phi : F \rightarrow G : x_1^{\epsilon_1} \cdots x_n^{\epsilon_n} \mapsto f(x_1)^{\epsilon_1} \cdots f(x_n)^{\epsilon_n}.$$

Definition 1.4. If G is a group and $X \subseteq G$, then X is said to be *free* if there are no non-trivial relations between members of X . This means that, if $x_1 \cdots x_n$ is a reduced product of X -letters, and $x_1 \cdots x_n = \mathbf{1}$, then $n = 0$.

Let F be a free group. It is straightforward to check that $X \subseteq F$ is a basis (as defined in definition 1.3) if and only if it is a free generating set of F .

A fundamental result in the theory of free groups is the Nielsen–Schreier theorem. It states that subgroups of free groups are themselves free. The theorem was first proved in the finitely generated case by Nielsen [34]. Schreier [39] later used a different method to prove the general case. English versions of both proofs can be found in chapters 2 and 3 of Johnson’s book [25].

Theorem 1.5 (Nielsen–Schreier). *If F is a free group and H is a subgroup of F , then H is a free group.*

1.4 Free abelian groups

Definition 1.6. Let X be a set. The *free abelian group on X* , written $\text{FA}(X)$, is the quotient of the free group on X by its commutator subgroup. In other words,

$$\text{FA}(X) = \text{F}(X) / \langle \{\alpha\beta\alpha^{-1}\beta^{-1} : \alpha, \beta \in \text{F}(X)\} \rangle.$$

The process of taking the quotient of a group by its commutator subgroup is called *abelianisation*.

We use additive notation for abelian groups. So every $\alpha \in \text{FA}(X)$ may be written as a finite sum

$$\alpha = n_1x_1 + \dots + n_kx_k,$$

where $k \geq 0$, the $x_1, \dots, x_k \in X$ are distinct, and $n_1, \dots, n_k \in \mathbb{Z} \setminus \{0\}$. This expression is unique up to the ordering of its terms.

Definition 1.7. If $F = \text{FA}(X)$ is a free abelian group and $B \subseteq F$, then B is a *basis* of F if every $\alpha \in F$ can be uniquely written as a finite sum $\alpha = n_1b_1 + \dots + n_kb_k$ with $k \geq 0$, $b_1, \dots, b_k \in B$ distinct, and $n_1, \dots, n_k \in \mathbb{Z} \setminus \{0\}$.

Free abelian groups enjoy a similar universal property to free groups. Let $F = \text{FA}(X)$ be a free abelian group, and let A be any abelian group. If $f : X \rightarrow A$ is any function, then f has a unique extension to a group homomorphism

$$\phi : F \rightarrow A : \sum n_ix_i \mapsto \sum n_if(x_i).$$

1.5 Choice principles

In the following chapters, we will investigate the relationship between the Axiom of Choice, the Nielsen–Schreier theorem, and several related theorems. First, we list the well-known set theoretic choice principles.

AC (Axiom of Choice): *For any family $\{X_i : i \in I\}$ of non-empty sets there is a function which assigns, to each $i \in I$, a single element of X_i .*

BPIT (Boolean Prime Ideal Theorem): *Every boolean algebra has a prime ideal.*

AC_{fin} (Axiom of Finite Choice): *For any family $\{X_i : i \in I\}$ of non-empty finite sets there is a function which assigns, to each $i \in I$, a single element of X_i .*

AC_n (Axiom of Choice for n -element sets): *For any family $\{X_i : i \in I\}$ of n -element sets there is a function which assigns, to each $i \in I$, a single element of X_i .*

These statements have been studied in depth, and their relative strengths (in ZF) are known – see figure 1.1 below. We will also meet the following algebraic choice principles. Their deductive strengths are largely unexplored. Determining them is the subject of this dissertation.

NS (Nielsen–Schreier): *If F is any free group and $K \leq F$ is any subgroup, then K is a free group.*

NS_{norm} (Nielsen–Schreier for normal subgroups): *If F is any free group and $K \leq F$ is a normal subgroup, then K is a free group.*

NS_{red} (reduced Nielsen–Schreier): *If F is the free group on a set X and $K \leq F$ is any subgroup, then K has a basis that is reduced with respect to X . (For a definition of reduced bases, see section 5.6.)*

NS_{ab} (Nielsen–Schreier for abelian groups): *If F is a free abelian group and $K \leq F$ is a subgroup, then K is a free abelian group.*

CB₁ (Cardinality of bases, version 1): $F(X) \cong F(Y) \Rightarrow |X| = |Y|$ for any sets X and Y .

CB₂ (Cardinality of bases, version 2): $|F(X)| = |F(Y)| \Rightarrow |X| = |Y|$ for infinite sets X and Y .

Figure 1.1 summarises the main results of this thesis. Double-headed arrows represent

equivalences, and the remaining solid arrows stand for strict implications. Implications that may be equivalences appear as dashed arrows. The unlabelled arrows are taken from diagram 2.21 of Herrlich [14].

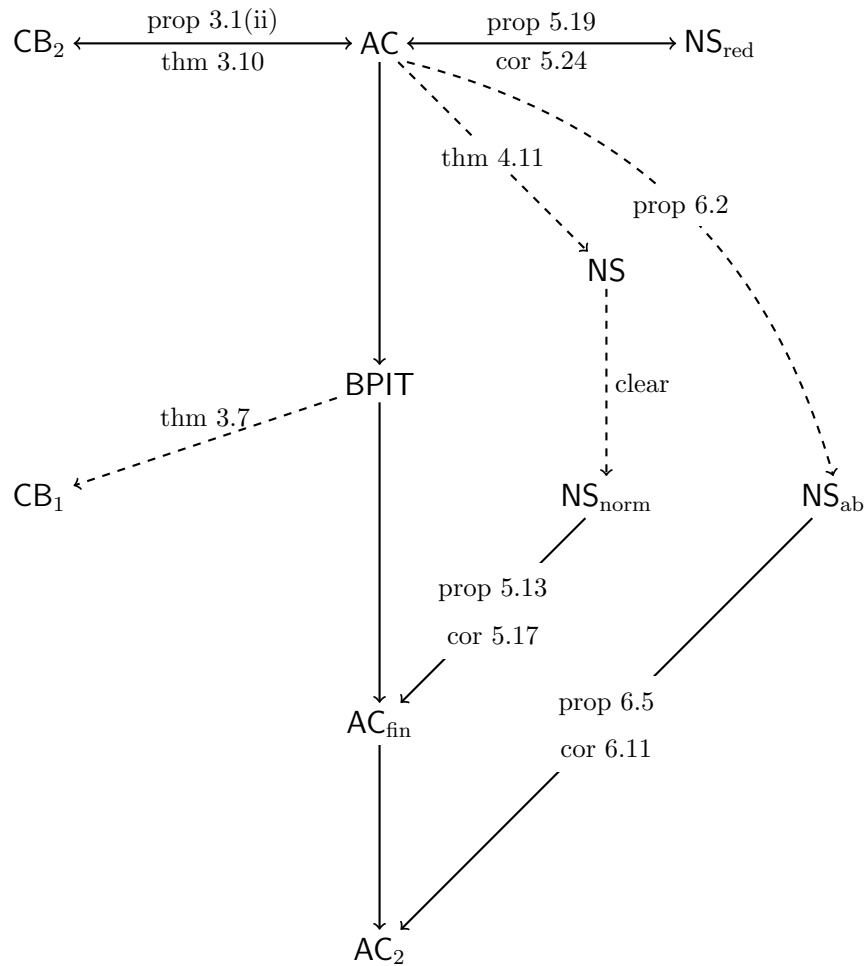


Figure 1.1: Implications between Choice principles

Chapter 2

Fraenkel–Mostowski models

We now turn to a procedure for proving independence results concerning the Axiom of Choice, which was developed by A. Fraenkel and A. Mostowski. The purpose of the method is to produce new models of set theory from old ones, and to control the behaviour of the new models by choosing suitable parameters. It later inspired P. Cohen’s proof ([3], [4]) of the independence of the Axiom of Choice from ZF by constructing a symmetric submodel of a generic extension of a given model of ZFC.

In section 2.1 we define Fraenkel–Mostowski models. After going through a sample application of Fraenkel–Mostowski models in section 2.2, two new models are introduced in section 2.3, and we explore some of their basic properties. Section 2.4 concludes the chapter by introducing a theorem which allows us to easily transfer statements from ZFA to ZF.

2.1 Setup

A Fraenkel–Mostowski model \mathfrak{M} is constructed as a substructure of a given model \mathfrak{N} of set theory. \mathfrak{M} consists of those sets in \mathfrak{N} that are sufficiently symmetric under a specified group of automorphisms of \mathfrak{N} . This automorphism group controls the properties of \mathfrak{M} . Since there are no non-trivial \in -automorphisms for ZF-models, the Fraenkel–Mostowski

method uses models of ZFA instead.

So let \mathfrak{N} be a model of ZFA + AC with universe V and set A of atoms. \in -automorphisms of V are obtained by letting π be any permutation of A , and extending π to all of V by setting

$$\pi(x) = \pi \ulcorner x$$

for any $x \in V$. We will always identify permutations of A with their canonical extensions to V . Let $\mathcal{G} \in \mathfrak{N}$ be any group of permutations of A , viewed as automorphisms of \mathfrak{N} .

Definition 2.1. If $x \in V$, then

$$\text{orb}(x) = \{\pi(x) : \pi \in \mathcal{G}\} \subseteq V$$

is the *orbit* of x ,

$$\text{stab}(x) = \{\pi \in \mathcal{G} : \pi(x) = x\} \leq \mathcal{G}$$

is the (*setwise*) *stabiliser* of x , and

$$\text{fix}(x) = \{\pi \in \mathcal{G} : (\forall y \in x)\pi(y) = y\} \leq \mathcal{G}$$

is the (*pointwise*) *stabiliser* of x .

It is easily verified that $\text{fix}(x) \leq \text{stab}(x)$ for any set x . But equality needn't hold, as there might be elements of \mathcal{G} which permute the members of x without moving x itself.

Before defining Fraenkel–Mostowski models, we need to introduce another parameter of the construction:

Definition 2.2. A set \mathcal{F} of subgroups of \mathcal{G} is a *normal filter* if

1. $\mathcal{G} \in \mathcal{F}$,
2. $(\forall H, K \leq \mathcal{G}) (H \in \mathcal{F} \wedge H \leq K \Rightarrow K \in \mathcal{F})$,
3. $(\forall H, K \in \mathcal{F}) H \cap K \in \mathcal{F}$,
4. $(\forall \pi \in \mathcal{G}) (\forall H \in \mathcal{F}) \pi H \pi^{-1} \in \mathcal{F}$,

5. $(\forall a \in A) \text{stab}(a) \in \mathcal{F}$.

Definition 2.3. Let $x \in V$. x is \mathcal{F} -*symmetric* if $\text{stab}(x) \in \mathcal{F}$, and it is *hereditarily \mathcal{F} -symmetric* if x is \mathcal{F} -symmetric and all members of the transitive closure of x are \mathcal{F} -symmetric. We will omit the reference to \mathcal{F} if it is clear from the context.

As normal filters are upward closed, members of a normal filter \mathcal{F} can be thought of as ‘large’ subgroups of \mathcal{G} . Hence the name *symmetric*: a set x is symmetric if it has a ‘large’ stabiliser, i.e. if it is left unchanged by ‘most’ permutations in \mathcal{G} .

Definition 2.4. Given a set A of atoms, a group \mathcal{G} of permutations of A , and a normal filter \mathcal{F} of subgroups of \mathcal{G} , define the substructure $\mathfrak{M} \leq \mathfrak{N}$ to consist of all hereditarily symmetric sets of V , with the \in -relation restricted from \mathfrak{N} . \mathfrak{M} is called the *Fraenkel–Mostowski model* with respect to A , \mathcal{G} , and \mathcal{F} .

The next theorem states that Fraenkel–Mostowski models are models of ZFA.

Theorem 2.5 (Jech [22], page 46). $\mathfrak{M} \models \text{ZFA}$.

We now introduce the notion of pure, or atomless, sets. As they don’t involve any atoms, we expect them to behave like ZF-sets. And indeed, the collection of all pure sets constitutes a model of ZF. Objects such as the ordinals or the real numbers, are implemented as pure sets in ZFA.

Definition 2.6. A set $x \in \mathfrak{N}$ is *pure* if it is not an atom and its transitive closure contains no atoms. The collection of all pure sets is the *kernel* of \mathfrak{N} .

Notice that, as pure sets don’t involve atoms that could be moved by members of \mathcal{G} , each pure set is fixed by *all* permutations of the atoms. Hence $\text{stab}(x) = \mathcal{G} \in \mathcal{F}$ for any pure set x and any normal filter \mathcal{F} . So the kernel of a Fraenkel–Mostowski model \mathfrak{M} is always the same as the kernel of its parent model \mathfrak{N} .

It may not be entirely clear how to produce a normal filter \mathcal{F} of subgroups of \mathcal{G} . The easiest way of doing this is to define a normal ideal \mathcal{I} of subsets of A and to take \mathcal{F} to be the filter induced by \mathcal{I} . This method is used for all models discussed in this thesis.

Definition 2.7. A set \mathcal{I} of subsets of A is a *normal ideal* if

1. $\emptyset \in \mathcal{I}$
2. $(\forall E, F \subseteq A) (E \in \mathcal{I} \wedge F \subseteq E \Rightarrow F \in \mathcal{I})$
3. $(\forall E, F \in \mathcal{I}) E \cup F \in \mathcal{I}$
4. $(\forall \pi \in \mathcal{G}) (\forall E \in \mathcal{I}) \pi^{\ast}E \in \mathcal{I}$
5. $(\forall a \in A) \{a\} \in \mathcal{I}$

Corresponding to the intuition that members of a normal filter \mathcal{F} are ‘large’, we may think of members of a normal ideal as ‘small’ sets of atoms.

Normal ideals of subsets of A are easy to find. The smallest possible normal ideal is $\mathcal{I} = \{E \subseteq A : E \text{ is finite}\}$, the *finite ideal*. This is the most common choice for Fraenkel–Mostowski models.

Definition 2.8. Every normal ideal \mathcal{I} of subsets of A *induces* a filter \mathcal{F} of subgroups of \mathcal{G} , defined by $\{H \leq \mathcal{G} : (\exists E \in \mathcal{I}) \text{fix}(E) \leq H\}$.

It is easy to check that \mathcal{F} is a normal filter. A description of the induced filter in terms of supports is useful:

Definition 2.9. If $E \subseteq A$ and $x \in \mathfrak{M}$, then E is a *support for x* if $\text{fix}(E) \leq \text{stab}(x)$.

In other words, E is a support for x if every permutation $\pi \in \mathcal{G}$ fixing all points of E satisfies $\pi(x) = x$. Supports capture information about the atoms in the transitive closure of x which are responsible for the asymmetry of x . For example, pure sets – which are fixed under all possible permutations of the atoms – have an empty support. It is important to note that supports, if they exist, are in general not unique.

Observe that

$$\begin{aligned} x \text{ is symmetric} &\Leftrightarrow \text{stab}(x) \in \mathcal{F} \\ &\Leftrightarrow (\exists E \in \mathcal{I}) \text{fix}(E) \leq \text{stab}(x) \\ &\Leftrightarrow x \text{ has a support in } \mathcal{I}. \end{aligned}$$

This means that a set $x \in \mathfrak{N}$ is in the Fraenkel–Mostowski model \mathfrak{M} if and only if x and all members of the transitive closure of x have supports in \mathcal{I} .

We are now ready to see an important Fraenkel–Mostowski model, and to prove a basic independence result. A large catalogue of Fraenkel–Mostowski models and their properties is in Howard and Rubin [19].

2.2 An example

In this section, we review an example from H. Läuchli’s influential paper [31]. It illustrates how the Fraenkel–Mostowski method is used to obtain independence results in set theory, and it foreshadows some proofs that we will encounter later in the text. First, we introduce the model \mathfrak{M} , called Fraenkel’s basic model. It is the simplest non-trivial Fraenkel–Mostowski model. The three parameters are

- (a) a countably infinite set A of atoms,
- (b) the full symmetry group $\mathcal{G} = \text{Sym}(A)$ of A , and
- (c) the normal filter \mathcal{F} of subgroups of \mathcal{G} induced by the finite ideal on A .

We now present H. Läuchli’s proof that there is a free group in \mathfrak{M} with a subgroup that is not free. In section 5.5 we give a more refined argument to show that the Nielsen–Schreier theorem fails in a Fraenkel–Mostowski model satisfying the Boolean Prime Ideal Theorem.

Theorem 2.10 (Läuchli [31]). $\mathfrak{M} \models \neg\text{NS}$.

Proof. Let $F = F(A)$ be the free group generated by A in \mathfrak{M} . We will show that the commutator subgroup

$$K = \langle \{\alpha\beta\alpha^{-1}\beta^{-1} : \alpha, \beta \in F\} \rangle \leq F$$

is not free. If it is, then there is a basis $B \in \mathfrak{M}$ with a (necessarily finite) support $E \subseteq A$. We will derive a contradiction.

Let $u, v \in A \setminus E$ be distinct, and let $\alpha = uvu^{-1}v^{-1} \in K$. If $\phi \in \mathcal{G}$ is the transposition (uv) , then $\phi(\alpha) = \phi(u)\phi(v)\phi(u)^{-1}\phi(v)^{-1} = vuv^{-1}u^{-1} = \alpha^{-1}$, and $\phi(B) = B$ because $u, v \notin E$. Writing $\alpha = b_1 \cdots b_n$ as a reduced product of elements of B^\pm , we deduce that $\phi(b_1) \cdots \phi(b_n) = b_n^{-1} \cdots b_1^{-1}$, i.e. that

$$\phi(b_n) = b_1^{-1}, \phi(b_{n-1}) = b_2^{-1}, \dots, \phi(b_1) = b_n^{-1}. \quad (2.1)$$

As no $b_i \in B^\pm$ is equal to its own inverse, $n = 2k$ must be even. This allows us to define $\beta = b_1 \cdots b_k$ as the ‘first half’ of α . Since β is a product of elements of B^\pm , $\beta \in K$. Write $\beta = a_1 \cdots a_m$ as a reduced A -word, with $a_1, \dots, a_m \in A^\pm$. Then

$$\begin{aligned} a_1 \cdots a_m \phi(a_m)^{-1} \cdots \phi(a_1)^{-1} &= \beta \phi(\beta)^{-1} \\ &= b_1 \cdots b_k \phi(b_k)^{-1} \cdots \phi(b_1)^{-1} \\ &= b_1 \cdots b_k b_{k+1} \cdots b_n && \text{(by (2.1))} \\ &= \alpha \\ &= uvu^{-1}v^{-1}. \end{aligned}$$

We conclude that

$$a_1 = u, a_2 = v, \phi(a_3) = a_3, \dots, \phi(a_m) = a_m.$$

As a_3, \dots, a_m are fixed by ϕ , none of them can be equal to u or v . Hence the sum of the exponents of the letter u in $\beta = a_1 \cdots a_m$ is 1, contradicting the choice of β as an element of the commutator subgroup of F . \square

Hence every proof of the Nielsen–Schreier theorem in ZFA must use a fragment of the Axiom of Choice. In section 2.4 we will see how this result can be transferred from ZFA to the standard set theory ZF.

The idea of splitting α and writing it as a product of its two halves is critical. It will be a recurring theme in chapter 5, even in sections that have nothing to do with Fraenkel–Mostowski models.

2.3 Two models

The Dawson–Howard model

The *Dawson–Howard* model is a close relative of the well studied cousin, Mostowski’s ordered model (see Jech [22], section 4.5). It was introduced by Dawson and Howard [6] and is called $\mathcal{N}29$ in Howard and Rubin [19]. The three parameters A , \mathcal{G} , and \mathcal{F} are defined as follows:

- (a) Let $\{\langle A_i, <_i \rangle : i < \omega\}$ be a collection of pairwise disjoint linearly ordered sets, each isomorphic to $\langle \mathbb{Q}, < \rangle$. The set of atoms is $A = \bigcup_{i < \omega} A_i$.
- (b) \mathcal{G} consists of all permutations π of A such that $\pi|_{A_i} \in \text{Aut}(\langle A_i, <_i \rangle)$ for all $i < \omega$.
- (c) \mathcal{F} is induced by the finite ideal.

Howard and Rubin [19] (p. 312 - 313) prove that

Theorem 2.11 (Howard and Rubin [19]). *BPIT is true in the Dawson–Howard model.*

We will see later that both NS and NS_{ab} fail in the Dawson–Howard model. Hence neither of these choice principles is deducible in ZFA from BPIT . In particular, NS and NS_{ab} are not theorems of ZFA . The transfer theorem described in section 2.4 will be used to obtain the same results for ZF .

Van Douwen's model

Van Douwen's model is the same as the Howard-Dawson model, except that the linear ordering of the A_i is discrete. It was introduced by van Douwen [40], and it is denoted by $\mathcal{N}2(LO)$ in Howard and Rubin [19]. The three parameters are defined by:

- (a) Let $\{\langle A_i, <_i \rangle : i < \omega\}$ be a collection of pairwise disjoint linearly ordered sets, each isomorphic to $\langle \mathbb{Z}, < \rangle$. The set of atoms is $A = \bigcup_{i < \omega} A_i$.
- (b) \mathcal{G} consists of all permutations π of A such that $\pi|_{A_i} \in \text{Aut}(\langle A_i, <_i \rangle)$ for all $i < \omega$.
- (c) \mathcal{F} is induced by the finite ideal.

We prove some elementary properties that will be useful later.

Lemma 2.12.

- (i) A can be linearly ordered in van Douwen's model.
- (ii) The family $\{A_i : i < \omega\}$ doesn't have a choice function.

Proof.

- (i) Define a linear order $<$ on A by

$$a < b \Leftrightarrow \begin{cases} a, b \in A_i \text{ and } a <_i b \text{ for some } i < \omega, \text{ or} \\ a \in A_i \text{ and } b \in A_j \text{ for some } i < j < \omega \end{cases}$$

All elements of \mathcal{G} preserve $<$, so it has empty support.

- (ii) As every $\pi \in \mathcal{G}$ fixes each A_i setwise, all of the A_i are sets in the model, with empty support. Hence $\{A_i : i < \omega\}$ is a set of the model, also with empty support.

Now suppose $C \subseteq A$ intersects each A_i in a single point and has a finite support $E \subseteq A$. Let $i < \omega$ be such that $A_i \cap E = \emptyset$, and let $\pi \in \text{fix}(E)$ act non-trivially

on A_i . Since $\pi \in \text{fix}(E)$, it maps C to itself. If we let a be the single member of $C \cap A_i$, then we have

$$\begin{aligned}\pi(C) = C &\Rightarrow \pi(a) \in C \\ &\Rightarrow \pi(a) = a,\end{aligned}$$

because π maps A_i to itself. Hence $a \in A_i$ is fixed by π , contrary to the assumption that π acts non-trivially on A_i . Thus E isn't a support for C , so C isn't a set of the model.

□

2.4 A transfer theorem

When proving properties of Fraenkel–Mostowski models, we obtain consistency and independence results for the set theory ZFA. However, as ZF (with or without AC) is the most wide spread set theory, it would be desirable to prove such results for ZF. This motivates us to seek a class of statements that can be transferred from Fraenkel–Mostowski models to ZF-models.

Definition 2.13 (Pincus [35]). A sentence Φ of set theory is *transferable* if there is a metatheorem: *If Φ is true in a Fraenkel–Mostowski model, then Φ is consistent with ZF*

Not every sentence is transferable. For instance, the statement ‘there are at least two empty objects’ is true in some Fraenkel–Mostowski models, whereas it fails in all ZF-models.

A more subtle example is the Antichain Principle AP – *every poset has a maximal antichain*. Halpern [12] constructed a Fraenkel–Mostowski model satisfying $\text{AP} \wedge \neg\text{AC}$, showing that the Axiom of Choice is not equivalent to the Antichain Principle in ZFA. However, AP is equivalent to the Axiom of Choice in ZF (see Herrlich [14], p. 11). More examples of non-transferable statements can be found in Howard’s publication [15].

Despite these obstructions, large classes of transferable statements have been found by Jech and Sochor [24] and Pincus [35]. Theorem 2.17 at the end of this section lists some of them.

Standard proofs of the independence of the Axiom of Choice from ZF – for example, the proof given in Jech’s book [22] – extract a symmetric submodel from a generic extension of a ZFC-model. The process is similar to constructing Fraenkel–Mostowski models, which are symmetric submodels of a ZFA-model. This is more than a superficial resemblance. Indeed, the approach taken by Jech and Sochor [24] embeds Fraenkel–Mostowski models in symmetric submodels of generic extensions of ZFC-models.

It was observed that sets of sets of ordinals in a ZF-model have so little internal structure that they can be used to approximate ZFA-atoms. Using this embedding technique, many independence results in ZFA can be transferred directly to ZF, as was done by Jech and Sochor [23] and Pincus [35].

Definition 2.14 (Pincus [35], simplified). Let $\mathbf{x} = \langle x_1, \dots, x_n \rangle$ be a tuple of variables. A formula $\phi(\mathbf{x})$ is *boundable* if, for some absolutely definable ordinal α ,

$$\text{ZFA} \vdash \phi(\mathbf{x}) \Leftrightarrow \phi^{V_\alpha(\mathbf{U}^{\mathbf{x}})}(\mathbf{x}),$$

where $\bigcup \mathbf{x}$ stands for $x_1 \cup \dots \cup x_n$. A sentence Φ is *boundable* if it is the existential closure of a boundable formula.

Example 2.15. $\langle F, \mathbf{1}, * \rangle$ is a free group on X can be written as

$$\phi(F, \mathbf{1}, *, X) = (\exists f) (f : F \rightarrow F(X) \text{ is an isomorphism}).$$

We have $F(X) \in V_{\omega+1}(X)$. In order to determine whether or not there is an isomorphism $F \rightarrow F(X)$, it suffices to check, for each member of $\mathcal{P}^3(F \cup F(X))$, if it is a bijection and preserves the group operation $*$. Hence

$$\text{ZFA} \vdash \phi(F, \mathbf{1}, *, X) \Leftrightarrow \phi^{V_{\omega+4}(F \cup \mathbf{1} \cup * \cup X)}(F, \mathbf{1}, *, X),$$

and ϕ is a boundable formula. Similarly, $\langle F, \mathbf{1}, * \rangle$ is a free group, written as

$$\psi(F, \mathbf{1}, *) = (\exists X \in \mathcal{P}(F)) \phi(F, \mathbf{1}, *, X)$$

is bounded by $V_{\omega+4}(F \cup \mathbf{1} \cup *)$.

Example 2.16. $\neg\text{NS}$ may be written as $(\exists\langle F, \mathbf{1}, * \rangle)(\exists X)(\exists K)\chi(F, \mathbf{1}, *, X, K)$, where

$$\begin{aligned} \chi(F, \mathbf{1}, *, X, K) = & (X \in \mathcal{P}(F) \wedge \langle F, \mathbf{1}, * \rangle \text{ is a free group on } X) \\ & \wedge (\langle K, \mathbf{1}, *|_K \rangle \text{ is a subgroup of } \langle F, \mathbf{1}, * \rangle) \\ & \wedge (\langle K, \mathbf{1}, *|_K \rangle \text{ is not a free group}) \end{aligned}$$

We saw in example 2.15 that $X \in \mathcal{P}(F) \wedge \langle F, \mathbf{1}, * \rangle$ is a free group on X is bounded by $V_{\omega+4}(F \cup \mathbf{1} \cup * \cup X)$. Similarly, $\langle K, \mathbf{1}, *|_K \rangle$ is a subgroup of $\langle F, \mathbf{1}, * \rangle$ is bounded by $V_1(K \cup F \cup \mathbf{1} \cup *)$, and $\langle K, \mathbf{1}, *|_K \rangle$ is not a free group is bounded by $V_{\omega+4}(K, \mathbf{1}, *|_K)$. Hence $\neg\text{NS}$ is bounded by $V_{\omega+4}(F \cup \mathbf{1} \cup * \cup X \cup K)$.

Usually, the negation of a Choice Principle is boundable, because its failure is witnessed by some set. For example, in order to show that AC fails, it suffices to find one family of non-empty sets with no choice function, and to show that NS fails, we only need one free group with a non-free subgroup. On the other hand, it is easy to see that choice principles such as NS or AC are not boundable, as they make a statement about *all* sets of a certain type, regardless of their size. In other words, they cannot be verified by looking at an initial segment $V_\alpha(A)$ of the universe.

Pincus [36] gave a list of transferable statements, among which are all boundable sentences. The introduction of Pincus' article [37] states that – among other choice principles – BPIT can be added to this list. The following version of the theorem suffices for our purposes.

Theorem 2.17 (Transfer Theorem, Pincus [36], Pincus [37]). *If Φ is a conjunction of any of the following types of sentences*

1. *boundable sentences,*
2. $\text{BPIT},$

then Φ is transferable.

Chapter 3

The size of bases

The concept of the dimension of a vector space is based on the fact that any two bases of a vector space have the same cardinality in ZFC. However, Halpern [11] showed that this fact is not equivalent to the Axiom of Choice by deducing it from the Boolean Prime Ideal Theorem. Howard [16] asked whether the same is true for free groups. We will show that the answer is *yes*. In this section we shall investigate the following two choice principles.

CB₁ (Cardinality of bases, version 1): $F(X) \cong F(Y) \Rightarrow |X| = |Y|$ for any sets X and Y .

CB₂ (Cardinality of bases, version 2): $|F(X)| = |F(Y)| \Rightarrow |X| = |Y|$ for infinite sets X and Y .

Proposition 3.1.

(i) $ZFC \vdash CB_1$.

(ii) $ZFC \vdash CB_2$.

Proof.

(i) A proof can be found on page 3 of Johnson's book [25].

(ii) By the Axiom of Choice $|F(X)| = |X|$ for any infinite set X . The result follows immediately.

□

We will show that the CB_1 is not equivalent to the Axiom of Choice, whereas CB_2 is equivalent to the Axiom of Choice. The results in sections 3.1 and 3.2 have been published by Kleppmann [27].

First, let us see what is true in the absence of the Axiom of Choice.

Proposition 3.2. *Let F_1, F_2 be free groups. Then $F_1 \cong F_2$ if and only if there is a basis X_1 of F_1 and a basis X_2 of F_2 with $|X_1| = |X_2|$.*

Proof.

⊃ Let $\phi : F_1 \rightarrow F_2$ be an isomorphism, and let X_1 be any basis of F_1 . Then $\phi(X_1) \subseteq F_2$ is a basis of F_2 which has the same size as X_1 .

⊃ Let $f : X_1 \rightarrow X_2$ be a bijection. This can be viewed as an injection $X_1 \hookrightarrow F_2$, so it has a unique extension to a homomorphism $\phi : F_1 \rightarrow F_2$ by the universal property of free groups. It is easily verified that ϕ is an isomorphism.

□

3.1 Bases of isomorphic free groups

We show here that CB_1 is not equivalent to the Axiom of Choice. This will be done by deducing CB_1 from the Boolean Prime Ideal Theorem. In order to prove our result, we need to state two well known theorems. The first one is a direct consequence of the Structure Theorem for finitely generated modules over a principal ideal domain.

Theorem 3.3 (Cohn [5], page 316). *If M is a finitely generated module of rank m over a principal ideal domain R , and $N \leq M$ is an R -submodule of M , then N is finitely generated of rank $n \leq m$.*

We only need a special case of this theorem. As every abelian group can be naturally viewed as a \mathbb{Z} -module, and \mathbb{Z} is a principal ideal domain, we have:

Theorem 3.4. *If F is a free abelian group of finite rank m , and $K \leq F$ is a subgroup, then K has rank $\leq m$.*

The second theorem is an infinite version of P. Hall's Marriage Theorem [10]:

Theorem 3.5 (M. Hall [9], page 45). *Let $F = \{S_i : i \in I\}$ be a family of non-empty finite sets. The following are equivalent:*

1. *There is an injection $c : I \rightarrow \bigcup F$ satisfying $(\forall i \in I) c(i) \in S_i$.*
2. *$|\bigcup_{j=1}^k S_{i_j}| \geq k$ for any choice i_1, \dots, i_k of finitely many indices in I .*

Halpern [11] showed that Theorem 3.5 is a consequence of BPIT in ZF set theory.

Definition 3.6. Let X be a set, $F = \text{FA}(X)$, and $\alpha \in F$. Write α as $n_1x_1 + \dots + n_kx_k$, where $x_1, \dots, x_k \in X$ are distinct and n_1, \dots, n_k are non-zero integers. The set of X -components of α is $\mathcal{C}_X(\alpha) = \{x_1, \dots, x_k\}$.

Theorem 3.7. $\text{ZF} \vdash \text{BPIT} \Rightarrow \text{CB}_1$.

Proof. Let

$$F(X) \cong F(Y) \tag{3.1}$$

be isomorphic free groups. We want to show that $|X| = |Y|$. Abelianising both sides of (3.1), we obtain

$$\text{FA}(X) \cong \text{FA}(Y).$$

Without loss of generality we reduce to the notationally simpler case of one free abelian group F with two bases X and Y . So each $y \in Y$ may be written uniquely as

$$y = n_1x_1 + \dots + n_kx_k, \quad (3.2)$$

where $x_1, \dots, x_k \in X$ are distinct and n_1, \dots, n_k are non-zero integers.

Claim. The union of any k of the $\mathcal{C}_X(y)$ has size $\geq k$.

Let $y_1, \dots, y_k \in Y$ be distinct, and let K be the subgroup of F generated by $\{y_1, \dots, y_k\}$. Note that the rank of K is k because $\{y_1, \dots, y_k\} \subseteq Y$ is free.

Let $\mathcal{C} = \bigcup_{i=1}^k \mathcal{C}_X(y_i) \subseteq X$, and let H be the subgroup of F generated by \mathcal{C} . As above, the rank of H is $|\mathcal{C}|$ because $\mathcal{C} \subseteq X$ is free. By definition, $K \leq H$, so $k \leq |\mathcal{C}|$ using theorem 3.4.

Applying theorem 3.5, we conclude that there is an injection $c : Y \rightarrow \bigcup\{\mathcal{C}_X(y) : y \in Y\}$ satisfying $(\forall y \in Y) c(y) \in \mathcal{C}_X(y)$. As each $\mathcal{C}_X(y)$ is a subset of X , this is an injection $Y \rightarrow X$.

An injection $X \rightarrow Y$ is obtained by swapping X s and Y s in the proof. By the Schröder-Bernstein theorem, $|X| = |Y|$. □

Howard [18] asked the following question:

Question. *Is CB_1 provable without any form of the Axiom of Choice?*

The answer is unknown. However, a construction by Läuchli [31] may be relevant here. He defines a Fraenkel–Mostowski model with a vector space that has two bases of different cardinalities. If a similar construction for free abelian groups can be made to work, then the transfer theorem would imply that the answer to this question is *no*.

3.2 Bases of equipollent free groups

In this section we will show that CB_2 is equivalent to the Axiom of Choice. We have already seen that CB_2 follows from AC.

In order to prove $\text{ZF} \vdash \text{CB}_2 \Rightarrow \text{AC}$, we will need two lemmas. The first one identifies a condition for cardinals to be well-ordered, and the second is an estimate of the cardinality of $F(X)$ in terms of the cardinality of X .

Lemma 3.8 (Jech [22], page 157). *If \mathfrak{p} is an infinite cardinal and \aleph is an aleph, and if $\mathfrak{p} + \aleph = \mathfrak{p} \cdot \aleph$, then either $\mathfrak{p} \geq \aleph$ or $\mathfrak{p} \leq \aleph$. In particular, if $\mathfrak{p} + \aleph(\mathfrak{p}) = \mathfrak{p} \cdot \aleph(\mathfrak{p})$, then \mathfrak{p} is an aleph.*

Lemma 3.9. *Let X be any set. Then*

$$\sum_{n < \omega} |X|^n \leq |F(X)| \leq \sum_{n < \omega} (2|X|)^n.$$

Proof. Define two injections as follows:

$$\begin{aligned} \bigcup_{n < \omega} X^n &\hookrightarrow F(X) : \langle x_1, \dots, x_n \rangle \mapsto x_1 \cdots x_n \\ F(X) &\hookrightarrow \bigcup_{n < \omega} (X^\pm)^n : x_1^{\epsilon_1} \cdots x_n^{\epsilon_n} \mapsto \langle x_1^{\epsilon_1}, \dots, x_n^{\epsilon_n} \rangle, \end{aligned}$$

□

Theorem 3.10. $\text{ZF} \vdash \text{CB}_2 \Rightarrow \text{AC}$.

Proof. To simplify notation, we write $F(\mathfrak{c})$ for $|F(X)|$ when X is a set with $|X| = \mathfrak{c}$.

Let \mathfrak{p} be any infinite cardinal. We will show that \mathfrak{p} is an aleph. Since $\mathfrak{p} \leq \mathfrak{p}^{\aleph_0}$, it suffices to prove that $\mathfrak{q} = \mathfrak{p}^{\aleph_0}$ is an aleph. This will be done by showing that $\mathfrak{q} + \aleph(\mathfrak{q}) = \mathfrak{q} \cdot \aleph(\mathfrak{q})$ and applying lemma 3.8. Since we are assuming CB_2 , it suffices to show that $F(\mathfrak{q} + \aleph(\mathfrak{q})) = F(\mathfrak{q} \cdot \aleph(\mathfrak{q}))$.

Claim. $F(\mathfrak{q} \cdot \aleph(\mathfrak{q})) = \mathfrak{q} \cdot \aleph(\mathfrak{q}) = F(\mathfrak{q} + \aleph(\mathfrak{q}))$.

For the following calculations, we first note that, for any cardinals a and b satisfying $0 < a \leq \aleph_0$ and $0 < b < \aleph_0$,

$$\begin{aligned}
 (a\mathfrak{q}\aleph(\mathfrak{q}))^b &= \mathfrak{q}^b \cdot (a \cdot \aleph(\mathfrak{q}))^b \\
 &= \mathfrak{q} \cdot \aleph(\mathfrak{q})^b \\
 &= \mathfrak{q}\aleph(\mathfrak{q}),
 \end{aligned} \tag{3.3}$$

The first equality of the claim follows from:

$$\begin{aligned}
 \mathfrak{q}\aleph(\mathfrak{q}) &\leq F(\mathfrak{q}\aleph(\mathfrak{q})) \\
 &\leq \sum_{n < \omega} (2\mathfrak{q}\aleph(\mathfrak{q}))^n && \text{(by lemma 3.9)} \\
 &= \sum_{n < \omega} \mathfrak{q}\aleph(\mathfrak{q}) && \text{(by (3.3))} \\
 &\leq \aleph_0 \cdot \mathfrak{q}\aleph(\mathfrak{q}) \\
 &= \mathfrak{q}\aleph(\mathfrak{q})
 \end{aligned}$$

For the second equality of the claim, we have:

$$\begin{aligned}
 F(\mathfrak{q} + \aleph(\mathfrak{q})) &\geq \sum_{n < \omega} (\mathfrak{q} + \aleph(\mathfrak{q}))^n && \text{(by lemma 3.9)} \\
 &\geq (\mathfrak{q} + \aleph(\mathfrak{q}))^2 \\
 &= \mathfrak{q}^2 + 2\mathfrak{q}\aleph(\mathfrak{q}) + \aleph(\mathfrak{q})^2 \\
 &\geq \mathfrak{q}\aleph(\mathfrak{q})
 \end{aligned}$$

and:

$$\begin{aligned}
F(\mathfrak{q} + \aleph(\mathfrak{q})) &\leq \sum_{n < \omega} (2(\mathfrak{q} + \aleph(\mathfrak{q})))^n && \text{(by lemma 3.9)} \\
&= \sum_{n < \omega} 2^n \sum_{k \leq n} \binom{n}{k} \mathfrak{q}^k \aleph(\mathfrak{q})^{n-k} \\
&= \sum_{n < \omega} \sum_{k \leq n} 2^n \binom{n}{k} \mathfrak{q}^k \aleph(\mathfrak{q}) \\
&= \sum_{n < \omega} \mathfrak{q}^n \aleph(\mathfrak{q}) \\
&\leq \aleph_0 \cdot \mathfrak{q}^{\aleph(\mathfrak{q})} \\
&= \mathfrak{q}^{\aleph(\mathfrak{q})}
\end{aligned}$$

□

We conclude that:

Corollary 3.11. $\text{ZF} \vdash \text{CB}_2 \Leftrightarrow \text{AC}$.

Chapter 4

Nielsen–Schreier

In this chapter, we will prove the Nielsen–Schreier theorem. To the best of the author’s knowledge, this proof doesn’t appear in the literature, although many of its parts are inspired by various published proofs. The approach taken here uses spanning trees of Schreier graphs, as in chapter VIII of Bollobás’ book [2]. The advantage of the given proof is that the use of graphs make it intuitive and easy to picture, while demanding a minimal amount of prerequisite knowledge.

Schreier graphs are defined in section 4.1, and some examples are given. This prepares the reader for the proof of the Nielsen–Schreier theorem in section 4.2. Later, in section 4.3, we find easily verified classification criteria for Schreier graphs. These will be useful when analysing the use of the Axiom of Choice in proofs of the Nielsen–Schreier theorem.

4.1 Schreier graphs

Schreier graphs are graphs that hold information about a free group F , a subgroup $K \leq F$, and the relation between them.

Definition 4.1. A *directed graph* (or *digraph* for short) is a pair $G = \langle V, E \rangle$ consisting of a set V of *vertices*, a set E of *edges*, together with three functions $\alpha : E \rightarrow V$,

$\omega : E \rightarrow V$, and $\eta : E \rightarrow E$ satisfying

1. $(\forall e \in E) (\eta(e) \neq e \wedge \eta^2(e) = e)$,
2. $(\forall e \in E) (\alpha(\eta(e)) = \omega(e) \wedge \omega(\eta(e)) = \alpha(e))$.

$\alpha(e)$ is the *initial vertex* of e , $\omega(e)$ is the *terminal vertex* of e , and $\eta(e)$ is the *inverse* of e . We also write e^{-1} for $\eta(e)$.

Notice that the initial and terminal vertices of an edge may be the same (such edges are called *loops*), and that there may be more than one edge between any pair of vertices.

Definition 4.2. Let $F = F(X)$ be a free group, and let K be a subgroup. The *Schreier graph* of $K \leq F$ is a digraph $G = \langle V, E \rangle$ with edges labelled by elements of X^\pm . The vertices of G are the right cosets of K in F :

$$V = \{K\xi : \xi \in F\}.$$

Given any two vertices $K\xi, K\zeta$ and any letter $x \in X^\pm$, there is an edge labelled x from $K\xi$ to $K\zeta$ if and only if $K\xi x = K\zeta$.

Every edge $e \in E$ with label $x \in X^\pm$ is accompanied by its inverse edge e^{-1} , which has label x^{-1} . When displaying Schreier graphs, we shall avoid unnecessary visual clutter by only showing edges with label in X .

Definition 4.3. A digraph is a *Schreier graph* if it is the Schreier graph of a subgroup of a free group.

Example 4.4. Let $F = F(\{a, b\})$ be the free group on two generators, and let C be its commutator subgroup. The Schreier graph of $C \leq F$ is shown in figure 4.1.

We now introduce some vocabulary for talking about directed graphs.

Definition 4.5. Let $G = \langle V, E \rangle$ be a digraph.

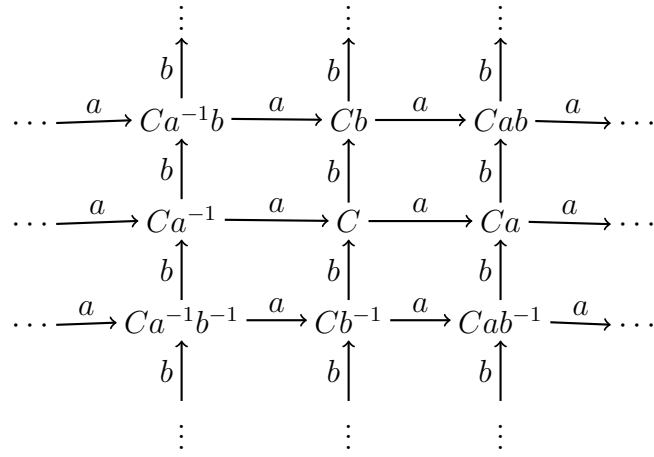


Figure 4.1: The Schreier graph of the commutator subgroup C of $F(\{a, b\})$

A *path* is a finite sequence $p = e_1 \cdots e_n$ of edges such that $\alpha(e_{i+1}) = \omega(e_i)$ for $i = 1, \dots, n-1$.

The path p *begins* at $\alpha(p) = \alpha(e_1)$ and *ends* at $\omega(p) = \omega(e_n)$.

If $p = e_1 \cdots e_n$ and $p' = e'_1 \cdots e'_m$ are paths with $\omega(p) = \alpha(p')$, then their *composition* is $pp' = e_1 \cdots e_n e'_1 \cdots e'_m$.

p is a *cycle* if $\alpha(p) = \omega(p)$.

p is *reduced* if $e_{i+1} \neq e_i^{-1}$ for $i = 1, \dots, n-1$, i.e. if there is no back-tracking.

The *inverse* of p is $p^{-1} = e_n^{-1} \cdots e_1^{-1}$.

For later reference, we also need the following definitions:

Definition 4.6. A digraph $G = \langle V, E \rangle$ is *connected* if, for any $v, w \in V$, there is a path in G beginning at v and ending at w .

Definition 4.7. Let $G = \langle V, E \rangle$ be a digraph. $T = \langle V_T, E_T \rangle$ is a *spanning tree* of G if $V_T = V$, $E_T \subseteq E$, $(\forall e \in E_T) e^{-1} \in E_T$, and any two vertices can be joined by a unique reduced path in T .

For any vertex $K\xi$ and any $x \in X^\pm$, there is one edge labelled x terminating at $K\xi$

(the edge coming from $K\xi x^{-1}$) and there is one edge labelled x starting at $K\xi$ (the edge going to $K\xi x$).

Using this observation, there is a natural interpretation of words $x_1 \cdots x_n$ with $x_i \in X^\pm$ as paths in the Schreier graph starting at the vertex K : For $i = 1, \dots, n$, let e_i be the edge labelled x_i starting at $Kx_1 \cdots x_{i-1}$ and ending at $Kx_1 \cdots x_i$. Then the path $e_1 \cdots e_n$ starts at K , ends at $Kx_1 \cdots x_n$, and the label of e_i is x_i for each i . To simplify notation, we will often associate words $x_1 \cdots x_n$ ($x_i \in X^\pm$) with their corresponding paths in the Schreier graph.

Definition 4.8. Let $G = \langle V, E \rangle$ be a digraph, and let $v \in V$ be a vertex. The set of cycles in G based at v can be regarded as a group where the group operation is concatenation.

We now prove a proposition which allows us translate algebraic statements about subgroups of free groups to easily visualised statements concerning cycles in graphs.

Proposition 4.9. *Let K be a subgroup of a free group F , and let G be the Schreier graph of $K \leq F$.*

- (i) *The group of cycles in G based at K (the vertex) is isomorphic to K (the group).*
- (ii) *G is connected.*

Proof.

- (i) Let $x_1 \cdots x_n$ be a word in F , with $x_i \in X^\pm$ for all i . Then

$$\begin{aligned} x_1 \cdots x_n \in K &\Leftrightarrow Kx_1 \cdots x_n = K \\ &\Leftrightarrow \text{the path } x_1 \cdots x_n \text{ starting at } K \text{ is a cycle.} \end{aligned}$$

Since composition of paths in the Schreier graph corresponds to composition of words in the free group, $K \leq F$ is isomorphic to the group of cycles based at K .

- (ii) The observation before this proposition shows how to construct a path from K to $Kx_1 \cdots x_n$ for any $x_1 \cdots x_n \in F$. So if $K\xi$ and $K\zeta$ are two cosets, let p_1 be a path from K to $K\xi$, and let p_2 be a path from K to $K\zeta$. Then $p_1^{-1}p_2$ is a path from $K\xi$ to $K\zeta$.

□

Example 4.10. Recall from example 4.4 the Schreier graph of the commutator subgroup of $F(\{a, b\})$. It is clear from figure 4.1 that any finite set of cycles based at C only covers a bounded area of the Schreier graph. It follows immediately that the commutator subgroup, unlike the surrounding free group $F(\{a, b\})$, has no finite generating set.

4.2 A proof of the Nielsen–Schreier theorem

The crucial property of Schreier graphs is part (i) of proposition 4.9. Using this representation, we only need to find a particular set B of cycles such that every cycle can be written uniquely as a product of members of B . Then B is a basis for the subgroup K , showing that K is free. A spanning tree of the Schreier graph allows us to find B .

Theorem 4.11 (Nielsen–Schreier). *If F is a free group and K is a subgroup of F , then K is a free group.*

Proof. Let X be a set, let $F = F(X)$ be the free group on X , and let $K \leq F$ be a subgroup.

Using the Axiom of Choice, we find a spanning tree $T = \langle V_T, E_T \rangle$ of the Schreier graph $G = \langle V_G, E_G \rangle$ of $K \leq F$.

Let $e \in E_G$ be any edge. Since T is a spanning tree of G , there is a unique reduced path $\bar{\alpha}(e)$ in T from K to $\alpha(e)$. Similarly, there is a unique reduced path $\bar{\omega}(e)$ in T from K to $\omega(e)$. We combine the two paths with the chosen edge to form a cycle in the Schreier graph. This is done using the function λ defined by

$$\lambda : E_G \rightarrow K : e \mapsto \bar{\alpha}(e) \cdot e \cdot \bar{\omega}(e)^{-1}$$

Note that

$$\begin{aligned} \lambda(e)^{-1} &= \bar{\omega}(e)e^{-1}\bar{\alpha}(e)^{-1} \\ &= \bar{\alpha}(e^{-1})e^{-1}\bar{\omega}(e^{-1})^{-1} \\ &= \lambda(e^{-1}) \end{aligned} \tag{4.1}$$

For the second equality, we used the identities $\omega(e) = \alpha(e^{-1})$ and $\alpha(e) = \omega(e^{-1})$, as well as the uniqueness of reduced paths in T .

From figure 4.2 we see that $\lambda(e)$ is an X -reduced word when $e \in E_G \setminus E_T$, and $\lambda(e) = \mathbf{1}$ when $e \in E_T$. Now define

$$B = \{\lambda(e) : e \in E_G \setminus E_T \text{ and } e\text{'s label is not in } X^-\}.$$

We will show that B is a basis for K , implying that K is a free group. There are three steps.

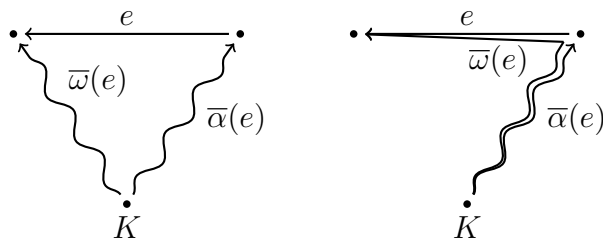


Figure 4.2: The left diagram shows $\lambda(e)$ in the case $e \in E_G \setminus E_T$, and the right diagram shows $\lambda(e)$ when $e \in E_T$.

1. $B \subseteq K$:

All of the $\lambda(e)$ correspond to cycles in the Schreier graph, so they are elements of K by proposition 4.9(i).

2. $\langle B \rangle = K$:

Choose any $\xi \in K$, and write it as a reduced X -word $\xi = x_1^{\epsilon_1} \cdots x_n^{\epsilon_n}$, where $x_i \in X$ and $\epsilon_i \in \{1, -1\}$ for $i = 1, \dots, n$. ξ corresponds to a cycle $e_1^{\epsilon_1} \cdots e_n^{\epsilon_n}$ based at K in the Schreier graph, where the label of each edge e_i is x_i .

$$\begin{aligned} \lambda(e_1)^{\epsilon_1} \cdots \lambda(e_n)^{\epsilon_n} &= \lambda(e_1^{\epsilon_1}) \cdots \lambda(e_n^{\epsilon_n}) && \text{(by (4.1))} \\ &= \bar{\alpha}(e_1^{\epsilon_1}) e_1^{\epsilon_1} \bar{\omega}(e_1^{\epsilon_1})^{-1} \bar{\alpha}(e_2^{\epsilon_2}) \cdots \bar{\omega}(e_{n-1}^{\epsilon_{n-1}})^{-1} \bar{\alpha}(e_n^{\epsilon_n}) e_n^{\epsilon_n} \bar{\omega}(e_n^{\epsilon_n})^{-1} \end{aligned}$$

The path condition $\omega(e_i^{\epsilon_i}) = \alpha(e_{i+1}^{\epsilon_{i+1}})$ and the uniqueness of reduced paths in T imply that $\bar{\omega}(e_i^{\epsilon_i}) = \bar{\alpha}(e_{i+1}^{\epsilon_{i+1}})$. Moreover, $\bar{\alpha}(e_1^{\epsilon_1}) = \mathbf{1} = \bar{\omega}(e_n^{\epsilon_n})$, because $\alpha(e_1^{\epsilon_1}) = K = \omega(e_n^{\epsilon_n})$. So

$$\begin{aligned} &= \mathbf{1} e_1^{\epsilon_1} \mathbf{1} e_2^{\epsilon_2} \mathbf{1} \cdots \mathbf{1} e_n^{\epsilon_n} \mathbf{1} \\ &= \xi, \end{aligned}$$

showing that $\xi \in \langle B \rangle$. See figure 4.3 for an illustration.

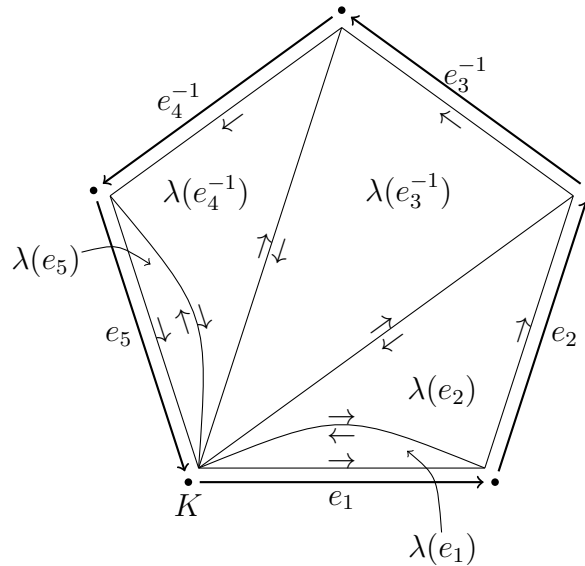


Figure 4.3: $e_1 e_2 e_3^{-1} e_4^{-1} e_5 = \lambda(e_1) \lambda(e_2) \lambda(e_3^{-1}) \lambda(e_4^{-1}) \lambda(e_5)$.

3. B is free:

Each $\lambda(e) \in B$ contains one edge, e , of the Schreier graph which doesn't occur in any other element of B . Hence, if $\xi = \lambda(e_1)^{\epsilon_1} \cdots \lambda(e_n)^{\epsilon_n}$, where $n > 0$, $\lambda(e_i) \in B$, and $\epsilon_i \in \{1, -1\}$ for $i = 1, \dots, n$, is B -reduced, then

$$\ell_X(\xi) \geq \ell_B(\xi) = n > 0. \quad (4.2)$$

In particular, $\xi \neq \mathbf{1}$.

□

The only place in this proof where the Axiom of Choice was used is the assertion of the existence of a spanning tree in the Schreier graph. As the next example shows, the geometrically intuitive and constructive nature of this proof lets us find explicit bases of some subgroups of free groups.

Example 4.12. We construct a basis for the commutator subgroup of the free group $F(\{a, b\})$ on two letters by exhibiting a spanning tree of the Schreier graph found in example 4.4.

Identify right cosets $C\xi$ with points of the grid $\mathbb{Z} \times \mathbb{Z}$. Then

$$T = \{ \langle \langle m, n \rangle, \langle m + 1, n \rangle \rangle : m, n \in \mathbb{Z} \} \cup \{ \langle \langle 0, n \rangle, \langle 0, n + 1 \rangle \rangle : n \in \mathbb{Z} \}$$

is a spanning tree. It is highlighted in figure 4.4. Using the proof of theorem 4.11, we deduce that

$$\{ b^n a^m b a^{-m} b^{-(n+1)} : m, n \in \mathbb{Z}, m \neq 0 \}$$

is a basis for C .

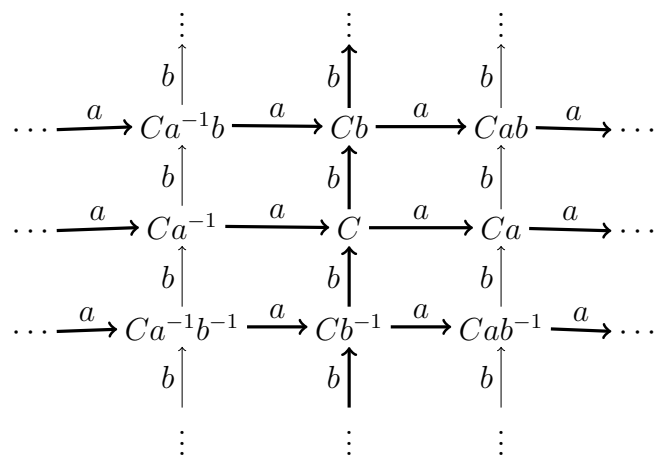


Figure 4.4: The Schreier graph of the commutator subgroup C of $F(\{a, b\})$

4.3 Classifying Schreier graphs

In this section, we show that a digraph is the Schreier graph of a subgroup of a free group if and only if it is connected and satisfies a regularity condition. Later, we show that the subgroup is normal if and only if the corresponding Schreier graph also satisfies a homogeneity condition. These classification results will allow us to determine how much of the Axiom of Choice is used when asserting the existence of spanning trees in Schreier graphs.

Recall from section 4.1 the following observation about Schreier graphs: For any vertex $K\xi$ and any $x \in X^\pm$, there is one edge labelled x terminating at $K\xi$, and there is one edge labelled x starting at $K\xi$. This property deserves a name:

Definition 4.13. If $G = \langle V, E \rangle$ is a digraph with edges labelled by elements of a set X^\pm , then G is *X-regular* if, for every $x \in X^\pm$ and $v \in V$, there is one edge labelled x starting at v and there is one edge labelled x ending at v . G is *regular* if it is *X-regular* for some X .

Before classifying Schreier graphs, we introduce a useful piece of notation.

Definition 4.14. Let $F = F(X)$ be a free group, let $K \leq F$ be a subgroup, and let G be the Schreier graph of $K \leq F$. The expression $K\xi \xrightarrow{x} K\zeta$ means *there is an edge in G which starts at $K\xi$, ends at $K\zeta$, and has label x .*

Proposition 4.15. *Let $G = \langle V, E \rangle$ be a digraph. G is a Schreier graph if and only if it is regular and connected.*

Proof.

- ⊞ X -regularity was observed in section 4.1. Proposition 4.9(ii) shows that Schreier graphs are connected.
- ⊞ Let X be a set such that G is X -regular, and fix any vertex $v \in V$ for the rest of this proof. As mentioned in section 4.1, X -regularity gives a natural interpretation

of words $x_1 \cdots x_n \in F$, where $x_i \in X^\pm$ for $i = 1, \dots, n$, as paths in G beginning at v .

Let K be the group of cycles in G based at v . By identifying the cycles in G with words $x_1 \cdots x_n$, where $x_i \in X^\pm$, we may view K as a subgroup of the free group $F = F(X)$. We will show that G is the Schreier graph of $K \leq F$.

Define a function $L : V \rightarrow F/K$ from vertices of G to right cosets of K in F as follows: Let $w \in V$, and let $\alpha \in F$ represent a path in G from v to w (this exists, as G is connected). Define $L(w) = K\alpha$. We must check that $L(w)$ is independent of the choice of α :

Suppose α, β are two paths in G from v to w . Then $\alpha\beta^{-1}$ is a cycle in G based at v , so that $\alpha\beta^{-1} \in K$. Hence $K\alpha = K\beta$.

So L is a well-defined labelling of the vertices. In fact, L is a bijection:

Injectivity: Suppose $L(w_1) = L(w_2)$. In other words, if α, β are paths in G starting at v and ending at w_1, w_2 , respectively, then $K\alpha = K\beta$. It follows that $\alpha\beta^{-1} \in K$, i.e. that $\alpha\beta^{-1}$ is a cycle in G . Hence the paths represented by α and β have the same end points, i.e. $w_1 = w_2$.

Surjectivity: If $K\alpha$ is a coset, let $w \in V$ be the end point of the path represented by α and starting at v . Then $L(w) = K\alpha$.

From now on, we identify vertices of G and cosets of $K \leq F$ using the function L . In particular, the vertex v that was fixed at the beginning of the proof is now referred to as K .

It remains to check that, for each $x \in X^\pm$ and any $K\xi, K\zeta \in V$, $K\xi \xrightarrow{x} K\zeta$ if and only if $K\xi x = K\zeta$; see also figure 4.5.

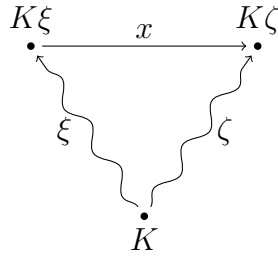


Figure 4.5: The labelling in the Schreier graph of $K \leq F$

$K\xi \xrightarrow{x} K\zeta \Leftrightarrow$ the two paths represented by $\xi x, \zeta$ starting at K have the same endpoint

$$\Leftrightarrow \xi x \zeta^{-1} \text{ represents a cycle based at } K$$

$$\Leftrightarrow \xi x \zeta^{-1} \in K$$

$$\Leftrightarrow K\xi x = K\zeta,$$

as required.

□

Normal subgroups of free groups will play an important role in chapter 5. It will be useful to know what the Schreier graphs of such groups look like. Here we find a simple condition on Schreier graphs which characterises the normal subgroups.

Definition 4.16. Every $\alpha \in F$ may be viewed as a translation function on G , sending the vertex $K\xi$ to the vertex $K\alpha\xi$. G is *translation invariant* if

$$K\xi \xrightarrow{x} K\zeta \Leftrightarrow K\alpha\xi \xrightarrow{x} K\alpha\zeta$$

for all words $\alpha \in F$, all letters $x \in X^\pm$, and all vertices $K\xi, K\zeta \in V$. So G is translation invariant if it ‘looks the same everywhere’.

We can now classify the Schreier graphs of normal subgroups of free groups:

Proposition 4.17. *Let $F = F(X)$ be a free group, and let $K \leq F$ be a subgroup. Then K is normal if and only if the Schreier graph of $K \leq F$ is translation invariant.*

Proof.

⊞ Suppose K is a normal subgroup of F . Let $\alpha, \xi, \zeta \in F$ and $x \in X^\pm$ be arbitrary.

Then

$$\begin{aligned}
K\xi \xrightarrow{x} K\zeta &\Leftrightarrow K\xi x = K\zeta \\
&\Leftrightarrow \xi x \zeta^{-1} \in K \\
&\Leftrightarrow \alpha \xi x \zeta^{-1} \alpha^{-1} \in K && \text{(as } K \text{ is normal)} \\
&\Leftrightarrow K\alpha\zeta = K\alpha\xi x \\
&\Leftrightarrow K\alpha\xi \xrightarrow{x} K\alpha\zeta
\end{aligned}$$

⊞ If K is not normal in F , then there are $\alpha \in F$ and $\beta \in K$ with $\alpha\beta\alpha^{-1} \notin K$. As β can't be the identity, we let $x \in X^\pm$ be the first X -letter of the X -reduction of β , and we define $\zeta = \beta^{-1}x$. Then

$$\begin{aligned}
x\zeta^{-1} = \beta \in K &\Rightarrow Kx = K\zeta \\
&\Rightarrow K \xrightarrow{x} K\zeta.
\end{aligned}$$

But, on the other hand,

$$\begin{aligned}
\alpha x \zeta^{-1} \alpha^{-1} = \alpha \beta \alpha^{-1} \notin K &\Rightarrow K\alpha x \neq K\alpha\zeta \\
&\Rightarrow \neg(K\alpha \xrightarrow{x} K\alpha\zeta)
\end{aligned}$$

□

Combining this result with proposition 4.15, we obtain a full classification.

Corollary 4.18. *The Schreier graphs of normal subgroups of free groups are precisely the regular, connected, and translation invariant digraphs.*

Chapter 5

Nielsen–Schreier and the Axiom of Choice

All proofs of the Nielsen–Schreier theorem use the Axiom of Choice, so it is natural to ask whether it is equivalent to the Axiom of Choice. In this chapter we attempt to answer this question.

Section 5.1 gives a short account of all results that have been published in this area. In section 5.2 we analyse how the Axiom of Choice is used in the proof of theorem 4.11, as well as several other proofs.

Many approaches are available to anyone who wants to deduce the Axiom of Choice from the Nielsen–Schreier theorem. One approach that comes to mind is to reverse-engineer the proof of the Nielsen–Schreier theorem given in chapter 4, i.e. to construct a spanning tree of a Schreier graph of $K \leq F$ from a basis of K . In section 5.3, we show that this is not possible.

Section 5.4 presents a new proof that the Nielsen–Schreier theorem implies the Axiom of Finite Choice. For this proof we introduce counting homomorphisms and representative functions. They are a tool for constructing choice functions from bases of algebraic structures. The technique is sufficiently general, so that it can be used for free abelian

groups in chapter 6.

The results in section 5.4 are strengthened in section 5.5. We show that the Nielsen–Schreier theorem does not follow from the Boolean Prime Ideal Theorem. In particular, it doesn’t follow from the Finite Axiom of Choice. So the implication proved in section 5.4 cannot be reversed.

The chapter is concluded by section 5.6, where we show, using the technology developed in section 5.4, that a strong form of the Nielsen–Schreier theorem is equivalent to the Axiom of Choice.

5.1 A brief history

The first result concerning the relationship between NS and the Axiom of Choice was Läuchli’s theorem using Fraenkel–Mostowski models, which was presented in section 2.2:

Theorem 5.1 (Läuchli [31]). *NS is not a theorem of ZFA.*

This means that every proof of the Nielsen–Schreier theorem in set theory with atoms must use the Axiom of Choice. We saw in example 2.16 that $\neg\text{NS}$ is a boundable statement. Hence the Transfer Theorem (theorem 2.17) immediately gives the corresponding result for ZF:

Theorem 5.2. *NS is not a theorem of ZF.*

In 1985, Howard proved a more specific result. He showed that

Theorem 5.3 (Howard [16]). $\text{ZF} \vdash \text{NS} \Rightarrow \text{AC}_{\text{fin}}$.

This is the strongest known theorem about the deductive strength of the Nielsen–Schreier theorem. However, two variations have been investigated, and both of them have turned out to be equivalent to the Axiom of Choice. Before stating the theorems, we need some definitions.

Definition 5.4 (Howard [16]). Let $F = F(X)$ and $B \subseteq F$. B is *level* (with respect to X) if, for all $\beta \in \langle B \rangle$, $\beta \in \langle \{b \in B : \ell_X(b) \leq \ell_X(\beta)\} \rangle$.

B has the *Nielsen property* (with respect to X) if

- (i) $B \cap B^{-1} = \emptyset$,
- (ii) if $b_1, b_2 \in B^\pm$ and $\ell_X(b_1 b_2) < \ell_X(b_1)$, then $b_2 = b_1^{-1}$,
- (iii) if $b_1, b_2, b_3 \in B^\pm$ and $\ell_X(b_1 b_2 b_3) \leq \ell_X(b_1) - \ell_X(b_2) + \ell_X(b_3)$, then $b_2 = b_1^{-1}$ or $b_3 = b_2^{-1}$.

The Nielsen–Schreier theorem guarantees the existence of bases of subgroups of free groups. We can strengthen it by placing restrictions on the kind of basis that it produces. For example, requiring it to be level or to have the Nielsen property gives us two new versions of the theorem, both of which are provable in ZFC. It turns out that they are equivalent to the Axiom of Choice in the presence of the other axioms of set theory:

Theorem 5.5 (Howard [16], Howard [17]).

(i) *The statement*

If $F = F(X)$ and $K \leq F$ is a subgroup, then there is a basis B of K which has the Nielsen property with respect to X .

is equivalent to the Axiom of Choice.

(ii) *The statement*

If $F = F(X)$ and $K \leq F$ is a subgroup, then there is a basis B of K which is level with respect to X .

is equivalent to the Axiom of Choice

Federer and Jonsson [8] showed that every set with the Nielsen property is level. Hence

(ii) implies (i).

No more papers in this area have been published since 1987. In the following sections we will improve, extend, and complement the known results.

5.2 The use of the Axiom of Choice

When determining whether or not the Nielsen–Schreier theorem is equivalent to the Axiom of Choice, the first question that must be answered is: How much Choice do the known proofs use? If any of them doesn't use the full Axiom of Choice, then there is no point in trying to show that NS is equivalent to AC. We will see in this section that the full Axiom of Choice is necessary for the standard proofs.

The only invocation of AC was in the assertion that every Schreier graph has a spanning tree. It is well known that the existence of spanning trees in connected graphs is equivalent to the Axiom of Choice; see for example the paper by Delhommé and Morillon [7]. But not every graph is a Schreier graph. Is the class of Schreier graphs nevertheless large enough, so that this assertion requires the full Axiom of Choice?

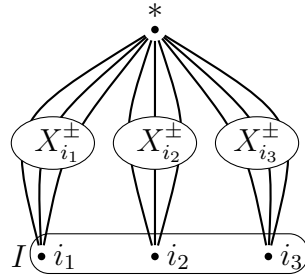
Proposition 5.6. *The existence of spanning trees in regular connected graphs is equivalent to the Axiom of Choice.*

Proof. The Axiom of Choice implies that every connected regular graph has a spanning tree by a standard application of Zorn's Lemma.

For the converse, let $S = \{X_i : i \in I\}$ be a family of non-empty sets. Without loss of generality, the X_i are pairwise disjoint. Let $X = \bigcup_{i \in I} X_i$. We will construct a connected X -regular graph such that every spanning tree immediately gives a choice function for S .

Let $G' = \langle V, E \rangle$ be the graph defined as follows. $V = I \cup \{*\}$, where $* \notin I$ is arbitrary. For every $i \in I$ and $x \in X_i^\pm$, E contains an edge labelled x from $*$ to i and an edge labelled x from i to $*$. The resulting graph is illustrated in figure 5.1.

Any spanning tree T of G' yields a choice function for S : For every $i \in I$ there is only

Figure 5.1: The graph G'

one branch in T connecting the vertices $*$ and i . This branch corresponds to a single element of X_i .

However, G' is not regular. To fix this, we add to each vertex as many loops (with suitable labels) as are necessary to make the graph X -regular, forming a new digraph G . Every spanning tree of G is a spanning tree of G' , because trees do not contain loops. Hence every spanning tree of G gives rise to a choice function for S . \square

Now the classification of Schreier graphs in proposition 4.15 immediately yields:

Theorem 5.7. *The statement*

Every Schreier graph has a spanning tree

is equivalent to the Axiom of Choice.

We briefly mention several other proofs, and state why all of them use the full Axiom of Choice.

Nielsen's proof

Nielsen's proof [34] of the theorem for finitely generated free groups is generalised to the infinitely generated case in chapter 3 of Johnson's book [25]. His proof relies on a well-ordering of the generating set of arbitrary free groups. Since any set can be used as a generating set, this requires the Well-ordering Principle.

Schreier's proof

An English version of Schreier's proof [39] is given in chapter 2 of Johnson's textbook [25]. The underlying strategy of the proof is exactly the same as in the proof given in chapter 4, but it is written using exclusively algebraic language instead of trees in digraphs. The Axiom of Choice is used to find a Schreier transversal (see chapter 2 of Johnson [25] for the definition). However, Schreier transversals are just spanning trees of Schreier graphs in an algebraic costume. So, by theorem 5.7, the full Axiom of Choice is used.

A topological proof

A proof using covering spaces in algebraic topology is given in section 1.A of Hatcher [13]. If $F = F(X)$ is a free group, then it is isomorphic to the fundamental group of a bouquet of circles indexed by elements of X . Every subgroup $K \leq F$ corresponds to a covering space of this topological space. It turns out that covering spaces are precisely the Schreier graphs of subgroups $K \leq F$. A spanning tree of the graph is used to show that its fundamental group, K , is a free group. Again, the full Axiom of Choice is used to find a spanning tree of a Schreier graph.

A proof using wreath products

Ribes and Steinberg [38] used wreath products to prove the Nielsen–Schreier theorem. Their approach also requires the existence of a Schreier transversal, so, as in Schreier's version, the full Axiom of Choice is used.

But what about the theorem?

Now we have seen that the standard proofs of the Nielsen–Schreier theorem all use the full Axiom of Choice. But this doesn't mean that there is no proof which uses less

Choice.

Question. *Is the Nielsen–Schreier theorem equivalent to the Axiom of Choice?*

5.3 Does Nielsen–Schreier imply the Axiom of Choice?

If our aim is to deduce the Axiom of Choice from the Nielsen–Schreier theorem, one possible approach is to reverse engineer the proof of NS – to start from the statement of the theorem and to work backwards to the place in its proof where the Axiom of Choice is used. So we would like to know if it is possible to construct a spanning tree of the Schreier graph of $K \leq F = F(X)$ from a basis of K . In this section we show that this is not possible in general.

The strategy is to find a Fraenkel–Mostowski model \mathfrak{M} containing a subgroup K of a free group F where K has a basis in \mathfrak{M} , but the Schreier graph of $K \leq F$ has no spanning tree in \mathfrak{M} . A suitable model is van Douwen’s model, described in section 2.3. It is constructed from a collection $\{\langle A_i, <_i \rangle : i < \omega\}$ of pairwise disjoint sets, each linearly ordered like \mathbb{Z} . The set of atoms is $A = \bigcup_{i < \omega} A_i$, the group \mathcal{G} of permutations consists of all $\pi \in \text{Sym}(A)$ satisfying $(\forall i < \omega) \pi|_{A_i} \in \text{Aut}(A_i, <_i)$, and the sets of \mathfrak{M} are precisely those that are hereditarily of finite support.

The natural choice for the free group is $F = F(A)$, the free group on the set of atoms in \mathfrak{M} . The subgroup we shall consider is defined by

$$K = \langle \{ab^{-1} : (\exists i < \omega) a, b \in A_i\} \rangle.$$

We can easily prove that the Schreier graph of $K \leq F$ has no spanning tree:

Lemma 5.8.

(i) *If the Schreier graph of $K \leq F$ has a spanning tree, then the family $\{A_i : i < \omega\}$ has a choice function.*

(ii) *The Schreier graph of $K \leq F$ has no spanning tree in \mathfrak{M} .*

Proof.

- (i) Let T be a spanning tree of the Schreier graph. For each $i < \omega$, we write $K_i = Ka$, where $a \in A_i$ is arbitrary. We must check that this definition doesn't depend on the choice of $a \in A_i$. For any $a_1, a_2 \in A$ we have

$$\begin{aligned} Ka_1 = Ka_2 &\Leftrightarrow a_1a_2^{-1} \in K \\ &\Leftrightarrow (\exists i < \omega)a_1, a_2 \in A_i, \end{aligned}$$

showing that K_i is well defined.

For every $i < \omega$, T has precisely one edge from K to K_i – otherwise there would be a cycle in T . Since the label of this edge is a member of A_i^\pm , it picks out one element of A_i .

- (ii) This follows from lemma 2.12(ii).

□

In general, the Schreier graph of $K \leq F$ is too complicated to draw, but figure 5.2 shows the central part of the Schreier graph when we only consider two sets A_i and A_j ($i, j < \omega$).

It remains to find a basis of K in \mathfrak{M} .

Lemma 5.9. *K is a free group in \mathfrak{M} .*

Proof. Let $<$ be the linear ordering of A given by lemma 2.12(i). Define

$$B = \{ab^{-1} : (\exists i < \omega)(a, b \in A_i) \wedge (a < b) \wedge (\forall c \in A)(a < c \Rightarrow b \leq c)\}.$$

Since $<$ is a linear ordering in \mathfrak{M} , and B is defined from $<$, $B \in \mathfrak{M}$.

As each of the A_i is ordered like \mathbb{Z} by $<_i$, it makes sense to talk about successors and predecessors of atoms. If $a \in A$, write $a + 1$ for the least $b \in A$ satisfying $b > a$, and

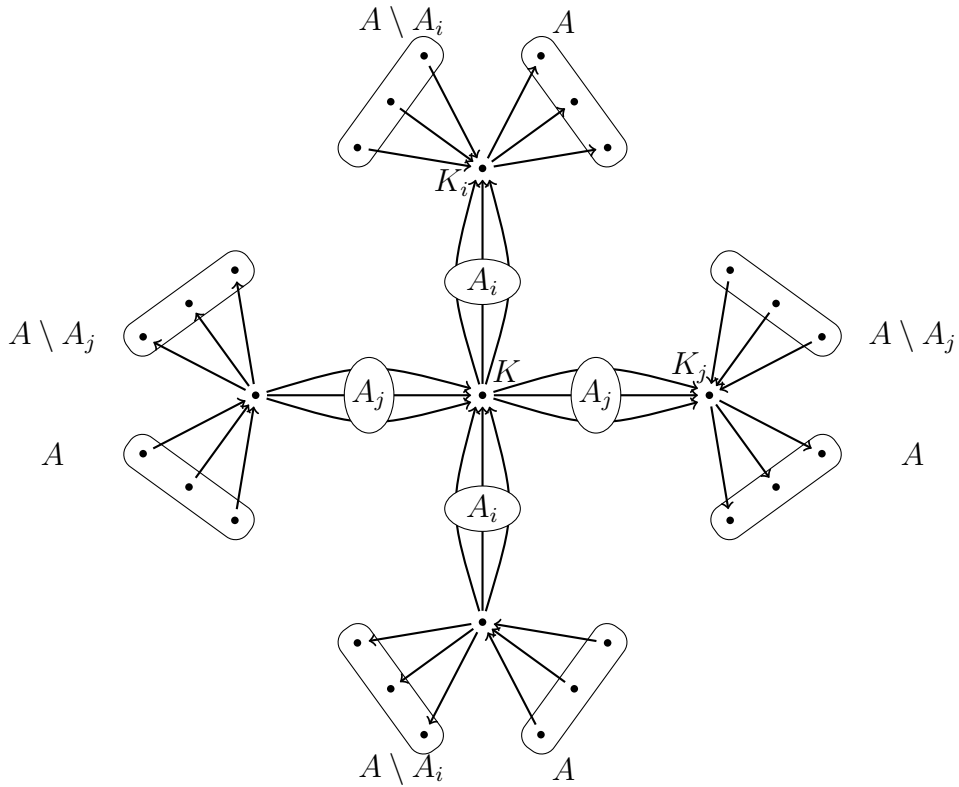


Figure 5.2: The Schreier graph of K

write $a - 1$ for the greatest $b \in A$ satisfying $b < a$. With this notation, the definition of B becomes much simpler:

$$B = \{a(a + 1)^{-1} : a \in A\}.$$

We will show that B is a basis for K .

(i) $\langle B \rangle = K$.

Let $i < \omega$, and let $a, b \in A_i$. If $a < b$, we can write

$$ab^{-1} = a(a + 1)^{-1} \cdot (a + 1)(a + 2)^{-1} \cdots (b - 1)b^{-1}.$$

If $a > b$, we have

$$ab^{-1} = (ba^{-1})^{-1} = (b(b + 1)^{-1} \cdots (a - 1)a^{-1})^{-1}.$$

It follows that $\{ab^{-1} : (\exists i < \omega) a, b \in A_i\} \subseteq \langle B \rangle$, i.e. that $\langle B \rangle = K$.

(ii) B is free.

Associate each member $a(a+1)^{-1} \in B$ with an arrow from a to $a+1$ and each $(a+1)a^{-1} \in B^{-1}$ with an arrow from $a+1$ to a . This turns A into a digraph with connected components $\{A_i : i < \omega\}$. Removing any $b \in B$ and its inverse from the digraph disconnects one of the A_i . In other words, $b \notin \langle B \setminus \{b\} \rangle$. This means that no $b \in B$ can be written as a product of other basis elements. Independence follows immediately: Suppose $b_1 \cdots b_n = \mathbf{1}$ is a reduced B -word with $n > 0$ and $b_1, \dots, b_n \in B^\pm$. Then $b_1 = b_n^{-1} \cdots b_2^{-1}$, giving a contradiction.

□

Combining lemmas 5.8 and 5.9 we get the following result:

Theorem 5.10. *There is a Fraenkel–Mostowski model \mathfrak{M} with a free group F and a subgroup K satisfying*

1. *The Schreier graph of $K \leq F$ has no spanning tree,*
2. *K has a basis B .*

This result is translated to ZF using the Transfer Theorem.

Corollary 5.11. *There is a model of ZF with a free group F and a subgroup K satisfying conditions 1. and 2. above.*

Proof. Write $\langle F, \mathbf{1}, * \rangle$ for the free group F , and write

$\phi(F, \mathbf{1}, *, X, K) = X$ is a basis of F and the Schreier graph of $\langle K, \mathbf{1}, *|_K \rangle \leq \langle F, \mathbf{1}, * \rangle$
has no spanning tree

$\psi(K, \mathbf{1}, *, B) = B$ is a basis of $\langle K, \mathbf{1}, *|_K \rangle$

In example 2.15 we saw that $\psi(K, \mathbf{1}, *, B)$ is a boundable formula.

It remains to show that $\phi(F, \mathbf{1}, *, X, K)$ is also boundable. Of course, X is a basis of F is just $\psi(F, \mathbf{1}, *, X)$, which is boundable. Write $G = \langle W, E \rangle$ for the Schreier graph.

The vertex set W is the set of right cosets of K , so $W \subseteq \mathcal{P}(F)$. Every edge of G can be written as a triple $\langle w_1, x, w_2 \rangle$, where $w_1 \in W$ is the beginning, $w_2 \in W$ is the end, and $x \in X^\pm$ is the label of the edge. So each edge is an element of $V_4(W \cup X)$. Hence $E \in V_5(W \cup X)$, and $G = \langle W, E \rangle \in V_7(W \cup X) \subseteq V_8(F \cup X)$. In order to verify that G has no spanning tree it suffices to check every element of $V_8(F \cup X)$. So ϕ is boundable, as required.

The corollary follows from the Transfer Theorem 2.17. □

This result shows that it is impossible to prove $\text{ZF} \vdash \text{NS} \Rightarrow \text{AC}$ by reducing the problem to the construction of a spanning tree in a Schreier graph from a basis of a subgroup $K \leq F$.

We conclude this section with one final remark. Notice that all elements of K have even A -length because the members of the generating set have length 2. Since all elements of the basis B constructed in the proof of lemma 5.9 have A -length 2, B is level. This is surprising in the light of theorem 5.5(ii), which says that the existence of level bases implies the Axiom of Choice. What is more, the property of being level is boundable, so it can be transferred to ZF.

5.4 Nielsen–Schreier implies the finite Axiom of Choice

As stated in section 5.1, Howard [16] showed that $\text{ZF} \vdash \text{NS} \Rightarrow \text{AC}_{\text{fin}}$. Here we prove a slightly stronger result with an entirely new proof. It is easier and shorter than Howard’s proof, and it introduces some general ideas that will be applied in later sections. Most of the material in this section also appears in Kleppmann’s article [29].

Representative functions

In this section we give a general description of representative functions and counting functions which will also be used in several other sections. The details will vary, so it

doesn't make sense to give precise definitions at this stage. But, as the fundamental mechanisms are always the same, we introduce the ideas by going over a simplified example.

We are given a non-empty set y , and we would like to pick an element from y without making any choices. Let $F = F(y)$ be the free group on y , and let

$$K = \langle \{wx^{-1} : w, x \in y\} \rangle \leq F.$$

Using NS, we may assume that K has a basis B , say. Notice that all members of K have even y -length, so $w \notin K$ for all $w \in y$. But we can use B to find representatives of letters $w \in y$ in the subgroup K . More precisely, we define a function $f : y \rightarrow K$ such that $f(w)$ behaves like w in a suitably defined sense. To define f , let $w \in y$ be arbitrary, and choose $x \in y \setminus \{w\}$. Since $wx^{-1} \in K$, we may write $wx^{-1} = b_1 \cdots b_n$ as a B -reduced word with $b_1, \dots, b_n \in B^\pm$. If $n = 2k$ is even, we define

$$f(w) = b_1 \cdots b_k$$

to be the 'first half' of wx^{-1} in terms of the new basis B . Intuitively, the first half of wx^{-1} should behave like w and the second half should behave like x^{-1} . Under the right circumstances, f is well defined and

$$wx^{-1} = f(w)f(x)^{-1}. \tag{5.1}$$

Of course, f will not be well defined in general, and it is far from obvious that it will exhibit the correct behaviour. However, a careful choice of parameters does make it work. If this is the case, we define a new function $g : y \rightarrow F$ by

$$g(w) = f(w)^{-1}w.$$

If (5.1) holds for all $w, x \in y$, then g is a constant function. Let $\alpha \in F$ be the value of g . It can be used to choose an element of y : As remarked earlier, $w \notin K$ for all $w \in y$; it follows that $f(w) \neq w$ for all $w \in y$, and that $\alpha \neq \mathbf{1}$. So we can take the first letter of the y -reduction of α as the chosen element of y .

Counting homomorphisms

Let Y be a family of non-empty pairwise disjoint sets, let $X = \bigcup Y$, and let $F = F(X)$ be the free group on X . It will be useful to count letters of words $\alpha \in F$. To this end we define, for each $y \in Y$, a counting function $\#_y : F \rightarrow \mathbb{Z}$. If $\alpha \in F$, we may write $\alpha = x_1^{\epsilon_1} \cdots x_n^{\epsilon_n}$ as an X -reduced word with $x_1, \dots, x_n \in X$ and $\epsilon_1, \dots, \epsilon_n \in \{1, -1\}$. Then $\#_y(\alpha)$ is equal to the sum of exponents of y -letters in α :

$$\#_y(\alpha) = \sum_{i: x_i \in y} \epsilon_i.$$

It is easy to check that each $\#_y$ is a group homomorphism from F to the additive group of integers. We now have the tools necessary for the proof.

The proof

As we will be concerned with normal subgroups of free groups, we introduce a new choice principle:

NS_{norm} (Nielsen–Schreier for normal subgroups): *If F is any free group and $K \leq F$ is any normal subgroup, then K is a free group.*

This principle only makes a statement about normal subgroups of free groups, so it is weaker than **NS**. Hence the implication **NS_{norm}** \Rightarrow **AC_{fin}** proved here is at least as strong as the already known implication **NS** \Rightarrow **AC_{fin}**. Before proving the full theorem, we must handle a special case.

Lemma 5.12. $\text{ZF} \vdash \text{NS}_{\text{norm}} \Rightarrow \text{AC}_2$.

Proof. Let Y be a family of pairwise disjoint 2-element sets. Let $X = \bigcup Y$, let $F = F(X)$ be the free group on X , and define the subgroup $K \leq F$ by

$$K = \bigcap \{\ker(\#_y) : y \in Y\}.$$

K is non-trivial, because it contains, for example, wx^{-1} for each $y = \{w, x\} \in Y$.

Moreover, as kernels of homomorphisms are normal, so is K . By NS_{norm} , there is a basis B for K .

Let $y \in Y$ be arbitrary but fixed. We shall show how to single out one element of y without making any choices. Define the swapping function $s_y : y \rightarrow y$ to transpose the two elements of y . For any $x \in y$, we have $y = \{x, s_y(x)\}$. To simplify notation, we write $x_i = s_y^i(x)$ for $i \in \mathbb{Z}$, so that $y = \{x_0, x_1\}$. Since $x_0x_1^{-1}, x_1x_0^{-1} \in K$, we may write

$$\begin{aligned} x_0x_1^{-1} &= b_{0,1} \cdots b_{0,\ell_0} \\ x_1x_0^{-1} &= b_{1,1} \cdots b_{1,\ell_1}, \end{aligned}$$

as reduced B -words, where the $b_{i,j} \in B^\pm$. From $x_0x_1^{-1} = (x_1x_0^{-1})^{-1}$ we deduce that $\ell_0 = \ell_1 = \ell$, say, and that

$$b_{1,1} = b_{0,\ell}^{-1}, \dots, b_{1,\ell} = b_{0,1}^{-1}. \quad (5.2)$$

There are two cases:

(1) ℓ is odd.

Set $k = (\ell - 1)/2$. The middle B -letter of $x_0x_1^{-1}$ is $b_{0,k+1}$, while the middle B -letter of $x_1x_0^{-1}$ is $b_{1,k+1} = b_{0,k+1}^{-1}$. Just one of these two is an element of B . The chosen element of y is the unique x_i such that the middle B -letter of $x_ix_{i+1}^{-1}$ is in B (and not in B^{-1}).

(2) ℓ is even.

Let $k = \ell/2$. Define the representative function f_y and its companion g_y as follows:

$$\begin{aligned} f_y : y \rightarrow K : x_i &\mapsto b_{i,1} \cdots b_{i,k} \\ g_y : y \rightarrow F : x_i &\mapsto f_y(x_i)^{-1}x_i. \end{aligned}$$

Then

$$\begin{aligned} f_y(x_0)f_y(x_1)^{-1} &= b_{0,1} \cdots b_{0,k}b_{1,k}^{-1} \cdots b_{1,1}^{-1} \\ &= b_{0,1} \cdots b_{0,k}b_{0,k+1} \cdots b_{0,\ell} \quad (\text{by (5.2)}) \\ &= x_0x_1^{-1}, \end{aligned}$$

so $g_y(x_0) = g_y(x_1)$, and g_y is a constant function taking just one value, α_y , say. We check that α_y mentions letters from y :

$$\begin{aligned} \#_y(\alpha_y) &= \#_y(f_y(x_0)^{-1}x_0) \\ &= \#_y(x_0) - \#_y(f_y(x_0)) \\ &= 1 - 0 \quad (\text{as } x_0 \in y \text{ and } f_y(x_0) \in K \leq \ker(\#_y).) \end{aligned}$$

Since $\#_y(\alpha_y) = 1$, α_y mentions at least one y -letter. So we choose an element of y by picking the first y -letter appearing in α_y .

□

This proof serves as an introduction to ideas used in the main proof. The general case is more complicated and requires more structure to carry out the argument using representative functions.

Proposition 5.13. $\text{ZF} \vdash \text{NS}_{\text{norm}} \Rightarrow \text{AC}_{\text{fin}}$.

Proof. Let Z be a set of finite non-empty sets. We will find a choice function for Z by induction on the size of its members. In order to do this, it will be useful to close Z under non-empty subsets. So let

$$Y = \{y : y \neq \emptyset \wedge (\exists z \in Z)y \subseteq z\}.$$

As $Z \subseteq Y$, it suffices to find a choice function for Y . Replacing each $y \in Y$ with $y \times \{y\}$, we may assume that the members of y are pairwise disjoint.

Let $X = \bigcup Y$, let $F = \text{F}(X)$ be the free group on X , and let $K \leq F$ be the subgroup defined by

$$K = \bigcap \{\ker(\#_y) : y \in Y\}.$$

As in lemma 5.12, K is a non-trivial normal subgroup of F . By NS_{norm} , K has a basis B , say.

For each n such that $2 \leq n < \omega$, write $Y^{(n)} = \{y \in Y : |y| = n\}$ and $Y^{(\leq n)} = \{y \in Y : |y| \leq n\}$. By induction on n , we will find nested choice functions c_n on $Y^{(\leq n)}$ for each $n < \omega$. Then $\bigcup_{n < \omega} c_n$ is a choice function for Y .

By lemma 5.12 there is a choice function c_2 on $Y^{(\leq 2)}$. So assume that $n \geq 3$ and that there is a choice function c_{n-1} on $Y^{(\leq n-1)}$. For every $y \in Y^{(n)}$ we define a function s_y as follows:

$$s_y : y \rightarrow y : x \mapsto c_{n-1}(y \setminus \{x\}).$$

Note that $y \setminus \{x\} \in Y^{(n-1)}$, because Y is closed under taking non-empty subsets, so $c_{n-1}(y \setminus \{x\})$ is defined. There are four cases:

(i) s_y is not a bijection.

In this case, $|s_y^{-1}y| \leq n - 1$, so defining

$$c_n(y) = c_{n-1}(s_y^{-1}y)$$

gives a choice of element of y . Again, this is well-defined, because Y is closed under taking non-empty subsets.

(ii) s_y is a bijection with at least two orbits.¹

As $s_y(x) \neq x$ for all $x \in y$, the number of orbits is $\leq n - 1$. But, since there are at least two orbits, the size of each orbit is also $\leq n - 1$. So we can choose a single element of y by picking a point from each orbit, and then picking one from among them. More precisely, we define

$$c_n(y) = c_{n-1}(\{c_{n-1}(\text{orb}(x)) : x \in y\}),$$

where $\text{orb}(x)$ is the orbit of $x \in y$ under the action of s_y .

(iii) s_y is a bijection with one orbit, and n is even.

If n is even, s_y^2 is a bijection with two orbits. Remembering that we are assuming $n \geq 3$, this gives us $\leq n - 1$ orbits of size $\leq n - 1$ each. A choice is made as in the previous case.

(iv) s_y is a bijection with one orbit, and n is odd.

For any $x \in y$, $y = \{x, s_y(x), s_y^2(x), \dots, s_y^{n-1}(x)\}$. For simplicity, we write $x_i = s_y^i(x)$ for $i \in \mathbb{Z}$, so that $y = \{x_0, x_1, \dots, x_{n-1}\}$.

¹Thank you to Thomas Forster for suggesting a simplification to this part of the proof.

Recall the basis B of K . We may write

$$\begin{aligned} x_0x_1^{-1} &= b_{0,1} \cdots b_{0,\ell_0} \\ x_1x_2^{-1} &= b_{1,1} \cdots b_{1,\ell_1} \\ &\dots \\ x_{n-1}x_n^{-1} &= b_{n-1,1} \cdots b_{n-1,\ell_{n-1}} \end{aligned}$$

as reduced B -words, with the $b_{i,j} \in B^\pm$. Before defining a representative function, we must prepare the ground. This is done in two steps:

- (1) If it is not the case that $\ell_0 = \dots = \ell_{n-1}$, let $\ell = \min\{\ell_i : i = 0, \dots, n-1\}$. Then $\{x_i : \ell_i = \ell\}$ is a proper non-empty subset of y , and we define

$$c_n(y) = c_{n-1}(\{x_i : \ell_i = \ell\}).$$

From now on, we assume $\ell_0 = \dots = \ell_{n-1} = \ell$.

- (2) Note that

$$(x_0x_1^{-1})(x_1x_2^{-1}) \cdots (x_{n-1}x_n^{-1}) = \mathbf{1},$$

i.e.

$$(b_{0,1} \cdots b_{0,\ell})(b_{1,1} \cdots b_{1,\ell}) \cdots (b_{n-1,1} \cdots b_{n-1,\ell}) = \mathbf{1}. \quad (5.3)$$

For $i = 0, \dots, n-1$, let k_i be the number of B -cancellations in

$$(b_{i,1} \cdots b_{i,\ell})(b_{i+1,1} \cdots b_{i+1,\ell}). \quad (5.4)$$

If it is not the case that $k_0 = \dots = k_{n-1}$, let $k = \min\{k_i : i = 0, \dots, n-1\}$.

Then $\{x_i : k_i = k\}$ is a proper non-empty subset of y , and we define

$$c_n(y) = c_{n-1}(\{x_i : k_i = k\}).$$

From now on, we assume $k_0 = \dots = k_{n-1} = k$.

As letters always cancel in pairs, (5.3) implies that $n\ell$ is even.² Since we are assuming that n is odd, it follows that ℓ is even. Define $m = \ell/2$, and note that

²I would like to thank John Truss and Benedikt Löwe for finding an error in this proof and suggesting a solution.

$k \geq m$: if not, then complete cancellation in (5.3) would not be possible. Now we can define a representative function f_y and its companion function g_y :

$$\begin{aligned} f_y : y \rightarrow K : x_i &\mapsto b_{i,1} \cdots b_{i,m} \\ g_y : y \rightarrow F : x_i &\mapsto x_i^{-1} f_y(x_i). \end{aligned}$$

Since there are $k \geq m$ cancellations in (5.4), we have $b_{i+1,1} = b_{i,\ell}^{-1}, \dots, b_{i+1,m} = b_{i,\ell-m+1}^{-1} = b_{i,m+1}^{-1}$. This implies that

$$f_y(x_i) f_y(x_{i+1})^{-1} = x_i x_{i+1}^{-1}$$

for each i . Hence $g_y(x_i) = g_y(x_{i+1})$ for all i , and $g_y : y \rightarrow F$ is again constant. If we let α_y be the constant value of g_y , then $\#_y(\alpha_y) = 1$, so α_y mentions at least one element of y . As in lemma 5.12, we choose an element of y by picking the first y -letter appearing in α_y .

□

Finiteness was used in this proof to define the functions s_y , giving a cyclic ordering of each finite set. Using this structure, it was possible to define the representative function. If we try to prove $\text{NS} \Rightarrow \text{AC}$, it seems likely that a similar structure could be used to define representative functions. But, as this remains an unsolved problem, we will employ the Fraenkel–Mostowski method to strengthen proposition 5.13 in the next section.

5.5 Nielsen–Schreier doesn't follow from the Prime Ideal Theorem

We have seen that NS_{norm} implies the Axiom of Choice for families of non-empty finite sets. So

$$\text{AC} \Rightarrow \text{NS} \Rightarrow \text{NS}_{\text{norm}} \Rightarrow \text{AC}_{\text{fin}}.$$

From what we have seen so far, it is possible that \mathbf{NS} is equivalent to \mathbf{AC}_{fin} . However, in this section we shall see that $\mathbf{NS}_{\text{norm}}$ does not follow from the Boolean Prime Ideal Theorem (defined in chapter 1.5). As $\mathbf{ZF} \vdash \mathbf{BPIT} \Rightarrow \mathbf{AC}_{\text{fin}}$, it follows immediately that $\mathbf{NS}_{\text{norm}}$, and hence also \mathbf{NS} , are strictly stronger than \mathbf{AC}_{fin} . The material in this section is adapted from Kleppmann [28].

Our aim is to find a model of \mathbf{ZF} set theory in which the Boolean Prime Ideal Theorem holds and $\mathbf{NS}_{\text{norm}}$ fails. Using the Transfer Theorem, it suffices to find a Fraenkel–Mostowski satisfying these properties. We can build on the work of Dawson and Howard, who introduced the Dawson–Howard model (see section 2.3) and showed that the Boolean Prime Ideal Theorem holds in it. It remains to be shown that $\mathbf{NS}_{\text{norm}}$ fails in this model.

For the rest of this section, we write \mathfrak{M} for the Dawson–Howard model. Recall that the set A of atoms in \mathfrak{M} is constructed by taking a family $\{\langle A_i, <_i \rangle : i < \omega\}$ of pairwise disjoint sets A_i , linearly ordered like \mathbb{Q} , and setting $A = \bigcup_{i < \omega} A_i$. The group \mathcal{G} of permutations of A consists of all $\pi \in \text{Sym}(A)$ satisfying $(\forall i < \omega) \pi|_{A_i} \in \text{Aut}(A_i, <_i)$. The sets of \mathfrak{M} are precisely those that are hereditarily of finite support. Inside \mathfrak{M} there is a free group $F = F(A)$ generated by A . We will find a subgroup of F which has no basis in \mathfrak{M} .

Definition 5.14. Recall from chapter 5.4 the counting homomorphisms $\#_{A_i} : F \rightarrow \mathbb{Z}$. Define, for the rest of this section, the subgroup K of F by

$$K = \bigcap_{i < \omega} \ker(\#_{A_i}).$$

As usual, K is a non-trivial normal subgroup of F . We will now show that K has no basis in \mathfrak{M} .

Theorem 5.15. $\mathfrak{M} \models \neg \mathbf{NS}_{\text{norm}}$.

Proof. Suppose there is a basis B for K in \mathfrak{M} . We will derive a contradiction. Let $E \subseteq A$ be a support for B . Since E must be finite, we may fix $i < \omega$ satisfying $A_i \cap E = \emptyset$. We also fix three arbitrary points $x < y < z \in A_i$. Having chosen x, y, z , we define $\beta = xy^{-1}$. Note that $\beta \in K$. Let $\pi \in \mathcal{G}$ have the following properties:

$$(i) \quad (\forall a \in E) \pi(a) = a,$$

$$(ii) \quad (\forall a \in A \setminus E) \pi(a) \neq a,$$

$$(iii) \quad \pi(x) = y, \pi(y) = z.$$

(i) says that $\pi \in \text{fix}(E)$, so that $\pi(B) = B$. By (iii), $\beta \cdot \pi(\beta) = xy^{-1} \cdot yz^{-1} = xz^{-1}$. So if we pick $\sigma \in \text{fix}(E)$ satisfying $\sigma(x) = x$ and $\sigma(y) = z$, then

$$\beta \cdot \pi(\beta) = \sigma(\beta). \tag{5.5}$$

Writing $\beta = b_1 \cdots b_m$ as a reduced B -word with $b_1, \dots, b_m \in B^\pm$, we get

$$\begin{aligned} \pi(\beta) &= \pi(b_1) \cdots \pi(b_m) \\ \sigma(\beta) &= \sigma(b_1) \cdots \sigma(b_m), \end{aligned}$$

which must also be reduced B -words. Substituting these into (5.5), we see that the right-hand side of the equation is B -reduced and has m B -letters, while the left-hand side has $2m$ letters. Hence m letters cancel out when reducing the left-hand side with respect to B . As letters always cancel out in pairs, $m = 2k$ is even. The letters that cancel out on the left-hand side of (5.5) are

$$b_{k+1} \cdots b_{2k} \pi(b_1) \cdots \pi(b_k) = \mathbf{1}.$$

Since $\pi(B) = B$ it follows that

$$\pi(b_k)^{-1} = b_{k+1}, \dots, \pi(b_1)^{-1} = b_{2k}.$$

Define

$$\gamma = b_1 \cdots b_k \in K$$

to be the ‘first half’ of β , and note that

$$\begin{aligned} \gamma \cdot \pi(\gamma^{-1}) &= b_1 \cdots b_k \pi(b_k)^{-1} \cdots \pi(b_1)^{-1} \\ &= b_1 \cdots b_k b_{k+1} \cdots b_{2k} \\ &= \beta. \end{aligned} \tag{5.6}$$

Since A is a basis for the free group F , γ can be written uniquely as a reduced A -word $a_1 \cdots a_\ell$ with $a_1, \dots, a_\ell \in A^\pm$. From (5.6) it follows that

$$a_1 \cdots a_\ell \pi(a_\ell)^{-1} \cdots \pi(a_1)^{-1} = xy^{-1},$$

where the right-hand side is already A -reduced. Thus

$$a_1 = x, \pi(a_2) = a_2, \dots, \pi(a_\ell) = a_\ell.$$

Now condition (ii) implies that $a_2, \dots, a_\ell \in E$.

But i was chosen so that $A_i \cap E = \emptyset$. Hence the only A -letter of $\gamma = a_1 \cdots a_\ell$ which lies in A_i is $a_1 = x$. So $\#_{A_i}(\gamma) \neq 0$, and hence $\gamma \notin K$, contradicting the definition of γ as a member of K . \square

Recall that, by theorem 2.11, $\mathfrak{M} \models \text{BPIT}$. Hence:

Corollary 5.16. $\mathfrak{M} \models \text{BPIT} \wedge \neg \text{NS}_{\text{norm}}$.

We saw in example 2.16 that $\neg \text{NS}$ is boundable. The same argument shows that $\neg \text{NS}_{\text{norm}}$ is boundable. By the Transfer Theorem 2.17 it follows that there is a ZF-model \mathfrak{N} satisfying $\mathfrak{N} \models \text{BPIT} \wedge \neg \text{NS}_{\text{norm}}$. Hence:

Corollary 5.17. $\text{ZF} \not\models \text{BPIT} \Rightarrow \text{NS}_{\text{norm}}$.

Since $\text{ZF} \vdash \text{BPIT} \Rightarrow \text{AC}_{\text{fin}}$, it follows that $\text{ZF} \not\models \text{AC}_{\text{fin}} \Rightarrow \text{NS}_{\text{norm}}$. In particular, neither NS_{norm} nor NS is equivalent to AC_{fin} . This strengthens theorem 5.3.

5.6 Reduced Nielsen–Schreier implies the Axiom of Choice

In section 5.4 we saw how representative functions can be used to define a choice function for a family of non-empty finite sets. We assumed that the members of the family are

finite in order to inductively construct a cyclic order on each them. This allowed us to define representative functions and to show that they are well-defined.

In this section, we give another application of representative functions. But this time we don't impose restrictions on the families for which we construct choice functions; instead, we deduce the Axiom of Choice from \mathbf{NS}_{red} , a strong version of the Nielsen–Schreier theorem which produces reduced bases – see below for the definition. This section is adapted from Kleppmann's paper [28].

Definition 5.18. Let $F = F(X)$ be a free group. If $K \leq F$ is a subgroup, and B is a basis for K , then B is *reduced* with respect to X if, for all $\beta \in K$, $\ell_B(\beta) \leq \ell_X(\beta)$.

This definition gives rise to a strong version of the Nielsen–Schreier theorem, defined as follows:

\mathbf{NS}_{red} (reduced Nielsen–Schreier): *If $F = F(X)$ and $K \leq F$ is a subgroup, then there is a basis B of K which is reduced with respect to X .*

Of course, we must check that it makes sense to adopt this as a choice principle. We show that the statement is provable in ZFC.

Proposition 5.19. \mathbf{NS}_{red} is a theorem of ZFC.

Proof. Consider the proof of the Nielsen–Schreier theorem given in chapter 4. The subgroup K of the free group $F = F(X)$ was thought of as the group of cycles based at K in the Schreier graph of $K \leq F$. A spanning tree was used to find a set B of cycles such that any cycle based at K can be expressed as a unique product of members of B : Every cycle

$$\xi = e_1^{\epsilon_1} \cdots e_n^{\epsilon_n}$$

of length n is written as a product

$$\lambda(e_1)^{\epsilon_1} \cdots \lambda(e_n)^{\epsilon_n} \tag{5.7}$$

of n elements of B . So the B -length of ξ cannot exceed the its X -length. As some cancellation may occur in (5.7), the B -length may be less than the X -length. \square

In section 5.1 we encountered level sets and sets with the Nielsen property. Both of these properties give rise to strong versions of the Nielsen–Schreier theorem, which, as stated in theorem 5.5, both imply the Axiom of Choice. To check that our results are not implied by theorem 5.5, we show that there are bases that are level and not reduced, and there are bases that are reduced and not level. As every basis satisfying the Nielsen property is level, there is no need to check the Nielsen property separately.

Example 5.20. Let F be the free group on $X = \{x, y\}$. Then $B = \{xy^2, x\}$ is a basis of the subgroup $K = \langle x, y^2 \rangle$. We verify that B is reduced and not level:

(i) B is reduced.

If $\alpha \in K$ is any word in x and y^2 , replace each occurrence of y^2 (of X -length 2) with $x^{-1} * xy^2$ (of B -length 2), thus making it a B -word of the same B -length. After reducing with respect to B we have $\ell_B(\alpha) \leq \ell_X(\alpha)$.

(ii) B is not level.

Letting $\alpha = y^2 \in K$, we have $\alpha = x^{-1} * xy^2$ in terms of B . As $\ell_X(\alpha) = 2 < 3 = \ell_X(xy^2)$, $\alpha \notin \langle \{b \in B : \ell_X(b) \leq \ell_X(\alpha)\} \rangle$.

Example 5.21. Let F be the free group on $X = \{w, x, y, z\}$. Then

$$B = \{wx^{-1}, xy^{-1}, yz^{-1}\}$$

is an independent set, so it is a basis for the subgroup $K = \langle B \rangle$.

(i) B is not reduced.

$\ell_B(wz^{-1}) = \ell_B(wx^{-1} \cdot xy^{-1} \cdot yz^{-1}) = 3$ is bigger than $\ell_X(wz^{-1}) = 2$.

(ii) B is level.

We have $\langle \{b \in B : \ell_X(b) \leq n\} \rangle = K$ for all $n \geq 2$. Since all members of K have even X -length, it follows that $\ell_X(\alpha) \geq 2$ for all $\alpha \in K \setminus \{\mathbf{1}\}$, and hence that $\alpha \in \langle \{b \in B : \ell_X(b) \leq \ell_X(\alpha)\} \rangle$.

The two properties of being level and reduced are in some sense complementary. If $F = F(X)$ is a free group, $K \leq F$ is a subgroup, and B is a level basis of K , then the elements $\beta \in K$ can be written as a product of a possibly large number of $b \in B^\pm$, with the X -length of each such b limited by $\ell_X(\beta)$. On the other hand, if B is a reduced basis of K , then each $\beta \in K$ can be written as a product of at most $\ell_X(\beta)$ factors $b \in B^\pm$, where there is no limitation on the X -length of such b .

We now show that the existence of reduced bases of subgroups implies the Axiom of Choice. But first we need a short lemma involving the following choice principle.

AC $_{\geq n}$ (Axiom of Choice for sets of size $\geq n$): *Any family $\{X_i : i \in I\}$ of sets of size $\geq n$ – including infinite sets – has a choice function.*

Lemma 5.22. *If $0 < m < \omega$, then $\text{ZF} \vdash \text{AC}_{\geq m} \Rightarrow \text{AC}$.*

Proof.

Claim. Let $n, k > 0$ be integers. Then $\text{ZF} \vdash \text{AC}_{n^k} \Rightarrow \text{AC}_n$.

Let $\{X_i : i \in I\}$ be a family of n -element sets. Then $\{X_i^k : i \in I\}$ is a family of n^k -element sets. Using AC_{n^k} , there is a function f defined on I such that $f(i) = \langle f_1(i), \dots, f_k(i) \rangle \in X_i^k$ for each $i \in I$. f_1 is a choice function for the original family $\{X_i : i \in I\}$.

Now let $S = \{X_i : i \in I\}$ be a family of non-empty sets. For each n with $0 < n < m$, let $S^{(n)} = \{X_i : |X_i| = n\}$, and let $T = S \setminus \bigcup_{n < m} S^{(n)}$. By $\text{AC}_{\geq m}$ there is a choice function f for T . For each n satisfying $0 < n < m$, let $k(n)$ be the least integer satisfying $n^{k(n)} \geq m$. Then $\text{AC}_{\geq m} \Rightarrow \text{AC}_{n^{k(n)}} \Rightarrow \text{AC}_n$ by the claim, so there is a choice function f_n for $S^{(n)}$.

Hence $f \cup \bigcup_{n < m} f_n$ is a choice function for S . □

We are now ready to prove the main theorem of this section.

Theorem 5.23. $\text{ZF} \vdash \text{NS}_{\text{red}} \Rightarrow \text{AC}_{\geq 3}$.

Proof. Let $\{X_i : i \in I\}$ be a family of sets, each of size ≥ 3 . We may assume without loss of generality that the X_i are pairwise disjoint. Define $X = \bigcup_{i \in I} X_i$ and let $F = F(X)$ be the free group on X . Let

$$K = \bigcap \{\ker(\#_{X_i}) : i \in I\} \leq F,$$

where the $\#_{X_i}$ are defined as in section 5.4. K is a non-trivial normal subgroup of F .

By \mathbf{NS}_{red} there is a basis B for K such that $\ell_B(\beta) \leq \ell_X(\beta)$ for all $\beta \in K$. Hence any $\beta \in K$ may be written uniquely as a B -reduced word $b_1 \cdots b_n$ with $0 \leq n \leq \ell_X(\beta)$ and $b_1, \dots, b_n \in B^\pm$. In particular, $\ell_B(xy^{-1}) \leq \ell_X(xy^{-1}) = 2$ for any distinct $x, y \in X_i$ and any $i \in I$. So, when $x \neq y$, the only possible B -lengths for xy^{-1} are 1 and 2. Note that $\ell_B(xy^{-1}) = 1$ means that either xy^{-1} or its inverse is in B .

From now on we will work in an arbitrary but fixed X_i , and we will show how to pick a single element of X_i without making any choices.

Definition. Regard X_i as the vertex set of a complete undirected graph. With every edge connecting $x \in X_i$ to $y \in X_i$ we associate the *length* $\ell_B(xy^{-1}) \in \{1, 2\}$. As $yx^{-1} = (xy^{-1})^{-1}$, the length does not depend on the ordering of x and y . Edges of length 1 are *short*, and edges of length 2 are *long*.

Since B is an independent set, there can't be any cycles consisting of short edges (we call this a *short circuit*). In particular, every triangle must have at least one long edge. Let

$$Y_i = \{x \in X_i : \text{there is a long edge with endpoint } x\}.$$

Note first that $Y_i \neq \emptyset$ because $|X_i| \geq 3$ and every triangle has a long edge. We now define a representative function $f_i : Y_i \rightarrow K$. Let $y \in Y_i$. Pick any $x \in X_i$ connected to y by a long edge, and write $yx^{-1} = b_1 b_2$, where $b_1, b_2 \in B^\pm$. Then $f_i(y)$ is defined to be

$$f_i(y) = b_1 \in K.$$

At first sight, it seems that we made a choice in picking an arbitrary $x \in X_i$ connected to y by a long edge. However, no choice is made if the value of $f_i(y)$ does not depend

on the chosen x . We will show that this is the case by using the fact that B is reduced to enforce suitable cancellation of B -letters.

Claim. $f_i : Y_i \rightarrow K$ is a well-defined function.

Let $y \in Y_i$, and let $x_1, x_2 \in X_i$ be connected to y by long edges. We must show that the value of $f_i(y)$ is the same for x_1 and x_2 . Write

$$\begin{aligned} yx_1^{-1} &= b_1b_2, \\ yx_2^{-1} &= c_1c_2, \end{aligned}$$

where $b_1, b_2, c_1, c_2 \in B^\pm$. As B is reduced with respect to X , $\ell_B(x_1x_2^{-1}) \leq \ell_X(x_1x_2^{-1}) = 2$, so that

$$\ell_B(b_2^{-1}b_1^{-1}c_1c_2) = \ell_B(x_1y^{-1} \cdot yx_2^{-1}) \leq 2.$$

It follows that $b_1^{-1}c_1 = \mathbf{1}$, i.e. that $b_1 = c_1$. Hence the value of $f_i(y)$ does not depend on the choice of vertex connected to y by a long edge.

Claim. If $y_1, y_2 \in Y_i$ are connected by a long edge, then $f_i(y_1)^{-1}y_1 = f_i(y_2)^{-1}y_2$:

Write $y_1y_2^{-1} = b_1b_2$ as a reduced B -word with $b_1, b_2 \in B^\pm$. Then $f_i(y_1) = b_1$. As $y_2y_1^{-1} = b_2^{-1}b_1^{-1}$, $f_i(y_2) = b_2^{-1}$. Hence $f_i(y_1)f_i(y_2)^{-1} = y_1y_2^{-1}$, proving the claim.

As before, we define a function g_i to go with f_i :

$$g_i : Y_i \rightarrow F : y \mapsto f_i(y)^{-1}y.$$

The last claim says that $g_i(y_1) = g_i(y_2)$ if $y_1, y_2 \in Y_i$ are connected by a long edge. More generally, if $y_1, y_2 \in Y_i$ and there is a path $y_1, z_1, \dots, z_n, y_2$ consisting of long edges, then

$$g_i(y_1) = g_i(z_1) = \dots = g_i(z_n) = g_i(y_2).$$

Our aim will be to show that there is a path consisting of long edges between any two points $y_1, y_2 \in Y_i$, showing that $g_i : Y_i \rightarrow F$ is in fact constant. This constant value is then used to pick a single element of X_i .

Claim. If $y_1, y_2 \in Y_i$ are distinct, then there is a path from y_1 to y_2 which consists of at most 3 long edges.³

Since $y_1, y_2 \in Y_i$, there are $x_1, x_2 \in X_i$ such that

$$\ell_B(y_1 x_1^{-1}) = \ell_B(y_2 x_2^{-1}) = 2.$$

If $x_1 = y_2$ or $x_2 = y_1$, then y_1 and y_2 are connected by a long edge, and we are done.

If $x_1 = x_2$, then the path y_1, x_1, y_2 consists of two long edges, and we are done.

So assume that the four points y_1, y_2, x_1, x_2 are all distinct. Then there are 4 edges connecting a point in $\{x_1, y_1\}$ with a point in $\{x_2, y_2\}$ – see figure 5.3. They can't all be short, as this would give a short circuit x_1, x_2, y_1, y_2, x_1 . Hence one of these 4 edges must be long, proving the claim.

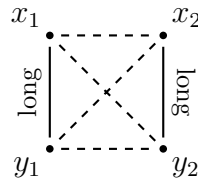


Figure 5.3:

We conclude that g_i is a constant function. Let its value be $\alpha_i = f_i(y)^{-1}y$. We check that α_i mentions letters from X_i :

$$\begin{aligned} \#_{X_i}(\alpha_i) &= \#_{X_i}(f_i(y)^{-1}y) \\ &= \#_{X_i}(y) - \#_{X_i}(f_i(y)) \\ &= 1 - 0, \end{aligned}$$

as $y \in Y_i \subseteq X_i$ and $f_i(y) \in K \leq \ker(\#_{X_i})$. Hence at least one X_i -letter appears in the X -reduced expression for α_i . Picking a the first X_i -letter appearing in the X -reduced expression for α , we have made the required choice. \square

³Thank you to Vu Dang for helping with this part.

Combine this theorem with lemma 5.22 to obtain the full result:

Corollary 5.24. $\text{ZF} \vdash \text{NS}_{\text{red}} \Rightarrow \text{AC}$.

As in section 5.4, the subgroup considered here was normal. So we actually proved a stronger result:

Theorem 5.25. *The statement*

If F is a free group and $K \leq F$ is a normal subgroup, then K has a reduced basis.

is equivalent to the Axiom of Choice.

Chapter 6

Free abelian groups

In the last chapter we were concerned with free groups and their subgroups. However, many of the questions considered in chapter 5 aren't special to free groups. As bases also make sense for, among others, free abelian groups, and vector spaces, one might try to find a class of structures in the model theoretic sense for which there is a notion of basis, i.e. a subset B such that every element of the structure can be written uniquely as a finite combination of elements of B . We can then consider the equivalent of the Nielsen–Schreier theorem in this general context. The translation of NS is:

If S is a structure with a basis and $T \leq S$ is a substructure, then T has a basis. (6.1)

However, this statement is not valid for all structures for which there is a notion of basis, as the following example shows.

Example 6.1.¹ Let F be the free monoid on one generator. Then F is isomorphic to $\langle \mathbb{N}, 0, + \rangle$ and has basis $\{1\}$. It is easy to verify that $K = \langle \mathbb{N} \setminus \{1\}, 0, + \rangle$ is a submonoid of F , with generating set $\{2, 3\}$. In fact, every generating set must contain 2 and 3. As $6 = 2 + 2 + 2 = 3 + 3$, we conclude that no generating set of K is a basis.

This example shows that it doesn't make sense to take a general statement such as (6.1) as an axiom of set theory. Based on the similarity with free groups, we will restrict our attention free abelian groups:

¹Thank you to Alex Kruckman for suggesting this example.

NS_{ab} (Nielsen–Schreier for abelian groups): *If F is a free abelian group and $K \leq F$ is a subgroup, then K is a free abelian group.*

Proposition 6.2. $ZFC \vdash NS_{ab}$.

Proof. A proof is available on page 41 of Lang’s classic book [30]. □

In section 6.1 we show that the abelian version of the Nielsen–Schreier theorem implies the Axiom of Choice for 2-element sets. The proof uses the representative functions introduced in section 5.4.

This implication is shown to be strict in section 6.2, where we prove that the Boolean Prime Ideal Theorem doesn’t imply the abelian version of the Nielsen–Schreier theorem. This is achieved with the same model as in section 5.5.

In section 6.3 we extend the representative functions introduced in section 6.1 to families of non-empty finite sets, and we discuss potential applications to vector spaces.

6.1 Abelian Nielsen–Schreier implies AC_2

In this section, we show that NS_{ab} implies AC_2 , the Axiom of Choice for families of 2-element sets. This shows that NS_{ab} can’t be proved entirely without the Axiom of Choice. The idea of the proof is similar to that of lemma 5.12. However, the definition of the representative function $f_y(x_i)$ as the ‘first half’ of $x_i x_{i+1}^{-1}$ cannot be translated, and picking the first y -letter in α_y is impossible. Both of these issues can be resolved in the commutative setting when working with a family of 2-element sets.

Before proceeding to the proof, we must translate the counting homomorphisms from section 5.4 to free abelian groups. Let Y be a family of pairwise disjoint 2-element sets. For the rest of this section we define $X = \bigcup Y$, and let $F = FA(X)$ be the free abelian group with basis X .

Definition 6.3. The counting functions $\#_y : F \rightarrow \mathbb{Z}$ are defined by

$$\#_y(n_1x_1 + \dots + n_kx_k) = \sum_{i:x_i \in y} n_i.$$

It is easy to check that the $\#_y$ are group homomorphisms from F to the additive group of integers. For the remainder of this section we fix a subgroup

$$K = \bigcap \{\ker(\#_y) : y \in Y\}$$

of F . By NS_{ab} there is a basis B for K . This allows us to define the positive and negative parts of elements of K :

Definition 6.4. Let $\beta \in K$ and write it in terms of the basis B as $\beta = \sum n_i b_i$, where the $b_i \in B$ are distinct and the $n_i \in \mathbb{Z}$ are non-zero. We define the *positive* and *negative parts of β with respect to B* as

$$\begin{aligned} \mathbf{p}(\beta) &= \sum_{i:n_i>0} n_i b_i, \\ \mathbf{n}(\beta) &= \sum_{i:n_i<0} n_i b_i. \end{aligned}$$

Here are some basic properties of \mathbf{p} and \mathbf{n} :

1. For all $\beta \in K$, $\beta = \mathbf{p}(\beta) + \mathbf{n}(\beta)$.
2. Multiplication by -1 swaps positive and negative parts: $-\mathbf{n}(-\beta) = \mathbf{p}(\beta)$ and $-\mathbf{p}(-\beta) = \mathbf{n}(\beta)$ for all $\beta \in K$.
3. The functions $\mathbf{p}, \mathbf{n} : K \rightarrow K$ are *not* group homomorphisms: Pick any $b \in B$ and define $\beta_1 = -b$, $\beta_2 = 2b$. Then $\mathbf{p}(\beta_1 + \beta_2) = \mathbf{p}(b) = b$ while $\mathbf{p}(\beta_1) + \mathbf{p}(\beta_2) = 0 + 2b = 2b$. Similarly, $\mathbf{n}(\beta_1 + \beta_2) \neq \mathbf{n}(\beta_1) + \mathbf{n}(\beta_2)$.

We have now defined all of the tools necessary to prove our next result.

Proposition 6.5. $\text{ZF} \vdash \text{NS}_{\text{ab}} \Rightarrow \text{AC}_2$

Proof. Recall that Y is a family of pairwise disjoint 2-element sets. Fix a member $y \in Y$. We will find a way of picking one of its elements without making any choices.

Write $y = \{x_0, x_1\}$. After stipulating that $i \equiv j \pmod{2} \Rightarrow x_i = x_j$, it makes sense to talk about points $x_i \in y$, where $i \in \mathbb{Z}$. This convention will improve readability later in the proof.

Now define the representative function f_y by

$$f_y : y \rightarrow K : x_i \mapsto \mathfrak{p}(x_i - x_{i+1}).$$

On a superficial intuitive level, it makes sense to associate x_i with the positive part of $x_i - x_{i+1}$ and $-x_{i+1}$ with the negative part of $x_i - x_{i+1}$. Amazingly, this definition works. As usual, f_y comes with its companion function g_y , defined by

$$g_y : y \rightarrow F : x \mapsto x - f_y(x).$$

f_y exhibits the good behaviour that we have come to expect from it:

$$\begin{aligned} f_y(x_i) - f_y(x_{i+1}) &= \mathfrak{p}(x_i - x_{i+1}) - \mathfrak{p}(x_{i+1} - x_{i+2}) \\ &= \mathfrak{p}(x_i - x_{i+1}) + \mathfrak{n}(x_{i+2} - x_{i+1}) \\ &= \mathfrak{p}(x_i - x_{i+1}) + \mathfrak{n}(x_i - x_{i+1}) \\ &= x_i - x_{i+1} \end{aligned}$$

Hence $g_y(x_0) = g_y(x_1)$ and g_y is a constant function. Let α_y be the single element of its image. Then

$$\begin{aligned} \#_y(\alpha_y) &= \#_y(x_0 - f_y(x_0)) \\ &= \#_y(x_0) - \#_y(f_y(x_0)) && (\#_y \text{ is a homomorphism}) \\ &= 1 && (x_0 \in y \text{ and } f_y(x_0) \in K \leq \ker(\#_y)) \end{aligned}$$

So, when writing α_y as a \mathbb{Z} -linear combination of basis elements $x \in X$, the coefficients of $x_0 \in y$ and $x_1 \in y$ cannot be equal. For if they were, they would both have to be $1/2$. An element of y is chosen by picking the member with the larger coefficient in α_y . \square

6.2 The implication is strict

Let \mathfrak{M} be the Dawson–Howard model described in section 2.3. We saw in corollary 5.16 that

$$\mathfrak{M} \models \text{BPIT} \wedge \neg \text{NS}.$$

In this section, we show that $\mathfrak{M} \models \neg \text{NS}_{\text{ab}}$. In particular, this means that, just like NS , NS_{ab} does not follow from BPIT , and that the implication $\text{ZF} \vdash \text{NS}_{\text{ab}} \Rightarrow \text{AC}_2$ cannot be reversed.

In order to prove the failure of NS_{ab} in the Dawson–Howard model, let $F = \text{FA}(A)$ be the free abelian group on A , the set of atoms in \mathfrak{M} . Define the usual subgroup

$$K = \bigcap \{\ker(\#_{A_i}) : i < \omega\} \leq F,$$

where the counting functions $\#_{A_i}$ are defined in section 6.1. If $\mathfrak{M} \models \text{NS}_{\text{ab}}$, then K has a basis B with finite support $E \subseteq A$. We will derive a contradiction. Recall definition 3.6, where we defined the set of A -components of $\alpha = n_1 a_1 + \dots + n_k a_k$, where $a_1, \dots, a_k \in A$ are distinct and $n_1, \dots, n_k \in \mathbb{Z} \setminus \{0\}$, to be $\mathcal{C}_A(\alpha) = \{a_1, \dots, a_k\}$.

Definition 6.6. If β is any element of the subgroup K , write $\beta = n_1 b_1 + \dots + n_k b_k$, where $b_1, \dots, b_k \in B$ are distinct and $n_1, \dots, n_k \in \mathbb{Z} \setminus \{0\}$. The set of A -components of β via B is $\mathcal{C}_A^B(\beta) = \bigcup_{i=1}^k \mathcal{C}_A(b_i)$.

Example 6.7. Let $i < \omega$, let $a, b, c, d \in A_i$ be distinct, and suppose that $\{a - b + c - d, c - d\} \subseteq B$. Defining $\beta = a - b \in K$, we see immediately that $\mathcal{C}_A(\beta) = \{a, b\}$. Moreover, since $\beta = (a - b + c - d) - (c - d)$ in terms of B , $\mathcal{C}_A^B(\beta) = \{a, b, c, d\}$.

Note that the sets $\mathcal{C}_A(\alpha)$ and $\mathcal{C}_A^B(\beta)$ are always finite, whatever the choice of $\alpha \in F$ and $\beta \in K$. Moreover, $(\forall \beta \in K) \mathcal{C}_A(\beta) \subseteq \mathcal{C}_A^B(\beta)$. As example 6.7 shows, this inclusion may be strict.

We now describe the ideas behind the proof. Our aim is to find $\beta \in K$ which can be expressed as a \mathbb{Z} -linear combination of elements of B in two different ways, giving the required contradiction. We will find an element $\beta = a_1 - a_2$ of K such that the set of

A -components of β contains a point $a \notin E \cup \{a_1, a_2\}$ (where E is the support of B). There are permutations of A which move a while at the same time fixing $E \cup \{a_1, a_2\}$. Such permutations fix β , but they don't fix its B -components. This gives two different B -expressions for β .

Having seen the strategy of the proof, we are now ready to prove some lemmas before moving on to the main theorem.

Lemma 6.8. *Let $\beta \in K$ and $j < \omega$ be arbitrary. Then $|\mathcal{C}_A(\beta) \cap A_j|$ is either 0 or ≥ 2 .*

Proof. Suppose there is $\beta \in K$ and $j < \omega$ with $|\mathcal{C}_A(\beta) \cap A_j| = 1$. Write $\beta = n_1 a_1 + \dots + n_k a_k$, where $a_1, \dots, a_k \in A$ are distinct and $n_1, \dots, n_k \in \mathbb{Z} \setminus \{0\}$. After reordering if necessary, $a_1 \in A_j$ and $a_2, \dots, a_k \notin A_j$. It follows that $\#_{A_j}(\beta) = n_1 \neq 0$, contradicting $\beta \in K \leq \ker(\#_{A_j})$. \square

Lemma 6.9. *There are $a_1, a_2 \in A$ with $a_1 - a_2 \in K$ and $\mathcal{C}_A^B(a_1 - a_2) \not\subseteq E \cup \{a_1, a_2\}$.*

Proof. Let $j < \omega$ be such that $E \cap A_j = \emptyset$, and let $a_1, a_2, a_3 \in A_j$ be arbitrary and distinct. (In particular, $a_1, a_2, a_3 \notin E$). If $\mathcal{C}_A^B(a_1 - a_3) \not\subseteq E \cup \{a_1, a_3\}$ or $\mathcal{C}_A^B(a_2 - a_3) \not\subseteq E \cup \{a_2, a_3\}$, then we are done. So assume that $\mathcal{C}_A^B(a_1 - a_3) \subseteq E \cup \{a_1, a_3\}$ and $\mathcal{C}_A^B(a_2 - a_3) \subseteq E \cup \{a_2, a_3\}$. Write

$$a_1 - a_3 = n_1 b_1 + \dots + n_k b_k \tag{6.2}$$

$$a_2 - a_3 = n'_1 b'_1 + \dots + n'_{k'} b'_{k'}, \tag{6.3}$$

where the $b_i \in B$ are distinct, the $b'_i \in B$ are distinct, and $n_i, n'_i \in \mathbb{Z} \setminus \{0\}$. Since $E \cap A_j = \emptyset$,

$$\mathcal{C}_A^B(a_1 - a_3) \subseteq E \cup \{a_1, a_3\}$$

implies that

$$\mathcal{C}_A^B(a_1 - a_3) \cap A_j \subseteq \{a_1, a_3\}.$$

This gives

$$\mathcal{C}_A(b_i) \cap A_j \subseteq \{a_1, a_3\} \text{ for } i = 1, \dots, k.$$

By lemma 6.8, $\mathcal{C}_A(b_i) \cap A_j$ is either \emptyset or $\{a_1, a_3\}$ for each $i = 1, \dots, k$. In other words, the b_i either mention neither a_1 nor a_3 , or they mention both. Since the left-hand side of (6.2) mentions a_1 and a_3 , at least one of the b_i mentions both. By rearranging the sum, we may assume that this is b_1 .

Subtracting (6.3) from (6.2), we obtain

$$a_1 - a_2 = n_1 b_1 + \dots + n_k b_k - (n'_1 b'_1 + \dots + n'_{k'} b'_{k'}). \quad (6.4)$$

Since $\mathcal{C}_A^B(a_2 - a_3) \subseteq E \cup \{a_2, a_3\}$, b_1 isn't equal to any of $b'_1, \dots, b'_{k'}$. Hence it doesn't cancel out when reducing the right-hand side of (6.4) with respect to B . So $a_3 \in \mathcal{C}_A(b_1) \subseteq \mathcal{C}_A^B(a_1 - a_2)$, proving that $\mathcal{C}_A(a_1 - a_2) \not\subseteq E \cup \{a_1, a_2\}$, as required. \square

Theorem 6.10. $\mathfrak{M} \models \neg \text{NS}_{\text{ab}}$.

Proof. By lemma 6.9, let $a_1, a_2 \in A$ be such that $\beta = a_1 - a_2 \in K$ and $\mathcal{C}_A^B(\beta) \not\subseteq E \cup \{a_1, a_2\}$.

Write $\beta = n_1 b_1 + \dots + n_k b_k$, where $n_1, \dots, n_k \in \mathbb{Z} \setminus \{0\}$ and $b_1, \dots, b_k \in B$ are distinct. By reordering the summands, we may assume that $\mathcal{C}_A(b_1) \not\subseteq E \cup \{a_1, a_2\}$. Let $a \in \mathcal{C}_A(b_1) \setminus (E \cup \{a_1, a_2\})$. Since $\{\pi(a) : \pi \in \text{fix}(E \cup \{a_1, a_2\})\}$ is infinite and $\mathcal{C}_A^B(\beta)$ is finite, there is $\pi \in \text{fix}(E \cup \{a_1, a_2\})$ with $\pi(a) \notin \mathcal{C}_A^B(\beta)$. Now

$$\begin{aligned} n_1 b_1 + \dots + n_k b_k &= \beta \\ &= \pi(\beta) && \text{(as } \pi \in \text{fix}(\{a_1, a_2\})\text{)} \\ &= n_1 \pi(b_1) + \dots + n_k \pi(b_k), \end{aligned}$$

so

$$n_1 b_1 + \dots + n_k b_k - (n_1 \pi(b_1) + \dots + n_k \pi(b_k)) = 0. \quad (6.5)$$

We have arranged $\pi \in \text{fix}(E)$, so $\pi(b_1), \dots, \pi(b_k) \in B$. Moreover, the $\pi(b_i)$ are distinct, as the b_i were chosen to be distinct. By the choice of π , we have $\pi(a) \notin \mathcal{C}_A^B(\beta)$, which shows that $\pi(b_1) \notin \{b_1, \dots, b_k\}$. Hence at least the one summand $n_1 \pi(b_1)$ remains when reducing the left-hand side of equation (6.5) with respect to B . Since $n_1 \neq 0$, (6.5) is a non-trivial B -expression for 0, so that B is no basis after all. This is the required contradiction. \square

We saw in example 2.16 that $\neg\text{NS}$ is a transferable statement. A similar argument shows that $\neg\text{NS}_{\text{ab}}$ is also transferable. Thus:

Corollary 6.11. $\text{ZF} \not\vdash \text{BPIT} \Rightarrow \text{NS}_{\text{ab}}$

In particular, as $\text{BPIT} \Rightarrow \text{AC}_2$, this shows that the implication $\text{NS}_{\text{ab}} \Rightarrow \text{AC}_2$ is not reversible.

6.3 More on representative functions

In this section we do not prove any new results. Instead, we present work that might lead to stronger and more general results in the future. The foundations for this section were laid in section 6.1 where we deduced AC_2 from NS_{ab} by finding representative functions for sets of size 2. Here we will construct representative functions for sets of any finite size.

Recall the set-up from section 6.1: We start with a family Y of pairwise disjoint non-empty finite sets. Then we let $X = \bigcup Y$, $F = \text{FA}(X)$, and $K = \bigcap \{\ker(\#_y) : y \in Y\}$. Using NS_{ab} , we obtain a basis B for K .

As the general case is rather involved, we present the construction for a family 3-element sets first. This special case illustrates all of the main ideas needed for the full construction.

Example 6.12. Assume Y is a family of pairwise disjoint 3-element sets. Let $y \in Y$, and write it as $y = \{x_0, x_1, x_2\}$. We will use the indices 0, 1, 2 to distinguish the elements of y , but we will not use them to choose from among them, or to put them in a certain order. Define

$$\beta_0 = 2x_0 - x_1 - x_2,$$

$$\beta_1 = -x_0 + 2x_1 - x_2,$$

$$\beta_2 = -x_0 - x_1 + 2x_2.$$

Each β_i distinguishes x_i from the other elements of y by putting more weight on x_i . Inspired by their shape, we call such elements of a free abelian group *spikes*. Note that $\beta_0, \beta_1, \beta_2 \in K$ and $\beta_0 + \beta_1 + \beta_2 = 0$. The representative function $f_y : y \rightarrow K$ is given by

$$\begin{aligned} f_y(x_0) &= \mathbf{p}(\beta_0) - \mathbf{n}(\beta_1) - \mathbf{n}(\beta_2) \\ f_y(x_1) &= -\mathbf{n}(\beta_0) + \mathbf{p}(\beta_1) - \mathbf{n}(\beta_2) \\ f_y(x_2) &= -\mathbf{n}(\beta_0) - \mathbf{n}(\beta_1) + \mathbf{p}(\beta_2) \end{aligned}$$

Let us define the companion function to f_y by

$$g_y : y \rightarrow F : x_i \mapsto 3x_i - f_y(x_i).$$

Our aim is to use f_y to show that g_y is a constant function. For this purpose we will need the following equality:

$$\begin{aligned} 2f_y(x_0) - f_y(x_1) - f_y(x_2) &= (2\mathbf{p}(\beta_0) + \mathbf{n}(\beta_0) + \mathbf{n}(\beta_0)) + (-2\mathbf{n}(\beta_1) - \mathbf{p}(\beta_1) + \mathbf{n}(\beta_1)) + \\ &\quad (-2\mathbf{n}(\beta_2) + \mathbf{n}(\beta_2) - \mathbf{p}(\beta_2)) \\ &= 2\beta_0 - \beta_1 - \beta_2 \\ &= 3\beta_0 - (\beta_0 + \beta_1 + \beta_2) \\ &= 3\beta_0 \\ &= 3(2x_0 - x_1 - x_2). \end{aligned}$$

Similar calculations show that

$$\begin{aligned} -f_y(x_0) + 2f_y(x_1) - f_y(x_2) &= 3(-x_0 + 2x_1 - x_2) \text{ and} \\ -f_y(x_0) - f_y(x_1) + 2f_y(x_2) &= 3(-x_0 - x_1 + 2x_2). \end{aligned}$$

These three equalities are summarised by the following matrix equation:

$$\begin{pmatrix} 2 & -1 & -1 \\ -1 & 2 & -1 \\ -1 & -1 & 2 \end{pmatrix} \begin{pmatrix} g_y(x_0) \\ g_y(x_1) \\ g_y(x_2) \end{pmatrix} = 0.$$

By elementary linear algebra, it follows that $g_y(x_0) = g_y(x_1) = g_y(x_2)$, i.e. that g is a constant function, as desired.

Having seen this special case, it is straightforward to find a generalisation for any family Y of pairwise disjoint non-empty finite sets. Let $y \in Y$ be arbitrary, and suppose $|y| = n \geq 2$. Writing $y = \{x_0, \dots, x_{n-1}\}$, we define, for each $i = 0, \dots, n-1$ a spike

$$\beta_i = (n-1)x_i - \sum_{j \neq i} x_j,$$

a representative function

$$f_y : y \rightarrow K : x_i \mapsto \mathbf{p}(\beta_i) - \sum_{j \neq i} \mathbf{n}(\beta_j),$$

and a companion function

$$g_y : y \rightarrow F : x_i \mapsto nx_i - f_y(x_i).$$

Fix any $i \in \{0, \dots, n-1\}$. Then

$$\begin{aligned} (n-1)f_y(x_i) - \sum_{k \neq i} f_y(x_k) &= (n-1) \left(\mathbf{p}(\beta_i) - \sum_{j \neq i} \mathbf{n}(\beta_j) \right) - \sum_{k \neq i} \left(\mathbf{p}(\beta_k) - \sum_{l \neq k} \mathbf{n}(\beta_l) \right) \\ &= (n-1)\mathbf{p}(\beta_i) - \sum_{j \neq i} ((n-1)\mathbf{n}(\beta_j) + \mathbf{p}(\beta_j)) + \sum_{k \neq i} \sum_{l \neq k} \mathbf{n}(\beta_l) \end{aligned}$$

There are $n-1$ pairs $\langle k, l \rangle$ where $k \neq i$, and $l \neq k$, and $l = i$. So

$$= (n-1)(\mathbf{p}(\beta_i) + \mathbf{n}(\beta_i)) - \sum_{j \neq i} ((n-1)\mathbf{n}(\beta_j) + \mathbf{p}(\beta_j)) + \sum_{k \neq i} \sum_{l \neq i, k} \mathbf{n}(\beta_l)$$

For each $j \neq i$ there are $n - 2$ pairs $\langle k, l \rangle$ where $k \neq i$, and $l \neq i, k$, and $l = j$. So

$$\begin{aligned}
&= (n - 1)(\mathbf{p}(\beta_i) + \mathbf{n}(\beta_i)) - \sum_{j \neq i} ((n - 1)\mathbf{n}(\beta_j) + \mathbf{p}(\beta_j) - (n - 2)\mathbf{n}(\beta_j)) \\
&= (n - 1)(\mathbf{p}(\beta_i) + \mathbf{n}(\beta_i)) - \sum_{j \neq i} (\mathbf{p}(\beta_j) + \mathbf{n}(\beta_j)) \\
&= (n - 1)\beta_i - \sum_{j \neq i} \beta_j \\
&= n\beta_i - \sum_j \beta_j \\
&= n\beta_i \\
&= n \left((n - 1)x_i - \sum_{k \neq i} x_k \right).
\end{aligned}$$

In summary, we have $(n - 1)f_y(x_i) - \sum_{k \neq i} f_y(x_k) = n \left((n - 1)x_i - \sum_{k \neq i} x_k \right)$ for all $i = 0, \dots, n - 1$. As in the earlier example, this gives a matrix equation

$$\begin{pmatrix} n - 1 & -1 & \dots & -1 \\ -1 & n - 1 & \dots & -1 \\ \vdots & \vdots & \ddots & \vdots \\ -1 & -1 & \dots & n - 1 \end{pmatrix} \begin{pmatrix} g_y(x_0) \\ g_y(x_1) \\ \vdots \\ g_y(x_{n-1}) \end{pmatrix} = 0,$$

which in turn implies that g_y is a constant function by elementary linear algebra.

In order to pick a single element of y , our standard procedure is to let α_y be the constant value of g_y . Then $\#_y(\alpha_y) = \#_y(nx_0 - f_y(x_0)) = n \neq 0$ implies that α_y mentions letters from y . If we were dealing with free groups, we could choose an element of y by picking the first y -letter appearing in α_y . But in free abelian groups, it is no longer possible to use the ordering of letters to make a choice. Instead, we must distinguish the letters by their coefficients in α_y . If we could guarantee that the y -letters appearing in α_y don't all have the same coefficient, then \mathbf{AC}_{fin} could be deduced from \mathbf{NS}_{ab} .

The above construction of representative functions works for vector spaces over fields whose characteristic does not divide n . This might give a fresh point of view on statements of current interest, such as

$\mathbf{B}(F)$ (existence of bases): *Every F -vector space has a basis.*

Blass [1] showed that the Axiom of Choice follows from $(\forall F)\mathbf{B}(F)$. However, if we restrict our attention to $\mathbf{B}(F)$ for a particular field F , such as the two-element field \mathbb{F}_2 or the rationals \mathbb{Q} , then we obtain a weaker Choice principle. A list of open questions relating to this principle is given at the end of Howard and Tachtsis [20]. Among them are:

Question. *Is there a field F for which $\mathbf{B}(F)$ implies AC?*

Question. *Is there a field F for which $\mathbf{B}(F)$ does not imply AC?*

The literature only offers partial answers. Keremedis [26] showed that $\mathbf{B}(\mathbb{Q})$ implies that every infinite well-ordered set of two-element sets has an infinite subset with a choice function. Later, Howard [18] proved that $\mathbf{B}(\mathbb{F}_2)$ implies that every well-ordered collection of two-element sets has a choice function. This was improved by Morillon [33], who deduced \mathbf{AC}_2 from $\mathbf{B}(\mathbb{F}_2)$. (This is not stated explicitly, but it is implicit in the proofs.) The most recent paper in this field is Howard and Tachtsis [20]. They showed that, for every field F in the Dawson–Howard model there is an F -vector space with no basis.

To end this chapter, I would like to formulate a conjecture. Its proof would be a significant improvement of the results published in the past few years. Representative functions seem to be a promising tool for attacking it.

Conjecture. *If F is a field of characteristic 0, then $\mathbf{ZF} \vdash \mathbf{B}(F) \Rightarrow \mathbf{AC}_{fin}$.*

Bibliography

- [1] A. Blass. Existence of bases implies the Axiom of Choice. *Contemporary Mathematics*, 31:31–33, 1984.
- [2] B. Bollobás. *Graph theory : an introductory course*. Springer Verlag, New York, 1979.
- [3] P. J. Cohen. The Independence of the Continuum Hypothesis. *Proc. Natl. Acad. Sci. USA*, 50(6):1143–1148, 1963.
- [4] P. J. Cohen. The Independence of the Continuum Hypothesis, II. *Proc. Natl. Acad. Sci. USA*, 51(1):105–110, 1964.
- [5] P. M. Cohn. *Classic algebra*. Wiley, 2000.
- [6] J. W. Dawson and P. Howard. Factorials of infinite cardinals. *Fundamenta Mathematicae*, 93:186–195, 1976.
- [7] C. Delhommé and M. Morillon. Spanning graphs and the Axiom of Choice. *Reports on Mathematical Logic*, 40:165–180, 2006.
- [8] H. Federer and B. Jonsson. Some properties of free groups. *Transactions of the American Mathematical Society*, 68:1–27, 1950.
- [9] M. Hall. *Combinatorial Theory*. Wiley Classics Library. Wiley, 1998.
- [10] P. Hall. On representatives of subsets. *Journal of the London Mathematical Society*, 10:26–30, 1935.

-
- [11] J. Halpern. Bases in vector spaces and the Axiom of Choice. *Proceedings of the American Mathematical Society*, 17:670–673, 1966.
- [12] J. Halpern. On a question of Tarski and a maximal theorem of Kurepa. *Pacific Journal of Mathematics*, 41:111–121, 1972.
- [13] A. Hatcher. *Algebraic Topology*. Cambridge University Press, 2002.
- [14] H. Herrlich. *Axiom of Choice*. Springer Verlag, Berlin, Heidelberg, 2006.
- [15] P. Howard. Limitations on the Fraenkel-Mostowski method of independence proofs. *Journal of Symbolic Logic*, 38:416–422, 1973.
- [16] P. Howard. Subgroups of a Free Group and the Axiom of Choice. *Journal of Symbolic Logic*, 50:458–467, 1985.
- [17] P. Howard. The existence of level sets in a free group implies the Axiom of Choice. *Zeitschrift für mathematische Logik und Grundlagen der Mathematik*, 33:315–316, 1987.
- [18] P. Howard. Bases, spanning sets, and the Axiom of Choice. *Mathematical Logic Quarterly*, 53(3):247–254, 2007.
- [19] P. Howard and J. E. Rubin. *Consequences of the Axiom of Choice*. American Mathematical Society, 1998.
- [20] P. Howard and E. Tachtsis. On vector spaces over specific fields without choice. *Mathematical Logic Quarterly*, 59(3):128–146, 2013.
- [21] T. Jech. *Set Theory: The Third Millennium Edition*. Springer, 2003.
- [22] T. Jech. *The Axiom of Choice*. Dover Publications, Inc., 2008.
- [23] T. Jech and A. Sochor. Applications of the θ -model. *Bulletin de l'Académie Polonaise des Sciences: Série des sciences mathématiques, astronomiques, et physiques*, 14:351–355, 1966.

- [24] T. Jech and A. Sochor. On θ -model of the set theory. *Bulletin de l'Académie Polonaise des Sciences: Série des sciences mathématiques, astronomiques, et physiques*, 14:297–303, 1966.
- [25] D. L. Johnson. *Presentations of Groups*. London Mathematical Society Student Texts. Cambridge University Press, 1997.
- [26] K. Keremedis. The Vector Space Kinna–Wagner Principle is Equivalent to the Axiom of Choice. *Mathematical Logic Quarterly*, 47(2):205–210, 2001.
- [27] P. Kleppmann. Generating sets of free groups and the axiom of choice. *Mathematical Logic Quarterly*, 60:239–241, 2014.
- [28] P. Kleppmann. Nielsen-Schreier and the Axiom of Choice. *Mathematical Logic Quarterly*, 2015. doi: 10.1002/malq.201400046.
- [29] P. Kleppmann. Nielsen-Schreier implies the finite Axiom of Choice, June 2015. arXiv:1506.03435v2 [math.LO].
- [30] S. Lang. *Algebra*. Graduate Texts in Mathematics. Springer, 3rd edition edition, 2005.
- [31] H. Läuchli. Auswahlaxiom in der Algebra. *Commentarii Mathematici Helvetici*, 37:1–18, 1962.
- [32] E. Mendelson. *Introduction to Mathematical Logic*. D. Van Nostrand Company, Inc., 1964.
- [33] M. Morillon. Linear forms and axioms of choice. *Commentationes Mathematicae Universitatis Carolinae*, 50(3):421–431, 2009.
- [34] J. Nielsen. Om Regning med ikke-kommutative Faktorer og dens Anvendelse i Gruppeteorien. *Matematisk Tidsskrift*, B:77–94, 1921.
- [35] D. Pincus. Zermelo-Fraenkel Consistency Results by Fraenkel-Mostowski Methods. *Journal of Symbolic Logic*, 37:721–743, 1972.

-
- [36] D. Pincus. Adding Dependent Choice. *Annals of Mathematical Logic*, 11:105–145, 1977.
- [37] D. Pincus. Adding Dependent Choice to the Prime Ideal Theorem. *Logic Colloquium*, 76:547–565, 1977.
- [38] L. Ribes and B. Steinberg. A Wreath Product Approach to Classical Subgroup Theorems, December 2008. arXiv:0812.0027v2 [math.GR].
- [39] O. Schreier. Die Untergruppen der freien Gruppen. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 5:161–183, 1927.
- [40] E. K. van Douwen. Horrors of topology without AC: A non-normal orderable space. *Proceedings of the American Mathematical Society*, 95(1):101–105, 1985.
- [41] E. Zermelo. Beweis, dass jede Menge wohlgeordnet werden kann. *Mathematische Annalen*, 59(4):514–516, 1904.